



Position ACN sur la proposition de règlement sur le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité (ECCC) - COM(2018)630

4 octobre 2018

L'ACN partage les objectifs du projet de règlement et notamment l'objectif de renforcement des capacités technologiques et industrielles nécessaires à la sécurisation du marché unique du numérique, ainsi que l'amélioration de la compétitivité de l'industrie européenne de cybersécurité.

La recherche de synergie et de cohérence dans les actions de recherche en cybersécurité au niveau européen par la création d'une communauté limitée aux entités établies dans l'UE et le financement d'infrastructures, de produits et solutions de cybersécurité, prévus dans ce projet de règlement sont également des objectifs de premier plan partagés par l'ACN.

L'identification de centres nationaux de compétences et leur mise en réseau constituent une démarche appropriée en vue de ces objectifs. Un lien très fort entre industrie et recherche dans ce domaine est un facteur majeur pour parvenir à ces objectifs. Une interaction avec les différents secteurs utilisateurs est également nécessaire.

Le cPPP cybersécurité et la création d'ECSO ont posé des bases essentielles et ont conduit à plusieurs avancées majeures dans la réalisation de ces mêmes objectifs. L'ACN partage l'idée d'amplifier les aspects positifs de cette expérience dans le cadre de ce projet de règlement.

A la lumière de ces enseignements, l'ACN souhaite que le futur ECCC :

- s'inscrive dans une synergie avec les autres initiatives existantes,
- prévoie une bonne association de l'ensemble des parties prenantes de l'écosystème de la cybersécurité (notamment industriels et académiques), et se dote de règles de transparence accrues dans tous les niveaux de son fonctionnement.
- intègre la vocation de cet écosystème à participer collégalement à l'élaboration d'une politique industrielle européenne en matière de cybersécurité,
- promeuve activement une logique d'incitation à l'investissement (éventuellement partagé) et à l'équipement des Etats-membres, compléments indispensables à la coordination des actions de recherche.
- adresse plus directement la problématique de la formation et de la sensibilisation à la cybersécurité : des ressources devraient être allouées notamment aux programmes de formation primaire et de reconversion / amélioration des compétences, ainsi que l'intensification des campagnes européennes de cyber-sensibilisation et de formation destinées aux citoyens et aux entreprises.
- apporte un soutien renforcé à la standardisation en particulier par le financement des travaux des experts en lien avec les besoins liés à la mise en œuvre des directives européennes. Ceci mis en œuvre par les ESO's (European standardisation organisation), le CEN, le CENELEC, et l'ETSI.

En conséquence, l'ACN souhaite appeler l'attention sur les points suivants :

1. Intégrer les acteurs industriels et académiques à la gouvernance du ECCC

La bonne association des acteurs industriels et académiques, moteurs de la cybersécurité, à la gouvernance du centre européen de compétence est une nécessité au bon fonctionnement de cette instance. A la lumière de l'expérience du cPPP, cette gouvernance multipartite est une clé de succès pour une telle initiative. La proposition visant à limiter la présence de ces acteurs majeurs à une assemblée consultative semble inappropriée.



2. Créer un lien fort et permanent avec les secteurs utilisateurs

Le concept d'« advisory body » a souvent démontré son inefficacité. L'ACN propose de le remplacer par une instance multipartite d'échanges entre l'écosystème de la cybersécurité (tel que défini dans le « Governing board » augmenté des industriels et des académiques) et les secteurs utilisateurs. Cette instance « Implementation board » pourrait être organisée en task forces sectorielles (énergie, défense, santé, transport, espace...) et avoir pour mission, sous le contrôle du « Governing board », d'alimenter l'ENISA pour la création de schémas de certifications sectoriels. Le ECCC pourrait avoir pour rôle, à travers ce « Implementation board » de fédérer toutes les autres initiatives cybersécurité sectorielles de l'UE et les TF pourraient être financées par les budgets prévus pour ces initiatives.

3. Assurer une bonne cohérence avec les initiatives existantes (ECISO, projets pilotes, NIS, ENISA) :

- le projet de règlement présente des similitudes avec certaines fonctions assurées par ECISO. L'ACN souhaite une clarification sur ce sujet et que le fonctionnement d'ECISO puisse servir de modèle au « Governing board ».
- La Commission européenne a initié un appel à projet concernant des consortia européens de recherche en cybersécurité (les projets « pilotes » du SU-ICT-03). Les termes de l'appel à projet concernant les projets pilotes rejoignent en partie les prérogatives proposées pour le ECCC. En particulier, l'une des missions de ces projets est de proposer et d'expérimenter des modèles de gouvernance. L'ACN souhaite que la combinaison de ces deux initiatives soit clarifiée.
- Le projet de règlement vise à réunir des représentants nationaux et à favoriser leurs échanges/synergies en matière de cybersécurité. Cette démarche est semblable à celle issue de la directive NIS et à celle impulsée dans le cadre du European Cybersecurity Act. L'ACN souhaite qu'une cohérence dans la représentation des Etats membres soit assurée entre ces textes.
- L'ECCC devrait jouer un rôle de premier plan pour accompagner l'ENISA dans sa mission d'élaboration des schémas de certification.

4. Renforcer la logique d'investissement dans les infrastructures et les produits et solutions de cybersécurité dans l'UE.

L'ACN propose que cet objectif du ECCC soit précisé et renforcé. En effet, une politique coordonnée de recherche n'atteindra une portée maximale sur la sécurité du marché unique du numérique que si elle s'appuie sur une politique volontariste d'équipement de chacun des Etats-membres en infrastructures et les produits et solutions de cybersécurité potentiellement issus de cette recherche. Aussi l'ACN est très favorable aux dispositions permettant de rechercher un co-investissement dans ces domaines, condition sine qua non du développement d'une industrie de pointe dans ce domaine.

5. Installer le siège de l'ECCC en France

Compte-tenu de la richesse de l'écosystème français et de la longue tradition de collaboration entre les industriels et les acteurs de la recherche académique, l'ACN propose que la France puisse accueillir le siège de l'ECCC.

A propos de l'ACN :

L'Alliance pour la Confiance Numérique (ACN) représente les entreprises (leaders mondiaux, PME, et ETI) du secteur de la confiance numérique notamment celles de la cybersécurité, de l'identité numérique, des communications sécurisées, de la traçabilité / lutte anti-contrefaçon et de la safe city. La France dispose dans ce domaine d'un tissu industriel très performant et d'une excellence internationalement reconnue grâce à des leaders mondiaux, des PME, des ETI et aux différents acteurs dynamiques du secteur. On dénombre environ 850 entreprises réalisant en France près de 9 Milliards d'euros de chiffre d'affaires dans ce secteur en forte croissance (plus de 12% de croissance chaque année depuis 2014). L'ACN est membre de la FIEEC (Fédération des Industries Electriques, Electroniques et de Communication) et participe activement à ce titre aux travaux du CoFIS (Comité de filière des Industries de Sécurité). Par ailleurs, l'ACN est également membre fondateur de l'ECISO (European CyberSecurity Organisation).