EUROPEAN
COMMISSION

Brussels, 5.7.2016
SWD(2016) 215 final

COMMISSION STAFF WORKING DOCUMENT

Report on the public consultation and other consultation activities of the European Commission for the preparation of the EU Cybersecurity contractual Public-Private Partnership and Accompanying Measures

Accompanying the document

Commission Decision

on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation

{C(2016) 4400 final}
{SWD(2016) 210 final}
{SWD(2016) 216 final}

1. INTRODUCTION

On 6 May 2015, the European Commission adopted the Digital Single Market (DSM) Strategy, which announced establishing a Public-Private Partnership (PPP) on cybersecurity in the area of technologies and solutions for online network security in the course of 2016.

The Commission has consulted stakeholders on the areas of work of the future cybersecurity contractual public-private partnership and also called for contributions on potential additional policy measures that could stimulate cybersecurity industry in the European Union. The Commission launched an online public consultation on 18 December 2015 for 12 weeks to seek views on the forthcoming cybersecurity cPPP. The consultation collected the views and expectations of enterprises, public organisations and citizens with respect to innovation in cybersecurity and the functioning of the European single market in the field of cybersecurity products and services. It was accompanied by a Better Regulation roadmap for a public-private partnership on cybersecurity.

With respect to cybersecurity standardisation, this public consultation complemented the public consultation on the development of the Priority ICT Standards Plan: "Standards in the Digital Single Market: setting priorities and ensuring delivery", in which cybersecurity was one of the areas covered. This resulted in the recently adopted Communication: ICT Standardisation Priorities for the Digital Single Market[1], part of the broader Digitising European Industry[2] package adopted on 19 April 2016.

In addition, the Commission and the European Union Network and Information Security Agency (ENISA) organised various workshops with stakeholders. The public consultation, the aforementioned events, the work of the Network and Information Security (NIS) Platform and the report of the European cybersecurity industrial leaders underpin the preparation of the cybersecurity cPPP and its accompanying measures.

2. ENGAGEMENT WITH EXTERNAL STAKEHOLDERS AND WORKSHOPS

2.1 European Network and Information Security (NIS) Platform

A cybersecurity strategic research agenda (SRA) has been developed by the Working Group 3 (WG3) on Secure ICT Research and Innovation under the European Network and Information Security Platform (NISP). This public/private cooperation supported by the European Commission was established to facilitate the implementation of the forthcoming NIS Directive. This SRA complements and reinforces the EU Cybersecurity Strategy[3], and provides input to cybersecurity research & innovation at national and European levels, including to the Horizon2020 programme. Over 200 organisations (mostly academia, research institutes and industry) contributed to this effort.

[1] COM(2016) 176 final
[2] COM(2016) 180 final
[3] JOIN(2013) 1 final

From the work of the NIS Platform WG3, research priorities emerged as follows: Fostering assurance; Focussing on data; Enabling secure execution; Preserving privacy; Increasing trust; Managing cyber risks; Protecting ICT infrastructures and Achieving user-centricity.

The needs of end users were well covered in the different layers of the SRA. These are: the individual layer, comprising consumers and society at large; the collective layer, where societal principles must be respected by all kinds of organisations and guaranteed by various European security actors; and the infrastructure layer, which aims at ensuring the protection of our critical infrastructures by several different agents.

The SRA of the NIS Platform served as an important input for cybersecurity industry to further develop the strategic research and innovation agenda required for the establishment of the contractual Public Private Partnership on cybersecurity.

2.2 Cybersecurity cPPP Preparatory Workshop, Brussels, 20 January 2016

The European Commission organised on 20 January 2016 in Brussels a preparatory workshop for cybersecurity contractual Public Private Partnership (cPPP) aiming at:

- Creating a platform for Member States and the industry to discuss the next steps in the cPPP formation process(as this partnership touches on national security issues, Member States have been much more involved in its creation process than it was the case of other, existing cPPPs):
- Informing the Member States and industry sector representatives about the prerequisites needed to conclude a cPPP, as well as discuss other possible policy measures to support European cybersecurity industry;
- Reaching an understanding among participants on key questions such as:
    - Desired structure and governance model of cPPP as well as Member States' role in this structure;
    - Membership criteria for the industry representatives in the legal entity with which the European Commission will conclude a contract for the establishment of the cPPP;
    - Desired degree of involvement of Member States in the process of creation of the legal entity and the development of the industry proposal.
- Understanding key requirements for the industry to:
    - Set up a legal entity ensuring their collective representation for the cPPP,
    - Develop an industry proposal for cPPP as required by the Horizon2020 Regulation.

The workshop included 25 national administration representatives (one per Member State), 21 national industry representatives (one per Member State), representatives of European Associations with a key stake in cybersecurity, various European Commission services, European External Action Service, European Defence Agency and ENISA.

The European Commission presented key policy assumptions behind the cybersecurity cPPP. Participants could discuss elements that are currently functioning well in cybersecurity

market, barriers to increase trust/cooperation that would allow to come up with replicable solutions allowing companies to achieve economies of scales across markets/borders, as well as possible actions to overcome aforementioned barriers.

The workshop also presented key instruments that can be used within cPPP according to Horizon2020 rules. It also provided participants with initial guidance on what type of activities could potentially be covered by the cPPP and which would need to fall under additional supporting actions. Participants were also made aware that some work, on which they can build further, had already been conducted, including: Strategic Research Agenda developed by the Network and Information Security Platform Working Group 3 that could be further streamlined for the needs of the cPPP; Flagship proposal of the European Organisation of Security; existing templates and base case examples from other cPPPs.

The European Commission strongly emphasized its neutrality in relation to the work done so far and made it clear that it was up to the industry to come up with its proposal, either building on the existing materials or starting from scratch. The participants were then invited to discuss among themselves the next steps related to different work streams reflecting the deliverables needed to conclude the cPPP. Based on the discussions the participants prepared a cPPP timeline with industry's own milestones and actions that need to be completed in order to come up with required deliverables on time.

2.3 The European Cybersecurity Industry Leaders Workgroup

Leading European industry players in the field of cybersecurity decided to establish a workgroup in 2015. This group worked on a set of concrete recommendations on cybersecurity for European citizens and businesses and cybersecurity industrial policy, for consideration by the European Commission.

The workgroup was composed of Airbus Group, Atos, BBVA, BMW, Cybernetica, Deutsche Telekom, Ericsson, F-Secure, Infineon and Thales.

The group presented a report to Commissioner Oettinger in January 2016 at the occasion of the International Forum on Cybersecurity in Lille. The report highlights recommendations for measures to make the EU more trustworthy and digitally secure. The report also recommends successful development of European cybersecurity champions.

2.4 ENISA Workshops and Experts meetings

ENISA organised a series of workshop and experts' group meeting in order to gather evidence and hear stakeholders on aspects related to the cybersecurity cPPP and/or specific industrial measures envisaged in the roadmap. In particular:

- Expert group meeting on aligning research programme with policy in the specialized area of NIS: the objective was to review findings from Trust & Security R&I projects, funded under the 7th Framework and Competitiveness and Innovation Programmes, and identify success stories and key research outcome that could be mainstreamed in cybersecurity industrial products and services.

- Expert group meeting on standardisation: this aimed at building on the ENISA report on cybersecurity standardisation (2015). The gaps firstly identified in 2015 were further analysed and prioritized, providing also the rationale of the choice made. A mapping of the gaps into the proposals of subjects of possible standards was considered, within the areas such as information sharing, general processes, sector-oriented standards (including energy, aviation), and technical standards.

- Workshop with Member States on IT security product certification: the goal was to bringing together institutional stakeholders from the ICT security certification ecosystem, including national security agencies, certification authorities, representatives of the SOG-IS Mutual Recognition Agreement and Common Criteria schemes and discuss achievements and current limits of the existing certification schemes and possible way forward.

- Workshop with industrial and institutional stakeholders on IT security product certification[4]: representatives from private and public sectors were invited to discuss the business case for security certification as well as technical, economic and legal issues related to the certification of security properties in ICT products, identify areas of investigation and/or possible actions by the European Commission aiming at improving the effectiveness and efficiency of the processes as well as institutional arrangements related to the security certification of ICT products in the EU.

- ENISA's Industry Collaboration Event 2016: this workshop was a follow-up of the 2015's ENISA event with representatives of the EU IT Security Industry. It focused on the demand side, and in particular identifying cybersecurity challenges and requirements in two key sectors (electronic payments and eHealth) and recognising to what extent suppliers of cybersecurity products and services are able to respond.

2.5 EU Council Presidency High Level Meeting on Cyber Security, 12-13 May

During EU Council Presidency High Level Meeting on Cyber Security in Amsterdam, a session dedicated to public- private partnership was organised. It addressed the theme of public-private cooperation, taking into consideration the following aspects: the size of and the main trends in the EU market for cybersecurity (looking at demand); the key strengths and weaknesses of EU cybersecurity companies in the global race (looking at supply); the key obstacles EU cybersecurity companies to successfully compete; the solutions the contractual PPP can provide to match the needs of the demand and the supply side of the cybersecurity market (looking at solutions); the enabling conditions that would be needed to support EU cybersecurity industry.

3. THE ONLINE PUBLIC CONSULTATION

[4] https://www.enisa.europa.eu/events/ict-security-certification-for-industry/security-certification-of-ict-products-in-europe

An online public consultation on the contractual Public Private Partnership on cybersecurity and possible accompanying measures took place from 18 December 2015 till 11 March 2016. This staff working document takes stock of the submitted contributions and preliminary trends that emerged from them focusing primarily on the quantitative analysis of the responses. A synopsis report of the consultation available at https://ec.europa.eu/digital-single-market/en/consultations.

3.1 Objectives of the Public consultation

The Commission launched the public consultation to seek stakeholders' views on the areas of work of the future cybersecurity public-private partnership as well as on potential additional policy measures that could stimulate cybersecurity industry in Europe.

3.2 Who replied to the consultation?

The consultation gathered 242 online replies (excluding one anonymous contribution, which was excluded from the data set in accordance with transparency rules, reducing the final number of online answers to 241). Among online contributions 171 were submitted on behalf of organisations, and 67 as individual responses. In three cases the respondents did not specify if they were responding as an individual or an organisation. The Commission also received 17 non-online contributions, which did not follow the structure of the online questionnaire. While these contributions have been taken into account in the qualitative analysis of the results, they were not included in the quantitative overview of responses given to specific questions.

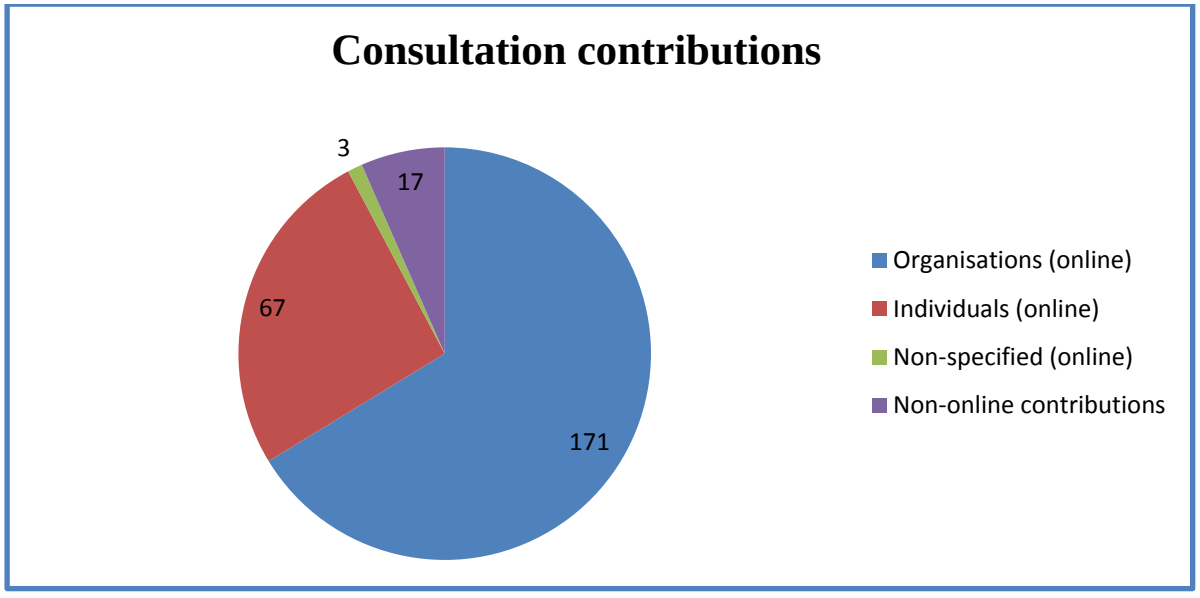

Chart 1 Overview: Online and non-online consultation contributions

The respondents represented a wide variety of organisations, with a good balance between big business and SMEs as well as contributions representing other types of stakeholders e.g.

research bodies, public administration and regulators as well as NGOs and industry representations.

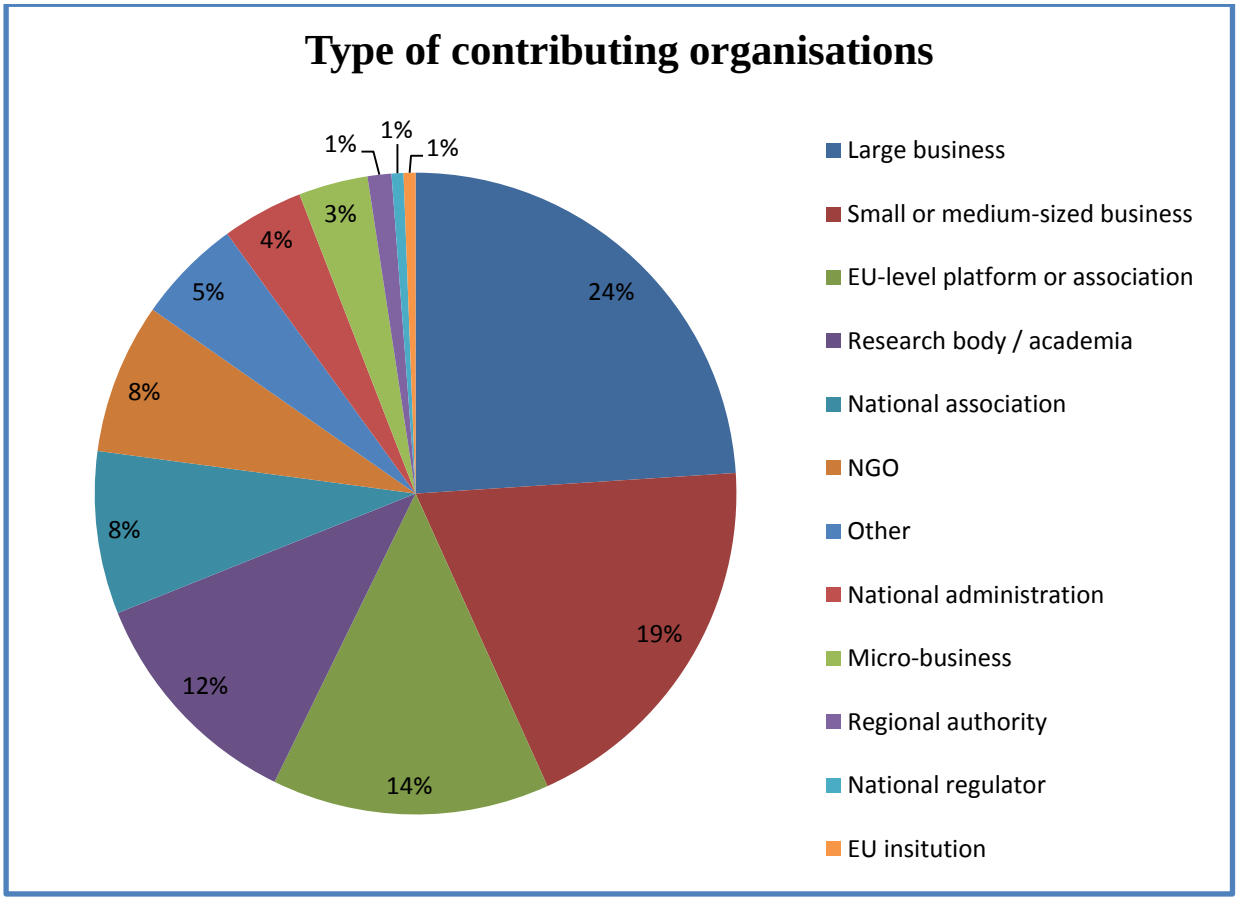

Chart 2 Overview: Type of contributing organisations to online consultation

Contributors represented different parts of the value chain of cybersecurity services and products:

- 135 suppliers of cybersecurity products and/or services
- 107 researchers
- 105 customers/users of cybersecurity solutions

Some respondents belong to more than one part of the value chain e.g. an IT company might be both a supplier and a customers of cybersecurity products and solutions.

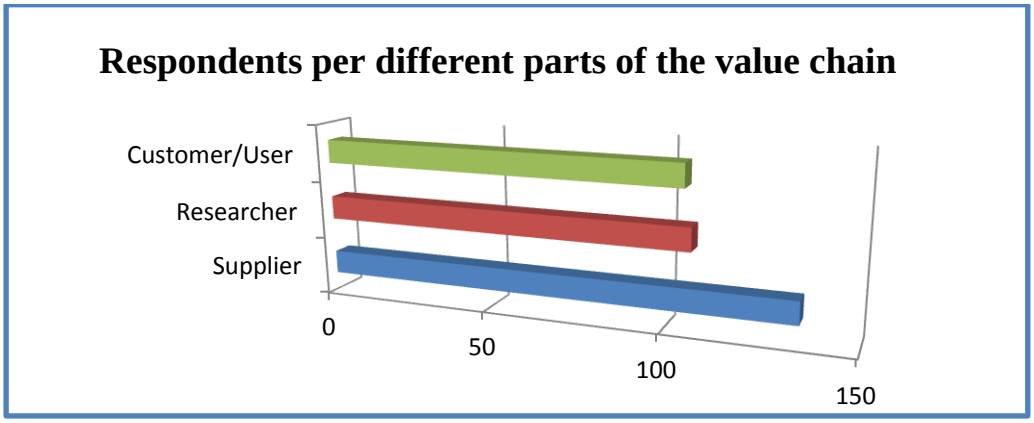

Chart 3 Overview: Part of the Value Chain Represented

The responses were also well-spread geographically. Individual responses came from 19 EU Member States, with the largest share of them coming from Italy (17.4%) and Spain (14.5%).

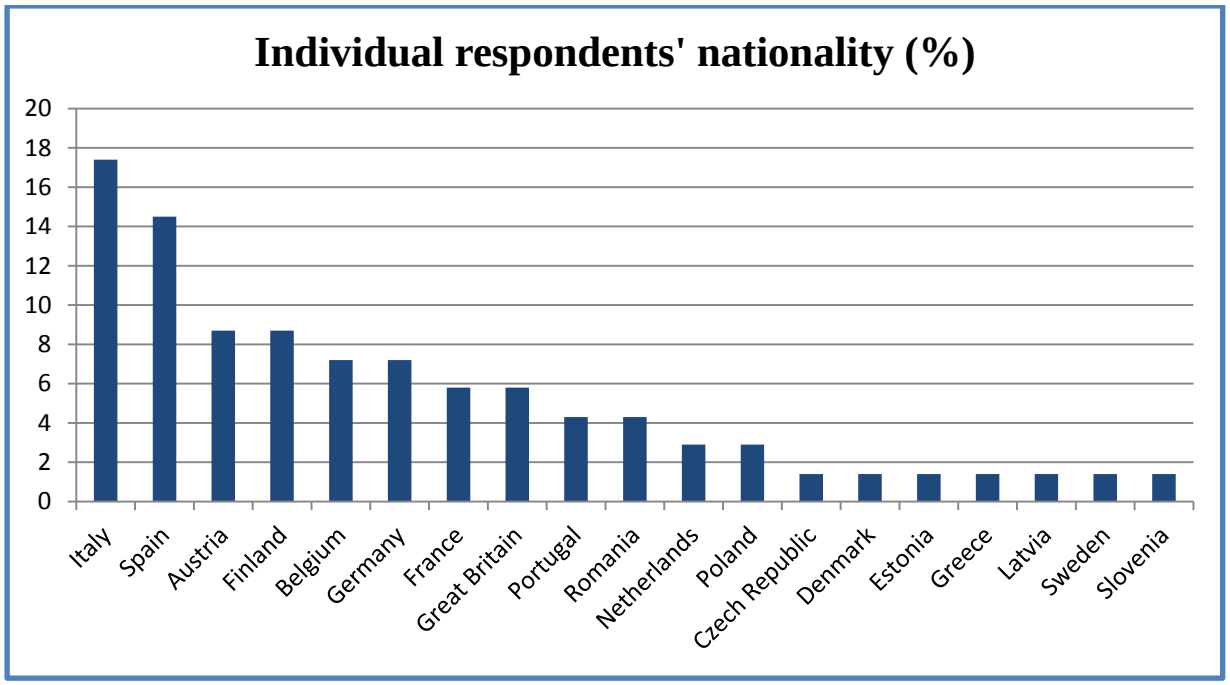

Chart 4 Overview: Nationality of individual respondents

The organisations taking part in the consultation are established in 23 different countries, including 18 EU members and a number of non-EU countries including Norway, Russia, Turkey, India and the United States of America.

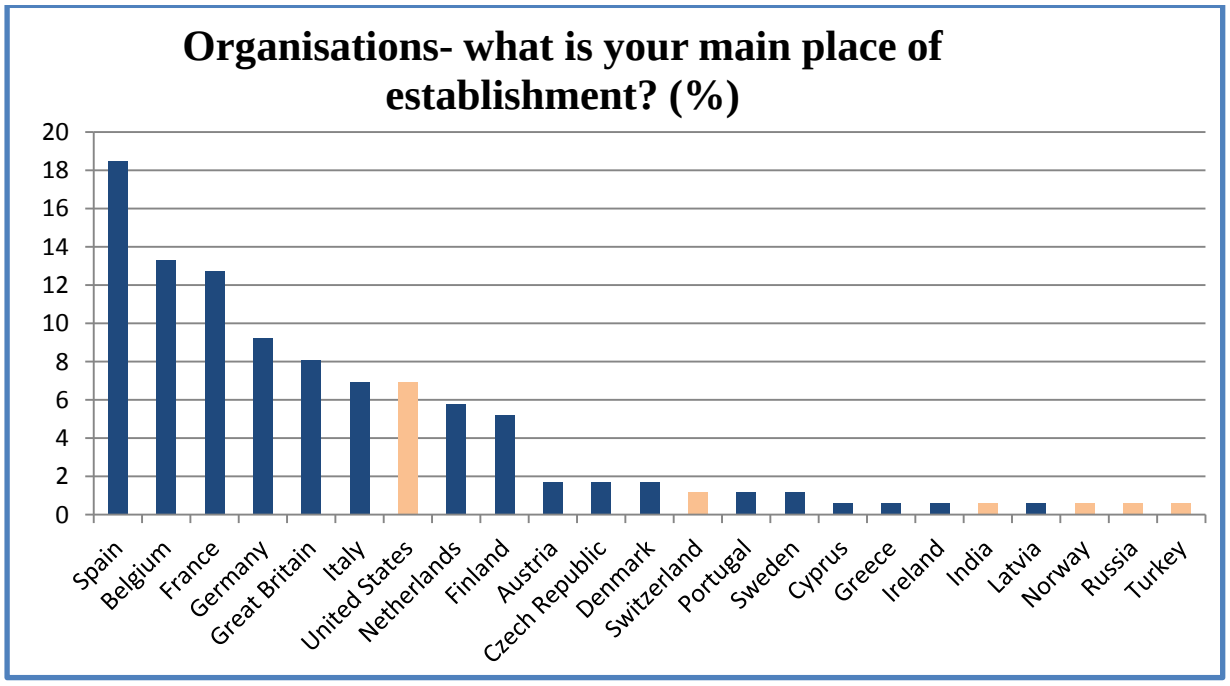

Chart 4 Overview: Place of establishment of responding organisations

(please note that a number of European associations are based in Belgium, which explains the high score of the country)

3.4 Trends observed in Response Analysis

The following trends were observed in the replies:

- The **harmonization of cybersecurity and privacy legal frameworks and regulations** as well as security requirements were among most frequently mentioned by the consultation respondents;
- **Most respondents welcomed the set-up of a cPPP on cybersecurity while pledging** for a clear priority areas that are limited in numbers and reflect a strategic focus.
- Critical infrastructure including finance and banking, energy and health were seen as the areas were the greatest socio-economic damage could be done in case of a major cyber incident. There was an overarching consensus among the respondents that **critical infrastructure protection should be a priority**.
- A large majority of respondents stated that there was a **lack of necessary goods and services** to secure the whole digital value chain. This was in particular true for Intrusion Detection Systems and Security Information and Event Management, EU trusted routers, hardware, cryptographic standards, and trusted cloud services.
- Many respondents **expressed the view that the EU cybersecurity internal market** was – in several areas – not very competitive. This is linked with substantial technological dependence on other regions. While some European products and services are as competitive as products and services offered in other parts of the world (e.g. some of the best anti-virus and anti-malware software are produced in Europe), EU providers often operate in niches and are not able to scale up across national borders, which influences their price competitiveness.
- The majority of respondents, especially SMEs, acknowledged challenges related to the access to resources to finance cybersecurity projects and initiatives. EU funds, venture funds, and bank loans are seen as the most useful financial instruments to stimulate business growth of cybersecurity players, in addition to own funding and national government support.
- Most of the respondents found that **standardization supported innovation**, because it furthered interoperability. A **combined approach to standardization** was preferred by most respondents – horizontal and cross-cutting for specific aspects relevant for specific industries. When asked about the future focus in the standardization field, there was a robust consensus among respondents on critical infrastructure protection.
- As far as the **gaps in standardization in cybersecurity are concerned**, most respondents identified interoperability issues related to IoT systems and critical infrastructures, industry 4.0, cloud, information sharing and cryptography. They also noted that all relevant standards in the field were from outside the EU (examples mentioned were AES, RSA, ECC, PKCS).

- The majority of respondents found **cybersecurity certification schemes as very important** for the development of the Digital Single Market in Europe. At the same time many respondents found that current **certification schemes did not support the needs** of the Europe's industry (note that the largest share of respondents did not know an answer to this question). The opposite view was presented by a number of global companies operating on the European market. Survey participants shared a number of ideas how a certification scheme could work – from a single European-level entity in charge defining any necessary standards or requirements to mutual recognition agreements remaining central and SOGIS[5] being promoted as a general European certification and mutual recognition body (based on mutual recognition by MS).
- At the same time a large share of respondents stated that they did not know whether certification schemes **were mutually recognized**. Among those, who expressed opinion more than half felt the current certification schemes are not widely recognised across EU Member States.
- Many consultation participants expressed the view that **increase in information sharing between private entities as well as private entities and government in terms of threat intelligence is needed**, as well as an enhanced **cooperation among national CERTs** at the international level, as cybersecurity matters are in essence cross-border problems. It was especially stressed that for real-time threat information sharing between industry and government more trust was needed and liability protection as well as privacy considerations needed to be addressed.
- Another fraction of participants stressed that **more support for open source software and open standards** (for exchanging threat information) was necessary for a functioning DSM.
- Respondents also frequently mentioned the needed of a **shift in liability and responsibility for software and hardware vulnerabilities,** as the market currently honoured insecure and convenient applications. One of suggested routes to address it was the focus on code openness and the removal of prohibitions on reverse engineering for all security research.
- In **terms of cybersecurity clusters in Europe**, the majority of respondents thought that these could be effective, but could benefit from greater support. Many within the positive-response group found that they were an effective tool for fostering industrial policy. A smaller and somewhat critical group found that clustering was not an effective tool. Across both groups, it was stated that in any case clusters could benefit from **greater coordination**.
- Among the bodies that merited most European attention, the respondents thought (descending order of importance) that these were Universities and Research Institutions, SMEs and start-ups. One of the reasons to choose those over others was the innovation-driving role, unconventional ideas and fundamental research for the benefit of all.

[5] Senior Officers Group for Information Systems agreement (Council Decision of March 31st 1992 (92/242/EEC))

IV. CONCLUSION

The stakeholder engagement for the cybersecurity cPPP initiative used a very broad range of consultation mechanisms, such as events, established public-private platforms, ad-hoc industrial grouping, workshops, experts group, online public consultation, etc. It enabled to foster engagement with Member States, institutional actors (such as national cybersecurity agencies or certification authorities), cybersecurity industry and demand sector (large companies, SMEs, industrial associations), academia, research institutes, consultancies and civil society, including open source and ethical hackers communities. These extensive consultations enabled to better understand the needs of the cybersecurity industry in Europe, as well as of their main customers (industry, public administration or citizens). This allowed the Commission to disentangle the respective benefits of using different policy instruments to address the issues identified, in particular the need to complement the cybersecurity cPPP with other industrial measures.