Observatoire du Monde Cybernétique

Lettre n°12 – Décembre 2012

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

Actualités p. 2

- La France annonce sa participation au Centre de recherche de Cyberdéfense de l'OTAN.
- Le Parlement européen exige des mesures contre les restrictions d'accès à Internet.
- Les Etats-Unis démentent être à l'origine de la cyberattaque ayant récemment touché l'Elysée.
- Suite à la conférence de l'UIT à Dubaï, aucune modification substantielle ne sera apportée au traité de 1988.
- Retour sur CHAMP, un nouveau projet de cyberarme.
- L'Armée de l'air américaine publie les résultats de la compétition CyberPatriot.
- L'Agence spatiale japonaise piratée : des données stratégiques sur une fusée compromises.
- Des hackers de « Team GhostShell » revendiquent le piratage d'agences fédérales et d'industries américaines.
- L'opérateur d'électricité allemand, 50Hertz, a été victime d'une attaque par déni de service qui a, pendant cinq jours, rendu inopérantes ses communications Internet.
- La Darpa vérifie la sécurité des appareils électroniques de son personnel avec le programme baptisé « enquêtes et vérifications des firmwares et logiciels ».
- La NSA décernera un prix au meilleur article scientifique sur la cybersécurité.
- Blocage de site Internet : la Turquie sanctionnée par la CEDH.
- L'Iran annonce, puis dément, avoir déjoué une cyberattaque de type Stuxnet.
- La Mauritanie s'attaque à la cybercriminalité.

Publications p. 5

Régulation et législation p. 7

Le projet de règlement européen en matière de protection des données – vers une « souveraineté des données » à l'européenne ?

En présentant son projet de règlement relatif à l'encadrement et à la protection des données à caractère personnel, la Commission européenne est venue réaffirmer une tendance déjà bien enclenchée : l'Europe veut protéger les données de ses citoyens. Présenté le 25 janvier dernier, le texte vise à refondre et améliorer le cadre juridique posé par la directive datant de 1995 et jugée aujourd'hui dépassée. Derrière ce projet, transparait la volonté d'affirmer une véritable « souveraineté des données » à l'européenne.

Agenda p. 11

[Bruxelles2] La France va participer au Centre de recherche de Cyberdéfense de l'OTAN

La France a annoncé sa participation au Centre d'Excellence de Cyber Défense de l'OTAN, le CCD-COE, basé en Estonie. La participation française devrait consister en l'envoi de deux ou trois experts qui renforceront un effectif de 32 personnes à Tallinn. La France est le douzième Etat à y être représenté et rejoint ainsi l'Allemagne, l'Espagne, l'Estonie, la Hongrie, l'Italie, la Lituanie, la Lettonie, le Pays-Bas, la Pologne, la Slovaquie et les Etats-Unis.

[laquadrature.net] Le Parlement européen exige des mesures contre les restrictions d'accès à Internet

La Quadrature du Net relève que le Parlement européen a adopté, le 11 décembre, deux rapports faisant part de sa volonté de *« protéger et de promouvoir les droits et libertés sur Internet, notamment en ce qui concerne la neutralité du Net »*. Si la Quadrature salue l'adoption de ces deux rapports, elle rappelle que l'essentiel est de légiférer afin de rendre concrètes ces propositions. Le premier rapport porte *« sur une stratégie pour la liberté numérique dans la politique étrangère de l'Union »*. Le second portant sur *« l'achèvement du marché unique numérique »*, *« appelle la Commission à proposer une législation visant à assurer la neutralité du réseau »*, rappelle la Quadrature.

[Le Figaro] Les Etats-Unis démentent être à l'origine de la cyberattaque ayant touché l'Elysée

L'ambassade américaine à Paris a, dans un communiqué, *« réfuté catégoriquement »* les accusations relayées par L'Express selon lesquelles les Etats-Unis seraient à l'origine de la récente cyberattaque ayant ciblé l'Elysée. Selon le communiqué, ces accusations ne reposeraient pas sur des faits avérés.

[TheGuardian] Aucune modification des traités à la conférence de l'UIT à Dubaï

La conférence sur la régulation d'Internet qui a eu lieu à Dubaï du 3 au 14 décembre sous l'égide de l'Union Internationale des Télécoms (UIT) n'a finalement pas entraîné de modification du Traité de 1988. Les États-Unis, des pays européens et africains ont refusé d'accepter les modifications demandées par des pays tels que la Chine, la Russie et les Emirats Arabes Unis. Ces modifications auraient fait entrer Internet dans le domaine d'application du Traité des télécoms. Le chef de la délégation américaine résume ainsi sa position : *« Internet a apporté au monde des avantages économiques et sociaux inimaginables depuis 24 ans. Le tout sans régulation de l'ONU. Nous ne pouvons franchement soutenir un traité de l'UIT qui serait incohérent avec le modèle de gouvernance multipartite d'Internet. »*

[Securityaffairs] De nouvelles armes de cyberguerre : le projet CHAMP

De nouvelles cyberarmes sont régulièrement développées. L'une des plus récentes est la nouvelle génération de missile testée par Boeing, capable d'attaquer les systèmes informatiques d'un pays sans causer de perte de vies humaines. Ce projet, développé dans les laboratoires de recherche de l'armée de l'air américaine et baptisé « CHAMP », fonctionne comme une arme à énergie micro-ondes pour bloquer définitivement les ordinateurs ciblés. Mais le projet est loin d'être abouti : Quid de son impact environnemental ? Comment évaluer la puissance nécessaire ?

[AFA] L'Armée de l'air américaine publie les résultats de la compétition CyberPatriot

L'Association de l'Armée de l'air américaine a publié les résultats de la compétition CyberPatriot, un projet éducatif dirigé par l'association depuis 2008, et destiné aux étudiants souhaitant développer leurs compétences en matière de cybersécurité. La finale aura lieu en mars 2013, à Washington. 26 équipes sont encore en lice.

[Reseaux Telecoms] L'Agence spatiale japonaise piratée : les données stratégiques d'une fusée compromises

L'ordinateur d'un des chercheurs de l'Agence japonaise d'exploration spatiale a été piraté, et des informations sur le programme de fusée à longue

portée Epsilon auraient été subtilisées. Cette fuite d'informations inquiète particulièrement les autorités japonaises en raison de l'usage potentiellement militaire d'Epsilon. Une cyberattaque de moindre importance avait déjà affecté un ordinateur de l'Agence en juillet 2011.

[NextGov] Des hackers revendiquent le piratage d'agences fédérales et d'industries américaines

Un groupe de hackers baptisé « Team GhostShell » a publié des informations – dossiers privés, adresses e-mail et relevés de compte – initialement stockées sur des serveurs appartenant à des agences fédérales et des contractants de la défense américaine. L'objectif du collectif était d'attirer l'attention sur la liberté d'information sur Internet.

[EurActiv] L'opérateur allemand de l'électricité 50Hertz attaqué par DDoS

Un opérateur d'électricité allemand, 50Hertz, a été victime d'une attaque par déni de service (DDoS et Botnet) qui a, pendant cinq jours, rendu inopérantes ses communications Internet. La gestion du courant n'a pas été affectée. Si les adresses IP de provenance étaient russes et ukrainiennes, difficile de dire s'il s'agissait réellement de la source primaire de l'attaque.

[Darpa] La Darpa vérifie la sécurité des appareils électroniques de son personnel

La DARPA souhaite auditer la sécurité des appareils électroniques de ses membres. Cette annonce fait suite aux accusations portées par le Congrès américain contre les routeurs chinois. Le programme, baptisé *« enquêtes et vérifications sur les firmwares et logiciels »,* a débuté le 12 décembre par une réunion d'information et de réflexion.

[Nsa.gov] Prix du meilleur article scientifique sur la cybersécurité

Afin d'encourager la recherche et l'innovation en cybersécurité, la NSA lance un concours du meilleur article scientifique sur le sujet. Un panel d'experts (d'In-Q-Tel, du Naval Research Laboratory, du MIT, de Goldman Sachs ou encore de l'Université de Carnegie Mellon) examinera les candidatures et sélectionnera les finalistes qui verront leurs articles annoncés sur le site de la NSA. Le gagnant présentera son texte à un public d'experts en cybersécurité et au personnel du gouvernement américain. Le concours est ouvert au public et ne se limite pas aux citoyens américains.

[PC INpact] Blocage de site Internet : la Turquie sanctionnée par la CEDH

La Cour européenne des droits de l'Homme a récemment condamné la Turquie pour le blocage du portail « Google Sites ». La Cour sanctionne ici les dommages collatéraux engendrés par une décision de blocage de site abusif. En l'espèce, c'est tout le portail « Google Sites » qui a été bloqué, restreignant également l'accès à des sites légitimes, alors que seule une page présentant un contenu litigieux était en cause. Selon la Cour, « *la mesure en cause est constitutive d'une "ingérence d'autorités publiques'' dans le droit de l'intéressé à la liberté d'expression, dont fait partie intégrante la liberté de recevoir et de communiquer des informations ou des idées* ». Cette décision ne vise toutefois pas à interdire toute mesure de blocage, bien au contraire : le blocage de sites Internet est légal tant qu'il respecte certaines conditions que les juges n'ont pas manqué de préciser dans leur décision.

[ISNA, AFP et BFM] L'Iran annonce, puis dément, avoir déjoué une cyberattaque

Dans un communiqué traduit par l'AFP, l'agence de presse des étudiants iraniens (ISNA) rapporte que l'Iran aurait été victime d'un nouveau virus similaire à Stuxnet. Le malware aurait visé une centrale électrique de la province méridionale de Hormuzgan. Des hackers au service du gouvernement auraient freiné sa diffusion. Mais cette information a rapidement été démentie par des officiels iraniens dans un second communiqué. Selon le responsable de la défense civile iranienne, *« Lors de la conférence de presse,* [ils ont] *annoncé que* [qu'ils étaient] *prêts à parer à d'éventuelles attaques qui viseraient les installations de Hormuzgan, mais les agences* [de presse] *ont rapporté, à tort, que ces attaques avaient eu lieu et qu'elles avaient été déjouées ».*

[Magharebia] La Mauritanie s'attaque à la cybercriminalité

Nouakchott, capitale de la Mauritanie, a accueilli au mois de décembre deux conférences sur la cybercriminalité. Ces conférences réalisées en partenariat avec l'Union internationale des télécommunications (UIT) ont permis de traiter de deux sujets clés : la cybersécurité des réseaux mauritaniens et la législation antiterroriste. Cette dernière est en effet un sujet majeur, comme l'a rappelé le secrétaire général au ministère de la Justice mauritanien : *« La Mauritanie a démontré qu'elle en fait un axe prioritaire, à travers l'arsenal législatif dont elle s'est dotée, permettant la création d'un pôle judiciaire spécialisé ».* La conférence sur la cybersécurité a quant à elle été l'occasion de souligner l'importance de la sensibilisation et de l'accompagnement du développement technologique mauritanien.

[ENISA] L'ENISA publie son programme de travail pour l'année 2013

L'ENISA a publié son programme de travail pour l'année 2013. Celui-ci se divise en trois *working segments* : l'étude des risques et stratégies de mitigation (WS1), l'amélioration de la résilience à l'échelle pan-européenne (WS2) et la sécurisation des télécommunications (WS3). Le programme rappelle que l'Agence travaille à plusieurs niveaux avec toutes les parties concernées par la cybersécurité en Europe, des États au grand public en passant par les CERTs, les fournisseurs d'accès et les entreprises.

[Symantec] Symantec dévoile ses prévisions sécurité pour 2013

Comme tous les ans, Symantec publie ses prévisions sur les principales menaces en sécurité informatique pour 2013. Cette année, l'éditeur de solutions de sécurité place les cyberconflits en première position, estimant qu'ils constituent une menace majeure et qu'ils risquent de s'amplifier. Viennent ensuite les « ransomwares » ; l'intégrité des données ; l'usurpation d'identité via les objets connectés ; les fausses pages sur les réseaux sociaux ; les passerelles sur les réseaux sociaux d'entreprises ; les attaques visant le mobile et le cloud et, enfin, la publicité sur mobile.

[Kaspersky Lab] Les prévisions de Kaspersky pour 2013

Dans sa dernière étude, Kaspersky retrace à son tour les grandes tendances de l'année 2012 et tente de prévoir les principales menaces de l'année 2013. Le document souligne que le volume des attaques ciblées contre les entreprises ne fera que s'accroître ; il anticipe également la multiplication des attaques cybercriminelles contre les services cloud. Autre tendance : le hacktivisme prendra une part de plus en plus importante. Autres faits majeurs de cette année, les actes de "cyberguerre" commandités par des Etats qui devraient être de plus en plus nombreux. Les Etats seront également au devant de la scène avec le développement d'outils légaux de cybersurveillance. Enfin, la question de la confidentialité et du respect de la vie privée rythmera cette année 2013.

[Sophos] Sophos publie son Security Threat Report 2013

Dans son *Security Threat Report 2013*, Sophos souligne le rapport entre l'augmentation du nombre de systèmes d'exploitation et la croissance des menaces informatiques et rappelle que *« plus il y existe de plates-formes et de technologies, plus les risques d'attaque augmentent »*. A terme, les systèmes traditionnels de sécurité seront inefficaces. Enfin, le rapport indique que la Norvège possède le plus faible taux d'exposition aux malwares (1,81%), tandis que Hong Kong paraît le pays le plus risqué avec un taux de 23,5%.

[WatchGuard] Les prédictions de WatchGuard sur la sécurité informatique en 2013

Si la législation en matière de cybersécurité devrait s'étoffer dans la plupart des pays, les cyberattaques devraient proliférer en 2013 et s'adapter aux nouvelles technologies, notamment aux smartphones et au cloud, cette dernière technologie permettant aux logiciels malveillants de s'infiltrer dans le navigateur plutôt que sur le système. Les nouvelles menaces devraient également exploiter les failles plus traditionnelles comme les faibles contrôles de sécurité sur IPv6. Enfin, WatchGuard estime même que les cyberattaques pourraient faire leurs premières victimes humaines durant l'année 2013.

[Le Figaro] Explosion des cyberattaques contre les entreprises

A l'occasion d'un colloque sur la cybersécurité organisé par l'OCDE et Europol, la Fondation de recherche stratégique (FRS) a annoncé les résultats de son étude sur la sécurité numérique. Selon la Fondation, les entreprises seraient actuellement victimes d' *« une avalanche d'attaques permanentes, mais dont les conséquences sont limitées, autant financièrement que techniquement. »* En revanche, l'arrivée progressive sur la scène des APT et des intérêts étatiques pourrait changer la donne. En 2012, les

grandes entreprises ont consacré environ 2% de leur chiffre d'affaires à la SSI.

[ENISA] Rapport sur la sensibilisation des entreprises à la cybersécurité

L'ENISA et le ministère de l'Intérieur américain ont conjointement tenu un atelier sur la sensibilisation des acteurs intermédiaires (entreprises) à la cybersécurité. Parmi les leçons retenues pour améliorer la sensibilisation, le rapport souligne l'importance des partenariats public-privé.

[CNIL] Cahier Innovation et Prospective n°1 : Le futur de la vie privée vu par 42 experts

La CNIL a publié le premier numéro des cahiers innovation et prospective. Issu d'entretiens avec de nombreux experts du monde numérique, le document propose la *« synthèse d'une réflexion prospective sur les enjeux de la vie privée, les libertés et les données personnelles à horizon 2020 »*.

Le projet de règlement européen en matière de protection des données

En présentant son projet de règlement relatif à l'encadrement et à la protection des données à caractère personnel[1], la Commission européenne est venue réaffirmer une tendance déjà bien enclenchée : l'Europe veut protéger les données de ses citoyens et relever le défi de la création d'une régulation, par définition territoriale, d'un phénomène éminemment déterritorialisé : la circulation des données. Présenté le 25 janvier dernier, le texte vise à refondre et améliorer le cadre juridique posé par la directive datant de 1995[2] jugée aujourd'hui dépassée.

Vers une meilleure protection des données personnelles des citoyens européens

L'harmonisation des législations nationales

En proposant un règlement, et non une directive, l'Europe souhaite harmoniser la protection des données personnelles au sein des pays membres de l'Union. L'objectif est d'éviter les distinctions entre Etats et d'en finir avec la *« fragmentation juridique actuelle »* [3]. Une fois adopté (entre 2014 et 2016), ce règlement entrera en vigueur deux ans plus tard et sera d'applicabilité directe[4] dans les Etats membres[5]. Ce statut de règlement n'est toutefois pas encore acquis. Face aux 6 Etats membres soutenant le principe (Allemagne, Bulgarie, Espagne, France, Luxembourg, Pays-Bas), cinq autres (Belgique, Danemark, Hongrie, Slovénie, Suède) demandent à la Commission européenne de transformer son projet en projet de directive, afin de bénéficier de plus de marge de manœuvre dans sa transposition au sein de leur droit national. Les autres membres ne se sont pas positionnés sur cette question. Le Royaume-Uni a quant à lui récemment fait part de son opposition au projet[6].

Un texte plus efficace grâce à des sanctions « enfin » dissuasives ?

Le texte actuel souffre de nombreuses critiques, la plus redondante étant l'absence de sanction et d'effectivité[7]. Selon Viviane Reding, vice-présidente de la Commission européenne en charge de la justice, des droits fondamentaux et de la citoyenneté, *« les autorités nationales indépendantes chargées de la protection des données seront renforcées afin qu'elles puissent mieux faire appliquer et respecter les règles de l'UE sur le territoire de l'État dont elles relèvent. Elles seront habilitées à infliger des amendes aux entreprises qui enfreignent les règles de l'Union relatives à la protection des données. Ces amendes pourront atteindre 1*

[1] Proposition de règlement du parlement européen et du conseil, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) - http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf (PDF)

[2] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML

[3] http://europa.eu/rapid/press-release_IP-12-46_fr.htm?locale=fr ; Bruxelles, le 25 janvier 2012 ; Commission européenne – Communiqué de presse

[4] En vertu de l'article 288 du TFUE

[5] Ce qui signifie que les Etats n'auront pas à adopter des mesures de transposition dans leur droit national, ce qui, par la même, réduit leur marge d'interprétation du texte.

[6] http://amberhawk.typepad.com/amberhawk/2012/11/uk-government-opposed-to-the-commissions-data-protection-regulation.html

[7] « L'Europe des données est un eldorado » Tribune d'Isabelle Falque-Pierrotin, Présidente de la CNIL, publiée dans les Echos le 25 septembre 2012 - http://www.cnil.fr/la-cnil/actualite/article/article/la-protection-des-donnees-personnelles-un-atout-pour-la-france-et-leurope/

million d'EUR ou 2 % du chiffre d'affaires annuel global de l'entreprise »[8] …à la suite d'un avertissement préalable non suivi d'effet[9].

De nouvelles contraintes pèseront sur les entreprises

Le projet prévoit de simplifier les choses en mettant fin à l'obligation de déclaration des traitements de données à caractère personnel. L'Europe avance que ces dernières réaliseront, une fois le règlement adopté, près de 2,3 milliards d'euros d'économies par an.[10] Mais, en contrepartie, les entreprises seront soumises à de nouvelles obligations.

1. Obligation de documentation

Le texte prévoit une obligation de « documenter » qui se traduira par la conservation de traces de tous les traitements de données à caractère personnel et par des études d'impact. Jusque-là implicite dans l'article 34 de la loi « Informatique et libertés » de 1978 modifiée, cette obligation de documentation devient plus concrète et plus lourde à mettre en œuvre.

2. Obligation de notification

Le texte prévoit également une obligation de notifier les atteintes aux données à caractère personnel. Cette obligation ne se restreint plus aux opérateurs de communication électroniques. Elle s'étend à toutes les entreprises et fait peser sur elles un processus lourd de notification : elle devra être faite dans les 24h, sous peine de justification du dépassement de délai. La notification sera adressée à la CNIL nationale et à la personne titulaire des données compromises.

3. La Commission européenne se réserve la possibilité d'imposer des mesures de sécurité

Le texte pourra également imposer aux entreprises la mise en place d'outils de sécurité informatique tels que les anti-virus, détecteurs d'intrusions, etc. (art. 30.3 et .4 du projet de règlement).

4. Le texte renforce le droit à l'oubli numérique

La loi Informatique et libertés prévoit déjà une durée de conservation maximale des données, ainsi que la possibilité pour le titulaire de données de demander leur suppression. Le projet de règlement indique que tout individu pourra obtenir la *« suppression de données le concernant si aucun motif légitime ne justifie leur conservation »*[11].

5. Le texte reconnaît la notion de « co-responsables de traitement »

Cette responsabilité conjointe existe *« si les obligations mutuelles des parties, vis-à-vis des dispositions du règlement, n'ont pas été préalablement définies contractuellement ».* Ainsi, en l'absence d'un contrat bien ficelé entre l'entreprise et ses partenaires opérant un ou des traitements de données à caractère personnel, *« une personne concernée pourrait, dans l'exercice de ses droits, se retourner vers n'importe lequel des co-responsables de traitement »*[12]. Il sera donc extrêmement important de définir au préalable, dans un contrat, les obligations mutuelles des parties.

[8] http://europa.eu/rapid/press-release_IP-12-46_fr.htm?locale=fr ; Bruxelles, le 25 janvier 2012 ; Commission européenne – Communiqué de presse
[9] http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/comment-nos-donnees-personnelles-seront-elles-protegees-demain-10-10-2012-1515441_56.php
[10] http://europa.eu/rapid/press-release_IP-12-46_fr.htm?locale=fr ; Bruxelles, le 25 janvier 2012 ; Commission européenne – Communiqué de presse
[11] http://europa.eu/rapid/press-release_IP-12-46_fr.htm?locale=fr ; Bruxelles, le 25 janvier 2012 ; Commission européenne – Communiqué de presse
[12] http://www.alain-bensoussan.com/avocats/la-directive-europeenne-bientot-revisee/2012/03/22

Un texte déjà critiqué

Ce texte, s'il part de l'intention louable de renforcer des droits des internautes, est déjà largement critiqué.

« Ne pas loger toutes les failles à la même enseigne ».

Certains fustigent l'idée d'une obligation de notification imposée à tous, en 24h, pour n'importe quelle atteinte aux données personnelles. Pour tempérer cette obligation, a été proposée l'instauration d'une échelle de gravité : des formalités plus ou moins lourdes seraient imposées selon l'intensité de l'atteinte (obligation de notifier plus ou moins rapidement, à la CNIL uniquement, à l'intéressé ensuite, etc.).[13]

D'autres qualifient certaines des dispositions du projet présenté par la Commission européenne d'inapplicables.

« L'opt-in » ou l'obligation de recueillir le consentement de l'intéressé avant de collecter ses données sonnerait la fin de nombreux services reposant sur la collecte et l'agrégation de données, à l'image des systèmes d'annuaires, par exemple.[14] Le droit à l'oubli tel que perçu par la Commission européenne serait quant à lui irréaliste en raison de contraintes techniques évidentes : les informations sont naturellement dupliquées sur le réseau ; en raison également de difficultés d'ordre pratique : difficile pour l'entreprise devant effacer les données de tenir au courant les tiers qui auraient répliqué ces données à leur tour. Enfin, force est de constater que l'effectivité du droit européen à l'encontre des opérateurs étrangers est encore très incertaine. Certains d'entre eux ne s'estiment pas contraints de respecter la réglementation française et européenne en matière de protection des données personnelles puisque leurs serveurs ne sont pas hébergés sur le sol européen. C'est là l'un des points essentiels du projet de règlement européen qui souhaite contraindre ces opérateurs à appliquer les textes européens dès lors qu'ils ciblent des clients établis en Europe. La question essentielle réside dans l'effectivité de cette mesure : comment les CNILs européennes vérifieront-elles la bonne application de leurs textes ? Et comment appliqueront-elles les sanctions qui seront désormais à leur disposition ?[15]

La volonté d'affirmer une « souveraineté des données » à l'européenne ?

Ce projet de règlement européen signe la volonté claire de l'Union européenne d'imposer sa vision de la protection des données, à travers l'élaboration d'une réglementation régionale[16]. Le champ d'application prévu par le texte est en effet extrêmement large : toutes les données des citoyens européens, y compris stockées à l'étranger, seraient concernées par le règlement. Le texte, a priori européen, s'appliquerait ainsi dans le monde entier. Ce projet visant à assurer une véritable *« souveraineté des données »* à l'européenne s'inscrit dans le droit fil de la dynamique enclenchée par le lancement de projets de clouds nationaux et européens. L'objectif pour l'Europe serait reprendre la main sur les données des citoyens de ses membres, face à des opérateurs internationaux gourmands en données (moteurs de recherche, services de cloud…) et des législations au champ d'application extrêmement large (Patriot Act, par exemple). Alors que certains tentent de recréer techniquement des frontières en se dotant de pare-feu ou d'internets/intranets nationaux, apparaissent des ilots législatifs en matière de protection et de circulation des données.

[13] http://lexpansion.lexpress.fr/high-tech/vie-privee-sur-internet-pourquoi-le-projet-de-bruxelles-fait-peur-aux-entreprises_346892.html
[14] http://lexpansion.lexpress.fr/high-tech/vie-privee-sur-internet-pourquoi-le-projet-de-bruxelles-fait-peur-aux-entreprises_346892.html
[15] http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/comment-nos-donnees-personnelles-seront-elles-protegees-demain-10-10-2012-1515441_56.php
[16] 16 TFUE et 8 CEDH

Le portail OMC
La nouvelle plateforme de la DAS

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

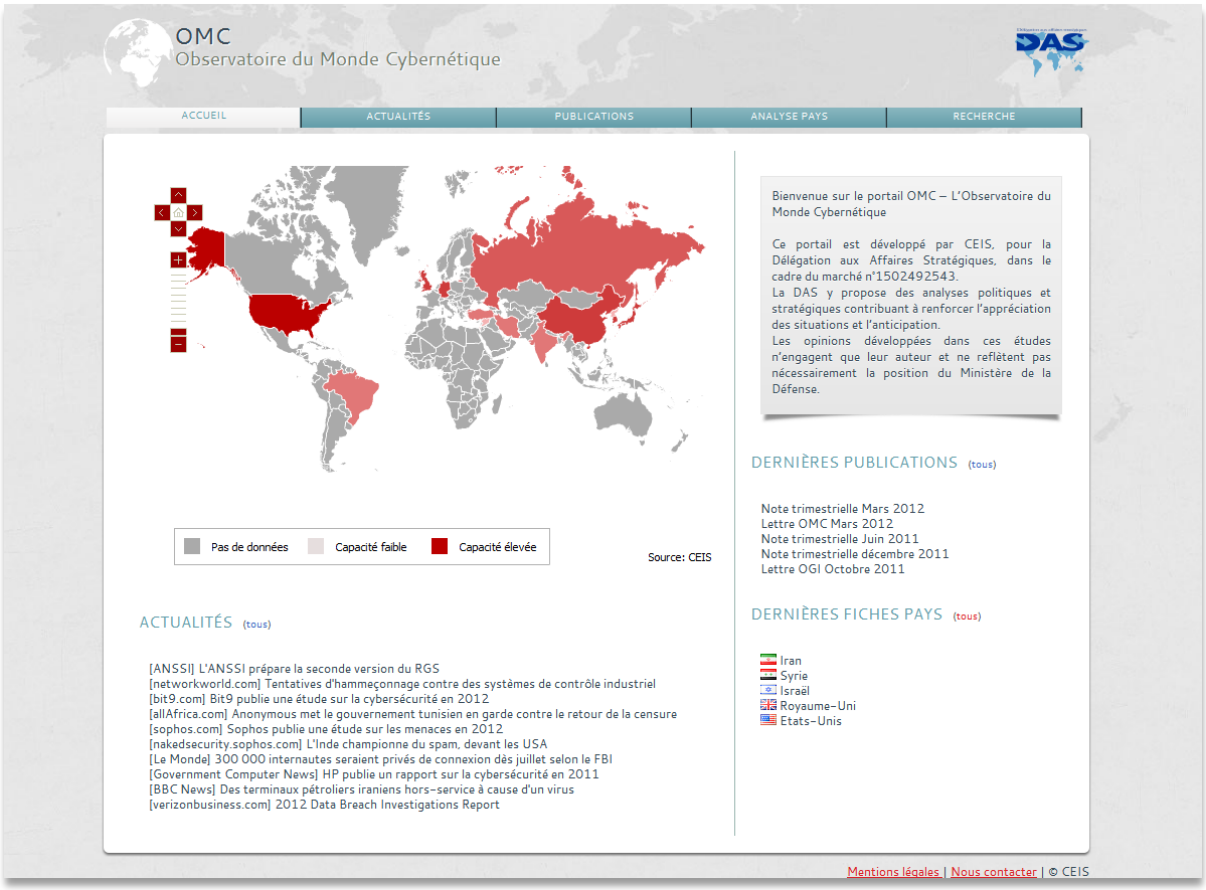

Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

CES Gov 2012	Las Vegas	9 – 11 janvier
SANS Security East 2012	Las Vegas	17 – 26 janvier
ISC SecureSanAntonio 2012	San Antonio	19 janvier
FIC 2013	Lille	28 – 29 janvier
Cyber Defence & Network Security 2013	Londres	28 – 31 janvier
NVTC Cybersecurity & Privacy Committee Event	McLean, Etats-Unis	29 janvier
Cyber Security for Government Asia 2013	Kuala Lumpur	29 – 30 janvier
European Security Round Table	Bruxelles	30 janvier
Reboot Annual Privacy and Security Conference	Vancouver	15 – 17 février
SANS Security Belgium	Bruxelles	18 – 23 février
Cyber Security Implementation Workshop	Savannah, Etats-Unis	19 – 21 février
Nullcon Goa	Goa, Inde	27 février – 2 mars

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