EUROSMART
The Voice of the Digital Security Industry

Eurosmart's feedback on ENISA's EU ICT Industrial Policy paper

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

Eurosmart, the voice of the digital security industry, is convinced that Cybersecurity is a unique opportunity to enhance citizens' confidence in their digital experience and for Europe to lead the worldwide digital revolution. Eurosmart agrees with most of the statements given by ENISA. The European and its member states need to heavily invest in key technologies which deserve mass EU funding in a comparable range to those provided in the US or China. At the same time, it is crucial to ensure that these technologies provide the same security level across Europe, especially for critical infrastructures, which is why European cybersecurity certification should be encouraged.

Moreover, in parallel with the regulatory and financing support given to the European ICT and cybersecurity ecosystem which is made of many SMEs, a real effort should be accomplished to foster the development of EU champions. For this purpose, the involvement of the European industry as well as the whole cybersecurity and ICT ecosystem (SMEs, research, academics) should be ensured in the European decision-making process. The EU legislative should provide a structured framework for the whole EU digital value chain to invest and develop technologies for the future. There are good examples such as the electronic payment where the digital security industry in Europe achieved outstanding results. ICT / cybersecurity can leverage these good practices and apply them in other segments (e.g. IoT).

Eurosmart disagrees with the general statement that no focus on "digital platform" is needed and thinks this depends on the definition of the term "digital platform". Europe need to care about key enabling technologies first, in this context a Trusted European Cloud (in the meaning of "digital platform") would be efficient and would help the deployment of multiple technologies.

Finally, the document mentions regulation as a potential barrier to access the market. Actually, the European digital security industry strongly believes that a regulatory framework at European level will strengthen the protection of European citizens as well as being an opportunity for the market. Eurosmart encourages to further explore a European regulatory approach on security requirements. Europe suffers from weak national implementations of European guidelines and transposal of direction. This lack of harmonization between member states will definitively lower security requirements and as such a European harmonized regulatory framework on cybersecurity certification is important to prevent a race to the bottom, therefore essential to protect European citizens.

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?

Eurosmart thinks, that Europe should ensure the appropriate regulatory and funding conditions to ensure the right development of key EU technologies for cybersecurity, it is the prerequisite for the development of the cybersecurity industry and its ecosystem. The mastery of these security technologies is necessary to ensure the independency and the sovereignty of the continent.

"Security/privacy by Design / by default", and the future "Cybersecurity by design" for all products to be placed on the EU market are true European assets to foster the EU ICT and digital industry. Thanks to the regulatory framework, and the long track record in digital security, worldwide trust could be established in the brand "Made in Europe". The European digital security sector has significant experience and know-how, has been developing many security certification schemes which have become world-wide references. This knowledge must be protected and fostered through different EU's initiatives and funding.

For instance, requirements for mandatory security certification in any public procurements would enhance the level of security and will incentivize major suppliers to implement these certifications. Companies would compete to make sure their products are trustworthy and reliable. This approach is a clear motivation for companies, and the European level of quality would be adopted beyond Europe.

Certification is a key asset to enable Europe's competitive advantage. Mandatory cybersecurity requirements – apart from safety functional certification – for placing products on the European Market, should be further explored. All products embedding ICT functionality must comply with "cybersecurity by default" principles. This approach could be beneficial for consumers and for the cyber-resilience of the European market, it would grant EU and non-EU companies which comply with EU rules and values, a clear competitive advantage. In parallel with this principle, effort should be made to accompany SMEs to use and adopt these requirements. Once again, Europe could take the lead thanks a normative power and make its baseline security requirements adopt world-wide.

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?

With cybersecurity industry holding the potential to become one of the most important economic drivers in Europe, Europe's competition policy should envisage an efficient way to encourage the emergence of big EU champions in the global ICT and cybersecurity markets. Competition policy should be more flexible when it comes to anti-trust policy which could deter big corporations from increasing their capacity.

On the other side, control on non-EU companies who intend to take control on EU organisations must be increased. European SMEs and industry are very weak in front of non-EU giant tech companies, and they constitute a unique asset in terms of patent and know-how which attract foreign companies. The European Union should edict specific rules to protect some ICT and cybersecurity segments (classified, critical etc.).

This approach should be extended to the decision-making process within the EU advisory body (ie. expert groups, certification ad-hoc groups, future European Cybersercurity Competence Centre) where an attention should be given to representativity of the organisations to reach a balanced involvement of the different actors from the ICT ecosystems: RTOs, SMEs, Industry, academics etc. The geographical representation is also a key element since some countries are more advanced in terms of cybersecurity and other could have non-EU interests and could play the role of "stowaways" in supporting non-EU interests. More globally, It is expected to provide strict rules in terms of origin, capital, internal decision-making procedure, to ensure that all actors represented in such forum are truly European.

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?

A market analysis is always beneficial. However, Eurosmart thinks, that the digital security market is such an area where Europe currently has significant competitive advantage. Eurosmart would appreciate if concrete actions are taken on already identified areas without waiting for the outcome of the thorough analysis.

More than a market analysis, a foresight study on assets, technologies developed in Europe and a mapping of external influences could be achieved to help both the ecosystem and the policy-maker to understand the future trends in cybersecurity/ICT. It would be wiser to analyses the strengths and the weaknesses in terms of investments, research, deployment of technologies, the identification of the key actors and contributors rather than analyzing the current market needs which are already well known.

In such a study, standardisation and certification could play an important role. Both topics are linked with each other and referencing proprietary solutions or non-EU patents in the European standardization approach may lead to a clear dependency and to a deadlock for the EU home-based solutions. That's why a mapping of the internal/external influence, based on the annual EU rolling plan for ICT standardisation could be a key element.

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

Without impeding the need of rapid concreate action for the EU ICT and Cybersecurity markets, this study should be independently and impartially managed by a "High level group" of experts under the umbrella of the European Commission and/or ENISA with the involvement of representatives from several DGs.

Such a strategic study is exceedingly too critical to be managed by a consultancy firm whose interests may be influenced by external resources. European public authorities should be granted with enough in-house expertise, and should be backed by selected experts to issue unbiased analyses whose objectives are to orientate strategic policy decision. This is also a matter of independency and sovereignty.

To ensure its independence and to make sure market knowledge is well represented, the selection process should be open and transparent. The fair involvement of the whole ICT/cybersecurity value chain should be ensured.

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

EU Funding and research programs should be favored within the Multiannual Financial Framework, to become comparable to support provided by the US and China to their own research and industry. Europe suffers from a lack of public investments and incentives towards its own ICT / Cybersecurity industries. These initiatives would be helpful in developing, deploying and mastering key digital technologies.

Products and services certified under the European certification framework are expected to become a word-wide trusted brand. European cybersecurity and ICT actors should be encouraged to certify their products and services and raise the security level of which. With the aim to make the Cybersecurity Act a success story as it has been the case for GDPR, European values of privacy and "cybersecurity-by-design" should be adopted and implemented by the whole value-chain. It would be a key competitive advantage to compete on the global ICT market. Funding programmes should also support the development of trusted and affordable certification scheme to support European Industry and European start-ups to develop and adopt them, giving the opportunity to scale up and reach critical mass.

The regulatory approach through reliable security requirements for product and services would motivate players from and outside Europe to implement them.

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

Europe should take care of its own data economy: in one hand to allow the European players to have access to dataset to refine their algorithms, on the other hand to protect European citizen's data, even if they are managed and processed outside Europe.

In terms of infrastructures, many PKI (Public Key Infrastructure) applications are not accepted on the long end, due to the lack of access to open, trustworthy, affordable and well-recognized PKI infrastructure, (i.e. cross-border applications for eHealth, eID, intelligent transport systems, e-government services etc). This is a clear obstacle to the development of a more interoperable and secure digital space.

A specific attention should be paid to root DNS which is part of the backbone on which every digital service is built on today. Europe should deploy its own root DNS to master critical infrastructure and technologies.

On standards, the global position of the European Standardisation Organisations (ESOs) must be reinforced. In the meantime, ESOs should be more active in avoiding the referencing of patents (proprietary) in the European standards.

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

The fact that European cybersecurity experts can be found around the world working for global leaders demonstrates Europe's expertise in the field. If the EU could incentivise experts to stay in Europe, it could considerably strengthen its cybersecurity ecosystem. To the contrary of what the ENISA document exposes, skilled ICT experts already exists in Europe, The legislator should initiate discussion on product recalls when it comes to malicious infections. In the current EU market surveillance policy, cybersecurity and digitalization are not tackled. Europe should define clear rules.

To conclude, incentives could be implemented for Insurance companies to take care about cybersecurity certified products. These incentives would be beneficial for consumers and would encourage them to favor cybersecure products.

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**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **Sarapis**, **SGS**, **STMicroelectronics**, **Tiempo Secure, Toshiba**, **Trusted Objects**, **Trust CB**, **WISekey**, **Winbond**), laboratories (**Keolabs**, **Serma**, **Brightsight**, **Red Alert Labs**, **Cabinet Louis Renaud**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, 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 General
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 3635 | mail eurosmart@eurosmart.com