AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Proposal for a European Cybersecurity Network and a Competence Centre

Fostering openness and excellence

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2017, directly supports more than 4.7 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

Introduction

The recent proposal to create a Cybersecurity Competence Network coupled with a European Cybersecurity Research and Competence Centre is an important strand in EU's Cyber Security Strategy, as outlined in the 2017 joint communication by the Commission and High Representative[1]. This initiative has the potential, if implemented appropriately, to reduce fragmentation and create synergies across the EU in research and investment as well as enhance industrial capacity building between Member States.

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. Given the weight of their investment and presence, US companies operating in Europe are contributing and have a strong interest in achieving a cyber-resilient Europe. The adoption of the funding proposed by the Multiannual-Financial Framework (MFF) through the Digital Europe programme will be vital for the successful achievement of Europe's cybersecurity ambitions including through the Cybersecurity Competence Centre & Network. AmCham EU welcomes that a funding programme has been created to target funding for supporting Europe's digital ambitions, identifying cybersecurity as a priority area.

We acknowledge the EU's legitimate ambition to strengthen its cyber industrial base with a focus on emerging technologies. However, this should not happen by excluding in any way non-EU partners, particularly US partners from participation. The cyber threats facing Europe are global in nature and actions of national states from other parts of the globe mean that maintaining and improving international cooperation with public and private partners - particularly between the EU and US - will remain essential to keep Europe safe, secure and resilient. This is equally true for financing research, development and innovation as well as for attracting foreign direct investment and for promoting international trade in cyber technologies.

The policy recommendations below aim at creating a European Cybersecurity Competence Centre and Network that is based on excellence and openness.

Third-country participation

The context of the proposal mentions the concern that 'at the moment, the Union is a net importer of cybersecurity products and solutions and largely depends on non-European providers. […] In the top 20 of the leading cybersecurity countries from a market perspective, there are only 6 Member States'. While this is a legitimate concern, it should not reduce the openness of EU's cybersecurity market. The development of innovation and competitive solutions depends on the one hand on willingness to invest or the availability of venture capital, and on the other hand the ability to scale up and meet market demands. Hence, **the European cybersecurity industry will benefit from a strong single market.**

Restrictions in the participation of third countries, such as those found in the European Parliament and Council positions on the Digital Europe programme, are in contradiction with the objective to strengthen cyber resilience[2]. Europe's cyber resilience is contingent with operators and providers using state of the art technologies and solutions regardless of their provenance (provided that there are no specific concerns with the relevant actor or nation state itself regarding security, for instance relating to back doors). There is a concern that the Cybersecurity Competence Centre & Network proposal could likewise lead to exclusion of non-EU partners in the implementation of Digital Europe and Horizon Europe projects. Many non-EU headquartered companies develop and export security solutions out of Europe, hence a general prohibition for participating to the Cybersecurity Competence Community will impact a significant number of IT specialists that work across the EU. **We therefore urge the EU co-regulators to carefully consider the impacts of restrictions in the participation of third countries during the trilogue negotiations of the Digital Europe programme**.

[1] https://www.consilium.europa.eu/media/21479/resilience_deterrence_defence_cyber-security_ec.pdf

[2] See AmCham EU's statement on third country participation in MFF funds, available here: http://www.amchameu.eu/system/files/position_papers/amcham_eu_recommendations_on_third-country_participation_in_mff_funds.pdf

Openness in these funding programmes is even more important given that funding models for the proposed Cybersecurity Centre & Network may influence public procurement practices at national level. This is potentially quite serious as there is a risk to restrict tendering procedures to the chosen few with existing capabilities. Participation to public procurement tenders should not be limited to companies on the basis of their geographic origins but should seek the most effective outcomes to develop and procure sound cybersecurity solutions since this breeds innovation and excellence.

Excellence in cybersecurity cannot be achieved solely at a local or regional level, and all companies wherever they are established should be entitled to take part in the Cybersecurity Competence Center & Network based on their excellence. In pursuing security innovation, European and non-European stakeholders should work together, irrespective of their country of origin, and use a technology-neutral approach to increase cybersecurity across the Internet ecosystem. Transatlantic and global cooperation on emerging technologies through the Digital Europe programme and the Cybersecurity Competence Centre & Network has the potential to make Europe more competitive and innovative on the international market. The approaches established in Horizon 2020 and its predecessors, where funding and platforms for collaboration between academia and industry across sectors and countries were provided, have provided a bedrock for R&D in the EU.

Governance structure & Definitions

Role with existing agencies (Article 12)

ENISA, as the permanent EU agency in charge of cybersecurity, should be at the centre of this initiative as an honest broker with existing governance structures. With the entry into force of the EU Cybersecurity Act[3], the agency will be playing an increased role in cybersecurity and therefore it would be consistent to grant ENISA with a key governing role of EU R&D projects and coordinating role of Member State cyber centres.

We therefore support the idea in the ITRE draft report to ensure that ENISA is consulted at all stages and works closely with the Centre to create synergies and consistency in strategic priorities, in line with **Amendment 84 on Article 12.7**: 'The European Agency for Network and Information Security (ENISA) shall ***permanently take part in the deliberations*** of the Governing Board***, in an advisory role without voting rights'*****.**

Likewise, the cooperation with international organisations is essential given that the Centre will be managing international projects, and should be an explicit mission of the Centre, as proposed in **Amendment 55 on Article 4.1.8.a (new)** in the ITRE draft report.

Voting rights to Member States (Article 15)

The proposal to link the voting rights to the financial contribution of Member States bears the risk to exclude certain Members States. This is problematic especially since all Member States have to implement these decisions. Furthermore, such a governance model seems to contradict the EU acquis on cybersecurity which has historically strived to deepen the cooperation between Member States and close the gap with regards their cybersecurity capabilities.

Public procurement (Article 4.4.c. and Article 5.2)

Granting the Competence Centre the power to determine how Member States define their public procurement practices could be inconsistent with the different legitimate needs of Member States (such as in the context of compliance with the NIS Directive, public security, intelligence, defence spending, etc.). This is even more problematic if the governance model allocates voting rights to the benefit of a few (see previous section).

[3] Political agreement reached on 10 December 2018

Standardisation and interoperability (Article 4.6.c)

It should be clarified that standardisation work should be carried out in close cooperation with international and European standardisation organisations. **Amendment 51 on Article 4.6.c** in the ITRE draft report goes in the right direction: '(c) ***supporting*** research and innovation for ***formal and non-formal*** standardisation in cybersecurity***, where appropriate in close cooperation with the European Standardisation Organisations;*** […]'. However, we question the notion of 'formal and non-formal' standardisation. Any standard should be defined according to the European standardisation procedure. Furthermore, a reference to international standardisation organisations should be included.

National Competence Centres

Out of consistency, there should be a more precise definition of what a national competence centre is and closer alignment with existing institutions, as many of these have already been set up for the NIS Directive. Therefore, we support **Amendment 62 on Article 6.4** in the ITRE draft report: '***The Commission shall issue guidelines further detailing the assessment procedure and explaining the application of the criteria'.***

Conclusion

Stronger EU cooperation is essential to enhance Europe's cyber-resilience and should be based on harmonisation, public-private partnership and global cooperation. Cyber-resilience is contingent with operators and providers using state of the art technologies and solutions regardless of their provenance. Therefore, it is fundamental that the future EU Cybersecurity Competence Centre and Network - and thus the Digital Europe and Horizon 2020 funding programmes - do not lead to restrict unnecessarily third-country participation, including in public procurement procedures. Furthermore, the future Centre & Network should be build on a solid governance system which gives an important role to ENISA, ensures consistency in national chapters and contributes to on-going international work.