ASSEMBLÉE NATIONALE

17ème législature

Jumeaux numériques

Question écrite n° 2457

Texte de la question

M. Olivier Marleix appelle l'attention de M. le ministre de l'économie, des finances et de l'industrie sur les risques de malveillance ou de sabotages des installations critiques et sensibles françaises évoqués par le Délégué général de l'armement (DGA) lors de son audition du 23 octobre par la commission de la défense et des forces armées de l'Assemblée nationale. Il souhaite plus particulièrement l'alerter sur la situation des jumeaux numériques des infrastructures d'importance vitale et autres réseaux critiques ou sensibles. Commandés par de grandes entreprises ou des opérateurs de services (EDF, RTE, circulation aérienne, SNCF...), ces jumeaux sont en effet indispensables à la conduite des installations ou aux simulations en mode normal ou dégradé des installations. Leur importance a notamment été évoquée lors du sabotage du réseau TGV survenu le jour de lancement des jeux Olympiques 2024 rendu possible par une connaissance très pointue du réseau. C'est pourquoi M. le député souhaite connaître le niveau de connaissance qu'a l'État de ces jumeaux numériques. En premier lieu, l'État dispose-t-il d'une liste des jumeaux numériques critiques ou sensibles ? Ensuite l'État a-t-il connaissance des entreprises qui développent ces clones numériques au profit des opérateurs et grandes entreprises ? Quelles sont les nationalités de ces entreprises ? L'État a-t-il connaissance des nationalités des détenteurs finaux ? Dans l'affirmative, dans quels pays sont développés ces jumeaux ? Sur quels serveurs sont-ils stockés et là encore dans quels pays ? Si ces entreprises sont françaises, font-elles l'objet d'une protection spécifique ? Enfin, les personnels des sociétés de services informatiques qui travaillent ou développent ces clones numériques font-ils l'objet d'un criblage par les services de sécurité intérieure ? Il souhaite obtenir des précisions à ce sujet.

Texte de la réponse

Le sujet des jumeaux numériques revêt des enjeux stratégiques en termes de souveraineté nationale et sur le plan capacitaire. Les problématiques de souveraineté reposent sur le traitement de données, pouvant être sensibles, par ces outils complètement dématérialisés. A ce titre, l'Etat porte une attention particulière à l'utilisation faite des jumeaux numériques (à différentes échelles : bâtiment, infrastructure, site ou territoire), notamment lorsqu'ils sont couplés avec des systèmes d'hypervision en temps adapté. L'offre est multiple : Dassault Systems, Sopra Steria, SNEF, ERIMA (titulaire du marché SECPRO de la défense), PRYSM, et des entreprises de taille plus modeste qui, en ajoutant des couches logicielles vendent leurs services à des sites sensibles, collectivités territoriales ou services de l'Etat. A titre d'exemple, l'IGN travaille actuellement sur le déploiement d'un jumeau numérique à l'échelle nationale qui comportera des restrictions sur les zones interdites à la prise de vue aérienne (ZIPVA). L'Etat ne dispose pas à ce jour de liste exhaustive des opérateurs mettant en œuvre des jumeaux numériques sur leurs sites, mais les opérateurs d'importance vitale (OIV) sont régulièrement sensibilisés sur le partage d'informations. Depuis 2013, les opérateurs d'importance vitale (OIV), désignés au titre du dispositif de sécurité des activités d'importance vitale (SAIV), régi par les articles L. 1332-1 et suivants du code de la défense, doivent identifier au sein de leurs structures les systèmes d'information d'importance vitale sans lesquels ils ne pourraient pas assurer leur protection ou la bonne réalisation de l'activité d'importance vitale pour laquelle ils ont été désignés. Ils ont l'obligation de déclarer les systèmes d'information

identifiés et de mettre en œuvre les mesures de cybersécurité établies par l'agence nationale de la sécurité des systèmes d'information (ANSSI). Le dispositif de SAIV prévoit aussi la possibilité pour les OIV de demander à ce que des enquêtes administratives de sécurité soient effectuées, en application de l'article L. 1332-2-1 du code de la défense, à la condition que ces enquêtes soient prévues dans les plans de protection validés par l'autorité administrative et qu'elles s'effectuent sur des personnes ayant un accès physique à un point d'importance vitale – soit un lieu, un site ou un établissement désigné comme infrastructure critique. Le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité (PRMD2412608L), déposé au Sénat le 15 octobre 2024, visant notamment à transposer la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques (REC), prévoit la possibilité pour un opérateur d'importance vitale de demander la réalisation d'une enquête pour les personnes ayant accès à distance à des systèmes d'information d'importance vitale ou pour les personnes qui occuperaient des fonctions sensibles au sein de l'entité.

Données clés

Auteur : M. Olivier Marleix
Circonscription : Eure-et-Loir (2e circonscription) - Droite Républicaine
Type de question : Question écrite
Numéro de la question : 2457
Rubrique : Défense
Ministère interrogé : Économie, finances et industrie
Ministère attributaire : Premier ministre

Date(s) clée(s)

Question publiée au JO le : 3 décembre 2024, page 6333
Réponse publiée au JO le : 11 février 2025, page 754