Observatoire du Monde Cybernétique

Lettre n°17 – Mai 2013

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

[AtlasInfo] Signature d'un protocole d'accord sur la cybersécurité entre la France et le Maroc

Le Maroc et la France ont conclu un protocole d'accord sur la cybersécurité visant à renforcer les compétences des autorités marocaines en sécurité des systèmes d'information. Il vise le développement sur le long terme de la coopération entre les deux pays, ainsi que le renforcement des compétences des autorités marocaines en sécurité des systèmes d'information via des échanges d'informations, d'expériences et d'expertises.

[Acus] L'Allemagne a organisé un exercice de cyberdéfense

L'Allemagne a organisé un exercice de cyberdéfense pour entraîner ses forces armées. Cet exercice a réuni le KSA (Strategic Reconnaissance Command) l'armée de terre, la marine et l'armée de l'air.

[TechWeek] Le gouvernement britannique investit 7,5 millions de livres dans deux centres de formation en cybersécurité

Le gouvernement britannique a annoncé que 7,5 millions de livres seraient injectés dans les centres de formation en cybersécurité d'Oxford et du Royal Holloway. Ces centres de recherche doctorale devraient permettre de compenser les lacunes de l'industrie nationale de la cybersécurité.

[01net] La Suisse organise un exercice de cyberdéfense

Tous les distributeurs de billets sont en panne, les sites web des banques inaccessibles, le réseau ferroviaire est gelé et une usine chimique a même explosé. Tout cela est l'œuvre des hackers Anonymous, qui souhaitent que la Suisse livre les noms de tous ses évadés fiscaux et qu'elle leur donne deux milliards de francs suisses. Ce scénario est celui d'un exercice stratégique de défense contre une cyberattaque massive menée contre la Suisse pour des raisons politiques, a annoncé un communiqué officiel. Ces exercices stratégiques de gestion de crise ont lieu tous les quatre ans et concernent tous les départements du gouvernement.

[TheHackerNews] Le fondateur de Liberty Reserve arrêté pour blanchiment d'argent

Arthur Budovsky Belanchuk, fondateur de Liberty Reserve, a été arrêté en Espagne dans le cadre d'une enquête menée par les autorités américaines et costaricaines. Le site a dans un premier temps été rendu inaccessible, ce qui pourrait indiquer une saisie gouvernementale et donc des pertes considérables pour ses utilisateurs. Budovsky est poursuivi par la justice du Costa Rica depuis 2011 pour blanchiment d'argent, et aurait financé Liberty Reserve avec l'argent généré par des sites pédopornographiques dits "professionnels", du trafic de drogue et du Black Market électronique. Le site était notamment réputé pour attirer divers criminels en quête de blanchiment.

[LeMonde] Le piratage du compte Twitter d'Associated Press fait plonger Wall Street

Mardi 23 avril à 13h07, l'agence de presse américaine Associated Press a vu son compte Twitter piraté annonçant qu'une explosion à la Maison Blanche a blessé Barack Obama. Entre 13h08 et 13h10, le Dow Jones perdait 136 Mds $ de capitalisation. Certains programmes logarithmiques des organismes financiers ont immédiatement suivi déclenchant une réaction en boule de neige. Le piratage a été revendiqué sur Twitter par la Syrian Electronic Army qui soutient le régime de syrien.

[Infosecurity] Les menaces sur les infrastructures critiques américaines en hausse de 68% en 2012

Selon le Département américain de la Sécurité Intérieure (DHS), les menaces portant sur les infrastructures critiques américaines sont en forte hausse. Le US-CERT a ainsi enregistré 190,000 incidents concernant des agences fédérales, des infrastructures critiques et des partenaires

industriels du DHS en 2012, soit une hausse de 68% par rapport à 2011.

[Reuters] Le directeur de la NSA au cœur d'une « cybertempête »

Le général Keith Alexander, directeur de la NSA et du U.S. Cyber Command, se retrouve au cœur d'un scandale national, accusé de vouloir espionner les citoyens américains.

L'installation par la NSA d'un gigantesque datacenter dans l'Utah et non le Maryland (base de la NSA) est à l'origine de ces spéculations, celui-ci servant supposément à capter et stocker des informations sur davantage d'américains. Alexander s'était souvent plaint de l'impossibilité d'agir, et notamment de l'ironie du fait que les Etats-Unis étaient certainement les seuls au monde à ne pas espionner les citoyens américains.

[Nasdaq] L'Iran attaque le secteur de l'énergie américain

Les pirates iraniens visent désormais les réseaux informatiques d'entreprises américaines du secteur de l'énergie. Ils auraient obtenu l'accès à des logiciels de contrôle leur permettant de manipuler les gazoducs et oléoducs.

Ce qui a alerté les autorités américaines, les dangers se révélant cette fois bien plus concrets que le cyberespionnage désormais courant.

[NZHeraldNews] Un dispositif d'espionnage américain aurait été testé sur le public néo-zélandais, à son insu

Le système d'espionnage ThinThread, développé par la NSA, aurait été testé entre 2000 et 2001 sur la population néo-zélandaise, sans son consentement.

La surveillance a été organisée avec la bienveillance et la participation des autorités néozélandaises. Les deux pays disposent d'une loi qui leur interdit de surveiller leurs propres citoyens. Une enquête a été ouverte.

[TribunedeGenève] Cybercriminalité : accord mondial sur le partage d'informations

Un accord de partage d'informations a été trouvé lors du 5e forum mondial des politiques de télécommunication et des technologies de l'information et de la communication. Cet « index global de cybersécurité » aura pour but de faciliter le partage d'informations liées aux crimes sur la toile entre les Etats membres.

[RIANovosti] Moscou et Washington lutteront ensemble contre la cybercriminalité

Vendredi 23 mai, le ministre russe de l'Intérieur Vladimir Kolokoltsev et le directeur du FBI Robert Muller ont annoncé qu'ils coopèreront dans la lutte contre la cybercriminalité à l'issue d'une rencontre avec à Washington.

[SCMagazine] La campagne de cyberespionnage "Operation Hangover" viendrait d'Inde

La société norvégienne Norman a découvert une campagne de cyberespionnage pouvant être originaire d'Inde, baptisée Opération Hangover (en raison de la grande occurrence de ce terme dans les bribes de texte analysées). Cette campagne a deux objectifs : récupérer des informations relevant de la sécurité nationale de divers pays pouvant intéresser l'Inde et réaliser de l'espionnage industriel. Les chercheurs de Norman suivent cette campagne depuis mars, campagne qui durerait depuis plusieurs années et ciblerait essentiellement le Pakistan et la Chine. Aucun lien formel n'a été constaté avec les autorités indiennes.

[PCINpact] L'Iran resserre la vis sur Internet à l'approche des élections

A l'approche des élections, l'Iran accroît son contrôle sur internet en en restreignant l'accès. Le trafic est beaucoup plus lent et certains services sont indisponibles. Skype, Gtalk et Oovoo (un service de discussion vidéo) sont ainsi inutilisables, après que des agents du gouvernement ont pris le

contrôle du Centre de Recherche de Technologie et d'Information. Ils auraient également tenté de filtrer des sites de Esfandiar Rahim Mashaei, le successeur désigné d'Ahmadinejad.

[PRNewswire] Le marché mondial de la cybersécurité atteindra 68 3400 Mds $ fin 2013

La société d'analyse britannique Visiongain vient de publier un rapport intitulé "Global Cyber Security Market 2013-2023" dans lequel elle estime que le marché mondial de la cybersécurité atteindra 68 3400 milliards de dollars à la fin de l'année 2013. Un chiffre qui s'explique par la demande croissante des gouvernements, du domaine militaire et du secteur privé.

[LeMondeInformatique] Trend Micro met à jour une opération mondiale de cyber espionnage

Les chercheurs en sécurité de Trend Micro ont découvert l'existence d'une opération de cyberespionnage toujours active, baptisée SafeNet.

Les attaques liées à cette campagne ont permis d'infecter des milliers d'ordinateurs appartenant à des entreprises, des gouvernements et d'autres organisations dans plus d'une centaine de pays à travers le monde : Inde, Etats-Unis, Chine, Pakistan, Philippines et Russie en tête. Les adresses IP qui servent à communiquer avec les serveurs de C&C ont été localisées dans plusieurs pays, mais essentiellement en Chine et à Hong Kong.

[CIOToday] Les Etats-Unis pourraient mener une cyberattaque contre les défenses aériennes syriennes

Les Etats-Unis envisageraient d'intervenir dans le conflit syrien en recourant aux attaques informatiques. Une cyberattaque contre les réseaux militaires de l'armée syrienne permettrait notamment d'aveugler ses défenses aériennes. C'est précisément pour cette raison que l'Air Force américaine s'est toujours intéressé aux capacités informatiques offensives : elles permettent de mettre hors-service les outils de surveillance et de défense d'un adversaire, sans l'attaquer physiquement.

[TheWashingtonPost] Un rapport confidentiel recense les designs de systèmes d'armes américains compromis par le cyberespionnage chinois

Le Pentagone a donné une liste des capacités militaires américaines apparemment compromises par une opération de cyberespionnage chinoise, dont des systèmes de missiles, d'avion de combat, d'hélicoptères, de navire ou même de F-35. Les cyberespions auraient eu accès aux plans de conception des systèmes, mais pas aux systèmes en tant que tels. Selon les analystes, ces accès permettraient à la Chine d'accélérer la modernisation de son armée en s'épargnant de nombreux investissements.

[CouncilonForeignRelations] Une feuille de route pour la coopération cyber Etats-Unis-Japon

Les gouvernements américains et japonais se sont rencontrés les 9 et 10 mai à Tokyo pour tenir le premier dialogue cyber entre leurs deux pays, près de deux ans après une première rencontre augurant un travail commun sur la cybersécurité. Les deux pays ont conjointement produit un document indiquant les sujets évoqués, de la cyberdéfense à la protection des infrastructures critiques, passant par le développement de normes et de règles de conduite dans le cyberespace. Aucune mention n'est cependant faite du cyberespionnage, alors que le Congrès américain vient d'accuser la Chine. Ceci peut être du à l'impossibilité pour les participants au dialogue - issus de 15 administrations différentes - de discuter de ce sujet sensible pour des raisons de confidentialité. La feuille de route liste des actions précises pour assurer la sécurité des infrastructures critiques des deux pays, présentant ainsi un point de départ pour cette coopération. En débutant par les infrastructures critiques, le document écrit le premier chapitre de la coopération cyber américano-japonaise, vouée à se développer et à servir de modèle de coopération bilatérale et de partage d'informations.

[ANSSI] L'ANSSI publie une note sur la sécurité des smartphones

L'usage des smartphones ou des tablettes est de plus en plus répandu en environnement professionnel. Les solutions de sécurisation actuelles sont quant à elles jugées peu efficaces pour assurer une protection correcte des données. Ce document a pour objectif de sensibiliser le lecteur aux principaux risques de sécurité des terminaux mobiles et d'indiquer des recommandations de sécurité génériques à appliquer pour les limiter.

[Agence Européenne de Défense] Un point sur les capacités de cyberdéfense des Etats membres

L'Agence européenne de défense a publié le 24 mai une étude dans laquelle elle réalise un inventaire des capacités de cyberdéfense des États membres de l'Union européenne.

[RAND] RAND publie un rapport sur les capacités des cyberattaques des Etats-Unis

L'institut de recherche sur la défense nationale de l'institution RAND (Research ANd Development) publie une étude intitulée « Brandishing Cyberattack Capabilities » consacrée à l'étude des capacités de cyberdéfense des Etats-Unis et leur doctrine d'emploi.

[SSI] Publication du deuxième volume de « Cyber Infrastructure Protection »

Le deuxième volume de l'ouvrage « Cyber Infrastructure Protection » a été publié par les presses universitaires de l'armée américaine. Ce volume traite entre autres des aspects économiques et sociaux de la cybersécurité, des cybercriminels et des infrastructures de diverses entités (administrations et entreprises).

[OCDE] L'OCDE propose une revue des méthodes de mesure de la valeur pécuniaire des données

Les données personnelles sont de plus en plus créatrices de valeur économique et sociale, mais c'est une valeur difficile à mesurer. L'OCDE publie un rapport qui examine les méthodes pouvant permettre d'estimer la valeur des données à caractère personnel.

[UKDefenceAcademy] La résilience stratégique dans la société du savoir mondialisé

L'académie de défense du Royaume-Uni a publié une étude intitulée « The Global Cyber Game - Archieving strategic resilience in the global knowledge society » dans lequel elle présente une synthèse de ses analyses stratégiques du cyberespace.

[StrategicStudiesQuaterly] Ordre international et coopération dans le cyberespace

Strategic Studies Quaterly publie un article qui examine le rôle des grandes puissances mondiales dans la mise en place d'un ordre international et la coopération dans le cyberespace.

[McKinseyGlobalInstitute] Les technologies disruptives et leur impact sur les sociétés, le business et l'économie

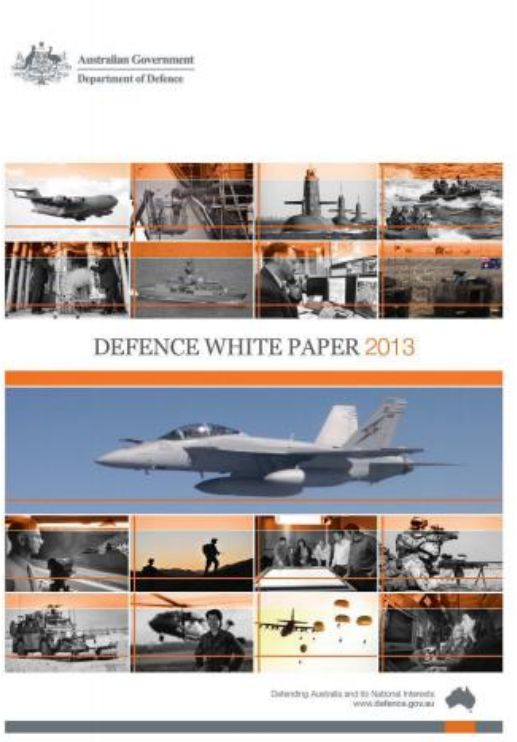
L'institut McKinsley publie un rapport intitulé "Disruptives technologies : Advances that will transform life, business, and the global economy" dans lequel il tente de mettre en avant les impacts de ces technologies sur la société, les entreprises et l'économie mondiale.

[IPCommission] Les Etats-Unis conseillent aux entreprises d'attaquer leurs attaquants

Considérant que la législation actuelle est inefficace, la Commission américaine contre le vol de la propriété intellectuelle invite les entreprises du secteur privé à faire se faire justice : ces entreprises devraient pouvoir *« activement récupérer leurs informations volées du réseau informatique de l'attaquant puis le rendre indisponible voire le détruire sans aucune limitation »*.

Le livre blanc de la défense australienne

Selon les résultats d'une étude publiée au mois de février 2013, une entreprise australienne sur cinq aurait subit au cours de l'année une cyberattaque, et ce, quel que soit le domaine d'activité (énergie, défense, banque, industrie). Déjà en 2011, afin de protéger leurs infrastructures critiques, l'Australie et les Etats-Unis s'unissaient en échangeant des informations et en organisant des exercices communs[1] au sein du traité ANZUS (*Australia, New Zealand, United States Security Treaty*).



En 2012, le gouvernement australien avait également adopté une loi[2] qui autorise les autorités à collecter et à conserver les données enregistrées par les internautes australiens dans le but de lutter contre la cybercriminalité, permettant ainsi une identification plus rapide des cybercriminels.

C'est dans le droit fil de ces initiatives que l'Australie place les problématiques touchant au cyberespace à la tête de ses priorités dans le Livre blanc sur la défense, tout comme l'a fait la France dans son document analogue récemment publié.

Un nouveau centre de cybersécurité

L'ouverture d'un centre des opérations de cybersécurité à Canberra, qui avait été annoncé par Julia Gillard[3] suite à l'étude de février 2013 précédemment évoquée, fait partie intégrante de la stratégie australienne en matière de cybersécurité exposée dans ce Livre blanc.

L'Australian Cyber Security Centre (ACSC), qui ouvrira ses portes à la fin de l'année, aura pour mission de contenir la cybercriminalité et protéger le pays contre les cyberattaques. Il mettra en relation plusieurs organismes publics concernés par la cybersécurité et travaillera en collaboration avec des partenaires industriels et des opérateurs d'infrastructures critiques.

Ce nouveau centre viendra en complément de l'actuel Cyber Security Operations Centre (CSOC) créé en 2009 dans le cadre de la stratégie de cybersécurité de l'Australie[4]. Il permettra de renforcer les partenariats publics-privés et regroupera des experts de plusieurs agences publiques concernées (Défense,

[1] http://www.theaustralian.com.au/australian-it/cyber-co-operation-added-to-australia-us-defence-treaty/story-e6frgakx-1226137837831
[2] http://www.watoday.com.au/opinion/political-news/authorities-gain-power-to-collect-australians--internet-records-20120822-24m03.html
[3] http://www.theinformationdaily.com/2013/02/12/australian-cyber-security-centre-to-open-in-the-capital-this-year
[4] http://www.couriermail.com.au/news/breaking-news/australia-and-uk-sign-defence-treaty/story-e6freono-1226556750604

Renseignements, Police fédérale, Commission du crime). Sa direction sera d'ailleurs assurée par le département de la défense puisque 95% de son personnel en seront issus.[5]

Le renforcement des partenariats extérieurs

L'Australie compte également renforcer ses partenariats existants en matière de cybersécurité. Le pays estime en effet que la position stratégique qu'il occupera en la matière dépendra nécessairement de son poids dans le cyberespace, les partenaires stratégiques jouant alors un rôle décisif. L'Australie s'inscrit ainsi dans sa stratégie de défense traditionnelle, qui a toujours été basée sur les partenariats. C'est dans cette optique que l'Australie et le Royaume-Uni ont signé un accord en matière de cyberdéfense au début de l'année 2013[6] basé sur le partage d'informations mais aussi de technologies.

Un cadre législatif international jugé pertinent

Contrairement à certains pays qui estiment que le droit international n'est en l'état pas adapté pour assurer une cybersécurité mondiale, l'Australie considère au contraire que le cadre législatif existant est applicable au cyberespace et souhaite devenir un acteur dans l'application de ces dispositions au niveau mondial, le pays étant signataire de la convention de Budapest sur la cybercriminalité de 2001 depuis le 30 novembre 2012[7].

L'investissement technologique, une condition nécessaire à la résilience

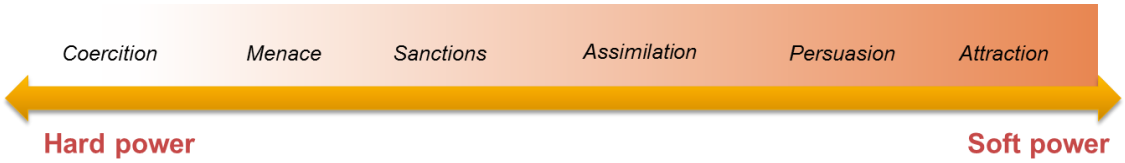
Le gouvernement australien, conscient de l'évolution rapide des cybermenaces, investira continuellement dans les technologies et les capacités d'analyse en matière de cybersécurité pour atteindre une résilience. Le but est de faire de l'Australie une cible difficile à atteindre. Pour ce faire, l'Australie souhaite favoriser les partenariats public-privé dans la R&D et établir une relation de confiance entre les autorités et les entreprises.

[5] http://www.zdnet.com/australian-cyber-security-centre-will-be-95-defence-staffed-7000011208/
[6] http://www.couriermail.com.au/news/breaking-news/australia-and-uk-sign-defence-treaty/story-e6freono-1226556750604
[7] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG

Cyberespace et puissance

Dans les relations internationales, la puissance est traditionnellement fonction des ressources dont disposent les acteurs traditionnels que sont les Etats. D'où la formule de Ray Cline, ancien numéro 2 de la CIA pendant la guerre froide, qui s'appuyait sur le produit de différentes ressources (population, territoire, économie, force militaire…) par la stratégie et la volonté. Pour tenir compte du changement de contexte (affaiblissement des Etats-nation, complexification des échanges internationaux…), Joseph Nye a ensuite proposé une autre définition : la puissance est schématiquement la capacité à obtenir des comportements voulus chez les autres grâce à trois options : la coercition (pouvoir militaire), l'assimilation (pouvoir économique) et l'attraction (pouvoir culturel). Cette conception, plus large, permet d'établir une échelle de puissance allant du « hard power » au « soft power ».

Echelle de la puissance selon Joseph Nye



Mais quid de la puissance à l'ère cyber ?

Premier constat : l'émergence du cyberespace, en accélérant la dilution de la puissance étatique, a contribué à modifier la façon dont les Etats expriment leur puissance. « *Les caractéristiques du cyberespace ont réduit certains des critères de pouvoir différenciant entre acteurs, et fournissent donc un bon exemple de la dilution de la puissance, typique du contexte politique de ce siècle. Les plus grandes puissances sont incapables de dominer ce domaine autant qu'elles le font dans d'autres domaines comme l'air ou la mer* », explique Joseph Nye dans un article de 2010 intitulé « cyber power »[8]. La puissance informationnelle compte finalement tout autant que la force matérielle. Elle la domine même parfois, l'intensité informationnelle permettant de réduire le besoin de force matérielle nécessaire pour parvenir à l'effet recherché. Le « soft power » prend donc le pas sur le « hard power ».

Deuxième constat : si l'on peut parler de « puissance cyber », c'est véritablement la combinaison intelligente des deux (le « smart power » selon Nye) qui est génératrice de puissance sur le long terme. Ne serait-ce qu'en raison des niveaux de développement très différents des Etats. D'où l'intérêt de « l'échiquier cyber » proposé par la Defence Academy du Royaume-Uni dans une étude intitulée « The global cyber game »[9]. En abscisse : les trois couches du cyberespace (physique, logique et cognitive), c'est-à-dire l'environnement. En ordonnée : les trois types de puissance distingués, c'est-à-dire les moyens d'action, lesquels vont de la coercition à la coopération (puissance « intégratrice »).

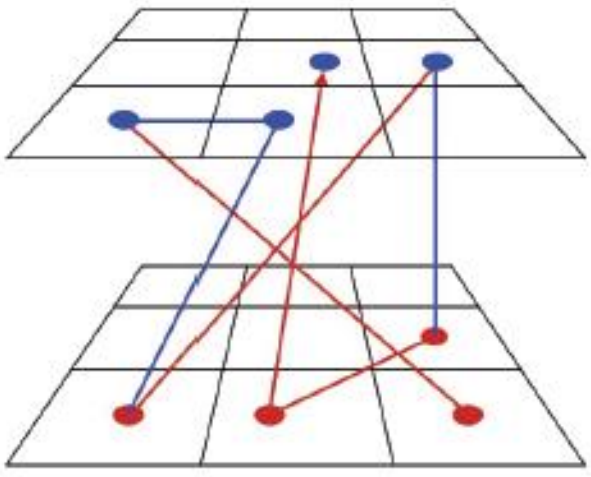
[8] http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf
[9] http://www.da.mod.uk/publications/library/technology/20130508-Cyber_report_final_U.pdf/view

L'échiquier cyber proposé la Defence Academy britannique

	Connection Physical data handling domain	**Computation** Virtual interactivity domain	**Cognition** Knowledge and meaning domain	
Cooperation Integrative social power (Infopolitik)	7	8	9	*Power as positive social reciprocity*
Co-option Economic exchange power	4	5	6	*Power as balanced social reciprocity*
Coercion Destructive hard power (Realpolitik)	1	2	3	*Power as negative social reciprocity*
	Information hardware	*Information software*	*Information wetware*	

L'intérêt de cette grille est triple. Elle permet tout d'abord d'avoir une vision globale de l'échiquier « cyber » et de toute la gamme des moyens susceptibles d'y agir. Elle permet également d'évaluer les capacités d'action d'un pays dans ou à travers le cyberespace. Les Etats-Unis sont ainsi dominants dans la plupart des cases de l'échiquier, même si leur domination est fortement contestée sur plusieurs points. Elle permet enfin de modéliser des conflits dans le cyberespace, comme dans l'exemple ci-dessous. Dans ce schéma, l'échiquier inférieur représente le type de puissance ou de moyen utilisé tandis que l'échiquier supérieur représente l'environnement cible. Les actions américaines présumées figurent par ailleurs en bleu et les actions chinoises en rouge.

Modélisation de l'affrontement Etats-Unis / Iran dans le cyberespace



Le portail OMC
La nouvelle plateforme de la DAS

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

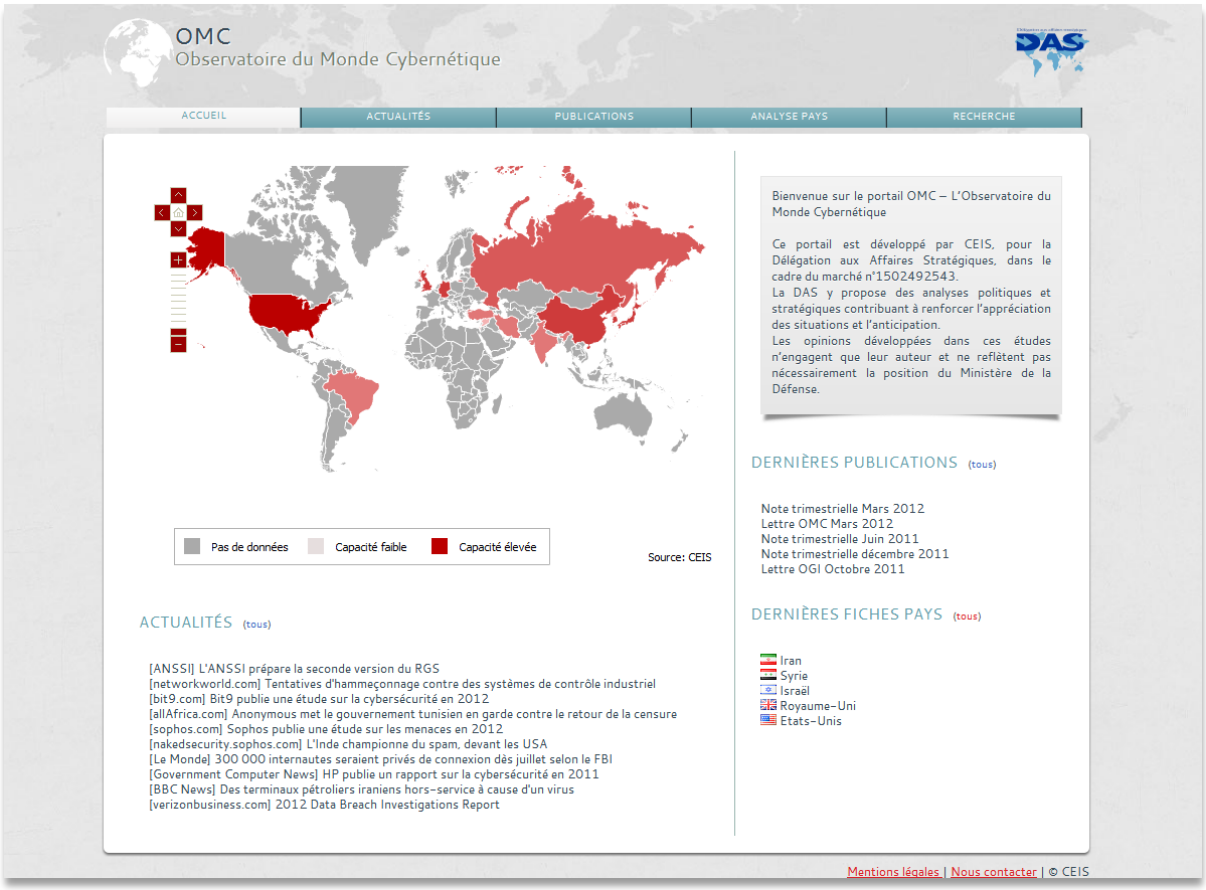


Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

Les frontières du cyberespace	Rennes	4 juin
SSTIC 2013	Rennes	5 – 7 juin
ACM Workshop on Information Hiding and Multimedia Security	Montpellier	17 – 19 juin
Hack in Paris	Paris	17 – 21 juin
Les Débats@Qualys	Paris	20 juin
La Nuit du Hack	Marne La Vallée	22 – 23 juin
Forum « Technology Against Crime / Technologie contre le crime » - TAC	Lyon	7 – 9 juillet
Technology Against Crime	Lyon	8 – 9 juillet
Cyber Intelligence Europe	Bruxelles	17 – 19 septembre
Les Assises de la Sécurité et des Systèmes d'Information	Monaco	2 – 5 octobre

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