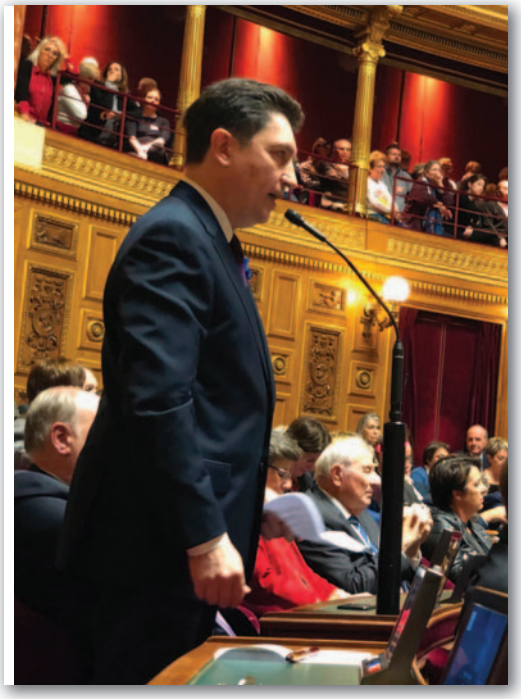
DANS QUEL MONDE VOULONS-NOUS VIVRE EN 2050 ?



Interview d'Olivier Cadic, sénateur des Français établis hors de France*
Par Marc Jacob et Emmanuelle Lamandé

Le 5 décembre 2018, la plateforme de service ARIANE du ministère de l'Europe et des Affaires étrangères (MEAE) a été victime d'une cyberattaque qui a conduit à une fuite de données concernant environ 500 000 personnes. Le sénateur Olivier Cadic fait le point sur cette attaque et plus largement sur la politique de cyberdéfense de la France.

Global Security Mag : Il y a moins d'un an, votre commission a lancé un audit suite à une cyberattaque réussie contre le ministère de l'Europe et des Affaires étrangères. Que s'est-il passé ?

Olivier Cadic : Le 5 décembre 2018, la plateforme de service ARIANE du ministère de l'Europe et des Affaires Étrangères (MEAE) a été victime d'une cyberattaque. Ce service permet aux ressortissants français qui s'inscrivent en ligne de recevoir des consignes de sécurité, lors de leurs voyages à l'étranger. Des données personnelles enregistrées lors de l'inscription sur la plateforme ont été dérobées. Plus de 500 000 personnes étaient concernées.
Nous avons auditionné le directeur général de l'ANSSI, le directeur des systèmes d'information et le directeur de la sécurité diplomatique du MEAE, la direction générale de la sécurité intérieure (DGSI), qui est l'un des services disposant des capacités d'investigation pour rechercher l'origine d'une cyberattaque, la CNIL et, enfin, la section spécialisée du parquet de Paris.
L'objectif de cette mission d'information, au-delà de la mise à jour de lacunes et d'insuffisances dans les procédures et les modes de fonctionnement, est d'inciter les administrations de l'État à améliorer leur résilience en favorisant l'émergence en leur sein d'une culture de la cybersécurité, en affectant les moyens nécessaires à la protection de leurs systèmes d'information et en garantissant, en cas de crise, la fluidité des relations entre les différents acteurs de la prévention et de la protection (ANSSI, DSI des ministères, CNIL), mais aussi de la judiciarisation.
Nous avons patiemment déroulé le fil de la cyberattaque d'ARIANE pour comprendre comment le MEAE avait réagi et quels enseignements il pouvait en tirer pour renforcer sa résilience.
Plusieurs recommandations à l'attention du gouvernement ont pu être formulées [1].

GS Mag : Pourquoi avoir lancé cet audit suite à cette cyberattaque en particulier ?

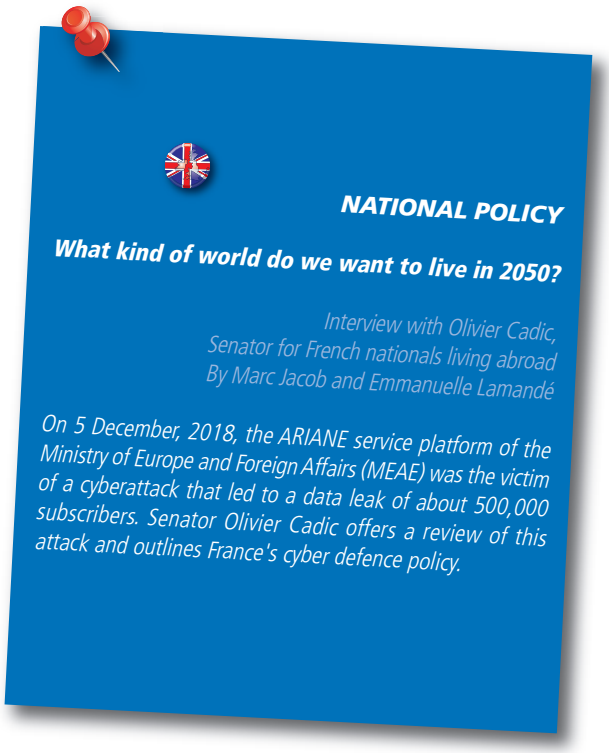
Olivier Cadic : Depuis trois ans, les avis budgétaires de notre commission sur le programme 129 « Coordination du travail gouvernemental », qui porte les crédits de l'ANSSI, soulignaient les résultats insuffisants de la mise en œuvre de la Politique de Protection et de Sécurité des Systèmes d'Information de l'État (PSSIE).
En outre, cette cyberattaque affectait un ministère sur lequel la commission était pleinement légitime à assurer un contrôle. Elle démontrait que nos craintes étaient justifiées.
Le MEAE bénéficie d'un niveau de protection élevé. Il n'a pas empêché la survenue d'une cyberattaque visant un système ouvert sur l'Internet. Les attaquants ont profité d'une faille dans une brique logicielle utilisée pour construire cette plateforme. L'éditeur du logiciel avait identifié cette faille et livré à la DSI du MEAE le correctif nécessaire. La mise à jour n'avait pas encore été installée. En l'espèce, cette mise à jour n'avait pas été considérée comme une absolue priorité. Les assaillants ont su habilement profiter de cette vulnérabilité.

LE MEAE CONSACRE DES MOYENS GLOBALEMENT INSUFFISANTS À LA CYBERSÉCURITÉ

GS Mag : Quels enseignements en avez-vous tiré ?

Olivier Cadic : Nous avons tiré cinq principaux enseignements :
- Premièrement, si quelques attaquants connaissent les failles, l'édition d'un correctif en révèle plus largement l'existence et suscite des appétits. Plus on tarde à installer une mise à jour, plus un Système d'Information est vulnérable.

- Deuxièmement, comme d'autres ministères, le MEAE consacre des moyens globalement insuffisants à la cybersécurité et concentre ceux-ci sur les systèmes d'information et de communication les plus stratégiques, comme la sécurité des postes et des réseaux diplomatiques.
- Troisièmement, il importe d'anticiper les vacances de postes et d'assurer une redondance, afin d'éviter une éventuelle vacance durant la phase de recrutement de postes au niveau de la chaîne de sécurité placée sous la responsabilité du Haut fonctionnaire de défense et de sécurité.
- Quatrièmement, la circulaire interministérielle du 17 juillet 2014 sur la Politique de Sécurité des Systèmes d'Information de l'État (PSSIE) est appliquée de façon hétérogène. Cela démontre le caractère très limité des interventions réglementaires : sans affectation de moyens, elles risquent de demeurer un seul instrument de communication.
- Cinquièmement, tout cela pose concrètement la question d'un pilotage interministériel par affectation de moyens, notamment par le respect d'un ratio obligatoire consacré à la cybersécurité. L'ANSSI n'a pas aujourd'hui de telles capacités.



EN 2018, L'ANSSI A TRAITÉ 78 ÉVÉNEMENTS DE SÉCURITÉ AYANT TOUCHÉ DES MINISTÈRES FRANÇAIS

GS Mag : Quel état faites-vous aujourd'hui de la menace ?

Olivier Cadic : Les attaquants informatiques poursuivent quatre types d'objectifs non exclusifs entre eux : l'espionnage, les trafics illicites, la déstabilisation et le sabotage.
Les ministères les plus attaqués sont dans l'ordre l'Éducation nationale, la Défense et les Affaires étrangères. Mais en intensité ce sont les ministères des Armées et des Affaires étrangères qui ont été les plus menacés.
Afin de mesurer concrètement la vulnérabilité des administrations de l'État aux cyberattaques, nous avons demandé la communication, par ministère, du nombre d'incidents consécutifs à des cyberattaques ayant fait l'objet d'une intervention de l'ANSSI (cf. tableau).
En 2018, l'ANSSI a été amenée à traiter 78 événements de sécurité consécutifs à des attaques informatiques ayant touché des ministères français.
15 d'entre eux se sont avérés majeurs, nécessitant pour leur traitement une expertise et un engagement important sur le moyen/long terme de la part de l'ANSSI (trois d'entre eux ont d'ailleurs fait l'objet d'une opération de cyberdéfense).
32 peuvent être qualifiés de notables, puisque demandant l'emploi d'expertises particulières pour leur résolution, tandis que 31 se sont révélés mineurs.
Au sein du ministère des Armées, le commandement de la cyberdéfense (COMCYBER), créé en 2017, assure la détection des attaques informatiques sur l'essentiel des systèmes ministériels. En 2018, ce ministère a traité 19 incidents, dont 4 en collaboration avec l'ANSSI.
Nous avons proposé à la commission que ces données soient désormais suivies annuellement.

TABLEAU DU NOMBRE D'INCIDENTS, PAR MINISTÈRE, CONSÉCUTIFS À DES ATTAQUES INFORMATIQUES

Ministères	Incidents traités par l'ANSSI	Commentaires
Ministère de l'Agriculture et de l'Alimentation	6	Dont un incident majeur
Ministère de la Cohésion des territoires	1	
Ministère de la Culture	4	
Ministère des Armées	4	Dont deux incidents majeurs
Ministère de l'Économie et des Finances	9	Dont deux incidents majeurs
Ministère de l'Éducation nationale et de la Jeunesse	24	Dont un incident majeur
Ministère de l'Enseignement supérieur et de la Recherche	2	
Ministère de l'Europe et des Affaires étrangères	11	Dont trois opérations de cyberdéfense et quatre incidents majeurs
Ministère de l'Intérieur	9	Dont deux incidents majeurs
Ministère de la Justice	8	Dont trois incidents majeurs
Ministère des Outre-Mer	1	
Ministère des Solidarités et de la Santé	8	Dont deux incidents majeurs
Ministère de la Transition écologique et solidaire	3	
Ministère du Travail	1	

Sources : Réponses au questionnaire parlementaire

LA DICTATURE 2.0 CHINOISE UTILISE SES « ROUTES DE LA SOIE » POUR TENTER DE PRENDRE LE CONTRÔLE DE PAYS

GS Mag : Vous faites de nombreuses conférences à l'international sur la cybersécurité, quel est le message que vous faites passer ?

Olivier Cadic : Le cyberespace est devenu un milieu de confrontation permanent pour les États ou les organisations non gouvernementales. Chaque ordinateur, chaque smartphone, chaque objet connecté peut être non seulement une cible, mais également le vecteur de cyberattaques, à l'insu même de son propriétaire.

Si nous voulons lutter contre l'espionnage, pouvons-nous accepter qu'un fabricant de télécommunications chinois équipe nos véhicules automobiles du système e-call, afin d'appeler les secours en cas d'accident, tout en sachant que cela permet à la Chine de savoir où on va, avec qui, et ce que nous nous disons ?

La Chine se définit comme un « État socialiste de dictature démocratique populaire ». Sa maîtrise de la technologie lui a permis de créer un cyber-mur pour imposer un contrôle social de sa population en combinant réseaux sociaux, caméras à reconnaissance faciale et intelligence artificielle.
Cette dictature 2.0 utilise ses « Routes de la soie » pour tenter de prendre subrepticement le contrôle de pays en liant son aide à la signature de contrats d'équipements technologiques. Ses progrès sont spectaculaires.
Elle constitue désormais la principale menace pour les démocraties. La confrontation est inéluctable si nous ne redressons pas la barre.

Pour être maître de notre destin, nous devons nous donner les moyens technologiques de nous défendre et être indépendants.
Les constructeurs européens n'ont que très peu de chance de rivaliser avec leurs concurrents chinois tant que l'accès au marché chinois leur est interdit.
La question essentielle pour nous aujourd'hui est de déterminer dans quel monde nous voulons vivre en 2050. Cela conditionnera tout le reste. ■■■

[1] http://www.senat.fr/notice-rapport/2018/r18-299-notice.html

* Olivier Cadic, sénateur des Français établis hors de France (groupe Union Centriste), est secrétaire de la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat, et co-rapporteur des crédits du SGDSN (en charge de la Politique de Sécurité des Systèmes d'Information de l'État) et de l'ANSSI.