CYBERSÉCURITÉ : UNE QUESTION DE CONFIANCE

Si cette notion se trouve au cœur du projet européen, elle prend tout son sens lorsqu'on parle de cybersécurité. C'est bien ce qui est ressorti des échanges du séminaire organisé par Confrontations Europe à Bruxelles le 21 juin, illustré par l'exemple du secteur énergétique.


© DR

La grande majorité des acteurs européens est convaincue de la nécessité d'une coopération entre États membres plus poussée pour renforcer notre capacité collective à faire face aux cybermenaces grandissantes. Ces considérations n'épargnent évidemment pas les acteurs de l'énergie, secteur critique pour le bon fonctionnement de nos sociétés. Mais beaucoup de questions semblent rester en suspens. Au cœur des débats, c'est bien celle de la confiance entre acteurs qui se pose. Que sommes-nous prêts à partager pour créer une approche collective européenne de la cybersécurité, et quels moyens accordons-nous à nos ambitions ? C'est ce que le « Paquet Cybersécurité », présenté par la Commission Européenne en septembre 2017, tente d'éclaircir.

Anticiper, prévenir et répondre aux attaques. Cela nécessite un partage d'information rapide et une capacité d'action coordonnée entre États. Si chacun s'accorde sur ce point, force est de constater que la ligne entre prérogatives nationales et délégation de pouvoir vers l'UE reste difficile à tracer. D'un côté, la Commission européenne souhaite transformer l'actuelle Agence Européenne de sécurité des réseaux (ENISA) en une Agence européenne de la cybersécurité dotée de plus de responsabilités. De l'autre, certains États, comme la France ou l'Allemagne, craignent qu'une agence européenne empiète sur leur propre agence nationale, qui sont, elles, bien mieux ancrées sur leur territoire. Pour Michal Boni, député européen, « il n'y a pas de cybersécurité européenne possible sans l'implication des institutions, des solutions et des économies nationales ». Une vision partagée par des acteurs de terrain, tels qu'Enedis, pour qui il est crucial de respecter la confiance mutuelle que les acteurs ont su créer avec leur agence nationale, collaborant étroitement dans la mise en œuvre de solutions de cybersécurité adaptées à un secteur particulier. Mais il ne faut pas non plus mésestimer les grandes disparités entre États membres, qui ne possèdent pas tous d'agence nationale ni même parfois de stratégie cybersécurité. Pour Michal Boni, c'est donc bien au niveau européen que la coordination doit s'opérer, et l'ENISA reste l'acteur le mieux placé.

Autonomie ou compétitivité, faut-il choisir ?

Il y a un clair intérêt stratégique pour l'Europe à développer une solide industrie de la cybersécurité et renforcer son autonomie numérique. Pour ECSO, membre du partenariat public-privé européen sur la cybersécurité, il s'agit de favoriser l'innovation et la maîtrise des compétences et technologies nécessaires à la sécurisation de nos systèmes, afin de réduire notre dépendance grandissante à des technologies provenant de pays tiers. Créer un marché de la cybersécurité est bien l'objectif visé par la Commission européenne lorsqu'elle propose de mettre en place une certification européenne des produits (une sorte de label européen de la cybersécurité) afin d'harmoniser le marché européen. Mais la cybersécurité étant un enjeu global, il faut donc pouvoir conserver l'interopérabilité avec les autres marchés du monde. Pour un acteur tel que Microsoft, il est en effet crucial de privilégier la reconnaissance mutuelle des standards, car une certification européenne risque de s'avérer trop coûteuse à obtenir pour les PMEs, et de ne profiter qu'aux géants déjà existants (Amazon, Google...) au détriment de la création d'un environnement européen compétitif. L'industrie insiste ainsi pour continuer à être impliquée dans les discussions sur la certification afin de construire la confiance à tous les niveaux, notamment régionaux, et ne pas freiner l'innovation. Les industries et les PMEs doivent collaborer et partager leurs pratiques afin de monter en compétences. Enfin, développer un leadership européen sur la cybersécurité passera aussi par une coopération avec d'autres régions du monde en pointe sur ces sujets.

Finalement, comme le fait remarquer Michal Boni, « *développer un marché européen de la cybersécurité est une opportunité unique de renforcer l'industrie et de créer un avantage compétitif de l'Europe sur la scène globale* ». Mais construire une autonomie européenne digitale ne signifie pas ériger un marché coupé du reste du monde.

Morgane Goret-Le Guen, *chargée de mission Energie & Numérique à Confrontations Europe*