Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES ÉTRANGÈRES
ET DU DÉVELOPPEMENT
INTERNATIONAL

Assemblée des
Français de l'étranger

Session de mars 2016

COMPTE RENDU DE LA COMMISSION DE LA SÉCURITÉ ET DE LA PROTECTION DES PERSONNES ET DES BIENS

Président : Bruno DELL'AQUILA
Vice-président : Gérard BENICHOU

MEMBRES ÉLUS

M. BERTE Jean-François
M. HASNAOUI Fwad
Mme LAVERGNE Cécile
M. MAINGUY Jean-Louis
Mme MARTIN Catya
M. PARTY Geoffrey
M. OUEDRAOGO Ousmane
Mme PRATO Régine
M. REGNARD Damien
M. SENAC Gérard
M. SEROL Hervé
Mme VARRIN Françoise

Synthèse des travaux de la Commission
Session de mars 2016

I. Protection des entreprises à l'international

Audition du Préfet Cyrille Schott, directeur de l'Institut National des Hautes Etudes de la Sécurité et de la justice (INHESJ).

Présentation de cet organisme sous la tutelle des ministères de l'Intérieur et de la Justice, rattaché comme l'IHEDN au Premier Ministre.

L'INHESJ:

- assure des formations généralistes (thèmes: sécurité et justice, sécurité des entreprises, intelligence économique, management de crises) ou formations à la demande

- fait de la recherche, organise des colloques et publie diverses revues dont DEFIS

Audition de M. Jean-Louis Kibort, directeur de la sûreté pour la branche Marketing et Services du Groupe Total.

Les crises, désormais permanentes pour ce type de groupes industriels, font de la Sûreté un sujet central qui ne peut plus être géré sur un mode réactif mais doit être anticipé et intégré dans tous les projets.

Ce « management » de la Sûreté est instauré au plus haut niveau et intègre:

- des plans de crises (identification des scénarios possibles, des plans d'actions, contacts, communication, tests et exercices)
- une identification permanente du personnel présent ou en déplacement
- la protection des sites et un audit performant des sous-traitants en gardiennage
- une évaluation permanente des procédures afin d'apporter les correctifs nécessaires.

Audition de M. Pierre Novaro, Président de Salix Security Governance, consultant en Sureté.

En raison de la législation, l'employeur est tenu de protéger au mieux la mobilité de ses collaborateurs.
Il faut donc pour les entreprises:

- connaître au mieux la localisation des employés
- apporter à ceux-ci les consignes de comportements différenciés en fonction des zones géographiques
- pouvoir recevoir les appels d'urgence
- enfin intervenir si besoin

Les sociétés de conseil en sûreté doivent pouvoir fournir des formations et des solutions de façon modulable en fonction de la taille des entreprises, de leurs cultures, des pays et des risques (notamment : cartographie fine des risques selon les pays, qualification des hôtels et des moyens de transport, sensibilisation des voyageurs).

II. Transport Aérien: défis actuels et perspectives

Audition de M. Patrick Rouby, directeur délégué de la Sécurité du Groupe Air France.

Une précision a été faite concernant les notions de Sécurité (absence d'intention de nuire) et de Sûreté (acte ou intervention illicite).
L'intervention de M. Patrick Rouby a permis de saisir la grande complexité de l'analyse des risques liés à la sûreté en raison de la taille de l'entreprise, du pavillon français, du nombre d'escales, avec dans chacune d'elles de nombreux intervenants (aéroports, contrôle aux frontières, sous-traitants) et de nombreux autres paramètres.
Ces risques, et notamment le risque terroriste en raison de son impact médiatique majeur, sont sans cesse évalués, analysés et prévenus, dans un contexte international qui se transforme en permanence mais avec la contrainte de gêner au minimum la fluidité du voyage aérien.

La compagnie, qui doit demeurer en conformité avec les réglementations internationales, européennes et françaises, assure un audit et une surveillance de toutes les escales (et leur environnement au sens large), assure une veille opérationnelle permanente avec tous les services compétents, prépare et active si besoin sa cellule de crise en coordination avec tous les organismes compétents (CdCS, équipes d'intervention).
Les perspectives des futures menaces ont enfin été évoquées, tout comme leur prévention: cyber attaques, explosifs intracorporels, «insiders», missiles, drones et laser.

Toute cette logistique dédiée à la lutte contre les atteintes à la sûreté mobilise en permanence plus de 50 personnes mais **la politique de la compagnie est de ne pas regarder à la dépense dans ce domaine et de faire tout ce qu'elle juge nécessaire en ce domaine** comme en matière de sécurité.

III. Le vote électronique: enjeux, contraintes et risques

Audition de Mme Véronique Cortier directrice de recherche au CNRS, spécialiste de la sécurité.

Notre commission a reçu, en commun avec la commission des lois, Mme Véronique Cortier auteure d'un travail de recherche sur le vote électronique et particulièrement sur les risques pesant sur ce type de scrutin.

Notre intervenante a fait un bref historique du vote: main levée, bulletin secret, voting machine avec cartes perforées et vote électronique qui recouvre deux grandes familles, le vote via des machines à voter dans les bureaux de votes et enfin vote par internet.

Celui-ci a été utilisé tant pour des mandats politiques que pour des mandats professionnels, et nous le savons, à plusieurs reprises pour les votes concernant les Français établis hors de France (Conseillers AFE avant la réforme, Conseillers Consulaires et Législatives).

Pour l'anecdote, ce système de vote est généralisé depuis 2005 en Estonie, alors qu'en Allemagne le système a été essayé et abandonné car jugé inconstitutionnel.

Il est évident que le vote électronique présente une grande avancée dans la vie démocratique des Français de l'Etranger et que cela s'est traduit par une augmentation sensible de la participation.

Néanmoins, cela ne doit pas nous rendre aveugle au risque qui pèse sur ce mode de scrutin.

D’une part, dans l’état actuel de la technologie, il existe toujours un doute possible sur l’identité du votant. D’autre part, le système actuel ne permet pas aux électeurs de suivre le processus de scrutin dans son ensemble, par exemple de constater le nombre de bulletins de vote dans l’urne en cours de vote.

Enfin, le problème le plus important est celui du risque d’une intrusion et d’une manipulation du scrutin. Il existe plusieurs exemples. Il y a quelques temps, un vote électronique organisé pour que les militaires américains puissent participer à des élections, a été piraté et manipulé par une équipe d’étudiants du Michigan. Ce qui est inquiétant, c’est que cela n’aurait jamais été détecté s’ils n’avaient pas, par jeu, fait jouer l’hymne de leur état, le Michigan, sur l’application de vote…. Le vote a été annulé.

Il existe d’autres menaces:

- Le risque de coercition: par exemple dans une même famille, votant sur le même ordinateur, un petit fils peut voter pour sa grand-mère en choisissant le candidat à sa place.
- Le risque plus étendu de vente et d’achat de bulletin de vote. C’est-à-dire que l’on peut vendre son login et son mot de passe à une personne qui votera à notre place. Ce qui n’est pas possible dans un bureau de vote.

Aujourd'hui, les chercheurs, comme Mme Véronique Cortier et son équipe, travaillent au développement de systèmes améliorés. Qu’attendre d’un bon système ?

Il s’agit:

- D’assurer la **confidentialité du vote**.
- D’assurer la **vérifiabilité individuelle** (chaque votant peut vérifier que son bulletin est dans l’urne), la **vérifiabilité universelle** (tout le monde peut vérifier que le résultat correspond aux bulletins dans l’urne) et la **vérifiabilité de légitimité** (tout le monde peut vérifier que les bulletins de vote proviennent de votants légitimes).
- D’assurer une disponibilité 24h/24.

Il faut donc souhaiter que le prochain système qui sera utilisé pour des élections françaises, s’efforce de remplir ces conditions.

IV. La Protection de l'information sensible à l'heure de la Révolution numérique

Audition d'un intervenant de la DGSI

Cet intervenant, spécialiste de la DGSI, nous a sensibilisés à l'ensemble des menaces informatiques qui se nourrissent bien souvent de notre manque de connaissance du sujet. La durée impartie à cet entretien, trop court, ne nous pas permis de balayer l'ensemble des menaces.

Il faut tout d'abord bien comprendre que nous vivons dans un monde connecté très largement dominé par les anglo-saxons, avec lesquels nous ne partageons pas la même vision sur les grands sujets. Notamment, la vision de ce que sont les données personnelles.

Au forum de Davos en 2012, les **données personnelles ont été qualifiées de pétrole du XXIe siècle**. Pour nous Français, il s'agit d'un bien qui nous appartient et qui est, justement, personnel. Mais pour les américains, il s'agit avant tout d'un objet marketing qui peut être commercialisable.

Pour bien illustrer cette idée, sachez que Google a acquis WAZE en 2013 pour 1 milliards de dollars, et Facebook a acquis What's app en 2014 pour 19 milliards de dollars. De quoi s'agissait-il ? Il s'agissait pour eux non seulement d'acquérir des données personnelles, mais aussi et surtout des répertoires. Près de 500 millions de répertoires dans le cas de What's app.

Nous devons bien saisir que la **gratuité est un leurre**. Ce que nous appelons des « freemiums » sont en fait des « pompes à données personnelles ». Avec une devise à retenir, « **si c'est gratuit, vous êtes le produit** ».

Ainsi, il nous faut comprendre et admettre que tout comme pour le pétrole au XXe siècle, certains états, officines, groupements criminels ou simples particuliers, sont et seront prêts à tout pour acquérir nos données personnelles mais aussi nos données professionnelles. Dans ce domaine, 90% d'entre nous font preuve d'une extrême candeur.

Le propos a été illustré par la démonstration de pièges simples pour récupérer des données personnelles ou professionnelles.

En voici quelques-uns:

Avec un logiciel facile d'accès, et alors qu'il était dans le couloir attendant son audition avec notre commission, notre intervenant a récupéré toutes les données de connexion via le wifi de nos « smartphones », portables et autres tablettes. Il nous a ensuite montré, comment, simplement grâce aux données de connexion de nos wifi il pouvait reconstituer tout le trajet suivi par une personne pendant plusieurs jours. Identifiant très précisément les lieux où elle était passée.

Il a également attiré notre attention sur la menace que pouvaient représenter les réseaux sociaux en nous donnant l'exemple de Robin Sage qui a fait beaucoup de bruit aux Etats-Unis. Mlle Sage, scientifique avenante de haut niveau dans le domaine de la défense, s'est constitué un réseau avec d'autres spécialistes de la défense et a bientôt échangé des informations professionnelles. Jusqu'au jour où quelques-uns ont commencé à se demander qui était vraiment Robin Sage et ce sont rendu compte qu'il s'agissait d'une équipe de spécialistes de l'informatique voulant démontrer les arnaques possibles par les réseaux sociaux…

L'intervenant de la DGSI nous a ensuite montré les nombreuses menaces pesant sur les entreprises en illustrant le fait que le point de faiblesse était souvent l'ignorance des employés qui sont les cibles de choix des pirates. Pour vous donner une idée, le piratage de TV5 monde par le pseu-

do « Cyber Caliphat » a couté 5 millions d'euros à la chaine. Il faut savoir que 90% des sociétés ayant subi des attaques informatiques disparaissent dans les deux ans.

Enfin, afin d'illustrer que les objets les plus simples peuvent s'avérer les plus dangereux, notre intervenant nous a invité à la plus grande méfiance avec les clefs USB. Il nous a montré comment une simple clef pouvait, à notre insu, installer des documents et/ou lancer des commandes sur nos ordinateurs. Nous montrant également que de simples programmes, gratuits, permettent de récupérer facilement des données que nous avions effacées ou formatées… Le seul moyen de les faire disparaitre véritablement étant l'utilisation de logiciels spécialisés.

Nous avons vu qu'il s'agit là d'un sujet vaste, aux exemples nombreux.

Notre commission pense qu'il y a là un véritable travail d'information et d'illustration à faire auprès de tous nos compatriotes vivant à l'étranger. De par leur situation ou les intérêts qu'ils représentent, ce sont des cibles de choix pour les pirates informatiques.

Nous voyons là un véritable sujet à creuser, ce que nous comptons faire dans les cessions à venir.

Pour le moment, nous vous invitons à consulter le site de l'ANSI (Agence Nationale de Sécurité Informatique) qui est justement fait pour promouvoir les bonnes pratiques permettant non pas d'effacer la menace, mais de la réduire.

V. Centre de crise et de Soutien (CdCS)

Monsieur Didier Canesse, Directeur adjoint du CdCS

M. Didier Canesse nous a rappelé les fonctions du CdCS: la **veille**, la prévention avec **l'information** de nos ressortissants sur les risques et les menaces auxquels ils peuvent être exposés au travers de **fiches conseils aux voyageurs** avec des informations pratiques pour aider nos ressortissants à organiser leur séjour à l'étranger mais aussi à partir d'une fiche sécuritaire comportant des cartes pour une meilleure visibilité.
L'analyse pour constituer ces fiches est fondée sur les informations des postes consulaires et d'autres sources, notamment des services de renseignement. Le CdCS peut donc faire l'objet de pressions en direct via les ambassades des pays concernés en France. C'est pourquoi, en aucun cas les conseils aux voyageurs doivent être lus comme un baromètre des relations bilatérales de la France avec les pays concernés.

Les informations du CdCS peuvent aussi aider certains pays à relever leur garde en matière de sécurité et mais aussi, à l'inverse, les inciter à faire des efforts en terme de sécurité pour les voyageurs dans leur pays.

Autre mesure d'information : **le portail « ARIANE** » permet aux voyageurs de s'inscrire avant leur départ avec toutes les informations les concernant. Ce portail n'est pas suffisamment connu des voyageurs. Il serait bon d'accentuer la communication auprès de nos concitoyens à l'étranger, pour cela les élus consulaires peuvent servir de relais auprès des français installés à l'étranger.

Nouvelles actions du CdCS:

- **Page spéciale pour les voyageurs d'affaires** avec des données économiques de base.
- **Depuis peu, le CdCS a développé un réseau avec les entreprises** françaises basées sur des lieux à risques. Il fournit des conseils soit en direct, soit par visio-conférences avec des experts.

C'est l'occasion d'un échange mutuellement avantageux. Les entreprises sont une bonne source d'informations car elles ont des capteurs, dans des régions où nos ambassades ne sont pas forcément présentes.

Un autre service est proposé aux entreprises avec des **missions de sécurité sur mesure**.
Toutes les entreprises peuvent saisir le CdCS quelle que soit sa taille pour obtenir ces conseils. Pour les PME/TPE qui, n'ayant pas les moyens de se fournir les services d'une société d'analyses stratégiques, ce service est gratuit et fiable.
La mission du CdCS s'arrête aux conseils leur permettant de prendre des décisions raisonnées sans intervenir dans la décision finale qui reste à l'entreprise.

Une des préoccupations constantes du CdCS est aujourd'hui la prévention des prises d'otages. C'est l'intérêt des formations auprès de personnes voulant se rendre en zones à risques, ONG, journalistes (notamment indépendants).
Il peut intervenir en réaction à des alertes communiquées par des services de renseignement qui auraient identifiés des risques. C'est un travail continu du CdCS.

Après la veille et le conseil, le CdCS organise de la préparation aux crises.
Aujourd'hui toutes nos ambassades doivent avoir un plan de sécurité tenu à jour. Le CdCS supervise ce travail et note les différentes lacunes qu'il signale aux ambassadeurs.

Un **effort de formation** est également mis en place avant le départ en poste pour les ambassadeurs, Consuls Généraux et n°2. Le volet formation à la gestion de crise a pris beaucoup d'importance dans ce programme de formation avant le départ en poste.

Le CdCS a également renforcé ses **actions de formation directement dans les postes diplomatiques** avec cinq à six missions par an. Tout est passé en revue et la formation se termine par un exercice « joué » localement.

Un nouveau concept a été développé depuis l'année dernière, suite aux événements au Népal, où il y avait une double crise, humanitaire et consulaire, frappant une toute petite ambassade avec peu de ressources. Des renforts ont donc été déployés rapidement venant de Delhi et du CdCS.

L'enseignement tiré est qu'il **est utile d'avoir un réseau de postes d'appui régionaux permettant de fournir, dans l'urgence, le premier échelon de renforts pour des petits postes à faibles ressources humaines**. Le CdCS a donc créé ce réseau via les grandes ambassades (Mexico, Brasilia, Delhi, Cambera, Moscou, Dakar, Addis Abeba et Johannesburg). Ces postes tiennent en permanence un vivier d'agents prêts à partir en renfort sous 24h au service d'une ambassade de leur région.

Chantier en cours depuis plusieurs mois : développement du géo-référencement qui reste pour l'instant un outil d'aide à la décision. Plusieurs postes ont développé ce genre de programme.

<u>Réponses aux crises :</u>

Le CdCS a compétence pour assurer le pilotage de la réponse globale de la France aux crises humanitaires et aux crises à l'étranger.

<u>Constat :</u>

Il y a une augmentation continue du nombre de crises dans le monde et du nombre de victimes françaises.

VI. Le renseignement, son évolution et les réformes en France par rapport à la menace, depuis les attentats islamistes de1995 à aujourd'hui.

Audition du Préfet Bernard Squarcini, consultant indépendant. Kyrnos Conseil.

Avant les années 70, les guerres des Services reflétaient classiquement un affrontement à distance entre autorités régaliennes auxquelles ont succédé dans les années 70 un terrorisme de l'ultra gauche et de l'ultra droite, rapidement suivi par les mouvements séparatistes (IRA et ETA).

Mais bientôt, à la suite des élections en Algérie, le terrorisme dû au fondamentalisme religieux nous a atteint (détournement de l'Airbus d'Air France et attentat du métro St Michel en 1995).
La progression rapide des réseaux du GIA puis du groupe Salafiste pour la prédication et le combat, a pu être en son temps bien canalisée (plus de 450 personnes incarcérées).
Mais bientôt apparait Al-Qaïda, puis Daech. La déliquescence de plusieurs pays à la suite du « Printemps Arabe » qui a entrainé la disparition ou la perte de contact avec les services de ces pays, et la mainmise sur d'importants stocks d'armes par divers groupes, mais également la contamination de l'Afrique noire, n'ont rien arrangé tandis que sur le sol national s'effectuait le recrutement d'islamistes dans les mosquées et la radicalisation favorisée par internet.

Enfin l'implication de la France dans la lutte contre Daech en Irak et en Syrie fait que pèse désormais sur nous une double menace à un niveau jamais atteint, en France comme à l'étranger.
Les attentats de janvier et novembre 2015 sont encore dans notre mémoire et nos cœurs.

Pour contrer cette menace qui a augmenté en quantité et efficacité, une réforme a été entreprise:

- avec l'unification du renseignement intérieur (DGSI),
- la création d'un coordonateur National du renseignement auprès du Président de la République.
- l'achat de matériel informatique ad hoc,
- le recrutement massif d'analystes
- la création de nouvelles qualifications d'infractions (terrorisme, retour du Djihad)
- et une loi sur le renseignement (permettant notamment les « opérations spéciales ») qui ne prend effet que ces temps-ci avec malheureusement presque trois ans de retard.

Enfin dorénavant les Services travaillent en commun avec les forces armées car il faut aller chercher à l'étranger ceux qui arment ou qui vont venir faire les attentats.

Malheureusement, en raison de la propagation du fanatisme, il nous faut apprendre à vivre autrement car cela va durer longtemps.

Assemblée des Français de l'Etranger
24ème session

Paris, le 17 mars 2016

Résolution de la
Commission de la sécurité et de la protection des personnes et des biens

Résolution : SEC/R.1/ /16.03

Objet : Modification du guide « Être victime à l'Etranger : Conseils, Démarches et Droits »

L'Assemblée des Français de l'Étranger,

Considérant :

- L'augmentation importante des agressions sexuelles envers nos compatriotes à l'étranger.
- Que le Guide « Être victime à l'Étranger: Conseils, Démarches, et Droits », disponible sur le site internet France Diplomatie dans son paragraphe intitulé « en cas d'agression sexuelle » ne stipule pas un accompagnement médical, juridique et psychologique à travers le poste consulaire.

Demande :

- Une nouvelle formulation de ce paragraphe pour une meilleure implication des services consulaires dans l'aide et l'assistance aux victimes.

Résultat	Adoption en Commission	Adoption en Séance
UNANIMITÉ		X
Nombre de voix « pour »	13	
Nombre de voix « contre »	1	
Nombre d'abstentions		

Réponse