Summary report on the public consultation on the contractual PPP on cybersecurity and possible accompanying measures

The public consultation on the contractual Public Private Partnership on cybersecurity and possible accompanying measures took place from 18 December 2015 to 11 March 2016. This note takes stock of the submitted contributions and trends that emerge from them, focusing primarily on the quantitative analysis of the responses. A summary report of the consultation will be published during Summer 2016.

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. The replies to this consultation have provided a valuable input to the creation of the cPPP on cybersecurity and have helped the Commission define the needs related to accompanying policy measures.

Who replied to the consultation?

The consultation gathered 241 **online** replies (excluding one anonymous which was excluded from consideration in accordance with the Commission's rules on transparency).

- 171 contributions came from organisations
- 67 from individuals
- 3 respondents did not specify whether 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 questionnaire. These have been considered in the qualitative analysis of the results, but not included in the quantitative overview of responses given to specific questions.

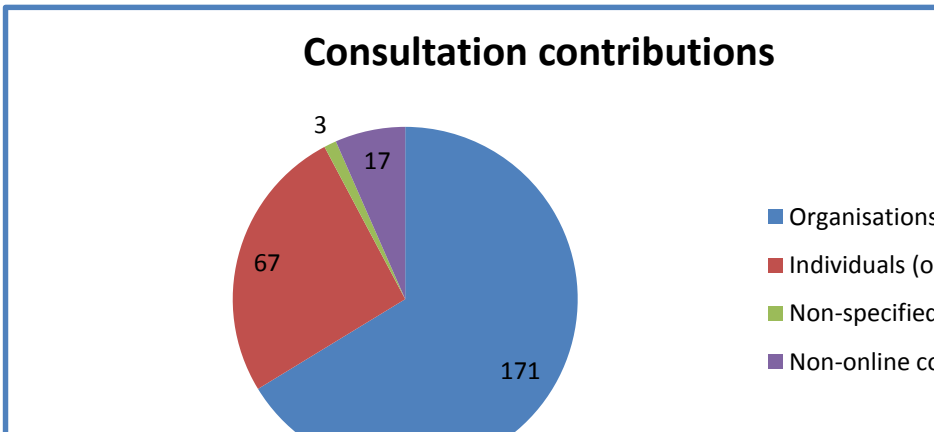

Chart 1 Overview: Online and non-online consultation contributions

Respondents represented a wide variety of organisations, with a good balance between big business and SMEs as well as other stakeholders e.g. research bodies, public administration and regulators, NGOs and industry.

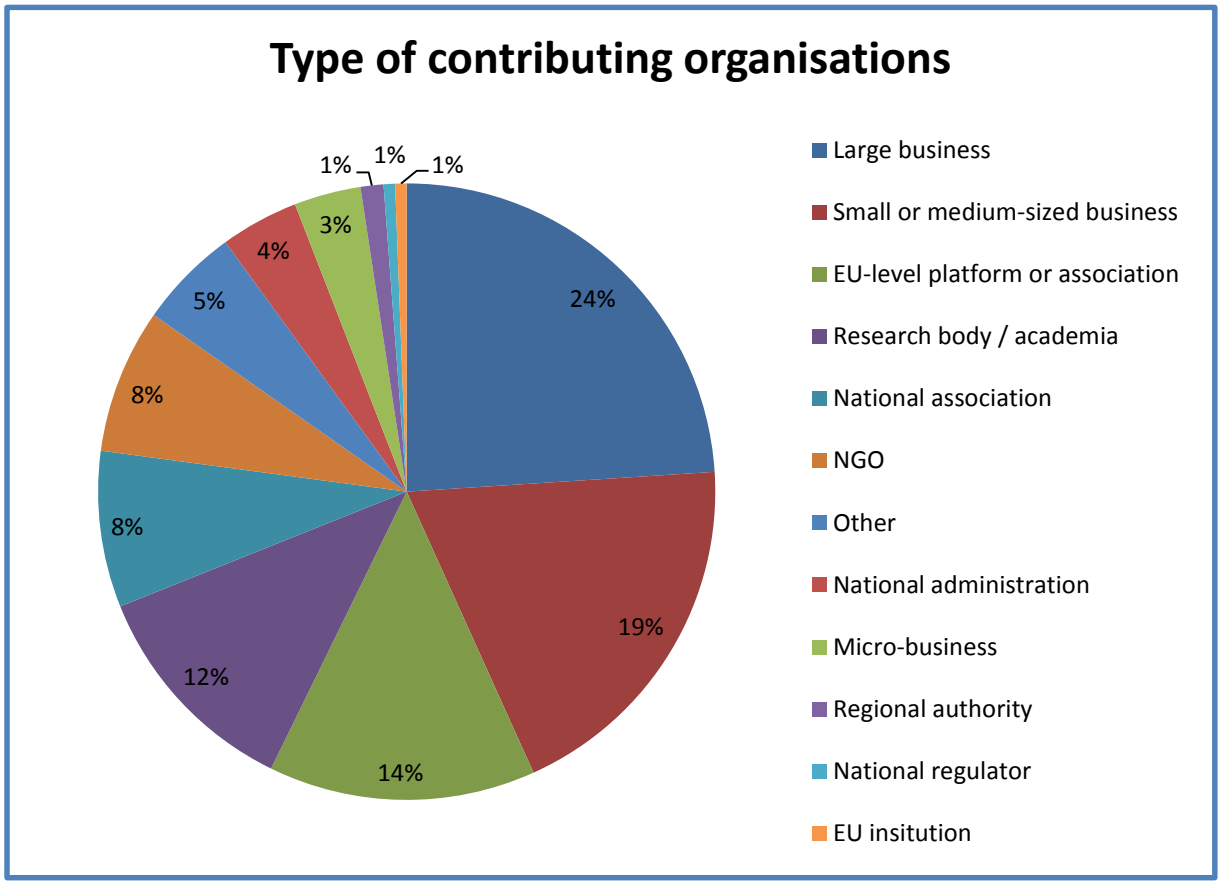

Chart 2 Overview: Type of contributing organisations to online consultation

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.

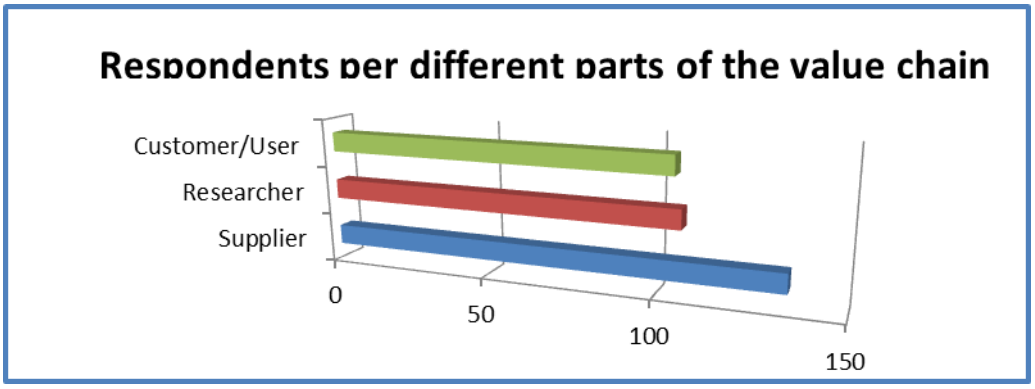

Chart 3 Overview: Part of the Value Chain Represented

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%).

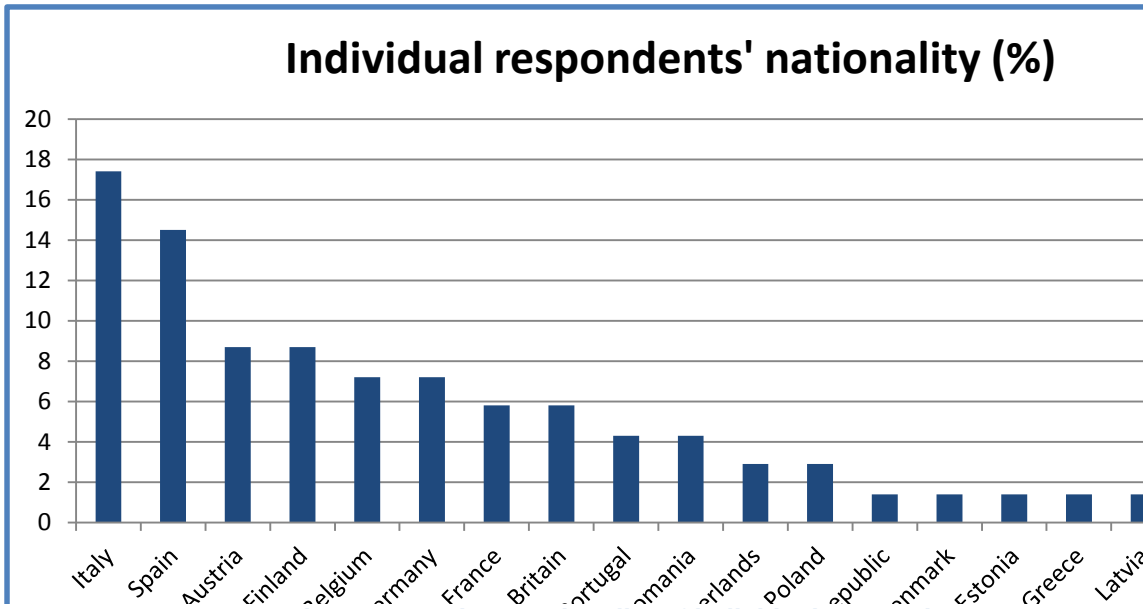

Chart 4 Overview: Nationality of individual respondents

Responding organisations are established in 23 countries, including 18 EU countries and five non-EU : Norway, Russia, Turkey, India and the United States.

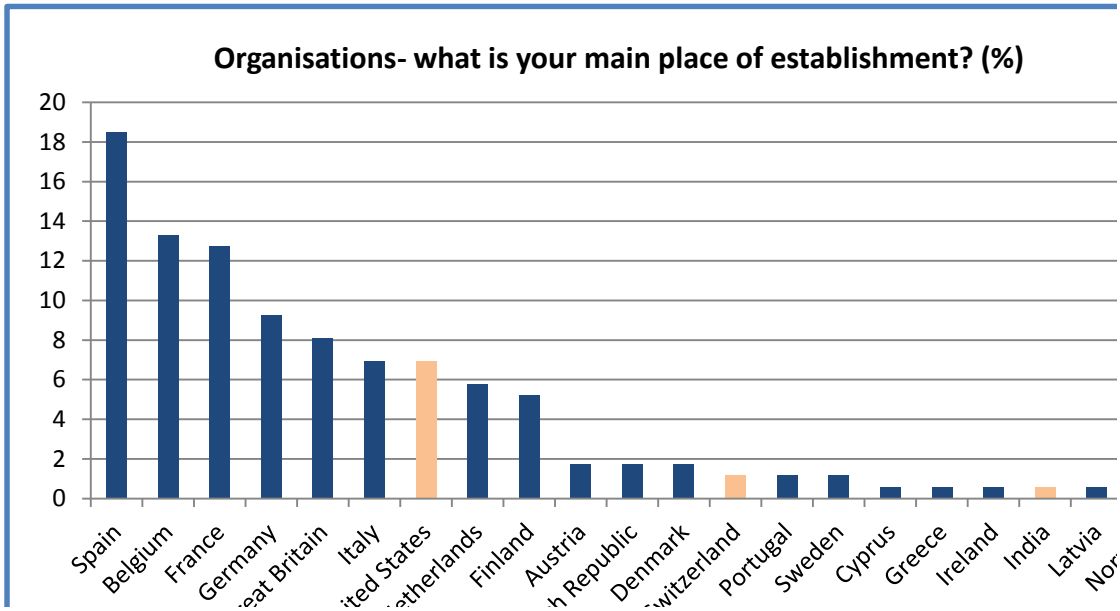

Chart 4 Overview: Place of establishment of responding organisations

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

Key findings

- **Most respondents welcome the set-up of a cPPP on cybersecurity, and ask** for a few clear priority areas with strategic focus.
- Critical infrastructure including finance and banking, energy and health were the areas were the greatest socio-economic damage could be done in a major cyber incident. Respondents agree that **critical infrastructure protection should be a priority**.
- Many **expressed the view that the EU internal cybersecurity market** was not very competitive in several areas due to technological dependence on other regions. Some European products and services are as competitive as counterparts offered in other parts of the world e.g. some of the best anti-virus and anti-malware software are produced in Europe. Yet, EU providers often operate in niches and are unable to scale up across the Single Market, which influences their price competitiveness.

Specific trends:

- A large majority of respondents (60.8%) stated the **lack of necessary goods and services** in Europe to secure the whole digital value chain. Particularly, this was true for Intrusion Detection Systems and Security Information and Event Management, EU trusted routers, hardware, cryptographic standards, and trusted cloud services.
- The majority of respondents especially SMEs, acknowledge 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 respondents (71.8%) found that **standardization supported innovation**, because it furthered interoperability. A **combined approach to standardization** was preferable – horizontal and cross-cutting for specific aspects relevant for specific industries. When asked about the future focus in the standardization field, there was consensus on critical infrastructure protection.
- When asked to identify the **gaps in standardization in cybersecurity**, most respondents identified interoperability issues related to IoT systems and critical infrastructures, industry 4.0, cloud, information sharing and cryptography.
- The majority of respondents stressed the importance of **cybersecurity certification schemes** for the development of the Digital Single Market in Europe. However, many (37.9%) thought the current **certification schemes did not support the needs** of Europe's industry (note that the largest share of respondents - 44.6% - did not know an answer to this question). The opposite view was presented by a number of global companies operating on the European market.
- A large share of respondents (50.4%) stated that they did not know whether certification schemes **were mutually recognized**. Among those who answered more than half felt the current certification schemes are not widely recognised across the EU.
- In **terms of cybersecurity clusters in Europe**, the majority of respondents to this open question 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. Both groups stated that clusters could benefit from **greater coordination**.
- Respondents thought that the bodies that merited most European attention, (descending order of importance) 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.