©JuSun/istockphoto

Cybersécurité : l'heure est à l'action

Sénateur représentant des Français établis hors de France, Olivier Cadic est président de la commission spéciale cybersécurité. Il alerte entreprises et pouvoirs publics sur des risques souvent sous-estimés.

Par Sandrine Weisz et Olivier Nifle

© AV

OLIVIER CADIC
Sénateur et président de la commission cybersécurité

Les attaques de cybersécurité désignent un spectre large…
Effectivement, on dénombre beaucoup de formes d'attaques. Parmi elles, le déni de service en ligne qui rend les services inaccessibles, le *fishing* ou hameçonnage (récupération d'informations personnelles à des fins malveillantes) qui touche les particuliers mais aussi les entreprises. Quant aux attaques contre des infrastructures critiques (transports, hôpitaux…) par des rançongiciels, elles visent à les bloquer ou les faire dysfonctionner, allant jusqu'à mettre en danger des vies humaines (voir encadré). Il y a aussi les vols de données à grande échelle et l'atteinte à l'intégrité de l'information : diffusion massive de *fake news* sur un produit, une entreprise ou un État et l'usurpation d'identité de personnalités économiques ou politiques. Enfin, si on se projette à échéance de trois ou quatre ans, nous devons préparer l'Europe à un conflit qui sera hybride : guerre physique et cyberattaques visant par ▸▸▸

exemple à déstabiliser les populations en donnant des fausses informations sur le conflit, des fausses consignes… Cela explique pourquoi le SGDSN (Secrétariat général de la défense et de la sécurité nationale) a publié le document « Tous responsables » afin de nous permettre de nous préparer. L'heure n'est plus à l'ignorance mais à l'action.

Vous dites qu'on voit la paille dans l'œil de son voisin, mais pas la poutre dans le sien…

Oui, prenons l'exemple des élections présidentielles de 2024 en Roumanie. Les résultats du premier tour du scrutin avaient été annulés après une diffusion massive de messages sur TikTok qui avait propulsé en quelques semaines un candidat d'extrême droite de 1,5 % des intentions de vote à plus de 24 % (Ndlr : 25 000 comptes TikTok ont été recensés comme très actifs deux semaines avant la date du scrutin). Mais en France, on s'étonne moins de la montée en puissance, grâce aux réseaux sociaux, de certains candidats. L'un d'eux a été baptisé par un hebdomadaire « le prince de Tik Tok ». Quelle naïveté !

DR

WASHINGTON
Échanges au Cisa (Cybersecurity and Infrastructure Security Agency), agence fédérale de cybersécurité. Février 2024

©solarseven/Istockphoto

Quels sont les pays particulièrement actifs dans le domaine de la cybercriminalité ?

La Russie a été identifiée par Viginum[1] dans plusieurs opérations nous visant. Nous avons également documenté la montée en puissance de la Chine qui s'est inspirée de la Russie et pille nos entreprises grâce au cyberespionnage. La Corée du Nord fait de la cybercriminalité, c'est même une source de revenus pour l'État. Si on doit établir aujourd'hui un podium des pays qui nous menacent, je dirais : Chine, Russie, Iran. D'autres pays comme l'Azerbaïdjan ont été dénoncés pour leur opération de déstabilisation en Nouvelle-Calédonie. La guerre cyber n'est pas une hypothèse lointaine. Elle est déjà en cours. La France en est une cible de choix.

La cybersécurité est-elle un enjeu européen ? Jusqu'où se fier à nos voisins ?

Quand je travaillais dans l'innovation, je disais souvent : *« Votre présent est mon passé. »* Aujourd'hui, au Sénat, je constate que nous vivons trop souvent dans le passé de nos adversaires. Nous sommes en réaction permanente, alors qu'eux agissent avec une stratégie de long terme. Les démocraties hésitent à utiliser les mêmes méthodes que leurs ennemis, par respect pour l'État de droit. Mais cette retenue ne doit pas devenir une faiblesse. La « cyber solidarité » entre l'Union européenne et les États-Unis, prônée par l'administration Biden, lorsque je m'étais rendu à la Maison Blanche l'an dernier, reste une nécessité absolue. Les coopérations policières et judiciaires progressent. La cybercriminalité ignore les frontières : si nous ne renforçons pas nos alliances, nous serons vulnérables, car nous sommes interdépendants.

Que conseillez-vous aux entreprises au regard de ces menaces ?

Le hasard favorise plutôt les entreprises les mieux préparées. Veiller à son indépendance technologique et anticiper les bouleversements géopolitiques ne sont plus des options, mais des impératifs de survie. Le respect de la norme ISO 27001

1 Service de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères

dite « Systèmes de management de la sécurité de l'information » remplit les obligations de la directive européenne NIS2. Les entreprises comme les administrations devraient s'y conformer.
Je conseille aussi de privilégier des outils souverains (voir encadré) : Olvid plutôt que Signal, Le Chat de Mistral pour l'IA, OVH pour l'hébergement, CybelAngel pour détecter les signaux faibles et réagir avant qu'une attaque ne se concrétise ou encore Odaseva, pour sa suite logicielle innovante couvrant la protection des données, la sécurité zéro-trust, l'archivage long terme, et la conformité RGPD.

50 % des PME victimes d'une cyberattaque feraient faillite dans les 12 mois suivants. Comment réagir ?
La réponse est claire : former ses employés à reconnaître un e-mail de *phishing*, mettre à jour régulièrement ses logiciels, et sauvegarder ses données hors ligne.
Le site cybermalveillance.gouv. fr est un outil exceptionnel pour se préparer. Les États-Unis ont unifié leur réponse avec le FBI comme point d'entrée unique pour tracer les cyberattaquants. En France, nous avons enfin le 17Cyber, une avancée majeure, inspirée du modèle israélien, que j'ai portée dès 2019 et que le Président de la République a concrétisée en décembre 2024. Il nous faut accélérer pour bloquer les transactions de paiement des rançons.

Est-ce que l'Europe en fait assez en matière de cybersécurité ?
L'Europe avance mais trop lentement selon mon avis. Ces directives sont essentielles, mais nous devons veiller à ne pas créer de failles avec nos alliés.
Par exemple, les autorités américaines imposent des délais d'une semaine pour corriger une faille critique, quand la réglementation DORA accorde trois mois pour installer un patch. Un tel écart pourrait mettre nos institutions financières en danger.

Une solidarité internationale totale est-elle vraiment envisageable ?
La montée du « moi d'abord », aux États-Unis comme en Europe, rend la tâche plus difficile. Pourtant, l'histoire nous enseigne une leçon : c'est la clarté des blocs et la fermeté des démocraties qui ont évité un conflit ouvert pendant la guerre froide. Aujourd'hui, face à la Chine et à la Russie, nous devons appliquer la même logique. Les régimes autoritaires construisent des digues pour isoler leurs populations. Nous, nous devons utiliser ces digues à notre avantage : protéger nos valeurs, nos économies, et dissuader toute agression. Nous avons l'impression de revenir au temps de la guerre froide, au regard de ces menaces. La guerre froide a été une période de tensions, mais aussi de stabilité, parce que chaque camp connaissait les lignes rouges de l'autre. Aujourd'hui, nous devons rétablir cette clarté.
Lors de mes récentes réunions avec les conseillers du Commerce extérieur à Los Angeles, San Diego, Atlanta, Miami et New York, j'ai constaté que la politique américaine, qu'elle soit démocrate ou républicaine, converge vers un même objectif : poursuivre une politique de découplage technologique et économique pour protéger ses intérêts face à des régimes autoritaires qui ne jouent pas selon les mêmes règles. J'y vois une logique fondée sur un réalisme indispensable plutôt qu'un retour en arrière. ■

DES ALTERNATIVES À LA *TECH* AMÉRICAINE

Dans les domaines du *cloud*, de la messagerie, des moteurs de recherche, de l'assistant conversationnel, l'Europe propose des solutions performantes, certes moins connues que celles des grands noms américains. Parmi elles : Mistral AI, Olvid, Leviia…■

INFRASTRUCTURES DE TRANSPORT VISÉES

©BoardingNow/Istockphoto

Plusieurs aéroports européens, dont ceux de Bruxelles, Heathrow à Londres, et Berlin, ont été touchés en septembre 2025 par une attaque « cyber » affectant un logiciel. Conséquence : problèmes d'affichage, d'enregistrement des passagers et annulations de vols. ■