Vers une autonomie stratégique européenne de la cybersécurité

Portée par le ministre Bruno Le Maire et la secrétaire d'État Agnès Pannier-Runacher sous l'angle économique ainsi que par Florence Parly sous l'angle Défense, l'autonomie stratégique européenne revêt un caractère essentiel de notre capacité à adresser les défis futurs en matière de numérique et de cyber notamment.

Cette souveraineté numérique faisant par ailleurs l'objet d'une commission d'enquête du Sénat, ne s'arrête pas aux frontières nationales.

Des partenariats stratégiques forts

En effet, pour assurer et renforcer cette souveraineté numérique et bâtir cette autonomie stratégique européenne, des partenariats stratégiques forts entre petites et grandes entreprises, présentes sur l'ensemble du vieux continent, seront nécessaires.

Nous avons l'obligation de poursuivre et de concrétiser le dialogue engagé avec des responsabilités à assumer de part et d'autre. Plus de structuration d'un côté, plus de rapidité dans les process et les décisions de l'autre. Le tout avec une convergence plus fine d'objectifs communs.

Une consolidation de la filière

Forte d'une reconnaissance de son expertise scientifique et de solutions robustes et agiles capables de répondre aux cyber risques et à leurs évolutions permanentes, la filière tricolore dispose de toutes les compétences et de toutes les énergies pour adresser ce marché européen et mondial.

Mais cela passe bien entendu par la consolidation de cette filière, une action collective capable de fédérer les talents et rendre interopérables des solutions qui à terme doivent se rassembler pour répondre aux besoins des utilisateurs finaux, qu'ils soient une entreprise ou un État. Le tout porté par une stratégie globale et une volonté politique affirmée.

Vers une cartographie des risques au niveau européen

L'autonomie stratégique européenne est donc un enjeu fort. La méthode EBIOS – sous l'impulsion de l'ANSSI – ambitionne d'aider les acteurs de la cybersécurité à mettre en place une cartographie des risques au niveau européen. Cette impulsion stratégique donnée par l'ANSSI nous ouvre le champ des possibles et favorisera incontestablement le passage à l'échelle, vital à la santé

économique de nos entreprises.

Cette cartographie globale doit émerger, s'appuyer et s'enrichir d'un partage et d'une mutualisation essentielle de nos expertises et de nos données techniques, au travers d'un modèle collaboratif. Cette nouvelle approche permettra ainsi d'élever le niveau de cybersécurité global poussé par une réglementation forte et un régulateur puissant.

Cette idée retenue par des experts est par ailleurs actuellement poussée au Luxembourg.

Cybersécurité, cloud et données

Enfin, il est essentiel de proposer nos solutions de cybersécurité dans le cloud et d'aborder la question de la souveraineté non pas sous l'angle du support ou de l'architecture physique mais bien sur le plan de la donnée. Elle est un élément central de cette souveraineté. Les technologies de protection de cette donnée existent, notamment la cryptographie. Elles permettent d'envisager un champ des possibles très large, qu'il s'agisse de sa localisation ou des méthodes pour la traiter ou y accéder.

Qu'elle soit localisée dans un cloud souverain, privé, public, en France, ou ailleurs…. la confiance est essentielle mais n'est plus un sujet de capacité technique. Il faut alors changer de combat et évoluer. Evoluer culturellement, et renforcer la coopération saine entre acteurs. Il faut enfin compter sur l'intelligence artificielle qui est un élément clé, lui aussi, de l'avenir, sur lequel nous investissons !