EUROPEAN CYBER SECURITY ORGANISATION

Executive summary: Increasing Digital Strategic Autonomy in the EU Cybersecurity

Suggestions for future EU initiatives, policies and priorities in cybersecurity

June 2022

www.ecs-org.eu

Increasing Digital Strategic Autonomy in the EU Cybersecurity Market

Suggestions for future EU initiatives, policies and priorities in cybersecurity

EXECUTIVE SUMMARY OF MAIN RECOMMENDATIONS

The definitions of Autonomy and Sovereignty vary according to the interlocutors and countries as they have different interests, needs and understanding of the concepts. We propose here a methodology considering diverse points of view, allowing to identify such priorities, starting from the identification of strategic digital issues and then moving to the examination of cybersecurity challenges pertaining to them and the needed strategic solutions.

As result of this prioritisation approach, we can recognize how important certain issues are in the short term (e.g., infrastructure and data protection, secure ID, implementation of the NIS2 Directive, trusted cloud services, development of trusted supply chains, etc.) or how important it is to prepare a long term future with the development of strategic technologies (e.g. 6G, quantum computing etc.). The analysis allowed also to recognize how certain topics like IoT, AI, encryption, microprocessors or education and training are and will remain strategic now and in the future. We are not going to delve here into these topics, as it has been done already in many studies and reports from the ECSO on the identified priorities for the future EU Programmes.

This study has identified **five main objectives** linked to the specific challenges leading us to outlining ***ten main recommendations*** that could constitute the basis for a European public – private flagship programme on European CYbersecurity Sovereignty and Autonomy (ECYSA), combining interests of the private sector with those of the public sector.

A. European solutions and Intelligence for Cyber Risk Management: make Europe a leader in cyber threat prevention, detection and response

An effective strategy of counteracting cyber threats should be built on the basis of cyber risk management. Cyber threats are evolving continuously, and different vulnerabilities are exploited to conduct successful cyberattacks (e.g., ransomware attacks). Malicious actors conduct phishing campaigns leveraging on human weaknesses, but they also utilise technical flaws like vulnerabilities in the main software libraries (e.g., Log4J).

Europe has a great competence in cyber threat detection and response and is looking increasingly to anticipate and prevent attacks (e.g., with threat prevention / Cyber Threat Intelligence). Yet, a large percentage of used risk mitigation solutions and information / data in Europe are coming from outside the EU. We need to enhance competence (from the user's side: CISOs and from the supplier's side) and create a holistic approach that will develop and implement EU solutions for cyber threat management and facilitate the exchange of information with the public sector in particular in case of crisis and boost sovereignty and competitiveness in situational awareness.

1 *Identify, with the **support of users / operators, key operational security requirements for effective IT/OT risk management driving priorities for the development of strategic solutions technologies and services needing "sovereign solutions" and trusted supply chains, in particular for cyber threat prevention, detection and response.***

2 *Support the creation of a "**European Cyber Threat Intelligence**" community **(the European Cyber Threat Alliance)** for strategic threat information sharing among the private sector (in particular among the **CISO community)** for threat prevention in strategic operations. Furthermore, this approach could **improve cooperation between the private and the public sector to anticipate and respond to cyber threats in case of crisis.***

B. **Resilient and Trusted Supply Chains: boost research, development and innovation of digital technologies and services of strategic cybersecurity priorities for the development and use of resilient and trusted supply chains**

Research and innovation should boost capability development and consolidation of trusted supply chains in the upcoming years. ECSO would support future R&I activities carried out by the European Cybersecurity Competence Centre. It will also support ENISA and the European standardisation bodies (CEN/CENELEC and ETSI) to foster certification and standardisation of components, systems and services that will be considered as strategic for Europe.

Yet not all can be manufactured in Europe. Achieving strategic autonomy is not about creating technological autarky, but it is more about boosting European potential and decreasing dependency on external suppliers while increasing competitiveness of the European economy. The objective is to develop trusted and resilient supply chains for the main strategic applications. These supply chains would be composed by elements that are certified following rules and criteria defined by national administrations.

Harmonisation of requirements and use of open standards for interoperability could help the gathering of EU solutions from small and large companies to create sovereign cybersecurity supply chains, which in turn could lead to a certain level of consolidation into European Champions.

3 ***Identify priority strategic technologies and services / tools responding to expected IT/OT operational scenarios to develop and use European solutions to increase strategic autonomy*** *and reduce future dependencies on vital infrastructure and services. Development should address all TRLs with an agile work programme to consider the fast-moving cybersecurity market and its needs.*

4 ***Build Resilient and Trusted Supply Chains*** *in a* ***"cyber-resilience by design" approach*** *to* ***improve security and sovereignty by increasing manufacturing under control of European bodies, diversifying supply chains with trusted partners, investing in inspection capabilities, leveraging upon agreed standards and European certifications****. European* ***trusted and sovereign supply chains should be based upon open standards for interoperability, operationalising "cybersecurity services architectures"****.* ***Trusted supply chains*** *can also be built upon* ***industrial alliances between SMEs and large companies and generate European Champions in strategic applications.***

C. **Investments in European Cybersecurity technology, data infrastructure, startups: increase investments to develop competitive regional, national and European resilient digital / cybersecurity ecosystems**

It is well known that SMEs constitute a large part of the European industrial fabric and a powerful reservoir of competence and an engine for innovation and potentially future "sovereign solutions". European regions would support the acceleration of the growth of SMEs in their ecosystem, as well as in synergy with other specialised regions.

European competence is widely recognized: our companies and experts are increasingly attracted by non-European investors and employers. Europe thus loses the competence in which it has initially invested. Without sufficient budgets and investments addressing strategic issues this competence is not producing the desired results to increase European competitiveness and European Cybersecurity Sovereignty and Autonomy.

We need more investments to keep innovative SMEs in Europe, higher budgets to retain competent experts in Europe, more money to develop European strategic solutions and capacity building of key infrastructure and services. That requires using "sovereign solutions" and more investments to make our solutions more competitive at global level. Following the US example, stronger public procurement could help to boost development of the entire European cybersecurity sector, which is currently still too fragmented and limited.

5 ***Provide support to SMEs: increase visibility of SMEs*** *via a* ***Marketplace; show their European origin via a Label "Cybersecurity made in Europe"; better qualify their capabilities*** *based upon an* ***independent "European Cybersecurity Rating"; develop regional cybersecurity ecosystems accelerating their marketing capability and competitiveness via regional EDIH.***

6 *Create a **public – private European Cybersecurity Investment Platform (ECIP) based upon an equity fund of funds specialised in cybersecurity** to support capacity building and investments in European companies (in particular SMEs) **to keep their strategic competence under European "sovereignty"**.*

7 ***Increase investments in strategic cybersecurity EU solutions and services and use of available resources in focused and federating strategic projects for R&I, development of capabilities and capacity building, in particular supported by harmonised public procurement.***

D. Human Factor and Skills: consider citizens awareness, skills, privacy and in general the human element as a key pillar of cybersecurity sovereignty and autonomy

Digital / Cybersecurity sovereignty and autonomy are not only about security, technology or economy. They are also about human factor. The digital transformation will induce a transformation of the society carrying new threats but also new opportunities (growing need for skills in the cybersecurity market, estimated to be of the order of 500.000 units). National public administrations should develop and implement a strategy to inform students from the youngest age about the potential risks (cyber hygiene) and career opportunities in cybersecurity. Cyber education in different EU countries should be coordinated at European level exchanging best practices. The training of professionals should be organised providing European certifications using a common taxonomy: this would facilitate the hiring process across the Union and harmonise identification of job opportunities. Women should be encouraged to join cybersecurity, as the employment gap in Europe is growing.

Awareness of cyber threats and the need for increased cybersecurity are also important factors to be addressed by citizens and decision makers to allow Europe to be less dependent by the consequences of cyber threats.

8 *Launch **Awareness campaigns at European** level **promoting EU solutions** and provide **Cyber Hygiene** of citizens and professionals at local, regional and national level.*

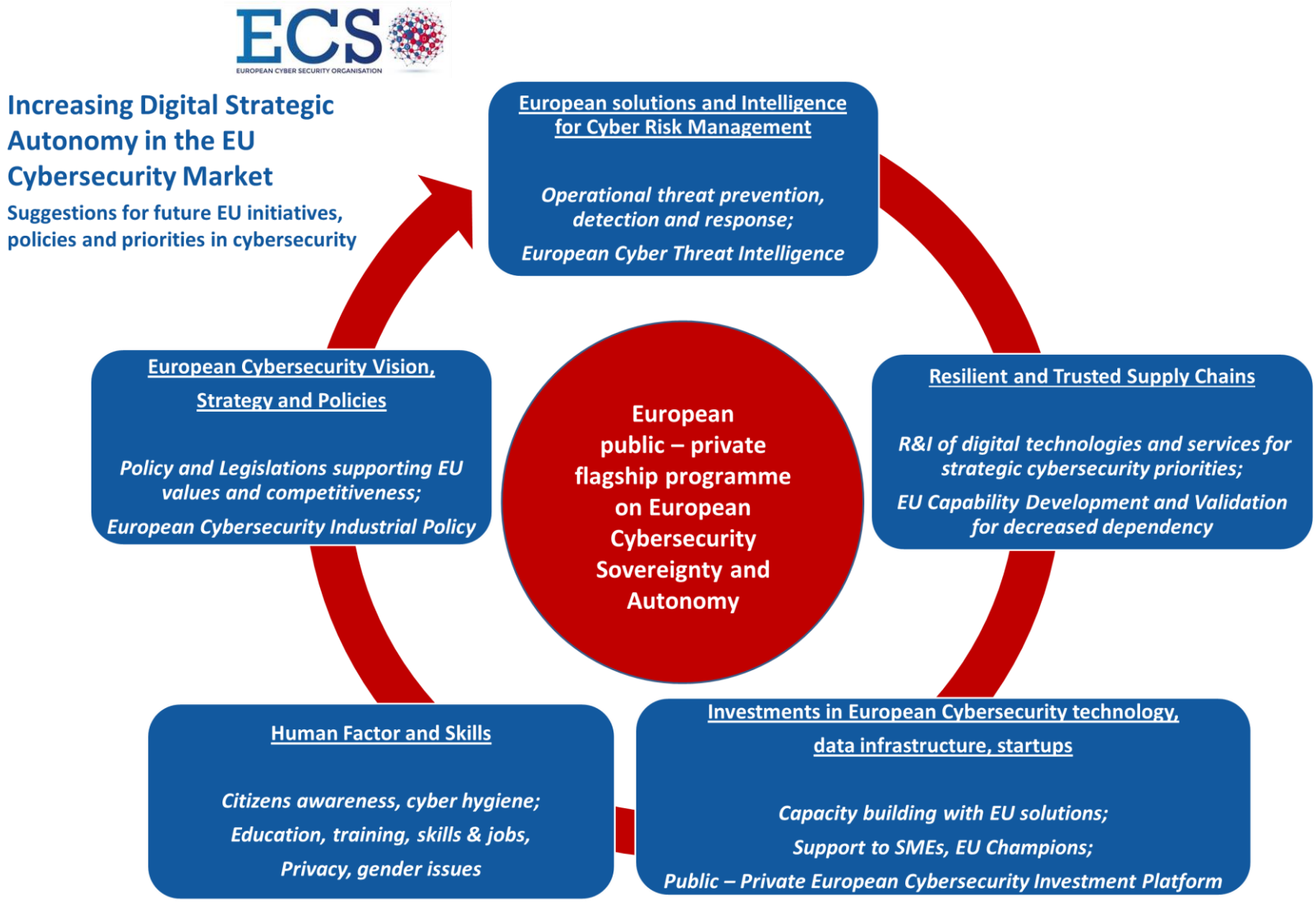
9 *Develop and implement a **strategic roadmap at European level for cybersecurity education (from the youngest age) and training of professionals (re-skilling and up-skilling)** to build up **competence and cover job needs** (also considering **gender and inclusion issues**) not only in the STEM domain.*

E. European Cybersecurity Vision, Strategy and Policies / Public – Private Cooperation: Further develop a European Cybersecurity Vision and Strategy and its Industrial policy, supported by a European public – private flagship programme on European CYbersecurity Sovereignty and Autonomy

Neither the public sector, nor a single EU country can achieve the above-mentioned goals alone. The digital transformation and cybersecurity are evolving too quickly in too many different domains. Communities of stakeholders are developing in different sectors with different level of maturity. For these reasons, we need to work together across European countries and across sectors. It also requires hand in hand cooperation of the public and the private sector. ECSO has shown in the last six years that this goal can be successfully achieved, and we will continue to develop in a public private partnership the European Cybersecurity Community implementing actions in the frame of a European cybersecurity industrial policy.

The creation of a Programme dedicated to European Cybersecurity Sovereignty and Autonomy will support the mentioned objectives. It should leverage upon a public - private (users and suppliers) partnership to identify strategic priorities, discuss economic and legislative issues, cooperate in decision-making processes for strategic investments on R&I, capability development and capacity building, to suggest standards and certification, on skills development and to increase operational cooperation on cyber threats anticipation, detection and response.

10 *Develop in **public private cooperation** a **EUROPEAN CYBERSECURITY VISION and STRATEGY, supported by a** European **public – private flagship programme on European CYbersecurity Sovereignty and Autonomy, define and implement those POLICIES AND LEGISLATIONS** (where needed) as well as formalise a pragmatic **EUROPEAN CYBERSECURITY INDUSTRIAL POLICY** which would support the **European global competitiveness** and the development of **trusted and sustainable European cybersecurity ecosystems.***



Click here to view the working paper.