GROUPE DE TRAVAIL CYBERSECURITE DE PARIS EUROPLACE,
JEUDI 19 JUIN 2025 - LA DEFENSE
INTERVENTION D'OLIVIER CADIC

1. *L'écosystème cybersécurité en France : quelles évolutions ? Est-il adapté ?*
2. *Actualité réglementaire française et européenne ;*
3. *La cybersécurité au sein du secteur financier vue du Sénat : quelle appréciation ? Quelles attentes ?*

Introduction

- Ces trois thématiques correspondent aux questions de cybersécurité et d'ingérences numériques étrangères que je suis depuis 8 ans en qualité de rapporteur budgétaire pour avis de la commission des affaires étrangères et de la défense du Sénat sur le budget du Secrétariat général de la défense et de la sécurité nationale, lequel chapeaute l'ANSSI notamment, mais aussi le GIP Cybermalveillance, et depuis 2021 le service VIGINUM de lutte contre les ingérences numériques étrangères.
- Les sujets que vous soulevez (l'écosystème de cybersécurité, l'actualité normative et la cybersécurité dans le secteur financier) sont pleinement d'actualité puisque précisément un projet de loi relatif à la résilience des entité critiques et au renforcement de la cybersécurité est en cours d'examen par le Parlement.
- Je préside au Sénat la commission spéciale sénatoriale qui a conduit le Sénat a adopté le 4 mars dernier un texte remanié par une centaine d'amendements en commission et en séance publique.

- A l'heure où nous nous parlons, ce texte n'est toujours pas discuté à l'Assemblée nationale. Il n'est même pas inscrit à la session extraordinaire de juillet alors même que j'avais attiré l'attention dès l'examen du budget 2024, fin 2023, sur la nécessité d'anticiper cette transposition qui devait intervenir avant le 17 octobre 2024 pour la directive NIS 2 pour la plus urgente. Nous sommes donc en retard, mais certains le sont encore plus que nous. Je reviens d'Espagne où le projet de loi de transposition n'est même pas encore présenté.

J'en viens maintenant aux trois thématiques qui nous intéressent.

1. L'écosystème cybersécurité en France : quelles évolutions ? Est-il adapté ?

L'évaluation de l'écosystème de cybersécurité en France entre dans mes attributions de rapporteur pour avis sur le budget du SGDSN et donc sur l'efficacité de la coordination interministérielle des services du Premier ministre.

Tous les ans ma préoccupation est d'obtenir un retour d'information suffisant sur les menaces et les réponses qui sont apportées par les différents acteurs.

De fait il y a originellement un écart à combler entre une vision étatique de la cybersécurité qui a tendance à se concentrer sur les services de l'Etat et à quelques centaines d'opérateurs d'importance vitale tandis que la réalité de la menace concerne des dizaines de milliers d'entreprises et de collectivités, sans parler des millions de particuliers.

Depuis la création en 2009 de l'ANSSI, l'écosystème a évolué en s'enrichissant d'une stratégie de cybersécurité en 2018 mais qu'il conviendrait maintenant d'actualiser.

En effet, j'ai constaté des évolutions qui vont dans le bon sens mais qui maintenant risquent de perdre en lisibilité et en efficacité :

- La création de cybermalveillance, complétée par celle du 17Cyber vont dans le bon sens ;
- Mais dans le même temps certaines menaces ont été sous-estimées et des attaques sévères et de plus en plus nombreuses ont impacté des hôpitaux, des universités, des collectivités territoriales et des entreprises. Les CERT consacrés à la santé ou à l'enseignement supérieur, ou encore les nouveaux CSIRT régionaux, n'ont pas donné satisfaction. A cet égard, je serais intéressé par votre retour d'expérience sur le CERT consacré au secteur financier et bancaire.
- J'ai remarqué des différences d'approches importantes entre les tenants du « foisonnement d'initiatives » et ceux, comme moi, qui sont partisans d'une meilleure lisibilité. J'ai observé avec étonnement qu'aucun CSIRT régional n'avait les mêmes périmètres de mission.
- Le projet de loi de transposition comporte d'ailleurs encore des points de réglages à fixer sur le nombre d'entités concernées par la transposition des directives, qu'ils s'agissent des entités « essentielles » ou « importantes » (15 000 ou plus ?), des seuils de collectivités territoriales assujetties (1 500 ?) à NIS 2, ou encore l'assujettissement ou

non des sociétés de financement qui n'est pas prévu par le Règlement DORA.

Cet écosystème est-il adapté ? C'est précisément l'objet du projet de loi que de le faire évoluer face à l'augmentation des menaces. Le rapport de la commission spéciale du Sénat livre un état des lieux : les attaques par rançongiciel ont augmenté de 30 % entre 2022 et 2023. La cybermenace n'épargne plus aucun secteur de la vie économique et sociale : 34 % de ces attaques visaient des TPE/PME, 24 % des collectivités territoriales, 10 % des entreprises stratégique, 10 % des établissements de santé et 9 % des établissements d'enseignement supérieur.

Selon le cabinet d'études économique Asteres, les cyberattaques ont coûté 2 milliards d'euros en 2022.

Le secteur financier est naturellement une cible de choix car son niveau élevé d'interconnexions constitue aussi une vulnérabilité pour les 22 000 entités financières.

2. Actualité réglementaire française et européenne

Pour remédier à ces risques croissants, ce projet de loi prévoit la transposition de 3 directives différentes :

- la directive sur la résilience des entités critiques (REC) acte le passage d'une logique de protection à une approche axée sur la résilience vis-à-vis des risques de toute nature dont la transposition actualise le dispositif français de sécurité des activités d'importance vitale (SAIV) ;

- la directive Network and Information Security (NIS 2), visant à assurer un niveau élevé de cybersécurité dans l'ensemble de l'Union, va

porter les 6 secteurs essentiels actuels à 18 secteur critiques et élargir le périmètre de régulation à 15 000 entités essentielles et importantes et près de 1 500 collectivités territoriales ;

- la directive Digital Operational Resilence Act (DORA) relative à la résilience opérationnelle numérique du secteur financier, bancaire et assurantiel.

S'agissant de la directive DORA qui vous intéresse plus particulièrement, j'ai notamment entendu l'Autorité des marchés financiers (AMF) faire le constat que les entités financières sont exposées à une large gamme de risques : le déni de service sur l'infrastructure de trading, et donc plus globalement l'atteinte à la disponibilité de l'infrastructure de trading, l'atteinte à la confidentialité et l'intégrité des ordres, la compromission de l'algorithme de négociation (porte dérobée, code malveillant ou simplement présentant des bogues importés depuis des sources externes comme l'open source ou ChatGPT), ou encore l'atteinte à l'intégrité du Système d'Information (SI) supportant les services algorithmiques en vue de compromettre et modifier l'algorithme.

3. La cybersécurité au sein du secteur financier vue du Sénat : quelle appréciation ? Quelles attentes ?

Le Sénat a voté la transposition de la directive DORA en apportant toutefois certains aménagements.

De l'ensemble de nos auditions publiques et malgré l'assurance de l'ANSSI et des ministères concernés d'avoir mené des concertations et produit une étude d'impact de 900 pages (!), j'ai été surpris de constater que l'ensemble des personnes entendues déplorait un manque

d'information et de concertation notamment sur les dispositions réglementaires d'application du projet de loi.

Je serais curieux d'avoir votre sentiment pour ce qui concerne le secteur financier.

Pour ce qui concerne les modifications apportées par le Sénat au projet de loi, plusieurs amendements de mon collègue Michel Canévet qui est rapporteur sur le titre III visent trois objectifs :

- Éviter des différences de traitement injustifiées entre les entreprises par l'application du règlement DORA aux succursales d'entreprises d'investissement de pays tiers (article 49) ;

- Simplifier la vie des entreprises, en créant un guichet unique de notification des cyber-incidents (article 43 A), en fusionnant des dispositifs de déclarations d'incidents (article 49) et en évitant le double assujettissement à la directive NIS 2 et au paquet DORA (article 62 A) ;

- Modérer les effets des surtranspositions en supprimant l'article 53, qui introduisait une précision superfétatoire et sans doute contreproductive concernant les pouvoirs du secrétaire général de l'Autorité de contrôle prudentiel et de résolution, et en reportant l'entrée en vigueur du titre III de la loi au 1er janvier 2030 pour les sociétés de financement (article 62), auquel le règlement DORA ne fait pas référence.

Nous avons également souhaité apporter des mesures de simplifications :

- Trouver une définition législative d'une « labellisation NIS 2 » pour permettre aux entreprises de valoriser, vis-à-vis de leurs

banques, de leurs assurances ou bien encore de leurs clients, leurs efforts en matière de cybersécurité ;

- Différer les dispositions en matière de contrôle et de sanctions pendant au moins trois ans, voire davantage pour certaines entités ;

- Instaurer un mécanisme de reconnaissance mutuelle entre États membres pour que les entités puissent se prévaloir du respect de leurs obligations au sein d'un des pays de l'Union européenne.

Les travaux en séance publique ont permis de revenir sur des rédactions communes avec le gouvernement sur les questions de contrôle et de reste à charge des coûts des contrôles, certains désaccords subsistants principalement sur le titre III relatif à la transposition de la directive DORA, notamment sur 2 mesures :

→ faire de l'Autorité des marchés financiers le guichet unique, en matière de déclaration d'incidents informatiques, pour les entreprises de marché et les prestataires de services sur cryptoactifs ;

→ appliquer le principe de proportionnalité pour l'application du règlement DORA aux sociétés de financement petites et non complexes.

Par ailleurs une mesure emblématique a été adoptée à mon initiative pour empêcher toute mesure instaurant des backdoors ou des failles dans le chiffrement des messageries.

J'espère avoir été dans le thème en introduisant cette conférence par un aspect très concret des travaux de la commission spéciale et de mon rôle de Sénateur.

Je vous remercie et me réjouis par avance du débat qui s’ouvre maintenant.