DIGITALEUROPE

DIGITALEUROPE position on the proposal for a European Cybersecurity Competence Network and Centre

Brussels, 31 January 2018

EXECUTIVE SUMMARY

DIGITALEUROPE welcomes the European Commission's proposal for a European Cybersecurity Competence Network and Centre. The creation of a European Cybersecurity Competence Centre, together with a Network of National Coordination Centres, has the potential to harmonise the currently fragmented cybersecurity market and increase the EU's competitiveness.

Although the goal of the proposal is welcomed, DIGITALEUROPE urges the co-legislators to better incorporate industry input in the governance of the proposal. Research, innovation and development of cybersecurity capacities require the involvement of all stakeholders in the global supply chain. Failure to consider the global nature of industry solutions will deprive Europe of crucial solutions, resources and instruments.

In this position paper we highlight areas where the proposal could more effectively support the following goals:

- Broader consideration of the EU market within the global nature of the ICT supply chain;
- More bottom-up approach that includes industry, especially the demand side, providing input to the governance and decision-making of the Competence Centre through either the Advisory Board or the Governing Board;
- In order to tackle cyber threats, consideration for reduction of the vulnerabilities of critical infrastructures, e.g. expanding the scope of the Community for security research and fostering greater sharing of sensitive non-classified information;
- Inclusion of non-EU products from markets which will fall under the scope of the Centre, e.g. public administration and critical infrastructures; and
- Greater promotion of the use and worldwide exploitation of research results, ultimately strengthening Europe's position as a global leader in cybersecurity on the global stage.

MISSION AND OBJECTIVES OF THE CENTRE: *ARTS. 3-4*

DIGITALEUROPE recommends that the mission of the Centre should be extended to include support to the integration of EU cybersecurity technologies in the global supply chain.

The mission of the proposed Centre is to retain and develop cybersecurity capacity in the Digital Single Market. It is essential to remember that supply chains are global, and that products and services integrate technologies from companies globally. Equally, global supply chains also incorporate the open source software community.

In order for the Centre to harness the most up-to-date cybersecurity solutions, the Centre should incorporate cybersecurity solutions into products irrespective of their origin. The diversity of global cybersecurity solutions available in the market will allow for greater choice for consumers alongside raising the level of the required security.

Similarly, the European Cybersecurity Certification Framework aims to improve the overall security of products being placed on the EU market. The Centre should complement this Framework via the development of certified products whilst maintaining a more global approach.

GOVERNANCE OF THE CENTRE, NETWORK OF NATIONAL CENTRES, AND COMMUNITY: *ARTS. 8, 9, 10, 12, 15 and 18*

Research, innovation and the development of any new capacities require the involvement of all stakeholders in the supply chain – customers, the research community and the private sector. Without granting a platform for industry to provide valuable input, the proposal will be faced with challenges in addressing market shortages of cybersecurity solutions, resources and instruments.

The proposal envisions the creation of a Governing Board tasked with the 'strategic orientation and the operations of the Competence Centre.' Under this proposed format, the current voting weight of the European Commission is disproportionate and grants the Commission a larger share of voting (50% of the votes). In addition, the Governing Board does not include industry input.

Although light representation of industry stakeholders is embedded within the proposed Cybersecurity Competence Community and the Industrial and Scientific Advisory Board, there is no clarity as to the impact of the work that this Advisory Board will have on the strategic decisions taken by the Governing Board.

Moreover, the Advisory Board will have 'no more than 16 seats' accommodating representatives from various stakeholder groups: the private sector (including SMEs, demand and supply side, all sectors), academics, consumer organisations, JRC, ENISA, etc. At a working group level, depending on the type of expertise required, broader participation from industry will be required to allow the sharing of best practices and provide highly valuable input.

When it comes to consistency with existing mechanisms, DIGITALEUROPE suggests that the roles of ENISA, Europol, the EDA and CERT-EU should be more clearly defined to increase their impact and transparency with the new initiative.

TASKS OF THE COMMUNITY: *ART. 9*

The proposed Cybersecurity Competence Community will be tasked with contributing to the reinforcement of cybersecurity research. Security research in the ICT sector can shed light on vulnerabilities, whether found in products provided by companies or in services provided by government institutions. Software and hardware vulnerabilities have been at the core of many recent, high-profile cybersecurity incidents.

It is imperative that security researchers be provided with clear guidelines in order to allow for all stakeholders to coordinate the disclosure of vulnerabilities. By doing so, vulnerabilities will be much more easily identified before any serious incidents can occur.

The Community should also be tasked with providing and contributing towards security ethical research guidelines. Most notably this research would be fed into the responsibility for the disclosure of Coordinated Vulnerability Disclosures (CVD) and in particular how these vulnerabilities are actually disclosed. This is essential because at the moment the CVD process is conducted at a more bilateral level (discoverer of vulnerability to the affected vendor).

Therefore, the Community should be enabled to collectively provide guidance on how the utilisation of CVD can drastically reduce vulnerabilities in critical infrastructures. This can be done through a process that ensures the disclosure of a vulnerability is conducted with more coordination with the service owners/providers who are developing a 'patch' for implementation that will limit the exploitation of such a vulnerability.

Finally, there appear to be no incentives proposed for the involvement of cybersecurity professionals in the Community. Art. 9 should state clearly the benefits and incentives for involvement in the Community and not only focus on tasks and obligations in order to attract the global top experts. A lack of incentives for cybersecurity experts to join will frustrate the development and high-level expertise required for the Community to be truly effective.

TRANSPARENCY OF THE CENTRE AND SHARING INFORMATION: *ARTS. 35-36*

DIGITALEUROPE advocates that in order to effectively combat global cyber threats, the Competence Centre should facilitate information sharing as part of the CVD process.

The protection of confidential, sensitive non-classified or commercially sensitive information should not inhibit sharing information within the Community for security research and for the reduction of vulnerabilities of critical infrastructures.

ESTABLISHMENT OF MARKET BARRIERS FOR PRODUCTS ORIGINATING FROM THIRD COUNTRIES: *ARTS. 3, 4(4)(C) and 5(2)*

DIGITALEUROPE is concerned that unintended market barriers may be result from the proposal's focus on increasing the competitiveness of the EU cybersecurity solutions industry.

This is reflected in Art. 3 as well as Arts. 4 and 5, which cover the supporting role the Centre will play towards public authorities and members of the Network or of the Community in the adoption, integration or procurement of cybersecurity solutions. The involvement of the Centre in such activity therefore risks distorting and fragmenting the ICT market.

USE AND EXPLOITATION OF RESULTS: *ART. 34(2)*

The strict use and exploitation of grant results imposed by the proposal (Art. 34), especially targeting the retaining of results in Europe, does not consider companies' business reality. This may therefore create a lack of interest for companies to join European actions and ultimately isolate the EU.

In addition, Art. 34 prevents the analysis of the results from Horizon Europe projects by globally active organisations. This is a by-product of the overall lack of incorporation of non-European organisations in the Community that is reiterated throughout the proposal.

--

For more information please contact:
Alberto Di Felice, DIGITALEUROPE's Senior Policy Manager for Infrastructure, Privacy and Security
alberto.difelice@digitaleurope.org or +32 2 609 53 10

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's members include in total over 35,000 ICT companies in Europe represented by 63 Corporate Members and 40 National Trade Associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Airbus, Amazon, AMD, Apple, Arçelik, Bosch, Bose, Brother, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, Intel, 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, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, 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