Digital Europe Programme

Eurosmart, the voice of the Digital Security Industry, strongly believes that Europe deserves a strong comprehensive approach to strengthen its cyber resilience. EU should concretely boost European Digital Industry to reach global competitiveness and bring more trust to citizens and enterprises.

The European Digital Security Industry has developed a unique and globally recognised know-how, but It suffers from poor public investments and small public initiatives that would protect this common asset. For this reasons Eurosmart does strongly support the achievement of the Digital Single Market, the digital transformation and the cybersecurity related initiatives.

Eurosmart is convinced that trust is the cornerstone of the achievement of the Digital Single Market. The legislator takes leverage upon public investment to drive competition and to address social challenges of the digital age.

Therefore, Eurosmart welcomes the European Commission proposal on "Digital Europe programme" and specifically acknowledges two of its objectives: "the efforts to reinforce and to harmonise upwards the cyber capability throughout Europe" and "the wide development of the cybersecurity solutions across the economy".

Europe world-wide leadership in cybersecurity is a prerequisite of the achievement of the Digital Single Market. Synergies and consistency are necessary for an efficient public action, on account of multiplication and fast-growing trend of cyberthreats. Even if public programs such as HORIZON2020, FP9, ECSEL, CEF and Digital Europe are big step forwards, the increase of cyber resilience capabilities in Europe remains scattered amongst several initiatives.

Eurosmart hence regrets the lack of a comprehensive master plan to support Cybersecurity in Europe.

Objectives 1 + 2 "High Perfomance Computing" and Artificial Intelligence

Eurosmart expects a strong economic race between China, US and the EEA on both these issues in the next years. High Performance Computing (HPC) and Artificial Intelligence (AI) are essential for digital sovereignty in the digital world as well as in the cyber security domain. For these reasons, EEA should be able to import those technologies from third countries, this includes the know-how on technologies, on capabilities and on new limits.

This approach could be based on already existing experiences like GPS in the US, GLONASS in Russia and GALILEO in Europe.

HPC would incorporate new technologies such as Quantum Computer and others; AI can be used both as "white hat" tool and "black hat" tool. This could lead to a better quality of the cyberattack counter-measures.

Objective 3 "Cybersecurity and trust" (art. 6)

The Conclusions of the European Council of 19 October 2017 specify that Europe must urgently address new emerging trends about cybersecurity such as digital secure identities, digital secure communication, digital secure infrastructure and their related applications.

The basis of the digital world is a combination of "Application and Software", "Hardware and Device", Net-, Web- Cloud-services and "Data Networks". The mastery of these elements is necessary to ensure our digital sovereignty.

The current proposal made by the Commission (art. 6) could lead to a sectorial approach and segment the effect of the public action. Eurosmart does advocate for a transversal approach which is not based on the sole applications.

The digital security industry asks the legislator to mention **the tree dimensions** in its proposal to avoid the risk of imbalances and to ensure a consistent development of its digital economy:

- **Software, incl. security and privacy by design**
- **Hardware, incl. security and privacy by design**
- **Secure Connectivity (Network).**

Objective 4 "Advanced digital skills"

Advanced digital skills should be considered since pre-school for the new "digital natives" generations. "Generation y" and "Generation z" should be addressed as well through specific programmes, considering that the development of digital skills must be part of all the academic programmes.

Even job descriptions show disruptive changes. For example, in the Industry 4.0 the requested knowledge on Cyber Physical Production Systems is linked to the hyper-connected-IT world likewise in production-OT world. More broadly, studies on machine construction does not address any elements on IT and even less with regards to IT-security.

Objective 5 "Deployment and best use of digital capacity and interoperability"

This topic should act as a bridge between the Cybersecurity Act and the related security level and certification schemes for Internet of Thinking Things (IoTT), the next generation after IoT.

Reinforcing links between PPP, EU Network of competence centers and Digital Innovation Hubs

Eurosmart welcomes the proposal to implement the program through European Partnerships which may include new public-private partnerships (PPP). The Digital security industry advocates for enhanced PPP. From a governance point of view, this option is the only way to involve all the stakeholders, national and regional bodies into a fair and transparent process without any additional administrative burden. The PPPs are the only way to bring together the relevant high-level experts

from both public and private sides. It facilitates links between the demand (both public and private from various sectors e.g. health, telecom, energy, space, defence, finance, transport) and supply side of the cybersecurity. This way stimulates a leverage effect both on the European cybersecurity excellence and know-how.

Eurosmart welcomes the proposal to create Digital Innovation Hubs but enjoins the legislator to avoid any fragmentation or dissipation of resources. Strong links must be created within the EU Network of competence centers.

The new framework will go beyond the R&I activities; therefore, we expect involvements and links with the Cybersecurity Public-Private Partnership (aka ECSO) to be specified in the current proposals.

Consistency with the Cybersecurity Act and its European Certification framework

The proposal for a Cybersecurity will establish a European Cybersecurity certification framework and both the industry and the public sector would take advantage of this opportunity, thus by enabling a trusted environment.

Even if the cybersecurity certification is likely to be based on a voluntary basis, some specific and regulated sectors or public procurements will make the approach mandatory. To achieve a high security level, the development of a candidate cybersecurity certification scheme could be necessary. However, the conception of such a scheme could not be affordable for some part of the industries, especially for SMEs.

With the aim of helping the capability level of the European industry and the increase in security level, the current Digital Europe Program should include in its objective the support and financing for the development of activities related to the definition of candidate certification schemes.

About us

Eurosmart, the Voice of the Digital Security Industry, is an **international non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are manufacturers of secure element, semiconductors, smart cards, secure software, High Security Hardware and terminals, biometric technology providers, system integrators, application developers and issuers.

EUROSMART members are companies (**BCA**, **Fingerprint Cards**, **Gemalto**, **Giesecke+Devrient**, **GS TAG**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Internet of Trust**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **SGS**, **STMicroelectronics**, **Toshiba**, **Trusted Objects**, **WISekey**, **Winbond**), laboratories (**CEA-LETI**, **Keolabs**, **SERMA**), research organisations (**Fraunhofer AISEC**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **Mobismart**, **Danish Biometrics**).

EUROSMART and its members are also active in many other security initiatives and umbrella organisations on EU-level, like CEN, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

Contact:

Pierre-Jean VERRANDO

Director of operations

Mobile: +32 471 34 59 64

EUROSMART

The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 00 | mail eurosmart@eurosmart.com