EUROPEAN CYBER SECURITY ORGANISATION

POSITION PAPER

Initial position on the EU cybersecurity package

OCTOBER 2017

www.ecs-org.eu

1. DISCLAIMER

This paper is an initial ECSO position on the issues covered by the EU Cybersecurity Package published on September 13th by the European Commission.

Due to the limited time available to respond to the request from the Horizontal Working Party on Cybersecurity of the Council, only an initial internal discussion has been possible among members leading to a compilation of elements received from the members for which a Board agreement has been requested in a time delay shorter than the one foreseen in the Statutes.

ECSO and its and its Members will continue to discuss and refine its position in future versions.

We could produce further versions of this paper with evolutions in our positions after discussions with all Working Groups.

2. PREAMBLE

Since the publication of the package, we have gathered comments both from the ECSO Board and from many ECSO members to provide the Horizontal Working Party of the Council, Member States and the Commission with comments from ECSO on the proposed Joint Communication.
Due to the very wide spectrum of cybersecurity and the different interests of ECSO members it would be difficult to report all the suggestions made. For this reason, we have advised our members to report their specific comments to the European Commission through the currently running public consultation on the cybersecurity package.
Also, while there was a general consensus on the majority of topics in the Joint Communication, we must recognise that there are important differences on the issue of certification. More time is needed to reach consensus on the details. For this reason, we have opted to give general considerations in the main text and give a general understanding of the various positions / suggestions in a companion paper. Yet, we expect that the ECSO working group dedicated to this topic will soon issue suggestions for a meta-scheme that could be used in the new EU certification framework in a few weeks.
This paper presents the positions and suggestions from ECSO on the package. The structure of this position follows the structure of the proposed EU Joint Communication and its content is more of political nature than technical. A final section on “other issues” has been appended with suggestions received from ECSO members on topics that are not mentioned or not enough detailed in the Joint Communication.

TABLE OF CONTENTS

3. MAIN RECOMMENDATIONS

1. ECSO, with the support of its members, are ready to be a major instrument for the effective implementation of the EU cybersecurity strategy.

2. A stronger role of ENISA provides the possibility for increased cooperation with industry. ENISA and ECSO have complementary and mutually sustaining roles.

3. Capability building must go hand in hand with “EU level capacity building” supported by adequate public and private investments. Investments should be stepped up, converging different EU funds (possible creation of an EU Cybersecurity Fund), national funds and investments from the private sector, towards strategic objectives in a strong Public – Private Cooperation. An EU model for investments in start-ups and SMEs should be developed.

Mowing towards a Single Cybersecurity Market, ECSO supports would expect to better support the growth and competitiveness of the ICT security industry and particularly of SMEs, also with the possible creation of European champions in the domain.

4. On certification, the proposed approach is an interesting starting point but different opinions and needs exists in the different sectors. An adequate EU Certification Framework could solve the present fragmentation challenge. Time to market and certification costs are key topics but should not come at expenses of quality in security. The EU Certification Framework should create a level playing field to increase EU competitiveness retaining European achievements in this domain. The legacy national and SOGIS MRA certification schemes have been fostering the emergence of worldwide leaders in the secure silicon and secure embedded software industry. The basic national certification schemes have created an initial market for national SME’s in the Cybersecurity arena. These are key assets to the European industry and European sovereignty and a smooth transition should be available from day 1.

5. Information sharing in public-private partnerships is an essential factor in the implementation of the NIS Directive and must be strengthened through sectoral ISACs. An appropriate mechanism to share trusted information within an ISAC and between CSIRT and ISACs should be developed.

6. A rapid emergency response mechanism to cyber threats (Blueprint) is needed at local / national / European level involving the private sector. European companies can contribute with their operational competence across borders.

7. The European Cybersecurity Research and Competence Centre and the network of competence centers must be designed a tool to boost EU capability. A cooperation with ECSO based on complementarity of activities should be envisaged to take stock of our unique governance and ability to build a stakeholder community linking national public-private organisations.

8. There is an urgent need to build a strong cyber skills base and improve cyber hygiene and awareness at citizen and business level. Investments, awareness and time are needed. Implementation requires the involvement of national and regional authorities, businesses and SMEs in a collective approach, involving all the ecosystem embedded in the EU regions. Increasing

the base of potential interested students from primary and secondary level could be helped by tackling also the gender issue.

9. Deterrence is a priority for the public and the private sector. ECSO members will be encouraged to participate in the public-private partnership for fighting cybercrime (attribution, forensics …).

10. ECSO is interested in developing international cooperation on cybersecurity. Europe should promote EU best practices and solutions in Third Countries.

4. GENERAL COMMENTS ON THE CYBERSECURITY PACKAGE

Cybersecurity has grown in interest and societal / economic impact all along these years. It has become a concern for all citizens and the society as a whole.

ECSO, as a pan-European association gathering both private organisation and national public administration in the cybersecurity cPPP welcomes the proposal made by the European Commission and the objectives identified in its cybersecurity legislative package

Increase capabilities and preparedness of Member States and businesses; Improve cooperation and coordination across Member States and EU, institutions, agencies and bodies; Increase EU level capabilities to complement the action of Member States, in particular in the case of cross-border cyber crises; Increase awareness of citizens and businesses on cybersecurity issues; Strengthen trust in the digital single market and in digital innovation through increasing the overall transparency of cybersecurity assurance of ICT products and services. (as referred in the Cybersecurity Act - page 69).

The proposed cybersecurity package is a considerable improvement of the 2013 Cybersecurity Strategy and an historic step forward. In the drafting of the previous strategy, industry was called to contribute mainly on standards, awareness and information sharing.

In light of the creation of the cPPP, research and innovation aspects, in particular, have been considered, with concrete and quantified objectives.

Following a deep analysis of the Joint Communication of the European Commission, ECSO and its members reached a set of common considerations described in this document and underline the lack of attention on one of the main Commission's multiannual strategic objective(s) targeted by the proposal/initiative (also referred in the Cybersecurity Act document, page 69): *Increase the global competitiveness of the EU companies operating in the ICT field.*

Today, we recognize that some elements "*to increase the global competitiveness of EU companies operating in the ICT field*" have been proposed in the 2017 package (e.g. certification, competence growth, training …). Yet, these elements are not considered in a global vision for the effective development of the European cybersecurity market and industry.

We still lack a full European cybersecurity industrial policy and effective investments for capacity building at national and European level.

As mentioned in the Joint Communication, we need to increase investments, but not only on research and development of capabilities. We are still very far from investments made by the public and the private sector in the US or other third countries. Europe could never catch up in "competence" if its market is not supporting such development. This is not only an economic issue, but also a security issue for all European countries: we need to increase our digital autonomy, while finding ways to establish fair and trusted international cooperation.

Beyond the generic statement to “increase the global competitiveness of EU companies operating in the ICT field” there is a lack of specific objectives. What are the figures to be reached? What position for the European industry? What reduction / limitation of the impact of cyber threats? The resilience to cyber-attacks, the deterrence and the international cooperation are well defined tools, but for what concrete objectives? Without these measurable objectives it will be difficult to set appropriate measures for the European market and industry.

We need to build up a common vision in Public Private cooperation, with clearly defined objectives for the market, the users and the suppliers. We should identify the needs and the viable solutions to achieve these objectives (some of which are already identified in the proposed package).

We need to put the different elements such as standardisation, certification, investments, research & innovation, international cooperation, requirements from the different verticals, support to industry development and in particular to SMEs, link to local / regional aspects, education, training, awareness and exercises in a comprehensive European cybersecurity industrial policy geared to support the achievement of commonly agreed objectives.

We must to give ourselves the means to reach concrete objectives in a defined time scale.

The evolution of ENISA, the creation of a network of competence and of a Research and competence centre as well as possible evolutions of ECSO and the PPP, should be seen in this global context, with better defined targets for the European market and industry. This is the best way to get the full commitment of private sector stakeholders on an EU cybersecurity strategy, may they be users, suppliers or financial investors.

- ***The 2017 Cybersecurity Package is a considerable improvement of the 2013 Cybersecurity Strategy***

ECSO is pleased to see that the legislative package contains useful measures which will further contribute to improve the security in the EU and the MS and strengthen the trust of companies and citizens in the digital single market and digital society. ECSO is particularly interested in those topics dealing with build-up of pro-active resilience. A significant number of suggestions made by ECSO members have made in the last months to the Commission and Member States (e.g. education, training, awareness of citizens and decision-makers, research, the creation of sectoral ISACs, an enhanced role of ENISA, an efficient EU certification framework to reduce fragmentation and increase security as well as competitiveness of the European industry) are present.

- ***ECSO is a unique public – private construct, leveraging upon effective cooperation with National Public Administrations. ECSO objectives go beyond simple R&I, tackling all market development issues including many of those mentioned in the Joint Communication. We need to clarify the role of ECSO with respect to the proposed bodies and instruments.***

ECSO is a unique construct with a very advanced governance, beyond the present approaches in EU public private partnerships, representing in its decision-making governance and working bodies both private and public sectors, users and suppliers from all sectors. ECSO is working not only on the R&I objectives but also on the different aspects linked to market development and deployment. The contribution from public administrations in our working groups and in the NAPAC (NAtional Public Administration Committee) is a considerable added value to our work. Yet, the future role of

ECSO with respect to the evolution of ENISA, the creation of the network of competence centres, the European Cybersecurity Research and Competence (EU CRCC) and a possible Joint Undertaking (JU) is not clear. ECSO and its members could provide and added value and contribution with its/their competence and approach in the majority of areas mentioned in the Joint Communication and Cybersecurity Act.

It is also in the interest of the Commission to leverage upon the achievements of ECSO and to continue such successful engagement and cooperation with industry.

- ***ECSO, with the support of its members, can be a major instrument for the effective implementation of the EU cybersecurity strategy: we are looking forward to a constructive cooperation, starting with this dialogue with the Council.***

ECSO members are looking forward to a constructive cooperation, validating operationally the Joint Communication and the needed investments. ECSO, with the support of its members, can be a major instrument for the effective implementation of the EU cybersecurity strategy. ECSO can work hand in hand with Member States and the Commission and ENISA to provide a comprehensive coverage of the proposed issues and identify best ways forward.

5. BUILDING EU RESILIENCE TO CYBER ATTACKS

5.1 Strengthening the EU Agency for NIS (also in the “Cybersecurity Act”)

- ***ECSO members are pleased with the stronger role of ENISA and its permanent mandate. Its objectives are very ambitious.***

ECSO members are pleased with the stronger role of ENISA and its permanent mandate. Its objectives are indeed extremely ambitious (policy development, information hub, certification authority, research and innovation, operational coordination). Also with this new mandate, the role and the contribution of national Agencies will remain fundamental.

The Joint Communication provides clarity and the possibility for increased cooperation with industry, especially in sector-based activities, also in close coordination with ECSO. A stronger role for ENISA will boost the partnership with ECSO and its members focused on moving from current ideas and initiatives to concrete actions. Both ECSO and ENISA should identify collaboration areas and benefit from each other’s role.

- ***Analysing the proposed future role of ENISA (and waiting for its finalisation), we have identified a number of complementary and mutually sustaining activities between ENISA and ECSO.***

Considering the tasks proposed in the package, we could cooperate in:

- Support to “capacity building”: ISACs; observatory for implementation of the NIS directives (and other legislative measures in the different applications) – activity already envisaged in ECSO WG3

- Identify priorities and disseminate information on research & innovation – activity already ongoing in ECSO WG6

- Education, training, awareness-raising and cyber exercises – activity already ongoing in ECSO WG5 and WG3

- Analysis of relevant market trends – activity already ongoing in ECSO WG2

  Certification – Harmonisation of certification schemes towards an European cyber security certification framework – activity already ongoing in ECSO WG1 (ECSO working with experts from all sectors, public and private, analysing the current certification schemes and identifying initial challenges from the industry to propose possible solutions for harmonisation)

- Support to international cooperation - some activity initiated in ECSO WG2

Cooperation is also envisaged for better information exchange on activities and workshops.

ENISA and ECSO are complementary: a document will be issued to present where the synergies stand, avoid the impression of duplication and clarify how ECSO can support the activities of ENISA as several objectives envisaged for ENISA are closely aligned to the activities of ECSO WGs.

5.2 Towards a single cybersecurity market

- ***Supporting the industry: better support the growth and competitiveness of the ICT security industry and particularly of SMEs***

The Cybersecurity Act reaffirms the increase of the global competitiveness of EU companies operating in the ICT field as a multiannual strategic objective for Europe. To achieve this important objective, implementing actions must be geared towards better support of the growth and competitiveness of the ICT industry and particularly of SMEs (for more detailed suggestions on SMEs, please look at the specific section on “other questions”).

- ***Creation of European champions***

A major challenge for the EU cyber industry is the lack of “scale” (i.e. the lack of global cyber players): EU needs global cyber champions. The vast majority of large, global cyber vendors are non-European. This creates a strong dependency and is putting EU sovereignty, infrastructure and jobs at risk. Hereafter three suggestions to improve this situation:

- Encourage and support the creation of one or more companies of large size as called in the past the “Airbus of cybersecurity” similar to what has been recently happening in the terrestrial defense, naval and rail sector that will be able to

compete effectively on a global scale. The market structure is different here, but a consolidation around few champions could provide a wider surface and weight in the international market while allowing competition.

- Create incentives for the EU agencies and EU Member States to purchase European solutions when possible and select European suppliers if available, in particular for sensitive applications.

- Increase the level of investments in critical domains (for national security, strategic or economic point of view) such as Industrial Control System cybersecurity, IoT cybersecurity, Cyber Artificial Intelligence, etc...

- ***Creation of an EU model for investments in start-ups and SMEs. Creation of an "EU Cybersecurity Fund"***

There is a need for designing an EU model for investment for SMEs. We propose mapping the potential capital venture and funding investment in EU and creating a "Bid" and "Search" platform. Also, EU should consider investing more in dedicated EU-based Cyber funds.

When analyzing the SMEs and start-ups funding situation and history, it becomes clear that the EU has a scale problem. EU cybersecurity start-ups and SMEs face funding problems and have great difficulty in raising the necessary funds for their technological and commercial development. In particular, SMEs need capital to be invested in marketing and business development but the EU market faces a lack of private capital risk/investors in cybersecurity domain. In Europe, most of the cyber investments are happening at the angel, Serie A or Serie B stage. At later maturity stages, proven start-ups are typically either acquired or funded by US and global venture funds.

- ***Building EU level capacity together: "capability building" must go hand in hand with "capacity building" supported by adequate public and private investments*.**

A harmonised and comprehensive capacity building in Member States (not only capability building) should be developed taking stock of the traditional instruments and architectures set up by the EC to build EU capability. The Joint Communication aims to achieve a shift in paradigm for the EU from a reactive to a proactive approach. Building EU capacity is a cornerstone to achieving this result, supported by adequate public and private investments.

- ***ECSO is ready to discuss how to develop the "duty of care" principle as an extension of "security by design".***

ECSO welcomes the mention of "security by design" as one of the 3 priorities of the EU certification framework and the EU industry is looking forward to discussing with MS and EU bodies on how to develop the "duty of care" principle mentioned in the Joint Communication for the secure development of lifecycle processes. Tackling a global approach for duty of care, we should consider also the possibility for a EU legal and regulatory compliance by design.

- ***General cybersecurity strategies should be complemented by sector-specific strategies, where needed***

As identified in ECSO WGs, where different sectors have different requirements, ECSO Members agree with the Joint Communication that specific sectors should be encouraged to develop their

own approach and that the general cybersecurity strategies should be complemented by sector-specific cybersecurity strategies, considering that sectors have different awareness level of cyber security threats , thus needs, with a priority for those areas linked to the implementation of the NIS Directive, but also to strategic economic areas for Europe like Industry 4.0.

- ***Liability must be carefully investigated together with the private sector and avoid potential legislations for "class actions"***

The concept of liability and the actions envisaged at European level in this respect must be carefully investigated together with the private sector. Beyond the challenge linked to attribution, a number of ECSO members expressed the potential risk that liability issues will lead Europe to legislations allowing "class actions" at EU level as in the US, as these could have negative impact on the market without necessarily increasing the security level.

- ***Foreign Direct Investments restrictions should be carefully considered to avoid creation of potential threats for access to capital and access to global talents.***

FDI (Foreign Direct Investments) restrictions is a sensitive issue which should be carefully tackled. It could be not enforceable in practice and could bring potential dangers to access to capital (to and from Europe) and access to global talent. A reciprocal approach with Third Countries could be a viable approach.

- ***Cybersecurity and information security are important pillars of privacy protection.***

Civil society issues are included in the Joint Communication when it comes to education, training, job creation etc. (see later). It is important to recognise privacy protection as an enabling factor for the effective uptake of solutions and services. Privacy protection is very relevant issue to be addressed. We see this as twofold: on the one hand there is the data protection issue with tools and applications that are secure by design in order to protect the data. On the other hand it is to be addressed how to foster information-sharing, while preserving privacy, confidentiality and data protection. A balance has to be found to take both needs into account, and a clear set of priority criteria could be useful in this respect.

Preventing and resolving conflicts between cybersecurity and privacy protection should be an important objective, which we hope will be adequately addressed by the implementation of the new General Data Protection Regulation (GDPR) as of next year.

Future European regulations on Privacy should allow protection against undue interference with electronic communications metadata and content as well as undue interference with users' devices or with data emitted by such devices. They should include measures to protect the digital ecosystem (data and infrastructure) effectively from cyberattacks and allow the high level of protection provided by the security requirements of the GDPR. They should also provide the ability to effectively protect endpoint devices and the IoT, thus allowing new threats to emerge.

- ***Secure digital identity***

An important topic that could be also considered when building a Single Cybersecurity Market is secure digital identities. Secure digital identities are a fundamental pillar and prerequisite for the success of the digital transformation of our economy and society. Without secure identification of

individuals, institutions, servers, machines and IoT devices there will be no trustworthy E-government, E-commerce, Industry 4.0, etc. Creation of a secure digital identity would enable EU and its nation states to pick up a common pace whilst moving towards efficient governance and services provided online by both, nations and EU institutions. Digital identity that is valid and accepted EU-wide will provide EU citizens to work, do business and use services safely yet conveniently. Providing people with the opportunity to have a safe and secure identity will also eliminate a number of online threats such as identity theft etc.

5.3 EU Certification Framework

- ***The document presented by Commission is an interesting starting point but different opinions and needs exists in the different sectors (see companion document: Elements from ECSO members on the EU Cybersecurity Certification Framework) .***

The document presented by Commission is an interesting basis upon which to build and must be considered as a step forward. Yet, different opinions and needs exist in the different sectors. For instance, the voluntary approach has been criticised by a number of ECSO members, while other members have welcomed it. The opinions diverge based on the market sector addressed (for instance B2B, B2C etc.) and the type of vertical.

Since last year, ECSO has been asked by the Commission to provide suggestions for an EU Certification Framework. This work has been supported also by the valuable contribution of experts from National Public Administrations. ECSO members have experienced in WG1 (standards and certification) the challenge to provide suggestions for a common Certification Framework, when combining needs from different sectors that have different maturity levels. Having experienced these difficulties, we have started to analyse the challenges the industry is currently facing in order to derive a general approach that can be used as basis to address sector specific needs. Thus, we appreciate the proposal for the creation of a common EU Framework and the possibility to develop, where needed, sector-specific strategies and certifications (in certain cases, with more mandatory requirements to well address sector specific needs, also for increasing security by design).

- ***The Commission must face the challenge of the fragmentation: an EU Certification Framework can be a good answer***

The Commission must face the challenge of the fragmentation: a European Digital Single Market needs a homogeneous interpretation of rules, including mutual recognition between Member States under a unified umbrella to facilitate the growth of the European market.

- ***The Framework can provide a minimum common baseline (specific regulation on higher levels, where needed) assuring synergies across vertical sectors***

A European certification framework, should provide a minimum common baseline of security requirements (and for higher levels it could be subject to sector-specific regulations to mandate, where needed, security by design). The definition of this common baseline layer should need the coordination across vertical sectors while at the same time facilitate the development of synergies across vertical sectors such that security technologies can be utilised in other vertical sectors.

- ***European achievements in certification (mainly based on the SOGIS MRA, national schemes and proprietary ones – see the SOTA document) and the competitive advantages of Europe must be retained***

European achievements in ICT Security Certification and the competitive advantages for our European industry established in the last decades must be retained and seamlessly integrated into the new framework. The EU certification framework should keep a high reputation recognised on a global level.

- ***Vertical requirements should be setup based on consensual agreement between the different public and private (users & suppliers) stakeholders: industry should be an active part of the future Framework***

The sector-oriented expert groups (suppliers, laboratories, certification bodies, national security agencies, regulators …), should have a main role in defining the vertical requirements. Particularly for high assurance levels having the setup of the requirements as a consensual agreement between those expert groups and national certification bodies with the support of ENISA and ensure that the certification schemes are well adapted to the specific needs of the different verticals / critical infrastructures.

We have not clearly seen mention of the contribution from the private sector in the texts dealing with certification. We would not discuss here the governance or the process (nor the role attributed to ENISA on this topic), as this will be directly discussed among public administrations, but the private sector should be part of the future Framework, not as « ad hoc or temporary experts » and should not only be represented by users as « risk owners » but also by suppliers with their technical and market competence.

- ***Time to market and certification costs are key topics but should not come at expenses of quality in security. A level playing field should be created to increase EU competitiveness***

Time to market and certification costs are key topics for any player in the Digital Single Market. Certification procedures should be as lean and fast as possible and considering time to market as a key factor from the economic point of view when applying quality procedures. In particular, the Certification Framework should be developed to also consider the needs of SMEs which are a major actor in innovation and fast deployment: the cost models should not negatively impact SME growth.

The Joint Communication mentions that *"The Framework would lay down the procedure for the creation of EU-wide cybersecurity certification schemes, covering products, services and/or systems, which adapt the level of assurance to the use involved (be it critical infrastructures or consumer devices)."* Clarification is needed about the assessment done for the assurance level which should also cover impact on robustness, resiliency of assessed services or products. The definition and evolution of criteria assigned to assessment processes should be considered as well.

A holistic European approach for ICT Security Certification should be carefully implemented, permitting the necessary development speed and the early generation of European reference markets, thus allowing the creation of a level playing field for European industry without forcing

countries to accept the cheapest certificate available, and improve their competitive position on the world market.

- ***Trusted technical standards: to be further developed***

Additional steps will be needed in the area of trusted technical standards. EU minimum standards for IT security should be introduced to ensure a uniform "state of the art" in close collaboration with CEN/CENELEC/ETSI, to further complete the cyber security landscape. ECSO is already working in that direction and is establishing a MoU with CEN/CENELEC and ETSI.

ENISA should only reference European standards or ISO/ITU/IEEE international standards, industry standards created by industry fora or consortia should be avoided to avoid un-faire competition between large non-European companies and European SME's.

5.4 Implementing the directive on the security of the NIS in full

- ***ECSO agrees that the full implementation of the NIS Directive is essential for cyber resilience and the protection of the ICT market.***

Standardised sectoral stress tests could be defined and performed to test the efficient implementation of the NIS Directive

- ***Information sharing in public-private partnerships should be strengthened through sectoral ISACs. An appropriate mechanism to share trusted information within an ISAC and between CSIRT and ISACs should be developed.***

It is clearly agreed that the NIS directive implementation will be beneficial. A multilayer approach will have to be measured against the timeliness and effectiveness, and could be complemented with direct involvement of critical private institutions. We would welcome ENISA playing an active role in this respect, going beyond the detection and stepping into the operational response. Consistently with what has previously been suggested by ECSO, cooperation and information-sharing between the public and private sector is important: trust needs to be strengthened for public-private partnerships with the creation of sectoral ISACs. It would be beneficial to have a clearly identified hub for Cyber Security, concentrating existing competences which could leverage and cooperate with other national and sectorial CERTs/ISACs.

Yet, a key point is to build the appropriate mechanism to share trusted information within an ISAC as well as between the CSIRT network and ISACs. An analysis of currently used mechanisms in the private and public landscape can be useful to identify possible issues that limit the capacity to share strategic information about threats or security incidents. Such an analysis could be the starting point for projects aimed at overcoming any limitations and targeting the development of policies and platforms for secure information-sharing, able to protect information confidentiality (the traditional governance and use of information in ISACs – e.g. in the US – is not always a success).

- ***When securing old legacy but still operational systems new threats should be considered in the implementation of the NIS Directive***

Many large industry investments have a very long lifetime and these systems are in many cases parts of our critical infrastructure. There is the need to consider in the implementation of the NIS Directive the tackling of new threats when securing old legacy but still operational systems.

- ***Possible further developments of the NIS Directive, including other strategic sectors for the EU economy***

Possible further developments of the NIS Directive could be examined in close exchange with industry (machinery in factories is one of the suggested priorities for the Certification Framework and the driving factor of the Industry 4.0 approach, but it is not addressed by the NIS Directive, despite manufacturing being a strategic sector for the EU economy).

Another aspect is that the current NIS do only cover the security of the IT systems of Critical Infra operators, i.e. the elements in the "logical" cyberspace inside computer memory, processors and I/O. With the introduction of IoT and cyber-physical issues into critical sectors such as transport, health and utilities the need for security measures for IoT and the cyber-physical dimension become evident.

5.5 Resilience through rapid emergency response

- ***Rapid emergency response to cyber threats is needed at local / national / European level: what involvement of the private sector?***

We understand that the "Blueprint" approach to provide an effective process for an operational response at EU and MS level to a large-scale incident is dedicated to public administrations. Yet, the private sector is also highly interested and could provide a valuable contribution.

Beside and beyond the sectorial needs and the involvement of several authorities and entities a further effort should be undertaken to ensure also the direct involvement of Private Institutions, especially those representing the Operators of Essential Services, in case of a large scale crisis. A wider involvement is needed starting with the tools and means for information sharing and, even more, defining the processes and workflows for operational decision making and crisis management at European level, both within the industry, but also across-sectors. Indeed some sectors are transversal such as the Banking Union, the energy, the transports.

- ***Measures for an operational approach to threat detection and response could possibly also include the private sector: it can provide valuable information on threats and/or provide support in detection and response to threats.***

We recognise that some parts of the Joint Communication promote the suggested approach for covering not only prevention and protection but also detection and response, but measures for a more operational threat detection and response approach seems to still be limited (maybe due to

sovereignty issues). Attack detection should result in actionable evidence for planning and carrying out appropriate response operations.

The economic sector (users & operators but also suppliers) has a vested interest in following and possibly participating in a rapid response mechanism, both at national and at European level. They are directly connected with CERTs and can provide valuable information on threats (users) or can provide support in detection and response to threats (cybersecurity service providers). Considering the present level of emergency the private sector cannot wait for 2020 for having the CERT relationship established.

The Joint Communication proposes to mainstream cyber incidents within the EU crisis management mechanisms. While understanding the need for a collective response and solidarity in case of an attack, it would be necessary to better understand how this could be applied as cyber threats usually propagates across countries, unlike forest fires, earthquakes or flooding (usually tackled by the EU crisis management mechanisms). Tools used in national emergencies could be only partially shared in case of a local need.

- ***Many EU companies working in different MS have direct competence on cross-border operational approaches and legislative issues***

Many EU companies working in different Member States have direct competence on multinational operational approaches and legislative issues linked to prevention, detection and possibly response to cyber threats. Their expertise could be useful in the definition, implementation and operation of a European rapid emergency mechanism.

5.6 A Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre (EU CRCC)

- ***Stepping up investments converging different EU funds, national funds and investments from the private sector, towards strategic objectives in a strong Public – Private Cooperation.***

The Joint Communication recognises the importance of scaling up investments (examples given as a comparison: the US) but there is no mention on how to increase investments beyond the suggested activities to “develop capabilities” (i.e. how to effectively increase and harmonise capacity building at Member State and EU level?). We should scale up investments converging different EU funds, national funds and investments from the private sector towards strategic objectives in a strong Public – Private Cooperation. Yet, for the moment the amount of needed / expected investments linked to this Joint Communication is not given.

- ***The EU CRCC could be a tool to boost EU capability: possible cooperation with ECSO to take stock of our unique governance and ability to build a stakeholder community linking national public-private organisations. ECSO cooperation for the EC impact assessment to examine available options for a future structure***

The creation of a dedicated structure, for instance a JU, as umbrella for the EU CRCC and the network of competence should be carefully examined. First, a JU is foreseen under the Lisbon Treaty as an instrument to support Research and Innovation (with "some links" to business), while one of the objectives should also be the market development and effective deployment and use. Second, looking at the governance of existing JUs, there are some doubts about the capability to host and coordinate the huge quantity and variety of stakeholders in Europe. For this reason, a cooperation with ECSO should be envisaged for the EC impact assessment to examine available options for a future structure to take stock of our unique governance and ability to build a stakeholder community linking national public-private organisations. Also, it is already ECSO's ambition to tackle issues linked to the cybersecurity industrial policy and market development / deployment and ECSO could therefore be the natural extension of the Centre towards more business approaches and interests.

- ***ECSO has similar or complementary targets to the EU CRCC: a structured dialogue between the Commission, MS and ECSO to envisage the best way to find synergies in the complementarity between the EU CRCC and ECSO should be established***

ECSO activities, with its support to the PPP, are already focused on gathering input from various stakeholders to understand the readiness and innovation of key digital technologies that have a cybersecurity scope, with similar or complementary targets to the EU CRCC (real or perception of duplications should be avoided, similarly for the mentioned links with ENISA):

- Contribute to the creation and development of an EU cybersecurity certification framework of products, services and systems (ECSO WG1);
- Supporting R&I (ECSO WG6),
- Boosting innovation and competitiveness of the EU industry (ECSO WG2, WG3 and WG4),
- Supporting high end skills development (ECSO WG5)

- ***The proposed EU competence network can also help Europe to develop a European digital sovereignty.***

Cybersecurity Research & Competence Centres have already started in many EU countries: the proposed EU network will accelerate such dynamics. This network can help Europe with the definition and development of approaches for increased European digital sovereignty developing a European industrial base for key technology capabilities.

- ***The Cybersecurity competence network should be based on excellence of cybersecurity centres in the EU combining research, education / training and business.***

The responsibilities and structure of the new Centre should be further defined. A dialogue between the Commission, MS and ECSO is needed to envisage the best way forward to find synergies in the complementarity between the EU CRCC and ECSO if the PPP evolves into a JU (or another instrument) and to define the role of ECSO in the evolving EU environment. ECSO's ambition is not to manage R&I but to contribute to the public – private dialogue for definition of priorities and

to support market implementation of innovation. For this, ECSO could be regarded as a primary advisory body to this Centre.

Also, RTO members of ECSO would like to understand if this Centre will be a partner or a competitor in future R&I programmes. The relationship between ENISA and this Centre should also be clarified to avoid the impression of overlapping responsibilities with the new ENISA mandate.

Similarly, more clear statements on the network of excellence and its link to this Centre are needed. There are many existing cybersecurity centres in Member States but they vary widely in purpose, activities, funding and partners. More clarity would be needed on how the selection & governance of this network is envisioned – also to ensure that societal benefit is safeguarded.

- ***Multi-national technical exercises supported by the Network***

Collective security will be dependent on individual state-level security and resilience. For that reason it would be very important to set up a platform (maybe based upon the network of cyber competence centres also with a link to the ENISA mandate) to provide Member States with the opportunity to conduct multi-national technical exercises, with the support of EU Industry. Competence centres should also be able to provide technical exercises, workshops and even essential cyber hygiene trainings for enterprises, NGO's, students and communities. In conclusion, these competence centres would not be merely aimed to serve governments and CNI-providers, but they would also support EU-s cyber security by educating people and smaller companies.

- ***Development of a network of national public private organisation***

There is a very large stakeholder base in Europe: the most recent study has identified about 60.000 suppliers of cybersecurity technologies, products or solutions. These stakeholders should also be supported, but a unique central node in Brussels or somewhere else in Europe would not be sufficient. The network of competence centres could be the basis for the development of a network of national public private organisations (also linked to ECSO) to provide a harmonised market development in Europe.

- ***Cyber defence: too early to make comments***

It is too early for ECSO and its members to express comments on the second phase of the Joint Communication and of the EU CRCC, moving towards cyber defence, but of course members would be interested in the development of dual use competences as they are already active in that domain with many of them favourable to the creation of a European Defence and the use of the European Defence Fund. The cyber defence dimension of the CRCC is something that needs to be carefully considered. It can be politically challenging for some organisations and nations to be part of such endeavour (if it relates to military capabilities).

5.7 Building a strong EU cyber skills base / Promoting cyber hygiene and awareness

- ***There is an urgent need to build a strong cyber skills base and improve cyber hygiene and awareness at citizen and business level. Investments, awareness and time are needed.***

ECSO members are pleased to see that the EU Joint Communication recognises the urgent need, also stressed in the last year by ECSO WG5, to build a strong cyber skills base and to improve cyber hygiene and awareness at citizen and business level. The approach tackles all the main issues but it should be further detailed.

While the malware threat is a very important and acute one, it's certainly not the only threat to guard against. Therefore, the EU should better develop a single portal to bring together all tools in a one-stop-shop offering advice to users on securing their systems, networks, and data.

- ***Implementation requires the involvement of national and regional authorities, businesses and SMEs in a collective approach, involving all the ecosystem embedded in the EU territories.***

We consider that developing collaboration between European regional ecosystems is key to develop a European cybersecurity value chain. We welcome the creation of a cybersecurity competence network and consider that this network should be based on excellence cybersecurity centers already existing in the EU combining research, training and business.

ECSO has identified more than 10 regions and local authorities (i.e. Brittany and West Finland) that have already developed a wide range of activities contributing to develop cybersecurity in the EU level such as R&D, skills and SME support - activities often supported by ERDF and Smart Specialisation Strategies. Moreover local and regional authorities are in charge of establishing innovative ecosystems combining the triple helix of knowledge (university-industry-government) but also education and training.

- ***The EU public and private sector already suffer from a lack of experts in this domain.***

The issue concerning education is and will remain a national level competence, but harmonisation and share of best practices at European level could allow a faster and higher quality response to this market need.

ECSO members (and not only) both from public and private sectors are missing technical experts and as such they cannot satisfy market requirements and business growth.

- ***Challenge not only on needed investments for education and training but also on lack of time to train high level instructors to cover the identified needs by 2022. Envisage creation of possible EU-certified curriculum for high-schools and professionals.***

Analysing the figures given in the Joint Communication (need of 350.000 cybersecurity experts for the private sector by 2022 in Europe), we have seen that the challenge is not only linked to the

needed investments for education and training. The main issue seems to be the lack of time to train high level instructors (even considering that only 20% of experts need such high expertise) to cover the needs by 2022. The creation of a possible EU-certified curriculum for high-schools and professionals should be envisaged.

ECSO has started an initiative ("EHR4-CYBER") in its WG5 as a potential framework to contribute to solving the skills shortage in cybersecurity by sharing best practices and possibly converging existing activities among ECSO members. This initiative could reinforce what is proposed in the Joint Communication (also in cooperation with the EU CRCC and ENISA).

- ***Increase the base of potential interested students from primary and secondary level tackling also the gender issue.***

What is also very important to increase the base of potentially interested students from primary and secondary level is the gender issue: there are still too few women interested in cybersecurity, despite the huge employment potential.

6. CREATING EFFECTIVE EU CYBER DETERRENCE

- ***Deterrence is a priority for the public and the private sector.***

Although Deterrence is not currently a priority for ECSO (not enough resources), it is a priority for a number of ECSO members.

- ***ECSO members will be encouraged to participate in the public-private partnership for fighting cybercrime (attribution, forensics …).***

The public-private partnership for fighting cybercrime called for in the Joint Communication foresees information-sharing between private undertakings including personal data in full respect of the GDPR.

ECSO members will be encouraged to participate in this public private sharing of information, also contributing to Europol on cyber forensics and monitoring of the darknet. The emergence of European champions in cybersecurity technology and services able to react to incidents will improve the efficiency of this public – private cooperation in Europe.

- ***The private sector is also interested in the envisaged creation by 2018 of a cyber defence training and education platform.***

The private sector is also interested in the foreseen action of building cybersecurity deterrence through the MS's defence capability with the envisaged creation by 2018 of a cyber defence training and education platform to address skill gaps in cyber defence.

- ***ECSO members could be particularly interested in driving up the uptake of IPv6.***

ECSO members could be particularly interested in the envisaged action concerning the introduction of requirements on IPv6 in EU procurement, research and project funding to drive up the uptake of IPv6.

7. STRENGHTENING INTERNATIONAL COOPERATION ON CYBERSECURITY

- ***ECSO is interested in developing international cooperation on cybersecurity.***

ECSO is interested in developing international cooperation on cybersecurity (activity foreseen in ECSO WG2). In particular, ECSO considers it important to look in more detail at strategies and the operational actions of 3rd countries such as the US, China, Israel, Asia, India, Japan in this domain.

- ***Promote EU best practices and solutions in Third Countries.***

Coordination with EU bodies will be welcome, in particular to promote EU best practices and solutions in 3rd countries.

Industry will closely follow the proposal made in the Joint Communication looking to modernise EU export controls – including the introduction of controls on the export on critical cyber-surveillance technologies.

- ***Modernise EU export controls and the evolution of the EU-NATO cooperation.***

Industry will also follow closely the evolution of the EU-NATO cooperation, for enhanced interoperability of cybersecurity standards and other cooperation in the frame of the EU approach to cyber defence.

8. OTHER ISSUES

(Suggestions received from ECSO members on topics that are not mentioned or not enough detailed in the package).

8.1 IoT security

IoT verticals are likely to expand in Europe. The number of connected devices is constantly increasing, due to the digitalization of components, systems and solutions, and an enhanced connectivity. This trend creates new opportunities for cyber offenders, especially because IoT devices are often not as well protected as traditional devices.

European security standards across different IoT verticals can reduce development effort, time and budget for all industry participants in the value chain of connected products. Certified secure anchor from the European smart security industry are available in scalable dimensions and are used today in many verticals, such as finance, transport, healthcare, energy sectors and automatic border control systems. Many devices like Mobile Phones, PCs, Tablets, Gateways, Connector, On-Board-Units, Pay-TV Decoder, and so on, use smart card security technologies, as well as embedded security. There is a need for consistency among standards and certification schemes.

As one main area of concern is the billions of unmanaged, low security IoT devices that will be connected over the network. “Ordinary” “internet for People” (IoP) devices have a screen and a UI and behind it a human being that provides at least some form of device management to her/his tablet/smartphone/PC/smartTV etc. by at least turning off and disconnecting the device if it begins to misbehave. With IoT and devices that is likely to be unmanaged and operational for a decade, this poses a tremendous threat – not to the device in itself necessarily but such fleets of IoT devices can be hijacked into botnets and cause damage to others.

Therefore, some form of minimum security level through IDAM (Identity & Access Management), patching and device management is likely to be necessary. In his case, certification against such standards is a key method to provide a higher level of security. The best certification method is still under discussion. Could be conformance declaration, voluntary or mandated or possibly through 3rd party certification and type approval, but higher emphasis should be given to IoT security in a text on certification.

8.2 SME related issues

Despite the overall strategy says that public-private partnership is fundamental to improve cyber resilience, **we miss in the text of the package a strong direct support to build the growth of a European competitive industry in the field of cybersecurity and in particular the support to SMEs.**

Cybersecurity technology is changing rapidly and only the SMEs, due to their agility, can provide the cutting-edge solutions needed to remain competitive. While the US has the largest domestic market, specific regulatory framework (e.g. the Small Business Act) and Silicon Valley ecosystem, Israel has a strong military-academic-industry partnership and China has a protectionism strategy, EU is still looking for an appropriate business models on SMEs.

Boost the demand for SMEs solution

Without a structured demand, SMEs and start-ups cannot grow at rapid pace. The most recent analysis do the EU market highlighted the fragmentation of the market (60000 companies, 98% of them are SMEs and startups). Here, the need is for more clarity on client demand in order to better address the market (specific business plan, prioritization).

- **European cyber security SMEs HUB to help SMEs consolidation**

We recommend the establishment of European cyber security SMEs HUB as platform that allows small companies first to get to know each other, and then to develop integrated solution and harmonize offering to get access to digital EU market. Government procurement at national level

is an opportunity for EU SMEs. However, cybersecurity is often only a part of a larger public tender, making difficult for SMEs to apply. In fact, SMEs with innovative and potentially disruptive technologies are not well equipped to work with major infrastructure service providers, large enterprise clients and on large government contracts. In this context, a HUB could facilitate the participation of SMEs to tender because structured cooperation among SMEs can drive wider SMEs engagement in the market (also abroad EU), reduce transition costs and the fragmentation of the offer, and finally support integrated offer in wider bids- in particular for public procurement. A concrete solution to be developed by such HUB could be the proposal of an EU harmonized form for SMEs that wish to apply for public procurement in different countries.

- **Create a "Made in the EU - EU trusted solution" label.**

We must create incentives for large companies to buy from European SMEs. The "Made in the EU - EU trusted solution" label is an option to be investigated to facilitate private procurements oriented towards European SMEs. This label could be a main differentiator stressing European qualities like data protection and high security standards. It should be seen more as a marketing tool to promote the European cybersecurity offerings on export market by increasing the visibility of SMEs.

- **Foster clusters cooperation**

We suggest the establishment of European network of clusters specialised in supporting SMEs, market and investments in cybersecurity. SMEs face limited export capability: many SMEs lack the knowledge of international markets they need to operate effectively overseas or even within the EU.

EU Funding for R&I&D of solutions that effectively reach the market

- **Requirements for minimum participation of SMEs in H2020 projects**

Estimation of SMEs participation and funding in FP7 and H2020 in this sector is of the order of 14 – 17%[1].This amount is too low comparing to the strategic place of SMEs in developing cutting-edge solutions. In establishing the cybersecurity cPPP, we set as a target that at least 20% of the participants of the H2020 calls to be funded should be SMEs, start-ups or high growth companies (50+% increase in annual revenue). The requirement of 20% is envisaged also to be adopted as a Key Performance Indicator for the cPPP monitoring that will be prepared by ECSO on yearly basis.

- **Adoption of cascading funding mechanisms in H2020 calls on cybersecurity**

According to the data collected by one of our members, the cascade funding model is going to be present in almost all the other areas of the LEIT ICT WP for 2018-2020. However, it is not present in cybersecurity domain. ECSO thinks that this should be adopted also for cybersecurity projects as it has proven to be a very efficient mechanism for supporting companies, in particular SMEs, in the adoption of new technologies. Moreover, consortium building funds should be available not only in reimbursement format but as a direct financing tool (e.g. Katana projects).

[1] ECSO Industrial Proposal 2016.

- **Review and simplify the SME Instrument**

Due to the high level of complexity for applying and administrative burden for SMEs, the current amount of money and the timeline are inadequate for SMEs looking to quick go to the market. Instead of providing 1.5M€ funding, we think it could be more appropriate having many small projects of 50K€ to 500k€ funding at the early phases.

- **EU investments vs foreign acquisitions**

EU cybersecurity start-ups and SMEs face funding problems and have great difficulty in raising the necessary funds for their technological and commercial development. Several innovative companies were acquired by foreign companies, such as Stonesoft (FI) acquired by McAfee, Secusmart (DE) acquired by Blackberry or Anubis Networks (PT) bought by BitSight. In particular, SMEs need capital to be invested in marketing and business development, but the EU market faces a lack of private capital risk/investors in cybersecurity domain. ECSO will establish contact with VCs and corporate investors in EU interesting in investing in EU.

ECS
EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

10, RUE MONTOYER - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE: WWW.ECS-ORG.EU - TWITTER: ECSO_EU