ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 15702	De **Mme Marie-France Lorho** (Non inscrit - Vaucluse)	**Question écrite**

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

Rubrique >numérique	**Tête d'analyse** >Lacunes dans la protection des réseaux numériques européens	**Analyse** > Lacunes dans la protection des réseaux numériques européens.

Question publiée au JO le : **01/01/2019**
Réponse publiée au JO le : **09/04/2019** page : **3267**

Texte de la question

Mme Marie-France Lorho interroge M. le ministre de l'Europe et des affaires étrangères sur les lacunes dans protection dont font preuve les réseaux numériques européens. Le nombre d'attaques informatiques, d'une gravité croissante, que rencontre la Commission européenne est alarmant : en 2011, le service européen d'action extérieure (SEAE) de Bruxelles faisait l'objet d'un piratage, survenu avant la réunion au sommet relative à l'implication européenne dans les frappes aériennes en Libye. En 2016, le site de la commission faisait encore l'objet d'une attaque informatique, affectant notamment des questions de sécurité nucléaire. Le 18 décembre 2018, le New-York Times révélait le contenu d'une opération de piratage de grande ampleur visant le SEAE. L'opération, qui aurait duré près de trois ans, aurait consisté en l'introduction de hackeurs dans le réseau de correspondance européenne (COREU) de l'Union européenne. Cette dernière attaque est particulièrement inquiétante : le réseau de communication, qui véhicule entre 25 000 à 30 000 messages par an, concerne en effet les 28 pays membres et constitue un organe de communication important entre eux, notamment en cas de crises diplomatiques. Si le porte-parole du Haut représentant de l'Union européenne pour les affaires étrangères assure que « nous améliorons nos systèmes de communication pour répondre aux menaces », ce système informatique européen semble particulièrement défaillant, notamment à l'heure où l'Union européenne s'est targuée de devenir, à l'horizon 2025, « le leader mondial de la cybersécurité ». Les cyberattaques dont a fait l'objet le réseau COREU ont-t-elles affecté les données françaises ? Il lui demande quels moyens il compte mettre en œuvre pour protéger les données diplomatiques françaises face à ces menaces qui risquent de compromettre le secret diplomatique des pays membres de l'Union européenne.

Texte de la réponse

Alors que nous aspirons à doter l'Union européenne d'une véritable autonomie stratégique, y compris dans le cyberespace, il est indispensable que les réseaux de l'UE bénéficient d'un niveau de protection élevé et que nous puissions échanger des informations classifiées en toute sécurité. Comme l'a souligné l'attaque contre le système de chiffrement COREU révélée en décembre 2018, les institutions de l'Union européenne restent une cible privilégiée des opérations cyber malveillantes. L'enquête menée par le Secrétariat du Conseil de l'Union européenne, en charge de la gestion du système COREU, a révélé que ce dernier n'avait été affecté que de manière limitée et circonscrite. Cet événement a toutefois mis en exergue la nécessité de renforcer les moyens techniques et diplomatiques de prévention et de gestion des incidents de cybersécurité, sur laquelle les autorités françaises sont mobilisées. Le gouvernement français a eu l'occasion de rappeler auprès des institutions européennes et des autres Etats membres

l'importance de garantir l'échange d'informations sensibles de façon pleinement sécurisée. Il a soutenu la proposition d'un plan d'action contre les activités hostiles visant les institutions européennes et demandé à ce qu'une étude approfondie des besoins des institutions européennes soit menée à cette fin. Les autorités françaises soutiennent activement les travaux actuellement menés afin de renforcer la sécurité des systèmes d'information et les capacités cyber des Etats membres à l'échelle de l'Union européenne. En décembre 2018, la réforme du mandat de l'Agence de cybersécurité de l'Union européenne (ENISA) a constitué une avancée importante, dans le sillage de la directive NIS de 2016. Des efforts sont actuellement engagés pour développer le recueil et l'échange des bonnes pratiques, l'évaluation mutuelle, la formation et la certification de sécurité au niveau européen. Les investissements ou la fourniture d'équipements étrangers dans les secteurs stratégiques constituent un autre enjeu majeur de sécurité et de souveraineté, sur lequel la coopération au niveau européen est en cours d'approfondissement. Enfin, en vue de renforcer les capacités de réaction aux attaques cyber à l'échelle européenne, les autorités françaises s'investissent pleinement dans les travaux visant à rendre opérationnelle la boîte à outil cyber-diplomatique adoptée en 2017 et qui permet à l'Union européenne et à ses Etats membres de répondre collectivement à une crise cyber.