ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 33267	De **Mme Marielle de Sarnez** (Mouvement Démocrate (MoDem) et Démocrates apparentés - Paris)	**Question écrite**

Ministère interrogé > Europe et affaires étrangères	**Ministère attributaire** > Europe et affaires étrangères

Rubrique >Union européenne	**Tête d'analyse** >Renforcement de la coopération européenne de lutte contre la cybercriminalité	**Analyse** > Renforcement de la coopération européenne de lutte contre la cybercriminalité.

Question publiée au JO le : **20/10/2020**
Réponse publiée au JO le : **08/12/2020** page : **9007**

Texte de la question

Mme Marielle de Sarnez attire l'attention de M. le ministre de l'Europe et des affaires étrangères sur l'augmentation inquiétante de la cybercriminalité, désormais considérée comme l'un des principaux facteurs de risque susceptible d'engendrer une crise internationale de grande ampleur. Comme l'a récemment précisé le directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi), ces cybermenaces en accroissement exponentiel revêtent trois aspects : l'espionnage économique, notamment dans le domaine de la recherche et de la santé du fait de la crise sanitaire et de la course aux vaccins, les menaces de nature militaire et celles liées à la grande criminalité. Dans un tel contexte, la coopération européenne est indispensable qu'il s'agisse de la prévention et de la recherche, de la détection des menaces et de leur traitement pénal. Elle lui demande par conséquent de lui préciser les initiatives que le Gouvernement entend prendre afin de renforcer cette coopération contre des menaces susceptibles d'engendrer des déstabilisations sérieuses.

Texte de la réponse

La cybercriminalité constitue une menace majeure pour la France. En pleine recrudescence, de nombreuses attaques ciblent les particuliers mais aussi les entreprises et les administrations. Elles visent à obtenir des informations personnelles afin de les exploiter ou de les revendre (données bancaires, identifiants de connexion à des sites marchands, etc.). Hameçonnage (phishing) et « Rançongiciel » (ransomware) sont des exemples connus d'actes malveillants portant préjudices aux internautes. La plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (Pharos) du ministère de l'intérieur a reçu plus de 1 584 130 signalements depuis sa création en 2009. La lutte contre la cybercriminalité s'inscrit essentiellement dans un cadre conventionnel international, venant compléter l'utilisation des instruments du droit de l'Union européenne (UE) en matière de coopération judiciaire pénale qui peut être particulièrement efficace entre les États membres. Ce cadre conventionnel et du droit de l'UE est appelé à évoluer dans le cadre de plusieurs négociations parallèles qui ont toutes pour objet de faciliter l'accès à la preuve numérique transfrontalière en matière pénale. Dans le cadre de l'UE, le paquet législatif « e-evidence », qui a fait l'objet d'une orientation générale du Conseil, est en cours d'examen au Parlement européen. Ces textes visent à accélérer et à simplifier l'accès des magistrats aux éléments de preuve électronique avec des projets de règlement et de directive sur l'accès transfrontière aux preuves électroniques. Après les élections européennes de mai 2019, les négociations avaient repris au Parlement européen. Cependant, les travaux relatifs à ces textes ambitieux, dont la France soutient les principes, ont été perturbés par la

crise sanitaire. Le Parlement européen devrait adopter sa position en décembre, les trilogues pourraient donc débuter en janvier 2021. Par ailleurs, ces textes produiront pleinement leurs effets en complémentarité avec d'autres instruments internationaux tels que le deuxième protocole additionnel à la convention de Budapest du Conseil de l'Europe et un accord entre l'Union et les États-Unis, qui sont en cours de négociation. Sur le plan bilatéral, le conseil JAI a également confié un mandat de négociation à la Commission européenne pour organiser l'accès réciproque à la preuve électronique dans la relation avec les États-Unis, en application du Cloud Act américain. Quatre sessions de négociation ont eu lieu entre septembre 2019 et mars 2020. Toutefois, la Commission européenne lie la poursuite de ces négociations à celles du paquet « e-evidence », soulignant la nécessité de disposer de positions consolidées au niveau européen avant de poursuivre les discussions avec les Etats-Unis au-delà des aspects techniques relevant des États membres. Aucune nouvelle session de négociation n'a eu lieu depuis mars 2020. Sur le plan multilatéral, le Conseil de l'Europe a poursuivi en 2020 ses travaux sur un projet de second protocole additionnel à la Convention de Budapest sur la cybercriminalité. Le futur texte ambitionne de répondre au niveau mondial aux mêmes enjeux de l'accès à la preuve numérique dans le contexte de l'informatique en nuage. Il vise aussi à développer de nouveaux outils pour faciliter la coopération judiciaire internationale. L'adoption de ce protocole, attendue pour la fin de l'année 2020, devra permettre aux acteurs de l'investigation de disposer d'une voie de coopération renforcée avec les 65 pays signataires de la Convention de Budapest. La France soutient activement l'extension de la Convention de Budapest, qui garantit un équilibre entre, d'une part, la coopération judiciaire au service de la lutte contre la cybercriminalité et d'autre part, le respect des libertés fondamentales. Certains États contestent toutefois le caractère universel de cette convention. Ainsi, à l'initiative de la Russie, l'assemblée générale de l'ONU a, le 27 décembre 2019, adopté une résolution visant à établir une convention des Nations unies en matière de lutte contre la cybercriminalité. Depuis l'adoption de cette résolution, l'Union et ses États membres, dont la France, se coordonnent pour éviter que le nouveau processus de négociation pour une convention des Nations unies ne remette en cause l'équilibre nécessaire entre renforcement des moyens dédiés à la lutte contre la cybercriminalité et respect des droits fondamentaux et de l'État de droit, qui prévaut actuellement dans le cadre de la Convention de Budapest. Au niveau technique, cette coopération prend la forme de contacts bilatéraux, notamment avec les pays sources de cybercriminalité. Elle passe aussi par des échanges entre les services compétents des différents États au sein des instances européennes (le centre européen de lutte contre la cybercriminalité [EC3] d'Europol, et Eurojust) ou internationales (le « Global Complex for Innovation » d'Interpol - IGCI).