DIGITALEUROPE

5 SEPTEMBER 2019

Response to ENISA consultation on EU ICT industrial policy

Executive summary

The EU Agency for Cybersecurity (ENISA) last July published a paper on EU industrial policy.[1] The paper contextualises Europe's position in the global ICT value chain and puts forward recommendations to guide the new European Commission and European Parliament.

In the following response to ENISA's consultation, we share our views on the most important issues that Europe needs to tackle in order to ensure ongoing and future European leadership in ICT.

Table of contents

[1] Available at https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/eu-ict-industry-consultation-paper

§

Responses to the consultation questions

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

DIGITALEUROPE supports the paper's goal of fostering European-originated ICT players that can compete and grow both across the EU and in the global market.

The paper identifies numerous factors that can explain Europe's current ICT position vis-à-vis other world regions. These include but are not limited to: an overly burdensome regulatory environment that discourages growth and risk taking; EU companies' relative reluctance to invest in new players with growth potential; and the EU's existing fragmentation across national and language lines.

All these factors merit specific attention and have more to do with the EU's own attitudes and policies than with external factors. In fact, we believe such factors play a greater role in explaining the current global marketplace as described in the paper. Unless these issues are tackled more decidedly, the EU's global standing will not improve.

Europe's ambition should be to become a worldwide hub for innovative technologies and services, being able to develop them here and trade them across the globe. Europe needs to develop capacities in key technologies, services and platforms, but it should also be able to choose freely between foreign alternatives. From this perspective, the term 'digital sovereignty,' which we find is not clearly defined in the paper, should avoid any binary connotation and recognise the reality of global supply chains and the overall globalised nature of the ICT industry.

'Digital sovereignty' is best understood as the ability to build and maintain technical and scientific expertise in critical digital technologies, in both the public and private sectors, while taking into account innovative technologies and the state of the art in a global market. 'Digital sovereignty' should therefore not be understood as an inward-looking, protectionist agenda but as a positive, outward-looking projection of European economic strength and values.

§

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?

Cybersecurity has emerged as a key political and economic priority for the EU, and we support the EU's efforts to strengthen the cybersecurity market in Europe and worldwide.

While some players can enjoy growth trading purely within Europe, European players developing cybersecurity solutions will enjoy further growth if they can operate and trade internationally. Real competitiveness for European players will only emerge in the latter scenario and it is therefore important to identify areas where Europe has a competitive advantage.

At present we see opportunities for Europe to emerge competitive in the global cybersecurity market through emerging technologies such as artificial intelligence and machine learning, particularly in the digital transformation of traditional industrial sectors, as well as competitive hardware security products (e.g. secure elements).

Moreover, it is important to keep in mind that Europe is home to globally leading companies in the telecommunications equipment market, and this leadership continues from GSM to EU-developed 4G and now EU-led 5G. Leading in the development of globally harmonised standards will in this context continue to be key to ensuring Europe's global competitiveness.

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.

Effective competition policy is vital in sustaining a healthy market where competition, innovation and growth can coexist. From this perspective, a correct understanding of ICT markets and clear evidence of harm are necessary lest competition action diminish innovation or limit European success stories in the longer term.

As stated in the paper, Europe has been at the forefront in this space, and overall we find that existing analytic tools are up to the task of addressing anticompetitive behaviour.

The paper suggests that a specific review of merger rules may be needed to stimulate the growth of European ICT businesses. However, and without expressing a view on specific merger cases or markets, we note that the paper also explicitly recognises (p. 8) that 'European ICT businesses typically neither grow by means of mergers nor acquisitions' not because mergers are blocked but because of a 'lack a strong entrepreneurial culture' and 'conservative attitudes in European companies.' As we argue in our response to Question 1, we believe tackling similar issues more decidedly might be more important in improving the EU's global standing.

§

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

We concur with the paper's findings (p. 2) that Europe cannot try to excel at everything but should instead 'gather the necessary evidence to identify the correct market segment and pursue a specific strategic approach.'

We believe that one of the EU's missions should be to identify how Europe can seek a competitive advantage in cybersecurity products. A solid grounding in evidence will be necessary in order to pursue an effective industrial strategy that recognises the reality of global supply chains and the overall globalised nature of the ICT industry.

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

The European Commission and ENISA, with support from a recognised market research company and the necessary industry input, would be best suited to conduct an independent and unbiased analysis.

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

We believe that the paper identifies some key issues that the EU will need to tackle in order to improve competitiveness and access to funding for European companies. These include:

- Reducing barriers for cross-border funding, by strengthening the European venture capital, financial and loan markets;
- Reducing administrative burden, which disproportionately affects small businesses;
- Improving support services and access to capital for innovative SMEs;
- Increasing the effectiveness of funding opportunities, avoiding fragmentation at both EU and Member State level that leads to inefficiencies and lost potential;
- Strengthening the academic spin-off model and focusing on skills and education as a priority.

The ENISA consultation also rightly points to public procurement as an important factor in stimulating the EU ICT industry and cybersecurity. With more than 250,000 public authorities in the EU spending 14% of EU GDP each year,[2] the public procurement market very much has the ability to drive innovation rather than what may in the short term appear as the lowest cost. ENISA could helpfully work with the European

[2] https://ec.europa.eu/growth/single-market/public-procurement_en

§

Commission in developing something akin to the Handbook for Green Procurement for cybersecurity as well as contribute to related policy debates around public procurement.

Most importantly, Europe should look to further strengthen its efforts to achieve a true digital single market. European companies will only be able to grow coherently in Europe, as opposed to having to migrate outside the EU when they are successful (see p. 14 of the paper), if they are presented with the necessary pan-European scale and addressable market.

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

Industrial and trade policies go hand in hand. A strategic coordination of these two key policy areas is vital and entails that any policy action considers the reciprocal impact on the other.

The paper correctly identifies practices of third countries, such as state subsidies, that distort competition and dump products on the EU market at prices that do not reflect production costs. As such, the EU needs appropriate tools – and to leverage existing ones – to address these behaviours.

European policymakers should coordinate their policy goals, objectives and principles of trade regulation closely with international partners to promote global alignment with rules and standards in order to avoid a fragmented policy landscape for businesses. The current rise of protectionism should urge the EU to take international leadership and defend the rules-based multilateral trade system.

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

We welcome ENISA’s contribution to the discussion on the EU’s future ICT industrial policy. A deeper understanding of how EU policies and initiatives can strengthen Europe’s competitiveness and global standing is desperately needed.

We share many of the proposals contained in the study – particularly those around removing fragmentation, improving pan-European access to venture capital and carrying out an evidence-based analysis of Europe’s competitive advantage – but urge caution on others.

Notably, we note that the paper conflates ICT as a whole with cybersecurity. This link is not a direct one and should be more carefully construed.

Strengthening the EU’s global standing in ICT markets is important, but focusing on origin does not in and of itself improve security. This instead requires effective practices throughout a product’s lifecycle, irrespective of origin – design and development, planning and ordering, sourcing and manufacture, delivery, use and end of life.

§

Similarly, the location of manufacturing (assembly) is not in itself a determining factor. Europe needs to excel in ICT developments, but the country of manufacturing is secondary. For example, there is virtually no 'ICT manufacturing' on US soil.

We look forward to future engagement with ENISA, the EU institutions and the Member States to further explore these issues and suggestions for EU policy action.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Senior Policy Manager for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Airbus, Amazon, AMD, Apple, Arçelik, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Epson, Ericsson, Facebook, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: Nederland ICT, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK