# Observatoire du Monde Cybernétique

Lettre n°18 – Juin 2013

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

**[Ministère de la Défense] [LeMonde] Cyberdéfense : Jean-Yves Le Drian annonce le renforcement des moyens du Ministère de la Défense**

Jean-Yves le Drian s'est exprimé sur la *« nouvelle donne stratégique »* que constitue la cyberdéfense et a précisé l'ampleur de l'effort financier et humain prévu par Livre blanc dans ce domaine. Le ministre de la Défense a reconnu implicitement que la France avait pris du retard dans ce domaine et a promis de tout faire pour rattraper le temps perdu.

**[ANSSI] L'ANSSI pilote un groupe de travail pour améliorer la sécurité des systèmes industriels**

A la suite de la publication en juin 2012 du guide sur « La cybersécurité des systèmes industriels », de nombreuses organisations ont souhaité poursuivre les travaux menés par l'ANSSI dans ce domaine. Ainsi, depuis février 2013, les acteurs industriels et étatiques ont constitué un groupe de travail piloté par l'ANSSI pour apporter des réponses concrètes et pragmatiques à la sécurisation des infrastructures industrielles. Les premiers livrables devraient être disponibles pour la fin d'année 2013.

**[France3] Christiane Taubira à Roubaix à propos de la cybercriminalité**

Christiane Taubira s'est rendue à l'ENPJJ (Ecole nationale de protection judiciaire de la jeunesse) de Roubaix pour assister aux Assises nationales des associations d'aide aux victimes, où elle a notamment évoqué la cybercriminalité. La Garde des Sceaux a expliqué avoir renforcé le budget de l'aide aux victimes de 25% en 2013.

**[Finextra] Le mandat de l'ENISA reconduit**

Le mandat de l'agence européenne de cybersécurité, l'ENISA, a été officiellement reconduit pour sept années, à compter du 19 juin 2013.

**[ZDNet] [Reuters] L'OTAN se dotera bientôt d'une capacité de cyberdéfense**

Les ministres des pays membres de l'OTAN se sont entendus pour renforcer les capacités de cyberdéfense de l'organisation, en approuvant la création d'une force d'action rapide destinée à protéger les réseaux informatiques de l'Alliance atlantique en cas de cyberattaques. Un désaccord persiste toutefois sur la gestion par l'OTAN de la protection de ses alliés les plus fragiles. Selon le secrétaire général de l'OTAN, Anders Fogh Rasmussen, la capacité de cyberdéfense de l'OTAN serait totalement opérationnelle en automne prochain pour assurer la protection de tous les réseaux informatiques de l'Alliance. Le sénateur Jean-Marie Bockel s'est félicité du lancement de cette force d'intervention, précisant que la France en sera l'un des maillons forts.

**[Reuters] Les banques anglaises craignent davantage une cyberattaque que la crise de l'Euro**

Le directeur de la Banque d'Angleterre (BoE) a rencontré cinq des plus grandes banques du pays, notamment pour discuter des menaces pesant sur leur activité. Quatre d'entre elles ont placé les cyberattaques en tête de leur liste, conscientes du potentiel destructeur d'une cyberattaque.

**[L'informaticien] PRISM : la NSA se livrerait à un vaste espionnage téléphonique et informatique**

Selon le Guardian et le Washington Post, et des informations fournies par Edward Snowden, ancien de la CIA, la NSA écouterait les communications de millions d'abonnés téléphoniques sur les réseaux américains. Dans le cadre d'un programme baptisé Prism, elle bénéficierait également d'un accès direct aux serveurs de neuf sociétés d'informatique et de services Internet parmi lesquels les géants Apple, Google, Microsoft ou encore Facebook, Yahoo, AOL, PayPal.

**[Guardian] La Grande-Bretagne aurait espionné des diplomates lors du G20 de Londres**

Le Guardian a publié un nouveau document fourni par Edward Snowden, accablant cette fois le GCHQ britannique. Celui-ci aurait espionné des diplomates lors du G20 tenu à Londres en 2009. Le GCHQ aurait eu accès aux communications Internet et téléphoniques des participants du G20 grâce à une équipe de 45 personnes affectées en permanence à cette tâche de surveillance. De faux cybercafés auraient même été créés pour pirater les ordinateurs s'y connectant. L'agence britannique aurait également eu accès aux e-mails et aux appels passés depuis des Blackberry.

**[Euronews] Anonymous menace l'Etat grec de cyberattaques en réplique à la fermeture de la chaîne publique**

Le groupe Anonymous a posté une vidéo menaçant le gouvernement grec de cyberattaques contre ses sites Internet, en réplique à la fermeture de la chaîne ERT et du licenciement de ses 2,650 employés.

**[Guardian] Obama demande l'établissement d'une liste de cibles étrangères potentielles pour des cyberattaques**

Barack Obama a demandé aux responsables de la sécurité et du renseignement de dresser une liste de cibles étrangères potentielles pour des cyberattaques d'origine américaine. Cette directive secrète datant d'octobre 2012 confirme les capacités offensives américaines et vise à mettre en place des outils et un cadre permettant au gouvernement de prendre des décisions rapides. L'élaboration d'une liste de cibles potentielles illustre la posture offensive des Etats-Unis dans le cyberespace.

**[Bloomberg] Le Pentagone prévoit un budget de 23 mds$ pour la cyberdéfense**

Le Pentagone a prévu de consacrer un budget de 23 milliards $ jusqu'en 2018 à la cyberdéfense. Le but est de favoriser le développement de projets de cyberdéfense et de capacités offensives.

**[TheWashingtonPost] Les Etats-Unis auraient perturbé la publication du magazine d'Al-Qaïda**

Les services de renseignement américains seraient parvenus à différer la publication du magazine en ligne d'Al-Qaïda en langue anglaise, Inspire. A sa publication, la deuxième page du magazine était en effet illisible, tandis que 20 autres pages étaient vides.

La version sabotée a cependant rapidement été enlevée et remplacée deux semaines plus tard par la version originale. La méthode employée par les américains pour réaliser ce piratage n'est pas connue, mais un officiel américain a révélé avoir travaillé à perturber la publication du magazine, notamment en en modifiant le contenu.

**[eWeek] Microsoft neutralise 1,2 million de botnets**

Microsoft, en collaboration avec le FBI, a annoncé avoir neutralisé 1,2 million d'ordinateurs contrôlés par le cheval de Troie Citadel.

**[LeFigaro] USA : une nouvelle loi contre les cybercriminels ?**

Une loi a été proposée à la Chambre des représentants américaine pour sanctionner les cybercriminels ayant espionné les Etats-Unis dans le but de leur voler des secret industriels. Le Cyber Economic Espionage Accountability Act permettrait ainsi le gel des actifs de ces individus aux Etats-Unis, le refus d'obtention d'un visa ou la révocation de celui existant.

**[NYTimes] Cybersécurité : des rencontres Chine-Etats-Unis dès juillet**

Les Etats-Unis et la Chine se sont accordés sur la nécessité d'ouvrir des discussions sur la cybersécurité et le cyberespionnage. Des rencontres régulières auront lieu dès juillet. Leur objectif : mettre en place des règles de conduite communes, notamment concernant le vol d'information et l'atteinte à la propriété intellectuelle des entreprises américaines.

**[Stuff] Les Etats-Unis et la Russie signent un pacte de cybersécurité**

Les Etats-Unis et la Russie ont signé un accord pour réduire le risque de conflit dans le cyberespace par la communication en temps réel d'incidents relevant de la sécurité nationale. Ce pacte a été annoncé à l'occasion du G8, et s'inscrit dans un effort plus large de coopération sur les thématiques de contre-terrorisme et d'armes de destruction massive. Une ligne directe sera notamment établie entre le coordinateur de cybersécurité américain et son homologue russe.

**[YNetNews] Cisco va construire un centre R&D en cybersécurité en Israël**

Cisco a annoncé le lancement d'une campagne de recrutement afin de constituer une équipe de professionnels de la sécurité. L'objectif final de Cisco est de porter ses effectifs à 2 000 personnes et faire ainsi fonctionner son nouveau centre de R&D en matière de cybersécurité

**[TheJerusalemPost] Netanyahu : *« Israël a besoin d'un dôme de fer numérique »***

Pour mieux résister aux cyberattaques croissantes venant d'Iran, Israël prépare un « dôme de fer numérique ». Affirmant constater une augmentation des attaques venues d'Iran depuis quelques jours, le premier ministre Benjamin Netanyahu a précisé qu'elles ciblaient des systèmes vitaux nationaux. Le projet d'un dôme de protection a été discuté avec les Etats-Unis, qui devraient donc participer à renforcer les défenses israéliennes.

**[NDTV] L'Inde disposerait de son système de cyberespionnage**

L'Inde se serait elle aussi dotée d'un programme de cyberespionnage à grande échelle. Mais, à l'inverse du programme PRISM, le programme indien n'aurait pas pour mission de collecter des données personnelles mais d'évaluer les principales menaces susceptibles d'affecter le cyberespace indien. Plusieurs entités y participent, à commencer par le Département de l'Electronique et des Technologies de l'Information. Sont également concernés le ministère de la Défense, l'Organisation Nationale de Recherche Technique et l'Organisation de Recherche et Développement de Défense.

**[RTS] L'Iran serait parvenu à faire taire ses cyberdissidents avant la présidentielle**

L'Iran a appris du passé, et contrairement aux élections de 2009 où la population s'était emparée du cyberespace pour exprimer et relayer sa contestation, le gouvernement a cette fois verrouillé Internet. Désormais, lorsqu'un Iranien souhaite se connecter, il constate un filtrage de Facebook, Twitter, Google ou Yahoo, et autres sites jugés dangereux. La bande passante a été ralentie, l'internaute est pisté et les logiciels permettant de contourner la censure (comme Kerio ou Open VPN) sont bloqués. Selon des experts, le recours au SMS pourrait être privilégié en cas d'éventuelle contestation.

**[IntelligenceOnline] Les cyber-consultants étrangers du royaume saoudien**

Le ministère de l'intérieur saoudien a annoncé la création de l'Organisme National de la Sécurité de l'Information et du Renseignement. Ce service de cybersécurité, presque exclusivement constitué de consultants étrangers (et notamment américains), devra sécuriser les réseaux du royaume.

**[Caribbean360] La Jamaïque veut améliorer la protection de son secteur technologique face aux cyberattaques**

Un CERT va ouvrir à Kingston, Jamaïque, pour améliorer la protection des infrastructures Internet du pays et coordonner la défense contre les cyberattaques. Il devrait être opérationnel en décembre.

**[StratégieGouv] Internet : prospective 2030 (Note d'analyse 02 - Juin 2013)**

Le Commissariat général à la stratégie et à la prospective a publié une étude confiée à des enseignants chercheurs de Télécom ParisTech et à des membres de la Fondation internet nouvelle génération (FING). Ils ont tenté d'identifier des tendances, incertitudes et tensions liées à l'évolution d'Internet à l'horizon 2030. Ils formulent également des propositions pour accompagner le développement industriel du numérique.

**[ANSSI] Référentiel d'exigences applicables aux prestataires d'audit de la SSI**

L'ANSSI a publié un Référentiel d'exigences applicables aux prestataires d'audit en matière de SSI, couvrant les activités d'audits de code source, de configuration, d'architecture et d'organisation ainsi que les tests d'intrusion. Les exigences du référentiel sont regroupées en trois domaines (le prestataire d'audit, les auditeurs qu'il emploie et le déroulement des audits), portant notamment sur l'adoption d'une charte d'éthique, la gestion des ressources et des compétences, la protection de son système d'information et sur son impartialité.

**[Huyghe] Glossaire de 500 mots de la cyberstratégie et de la stratégie de l'information**

Le chercheur à l'IRIS François Bernard Huyghe publie un lexique de cyberstratégie et de stratégie de l'information, recensant 500 mots. Prioritairement adressé aux étudiants, il s'adresse en réalité à tous.

**[FDA] Le matériel médical est trop sensible aux cyberattaques selon la FDA**

La Food and Drug Administration (FDA) a publié un communiqué pour rappeler aux professionnels de la santé américains les dangers pouvant provenir de piratages, la totalité des appareils pouvant selon elle être piratés (notamment Pacemaker et scanners). Des centaines d'équipements médicaux auraient ainsi déjà été infectés par des logiciels malveillants.

**[WebSense] Les cybercriminels utilisent le Canada comme base virtuelle**

Un rapport d'analyse des menaces fait état du choix des cybercriminels de localiser leurs serveurs au Canada, affectant ainsi l'image de ce pays. En 2012, le Canada était ainsi le 3e pays choisi par les cybercriminels pour placer leurs bases virtuelles pour mener de l'espionnage industriel, derrière les Etats-Unis et les Pays-Bas, mais devant notamment la Russie ou la Chine.

**[da.mod.uk] The Global CyberGame : Internet doit se préparer à une militarisation**

L'Académie de Défense britannique a publié un rapport intitulé « The Global Cyber-Game », rassemblant ses travaux et proposant des scénarios de cyberconflits. Selon cette institution rattachée au Ministère de la défense britannique, le cyberespace va se militariser, et les Etats devront prendre garde à ne pas développer d'arme susceptible de proliférer. Les auteurs préviennent également du risque de balkanisation du cyberespace. Enfin, l'augmentation exponentielle du trafic internet pose des questions de vulnérabilités infrastructurelles jusqu'alors peu considérées.

**[DBCDE] Une stratégie nationale australienne dans le domaine du Cloud**

Le gouvernement australien publie une stratégie nationale pour le cloud. Ce document identifie trois objectifs et un panel d'actions à entreprendre pour les atteindre : la maximisation de la valeur du cloud au sein du gouvernement, la promotion du cloud auprès des PME, des organisations à but non-lucratif et des consommateurs, et le soutien à un secteur de services cloud performant.

# Quel rôle pour l'Europe dans le cyberespace fragmenté de demain ?

Le cyberespace dessine une géographie nouvelle. Si les utopistes voient en Internet un outil transnational et sans frontières, la réalité les rattrape : le cyberespace se fragmente et tend vers ce que les experts qualifient de véritable « balkanisation ». Les signaux sont multiples : certains Etats créent leur internet national ; d'autres renforcent leur coopération à l'échelle régionale ou bilatérale ; les paradis numériques prospèrent en raison de législations défaillantes ou volontairement laxistes ; les produits numériques tournent le dos à l'universalité du web et tendent à enferment leurs utilisateurs dans des silos applicatifs très peu interopérables, voire complètement incompatibles. Et les révélations de ces dernières semaines sur les multiples systèmes d'espionnage mis en place par les grandes puissances du cyberespace vont sans doute accélérer cette tendance qui est en très large partie le fait d'acteurs non européens.

Le vieux continent est en effet nettement dominé au plan numérique, au point de constituer, comme le soulignait le rapport Morin-Desailly[1], « une colonie du monde numérique ». Soucieuse de trouver une troisième voie entre une gouvernance « multi-acteurs » dominée par les Etats-Unis et le souverainisme russe et chinois, l'Europe a-t-elle les moyens de ses ambitions ? Cherchant à protéger sa souveraineté numérique, l'Europe peut-elle tirer son épingle du jeu dans cette redistribution des cartes et résister à la suprématie américaine, sans pour autant basculer dans un repli protectionniste ? Pourrait-elle devenir le moteur d'une nouvelle dynamique dans le cyberespace ?

**Concept : Le Balkanisation, un terme historique appliqué au cyberespace**

Utilisé pour la première fois en 1918, dans une interview de Walther Ratheneau dans le New York Times, le terme de « balkanisation » fait écho au morcellement du territoire des Balkans suite à la signature de nombreux traités qui ont conduit à la création de plusieurs petits Etats qui ne coopéraient pas entre eux, allant même çà faire preuve d'hostilité les uns à l'égard des autres. Dans la continuité de cette définition, le cyberespace connait aujourd'hui d'autres facteurs qui contribuent tant métaphoriquement que concrètement à sa « balkanisation ». La première difficulté est qu'il n'existe pas de définition consensuelle du cyberespace. Perçu comme un territoire par certains, le terme est porteur d'une utopie[2] – liberté de circulation de l'information, transparence, partage, démocratie, égalité, pacification du monde et progrès – qui se joue des frontières. Utopie qu'il est difficile de concilier à l'exercice par l'État souverain de ses pouvoirs à l'intérieur de ses frontières[3]. Appliqué au cyberespace, le concept de balkanisation induit une fragmentation accrue des différentes strates (logique, physique et cognitive) du cyberespace (voir tableau ci-après).

[1] MORIN-DESAILLY (C.), Rapport d'information fait au nom de la commission des affaires européennes sur « l'Union européenne, colonie du monde numérique ? », Sénat, 20 mars 2013
[2] DESFORGES (A.), Cyberespace et internet : un réseau sans frontières ?, CERISCOPE Frontières, 2011, consulté le 14 mai 2013
[3] BIGO (D.), Frontières, territoire, sécurité, souveraineté, CERISCOPE Frontières, 2011, consulté le 20 juin 2013

## La notion de « frontières » au cœur de celle de « balkanisation »

Les frontières, dans leurs définitions classiques, sont entendues comme une ligne séparant des espaces territoriaux où s'exercent deux souverainetés différentes, cette ligne étant « *formée par la succession des points extrêmes du domaine de validité spatiale des normes de l'ordre juridique d'un Etat* »[4].

Le terme de « balkanisation » sous-entend que des groupes d'êtres humains s'opposeraient, conduisant ainsi au morcellement du territoire sur lequel ils étaient auparavant tous réunis. Il s'agirait peut être plus de parler de fragmentation, qui ferait référence au morcellement de territoire et des populations, mais aussi de l'accès aux services, à l'information, au Web de manière générale.

Mais le terme de balkanisation suppose l'existence de frontières. Et l'existence de celles-ci dans le cyberespace n'est pas quelque chose d'acquis. Car si pour les gouvernements, il semble logique qu'ils aient le pouvoir d'exercer une gouvernance sur « leur » cyberespace, pour d'autres, à l'image de John Perry BARLOW dans sa *Déclaration d'indépendance du cyberespace*, ce dernier se situe hors des frontières et donc du contrôle des Etats. Cette dernière conception s'appuie sur le fait que les concepts avancés par les Etats sont basés sur la matière alors que le cyberespace serait quant à lui immatériel.

Ainsi, s'il est perçu de façon similaire et en partage certaines caractéristiques, le cyberespace ne présente pas les mêmes caractéristiques que les espaces traditionnels (terrestre, maritime et aérien). Mieux encore, il offre la possibilité aux Etats d'« étendre » leurs territoires, de **repousser leurs frontières** et par là même leur souveraineté. Le corpus législatif américain[5] étend ainsi le principe de compétence territoriale par une sorte d'extraterritorialité dont bénéficient les Etats-Unis sur le territoire d'un autre Etat dès lors que l'entreprise est de droit américain ou lorsque les données d'une entreprise étrangères sont stockées sur le territoire américain. Cette extraterritorialité accordée par le droit américain se trouve renforcée par l'aspect « physique » du cyberespace : les serveurs DNS et de stockage de données sont majoritairement localisés sur le continent américain. La maîtrise du système d'adressage ainsi que la maîtrise des données offerte par les géants Facebook, Apple, Google ou encore Amazon viennent compléter cette suprématie.

Cette question est d'ailleurs au cœur du scandale provoqué par le programme PRISM[6]. Dans quelle mesure les Etats-Unis ont-ils le droit de surveiller les données échangées dans le cyberespace ? Où commencent et se terminent leurs frontières, et par conséquence leur compétence territoriale ? Il en est exactement de même pour l'interception des échanges des diplomates opérée par la Grande Bretagne lors du sommet du G20 de Londres en 2009[7].

[4] Tribunal arbitral, affaire de la frontière maritime entre le Sénégal et le Guinée Bissau, RGDIP 1990, p. 253.
[5] Patrioct Act, FISAA, etc.
[6] http://www.linformaticien.com/actualites/id/29316/prism-la-nsa-se-livrerait-a-un-vaste-espionnage-telephonique-et-informatique.aspx
[7] http://www.guardian.co.uk/uk/2013/jun/16/gchq-intercepted-communications-g20-summits

## Etat des lieux

La balkanisation du cyberespace est transversale. Elle se matérialise au cœur de chacune des différentes couches du cyberespace que sont la couche physique, logique, et cognitive[8]. Chacune de ces strates étant composées de divers éléments qu'il est possible de maîtriser. La maîtrise de la quasi-totalité de ces composants caractérise ainsi une « super-puissance » du cyberespace.

| Composants | | Strates | | |
|---|---|---|---|---|
| Culture (langue, politique, éthique, liberté, etc.)<br>Identités réelles - humanité | | Couche cognitive et humaine | CYBERESPACE | GOUVERNANCE |
| Usages | Communication, recherche, réseaux sociaux, loisirs, partage de connaissance, commerce, économie, diplomatie… | | | |
| | Mais aussi désinformation, propagande, conflits, renseignement… | | | |
| Perception/cognitif – Informations – sémantique (sens des informations, diffusion, visualisation) - Identités numériques (pseudonymat) | | | | |
| Contenus, données | | Couche logique ou logicielle | | |
| Applications d'Internet (Web, Mail, partage de fichiers, messagerie instantanée) | | | | |
| Systèmes d'exploitation et autres applications – softwares/programmes | | | | |
| Protocole de communication/transport/adressage | | | | |
| Machines : terminaux, périphériques et objets connectés | | Couche physique | | |
| Infrastructures, serveurs et connectivité (câbles sous-marins, réseaux sans-fil, datacenters, routeurs) | | | | |
| Enracinement géographique (conséquences stratégiques, politiques, juridiques…) | | | | |

Dans les années 1990, l'entrée sur le marché du navigateur Internet Explorer de Microsoft, est venue en opposition directe à Netscape Navigator, qui à l'époque dominait le marché. Les codes HTML alors utilisés étaient propres à chaque navigateur, les deux sociétés imposant des caractéristiques supplémentaires et exclusives, ouvrant par la même une guerre des standards, alors même qu'elles participaient aux travaux du W3C pour l'établissement des versions normalisées du HTML.

[8] Ce tableau s'inspire des conceptions suivantes : Characterizing cyberspace : past, present and future http://web.mit.edu/ecir/pdf/clark-cyberspace.pdf ; Cyberspace Operations Concept Capability Plan 2016-2028 http://www.fas.org/irp/doddir/army/pam525-7-8.pdf ; Olivier KEMP - Stratégie du cyberespace http://www.diploweb.com/Strategie-du-cyberespace.html
Il représente toutefois une perception propre du cyberespace et de ses composants, d'un point de vue stratégique.

Au-delà de l'impact des standards HTML évoqués, certains écosystèmes participent également à la balkanisation du cyberespace. Les utilisateurs de produits sont ainsi enfermé dans un écosystème basé sur des applications en silo, ou des services qui rendent difficile l'accès à des contenus non-autorisés ou de communiquer avec les utilisateurs d'autres produits, enfermés dans d'autres écosystèmes.

La balkanisation du cyberespace est également la conséquence de l'incompatibilité des différentes législations nationales. Certaines autorisent bien des choses que d'autres interdisent : tout comme la fiscalité, il existe des paradis numériques. En Suisse, nombre de sociétés proposent un abonnement pour quelques euros qui donnent accès à un VPN, permettant par exemple à des utilisateurs français de télécharger allègrement sans être inquiétés par les dispositifs mis en place par HADOPI[9]. Certains Etats cautionnant les hébergeurs *bulletproofs*, expriment une certaine tolérance de la cybercriminalité sur leur territoire et refusent de répondre à toute requête de coopération internationale.

A cela s'ajoute les cas de filtrage volontairement opérés par des pays comme la Chine ou la Corée du Nord. Cela a pour conséquence directe d'isoler les internautes de ces pays et d'assurer une censure sur les contenus du Web[10].

En opposition, de nombreux services globaux sont de plus en plus utilisés, à l'image du *cloud computing*, et participent à la mondialisation. Cependant, de tels services hébergent des données dans des pays où les législations sont différentes avec un risque de *dumping* bien réel : une entreprise aura tout intérêt à s'installer dans un pays où la législation lui est favorable. Les services Internet sont en outre largement fournis par des géants américains, qui dépendent donc de la législation américaine, conférant par la même un vaste pouvoir de contrôle au Etats-Unis sur le Web. Face à cette suprématie, des Etats comme la Chine développent leurs propres outils (Baidu, Weibo…) comme autant de substituts aux outils développés par ces géants américains (Google, Twitter…), ce qui contribue toutefois un peu plus à l'enclavement de leurs internautes.

## Quels scénarios ? Quels facteurs d'évolution ?

### *Les scénarios clés*


**L'utopie.** D'un point de vue utopique, le cyberespace ne devrait pas faire l'objet d'une gouvernance par les Etats mais devrait se gérer de manière autonome, un espace d'égalité, de partage de l'information, de communication, de neutralité. Cette hypothèse semble peu probable eu égard aux enjeux que représente le cyberespace et à ceux qu'il représentera dans l'avenir. Les Etats n'accepteront jamais d'abandonner partie de leur souveraineté pour laisser le cyberespace se réguler de manière autonome et devenir une sorte de « bien commun » de l'humanité.

**La gouvernance multi-acteurs.** Cette vision du cyberespace consisterait à rééquilibrer le système actuel caractérisé d'une part par la domination des Etats-Unis et d'autre part par une gouvernance essentiellement « technicienne », et donc relativement « a-démocratique », en s'appuyant sur un triptyque société civile, entreprises et Etats. Le risque est cependant de paralyser le développement du réseau en le soumettant à un mode de fonctionnement interétatique lourd et inadapté au développement des usages et au progrès technologique.

[9] http://www.pcinpact.com/news/64190-suisse-numerique-vpn-hadopi-anonymat.htm
[10] KRETCHUN (N.) et KIM (J.), A Quiet Opening, North Koreans in a Changing Media Encironment, 2013

**L'hyper-contrôle.** A l'opposé, d'autres Etats comme la Chine, la Russie ou l'Iran militent pour un cyberespace dans lequel chaque Etat chercherait à étendre le plus possible le contrôle sur « son » cyberespace. Le réseau perdrait sa dimension supranationale : il ne serait qu'une interconnexion de réseaux étatiques plus ou moins interopérables, reliés par des passerelles activées ou désactivées au gré des tensions politiques, économiques et militaires. Ce scénario aurait pour conséquence une « ultra-balkanisation » du cyberespace.

## Quel positionnement pour l'Europe ?

***L'Europe moteur de changement :*** dans ce contexte, l'Union européenne se doit de réagir, au risque dans le cas contraire de perdre le contrôle sur le cyberespace. Les textes fondateurs de l'Union européenne lui confère le devoir d'assurer à ses citoyens un espace de liberté, dans lequel les personnes sont libres de circuler et la croissance économique encouragée[11]. A ce titre, l'Europe apparait, grâce à la convention de Budapest, comme le candidat idéal pour la stimulation de la **coopération internationale et la lutte contre les paradis numériques**. La stratégie *« No disconnect »* mérite également d'être appuyée, dans un contexte de **défense des libertés sur Internet**.

**Le soutien de l'industrie du numérique** est un axe majeur d'évolution et d'investissement, si l'Europe souhaite conserver sa souveraineté dans le cyberespace et s'en servir comme levier pour sortir de la crise économique. L'Union ne peut plus se contenter d'être un simple acteur du cyberespace, qui consommerait des biens et des services à travers celui-ci. L'Europe doit devenir un véritable moteur de l'économique numérique et s'appuyer pour ce faire sur l'ensemble des leviers que sont le marché unique, la politique commerciale, la politique de concurrence, l'innovation et la recherche[12].

Les répercussions de la révélation du programme PRISM peuvent appuyer la démarche de **protection des données à caractère personnel** des citoyens européens dont le projet de règlement représente le cheval de bataille. Une démarche qui passe par un meilleur encadrement des transferts de données personnelles vers d'autres pays, notamment les Etats-Unis, dont la législation est perçue comme très intrusive. Cette condition est aujourd'hui vue comme nécessaire au maintien de la souveraineté de l'Union européenne dans le cyberespace, mais aussi à la protection patrimoine culturel de l'Europe.

***L'Europe isolée :*** mais l'Europe doit réagir sans pour autant se replier sur elle-même : une politique protectionniste trop poussée (protection accrue des données à caractère personnel, *data centers* européens, fiscalité numérique trop contraignante) risquerait d'isoler l'Union européenne et de faire fuir les entreprises et les investisseurs, avec un impact direct sur son économie et plus largement son développement.

Outre ces aspects relatifs à la cybersécurité, la cyberdéfense est également une problématique à envisager dans le cadre de la balkanisation du cyberespace. Un tel phénomène viendrait en effet agir directement sur une prérogative régalienne des Etats : la défense. Alors même que les cyberconflits se multiplient et que beaucoup d'Etats se dotent de doctrines de cyberdéfense[13], l'Union européenne n'affiche pas de réelle volonté en la matière en comparaison avec les initiatives prises par l'OTAN[14], notamment le manuel de Tallin[15]. Et ce constat se situe dans la mouvance actuelle dans laquelle l'Union laisse à l'OTAN le soin d'assurer la défense du vieux continent. L'Europe se doit donc d'imposer sa propre vision du cyberespace et conduire une véritable politique en la matière, se posant alors comme une alternative à l'affrontement sino-américain « dans » et « à propos » du cyberespace.

[11] Article 3 du traité sur l'Union européenne
[12] Communication de la Commission européenne de 2012, COM(2012) 582
[13] http://www.acus.org/natosource/new-rules-will-allow-military-commanders-counterattack-foreign-cyber-threats
[14] NATO Cooperative Cyber Defence Centre of Excellence
[15] The Tallinn Manual on the International Law Applicable to Cyber Warfare

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

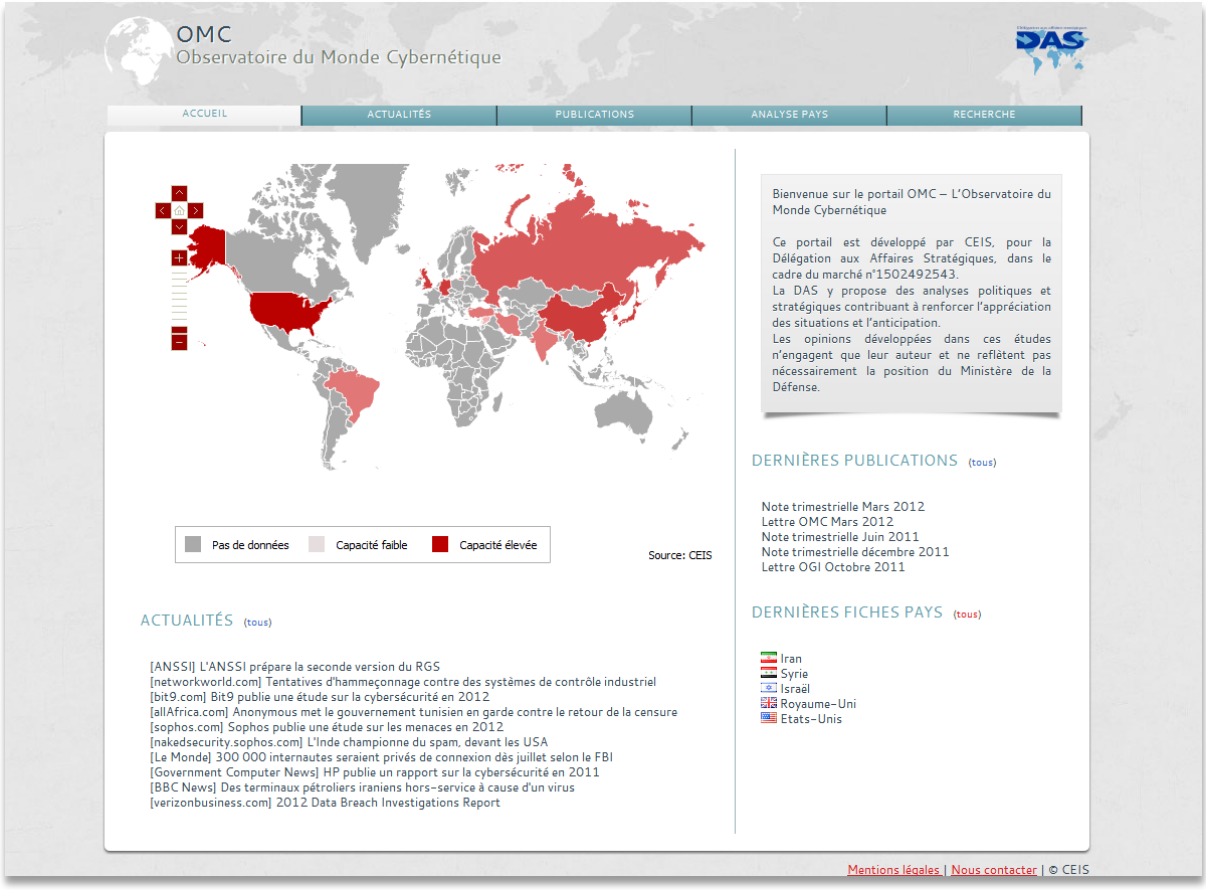


**Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/**

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

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

| | | |
|---|---|---|
| **Security Israël** | Tel-Aviv (Israël) | 25 - 27 juin |
| **European PCI DSS Roadshow par Vigitrust et Verizon** | Paris | 2 juillet |
| **Mobilité BYOD** | Paris | 2 juillet |
| **« Technology Against Crime / Technologie contre le crime » - TAC** | Lyon | 7 - 9 juillet |
| **Black Hat Training & Briefings USA 2013** | Las Vegas (USA) | 27 juillet - 1er août |
| **Les Assises de la Sécurité et des Systèmes d'Information** | Monaco | 2 – 5 octobre |
| **Mobility for Business** | Paris | 9 – 10 octobre |
| **CARTES Secure Connexions Event 2013** | Paris | 19 - 21 novembre |
| **6ème Forum International de la Cybersécurité (FIC)** | Lille | 21-22 janvier 2014 |

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