LA FRANCE S'ACCORDE DES MOYENS EN HAUSSE FACE À UNE MENACE CYBER QUI EXPLOSE !

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

En octobre dernier, le sénateur Olivier Cadic (UC - Français établis hors de France) a été élu vice-président de la commission des affaires étrangères, de la défense et des forces armées du Sénat, et reconduit pour 3 nouvelles années comme co-rapporteur des crédits du SGDSN (en charge de la politique de sécurité des Systèmes d'Information de l'État) et de l'ANSSI. L'occasion de faire le point sur ses activités, mais aussi sur l'état de la menace cyber en France.

Global Security Mag : Quel état faites-vous aujourd'hui de la menace cyber dans notre pays ?

Olivier Cadic : Avec l'évolution technologique et la généralisation des usages du numérique, la menace cyber ne cesse de se développer sous diverses formes.

La cybercriminalité s'est beaucoup professionnalisée, je dirais même industrialisée. Elle se développe à grande échelle grâce à des « rançongiciels » de plus en plus performants. Les chiffres cités par le directeur de l'ANSSI sont particulièrement frappants : 128 attaques par rançongiciels traitées par l'agence au 30 septembre 2020, contre 54 sur l'ensemble de 2019 !
Pour les cybercriminels, c'est un moyen facile de gagner de l'argent et même une manière de capter des devises étrangères pour des « États voyous » !
Les organismes publics et les opérateurs critiques, comme les hôpitaux, ne sont désormais plus épargnés et l'on voit se multiplier les attaques contre les collectivités territoriales, qui commencent tout juste à prendre la mesure du problème.

Risque plus classique, l'espionnage tend lui aussi à augmenter, avec comme objectifs la recherche d'informations stratégiques sur les politiques extérieures et de défense, mais aussi l'accès aux informations industrielles et secrets commerciaux, ainsi que le vol de données personnelles. En ouvrant des brèches dans les systèmes, le télétravail pourrait fournir de nouvelles facilités aux attaquants. Il est impératif de travailler à la sécurisation et à la robustesse des outils de travail à distance.

Les actes de piratage et de sabotage se développent eux aussi, particulièrement contre les institutions et administrations publiques. Ils émanent de cyberactivistes aux motivations idéologiques ou de cybergroupes à la main de puissances étrangères.

EN 2019, L'ANSSI A TRAITÉ 81 INCIDENTS DE SÉCURITÉ NUMÉRIQUE AYANT AFFECTÉ DES MINISTÈRES FRANÇAIS

Sur l'année 2019, l'ANSSI a été amenée à traiter 81 incidents de sécurité numérique ayant affecté les ministères français, un chiffre en légère progression (+3%) par rapport à l'année précédente (Cf tableau ci-contre).

Pour sa part, le ministère des Armées assure lui-même, via le commandement de la cyberdéfense (COMCYBER) la détection des attaques informatiques sur ses propres Systèmes d'Information. Il a traité 88 événements en 2019, contre 13 en 2018. À nos yeux, cette forte augmentation démontre une amélioration de la capacité de détection. N'oublions pas qu'il n'a été créé qu'en 2017.

Je finirai enfin par les cybermenaces qui visent notre démocratie. Les actions insidieuses qui transitent par les réseaux – manipulations, désinformation, propagande – sont de plus en plus utilisées par l'ennemi. Celles-ci présentent un grand potentiel de mobilisation en vue de déclencher des opérations terroristes ou de déstabiliser nos sociétés. Il s'agit d'une menace très grave, qu'il nous faut aussi prendre en compte.

Nombre d'incidents, par ministère, consécutifs à des attaques informatiques, traités par l'ANSSI en 2019

Ministères	Nombre d'incidents traités par l'ANSSI	Commentaires
Ministère de l'Agriculture et de l'Alimentation	8	Dont un incident majeur
Ministère de la Cohésion des territoires	1	
Ministère de la Culture	6	
Ministère des Armées	21	
Ministère de l'Économie, des Finances et de la Relance	11	
Ministère de l'Éducation nationale, de la Jeunesse et des Sports	22	
Ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation	1	
Ministère de l'Europe et des Affaires étrangères	14	
Ministère de l'Intérieur	14	
Ministère de la Justice	6	Dont une opération de cyberdéfense
Ministère des Outre-Mer	1	
Ministère des Solidarités et de la Santé	3	
Ministère de la Transition écologique	8	
Ministère du Travail, de l'Emploi et de l'Insertion	7	

« DÉSINFORMATION, CYBERATTAQUES, CYBERMALVEILLANCE : L'AUTRE GUERRE DU COVID-19 »

GS Mag : Vous avez publié en mai dernier un rapport intitulé : « Désinformation, cyberattaques, cybermalveillance : l'autre guerre du COVID-19 » [1]. Quels en sont les principaux enseignements ?

Olivier Cadic : Oui, nous avons voulu réagir vite en lançant plusieurs auditions avec mon collègue Rachel Mazuir, car la crise sanitaire a favorisé le déploiement de stratégies d'influence par certaines puissances étrangères et accru l'exposition au risque informatique. Notre rapport qui comporte 5 recommandations se veut alarmant et a placé la désinformation au premier plan.

La crise a, en effet, enclenché une guerre de la communication entretenue par certaines puissances étrangères. Ainsi, comme chacun a pu l'observer sur le site de l'ambassade de Chine à Paris, celle-ci distille des informations inexactes ou tronquées, afin de se prévaloir d'un succès contre la pandémie ou de montrer son caractère indispensable dans la lutte mondiale, grâce à la fourniture de produits sanitaires.

Nous avons également souligné que la Russie se montre active en Afrique pour dénigrer la présence française et critiquer ses initiatives. Se diffusent également sur ce continent des rumeurs et fausses informations attribuant la responsabilité de l'épidémie ou ses conséquences aux Français et aux Occidentaux, plus généralement. Cette semaine, dans « Jeune Afrique », le Président de la République l'a confirmé en dénonçant la désinformation menée en Afrique contre les forces et les intérêts français venant de la Russie et de la Turquie.

Nous sommes arrivés à la conclusion qu'il faut d'urgence que notre gouvernement instaure une force de réaction « cyber » pour lutter contre les campagnes de désinformation ou d'influence d'États totalitaires ou autoritaires qui s'en prennent aux démocraties. Car sinon « La dictature peut s'installer sans bruit », écrivait George Orwell.

NATIONAL POLICY

To counter a rocketing level of cyber threats France is boosting its resources!

Interview with Olivier Cadic, Senator for French citizens living abroad
By Marc Jacob and Emmanuelle Lamandé

Last October, Senator Olivier Cadic (UC - French citizens living abroad) was elected vice-chairman of the foreign affairs, defense and armed forces committee of the Senate, and reappointed for another 3 years at the SGDSN (responsible for the security policy of Information Systems of the State) as co-rapporteur of the budget, and at ANSSI. An opportune time then for us to review and provide an update on his activities and on the state of cyber threats in France.

Recommandations du rapport : « Désinformation, cyberattaques, cybermalveillance : l'autre guerre du COVID-19 »

1 - Mettre en œuvre une force de réaction cyber, afin de répondre aux fausses informations dans le domaine sanitaire, aux attaques contre les valeurs démocratiques et de lutter contre les campagnes de désinformation ou d'influence de certains acteurs étrangers ;
2 - Investir dans la sécurité informatique des acteurs de la santé ;
3 - Lancer sans tarder une campagne de communication à grande échelle pour promouvoir la plateforme cybermalveillance.gouv.fr [2] et diffuser les « gestes barrière numériques » ;
4 - Initier une communication régulière, au travers des médias, d'un top 10 des cyber-crimes constatés sur le territoire ;
5 - Unifier la chaîne de recueil et de traitement des plaintes en ligne, aujourd'hui de la compétence des autorités de police et de gendarmerie locales.

5G : 157 DEMANDES ONT ÉTÉ DÉPOSÉES AUPRÈS DE L'ANSSI EN 2020

GS Mag : Dès janvier 2019, vous aviez interpellé le ministre Jean-Yves Le Drian sur les risques que Huawei faisait courir pour notre sécurité dans le domaine de la 5G. Où en sommes-nous ?

Olivier Cadic : La commercialisation des offres 5G en France est imminente. Avec mon collègue Mickaël Vallet, nous avons fait le point sur l'application de la loi du 1er août 2019 relative à la sécurité des réseaux mobiles de 5ème génération. Cette loi confie à l'ANSSI le soin de délivrer aux opérateurs télécoms, sur la base d'une évaluation des risques et pour une durée limitée dans le temps, les autorisations d'utiliser des équipements destinés à constituer leurs réseaux.

L'exigence de continuité de ces réseaux est hautement stratégique. En effet, la 5G va permettre un nouveau bond dans le développement des usages numériques, notamment pour les entreprises. Il est donc essentiel que les opérateurs de télécommunications utilisent des équipements sûrs et non susceptibles de subir des interruptions de services. Or, un tel risque ne peut être exclu lorsque les équipements proviennent d'une entreprise comme Huawei soumise aux lois de son pays et aux pressions de ses gouvernants.
L'hypothèse d'un acte offensif étranger qui emprunterait ce canal doit donc être prise en compte. Il s'agit d'une menace majeure pour notre sécurité qui est avérée et qui ne fait plus débat.

Pour autant, le gouvernement a voulu tenir compte de l'équilibre du marché et de la situation des opérateurs de télécoms qui ne recourent pas tous aux mêmes fournisseurs.
Dans le courant de l'année 2020, les quatre opérateurs français de télécommunications ont déposé 157 demandes auprès de l'ANSSI, portant sur près de 65 000 équipements, essentiellement des antennes destinées aux zones urbaines. Environ la moitié de ces demandes (82) a donné lieu à une autorisation pour la durée maximale prévue par la loi, soit 8 ans ; un tiers (53) a donné lieu à une autorisation pour une durée inférieure à la durée maximale et 22 ont fait l'objet d'un refus. Toutes les décisions de refus et toutes les autorisations pour des durées réduites ont concerné des équipements Huawei.

CYBERSÉCURITÉ : DES PROGRÈS CONSIDÉRABLES ONT ÉTÉ ACCOMPLIS DEPUIS DIX ANS SOUS L'ÉGIDE DE L'ANSSI

GS Mag : Pour conclure, estimez-vous que la France fait des efforts suffisants en matière de cybersécurité ?

Olivier Cadic : L'augmentation des crédits soumis à notre examen dans ce domaine est le signe que cet enjeu important est bien pris en compte par le Gouvernement.
Connue comme le « pompier du cyber » pour ses interventions en cas de cyberattaques, l'ANSSI est avant tout chargée de préparer l'État et les opérateurs critiques à la menace, et de renforcer leur protection et leur résilience.
En 2021, l'Agence rejoindra le Campus Cyber qui va regrouper sur un même site, dans le quartier de la Défense, divers acteurs du secteur cyber. Je me félicite que l'ANSSI participe à ce projet phare, qui vise à permettre la structuration d'un « écosystème français de la cybersécurité ».

2021 permettra également l'installation d'une antenne de l'ANSSI à Rennes dans le cadre de la constitution d'un pôle de compétences en cyberdéfense, où est présent le ministère des Armées, à l'image de ce que j'ai pu observer à Beer Sheva en Israël. Celle-ci aura une capacité d'accueil de 200 agents.
Au final, des progrès considérables ont été accomplis depuis dix ans sous l'égide de l'ANSSI en termes de cybersécurité.

Face à une menace cyber qui ne cesse de se renforcer, nous sommes entraînés dans une course de vitesse. La France fait partie des pays « du premier cercle ». Notre compétence est reconnue et respectée. Cela devrait nous réjouir, même si chacun sait qu'en ce domaine, il faut toujours faire preuve d'humilité ! ■■■

[1] http://www.senat.fr/fileadmin/Fichiers/Images/commission/affaires_etrangeres/Coronavirus_suivi/4_pages_-_CYBER_vedf160420-2_01.pdf
[2] https://www.cybermalveillance.gouv.fr/