ACN's stance on the proposal for a regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) - COM(2018)630

October 4, 2018

The ACN agrees with the objectives of the draft regulation, in particular the objectives of strengthening the technological and industrial capabilities needed to secure the digital single market, and improving the competitiveness of the European cybersecurity industry.

The quest for synergy and consistency in cybersecurity research at European level through the creation of a community restricted to entities established within the EU, and the funding of cybersecurity infrastructures, products and solutions, provided for in this draft regulation, are also some of the foremost objectives that ACN shares.

In view of meeting these objectives, the identification of national competence centres and the creation of a network for them is an appropriate approach. Strong ties between industry and research in this field play a major role in achieving these objectives, while interaction with the various user sectors is also necessary.

The cybersecurity public-private partnership (cPPP) and the creation of ECSO have laid the foundations and led to major breakthroughs in accomplishing the same objectives. ACN also welcomes the idea of amplifying the positive aspects of this experience as part of this draft regulation.

In light of this information, ACN wishes that the future ECCC would:

- encourage synergy with other existing initiatives,
- anticipate the effective association of all stakeholders in the cybersecurity ecosystem (especially industrial and academic actors), and develop advanced rules for transparency in all levels of its operation.
- integrate the purpose of this ecosystem – to participate collectively in building a European cybersecurity industrial policy,
- actively promote an incentive logic to involve (in collaboration where necessary) and equip Member States, indispensably complementing the coordination of research projects.
- address the issue of cybersecurity training and awareness more directly: resources should be allocated in particular to training, either as part of initial training or skill conversion/upgrade programs, as well as the intensification of European cyber-awareness and training campaigns aimed at citizens and businesses.
- provide stronger support to standardisation efforts, in particular by funding the work of experts in relation to the requirement involved in implementing European directives. This as benn implemented by ESOs (European Standard Organisations), the CEN, the CENELEC and the ETSI.

ACN therefore wishes to draw attention to the following points:

1. **Including industrial and academic actors in the governance of the ECCC**

   The effective association of industrial and academic actors that drive cybersecurity, within the governance of the European Competence Centre, is necessary in order for this body to function optimally. In light of the cPPP's experience, a multipartite governance of this scope is the key to success for such an initiative. The proposal aiming to restrict the presence of such major actors to a consultative assembly seems inappropriate.

2. **Creating strong and permanent ties with user sectors**

   The concept of an advisory body has often revealed its ineffectiveness. ACN proposes to replace it with a multipartite body to facilitate communication between the cybersecurity ecosystem (such as the one defined in the enhanced governing board with industrial and academic actors) and user sectors. This “implementation board” may be organised in task forces by sector (energy, defence, healthcare, transportation, space, etc.) and under the purview of the governing board, be tasked with providing information to the ENISA to create sector-based certification schemes. Through this “implementation board”, the ECCC may adopt the role of uniting all other cybersecurity initiatives in the EU, while task forces may be funded by budgets planned for these initiatives.

3. **Ensuring consistency with existing initiatives (ECSO, pilot projects, NIS, ENISA):**

   - The draft regulation shares similarities with several functions performed by ECSO. ACN would like clarification on this topic and hopes that operating as ECSO can serve as an example to the governing board.
   - The European Commission has launched a request for proposals concerning European cybersecurity research consortia ("pilot" projects of SU-ICT-03). The terms of the request for proposals concerning pilot projects correspond in part to the prerogatives proposed for the ECCC. In particular, one of the missions of these projects is to propose and experiment with governance models. ACN wishes for the combination of these two initiatives to be clarified.
   - The draft regulation aims to gather national representatives and foster discussion/synergy in cybersecurity. This approach is similar to the one recommended in the NIS directive and the one put forth as part of the European Cybersecurity Act. ACN would like the guarantee of consistency in the representation of Member States between these legal provisions.
   - The ECCC should occupy a leading role to guide the ENISA in its mission to formulate certification schemes.

4. **Strengthening the logic of investing in infrastructures and cybersecurity products and solutions in the EU.**

   The ACN proposes that this particular objective of the ECCC be clarified and strengthened. A coordinated research policy would only have a maximum reach in the security of the digital single market if it is based on a voluntarist policy of equipping each Member State in terms of infrastructure and cybersecurity products and solutions that may potentially be the result of such research. In addition, ACN strongly supports the provisions that would allow seeking co-investment in these fields, an indispensable condition in the development of a cutting-edge industry in this field.

5. **Establishing the head office of the ECCC in France**

   Given the wealth of the French ecosystem and the long tradition of collaboration between industrial players and actors in academic research, ACN proposes that the head office of the ECCC be based in France.

About ACN:

The Alliance pour la Confiance Numérique (ACN - Alliance for Digital Trust) represents organisations (world leaders, SMEs and mid-sized enterprises) in the digital trust sector, particularly those specialising in cybersecurity, digital identity, secured communications, traceability / anti-counterfeiting and safe city. In this field, France boasts highly efficient industrial cooperation and internationally recognised excellence thanks to world leaders, SMEs, mid-sized enterprises, and the various dynamic actors in the sector. Currently about 850 organisations in France generate a profit of almost 9 billion euros in this rapidly growing sector (growth of more than 12% every year since 2014). ACN is a member of the Fédération des Industries Electriques, Electroniques et de Communication (FIEEC - Federation of Electric, Electronic and Communications Industries) and therefore actively participates in the work of the CoFIS committee (Comité de filière des Industries de Sécurité). ACN is also a founding member of the ECSO (European CyberSecurity Organisation).