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***

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRECCTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

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