VIGINUM, UNE AVANCÉE MAJEURE CONTRE LA DÉSINFORMATION

Interview d'Olivier Cadic, sénateur des Français établis hors de France [1]
Par Marc Jacob et Emmanuelle Lamandé

En 2022, le programme 129 [2] prévoit le financement de nouvelles missions, à commencer par VIGINUM. Cette nouvelle agence gouvernementale aura pour mission de détecter les opérations de désinformation sur les plateformes en ligne et d'en informer les pouvoirs publics. Pour le Sénateur Olivier Cadic, la mise en place de ce nouveau service représente une avancée majeure contre la désinformation, surtout à quelques mois de l'élection présidentielle.

Global Security Mag : Vous êtes co-rapporteur avec le sénateur Mickaël Vallet pour avis des budgets alloués au programme 129 consacré au financement du SGDSN et de l'ANSSI [2]. Quelles sont vos observations concernant ce programme dans le PLF 2022 ?

Olivier Cadic : En 2022, le programme 129 prévoit le financement de nouvelles missions, en particulier le nouveau service à compétence nationale VIGINUM. Il s'agit d'une nouvelle agence gouvernementale, dont nous saluons la création, qui aura pour mission de détecter les opérations de désinformation sur les plateformes en ligne et d'en informer les pouvoirs publics. VIGINUM est appelé à jouer un rôle important pendant les périodes électorales en fournissant toute information utile au Conseil supérieur de l'audiovisuel, au Conseil constitutionnel et à la commission nationale de contrôle de la campagne électorale.

La mise en place de ce service, à quelques mois de l'élection présidentielle, était plus que nécessaire, car nous le savons, à la lumière de ce qui s'est passé en France pendant la campagne de 2017, mais aussi chez un certain nombre de pays amis, les périodes électorales se prêtent particulièrement aux tentatives d'ingérence et de déstabilisation par les puissances hostiles aux démocraties.

Dès 2022, VIGINUM comprendra une cinquantaine d'agents, recrutés dans les domaines des technologies des réseaux sociaux, des sciences humaines et sociales, de la géopolitique et du big data, ayant déjà de l'expérience en matière de recherche des menaces sur Internet.

VIGINUM VIENT COMPLÉTER LE DISPOSITIF *ANTI-FAKE NEWS*

En 2020, dans un rapport intitulé « Désinformation, cyberattaques et cybermalveillance, l'autre guerre du Covid-19 », avec mon collègue Rachel Mazuir, nous avions appelé à la mise en place d'une « force de réaction rapide » contre les fausses informations. La création de cette structure, en faveur de laquelle nous plaidons depuis des années, est une avancée importante qui, après le vote de la loi de décembre 2018 contre la manipulation de l'information, complète notre dispositif *anti-fake news*.

Nous regrettons cependant une certaine timidité dans l'approche. En effet, VIGINUM n'aura pas la charge de la réaction aux campagnes de désinformation. Il nous semble au contraire indispensable que cette structure joue à terme un rôle moteur dans le pilotage de la réponse à apporter à ces attaques hybrides, même si bien entendu, elle n'en serait pas chargée seule.
Elle pourrait ainsi proposer au Gouvernement des modalités de réponse à certaines attaques, comme bloquer le site d'une ambassade étrangère diffusant de fausses informations. C'est, de mon point de vue, ce qui aurait dû être pratiqué l'an dernier pour le site de l'ambassade de Chine, lorsqu'il a circulé une fausse information concernant nos Ehpad au plus fort de la crise inhérente au Covid-19.

« FACT-CHECKING » : L'EXPÉRIENCE TAIWANAISE, SOURCE D'INSPIRATION

Je reviens de Taiwan où je me suis rendu avec une délégation sénatoriale en octobre dernier. Nous avons constaté une approche très intéressante sur la manière d'aborder les actions liées à la désinformation et à la propagation de « fake-news » par la Chine continentale : les autorités taiwanaises ont mis en place une organisation de « fact-checking » qui permet d'expliquer une fausse nouvelle en moins de 200 mots. J'ai indiqué au directeur du SGDSN que nous devrions nous inspirer de cette expérience taiwanaise pour définir le *modus operandi* de VIGINUM.

J'ai hâte de pouvoir évaluer le travail de concertation que cette agence mène avec les plateformes, réseaux sociaux et médias et de pouvoir étudier leurs méthodes de *fact-checking*.

Je souhaite la même réussite à la nouvelle agence VIGINUM que celle que nous constatons pour l'ANSSI.

LA MENACE NE FAIBLIT PAS

GS Mag : Justement, concernant l'ANSSI, quel regard portez-vous sur l'état de menace cyber en France, aujourd'hui ?

Olivier Cadic : Malheureusement, comme nous l'avions anticipé, l'état de la menace ne faiblit pas. Bien au contraire, les actes cybermalveillants, tels le cyber-rançonnage, l'espionnage mené par certaines puissances, ou encore le sabotage ont augmenté.
La pandémie a accru significativement l'exposition au risque de la société et des acteurs économiques, du fait du développement sans précédent des usages du numérique.

La lutte contre les menaces cyber constitue l'une des missions phares du SGDSN, à travers le rôle de l'ANSSI.

Selon le SGDSN, sur les neuf premiers mois de 2021, le nombre de cyberattaques recensées a doublé par rapport à l'année 2020.

Les acteurs publics sont particulièrement touchés.
En 2020, 128 incidents cyber ayant affecté les ministères ont été traités par l'ANSSI, contre 81 en 2019, soit une augmentation de 58%. De plus, 20% des victimes de rançongiciels signalées à l'ANSSI étaient des collectivités territoriales et 11% des hôpitaux.

L'ANSSI sera renforcée de 40 ETP supplémentaires en 2022. Nous nous en sommes réjouis.

NATIONAL POLICY

VIGINUM, a major step forward against disinformation

*Interview with Olivier Cadic, Senator for French citizens living outside France **
Marc Jacob and Emmanuelle Lamandé

*In 2022, program 129 ** provides for the funding of new missions, starting with VIGINUM. This new government agency will be tasked with detecting disinformation operations on online platforms and informing the public authorities. For Senator Olivier Cadic, the establishment of this new service represents a major step forward against disinformation, especially with only a few months to go before the presidential election.*

Ministères	Nombre d'incidents traités par l'ANSSI	Commentaires
Ministère de l'agriculture et de l'alimentation	14 (+6)	
Ministère de la cohésion des territoires	2 (+2)	
Ministère de la culture	11(+5)	
Ministère des armées	4 (-17)	
Ministère de l'économie des finances et de la relance	18 (+7)	Dont une opération de cyberdéfense
Ministère de l'éducation nationale, de la jeunesse et des sports	58 (+ 36)	
Ministère de l'enseignement supérieur, de la recherche et de l'innovation	3 (+2)	
Ministère de l'Europe et des affaires étrangères	14 (-)	Dont une opération de cyberdéfense et un incident majeur
Ministère de l'intérieur	13 (-1)	
Ministère de la justice	4 (-2)	
Ministère des outre-mer	2 (+1)	
Ministère des solidarités et de la santé	14 (+11)	
Ministère de la transition écologique	18 (+10)	
Ministère du travail, de l'emploi et de l'insertion	6 (-1)	

** Senator Olivier Cadic (UC - French established outside France) is vice-chairman of the Senate Foreign Affairs, Defense and Armed Forces Committee. His functions include the office of co-rapporteur of SGDSN credits (in charge of the State's Information Systems security policy) and ANSSI. He is also Chairman of the France-Gulf countries friendship group, and Member of the Board of Directors of the Institut Français.*
*** Program 129 "Coordination of government work" of the "government action policy" mission brings together the staff, strategy and forecasting, coordination and support functions carried out by the services of the Prime Minister.*
Under the auspices of this program, the Senate Foreign Affairs and Defense Committee examines action 2 "Coordination of security and defense", which represents a little more than half of the program's appropriations (53%). This action includes the resources intended for the General Secretariat for Defense and National Security (SGDSN), special funds and credits from the interministerial control group (GIC) which manages requests for authorisation to implement intelligence techniques issued by the services.
http://www.senat.fr/commission/etr/synthese_des_avis_budgetaires.html

400 ENTITÉS SUR LES 700 VISÉES ONT BÉNÉFICIÉ D'UN « PARCOURS DE SÉCURISATION CYBER »

GS Mag : Où en sommes-nous du déploiement du plan cyber de France Relance, dont une part consistante a été allouée à l'ANSSI ?

Olivier Cadic : En 2021, l'ANSSI s'est vu confier une enveloppe de 136 millions d'euros issue du plan France Relance en vue de participer à la mise en œuvre d'une « stratégie d'accélération cybersécurité » lancée en février dernier. L'agence, qui dispose de deux ans pour utiliser ces crédits, en consacre une grande partie au renforcement de la cybersécurité d'acteurs publics vulnérables, en premier lieu les collectivités territoriales et les hôpitaux, qui ont été des cibles privilégiées ces derniers temps.

Après un démarrage assez lent - qui n'a pas manqué d'inquiéter - le dispositif est monté en puissance : 400 entités sur les 700 visées ayant d'ores et déjà bénéficié d'un « parcours de sécurisation cyber ».

Toutefois, il faudra s'assurer qu'au-delà du diagnostic, les collectivités auditées ont bien la capacité de réaliser les adaptations recommandées. Par ailleurs, il faudra être attentif aux collectivités qui ne sont pas encore entrées dans le dispositif et qui sont sûrement les moins bien « outillées » pour solliciter cet accompagnement.

Enfin, il faudra envisager d'autres mesures pour les milliers de collectivités qui n'ont pas vocation à être prises en charge dans le cadre de ce plan, mais qui sont souvent les plus vulnérables et ont besoin d'une véritable acculturation au risque cyber.

CSIRT : 4 RÉGIONS SUR 13 ENGAGÉES DANS LE DISPOSITIF

GS Mag : Justement, quelles sont les solutions pour aider ces milliers de petites structures à se protéger ?

Olivier Cadic : L'ANSSI a considéré qu'il y avait un trou dans la raquette et a voulu créer un dispositif pour les acteurs de taille intermédiaire comme les ETI ou les collectivités territoriales, victimes de cyberattaques. Voilà pourquoi, l'autre grand volet du plan de relance cyber est la création de « centres régionaux de réponse cyber de proximité » ou « centres de réponse à incidents » (CSIRT).
Mis en place en partenariat avec les régions, ces centres doivent bénéficier chacun pour démarrer d'une subvention d'un million d'euros et d'un accompagnement technique de l'ANSSI, mais devront ensuite trouver un mode de financement pérenne en s'appuyant sur l'écosystème local.
Pour l'heure, seules 4 régions sur 13 se sont engagées dans le dispositif, ce qui est insuffisant.

Il faudra aussi définir une articulation logique et efficace entre ce réseau de centres de proximité et la structure ACYMA, plus connue sous le nom de « Cybermalveillance.gouv.fr ». Tout l'enjeu est de parvenir à une architecture lisible et cohérente, permettant d'orienter efficacement et rapidement les victimes, en évitant tout fonctionnement en silo.

IL EST URGENT D'AUGMENTER SIGNIFICATIVEMENT LE BUDGET ALLOUÉ À ACYMA

GS Mag : Le GIP ACYMA fait également partie des instruments de lutte contre les cybermalveillances, dont vous louez régulièrement la performance lors de vos conférences. Qu'en attendez-vous pour les années à venir ?

Olivier Cadic : Merci de me donner l'opportunité de saluer le travail de cette structure, dirigée par Jérôme Notin, qui accomplit un travail remarquable. Créée en 2017 sous la forme d'un groupement d'intérêt public associant acteurs publics et acteurs privés, ACYMA met en relation via une plateforme numérique les victimes d'actes de cybermalveillance avec des prestataires agréés pouvant les aider.

S'il se construit progressivement une notoriété auprès du grand public (+ 155% de visites sur la plateforme en 2020), ACYMA manque en revanche singulièrement de moyens pour les autres missions qui lui sont confiées : la sensibilisation de la population au risque cyber et la mise en place d'un observatoire de la cybermalveillance.

De fait, il fonctionne avec un budget de 1,6 million d'euros, provenant pour moitié de contributions publiques et pour moitié de contributions privées, qui lui permet d'employer 12 agents. Avec des moyens aussi limités, impossible d'envisager un service d'assistance téléphonique direct doté d'un numéro d'appel unique à l'image de ce que j'ai observé en Israël depuis bientôt trois ans. Je le réclame depuis 2019 !
Il est urgent d'augmenter significativement le budget alloué à ACYMA, c'est-à-dire au minimum de le doubler pour le porter à 3 millions d'euros.

Au vu des enjeux et de l'ampleur des risques dans le champ cyber, un tel effort est indispensable et ne semble pas hors de portée, surtout s'il est partagé entre les différents membres du GIP.
Le développement des actes cybermalveillants du fait de l'absence ou de l'insuffisance de la politique de prévention a un coût pour la société. Le préjudice pour l'État pour la seule arnaque récente sur les comptes professionnels de formation s'élève à plusieurs dizaines de millions d'euros.

Nous plaidons par ailleurs en faveur d'une grande campagne nationale de prévention contre la cybermalveillance, qui serait dotée d'une enveloppe de communication exceptionnelle et qui serait mise en œuvre par ACYMA.

LA PRÉSIDENCE FRANÇAISE DE L'UE, UNE OPPORTUNITÉ POUR FAIRE AVANCER LES DOSSIERS CYBER AU PLAN EUROPÉEN

GS Mag : Au 1er janvier 2022, la France prendra la présidence française de l'Union européenne. Quelles seront ses priorités en matière de cybersécurité ?

Olivier Cadic : La présidence française de l'Union européenne doit constituer une fenêtre d'opportunité pour faire avancer les dossiers cyber au plan européen.
Cela concerne d'abord la révision de la directive NIS de 2016, pour étendre le champ des secteurs considérés comme critiques (traitement des eaux usées, espace, administrations…) et rehausser les obligations imposées à leurs opérateurs. Il faudra, à cet égard, prêter attention à la concertation avec les secteurs professionnels concernés, tant lors de la révision que des désignations d'opérateurs, celle-ci semblant avoir été insuffisante pour la mise en œuvre de la directive NIS.

La France se donne par ailleurs l'objectif d'œuvrer au renforcement de la sécurité des institutions européennes, qui sont insuffisamment protégées.

Elle souhaite également favoriser le développement d'un « tissu industriel de confiance » à l'échelle européenne, par la mise en place du Centre européen de compétences industrielles en matière de cybersécurité et par des avancées en matière de certification de sécurité.
En effet, l'absence d'outil de certification commun à l'échelle européenne est un frein pour les entreprises qui souhaitent distribuer leurs solutions auprès de l'ensemble des pays européens.
La France a une longueur d'avance et cherche notamment à étendre à l'échelle européenne son approche de la certification, y compris dans le domaine du Cloud (certification SecNumCloud) et de la sécurisation des réseaux 5G.

Si la certification est nécessaire pour produire de la confiance, attention toutefois à ne pas tomber dans l'écueil de l'excès de normes qui ont un coût élevé pour les entreprises et in fine restreignent l'offre. Une idée intéressante et relativement simple, qui a été évoquée lors des auditions, serait de créer un label de qualité associé à un niveau de confiance correspondant à une lettre (A,B,C,D) sur le modèle de celui qui existe en matière de consommation énergétique.

Enfin, notre pays souhaite s'impliquer pleinement dans la mise en place de mécanismes de solidarité à l'échelle européenne, à savoir le cadre européen de réponse aux crises cyber *Blueprint* et le réseau de liaison *CyCLONe* (*Cyber Crisis Liaison Organisation Network*) qui doit être déployé dans tous les États membres.

C'est un volet très important, car on le sait les crises dans le champ cyber ne s'arrêtent pas aux frontières. Une approche collective et la mise en réseaux des compétences est indispensable.

OBJECTIF : RENFORCER LES FILIÈRES DE FORMATION EN MATIÈRE DE CYBERSÉCURITÉ

GS Mag : Dans les prochaines années, l'enjeu majeur ne sera-t-il pas de susciter les vocations dans le domaine de la cybersécurité et savoir retenir nos talents au service de notre souveraineté. Quelles préconisations faites-vous à ce sujet ?

Olivier Cadic : C'est exact. La cybersécurité doit devenir l'affaire de tous. Un travail de sensibilisation est plus que jamais nécessaire pour protéger nos démocraties et les valeurs qu'elles incarnent contre des agressions extérieures.

De manière plus globale, je salue l'objectif qui est de doubler les emplois de la filière, pour passer à 75 000 en 2025, contre 37 000 aujourd'hui. Mais pour cela, nous devons parcourir un long chemin vers la démocratisation de la filière cyber.

Une de mes priorités est de contribuer à renforcer les filières de formation en matière de cybersécurité : la pénurie de ressources humaines qualifiées est préoccupante. Il faut relier nos établissements scolaires et nos instituts de formation aux besoins du marché.

Et puis, je pense que pour stimuler les vocations, la France doit disposer d'un ou d'une « championne de la cybersécurité ».

Ainsi, la compétition WorldSkills ou Olympiade des métiers constitue une bonne opportunité pour développer et susciter les talents français dans ce domaine. Depuis 2019, la cybersécurité est devenue une discipline à part entière dans cette compétition internationale, au même titre que la coiffure ou la menuiserie ! J'espère que nous saurons présenter une équipe aguerrie et compétitive pour remporter cette épreuve lors des mondiaux en 2024 qui se dérouleront à Lyon ! ■■■

[1] Le sénateur Olivier Cadic (UC - Français établis hors de France) est vice-président de la commission des Affaires étrangères, de la Défense et des Forces armées du Senat. Dans le cadre de celle-ci, il est co-rapporteur des crédits du SGDSN (en charge de la politique de sécurité des Systèmes d'Information de l'État) et de l'ANSSI. Il est également Président du groupe d'amitié France-Pays du Golfe, et Membre du Conseil d'administration de l'Institut français.
[2] Le programme 129 « Coordination du travail gouvernemental » de la mission « Direction de l'action du gouvernement » regroupe les fonctions d'état-major, de stratégie et de prospective, de coordination et de soutien exercées par les services du Premier ministre.
Au sein de ce programme, la commission des Affaires étrangères et de la Défense du Sénat examine l'action 2 « Coordination de la sécurité et de la défense », qui représente un peu plus de la moitié des crédits du programme (53%). Cette action comprend les moyens destinés au Secrétariat général de la défense et de la sécurité nationale (SGDSN), les fonds spéciaux et les crédits du groupement interministériel de contrôle (GIC) qui gère les demandes d'autorisation de mise en œuvre des techniques de renseignement émises par les services.
http://www.senat.fr/commission/etr/synthese_des_avis_budgetaires.html