Observatoire du Monde Cybernétique

Lettre n°22 – Octobre 2013

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

[GSM] Fleur Pellerin réaffirme le besoin de fixer des règles européennes claires lors d'un débat au Sénat sur les données personnelles

Lors d'un débat organisé au Sénat sur les données personnelles jeudi 17 octobre 2013, Fleur Pellerin a réaffirmé que les données personnelles doivent être protégées par un cadre juridique strict.

[ZDnet] Big Data : Anne Lauvergeon favorable à un droit à l'expérimentation

La présidente de la commission « Innovation 2030 » a rendu ses conclusions dans lesquelles elle propose un droit à l'expérimentation concernant le Big Data. Objectif : introduire des exceptions au cadre juridique, comme l'exploitation de données à caractère personnel à des fins commerciales.

[RFI] La France, première victime de la cybercriminalité en Europe

Symantec a calculé que 41% des Smartphones français sont hackés, contre une moyenne de 29% en Europe. De plus, 43% des français sont connectés à des personnes qu'ils ne connaissent pas dans leurs réseaux sociaux.

[LeMonde] La surveillance de la NSA sur la France serait plus vaste que prévue

De nouvelles révélations décrivent l'étendue de la surveillance de la NSA en France : en moyenne de 3 millions d'interceptions quotidiennes avec un pic à sept millions pendant un mois en 2013. Les écoutes étaient activées automatiquement lorsqu'un mot clé était envoyé par message ou dit lors d'une conversation téléphonique. Avant cette révélation, la France était restée relativement silencieuse sur le programme d'espionnage de la NSA.

[Telegraph] Les institutions économiques britanniques vont mener des exercices de cyberdéfense

Les grandes banques britanniques vont lancer un exercice de cyberdéfense sous la supervision de la Banque d'Angleterre, du Trésor et de l'Autorité de Régulation Financière. Plusieurs milliers de personnes vont prendre part à l'exercice le mois prochain afin de se préparer à des cyberattaques majeures contre les banques, la bourse et les fournisseurs de paiement.

[PrivacyLawBlog] L'Union européenne débat de la protection des données personnelles

Le Conseil de l'Union européenne a récemment évoqué la possibilité de transformer la législation sur la régulation de la protection des données en principe afin qu'elle bénéficie aux institutions européennes ainsi qu'aux gouvernements des Etats membres. Ainsi, une seule autorité de protection des données superviserait toutes les collectes de données ainsi que leur utilisation au sein de l'Union européenne.

[ZoneMilitaire] La cyberdéfense est une des priorités pour la défense européenne

En préparation du sommet de l'UE relatif à la défense des 19 et 20 décembre 2013, Catherine Ashton et l'AED ont conjointement présenté un rapport dans lequel la cyberdéfense figure parmi les quatre priorités pour la défense européenne.

[Softpedia] La cybersécurité russe sera confiée au FSB

La Russie vient d'adopter une loi qui va permettre à son agence d'espionnage, le Federal Security Service (FSB), de superviser la sécurité des réseaux d'information des *smart grid*, la cyberdéfense et l'application des mesures cyber. La loi demande aussi aux autres agences de coopérer avec le FSB en ce qui concerne la cybersécurité.

[NationalCybersecurity] L'installation secrète de la NSA en Utah victime d'un accident

Le mécanisme d'une importante infrastructure de stockage de données de la NSA a été détruit, retardant l'ouverture du nouveau site d'un an. Ce type d'accident n'est pas sans rappeler le mode d'action du virus Stuxnet utilisé pour détruire les centrifugeuses iraniennes. Une surtension

électrique serait à l'origine de la destruction du mécanisme.

[BusinessKorea] Les Etats-Unis et la Corée du Sud vont accroître leur coopération en matière de cybersécurité

Les ministres de la Défense des deux pays ont annoncé la création d'un Conseil en matière de politique de cybersécurité. Cette annonce intervient après qu'un accord similaire a été passé entre les Etats-Unis et le Japon, dans le cadre d'un effort américain de contenir la menace cyber que représentent la Chine et la Corée du Nord.

[WashingtonPost] Les services de renseignement étrangers sont mis en haut niveau d'alerte suite aux révélations de Snowden

Le gouvernement américain a prévenu les services de renseignement étrangers que de nouveaux documents détaillant leurs coopérations avec les opérations secrètes américaines pourraient être révélés par Edward Snowden. Cela inclut les programmes de collecte de renseignements sensibles contre la Chine, la Russie et l'Iran. Les avertissements sont également à l'attention des pays alliés, afin d'adoucir le choc causé par l'espionnage américain.

[TheGuardian] La NSA espionnerait 35 leaders mondiaux

Selon les dernières révélations, la NSA aurait mis sur écoute les conversations téléphoniques de 35 leaders mondiaux, parmi lesquels plusieurs alliés américains. L'Agence a demandé aux autres services fédéraux de partager leurs listes de contacts afin de pouvoir collecter et mettre sur écoute un plus grand nombre de numéros de téléphone. Le Memo indique également que ces écoutes des leaders ont rapporté très peu d'informations.

[TheHackerNews] Des hackers iraniens ont tenté de pénétrer des ordinateurs de l'US Navy

La campagne iranienne de cyber espionnage n'a pas donné de résultats mais a inquiété le Department of Defense américain, qui craint que de futures attaques réussissent à exfiltrer des informations top-secrètes.

[TheHindu] L'Inde coopère avec le Brésil sur la gouvernance d'Internet

A la suite de la sixième rencontre de la Commission Inde - Brésil, les deux pays ont annoncé leur collaboration au niveau des Nations Unies sur la question de la cyber gouvernance. Plusieurs autres pays voudraient rejoindre l'Inde et le Brésil dans leurs efforts, afin que les Etats-Unis réforment leur système de surveillance.

[Mashable] La Chine aurait plus de surveillants d'Internet que de soldats

Surnommés les « analystes de l'opinion publique », cette armée de surveillants d'Internet surpasserait en nombre la quantité de soldats chinois, avec deux millions de personnes contre 1,5 millions. Ces deux millions de travailleurs censurent les commentaires indésirables et collectent des données sur certains utilisateurs.

[EurasiaNews] Analyse de la doctrine de cyberdéfense des Emirats Arabes Unis

Le cyber programme des Emirats Arabes Unis reste moins développé que celui des pays occidentaux ou de la Chine mais est cependant très orienté vers les capacités offensives. Ces capacités seraient utilisées sous la forme de frappes préemptives et éventuellement à des fins de dissuasion. Le développement de cette doctrine reste dépendant des investissements publics et privés américains

[CCTV] La Chine et l'ASEAN vont augmenter leur coopération sur le front de la cybersécurité.

La Chine et l'ASEAN ont discuté de la manière de promouvoir le développement économique régional en sécurisant et contrôlant le cyberespace. La cybermenace a augmenté dans la région du fait de son développement rapide et du nombre croissant d'utilisateurs d'internet.

[TheHindu] L'Inde reste discrète sur la surveillance de la NSA

Malgré le consensus des BRICS sur la surveillance de la NSA, l'Inde est restée plus silencieuse que les autres dans la condamnation des agissements américains, et cela même après le blocage par les pays occidentaux de la proposition de régulation du cyberespace par les Nations Unies.

[TheEpochTimes] La Chine aurait installé des backdoors dans certains équipements de l'armée américaine

Des chercheurs ont découvert une backdoor, susceptible d'avoir été intégrée lors de l'assemblage en Chine, dans une puce destinée à l'armée américaine. La puce est employée dans des systèmes d'armes, des centrales nucléaires et des systèmes de contrôle des transports publics, et peut être utilisée comme une arme à la manière de STUXNET selon eux.

[Yahoo] Israël a été frappé par une cyberattaque majeure le mois dernier

Les réseaux israéliens ont été frappés par un troyen, causant l'arrêt du trafic routier dans la ville de Haïfa. La cyberattaque n'était pas assez sophistiquée pour venir d'Iran, selon certains experts. Il a cependant été dit que cette attaque était du plus haut niveau rencontré à l'heure actuelle par Israël, et qu'une attaque similaire (contre une infrastructure) serait un élément déclencheur de conflit majeur avec Israël.

[SecurityWeek] Le Brésil lance un système d'emails sécurisés

Dans la continuité du discours officiel à l'encontre de la surveillance américaine, le gouvernement brésilien a mis en place un système de mails sécurisés qui devraient empêcher la surveillance étrangère.

[GlobalVoicesOnline] Le Brésil importe beaucoup de technologies de surveillance de masse

Dans la perspective de la Coupe du monde de 2014 et des Jeux Olympiques de 2016, le Brésil renforce sa sécurité et ses systèmes de surveillance, afin de pouvoir assurer la sécurité de la foule de visiteurs attendus. IBM et CISCO contribuent à la mise en place d'un Commandement Mobile et d'un Centre de Contrôle Mobile équipé avec des systèmes d'écoute de communications et de surveillance vidéo.

[Janes] Le Brésil et la Russie vont collaborer en matière de cybersécurité

Le Brésil et la Russie ont annoncé qu'ils avaient conclu un partenariat stratégique en matière de cybersécurité, à travers le développement de technologies communes.

Le nucléaire : leader de la coopération public-privé en matière de cybersécurité

La multiplication des cyberattaques contre les entreprises et les infrastructures d'importance vitale et l'interconnexion croissante des économies constituent aujourd'hui la première faiblesse des Etats. En effet, si les réseaux et systèmes d'information étatiques sont souvent bien protégés, il n'en est pas toujours de même pour les entreprises.

Depuis plusieurs années, des initiatives se créent pour permettre le partage d'information dans le domaine de la cybersécurité entre les entreprises et les agences fédérales (réseau Infragard[1], programme d'information pour la protection des infrastructures critiques[2], centre de coordination des infrastructures nationales[3]) mais les débats récents sur l'espionnage des entreprises américaines et sur les nombreuses cyberattaques lancées contre celles-ci ont renforcé l'idée selon laquelle une véritable stratégie de protection des entreprises était nécessaire. Un domaine fait cependant figure d'exemple dans la politique de cybersécurité : le nucléaire.

Le nucléaire : une coopération public-privé avancée

Le nucléaire représente près de 20% de l'énergie produite aux Etats-Unis grâce à 104 centrales nucléaires établies à travers le pays. Les Etats-Unis sont aujourd'hui le premier producteur d'énergie nucléaire au monde[4]. A ce titre, le secteur du nucléaire est un segment critique de l'économie américaine et peut être qualifié d'infrastructure d'importance vitale[5]. L'industrie du nucléaire s'est regroupée au sein de l'Institut de l'énergie nucléaire[6] dont l'objectif est de promouvoir l'utilisation de ces technologies devant les institutions fédérales. Il participe donc à l'élaboration du cadre juridique en la matière et se veut un forum pour apporter des solutions aux enjeux techniques et économiques.

Si la cybersécurité n'était pas une priorité du secteur, les attentats du 11septembre 2001 ont amené ce sujet dans le spectre d'étude de la Commission de régulation du nucléaire lorsque celle-ci a obligé les centrales à renforcer leur sécurité, la cybersécurité en faisant partie. En 2002, les cyberattaques étaient incluses dans la liste des menaces pesant sur le nucléaire. C'est en 2005 que la Commission de régulation du nucléaire a adopté une liste de recommandations pour aider les centrales nucléaires à établir et à maintenir une politique en matière de cybersécurité. Ces recommandations avaient été développées par l'Institut de l'énergie nucléaire c'est-à-dire par les acteurs de l'industrie nucléaire eux-mêmes avant d'être reprises par la Commission de régulation. Au moment de leur adoption il existait donc un consensus général sur les besoins en matière de cybersécurité, ce qui a nettement facilité leur mise en œuvre. Sur le plan de la coopération entre l'administration fédérale et le secteur privé, le cas du nucléaire fait donc figure d'exemple.

[1] https://www.infragard.org/
[2] http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program
[3] http://www.dhs.gov/national-infrastructure-coordinating-center
[4] World Nuclear Association, "Nuclear Power in the USA", 31 juillet 2013, disponible sur http://www.world-nuclear.org/info/Country-Profiles/Countries-T-Z/USA--Nuclear-Power/#.UihU2j-Gky4
[5] Le USA PATRIOT Act définit les infrastructures d'importance vitale comme "les systèmes et actifs, physiques ou virtuels, si vitaux aux Etats-Unis que leur incapacité ou destruction aurait un impact débilitant sur la sécurité, la sûreté économique nationale, la santé et la sécurité publique ou la combinaison de ces questions"; Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct
Tettorism (USA PATRIOT ACT) ACT OF 2001, PUBLIC LAW 107–56—OCT. 26, 2001, Section 1016 (e)
[6] http://www.nei.org/

Un autre sujet qui fait aujourd'hui débat, celui de la notification en cas de cyberattaque, a également fait l'objet d'une réglementation. En effet, dès 2009, la Commission de régulation a obligé les centrales nucléaires à notifier les incidents ayant ou pouvant avoir un impact sur leur sécurité, l'aspect cybersécurité étant inclus[7]. Le secteur de l'énergie dans sa globalité est également soumis à cette obligation dans la mesure où toute faille dans la cybersécurité des entreprises devra être notifié au Centre d'analyse et de partage d'informations du secteur de l'électricité (ES-ISAC) conformément au standards CIP-008[8]. Le secteur de l'énergie, et du nucléaire en particulier, est donc très avancé dans la mise en œuvre de hauts standards de cybersécurité. Il démontre bien que la coopération public-privé constitue le socle de toute politique de cybersécurité.

Vers une extension de ce cadre à toutes les entreprises

Le début d'année 2013 aura été marqué par une succession d'échanges véhéments entre les Etats-Unis et la Chine sur la question de l'espionnage industriel. L'activité normative de l'administration fédérale a franchi une étape lors de la publication d'un décret présidentiel le 12 février 2013 intitulé « Améliorer la cybersécurité des infrastructures critiques ». Ce décret organise le partage d'informations entre le secteur privé et les agences fédérales et confie à l'Institut national des standards et des technologies le soin de rédiger, en coopération avec le secteur industriel, un guide de la cybersécurité dont une version préliminaire a été publiée le 28 août 2013[9]. La méthodologie adoptée par l'Institut a pour objectif de faire adhérer les décideurs du secteur privé aux futurs règles et standards afin de faciliter leur mise en œuvre par les entreprises. En revanche, contrairement à ce qui s'est fait dans le domaine du nucléaire, le guide n'a pas pour mission de remplacer la politique de cybersécurité d'une entreprise, simplement de l'épauler pour l'améliorer. Ce guide se décompose en trois parties. Une première partie est dédiée aux pratiques et références des opérateurs d'importance vitale et présente celles qui sont le plus à même d'assurer un haut niveau de cybersécurité, dégageant cinq grandes fonctions stratégiques (identifier, protéger, détecter, dépondre, récupérer) auxquelles elles doivent répondre. La deuxième partie explique comment mettre en œuvre les recommandations et enfin la troisième décrit comment gérer la cybersécurité pour chaque grande fonction déterminée dans la première partie. La version finale de ce guide est attendue pour le mois de février 2014. En attendant sa publication, dans la continuité de sa méthode de travail, l'Institut recueille l'avis des industriels sur la version préliminaire.

Si ce guide n'a pas vocation à contenir des règles obligatoires, une proposition de loi[10] comportant des normes en matière de cybersécurité est en passe d'être votée par le Sénat. Alors que la commission du commerce avait déjà échoué par deux fois à se mettre d'accord, elle l'a adoptée fin juillet. Elle a pour objectif de *"fournir une coopération public-privé dynamique et volontaire afin d'améliorer la cybersécurité, de renforcer le développement et la recherche en matière de cybersécurité, le développement d'une main d'œuvre et de programmes éducatifs ainsi que la vigilance et la préparation du public"*[11]. Elle vient codifier la compétence de l'Institut national des standards et des technologies dans l'émergence de standards et de bonnes pratiques pour la cybersécurité et insiste sur l'importance de la collaboration entre le secteur privé et l'administration pour aboutir à cet objectif.

Afin d'encourager l'application des standards et pratiques qui seront adoptés, la Maison Blanche mène des consultations avec différentes agences fédérales pour établir une liste d'avantages dont pourraient bénéficier

[7] Nuclear regulatory commission Code of Federal regulations, "Reporting of Safeguards Events", 10 CFR 73.71
[8] http://www.wecc.biz/Standards/BCApproved%20Standards/CIP-008-1.pdf
[9] NIST, *Discussion Draft of the Preliminary Cybersecurity Framework*, 28 août 2013, disponible sur http://www.nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf
[10] Cybersecurity Act, S 1353 - 113th Congress (2013-2014), disponible sur http://www.govtrack.us/congress/bills/113/s1353/text
[11] Cybersecurity Act, *op. cit.*

les entreprises mettant en œuvre les standards établis. Une première liste de huit avantages a été publiée par la Maison Blanche afin de présenter l'état d'avancement de ses travaux. A titre d'exemple on peut citer la mise en place d'une assurance pour les entreprises adoptant les standards de cybersécurité, l'octroi de subventions supplémentaires ou encore des immunités en cas de dommage. Les entreprises appliquant les standards et bonnes pratiques et bénéficiant à ce titre des avantages décidés par l'administration fédérale seront regroupées au sein d'un programme volontaire pour la cybersécurité des infrastructures d'importance vitale qui sera créé en février 2014. A moyen terme, l'objectif de l'administration Obama est de rendre obligatoire la notification en cas d'incident.

Si les premières réactions d'experts en sécurité informatique sont très critiques quant à la capacité des standards et bonnes pratiques élaborés à assurer un niveau élevé de cybersécurité et à protéger efficacement les opérateurs d'importance vitale[12], il faut cependant saluer les efforts entrepris pour renforcer la cybersécurité dans les entreprises. L'échange d'information constitue un des fondements de la politique de cybersécurité des Etats-Unis et s'effectue dans les deux sens, les agences de renseignement commençant à partager des informations avec les infrastructures critiques sur de possibles menaces et vulnérabilités dont elle ne pourrait pas avoir connaissance en ayant recours à de simples sources ouvertes. Cependant, si les discours catastrophistes tenus par les membres de l'administration fédérale et des agences de renseignement[13] participent à l'acceptation du principe d'échange d'informations, ils donnent également un fondement à plus de surveillance des entreprises sous couvert de leur protection. Mais cette mutation des relations entre le secteur public et le secteur privé n'est pas propre aux Etats-Unis, le même processus étant engagé en Europe où la lutte contre les cyberattaques devient une préoccupation majeure.

[12] Antone GONSALVES, "NIST cybersecurity framework proposal provides no measurable cybersecurity assurance", *CSO*, 5 septembre 2013, disponible sur http://www.csoonline.com/article/739139/nist-cyber-security-framework-proposal-provides-no-measurable-cybersecurity-assurance-

[13] Robert K. ACKERMAN, "Cyber Command Call for Consolidated Activities", *Signal Online*, 12 juin 2013, disponible sur http://www.afcea.org/content/?q=node/11185 ; Mike LEVINE, "Outgoing DHS Secretary Janet Napolitano Warns of 'Serious' Cyber Attack, Unprecedented Natural Disaster", ABC News, 27 août 2013, disponible sur http://abcnews.go.com/blogs/politics/2013/08/outgoing-dhs-secretary-janet-napolitano-warns-of-serious-cyber-attackunprecedented-natural-disaster/

PRISM

Contexte et enjeux

PRISM est le premier programme de collecte de données révélé par Edward Snowden à travers les publications le 6 juin 2013 du *Guardian* et du *Washington Post*. Egalement appelé *US-984XN*, ce programme collecte des données directement dans les serveurs d'entreprises américaines. Cette méthode, appelée « *downstream* », est complétée par l'interception « *upstream* » de communications transitant principalement à travers les câbles internet sous-marins.

Si la collecte massive de données n'est pas une tendance nouvelle au sein de l'armée américaine - l'Information Dominance Center ayant commencé ses tests sur Internet dès 1999 - celle-ci a pris une ampleur croissante et a soulevé de nombreuses interrogations quant à sa légalité et son efficacité. PRISM apparaît comme l'aboutissement de ce besoin croissant d'accumulation de données par la *National Security Agency* (NSA) et il convient de ce fait d'analyser les raisons de sa mise en place, son mode de fonctionnement et son efficacité par rapport aux conséquences économiques auxquels les Etats-Unis sont confrontés.

Les raisons d'une montée en puissance de la collecte massive de données

Les origines du programme PRISM peuvent être trouvées dans les décisions politico-militaires au cours de ces vingt dernières années, avec une importance croissante donnée au cyber et au renseignement électromagnétique s'accompagnant d'un cadre juridique permissif et ne disposant que de peu d'instruments de contrôle.

Le volontarisme d'acteurs politiques et militaires

Bien qu'il soit difficile d'établir les liens exacts entre les différents acteurs ayant autorisé et favorisé le développement des programmes de collecte massive de données, il est possible de faire ressortir des tendances au sein des politiques et militaires américains.

La première est liée à l'application des moyens *Big Data* au contre-terrorisme au début des années 2000, à travers la mise en place dès 1999 d'un moteur de recherche et de collecte de données sur internet, mis en place par *l'Information Dominance Center*. En 1999, le général Keith Alexander - directeur actuel de la NSA - était à la tête de ce centre et a continué par la suite à demander des moyens croissants pour collecter des données. L'opposition en 2001 entre le général Alexander et le directeur de la NSA de l'époque, Michaël Hayden, est alors révélatrice de deux visions : d'une part, la volonté de collecter un maximum de données dans le cadre de la lutte antiterroriste, et d'autre part la volonté de respecter un cadre juridique protecteur pour les citoyens américains. Malgré l'opposition de Hayden, le général Alexander fut nommé en 2005 à la tête de la NSA et initia en 2007 le programme PRISM avec une première entreprise : Microsoft.

La seconde tendance est la forte sensibilisation de l'administration des présidents Bush puis Obama aux questions de cyberdéfense. Les liens entre la NSA et l'entreprise *Booz Allen Hamilton*, à travers la personne de John J. McConnell, ont permis - entre autres - à l'Agence de se doter dès les années 2000 d'une capacité cyber et de proposer des modes d'action au Président Bush dans le cadre de l'opération *Olympic Games*. Cette utilisation des moyens cyber, initiée sous la présidence de Georges W. Bush, a été intensifiée par Barack

Obama. En 2010, le *CyberCommand* nouvellement créé fut mis sous le commandement du général Alexander, s'ajoutant à ses fonctions de directeur de la NSA.

Un cadre juridique permissif et ne disposant que de faibles instruments de contrôle

Le cadre juridique autorisant le programme PRISM est le *Foreign Intelligence Surveillance Act* (FISA), amendé en 2008 afin de permettre au gouvernement américain d'espionner les communications des étrangers à l'étranger. Il autorise la collecte de données sur les communications étrangères ou entre un citoyen américain et un étranger. Il a été étendu jusqu'en 2017 par le Sénat américain, et spécifie que l'espionnage ne doit pas viser intentionnellement un citoyen américain ou une personne située aux Etats-Unis, et ne doit pas aller à l'encontre du quatrième amendement de la constitution des Etats-Unis qui protège la vie privée des citoyens.

Ce cadre juridique s'est avéré permissif pour la NSA car il a permis à l'Agence de collecter non intentionnellement des données sur les citoyens américains, directement dans les serveurs des entreprises participant au programme PRISM. De plus, le caractère secret du programme PRISM n'a pas permis à l'instance de contrôle compétente, la *Foreign Intelligence Surveillance Court* (FISC), d'avoir de la visibilité sur l'ampleur du programme et d'exercer son contrôle sur les actions de la NSA.

L'avance technologique et le volontarisme d'acteurs politiques et militaires américains ont ainsi contribué à l'émergence du programme PRISM en 2007, bénéficiant alors d'un cadre juridique peu contraignant.

Le fonctionnement du programme

Lancé en 2007, le programme PRISM permet à la NSA de collecter des données directement dans les serveurs d'entreprises américaines. En juin 2013, neuf d'entre elles faisaient partie du programme: Microsoft, Yahoo, Google, Facebook, Paltalk, Youtube, Skype, AOL et Apple. Au moment des révélations d'Edward Snowden, Dropbox devait être ajouté au programme. A titre d'exemple, Microsoft aurait fourni à la NSA et au FBI sa clé de chiffrement, permettant aux deux agences d'accéder aux données stockées sur Skydrive et d'intercepter les appels passés sur Skype. Les accords avec les entreprises participant au programme sont également financiers, la NSA remboursant les frais que les entreprises doivent engager pour se mettre en accord avec le cadre juridique du programme.

Les données recueillies sur les serveurs de ces entreprises stockant de très grandes quantités de données permettent ensuite aux analystes de la NSA d'effectuer des recherches à l'aide d'un outil central appelé *Xkeyscore*, qui effectue des recherches sur toutes les données collectées à travers les interceptions de communications (*upstream*) ou venant des serveurs des entreprises du programme PRISM (*downstream*). L'intérêt du programme par rapport aux interceptions de télécommunication réside dans le fait qu'il permet à la NSA d'accéder au contenu des données et non juste aux métadonnées (données externes au message telles que le nom des destinataires, la date, l'heure, les coordonnées GPS des interlocuteurs). La NSA peut ainsi collecter des vidéos, des photos, des e-mails, des documents et des identifiants de connexion.

Efficacité et conséquences de PRISM

Au-delà de l'efficacité du programme en matière de renseignement électromagnétique, il est possible de dégager certaines conséquences économiques de la révélation de PRISM.

PRISM est révélateur de la puissance du renseignement électromagnétique aux Etats-Unis, parfois au détriment des autres formes de renseignement et de son efficacité globale. L'approche uniquement basée sur le renseignement électromagnétique s'est par exemple révélée « être un complet désastre » selon certains

anciens responsables de la sécurité nationale suite à la tentative de la NSA de créer une force de réaction rapide interservices en 2010. De même, les graphes de la NSA construits à partir de la gigantesque base de données de l'agence, et baptisés B.A.G, ont été critiqués par d'autres services américains pour leur manque d'utilité opérationnelle.

Les conséquences économiques du programme PRISM sont importantes. Le discours officiel américain visant à décrédibiliser les équipementiers informatiques chinois, en insistant sur le fait que ceux-ci espionnaient pour le compte du gouvernement, et ainsi donner un avantage aux entreprises américaines du même secteur, a connu un coup d'arrêt lors des révélations de PRISM. Estimées en août 2013 à 35 milliards sur trois ans, les pertes sont principalement dues à une perte de crédibilité des entreprises américaines face à leurs concurrents, et à la difficulté pour les multinationales américaines de respecter les obligations imposées par le gouvernement américain et la politique de protection de données des autres pays.

L'impact politique des révélations du programme PRISM est essentiellement national, en montrant que la NSA agit au-delà des limites qui lui sont fixées par la loi sans, être l'objet de mécanismes de contrôle. La collecte de données sur les citoyens américains est en effet interdite par le quatrième amendement de la constitution et, bien que cette collecte soit « non intentionnelle », comme l'a rappelé lors de ses interventions le directeur de la NSA, il reste néanmoins possible pour l'Agence de faire des recherches sur ces données une fois stockées.

Au niveau international, PRISM a été peu critiqué du fait de la légalité du programme et de la collecte de données à travers les géants du web. Les premières critiques officielles sur ce qui est appelé plus généralement « l'affaire PRISM » ont été lancées par l'Allemagne à la découverte du programme *Tempora* sur les interceptions de communication en Europe, méthode « *upstream* » donc et non « *downstream* » à la manière de PRISM. Le débat sur la protection de la vie privée et des données personnelles dont se sont saisis plusieurs pays et l'Union européenne pourrait cependant influencer la légalité de la collecte d'informations du programme PRISM.

Premier programme révélé par les documents d'Edward Snowden, le programme PRISM est avant tout une preuve de la montée en puissance de la NSA et de la difficulté pour les autorités américaines d'exercer un contrôle sur les actions de l'Agence. Ce programme fournit à moindre coût une très grande quantité de données qui ne se limitent pas aux métadonnées, et représente en ce sens un très bon complément aux collectes de données « *upstream* ». Les conséquences du programme concernent avant tout la compétitivité des entreprises américaines et le respect du droit américain, et suscitent un débat intense au niveau national sous la pression des lobbys et des politiques américains.

Le portail OMC
La plateforme de la DAS

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

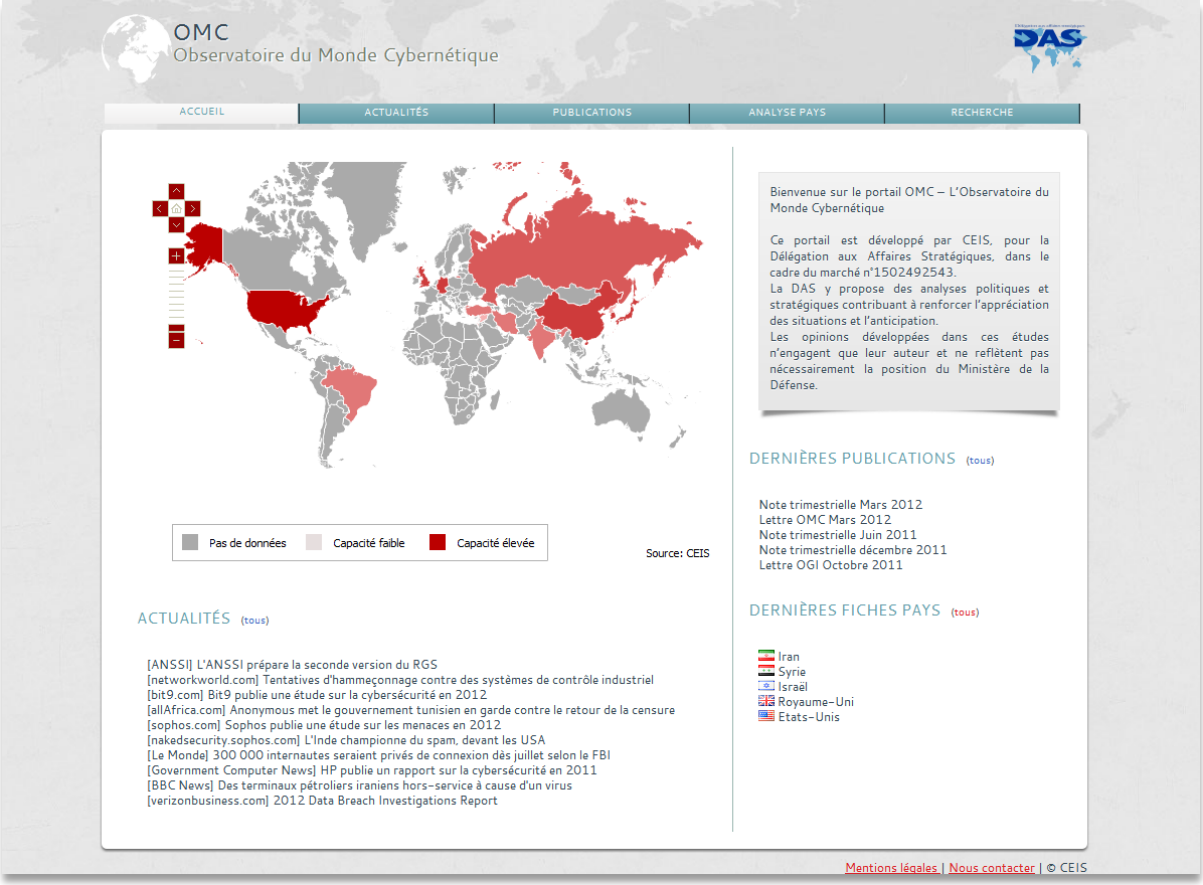

Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

L'accès au portail est réservé aux organisations publiques.

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

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

API Cybersecurity Conference & Expo	Houston, Etats-Unis	12-13 novembre
Oil and Gas Cybersecurity Conference	Londres, Royaume-Uni	
19th Azerbaijan International Telecommunications and Information Technologies Exhibition and Conference	Baku, Azerbaïdjan	25 novembre
ASE Cyber Security Conference	Orlando, Etats-Unis	2-5 décembre
Botconf'13	Nantes	5-6 décembre
Secutic Day PACA	Marseille	10 décembre
Colloque annuel du CDSE	Paris	19 décembre
Forum International de la Cybersécurité	Lille	21 – 22 janvier

CEIS

Compagnie Européenne
d'Intelligence Stratégique

Téléphone : 01 45 55 00 20
Télécopie : 01 45 55 00 60
E-mail : gtissier@ceis.eu

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