Observatoire du Monde Cybernétique

Lettre n°10 – Octobre 2012

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

[RPFrance] Adhésion de la France au Centre d'Excellence de Cyberdéfense de Tallinn

La France a annoncé le renforcement de sa coopération avec le Centre d'Excellence de Cyberdéfense de Tallinn (CCDCOE) en décidant, au travers de son État-major des armées, d'y adhérer en tant que sponsor. Selon le communiqué de presse, *« la France fait de la cyberdéfense une de ses priorités nationales. Elle s'applique à renforcer la coopération bilatérale avec ses principaux alliés et soutient l'action de l'OTAN et de l'UE dans ce domaine. »* Des personnels y seront détachés à partir de l'été 2013.

[Le Monde] Contre l'espionnage industriel, Bercy relance l'idée d'instituer un « secret des affaires »

Une loi est à l'étude du côté de Bercy et à l'Assemblée Nationale pour instituer un « secret entreprise », afin de mieux protéger les entreprises françaises contre l'espionnage industriel. Mais une telle proposition serait difficile à mettre en place pour des raisons pratiques : les patrons responsables de l'apposition du « sceau ''secret entreprise'' » définiraient ainsi eux-mêmes le champ d'une sanction pénale. Un cadre de GDF Suez estime toutefois que la loi pourrait avoir *« un effet dissuasif important (…) : elle obligera les entreprises à se demander quelles informations sensibles elles doivent protéger, et comment le faire. »*

[ExpertSolutions] La Suisse se dote d'une stratégie nationale de protection contre les cyber-risques

La confédération Suisse s'est dotée d'une stratégie nationale en matière de cybersécurité. Partant du constat que les moyens alloués sont insuffisants, le texte prévoit des efforts importants en matière de formations, de législation et de mise en place d'organes adaptés. La stratégie identifie notamment sept champs d'action : Recherche et développement ; Analyse des risques et vulnérabilités ; Analyse de la menace ; Formation et développement des compétences ; Gouvernance d'Internet et directives internationales ; Gestion de la continuité et des crises ; Développement des bases juridiques.

[ISO] Nouvelle norme ISO sur la cybersécurité

Une nouvelle norme ISO devrait voir le jour afin d'encadrer le partage de l'information sur Internet et la gestion des incidents associés. La norme 27032 intitulée « Technologies de l'information – Techniques de sécurité – Lignes directrices pour la cybersécurité » doit apporter une solution *« globale, collaborative et multipartite pour réduire les risques »* du cyberespace.

[Le Figaro ; Le Point] Après la France, les Etats-Unis et le Canada écartent Huawei et ZTE

Un rapport du Congrès américain estime que les sociétés chinoises Huawei et ZTE menacent la sécurité américaine dans la mesure où *« elles subissent l'influence d'un État étranger ».* Des soupçons amplifiés par le fait que le dirigeant actuel de Huawei serait un ancien cadre de l'Armée populaire de libération. Cette position a été suivie par le Canada qui, après la France (à travers le rapport du sénateur Jean-Marie Bockel) et les Etats-Unis, s'est prononcé contre l'usage des équipements des fabricants chinois Huawei et ZTE. Le porte-parole du premier ministre canadien a invoqué *« l'exception au titre de la sécurité nationale »* afin de justifier la mise à l'écart des fabricants.

[NYTimes] Virus Shamoon : les américains pointent du doigt l'Iran dans l'attaque d'Aramco

Le virus Shamoon qui a touché la compagnie pétrolière Aramco à la mi-octobre a entraîné la suppression de données sur les trois quarts des ordinateurs de l'entreprise. Les responsables américains pointent du doigt l'Iran, sans être en mesure de prouver ces accusations pour le moment.

Il pourrait s'agir selon eux d'une réponse aux virus Stuxnet et Flame ayant touché les infrastructures nucléaires et pétrolières iraniennes. Leon Panetta, secrétaire à la Défense américain, a parlé à propos de l'attaque d'*« escalade significative de la menace cyber ».*

[DefenseSystems] Etats-Unis: l'armée développerait un smart grid tactique

Un centre de R&D de l'armée américaine mènerait actuellement des essais sur un smart grid destiné à soutenir les opérations tactiques et à améliorer la logistique actuelle d'utilisation de l'énergie, jugée relativement inefficace. Le dispositif mettrait à disposition des soldats des outils mobiles de gestion de l'énergie qui n'existaient pas auparavant.

[FederalNews] L'US Air Force tente d'établir sa doctrine en matière de cybersécurité

L'armée de l'air américaine tente de créer une doctrine unique en matière de cybersécurité afin de surmonter sa vision jugée pour le moment obsolète. Le général Mark Welsh estime en ce sens qu'il faut des capacités offensives, une hiérarchisation dans la protection des systèmes, et préconise l'achat en urgence de certains matériels critiques. Il en appelle à l'industrie dans la course à l'armement à laquelle pourrait se livrer l'armée de l'air.

[RPDefense] Israël développe un « Dôme de fer digital » contre les cyberattaques

Le premier ministre israélien Binyamin Netanyahou a indiqué que son pays était en train de mettre sur pied un « dôme » de protection contre les cyberattaques, comparant celui-ci au mur de protection qui sépare le pays de la Cisjordanie et au système antimissile « Dôme de fer ». *« Chaque jour, des hackers tentent d'infiltrer les systèmes informatiques israéliens »*, a-t-il rappelé.

[TheNewNewInternet] Un chercheur du MIT révèle un réseau Internet parallèle en Iran

Un chercheur du MIT, Collin Anderson, aurait trouvé un Internet parallèle en Iran, spécifique au pays, inaccessible depuis l'extérieur et basé sur des adresses IP privées. Il dit s'être connecté à 46 000 utilisateurs sur un total potentiel de 17 millions. Parmi les hôtes cités, se trouvent l'autorité des télécommunications, le ministère de l'agriculture, le ministère de l'éducation et l'autorité en charge d'Internet.

[Kaspersky] Le laboratoire de Kaspersky révèle l'existence de miniFlame successeur de Flame et de Gauss

Le laboratoire de Kaspersky révèle l'existence de miniFlame (ou SPE), un virus basé sur la plateforme de Flame. Pour le chef du laboratoire Alexander Gostev, *« miniFlame vient prouver à nouveau qu'il existe une collaboration entre les créateurs de Stuxnet, Duqu, Flame et Gauss ».* Virus ciblé, façonné pour voler des informations, il n'aurait infecté qu'entre 50 et 60 ordinateurs dans le monde. Si Kaspersky n'est pas encore en mesure de déterminer le vecteur d'infection de miniFlame, Gotsev peut cependant en décrire le fonctionnement : *« miniFlame vient dans un deuxième temps lors d'une cyberattaque. D'abord, Flame ou Gauss sont utilisés pour infecter le plus de victimes possibles afin de collecter le plus d'informations possibles. Une victime intéressante est alors repérée et miniFlame se déploie afin de mener une surveillance plus approfondie. »*

[eugene.kaspersky.com] Kaspersky met au point un OS sécurisé dédié aux Scadas

Kaspersky, l'éditeur de logiciels antivirus, va se lancer dans la création d'un système d'exploitation ultra-sécurisé. Il sera particulièrement adapté aux systèmes de gestion automatisée SCADA utilisés par les industries critiques, actuellement gérés par des serveurs Linux ou Windows. *« Pour être entièrement sécurisé, le noyau doit être entièrement vérifié pour ne permettre aucune vulnérabilité ou double usage du code. »* Objectif : concevoir un système d'exploitation avec la sécurité comme priorité, *by design,* et non comme accessoire.

[RussiaBTH] L'armée russe va lancer un appel d'offres pour des outils de LID et de LIO

L'armée russe va lancer un appel public pour la mise en place de systèmes de lutte informatique défensive (LIO) et offensive (LID). Parmi les technologies demandées, rapporte le journal *Kommersant*, figurent *« des méthodes qui permettent de contourner les antivirus, des outils de protection des réseaux, ainsi que des*

technologies de protection des systèmes d'exploitation. »

[ZDNet] L'ASEAN et le Japon se liguent contre les cyberattaques supposées de la Chine

Le journal japonais Yomiuri Shimbun révèle que les dix pays membres de l'ASEAN et le Japon auraient créé une ligue informelle afin de lutter contre des cyberattaques, probablement d'origine chinoises, visant leurs sites gouvernementaux. Un exercice du type de ceux organisés par l'ENISA devrait avoir lieu afin de préparer une *« réponse coordonnée en cas d'attaque. »*

[RPDefense] L'armée indienne inaugure son école de la cyberguerre

L'armée de l'air indienne lance une école de cyberguerre à Bangalore. Celle-ci mènera des efforts de recherche et formera la main-d'œuvre nécessaire aux forces armées.

[ENISA] L'ENISA publie un rapport d'analyse sur les exercices de cybersécurité en Europe

L'ENISA a analysé 85 cyber-exercices nationaux et internationaux ayant eu lieu entre 2002 et 2012. Le résultat quantitatif est plutôt positif, puisque le nombre d'exercices réalisés est en constante augmentation et la coopération internationale a tendance à s'accroitre (64% des exercices internationaux ont impliqué plus de 10 pays). Sept recommandations sont faites pour améliorer, intensifier et complexifier les futurs exercices.

[MELANI] Rapports semestriel sur la « Sûreté de l'information : situation en Suisse et sur le plan international »

Selon le rapport semestriel de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information suisse, MELANI, les petites et moyennes entreprises seraient particulièrement exposées aux cyberattaques. En cause : le BYOD (*Bring Your Own Device*) et le gommage de la frontière entre vie privée et vie professionnelle. En ce sens, la Centrale de surveillance insiste dans son rapport sur la nécessité de *« protéger l'information et plus seulement les ordinateurs et les réseaux où sont stockées les données »* et de sensibiliser aux bonnes pratiques élémentaires.

[HP] Étude : le coût de la cybercriminalité augmente de près de 40 % ; la fréquence des attaques est doublée.

HP présentait le 16 octobre dernier les résultats de sa dernière étude sur la cybercriminalité. Portant sur un panel d'entreprises américaines, les travaux révèlent une hausse de 42% du nombre d'attaques informatiques et un coût total supporté par les entreprises de 8,9 milliards de dollars. Des études spécifiques ont également été réalisées en Australie, en Allemagne, au Japon, et au Royaume-Uni.

[Verizon Business] Verizon publie son « 2012 Data Breach Investigations Report »

Le 24 octobre était révélée l'étude « Verizon 2012 and 2011 Data Breach Investigations Reports ». Dans ce rapport, l'entreprise spécialisée dans les télécommunications dresse une série d'états des lieux de la cybercriminalité, secteur par secteur.

[DHS.GOV] Etats-Unis : un rapport préconise un recrutement d'urgence au DHS

Une *task force* sur les ressources humaines de la cybersécurité au sein du Department of Homeland Security (DHS) vient de remettre son rapport. Parmi les recommandations figure le recrutement urgent de 600 experts en cybersécurité. Objectif : palier les nombreuses difficultés rencontrées dans ce domaine : manque de main-d'œuvre, annonces de recrutement floues et compétences inadaptées.

[CSIS] Quelle stratégie cyber pour l'Armée de populaire de libération chinoise?

Le Center for Strategic and International Studies a publié une note sur le futur de l'armée chinoise. Le document livre quelques éléments sur la conception militaire chinoise du cyberespace. La stratégie de la « guerre du peuple » appliquée au cyberespace pourrait ainsi inclure la population civile, au sein de laquelle les utilisateurs expérimentés pourraient protéger les réseaux chinois et attaquer ceux de l'ennemi. Les auteurs du rapport estiment que les chinois considèrent l'espace comme un champ de la guerre à part entière qui peut être utilisé en parallèle des opérations physiques. Enfin, le cyber est intégré dans les systèmes C4ISR et au renseignement de manière générale.

[unodc.org] L'ONU publie un rapport pour lutter contre le cyberterrorisme

L'ONUDC (Office des Nations unies contre la drogue et la criminalité) a annoncé la publication d'un rapport esquissant des mesures de lutte contre le cyberterrorisme. Par « cyberterrorisme », l'Office entend l'utilisation, par les terroristes, d'Internet à des fins de recrutement, de diffusion d'informations et de planification des attaques. L'objectif de ce rapport est d'apporter *« des réponses efficaces (…) à ce défi transnational ».*

Retour sur évènement : Symposium des SIC

La cyberdéfense : enjeu mondial, priorité nationale

Le 10 octobre dernier se donnaient rendez-vous experts du monde militaire, de la recherche et de l'industrie, afin de fêter les 70 ans de l'arme des Transmissions.

L'arme des transmissions

Les Transmissions mettent en œuvre des SIC, Systèmes d'Information et de Communication militaires. Leur objectif : permettre aux opérationnels de disposer de *« capacités fiables de transmission des ordres et des comptes rendus »*[1]. Cette fonction vitale et essentielle à la conduite des opérations s'est nécessairement adaptée et développée en intégrant les innovations technologiques récentes. Le développement du réseau, de l'interopérabilité des SIC, la numérisation du champ de bataille : autant de défis que les Transmissions ont su relever et doivent encore affronter.

Ces systèmes qui contribuent à prendre l'ascendant sur un adversaire ont évolué, se sont informatisés et connectés ; faisant ainsi de la maîtrise du cyberespace un enjeu clé. La table ronde intitulée « La cyberdéfense : enjeu mondial, priorité nationale » tenue durant l'après-midi, a été l'occasion pour les différents intervenants[2] de souligner quelques fondamentaux.

Une cyberstratégie fortement influencée par l'absence de frontières entre civil et militaire

Convergence des technologies. Si auparavant les technologies étaient pour certaines impulsées par le secteur de la défense vers le monde civil, l'affirmation tend aujourd'hui à se nuancer. Désormais, les applications et technologies poussées par l'individu, le monde civil, sont bien plus nombreuses à influencer le monde militaire.

Confusion des profils. Il y a également convergence, voire confusion des profils : au sein du cyberespace, discriminer un acte civil d'un acte militaire, ou une cible civile d'une cible militaire serait extrêmement complexe. Cette confusion est d'autant plus présente qu'il est aisé pour un individu d'être *« civil la journée, hacker menaçant les intérêts de l'Etat le soir ».*

On assiste donc à une confusion des technologies, des lieux (théâtres d'opération) et profils civils et militaire. La conséquence directe est, selon les intervenants, l'impossibilité de transposer purement et simplement les doctrines et stratégies précédemment appliquées lors de conflits plus classiques (à l'image de la Seconde guerre mondiale). Une stratégie pertinente dans le cyberespace devra donc tenir compte de cette porosité des deux domaines.

Un « défi commun ». Partant de ce constat, les orateurs préconisent d'une part l'élaboration d'une défense commune aux différents acteurs industriels, militaires, politiques et civils. Ce *« défi commun »* au ministère de la défense et à ses principaux collaborateurs nécessite une coopération et un partage d'informations

[1] Symposium des SIC, livret, « Le 70ème anniversaire de l'arme ».

[2] Nicolas Arpagian, (INHESJ) – CA Coustillere (EMA) – M. Moliner (Orange) – M. Salvador (Sogeti) – M. Ventre (CNRS)

accrus. Tous doivent bénéficier de réseaux pleinement résilients et résistants aux attaques. Une volonté de défense commune qui se traduit également par la transversalité caractérisant la chaine opérationnelle de cyberdéfense au sein même des activités de défense.

Un « engagement patriotique personnel ». Les intervenants soulignent d'autre part l'importance de la mise en œuvre de la réserve citoyenne. Son objectif : sensibiliser, à travers un *« engagement patriotique personnel »* aux risques « cyber », sans attendre l'incident majeur qui aurait des conséquences irréparables (attaque ciblée combinée à l'encontre des réseaux ferroviaires, de distribution d'eau, etc.).

La proximité entre monde civil et monde militaire s'illustre enfin par la fourniture de solutions civiles industrielles aux militaires. Les experts en ont notamment profité pour aborder la question de la protection des infrastructures sensibles et, plus précisément, la position délicate des opérateurs de télécommunications.

La difficile position des opérateurs de télécommunication

Il ne se passerait pas une journée sans que l'opérateur Orange n'ait à détecter une activité hostile sur ses autoroutes de l'information. Les opérateurs de télécommunications sont ainsi contraints de trouver le juste milieu entre neutralité du réseau et protection des intérêts de leurs clients : particuliers, PME, multinationales... Un dilemme particulièrement difficile à gérer puisque ces opérateurs *« ne sont pas faits pour résister aux attaques massives d'un Etat ; ils n'en ont ni la vocation, ni les moyens ».* L'occasion pour les intervenants de pointer du doigt les activités de certains Etats qui mettraient en péril eux-mêmes le bon fonctionnement de leur propre réseau, en ayant des activités hostiles provoquant inévitablement des ripostes venues de pays cibles, ou de victimes collatérales.

Le « cyber », un domaine de défense à part entière

Si les conférenciers ont rechigné à considérer le cyberespace comme un véritable champ de bataille, ils ont confirmé qu'il s'agit là d'un domaine de défense à part entière. La cyberattaque est alors principalement perçue comme un outil participant d'une opération bien plus large, combinant effets cinétiques et virtuels. Faire tomber un réseau en amont d'une opération classique, c'est surtout placer l'ennemi dans une situation complexe, dans l'impossibilité de passer des ordres, de coordonner ses troupes, etc. Combiné à l'arme électronique, les effets peuvent être redoutables.

Exemple de scénario envisagé :

Déstabilisation d'un Etat (à travers les réseaux sociaux : cela monopolise les agences de renseignement qui baissent la garde sur les infrastructures sensibles) → Neutralisation des systèmes informatisés → Lancement de l'opération de grande envergure ainsi facilitée.

Smart grids : Quelles vulnérabilités ?

L'ADEC, Association pour le Développement des Entreprises et des Compétences, définit les smart grids comme des *« réseaux intelligents visant à intégrer de manière efficiente les actions de l'ensemble des utilisateurs (producteurs et consommateurs) afin de garantir un approvisionnement électrique durable, sûr et au moindre coût »*.[3] Alors que la continuité de l'approvisionnement et les coûts de déploiement du smart grid ont occupé pendant longtemps les débats, les entreprises d'électricité semblent actuellement accorder plus d'importance à l'équilibre entre la sécurité et la fiabilité du réseau, dans l'attente de nouvelles réglementations plus contraignantes. Certains estiment que les deux vont de pair : en augmentant la sécurité du smart grid, les entreprises pourraient prévenir des pannes de courant prolongées potentiellement provoquées par des cyberattaques, améliorant de fait la fiabilité du réseau.

Un état des lieux : quel niveau de risque ?

En août 2012, le département de la Sécurité intérieure des États-Unis (*United States Department of Homeland Security* ou *DHS*) a émis un avertissement contre RuggedCom, fournisseur leader en commutateurs et routeurs ainsi qu'en produits liés aux entreprises d'électricité situées en Amérique du Nord, Europe et Chine, et filiale de Siemens depuis 2011.[4] Le DHS a signalé une faille de sécurité qui pouvait être exploitée pour décrypter le trafic de données entre routeur et utilisateur final (*end user*). Selon Justin Clarke, expert en sécurité qui a révélé la faille, les pirates étaient en mesure de lancer des attaques par déni de service (DOS), d'infiltrer et de contrôler les réseaux électriques à haute tension sur lesquels sont connectés turbines, appareils et autres installations industrielles. Et M. Clarke de poursuivre : « *Si vous arrivez à pénétrer, il n'y a pratiquement pas d'authentification, il n'y a pratiquement aucun frein ou contrepoids pour vous arrêter* (…) *Pour accéder au réseau de RuggedCom, il faut simplement extraire la clé logicielle utilisée pour crypter le trafic* ».

Ces failles peuvent s'expliquer par le fait qu'avant le déploiement du smart grid, les technologies de réseau étaient développées pour des systèmes industriels fermés. En connectant la technologie héritée de cette période au monde informatique d'aujourd'hui, les fournisseurs IT ouvrent involontairement la porte au piratage.

Quelques exemples de failles récentes		
Cibles	Failles / Modes opératoires des pirates	Date
Contrôleurs logiques programmables (PLC) Simatic de **Siemens**[5]	Des attaquants peuvent commander à distance les PLC et collecter des informations de ces appareils (failles détectées par le créateur de Metasploit, H.D. Moore).	Mai 2012

[3] ADEC, Présentation sur Les réseaux électriques intelligents et la cyber sécurité, 06.2011.
[4] Greentechmedia.com, Smart Grid Cybersecurity: DHS Reports Vulnerability in RuggedCom's Software, 23.08.2012.
[5] Threatpost.com, Metasploit Holding On Siemens Exploits, 23.05.2011.

Interfaces de script ActiveX et application de serveur WebWare d'**ABB**[6]	Dépassement de tampons (*buffer overflow*) dans les interfaces de script COM et ActiveX sur le serveur WebWare.	Avril 2012
Contrôleurs logiques programmables (PLC*) D20 de **General Electric**[7]	En se connectant sur le serveur TFTP (*Trivial File Transfer Protocol*) des PLC* D20, un attaquant peut altérer la configuration de l'appareil (modifier les droits d'administration, mots de passe...) et partager ces informations sur des sites dédiés au piratage.	Janvier 2012
Contrôleurs logiques programmables (PLC) Simatic et logiciel Step 7 (S7) de **Siemens**	Ver Stuxnet (Symantec a depuis rapporté qu'une variante de ce ver, Duqu, a été développée vraisemblablement par le même groupe qui se cache derrière Stuxnet).	Décembre 2010

Cet avertissement de l'ICS-CERT (Équipe de réponse aux urgences informatiques pour les systèmes de contrôle industriel du DHS ou Industrial Control Systems Computer Emergency Response Team) n'était que le dernier d'une longue liste. L'ICS-CERT a rapporté en août 2012 90 vulnérabilités sur les sept premiers mois de l'année contre 60 en 2011. En multipliant ces avertissements, le DHS fait pression sur l'industrie pour qu'elle investisse davantage dans le secteur de la cybersécurité, face aux risques de ruptures d'approvisionnement en électricité.

En décembre 2011, le DHS a émis un avertissement contre un autre poids lourd du smart grid, Schneider Electric. En cause : les contrôleurs logiques programmables (*programmable logic controller* ou *PLC**) fabriqués par le géant français. Ces automates contenaient des informations d'identification codées en dur qui pouvaient être exploitées par un attaquant pour contourner le mécanisme de sécurité des appareils et accéder à ses commandes. Il était ensuite possible pour le pirate de visualiser ou altérer le logiciel embarqué, d'exécuter un code arbitraire ou de lancer une attaque par déni de service (DOS).[8]

Telvent, filiale de Schneider Electric, a également fait l'objet de critiques sur la sécurité de ses produits. Mocana, société californienne spécialisée en cybersécurité, a testé la vulnérabilité des unités déportées (*Remote Terminal Units* ou *RTU*) d'une entreprise d'électricité de Californie du Sud, fournies par Telvent et servant à opérer sa sous-station. Une seule journée a suffi pour trouver comment les hackers pourraient pénétrer le réseau, prendre le contrôle de ces RTU, peut-être provoquer l'explosion de transformateurs et générer des pannes de courant géantes.[9]

Mocana a identifié les vulnérabilités suivantes : « *Notre analyste a réussi à montrer qu'il pouvait récupérer et altérer la mémoire de données sur les RTU de Telvent, à distance* (…) *Il a pu extraire les éléments d'identification des administrateurs (sans permission)* (…) *Il a pu extraire les tokens de sessions d'administrateur en direct (tels que les cookies web)* ». Tout cela a été possible car « *le chiffrement SSL (secure sockets layer) n'était pas en place sur les interfaces d'administrateurs* (…) *le service VxWorks WDB était exposé par défaut et ne pouvait être désactivé* (…) *et les éléments d'identification des administrateurs*

[6] Blog.industrialdefender.com, ABB makes the tough, but right choice to not patch in latest advisory, 09.04.2012.
[7] Community.rapid7.com, Metasploit Updated: Forensics, SCADA, SSH Public Keys, and More, 19.01.2012.
[8] Greentechmedia.com, Smart Grid Cybersecurity Vulnerabilities Revealed, 16.11.2012.
[9] *Ibid*.

n'étaient pas stockés par un hachage cryptographique ». Notons que VxWorks, logiciel simple de Wind River Systems, est le leader des softwares déployés sur les appareils intelligents.

Les attaques visant à une déstabilisation du réseau ne sont pas les seules menaces pesant sur le smart grid : des compteurs intelligents vulnérables pourraient par exemple devenir une aubaine pour le vol d'électricité (à travers des programmes non autorisés qui commandent au compteur de sous-estimer la consommation individuelle).[10]

Quelles solutions ? Un marché de la cybersécurité du smart grid en construction

Pour reprendre notre second exemple, l'entreprise aidée par Mocana ne pouvait installer la nouvelle version de VxWorks où la faille avait été corrigée : les RTU de Telvent avaient trop peu de mémoire et de puissance de traitement. Ils ne pouvaient pas non plus être protégés par un pare-feu en raison de la nature de l'exploit et du potentiel physique de la vulnérabilité (une simple clé USB suffisait par exemple). L'entreprise d'électricité a donc choisi de remplacer intégralement son parc de RTU. L'entreprise d'électricité a estimé que le coût du remplacement était bien moindre que ce qu'il aurait fallu payer pour réparer le système en cas de cyberattaque.

Selon le cabinet GTM Research, les dépenses en produits et services de cybersécurité passeront de $120 millions en 2011 à $237,6 millions en 2015, faisant de ce segment le second poste de dépenses informatiques des entreprises d'électricité après l'automatisation de la distribution.[11]

Devant ces prévisions, le marché s'organise : en juillet dernier, EnerTech Capital and Export Development Canada (EDC) a annoncé un investissement de $3,85 millions dans la start-up spécialisée dans la cyber sécurité du smart grid N-Dimension Solutions Inc.[12] Les principaux acteurs - IBM, Cisco, HP, Microsoft, Accenture, CapGemini, Logica, Lockheed Martin, etc. - ne sont pas en reste et annoncent des solutions avancées pour leurs nouvelles offres dédiées au smart grid.[13] Des sociétés telles que MacAfee et Symantec pourraient très bien investir le secteur dans les années à venir.

Par ailleurs, les gouvernements et les régulateurs renforcent leur pression, notamment outre-Atlantique. En juillet, l'Agence de Sécurité Nationale des États-Unis (*National Security Agency*) a rapporté que les tentatives de cyberattaques avaient été multipliées par 17 entre 2009 et 2011.[14] Le même mois, une commission « énergie » du Sénat américain a rencontré des experts du GAO (*Government Accountability Office*), du FERC (*Federal Energy Regulatory Commission*) et du NERC (*North American Electric Reliability Corporation*) au sujet des vulnérabilités des États-Unis face aux cyberattaques.[15] L'absence de régulation spécifique à la cybersécurité des smart grids est un des facteurs de risque les plus discutés actuellement aux États-Unis.[16]

[10] Greentechmedia.com, Black Market Power and Phantom Blackouts: Smart Grid's Real Security Problems, 26.10.2010.
[11] Greentechmedia.com, Smart Grid's Utility Enterprise Market to Hit $8.2 Billion, Says GTM Research Report, 12.09.2011.
[12] Profectio.com, EnerTech Capital Investment in Critical Infrastructure Cyber Security Company, 24.07.2012.
[13] Bloomberg Businessweek, ABB in Cyber Arms Race With IBM as Industries Collide, 12.07.2012.
[14] New York Times, Rise is Seen in Cyberattacks Targeting U.S. Infrastructure, 26.07.2012.
[15] Smartgridnews.com, Cybersecurity and the grid: How bad is it and how do we make it better?, 18.07.2012.
[16] Smartplanet.com, Is the smart grid vulnerable to cyber warfare?, 25.07.2012.

Le portail OMC
La nouvelle plateforme de la DAS

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

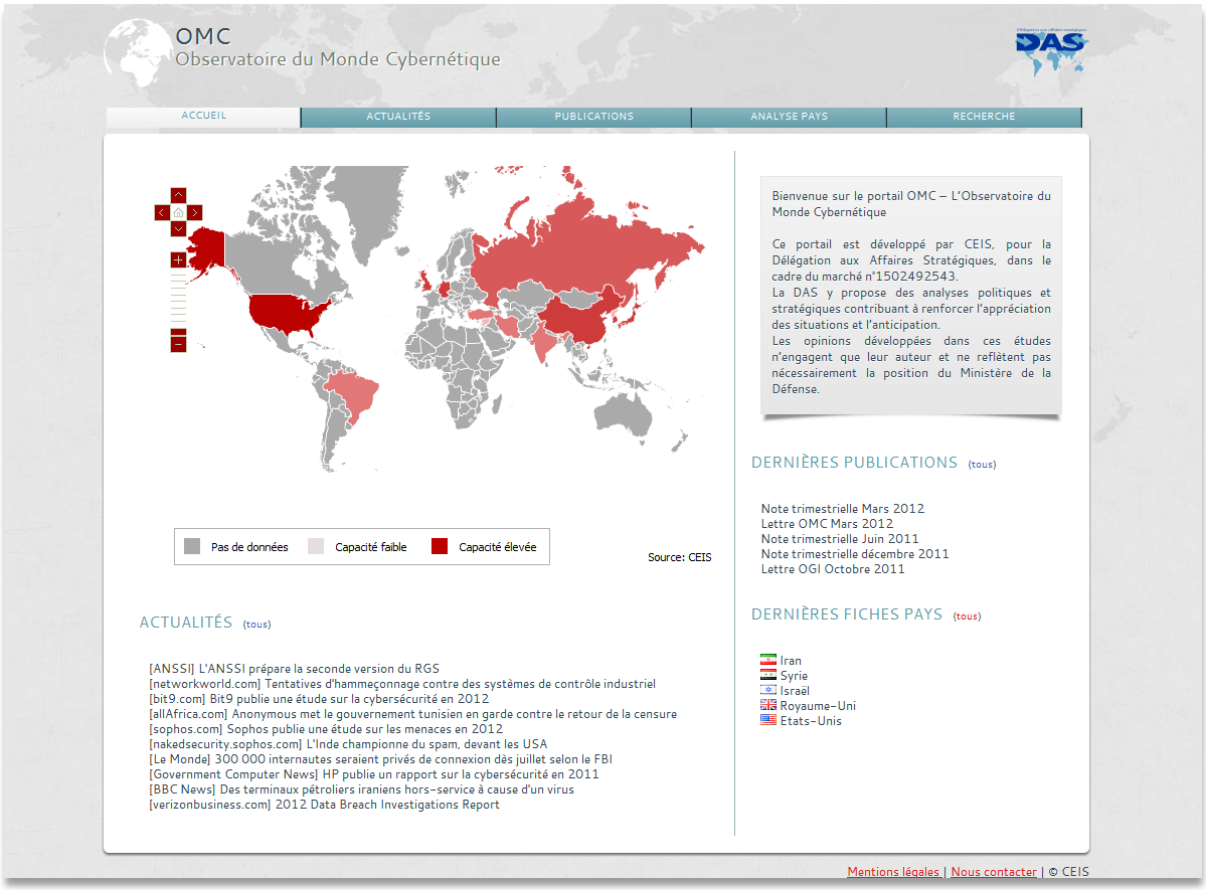

Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

Cyber Warfare & Security Forum	Brasilia	30 et 31 octobre
"The United States Commercial Service" et FireEye, Inc organisent une conférence sur le thème « Le paysage des menaces en évolution : Sécuriser votre entreprise contre les attaques ciblées. »	Paris	7 novembre
SC12	Salt Lake City (Etats-Unis)	10 – 16 novembre
Forum pour la Gouvernance d'Internet	Bakou (Azerbaïdjan)	Novembre
C&ESAR 2012 L'informatique en nuage, menace ou opportunité ?	Rennes	20 – 22 novembre
DefenceDays - Congrès sur la défense	Paris	28 – 29 novembre
Conférence mondiale des télécommunications internationales	Dubai	03 – 14 décembre
Colloque CDSE / Europol : "Les entreprises et l'Etat face aux cybermenaces "	Paris	6 décembre
SANS Cyber Defense Initiative (CDI) 2012	Washington DC	07 – 16 décembre

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