Pour une stratégie offensive de lutte contre la désinformation à l'ère du numérique

Olivier CADIC
Sénateur représentant les Français établis hors de France
Vice-président de la commission des Affaires étrangères, de la Défense et des Forces armées

Si l'on définit la désinformation comme l'art de tromper le jugement d'autrui, la manœuvre est aussi vieille que l'humanité. Des hordes de comptes robotisés pilotés depuis l'étranger s'apprêtent-elles à polluer le débat public sur les réseaux sociaux en diffusant massivement de fausses informations pour influencer l'élection présidentielle des 10 et 24 avril, s'interrogeait le journal Le Monde, le 18 février dernier ?

Quel chemin parcouru depuis la dernière échéance présidentielle ! La société civile a pris conscience qu'elle vivait en pleine guerre froide de l'information.

Une guerre de la communication a été enclenchée, une guerre destinée à réécrire l'histoire et à dénigrer les démocraties pour préparer la reconfiguration du paysage géopolitique de l'après-crise, c'est le constat que je posais avec mon collègue sénateur Rachel Mazuir dans notre rapport « Désinformation, cyberattaques, cybermalveillance : l'autre guerre du Covid-19 », publié en juin 2020, tandis que des millions de Français avaient basculé dans le télétravail. Dans nos recommandations, nous avions appelé à la mise en place d'une « force de réaction rapide » pour contrer les fausses nouvelles, une structure en faveur de laquelle je plaidais depuis des années pour compléter notre dispositif anti-fake news, après le vote de la loi contre la manipulation de l'information en décembre 2018.

Nous avons été entendus par le gouvernement qui a lancé, en février 2021, une stratégie d'accélération de la filière cybersécurité en France et la création de Viginum, opérationnelle depuis décembre 2021.

Cette nouvelle agence gouvernementale a pour mission de détecter les opérations de désinformation sur les plateformes en ligne et d'en informer les pouvoirs publics. Viginum est appelée à jouer un rôle important pendant les périodes électorales en fournissant toute information utile au Conseil supérieur de l'audiovisuel, au Conseil constitutionnel et à la Commission nationale de contrôle de la campagne électorale.

Il s'agit d'une avancée importante, mais je regrette une certaine timidité dans l'approche. Viginum est uniquement chargée de remonter des observations et n'a pas de pouvoir contraignant. Autrement dit, ses agents ont interdiction d'interagir avec les autres utilisateurs : pas question de poster quoi que ce soit sur les réseaux sociaux.

Face à la propagation de fake news par la Chine continentale, les autorités taiwanaises ont mis en place une organisation de « fact-checking » qui permet d'expliquer une fausse nouvelle en moins deux heures et en moins de 200 mots. J'ai indiqué au directeur du SGDSN que nous devrions nous inspirer de cette expérience taiwanaise pour définir le modus operandi de Viginum.
Autre remarque : demeurer sur la défensive ne devrait pas rimer avec faiblesse de réaction. Lorsque le site de

l'ambassade de Chine publie, en pleine crise du Covid, que nous laissons mourir les gens dans les Ephad, on se contente de convoquer l'ambassadeur. Si notre ambassade à Pékin racontait ce qui se passe au Xinjiang, son compte serait immédiatement fermé et l'ambassadeur expulsé, nous a confié un diplomate lors de son audition devant la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat.

On entend souvent dire que la meilleure des protections c'est l'éducation, qu'il faut miser sur l'esprit critique ou bien encore que les plateformes de réseaux sociaux doivent s'autoréguler. Tout cela est vrai, il n'empêche que l'attaquant a toujours un coup d'avance sur sa cible.

C'est pourquoi je prône la création d'une CyberForce qui lutterait de manière offensive. Le but serait d'inverser le jeu. Ainsi, en adoptant cette nouvelle cyber-doctrine, les démocraties pourraient faire passer des messages offensifs aux populations vivant sous dictature en leur laissant entendre qu'un autre monde est possible et souhaitable.

Le temps fera son œuvre. Pour l'heure, je suis heureux de constater que nous avons accompli en 2021 un grand pas vers un « écosystème français » qui place la France en pointe en matière cyber, à l'image de ce que j'ai pu observer à Beer Sheva en Israël en janvier 2019. Je pense au développement de diverses initiatives, comme le Campus Cyber de la Défense ou le pôle de compétences en cyberdéfense à Rennes.

Dans ce domaine la France est en avance et c'est heureux, car nos sociétés démocratiques sont très perméables aux actions massives et répétées de désinformation et de manipulation de l'opinion. Dans cette bataille des opinions, les démocraties européennes ne doivent pas se montrer naïves. Elles doivent au contraire accroître la défense et la promotion de leurs valeurs en renforçant leur vigilance et en se dotant d'instruments efficaces.
Début mai 2018, je m'étais rendu au Pentagone qui avait établi que les fake news étaient clairement la principale menace en termes de guerre hybride.

L'adoption de la Loi de Programmation Militaire par le Sénat, le 29 mai 2018, a inclus ma proposition de prise en compte de « la manipulation de l'opinion publique par l'utilisation massive des médias numériques et des réseaux sociaux avec pour objectif l'altération du fonctionnement normal des institutions démocratiques ».

La présidence française de l'Union européenne doit constituer une fenêtre d'opportunités pour faire avancer les dossiers cyber au plan européen, comme la lutte contre la désinformation.

En mai 2017, le président Macron répondait en ces termes à une journaliste russe de RT qui se plaignait d'avoir été exclue de son QG pendant la campagne présidentielle : « Quand des organes de presse répandent des contrevérités infamantes, ce ne sont plus des journalistes, ce sont des organes d'influence », a-t-il justifié pour interdire d'accès Russia Today et Sputnik à son quartier général.

La crise ukrainienne aura agi comme un catalyseur : c'est toute l'Europe qui vient de bannir ces organes qu'il convient de qualifier d'ingérence, désormais.

Le prochain quinquennat devra permettre d'armer une cyber-stratégie pro-active, doublée d'efforts législatifs, dont la meilleure échelle est assurément l'Europe. N'attendons pas un « 11-Septembre de la Cyber » pour comprendre que les démocraties doivent s'allier sans tarder pour combattre un ennemi qui se joue des frontières et cherche à les détruire de l'intérieur.