DU en Investigation Numérique Pénale – Denis JACOPINI témoigne

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	DU en Investigation Numérique Pénale – Denis JACOPINI témoigne				

Vous souhaitez connaître le droit, les éléments théoriques ainsi que les outils liés au métier d'investigateur numérique en matière pénale ? Cette formation de 130 heures qui débouche sur le premier Diplôme Universitaire en Investigation Numérique Pénale de France est faîte pour vous. Attention, les places sont limitées.

Contenu de la formation :
• Acquisition des bases et des fondamentaux en matière informatique dans le cadre d'une expertise pénale ;
• Connaissance de la Procédure pénale ;
• Connaissance des missions, de l'organisation professionnelle et des bonnes pratiques d'un enquêteur numérique ;
• Acquisition des méthodes et pratiques d'extraction de données post mortem :
• *Extraction de données à partir de supports physiques*
• *Extraction de données à partir de terminaux mobiles*
• *Extraction de traces internet*
• *Manipulation d'objets multimédia*
• Acquisition des méthodes de fouille de données

2019 06 14 Plaquette INPA5 v12

Cette formation est réalisée en partenariat avec :
• UFIN (Union Française de l'Investigation Numérique)
• CNEJITA (Compagnie Nationale des Experts de Justice en Informatique et Techniques Associées)
• AFSIN (Association Francophone des Spécialistes de l'Investigation Numérique)
• Gendarmerie nationale

Denis JACOPINI, Expert de Justice en Informatique spécialisé en Cybercriminalité et en Protection des Données Personnelles (RGPD) témoigne :
C'est avec grand plaisir que je vous témoigne ma grande satisfaction à l'issue de cette formation. Même si j'avais déjà une expérience en tant qu'Expert de Justice en Informatique, étalée sur 8 mois, le contenu de cette formation m'a permis d'être désormais mieux équipé (mentalement, organisationnellement et techniquement) et en plus grade confiance pour les futures expertises pénales qui me seront confiées.

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et*

les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Source : *Diplôme d'Université : Investigation Numérique Pénale – Ametys*

Risque de cyberattaque terroriste très élevé

 © Dieter Telemans	**Risque de cyberattaque terroriste très élevé**

Le commissaire chargé de la Sécurité nous explique ce que l'Europe a fait pour améliorer la sécurité de ses citoyens. Il avoue craindre « tous les types de menaces ».

Il est « Le Dernier des Mohicans ». L'ultime commissaire britannique envoyé par Londres avant le Brexit. Dans son bureau du Berlaymont placé sous haute sécurité, trônent deux grandes photographies de Sa Majesté. Sur le sofa, des coussins décorés de l'Union Jack. « No doubt », c'est bien ici une partie de l'île encore arrimée à l'Europe.
Julian King, formé à la fois à Oxford et à l'ENA, est l'un des plus brillants diplomates du Royaume. Sa mission? Créer l'Union européenne de la sécurité ainsi que gérer la lutte contre le terrorisme et le crime.
L'Echo l'a rencontré, un an après les attentats terroristes à Bruxelles.

Comment avez-vous vécu les attaques du 22 mars?
J'étais ambassadeur du Royaume-Uni en France. Je revenais du marché de Rungis. C'était tôt le matin. J'ai mis du temps à me remettre de cette nouvelle. Dès mon retour à la résidence, j'ai demandé qu'ils mettent le drapeau en berne.

Qu'avez-vous ressenti?
Je craignais de nouveaux attentats depuis mon entrée en fonction à Paris. C'est arrivé dans la capitale du pays voisin, là où ma femme vit et travaille. Son bureau n'était pas loin de Maelbeek. J'ai eu peur que mes amis m'appellent pour m'apprendre une mauvaise nouvelle.
Trop de gens qui ont grandi dans nos pays sont partis se radicaliser en Syrie et en Irak. La prévention de la radicalisation est la clé.

Qu'est-ce que les attentats ont changé?
Après chaque attaque, à Paris, Bruxelles et Nice, j'ai été frappé de voir à quel point nos villes sont résilientes. Ces événements sont horribles. Très difficiles à vivre pour les victimes mais aussi pour les gens qui doivent monter en première ligne et tous les habitants de la ville. Je suis touché par la capacité des Belges et des Français à dépasser le drame. À reprendre leur vie. Et le lien profond qu'ils ont avec leur communauté.

Qu'a fait l'Europe, depuis lors, pour améliorer la sécurité de ses citoyens?
Nous avons commencé par renforcer les frontières extérieures. Nous avons créé un corps de garde-frontières et de garde-côtes, déployé du personnel de Frontex et d'Europol pour soutenir les autorités en Grèce et en Italie, adopté une directive sur le contre-terrorisme qui criminalise les allers-retours d'Irak et de Syrie. Nous avons renforcé le code Schengen pour contrôler systématiquement toute personne qui entre dans l'espace Schengen, y compris les citoyens Européens.
Nous avons proposé de créer un système interactif pour contrôler les nationaux des pays tiers, c'est à l'étude au Parlement. Nous allons aussi mettre en place un système de précontrôle des étrangers n'ayant pas besoin de visas, appelé Etias et calqué sur le modèle Esta des Etats-Unis.
Nous avons renforcé notre capacité de connaître ceux qui arrivent dans l'espace européen, et c'est un élément vital pour notre sécurité.

Qu'avez-vous fait pour accroître la sécurité intérieure?
Nous avons renforcé les capacités des forces de l'ordre. Nous avons mis plus d'argent, de personnel et de moyens dans Europol. Nous avons consolidé les bases de données policières et réformé la plus importante: le système Schengen. Nous voulons obliger les polices nationales à partager leurs informations à travers ce système. Dans les faits, ils le font de plus en plus. Mais ce sera encore plus vrai lorsque l'obligation d'échanger sera adoptée par le Conseil européen.
Nous devons aussi accroître la capacité des agents d'aller chercher une information là où elle se trouve.
Pour éviter, comme après les attaques de Paris, qu'un terroriste comme Salah Abdeslam puisse déjouer les contrôles…
Oui. Les renseignements existaient mais lors de ce fameux contrôle entre Paris et Bruxelles, la police n'a pas été capable d'aller les chercher. Nous allons proposer un paquet de mesures pour améliorer la qualité des informations, le traitement de données, l'utilisation plus fréquente de la biométrie et accroître la rapidité d'obtention des informations.
La moitié des business européens ont déjà subi une cyber-attaque.

Quand allez-vous proposer ces mesures?
Mon équipe y travaille, son rapport devrait être prêt d'ici avril. Nous ferons ensuite des propositions.

Les États européens appliqueront-ils ces mesures?
Nous insistons beaucoup là-dessus. Pour la première fois depuis mon arrivée l'été dernier, la Commission a lancé des procédures d'infraction contre plusieurs États qui n'appliquent pas les mesures convenues l'an dernier. Trois procédures contre des États qui n'ont pas appliqué la directive sur les explosifs et cinq procédures contre des États qui n'ont pas appliqué l'arrangement de Prüm sur les échanges d'information.

Que pensez-vous de la création d'un « FBI Européen », comme le préconise Guy Verhofstadt?
Je ne suis pas persuadé que cela arrive dans un futur immédiat. Il y a des questions légales, des difficultés constitutionnelles à lever. Mon objectif, pour le moment, est de construire une coopération pratique entre les agences de renseignements nationales. Certains prétendent qu'il n'existe aucun échange entre elles, mais ce n'est pas vrai. Cette collaboration existe, les agences européennes ont d'ailleurs depuis peu une plateforme commune aux Pays-Bas.

Vous n'aimez pas parler du Brexit. Mais dites-moi, le Royaume-Uni continuera-t-il à coopérer avec l'UE après son départ?
Je l'espère. Je ferai tout durant les deux années à venir pour renforcer notre sécurité commune contre le terrorisme, le cyberterrorisme et le crime organisé. Ces menaces affectent tous les pays d'Europe, qu'ils soient ou pas dans Schengen ou dans l'UE, et c'est le cas en particulier des cyberattaques. Notre combat sera plus efficace si nous le menons ensemble. Ce sera vrai demain, dans deux ans et dans cinq ans. Il est important qu'après le Brexit l'Union européenne et le Royaume-Uni conservent une coopération étroite en matière de lutte contre le terrorisme.

Quant à la coopération entre l'Europe et les Etats-Unis, résistera-t-elle à l'arrivée de Donald Trump?
Jusqu'à présent, tous les représentants des Etats-Unis que j'ai rencontrés ont été clairs. Ils comprennent l'importance de notre coopération et veulent la maintenir.

Quel est le niveau de risque d'attentat terroriste à Bruxelles?
Nous ne sommes pas chargés d'évaluer ce niveau, mais nous écoutons ce que chaque État nous dit. Et il est clair que la menace terroriste dans un État qui a subi une attaque est très très élevée. Il est très important de ne pas donner l'impression que la menace a disparu. Ou que nous avons réduit la menace à zéro.

Les terroristes se concentrent sur les espaces publics, les métros ou les aéroports. Comment sécuriser de tels lieux?
Chaque État a développé de très bonnes pratiques dans la gestion de la sécurité des espaces publics. Nous mettons ensemble tous les experts pour tirer les leçons des meilleures pratiques et nous dressons une liste de lignes directrices. Nous allons continuer ce travail et le faire avec les meilleurs praticiens.

Vous craignez des menaces d'isolés ou des groupes organisés?
Tous les types de menaces. Celles de loups solitaires, et c'est pourquoi la lutte contre la radicalisation est une partie importante de nos travaux. Mais aussi les menaces d'attaques organisées inspirées par Daech, qui ne sont pas réduites parce ce qu'ils sont en difficulté sur le terrain en Syrie et en Irak.

La plupart des auteurs des attaques à Bruxelles et Paris étaient Européens…
Trop de gens qui ont grandi dans nos pays sont partis se radicaliser en Syrie et en Irak. La prévention de la radicalisation est la clé.

Que fait l'Europe pour lutter contre la radicalisation?
Nous agissons à deux niveaux. D'abord nous nous attaquons à la propagande de Daech sur internet, qu'ils continuent à déverser malgré leur déroute sur le terrain. Nous travaillons pour l'instant avec les plus grands groupes du web. Nous avons besoin de leur aide pour trouver des moyens industriels qui arrêtent cette propagande.
L'autre risque majeur ce sont les gens qui, au sein des communautés, cherchent à pousser les plus fragiles à la violence. Le moyen le plus efficace pour les empêcher d'agir est de travailler localement. Nous avons développé, au niveau européen, des moyens pour œuvrer avec ces communautés, soit pas des fonds, soit par la mise en place d'un réseau d'organisations où ils reçoivent du soutien.

Craignez-vous une cyberattaque terroriste, par exemple contre une centrale nucléaire ou une tour de contrôle aérienne?
Les terroristes comme Daech n'utilisent pas, pour l'instant, de tels moyens. Mais le risque d'une cyberattaque terroriste est très élevé. La cybercriminalité augmente de manière exponentielle. Au Royaume-Uni, un pays que je connais bien, la moitié des crimes connus sont des cybercrimes. Si vous regardez l'Europe, la moitié des business européens ont déjà subi une cyberattaque.

Comment affrontez-vous ce risque?
Notre première ligne de défense consiste à avertir le public du danger de manipulation sur internet. Nous devons ensuite construire une résilience, à chaque niveau. Apprendre aux individus à protéger leurs appareils, changer leur code. Il faut aussi mettre en place les moyens nécessaires pour protéger les infrastructures critiques, comme les unités de production d'énergie, exposées aux cyberattaques. Nous travaillons à la création d'une agence européenne qui planifie la protection des infrastructures et mette en place un réseau d'échange d'information, le tout en application de la directive NIS.
Nous travaillons aussi avec le secteur privé, généralement très avancé sur ces questions de sécurité, et lancer des partenariats. Nous allons mobiliser 1,8 milliards d'euros pour des recherches en cybersécurité d'ici 2020. C'est un effort important.
Nous préparons également des exercices conjoints avec l'Otan pour contrer les cyberattaque.
*Enfin, j'espère que nous pourrons faire un examen complet de tout notre travail sur la cybersécurité sous présidence estonienne, avant la fin de cette année…**[lire la suite]***

***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 : *« Le risque d’une cyberattaque terroriste est très élevé » | L’Echo*

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

---

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

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

Déchiffrement des communication numériques (Telegram et autres). Où en est-on ?

Déchiffrement des communication numériques (Telegram et autres). Où en est-on ?

Ce mardi 23 Août, Bernard Cazeneuve se réunissait avec son homologue allemand pour discuter d'une initiative européenne contre le chiffrement des données, afin de lutter contre le terrorisme. Une initiative qui ne fait pas l'unanimité.

Une initiative européenne contre les chiffrements trop forts ?

Face au terrorisme international et sachant que les messageries instantanées visées par le projet de loi sont majoritairement américaines, Bernard Cazeneuve s'en remet à une initiative européenne. L'idée serait d'étendre aux services de messageries et d'appels sur internet, les mêmes règles de sécurité et de confidentialité destinées jusque-là, aux opérateurs télécom. Le ministre a ainsi fermement déclaré vouloir obliger les services en ligne «*non coopératifs*» à «*retirer des contenus illicites ou déchiffrer des messages dans le cadre d'enquêtes judiciaires, que leur siège soit en Europe ou non*».

Conscient de la polémique qui entoure ce projet de loi, le ministre a précisé que l'utilisation des données déchiffrées ne servirait que dans le cadre « *judiciaire* ». Ce qui voudrait dire qu'elles ne seraient pas utilisées par les services secrets, comme le redoutent beaucoup de personnes. Se voulant rassurant, il a insisté « *Il n'a bien sûr, jamais été question de remettre en cause le principe du chiffrement des échanges* ». Le 16 septembre prochain, le projet de loi contre le chiffrement des données sera discuté lors du sommet des chefs d'états européens.

…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Une initiative franco-allemande contre le chiffrement numérique

---

Les services de renseignement devraient-ils avoir accès aux clés de déchiffrement ?

Les services de renseignement devraient-ils avoir accès aux clés de déchiffrement ?

Une initiative franco-allemande va tenter de convaincre les acteurs internationaux d'Internet et de l'informatique de la nécessité d'ouvrir leurs codes et leurs chiffrements pour lutter contre le terrorisme. Des voix s'élèvent au nom de la sécurité et des libertés.

Après le conseil restreint de Défense à l'Élysée le 4 août 2016, le ministre de l'Intérieur, Bernard Cazeneuve, a parlé chiffre. Avec son homologue allemand, Thomas de Maizière, il a proposé le 23 août une initiative européenne à vocation internationale pour « faire face au défi du chiffrement, une question centrale dans la lutte antiterroriste ». Le sujet est brûlant. Pas seulement depuis l'assassinat du père Hamel par des usagers de Telegram , d'ailleurs pas considéré comme la solution la plus hermétique d'un marché en plein essor.

Outre Telegram, les terroristes, des criminels et des gens très soucieux de l'intégrité de leurs communications utilisent pléthore de dispositifs de chiffrement comme ChatSecure, Conversations, Kontalk, Signal, Threema ou WhatsApp (même s'il appartient à Facebook depuis 2014), sans parler des anonymes Tor (réseau décentralisé) ou ToX (pair à pair). Là n'est d'ailleurs pas la question centrale. L'ennemi pourrait émigrer vers d'autres cieux numériques voire créer son propre outil chiffré…

Incapable de casser le code

Depuis l'audition à l'Assemblée le 10 mai de Patrick Calvar, le directeur général de la sécurité intérieure, la pression monte. Pour les attentats de Bruxelles, le DGSI avoue que « même une interception n'aurait pas permis de mettre au jour les projets envisagés puisque les communications étaient chiffrées sans que personne soit capable de casser le chiffrement ». Face au chiffrement aléatoire et autres complications futures, le DGSI a une réponse martiale : « Je crois que la seule façon de résoudre ce problème est de contraindre les opérateurs. » Nous y voilà. En février, le FBI s'est heurté au refus d'Apple de livrer les données de l'iPhone d'un des meurtriers de Daech qui a tué 14 personnes à San Bernardino le 2 décembre 2015. Avant que le FBI n'annonce avoir réussi à casser le chiffre de la pomme…

Bernard Cazeneuve ne dit pas autre chose. Il prend pour exemple sa négociation avec les majors d'Internet en février 2015 qui a permis d'élaborer une charte sur le retrait des contenus et le blocage des sites haineux. « Sur le chiffrement, il faut que nous ayons la même méthode, la même volonté, le sujet est crucial. »

Sauf qu'un courrier, publié par Libération, du directeur de l'Agence nationale de sécurité des systèmes d'information (ANSSI) et lui-même cryptologue, Guillaume Poupard, affirme le contraire aux autorités : « Un affaiblissement généralisé serait attentatoire à la sécurité numérique et aux libertés de l'immense majorité des utilisateurs. » Permettre une intrusion des services de renseignement (par des « portes dérobées ») pourrait profiter à des gens ou des États (pas seulement islamiques) mal intentionnés. Quelle tendance va l'emporter ? En cette époque sécuritaire, de l'état d'urgence éternel et du désarroi politique…

Article original de Olivier Berger

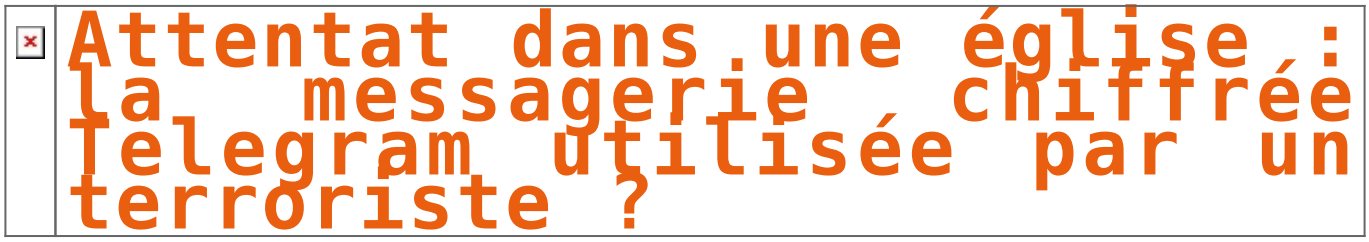
Réagissez à cet article

Original de l'article mis en page : Lutte contre le terrorisme : Faut-il ouvrir la porte du chiffrement aux services de renseignement ? – La Voix du Nord

---

Attentat dans une église : la

messagerie chiffrée Telegram utilisée par un terroriste ? – Politique – Numerama



Selon La Voix du Nord, au moins l'un des deux auteurs de l'attentat de l'église de Saint-Étienne-du-Rouvray utilisait régulièrement la messagerie chiffrée Telegram pour communiquer avec des islamistes, et aurait posté un message une heure avant l'attentat.

Il faut s'attendre à voir très vite renaître le débat sur le chiffrement et l'obligation qui pourrait être faite aux fournisseurs de messageries électroniques de laisser les services de Renseignement accéder aux communications. La Voix du Nord affirme qu'Adel Kermiche, l'un des deux coauteurs de la tuerie de l'église de Saint-Étienne-du-Rouvray, près de Rouen, utilisait la messagerie chiffrée Telegram, à des fins djihadistes. Il aurait envoyé un message sur un canal de discussion une heure avant l'attaque.
« Selon nos informations, Adel Kermiche avait ouvert sur Telegram une « private channel » (haqq-wad-dalil), une chaîne lui permettant de s'adresser à une audience ultra-sélectionnée. Il avait choisi pour nom de code Abu Jayyed al-Hanafi et la photo de Abou Bakr al-Baghdadi, chef suprême de l'État islamique, comme représentation », écrit le quotidien régional.

TÉLÉCHARGER (SIC) CE QUI VA VENIR ET PARTAGER LE EN MASSE ! ! ! !
Selon les membres arabophones de la rédaction de Numerama, haqq-wad-dalil signifierait quelque chose comme « preuve de la vérité » ou « guide de la vérité ».
La Voix du Nord ajoute que « le terroriste correspondait depuis des mois via ce canal avec près de 200 personnes, dont une dizaine de Nordistes », qui étaient d'abord approchés par Facebook. Le matin de l'attentat, le 26 juillet 2016 à 8h30, il aurait envoyé sur ce salon un message qui disait : « Télécharger (sic) ce qui va venir et partager le en masse ! ! ! ! ».
Le quotidien ne dit rien d'un éventuel document qui aurait pu être mis en partage par la suite, ce qui ne laisse la voie qu'à des spéculations. Peut-être Kermiche avait-il prévu de filmer son acte odieux, ou des revendications, et espérait trouver des relais à sa diffusion à travers ses contacts sur Telegram.
Si cette information se confirme ce serait, à notre connaissance, la première fois qu'un lien direct est effectué entre un attentat terroriste en France et l'utilisation de messageries chiffrées.

COMMENT SURVEILLER TELEGRAM ?
La Voix du Nord ne dit pas par quel biais le message aurait été découvert. Il est possible que les enquêteurs aient trouvé ce message en accédant à l'historique Telegram du terroriste, depuis son téléphone mobile qui n'aurait pas été bloqué. Le plus probable est toutefois que l'information provienne d'un autre utilisateur du salon haqq-wad-dalil, puisque le quotidien cite le témoignage de l'un d'entre eux, qui explique que les échanges pouvaient y être « écrits ou oraux mais toujours détruits rapidement ».
Il est connu depuis de très nombreux mois que Telegram, qui dispose de plus de 100 millions d'utilisateurs à travers le monde, est aussi utilisé par des djihadistes qui recherchent la sécurité d'une messagerie chiffrée.
Après avoir refusé d'opérer la moindre censure, en tout en continuant à livrer la moindre information personnelle sur ses utilisateurs, Pavel Durov a fini par décider en novembre 2015 de fermer des salons de discussion liés à l'État islamique, pour mettre fin aux accusations de complicité passive. Il avait appelé les internautes à les signaler pour permettre leur fermeture.
Théoriquement, les canaux de discussion peuvent être infiltrés par les agents des services de renseignement. Reste qu'en l'absence de communication d'informations sur les utilisateurs, il peut être difficile de remonter jusqu'à l'auteur d'un message présentant une menace particulièrement élevée.
Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : Attentat dans une église : la messagerie chiffrée Telegram utilisée par un terroriste ? – Politique – Numerama

---

Détecter les futurs terroristes sur Internet ? L’Europe veut s’inspirer d’Israël

Détecter les futurs terroristes sur Internet ? L’Europe veut s’inspirer d’Israël

---

Le coordinateur de l'anti-terrorisme pour lUnion européenne, Gilles de Kerchove, s'est rendu en Israël pour trouver des solutions technologiques qui permettraient de détecter automatiquement des profils suspects sur les réseaux sociaux, grâce à des algorithmes de plus en plus intrusifs.

Plus les attentats en Europe se multiplient, plus on découvre que les profils psychologiques et sociaux des kamikazes et de leurs associés sont très divers, jusqu'à paraître indétectables. Le cas de Mohamed Lahouaiej-Bouhlel, dont on ne sait pas toujours très bien s'il s'agit d'un déséquilibré qui se cherchait un modèle ultra-violent à imiter, ou d'un véritable djihadiste islamiste radicalisé à une vitesse inédite, laisse songeur. Bisexuel, amant d'un homme de 73 ans, mangeur de porc, aucune connexion connue avec des réseaux islamistes… l'auteur de l'attentat de Nice était connu des services de police pour des faits de violence de droit commun, mais n'avait rien de l'homme que l'on pourrait soupçonner d'organiser une tuerie motivée par des considérations idéologiques.
Or c'est un problème pour les services de renseignement à qui l'on demande désormais l'impossible, à la Minority Report, c'est-à-dire de connaître à l'avance le passage à l'acte d'un individu, pour être capable de l'appréhender avant son méfait, même lorsqu'objectivement rien ne permettait de présager l'horreur.

C'EST POUR ÇA QUE JE SUIS ICI. NOUS SAVONS QU'ISRAËL A DÉVELOPPÉ BEAUCOUP DE MOYENS DANS LE CYBER

Néanmoins, l'Union européenne ne veut pas se résoudre à la fatalité, et va chercher en Israël les méthodes à appliquer pour détecter sur Internet les terroristes susceptibles un jour de passer à l'acte. « C'est un défi », explique ainsi à l'agence Reuters Gilles de Kerchove, le coordinateur de l'UE pour l'anti-terrorisme, en marge d'une conférence sur le renseignement à Tel Aviv. « Nous allons trouver bientôt des moyens d'être beaucoup plus automatisé » dans la détection des profils suspects sur les réseaux sociaux, explique-t-il. « C'est pour ça que je suis ici ».
« Nous savons qu'Israël a développé beaucoup de moyens dans le cyber », pour faire face aux attaques d'Israéliens par des Palestiniens, ajoute le haut fonctionnaire européen, et l'UE veut s'en inspirer.

ÉTABLIR DES PROFILS SOCIOLOGIQUES ET SURVEILLER LES COMMUNICATIONS

Selon un officiel israélien interrogé par l'agence de presse, il s'agit d'établir constamment des profils types de personnes à suspecter, en s'intéressant non plus seulement aux métadonnées qui renseignent sur le contexte des communications et les habitudes d'un individu, mais bien sur le contenu-même des communications sur les réseaux sociaux.
Mis à jour quotidiennement au gré des nouveaux profils qui émergent, des paramètres comme l'âge de l'internaute, sa religion, son origine socio-économique et ses liens avec d'autres suspects, seraient aussi pris en compte par les algorithmes israéliens – ce qui semble difficilement compatible en Europe avec les textes internationaux protégeant les droits de l'homme, que l'Union européenne s'est engagée à respecter.

DES BOÎTES NOIRES TOUJOURS PLUS INTRUSIVES ?

En somme, c'est exactement ce que nous redoutions avec les fameuses boîtes noires permises par la loi Renseignement en France, dont le Conseil constitutionnel n'a su que dire, et qui se limitent officiellement aux métadonnées. Là aussi, il s'agit d'utiliser des algorithmes, dont on ne sait pas du tout sur quoi ils se basent, pour détecter des profils suspects.

Eagle Security & Defense, une société israélienne proposant des solutions de surveillance sur Internet, a reçu la visite de Christian Estrosi en début d'année.
Il n'est toutefois pas dit que la technologie israélienne soit importée telle quelle, d'autant que M. De Kerchove a lui-même rappelé que le droit européen n'autoriserait pas un tel degré d'intrusion dans la vie privée. Mais le mécanisme décrit par l'officiel d'Israël est très proche.
Il vise tout d'abord à réaliser une première détection sommaire des profils suspects, puis à déterminer parmi eux ceux qui doivent faire l'objet d'une surveillance individualisée. C'est exactement ce que prévoit la loi Renseignement, qui autorise l'installation de boîtes noires chez les FAI ou les hébergeurs et éditeurs pour détecter des comportements suspects d'anonymes, avant de permettre une identification des personnes dont il est confirmé qu'elles méritent une attention particulière.
En Israël, le ratio serait d'environ 20 000 personnes considérées suspectes pour 1 million d'internautes, sur lesquelles ressortiraient entre 10 et 15 profils nécessitant une surveillance étroite.

CHRISTIAN ESTROSI DÉJÀ INTÉRESSÉ

L'information de Reuters confirme ce qu'indiquaient Les Échos le week-end dernier dans un reportage bien informé. « L'Etat hébreu, dont la population a connu sept guerres et deux Intifada depuis sa création, est bel est bien devenu un cas d'école, dans sa façon de gérer une situation d'insécurité permanente. Une expertise dans la mire des décideurs européens », écrivait le quotidien,
Il précisait qu'en février dernier, l'ancien maire de Nice et actuel président de la région Provence-Alpes-Côte d'Azur, Christian Estrosi, s'était déjà rendu en Israël, où il aurait rencontré le PDG de la société Eagle Security and Defense, Giora Eiland, qui est aussi ex-directeur du Conseil de sécurité nationale israélien.
Lors de cette visite, Christian Estrosi aurait insisté sur la nécessité « d'être à la pointe de la lutte par le renseignement contre la cybercriminalité lorsqu'on sait que la radicalisation se fait par le biais des réseaux sociaux ». On imagine que cette conversation lui est revenue en mémoire lorsque sa ville a été meurtrie.
Article original de Guillaume Champeau

Réagissez à cet article

Original de l'article mis en page : Détecter les futurs terroristes sur Internet ? LEurope veut sinspirer dIsraël – Politique – Numerama

Le nombre de cyberattaques contre des cibles françaises double chaque année

Le nombre de cyberattaques contre des cibles françaises double chaque année

Le salon international Eurosatory de défense et de sécurité s'ouvre lundi près de Paris alors que les cyberattaques contre des cibles françaises se multiplient.

Le salon international Eurosatory de défense et de sécurité s'installe comme tous les deux ans à partir de lundi à Villepinte, près de Paris. Cette manifestation qui rassemble les stratèges et les industriels du monde entier met de plus en plus l'accent sur deux concepts devenus incontournables : l'utilisation des drones et les outils de la cyberguerre. Une demi-douzaine de conférences se tiendront cette semaine sur la cybermenace et sur les moyens de la contrer ou de la mettre en œuvre. En France, depuis l'adoption du livre blanc 2013 et la loi de programmation militaire 2014-2019, la dimension « cyber » de nos armées « a changé de braquet », comme le confie au *JDD* l'un des meilleurs experts gouvernementaux de ce dossier.

Selon lui, le nombre de cyberattaques contre des cibles françaises double chaque année et le niveau de sophistication des agressions également. « Un individu aujourd'hui peut nous faire autant de mal qu'un État », précise notre source. Chaque jour en France, les unités informatiques liées aux institutions ou aux entreprises du secteur de la défense sont agressées par des milliers d'attaques. Des raids visant à saturer des adresses liées au ministère de la Défense se multiplient et il peut arriver que le compte personnel du ministre soit visé avec intention de nuire. Au point qu'aujourd'hui pas une seule clé USB ne peut entrer dans une installation de défense française sans être passée par une « station blanche » de décontamination.

Détruire sans avoir à bombarder

Mais le plus grand risque serait évidemment que nos unités militaires engagées sur un théâtre d'opérations soient attaquées en pleine action. Le pacte défense cyber lancé début 2014, et renforcé après les attentats de 2015, a prévu un investissement de plus d'un milliard d'euros et le triplement des effectifs militaires et civils concernés. « Aujourd'hui, plus un seul déploiement d'une unité sur le terrain ne se conçoit sans un accompagnement cyber », indique notre source.

Un officier général « cyber » est affecté en permanence auprès de l'état-major au Centre de planification et de conduite des opérations (CPCO). Il ne s'agit pas seulement de se protéger lors d'une attaque mais aussi de se défendre lorsqu'elle est en cours ou même d'attaquer en cas de besoin. Tout comme le fait depuis longtemps Israël contre ses adversaires au Moyen-Orient, l'État hébreu étant avec les États-Unis, la Chine et la Russie l'un des quatre pays les plus avancés dans ce domaine avec des moyens dix à vingt fois plus importants que ceux de la France. Mais on réfléchit à Paris à l'idée de créer une cyberarmée à l'image de l'US Cyber Command américain. Pour se préparer à ces guerres invisibles où l'on peut détruire une installation ennemie sans avoir à la bombarder ou à brouiller ses radars depuis un ordinateur pour mieux déclencher des raids plus… conventionnels.

Article original de François Clemenceau – Le Journal du Dimanche

---

Réagissez à cet article

Original de l'article mis en page : Faut-il investir dans la guerre invisible? – leJDD.fr