Lettre n°46 - janvier 2016 - disponible sur omc.ceis.eu

«Don't assume a crack is too small to be noticed, or too small to be exploited,(…). If you do a penetration test of your network and 97 things pass the test but three esoteric things fail, don't think they don't matter. Those are the ones the NSA, and other nation-state attackers will seize on(…) We need that first crack, that first seam. And we're going to look and look and look for that esoteric kind of edge case to break open and crack in» ***Rob Joyce, responsable du Tailored Access Operations de la NSA, conférence Enigma 2016***

Table des matières

LA SECURITE DES VEHICULES CONNECTES

L'explosion des IoT

Les objets connectés sont de plus en plus omniprésents dans notre quotidien : webcam, réfrigérateur, bracelet serrure, thermostat, capteur, etc. On les retrouve dans tous les domaines : domotique, santé, jardinage... Selon Cisco, le nombre d'objets connectés passera de 15 milliards aujourd'hui à 50 milliards en 2020. Intel est encore plus optimiste, affirmant que plus de 200 milliards d'appareils seront connectés d'ici là.[1] L'internet des objets (IoT) se développe dans tous les secteurs : l'espace professionnel avec l'usine du futur par exemple, l'espace public avec les smart-cities ou encore l'espace privé avec les maisons connectées. La donnée y est l'élément-clé : collectée, elle génère de la valeur informationnelle qui s'enrichit continuellement en la croisant avec d'autres données, à l'aide d'algorithmes et des technologies du big-data.

Malheureusement, la sécurité de ces objets a été très peu prise en compte pour des raisons d'optimisation de leur consommation : utiliser les algorithmes de chiffrement, par exemple, consomme beaucoup plus d'un point de vue énergétique pour l'objet. Ainsi, comme expliqué lors de l'atelier de Digital Security au Forum International de la Cybersécurité 2016, on peut observer de nombreuses vulnérabilités sur ces équipements, sur les serrures connectées[2] par exemple : pas de chiffrement, algorithmes faibles, absence de mises à jour de l'objet connecté, etc.

Au sein de l'Internet des Objets, un des marchés les plus prometteurs est la voiture connectée : selon une étude de Marketsandmarkets[3], le marché atteindrait les 100 milliards de dollars d'ici 2018.

L'automobile de demain sera un objet connecté.

Les véhicules connectés sont un sujet de fort intérêt pour les constructeurs. Déjà en janvier 2015, de nombreuses marques avaient présenté au CES (Consumer Electronics Show) leurs prototypes de véhicules connectés : Audi (A7 Piloted Driving) ou encore Renault (Next Two). Mais un nouveau type de concurrents est apparu face à ces derniers : les entreprises high-tech, comme Akka Technologies avec son Link'n'Go ou le tandem Valeo-Sagem avec son prototype Drive4U, sans oublier de mentionner Google avec sa Google Car. Sur un marché où le nombre de voitures connectés pourrait atteindre 152 millions d'ici à 2020, selon le cabinet IHS Automotive[4], les investissements sont de plus en plus nombreux : au CES 2016, près d'un quart de la surface totale occupée par le salon était consacré à ce sujet. Les constructeurs, devenant des maillons secondaires, cherchent à développer – ou à s'attacher – une expertise dans le logiciel et les services. Ainsi, Nissan s'appuie sur la plate-forme cloud Microsoft Azure, Audi exploite les semi-conducteurs de Qualcomm, Ford s'allie à Amazon autour de l'assistant personnel Echo, et BMW s'associe à AT&T sur la partie connectivité.

L'informatique se fait ainsi une place de plus en plus importante au sein du véhicule : selon le spécialiste Charles Miller[5], on peut y retrouver 20 à 30 ECU (Electronic Control Unit) par voiture. Les ECU sont des

[1] http://www.fool.com/investing/general/2016/01/18/internet-of-things-in-2016-6-stats-everyone-should.aspx
[2] http://www.linformaticien.com/actualites/id/39305/serrures-connectees-vous-pensiez-vraiment-etre-en-securite.aspx
[3] http://www.usine-digitale.fr/article/bousculade-sur-le-marche-de-la-voiture-connectee.N231344
[4] https://www.ihs.com/industry/automotive.html
[5] https://www.youtube.com/watch?v=n70hIu9lcYo

composants électroniques qui sont assimilés à des petits PC exécutant chacun une fonction bien spécifique au sein du véhicule. Chaque ECU d'une voiture est relié à un autre ECU à travers un CAN (Controller Area Network). Le CAN est un simple BUS qui permet d'interconnecter chaque ECU et de les faire communiquer. Il envoie un message en *broadcast* : ainsi, tous les ECU reçoivent les messages injectés au CAN. Comme montré ci-dessous, tous les ECU sont interconnectés à un ou plusieurs CAN, et peuvent être donc facilement accessibles.

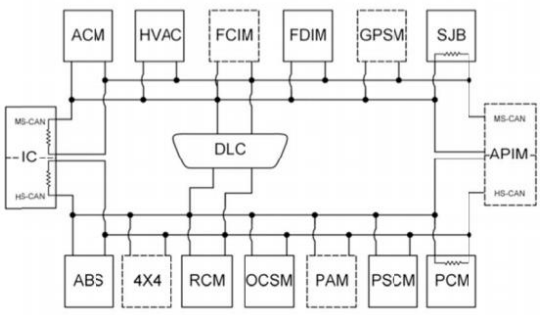


Schéma CAN d'une Toyota Escape de 2010 – Source : http://illmatics.com/car_hacking.pdf

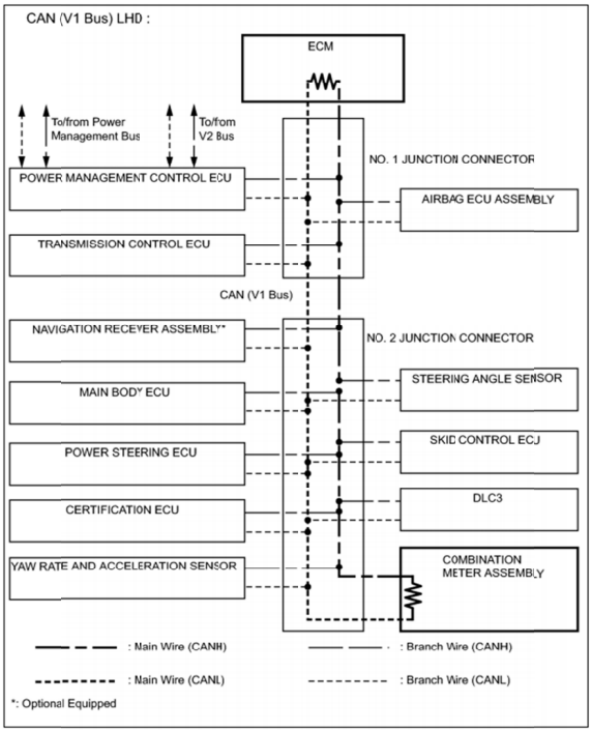


Schéma CAN d'une Toyota Prius de 2010 – Source : http://illmatics.com/car_hacking.pdf

En juillet 2015, Charlie Miller and Chris Valasek ont démontré à Wired[6] qu'il était ainsi possible de conduire à distance une Jeep Cherokee, en contrôlant ces différents ECU. Tout d'abord, ils ont découvert une faille permettant la prise de contrôle de la console de bord du véhicule via la radio (GSM, Wifi et Bluetooth). L'architecture de la Cherokee interconnecte la console de bord aux 2 réseaux CAN (voir ci-dessous) : CAN-C et le CAN-IIHS. Cette prise de contrôle a permis d'accéder facilement au CAN-C regroupant les fonctions classiques de la console de bord, et d'émettre des ordres vers les fonctions de confort (portes, climatisation, sièges chauffants, etc.). Ensuite, ils ont injecté, lors du processus de mise à

[6] http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

jour, un logiciel « maison » dans le contrôleur dédié aux réseaux CAN-IIHS et ont injecté des messages aux fonctions ECU du véhicule, tel que le régulateur de vitesse, le volant, la boite de vitesse, etc.

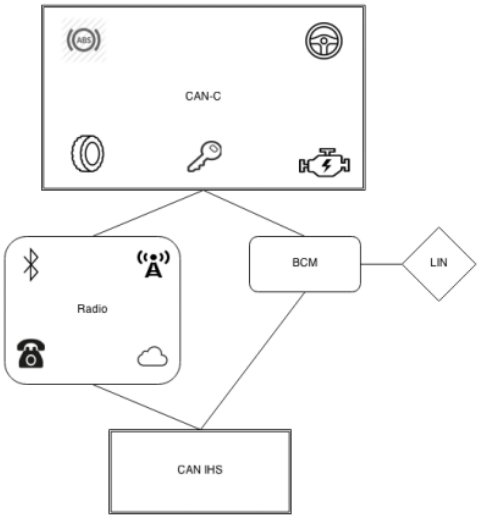


Diagramme de l'architecture de la Jeep Cherokee – Source : http://illmatics.com/Remote%20Car%20Hacking.pdf

Cette interconnexion des ECU au sein du CAN a ainsi permis aux deux chercheurs de piloter à distance la voiture. Suite à cette découverte très médiatisée, 1,4 million de Jeep Cherokee ont dû être mises à jour avec une nouvelle version du logiciel.

L'informatisation grandissante de l'automobile pose donc de sérieux problèmes en augmentant les vecteurs d'attaques informatiques. Historiquement, les voitures ont été conçues pour fonctionner en système fermé, sans ou avec très peu d'interactions avec le monde extérieur. Mais les connexions avec le monde extérieur se multiplient : pour qu'un véhicule puisse évoluer en toute autonomie sur la route ou dans le trafic, il lui faudra aussi être connecté à des bases de données (trafic, cartographie, etc.) afin que ses capteurs puissent anticiper les obstacles et les éviter. De plus, en avril 2018, un dispositif européen appelé eCall[7] sera obligatoirement installé dans toutes les voitures neuves : c'est un appel d'urgence à déclenchement automatique (en cas d'accident, il prévient les secours en leur indiquant le lieu où celui-ci s'est produit).

Pour essayer d'étudier et de contenir ces attaques, les autorités ont commencé à agir : en France, la Gendarmerie nationale a créé en juillet 2015 un « Observatoire des systèmes de transports intelligents de la Gendarmerie nationale ». Il a un double objectif : réfléchir aux vulnérabilités qui existent dans tous ces systèmes et profiter de ces nouvelles technologies pour développer de nouveaux modes d'action. Selon l'Observatoire, il existe deux points névralgiques en termes de sécurité au sein d'un véhicule connecté[8]. D'une part le Datacenter, où le constructeur automobile héberge le système informatique qui fait tourner ses applications, et qui exploite les données des clients et du véhicule pour faire des mises à jour de ses services. D'autre part, la prise de diagnostic à bord du véhicule qu'utilisent les garagistes en y branchant leur valise de maintenance afin de vérifier les systèmes électroniques.

[7] https://ec.europa.eu/digital-agenda/en/ecall-time-saved-lives-saved
[8] https://congresitsbordeaux2015.wordpress.com/tag/observatoire-central-des-systemes-de-transports-intelligents/

Les différents *Proof of Concept*[9] concernant les véhicules connectés ont ainsi démontré la faisabilité de ce type d'attaques au sein du monde civil. Mais le monde militaire est aussi concerné.

Le risque n'est pas uniquement civil : il est aussi militaire

Depuis quelques années, le monde militaire témoigne un réel intérêt pour les véhicules connectés. Aux Etats-Unis, une des missions du TARDEC (*Tank Automotive Research Development Center*) est le développement de véhicules autonomes pour l'armée.

En mai 2014[10], le TARDEC a testé un convoi de sept véhicules autonomes évoluant à plus de 60 km/h[11]. L'objectif sur 30 ans de ce projet, nommé AMAS (*Autonomous Mobility Appliqué System*), est d'introduire l'usage de véhicules autonomes pour sa logistique et peut-être même des scénarios de combat, comme les convois. La technologie utilisée pour rendre autonomes ces véhicules provient des constructeurs automobiles et de Google : les failles dans le monde civil risquent donc d'être applicables au sein du monde militaire.

La technologie est déjà en cours de déploiement en conditions réelles sur certaines bases militaires, comme celle de Fort Bragg (Caroline du Nord) ainsi que l'Académie Militaire et l'université de Stanford. C'est le programme Aribo[12] (*Applied Robotics for Installations and Base Operations*), qui consiste à utiliser des véhicules autonomes pour transporter des soldats blessés ou acheminer le personnel depuis les parkings de stationnement jusqu'aux bâtiments, ainsi que convoyer de la nourriture ou des munitions.

De plus, certains véhicules, dont les tout-terrain, sont achetés par les armées à des constructeurs civils, tel que Ford, Renault, etc. Ainsi, en mai 2015, la France a commandé 1000 Ford Ranger qui proposent de série un ordinateur de bord[13]. De nouveaux vecteurs d'attaques feront ainsi leur apparition, et il sera nécessaire d'analyser la sécurité de ces composants électroniques.

Les voitures ne sont pas les seuls véhicules connectés possibles : les véhicules de combat, tel que le char ADAMS et les hélicoptères autonomes, sont les objectifs à long terme pour le TARDEC[14]. Il est important d'insister sur le fait que ces véhicules autonomes armés pourront causer des dégâts humains importants s'ils se font pirater.

[9] http://www.japantimes.co.jp/news/2015/12/15/national/experiment-shows-japanese-cars-can-hacked-smartphones-connected-internet/
[10] http://www.futura-sciences.com/magazines/high-tech/infos/actu/d/technologie-armee-us-teste-convoi-vehicules-autonomes-54384/
[11] https://www.youtube.com/watch?v=bnb4esO0V34
[12] https://www.us-ignite.org/resources/BoeBRAswZPdBuEe5RxzPdJ/
[13] http://www.auto-selection.com/fiche-technique/ford/ranger/2011/3-2-tdci-200-4x4-wildtrak-a-141614.php
[14] http://www.army.mil/article/129040/Autonomous_vehicles_to_exploit_capabilities_of_machines__Soldiers/

LES MOYENS FOURNIS PAR LE GOUVERNEMENT AMERICAIN POUR PROTEGER SES ENTREPRISES

Ces dernières années, le gouvernement américain a clairement montré l'importance de renforcer la cybersécurité à travers une stratégie claire et des engagements forts.

En février 2013, Barack Obama a signé un décret présidentiel sur la cybersécurité, quelques jours après une série d'attaques informatiques contre des entreprises et des médias américains (Sony Pictures), et inscrit le pays dans un vaste programme de protection informatique. Ce décret a été conçu pour poser les fondations d'une réelle collaboration public-privé.

Plusieurs objectifs-clés sont alors annoncés et ils seront le fil conducteur de la stratégie de l'administration Obama en termes de cybersécurité :

- Mettre en place un cadre (méthodologies, normes, etc.) pour réduire le risque sur les infrastructures critiques ;
- Partager les informations sur les cybermenaces ;
- Renforcer la cyberdéfense ;
- Donner des gages aux internautes sur le respect de la vie privée.

Cet article dresse un état des lieux des différents moyens fournis par le gouvernement américain pour protéger ses entreprises nationales.

On observe tout d'abord que le gouvernement s'adresse en priorité aux infrastructures critiques, du fait de leur criticité pour la sécurité intérieure et l'économie du pays.

Développement d'un *framework* pour les entreprises

Dans son décret présidentiel de février 2013, l'administration Obama a annoncé la création d'un *framework* pour la sécurité des infrastructures critiques. Ce dernier devait comprendre un ensemble de normes, de méthodes, de procédures et de processus qui harmonise la méthodologie, le « business » et les approches technologiques dans l'objectif de prévenir les risques informatiques. Ce *framework* devait intégrer, dans la mesure du possible, les différentes normes obligatoires et les bonnes pratiques de l'industrie.

Le NIST (*National Institute of Standards and Technology*) a publié son guide « *Framework for Improving Critical Infrastructure Cybersecurity* » en février 2014[15]. Ce dernier, créé par le gouvernement en collaboration avec le secteur privé, fournit une méthodologie et des outils pour :

- Décrire l'état actuel de la cybersécurité au sein d'un système d'information ;
- Décrire l'état cible de cybersécurité que l'on désire atteindre ;
- Identifier et prioriser les possibilités d'amélioration dans le cadre d'un processus continu et reproductible ;

[15] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

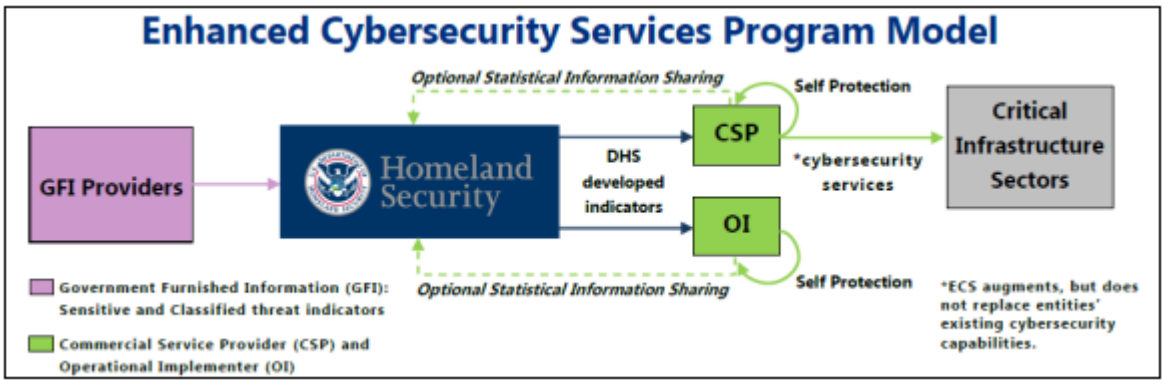
- Evaluer les progrès vers l'état cible ;
- Communiquer entre les parties prenantes internes et externes sur les risques en matière de cybersécurité.

Function	Category	Subcategory	Informative References
			8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	• **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	• **COBIT 5** DSS04.03 • **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2 • **NIST SP 800-53 Rev. 4** CP-2, IR-8
		PR.IP-10: Response and recovery plans are tested	• **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.17.1.3 • **NIST SP 800-53 Rev.4** CP-4, IR-3, PM-14
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	• **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 • **ISO/IEC 27001:2013** A.7.1.1, A.7.3.1, A.8.1.4 • **NIST SP 800-53 Rev. 4** PS Family
		PR.IP-12: A vulnerability management plan is developed and implemented	• **ISO/IEC 27001:2013** A.12.6.1, A.18.2.2 • **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4.3.3.3.7 • **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5 • **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	• **COBIT 5** DSS05.04 • **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 • **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1

Extrait du framework pour l'amélioration de la cybersécurité des infrastructures critiques

Il est important de noter que le framework publié par le NIST ne s'adresse pas uniquement aux opérateurs d'infrastructures critiques, mais qu'il peut aussi être appliqué à toute entreprise du secteur privé.

Partage d'information entre le monde public et le monde privé



Processus du modèle américain de partage d'information en 2014 - Source : http://www.dhs.gov/sites/default/files/publications/ECS-Fact-Sheet.pdf

En février 2015, la Maison Blanche a annoncé la création d'un Centre d'intégration du renseignement sur les cyber-menaces (*Cyber Threat Intelligence Integration Center* - CTIIC). Cette agence est un centre d'analyse des données recueillies auprès des agences gouvernementales et des entreprises. Elle va ainsi centraliser les informations avant de les diffuser au sein des 23 agences gouvernementales.

De plus, le Congrès a voté en 2015 le CISA *(Cybersecurity Information Sharing Act*)[16], qui incite les entreprises à échanger des données sur les cybermenaces entre elles et avec le gouvernement. Cette loi vise à améliorer la cybersécurité aux États-Unis à travers le partage renforcé d'informations, entre entreprises privées et vers les agences fédérales, et à écarter le risque de poursuites dans le cadre de ces échanges. Néanmoins, des experts en sécurité, des géants du Net, des professeurs de droit, mais aussi des associations de consommateurs ont exprimé leur opposition à cette loi[17], au motif qu'elle permettrait aux entreprises de récolter beaucoup de données sur les utilisateurs au nom de la cybersécurité, ces dernières étant partagées avec le Département de la Sécurité intérieure. Précisons que le projet de loi a été validé et signé par le président Barack Obama le 18 décembre 2015[18].

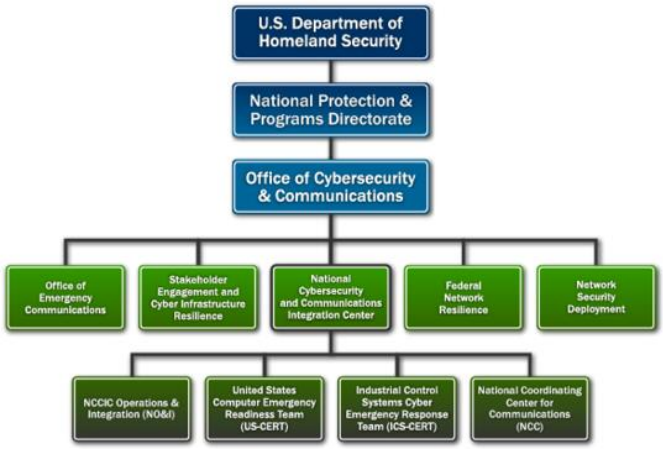
Etablir des partenariats pour sécuriser la technologie

Dans l'objectif d'aider les entreprises à se protéger, les Etats-Unis ont également mis en place d'autres actions, plus techniques.

Le centre d'alerte aux attaques informatiques du Département de la Sécurité intérieure (DHS) des Etats-Unis (US-CERT) a été créé en 2003 pour protéger l'infrastructure Internet du pays en coordonnant la défense et les réactions aux cyber-attaques[19].

En continu, il est le bras opérationnel du NCCIC (*National Cybersecurity and Communications Integration Center*) qui analyse, trie, et répond aux incidents, et fournit une assistance technique aux exploitants des systèmes d'information. Il diffuse des notifications en temps réel concernant les menaces de sécurité actuelles et potentielles, les *exploits* et les vulnérabilités au public via son système national d'alerte, le NCAS (*National Cyber Awareness System*).

L'US-CERT travaille en coopération directe avec l'ICS-CERT, traitant de la sécurité liée aux systèmes de contrôle industriel. Les deux entités opèrent ensemble au sein du NCCIC, afin de fournir une source unique de soutien aux responsables des infrastructures critiques[20].



Organigramme du NCCIC - Source http://www.dhs.gov/national-cybersecurity-and-communications-integration-center

[16] https://www.congress.gov/bill/113th-congress/senate-bill/2588
[17] http://www.nytimes.com/2015/10/28/us/politics/senate-approves-cybersecurity-bill-despite-flaws.html
[18] http://www.engadget.com/2015/12/18/house-senate-pass-budget-with-cisa/
[19] https://www.us-cert.gov/
[20] https://ics-cert.us-cert.gov/

Le DHS élabore un système pour le partage automatique des indicateurs de risques informatiques avec le secteur privé et le gouvernement[21]. L'agence américaine utilise déjà ce système pour envoyer des indicateurs, et a commencé en automne 2015 à en recevoir de l'extérieur. Les entreprises intéressées peuvent donc travailler avec le NCCIC pour préparer leurs réseaux à l'échange automatisé des indicateurs de menaces informatiques.

Ainsi, le rôle du NCCIC est de partager les informations entre les partenaires du secteur public et privé pour les sensibiliser aux vulnérabilités, aux incidents et aux mesures d'atténuation. Les utilisateurs de systèmes d'informations et de systèmes de contrôle industriel peuvent aussi souscrire des services d'information, des flux RSS et d'autres services informationnels gratuits.

D'autres programmes ont été lancés par le gouvernement pour aider les sociétés privées américaines de façon plus concrète. Le journaliste Brian Krebs a révélé en décembre 2015 l'existence du programme NCATS (*National Cybersecurity Assessment and Technical Services*)[22], à travers lequel le DHS offre des tests d'intrusion aux entreprises privées. NCATS a pour objectif de tester gratuitement les défenses des sociétés américaines, à commencer par les banques et les acteurs du secteur de l'énergie, secteurs considérés comme étant les plus vulnérables pour le pays. Ce programme complet de tests d'intrusion se scinde en 2 volets :

- une évaluation des risques et vulnérabilités. Un audit sur les systèmes d'exploitation, les bases de données et applications Web est réalisé afin d'y détecter des vulnérabilités connues et de tester leur exploitation, de l'ingénierie sociale à destination des employés de la société auditée et du spearphishing ;

- une appréciation au fil de l'eau de la « cyber-hygiène » des entreprises. Une évaluation récurrente des systèmes accessibles par Internet est effectuée, afin de découvrir et corriger rapidement les vulnérabilités.

Pour le moment, les mesures proposées par le gouvernement américain aux entreprises du secteur privé américain se destinent principalement à des opérateurs d'infrastructures critiques, dont les activités sont essentielles pour la sécurité intérieure et économique des Etats-Unis. Une attaque sur ce type d'acteurs pourrait avoir des fortes conséquences pour le pays : pannes géantes d'électricité, chute de la bourse, etc. Il est important de noter qu'il est difficile de s'adresser directement à toutes les sociétés américaines, du fait de leur nombre important et de leur nature très hétérogène. Ainsi, comme l'avait précisé Guillaume Poupard[23] en évoquant la LPM et les opérateurs d'importance vitale (OIV), l'objectif est ici de créer une réaction en chaîne : ces normes et mesures seront acceptées, « digérées » par les opérateurs d'infrastructures critiques, puis peu à peu feront tâche d'huile, et déborderont à terme sur tous les autres secteurs.

[21] https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ais-october2015.pdf
[22] http://krebsonsecurity.com/2015/12/dhs-giving-firms-free-penetration-tests/
[23] http://www.cnis-mag.com/assises-de-la-securite-2014-anssi-nouvelle-vague-proteger-du-cac-au-particulier.html

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** 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 **DGRIS** a confié à **CEIS** la réalisation de 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
Direction Générale des Relations Internationales et de la Stratégie
14 rue Saint-Dominique - 75700 – Paris SP 07

CEIS
280 Boulevard Saint-Germain - 75007 - Paris
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com