Coronavirus : la cybersécurité conjugue résilience et relance

Jean-Charles LARSONNEUR
Député du Finistère

La crise sanitaire que nous traversons est inédite par sa soudaineté, son universalité et sa violence. Si elle agit comme un révélateur de nos vulnérabilités dans le domaine cyber, elle représente également un moment de prise de conscience dont nous devons collectivement nous saisir, ainsi qu'un puissant catalyseur de solutions plus sûres, plus résilientes et plus souveraines. Outre nos armées, les opérateurs d'importance vitale, les secteurs de la santé, de la grande consommation, des banques, des médias, mais aussi les particuliers ont été touchés par une recrudescence d'actes malveillants : déni de service, campagnes d'hameçonnage, diffusion de programmes espions ou fausses nouvelles. En grec ancien, la krisis renvoie à la notion de pic ou d'acmé, mais aussi à l'action de trier, de passer au crible. De cette crise, nous devons tirer les enseignements pour mieux aborder le monde d'après.

Le confinement a d'abord engendré une intensification du recours au télétravail. Les mesures de distanciation sociale et l'évolution des pratiques donnent à penser que ce phénomène sera durable. Or, les vulnérabilités que le travail à distance crée dans les systèmes d'information sont largement exploitées par les cyberattaquants. À l'évidence, nos entreprises et institutions avaient insuffisamment anticipé cette tendance et continuent parfois de sous-estimer les risques, notamment de demandes de rançon, d'escroqueries ou d'espionnage. Le recours massif à des outils comme Zoom en est une illustration. Cette application a démontré de sérieuses fragilités, poussant des États comme Taïwan à bannir son utilisation par les opérateurs publics. Au début de la crise, les première auditions à huis-clos de la commission de la Défense et des Forces armées de l'Assemblée nationale ont été organisées via ce logiciel. La mobilisation des députés et des acteurs institutionnels a permis qu'une solution souveraine lui soit rapidement préférée (Orange Videopresence). Il existe en outre des solutions alternatives poussées par l'ANSSI comme Tixeo. Dans le domaine des messageries instantanées, on peut regretter l'utilisation de WhatsApp à des fins professionnelles quand d'autres applications offrent des communications plus sécurisées (Citadel, Signal). Les projets de cloud et de messagerie souveraine (Tchap) sont aujourd'hui plus que jamais une nécessité. En somme, ce virage digital est l'opportunité de diffuser plus largement une culture et une conscience du risque cyber, par des actions de formation, de pédagogie et de prévention en s'appuyant sur les outils existants comme la plateforme cybermalveillance.fr. Pour les entreprises, le cyber ne doit plus être perçu comme une contrainte et une charge financière mais comme un investissement au service de la performance économique.

Le deuxième enseignement que l'on peut tirer se trouve dans la vulnérabilité de certains établissements publics (hôpitaux, collectivités territoriales…). Nombre d'entre eux ont été la cible de cyber malveillances. Dans la mesure où l'on ne peut exclure de nouvelles vagues épidémiques, il serait déraisonnable de faire l'économie d'investissements importants dans la cybersécurité du parc hospitalier, sous peine de paralysie. À cet égard, je salue la constance avec laquelle les gouvernements ont soutenu l'ANSSI,

responsable de la cyberprotection et de la lutte informatique défensive. Entre 2015 et 2020, les effectifs de l'ANSSI sont passés de 460 à 692 ETP. L'objectif est de les porter à 750 pour un fonctionnement optimal selon le directeur général. Les ressources budgétaires ont suivi une évolution analogue (+ 62 % en 3 ans, 49,6 millions d'euros en 2018). La crise économique ne doit pas enrayer cette montée en puissance. Le BSI (son équivalent allemand) dénombre 850 agents et dispose d'un budget d'environ 110 millions d'euros par an. Enfin, outre ce levier financier, je soutiens la mise en place de « référents cyber » au sein des établissements publics et des collectivités locales pour améliorer la prophylaxie numérique et la diffusion de bonnes pratiques, en lien avec les représentants locaux de l'ANSSI.

Par ailleurs, les fausses informations prolifèrent dans le terreau fertile que constituent les capacités de viralité offertes par les réseaux sociaux et la défiance de nos concitoyens. Certaines relèvent de la stratégie d'influence de puissances étrangères, d'autres du complotisme. Mais la frontière entre liberté d'opinion, propagande et désinformation est ténue. L'État a trop longtemps laissé faire. Cette majorité a œuvré pour que voie le jour un dialogue renforcé avec les grandes plateformes, noué au niveau interministériel sous l'impulsion de l'Ambassadeur du Numérique. La responsabilité des réseaux sociaux et des hébergeurs est désormais engagée. Facebook a ainsi mis en place un onglet avec des informations vérifiées et référencées, Twitter ayant pour sa part censuré certains tweets du président brésilien Jair Bolsonaro. Cette dynamique doit être activement poursuivie et entretenue.

Enfin, la loi de programmation militaire 2019-2025 prévoit la création de 1 500 postes et un montant de 1,6 milliard d'euros au profit de la cyberdéfense, par exemple sur le pôle de Bruz en Bretagne. Nous devrons, je le souhaite, aller plus loin dans le domaine de la cybersécurité maritime, en faisant fond sur les dispositifs existants, notamment à Brest (MICA Center, MSC-HOA pour la Corne de l'Afrique) ou encore à Toulon. En dépit des inévitables tensions à venir sur les budgets nationaux, je plaide pour préserver ces orientations dans l'actualisation de la loi de programmation militaire en 2021.

Vous l'aurez compris, les défis sont immenses, et la majorité présidentielle pleinement à la tâche pour les relever.