Informal Exchange of views with Deputy Director of DG CNECT, K. Rouhana and Director and Director for Digital Society, Trust and Cybersecurity at DG CNECT, Mrs. Despina Spanou

Executive summary

Deputy Director of DG CNECT, K. Rouhana and Director and Director for Digital Society, Trust and Cybersecurity at DG CNECT, Mrs. Despina Spanou were invited by the ECSO secretariat to have an informal exchange of views with members of the Board of Directors.

This informal exchange comes at a timely moment. As announced in its Joint Communication of 13 September 2017, the European Commission (EC) recently published a call for proposal on the set up of a European Network of Competence Centres and a Cybersecurity Research and Competence Centre. It is also currently designing internally the new Multi-Annual Financial Framework where cybersecurity will be an important priority area in terms of future investments.

K. Rouhana thanked the Chairman of the Board of Directors for the invitation to speak and have an exchange of views with the ECSO Board of Directors. He underlined the importance of ECSO and of this partnership which will run until the end of 2020. ECSO's support and involvement in actions designed together with the EC is significant, he said. Since the publication of the cybersecurity legislative pack in September last year, ECSO's views and considerations, together with the Council, the European Parliament, ENISA and other stakeholders, have been important to ensure a satisfactory level of understanding of the work, ambitions and endeavours of the EC and that any changes would be done in a well-informed way.

THE CYBERSECURITY ACT is progressing. The EC is hoping to have a text that is suitable for the industry and gather a large consensus around it including from Member States (MS) and the European Parliament.

THE CALL FOR PILOT PROJECTS to set-up the Network of Competence Centres and the Cybersecurity Research and Competence Centre.

The EC has amended its work programme in the ICT LEIT for 2018 to make sure to set this actions in motion with the EUR 50 million fund made available as it was promised in the strategy.

This action addresses the large fragmentation across Member States (MS) in R&I with substantial number of academic teams (around 600 teams across the EU) working, mostly, in isolation on cybersecurity across Europe. This means that a lot of effort is put in Europe by MS in this field in terms of resources, but it is not reflected in the output in terms of cited publications and patterns and products and services and exports by industry in general. This is a phenomenon that also occurs in other areas where in Europe the effort is dispersed. This fragmentation should be addressed by creating a common agenda, share facilities and human resources.
Moreover, the research done, very often, is to maintain the knowledge at the state of the art and it is not sufficient in terms of critical mass. We would like these research centres to be in the lead and come up with breakthroughs that could bring a competitive advantage for the industry to exploit. This is the reason why we put this proposal on the table.
The question is: how to consolidate and aggregate this research around common agendas that are in line with the industry expectation and at the same time boosts industry / academia collaboration across Europe and avoid creating islands of academic research. This boost could be done by

aggregating more the research effort across Europe working with industry, national authorities with the agencies to make sure we get the maximum out of our effort. This is the proposal for the pilot phase, but it is also a way to get lessons learnt to be feed into our next Financial Framework.

The text of the call explicitly ensures **industry participation and involvement in this action** to maximise the **industry / academia collaboration** and further consolidate our effort in this field. The objective of this call is not to replace the supply industry with competence centres but to make sure that the entire supply chain is represented. **It is a way of connecting the suppliers with their clients**. **The supplier industry in cybersecurity in Europe is essential. It is a "must have"**. The support to the supplier industry is essential for us and dependency in this area to technologies from outside Europe is more than dangerous.
The key part of the work expected from these pilots is about how to ensure collaboration of R&I and industry. We need the academia, the supply industry and the users to be systematically part of each project.

The intention is to give a boost to the ECSO agenda and not deviate from the Strategic Research and Innovation Agenda (SRIA) proposed by the partnership. The text of the call clearly refers to the ECSO SRIA as the starting ground. Our action is to support this agenda.

We have put indications of a timeline to make sure we don't receive proposals of 18 months but longer. The pilots will test how the governance of the network could work and all the lessons we learn from now until 2020 will feed into the work programme in 2021 and adjustments will be made every year. The set-up of the governance of the centre is a process which will not stop in 2021. We are not fixing the structure and it is not our plan. The role of the competence centre for us is to help us in the coordination, it has an implementation role. The centre will be our support and implementation mechanism for R&I in FP9 and it will also help us with the support of the coordination of the academic effort and industry / academia collaboration in the future.
The evaluation of the proposal will be done independently. Every word of the text call counts especially in the text of this call.

THE MULTI-ANNUAL FINANCIAL FRAMEWORK (MFF)

We are ambitious in terms of cybersecurity. We would like to continue investing in R&I in partnership with industry, national authorities, the MS and the academic community to keep part of our proposal for FP9 cybersecurity. But **we would also like to see whether we could co-invest with the MS in a roll out of technologies and deployment of cybersecurity solutions starting with the areas of public interest where there is legitimacy for public intervention. Also, to make sure that the latest technologies are available for businesses and SMEs across the Union**.
We do a bit of the roll out and uptake of technologies through the CEF Programme today, but this is a bit embryonic and the budgets that we have today are limited to draw MS attention and investments by the private sector. We are looking at how to reinforce that part.
Our presence in FP9 and the roll out of technologies, these are the big areas of investments in cybersecurity in the future and in both we need your help to make sure we are going into the right direction and make sure we are focusing on the right priorities.
We must make sure that Europe is in the lead in the supply of these technologies and solutions to shield our society and economy. Dependency on technology coming from outside of Europe is very risky and we know this. Our ambition is to shield our society and our economy also through strategic

investment related to defence and security. This is how we see our investment in the future. The partnership that we have together is an essential part of all our mechanisms in support to this field.
There are 5 major areas that are developing today and that need to be addressed. These are: **Cybersecurity**, **Artificial Intelligence**, (the EC will announce on 25 April a strategy in this field), **Computing infrastructure and data** (High Performance Computing), **next generation internet** (what are the connectivity needs of the future), **key technologies for microelectronics / alternative electronics**. These are interlinked between them. This is part of the thinking that we must do together and how these partnerships in the future should develop so that we don't create silos. This is part of our overall governance. **For all these big areas, investment is focusing on R&I and roll out of technologies** as well as their use by the public sector to start with and by the private sector accompanying companies in their digital transformation.

ON THE PARTNERSHIP WITH ECSO AND THE FUTURE AMBITIONS

ECSO is our privileged partner today for the discussion on future investments on R&I and we want to enlarge this discussion to strategic infrastructures key capacities. We would like ECSO to be our key partner in these discussions. This is a unique partnership in which we have national authorities and industry together and we want this partnership to be carried out with us in the future.

Partnership is a key part of our approach in R&I and in our policy. Working together with MS and industry is important and we need to make sure that the partnerships that we have help us align our strategies across Europe. ECSO is an essential vehicle for that.

Our intentions between now and 2020 are clear and the role of ECSO in this call is important for us. For the future, we are looking at different options on how to improve the PPP. Partnerships will remain a key part of our approach in the future. One way forward would be to continue the cPPPs another would be to transform them partnership into Joint Undertakings (JU) like body with a governance structure. We have possibilities that are offered to us to strengthen further our partnership and make it fit for our purpose and so we need to look at the best way to continue this partnership that we have.

Nothing is set in stone for the moment. The EC will not propose a type of partnership for the different areas and Framework of R&I or for the other frameworks at this stage. We are looking at implementation mechanisms that are flexible enough to make sure that we implement what we want in the future. Part of the options that we are looking at is a partnership for cybersecurity that would enable us to do procurement, if need be, of joint capacities with MS to reinforce our cybersecurity capacity. We see there a key role for industry and for ECSO. Also, we want that structure for implementation to help us support the coordination that we have started on research across Europe using the agendas that have established together to reinforce collaboration and aggregation. In terms of the implementation we would like a partnership that would enable us to do all this. We see the clear role of ECSO continuing within this structure and reinforcing it.

We need investments in Europe. We have the strength to do it because we have a large demand which unfortunately is fragmented and is below critical mass. This makes it difficult for SMEs to operate and grow in such a market. It is also very difficult to attract investors in this market and shield ourselves from foreign direct investment.

On the support of the innovation ecosystem we are working together in this partnership and **the role of SMEs is essential** in this. We have designed specific measures for SMEs in our framework Programme, we have developed digital innovation hubs to bring the technologies toward SMEs but we have also put on the table access to finance with a scheme for SMEs of EUR 8 billion.

It is difficult to find the investors who know about this sector, so we are working together with the European Investment Bank to create a critical mass of financial investors, venture capitals, business angels including banks for loans to make sure that we have these specialised investors that can invest in technologies. We have also discovered that in the public intervention on investment, Europe misses today the endowment funds (intermediate layer). Governments have replaced this with government intermediary layers such as the European Investment Bank. These government funds invest today only in early stage of growth of company and often drop when it comes to scaling up. We are looking into this issue and try to set-up investments at all stage of development. **This is where ECSO could help, by linking SMEs to the investing actors to get references**.

It is important that ECSO does not lose focus of the priorities in the next couple of years. The work done here will allow us to build the future. What will be done in 2018 and 2019 is fundamental, **we need ECSO to build the basis of future action** as all of them has been designed in the framework of a larger scale. For us cybersecurity is one policy including a regulatory part and an investment part which goes hand in hand. **Your views are extremely important on all the policy aspects not only as far as our partnership on R&I but also on the investment aspects**.