ROADMAP			
TITLE OF THE INITIATIVE	**Public Private Partnership on CYBERSECURITY**		
LEAD DG – RESPONSIBLE UNIT – AP NUMBER	CNECT / H4	**DATE OF ROADMAP**	14/12/2015
LIKELY TYPE OF INITIATIVE	Decision for the establishment of a contractual Public Private Partnership/possible Communication		
INDICATIVE PLANNING	June 2016		
ADDITIONAL INFORMATION	*https://ec.europa.eu/eusurvey/runner/CybersecurityContractualPPPandPossibleAccompanyingMeasuresConsultation*		
This indicative roadmap is provided for information purposes only and can be subject to change. It does not prejudge the final decision of the Commission on whether this initiative will be pursued or on its final content and structure.			

A. Context, Subsidiarity Check and Objectives

Context

Over the last two decades, the Internet and more broadly cyberspace has gained an ever stronger and deeper impact on all parts of society. Our daily life depends on seamlessly working information and communication technology, which has become the backbone of our economic growth and is a critical resource on which all economic sectors rely; it is also an indispensable element of modern public administration. At the same time, the omnipresence of information systems across all sectors and walks of human life leaves us exposed to numerous types of cyber risks that might have profound impact not only in the digital sphere but on the very physical off-line world as well. Cybersecurity is also a fundamental element of building trust needed to create and reap the benefits of the digital economy.

While citizens and businesses across Europe are facing challenges with respect to digital security, the market supply for ICT security products and services in Europe remains very fragmented, making it difficult for European companies to compete on the national and global level on one hand; and for European citizens and enterprises to have access to viable technology taking into account the fundamental rights such as the right to privacy on the other.

In the Digital Single Market (DSM) Strategy published on 6 May 2015 the Commission :

- noted that specific gaps that still exist in the fast moving area of technologies and solutions for online network security
- noted that a more joined-up approach to stepping up the supply of more secure solutions by EU industry and to stimulating their take-up by enterprises, public authorities, and citizens is needed.
- Committed to initiating in the first half of 2016 the establishment a Public-Private Partnership on cybersecurity in the area of technologies and solutions for online network security.

The initiative aims to build upon and, where appropriate, complement past and on-going Commission initiatives:

- In 2006, a Strategy for a Secure Information Society was adopted in response to the urgent need to coordinate efforts for building up trust and confidence of stakeholders in electronic communications and services.
- The Commission adopted in 2009 a Communication on Critical Information Infrastructure protection (CIIP) focusing on the protection of Europe from cyber-attacks and cyber disruptions by enhancing preparedness, security and resilience. The Communication launched an action plan with five pillars of actions: preparedness and prevention; detection and response; mitigation and recovery; international cooperation; criteria for the ICT sector. The CIIP Action Plan put forward, for the ICT sector, the necessary sector-specific policies complementing the overall European Programme for Critical Infrastructure Protection.
- The Commission second Communication on CIIP of 2011 on "Achievements and next steps: towards global cyber-security" took stock of the results achieved since the adoption of the CIIP action plan in 2009 and described the next priorities planned under each action both at EU and at the international level.
- In 2013 the **European Cybersecurity Strategy** was adopted. One of its five priorities is to develop industrial

and technological resources for cybersecurity. The strategy proposes to mobilise public and private resources to stimulate innovation and the competitiveness of secure ICT solutions supply in Europe. For this reason the EU Cybersecurity strategy has launched a public-private platform at EU level (so-called **Network and Information Security (NIS) Platform**). which looked into future research priorities, identified key challenges and corresponding desired outcomes in terms of innovation-focused, applied but also basic research in cybersecurity, privacy and trust and proposed new ways to promote truly multidisciplinary research that foster collaboration among researchers, industry and policy makers. This has resulted in the publication of a **Cybersecurity Strategic Research Agenda**[1] (SRA) of the NIS Platform in the third quarter of 2015.

- The 2014 Communication, 'For a European Industrial Renaissance', stressed the need for Europe to focus on post-crisis growth and modernisation and recognised the central importance of industry for creating jobs and growth.
- The first comprehensive piece of EU cybersecurity legislation, the **Network and Information Security (NIS) Directive** has been proposed by the European Commission in 2013 along with the European Cybersecurity Strategy and is now nearing adoption. Its implementation would be a step-change in EU cybersecurity: national capabilities and preparedness against cyber incidents would be improved; the Directive would also put in place an EU-wide approach to cybersecurity and strengthen the currently limited cooperation among Member States; and key sectors of the economy would be subject to security obligations following an approach aimed at harmonising the internal market. It is therefore very likely that the implementation of the business requirements under NIS Directive will lead to increase demand for cybersecurity solutions.
- The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted in 2014, with which the EU has managed to lay down the right foundations and a predictable legal framework for people, companies (in particular SMEs) and public administrations to safely access to services and do transactions online and across border in just "one click".
- A number of cybersecurity projects were financed under **FP7 and CIP** (7th Framework Research Programme and Competitiveness and Innovation Programme). 101 R&I Projects have together received 334 M€ EU funding between 2007 and 2014. These projects explored and covered a very diverse range of topics, including secure network infrastructure, resilience, threat detection, trustworthy service infrastructures, secure software engineering, cryptography, online privacy, biometrics, identity management, authentication, fight against botnets. They have given EU support to academic research and industry to test new waters, and develop solutions to better protect users. It has also led to the creation of some spin-offs and start ups and demonstrated the scientific excellence in Europe in cybersecurity and privacy. However, they have not sufficiently stimulated the competitiveness and innovation capacities of the digital security and privacy industry in Europe. The participation of innovative SMEs has been relatively limited (around 10%). New trends in digital technologies and cyber have emerged (social engineering, hybrid threats, complex attacks…). There is a need to further support European companies to meet current and emergent cybersecurity challenges. Half a billion Euro of EU R&I funding will support research and innovation in this area under **Horizon 2020**. In the H2020 work programme 2016-17, cybersecurity and privacy topics have been regrouped under a single **Digital Security Focus Area**, making it easier for potential participants to find relevant opportunities. Sector-specific and technology-specific cybersecurity issues are also addressed in other Societal Challenges and LEIT-ICT (e.g. cloud, IoT)

Despite these efforts, the increasing frequency and severity of cyber incidents and rising costs of protecting European consumers, enterprises and governments have amplified the urgency to further increase the cybersecurity efforts on the European level.

Issue

Europe faces growing cybersecurity challenges

Digital technologies and the Internet are the backbone of our society and economy. At the same time cybersecurity incidents are increasing at an alarming pace and can also have a more and more profound effect on daily functioning of the society and economy, given that digitisation is embracing new areas of our society and economy every day. Cybersecurity incidents may disrupt the supply of essential services we take for granted such as e.g. water, healthcare, electricity or mobile services.

The increased dependence of different sectors on IT solutions as well as interdependence between current and future infrastructures (e.g. in smart cities environments, driverless cars, Internet of Things), amplifies vulnerabilities. Increasingly public and private sector business entities have the core business, operational critical data and "digital assets of their operations" in digital form, implemented by various ICT systems, applications, services and operations.

[1] https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/strategic-research-agenda-final-v0.96/view

At the same time, businesses across Europe are facing challenges with respect to digital security. While the estimates of the scale of damages (financial theft, loss of intellectual property, etc.) differ depending on the methodology used in particular studies, the figures consistently come up in a range of several hundred billions euros[2] and are rapidly rising.

The NIS Directive soon to be adopted is a first step to bringing about a high common level of cybersecurity across the EU through improving national cybersecurity capabilities (currently uneven across the EU); enhancing cooperation between Member States and ensuring a high level of risk management practices in key sectors by requiring companies covered by the Directive to adopt risk management practices and report major incidents to the national authorities.

However, further actions are needed to ensure that Europe has access to competitive, innovative and interoperable ICT security products and solutions, which possess technical qualities allowing addressing these growing interdependences, while safeguarding fundamental rights. It is also necessary to stimulate awareness and voluntary uptake of cybersecurity solutions and processes by public and business actors not covered by the NIS Directive proposal (efforts in this regard have been started by the NIS Platform) as well as by citizens at large to better protect our society and economy against disruptions of digital technologies.

Cybersecurity threats are borderless but European industry and market significantly fragmented

While cyberspace is borderless by nature, market supply for ICT security products and services in Europe is significantly fragmented. According to a pan-European study conducted for the European Commission the EU market has been dominated by a small group of global vendors, competing with a high number of smaller European suppliers. At the time of the study, while the levels of market concentration varied across market segments (hardware, software, services) the top five vendors controlled 20.4% of total market (and they all came from outside the EU). The EU suppliers, while showing a positive dynamism, remain mostly national or regional players. Their cumulative market share was estimated at round 16.5% of the total EU NIS market revenues.[3] The fragmentation of the cybersecurity supply industry in Europe was also reflected in a number of studies conducted on a national level by some Member States.[4]

Historically, industrial development in this area has been stimulated by governmental purchase and some highly innovative European companies in this sector are still largely dependent on public procurement in their home country. A side effect of this situation is limited willingness for cross-border purchasing, which is a barrier to the development of a common cybersecurity market. At the same time smaller, newer players while initiating their business in limited, country markets, struggle with making international expansion as buying behaviours can be biased towards established (often global) brands that can leverage strong market presence and marketing budgets to protect their market share from new entrants. In the wider context this leads as well to the risk of over-reliance of European buyers on third country supply.

Whereas some initiatives across a few member states aim to bring together the competencies and industrial players in this area, potentially helping European companies to join forces and expand across a number of European countries, the fragmentation is still considerable: the industry is nowhere near some more structured segments of the ICT industry, such as microelectronics, where well-established regional cluster of excellence and ecosystems can be identified, leveraging academia, industrial, institutional and customers/users capacities, and enabling this industry to compete on a global scale.

The market fragmentation has been a result, among others, of:

- A number of different NIS policies across Member States (which would be partly addressed by the implementation of the NIS Directive)
- Dependence on public procurement and government purchase making many companies dependent on public procurement in their home country
- Insufficient uptake of process standards for cybersecurity in organisations as well as lack of consideration for cybersecurity as a functional requirement in the development of new technical standards;
- Lack of a well-functioning mechanism of certification
- Barriers of trust for cross-border purchase

Global competitiveness challenge and outflow of European know-how

This industry and market fragmentation is a clear barrier for European companies to compete and grow their businesses across borders in Europe but also on a global scale. While European companies tend to be strong and innovative, their size and capacity (mostly SMEs with few larger actors) are smaller in comparison to their US, Israeli, Chinese, South-Korean, Japanese or Russian counterparts as they experience difficulties in expanding

2 See reports: *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II;* Center for Strategic and International Studies; June 2014;; *Norton Report on Cybercrime (2013);* *Global Report on the Cost of Cyber Crime* 2014, Ponemon Institute;
3 The European Network and Information Security Market: Scenario, Trends and Challenges - A study for the European Commission, DG Information Society and Media; 2009. A new market study is being conducted by an external contractor for the European Commission at the moment and will feed into the cPPP creation process.
4 Competitive analysis of the UK cyber security sector, A study for the A study for the Department for Business, Innovation and Skills, 2013; *L'observatoire de la filière de la confiance numérique en France* - Etude pour l'Alliance pour la Confiance Numérique (ACN), 2013; Der IT-Sicherheitsmarkt in Deutschland; Bundesministerium für Wirtschaft und Energie, 2014;

beyond national borders.

The difficulty to compete on the European and global levels often leads to mergers and acquisitions of European SMEs by non-European actors, weakening the European sector and leaving Europe also more vulnerable and technologically dependent on others.[5]

The barriers preventing European cybersecurity companies from scaling up their operations have also an unintended consequence of the outflow of highly qualified specialists, who leave the EU to look for better job and research opportunities on other markets.

Should Europe fail to stimulate a common cybersecurity market and to create opportunities to grow for its companies, it risks losing its cybersecurity industry all together as it might not be able to stand fierce global competition.

Missed economic opportunities vs. a chance for competitive advantage

This development would also be a missed opportunity for the European economic growth as the global cyber security market is expected to be among the fastest growing segments of the ICT sector in the coming decade. In 2013 the cyber security market was worth $65.9 billion (with the European market constituting around 17% of it) and is expected to grow to $80-120 billion by 2018.

The fragmentation of the market results in limited possibilities of achieving the economies of scale needed to meet the growing demands of European economy, which is currently undergoing an accelerated digital transformation. While the demand for security products and solutions by some sectors is likely to increase in the coming years as a result of the prospective implementation of the currently negotiated NIS Directive, it is crucial that this market development opportunity is not confined by entry barriers between different EU countries.

While cybersecurity is usually looked through the prism of vulnerabilities and risks, it is also a major opportunity for Europe and could become our competitive advantage. Making the EU a strong player in cyber security preparedness and trustworthy ICT will contribute to our ambitious goals for the Digital Single Market to create growth and jobs. Also, this would mean providing trustworthy European solutions (ICT products, services and software) for protecting information held by citizens, companies and public institutions.

Subsidiarity check

The Commission decision concerning the establishment of **a contractual Public-Private Partnership (cPPP) will be possibly accompanied** by a **Communication which would present** a limited set of well-targeted **accompanying measures**, complementing the cPPP and contributing to its objectives. Such measures will be carefully chosen following analysis of the evidence coming from various sources including public consultation. The measures which will be considered for that purpose will be chosen among the following: support to the development of competitive clusters/centres of excellence, ensuring interoperability of solutions through technical and process standards, improving readability and trustworthiness of security levels through mechanisms such as certification (either regulatory or non-regulatory) and/or labelling, measures addressing access to finance, procurement, start-up support). Only those measures that would have a tangible added value addressing specific gaps and needs of the cybersecurity market and do not overlap with the existing horizontal instruments will be retained.

The European Union is empowered to adopt measures with the aim of establishing or ensuring the functioning of the Internal Market, in accordance with the relevant provisions of the Treaties (Article 26 of the Treaty on the Functioning of the European Union — TFEU). In view of a huge fragmentation of the market for ICT security products and solutions, the EU action is needed to achieve a single market in this field, which is also a prerequisite for a well-functioning digital economy.

The stated objectives can be better achieved at the EU level, rather than by the Member States alone, in view of the cross-border aspects of the cybersecurity challenge as well as the activity of global competitors working across the markets.

Therefore, the EU may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, the proposed measures do not go beyond what is necessary in order to achieve those objectives.

The legal basis for specific measures suggested in this Roadmap is as follows:

- **Contractual Public Private Partnership (non-regulatory measure)**

Article 25 in the Regulation of the European Parliament and of the Council establishing Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020) – provides the legal framework for the establishment of a public-private partnership. Article 25(2)(b) specifies that this partnership should be based on a contractual arrangement between the EC and the industry partners. The contractual agreement should specify the objectives of the partnership, respective commitments of the partners, key performance indicators, and outputs to

[5] See for example: *Cyber Security M&A Decoding deals in the global Cyber Security industry*

be delivered, including the identification of research and innovation activities that require support from Horizon 2020.

➢ **Other measures**

The final list of measures to be implemented (based, among others, on the external studies and the analysis of the public consultation input) will also undergo a subsidiary check.

Main policy objectives

The measures under consideration would aim to:

a. Overcome current ICT security products and solutions supply market fragmentation to create a European single market for innovative ICT security products and solutions helping European supply industry achieve economies of scale and compete on a European and global level

b. Secure European digital technologies - ensure that European citizens, enterprises (including SMEs), public administrations have access to the latest digital security technology developments, which are interoperable, competitive, trustworthy and based on European rules and values

c. Limit the risk and the impact of cybersecurity incidents, while increasing consumers' and citizen's trust and fostering the EU digital economy

These broad objectives can be met by achieving more specific goals for both supply and demand side of the ICT secure products and solutions market.

On the supply side:

1. Stimulating competitiveness of the European ICT security products and solutions industry through innovation
2. Ensuring economies of scale through engagement with users/demand side industries and bringing together a critical mass of innovation capacities;
3. Stimulating the emergence of strong European actors in cybersecurity (both large and SMEs) that can compete globally

On the demand side:

4. Mainstreaming cybersecurity across different economic areas by making it a functional requirement in both emerging digital technologies (e.g. cloud, big data, 5G, embedded systems); industrial sectors essential for a well-functioning single market (e.g. energy, automotive, rail, aviation, health, banking, finance…) as well as public administration.
5. Increase awareness and stimulate voluntary uptake of cybersecurity solutions and processes by public and business actors not covered by the NIS Directive proposal (building also on the work done to date by the NIS Platform)

Cross-cutting on the demand/supply side:

6. Stimulating trust among institutional and industrial actors facilitating the creation of a single European market for cybersecurity products and services.
7. In mid-term, creating the right framework for EU-wide interoperability (technical and process standards) and a well-functioning mechanisms of certification
8. Increase readability and trustworthiness of the ICT security products and solutions through labelling

The Contractual Public Private Partnership on cybersecurity will directly contribute to the first two objectives while a Communication could identify a limited and well-defined set of new measures, with additional impact, addressing specific gaps not addressed in other horizontal policies and instruments.

B. Option Mapping

The policy options that are considered ideally cover option (ii) to ensure a comprehensive approach to the challenge set in this Roadmap and at minimum option (iii).

(i) No EU action / no change in EU action

This would maintain the status quo of largely national approaches and would not serve to create a well-functioning European market for cybersecurity products and services. The inaction could result in:

- Difficulty to face fierce global competition leading to the increased number of mergers and acquisitions by non-European actors and consequently a substantial weakening of the European ICT industry of security products and services
- Increased vulnerability and technological dependence of Europe on providers from other geographies coupled with the lack of access for European citizens and businesses to security products and solutions based on European values
- Inability of European suppliers to meet the growing demand spurred by the implementation of the NIS directive. This would lead to losing European and global cybersecurity market share by

European actors

- The outflow of the highly qualified specialists to other geographies/markets, which present better professional opportunities
- Missed opportunity to reinforce trust in the digital economy and reap the benefits of the digital single market
- Missed opportunity for Europe to become a global leader in the field of cybersecurity

(ii) **Stimulate European competitiveness and demand for secure IT products and solutions through innovation and other supporting measures**

This policy option assumes a comprehensive approach to nurture a European-grown cybersecurity.

To address both the supply and demand side objectives the Commission, will:

1. Launch a contractual public-private partnership on cybersecurity

- **A Contractual PPP gathering industrial and public resources** would deliver innovation against a jointly-agreed roadmap for strategic research and innovation (based on the Strategic Research Agenda developed by the NIS Platform). It would contribute to achieving both supply and demand side objectives through:
  - **Building trust among Member States and industrial actors by fostering bottom-up cooperation** on research and innovation in the upstream part of the innovation life cycle. This should help facilitate cross-border purchase in the future and will also be a first step in the necessary process of collaborative effort needed to ensure the success of other policy initiatives in areas such as standardisation and certification.
  - **Helping align the demand and supply sectors for cybersecurity products and services** by allowing industry to effectively and efficiently elicit future requirements from end-users in various categories (e.g. SMEs, public administration and citizens; big companies and critical infrastructure operators) as well as sectors (e.g. energy, health, transport, finance) and possibly identify commonalities contributing to economies of scale.
  - While cybersecurity challenges may differ across different sectors, the cPPP will be an opportunity to identify and **seek synergies to develop common, sector-neutral technological building blocks with maximum replication potential** (e.g. encrypted storage and processing, secured communication, etc.), which should help ensure the compatibility of solutions across borders while leaving enough flexibility for products to be further adapted to national/business needs when reaching specific markets/customers.
  - At the same time a cPPP is also a good vehicle to **engage industries that are big costumers of cybersecurity solutions** (or are likely to become bid demander because of the digitalisation they are undertaking and/or the requirements of the NIS Directive in some cases) to define common digital security and privacy requirements for their sector.
  - The cPPP would also be one of **mechanism to implement the DSM Priority Standardisation Plan**
  - **Finally cPPP** can also contribute to defining mechanisms to ease access to finance (including venture capital, sovereign welfare funds, EIB/EIF, etc.), as well as developing human capacities in the field of cybersecurity

cPPP would allow to maximize the use of available funds through better coordination with Member States and better focus on a few technical priorities. It should leverage funding from Horizon 2020 Leadership in Enabling and Industrial Technologies (LEIT-ICT) and Societal Challenge Secure Societies (SC7) to deliver societal benefits for users of technologies (citizens, SMEs…) and provide visibility to European R&I excellence in cybersecurity.

2. Implement accompanying policy measures

This Roadmap presents a list of possible additional measures, which need to be taken into account in order to establish a comprehensive cybersecurity industry policy. They will be subject to consultation and impact assessment in case of significant expected impacts.

- **Additional supply side measures could include:**
  - **supporting** the development of globally competitive **clusters/centres of excellence (**through leveraging smart specialisation approach across different regions and also building on activities envisaged to be financed by the European Structural and Investment Fund)
  - **supporting cybersecurity technology export and access to foreign markets.** This could e.g. include access to low-interest loans to enable acquisitions or legal entity establishment in the target countries.
  - **facilitating access to financial resources** (e.g. equity funding, venture funding, EIB/EIF instruments, etc.)
  - **cybersecurity start-up support** policy measures
  - **human resources and skills support measures** (e.g. support community-built sharable curriculum and training modules in order to make curricula and training more agile and responsive to real life security threats and changes in the technology environment)
    - **other industrial policy instruments**

- **Additional cross-cutting measures:**
  - Ensuring interoperability of solutions and practices - this could be achieved by d**eveloping technical and process standards** (as necessary but beyond what is possible to achieve through joint industrial cooperation under Horizon 2020). The EU Rolling Plan for ICT Standardisation as well as Priority ICT Standards Plan are essential instruments in this regard.
  - **Improving readability and trustworthiness** of security levels for public and private buyers and therefore increasing demand for European ICT security products and solutions through:
    - **Voluntary European labelling schemes**
    - **Certification** (market or regulatory driven). The opportunity to build on existing international and European arrangements and develop faster, more innovation-friendly and more flexible mechanism should be explored.
    - **Promoting Open Source solutions** to avoid vendor lock-in
  - **Introducing mechanisms** (auditing) for assessing the cybersecurity capacity of companies when this is a precondition for proper diligence and reporting, including affected customers.
  - **Public procurement** measures e.g. pre-commercial procurement / public procurement of Innovation (PCP/PPI).
  - **Other industrial policy instruments**

Designing a comprehensive approach could allow the Commission to present an encompassing industrial policy for the Cybersecurity industry that would go beyond the mere research & innovation questions the cPPP itself would be able to address (e.g. certain types of standardisation, certification, auditing, etc.). This holistic approach package will describe different areas, where European action is needed and can bring an added value in order to develop or maintain a highly competitive cybersecurity industry in Europe.

This would make it possible for European citizens, enterprises (including SMEs), public administrations to have access to the latest digital security technology developments, secured infrastructures and best practices, which are trustworthy and based on European rules and values.

(iii) **Stimulate competitiveness of the European cybersecurity industry through innovation**

This option would limit Commission action on the Contractual PPP. The establishment of the cPPP would plant the seed for mid-term innovation and long term competitiveness..

Proportionality check

None of the policy options is a priori contrary to the principle of proportionality. Respect for such principle will guide the preparation of the Communication from the identification and evaluation of the different policy options to the drafting of proposals.

C. Data collection and Better Regulation instruments

Data collection

The Commission aims to back up the Communications with a wide range of evidence and data, including:

- The types of digital security products and services provided in Europe;
- The technologies, solutions and services implemented;
- The application areas of cybersecurity and the resulting characteristics of demand in different sectors;
- The ties with the traditional European security and defence sector;
- The geographic areas, which display different demand and supply characteristics, depending on market maturity, threat levels and the regulation in place;
- The size and characteristics of the players in Europe, ranging from the large amount of SMEs specialised on niche markets to a few large global actors.
- Results of workshops organised on specific industrial policy instruments, in particular those prepared by ENISA.

This information will be gathered through a robust consultation process and studies conducted by external contractors. In particular the following data and stakeholders input will be taken into consideration:

- The **Strategic Research Agenda** (SRA) in the area of secure information and communication technologies (ICT) published in September 2015[6]. This document identifies the key challenges and desired outcomes in terms of innovation-focused, applied research as well as for cybersecurity. It proposes new ways to promote

[6] https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/strategic-research-agenda-draft-v02.63/at_download/file

truly multidisciplinary research that fosters collaboration between researchers, industry and policymakers, and recognises the difficulties faced by some segments, such as SMEs in engaging with traditional research mechanisms. The SRA is the result of more than a year's work by the Working Group on Secure ICT Research and Innovation of the **Network and Information Security (NIS) Platform** that was launched by the European Commission in spring 2013 and gathers actors from the industry, research/academia and public authorities. WG3 organised several expert meetings to structure its activities.

- The "**Cybersecurity Industry Market Analysis**", which is currently being carried out by an external contractor to obtain data about the cybersecurity situation in Europe. The study will assess in depth the strengths and the weaknesses of the current European industrial sector in cybersecurity and compare it with the same sector in other parts of the globe that are clear competitors of the EU. The study methodology envisages a range of consultation tools including interviews, online questionnaires, workshops and discussion forums. This study should provide the necessary economic/market analysis evidence to support industrial policy making, including the choice of relevant instrument(s) among the range of industrial policy tools at the disposal of the European Commission and Member States. The results of the study should be available in the first half of 2016.
- The Study on "**Synergies between the civilian and defence cybersecurity markets**", which is currently being carried out by an external contractor. The aim of the study is to identify how synergies between the civilian and defence cybersecurity markets can be encouraged and where these synergies could lead to improved efficiency an innovation of the markets. The study should also identify issues and challenges facing the markets and present possible solutions that facilitate synergies through the Horizon 202 research programme. The methodology of the study envisages desk research, interview programmes, and extensive literature review. The final report of the study should be available in the first half of 2016.
- Relevant data from the Impact Assessment accompanying the Proposal for the NIS Directive SWD (2013) 31 final
- Input from bi-lateral meetings and consultation between DG CONNECT and Member States as well as industry actors active in the field of cybersecurity.
- The results of a broad based public consultation targeting all interested parties, which will be launched along with the Roadmap in autumn 2015.
- Additional studies and impact assessment might be needed at a later stage should the Commission suggest in the Communication the intention to explore the necessity of introducing regulatory measures to encourage market harmonisation (e.g. revised framework for ICT security certification).

Consultation approach

The work on the Communication has been accompanied by a robust consultation strategy, including the following past activities and future plans:

- A public consultation, which will be launched in December 2015. With this public consultation the Commission will call for contributions by all relevant stakeholders (supply industry, Member States, civil society, user groups, demand/customer industries…) on the areas of work of a future cybersecurity contractual PPP, and on the cybersecurity aspects of standardisation addressed in the DSM. The consultation can be found under the following link:

  https://ec.europa.eu/eusurvey/runner/CybersecurityContractualPPPandPossibleAccompanyingMeasuresConsultation
- The ongoing stakeholder dialogue within the NIS Platform Working Group 3 which resulted in the publication of the Strategic Research Agenda (please see the section above on Data Collection).
- Continuous engagement with representatives from the cybersecurity industry in Europe, as well as with producers of components and equipment, operators of critical infrastructures and both public and private sector users. In addition, the voices of public authorities, national and European security agencies, but also of consumers and citizens are essential for the quality and legitimacy of the initiative and could be conducted through the NIS Platform, which is fully open and transparent process;

Will an Implementation plan be established?

Yes Once the final scope of the package is known following the consultation procedure, an implementation plan will be presented outlining the next steps in the process.

Will an impact assessment be carried out for this initiative and/or possible follow-up initiatives?

No. The Communication would focus on non-regulatory measures, it would be accompanied by a Staff Working Document outlining both the intended impacts of the measures under consideration and the evaluation of past policy and research & Innovation programmes. The evidence would also underpin the Decision on a contractual Public-Private Partnership. An impact assessment might be needed at a later stage should the Commission suggest in the Communication the intention to explore the necessity of introducing specific measures to encourage market harmonisation (e.g. certification, labelling) likely to have significant impacts.