ASSEMBLÉE NATIONALE

9 novembre 2022

D’ORIENTATION ET DE PROGRAMMATION DU MINISTÈRE DE L’INTÉRIEUR - (N° 436)

Commission	
Gouvernement	

Rejeté

AMENDEMENT

N º 526

présenté par

M. Lopez-Liguori, Mme Le Pen, M. Barthès, M. Baubry, Mme Auzanot, M. Allisio, M. Ballard, M. Beaurain, M. Bentz, M. Berteloot, M. Bilde, M. Blairy, Mme Blanc, M. Boccaletti, Mme Bordes, M. Bovet, M. Buisson, M. Cabrolier, M. Catteau, M. Chenu, M. Chudeau, Mme Colombier, Mme Cousin, Mme Da Conceicao Carvalho, M. de Lépinau, M. Dessigny, Mme Diaz, Mme Dogor-Such, M. Dragon, Mme Engrand, M. Falcon, M. François, M. Frappé, Mme Frigout, Mme Galzy, M. Giletti, M. Gillet, M. Girard, M. Gonzalez, Mme Florence Goulet, Mme Grangier, M. Grenon, M. Guiniot, M. Guitton, Mme Hamelet, M. Houssin, M. Hébrard, M. Jacobelli, M. Jolly, Mme Laporte, Mme Lavalette, Mme Lechanteux, Mme Lelouis, Mme Levavasseur, Mme Loir, Mme Lorho, M. Lottiaux, M. Loubet, M. Marchio, Mme Martinez, Mme Alexandra Masson, M. Bryan Masson, M. Mauvieux, M. Meizonnet, Mme Menache, M. Meurin, M. Muller, Mme Mélin, M. Ménagé, M. Odoul, Mme Mathilde Paris, Mme Parmentier, M. Pfeffer, Mme Pollet, M. Rambaud, Mme Ranc, M. Rancoule, Mme Robert-Dehault, Mme Roullaud, Mme Sabatini, M. Sabatou, M. Salmon, M. Schreck, M. Taché de la Pagerie, M. Jean-Philippe Tanguy, M. Taverne, M. Tivoli et M. Villedieu

---

ARTICLE PREMIER

RAPPORT ANNEXÉ

Après l’alinéa 30, insérer l’alinéa suivant :

« La commande publique dans le domaine du cyber devra être dirigée exclusivement vers des entreprises dont la société mère est établie en France ou dans un État membre de l’Union européenne, afin de favoriser l’écosystème français et européen et éviter tout risque d’espionnage, de vol de données ou de piratage provenant d’un État extra-européen. Il s’agit aussi d’éviter de contracter avec des entreprises soumises à des législations hors Union européenne. »

EXPOSÉ SOMMAIRE

Dans le cadre du développement de la menace cyber plusieurs constats peuvent être faits.

On observe d’abord, une progressive convergence dans les techniques et outils employés par les groupes cybercriminels et les attaquants travaillant au profit d’intérêts interétatiques. Les acteurs sont plus furtifs, plus compétents et disposent d'outils plus sophistiqués.

En outre, les tentatives de pré-positionnement intervenant au sein d’infrastructures nationales appartenant à des domaines critiques (transport, énergie, approvisionnement) vont croissant. Celles-ci pourraient offrir, à terme, des marges de manœuvre à d’éventuels assaillants souhaitant entreprendre des activités de sabotage.

Par ailleurs, les tentatives de compromission de cible(s) de haute valeur augmentent également. L’utilisation d’outils sophistiqués complique la détection de ce type de compromission et l’attribution des attaques à leurs commanditaires. Les pratiques décrites ci-dessus concernent également les attaquants répondant à des intérêts étatiques, dans un but d’espionnage.

A la vue de ces inquiétantes évolutions, il est nécessaire d'avoir recours à des entreprises françaises et européennes pour assurer la cybersécurité intérieure, afin de limiter au maximum les risques d'ingérence ennemie. Cela permettra aussi de stimuler l'écosystème tech français et européen et de faire émerger des géants du numérique, des acteurs avec lesquels l'Etat pourra passer des contrats en toute confiance.

Il s'agit aussi d'éviter de contracter avec des entreprises soumises à des législations extra territoriales telles que le cloud act aux Etats-Unis par exemple. Le cloud act permet aux autorités américaines d’accéder aux données stockées par des entreprises américaines ou étrangères présentes sur le sol américain. Cette intrusion met en péril les données des Français au bout de la chaine. Une vigilance accrue sur ce point est donc particulièrement nécessaire.