Observatoire du Monde Cybernétique

Lettre n°30 – Juin 2014

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

[ANSSI] L'homologation de sécurité en neuf étapes

L'ANSSI a mis en place un système d'homologation de cybersécurité afin d'attester que les risques résiduels, menaçant le système d'information des entreprises, sont connus et maîtrisés des responsables de la sécurité informatique.

[ZDNet] Redressement productif : le gouvernement valide les plans cybersécurité, cloud et souveraineté télécom

Le ministère du Redressement productif a validé, jeudi 5 juin, 7 plans pour rajeunir l'industrie française. Le cloud (100 000 emplois d'ici 2020), la cybersécurité (40 000 emplois en 2014) et la souveraineté télécoms (5G et fibre optique) sont des éléments clés de cette feuille de route.

[NextInpact] La Commission numérique ouvre ses portes : les 13 personnalités dévoilées

Claude Bartolone, président de l'Assemblée nationale, a inauguré la Commission numérique. Celle-ci a pour principaux objectifs de réfléchir et de faire des propositions concernant le numérique. Les principaux sujets qui seront abordés par les députés sont : la liberté d'expression sur internet, le respect de la vie privée, le droit à l'information, les données personnelles, le droit à l'oubli, la neutralité du Net, l'économique numérique, l'open data et la lutte contre la cybercriminalité. Une critique à été formulée à l'égard de cette commission : sa courte durée de vie, limitée à une année.

[AFDEL] Livre blanc « Filière cybersécurité en France »

L'AFDEL a rédigé un livre blanc critiquant le plan de cybersécurité, validé par Arnaud Montebourg, dans le cadre des 34 plans de la Nouvelle France Industrielle. Le rapport indique que plutôt que de créer un fond d'investissement semi-public se focalisant sur la nationalité des entreprises, il serait plus profitable d'ouvrir le marché aux investisseurs étrangers. Ces derniers auraient le capital nécessaire et le savoir-faire pour permettre aux PME et start-up d'atteindre leur taille critique.

[NextInpact] Cybercriminalité : les principales mesures du rapport Marc Robert

Dans son rapport sur la cybercriminalité, le procureur Marc Robert détaille les mesures issues du groupe de travail interministériel sur la lutte contre la cybercriminalité. Le document propose notamment la création d'un CERT français plu « grand public » que le CERT-FR dédié aux OIV, ainsi que la mise en place d'une délégation interministérielle chargée de la lutte contre la cybercriminalité qui serait dotée d'un pouvoir de sanction administrative (en matière d'analyse des contenus « manifestement illicites ».

[The Guardian] Le gouvernement du Royaume-Uni veut durcir les peines sanctionnant les cybercriminels

Le gouvernement du Royaume-Uni veut durcir les peines sanctionnant les responsables de cyberattaques qui causeraient la perte de vies humaines, des blessures, la propagation de maladies ou qui menaceraient la sécurité du Royaume. La peine maximale encourue serait de 14 ans d'incarcération, contre 10 ans actuellement. Les peines pour toute personne menant des opérations de cyberespionnage seront également alourdies. Cette réforme aurait cependant une limite : elle empêcherait les experts en cybersécurité de tester les cyberdéfenses des entreprises car cela serait considéré comme un acte cybercriminel.

[CSMonitor] Les élections ukrainiennes ciblées par des cyberattaques

Trois vagues de cyberattaques ont eu lieu entre le 22 et le 26 mai. La première attaque a débuté quatre jours avant les élections lorsque CyberBerkut, une équipe de hackers pro-russes, a infiltré le réseau informatique des élections et supprimé les fichiers nécessaires à son fonctionnement. Le système a été remis en état à partir de sauvegardes dès le lendemain, mais 40 minutes avant le résultat des élections, un nouveau virus a été découvert et supprimé sur le réseau des élections centrales, virus qui avait pour finalité de changer le résultat des élections, en

donnant Dmytro Yarosh (Secteur Droit) gagnant avec 37% des voix. Cette opération semble en accord avec la rhétorique russe, qui chercherait ainsi à décrédibiliser ces élections. Après la fermeture des bureaux de vote, les réseaux ont subi des attaques DDoS retardant pendant deux heures l'annonce du résultat des élections.

[Spiegel] Snowden : Der Spiegel publie 200 pages de documents confidentiels sur les activités de la NSA en Allemagne

Le journal Der Spiegel a publié 200 pages de documents confidentiels, dévoilés par Edward Snowden, sur les activités de la NSA en Allemagne et sa coopération avec le BND. Les documents mettent en évidence le rapprochement entre les deux agences dans les activités de renseignement électromagnétique. Selon trois experts en droit constitutionnel allemand (Hans-Jürgen Papier, Wolfgang Hoffmann-Riem, Matthias Bäcke) cette coopération est anticonstitutionnelle car le Parlement n'avait pas été consulté au préalable. On apprend également que l'Allemagne serait devenue le centre des opérations d'espionnage de la NSA en Europe. En effet, pas moins de 6 bases opérées par la NSA sont localisées dans le pays.

[Janes] La Marine indonésienne établira un commandement cyber

L'Amiral Marsetio a annoncé que la Marine indonésienne établira un commandement cyber. Ce dernier aura comme mission de coordonner et de protéger les flux de communications des forces navales.

[Globalpost] Première rencontre diplomatique bilatérale entre les Etats-Unis et le Brésil depuis les révélations de Snowden

Joe Biden, vice-président des États-Unis, a été reçu par Dilma Rousseff, présidente du Brésil, mardi 17 juin 2014. C'est la première rencontre diplomatique bilatérale depuis les révélations de Snowden sur les activités d'espionnage de la NSA à l'encontre de Rousseff et du conseil d'administration de Petrobras, suivie du discours de Dilma Rousseff devant la 68ème Assemblée Générale de l'ONU accusant les États-Unis d'avoir « violé les libertés civiles des brésiliens ». Au cours de cette réunion diplomatique, Joe Biden a assuré la présidente brésilienne que Barack Obama avait pris des mesures pour s'assurer « qu'internet ne devienne pas un outil gouvernemental de répression ».

[White House] Accord de coopération cyber entre les Etats-Unis et l'Australie

Les États-Unis et l'Australie ont officiellement réitéré leur volonté de coopérer face aux cybermenaces. Le communiqué de presse de la Maison Blanche fait état d'un engagement bilatéral d'assistance en cas de cyberattaques. La coopération cyber entre les deux pays était déjà importante du fait de la « Five Eyes Alliance ».

[Facebook] Anonymous démarre sa campagne de cyberattaques contre le gouvernement brésilien et les sponsors de la Coupe du Monde 2014

Le groupe de hackers Anonymous a lancé, mercredi 11 juin à 13h00, sa première cyberattaque massive contre les sites internet du gouvernement brésilien et des sponsors de la Coupe du Monde 2014 dans le cadre de l'opération #OpWorldCup.

[People's Daily Online] Putter panda : la Chine rejette les accusations formulées par Crowdstrike

La Chine a officiellement rejeté l'accusation, formulée par l'entreprise de cybersécurité Crowdstrike et relayée par le gouvernement américain, selon laquelle l'armée chinoise serait liée à un groupe de hackers surnommé « Putter Panda ». Ces cybercriminels sont accusés d'avoir exfiltré des informations confidentielles d'entreprises américaines et européennes opérant dans le secteur spatial et des satellites. Selon le porte-parole du ministère des Affaires Étrangères, Hua Chunying, l'attitude des États-Unis est contre-productive : « plutôt que d'accuser d'autres pays

de cyberespionnage, les américains feraient mieux de se repentir et de corriger leurs propres erreurs ».

[The Diplomat] Le Japon offrira avec les États-Unis une aide technique aux pays membres de l'ASEAN dans la lutte contre les cybercrimes

Le Japon a annoncé, samedi 7 juin, qu'il offrira avec les États-Unis une aide technique aux pays membres de l'ASEAN dans la lutte contre les cybercrimes. Les deux pays financeront l'envoi d'experts, ce qui représenterait une dépense de 400 000 dollars. Selon une source du gouvernement japonais, cette assistance serait motivée par l'intensification des cyberattaques chinoises.

[CCTV] 30% des cyberattaques ciblant la Chine seraient lancées par des serveurs localisés aux Etats-Unis

L'agence gouvernementale de cybersécurité Computer Emergency Response Coordination Team a dévoilé qu'onze millions d'ordinateurs chinois sont infectés par des malwares et contrôlés de l'étranger. Les attaques venant des États-Unis représenteraient 30% du total.

[The Washington Post] Newscaster: l'opération de cyberespionnage iranienne, mise en place depuis 2011, dévoilée

Le site internet de cybersécurité « iSIGHT Partners » a découvert une opération d'espionnage menée depuis 2011 par des hackers iraniens, et ciblant des hauts fonctionnaires et des officiers militaires américains. Les hackers, se constituaient une fausse identité de journaliste sur internet puis entraient en contact avec les cibles à travers les sites de réseaux sociaux. Une fois la relation établie, ils envoyaient aux victimes des messages de « spear-phishing » afin de capturer leurs identifiants et codes d'accès. « iSIGHT Partners » n'a pas réussi à déterminer, le type et la quantité de données exfiltrés grâce à cette opération.

[Schneier] Etude de la sécurité du chiffrement symétrique contre la surveillance de masse

Une étude publiée le 21 juin étudie la sécurité des algorithmes de chiffrement symétriques face à la menace des programmes de surveillance de masse, notamment aux ASAs (Algorithm-Substitution Attacks), attaques qui consistent à remplacer l'algorithme de chiffrement original à l'insu des utilisateurs. L'étude explicite le fonctionnement de ce type d'attaque et propose des solutions de défense.

[NetworkWorld] Une étude de McAfee met en garde contre une recrudescence des rootkits

Dans une étude publiée le 24 juin, des chercheurs de la société McAfee mettent en garde contre une recrudescence des rootkits, dont le nombre de nouvelles créations a atteint le niveau de 2011. Les rootkits, qui facilitent la furtivité des malwares en s'intégrant au noyau du système d'exploitation, avaient vu leur croissance ralentie par le passage aux systèmes 64 bits, intégrant des protections contre ce type de faille. Cependant, si ces nouvelles protections ont augmenté le coût de réalisation de rootkits, l'augmentation du nombre de systèmes 64bits incite également les attaquants à investir dans ce domaine. Une technique commune consiste à utiliser des certificats volés afin de faire passer le malware pour un driver légitime, signé numériquement.

[NSFOCUS] Publication d'un rapport de menace du fait des serveurs NTP

La société NSFOCUS, spécialisée en solutions et services en sécurité réseau pour les entreprises, a publié le 26 juin un rapport révélant l'état de la menace posée par les serveurs NTP encore vulnérables aux attaques. Les serveurs NTP (Network Time Protocol) sont utilisés pour synchroniser les horloges internes des ordinateurs, mais ils peuvent être utilisés comme outil pour lancer des attaques DDoS par amplification. En effet, une simple commande adressée à ce type de serveur renvoie l'adresse des 600 derniers ordinateurs qui ont communiqué avec celui-ci. Ainsi, en usurpant l'adresse IP de la victime, un attaquant bénéficie d'un facteur d'amplification supérieur à 700. Le nombre de serveurs NTP vulnérables est passé de 432 120 en décembre 2013 à 21 156 en mars 2014, mais 17 000 seraient encore vulnérables d'après le rapport.

Etude : « Whois Privacy and Proxy Service Abuse »

Richard Clayton et Tony Mansfield, chercheurs respectivement au Computer Laboratory de l'Université of Cambridge et au National Physical Laboratory d'Hampton Road, ont publié le 22 juin une étude sur les abus du système Whois et des services de proxy. Ce rapport fait suite à une proposition de l'ICANN en date du 19 mai visant à introduire des mesures pour assurer la véracité des informations de contact fournies lors de l'enregistrement d'un nom de domaine. L'étude démontre que si entre 29 et 55% des criminels utilisent des services de proxy ou d'anonymisation lors de l'enregistrement d'un nom de domaine, c'est aussi le cas de 28% des banques et 44% des sites pour adultes légaux. Ainsi, mettre fin à ce type de services « pourrait affecter une partie substantielle d'activités légales, alors que les criminels se contenteraient probablement de renseigner des informations incomplètes ou erronées » lors de l'enregistrement de leur site web.

[IBM] Publication de l'IBM Security Services 2014

IBM a publié son rapport 2014. Sur les milliards d'alertes émises par les équipements de sécurité installés au sein des entreprises, seules quelques centaines cachent des cyberattaques à haut risque. La finance et l'assurance restent les secteurs les plus visés (regroupant 23,8% des incidents), devant l'industrie (21,7%) et l'information et la communication (18,6%). Le commerce ne représente que 6,2% des cyberattaques recensées.

[CLUSIF] Le CLUSIF publie son panorama des référentiels de sécurité des systèmes industriels

Le Club de la Sécurité de l'Information Français a publié, le mercredi 18 juin, son panorama des référentiels de sécurité des systèmes industriels et les 5 étapes clés d'un programme de sécurisation. Les systèmes industriels (chaîne de montage, système d'arme dans la défense, distribution d'énergie, réseau d'eau) utilisent les réseaux afin d'optimiser leur fonctionnement. Toutefois, cela crée de nouveaux risques que les organisations doivent prendre en compte.

[U.S. GAO] L'US Government Accountability Office dénonce l'inquiétante vulnérabilité des infrastructures portuaires

Un rapport de l'US Government Accountability Office (GAO), publié le 5 juin, fait état de l'inquiétante vulnérabilité des infrastructures portuaires face à de potentielles cyberattaques. Aucun diagnostic sur l'efficacité ou la résilience de leurs systèmes de cybersécurité n'a pour l'instant été mené par le Department of Homeland Security ou par la Garde Côtière. Une cyberattaque endommageant les systèmes de communications et d'informations des ports maritimes américains serait désastreuse pour l'économie nationale. D'où la demande du GAO de catégoriser ces infrastructures comme opérateur d'importance vitale et de mieux former la Garde Côtière à la cybersécurité.

[Vodafone] Rapport sur la coopération de Vodafone avec les Etats

Vodafone a publié un rapport détaillant sa coopération souvent forcée avec les États dans lesquels elle opère. L'entreprise de télécommunication anglaise affirme son attachement aux respects de la vie privée de ses clients, mais explique qu'elle doit dans certaines occasions se plier aux exigences des gouvernements et dévoiler des informations sur ses clients. Tout refus entrainerait l'annulation de sa licence d'exploitation et des poursuites judiciaires. Du fait de cette situation, l'entreprise a décidé de faire preuve de la plus grande transparence possible en détaillant les exigences de chaque pays auxquelles elle a dû répondre.

[McAfee] Estimation du coût global des cybercrimes

Selon McAfee, les cybercrimes coûteraient entre 375 et 575 milliards de dollars par an soit 0.8% de l'économie mondiale contre 0.9% pour le trafic de drogue ou 0.89% pour la piraterie. Les cybercrimes sont également responsables de la destruction de 200 000 emplois américains et 150 000 emplois européens.

Visualisation du cyberespace

Le cyberespace est difficile à représenter dans sa dimension technique, du fait de sa taille et de sa complexité. Il est en effet composé de multiples couches correspondant à différents niveaux d'abstraction. Afin d'assurer la sécurité des réseaux dont ils sont responsables, les administrateurs système utilisent des outils de surveillance de ces multiples couches du cyberespace. Mais ces derniers n'apportent généralement pas une visualisation explicite de l'environnement virtuel qui approcherait une représentation cognitive du cyberespace.

Une interface visuelle représentant explicitement le cyberespace, corrélant les données relatives au réseau et à sa sécurité, serait utile non seulement aux administrateurs réseaux, mais permettrait également d'apporter une perception de situation aux néophytes, particulièrement dans le cadre d'une gestion de crise cyber. Nombre de chercheurs se sont penchés sur cette problématiquedepuis 10 ans, mais pour l'heure les programmes ayant une telle ambition ne sont encore qu'à l'état de projet.

La visualisation des données

Visualisation et théorie cognitive

Un outil de visualisation du cyberespace se doit d'utiliser les connaissances issues des travaux de recherche en matière de communication de l'information appliquée à l'informatique. Un domaine à part entière - la visualisation d'information - a en effet émergé « à partir des recherches dans des disciplines telles que l'interaction homme-machine, les sciences informatiques, le graphisme, le design, la psychologie et les méthodes commerciales »[1].

Pour les créateurs de VisAlert[2], l'interface d'un tel outil devrait être aussi proche que possible de la représentation cognitive de l'utilisateur afin de rendre la compréhension plus rapide et plus précise. Cela revient à dire que cette interface doit être intuitive, et par là-même qu'il y a une corrélation entre la vitesse de prise en main de l'outil et son efficacité sur le long terme.

Quelques écueils sont à éviter, comme, par exemple, la surcharge visuelle, quitte à traiter indépendamment les différents niveaux d'abstraction du cyberespace.

Certains experts estiment en outre qu'un outil de visualisation devrait éviter la troisième dimension[3] car la perspective prive celui-ci de l'efficacité de certains attributs de visualisation, notamment la taille des objets représentés.

Enfin, il faut prendre en compte le pourcentage non négligeable d'individus atteints d'une forme quelconque de daltonisme, presque 10% pour les hommes, lors des choix de code couleur comme attribut de visualisation afin de distinguer celles-ci. Eviter l'utilisation du rouge et du vert, couleurs concernées par la forme la plus courante de daltonisme, semble donc judicieux.

[1] Benjamin B. Bederson et Ben Shneiderman, *The Craft of Information Visualization : Readings and Reflections*, 2003, Morgan Kaufman
[2] http://digital.cs.usu.edu/~erbacher/publications/VisAlertCGA2006.pdf
[3] Jay Jacobs, Bob Rudis, *Data-Driven Security*, 2014

Sources de données

On peut distinguer plusieurs catégories de sources de données utiles à la visualisation du cyberespace.

En premier lieu, nous retrouvons les caractéristiques propres au réseau et aux éléments le constituant : la nature des éléments (poste client, serveur, équipement réseau, etc.) et leurs caractéristiques (adresse IP, système d'exploitation, logiciels, paramétrage, etc.).

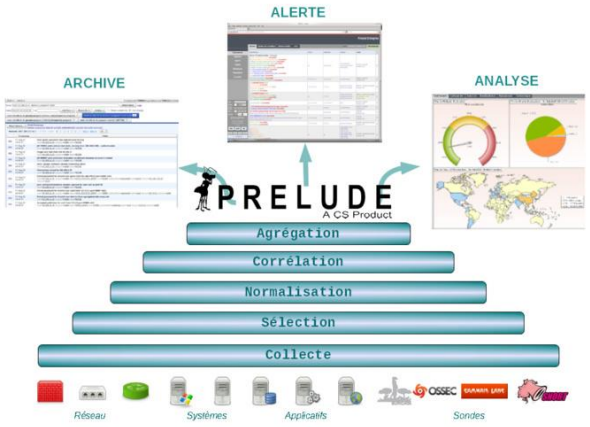
Ensuite viennent les évènements réseaux survenant sur les différents éléments du réseau et recueillis dans les logs (journaux d'évènements). A ce sujet, le domaine se retrouve confronté à une grande diversité des formats de log. Les travaux de l'organisation MITRE en vue de la création d'une norme à vocation universelle appelée CEE (Common Event Expression) ont suscité beaucoup d'espoirs dans la communauté, jusqu'à ce que ces travaux ne prennent fin en juillet 2013 à la suite de l'arrêt du soutien financier du gouvernement U.S..

Ces évènements sont analysés par un SIEM (Security Information and Management System). Ces systèmes gèrent et corrèlent les logs à la recherche d'une même cause à différents évènements, fournissant le résultat de ces analyses au sein de rapports et de tableaux de bord et lançant les alertes qui constituent la troisième catégorie de données. Du fait de la multiplicité et du volume des logs, cette tâche est cependant difficile à traiter en temps réel. Pourtant, cet élément est capital en matière de visualisation.

D'une visualisation statique à une visualisation dynamique

Visualisation statique

Les SIEM et les scanners de vulnérabilité permettent de réunir les données nécessaires à la génération de cartes d'un réseau assorties des vulnérabilités et des attaques recensées sur une période donnée. Pourtant ceux-ci ne fournissent pas une telle représentation et ces outils se contentent de rapports et de tableaux de bord plus arides.



PRELUDE, un SIEM Open Source[4]

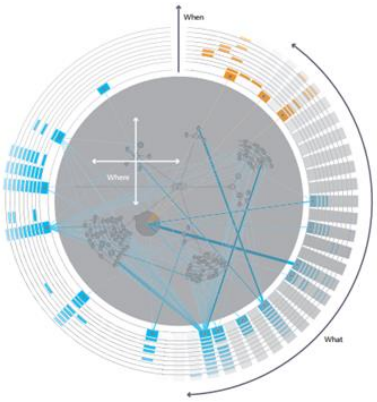
[4] Une version spécifique est commercialisée par la société CS : http://www.c-s.fr/CS-acquiert-la-solution-Prelude-IDS-dans-le-cadre-de-son-offre-de-cyber-securite_a444.html

Un rapport de vulnérabilité de Nessus 5 (scanner de vulnérabilités), indiquant pour chaque machine appartenant au réseau scanné le nombre de vulnérabilités détectées ainsi que leur type

Visualisation dynamique

Un outil de visualisation du cyberespace doit permettre de posséder une perception de situation : la possibilité de pouvoir observer en temps réel un réseau et les évènements le concernant, et ainsi permettre une surveillance efficace de celui-ci.

Les chercheurs à l'origine de VisAlert ont opté pour une interface visuelle en deux dimensions basée sur trois axes : « Quoi, Quand, Où ». Cela permet à l'utilisateur de voir l'état du réseau en temps réel, mais également de corréler cette conjoncture avec les évènements précédents et ainsi de pouvoir déterminer la stratégie de l'attaquant (et ainsi pouvoir prévoir et parer son prochain coup). La carte du réseau se situe au sein du disque, alors que les évènements, classés par catégories d'alertes, sont inscris sur les cercles chronologiques externes. Des faisceaux lient les évènements du moment t0 (le cercle intérieur) aux éléments du réseau auxquels ils correspondent.



VisAlert – Concept

VisAlert – Illustré en situation

L'outil exploite des alertes de type Snort (en bleu) et évènements Windows (en orange). Ici, l'attaquant tente d'accéder à un système vulnérable, tout en sondant intensivement un autre système afin de détourner l'attention de la cible réelle.

De la visualisation du cyberespace à l'interaction avec celui-ci

Plan X : Philosophie et objectifs du projet de la DARPA

Initié fin 2012, le projet Plan X conduit par le DARPA Cyberwar Laboratory a pour principal objectif d'apporter des outils et des capacités cyber warfare « clés en mains »[5]. Ces outils doivent être particulièrement intuitifs afin de ne nécessiter qu'une formation cyber minimale : il s'agit de créer l'outil du cybersoldat. L'outil doit en outre pouvoir apporter la perception de la situation cyber tant aux niveaux stratégique que tactique. Il s'agit ainsi de développer une interface de visualisation du cyberespace permettant d'interagir avec cet environnement, notamment avec le déclenchement de cyberattaques prédéfinies.

Visualisation et interfaces 3D

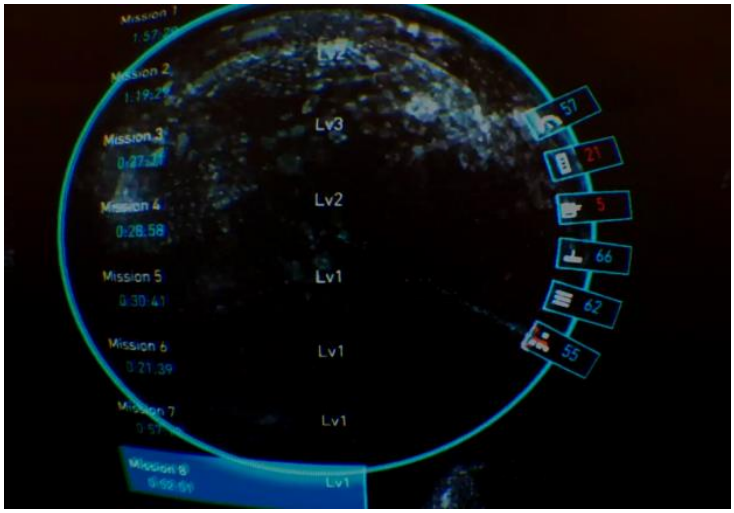
Plan X repose sur un moteur graphique 3D afin de représenter le cyberespace. La DARPA expérimente avec l'Oculus Rift6 l'idée d'offrir une plus grande immersion de l'utilisateur dans l'univers cyber, en lui permettant de « nager au sein de l'information et [de] la comprendre ». La DARPA envisage ainsi abandonner le clavier et ne se baser que sur des interfaces aussi intuitives que possible. Il n'est plus question pour l'utilisateur de devoir saisir les adresses IP des cibles ou de coder des attaques, l'interface et le système en arrière plan doivent permettre d'effectuer en toute simplicité les opérations les plus complexes. Autre support en cours d'expérimentation : des tables tactiles d'affichage 3D holographique.

Proof-of-Concept - Plan X sous Oculus Rift

Les nouvelles générations - celles qui ont grandi à l'ère d'un internet et d'une informatique omniprésents et qui ont été habituées à travers les jeux vidéos à jongler avec différents niveaux d'abstraction informatique - seront particulièrement réceptives et à l'aise avec ce type de technologie. Le Cyber Command prévoit ainsi de recruter ses futurs « cybersoldats » à la sortie du lycée et de l'université afin d'intégrer le plus rapidement cette génération au sein de leurs forces cyber.

Les premières démonstrations, simples preuves de concept, laissent cependant à penser que l'outil en développement est encore loin d'offrir une visualisation claire et aisée du cyberespace.

[5] http://www.defense.gov/news/newsarticle.aspx?id=122455
[6] http://www.wired.com/2014/05/darpa-is-using-oculus-rift-to-prep-for-cyberwar/



Proof-of-Concept - Plan X sous Oculus Rift

Un outil unifié de visualisation et d'interaction avec le cyberespace doit encore cumuler au sein d'une même interface les informations concernant l'état du réseau et les éléments permettant l'action, que celle-ci soit de type défensif ou offensif. Cela implique un travail d'automatisation à l'extrême des actions, bien loin de ce qui est envisageable dans le domaine civil notamment du fait de l'hétérogénéité des éléments constitutifs des réseaux. Faute de cette simplification, la représentation ne pourrait que souffrir d'une surcharge visuelle qui desservirait grandement l'outil et compliquerait son accessibilité au plus grand nombre.

Le domaine civil peut quoiqu'il en soit reprendre à son compte l'idée d'une représentation interactive du cyberespace, permettant l'action à des fins défensives sur les éléments du réseau sous la responsabilité de son opérateur. L'adaptation et la configuration de l'outil seraient facilitées par la connaissance du réseau de l'entreprise concernée.

Le portail OMC
La plateforme de la DAS

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

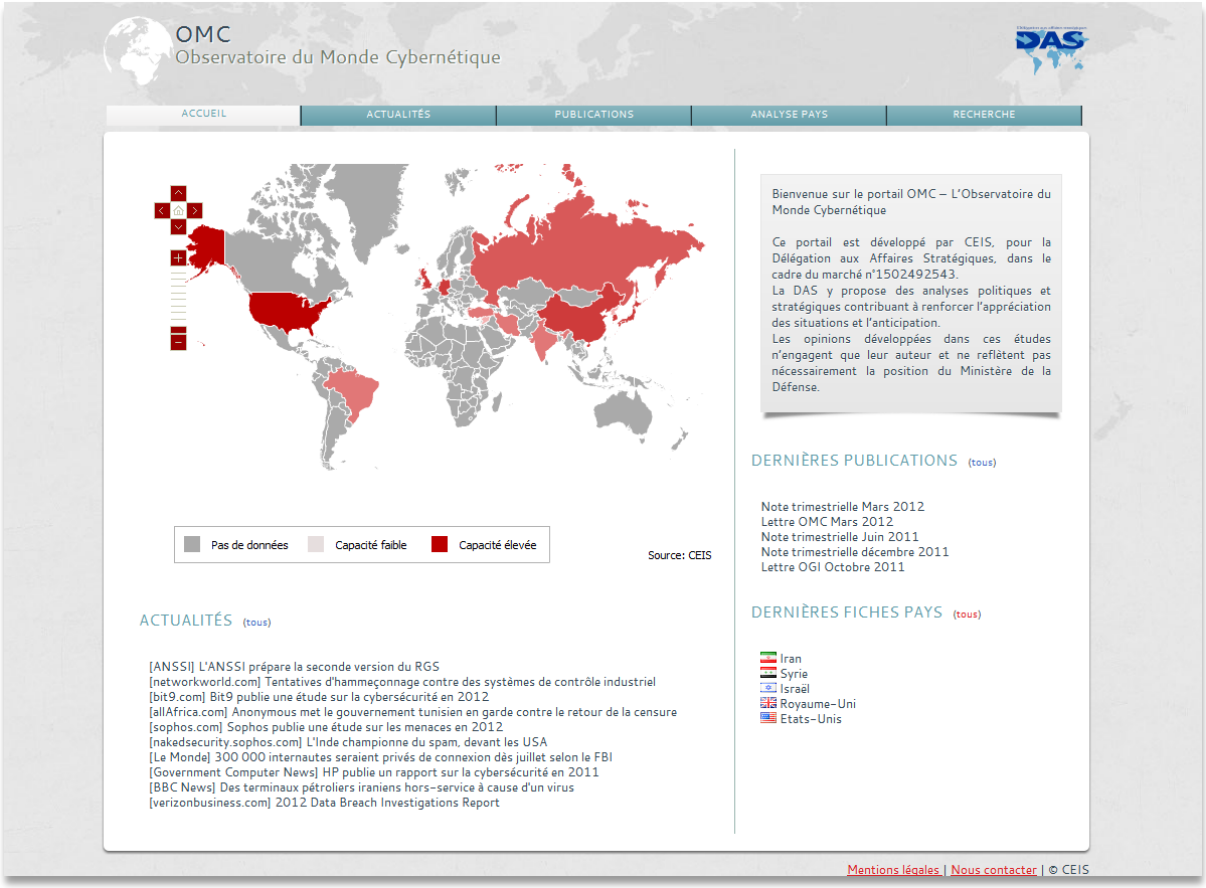


Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

RSA Conference	Singapour	22 - 23 juillet
Black Hat USA	Las Vegas	2 - 7 août
SecProTec East Africa 2014	Kenya	20 - 22 août
Cyber Europe 2014	Belgique	22 - 24 septembre
NFC World Congress	Marseille	22 - 24 septembre

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