Cyberattaques des présidentielles. Qui serait responsable ?

	Cyberattaques des présidentielles. Qui serait responsables ?

Les cyber-attaques que la Russie est soupçonnée de mener en France dans le cadre de la campagne présidentielle sont « une forme d'ingérence inacceptable », a estimé dimanche le ministre français des Affaires étrangères Jean-Marc Ayrault.

» Les cyberattaques russes, grande menace pour les États-Unis et l'Europe
Dans une interview au *Journal du Dimanche*, le chef de la diplomatie française a déclaré : « Il suffit de regarder pour quels candidats, à savoir Marine Le Pen ou François Fillon, la Russie exprime des préférences, dans la campagne électorale française, alors qu'Emmanuel Macron, qui développe un discours très européen, subit des cyberattaques. Cette forme d'ingérence dans la vie démocratique française est inacceptable et je la dénonce ».
« La Russie est la première à rappeler que la non-ingérence dans les affaires intérieures est un principe cardinal de la vie internationale. Et je la comprends. Et bien la France n'acceptera pas, les Français n'accepteront pas qu'on leur dicte leurs choix », a ajouté le ministre.

Quels éléments a-t-on pour de telles affirmations ?
Denis JACOPINI : Aujourd'hui la Russie, hier la Chine et demain qui ? Quels sont les éléments permettant d'affirmer de tels propos ?
L'adresse IP ?
Si c'est l'adresse IP qui est prise en compte, n'est-on nous pas en train de mélanger l'adresse IP ayant accédé aux systèmes informatiques et celle du commanditaire de l'attaque ?
Signatures et codages de caractères
Si ce sont les signatures présentes dans les codes ou les codages de caractères qui sont pris en compte, ne risque t-on pas de reproduire l'attribution hâtive de l'attaque de la chaîne TV5 monde à l'Etat islamique
alors même que très vite après l'attaque, de nombreux experts avaient mis en doute la crédibilité de la revendication.
A mon avis
En raison du refus de certains pays pour coopérer en matière de lutte contre la cybercriminalité, il devient très compliqué de remonter jusqu'aux ordinateurs utilisés pour mener de telles attaques, pire encore pour remonter jusqu'aux commanditaires des attaques informatiques.
Les infos circulant encore ce matin font référence une fois de plus à des accusations qui sembleraient bien être sans preuve…
Malgré l'absence de preuve, Ayrault dénonce une «ingérence» de la Russie dans la présidentielle
Je serais bien intéressé
En tant qu'Expert judiciaire spécialisé en cybercriminalité, je serais bien intéressé pour expertiser les éléments concernés par cette affaire.
A bon entendeur…

Qu'en pensez-vous ? Merci de me laisser votre avis ou commentaire

---

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Paris dénonce à nouveau les cyberattaques de Moscou*

Le fonctionnement d'Internet ne tient qu'à (presque) un fil

L'imaginaire populaire associe souvent Internet aux satellites, mais 99,8 % du trafic intercontinental passe par les 366 câbles sous-marins répartis sur la planète. « Grâce à la fibre optique, les capacités de ces câbles sont des millions de fois supérieures à ce que nous savons faire avec les satellites ».
Rien n'est plus facile que de couper Internet : il suffit de sectionner des câbles. Ils sont simplement enterrés, voire posés sur le fond des océans.

La câbles sous marins ont pris une importance prépondérante pour l'acheminement des connexions internet. Se sont des ressources de plus en plus essentielles et toutes perturbations provoqueraient de très importantes conséquences.
Selon le New York Times les Russes joueraient actuellement avec les nerfs des autorités américaines en laissant des navires très proches de ces câbles sous-marins et n'hésitant pas à frôler ces derniers… Or, il faut savoir que non seulement ces câbles sont très difficile à protégés du fait de leur longueur de plusieurs milliers de kilomètres mais aussi bizarre que cela puisse paraitre, aucune loi maritime n'interdit de s'en approcher, la navigation était libre dans les eaux internationales.
D'après le même journal, la coupure d'un de ces câbles rendrait les liaisons intercontinentales quasiment impossibles dans les fait tant les ressources sont très utilisées avec des possibilité de re-routage très limité dans les faits.
Ultra-rapides puisqu'ils évitent la perte de temps induite par la durée nécessaire pour effectuer une transmission par satellite mais pourtant vulnérables, ces câbles se retrouvent parfois à 1 ou 3 mètres sous le fond à proximité des côtés et au large, touchent le fond des océans. Pas suffisant hélas aujourd'hui pour se mettre à l'abri des menaces humaines et naturelles : Requins, tremblements de terre, bateaux et pêcheurs véreux coupant parfois des kilomètres de câbles pour les revendre comme en 2007 au Vietnam.
En 2015, c'est une ancre qui fût à l'origine d'une section de câble privant presque toute l'Algérie d'Internet pendant deux semaines. Tout comme en Égypte en 2008 (perte immédiate de 70% de sa capacité de connexion à internet).

Actuellement, 99,8% du trafic internet intercontinental transite via 366 câbles sous-marins soit plus d'un million de kilomètres de câbles à fibre optique parsemant le fond des océans. Une fois en surface, ils sont rattachés à des stations d 'atterrissement. Ces dernières sont d'ailleurs elles aussi assujetties aux menaces. « En cas de conflit militaire, si plusieurs câbles sont sabotés,nous risquons rapidement une saturation de notre accès à Internet» s'inquiète Jean-Luc Vuillemin.
Heureusement, des systèmes de secours existent comme le principe de redondance. 01net l'a vulgarisé parfaitement dans ses lignes il y a quelques années : « Les câbles transatlantiques rejoignent eux la Bretagne et la Normandie. Pour garantir les transmissions sous-marines dans les deux sens, plusieurs sécurités sont prévues. Le câble lui-même comporte deux paires de fibres optiques au lieu d'une. Le doublage suffit pour résoudre les problèmes électroniques, comme la panne d'un multiplexeur ou d'un routeur, la plus courante. Chaque opérateur crée ensuite des redondances du réseau en posant plusieurs câbles distants sur chaque liaison desservie. Celle entre la France et les Etats-Unis se répartit entre sept câbles, directs ou transitant par le Royaume-Uni. »
Enfin, certains ont trouvé une alternative au sabotage physique des câbles, les services de renseignements de certains pays avec leurs mouchards placées eux-aussi au fond de l'eau.

Facebook et Microsoft main dans la main
En mai 2016, Facebook et Microsoft ont annoncé la construction en duo d'un câble sous-marin à fibres optiques, qui traversera l'océan Atlantique pour relier Virginia Beach aux USA jusqu'à Bilbao en Espagne.

Le général Keith B. Alexander, chef du Cyber Command veut un deuxième Internet aux Etats-Unis
Pour certains, la cyberguerre est un sujet de scénario de films de science fiction ; pour d'autres, c'est la réalité de la guerre contemporaine.
Dans un entretien avec plusieurs journalistes, dont rend compte cette semaine le New York Times, le général Alexander propose la création d'un réseau Internet distinct de celui qui existe aujourd'hui, afin de sécuriser le réseau électrique américain, considéré comme le maillon faible de la sécurité des Etats-Unis.
Cette proposition d'une ampleur considérable, financièrement et techniquement, est lancée publiquement par le général en anticipation d'une remise à plat de tous les enjeux stratégiques liés à Internet par la Maison Blanche d'ici à janvier. Elle fait partie d'un exercice classique aux Etats-Unis de lobby public en faveur d'arbitrages budgétaires par chaque branche de l'appareil militaire, mais pas seulement.

Des « bombes logiques » dans le réseau électrique
Le réseau électrique américain actuel utilise les réseaux Internet et se révèle donc particulièrement vulnérable. C'est la thèse développée au début de l'année par Richard A. Clarke, un ancien responsable de la Sécurité de l'administration Clinton, dans un livre coécrit avec Robert K. Knake, intitulé « Cyber War : The Next Threat to National Security and What to do About It » (« Cyber guerre : la prochaine menace à la sécurité nationale et ce qu'il faut faire »).
Clarke affirme que les services américains ont découvert dans le réseau électrique américain des « bombes logiques » chinoises. Une « bombe logique », c'est comme un virus informatique, dormant, qui peut se déclencher à distance et des années plus tard si nécessaire. Ces « bombes » auraient pu être introduites par une faille dans le réseau internet utilisé par les producteurs et distributeurs d'électricité.

Dans son livre, Richard A. Clarke utilise cette découverte pour plaider en faveur d'un réseau internet séparé pour les installations vitales des Etats-Unis (comme le montre le schéma ci-dessus).
En effet, selon lui, la vulnérabilité du Net américain peut potentiellement mettre les Etats-Unis à genoux en peu de temps en cas de cyber-attaque, privant le pays d'électricité, de transports, de services d'urgence, et affaiblissant même sa capacité de défense.
L'ancien conseiller de Bill Clinton se livre même à un exercice de simulation de cyberguerre avec la Chine, avec des étudiants, basé sur un scénario étrangement similaire à un sujet de tension entre Washington et Pékin il y a quelques mois, peu après la sortie du livre.
Il imagine ainsi une crise entre la Chine et le Vietnam sur la souveraineté d'îles riches en hydrocarbures dans la mer de Chine, et un engagement de Washington au côté du Vietnam. Ça ne vous rappelle rien ? C'est ce qui s'est produit l'été dernier, sur le plan diplomatique uniquement…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : « Qui a le savoir, a le pouvoir »: Les câbles sous-marins, le maillon faible de la cyberguerre

---

Le délit de consultation habituelle de sites terroristes est réinstauré

Le délit de consultation habituelle de sites terroristes est réinstauré

Lors de de la commission mixte paritaire pour le projet de loi relatif à la sécurité publique, les parlementaires ont réinstauré le délit de consultation habituelle de sites terroristes en y ajoutant une condition supplémentaire.

Censuré par le Conseil constitutionnel, le délit de consultation habituelle provoquant directement à la commission d'actes de terrorisme ou faisant l'apologie de ces actes est en train de faire son retour dans la législation française. Une nouvelle version de l'article 421-2-5-2 du code pénal a en effet été proposée par les parlementaires lundi 13 février, trois jours à peine après le verdict des Sages de la rue de Montpensier.
C'est dans le cadre de la commission mixte paritaire, chargée de négocier la version définitive du projet de loi relatif à la sécurité publique en faisant appel à sept députés et sept sénateurs, que le nouvel article de loi a été déposé, sous l'impulsion du député Éric Ciotti et le sénateur Philippe Bas, ce dernier déclarant le jour de la censure que cette disposition est « *essentielle à la lutte antiterroriste* ».
Suivre
Philippe Bas
@BasPhilippe
J'ai fait rétablir en le modifiant le délit de consultation de sites terroristes à la #CMP de la loi sur la sécurité publique.
18:46 – 13 Févr 2017
•
•
3131 Retweets
•
2929 j'aime
Suivre
Eric Ciotti
@ECiotti
Avec Philippe Bas, nous venons de rétablir en CMP le délit de consultation des sites djihadistes annulé de façon ahurissante par le CC
17:44 – 13 Févr 2017
•
•
115115 Retweets
•
106106 j'aime
« *J'ai fait rétablir en le modifiant le délit de consultation de sites terroristes à la CMP de la loi sur la sécurité publique* », s'est félicité Philippe Bas. Plus offensif, Éric Ciotti a chargé le Conseil constitutionnel qui a « *annulé de façon ahurissante* » cet article né avec la loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.
La nouvelle rédaction du texte est la suivante (les changements par rapport à la première version du texte ont été mis en gras) :
Le fait de consulter habituellement **et sans motif légitime** un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ce service comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie est puni de deux ans d'emprisonnement et de 30 000 € d'amende **lorsque cette consultation s'accompagne d'une manifestation de l'adhésion à l'idéologie exprimée sur ce service**.
Constitue notamment un motif légitime […] la consultation résultant de l'exercice normal d'une profession ayant pour objet d'informer le public, intervenant dans le cadre de recherches scientifiques ou réalisée afin de servir de preuve en justice ou le fait que cette consultation s'accompagne d'un signalement des contenus de ce service aux autorités publiques compétentes.
LA NOUVELLE VERSION DEMANDE DÉSORMAIS DE VÉRIFIER UNE MANIFESTATION DE L'ADHÉSION À L'IDÉOLOGIE…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Le délit de consultation habituelle de sites terroristes fait son retour – Politique – Numerama

---

Comment faire face au risque de Cyberattaques sur les infrastructures énergétiques ?

Comment faire face au risque de Cyberattaques sur les infrastructures énergétiques ?

Cette étude analyse les risques de cyberattaques sur des infrastructures énergétiques européennes, ainsi que leurs potentielles conséquences, notamment sur les réseaux électriques. Elle offre également une approche comparative des mesures prises par différents pays d'Europe afin de protéger leur industrie et collaborer à l'échelle de l'Union européenne.

La digitalisation de l'industrie énergétique permet de révolutionner les processus de production, de stockage, de transport et de consommation d'énergie. Nos infrastructures énergétiques, conçues il y a plusieurs décennies et prévues pour demeurer fonctionnelles pour de nombreuses années encore, côtoient désormais des équipements numériques avec lesquels elles interagissent au quotidien. Ces évolutions, qui sont aujourd'hui un gage de disponibilité, d'efficacité et de réactivité sur toute la chaîne de valeur énergétique, ouvrent pourtant la voie à un type de menace qui jusqu'en 2010 avait relativement épargné cette industrie : les cyberattaques.

Le nombre et la technicité des attaques ont augmenté après les dégâts causés par le virus Stuxnet au sein du complexe d'enrichissement nucléaire iranien de Natanz, bien que cette attaque demeure la plus sophistiquée observée à ce jour. Et s'il y a une réelle prise de conscience des enjeux dans le secteur énergétique, les risques persistent. Les politiques de transition énergétique et les efforts d'intégration des énergies renouvelables ne feront que renforcer cette tendance tant que la cybersécurité ne fait pas partie de la réflexion sur l'avenir du système énergétique.

La réglementation tente de s'adapter, notamment en France où les autorités collaborent étroitement avec les entreprises de l'énergie pour faire émerger un cadre réglementaire contraignant, et protéger les Opérateurs d'Importance Vitale (OIV). Cette démarche inspire également d'autres pays d'Europe, mais des mesures communes à toute l'Union européenne sont à prendre rapidement afin de garantir la sécurité de nos réseaux énergétiques, fortement interconnectés.

LIRE L'ETUDE (PDF)

Original de l'article mis en page : Cyberattaques et systèmes énergétiques: faire face au risque | IFRI – Institut français des relations internationales

---

Réagissez à cet article

La CyberMenace jihadiste grandit

	La CyberMenace jihadiste grandit

Un cyber-attentat de grande ampleur, qui causerait des dégâts physiques ou même des morts, n'est peut-être pas encore à la portée des groupes jihadistes mais cela pourrait changer sous peu et il faut s'y préparer, estiment des spécialistes.
D'autant qu'ils sont déjà en mesure de trouver, auprès de hackers et de mercenaires de l'ère digitale prêts à tout pour de l'argent, les capacités techniques qui leur manquent pour utiliser internet pour autre chose que de la propagande et du recrutement, ajoutent-ils.
« Daech (acronyme arabe du groupe État islamique), Al Qaïda, tous les groupes terroristes aujourd'hui : nous avons le sentiment que pour l'instant, ils ne disposent pas des compétences offensives cyber », déclare à l'AFP Guillaume Poupard, directeur de l'Agence nationale des systèmes d'information (ANSSI).
« Ces compétences sont compliquées à acquérir, même si ce n'est pas l'arme atomique. Avec quelques dizaines de personnes, un petit peu d'argent mais pas tant que ça, il y a la possibilité d'être efficace. Ils pourraient monter en compétence. Nous avons le sentiment que pour l'instant ils n'y sont pas. Ils ont d'autres soucis, et c'est compliqué pour eux », ajoute-t-il à Lille, où il a participé mercredi au 9e Forum international de la Cybersécurité.
« Les voir à court terme mener des attaques informatiques avec des impacts majeurs, on n'y croit pas trop. En revanche ça pourrait changer très vite. Notre vraie crainte, et on y est peut-être déjà, c'est qu'ils utilisent les services de mercenaires. Ce sont des gens qui feraient tout et n'importe quoi pour de l'argent », ajoute-t-il.

– Inscrit dans l'ADN –
Ce recours par des groupes jihadistes à des sous-traitants informatiques pour monter des cyber-attentats (mise en panne de réseaux électriques, paralysie de réseaux de transport ou de systèmes bancaires, prise de contrôle de sites ou de médias officiels, sabotage à distance de sites industriels critiques, par exemple), le directeur d'Europol, Rob Wainwright, l'évoquait le 17 janvier à Davos.
« Même s'il leur manque des savoir-faire, ils peuvent aisément les acheter sur le darknet (partie d'internet cryptée et non référencée dans les moteurs de recherche classiques qui offre un plus grand degré d'anonymat à ses utilisateurs, ndlr), où le commerce d'instruments de cyber-criminalité est florissant », estimait-il lors d'une table ronde intitulée « Terrorisme à l'âge digital »…[lire la suite]

Réagissez à cet article

Tracfin : le renseignement financier cible la FinTech

Tracfin : le renseignement financier cible la FinTech

Financement participatif détourné, paiement mobile opaque, transactions virtuelles anonymes… Tracfin met l'accent sur les risques numériques et appelle la FinTech à coopérer. Son objectif : mieux lutter contre le blanchiment de capitaux et le financement du terrorisme.
Tracfin, la cellule française de renseignement financier, a remis ce jeudi au ministre de l'Économie et des Finances, Michel Sapin, son rapport d'analyse des risques de blanchiment de capitaux et de financement du terrorisme. Financement participatif détourné, paiement mobile opaque, transactions virtuelles anonymes… Tracfin met l'accent sur les risques numériques émergents.
Selon le rapport, *« les risques d'escroquerie dans la finance participative (crowdfunding) sont élevés, par exemple par le détournement des paiements ou par l'élaboration de fraudes du type pyramide de Ponzi »*, surtout pour les plateformes de prêt. Quant aux plateformes de dons et de cagnottes en ligne, elles sont exposées à des risques *« importants de blanchiment de capitaux et de financement du terrorisme »*,. Certes, les fonds collectés restent limités, mais ils ont tout de même été multipliés par deux entre 2014 et 2015, observe Tracfin. **196,3 millions d'euros** ont été collectés via les plateformes de prêt l'an dernier, 50,3 millions d'euros pour l'investissement et 50,2 millions d'euros pour les dons.

Cadre européen pour le financement participatif

En France, un cadre juridique dédié au financement participatif a été mis en place en 2014. Il impose aux plateformes de prêt et d'investissement le choix d'un statut de conseiller en investissement participatif (CIP), régulé par l'Autorité des marchés financiers (AMF), ou d'intermédiaire en financement participatif (IFP), régulé par l'Autorité de contrôle prudentiel et de résolution (ACPR). Ces plateformes sont donc bien assujetties au dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme (**LCB/FT**).
En revanche, la démarche restait facultative pour les plateformes de dons et les cagnottes en ligne. Mais elles seront aussi soumises à ce régime à partir de 2017, une ordonnance transposant une directive européenne dans ce domaine ayant été publiée le 2 décembre. C'est une bonne chose pour le directeur de Tracfin, Bruno Dalles, qui recommande l'adoption d'un cadre règlementaire dédié au financement participatif à l'échelle européenne. Car le cadre réglementaire national ne s'applique pas aux plateformes qui proposent, depuis l'étranger, d'effectuer des dons, prêts ou investissements…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Tracfin : le renseignement financier cible la FinTech

La coopération Internationale renforcée dans le Cloud

	La coopération Internationale renforcée dans le Cloud

« Le quinzième anniversaire de la Convention de Budapest sur la cybercriminalité est un tournant dans la mesure où la Convention atteint maintenant les « nuages », a déclaré le Secrétaire Général du Conseil de l'Europe Thorbjørn Jagland lors de l'inauguration de la Conférence Octopus 2016.

Les données et donc les preuves électroniques sont de plus en plus stockées sur des serveurs relevant de juridictions étrangères, inconnus ou multiples. C'est pourquoi, il peut être extrêmement difficile pour les autorités chargées de la justice pénale d'obtenir régulièrement de telles preuves. Faute de celles-ci, les délinquants qui opèrent dans le cyberespace ne peuvent être poursuivis.
Le Secrétaire Général a salué le jeu de recommandations adoptées par le Comité de la Convention sur la cybercriminalité lors de sa réunion des 14-15 novembre, dans lesquelles il voit une réponse véritable au problème de l'informatique en nuage (cloud computing). Les recommandations prévoient la négociation d'un protocole additionnel à la Convention à partir du milieu de 2017.
« La coopération entre les Etats s'est considérablement améliorée. Cela est dû pour beaucoup au travail du Comité de la Convention. Les notes d'orientation adoptées par le Comité ont aidé à préserver la pertinence et l'actualité de la Convention, à renforcer notre capacité de combattre le terrorisme, le vol d'identités ou les attaques contre des infrastructures d'informations critiques », a déclaré le Secrétaire Général, qui a invité les gouvernements à mieux protéger les droits des particuliers dans le cyberespace.
« Nous avons élaboré une sorte de « triangle dynamique » – Convention, Comité et renforcement des capacités – si bien que la Convention de Budapest reste aujourd'hui le traité international le plus important sur la cybercriminalité et la preuve électronique », a-t-il conclu.
A l'occasion de la conférence, Andorre a ratifié la Convention en présence d'Eva Descarrega Garcia, Secrétaire d'Etat andorrane à la Justice et à l'Intérieur.
68 Etats sont soit déjà parties à la Convention de Budapest, soit se sont formellement engagés à la respecter. Au moins 70 pays de plus ont pris la Convention comme source d'inspiration pour élaborer leur législation interne.
[Discours de Thorbjørn Jagland (*anglais*)]

Réagissez à cet article

Original de l'article mis en page : Cybercriminalité : vers un

Denis JACOPINI intervient au Conseil de l'Europe lors de la conférence Octopus 2016

Denis JACOPINI intervient au Conseil de l'Europe lors de la conférence Octopus 2016

A l'occasion de sa conférence annuelle consacrée à la lutte de la Cybercriminalité à travers le monde du 16 au 18 Novembre prochain au Conseil de l'Europe, Denis JACOPINI intervient au Workshop n°7

Au programme :

• La Convention de Budapest: 15e anniversaire
• Criminalité et compétence dans le cyberespace : la voie à suivre
Ateliers
• Coopération entre les fournisseurs de service et les services répressifs en matière de cybercriminalité et de preuve électronique
• L'accès de la justice pénale aux preuves dans le Cloud: les résultats du groupe sur les preuves dans le Cloud (Cloud Evidence Group)
• Renforcement des capacités en cybercriminalité: les enseignements tirés
• L'état de la législation en matière de cybercriminalité en Afrique, en Asie/Pacifique et en Amérique latine/aux Caraïbes
• Le terrorisme et les technologies de l'information : la perspective de la justice pénale
• Coopération internationale: amélioration du rôle des points de contact 24/7
• A la recherche des synergies: politiques et initiatives en cybercriminalité des organisations internationales et du secteur privé

Participation

La conférence sera l'occasion, pour les experts en cybercriminalité des secteurs public et privé ainsi que les organisations internationales et non gouvernementales du monde entier, d'échanger.

La conférence Octopus fait partie du projet **Cybercrime@Octopus** financé par les contributions volontaires de l'Estonie, du Japon, de Monaco, de la Roumanie, du Royaume-Uni, des Etats-Unis d'Amérique et de Microsoft ainsi que du budget du Conseil de l'Europe.
Agenda Octopus 2016

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Octopus 2016

60 millions de Français fichés dans une base de données commune des titres d’identité

	60 millions de Français fichés dans une base de données commune des titres d’identité

Un décret publié pendant le pont de la Toussaint officialise la création d'un gigantesque fichier national.
Soixante millions de Français glissés, à l'occasion d'un week-end de pont de la Toussaint, dans une même base de données : un décret paru au Journal officiel dimanche 30 octobre, et repéré par le site NextInpact, officialise la création d'un « traitement de données à caractère personnel commun aux passeports et aux cartes nationales d'identité ». En clair, les données personnelles et biométriques de tous les détenteurs d'une carte d'identité ou d'un passeport seront désormais compilées dans un fichier unique, baptisé « Titres électroniques sécurisés » (TES). Cette base de données remplacera à terme le précédent TES (dédié aux passeports) et le Fichier national de gestion (dédié aux cartes d'identité), combinés dans ce nouveau fichier.

La base de données rassemblera ainsi des informations comme la photo numérisée du visage, les empreintes digitales, la couleur des yeux, les adresses physiques et numériques… Au total, la quasi-totalité des Français y figurera, puisqu'il suffit de détenir ou d'avoir détenu une carte d'identité ou un passeport pour en faire partie – les données sont conservées quinze (pour les passeports) à vingt ans (pour les cartes d'identité)…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : 60 millions de Français fichés dans une base de données commune des titres d'identité

Le réseau informatique des drones militaires américains

piraté ?

Le réseau informatique des drones militaires américains piraté ?

Le 9 septembre dernier, le réseau informatique de la base Creech de l'US Air Force, dans le Nevada, est tombé en panne, peut-être en raison d'un acte de piratage. C'est de là que sont conduites les opérations de surveillance et de bombardement par drones. Le réseau n'est toujours pas rétabli complètement.

L'armée américaine s'est-t-elle fait pirater le réseau de communication qu'elle utilise pour piloter à distance sa flotte de drones tueurs, qui bombardent quotidiennement dans de multiples pays du monde dont l'Afghanistan, la Syrie, le Pakistan, la Somalie, ou l'Irak ? La question se pose alors que BuzzFeed dévoile que l'US Air Force a reconnu que le réseau informatique de sa base Creech Air Force, dans le Nevada, était tombé en panne le 9 septembre dernier, et qu'il n'avait toujours pas pu être rétabli complètement depuis.
La base Creech Air Force est celle qui abrite les militaires qui, joystick à la main et yeux rivés sur un écran, déclenchent les frappes aériennes à des milliers de kilomètres de distance – parfois en utilisant uniquement des collectes de métadonnées pour présumer de l'identité des cibles, l'armée ayant développé des algorithmes pour les détecter. Les drones sont pilotés à travers des liaisons satellite qui permettent de relayer les ordres du Nevada jusqu'aux théâtres de guerre, avec un minimum de temps de latence et en toute sécurité.
Mais le système repose au moins partiellement sur le réseau SIRPnet (*Secret Internet Protocol Router Network*), une sorte de réseau Internet privé de l'armée américaine, utilisé pour véhiculer des informations confidentielles en toute sécurité. Or selon un appel d'offres étonnamment détaillé publié par l'armée, « *le système SIRPNet actuellement en opération à Creech AFB a échoué et des services essentiels ont été touchés* ». Elle précise que « *les systèmes ont été quelque peu restaurés avec l'utilisation de plusieurs appareils moins puissants* », et que « *cette solution temporaire a stabilisé les services, mais ne sera pas capable de satisfaire la demande encore très longtemps* ». Or, « *si cette solution échoue, il n'y actuellement aucun système de sauvegarde* »…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Un système essentiel pour les drones tueurs américains est tombé en panne – Politique – Numerama