Observatoire du Monde Cybernétique

Lettre n°14 – Février 2013

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

[RPDéfense] Une formation en cyberdéfense unique en France

Une formation d'ingénieur en cyberdéfense sera proposée à la rentrée 2013 par l'école d'ingénieurs de l'université de Bretagne Sud (ENSIBS). Les 25 membres de la prochaine promotion étudieront pendant 3 ans, en alternance, les thématiques de cybersécurité. Cette formation unique en France suscite un fort engouement auprès des professionnels du secteur : de nombreux partenaires seraient prêts à accueillir les étudiants en alternance, dont Alcatel-Lucent, Thales ou encore Orange.

[Europol] Rançongiciel : Europol démantèle un gang de cybercriminels

Europol a démantelé un gang de cybercriminels originaires d'Europe de l'est et spécialisé dans le rançongiciel. Les onze membres de ce groupe criminel se faisaient passer pour des agents de police accusant l'utilisateur d'activités illégales et exigeaient de la victime qu'elle acquitte une amende de 200€ pour reprendre le contrôle de son ordinateur.

[Acus] La Grande-Bretagne rejoint le centre de cyberdéfense de l'OTAN

David Cameron a annoncé, lors d'un rendez-vous bilatéral avec le premier ministre de l'Estonie, que la Grande-Bretagne souhaitait intégrer le centre de cyberdéfense de l'OTAN cette année. Deux autres Etats ont annoncé rejoindre le Centre de l'OTAN en 2013 : la Turquie et la France.

[CourierMail] L'Australie et la Grande-Bretagne signent un traité de défense

L'Australie et la Grande-Bretagne ont signé un accord invitant les deux Etats à partager des informations, de la technologie, une politique globale de défense ainsi que du personnel. La cybersécurité et les menaces internationales font aussi partie de l'agenda politique des deux pays.

[TheInformationDaily] Le Centre de Cybersécurité australien ouvrira cette année à Canberra

Julia Gillard, premier ministre australienne, a annoncé l'ouverture au cours de l'année 2013 d'un nouveau centre de cybersécurité. Basé à Canberra et composé d'experts nationaux en cybersécurité, son objectif sera de contenir la cybercriminalité et de protéger le pays contre les cyberattaques.

[TheFiscalTimes] Le Pentagone se constitue un arsenal « cyber »

Le Pentagone a initié un travail de recherche en partenariat avec des industriels de défense tels que General Dynamics et Lockheed Martin. Objectif : développer un arsenal de cybersécurité à même de protéger les réseaux du Département de la Défense américain, mais également de mener des attaques contre des réseaux étrangers.

[ComputerWeekly] L'opération Beebus cible les industries américaines aérospatiales et de défense

Des experts ont découvert une campagne de cyberattaques menées contre des industriels américains de l'aérospatiale et de la défense. Le virus utilisé, baptisé Beebus, exploitait une faille des fichiers PDF et .doc et était déployé par l'envoi de courriels aux pièces jointes corrompues. Une fois installé, le logiciel malveillant communiquait avec des serveurs lui commandant l'envoi de fichiers prélevés.

[TheHill] La directive présidentielle américaine sur la cybersécurité a été signée

Barack Obama a signé mardi 12 février 2013 une directive présidentielle sur la cybersécurité, dont l'objectif est d'améliorer la résilience des infrastructures critiques américaines. Elle propose une série de bonnes pratiques censées augmenter le volume, la rapidité et la qualité de la transmission d'informations liées aux cybermenaces entre acteurs privés. La version finale de cette directive devrait être publiée d'ici un an.

[Voanews] La Maison Blanche dévoile une nouvelle cyberstratégie contre l'espionnage

L'Administration Obama a dévoilé une nouvelle stratégie destinée à protéger les entreprises américaines contre l'espionnage industriel. Les entreprises américaines ont estimé avoir perdu plus de 300 milliards de dollars d'informations en 2012.

La nouvelle stratégie doit renforcer l'engagement américain et la coopération de ses alliés. Un changement de la législation est à l'étude.

[NyTimes] L'administration Obama autorise les cyberattaques préemptives

L'administration Obama s'est donné les outils nécessaires à l'instauration d'un droit de cyberattaque préemptives sur des cibles étrangères. Selon le New York Times, ces attaques seraient menées dès lors que la Maison Blanche estimerait nécessaire de protéger ses intérêts vitaux en attaquant une cible avant même que celle-ci ne lance une quelconque offensive sur le territoire américain. Les opérations en question seront conduites par le Cyber Command.

[Smh] Les Etats-Unis condamnent un gang de cybercriminels d'Europe de l'Est

Les Etats-Unis ont condamné récemment trois jeunes Européens pour des faits de cybercriminalité. Les cybercriminels se seraient introduits dans plus d'un million d'ordinateurs, y compris ceux de la NASA, en utilisant un logiciel malveillant dénommé "Gozi Virus", et auraient ainsi pu se procurer de nombreuses données bancaires.

[USAirForce] L'USAF Space Command va renforcer son équipe cyber

L'Air Force Space Command prévoit d'ajouter 1000 nouveaux éléments à son équipe de 6000 professionnels cyber à l'horizon 2014.

Cette vague de recrutement devrait s'étendre sur deux années et cibler 70 à 80% de civils. Elle reste cependant conditionnée par le contexte budgétaire.

[JPost] Le centre de contrôle de cyberdéfense de Tsahal enfin opérationnel

Il aura fallu attendre deux ans pour que les forces armées israéliennes créent leur centre de contrôle de la cyberdéfense. Tout juste opérationnel, ce centre est composé d'une vingtaine de spécialistes et fonctionne tous les jours de la semaine, 24h/24. Ce centre est lié au Shin Bet, ainsi qu'au système Tehila, centre serveur sécurisé assurant la sécurité et la disponibilité de nombreux services aux autorités gouvernementales depuis ou vers Internet. Le personnel est pour le moment insuffisant mais des recrutements sont à prévoir.

[RIANovosti] Un département de sécurité informatique verra le jour en Russie

Le ministère russe des Affaires étrangères va ouvrir un département chargé de la sécurité informatique internationale. Sa mission sera de *« faire progresser les initiatives russes en matière de règles de conduite sur Internet et de renforcer les mesures de confiance dans le cyberespace »*.

[Renesys] Le Bangladesh se connecte à Internet via l'Inde

Depuis 2006, le Bangladesh était connecté à Internet par un unique câble sous-marin, le Sea-Me-We 4 (SMW4) s'étendant sur 4 segments de Marseille à Singapour. Cette solution ne semble plus être exclusive, comme l'ont constaté les observateurs de Renesys. La connectivité du Bangladesh n'est plus autant affectée par les coupures de ce réseau, suggérant l'existence d'une connexion alternative. Celle-ci se ferait par le câble terrestre ITC via l'Inde, comme observé depuis novembre 2012, et apporte une alternative performante au câble SMW4 dont les coupures perturbaient considérablement la connectivité du pays.

[Softpedia] Le ministère de la défense chinois rejette les accusations de Mandiant

Le ministère de la défense chinois a publié mardi un communiqué en réaction au rapport de la société Mandiant qui fournissait des éléments mettant en cause l'armée chinoise dans le piratage de nombreux sites américains. Les autorités chinoises rejettent toute implication étatique dans

ces attaques, réfutent la crédibilité du rapport en question et dénoncent l'irresponsabilité de Mandiant de publier de telles informations. De plus, le ministère de la défense chinois rappelle qu'il n'existe aucune définition internationalement acceptée de ce qu'est une cyberattaque. Enfin, le communiqué se conclut sur la volonté chinoise de privilégier la négociation et menace que de telles accusations publiques détériorent le climat de coopération existant.

[China] La société Huawei encourage la stratégie de cyberdéfense australienne

Le gouvernement australien a récemment annoncé la création d'un centre de cybersécurité. Le groupe Huawei souhaite encourager cet effort qui devrait centraliser des ressources de plusieurs agences publiques. La société travaille également sur la création d'un Centre d'évaluation de cybersécurité en Australie, qui pourrait s'inspirer de celui déjà créé au Royaume-Uni.

[TheRegister] Singapour autorise les attaques préventives contre les cybercriminels

Le gouvernement singapourien a adopté un amendement lui permettant de prendre des mesures offensives préventives contre toute cybermenace avant que celle-ci n'affecte une quelconque cible.

[EcoFin] Le Kenya lance sa stratégie nationale de cybersécurité

Le Kenya s'est doté d'une stratégie de cybersécurité et d'un plan directeur, qui s'inscrivent dans le plan directeur des Technologies de l'Information et des Communications lancé le 14 février. Le gouvernement kenyan souhaite élaborer un guide de procédures à destination des administrations et des entreprises en cas de cyberattaques.

[Enisa] Rapport sur l'exercice de cybersécurité « Cyber Europe 2012 »

L'ENISA a publié le rapport sur l'exercice de cybersécurité paneuropéen "Cyber Europe 2012", auquel ont participé près de 600 intervenants de 29 Etats. L'agence européenne en tire des conclusions relativement positives et propose des recommandations, dont l'organisation plus fréquente de tels exercices, davantage de formation et l'implication accrue du secteur privé dans les procédures de crise.

[Mandiant et GBTimes] "APT1: Exposing One of China's Cyber Espionage Units"

Dans son dernier rapport, la société Mandiant décrit l'activité d'un groupe de hackers baptisé « APT1 ». Ce groupe serait, selon le document, la plus importante unité de cyber-espionnage de l'armée chinoise. Sont détaillés ses objectifs, ses modes opératoires et ses capacités. Ce rapport, s'il ne fait pas l'unanimité, démontrerait selon certains observateurs que l'*« on peut identifier les agresseurs et le lieu où ils se trouvent* » si l'on s'en donne la peine.

[GlobalSecurityMag] PandaLabs : près d'un tiers des ordinateurs analysés dans le monde étaient infectés en 2012

Panda Security a publié le rapport annuel 2012 de son laboratoire Pandalabs sur la sécurité informatique, faisant état de la considérable augmentation et diversification des cybermenaces. Ainsi, plus de 27 millions de nouvelles souches de codes malveillants ont été créées en 2012 (pour un total de 125 millions), affectant près d'un tiers du parc informatique mondial. Les attaques contre les mobiles ont explosé en 2012, notamment pour les opérations d'escroquerie bancaire. Les logiciels malveillants les plus fréquemment rencontrés sont de loin les chevaux de Troie, puis les virus, mais également les rançongiciels, en augmentation. Ce rapport témoigne de la capacité des cybercriminels à réinventer leurs pratiques et à diversifier leurs méthodes.

[NorthernStar] Un rapport traite de la cybercriminalité en Australie

La première étude réalisée sur la cybercriminalité en Australie démontre qu'en l'espace d'un an, une entreprise australienne sur cinq a été touchée par des cyberattaques. Les entreprises affectées par ce phénomène proviennent de tous les secteurs (énergie, défense, banque, industrie). Les cyberattaques les plus dangereuses sont les rançongiciels ou les virus trojan. 90% des entreprises de l'étude utilisaient pourtant des protections anti-virus ou des filtres anti-spams.

[PublicServiceEurope] La cyberstratégie de la Grande-Bretagne manquerait de moyens

Le rapport rendu par le National Audit Officie en février 2013, qui juge les choix stratégiques opérés par la Grande-Bretagne globalement satisfaisants, critique le manque de personnel qualifié en cybersécurité. Selon la même étude, il est nécessaire que le gouvernement favorise le développement des qualifications cyber dès le plus jeune âge afin de pouvoir disposer, à l'avenir, d'un nombre suffisant de personnel hautement qualifié. L'un des moyens d'y parvenir serait de revoir la politique salariale dans les entreprises publiques qui souhaitent embaucher ce type de personnel, afin d'encourager les jeunes étudiants dans cette voie.

[FierceGovernmentIt] Un rapport du congrès évoque la cyberstratégie des Etats-Unis

Le Government Accountability Office (GAO) a publié en février 2013 un rapport sur la cybersécurité des Etats-Unis. Le document avait comme objectifs : i) d'identifier les défis auxquels fait face le gouvernement fédéral et ii) de déterminer dans quelle mesure la cyberstratégie actuelle répondait à ces défis. Le rapport démontre que le nombre de cyberattaques a considérablement augmenté depuis 2006, passant de 5503 cyberattaques à 48000 en 2013. Le rapport développe plusieurs points à améliorer comme la promotion de l'éducation et la conscience des dangers liés au cyber, ou encore la recherche et le développement.

« *An Open, Safe and Secure Cyberspace* »

La stratégie de cybersécurité européenne

Le 7 février 2013, la Commission européenne a dévoilé, dans un document intitulé « *An Open, Safe and Secure Cyberspace* », sa stratégie en matière de cybersécurité. Une prise en compte nécessaire de la part des autorités européennes tandis que les cyberattaques à l'encontre des particuliers, entreprises ou organismes publics européens se sont multipliées.

Trois grandes nouveautés sont à souligner. Le document recommande le vote d'une directive qui obligerait les Etats membres de l'UE à adopter une stratégie en matière de sécurité des réseaux d'information (SRI ou NIS) et à désigner des autorités nationales compétentes en la matière. La cyberstratégie appelle également à la création d'un mécanisme de coopération entre les Etats membres et la Commission qui permettrait de diffuser des messages d'alerte rapides ainsi que les incidents rencontrés. Enfin, les opérateurs d'infrastructures de secteurs clés, qu'il s'agisse des services financiers, des transports, de la santé ou de l'énergie, devront adopter des mesures de gestion des risques et signaler les incidents importants dont ils sont victimes aux autorités nationales chargées de la SRI.

Cette cyberstratégie survient à une époque où les précédentes améliorations faites en matière de cybersécurité, notamment avec l'instauration du CIIP, apparaissent datées. C'est ce que la Commission notait le 10 mai 2011 lors d'un débat organisé à Bruxelles organisé par le *Security & Defence Agenda*, en estimant que les Etats membres étaient « *sous-équipés et pas du tout préparés face aux cybermenaces* »[1].

Liberté et sécurité : deux principes fondant la stratégie européenne

« Our freedom and prosperity increasingly depend on a robust and innovative Internet. […] But freedom online requires safety and security too. »

Dans ce texte, la Commission européenne fait de la « sécurité » et de la « liberté » les deux piliers de sa réflexion. Deux notions qui, en pratique, reste difficilement conciliables.

Evoquant les Printemps arabes, sont mises en avant les notions suivantes : les « droits et libertés fondamentaux en ligne », la « démocratie », l'« accès et l'ouverture » du réseau ou encore l'exercice de la « liberté d'expression ». Le texte fait ainsi écho à la stratégie *no disconnect* présentée quelques mois auparavant. Dans cette stratégie, Neelie Kroes appellait déjà au développement d'*« outils technologiques destinés à améliorer la protection de la vie privée et la sécurité des populations qui utilisent des TIC dans des régimes non démocratiques »*[2]. Plus précisément, la Commission européenne souhaitait fournir aux dissidents

[1] EU Observer, http://euobserver.com/justice/116239

[2] « Stratégie numérique: Mme Kroes invite M. Karl-Theodor zu Guttenberg à promouvoir la liberté d'expression sur l'internet au niveau mondial », http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1525&format=HTML&aged=0&language=FR&guiLanguage=en

des « *logiciels qui peuvent être installés sur un ordinateur de bureau, un ordinateur portable, un* smartphone *ou tout autre appareil »*[3].

Face à cette vision ouverte et libératrice du réseau, la Commission européenne associe la notion de « sécurité ». Martelant que les lois du monde physique s'appliquent au cyberespace, le texte s'insère dans la dynamique amorcée depuis quelques temps déjà et fait de la vision européenne de la protection de la vie privée et des données à caractère personnel (ou « *privacy* ») un élément phare de la politique européenne.

C'est sur cette double réflexion, alliant liberté et sécurité, que la Commission européenne pose les bases d'une stratégie de cybersécurité relativement ambitieuse.

L'ENISA comme acteur majeur de la stratégie européenne

Le texte annonce rapidement la volonté de la Commission de moderniser les fonctions de l'ENISA. Volonté illustrée sur la presque totalité des axes de la stratégie. L'ENISA est en effet perçue comme premier interlocuteur, noyau d'expertise et de soutien. L'Agence sera chargée entre autres : d'assister les principaux acteurs nationaux dans le développement de capacités de cybersécurité, de proposer une feuille de route de formation et d'entrainement, d'organiser des challenges et championnats ainsi qu'un mois dédié à la cybersécurité. En confiant à l'Agence un rôle si déterminant dans la mise en application de sa stratégie, l'Europe vient redorer le blason d'une institution au rôle effectif parfois décrié.

Cette volonté de faire de l'ENISA l'artisan de la stratégie de cybersécurité européenne se traduit également quant au choix des termes employés. La SRI ou « NIS », Network and Information Security, désignant l'objectif à atteindre (concept remplaçant parfois celui plus générique de « cybersécurité » dans le texte), est directement issu de la dénomination de l'ENISA - l'European Network and Information Security Agency. La mission semble ainsi taillée pour l'Agence.

Pour un meilleur partage de l'information entre acteurs publics et privés et une mise à niveau des Etats membres

Afin d'assurer une « NIS » efficiente, la Commission européenne s'appuie sur le développement du partage d'information. Partage d'information ne pouvant être mené qu'après la mise à niveau des Etats en matière de cybersécurité. C'est là l'objectif premier de la directive accompagnant le document stratégique : contraindre les Etats membres à assurer un haut niveau de cybersécurité ; à créer de l'information (à travers l'obligation de notification d'incidents majeurs) et à la partager entre interlocuteurs qualifiés (création de CERT et d'institution nationale compétente). Le tout accompagné d'exercices européens encadrés par l'ENISA.

[3] Sont ici visés : VPN, proxys ou autres technologies permettant de garder l'anonymat sur Internet.

L'harmonisation des niveaux de cybersécurité de chaque Etat membre, un préalable impératif au développement d'une stratégie européenne

La Commission européenne reconnait que malgré les efforts de certains Etats membres, les écarts de maturité sont encore importants. Nombreux sont les Etats à ne pas bénéficier de capacités de cybersécurité et de cyberdéfense développées (absence de document stratégique identifiant les enjeux, absence d'autorité nationale compétente et bénéficiant des moyens nécessaires, etc.).

Considérant que l'harmonisation des niveaux de cybersécurité de chaque Etat membre est un préalable impératif au développement d'une stratégie européenne, la Commission préconise au sein de son projet de directive l'adoption des mesures suivantes :

Article 4	L'article 4 de la directive pose le principe selon lequel chaque Etat membre devra garantir un niveau important de sécurité du réseau et des SI sur leur territoire. *Ce simple principe général pourrait en réalité cacher une disposition déterminante, ouvrant la voie à la mise en œuvre de la responsabilité d'un Etat ne respectant pas ces diligences.*
Article 5	Chaque Etat membre devra adopter une stratégie de cybersécurité (NIS) et un plan de coopération. *La directive va jusqu'à détailler, point par point, les éléments qui devront être abordés par la stratégie exigée. Citons : la définition des objectifs et priorités, l'identification de mesures de prévention, de réponse et de recouvrement d'activité ou encore un point sur le niveau d'éducation et d'entrainement en matière de cybersécurité.*
Article 6	Chaque Etat membre devra désigner une autorité nationale compétente en matière de cybersécurité (ou NIS). Ils devront lui fournir les moyens nécessaires (financiers, humains…) à son bon fonctionnement. C'est cette autorité qui réceptionnera les notifications d'incidents adressées par les acteurs publics et privés concernés.
Article 7	Chaque Etat devra désigner/créer un CERT national, capable de répondre en urgence aux incidents. Le CERT sera sous la supervision de l'autorité nationale mentionnée ci-dessus.
Article 8	Cet article pose le principe d'un mécanisme de coopération et de circulation de l'information entre autorités nationales. Cette coopération sera assistée par l'ENISA.
Article 9	Cet article rappelle que le partage d'information devra s'appuyer sur une infrastructure de communication sécurisée.
Article 14	L'article 14 est un article clé : il pose le principe de l'extension de l'obligation de notification d'incidents de sécurité informatique à divers acteurs. Sont toutefois exclues les « micro-entreprises »[4] : « entreprise dont l'effectif est inférieur à 10 personnes et dont le chiffre d'affaires ou le total du bilan annuel n'excède pas 2 millions d'euros »[5].

[4] Recommandation 2003/361/CE de la Commission, du 6 mai 2003, concernant la définition des micro, petites et moyennes entreprises [Journal officiel L 124 du 20.05.2003].

	Ces acteurs devront notifier à l'autorité nationale compétente les incidents *ayant un impact significatif* sur leur réseau, leur SI et donc leur cœur d'activité. Le texte accorde une place importante à l' « état de l'art » qui devra constituer le levier d'appréciation des mesures mises en œuvre par les entreprises et administrations. Le texte prévoit une information du public à la discrétion de l'autorité nationale compétente, si cette dernière juge l'incident d'intérêt public. Quoi qu'il en soit, un résumé annuel des notifications reçues devra être rendu public.
Article 15	Cet article prévoit une coopération étroite entre les autorités nationales compétentes en matière de cybersécurité et les autorités judiciaires ainsi que les CNILs européennes.
Article 16	L'article 16 amorce une dynamique de standardisation en matière de cybersécurité.

Quel mécanisme de partage d'information ?

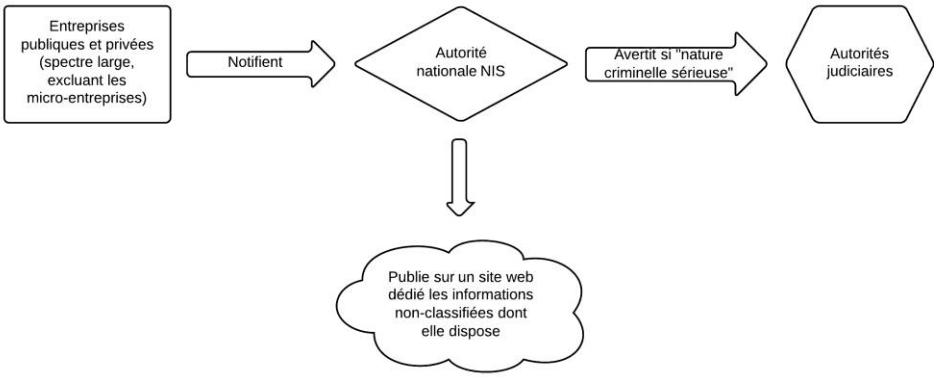

Figure 1. Le mécanisme de partage d'informations tel qu'envisagé par la Commission européenne - Source : CEIS

Le partage d'information semble également être la préoccupation principale outre-Atlantique. En témoigne l'*executive order* récemment signé par le président Barack Obama. La stratégie énoncée se déroule en trois temps. Avec cet *executive order*, Obama souhaite que soit mis en place, dans les 120 jours suivant l'annonce du texte, un système permettant le partage d'informations non-classifiées sur les menaces informatiques concernant les infrastructures critiques du pays. L'objectif étant d'encourager par la suite un véritable partenariat public-privé entre le gouvernement et les entreprise détentrices de près de 80% des infrastructures critiques nationales américaines. De ce partenariat découlera, dans les 8 mois, le développement de capacités de cyberdéfense et de protection des infrastructures critiques. Les résultats des travaux devraient être intégrés au sein du National Infrastructure Protection Plan.

Equivalent du décret du président de la République, l'executive order est un acte exécutif pris par le président des Etats-Unis d'Amérique. Il vient, en général, orienter la politique menée par l'exécutif, en clarifiant une loi déjà votée par le Congrès.

[5] http://europa.eu/legislation_summaries/enterprise/business_environment/n26026_fr.htm

Sensibilisation et formation : enjeu majeur de la stratégie européenne

La Commission européenne prévoit dans son document la mise en œuvre de projets concrets de sensibilisation et de formation en matière de cybersécurité. Citons : un projet de licence en matière de sécurité informatique, à l'image du permis de conduire ; un mois de la cybersécurité à l'échelle européenne ; l'introduction de l'enseignement de bonnes pratiques dans les écoles ; etc.

Vers un marché unique européen appliqué à la cybersécurité

Afin d'éviter tout risque de dépendance excessive de l'Union européenne aux prestataires non-européens en matière d'outils de cybersécurité, la Commission européenne propose une série de mesures. Objectif : s'assurer que les composants et logiciels exploités dans les infrastructures européennes soient *« dignes de confiance, sécurisés et [garantissent] la protection des données personnelles »*.

Au nombre des mesures envisagées :

- Le développement de « labels » pouvant devenir de véritables arguments commerciaux ;
- L'amélioration de la coopération et de la transparence sur la sécurité des produits IT ;
- La création d'ici 2013 d'une plateforme rassemblant les principaux acteurs publics et privés afin d'identifier les bonnes pratiques à assurer tout au long de la chaine de production ;
- Adopter d'ici 2014 des standards de sécurité et déboucher sur la création d'une certification à l'échelle européenne.

Un document critiqué

De nombreuses personnalités du secteur industriel ont pu critiquer l'extension – voire la « généralisation » de l'obligation de notification d'incident de sécurité, craignant pour leur image et les coûts de communication engendrés. Est également discutée la création d'autorités nationales compétentes en matière de SRI. L'application d'une telle mesure exigerait la centralisation des organismes existants. Des bouleversements que craignent certains Etats comme l'Angleterre ou l'Allemagne.

D'autres voient dans cette cyberstratégie un « patchwork » de plusieurs actions disparates allant à l'encontre d'une vision d'ensemble de la cybersécurité de l'UE. Ce reproche souligne la diversité des mesures annoncées dans la stratégie, qui viennent s'ajouter à la création récente d'un Centre européen de lutte contre la cybercriminalité, la proposition de mesures législatives relatives aux attaques visant les systèmes d'information, ou encore le lancement de l'Alliance mondiale contre les abus sexuels commis contre des enfants via Internet.

Mais surtout, **la cyberdéfense reste la grande absente de la stratégie européenne**. Si le document précise vouloir développer une politique et des moyens de cyberdéfense, en liaison avec la politique de sécurité et de défense commune (PSDC), il reste muet sur les modalités de ce développement. Notons toutefois que le document précise que l'Europe ne plaide pas pour l'adoption de nouveaux outils législatifs en droit international et que *« si les conflits armés s'étendent dans le cyberespace, le droit international humanitaire s'appliquera au cas par cas »*. Une prise de position concise, mais riche d'enseignements.

Le portail OMC
La nouvelle plateforme de la DAS

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

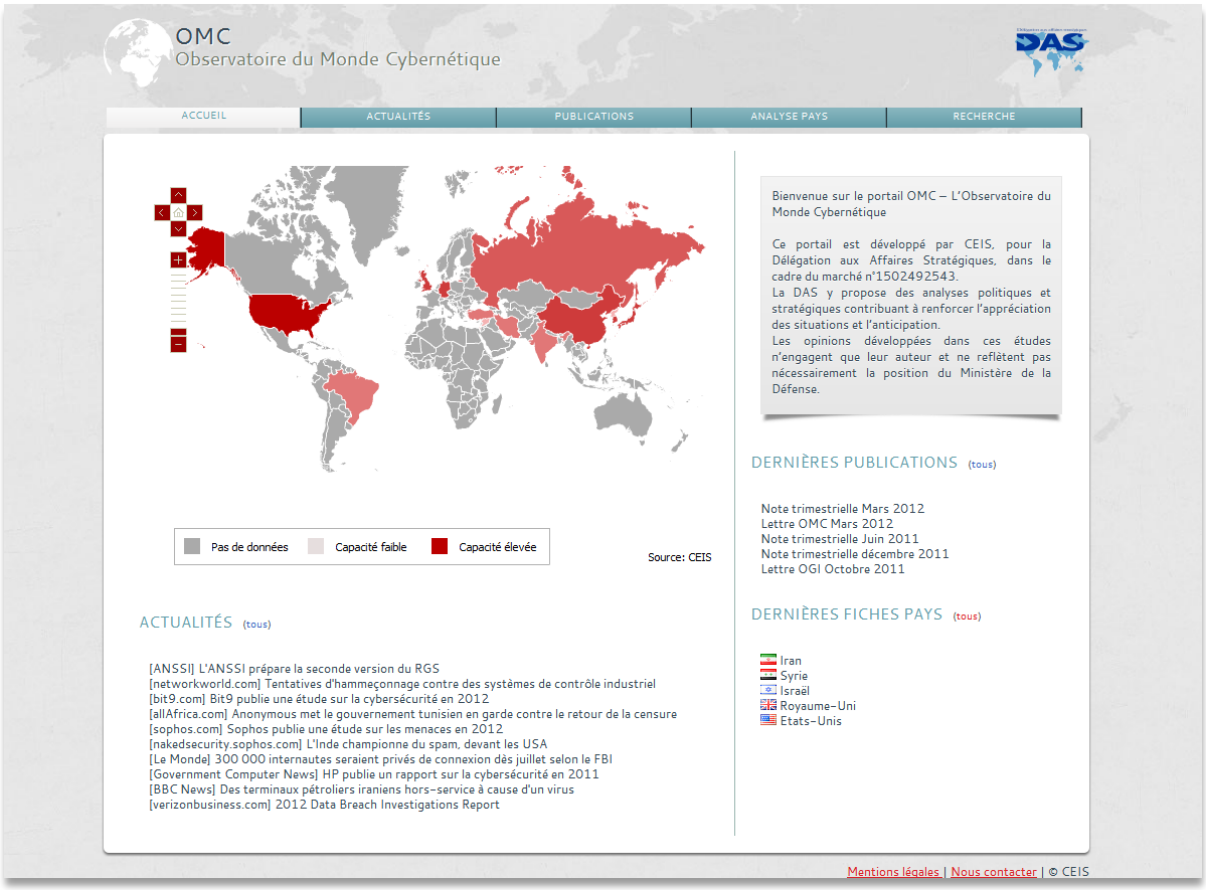

Figure 2. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

Nullcon Goa	Goa, Inde	27 février – 2 mars
Saudi Safety and Security (SSS)	Dammam, Arabie Saoudite	3 – 6 mars
IFSEC West Africa	Lagos, Nigeria	5 – 6 mars
Black Hat Briefings & Training Europe	Amsterdam, Pays-Bas	12 – 15 mars
Cyber Intelligence Asia conference & exhibition	Kuala Lumpur, Malaisie	12 – 15 mars
JSSI – Journée de la Sécurité des Systèmes d'Information	Paris	13 mars
Infosecurity Belgium 2013	Bruxelles	20 – 21 mars
Matinale du Cercle de la sécurité	Paris	26 mars
International Forensic Sciences, Cyber Security and Surveillance Technologies	Istanbul, Turquie	27 – 29 mars
Cyber Security for the Chemical Industry Europe	Francfort, Allemagne	26 – 27 mars
NSC – No Such Conference (Hacking éthique)	Paris	15 – 17 mai
SSTIC 2013	Rennes	5 – 7 juin
GS Days	Paris	4 avril
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
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

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