Initial recommendations and actions for an increased European CYbersecurity Sovereignty and Strategic Autonomy (CYSSA)

EXECUTIVE SUMMARY

Analysis of ECSO WGs & TFs with a S&A filter

We have reviewed the different activities and initiatives in Working Groups and Task Forces that have been started in the last 5 years of ECSO and which are relevant for our sovereignty and autonomy looking at them via a Sovereignty & Autonomy filter ("S&A filter").

We have then identified possible future "*Next Steps for S&A*" that could be performed by our WGs / TFs to develop and adopt Sovereign and Autonomous solutions.

A deeper analysis and identification of priorities using the S&A filter should now be done at WG level, reviewed with the Strategy Committee and proposed at the Board for validation.

This bottom up / top-down approach could allow identification of the most strategic areas for S&A development of the European ecosystems and could provide guidelines for ECSO activities and suggestions for the strategy of the EU Competence Centre.

Understanding where we are

We have to see what development is ongoing in Europe and what are solutions / competences available in Europe (and how much they are under sovereign "control") and what are the priorities to be established for the development of strategic solutions in Europe to guarantee a sufficient level of autonomy in the future and consistently contribute to trusted / sovereign supply chains.

We have then to see which technologies we will be dependent upon (including analysis of the impact of this dependency, i.e. the cost of a "non-EU autonomy") and what should be done to have a number of diversified suppliers (EU and non-EU) and ensure that their solutions can be qualified as trusted (validation/ certification) to transform this "non-autonomy" into an "chosen dependency". For the solutions developed in Europe (and for those purchased) we must identify the comprehensive life cycle cost in order to take informed decisions for investments.

We have also to identify which are the competence in general (beyond technologies) needed to increase our autonomy, particularly in case of crisis.

A possible approach and future actions

The process could start with a relatively simple but comprehensive future scenarios should be developed by (possibly) a group of members belonging to the strategy committee and the secretariat (supporting the CYSSA) considering S&A issues.

These scenarios and their key operational challenges (not only technological) will then be reviewed by the CISOs Community - CEC (previously users' community) and the wider WG3 for what concerns the importance of their operations in light of business continuity and sovereignty issues. They should verify which are the sensitive applications, infrastructure and operations (and their possible evolutions) that would need trusted / sovereign supply chains. This work should also consider that certain applications / domains could be less sensitive (and / or less mature) and could leverage upon solutions which are not necessarily produced in Europe (and sometimes even not certified, as reported in the recent ECSO survey on CISOs).

A detailed analysis of needs for S&A from the CEC could take a certain time. For this reason and to be pragmatic, it would be reasonable to consider in parallel proposals for S&A priorities from each working group according to the perception of present and future S&A needs in their domain.

These priorities would then be checked with respect to the CEC strategic requirements identified in future possible scenarios (when available).

Today the WG6 has already started to identify which are the technology solutions with respect to possible future operational needs.

The WG1, in cooperation with WG2 and WG6, will then have to see what is available in Europe ("autonomous solutions") and what is brought from outside EU and how these solutions (internal and external EU) can be validated / certified to integrate trusted (and, if needed, sovereign) and resilient supply chains according to economic, geopolitical and societal issues.

For all these solutions we should have also to consider how they comply with standards – WG1, what investment efforts to keep and develop in Europe the needed competences, solutions (and suppliers) – WG2, how SMEs (users and suppliers) would contribute to / adopt the different solutions - WG4, and how the local / regional / national markets & ecosystems would support and use such solutions – WG4.

At last, we need to see what awareness of decision makers and citizens (e.g. on data management and privacy) is needed is needed to take informed decisions and proper use of solutions, what impact these strategic solutions would have on the civil society, what training would be needed by users – WG5.

A document to be prepared for strategic S&A and a European public – private flagship initiative on S&A.

What is described here, is an ideal process for identification of key issues for S&A. This would take time and resources that we (ECSO) likely will not have in the short time. Nevertheless, we will make an comprehensive analysis of the S&A needs based on this ideal approach (at least for what concerns some validation from WGs) and we would propose by end 2021 a strategic S&A document listing key domains, technologies and other strategic competences (e.g. human factors, training etc.) to ensure that a sound level of EU strategic autonomy can be reached a sound level , linking the suggestions from the different WGs, identifying in particular where there is a need to build trusted ecosystems / resilient supply chains based on solutions "made in Europe".

This document, foreseen by ECSO in the second half 2021, could include among other things:

- ⇨ Topics needing focussed EU and Member States investments for strategic R&I
- ⇨ Topics needing an effective and ambitious industrial policy (e.g. standards, certification, legislations / regulations, trade agreement for strategic components and resilient supply chains, etc.) to support strategic autonomy
- ⇨ Initial analysis of costs of limited EU strategic autonomy
- ⇨ Investments to develop the "go to market" (e.g. DEP, recovery fund, etc.) and to keep strategic competence in Europe (e.g. EU cybersecurity fund for SMEs)
- ⇨ Suggestions for specific procurement rules for sensitive issues
- ⇨ Analysis of a "chosen dependency" for certain products
- ⇨ Suggestions for the development of a European public – private flagship initiative on S&A

Sound results of this "ideal" virtuous circle, despite being called as urgently needed by the highest public and private decision makers, would not be possible without adequate resources, yet we do not see in the short term budgets (public / private) that could support it.

For this reason, we would propose to get the support from top managers from ECSO members and of the wide European Cybersecurity Community, who would interact with public administrations (at national and European level) and with other investors, to promote a major public – private flagship initiative at European level, focussing objectives and resources to strategic S&A solutions which could complement and support the actions foreseen by the European Competence Centre and its approach. ECSO would of course provide support to the coordination of this initiative.

CONCLUSIONS AND MAIN SUGGESTED ACTIONS

1) Identification of comprehensive future scenarios (technological, economic, political societal) and possible variants to evaluate possible priority solutions for EU resiliency and increased strategic autonomy

Major strategic topics have started in Europe on High Performing Computers, Cloud, 5G, Blockchain, Artificial Intelligence, … Yet, the cybersecurity approaches linked to each of these domains and their interdependences have not be sufficiently considered. ECSO is participating to a new initiative, called Transcontinuum, to tackle in a comprehensive vision, the technology challenges of these domains. Beyond technological challenges, also geopolitical, legislative and societal aspects should be considered when looking at the impact of possible EU dependencies.

We must consider ongoing initiatives in a comprehensive way and assess if they are really driven by resiliency and sovereignty objectives or if something strategic is missing.

For identifying the most important priorities, we need to have a reasonable understanding of present and future challenges and how they could impact our national security, our society and our economy. We have to understand what as well the impact of potential crisis could be if we are dependent on foreign solutions.

We need to identify possible future evolution scenarios and then we need to see what possible solutions could provide sufficient resiliency for these scenarios but also for unforeseen threats to these scenarios (the variants).

On top of that, when identifying strategic priorities we should consider what political/trade agreements would be **needed (for supply of strategic components, including raw materials) to achieve a good level of S&A across Europe**.

When threats could impact sensitive / strategic interests, these solutions that should have been validated and approved by national administrations, are strongly supported by suitable legislations and procurement rules.

A **comprehensive analysis of costs (costs throughout the lifetime of the solutions / service) of S&A EU solutions should be made, including what would be the impact / cost of a non-EU S&A approach, to better understand S&A dynamics and costs.**

2) Converging views in S&A across Europe in public – private cooperation

Even with an improved understanding of the strategic needs for an increased S&A in Europe and S&A priority driven investments, the **challenge to find a convergence of S&A across Europe could remain**. Europe is still heavily fragmented in its S&A views (liberal approaches, East and West, larger and smaller countries, more and less mature countries, diverging economic and societal interests …). Yet, **a common a progressive maturity effort, possibly driven by the European Parliament and Council, and in an effective public – private cooperation Europe will find its ways for an increased sovereignty and autonomy**.

3) Make or Buy strategic solutions

Understanding of what solutions and competences (including "soft") are (or will be) available in Europe ("autonomous solutions") and what is (or will) brought from outside EU and how these solutions (internal and external EU) can be validated / certified to integrate trusted (and, if needed, sovereign) supply chains according to economic, geopolitical and societal issues.

4) Selection of priorities for investments of resources based upon a Sovereignty & Autonomy filter

As resources are limited and evolutions are frequent in the IT/cyber sector, we cannot follow in the same way all the different alternatives in the possible future scenarios. We must set priorities.

The analysis of the past, ongoing and envisaged ECSO activities **based upon Sovereignty & Autonomy issues (the "S&A filter") could better identify the needed priorities for investments.**

Applying the S&A filter for selecting priorities should not only be applied to ECSO but should also be considered by the European Commission in its future work programmes.

The European Commission could consider the increase of S&A as an important weighting factor in the evaluation of its future funded projects, according to a Work Programme that would underline their importance for such objective.

5) A European flagship initiative supported by ECSO and the European Cybersecurity Community for the development of the European cybersecurity ecosystem in a S&A approach

ECSO ambition, as for the past 5 years, is to federate and support the Cybersecurity Community at European level, also in line with the objectives of the EU Competence Centre. ECSO is continuously evolving to follow the ever-changing needs of the European cyber ecosystem and will increasingly support the development of European S&A approaches. **In particular, its working groups will propose S&A priorities that will be compared to those deriving from a comprehensive analysis of needs from possible future scenarios** (from the Board, Strategy Committee and CYSSA).

We propose to get the **support from top managers from ECSO members and of the wide European Cybersecurity Community**, who would interact with public administrations (at national and European level) and with other investors, **to promote a major public – private flagship initiative at European level**, focussing objectives and resources to strategic S&A solutions which could complement and support the actions foreseen by the European Competence Centre and its approach. ECSO would of course provide support to the coordination of this initiative.

This flagship would be a European public-private initiative would federate existing competences for increasing the European S&A within an agreed common scenario / vision started in close coordination with national administrations (considering the different sovereignty concerns) to get strong political and economic support and trust while remaining in line with and provide support to the objectives of the ECCC (EU competence Centre) federating projects.

Such flagship could be a comprehensive programme dealing with:

- **fostering regulations (demanding the use of EU solutions in specific sensitive sectors),**
- **support for public procurement of certified / trusted European solutions,**
- **support to R&I of technologies to increase European cybersecurity autonomy,**
- **support the identification, development, public – private funding and implementation of "federating projects",**
- **support to European standards and certification of trusted / resilient supply chains,**
- **support to awareness of choosing and using trusted European solutions,**
- **support to training and skills to increase competence in Europe,**
- **support to investments in startups / SMEs to keep key innovative technologies in Europe.**

In certain cases, the challenge would be to federate interoperable European solutions to integrate them into a higher level "platform" gathering the best EU competence for specific applications.

These "higher level platforms" could be managed, for instance, by "flexible JVs" (industrial alliances for strategic cybersecurity solutions) or EEIG (European Economic Interest Group) where specific solutions from suppliers would be integrated following validation and interoperability tests, e.g. in common EU infrastructure supporting such approach. This approach could be stimulated and supported by the "federating projects" of the ECCC and by the EDIH (European Digital Innovation Hub) initiative.

NOTE ON DEFINITIONS USED

Digital Sovereignty can be defined as the power of a country to independently define and enforce laws or regulations (including usage of standards and certifications) dealing with digital issues.

Strategic Autonomy is an enabler of sovereignty and can be understood as the capability of a stakeholder (public or private) to master certain technologies, and their implementation in products, systems or services. Their manufacturing can be done outside a country (or a continent) if the manufacturer controls the full supply chain or if national administrations can certify that certain components or equipment manufactured somewhere in the world and possible updates /patches (following certain rules) are compliant with national security laws (sovereignty laws) and that they can be used with trust in the supply chain.

The interpretation of Strategic Autonomy can be different according to the different interest of stakeholders form Political, Economic and Societal (citizens) aspects. Common views and objectives are this not so easy to reach.

The previous definitions should be complemented by the concept of "Dependency". We should identify, and possibly develop / produce those components or services that are critical and essential (upon which we are "dependent"), from those that can be replaced by others provided by different "less sensitive" suppliers. Linked to autonomy and dependency concepts there are also the concepts of Resiliency of the supply chain elements and availability of the needed Competence in case of crisis. If we are autonomous there are lower chances to suffer from a disruption in the supply chain in case of crisis. Similarly, if we have a sufficient level of competence, we react and overcome to crisis situations.

SUGGESTED NEXT STEPS ACTIVITIES for WGs

WG3	
WG3 - 1: Creation of the CISOs European Community – CEC for increased sharing of strategic threat information and possible prevention & response to these threats	Effective cooperation among CISOs of private users & operators within a sector, across sectors and across Europe ("CISOs European Community" – CEC, supported by an information sharing / IoC platform) to raise awareness and provide an increased sharing of strategic threat information and possible detection & response to these threats. The ECSO CEC could explore ways and means to develop such an approach and see how this could be complementary to what is currently under development by the EC and MS.
WG3 - 2: Identification of main areas and operational requirements that would need "sovereign" solutions	CISOs in the CEC could identify what are the main areas and the operational requirements that would need "sovereign" solutions considering the sensitiveness (operational, societal, economic, …) of used data.
WG3 - 3: Creation of an independent European Cybersecurity Rating	An independent European approach for sovereign cybersecurity rating of companies and / or products to allow CISOs to better understand if a product / service and the supply chain is trusted, if it is allowing a sufficient data sovereignty or subject to third country laws etc.
WG6	
WG6 - 1: Identification of strategic technologies / services to be developed in light of S&A and evaluation of potential cost advantages for such autonomous solutions	Identification, in a comprehensive vision, of the strategic technologies / services to be developed in light of S&A and demonstrate, when possible, how autonomous solutions could have a lower comprehensive cost (considering all the life cycle and potential impact of threats) and not only specific security / sovereignty advantages (see also LP-TF-1).
WG6 - 2: Identification of strategic solutions for improved security by design and S&A in cooperation with other EC initiatives in a multi-sectoral & multi-technology approach (Transcontinuum)	Cooperation with other initiatives / PPPs to provide a better and more consolidated understanding of needs in a wider and possibly comprehensive vision of the future digital landscape to identify and develop strategic solutions effectively needed to increase European S&A also in a "security by design" approach (also link to CYSSA)
WG6 - 3: Identification of strategic S&A technologies for dual use	Creation of a matrix of capabilities and technologies to assess to which extent key dual use and space technologies could satisfy the development of strategic capabilities for S&A
WG1	
WG1 - 1: Update COTI in light of European S&A issues	Updated COTI to look at challenges of the industry relying on trustworthy solutions to ensure business continuity and European S&A issues. What certification of products (components, equipment, systems, services) / innovations are most urgent to increase S&A (beyond economic / market interests) for critical infrastructures and related services?
WG1 - 2: Certification approaches considering also strategic dependencies	Identification of certification approaches that should be developed or used, being more adapted to reinforce European S&A, in particular considering strategic dependencies and operational aspects

WG1 - 3: Support to the development and / or use of EU standards to reinforce European S&A	Identify what EU standards would be needed (existing or to be developed) to reinforce European S&A
WG1 - 4: Trustworthiness and "sovereignty" all along the life cycle of solutions / services	Identify solutions / process to assure trustworthiness and "sovereignty" all along the life cycle and the associated (and possibly quantified) risk management of solutions / services. This "duty of care" approach should tackle all the different steps: from development, production and certification of the different elements of the chain (including "sovereign procurements" for the most sensitive issues) to implementation, use, awareness / training, as well as updates and patching
WG1 - 5: Understanding trusted, resilient & sovereign supply chains which can be adopted across Europe	Understanding the challenges for EU sovereign supply chains for improved risks management of sensitive applications. How to build trusted, resilient & sovereign supply chains which can be adopted across Europe? What could be mastered in Europe and what purchased by non-EU trusted suppliers? What investments and political or trade engagements (components, raw materials, etc.) would be needed?
WG1 - 6: Priorities supported by EU funding for the development of strategic S&A capabilities and capacities for trusted & sovereign supply chains	Suggestion of priorities for the development of strategic S&A capabilities and capacities for trusted supply chains with the support of EU funding
WG1 - 7: Creation of a European federated public-private initiative to develop strategic S&A solutions and trusted EU supply chains on cybersecurity	Creation of a European public-private initiative federating existing competences for increasing the European S&A within an agreed common scenario / vision (a strategic roadmap to build trusted ecosystems and supply chains) started in close coordination with national administrations to get strong political support and thrust while remaining in line with the objectives of the ECCC (EU Cybersecurity Competence Centre) approach (see also WG2 - 4). As recently done in other main IT sectors , a group of high level managers (CEOs) from ECSO members could propose to national and European public administrations as well as to other main private representatives, ways and means to develop "federated" approaches (industrial alliances) for strategic cybersecurity solutions which can then also be supported at EU level by EU Institutions and instruments
WG2	
WG2 - 1: European market analysis using an S&A point of view	Market analysis and commercial impact assessment of increased European strategic cybersecurity autonomy as well as using sovereign supply chains. Leverage upon guidance and needs from other ECSO WGs (technology, users' needs, EU industry, skills etc.) in an increased dialogue between the R&D/RTO community and market players (provider/users/investors) to develop a better understanding of strategic needs, create real synergies and pooling & coordinating investment towards an increased S&A.
WG2 - 2: Increased visibility of European companies and solutions in the Market Registry	European actors appearing in the Market Radar / Registry to be given enhanced visibility directly supporting EU S&A (with the use of EU solutions) also when adopting the Cybersecurity made in Europe Label (see also WG4 - 2).
WG2 - 3: Creation of a European cybersecurity Fund of Funds also targeting S&A issues	A European cybersecurity Fund of Funds to target market / economic issues and support an increase in S&A keeping strategic companies in Europe and with a European management and ownership (contribution to S&A could likely also be obtained if support to the fund is provided by national administrations, looking at reinforcing national competence and "sovereign" solutions for sensitive issues).

WG2 - 4: European industrial alliances to create "trusted cybersecurity supply chains"	Build European industrial alliances to create "trusted supply chains" in cybersecurity (see also WG1 - 7). The challenge is to federate interoperable European solutions to provide solutions integrating the best EU competence for specific applications. These "solution platforms" could be managed by "flexible JVs" or EEIG (European Economic Interest Group) where specific solutions from suppliers would be integrated following validation and interoperability tests, e.g. in common EU infrastructure supporting such approach. This approach could be stimulated and supported also by the EDIH (European Digital Innovation Hub) initiative.
WG2 - 5: Improved trade conditions based upon strategic reciprocal dependencies	Support the development of those S&A solutions that could give Europe a competitive advantage wrt non-EU suppliers, in a way to create a reciprocal dependency on different strategic issues (Europe could be dependent by some strategic suppliers for certain issues, but those strategic suppliers could become dependent of Europe on other key issues).
WG4	
WG4 - 1: European cybersecurity SME Hub and Marketplace	Creation of a European cybersecurity SME Hub where SMEs would be able to better display like in a marketplace their competence and services / products as a strategic tool for the promotion of EU solutions (autonomy) in innovative sectors.
WG4 - 2: Spreading adoption of the Label "Cybersecurity made in Europe"	The adoption of the Label "Cybersecurity made in Europe" should be widely supported in the different EU countries as it would be a major contributor in promoting the use of European solutions (autonomy) and competitiveness of our industry
WG4 - 3: Continue and extend Cyber Investment Days initiatives	The Cyber Investment Days should be continued and multiplied, as this approach would also help to keep companies and competence in Europe, developing specific Capital Venture investments dedicated to cybersecurity in Europe and increase European strategic autonomy
WG4 - 4: Federation of European Cybersecurity Digital Innovation Hubs	Network of European Digital Innovation Hubs focussed on cybersecurity (in the frame of ECSO local and regional approach) also to develop the EU strategic autonomy at the very core market level. Further analysis could be made considering the effective needs and possible (economically, operationally) use of sovereign solutions / services at local / regional level..
WG4 - 5: Support to SMEs as users of cybersecurity solutions	Support to threat awareness, risk management and use of (at least basics) cybersecurity solutions for SMEs in Europe that have to face challenges and threats of the digital transformation with limited resources (and competence).
WG5	
WG5 - 1: Cybersecurity skills platform to better fit European needs, views and values	Provide curricula and practical skills assessment which would better fit European needs, views and values. A specific vehicle (job competence platform or other mechanisms) should be developed to better carry the competence validation and the opportunities to keep such competence within Europe (competence that will support the development of our autonomy).
WG5 - 2: Network of national Y4C chapters to develop the new European cyber generations	Cooperation with MS and national bodies, linking them into a "network of national Y4C chapters", for instance based upon student associations across universities (or similar national initiatives) for harmonising approaches and understanding of common issues and sharing of best practices
WG5 - 3: European Cyber Range Community	Creation of a European Cyber Ranges Community which could contribute to European strategic autonomy as it can be modelled according to effective (EU) market needs, without having non-EU imposed criteria for ranges. It would also highlight the European competence and excellence in cyber range solutions and services which could, if properly consolidated and showcased, surpass non-EU capabilities in this area.
WG5 - 4: Awareness and Cyber Hygiene also for increased understanding of S&A issues	Increasing awareness of decision makers and professionals in Europe as a prerequisite to build the needed sound basis for appreciating the need for procuring, implementing and using S&A solutions. A continuous effort in this direction is needed to support our S&A efforts, together with a proper cyber hygiene for the appropriate use of IT in the digital transformation
WG5 - 5: European Citizens' Cybersecurity Policy	Increased consideration of civil society, human factors and citizens issues in light of a European S&A, promoting, teaching and supporting implementation in legislations, technologies and services of European values, stressing the importance to defend European

	interests (political, economic, cultural etc.). This approach could be seen as a real "European Citizens' Cybersecurity Policy".
LP-TF	
LP-TF - 1: Cybersecurity procurement for sensitive applications	Ensure that strategic / sensitive tenders in Europe are not flooded by non-trusted solutions and that the offer should be compared against the comprehensive market value (i.e. the cost / impact on all the different steps involved in the production and use) of the solutions rather than against the pure purchase cost for the same tender
LP-TF - 2: Tracking market regulation rules impacting strategic EU companies	Analysis and follow up of market regulation rules (in cooperation with WG2) such as foreign subsidies and FDI (Foreign Direct Investments) in strategic EU companies (and their technologies) for which Europe would keep a sufficient level of control
LP-TF - 3: Recommendations on coming EU legislations impacting cybersecurity	Recommendations for S&A from the LP-TF, when considering the large legislative activity impacting cybersecurity expected in 2021 and beyond. This point will be detailed when legislations and LP-TF will develop further.
NAPAC	
NAPAC - 1: NAPAC evolutions to discuss ECSO activities for increased S&A	The NAPAC should continue to regularly review the recommendations that ECSO WGs / TFs will make to follow closely the objectives of the ECCC, the EU policies and regulations, with a further focus for an increased European S&A. In particular, considering that sovereignty issues are in the remit of national administrations, their advice and guidance will be of particular importance also for the definition of priorities for investments in strategic autonomy and the identification of key issues for sovereign supply chains.
CYSSA	
CYSSA - 1 European flagship initiative for the development of the European cybersecurity ecosystem in a S&A approach.	Analysis and development of a comprehensive vision (national security & geopolitics, societal issues, economic, technology evolutions, business models evolution, …) we will be able to envisage and possibly anticipate future strategic needs which should be included in an S&A approach. This will allow the identification of those strategic EU solutions and needed legislations to build upon trustworthy supply chains, establishing a collective message towards sovereignty recovery, focussed and targeted investments/resources for an increased S&A. Capabilities and capacities would then be developed in a European flagship initiative supported by ECSO and the European Cybersecurity Community