Observatoire du Monde Cybernétique

Lettre n°16 – Avril 2013

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

[Défense.gouv.fr et Challenges] Livre blanc sur la défense et la sécurité nationale : La cyberdéfense et le renseignement érigés en priorité nationale

Le Livre blanc de la Défense de 2013 fait la part belle à la cyberdéfense. L'affirmant en tant que priorité nationale, il évoque la lutte informatique offensive. Il est également indiqué qu'une attaque informatique de grande ampleur sera considérée par la France comme un acte de guerre. Une chaîne de commandement centralisée à l'état-major pour les armées sera chargée de développer les capacités offensives, la partie défensive demeurant une prérogative interministérielle. Le Livre blanc 2013 vise l'autonomie dans la production de systèmes de sécurité, envisage de renforcer les effectifs pour ces missions, et annonce la mise en place d'une réserve opérationnelle et d'une réserve citoyenne pour la cyberdéfense.

[Sénat] Proposition de résolution sur la proposition de directive du Parlement européen

Suite à la publication par le Parlement européen de la stratégie européenne de cybersécurité et du projet de directive correspondant, le Sénat français réagit par une proposition de résolution. Par cette proposition de résolution, le Sénat « se félicite de la publication de la stratégie européenne de cybersécurité, qui témoigne d'une approche globale et cohérente de l'Union européenne des risques et des enjeux soulevés par la multiplication des attaques contre les systèmes d'information et de communication » et appelle les institutions européennes et les Etats membres à une mise en œuvre rapide des priorités énoncées par la nouvelle stratégie européenne de cybersécurité.

[Programmez] Création de l'European Cyber Security Group (ESCG)

Un groupe d'entreprises européennes de sécurité de l'information ont annoncé la formation d'un consortium de cyberdéfense. L'European Cyber Security Group (ECSG) regroupe notamment S21sec, LEXSI, CSIS et Fox-IT.

Composé de 600 experts, l'ESCG veut proposer les services les plus complets et rapides pour les entreprises et les gouvernements.

[Europa] La Commission européenne se réjouit de l'extension du mandat de l'ENISA

Le Parlement européen a massivement approuvé l'extension du mandat de l'ENISA et le renforcement de la cybersécurité européenne.

Un nouveau mandat de 7 ans a été accordé à l'Agence européenne chargée de la sécurité des réseaux et de l'information, désormais placée au centre de la nouvelle stratégie européenne de cybersécurité. L'agence va ouvrir une branche à Athènes, en supplément de son siège à Héraklion, pour se rapprocher de ses partenaires.

[e-orientations] L'institut Leonard de Vinci lance un MBA « Sécurité des réseaux numériques »

Suite à la mise en exergue, par le rapport Bockel, du fait que les formations dédiées à la cybersécurité ne couvrent qu'un quart des besoins de recrutement, l'Institut Léonard de Vinci annonce le lancement d'un MBA « Sécurité des réseaux numériques ». Le cursus a pour objectif de former des experts de l'IT et des stratèges du management de la cybersécurité et de l'économie numérique.

[01net] Pays-Bas : l'identification électronique nationale plombée par une attaque DDoS

Mercredi 24 avril, le système DigiD, qui permet aux citoyens hollandais de s'authentifier auprès de la quasi-totalité des services publics en ligne, a été rendu indisponible suite à une attaque DDoS. Ce service est utilisé par près de 60% de la population, l'attaque touchant ainsi près de 10 millions de personnes.

[L'Entreprise] Le gouvernement anglais offre des subventions aux PME pour améliorer leur sécurité informatique

Le ministre britannique chargé des Sciences et des Universités David Willetts a présenté son programme d'investissement en matière d'innovation et de technologie. Le gouvernement annonce qu'il accordera jusqu'à 5.000 livres aux PME britanniques pour qu'elles améliorent leur cybersécurité. Cette incitation financière devrait pousser les petites entreprises jusqu'alors peu concernées à renforcer leur sécurité.

[Bloomberg] Les réseaux des navires de combat américains sont pénétrables

Des spécialistes en cybersécurité de la Navy américaine ont mené des tests de vulnérabilité sur les réseaux de nouveaux navires de combat en zone littorale, et y ont détecté de graves défaillances. Dans un rapport qui n'a pas été publié, les spécialistes affirment que ces réseaux sont vulnérables aux cyberattaques et doivent donc être sécurisés de toute urgence.

[Forbes] Un chercheur aurait trouvé une faille dans les systèmes de navigation d'avions

Hugo Teso, chercheur pour la société allemande N.Runs, a affirmé avoir découvert une faille dans les systèmes de navigation des avions fabriqués par des sociétés telles que Honeywell, Thales et Rockwell Collins. Il a affirmé pouvoir depuis son téléphone modifier la direction, l'altitude et la vitesse de vol en exploitant le manque d'authentification du protocole ACARS (Aircraft Communications Addressing and Report System). Si avérées, de telles failles représenteraient un risque considérable que les sociétés en question ont déclaré prendre très au sérieux.

[BusinessInsider] Les Bitcoins, cible des cybercriminels

Les chercheurs de Kaspersky Lab ont repéré un virus lancé sur Skype, qui générerait de la monnaie virtuelle. Via une campagne classique de spam, les criminels introduisent dans l'ordinateur des victimes un logiciel malveillant, peu détecté par les antivirus, qui leur permet de générer de la monnaie bitcoins depuis ces ordinateurs. Les bitcoins, échangés à environ 130 dollars l'unité, ont été créés en 2009 lors de la crise financière pour proposer une alternative aux monnaies contrôlées par les banques centrales, et profitent d'un récent essor qui attire donc désormais les convoitises des cybercriminels.

[LeMonde] Le CISPA voté par la Chambre des représentants américaine

Le Cyber Intelligence Sharing and Protection Act (CISPA), loi de protection et de partage des renseignements sensibles entre entreprises et autorités américaines, a été voté à une large majorité à la Chambre des représentants américaine. Ce texte permet le partage d'informations sensibles entre équipementiers, entreprises et le gouvernement au nom de la cybersécurité. Il n'y aurait pas dans le texte d'obligation de divulguer les attaques subies. Ce projet de loi, contesté, ne satisferait même pas la Maison Blanche dans sa forme actuelle.

[01Net] Les Anonymous peinent à créer un blackout du Web contre CISPA

Le groupe Anonymous a lancé un appel à la mobilisation en ligne contre le projet de loi CISPA, validé par la chambre des représentants américaine. Jugeant qu'il s'agissait d'une résurrection des projets SOPA et PIPA auxquels ils s'étaient vivement opposé, les Anonymous ont appelé à organiser un blackout d'Internet, le 22 avril. Quelques 430 sites ont répondu à l'appel, essentiellement des blogs et sites personnels, ce qui reste un chiffre relativement faible comparé à la mobilisation contre SOPA ou PIPA.

[NoVAInfosec] Le responsable du pôle cybersécurité de la DARPA recruté par Google

Peiter Zatka a quitté le poste qu'il occupait à la DARPA en tant que responsable des activités de recherche sur la cybersécurité pour un poste au sein de l'équipe Motorola Mobility de Google.

[LeMonde] La police japonaise recommande le blocage du réseau TOR

La National Police Agency (NPA), l'agence de coordination de la police japonaise, souhaite que

les fournisseurs d'accès Internet bloquent l'accès au réseau anonyme TOR (The Onion Router).

[AlShorfa] Les pays arabes travaillent à la lutte contre le cyberterrorisme

Les pays arabes se rapprochent de l'adoption d'une stratégie unifiée de lutte contre le cyberterrorisme. Les experts des pays du Golfe constatent une explosion du recours à Internet par les terroristes dans des démarches de financement et de planification des opérations, et appellent à développer un cadre juridique permettant d'entraver ces activités. Les dirigeants arabes souhaitent développer la coopération entre pays du Golfe, sur la base d'échanges d'informations sur des individus via le Bureau de la Police Criminelle Arabe.

[Idg] L'Arabie Saoudite devrait investir 400M$ dans la prévention de perte de données

Selon une étude de marché conduite par le groupe InfoWatch, l'Arabie Saoudite devrait investir jusqu'à 400M$ dans la prévention de perte de données, et ce dans les cinq prochaines années. Selon le rapport, en 2012, plus de 1 milliard de données auraient été compromises.

[LaTribune] Les experts algériens préconisent une approche globale contre les cyber-attaques

Une conférence sur la stratégie de cybersécurité algérienne s'est tenue le 7 avril à l'Ecole nationale supérieure des sciences politiques, à Alger. De nombreux experts nationaux en la matière y ont participé et ont appelé au développement d'une stratégie privilégiant une approche nationale globale de prévention contre les cyberattaques et de protection des institutions et organismes publics.

L'Algérie développe déjà une approche défensive à travers l'achat d'équipements de protection, et devrait de l'avis de certains développer une approche offensive pour faire face à toute forme d'attaque, ainsi qu'un cadre juridique adéquat.

[RIANovosti] La police russe prévoit de dépenser 1,3 million de dollars en cyberdéfense

Le ministère de l'intérieur russe a annoncé l'allocation de près d'1,3 million de dollars au développement d'un système de sécurité protégeant ses réseaux informatiques des cyberattaques. Ce système devra être capable de détecter et bloquer les intrusions, et devra être similaire à ceux déployés par le FSB, les services de sécurité russes.

[Reuters] Les Etats-Unis et la Chine vont travailler ensemble sur la cybersécurité

Un groupe de travail sino-américain sur la cybersécurité devrait être constitué, d'après le secrétaire d'Etat américain John Kerry. A l'occasion d'une visite en Chine après des mois de tensions et d'accusations mutuelles de piratage, John Kerry a affirmé que les deux pays s'étaient entendus sur le besoin d'accélérer les mesures de cybersécurité et de nourrir le dialogue.

[TheHindu] Des hackers indiens défacent 37 sites brésiliens

En réplique au piratage de sites indiens par le groupe "hi tech Brazil hack team", des pirates indiens ont pris le contrôle de 37 sites brésiliens, y laissant un message provocateur invitant à davantage d'actions. L'ampleur de l'attaque brésilienne contre les serveurs indiens n'a pas été évaluée avec précision, mais le CSRT (Cyber Security Response Team) indien suspecte qu'une quantité non-négligeable de données aurait été dérobée ou endommagée. Des statistiques du CSRT font état plus de 16,000 sites indiens piratés chaque année.

[TheNewZelandHerald] Des hackers tentent de dérober de la technologie militaire néo-zélandaise

Le premier ministre néo-zélandais John Key a révélé que les agences de renseignement nationales ont détecté des tentatives de piratage de données technologiques pouvant être utilisées dans la conception d'armes de destruction massive. Il en a profité pour réaffirmer le besoin de modifier la législation nationale en faveur d'une meilleure protection contre le cyberespionnage, en autorisant la surveillance des citoyens par les autorités.

[DAS] L'utilisation stratégique du cyberespace au Moyen-Orient

La Délégation aux Affaires Stratégiques (DAS) a publié l'étude confiée à Olivier Danino sur l'utilisation stratégique du cyberespace au Moyen-Orient. Le document revient entre autres sur l'utilisation faite du cyberespace par les groupes étatiques et non-étatiques de la région, distinguant les groupes terroristes, insurgés et blocs étatiques, adoptant des stratégies institutionnelles (Israël), asymétriques (Iran et Syrie), structurées autour de CERTs (pays du Golfe) ou tournées vers des structures extérieures (Turquie).

[CICDE] Le CICDE publie une note de réflexion sur les réseaux sociaux et les forces armées

Le Centre interarmées de concepts, de doctrines et d'expérimentations (CICDE) a publié une Réflexion doctrinale interarmées (RDIA) intitulée "Réseaux sociaux, Nature et conséquences pour les forces armées". Dans cette note, le CICDE rappelle la pleine expansion des réseaux sociaux et le bouleversement des circuits traditionnels de la communication qu'ils induisent. Ce bouleversement est à l'origine de risques pour les armées, en termes d'intrusion numérique, de divulgation de données sensibles ou de difficulté à conduire une communication de crise ; mais est également à l'origine d'opportunités dans les domaines opérationnels et sociétaux. Le CICDE invite donc à s'interroger sur l'usage des réseaux sociaux pour les forces armées et à anticiper leur évolution pour faire face aux risques potentiels, encadrer les pratiques émergentes au sein de la communauté internaute militaire et saisir les opportunités en matière opérationnelle.

[ZDNet] 30% des attaques informatiques réalisées depuis la Chine

Verizon a publié une étude sur l'origine des attaques par vol de données. Selon ces analyses, 30% des fuites de données examinées sont consécutives à une intrusion depuis une adresse IP chinoise. Dans 96% de ces cas d'intrusion, la motivation serait liée au cyberespionnage. Mais de manière plus surprenante, la Roumanie se classe deuxième de ce classement avec un taux de 28%. Les attaques originaires de Roumanie sont cependant quasi exclusivement motivées par la recherche de profit. Les Etats-Unis occupent la troisième place, avec 18%. Suivent la Bulgarie (7%) et la Russie (5%).

[TribLive] La cyberguerre grimpe dans la liste des priorités du Pentagone

Les Etats-Unis ont publié leur budget de Défense pour 2014, donnant un aperçu budgétaire de leurs capacités cybernétiques. Ainsi, le budget alloué à la cyberguerre passera de 3,9 à 4,7 milliards de dollars, une grande partie de ce budget étant allouée au développement de capacités offensives.

[Symantec] Internet Security Threat Report 2013

Le nombre de cyberattaques ciblées a augmenté de 42% en 2012 dans le monde, selon un rapport de Symantec. Ces attaques ciblées, relevant du cyberespionnage, touchent de plus en plus le secteur industriel ainsi que les PME de moins de 250 salariés (qui sont la cible de 31% de ces attaques). A noter que les cybercriminels visent les chaines logistiques et les écosystèmes de sous-traitants pour accéder aux informations sensibles des grandes entreprises et à une des données à forte valeur.

[mod.gov.cn] La Chine publie son livre blanc de la défense et y évoque le cyberespace

La Chine a publié son huitième livre blanc de la défense depuis 1998. Il n'y est pas fait mention des capacités informatiques dont disposerait l'armée chinoise, mais le document rappelle la position du pays sur les différents espaces de conflit, mentionnant le cyberespace à deux reprises. Ainsi la Chine affirme la posture de défense active de ses forces armées contre les agressions et autres menaces pesant sur les intérêts nationaux dans l'atmosphère et le cyberespace, se réservant également le droit de contre-attaquer en cas d'agression.

L'Europe, colonie du monde numérique ?

L'Europe est-elle devenue « une colonie du monde numérique » ? Tel est le titre, un rien provocateur, du rapport présenté au nom du Sénat par Mme Catherine Morin-Desailly[1]. Le constat est sans appel : *« le numérique défie la vieille Europe. Il ébranle la puissance économique traditionnelle en captant la valeur et en bouleversant secteurs et marché ; il se joue de l'impôt et exploite la concurrence fiscale entre Etats membres de l'Union européenne ; il défie les règles de droit et fait advenir dans le cyberespace des règles concurrentes aux règles étatiques ».* **Le constat est certes déjà connu, mais jamais un rapport n'avait dressé une vision aussi globale et politique de la situation.**

Les raisons du retard européen au plan numérique sont nombreuses : cloisonnement des marchés, manque d'interopérabilité, insuffisance des investissements dans les réseaux, rareté des compétences… Mais ce retard est aggravé par l'absence de vision politique globale dans le domaine numérique, au point que l'on peut parler aujourd'hui d'un véritable recul européen. « *Sur les 9 sociétés d'application TIC figurant sur la liste Financial Time Global 500, une seule est européenne. Et sur les 54 sites web les plus visités en Europe, seulement quatre sont d'origine européenne. »* Pendant des années, l'Europe a finalement promu l'usage du numérique, mis l'accent sur le « *bien-être du consommateur européen* », sur le développement des infrastructures, en oubliant tout simplement de favoriser le développement des offres de services et de contenus correspondantes, accentuant de ce fait la domination américaine. Le résultat est que l'Europe a reculé à la fois sur les équipements face à l'Asie mais aussi face aux Etats-Unis en matière de services intermédiaires et de contenus (les « Over the top » ou OTT), là où les taux de marge sont les plus élevés.

A côté des infrastructures, il apparait donc essentiel de promouvoir le développement de services européens, de la gestion des identités jusqu'aux systèmes de paiement. Le rapport constate qu'il est d'ailleurs regrettable, alors que Visa et Mastercard assurent déjà respectivement 35 et 22 % des opérations de paiement par carte dans l'Union, que les trois projets de schémas de paiement 100 % européens initiés par SEPA, Payfair, Monnet et EAPS n'aient pu pour l'instant s'imposer.

Trois défis

Le défi est donc d'abord économique et industriel : le numérique ne doit pas être considéré comme un simple secteur industriel mais comme un « facteur de renversement des modèles d'affaires existant » et un levier de croissance qui imprègne progressivement l'ensemble des secteurs. Un rapport de l'Inspection Générale des Finances[2] publié en 2012 estimait le poids du numérique à 5,2 % du PIB et 1,15 millions d'emplois en 2009. A cette contribution directe, il faut encore ajouter la contribution indirecte : Internet aurait contribué au quart de la croissance en 2010, et pourrait même représenter selon la société de conseil McKinsey la moitié de la croissance d'ici 2015. Près de 80 % de l'économie française est ainsi concerné par l'économie numérique, phénomène encore accentué par le *business model* phare de l'ère numérique basé sur l'intermédiation.

Avec le développement de ce modèle, le défi est également fiscal. « *Malgré une intense activité sur le territoire des Etats Membres de l'Union européenne, les grandes entreprises du numérique ne paient*

[1] http://www.senat.fr/rap/r12-443/r12-4431.pdf
[2] http://www.igf.finances.gouv.fr/webdav/site/igf/shared/Nos_Rapports/documents/2012/2011-M-060-02.pdf

quasiment pas d'impôt en Europe, relève le rapport. *Alors qu'elles captent une part croissante de la valeur ajoutée au détriment des autres acteurs de la chaîne de valeur* ». Fiscalité et numérique font en effet mauvais ménage : technologies et modèles d'affaire évoluent trop vite, les actifs sont incorporels, lieux d'établissement et de consommation sont de plus en plus dissociés. Un exemple (non cité dans le rapport) : le Conseil régional de Bretagne a décidé en novembre 2012 de confier la gestion de son infrastructure informatique non critique à la société américaine Amazon, dont les infrastructures européennes sont basées en Irlande.

C'est en fait tout simplement la souveraineté des pays européens, c'est à dire l'autorité effective d'un Gouvernement sur un territoire géographique, qui est en cause : « *celles de certains pays [sont] étendues, d'autres [sont] réduites en proportion de l'implantation respective des opérateurs internet* ». Grâce à ces opérateurs, les Etats-Unis disposent d'un levier formidable et bénéficient d'une sorte « *d'extension extra territoriale de leur souveraineté* », laquelle devrait encore progresser avec les services de cloud. Comme l'explique Pierre Bellanger, PDG de Skyrock, « *l'objectif n'est plus seulement de ne plus avoir besoin des autres nations, mais aussi que les autres nations aient besoin de soi* »[3].

Quelles solutions ?

Face à ces défis, quelles sont les solutions proposées par le rapport ? Au plan politique, il s'agit d'abord « *d'institutionnaliser le caractère politique et transversal de l'ambition numérique de l'Union européenne* » en créant une formation du Conseil de l'Union dédiée aux questions numériques. Il importe également d'encadrer la politique de la concurrence par des objectifs politiques en termes de sécurité des réseaux, de maîtrise des données, de promotion de la neutralité du net, de promotion de l'industrie numérique européenne[4]. A l'image des Etats-Unis, où la politique anti-trust n'est jamais déconnectée de la politique industrielle, comme l'a souligné lors d'une audition M. Marc Mossé, directeur des affaires juridiques et publiques de Microsoft France.

Les outils de la politique de la concurrence ne suffisent cependant pas. Il faut aussi actualiser la réglementation sectorielle en matière de numérique, indique le rapport qui plaide pour la création de règles pour les moteurs de recherche, réseaux sociaux ou fournisseurs de contenus et d'application. Il s'agirait par exemple de transposer la notion de facilité essentielle en vertu de laquelle « *une entreprise qui possède ou utilise elle-même une installation essentielle, c'est à dire sans laquelle ses concurrents ne peuvent offrir de services à leurs clients et qui leur refuse l'accès à cette installation, abuse de sa position dominante* »[5].

Au plan règlementaire et normatif, attention, cependant, à ne pas se tirer une balle dans le pied en créant des règles qui seront rapidement inadaptées par rapport aux usages et pourraient entraver l'innovation. M. Stéphane Grumbach, directeur de recherche à l'INRIA déplore par exemple que *« l'Europe s'interdise de*

---

3 http://www.skyrock.fm/bellanger/de la souverainete en general et de la souverainete numerique en particulier.pdf

4 Voir à ce sujet la communication de la Commission européenne intitulée « une industrie européenne plus forte au service de la croissance et de la relance économique » dans laquelle le numérique occupe une place importante : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0582:FIN:FR:PDF

5 CJCE, 3 octobre 1985, aff. 311/84 CBEM, dit Telemarketing. Lire à ce propos l'article suivant : http://www.art-telecom.fr/fileadmin/reprise/communiques/lettre/pdf/lettre59-page21-infra-reg.pdf

travailler sur ses données et même en fasse cadeau à d'autres, effet paradoxal de l'extrême attachement des européens au respect de la vie privée et de leur hantise des fichiers de personnes développées par les totalitarismes ». La prudence devra également être de mise lors des discussions sur la fiscalité du numérique et la notion « d'établissement stable virtuel » évoquée par le Gouvernement dans sa feuille de route numérique.

Une politique industrielle active

Il faut en fait se garder de toute position dogmatique. La protection de la vie privée ne saurait être abordée sous un angle exclusivement juridique, tant les données sont devenues un enjeu concurrentiel et constituent un nouvel « or noir ». Le Boston Consulting Group estimait en 2012 que les données personnelles collectées auprès des utilisateurs européens pouvaient être valorisées à 315 milliards d'euros et pourraient à terme représenter 1 000 milliards d'euros. Même pragmatisme sur les aides d'Etat : les restrictions auxquelles sont soumises les entreprises européennes constituent souvent un handicap. Il faut donc promouvoir une harmonisation des règles du jeu grâce à la politique commerciale commune, à la fois au niveau multilatéral et dans le cadre des accords bilatéraux et régionaux, tout en utilisant avec fermeté le levier de la réciprocité. « *L'Union européenne ouvre 95 % de ses marchés publics aux pays tiers, mais, en retour, nos entreprises subissent des pratiques discriminatoires : seulement 32 % des marchés américains et 28 % des marchés japonais sont ouverts* », souligne le rapport.

Le soutien à l'industrie numérique passe également par l'achat public, largement utilisé dans le monde, y compris dans des pays libéraux comme les Etats-Unis, le Japon ou la Corée du Sud. Exemple : le système américain d'APAC (achat public avant commercialisation) via deux programmes non fiscaux : le Small Business Innovation Research (SBIR) et le Small Business Technology Transfer (STTR). De façon concrète, ces programmes d'APAC se déroulent en trois temps : 1. Appel public à la concurrence et attribution de subventions limitées pour que les entreprises démontrent la faisabilité de leur projet, 2. Attribution d'un marché avec les entités sélectionnées lors de la première phase pour financer la R&D (entendue au sens large puisqu'en matière numérique, la R&D est moins technologique que liée aux modèles d'affaires ou au marketing), 3. Passation d'un marché public avec les lauréats de la seconde phase et introduction de l'innovation sur le marché privé.

La politique industrielle doit enfin s'appuyer sur un tissu d'investisseurs dynamique. La croissance du numérique est en effet intimement liée au capital-risque, tant en phase d'amorçage, de décollage ou de développement. Or le retard européen est patent dans le domaine : faible liquidité des places financières, frilosité des fonds, complexité des introductions en bourse… « *Le capital risque est un élément décisif de la souveraineté et de l'expansion américaine dans le monde numérique* », relève ainsi Mme Moreau-Desailly.

Et la sécurité ?

Autre priorité édictée par le rapport : la cybersécurité. Celle-ci souffre tout d'abord de la dispersion des acteurs concernés. Le pilotage de la stratégie numérique incombe en effet à la DG Connect, qui doit aussi composer avec la DG « marché intérieur » et la DG « Home affairs » compétente en matière de lutte anti-cybercriminalité. Le volet opérationnel n'est pas non plus épargné : le dispositif fonctionnerait mal en raison des propensions de chacun des Etats membres à vouloir garder leur souveraineté sur ce domaine sensible. On se limite donc souvent au plus petit dénominateur commun. L'efficacité de l'ENISA, Agence européenne chargée de la sécurité des réseaux, est contestée, tandis que le CERT européen chargé de prévenir et de répondre aux attaques visant les institutions européennes ne disposerait pas encore des moyens nécessaires. Dernier événement en date : la publication en février 2013 d'un projet de directive visant à mettre en place

« *des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union* »[6]. Si le rapport reste muet à ce propos, ce projet soulève déjà quelques interrogations. Certes, il a l'intention louable d'étendre à de nouveaux secteurs les obligations qui incombaient jusque là uniquement au secteur des communications électroniques (comme par exemple la notification aux autorités des incidents informatiques), mais sa mise en œuvre devrait s'avérer longue et complexe.

Le rapport propose enfin de faire bénéficier les industries d'équipements numériques stratégiques (comme les routeurs de cœur de réseaux) de la préférence européenne, déjà implicitement reconnue pour les marchés publics de défense et de sécurité. Ces produits devraient donc être labellisés par une autorité nationale ou européenne de sécurité avant leur diffusion sur le marché.

Gouvernance internet : une troisième voie ?

Dernier point abordé par le rapport : la gouvernance internet. La marge de manœuvre européenne apparait là aussi fort étroite, coincée entre l'approche étatiste proposée par certains Etats comme la Russie ou la Chine et la vision multi-acteurs défendue par la puissance dominante. L'objectif serait de trouver une sorte de troisième voie : « *sans céder à la revendication de certains pays d'une reprise en main intergouvernementale d'Internet, il faut reconnaître la responsabilité particulière des États dans la gouvernance multi-acteurs qui sied à l'internet* », explique le document. L'Europe se donnerait ainsi pour mission d'éviter que ne se creuse le clivage entre les Etats-Unis et la Chine en rendant plus transparent le fonctionnement de l'ICANN et en revalorisant en même temps le rôle des gouvernements « *pour la défense d'une forme d'ordre public sur internet* ». Une troisième voie que l'on pourrait qualifier selon l'expression de Joël de Rosnay de *« corrégulation catalysée par les Etats* ».

[6] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_fr.pdf

David E. Sanger et la cyberstratégie américaine

La Chaire Castex de Cyberstratégie accueillait le 18 avril dernier David E. Sanger, journaliste du New-York Times rendu célèbre pour, entre autres, la publication de son livre sur l'affaire Stuxnet ou encore « Olympic Games » — « Confront and conceal, Obama's secret wars and Surprising use of American Power ». L'occasion pour ce journaliste — et correspondant en chef du New-York Times à la Maison Blanche — de tirer les enseignements de l'affaire Olympic Games et de soulever le débat sur la cyberstratégie américaine.

L'originalité du cas Stuxnet

Sans revenir sur les détails de l'affaire Olympic Games, l'auteur soulève qu'il s'agit d'une première. Stuxnet est aujourd'hui un cas unique et incontournable pour deux raisons.

Si jusque là les cyberattaques consistaient généralement dans des affrontements ordinateur vers ordinateur (atteinte aux données, au fonctionnement de l'ordinateur, etc.), Stuxnet avait bien pour finalité de faire exploser les centrales nucléaires iraniennes de Natanz. C'est ce que Sanger démontre quand il rapporte les faits : les équipes de la Maison Blanche sont en effet allées jusqu'à reproduire les centrales et à les faire réellement exploser pour éprouver leur nouvel outil informatique. Conséquence si difficile à croire que les débris auraient été rapatriés aux Etats-Unis, afin de convaincre le président de l'époque, Georges W. Bush.

Stuxnet est également une première en ce qu'il s'agit du premier acte hostile assumé d'un Etat contre un autre Etat, en lieu et place d'un acte de guerre plus « classique ». Nous sommes résolument dans « une nouvelle ère », selon Sanger.

Conséquences sur la définition de l'acte de cyberguerre

Les cyberattaques peuvent-elles être qualifiées d'actes de guerre ? Et si oui, dans quelle mesure ? Pour David E. Sanger, la réponse est simple : les cyberattaques sont, majoritairement, des actes d'espionnage et de vol de données. Elles ne peuvent en aucun cas aujourd'hui être qualifiées d'actes de guerre. Stuxnet et l'affaire Olympic Games ne sont que l'exception à cette règle.

Que penser alors du positionnement américain en la matière ? Qu'est-ce qu'un acte de cyberguerre pour les Etats-Unis ? A cette question, le journaliste répond qu'il est justement de l'intérêt des Etats-Unis de ne pas donner de définition claire et stricte de ce qu'est un acte de cyberguerre. L'acte de cyberguerre sera suffisamment évident en lui-même pour que l'on sache que l'on est en présence d'un acte de guerre.

Se distinguant des discours habituels, il souligne que les Etats-Unis ne souhaitent pas s'enfermer dans des définitions trop restrictives pour plusieurs raisons. La première est de conserver une marge de manoeuvre face à un type de conflit nouveau ; la seconde est de ne pas donner à l'adversaire une définition trop précise du seuil au delà duquel ses actes justifieraient une riposte de la part des Etats-Unis.

Le positionnement stratégique des Etats-Unis et son impact sur leur stratégie de cyberdéfense

Lors de la préparation de l'affaire Olympic Games, Barack Obama a exprimé ses inquiétudes quant à la réutilisation du virus par d'autres acteurs, mais aussi quant au risque que cela justifie une éventuelle riposte de la part d'autres Etats.

Pour leur part, les Etats-Unis semblent être dans une position difficile, souligne David Sanger. Si le pays se positionne en faveur de ripostes préventives, la mise en oeuvre d'une telle stratégie serait difficile à assumer selon le journaliste. Comment justifier l'imminence de cyberattaques massives contre ses infrastructures ? S'il est aisé de prouver l'imminence d'une attaque classique, la préparation d'une cyberattaque peut être niée très facilement par l'adversaire. L'intention reste le seul élément pouvant prouver l'imminence de l'attaque dématérialisée. Mais comment prouver cette intention ? Aussi, comment prouver le lien entre un Etat, dont les organes représentatifs politiques se seraient engagés à ne pas attaquer un allié, et un groupuscule se réclamant de cet Etat ? Pour mitiger les risques et diminuer le nombre d'attaques subies, les Etats-Unis ont mis en place une stratégie de e-diplomatie avec certains Etats clés : la Chine, la Russie. Mais quid de son efficacité ?

La cyberdéfense américaine se traduit également par des efforts colossaux pour améliorer la résilience de leurs réseaux. L'auteur le martèle : la résilience des infrastructures critiques est essentielle à toute stratégie de cyberdéfense. Il faut avoir la capacité d'absorber l'attaque, de retrouver son état de fonctionnement initial puis de riposter. Les cyberattaques auront lieu quoi qu'il arrive : elles sont inévitables et elles ne peuvent être contrées comme n'importe quelle autre menace. Ce qui justifie que l'on s'y prépare.

David Sanger soutient à ce propos que les Etats-Unis sont l'un des pays — sinon LE pays — les plus vulnérables du point de vue "cyber". Si les réseaux militaires sont bien défendus selon le journaliste, ce sont les réseaux civils qui inquiètent et, plus précisément, les espaces en .com et .edu.

Olympic games au coeur de la « Light footprints strategy » et de « la guerre du futur »

L'opération Olympic games se situe dans une problématique bien plus globale. Dans un contexte de restrictions budgétaires, les frappes à distance sont désormais au coeur de la stratégie militaire américaine.

Cette stratégie, dite de "light footprints" favorise d'une part la prévention des conflits violents par divers moyens et, d'autre part, les interventions aériennes, les frappes chirurgicales de drones et, plus globalement, les interventions à distance afin d'éviter le déplacement des troupes et de réduire les coûts. Une telle stratégie laisse ainsi une place de choix aux cyberattaques.

Ainsi, le récit de l'affaire Olympic games tel que rapporté par David Sanger prend tout son sens. L'évolution de la position du président Obama, la transmission du projet Olympic games de Georges W. Bush à son successeur, l'attachement du nouveau président au déploiement de drones et sa réticence à engager ses troupes sur le terrain font en effet corps avec cette nouvelle stratégie.

La mise en oeuvre de l'outil cyber dans le cadre d'opération classiques nécessite toutefois un contexte favorable : David Sanger rappelle que l'outil cyber ne peut servir efficacement sur tous les théâtres de guerre. Certains, très peu connectés, ne favorisent pas une utilisation profitable de l'arme cyber.

Le portail OMC
La nouvelle plateforme de la DAS

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

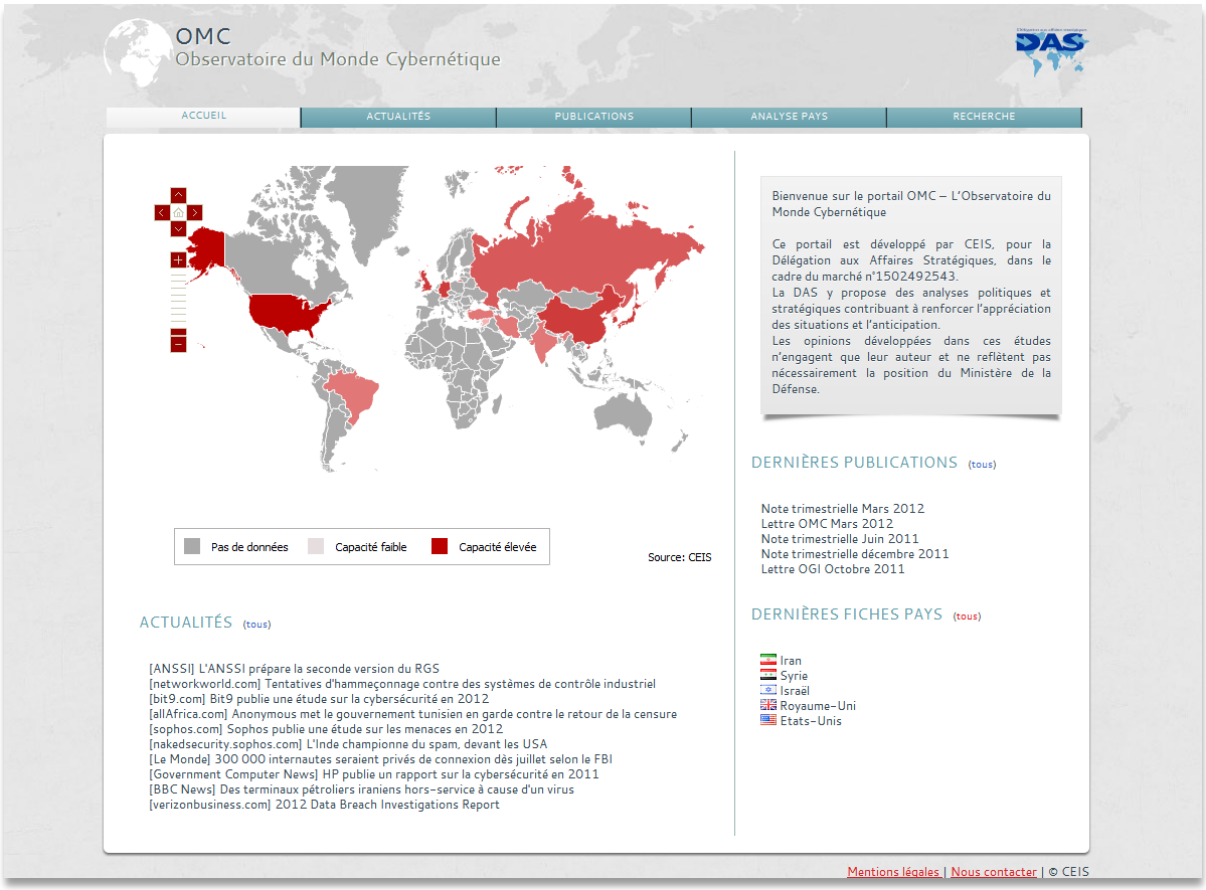

Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

Hackito Ergo Sum	Paris	2 – 4 mai
Le Cercle européen de la sécurité et des systems d'information	Paris	16 mai
NSC – No Such Conference (Hacking éthique)	Paris	15 – 17 mai
Data Centres Europe 2013	Nice	29 – 30 mai
SSTIC 2013	Rennes	5 – 7 juin
ACM Workshop on Information Hiding and Multimedia Security	Montpellier	17 – 19 juin
Hack in Paris	Paris	17 – 21 juin
La Nuit du Hack	Marne La Vallée	22 – 23 juin
Technology Against Crime	Lyon	8 – 9 juillet
Cyber Intelligence Europe	Bruxelles	17 – 19 septembre
Les Assises de la Sécurité et des Systèmes d'Information	Monaco	2 – 5 octobre

CEIS

Compagnie Européenne
d'Intelligence Stratégique

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

Les opinions exprimées dans cette lettre n'engagent que la responsabilité de leurs auteurs.

Retrouvez cette lettre et l'ensemble des articles cités sur le portail
https://omc.ceis.eu/
(Accès soumis à authentification)

La Délégation aux Affaires Stratégiques propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation.

Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la DAS a confié à la **Compagnie Européenne d'Intelligence Stratégique (CEIS)** cet Observatoire du Monde Cybernétique, sous le numéro de marché 1502492543.

Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la défense et des anciens combattants
Délégation aux Affaires Stratégiques
Sous-direction Politique et Prospective de Défense
14 rue St Dominique 75700 PARIS SP 07