ECIS position on the Cybersecurity Competence Centre and Network of National Coordination Centres ("CCCN")

Brussels, May 2019

The European Commission's proposal to establish a Cybersecurity Competence Centre and Network of National Coordination Centres ("**CCCN**") was adopted on 17 April by the European Parliament's Committee on Industry, Research and Energy ("**ITRE**") but awaits the start of another EU mandate for it to pass to trilogue. Whereas ECIS welcomes the initiative's goal to reduce fragmentation across Member States by creating synergies in cybersecurity R&D at national and EU level, we have concerns regarding the *proposed* exclusion of companies headquartered in third countries and thus a departure from a highly effective approach within H2020 and predecessors.

The proposed legislation reads:

> "*At the moment, the Union depends on non-European cybersecurity providers. However, it is in the Union's strategic interest to ensure that it retains and develops essential cybersecurity technological capacities to secure its Digital Single Market, and in particular to protect critical networks and information systems and to provide key cybersecurity services.*"

Many key industry players already actively engaged in developing cyber competencies (for instance improving cyber skills and education), have concerns around Articles 4 and 8.3 of the proposed legislation, which would make third-country participation in the future of European R&D efforts on cybersecurity more difficult, or in certain cases, impossible.

Though there is a legitimate preoccupation surrounding the EU's dependence (as a net importer of cybersecurity products and solutions) on non-European providers, questions remain as to whether this should interfere with the openness of the EU's cybersecurity market. On the one hand, in order to strengthen the cyber industrial base in Europe, EU legislation must be drafted so as to preserve the economic, security and defence interests of the EU and its Member States. However, due to approaches established through frameworks such as Horizon 2020, funding and platforms for cross-border and cross-sector collaboration have created an invaluable R&D infrastructure in the EU cybersecurity space.

Equally, much of the pre-eminent cybersecurity research which has led to the development of outstanding products and services has been the work product of EU subsidiaries of global entities, or developed as a result of cross-border collaboration. In this regard, the open nature of much of security research and development and the open source development process that very often accompanies it, would be negatively affected by discriminating against contributors to such efforts by country of origin. Therefore, non-discrimination with respect to third-country partners and European experts working on global cybersecurity mandates might be regarded as critical to the success of the proposed CCCN, and to the Digital Single Market ("**DSM**"), more broadly.

Cyber threats are global in nature and have been evolving so rapidly that industries have not been able to wait for governments and regulators to intervene. Individual businesses have therefore started to take matters into their own hands and have already launched initiatives to

tackle such issues. The "Charter of Trust" is just one example of an attempt by industry players to initiate close collaboration across global supply chains and to establish principles designed to defeat cyber risks to business.

ECIS maintains that the key to addressing cybersecurity challenges is strong dialogue and open collaboration between stakeholders not only across sectors (such as employment, government and educational sectors), but indeed also across the world. International cooperation must be strengthened in order to keep Europe safe, secure, and resilient.

As set out in AmCham EU's recent position paper on the CCCN proposal released on 15 January 2019, "*aggregate US investment in Europe totalled more than €2 trillion in 2017, directly supporting more than 4.7 million jobs in Europe, and generating billions of euros annually in income, trade and research and development*."[1] Such significant contributions made by U.S.-headquartered companies with operations in the EU represent their vested interest in operating in a "cyber-strong" Europe. It therefore follows that third-country entities often offer unique expertise and experience which would no longer be available following the implementation of exclusionary instructions by the CCCN.

For the reasons set out above, ECIS submits that the restriction of non-EU market participants contradicts the EU's objective to strengthen cyber resilience and that intentions to exclude third-country involvement may hamper the beneficial impacts of the establishment of the CCCN.

ECIS commends the existing adequate protections under Horizon 2020 which ensure that sensitive areas can be restricted to EU entities, and considers that such discretion could be usefully extended to the CCCN initiative. There is no denying that there should be certain security-related restrictions and conditions for partnership between European and third-country entities, which would reaffirm the guiding principle of promoting healthy, home-grown competition and cyber-defence capabilities. On the other hand, ECIS fears that a blanket approach could stifle local and international cybersecurity efforts and progress.

[1] *See:* https://www.amchameu.eu/system/files/position_papers/pop_cybersecurity_competence_centre_and_network.pdf