Observatoire du Monde Cybernétique

Lettre n°35 – Novembre 2014

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

[theatrum-belli.org] Le Gicat coopère avec Hexatrust

Le Groupement des industries françaises de Défense terrestre et aéroterrestre (Gicat) s'allie avec Hexatrust, afin de porter l'excellence française en matière de logiciels de protection numérique. Les deux groupements se sont donnés comme premier objectif de réaliser un catalogue d'offres vantant les mérites de la cybersécurité française, qui sera distribué sur différents salons.

[7seizh] Appel à projets cybersécurité de la Région Bretagne

La région Bretagne a récemment lancé un appel à projet cybersécurité. Cette initiative portée par la Meito dans le cadre du Pôle d'excellence cyber a pour objectif d'accélérer la mise sur le marché de solutions de cybersécurité développées par les PME régionales. La date limite de dépôt des dossiers était le 1er décembre 2014.

[La Tribune] Airbus Helicopters victime d'un piratage informatique américain ?

Airbus Helicopters aurait fait part de « fortes suspicions » d'avoir été victime d'une cyberattaque venant des Etats-Unis dans le contexte de l'appel d'offres international lancé par la Pologne qui l'oppose à l'italien AgustaWestland et à l'américain Sikorsky pour la fourniture de 70 hélicoptères.

[Numerama] OpAntiRep : Anonymous s'attaque à la gendarmerie française

Le mouvement social de soutien au manifestant Rémi Fraisse s'est étendu au Web, mobilisant de nombreux hacktivistes autour de l'opération baptisée « OpAntiRep ». Le 22 novembre (érigé en journée internationale contre les répressions et violences policières), les Anonymous ont lancé l'offensive médiatique par une campagne sur Twitter, une série de défigurations, ainsi que la divulgation de données à caractère personnel à l'encontre des forces de l'ordre françaises et italiennes.

[01net] Vers la reconnaissance juridique du vol de données

La loi antiterroriste du 13 novembre constitue un tournant dans la prise en compte pénale du « vol de données ». Elle modifie en effet l'article 323-3 du code pénal. Le texte qui se contentait de réprimer l'introduction frauduleuse de données dans un système informatique, leur modification ou leur suppression, cible aujourd'hui les faits « d'extraire, de détenir, de reproduire ou de transmettre » frauduleusement des données.

[Le Monde] « Onymous » : une opération d'envergure contre les marchés noirs en ligne

Début novembre 2014, les autorités américaines et européennes ont annoncé avoir fermé plus de 400 sites Web utilisant des adresses en .onion. Elles sont parvenues à pister la localisation de serveurs et plusieurs administrateurs de sites ont été arrêtés. Cette action, qui a notamment permis la fermeture de Silk Road 2.0, a été coordonnée dans le cadre de l'opération dite Onymous. Cette opération a notamment soulevé de nombreuses interrogations quant aux garanties d'anonymat fournies par le réseau Tor.

[Nice Matin] Un piratage informatique déjoué au CHU de Nice

Le CHU de Nice a été victime, en juillet dernier, d'une intrusion dans ses systèmes informatiques. Le maliciel, qui a touché une douzaine de postes, avait pour objectif de collecter des données médicales sensibles. Derrière cette attaque, un infirmier curieux qui a, par la suite, accepté de coopérer avec la Police judiciaire.

[NextImpact] Nouveau projet de loi allemand à l'encontre des Etats-Unis

Le Parlement allemand annonce un nouveau projet de loi dans le domaine numérique, qui devrait sensiblement déplaire aux Etats-Unis. Ce projet veut encadrer la vente de produits numériques par les sociétés américaines sur le territoire allemand. Pour éviter toute restriction, ces sociétés devraient dévoiler leurs codes sources au gouvernement,

évitant ainsi une utilisation malveillante de certains programmes par les agences de renseignements américaines.

[Le Monde] Des espions anglais et américains ont-ils créé le virus Regin ?

Selon les experts de Symantec et de Kaspersky, le malware Regin serait, en raison de sa complexité, l'œuvre d'un Etat. Les Etats-Unis et le Royaume-Uni sont pointés du doigt, notamment par Ronald Prins, expert chez Fox-IT. En effet, plusieurs des fonctionnalités de Regin correspondent aux programmes de la NSA révélés par Edward Snowden et, plus précisément, aux attaques qui ont été menées par la NSA et le GCHQ contre Belgacom et les institutions européennes. La Belgique fait bien partie des pays dont les réseaux ont été infectés par le malware.

[Symantec] Le malware Regin, presqu'aussi redoutable que Stuxnet

Symantec a révélé qu'un virus informatique très sophistiqué avait été utilisé dans une attaque contre des opérateurs télécoms russes et saoudiens. Ce virus, baptisé « Regin », serait au moins aussi redoutable que Stuxnet, qui avait causé de gros dégâts en 2010 dans le programme nucléaire iranien. On ignore encore de quelle manière le virus infecte les systèmes informatiques. Il s'est jusqu'à présent attaqué à des fournisseurs d'accès à internet en Russie, Arabie Saoudite, au Mexique, en Irlande et en Iran. Son objectif serait de dérober des données confidentielles, et il aurait la capacité de s'adapter à tous types de réseaux. Il serait aussi capable, dans certains cas, de faire disparaître toute trace de son passage une fois sa mission accomplie.

[Le Soir] Le Centre belge de cybersécurité ne sera pas prêt avant 2015

Le Centre Cyber Security Belgique (ou CCSB) ne devrait être opérationnel que début 2015, selon le cabinet du Premier ministre Charles Michel.

[Numerama] L'Europe adopte une position sur l'avenir de l'ICANN

Le jeudi 27 novembre, le Conseil de l'union européenne a rappelé sa volonté de réformer l'ICANN, afin d'assurer transparence, responsabilité et prise en compte démocratique des acteurs au sein d'une gouvernance multipartite. Les détails de cette prise de position seront bientôt publiés.

[SCMagazine] Londres simule une cyberattaque terroriste

Au programme du 2015 Cyber Security Challenge UK Masterclass, le Royaume-Uni souhaite simuler une attaque terroriste informatique ciblant les infrastructures critiques du pays. Les acteurs essentiels du réseau tels que BT, le GCHQ, NCA, Juniper ou encore le groupe Airbus seront sollicités pour cet exercice.

[Wired UK] Le GCHQ britannique travaille avec les opérateurs télécoms du territoire

Le GCHQ britannique est au centre d'une nouvelle affaire de surveillance de masse, avec la coopération des opérateurs télécoms privés du territoire. Selon une enquête de Channel 4 News et de WRD, l'agence aurait accès aux réseaux et infrastructures des agences de télécommunications. Certains cas feraient référence à de la collecte d'informations par les compagnies privées, ensuite acquises par le GCHQ. Différents projets ont été mis à jour entre l'agence et les compagnies privées, révélant une forte collaboration entre le secteur privé et le secteur public.

[Homeland Security] L'US Army crée une « Cyber Branch »

L'US Army annonce la création d'une section « cyber ». Cette section fera désormais partie des choix de carrière envisageables, aux côtés des traditionnelles branches de l'infanterie, artillerie etc. Objectif : renforcer le recrutement, les budgets et l'innovation en termes de cyberdéfense.

[NATO] Lancement du plus important exercice OTAN de cyberdéfense jamais organisé

Le 18 novembre 2014, l'OTAN a lancé son plus grand exercice multinational de cyberdéfense, Cyber Coalition 2014. Cet exercice d'une durée de trois jours a permis de tester la capacité de l'Alliance à défendre ses réseaux. C'est le septième exercice annuel de ce type. Plus de 670 experts ont participé à cette opération démultipliée dans des dizaines de sites localisés dans les pays membres de l'Alliance mais aussi quelques pays partenaires.

[Reuters] De nombreux médias occidentaux pris pour cible par la SEA

Le 27 novembre, la Syrian Electronic Army a attaqué de nombreux sites de médias occidentaux. Cette attaque exploitant une faille DNS marque le retour du collectif de pirates informatiques pro-gouvernementaux, jusque-là resté silencieux. Parmi les cibles : The Daily Telegraph, Forbes ou encore PC World.

[GData] Uroburos : la campagne est toujours active

Selon l'éditeur de sécurité allemand GData, le rootkit attribué à la Russie, Uroburos, serait toujours en activité. En effet, 9 mois après la première publication sur Uroburos, une nouvelle version d'agent.BTZ serait en circulation.

[Le Monde] Le changement de stratégie de Daesh sur Internet

Après une première étape de communication massive sur les réseaux sociaux, les combattants de Daesh se font plus discrets. Suite aux instructions données par leur Comité général, photos, vidéos et messages compromettants sembles proscrits sur les réseaux sociaux, au profit d'une plus grande vigilance. L'objectif derrière cette « *#CampagneDeDiscrétionMédiatique* » est d'éviter de renseigner l'ennemi sur les déplacements, tactiques, opérations en préparation, informations techniques sur les armes employées, identité des membres ou encore localisation des casernes. Cette initiative laisserait supposer que de véritables spécialistes des réseaux sociaux seraient à la manœuvre.

[AP] Mosul : Daesh coupe le réseau de télécommunications afin d'endiguer les échanges

Selon Associated Press, Daesh aurait coupé, le 26 novembre, la totalité des communications téléphoniques afin d'empêcher toute coordination et tout échange des forces syriennes, iraquiennes et américaines. Cette coupure aurait provoqué une situation de paralysie et de chaos dans les rue de Mosul. Cet acte traduit un revirement complet de stratégie de la part de Daesh. Il pourrait également s'agir d'un aveu de faiblesse quant à l'impossibilité de s'assurer de l'allégeance de la population de Mosul.

[Recorded Future] Retour sur les malwares russes

Dans son dernier rapport, Recorded Future revient sur les opérations APT28, Energetic Bear et Uroburos, jusque-là attribuées à la Russie. Si chaque opération semble avoir des cibles différentes, les mécanismes et modes opératoires sont similaires. De ses travaux, Recorded Future déduit que les trois opérations auraient été coordonnées et synchronisées, témoignant ainsi du fait que la Russie est désormais un acteur majeur dans l'élaboration de menaces persistantes et avancées.

[Le Monde] La Russie veut développer une alternative à Wikipédia

La Russie, critiquant la pertinence et la fiabilité de Wikipédia, veut développer une version alternative en utilisant les nombreux ouvrages présents dans les bibliothèques nationales. Cette initiative permettra de présenter de manière plus objective la population et le pays, car la Russie craint une altération des articles publiés sur Wikipédia. Selon des historiens, cet effort est destiné à glorifier l'histoire russe au sein du pays, et à se détacher petit à petit des interprétations étrangères sur son développement.

[SCMagazine] La Russie débloque 500 millions de dollars pour sa cyberarmée

Les effectifs militaires russes vont se doter d'une nouvelle cyberforce. L'Etat devrait allouer près de 500 millions de dollars pour le développement de ses effectifs. Le but étant de renforcer le potentiel militaire du pays en matière de cyberdéfense, en proposant à des spécialistes informatiques de la société civile de s'engager dans l'armée.

[GSM] CyberArk publie un rapport sur les nouvelles tendances en matière d'attaques ciblées avancées

Dans son étude baptisée « Privileged Account Exploits Shift the Front Lines of Security », CyberArk détaille les tendances des attaques ciblées et avancées. Ces attaques s'orienteraient désormais vers l'exploitation malveillante des comptes à privilèges.

[Le Parisien] Iran : un filtrage plus ciblé d'internet opérationnel d'ici 6 mois

Le projet de système de contrôle d'Internet iranien lancé début 2013 devrait être opérationnel dans 6 mois, selon le ministre iranien des Télécommunications. Le tri effectué sera sélectif et ciblera certains contenus diffusés sur les réseaux sociaux, ainsi que des sites considérés comme non-islamique ou anti-régime.

[DYN] Chine : une erreur de routage détourne une part du trafic Interne russe

L'entreprise China Telecom aurait, suite à une erreur de routage, détourné une importante partie du trafic russe. Ce détournement s'inscrit dans le cadre de l'accord de peering signé entre les deux pays. Cette affaire relance la problématique de la sécurité du protocole BGP, encore sujet à de nombreuses erreurs de routage.

[RFI] Les géants du Net réunis en Chine pour un « monde interconnecté »

La chine organisait, le 19 novembre dernier, sa « conférence mondiale de l'Internet » sur le thème « un monde interconnecté partagé et administré par tous ». Au rendez-vous, de nombreux experts du Web dont le géant du e-commerce Alibaba, Baidu, ou encore Facebook et Amazon.

[The Guardian] Le développement des logiciels « spyware » mieux encadré en Europe

De nombreux logiciels intrusifs sont développés en Europe par des sociétés privées. Ceux-ci étant considérés comme potentiellement dangereux dans de mauvaises mains, l'Europe veut limiter l'exportation de ces logiciels. Des licences d'exportations sont à l'étude et les entreprises désirant vendre leurs produits sur les marchés internationaux, devront recevoir une certification avant tout échange. Le gouvernement britannique, premier à proposer cette idée, veut établir un consensus au sein de la Commission Européenne.

[Citizen Lab] L'espionnage des associations de défense des droits de l'Homme est presque constant

Dans son dernier rapport sur les affaires d'espionnage, Citizen Lab lève le voile sur un acteur qui subit de nombreuses attaques informatiques, sans pour autant avoir les moyens de se défendre : les associations de défense des droits de l'Homme. Sur une période de quatre années d'études, dix associations ont été suivis de près et de nombreuses attaques ont été identifiées. .

La cybersécurité, priorité nationale en Equateur

Le 24 novembre 2014, plusieurs ordinateurs privés du gouvernement équatorien, dont celui du Président de la République Rafael Correa, ont été la cible de cyberattaques[1]. Si aucune donnée sensible n'a été volée, ces cyberattaques ont entraîné une paralysie des systèmes informatiques de plusieurs hauts fonctionnaires d'Etat. C'est la deuxième cyberattaque de ce type en l'espace de deux mois. Le 17 octobre 2014, les réseaux informatiques du gouvernement avaient déjà subi une tentative de cyberespionnage, cette fois-ci en provenance de la Colombie[2]. L'augmentation de la cybercriminalité, la crainte d'un futur conflit cybernétique conjuguées à des infrastructures de cybersécurité insuffisantes, ont conduit le gouvernement équatorien à réagir et faire de la cyberdéfense l'une de ses priorités. Conformément au Plan stratégique de recherche, développement et innovation pour les TIC élaboré par le Ministère des Télécommunications (Mintel) en 2014[3], un CERT sera mis en place en 2015. En termes de cyberdéfense militaire, la ministre de la Défense, Maria Fernanda Espinosa, a déclaré en septembre 2014, que l'Equateur allait également créer un commando spécialisé de cyberdéfense.

Une révolution numérique confrontée à une évolution des cybermenaces

En Equateur, l'accès aux TIC s'est considérablement développé pendant la dernière décennie. Le taux de pénétration Internet sur le territoire équatorien a été multiplié par 10 entre 2006 et 2013 pour atteindre 65% au 1er mai 2014[4]. Près de 10 millions d'Equatoriens ont ainsi accès à Internet. Le développement du taux de pénétration Internet est le plus rapide de la région, près de 38,77% par an[5], suivi de la Colombie, 24,19% et de l'Argentine, 17,94%. En juin 2014, le ministère des télécommunications de l'Équateur a signé l'accord ministériel 035-2014, qui stipule que d'ici 2017, 90% du pays sera couvert par les réseaux large bande fixes et mobiles[6]. En termes d'infrastructures, Telconet a entrepris la construction de deux Datacenter à Quito et Guayalquil. En 2012, Telconet a construit le premier Datacenter Tier IV de l'Amérique latine à Guayaquil[7].

Cette révolution technologique, véritable moteur de développement économique et social, est aussi un facteur de multiplication des vulnérabilités. Les années 2013 et 2014 ont marqué un tournant, l'Equateur étant de plus en plus en proie aux cybermenaces.

Essor de la cybercriminalité et du hacktivisme

En 2013, l'Unité de recherches sur les délits cybernétiques a enregistré un nombre exponentiel de plaintes dues à des fraudes électroniques ou informatiques. On constate une augmentation de 58,94% concernant le vol du numéro de cartes bleues, 34,48% pour l'usurpation d'identité ou encore le piratage de données sensibles[8]. Ces délits informatiques sont majoritairement orchestrés par des criminels locaux. De plus, le domaine .ec est le 8ème domaine le plus exploité

[1] http://sputniknews.com/latam/20141123/1015048657.html
[2] http://colombiareports.co/cyber-attacks-govt-originated-colombia-ecuadors-president/
[3] http://www.telecomunicaciones.gob.ec/ecuador-cuenta-con-una-propuesta-de-plan-estrategico-de-investigacion-desarrollo-e-innovacion-de-las-tic/
[4] http://www.nuestraseguridad.gob.ec/es/articulo/ciberseguridad-escenarios-y-recomendaciones
[5] http://www.nuestraseguridad.gob.ec/es/articulo/ciberseguridad-escenarios-y-recomendaciones
[6] https://www.telegeography.com/products/commsupdate/articles/2014/06/06/ministry-signs-pledge-for-90-broadband-coverage-by-2017/
[7] http://www.nearshoreamericas.com/cnt-builds-data-centers-ecuador/
[8] http://www.rebelion.org/docs/189922.pdf

pour le phishing dans le monde, selon Symantec[9]. En septembre 2014, la ministre de la Défense, María Fernanda Espinosa déclarait ainsi que l'Equateur était l'un des 10 pays d'Amérique latine les plus vulnérables aux cybermenaces[10].

L'écosystème hacktiviste est lui aussi très actif, notamment suite à l'affaire Snowden. En 2013, le collectif Ecuador Cyber Army s'illustrait par quelques défacements[11]. Le groupe Anonymous Ibéroamérica[12] a lancé, avec les collectifs Lulzsec et Anonymous, l'opération « Condor Libre » afin de défendre la liberté d'expression. En juillet 2013, le hacker connu sous le nom de Jester a lancé plusieurs cyberattaques par déni de service contre des sites web équatoriens dont le site web du ministère du tourisme équatorien, afin de protester contre la possibilité que l'Equateur accorde l'asile à Edward Snowden. Le hacker patriote a d'ailleurs déclaré qu'il envisageait de diriger des attaques similaires contre n'importe quel pays qui envisagerait d'accorder l'asile à Snowden. L'attaque a cessé après que l'Équateur a annoncé qu'il n'accorderait pas l'asile à Snowden[13].

Un pays en proie au cyberespionnage et au sabotage informatique

En février 2014, les experts de recherche en sécurité de Kaspersky Lab ont découvert une vaste campagne mondiale de cyberespionnage baptisée The Mask. Principales cibles : des institutions gouvernementales, des bureaux diplomatiques et des ambassades, des compagnies pétrolières et gazières, des organismes de recherche et des militants. Le malware multiplateforme – Careto – a infecté les ordinateurs d'une centaine de gouvernements et industriels de plus de 30 pays. Les soupçons portent encore aujourd'hui sur une origine étatique et hispanophone. L'objectif principal des attaquants était de recueillir des données sensibles sur les systèmes infectés[14]. La détection est extrêmement difficile en raison des capacités de furtivité et les fonctionnalités du rootkit intégré. En août, c'est au tour de Kaspersky Lab[15] d'annoncer la découverte d'une nouvelle campagne de cyberespionnage : « El Machete ». Cette campagne cible depuis au moins 4 ans des agences gouvernementales et militaires, ainsi que des acteurs judiciaires. Active principalement en Equateur et au Venezuela, elle touche également la Colombie, le Pérou ou Cuba[16]. Récemment, les cyberattaques se sont largement concentrées sur la fonction présidentielle. En février 2013, le système informatique supportant les élections présidentielles a été victime de près de 1 400 tentatives de sabotage, selon le Mintel[17]. Le 22 novembre, le président Rafael Correa annonçait même que ses ordinateurs personnels avaient été la cible d'une intrusion informatique.

Des initiatives en faveur d'une meilleure prise en compte de la cybersécurité

Le renforcement de l'arsenal législatif et règlementaire

C'est l'Unité d'investigation du délit cybernétique, entité rattachée à la Police nationale, qui identifie et répertorie les délits informatiques, et organise le partage des informations avec les autres organisations. Cette organisation a contribué à la mise en place du logiciel de chiffrement Pretty Good Privacy (PGP), destiné à renforcer la sécurité des communications des hauts fonctionnaires. Parallèlement, la police équatorienne bénéficie de formations régulières afin d'améliorer la lutte contre la cybercriminalité, notamment contre la pornographie infantile[18]. Cette amélioration passe

[9] http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf
[10] http://www.ecuavisa.com/articulo/noticias/actualidad/79426-ecuador-se-blinda-contra-ciberataques
[11] http://www.zone-h.org/archive/notifier=Ecuador%20Cyber%20Army?zh=1
[12] http://www.telegrafo.com.ec/noticias/tecnologia/item/mas-paginas-web-oficiales-hackeadas.html
[13] http://politicalfilm.wordpress.com/2013/07/03/cyber-war-unleashed-on-ecuador/
[14] http://www.kaspersky.com/about/news/virus/2014/Kaspersky-Lab-Uncovers-The-Mask-One-of-the-Most-Advanced-Global-Cyber-espionage-Operations-to-Date-Due-to-the-Complexity-of-the-Toolset-Used-by-the-Attackers
[15] http://www.kaspersky.com/about/news/virus/2014/Kaspersky-Lab-identifies-cyber-espionage-campaign-targeting-Latin-America
[16] http://www.andes.info.ec/en/news/ecuador-one-victims-cyber-espionage-campaign-started-2010.html
[17] http://www.bnamericas.com/news/technology/ecuador-minister-decries-first-world-cyber-attack-in-2013-presidential-elections1
[18] http://www.ecuadortimes.net/2014/08/07/ecuador-seat-cyber-police/

également par le renforcement de l'arsenal législatif et règlementaire. Par exemple, le Secrétariat national de l'administration publique qui dépend du Mintel va bientôt promulguer le Décret 166[19]. Ce décret obligera toutes les organisations administratives à mettre leurs systèmes informatiques en conformité avec les nouvelles normes de sécurité édictées.

Début 2014, le Mintel a élaboré le Plan stratégique de recherche, développement et innovation pour les TIC en Équateur pour la période 2014-2018[20]. En coopération avec l'Institut national de prévention (INP), ce Plan stratégique présente un audit des infrastructures cyber mises en place et définit les grands enjeux des TIC en Equateur[21]. Deux enjeux majeurs ont été retenus : renforcer la législation contre les activités cybercriminelles et sensibiliser la population.

Vers la création du premier CERT équatorien

Par ailleurs, le Plan prévoit la mise en place d'un CERT qui doit permettre à l'Equateur de pouvoir répondre à d'éventuelles cyberattaques[22]. Les principales missions du CERT Ecuador sont[23] :

1. Détecter et identifier les principales menaces cybernétiques et y répondre efficacement. Le CERT contribue à assurer la sécurité et la résilience des systèmes essentiels qui sous-tendent la sécurité nationale, la sécurité publique et la prospérité économique du pays. Le CERT agit comme un centre national de coordination pour la prévention, l'atténuation, la préparation, l'intervention et le rétablissement en matière d'incidents informatiques.

2. Collaborer avec les services de police spécialisés dans la lutte cybernétique et avec d'autres CERT régionaux. Le CERT communique à ses partenaires des renseignements techniques sur les menaces, les vulnérabilités, les risques et les incidents, dans le but d'améliorer la compréhension collective au sujet des incidents et des menaces cybernétiques.

3. Participer à la formation du personnel. Par exemple, proposer des programmes de cyberdéfense dans les universités, ou améliorer la formation des fonctionnaires qui travaillent au sein de l'Unité d'investigations des délits informatiques.

4. Conseils techniques concernant l'intervention et le rétablissement en cas d'attaques ciblées. Le CERT fournit un accompagnement technique, de la reconstruction de SI et de l'analyse forensique des malwares.

La cyberdéfense équatorienne, pilier de la modernisation des Forces armées

En septembre 2014, le gouvernement a décidé d'investir 8 millions de dollars dans la création d'un Commando spécialisé dans la cyberdéfense[24]. L'objectif de ce commando est de lutter efficacement contre les cyberattaques et le cyberespionnage. Cette équipe sera installée au sud de la capitale, près du Fort militaire d'Atahualpa. Le commando de cyberdéfense comptera une trentaine de personnes à l'horizon 2015, pouvant être déployées sur l'ensemble du territoire équatorien. Cette unité est l'une des priorités du programme de modernisation des forces armées équatoriennes (2014-2017), dont l'objectif principal est de renforcer les capacités opérationnelles d'intervention de l'État.

Ces initiatives témoignent d'une véritable prise de conscience du gouvernement équatorien par rapport aux conséquences d'une cyberattaque à grande échelle sur les infrastructures critiques du pays. Ainsi, l'Equateur semble adopter une cyberstratégie nationale qui englobe l'ensemble des aspects civils et militaires.

---

[19] http://www.symantec.com/es/mx/page.jsp?id=cybersecurity-trends

[20] http://www.telecomunicaciones.gob.ec/ecuador-cuenta-con-una-propuesta-de-plan-estrategico-de-investigacion-desarrollo-e-innovacion-de-las-tic/

[21] http://www.industrias.ec/archivos/CIG/file/CARTELERA/MINTEL-TIC%20para%20el%20Desarrollo.pdf

[22] https://sites.google.com/site/certecuadorcc/home

[23] https://sites.google.com/site/certecuadorcc/home

[24] http://www.ecuavisa.com/articulo/noticias/actualidad/79426-ecuador-se-blinda-contra-ciberataques

Conclusion

« *Le plus grand danger pour l'Equateur serait le déclenchement d'une cyberguerre, car le pays n'est pas préparé*[25] ». La crainte de Rafael Correa face à un éventuel cyberconflit a conduit le gouvernement à investir dans le renforcement de ses capacités cyber. La mise en place d'un CERT et du Commando de cyberdéfense sont les premières étapes de cette restructuration et doivent conduire à moyen terme sur la formulation d'une cyberstratégie nationale. D'autre part, pour mener à bien ses nouvelles ambitions, l'Equateur doit nouer des partenariats technologiques à l'échelle régionale et internationale. L'Equateur a ainsi tout intérêt à ratifier la convention de Budapest, qui promeut la coopération à l'échelle internationale.

Lors de la 2ème Rencontre internationale sur la Sécurité intégrale qui avait lieu cette année en Equateur du 19 au 21 novembre, les représentants des pays participants (Chili, Colombie, Equateur, Uruguay, Mexique, Royaume-Uni, Chine, Etats-Unis) ont discuté de la nécessité de formuler une cyberstratégie régionale en Amérique latine face à l'augmentation des menaces[26]. La création d'un réseau d'unités de police pour l'échange d'informations en matière de cybercriminalité entre les pays de l'UNASUR est l'un des projets envisagés au niveau régional. Cette coopération régionale a déjà été couronnée de succès. En février 2012, l'Opération Unmask est lancée par la Colombie, l'Argentine, le Chili et l'Espagne contre la campagne de cyberespionnage The Mask[27]. Leurs efforts ont permis l'arrestation de 31 personnes. Un an et demi plus tard, la plate-forme internet Historia est créée pour partager les informations sur les sites pédopornographiques entre les pays membres que sont l'Argentine, le Brésil, le Chili, la Colombie, le Costa Rica, l'Équateur, l'Espagne, l'Uruguay[28].

[25] http://www.eltiempo.com/archivo/documento/CMS-14698657
[26] http://www.prensa-latina.cu/index.php?option=com_content&task=view&id=3296801&Itemid=1
[27] http://www.coha.org/cyber-security-and-hacktivism-in-latin-america-past-and-future/
[28] http://www.coha.org/cyber-security-and-hacktivism-in-latin-america-past-and-future/

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

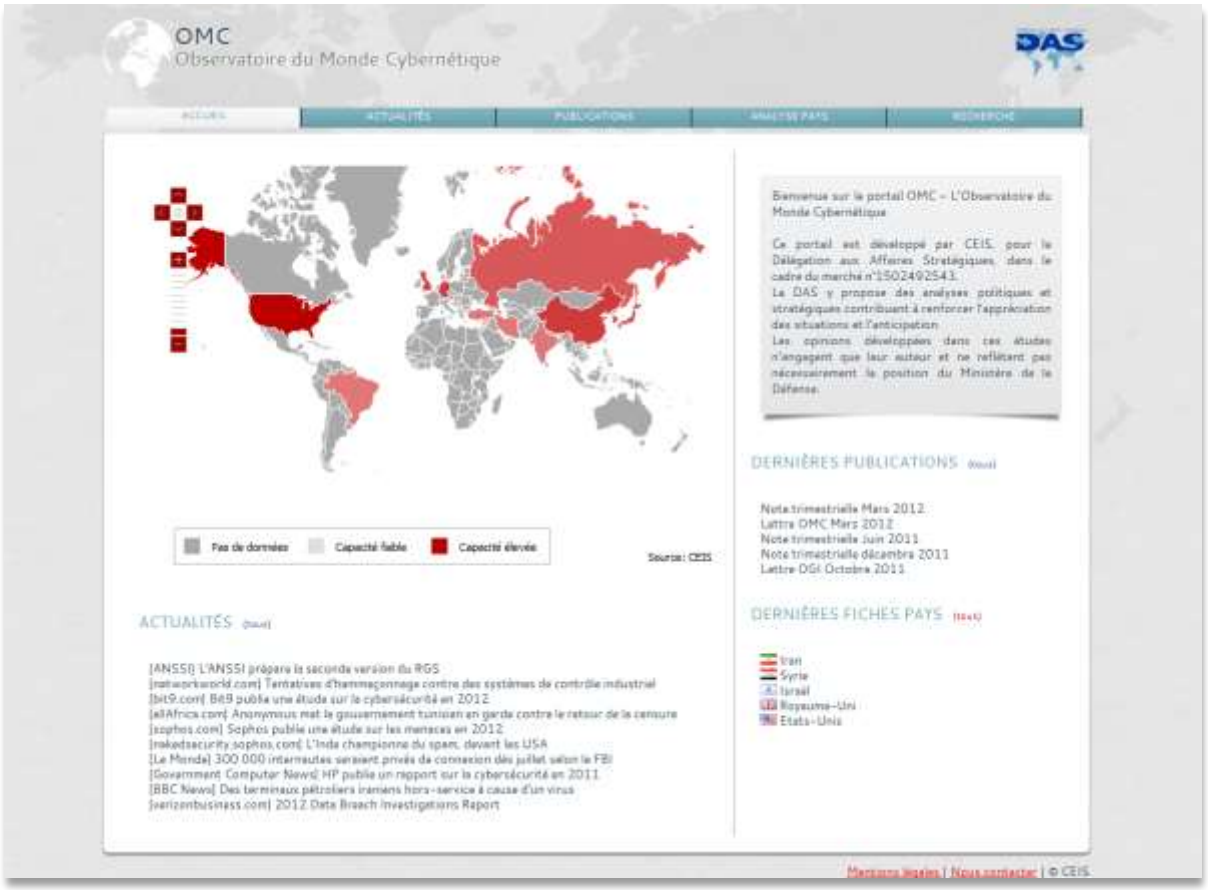

Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

IT Tour 2014	Toulouse	2 décembre
Botconf	Nancy	3 – 5 décembre
Mobile Network Security Strategies	Westin Times Sqaure, NYC, Etats-Unis	3 décembre
Penser la sécurité à l'ère de la mobilité - CDSE	Paris	4 décembre
3èmes Universités de la sécurité	Lyon	4 – 5 décembre
3rd Annual Cyber Security and Digital Forensics Exchange	Amelia Island, Floride, Etats-Unis	7 – 9 décembre
La sécurité privée à l'horizon 2020	Paris	8 décembre
Congrès annuel du CESIN	Reims	10 – 11 décembre
Entre cyberguerre et sécurité numérique : quel quotidien pour le RSSI en 2015 ?	Reims	10 – 11 décembre
Congrès objet connectés	Paris	10 décembre
SSR 2014: Security Standardisation Research	University of London, Royaume-Uni	16 décembre
Conférence WebRTC	Paris	16 – 18 décembre
31c3 Chaos Communication Congress	Hambourg	27 – 30 décembre

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