AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Consultation response

ENISA consultation paper ‘EU ICT Industrial Policy: Breaking the Cycle of Failure’

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 2018, directly supports more than 4.8 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

Executive summary

The American Chamber of Commerce to the European Union (AmCham EU) welcomes ENISA's objective to make the European cybersecurity market more competitive. ENISA's expertise and resources would be best used by focusing on whether the EU should develop a competitive advantage in cybersecurity and how to do it, instead of looking at the broader information and communications technology (ICT) industry.

Europe faces increased global competition for investment. AmCham EU wants to create the right environment in the EU to conduct business and ensure a solid infrastructure, to foster skills, talent, innovation and labour flexibility while strengthening the Single Market. An industrial policy approach should seek global competitiveness, creating an innovation-friendly environment, enabling companies to scale-up and making the EU attractive to investments, including from outside the EU and to allow people to reap the full benefits of an effective market.

1. Do you agree with the principles outlined in this paper? Please outline where you agree or disagree.

Objective & scope

AmCham EU welcomes ENISA's objective to make the European cybersecurity market more competitive, which will contribute to fostering competition and innovation globally and thus enhance cybersecurity solutions. The overall objective, however, should be to maintain and increase security. Strengthening the EU cybersecurity industry is an important element of that, but so too is working with trusted partners, improving the security baseline and promoting best practices in value chain security.

Hence, ENISA should take into account that the cybersecurity market is not a uniform market. From a cybersecurity industry perspective, we see multiple coexisting markets which are subject to segmentation which can either be geographical, based on the market size, on the buyers or on the products (ie, hardware, software, security services, cloud/ network, infrastructure providers, system integrators) which require different strategic approaches.

The concept of 'digital sovereignty' is also ambiguous and should be clearly defined, ie, by evaluating the trustworthiness of companies involved in the market and address areas of high risk.

2. Do you think Europe should focus on developing the cybersecurity market? If yes what do you think are Europe's competitive advantages and how do you envisage that these advantages will develop?

Stimulating the European cybersecurity market will stimulate the global market and hence foster the development of ever more innovative and competitive cybersecurity solutions.

Not all ICT is (equally) strategic. ENISA should help to deepen the question of whether the EU can and should seek a competitive advantage in cybersecurity products and services, and as a second step, support the identification of strategic areas and solutions. From a market perspective it is necessary to consider that no country or region can reasonably expect to compete in all market segments. Instead, a strategic approach should help identify the markets in which the EU wants to compete, build the competences (internally or by partnering externally), work towards achieving an innovation-friendly environment, and ultimately help organisations to scale in Europe. By achieving these objectives, the EU will not only help its companies to become more innovative, but it could also help attract (or retain) foreign investments to the Single Market. However, for the latter to happen, the EU must ensure that the regulatory framework does not limit a company's ability to conduct business on the basis of its ownership or origin.

3. Do you think competition policy and/or legislation or the interpretation thereof needs to be changed in respect of the European ICT and cybersecurity markets? Please explain.

EU competition policy and legislation are highly flexible and well suited to address developments in the European ICT and cybersecurity markets. EU competition law will evolve to address developments, and indeed the Commission is a global leader in considering how developments in the digital economy should be addressed in EU competition enforcement. But AmCham EU does not believe that changes are required in the underlying legislation and agrees with DG COMP that the fact-based, case-specific approach is best to ensure that competition enforcement does not inadvertently chill innovation or new legislation does not distort competition.

When discussing the digital economy including cybersecurity, the EU should carefully assess existing legislation to determine that it's fit for purpose before introducing new legislation. For example, appropriate regulation can help harmonise and set standards. To avoid hindering innovation, new digital economy rules should be technology-neutral and set an overarching goal rather than prescribing the 'how'. In order to tackle cyber risks in complex value chains such as IoT, the best way forward is public-private partnerships. Any European solution should draw on existing international standards and practices reflecting the global nature of the technologies.

It is important that the EU take steps to ensure a diverse and competitive supply chain for ICT, in particular as the 5G rollout commences. There are concerns about the limited number of suppliers for 5G networking equipment leading to a market consolidation, a lack of diversity and the potential for lock in. Increasingly, certain non-European firms are dominating the market for telecom equipment. It will be essential 5G be deployed based upon: open interoperable standards to avoid lock in; multiple vendors providing market opportunities for all competitors, and market transparency ensuring a level playing field for new entrants. These concerns echo the 2019 Prague Principles.

4. Do you agree a more thorough market analysis needs to be carried out to identify where Europe has a competitive advantage in cybersecurity/ICT?

Yes, it is necessary to identify the market areas where Europe can effectively compete in the ICT sector as whole, including cybersecurity. This market assessment can, in a second step, inform the definition of strategic sectors and industrial policy solutions.

5. Which body or bodies do you think would be most appropriate to carry out this market analysis? Please explain.

A proper market analysis would require a horizontal implication of various institutional structures (non-exhaustively including DG CONNECT, DG GROW, DG RTD, DG EMPL, JRC, and agencies such as ENISA, INEA, EASME, ERCEA). This should also include relevant stakeholders, such as individual organisations, trade associations or business groups, to be consulted in the process to ensure that these findings are market-based.

6. What do you think could be done to improve the financial standing and ability to grow/expand of European cybersecurity undertakings?

7. Are there any other initiatives that could be put in place to stimulate the European cybersecurity/ICT market?

AmCham EU published a full set of recommendations for the next European Commission's mandate to stimulate the ICT market, including cybersecurity, available: http://www.amchameu.eu/system/files/position_papers/towards_a_digitalised_single_market_final.pdf. We are also developing an EU industrial policy strategy paper which we will share upon finalisation.

As for some of the wider issues ENISA raises in its consultation, namely section 2.1 on state subsidies that distort competition and dumping products on the EU market at prices that do not reflect production costs, we agree the EU needs appropriate tools – and to leverage existing ones – to address these behaviours.

The EU's normative power

The way in which ENISA envisages the EU's use of normative power through the EU Cybersecurity Act raises some concerns. ENISA seems to suggest that 'trust labels' (section 4.1) should be used to favour products manufactured in the EU. Certification is an effective tool to increase cybersecurity. By creating a voluntary certification framework, the EU might create a stronger incentive for companies operating in the EU market to use this tool. However, certification should not be used as a market barrier, and a trust label should not be used to give a false sense of security to consumers. Modern supply chains are very complex. The emphasis should not be on place of manufacture but on the adoption of effective practices throughout a product's lifecycle – design and development, planning and ordering, sourcing and manufacture, delivery, use and end of life. It is important for companies to have, and to be able to demonstrate, a controlled development, manufacture, logistics and channel environment, using approved processes and tools together with software modules and hardware components. Companies should limit the introduction of malware and rogue raw materials and develop technology, build devices and deploy processes to address counterfeit solutions.

8. Are there any other issues that you would like to raise to contribute to this debate?

Herewith we would like to outline some of the areas for further consideration:

Reduce market fragmentation and regulatory barriers to innovation, focusing the EU's existing regulatory power on instances of real market failure.

Embrace a risk-based entrepreneurial culture and facilitate access to venture capital.

Better match demand and supply of cybersecurity skills.

Use public procurement to stimulate the ICT market. The EU public procurement market, representing 14% of EU GDP, is an essential tool to develop the cybersecurity market and for the public sector to **require the best security features** in the products and services it procures and not pursue protectionist goals.

Whether such security is provided by EU or non-EU companies should remain irrelevant. Public procurement should seek the best available products and services. It should ensure a high level of quality and security rather than just the lowest price. Eg, ENISA could work with the Commission to develop something akin to the Handbook for Green Procurement for cyber security. And any wider public procurement measures should be designed in a WTO GPA compliant manner.

In addition, **a harmonised and strong protection system of IPR** is crucial to encourage innovation and investment. However, it is unclear what change ENISA suggests to existing IP legislation.