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

PROLOGUE

Members of the ECSO Secretariat have started discussing with the top ENISA management about European Sovereignty, since 2014. It has been a long journey to understand the different issues and possible way forward. With the progress of the digital transformation, it has become clearer that Europe needs a higher level of control on its digital infrastructure and its data.

Yet, we are still trying to identify at national and European level which are the most critical technologies, services and other strategic elements composing the cybersecurity ecosystem (including human factors and competences) that we need to master. We need also to understand which is our degree of dependency on external factors (extraterritorial laws, geopolitical issues, etc.) that we cannot control but that could have a high impact on our digital society.

This document is the first synthesis made under the CYSSA (Cyber Security Sovereignty and Autonomy) Working Party to present the different past and ongoing activities on digital / cybersecurity sovereignty and strategic autonomy of the different ECSO Working Groups (WGs) and Task Forces (TFs). As conclusion of this analysis we will give at the end some recommendations on how to better identify challenges and priorities to tackle cybersecurity sovereignty and strategic autonomy at national and European level.

The CYSSA Working Party is for the moment only a "virtual body" which creation and ToRs have been agreed by the ECSO Board in September 2020. To start the work, the ECSO Secretariat is proposing to the Board and the WGs a synthesis of the situation and of the many ongoing discussions / papers in order to stimulate priority activities in the WGs and focussed actions on Sovereignty and Autonomy (S&A).

As per its ToRs (see Annex 1), CYSSA will identify those activities of the different ECSO WGs and TFs that are relevant for the European Cybersecurity Sovereignty and Strategic Autonomy, illustrating them in a comprehensive way and providing them with an adequate visibility for the main European and national stakeholders. It will also identify further actions, in cooperation with WGs and the Strategy Committee, to be carried on by the WGs and TFs to increase sovereignty and autonomy in Europe. The idea is not to increase the activity of the WGs, on the opposite, the S&A approach should allow better targeting use of limited resources towards those activities that are relevant for S&A of Europe.

First of all, we would remind here what we define as "sovereignty" and "autonomy"[1]. They are complementary concepts but their definition and use are maybe different from the buzzwords used in Brussels.

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.

[1] In the following, when needed, we will refer to Sovereignty and Autonomy as S&A.

A particular case strategic autonomy could be considered when a company, not subject to a "sovereign decision", decides to limit access (e.g. for strategic business reasons) to its technology or services. This act could cause serious damages to third parties if they are dependent on that supplier.

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.

The diversification of suppliers contributes to the concept of resilience of trusted supply chains (trusted in the sense that suppliers underwent an "audit for trust" according to certain criteria) hence to the continuity of National / Country security and to critical activities but also business continuity.

It is the duty of a sovereign country to provide secure or vital services to its citizens, society or economy independently from the (potentially) critical situations. At the same time it is the prerogative of a sovereign country to define and enforce laws. Therefore, when continuity is needed in National / Country security or in vital activities, a resilient and trusted supply chain could be considered as "sovereign" when it fulfils national laws and strategic / vital needs.

Representatives from Member States in European Institutions elaborate European regulations laws that are applied the same way across EU countries: this could be considered as a form of "delegated European sovereignty" or "Co-Sovereignty". Directives, being transposed in each EU country according to national laws are only an "adapted" expression of a common European views and as such are closer to national sovereignties.

European autonomy is a concept more easily adopted, as it is linked to (industrial) competence and capabilities. These depend mainly on the investments made and on human resources, not on political or legal decisions (as for sovereignty).

While cooperating with its partners at global level, Europe must be able to develop its cybersecurity ecosystems according to its own rules and value. This is the way to European sovereignty.

ECSO, in its continuous improvement endeavours to face evolving challenges. It will adapt its structure, objective and activities to continue federating the European cybersecurity community, also in light of the new regulation on Competence Centres, with highest priority to develop our cybersecurity sovereignty and strategic autonomy with an increased Resilient ecosystem and Competence .

INTRODUCTION

The COVID-19 crisis and the strong acceleration of the digital transformation has enhanced the need for cybersecurity in our society and a higher level of digital autonomy.

Looking at this crisis from different points of view (geopolitical, economic, societal and technological) we can recognize that the geopolitical and societal approaches are driving strategic decisions to counter the crisis, in particular pushing for a higher sovereignty, while the economic and technical approaches are more linked to autonomy.

Public administrations (and media) are in the driving seat for the political and societal issues, while industry (at large) is the main driving force of the technological and economic aspects.

Yet all these approaches need to be linked for a sound development of the digital ecosystem. Public – Private cooperation is even more needed than in the past, as it provides a strong link between sovereignty and autonomy and will support the needed recovery.

Over the past years, ECSO has consolidated its unique position as the leading close to market collaboration platform in Europe, promoting European cybersecurity companies, forming a regional and European ecosystem where demand meets supply, funding, resources and know-how.

For years ECSO and its members have urged the Commission to develop and support the implementation of a European cybersecurity industrial policy. This has not occurred yet and ECSO, from the beginning, decided to develop and support its own views for such an industrial policy with its limited resources and with its limited dissemination capacity, and with the support of its members. The ECSO cybersecurity industrial policy has been deployed in the activities of its Working Groups thus contributing to the development of the European cybersecurity ecosystem and of an effective increase of S&A.

In ECSO we have proposed since the beginning in 2016 the development of the European cybersecurity ecosystem in public – private cooperation, supported by a sound industrial cybersecurity policy. Our message has been heard at national and European level as many activities have been developed in the last 5 years to support the growth of Europe in this sector.

Approaches and understanding of the issues are still different across EU countries and even in Brussels, while giving increasing visibility to cybersecurity, the priorities for the future seem to consider cybersecurity as a kind of add-on to main challenges, instead of having it as (the many time called) "build in by design".

Even now, with a growing level of maturity as demonstrated in our public – private cooperation and with a growing digital transformation, it is still complex to have a clear understanding of what the future will be and a have vision of which strategic solutions should be "sovereign" (i.e. follow under scrutiny of public administrations) or mastered for an increased autonomy (with increased investments in particular from the private sector).

The complexity is actually increasing because of the dependency of the society on the digital transformation in addition to the continuous evolution of the societal, economic and political situations. Another important aspect having an increasing impact on the digital transformation is the scarcity of resources (investments, raw materials, etc.) and the "competition" with other priorities (e.g. climate change, pandemics).

Since the creation of ECSO in 2016 we have organised our working groups in activities that could support the growth of the political understanding, the awareness of decision makers and citizens, the skills and competence of professionals, the technology innovation, the investments in strategic sectors and companies, the protection of vital services and the economic growth …

ECSO WGs have produced deliverables that, even if having started without a comprehensive strategic vision for sovereignty and autonomy, can be well perceived through this prism.

We would review hereafter the different activities and initiatives that have been started in the last 5 years of ECSO in Working Groups and Task Forces, and which are relevant to build an ECSO approach to sovereignty and autonomy,

For those activities which are relevant to S&A, we have analysed the activity of the WGs via an S&A filter, and present here the results of this exercise including potential future "*Next Steps for S&A*" that could be performed by our WGs / TFs to identify, 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.

ECSO WGs and TFs ACTIVITIES IN LIGHT OF S&A ISSUES

WG3

ECSO WG3 worked from the beginning to identify the challenges and the needs of the main different vertical applications. It has engaged directly with users (operators, companies, governments) to understand cyber threats, share information among trusted peers, link supply and demand. WG3 acted as a transversal WG providing recommendations on policy, technology and strategy capacity / capability mapping sectoral needs and requirements for standardisation / certification; education, training and exercises; research / technologies; local / regional initiatives.

Professional users / operators but also citizens still often consider cybersecurity as an (expensive) "add on". Some of them, those more exposed to critical consequences of cyber threats, are progressively adopting more protective postures. Indeed, certain applications (infrastructure / vital services) are of strategic importance both for national security, for society / citizens' vital services, economy etc. Yet, looking at the cost of solutions, users are often opting for a best performance / price ratio, not necessarily including in the performance aspects the "sovereign" concept (including the protection of sensitive data in a trusted / sovereign environment) or even the resiliency concept.

We know that applications do not have the same level of maturity and / or criticality: the situation is different according to the considered sector and the sensitiveness of managed data and the possible impact to physical security - IT vs OT issue (e.g. for non-EU organisations owning critical infrastructures, interconnectivity of the infrastructures etc).

It is difficult today for a user (e.g. CISO) to quantify and justify with respect to its management the purchase of solutions / services which could be more expensive simply because they better respond to "sovereign" requirements, in particular when those requirements are not mandated by regulations.

Users / Operators dialogue and cooperation: strategic threats identification and information sharing for adequate response from the European private sector. The identification and response / recovery phases would need a good knowledge of threats and trusted solutions for an adequate risk management.

An increased European autonomy could allow essential and important entities (including those linked to manufacturing) to identify and respond in an independent way to cyber and hybrid threats, without being subjected to external (non-EU) interests which for different reasons could not have the same objectives, in particular in case of international crisis.

Member States have created national CSIRTs and linked them in a network. The last E.C. strategy envisages the creation of a network of national SOCs. There is a good dialogue between public administrations and private users at national level and among the public sector at national and European level, well following sovereignty issues. Yet, Chief Information Security Officers (CISOs) of users and operators from essential and important entities are not sufficiently connected between themselves and with public administrations across Europe. This could lead to major problems in case of cyber-attacks of large scale as detection and reaction time is of the essence.

SUGGESTED NEXT STEPS for WG3 in S&A - 1: Creation of the CISOs European Community – CEC for increased sharing of strategic threat information and possible prevention & response to these threats

An effective cooperation among CISOs of private users & operators within a sector, across sectors and across Europe (network called the "CISOs European Community" – CEC – an evolution of the ECSO Users Committee, possibly supported by an information sharing / IoC platform) could raise awareness and provide an increased sharing of strategic threat information and possible prevention & response to these threats. This approach from the private sector could provide some form of "autonomy awareness (for business continuity) and be activated in parallel to the approach foreseen by the public sector (at national and EU level) which would provide the "sovereign" approach (vital security).

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 as announced in the December 2020 EU cybersecurity strategy and which link this could have with the activity of the future EU Joint Cyber Unit. Representatives from the CEC could be invited as guests of the NAPAC (ECSO informal gathering of representatives from national public administrations) to present strategic / sovereign needs in the different sectors.

Sovereign solutions for users' protection and resilience.

It is only with the present evolution towards a dialogue among users' CISOs or equivalents (i.e. the CEC) that the discussion has moved towards more strategic and sensitive issues that can be linked to S&A needs.

The creation of such dialogue among trusted peers will allow sharing strategic threat intelligence among private users & operators from different sectors and different EU countries. This is particularly important when needing to protect sensitive strategic information and vital operations, to anticipate or better respond to threats.

Protection of users' data and operations would call for "sovereign" solutions for a trusted control of data management (e.g. for resilient operations and IP protection).

It could also be envisaged to develop an independent European approach for sovereign cybersecurity rating of companies and / or products.

SUGGESTED NEXT STEPS for WG3 in S&A - 2: Identification of main areas and operational requirements that would need "sovereign" solutions

CISOs in the CEC could identify (without compromising confidential information) what are the main areas and the operational requirements that would need "sovereign" solutions considering the sensitiveness (operational, societal, economic, …) of used data.

SUGGESTED NEXT STEPS for WG3 in S&A - 3: Creation of an independent European Cybersecurity Rating

An independent European approach for sovereign cybersecurity rating of companies and / or products could 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

The initial objectives of the ECSO WG6 was to define the cyber security EU R&I roadmap and vision to strengthen and build a resilient EU ecosystem. For this, it has analysed the challenges that enable and support the digital transformation of the society and of the main industrial sectors. It should now move forward to identify and sustain the R&D issues linked to EU strategic autonomy by developing and fostering trusted technologies.

R&I priorities for the development of strategic European solutions. After the first recommendation of R&D priorities for H2020 in the frame of the cPPP with the E.Commission, the WG6 has developed scenarios and priorities for Horizon Europe and Digital Europe Programme (see abstract in Annex 2 and 3).

These priorities have been selected also keeping into account a tentative global technology vision. Link has been made with activities in other WGs (e.g. WG1 on certification, WG3 on users' needs, WG5 on skills).

The WG6 has proposed, with the support of the Scientific and Technology Committee, an initial segmentation and selection also considering some S&A needs, but more work would be needed from WG3 from users / CISOs to identify effectively strategic operational issues, cooperation with WG1 and WG2 to identify what exists or is under development in Europe and what else should be needed, based upon possible future

comprehensive scenarios to consider not only technology evolutions but also societal and unexpected ecosystem / market evolutions.

SUGGESTED NEXT STEPS for WG6 in S&A - 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).

Cooperation across key technologies for a comprehensive vision. The WG6 has started to cooperate with other cPPPs (ETP4HPC, 5G IA, BDVA, etc…) to identify global challenges and the need to address them in a transversal and coordinated way liking our R&I priorities to priorities in other sectors (I.A., 5G, HPC, etc) in the "Transcontinuum approach".

Cooperation has also been initiated with JUs, Pilots on Competence Centres, EC projects and other initiatives to monitor the evolution of the cybersecurity ecosystem and understand gaps.

SUGGESTED NEXT STEPS for WG6 in S&A - 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 (also link to CYSSA). With this multi-sectoral & multi-technology approach, it would be easier to identify and develop those strategic solutions effectively needed to increase European S&A also in a better "security by design" approach.

Dual use technologies to be mastered in Europe. WG6 has worked in collaboration with the European Defence Agency to understand how the already available and soon-to-be-commercialised technologies developed for civilian or industrial applications (dual use) can be used in the cyber defence domain (of particular importance for national sovereignty). The main motivation behind is to increase cyber resilience in the defence domain and ensure synergies between civil and defence sectors to better use and leverage the respective investments in Research and Innovation (R&I). The objective is to define the challenges for the defence sector to identify potential gaps in cybersecurity technologies and what are the collaborative actions needed to sustain long-term European cybersecurity and cyber defence capability development strategies.

ECSO WG6 has already identified an initial list of priorities for Research and Technological development to address cyber response operation, as one of the already identified EU capability development priorities. A similar approach has now been started in cooperation with ESA for space issues.

SUGGESTED NEXT STEPS for WG6 in S&A - 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

The ECSO WG1 is supporting the roll-out of EU ICT security certification schemes, standard and legislation recommendations (MoU with ETSI, CEN/CENELEC, collaboration with EC, ENISA and JRC, member of the SCCG) and the establishment of trusted and resilient supply chains.

ECSO WG1 has supported from the beginning the development of a European methodology for certification, also suggesting priorities for future certifications and standards, in other to develop supply chains based upon trusted and validated services, process and components.

It could now evolve towards activities closer linked to S&A issues but more resources would be needed, including improved market analysis and geopolitical knowledge in the frame of a shared EU cybersecurity industrial policy.

To emphasize the importance of such WG to sovereignty, it could be renamed "**Trusted and Resilient Solutions & Sovereign Supply Chains".**

European certification challenges and approaches to support European sovereignty. Standardisation and certification are key to support (national) sovereignty within a well-defined strategic vision and industrial policy (if they exist…). The digital transformation with its increased attack surface and constant evolving threats has put emphasis on increased cybersecurity requirements for suppliers and an improved management of trusted and resilient supply chains to ensure business and service continuity.

For certain (vital) applications the supply chain should not only be "trusted" or "resilient" but also "sovereign" (in the sense of having the full control of data in the country). Certifications at EU level could provide an indication (compliancy) of the security of a product/service/system. Harmonisation at EU level and mutual recognition by member states of national certification schemes as well as the use of standards which really sustain the European industry and its solutions are fundamental to support trusted, resilient and when needed, sovereign EU solutions.

As ECSO WG1 has also dealt with cybersecurity certification approaches (e.g. meta scheme to establish an EU cybersecurity certification scheme, composition approach - inter-relationship / composition of certified components and reuse of evidence, …) and has identified the challenges for roll-out of certification schemes: framework consistency and market needs. The WG1 is also working on understanding the systems' & services' dependencies, needs and current approaches for risk management and operational aspects.

In WG1, we have developed the SOTA and the COTI providing respectively the State of the Art Syllabus and the Challenges of the Industry for certification. These documents could now evolve to better consider S&A issues.

SUGGESTED NEXT STEPS for WG1 in S&A - 1: Update COTI in light of European S&A issues

Update COTI to look at what could be the challenges of the industry to rely on trustworthy solutions to ensure business continuity and European S&A issues. Special attention should be given at the following question: 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?

SUGGESTED NEXT STEPS for WG1 in S&A - 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.

SUGGESTED NEXT STEPS for WG1 in S&A - 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.

Understanding needs for trusted, resilient & sovereign supply chains. Sovereign supply chains in line with European standards are of primary importance for S&A. We know that not everything can be done in Europe because of the needed investment, due to the breadth of IT & cybersecurity issues as well as the fast-evolving pace of the digital world. Certifications according to national / EU laws can then qualify as trusted (and allow their insertion in "sovereign supply chains") also those elements which come from outside Europe.

Definition of needs for sovereignty of solutions & services could also tackle customisation of products, patching, updating etc. Yet, differences in interpretation of EU sovereignty across the EU, according to local political & economic interests, could lead to different levels of security and certification.

SUGGESTED NEXT STEPS for WG1 in S&A - 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.

SUGGESTED NEXT STEPS for WG1 in S&A - 5: Understanding trusted, resilient & sovereign supply chains which can be adopted across Europe

Understanding the challenges for EU sovereign supply chains and improved risks management. How to build trusted, resilient & sovereign supply chains which can be adopted across Europe? What should 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?

SUGGESTED NEXT STEPS for WG1 in S&A - 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.

Strategic S&A solutions and trusted EU supply chains on cybersecurity. Europe is progressively building the key bricks for an S&A approach, with its EU certification approach, the coming EU Centre, the National Centres and the Network, the Public-Private Community (already initiated by ECSO) to develop European competences (and capacities) in cybersecurity.

For the moment, we have a political guidance from the Commission on strategic priorities for technology sovereignty linked to three IT aspects: High performance computing, Connectivity and Cloud.

While all these three topics are linked to cybersecurity, we cannot see a clear policy guidance being put forward for an increased S&A in cybersecurity. Something more specific would be needed, like what is happening for AI, encryption, 5G (and in the future 6G) … and the appropriate use of cybersecurity in all applications.

The example of GAIA-X in the cloud sector is also an interesting one when discussing "sovereignty". Similar to the initial Airbus agreement, the initiative is coming from the European private sector with a strong support from certain public administrations. In GAIA-X the urgent need to manage data following "European rules" and the impossibility to invest in the short term to develop a full European autonomous cloud led to a cooperation with non-EU companies which can participate in the initiative if they comply with basic principles, is necessary. This would allow the development of trusted services for data management and boost the European market.

Even if not totally adaptable to the cybersecurity domain, there could be a similar public-private agreements to support trusted European approaches / solutions / services while also using those (certified) offering coming from outside EU when Europe cannot produce on its own (for whatever reason).

As cyber stakeholders (suppliers and users) are widely distributed in Europe, a political agreement would be needed across all the EU countries (which could be more challenging from the political point of view but also would provide higher weight of such agreement).

Also, major European companies having market interest at global level (and often making a larger part of their business outside Europe) have to balance their position on European S&A with respect to their global market interests.

SUGGESTED NEXT STEPS for WG1 in S&A - 7: Creation of a European public-private initiative federating existing competences to develop strategic S&A solutions and trusted EU supply chains on cybersecurity (link with SUGGESTED NEXT STEPS for WG2 in S&A - 4: European industrial alliances to create "trusted cybersecurity supply chains")

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 (considering the different sovereignty concerns) to get strong political support and trust while remaining in line with the objectives of the ECCC (EU Cybersecurity Competence Centre) .

As recently done in other main IT sectors (e.g. AI), a group of high level managers (e.g. CEOs) from ECSO members could propose to national and European public administrations as well as to other main private representatives, ways and means (based upon an analysis and strategic roadmap made in ECSO) 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

The ECSO WG2 has developed and maintains a view on the Cybersecurity Industry in Europe, supporting stakeholders to improve their market knowledge (products, suppliers) and the growth of European companies via dedicated cybersecurity investments. The international dialogue supported by our WG2 could also be beneficial to S&A in defining synergies and cooperation with external trusted partners and keeping competence in Europe.

Cybersecurity Market knowledge and Market Radar / Registry to provide visibility to European solution providers. In its WG2, ECSO has developed a Cybersecurity Market Taxonomy which is a key tool to provide clear identification of available competences and products in Europe. This market knowledge is fundamental to have a good understanding of what Europe is producing and / or mastering, where competence is and what is missing.

In WG2 we have developed a Market Radar (boosting marketing capabilities of European cybersecurity companies by improving the visibility of their solutions and services). The Radar is allowing a first visibility of the European actors and their solutions. It will soon become a Market Registry with more interactive features and services for the community.

SUGGESTED NEXT STEPS for WG2 in S&A - 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 pooling & coordinating investment towards an increased S&A.

SUGGESTED NEXT STEPS for WG2 in S&A - 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).

EU cybersecurity investments and Fund of Funds for European companies. In the last years we have facilitated innovative private and public investment capabilities, fostering understanding of the dynamics of the market and creating a community of investors and brokers supporting European industries.

More recently we have initiated the creation of an EU cybersecurity Fund of Funds (FoF) to allow first investments in European start/scale ups to keep their competence in Europe and possibly supporting their global development. In the following, such financial scheme would also support investments in European solutions / services to be adopted by (infrastructure) users. This approach will also help in keeping companies and competence under "European control".

SUGGESTED NEXT STEPS for WG2 in S&A - 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).

Market consolidation and growth with increased competitiveness of the European industry. The issue is not only about the competitiveness of large European companies active in this domain or the prestige they could have at global level, but also to be able to provide advanced/innovative and continuously updated solutions / services in a very (global) competitive market. This needs a large economic surface that few European companies have.

Another limitation is due to the origin of our major cybersecurity companies coming from the traditional defence market. These companies are used to their national professional markets with close links to the public administrations, a market having procedures and timing that are not always the same as in the more competitive global commercial market, mainly composed by private customers (professionals or consumers). As professional (dual) solutions are penetrating the defence market, competition from more dynamic companies is increasing, particularly in those areas handling sensitive data and hence more closely linked to S&A issues.

One of the topics that could be tackled by an S&A approach for European cybersecurity companies is the possibility to evolve into unicorns (not only start-ups/SMEs but also larger companies) and effective global (cybersecurity) market leader (European Champions). The issue here is not to build a European "cybersecurity Airbus", as sometimes is called the merging of different competence into one larger body, as the market structure is not the same (cybersecurity is composed by many different solutions that cannot be integrated in a unique system as in a plane).

For SMEs, the most urgent challenge is to facilitate a sustainable path and ecosystem for them to scale up and exit/IPO with the support of European investments instead of looking to access funds from the US or other markets. For larger companies, the challenge is to move from traditional approaches linked to secure national professional business into more challenging and dynamic global initiatives.

In the "fragmented" (politically, technically, economically) European market, EU companies, even if not becoming large unicorns, could federate their efforts and drive innovation and procurement, in close cooperation with suppliers (including SMEs) and research centres but also with strategic customers (operators …) and public administrations (for strategic procurements) to create a European approach in light of an increased S&A.

SUGGESTED NEXT STEPS for WG2 in S&A - 4: European industrial alliances to create "trusted cybersecurity supply chains" (link with SUGGESTED NEXT STEPS for WG1 in S&A - 7: Creation of a European federated public-private initiative to develop strategic S&A solutions and trusted EU supply chains on cybersecurity)

We should build in Europe industrial alliances to create "trusted supply chains" in cybersecurity (see also LP-TF for the foreign investments issue). Cybersecurity is not a market composed by large systems but composed by a variable number of different solutions. We should therefore consider the consolidation of competence in

ad-hoc bodies of limited but functional size, smaller size than the traditional "IT unicorns" (i.e. of the size adapted to the specific cybersecurity solutions and sectors).

The challenge would be 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 or a flagship programme as envisaged in our last recommendation.

International cooperation – dialogue with trusted third countries / allies for "reciprocal-dependency". The ECSO WG2 had in the past some exchanges for cooperation and dialogue with ministries and companies from non-EU countries (USA, Japan, Israel) in particular on certification issues and critical infrastructure protection and investments. This dialogue could go further in the domain of S&A, envisaging stronger partnerships across countries.

As Europe is dependent on certain suppliers (i.e. those for which a dependence on technologies, components, etc. might have political consequences in terms of sovereignty) we could identify, to balance the present situation, those strategic components/services and products where Europe is leader on the global market and use them as a bargaining chip when negotiating trade conditions with non-EU strategic partners.

SUGGESTED NEXT STEPS for WG2 in S&A - 5: Improved trade conditions based upon strategic reciprocal dependencies

While remaining a very political and sensitive issues, ECSO could work (in line with position from public administrations) to 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

The ECSO WG4 has supported the development of SMEs, start-ups and high growth companies, to help them create more market transparency and reach out far beyond their traditional home markets which are usually nationally or regionally limited in order to partner in R&D international project and access to European market and funds.

Support to SMEs to develop and market innovative European solutions. Support to SMEs (as suppliers of cybersecurity solutions and services) is a key issue when looking at increase of strategic autonomy. We have in Europe a huge number of SMEs with high competence. Issues linked to their development are not only about investments but also to support their activities and growth (accelerators etc) providing them an adequate market place for promoting their solutions.

SUGGESTED NEXT STEPS for WG4 in S&A - 1: European cybersecurity SME Hub and Marketplace

The creation of a European cybersecurity SME Hub where SMEs would be able to better display like in a marketplace their competence and services / products could be a strategic tool for the promotion of EU solutions (autonomy) in innovative sectors. It would support *SMEs in Europe that are either directly selling their products to the market or be key suppliers to strategic integrators (this having a major potential impact on sensitive applications).*

Label "Cybersecurity made in Europe. ECSO has recently created with its members / partners the label "Cybersecurity made in Europe". This is a marketing initiative (not a certification label) which would provide visibility to true European companies according to 5 "European" criteria defined by our Partners.

SUGGESTED NEXT STEPS for WG4 in S&A - 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 solutions coming from European suppliers, hence supporting the use of European solutions (autonomy) and competitiveness of our industry.

Cyber Investor Days. With its "Cyber Investor Days" across Europe ECSO is supporting investments of European investors in European SMEs.

SUGGESTED NEXT STEPS for WG4 in S&A - 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.

European Digital Innovation Hubs. The ECSO WG4 has also developed coordinated activities between Regions, Clusters (both business oriented and triple helix) and local bodies (e.g. smart cities) for accelerating the commercialisation and scaling up of the interregional innovation projects (European Smart Cyber Regions[2]: Inter-regional acceleration programme Inter-regional cooperation, Federated Cyber Range). Part of the services proposed by the Smart Cyber Regions project for the deployment and commercialisation of cybersecurity solution will be integrated by the future European Digital Innovation Hubs).

SUGGESTED NEXT STEPS for WG4 in S&A - 4: Federation of European Cybersecurity Digital Innovation Hubs

With its local and regional approach ECSO is developing 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 also in the frame of the Network of European Digital Innovation Hubs and the approach to federate at EU level DIH focussed on cybersecurity.

Support to SMEs as users of trusted European solutions. Support to SMEs (as cybersecurity users) is a key issue when looking at the digital transformation and the "Recovery". SMEs are the fabric of the European economy and their protection against cyber attacks will also contribute to increase our strategic autonomy.

SUGGESTED NEXT STEPS for WG4 in S&A - 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

Education, Training, Exercises/Ranges are fundamental in building up skills and awareness (including cyber hygiene) at European level. They are the basis upon which ECSO WG5 would build its actions for an increased European S&A.

A bigger effort should be done here across Europe or we will never be able to develop a true European vision with increased S&A, remaining dependent on external strategic competences and capacities.

[2] Previously called "Cyber Valleys"

ECSO has developed several initiatives relevant to European S&A contributing to an increased cybersecurity resilience, competences and capacity building effort, through increased education, professional training and skills development, as well as actions on awareness-raising and gender inclusiveness.

EHR4CYBER (European Human Resources 4 Cyber) providing curricula and practical skills assessment for European needs, views and values. EHR4CYBER is looking at improving skills in professionals and developing harmonised skills verification through use case model approach (which skills needed for specific tasks or scenarios) and minimum curricula (for university degrees), as well as supporting HR specialists in hiring cybersecurity talent.

SUGGESTED NEXT STEPS for WG5 in S&A - 1: Cybersecurity skills platform to better fit European needs, views and values.

The EHR4CYBER *approach is expected to largely contribute to European strategic autonomy as it would 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).*

Y4C (Youth4Cyber): allowing new generations of Europeans to better deal with digital challenges. The Y4C initiative, still in its early phase, should foster the awareness of the young population (6 – 26) on cyber threats and cyber hygiene but also trigger vocations for a career in cybersecurity. Understanding of cyber issues from an early age would dramatically change the future European approach, allowing new generations to deal with digital challenges in a more responsible way and better consider the opportunity and the importance for an increased S&A.

SUGGESTED NEXT STEPS for WG5 in S&A - 2: Network of national Y4C chapters to develop the new European cyber generations

As education is a national prerogative, this initiative should be built primarily in 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.

European Cyber Ranges: cyber ranges responding to common European views. ECSO is starting its European Cyber Range Community approach with a charter of criteria to identify cyber ranges responding to common European views, consolidating and showcasing them in a way that would also facilitate the capacity of end users to adequately select and acquire cyber ranges or cyber-range enabled services best fitting their needs.

SUGGESTED NEXT STEPS for WG5 in S&A - 3: European Cyber Range Community

The European Cyber Ranges Community approach is expected to largely 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.

Awareness and Cyber Hygiene: increasing awareness of decision makers and professionals in Europe in the digital transformation. ECSO WG5's objective is also to raise awareness on basic cyber hygiene skills (through the awareness calendar) and support EU and members' awareness initiatives.

SUGGESTED NEXT STEPS for WG5 in S&A - 4: Awareness and Cyber Hygiene also for increased understanding of S&A issues

Increasing awareness of decision makers and professionals in Europe is 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.

Civil Society, Human Factors & Citizens issues: towards a "European Citizens' Cybersecurity Policy". A new areas for ECSO WG5's, but somehow already tackled when dealing with gender issues, privacy and European values in innovative technologies, consumers users, as well as in education of the young population.

SUGGESTED NEXT STEPS for WG5 in S&A - 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".

W4C (Women4Cyber): spreading across Europe and beyond European messages, competence and values with relevance to gender issues. The W4C initiative, now a self-standing Foundation, is supporting an enhanced participation of women in cybersecurity, considering the huge future needs of experts (in all fields, not only STEM) that the protection of the digital transformation will require. Differently from other ECSO initiatives, W4C has an approach which goes beyond the European focus. Yet, it is very relevant for Europe as it is spreading across Europe and beyond European messages, competence and values. W4C could be an important contributor to a wider acceptance of European solutions and best practices across the world, supporting the development of European autonomous approaches.

Legislative & Policy Task Force (LP-TF)

The ECSO Legislative & Policy Task Force is expected to contribute to **identifying the strategic areas where specific EU legislations would be needed to support the development of the European cybersecurity ecosystem but also to reinforce sovereignty** (e.g. adoption of trusted / certified European solutions / services for sensitive applications**) and support the increase of strategic autonomy** (e.g. via specific funding programmes etc.).

Legislations and Policies for increased Sovereignty and Autonomy. We are just at beginning of the activity of the ECSO Legislative & Policy Task Force[3] (LP-TF) but its wide span of foreseen activities, looking at the different legislations and regulations on IT & cybersecurity at European level[4] including those linked to public procurement, is a promise for interesting contributions to our S&A recommendations.

As sovereignty is closely linked to law / legislations, it is of fundamental importance to understand what is missing or what should be improved in EU legislations to increase sovereignty in specific sensitive areas.

[3] Previously called Legal & Regulatory Task Force (LRTF)

[4] EU Industrial Strategy (Digital Education Action Plan, Implementation of the EU Gender Strategy, coordinated investment by Member States and industry in the form of new IPCEIs, Follow-up to the 5G Communication and the Recommendation on cybersecurity of 5G networks …), SME Strategy for a sustainable and digital Europe (Capacity-building and support for the transition to sustainability and digitalisation; Reducing regulatory burden and improving market access; Improving access to financing); EU Programmes (e.g. Horizon Europe, Digital Europe Programme, Recovery Fund, InvestEU, …); New Cybersecurity Strategy; Digital Services Act; Data Act; EPCIP review (on E. Critical Infrastructures), European Cybersecurity Industrial, Technology and Research Competence Centre Regulation; Legislations with impact on WG1 issues: New Legislative Framework; Radio Equipment Directive (RED); Machinery Directive; Medical devices regulation; European Secure Digital Identity for citizens …

The European Commission has understood the challenge of the digital transition and is reviewing many directives such as the e-commerce (today called the Digital Services Act and the Digital Markets Act), the NIS Directive 2.0, the definition of critical infrastructures, the revisions of the NLF, Machinery Directive, RED, General Product Safety Directive, secure eID, etc. Collective European Sovereignty is strengthened through the regular revision and updates (when necessary) of these important legislations (Directives and regulations) that rule our society, economy and markets.

SUGGESTED NEXT STEPS for LP-TF in S&A - 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.

SUGGESTED NEXT STEPS for LP-TF in S&A - 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.

SUGGESTED NEXT STEPS for LP-TF in S&A - 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.

National Public Administrations Committee (NAPAC)

The ECSO NAPAC is a Committee which regularly meets under the lead of the representatives of the ongoing EU Presidency. It is reviewing the activities of the Board and of the ECSO WGs, providing, when needed an important advice for effective step forwards from the private sector of common recommendations and concrete actions.

SUGGESTED NEXT STEPS for NAPAC in S&A - 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.

CYbersecurity Sovereignty and Strategic Autonomy Transversal Working Party "CYSSA"

The ECSO activity within CYSSA is just starting with this paper. The CYSSA can provide a comprehensive understanding of the complex and interlinked challenges across WGs for an increased S&A. Its activity could help the Strategy Committee and the Board to define S&A objectives within possible global evolution scenarios. This discussion has been initiated also at the last General Assembly with the gathering of some important European cybersecurity experts (under the initial name of "The League") to present some major future challenges.

We would now develop a global vision towards a sound European cybersecurity ecosystem by 2030. This vision should consider the different technical and regulatory aspects and initiatives developed in our WGs but it will also consider market needs and foresight of application / societal evolutions in light of S&A issues. It would leverage also on the work of the ENISA "Forecast on emerging and future cybersecurity challenges".

SUGGESTED NEXT STEPS for CYSSA in S&A - 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.

THE VIRTUOUS CIRCLE OF DIGITAL SOVEREIGNTY AND STRATEGIC AUTONOMY

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 needs will then 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 that could identified 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) supply chains according to economic, geopolitical and societal issues.

We have to see what development is ongoing in Europe 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 identify which technologies Europe will 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.

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

At last, we need to see what awareness of decision makers and citizens is needed, what impact these strategic solutions would have on the civil society, what training would be needed by users – WG5.

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 theoretical 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.

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 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 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.**

ECSO would provide support to the coordination of this initiative.

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.

ANNEX 1 – From the CYSSA ToRs

1- Objective

The objective of the ECSO Transversal Working Party on Cybersecurity Sovereignty and Strategic Autonomy (CYSSA) shall be to develop and convey "common messages" on European Cybersecurity Sovereignty and Strategic Autonomy, supporting the development of opportunities for European solutions and growth of our industry.

The activities of the CYSSA TWP would also be in line with ambitions of the E.Commission on strategic autonomy and would meet institutional expectations of the Competence Centre approach.

This approach should help the European members of ECSO to develop their market and make ECSO recognised as the leading voice for the European cybersecurity sovereignty, attracting more support and participation from EU industry and administrations.

2- Mandate[5]

The CYSSA shall perform, inter alia, the following functions:

- Identify those strategic technologies / EU solutions and needed legislations to build upon trustworthy supply chains, building a collective message towards sovereignty recovery and focussed investments.
- Identify, in case of dependencies on certain suppliers how (technologies, components, etc) Europe could make other dependent on our strategic solutions for their supply chain, in order to have better trade conditions.
- Identify those activities of the different ECSO Working Groups that are relevant for the European Cybersecurity Sovereignty and Strategic Autonomy, inserting them in a comprehensive picture and provide them an adequate visibility to main European and national stakeholders.
- Assess when possible, the European market and commercial impact of policy driven strategic cybersecurity autonomy.
- Present the findings of this WP to the Strategy Committee, NAPAC and Board of Directors for external advocacy and actions, thus providing strategic guidance and recommendations for the ECSO WGs and LP-TF (Legislative and Policy TF);
- Receive, review and recommend proposals to the ECSO Working Groups and Board of Directors on the drafting of the ECSO common position papers and recommendations relative to European Cybersecurity Sovereignty and Strategic Autonomy also in collaboration with the LP-TF;
- Such other duties as may from time-to-time be assigned to the Working Party by the Board of Directors.

This Working Party should not duplicate work of other WGs but would gather findings and recommendations from ECSO WGs filling gaps when needed.

This Working Party would also strive for cooperating and convergence of views with the C.C. Pilots in order to consolidate the European Cybersecurity Community.

[5] NOTA: The mandate should remain flexible, according to evolving needs

ANNEX 2 – WG6 Priorities for the Horizon Europe Programme

The WG6 priorities for the Horizon Europe Programme are structured in 4 pillars.

1) ECOSYSTEM, SOCIAL GOOD AND CITIZENS

- APPROACHES, METHODS, PROCESSES TO SUPPORT CYBERSECURITY ASSESSMENT, EVALUATION AND CERTIFICATION
- BUILDING AND OPERATING RESILIENT SYSTEMS: ADAPTIVE SOFTWARE HARDENING, SELF-HEALING SYSTEMS AND RASP (runtime application self-protection)
- DEVELOPMENT OF DIGITAL FORENSICS MECHANISMS AND ANALYTICAL SUPPORT
- CYBER RANGES AND SIMULATION ENVIRONMENTS
- CYBER-PHYSICAL SYSTEMS SECURITY AND CYBER SECURE PERVASIVE TECHNOLOGY

The first pillar of the proposed R&I strategy identifies the importance to **create a sustainable ecosystem in Europe** where a cybersecurity culture and best practices need to flourish to address the needs of the citizens, society and develop the needed skills to cope with a fast-changing digital society or even digital world powered by cyber technologies. In this context, it is key to look at the societal impact of cyber technologies and moreover the threats that the use of insecure cyber technologies or the misuse of them can bring to citizens as individual entities or society as a whole. This may provoke a lack of trust and, subsequently, of acceptability of the digital world, and what can be done to build a more reliable and secure digital society. Moreover, the citizens' perception of cyber technologies may differ considerably from the actual state of the affairs and is connected closely with education and awareness.

Main levers to drive the priorities

- Development of resilient systems, including software, with a security by design approach to reduce the financial impact of zero-day attacks.
- Definition of risk management strategy and countermeasures to manage future unknown (evolving) attacks or fast-adaptable attacks that changes their behaviours exploiting vulnerabilities and potentially weak countermeasures.
- Vulnerability management and development of tools to support cybersecurity assessment, evaluation and certification.
- Develop measures for a trustworthy supply chain.
- Development of adaptive digital forensics mechanisms to cope with new emerging threats and increasingly heterogeneous distributed devices and technologies.
- Develop cyber range technologies and services and maximization of the benefits of the usage of cyber ranges within training contexts.
- Develop sector specialisation of cyber ranges as an enabler of the simulation and defence scenarios of critical infrastructures, essential services and application domains.
- Cybersecurity pervasive technology and management of cybersecurity challenges related to this machine economy based on the Internet of Things and Cyber Physical Systems
- Develop methodologies, tools and platforms to develop human body embedded devices with security by design.

2) APPLICATION DOMAINS AND INFRASTRUCTURE

- CYBER RESILIENT DIGITISED INFRASTRUCTURES
- SECURE QUANTUM INFRASTRUCTURES
- CYBER SECURE FUTURE COMMUNICATION SYSTEMS AND NETWORKS
- VERTICAL SECTORS CYBER CHALLENGES
    - Industry 4.0 and ICS
    - Energy (oil, gas, electricity), and smart grids
    - Transportation (road, rail, air; sea, space)
    - Financial Services, e-payments and insurance
    - Public services, e-government, digital citizenship
    - Healthcare
    - Smart cities and smart buildings (convergence of digital services for citizens) and other utilities
    - Robotics
    - Agri-food

The second pillar of the R&I cybersecurity strategy focuses on the **digitisation of vertical sectors** and the need for **resilient infrastructures**. The economic sectors identified in the ECSO SRIA v1.0 have been clustered into Industry, Finance, Health, Construction, Energy, Transport, Public services and Telecom. These sectors have grown in a process of vertical integration which was largely triggered by the key technological and organisational trends that characterise the 4th industrial revolution. To some extent, the digital transformation may potentially blow up or at least shaken historical siloes which today do not necessarily find a technological relevance. An interesting example to consider is the penetration of IT vendors into very structured industries like automotive. A shift of power that may lead to a redefinition of market segments for cybersecurity as well. In addition, we may have to consider sectors which are not yet tagged as "critical" from a cybersecurity perspective but are still vital for the human and may need to enter into the frame if we consider the technological changes affecting them.

Main levers to drive the priorities

- Enhance the security level of highly critical infrastructure, including, energy (electricity, gas, oil), water distribution, telecommunications, etc.
- Improvement of the reaction to cyber incidents, sharing information among the relevant stakeholders involved in critical infrastructure management and operation.
- Increase trust in the 4th industrial era to reduce the impact of cyber threats on business continuity.
- Develop cyber secure communication systems and networks of the future.
- Manage security orchestration in heterogenous systems and networks

3) DATA AND ECONOMY (TO PROVIDE THE FOUNDATIONS FOR A TRUSTWORTHY AND RELIABLE DATA-DRIVEN ECONOMY OF THE FUTURE)

- DATA SECURITY AND MALICIOUS USE OF DATA
- END-TO-END PRIVACY
- ECONOMIC ASPECTS OF CYBERSECURITY

The third pillar builds on **data and economy**. Data will be the key driver to our digital economy and has attracted a lot of discussion for its implication in the digital transformation of the society and the digitalisation

of the vertical sectors. Securing the data, the algorithms that operate on top of them, as well as their final results will be of paramount importance for the future of the data-driven economy in the Digital Single Market. The innovative aspect driving the need for investment should deal with data security, privacy aspects and how data interacts with the economy, requiring the definition of specific data economy models.

Main levers to drive the priorities

- Support the needs of digital services with new trustworthy privacy preservation techniques to protect the economic growth and European digital transformation.
- Provide tools and mechanisms for supporting the processing, mining and dissemination of personal data and models with privacy guarantees.
- Verify the correctness of the information to increase trust in digital services.

4) BASIC AND DISRUPTIVE TECHNOLOGIES (TECHNOLOGIES, METHODOLOGIES, AND BUILDING BLOCKS TO DEVELOP AND A SECURE AND RESILIENT DIGITAL SINGLE MARKET)

- SECURE AND TRUSTWORTHY ARTIFICIAL INTELLIGENCES
- SOFTWARE AND HARDWARE CYBERSECURE ENGINEERING AND ASSURANCE
- CRYPTOGRAPHY
- BLOCKCHAINS AND DISTRIBUTED LEDGER TECHNOLOGIES
- IOT SECURITY
- ARTIFICIAL INTELLIGENCE TECHNIQUES FOR BETTER SECURITY AND MALICIOUS USE OF AI

The fourth pillar is the **development of basic and disruptive technologies** that are expected to have a strong impact on markets, industries and citizens in the future and which will efficiently support the three strategic pillars mentioned above. Some identified prominent technologies are Artificial Intelligence, Blockchain, IoT, and Quantum Computing.

Main levers to drive the priorities

- Model and validate security properties for AI-driven systems, inherently dynamic and dependant on the availability and quality of data
- Define trustworthy AI-based systems to increase trust in the decision process and foster society at large to obtain the expected social benefits.
- Design and implement procedures that can produce concrete security guarantees for the overall system along the product chain, from hardware implementation to product deployment.
- Design and implement technologies for trusted electronics and continuously assess their quality and security
- Design of cryptographic schemes and systems.
- Develop procedures for the secure evaluation and efficiently implemented cryptographic algorithms
- Design new digital-based currency that is as secure and privacy-friendly.
- Address IoT challenges at all layers in the stack (device, connectivity, platform and application), and a across different layers or IoT systems as a whole.
- Design a new family of applications, aware of relevant adversarial behaviour and capable of both detecting when they are under attack and adapting their behaviour as needed.

ANNEX 3 – WG6 Priorities for the Digital Europe Programme

SUPPORT TO POLICY IMPLEMENTATION

- DEVELOP TOOLS TO SUPPORT THE IMPLEMENTATION OF EU CYBERSECURITY ACT
- THREAT MANAGEMENT AND CROSS-VERTICAL PLATFORMS
- GOVERNANCE, POLICY AND LEGAL ASPECTS

Main challenge

There is a growing need to define standardised and harmonised approaches to support the implementation of cybersecurity policies in Europe. The common definition of certification schemes (through the EU Cybersecurity Act) is needed to reduce the fragmentation in Europe and will bring confidence in the security of products and services. The definition and support of a federation of databases (on IoT vulnerability, incident reporting, and threat intelligence) are also needed to establish trusted and coordinated prevention and responses. To effectively combat the current cyber threat-scape, a more in-depth collaboration is required, and information sharing will be at the basis of comprehensive security analytics and applied threat intelligence. Information sharing is at the core of the NIS Directive and solutions to establish trust and confidentiality are strategic to its right implementation. Finally, the definition of a common 'controls framework' and tools for international players operating in the EU market would improve compliance to European regulations.

Impact

- Support to the EU Cybersecurity Act and the implementation of the NIS Directive
- A trustworthy and reliable supply chain
- Alignment of cybersecurity in the context of safety and security legislations
- Digital autonomy through the development of threat intelligence platforms
- A common taxonomy and regulatory framework across sectors and countries
- A faster and more efficient response due to harmonisation and simplification of regulatory requirements
- Increased trust among Member States
- Raised level of cyber resilience in Europe, enhanced business continuity of ICT systems and services

SUPPORT TO TECHNOLOGY IMPLEMENTATION

- DEPLOYING RESILIENT DIGITAL INFRASTRUCTURES IN THE FIELD
- PLATFORM FOR PRIVACY MANAGEMENT
- PLATFORM FOR IDENTITY MANAGEMENT
- ESTABLISHING AN ENGINEERING PLATFORM FOR TRUSTWORTHY HARDWARE, SOFTWARE. AND SYSTEMS

Main challenge

Europe has a long-standing tradition in research but targeted investment in digital technologies is needed and is key to introduce breakthrough innovation into the market and support the uptake and deployment across Europe of existing critical or tested innovative digital solutions. New cost-effective digital solutions should be integrated in new platforms and services to ensure the deployment of the latest cybersecurity

solutions to drive the digital transformation of the European economy and society. Resilient communication and computing infrastructures, including 5G networks and edge computing, are needed to enable the secure deployment of applications and services of strategic importance. Identity management solutions based on decentralised technologies, self-sovereign identity and blockchain, will reduce the burden for citizens, company and governments to access services, lower the administrative costs, and speed up processes. This will also reduce identity fraud and increase user convenience. To effectively empower citizens, a platform is needed to help them manage their privacy and the information they share. Information and data are at the centre of the decision process and can have crucial political, societal and economic implications. This requires specific platforms to increase the credibility and reliability of web information. Several services and platforms should be made available to the research community and industry, such as tools for secure software development and runtime checking, platforms for the development and assessment of trusted electronic technology, adaptive honeypots to collect malware samples and link them with malware intelligence services, and tools for developing forensics capabilities. Finally, the DEP provides the ideal environment to define, exercise and deploy migration strategies for quantum-resistant crypto for larger scale deployments.

Impact

- Trusted network infrastructure developed and managed by European stakeholders and strategic for the development of resilient application domain services
- Better understanding of potential vulnerabilities in 5G technologies to anticipate cross-platform attacks
- Sovereign self-identities and better privacy-preserving digital identity
- Intelligent platforms for verification and decision making
- Development of technologies with secure-by-design principles and more resilient to zero-day vulnerabilities
- Better preparedness for the advent of quantum technology and its impact
- Better situational awareness of organisations and EU citizens about the technologies they use

SUPPORT TO COMPETITIVENESS AND MARKET DEVELOPMENT

- INVESTMENTS IN EUROPE AND DEVELOPMENT OF REGIONAL ECOSYSTEM
- PLATFORMS FOR MARKET SUPPORT TO SMES
- INTERNATIONAL COOPERATION AND INVESTMENTS

Main challenge

Although Europe has a well-recognised industrial cybersecurity expertise landscape, the European cybersecurity ecosystem suffers from a twofold weakness: the strong fragmentation across the different market segments and a lack of private investment on a similar scale as exists in the US or China. In order to facilitate the emergence of pan-European players, the EU should be actively creating industry market-oriented initiatives. Through an EU-wide service programme made of four pillars, the cluster “Support to market development” is expected to play a key role in the development of the European cybersecurity businesses.

Impact

- An independent market analysis of the cybersecurity landscape to improve market knowledge for investors and providers
- Support to SMEs through a suite of customised services to increase their visibility to potential business partners and investors

- Leveraging the strength of regional ecosystems (smart specialisation) to accelerate the commercialisation of "Cybersecurity Solutions Made in Europe"
- European Investor Roadshow to strengthen the development of the cybersecurity investment ecosystem

Fostering international cooperation with strategic business partners in countries such as Japan, to initiate a long-term cooperation

SUPPORT TO COMPETENCE BUILDING

- OPERATIONAL, INTEROPERABLE AND COGNITIVE CYBER RANGES
- CITIZENS AND SOCIAL GOOD
- JOBS AND PROFESSIONAL SKILLS

Main challenge

EU policies must support the enhancement of digital competences, skills, education and awareness-raising at all ages and levels. Cyber ranges are becoming more visible and their capability to support R&D, training, testing and certification make them one of the key technological elements in cybersecurity. The use of simulation, games and virtual/augmented reality, adapted to each learning period, can also help to better understand what the risks of living in the digital world are and how to behave in it. Currently, there is a fragmentation in cybersecurity education and professional training, and there is a strong need for an aggregated European competence assessment model that is based on dynamic skills and competence building. We need to understand the demand for cybersecurity job opportunities and the motivations for involvement in cybersecurity (for women and girls in particular) and for this, a one stop shop to map competences, job profiling and job opportunities for a baseline understanding of the market would be strategic and key for addressing the skills gap.

Impact

- More cybersecure aware citizens at all ages
- EU-wide minimum curricula and common language and taxonomy of competences
- Harmonisation of job profiling (based on existing frameworks) and support to HR departments, ensuring the right people are recruited for the right jobs (more experts)
- Reducing the skills gap
- Raised situational awareness
- Fundamental (cyber)security awareness becoming a common knowledge and skill, making the EU more vigilant and resilient

Support to SMEs: ***Increased visibility of European companies and solutions in the Market Registry***

European actors appearing in the Market Radar / Registry based on a common European market-driven taxonomy to be given enhanced visibility directly supporting EU Strategic Autonomy (with the use of EU solutions) also when adopting the Cybersecurity made in Europe Label

The role of EDIHs: ***Federation of European Cybersecurity Digital Innovation Hubs***

With its local and regional approach to enable digital transformation of SMEs and public sectors, ECSO/Smart Regions Platform is developing 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 also in the frame of the Network of European Digital Innovation Hubs and the approach to federate at EU level DIH focussed on cybersecurity