EUROPEAN
COMMISSION

Brussels, 5.7.2016
SWD(2016) 216 final

COMMISSION STAFF WORKING DOCUMENT

Contractual Public Private Partnership on Cybersecurity & Accompanying Measures

Accompanying the document

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

{C(2016) 4400 final}
{SWD(2016) 210 final}
{SWD(2016) 215 final}

Table of Contents

I. Policy context - digital society and economy – opportunities vs. vulnerabilities

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 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 increased dependence of different sectors on IT solutions as well as interdependence between current and future infrastructures (e.g. in smart cities environments, connected cars, energy smart grids), amplifies vulnerabilities and lead to an increase of cybersecurity threats. The growth of the "Internet of Things" results in ever more devices that are connected online, widening the potential entry points for threats (i.e. attack surface) and disruption.

Cybersecurity incidents are increasing at an alarming pace with potentially more and more profound effects on the daily functioning of the society and economy, given that digitisation is embracing new areas of our society and economy every day. They may disrupt the supply of essential services we take for granted such as e.g. water, healthcare, electricity or transport.

Critical infrastructures, such as for example electricity generation plants or transportation systems, are controlled and monitored by Industrial Control Systems (ICS), including SCADA (Supervisory Control and Data Acquisition) systems. Today ICS products are mostly based on standard embedded systems platforms and they often use commercial off-the-shelf software. This results in the reduction of costs and improved ease of use but at the same time increases the exposure to computer network-based attacks. Vulnerabilities of communication networks and information systems may be exploited for financial or political motivation to shut off power to large areas or directing cyber-attacks against power generation plants. Looking at energy distribution grids, the

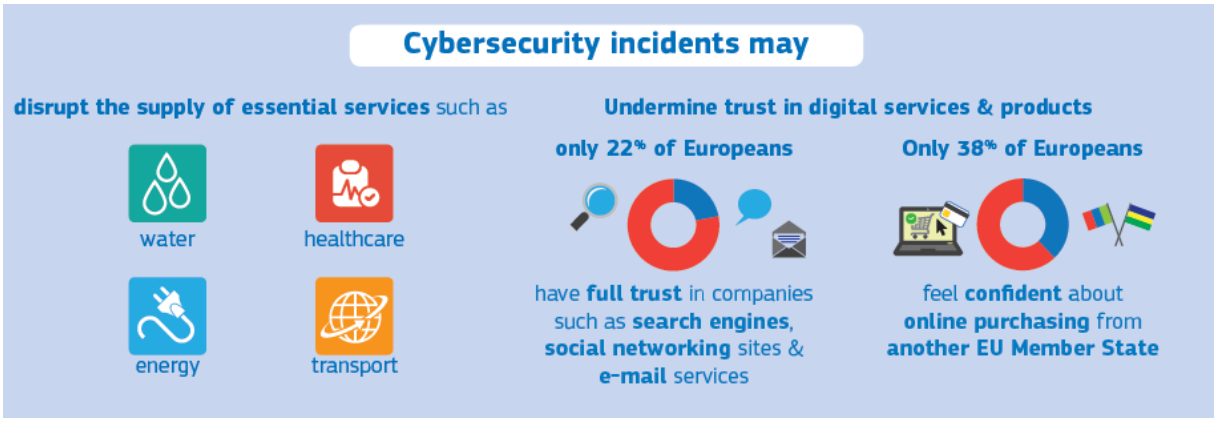
Dragonfly Attack

In 2014 the attackers, managed to compromise a number of strategically important organizations for spying purposes. The attack targeted energy grid operators, electricity generation firms, pipeline operators, across numerous countries including, Spain, France, Italy, Germany, Romania, Poland, Turkey, and United States and potentially could have led to damage or disruption to energy supplies in affected countries.

situation is even more complex as with the roll-out of smart-metering systems and the flourishing of energy third party services, the traditional barriers between the energy systems and the end-user networks are becoming more and more blurred.

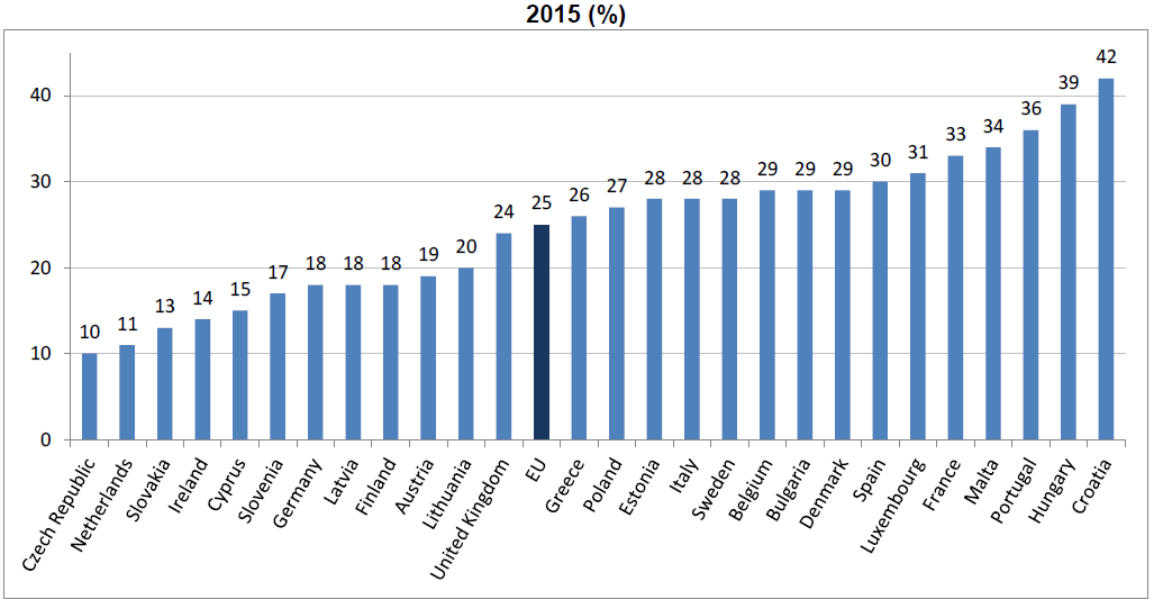
Cyber threats also target public administration services, as was the case e.g. in the summer of 2015 when a cyber-attack on the German lower house of parliament enabled hackers to steal official data.

They can also undermine trust needed to create and reap the benefits of the Digital Single Market - a flagship project of the European Union. In a nutshell:



The need for protection concerns equally the citizens, public administration and businesses. According to the survey on information and communication technology (ICT) usage in households and by individuals in the European Union (EU) the proportion of internet users having experienced certain common security issues over the internet – such as viruses affecting devices, abuse of personal information, financial losses or children accessing inappropriate websites – stood at 25% in 2015.

Share of internet users who experienced security related problems in the EU Member States, 2015 (%)



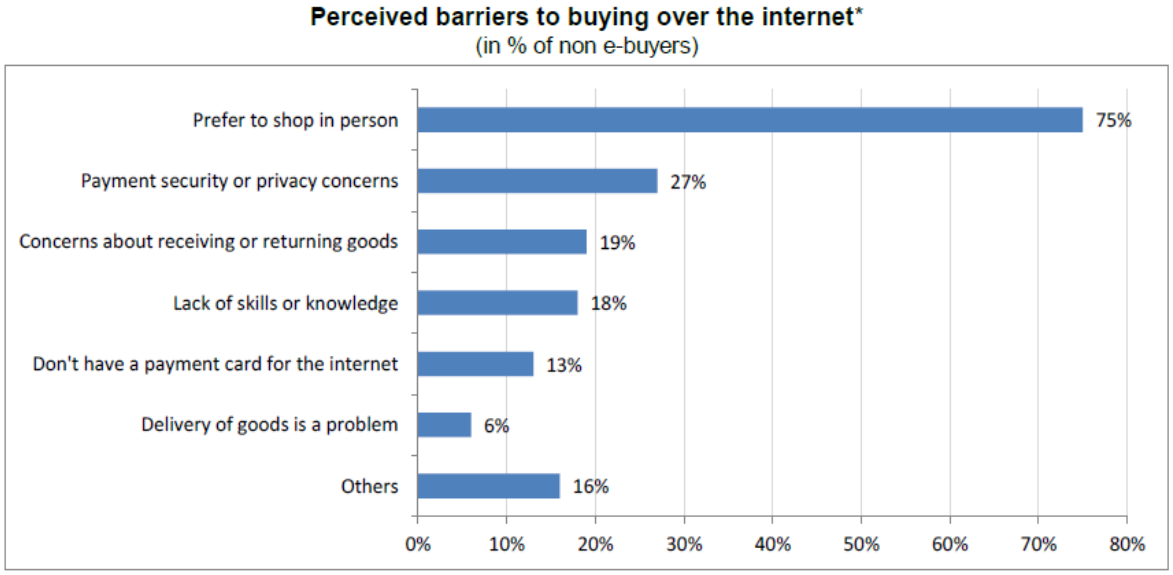
Romania: data not available

Source: Eurostat

Security concerns prevented some internet users in the EU from doing certain activities over the internet: almost 1 in 5 did not shop online (19%) or did not carry out banking activities (18%) in 2015, and 13% of them did not use the internet with a mobile device via wireless

connection from places other than home.[1] Notably, more than 1 internet user out of 5 did not buy or order goods or services on-line for private use due to security concerns in Romania (35%), Sweden (34%), Portugal (30%), France (29%), Spain and Latvia (both 28%), Finland (27%), Italy and Malta (both 25%), Slovenia (24%), Denmark (22%) and the Netherlands (21%)[2].

As to those people in the EU who did not make any purchases over the internet in 2015, an overwhelming majority had a preference to shop in person. More than a quarter (27%) reported that payment security or privacy concerns prevented them from shopping electronically, which was the first reason for not shopping online beyond the preference to shop in person.[3]



Source: Eurostat

Just as consumers, who take advantage of digital opportunities, businesses across Europe also largely depend on smoothly running information systems. This concerns not only the organisations, whose business model is based on online activity such as e.g. e-commerce platforms, but practically all types of businesses as the use of information and communication technologies influences the way that enterprises are run, information shared with partners and customers. 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 customer relation management, applications, services and operations (e.g. customer relationship management, supply chain management or enterprise resource planning). According to the survey on information and communication technology (ICT) usage in enterprises only 3% of enterprises in the EU 28 do not have access to Internet.[4]

In view of this profound change, businesses across Europe, both big organisations and Small and Medium Enterprises (SMEs), also face challenges with respect to digital security. The *2015 Information Security Breaches Survey* (2015) conducted in the United Kingdom showed that 90% of large organisations and 74% of small and medium-sized businesses reported they

[1] http://ec.europa.eu/eurostat/documents/2995521/7151118/4-08022016-AP-EN.pdf/902a4c42-eec6-48ca-97c3-c32d8a6131ef
[2] Source: Eurostat
[3] http://ec.europa.eu/eurostat/documents/2995521/7103356/4-11122015-AP-EN.pdf/276b6a7c-69a6-45ce-b6bf-488e975a8f5d
[4] http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_enterprises#Enterprise_use_of_information_technology

had suffered from an information security breach. For companies with more than 500 employees the average cost of the most severe breach was between €1.86 million and €4.01 million whereas for SMEs it oscillated between €95,840 and €397,167[5] While the estimates of the scale of cybersecurity damages (financial theft, loss of intellectual property, etc.) differ depending on the methodology used in particular studies, the global figures consistently come up in a range of several hundred billions euros[6] and are rapidly rising.

According to the *OECD Digital Economy Outlook 2015*, the digital security threat landscape continues to evolve, sustained by often profitable business models. For example, one of such models is based on "“ransomware”, which is a type of file-encrypting malware increasingly deployed by cybercriminals to encrypt the computer files of an organisation or individual, who must then make a payment (i.e. the “ransom”) in exchange for decryption of their files. The most prominent strain of ransomware is “CryptoLocker”, which is spread via email attachments. Experts estimate that "CryptoLocker infected some 234 000 computers during its first two months alone, before being disrupted by a multinational law enforcement effort, involving Canada, Germany, Luxembourg, the Netherlands, Ukraine, the United Kingdom and the United States".[7]

Also, cyberattacks leading to data breaches where the personal data of millions of European individuals in the EU get compromised have become more and more common in the recent years. Similarly to the business model behind ransomware, the breached company could be requested to pay a sum of money to the attackers in exchange for not publishing the data online. This type of incidents can have a direct impact on citizens in the form of e.g. identity theft or financial fraud (stolen credit cards) directly impacting the trust in the Digital Single Market (DSM).

Cyberattacks are also detrimental to innovation as the theft of IP and business confidential information has significant economic implications. A company investing in research and development expects a return on investment, which might be compromised as a result of a cybercrime.

According to the 2015 Eurostat survey on ICT usage in enterprises, the awareness among European enterprises related to cyber threats and the need to have a proper ICT security policy is growing, though there is still much room for improvement. In 2015, almost one out of three enterprises in the EU 28 had a formally defined ICT security policy. The share of large enterprises with such a policy was almost three times the share of small ones.[8]

This awareness is likely to be further boosted by the forthcoming Network and Information Systems Directive. The Directive is a first legislative step in 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 Member States to ensure that undertakings covered by the Directive to adopt risk management practices and report major incidents to the national authorities.

[5] http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html
[6] 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;
[7] http://ec.europa.eu/eurostat/documents/42577/3222224/Digital+economy+outlook+2015/dbdec3c6-ca38-432c-82f2-1e330d9d6a24
[8] http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises

II. Challenges & gaps hampering Europe's cybersecurity internal market

Challenges facing Europe's cybersecurity internal market

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 geographically fragmented, making it difficult for Europe's companies, especially SMEs, to compete on the European and global level on one hand; and for European citizens and enterprises it reduces the choice of viable and usable cybersecurity technologies (taking also into account the fundamental rights such as the right to privacy and data protection) that individuals in EU and enterprises have access to.

According to the Recommendations on Cybersecurity for Europe prepared by the European Cybersecurity Industry Leaders, the fragmentation of the European cybersecurity market is currently the main barrier to the creation of strong EU businesses in the field.[9]

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). [10] The EU suppliers, while showing a positive dynamism, remain mostly national or regional players.

This industry and geographical 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 beyond national borders.

The key market leaders in the cybersecurity field operating in Europe come from third countries, mainly the US. On the one hand, the presence of third country suppliers drives the competitiveness and innovation in the market;[11] on the other hand it is threatening to domestic companies, which due to the geographical market fragmentation in the EU, are unable to scale up their activities an become globally competitive through their domestic European market.

The difficulty to compete on the European and global levels often leads to mergers and acquisitions of Europe's SMEs by non-European actors, weakening the European sector and leaving Europe also more vulnerable and technologically dependent on others.[12]

Another challenge is the outflow of European know-how. The Global Cybersecurity Status Report indicates an alarming shortage of skilled cybersecurity professionals around the world. According to different estimates the demand for the cybersecurity workforce will rise to 6 million globally by 2019, with a projected shortfall of 1 - 1.5 million.[13] The situation is no

[9] Recommendations on Cybersecurity for Europe, A report to M Gunther Oettinger, European Commissioner for Digital Economy and Society, prepared by the European Cybersecurity Industry Leaders (Thales, Atos, Airbus Group, BBVA, BMW, Cyberentica, Deutsche Telekom, Ericsson, F-Secure, Infineon), January 2016 - https://ec.europa.eu/digital-agenda/en/news/commissioner-oettinger-receives-final-report-european-cybersecurity-industrial-leaders

[10] The European Network and Information Security Market: Scenario, Trends and Challenges - A study for the European Commission, DG Information Society and Media; 2009.

[11] Study on synergies between the civilian and the defence cybersecurity markets; IPACSO (2015) Market – Market Analysis – Trends and Challenges – Market Size

[12] See for example: Cyber Security M&A Decoding deals in the global Cyber Security industry, PriceWaterhouseCoopers, 2011

[13] http://www.isaca.org/cyber/Documents/2015-Global-Cybersecurity-Status-Report-Data-Sheet_mkt_Eng_0115.pdf; http://www.ksat.com/news/cybersecurity-workforce-shortage-millions-of-experts-needed

different in Europe. Although academic organisations are educating highly qualified and trained cybersecurity professionals, this talent is many a time not absorbed by the EU cybersecurity market.[14] 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.

Failing to stimulate a common European cybersecurity market and to create opportunities to grow for its companies would also be a missed opportunity for the European economic growth. The global cyber security market is expected to be among the fastest growing segments of the ICT sector in the coming decade with the average rate expected to grow by 7-8% a year over the next five years. Europe is the second largest regional market (27%) behind North America, which controls a large segment of the global market. Forecasts suggest that Europe's stake in the global cybersecurity market will fall to 23% by 2019 due to the predicted rise of other regions, particularly Asia Pacific.[15]

The geographical fragmentation of the market results in limited possibilities of achieving by Europe's companies 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 future NIS Directive, it is crucial that this market development opportunity is not confined by entry barriers between different EU Member States.

Gaps hampering good functioning of the European internal cybersecurity market

Insufficient level of trust for cross-border purchases

The lack of trust needed for cross-border purchase of cybersecurity products and solutions is one of key gaps resulting in geographic market fragmentation. 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.

Lack of efficient coordination mechanisms among cybersecurity ecosystem actors

[14] Study on synergies between the civilian and the defence cybersecurity markets; IPACSO (2015) Market – Market Analysis – Trends and Challenges – Market Size
[15] Idem

Whereas some initiatives across a few member states aim to bring together the competencies and industrial players in this area[16], potentially helping European companies to join forces and expand across a number of European countries, the gap is still considerable: the industry is nowhere near some more structured segments of the ICT industry, such as e.g. 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.

Insufficient dialogue between demand and supply side of cybersecurity products and solutions

There is also a clear need for more efficient mechanism of coordination between demand and supply side of cybersecurity products and solutions at the stage of research and innovation to allow cybersecurity providers to come up with solutions that are both trusted and sought by its potential customers. Currently there is no effective way to 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), which would allow to identify possible commonalities and allow to replicate solutions (which could be further adapted to individual needs), while achieving economies of scale.

So far 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 provided EU support to academic research and industry to test new waters, and develop solutions to better protect users. However the FP7 approach based on addressing cybersecurity through specific topics created challenges related to coordination of the research efforts, making it more difficult to respond to changing cybersecurity market needs and increase the competitiveness of the Europe's cybersecurity sector.[17]

Cybersecurity funding gap

While innovation is booming in Europe, the European Union still lacks the culture of investing in cybersecurity. There are many innovative SMEs in the field but they are often unable to scale up their operations due to the lack of easily available funding to support them in the early phases of development. In the recent public consultation conducted by the European Commission 75% of respondents stated they did not feel they had sufficient access to financial resources to finance cybersecurity projects and initiatives.[18] European companies have limited access to venture capital as well as little budget available for marketing to improve their visibility, or to deal with different sets of standardization and compliance requirements.

[16] See for example: https://www.thehaguesecuritydelta.com/news/newsitem/661-common-ambitions-strengthening-cooperation-between-european-security-clusters
[17] SWD(2016) 215
[18] SWD(2016) 215

Lack of a well-functioning mechanism ensuring trustworthiness & readability of cybersecurity products and solutions

Trustworthiness of acquired products and solutions is one of important features the buyers are considering. However, a simple claim that a product is secure is often not enough to ensure user's trust in it. At the moment, a number of security certification schemes for ICT products exist[19] in the European Union but they are effective only in a few Member States and the use of existing schemes is not actively promoted. An ICT vendor might need to undergo several certification processes in order to sell in several Member States of the European Union. In the worst case scenario, an IT product or service designed to fulfil the security requirements in one Member State cannot be placed on the market in another one. There is also a clear gap for sectorial industries (e.g. transport, energy, health, etc.), which do not have a solid and reliable scheme providing them assurance on the level of security of ICT components that they want to integrate in their systems.

In the recent public consultation of the European Commission almost 38% of respondents stated that the current ICT security certification schemes did not adequately support the needs of European industry (either supplying or buying cybersecurity solutions), compared to only 17.5% of respondents, who felt that the existing schemes were sufficient.[20]

The below graph presents the intervention logic to address the above mentioned gaps through contractual Public Private Partnership and other policy measures announced by the Communication "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry":

[19] E.g. Commercial Product Assurance in the UK, Certification Sécuritaire de Premier Niveau in France, Senior Officers Group for Information Systems (SOG-IS) covering 10 EU and EFTA countries - Austria, Finland, France, Germany, Italy, the Netherlands, Norway, Spain, Sweden and United Kingdom).

[20] SWD(2016) 215


Gaps
Objectives
Measures
Insufficient level of trust for cross-border purchase of cybersecurity products and solutions
Build trust among Member States and industrial actors
Through cPPP encourage cooperation at the early stages of innovation between Member States and industrial actors
Insufficient dialogue between demand and supply side of cybersecurity products and solutions
Help align the demand and supply sectors for cybersecurity products and services
Through cPPP create a space for a structured cooperation between demand and supply side
Seek synergies to develop common, sector-neutral technological building blocks that could be used across different sectors
Through cPPP encourage dialogue within specific sectors to identify synergies
Lack of efficient coordination mechanisms among actors of cybersecurity ecosystem
Enhance cooperation bewteen different cybersecyrity actors on regional and cross-border levels
contractual Public Private Partnership (cPPP) on cybersecurity
Cluster support measures
Lack of sufficient access to financing for cybersecurity SMEs
Encourage the cluture of investing in cybersecurity in Europe & ease access to finaning for cybersecurity SMEs
Awarness raising measures among cybersecurity community related to existing financing mechanisms
Work with regions to unlock existing funds for cybersecurity community
Lack of a well-functioning mechanism ensuring trustworthiness & readability of cybersecurity products and solutions
Create a well-functioning mechanisms ensuring trustworthiness & readability of cyberscurity products and solutions
Avoid potential market fragmentation caused by different/overlapping schemes
Develop with Member States, ENISA and industry a Roadmap towards the possible establishement of a European certification scheme
Contractual Public Private Partnership on cybersecurity
Accompanying measures

III. Current policy landscape in the field of cybersecurity

Given the development of threats to cybersecurity and cybercrime in recent years, the Commission has designed a coordinated policy in close cooperation with Member States and the other EU institutions, as well as with the industry and relevant stakeholders.

In 2013 the European Cybersecurity Strategy[21] was adopted and the EU sent out a strong massage that cybersecurity was a challenge that needed a European response and where European action could bring added value to activities carried out by Member States. This strategy set out a joint vision of the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy for "an open, safe and secure cyberspace".

The Strategy sets out five strategic priorities, which cover challenges that have both an EU-internal and an international dimension. Priorities relevant for this initiative relate to raising the level of protection and resilience of European networks and to developing industrial and technological resources for cybersecurity.

On network and information security, in line with the Strategy, the Commission proposed the first comprehensive piece of EU cybersecurity legislation, the Network and Information Security (NIS) Directive[22]. After three years of negotiations this piece of legislation is expected to be adopted soon and its implementation is expected to be a step-change in EU cybersecurity. The Directive will help improve the national cybersecurity capabilities across the EU, which are now uneven. Member States that need to improve their capabilities will be given the possibility to catch up with those who are best in class.

The forthcoming Directive foresees that each Member State establishes a dedicated incident response team to enable rapid reaction to cyber-threats and cyber-incidents. The cooperation between the Member States, which now takes place in limited circles, will also be enhanced.

The Directive also focuses on traditional, classical infrastructure: it provides for security and reporting obligations for companies managing critical infrastructure in key important economic sectors such as energy, transport and banking that use digital infrastructure to provide their service. Comparable obligations will also apply to key digital service providers.

In 2013 the Commission has also launched a public-private platform at EU level (so-called Network and Information Security (NIS) Platform) to identify good cybersecurity practices that organisations can implement in order to increase their resilience. These practices were expected to facilitate the future implementation of the NIS Directive, but are also relevant to a wide range of organisations that will not be covered by the Directive. The Platform gathered almost 600 stakeholders representing the business community, civil society, academia, researchers and member states. NIS Platform work has been divided into three sub-groups dealing with risk management; voluntary information exchange and incident coordination as well as secure ICT research and innovation.

Over the course of two years the working groups have developed a number of deliverables, including the Strategic Research Agenda, 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. It also proposed new ways to promote truly multidisciplinary research that foster collaboration among researchers,

[21] JOIN(2013) 1
[22] COM/2013/048

industry and policy makers. This has resulted in the publication of a Cybersecurity Strategic Research Agenda[23] (SRA) of the NIS Platform in the third quarter of 2015.

Apart from policy initiatives, the European Commission has been financing through FP7 and CIP (7th Framework Research Programme and Competitiveness and Innovation Programme) a number of cybersecurity projects. This support also continues under Horizon2020 Framework Programme.[24]

Other past and recent initiatives, worth noting, and which any future initiatives in the field of cybersecurity should build on include:

- On 27 April 2016 the reform of the Data Protection rules has been adopted[25] establishing a modern and harmonised data protection framework across the EU. It comprises Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR) and Directive (EU) 2016/680 on the protection of personal data by authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses. In particular, the GDPR regulatory framework asks for the implementation of security measures of processing appropriate to the risk, data breach notification, and a EU wide certification scheme.
- A Strategy for a Secure Information Society[26] adopted in 2006 in response to the urgent need to coordinate efforts for building up trust and confidence of stakeholders in electronic communications and services.
- A Communication on Critical Information Infrastructure protection (CIIP)[27] adopted in 2009 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[28] (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.
- The Digital Agenda for Europe[29] lists a set of appropriate measures, in particular on data protection in the Union, on network and information security and on cyber-attacks.
- The 2014 Communication, 'For a European Industrial Renaissance'[30], which 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 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 laid down the right foundations and a predictable legal framework for

[23] https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/strategic-research-agenda-final-v0.96/view
[24] SWD(2016) 210
[25] OJL 119, 4.5.2016.
[26] COM(2006) 251
[27] COM(2009) 149
[28] COM(2011) 163
[29] COM(2010) 245
[30] COM(2014) 014

people, companies (in particular SMEs) and public administrations to safely access to services and do transactions online and across border in just "one click".

As a result of the increasing pervasiveness of digital technologies in other industrial sectors, the relevance of cyber-security and privacy is well understood also in more sectorial policy area. The energy sector could be taken as good example:

- The 2011 Communication on 'Smart Grids: from innovation to deployment'[31] highlighted data protection and security as one of the five challenges for smart grid deployment and identified a number of measures to accelerate this deployment, including the 'privacy by design' approach and assessment of network and information security and resilience.
- The opinions of the Working Party on the protection of individuals with regard to the processing of personal data set up in accordance with Article 29 of Directive 95/46/EC, and the European Data Protection Supervisor's opinion of 8 June 2012 provide guidance to safeguard personal data and guarantee data security when data are processed in smart metering systems and smart grids. Opinion 12/2011 of the Working Party on smart metering recommends Member States to proceed with implementation plans which require a Privacy Impact Assessment.
- The Commission Recommendation 2012/148/EU sets out specific guidance on data protection and security measures for smart metering systems and invites Member States and stakeholders to ensure that smart metering systems and smart grid applications are monitored and that fundamental rights and freedoms of individuals are respected.
- Recommendation of 9 March 2012 "on preparations for the roll-out of smart metering systems" (2012/148/EU) underlines that in order to mitigate the risks on personal data and security, Member States, in collaboration with industry, the Commission and other stakeholders, should support the determination of best available techniques for each common minimum functional requirement listed in point 42 of the Recommendation.
- Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (2014/724/EU) states that Member States should encourage data controllers to consider as a complementary element to the Data Protection Impact Assessment, the Best Available Techniques process to enhance the level of cyber-security and privacy of smart-metering systems.
- In October 2014 the European Commission Smart Grid Task Force launched the Best Available Technique Process to identify the most effective techniques to enhance the level of cyber-security and privacy of the smart-metering system
- In October 2015 the Commission set up and coordinated an ad-hoc Energy Expert Cyber Security platform with the aim of defining a full-sector strategy on cyber security in energy

While progress has been made, in its Digital Single Market (DSM) Strategy[32] published on 6 May 2015 the Commission noted specific gaps that still existed in the fast moving area of technologies and solutions for online network security. The Strategy emphasised 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.

[31] COM(2011) 202
[32] COM(2015) 192

The Commission also noted that more coordinated action aimed at supporting the development of an industrial strategy for cybersecurity is still missing. Such action could stimulate the take-up and the supply of secure ICT solutions in Europe. This is crucial as a high level of network and information security and of public safety online across the EU is essential to ensure consumer confidence and to keep the online economy running. This will, in turn, preserve the functioning of the Internal Market and will boost growth and jobs in the European cybersecurity industry.

IV. Towards strong European cybersecurity industry – Policy Options

In view of challenges and gaps to increasing the competitiveness of the Europe's cybersecurity industry and improving the functioning of Europe's internal cybersecurity market, the EU action is needed to achieve a single market in this field, which is also a prerequisite for the success of the Digital Single Market Project.

Taking into consideration the objectives set in the accompanying Commission Decision establishing the Contractual Public Private Partnership (cPPP)[33], accompanying Staff Working Document assessing the implementation and participation in the EU Trust and Cybersecurity RTD an innovation programme funded by FP7 and CIP grants (2007-2013)[34], the European Commission services have considered the below three scenarios related to enhancing cybersecurity industry in Europe.

The suggested options have been carefully chosen following analysis of the evidence coming from various sources including cybersecurity market studies as well as the contribution of more than 250 different organisations representing both the supply and demand side of the cybersecurity industry to the public consultation conducted by the European Commission[35].

Scenario 1: Business as usual

This scenario assumes continuing business as usual, without enhancing cybersecurity industry policy. The scenario focuses on continuing to finance cybersecurity projects within Horizon2020 research and innovation programme, without putting additional effort to streamline this research and conduct it against a commonly agreed Strategic Research Agenda for cybersecurity.

So far 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.

These projects provided EU support to academic research and industry to test new waters, and develop solutions to better protect users. They have 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

[33] C(2016) 4400
[34] SWD(2016) 210
[35] SWD(2016) 215

capacities of the digital security and privacy industry in Europe. The participation of innovative SMEs has been relatively limited (around 10%). Also, in the meantime new trends in digital technologies and cyber have emerged (social engineering, hybrid threats, complex attacks). A more detailed evaluation of the FP7 programme can be found in the Commission Staff Working Document: An assessment of the implementation and participation in the EU Trust and Cybersecurity RTD and innovation programme funded by FP7 and CIP grants (2007 - 2013).[36]

Horizon2020 envisages that half a billion Euro of EU R&I funding will support research and innovation in this area over the period 2014-2020. 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).

However, these efforts, due to the lack of a sufficient and structured dialogue between the supply and demand side of cybersecurity products and solutions, are not likely to address the gaps identified. Without creating the conditions for a continuous dialogue between the demand and supply side, it is difficult to define synergies allowing European cybersecurity industry to come up with solutions that could be replicable and lead to economies of scale. For the same reasons, the research projects on their own are not likely to contribute to creating the increased level of trust between different stakeholders, especially between public authorities and the industry.

At the same time research and innovation projects alone, even if created through a very close cooperation between the demand and supply sides, are not likely to address issues related to market fragmentation (e.g. the lack of standards, multitude of certification schemes), nor to industry fragmentation (e.g. the scarcity of clusters and cross-border centres of excellence, challenges related to access to financing, etc.).

Therefore continuing business as usual would maintain the status quo of largely national approaches and would not serve creating 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 reduced 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.

[36] SWD(2016) 210

Scenario 2: Stimulate European cybersecurity industry competitiveness through innovation

The establishment of the contractual Public Private Partnership (cPPP) on cybersecurity would plant the seed for mid-term innovation and long term competitiveness of Europe's cybersecurity industry. This option would limit the Commission's action to the cPPP.

A. Options for addressing Cybersecurity R&I

When considering the different kinds of instruments at its disposal, the Commission had the following options:

I. NIS Platform

While the role of building trust among different stakeholders (not only cybersecurity industry representatives) is partly fulfilled by the NIS Platform (NISP), the focus of this forum is on the support for the forthcoming NIS Directive implementation (risk management practices, incident notification, exchange of best practices, etc.). While building on some of the work done by the NISP (e.g. the Strategic Research Agenda), the EU cybersecurity industry representatives consulted by the Commission on a number of occasions[37] expressed a clear need for creating a more structured platform representing the cybersecurity industry as such, which would allow it to take up a continuous dialogue with the demand side and translate it into concrete projects linked to available research and innovation resources. While NIS Platform was ruled out as a principle instrument to achieve the objectives of this initiative, efforts will be made to ensure synergies with its work, whenever relevant. In particular, the NIS platform could be used to identify clear needs and potential market opportunities by the cybersecurity industry.

II. Joint Technology Initiative

A joint-undertaking (JTI) was a possibility to support the research and innovation objectives of this cybersecurity initiative. However, JTI is a complex instrument and the cybersecurity initiative is coming in the middle of the Horizon2020 programming.

Setting up JTI in the middle of H2020 would have required renegotiating the current H2020 Regulation[38]. Obtaining financial commitment from Member States to contribute to a JTI on cybersecurity would also have been difficult within such a short timeframe, especially in view of current budgetary constraints of many Member States.

While time and budget constraints ruled out the use of a JTI at this stage, this might be an option to explore with Member States for the next Framework Programme of Research and Innovation beyond H2020.

[37] See SWD(2016) 215
[38] https://ec.europa.eu/programmes/horizon2020/

III. Contractual Public Private Partnership

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

The preferred option for the research and innovation aspects was the contractual PPP[39], also reflected in the Digital Single Market Strategy[40].

Building on the success of the previous contractual Public Private Partnerships and in view of the need of not only streamlining the research but also helping the industry to create sustainable pan-European structure for cooperation both within the industry and with the demand side, this scenario assumes establishing a contractual PPP on cybersecurity.

The EU research framework programme Horizon2020 allows for the implementation through public-private partnerships (PPPs) in the case of research and innovation activities of strategic importance to the Union's competitiveness and industrial leadership, or to address specific societal challenges.

Contractual PPPs follow the Horizon2020 rules and procedures, with industry providing key advice on research priorities. The contractual arrangement forming the basis for each contractual PPP is concluded by the EU, represented by the European Commission and representatives of the respective industry grouping. It specifies the partnership's objectives, commitments, key performance indicators and expected outputs. Each contractual arrangement mentions an indicative budget.

For a cPPP to be supported under Horizon2020, it must prove that the results will provide added value at the EU level and boost both industrial competitiveness and sustainable growth. It must also have a convincing long-term roadmap for research and innovation activities. The roadmaps commit the private side of each PPP to a shared vision and clear, quantifiable objectives. Crucially, the involvement of industry ensures that the research and innovation planned meet industry's needs.

In view of the previous experience, the cPPP on cybersecurity is the right instrument in the research and innovation field to help achieve both supply and demand side objectives through:

- **Building trust among Member States and industrial actors by fostering bottom-up cooperation** on research and innovation at the early stages 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.
- **Seeking synergies to develop common, sector-neutral technological building blocks with maximum replication potential** (e.g. encrypted storage and processing,

[39] 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 European Commission 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 be delivered, including the identification of research and innovation activities that require support from Horizon 2020.

[40] COM(2015) 192

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.

- **Engaging 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 forthcoming NIS Directive in some cases) to define common digital security and privacy requirements for their sector.

  The cPPP could also be one of the **mechanisms to implement the DSM Priority Standardisation Plan**

The cPPP will allow maximising the use of available funds through better coordination with Member States and better focus on a few technical priorities.

The cPPP should leverage funding from Horizon2020 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.

The technical priorities were defined based on the Strategic Research Agenda developed by the NIS Platform published in September 2015[41]. This document identified the key challenges and desired outcomes in terms of innovation-focused, applied research as well as of cybersecurity. It proposed new ways to promote truly multidisciplinary research that fosters collaboration between researchers, industry and policymakers, and recognised the difficulties faced by some segments, such as SMEs in engaging with traditional research mechanisms.

The SRA was the result of more than a year's work by the Working Group on Secure ICT Research and Innovation (WG3) of the Network and Information Security (NIS) Platform launched by the European Commission in spring 2013 and gathering actors from the industry, research/academia and public authorities. The NIS Platform SRA was then further tailored by the industry to match the goals of the contractual PPP and available resources.

The Strategic Research and Innovation Agenda presented by the Industry enlists the following technical priorities:

- Assurance and security / privacy by design
- Identity, access and trust management (e.g. Identity and Access Management, Trust Management)
- Data security (e.g. data protection techniques, privacy-aware Big Data analytics, secure data processing, secure storage; user empowerment, operations on encrypted data)
- Protection of the ICT Infrastructure (Cyber Threats Management, Network Security, System Security, Cloud Security, Trusted hardware/ end point security/ mobile security)
- Cybersecurity services (e.g. auditing, compliance and certification, risk management, cybersecurity operation, security training services)

The Industry's SRIA mentions also a number of non-technical areas where action is needed:

- Education, training, skills development

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

- Fostering innovation in cybersecurity:
    - Development of a cybersecurity ecosystem
    - Defining the cybersecurity value chain
    - Boosting SMEs
    - Bottom-up Track for Cybersecurity Innovation
- Standardisation, regulation and certification
- Societal aspects

The development of open source software and open standards (e.g. for exchanging threat information) can help foster trust, transparency as well as disruptive innovation. Well-administered open source portals and the communities behind it (including ethical hackers) are a great source for SMEs and start-up to build secure IT infrastructure with a low entry cost. The contribution of such communities to the cybersecurity cPPP should therefore be encouraged, also in view of bringing disruptive innovation. The output of research and innovation projects should also participate to the sustainability of a well-maintained open source ecosystem.

The cPPP will be implemented in an open and transparent manner. It will be supported by the "European Cybersecurity Organisation" Association (ECSO). A detailed description of the governance structure, Strategic Research Agenda and key performance indicators of cybersecurity cPPP can be found in the Industry Proposal and Strategic Research and Innovation Agenda[42], which is part of the package presented by the European Commission.

Scenario 3: Stimulate European cybersecurity industry competitiveness through innovation & supporting measures

While the establishment of the cPPP will plant the seed for mid-term innovation and long term competitiveness of European cybersecurity industry, it will not allow, on its own, to overcome internal market challenges within cybersecurity sector. This is why, following a thorough analysis and consultation process with stakeholders, the Commission, in the DSM Strategy decided to further look into additional measures. This policy option assumes a comprehensive approach to nurture a European-grown cybersecurity, including setting up a contractual Public Private Partnership on cybersecurity as well as implementing a set of well-targeted and actionable accompanying measures to overcome the challenges of cybersecurity internal market in Europe. Ultimately, this approach should 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.

A. Scale up investment & industrial cooperation in Europe

Supporting the development of globally competitive clusters/centres of excellence

With the strategic goal of creating growth and jobs, the European Union has been looking with growing interest into solutions allowing industries, technologies, academia and other

[42] See the Industry Proposal at https://ec.europa.eu/digital-single-market/en/

stakeholders cooperate in new, efficient ways. Economic clusters, which can be broadly defined as "*a group of firms, related economic actors, and institutions that are located near each other and have reached a sufficient scale to develop specialised expertise, services, resources, suppliers and skills*"[43] can be a natural starting point to look for such cross-linkages.

While working together SMEs can be more innovative, create more jobs and register more international trademarks and patents than they would alone. Belonging to a cluster enables the involved companies to improve their competitiveness and thus achieve a higher performance, mainly by increasing the productivity through better access to specialised suppliers, technology and information, and higher innovation potential of cooperating companies. This is due to the transfer of knowledge within the Cluster, the generation of new ideas and the higher pressure on innovation and expansion of the Cluster.[44]

Clusters are predominantly a market-driven phenomenon. Most successful clusters are created spontaneously as a result of natural competitive advantages, market forces or simply by chance. However, owing to dedicated cluster policies in Member States, notably since the end of the 1990s, there are an increasing number of cases where forward-looking public policies, business initiatives or top-class universities and research institutes have been instrumental in the emergence of strong clusters by acting as a catalyst and helping to unleash the economic and scientific potential of particular regions.[45]

In this context, in the European Union the majority of clusters focusing on cybersecurity can be found in Western Europe (e.g. G4C in Germany, Malvern Cluster in the UK, which success encouraged the government to support the development of 17 regional cybersecurity clusters, Pôle d'Excellence Cyber in France, the Hague Delta Cluster in Netherlands or INCIBE in Spain), although some initiatives start appearing also in the Central and Eastern Europe e.g. in the Czech Republic and Estonia.

Cybersecurity community views on clusters as a supporting instrument

In the recent public consultation on cPPP and possible accompanying measures the majority of respondents to this open question stated that clusters can be an effective cybersecurity industry supporting tool. They are seen as crucial stimulus for start-ups, universities and research institutes to find cross-linkages between them as well as with traditional industries. Some respondents also see clusters as a useful policy tool, which can help achieve a common understanding of cybersecurity challenges - a necessary prerequisite for developing cybersecurity policies. Some respondents felt that using inter-cluster synergies, complementarities and exchanging best practices could help leverage European expertise both to EU citizens and businesses.

At the same time, many respondents saw the need to improve the functioning of existing clusters, mostly referring to the need of better coordination on the regional level but also within the European Union and beyond. Insufficient coordination leads to both duplication of efforts and differences in how cyber-security issues are approached across Europe.

43 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Towards world-class clusters in the European Union: Implementing the broad-based innovation strategy, COM(2008) 652; http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52008DC0652R(01)

44 http://ec.europa.eu/growth/smes/cluster/index_en.htm

45 Idem

The development of skilled work force, transfer of knowledge, mapping of innovation products and services, and security awareness rising were among ideas spontaneously mentioned by respondents as further goals of clusters, in addition to stimulating innovation and competiveness of the industry.[46]

European Union's instruments to support cluster development & SMEs

Cluster programmes in Europe aim at increasing innovation capabilities and competitiveness of local and regional actors, with a special focus on SMEs. This policy, actively developed since 2008 brings tangible results - according to the European Cluster Excellence Scoreboard[47], for a number of selected emerging industries[48] and regions in the period 2010-2013, 33.3 % of firms in clusters showed employment growth superior to 10%, as opposed to only 18.2% of firms outside clusters.

The EU cluster policy has been evolving over the past ten years, from a horizontal approach of having cluster initiatives available in all industrial sectors, to today's focus on important industrial sectors of high relevance on political agendas, with a special attention given to emerging industries. It has also become clear that it is essential to enable cross-sectorial collaboration between cluster actors from different industries. In its 2014 Communication 'For a European Industrial Renaissance[49]' the European Commission highlighted that clusters can facilitate such cross-sectorial and also cross-border collaboration, helping SMEs to grow and internationalise[50].

The cybersecurity industry could take advantage, among others, of the following cluster instruments and programmes:

- Policies, programmes and activities supporting clusters in the emerging industries e.g. the Horizon2020 action for 'Cluster facilitated projects for new industrial value chains'[51] (the action kicked off in 2015 with a budget of 24.9 million from the Innovation in SMEs work programme, annual calls of 16 million and 18.5 million will be announced in 2016 and 2017 respectively); The programme promotes cross-border and cross-sectorial collaboration, innovation and entrepreneurship across different regions and value chains, with a special focus on SMEs in emerging industries;
- The European Cluster Observatory[52] that provides information, mapping tools and analysis of EU clusters and cluster policy with a particular focus on emerging industries;
- Instruments supporting internationalization of clusters:
    - **European Cluster Collaboration Platform (ECCP)[53],** which facilitates cluster cooperation within the EU and helps clusters access international markets. This instrument allows European cluster organisations profile themselves, exchange experience and search for potential partners for transnational cooperation;

[46] SWD COM(2016) 215
[47] http://www.emergingindustries.eu/scoreboard.aspx
[48] Emerging industries are new industrial sectors or existing industrial sectors and value chains that are evolving into new industries
[49] COM(2014) 014
[50] Cluster Programmes in Europe, September 2015: http://ec.europa.eu/DocsRoom/documents/12925
[51] http://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/main/h2020-wp1415-sme_en.pdf
[52] http://ec.europa.eu/growth/smes/cluster/observatory/index_en.htm
[53] http://www.clustercollaboration.eu/

- **European Strategic Cluster Partnerships for going International** – an instrument helping international cluster cooperation in new areas, notably in support of emerging industries. These partnerships encourage clusters from Europe to work together to exploit synergies and develop a joint 'European' strategic vision with a global perspective and common goals towards specific third markets. Within this action a non-funded Partnership in the cybersecurity area called G2CS (Gateway to Cyber Security Solutions in Europe) is planned under COSME Programme.
- Forthcoming **COSME[54] 2016 Cluster Internationalisation Programme** with a strand on dual use security supporting the targeted establishment of *European Strategic Cluster Partnerships for going International* in this area. Within this programme two Partnerships will be reserved for the Defence and Security sector. The aim will be to support European defence-related clusters to intensify collaboration across borders with other non-defence industrial clusters and to develop and implement joint strategies in areas of dual use technologies, products and services towards non-EU countries.

- Instruments **supporting cluster excellence** by providing methodology and trainings for cluster organisations to improve their internal management process services offer[55].

The cluster support tools should be also seen in the wider context of Smart Specialisation – a strategic approach to economic development ensuring synergies between Horizon2020 and the European Structural and Investment Funds (ESIF) in the interest of regions. Applying this approach to cybersecurity field by involving regions, regional clusters and representatives of the cybersecurity sector can help unlock the full potential of available funds.

Building on previous experiences, the process of finding synergies and unlocking regions' potential in cybersecurity would involve:

1. **Interregional knowledge building -** mapping and matchmaking potential partners combining information from different sources starting from the EYE-RIS3 database, in which 19 regions have self-identified themselves as having research and innovation strategies for smart specialisation (RIS3) priorities in the domain of **of Trust and CyberSecurity.**
2. **Connecting key stakeholders - identifying lead regions for each priority area** as well as other participating regions. Map actors and regional ambitions and challenges and available funding and synergies among funding sources and identification of new domains of co-investments. This can be followed by an info day (and or a series of events located in MS) open to regional and national authorities as well as other actors interested in taking part in a such Platform to jointly align priorities, investment efforts and innovation support activities in this thematic area. The objective is to learn about ideas for joining forces with other regions in this area but also to have a joint declaration of intent. (see the example of the declaration of the Vanguard initiative[56])
3. **Facilitating demonstration projects of practical collaboration** in the field of research and innovation (this can include e.g. aligning infrastructure to share common

[54] Programme for the Competitiveness of Enterprises and Small and Medium-sized Enterprises
[55] http://ec.europa.eu/growth/smes/cluster/excellence/index_en.htm
[56] http://www.s3vanguardinitiative.eu/sites/default/files/contact/image/final_declaration_of_milan_final_27_10.pdf

facilities– interoperability issues – testing - product development – coordinate public procurement) and bringing new product to the market.

Taking advantage of ESIF funds can be also facilitated if the process of streamlining cybersecurity in strategic and operational documents of ESIF in the Member States and regions interested in investing in the development of cybersecurity industry.

In addition to ESI funds, there are a number of other instruments that could facilitate access to financing and boost investment in the cybersecurity field e.g. the European Fund for Strategic Investment (EFSI) – an initiative launched to help overcome the current investment gap in the EU by mobilising private financing for strategic investments and SMEs. EFSI provides support to individual projects but also to Investment Platforms (a number of investment projects with a thematic or geographic focus) in the form of equity and quasi-equity investments, loans, guarantees to projects and counter-guarantees to intermediaries.[57]

EFSI support is accompanied by additional tools - the European Investment Advisory Hub (EIAH) providing a single access point to wide ranging advisory support for projects and investments engaging with public and private promoters at all levels of the project cycle, from upstream project identification, through to planning and preparation to implementation; and the European Investment Project Portal (EIPP) enabling EU based project promoters – public or private – to reach potential investors worldwide.[58]

Another instrument, which aims to improve access to finance for SMEs is the aforementioned Programme for the Competitiveness of Enterprises and Small and Medium-sized Enterprises (COSME). Through the Loan Guarantee Facility COSME funds guarantees and counter-guarantees for financial intermediaries (e.g. guarantee organisations, banks, leasing companies) to help them provide more loan and lease finance to SMEs. COSME targets companies, who have 10 or fewer employees with an average guaranteed loan of about €65,000. Another part of the Programme – The Equity Facility for Growth (EFG) is dedicated to investments in risk-capital funds that provide venture capital and mezzanine finance to expansion and growth-stage SMEs, in particular those operating across borders. A call for expression of interest for both parts of COSME Programme has been launched and is open until 30 September 2020.[59]

While eligible to benefit from the above mentioned and other support mechanisms, so far the cybersecurity industry in Europe has not yet taken advantage of them to any greater extent.

B. Improve readability & trustworthiness of security levels for public & private buyers

We are witnessing an increase in cybersecurity risk spanning across many sectors due to the increased use of public communication networks such as the internet but also mobile communication networks, the pervasiveness and reliance on ICT products within public and private critical sectors and finally the need to ensure at least the same level of safety in those cases where connectivity may introduce previously unaccounted for security risks (e.g. medical devices, smart meters, connected cars).

[57] EFSI Steering Board Rules Applicable to Operations with Investment Platforms or Institutions: http://www.eib.org/attachments/strategies/efsi_steering_board_rules_applicable_to_operations_with_investment_platforms_and_npbs_or_institutions_en.pdf

[58] European Structural and Investment FUNDS and European Fund for Strategic Investments complementarities : http://ec.europa.eu/regional_policy/sources/thefunds/fin_inst/pdf/efsi_esif_compl_en.pdf

[59] http://ec.europa.eu/growth/access-to-finance/cosme-financial-instruments/index_en.htm

In this context, ICT products need to be secure. However, just to claim that a product is secure is not an enough proof to provide trust for the user of this product. More formal processes may be needed to check the security of an ICT Product and to maintain a chain of trust from the manufacturer (Automatic teller machine, smartphone) to the operator (banks, telecommunication) and to the final end-user. To satisfy the need of trust in the security of the ICT products, industry and/or public authorities may rely on security certification.

By proving evidence that a product will perform its stated security functions or that it meets a given minimum set of security requirements, security certification of ICT products, can thus contribute significantly to reinforcing our trust in that product and increasing the security of digital services.

Security Certification can also improve the attractiveness of European ICT products in a global market where individuals, private companies and public procurers increasingly seek assurances that the ICT products they purchase are secure.

However, security certification of ICT products does come at a cost both in terms of the financial resources as well as the time necessary to successfully complete the process. In some cases, security certification may represent a barrier to entry for some vendors, notably for Small and Medium-Sized Enterprises as well as lead to market inefficiencies and fragmentation.

The benefits and costs, the opportunities and the risks associated with ICT Product Security Certification are further discussed below.

With a view to the Single Market, the effects, either positive or negative, that security certification may have on the market for ICT products, and especially the risk of fragmentation, deserve our particular attention.

ICT Product Security Certification and Certification Schemes

To better understand the role of ICT Product Security Certification, it is important to first point out the positive effects that security certification may have in the market, on the digital society at large and, finally, for individual European citizens.

There are well recognised benefits associated with ICT Product Security Certification.

Improving the Market for ICT Products - The security properties of an ICT product are a quality dimension which is difficult to assess for an end user prior to purchase. An end user does not have all the necessary information to make a sound judgement on which product is more secure. This is a typical case of information asymmetry which is commonly considered a condition leading to market failure. IT security certification, by providing an independent and trustworthy testament as to a product's security properties, can therefore play a major role in reducing the aforementioned information asymmetry and lead to an overall improvement in the market for secure ICT products for end users as well as vendors of "truly" secure products.

Reducing Cybersecurity Risk - From a cybersecurity risk perspective, ICT products that are insecure or vulnerable to attacks increase the overall cybersecurity risk that an organisation faces and they can generate cascading effects in the ICT infrastructure where the IT products are deployed. In the context of a cybersecurity risk management process, ICT security certification, by empowering end users to confidently identify, purchase and deploy secure ICT products in their organisations, contributes therefore significantly in the reduction of the overall cybersecurity risk.

Ensuring Safety - Another important emerging aspect related to ICT security Certification is related to how an ICT security incident could impact safety-critical systems (systems whose failure could endanger human life, lead to substantial economic loss, or cause extensive environmental damage). A good example is that of medical devices where cybersecurity is already being considered in the on-going review of the Medical Device Directive. Other examples are transport, energy generation, transport and distribution, telecommunications, and the management of water systems. In all these areas which are becoming increasingly digital and interconnected, an ICT failure due a security incident may lead to extensive disruption of normal activities and possibly endanger human life. ICT product security certification can contribute to reducing the risk of such an incident. How future sectorial safety-relevant regulations and standards address cybersecurity threats is important area of investigation.

As mentioned in the introduction to this section, despite the aforementioned benefits, ICT Product Security Certification also presents notable costs and risks. In particular, certification must address the dynamic nature of the ICT system where security products are implemented and deployed. In addition, security properties are not easy to compose. In other words, a system composed by secure components certified for a specific property (e.g., confidentiality) does not guarantee that the composed system will also support this property. In order to understand how to balance the costs and benefits, a brief overview of the key concepts and actors is necessary.

Conformity assessment is carried out by the manufacturer or service provider in order to demonstrate the conformity of its product/service to the applicable requirements. If required by the relevant legislation applying to the product/service a third body (conformity assessment body) is involved in the conformity assessment process. In any case the responsibility of demonstrating conformity is always with the manufacturer or service provider.

The horizontal EU framework for conformity assessment is laid down under Regulation765/2008[60] and Decision 768/2008. The framework provides for accreditation of conformity assessment bodies by the national accreditation bodies of the Member State they are legally established.

So, seeing as ICT Security Certification may be considered as a particular example of what is generally known as conformity assessment, it makes sense to rely upon relevant EU legislation for the definitions of important concepts. In this case, unless otherwise indicated, the definitions below are taken from Regulation 765/2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.

Security Requirements - ICT Security Requirements describe functional and non-functional requirements that need to be satisfied in order to achieve the security attributes of an ICT product. Security requirements can be formulated on different abstraction levels. At the highest abstraction level they basically just reflect security objectives. An example of a security objectives could be "The system must maintain the confidentially of all data that is classified as confidential". In the context of ICT security certification, it is important that the security requirements are transparent i.e. the vendor and the end user must both be aware of these requirements.

[60] Regulation 765/2008 is presented in more detail below

Conformity assessment - The process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled.

Conformity assessment body - A body that performs conformity assessment activities including calibration, testing, certification and inspection.

Accreditation – "Accreditation" shall mean an attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectorial schemes, to carry out a specific conformity assessment activity. Accreditation is a public authority activity.

Mutual Recognition Agreements (MRA) - are established between parties and are based on the mutual acceptance of certificates, marks of conformity and test reports issued by the conformity assessment bodies of either party in conformity with the legislation of the other party.

ICT Product Security Certification Schemes[61]

A certification scheme, for the purposes of this document, is an organisational structure that encompasses all the actors and activities necessary for well function ICT Product Security Certification to take place. These include[62]:

- Establishing the security requirements for ICT products (standards and technical specifications including the evaluation methodology);
- Deciding if conformity assessment bodies have to be involved or not;
- Conformity assessment procedures (such as the one set out in the horizontal menu of Regulation 768/2008/EC), selecting the most appropriate ones for the sector.

A typical IT Product Security Certification Scheme will foresee therefore the existence of the following three elements:

- Possible legislative requirement for products/services;
- Relevant harmonised standards;
- Conformity assessment procedures (such as the one selected from horizontal menu of Regulation 768/2008/EC);
- If required, involvement of Conformity Assessment Bodies (private actors).

Voluntary vs Regulated Schemes

It should also be noted that there are three main types of schemes as regards the role of policy makers and regulators[63].

Non-regulated conformity is both initiated and implement by private actors. The state plays no significant role.

Regulated conformity is initiated by laws which are brought forward by the state. It is still implemented by private actors (manufacturers, conformity assessment bodies) but according to the legislative provisions.

[61] Examples of various ICT Security Certification Schemes have been included in the Annex to this document
[62] CRISP Project - Evaluation and Certification Schemes for Security Products - Report on security standards and certification in Europe - A historical/evolutionary perspective: http://crispproject.eu/wp-content/uploads/2014/10/CRISP_Deliverable_2-1_Sec_Standards_Certification_Europe-Compressed.pdf
[63] CRISP Project

Co-Regulated: The criteria supporting the certification scheme as well as the procedure are bought forward by national public authorities or EU institutions; conformity of private actors is initiated on a voluntary basis.

The use and applicability of non-regulated or regulated schemes may depend on several factors including the perceived level of cybersecurity risk of the activity or ICT product category (including the political sensitivity of a specific market e.g. defence procurement), the particular market structure, the existence of related legislation (a prerequisite for regulated schemes).

Overcoming the challenges to ICT Product Security Certification in the Single Market

As mentioned in the introduction to this section, despite the many benefits, there are two important challenges at European level associated with ICT Product Security Certification. The first is the risk of market inefficiencies and fragmentation in case of diverging national schemes. The second is the need to increase both the efficiency and effectiveness of security certification schemes.

Reducing market inefficiencies and risk of fragmentation of the Single Market

Having defined in the previous chapter the key components that make up an ICT Product Security Certification Scheme, it is now easy to identify the reasons behind inefficiencies in the market for certified ICT products as well as a risk of market fragmentation.

Inefficiencies as well as fragmentation may appear in "regulated" (see previous chapter) certification schemes and in particular when the scheme is national i.e. one member state defines the standards and evaluation methodology used by the scheme while recognising as accredited only those certification bodies within its own territory.

In such a scenario, an ICT vendor will have to undergo the national certification scheme that corresponds to each individual market greatly increasing the incurred costs.

In another scenario, when the certification requirements affect the ICT product design itself, a problem of interoperability also arises: an ICT product designed to fulfil the requirements of one Member States will not be able to be sold in the market of another, especially in regulated markets.

Market inefficiencies and fragmentation could be overcome by EU Member States by:

1) making use of European (or international) standards;
2) agreeing to the maximum extent possible on common security requirements;

The above principles and the existence of an EU-wide framework are especially relevant in cases where the security requirements are based on legislative acts., Diverging Member State national requirements does lead to hampering the free movement of ICT products and services in the EU which implies a de facto fragmentation in the Digital Single Market while possibly this may be perceived as Technical Barriers to Trade in the light of the World Trade Organisation. The use of European Standards and even international standards to express security requirements and, to the extent possible, mutually recognised evaluation methods reduces the risks of market fragmentation and restrictions to trade.

Finally, Mutual Recognition Agreements[64] have allowed to build trustworthiness in ICT Products among the countries that signed up for the scheme, while keeping markets open.[65]

Improving Efficiency and Effectiveness

The efficiency and effectiveness of a Certification scheme may be determined by the quality of previously described elements, namely the security requirements, the evaluation methodology and the certification bodies themselves.

To improve the effectiveness of the security certification, the security requirements should correspond to the real operating environment of the product and appropriately take into account current or new cybersecurity threats.

Another factor that needs to be taken into account is the fact that testing a given product for vulnerabilities can only produce relatively short-lived test results, as attackers and security researchers continuously discover new ways of attacking systems and vulnerabilities in components used in products. Current and emerging trends in software and hardware development models and ICT lifecycle management should be taken into account.

To improve efficiency, security requirements as well as the assurance level should be appropriate to the risk presented to allow for a meaningful certification which is efficient in terms of cost/time and effective in terms of addressing real threats.

Gains in efficiency may also be sought in widening the scope of applicability of the certification scheme or elements thereof.

Under Regulation 765/2008[66], the essential requirements determine, amongst others, "the hazards to be dealt with". In the specific context of security requirements, we may thus conclude that determining the security requirements will depend on the specific security threats that an ICT product will face in the environment in which it is expected to operate while being used as intended. In fact, the certification of an IT product may be valid only in a specific context or specific set of applications.

However, with the prevalent reuse of commercial, not tailor-made ICT components across many industries and in many scenarios, it may be possible to identify a set of common security requirements and certification needs. The development or uptake of common standards and evaluation methodologies can contribute significantly to the reduction of the resources necessary both in terms of time cost. Still, common standards and methodologies may be sector specific and an analysis should be conducted to evaluate the cross-sector usability.

Furthermore, the "reuse" of institutional elements of certification schemes such as Accreditation processes and Mutual Recognition Agreements can further increase the overall efficiency of ICT Product Security Certification in the Single Market.

A Roadmap towards improving the European ecosystem for ICT product security certification

Moving forward, it should be noted and seriously taken into account that ICT security certification touches upon Member States cybersecurity political sensitivities.

[64] E.g. the Senior Officers Group for Information Systems (SOG-IS) MRA, which is detailed further below.
[65] Security Certification of ICT Products has been developed outside the context of 765/2008 and therefore MRAs between a subset of EU Member States as well as Norway are still in use. See, for example the Senior Officers Group for Information Systems (SOG-IS) Mutual Recognition Agreement.
[66] See Annex to this SWD

Gradually building consensus should therefore be a common attribute in all the EC's activities in this area. Among the themes that need to be explored further are the following:

- Lay down the requirements for ICT security. How to further harmonize the use of security certification requirements in public procurement and within the context of conformity assessment of goods and market surveillance in the EU.
- How to ensure, in a cost efficient and effective manner, the appropriate level of security of ICT products in Europe while continuing to benefit from open global markets.
- Work towards a European label[67], i.e. a seal of trustworthiness of European ICT products with a view to promote and facilitate the sales of European ICT products on a global market.

[67] Note that Regulation 765/2008, Dec 768/2008 provides for CE Marking a sign of conformity and forbid other markings/labels that overlap with the CE Marking.

V. Annexes

A. Certification – explanatory note

I. National and international ICT Security Certification Schemes – some examples

Commercial Product Assurance (CPA)[68] – UK

CPA evaluates commercial off-the-shelf products and their developers against published security and development standards. A security product that is successfully assessed is awarded Foundation Grade certification. This means the product has been proved to demonstrate good commercial security practice and is suitable for lower threat environments.

CPA certification is valid for 2 years and allows products to be updated during the lifetime of certification as vulnerabilities and updates are required. Products are tested against CPA Security Characteristics, so vendors are aware of the assessment criteria to develop against and data owners can be confident that certified products have been tested against CESG standards.

CPA is open to all vendors, developers and suppliers of security products with a UK sales base. Foundation Grade assessment is carried out by independent approved CPA test labs. The product vendor should contact a lab to initiate product testing and agree terms.

- There is no Mutual Recognition Agreement (MRA) for CPA, which means that products tested in the UK will not normally be accepted in other markets.

Certification Sécuritaire de Premier Niveau (CSPN)[69] – FR

The CSPN is an IT Security Certification Scheme established by the National Cybersecurity Agency of France (Agence nationale de la sécurité des systèmes d'information – ANSSI) in 2008. Its main purpose is to offer a faster and cheaper alternative for IT Security Certification as compared to the Common Criteria (see below) approach.

CSPN evaluations follow a "black box" testing approach within a limited amount of time. It is therefore necessarily less rigorous and targeted to low threat environments.

The security criteria as well as evaluation methodology and process are based on an ANSSI created standard which is available on the Agency's website.

Finally, the CSPN mostly covers IT security products such as Anti-Virus, Firewalls Access Control Mechanisms, and Secure Storage Devices. It can also be applied to hardware or embedded systems.

- There is no Mutual Recognition Agreement (MRA) for CSPN, which means that products tested in the FR will not normally be accepted in other markets.

Common Criteria Recognition Arrangement

The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM)

[68] https://www.cesg.gov.uk/scheme/commercial-product-assurance-products-foundation-grade
[69] http://www.ssi.gouv.fr/administration/produits-certifies/cspn/

are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that:

Products can be evaluated by competent and independent licensed laboratories so as to determine the fulfilment of particular security properties, to a certain extent or assurance;

Supporting documents, are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies;

The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation;

The CCRA currently has 17 Certificate Producing members as well as 8 Certificate Consuming members.

The CCRA certificates up to Evaluation Assurance Level (EAL) 2 are recognized by all the signatories of the CCRA.

For Higher EALs, Certificates have to be based upon common Protection Profiles.

Senior Officers Group for Information Systems (SOG-IS) MRA

The SOG-IS agreement was produced in response to the EU Council Decision of March 31st 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council recommendation of April 7th (1995/144/EC) on common information technology security evaluation criteria.

The agreement was updated in January 2010 and the full text can be downloaded in the section "Agreement" of the Web site. Participants in this Agreement are government organisations or government agencies from countries of the European Union or EFTA (European Free Trade Association), representing their country or countries. As of June 2011, the national bodies participating in the agreement are:

- Austria, Bundeskanzleramt
- Finland, FICORA - Finnish Communications Regulatory Authority
- France, ANSSI - Agence Nationale de la Sécurité des Systèmes d'Information
- Germany, BSI - Bundesamt für Sicherheit in der Informationstechnik
- Italy, OCSI - Organismo di Certificazione della Sicurezza Informatica
- The Netherlands , NLNCSA - Netherlands National Communications Security Agency, Ministry of the Interior and Kingdom Relations
- Norway, SERTIT - Norwegian National Security Authority operates the Norwegian Certification Authority for IT Security
- Spain, CCN - Centro Criptológico Nacional, Organismo de Certificación de la Seguridad de las Tecnologías de la Información
- Sweden, FMV - Försvarets Materielverk
- United Kingdom, CESG - Communications-Electronics Security Group

The participants work together to coordinate the standardisation of Common Criteria protection profiles and certification policies between European Certification Bodies in order to have a common position in the fast growing international CCRA group. They also coordinate the development of protection profiles whenever the European commission launches a directive that should be implemented in national laws as far as IT security is involved.

The agreement provides for member nations to participate in two fundamental ways: either as certificate consuming participants or as certificate producers. For certificate producing nations there are also two levels of recognition within the agreement:

- Certificate recognition up to Evaluation Assurance Level 4
- Certificate recognition at higher levels for defined technical areas when schemes have been approved by the management committee for this level.

The original agreement signed in 1997 (updated to incorporate the use of Common Criteria in 1999) was updated in 2010 for two reasons; firstly to provide a robust mechanism allowing new schemes to take part as certificate producers and, secondly, to limit the higher levels of recognition to agreed technical domains where adequate agreement around evaluation methodology, laboratory requirements, attack methods etc. are in place.

II. Security Certification and Conformity Assessment in the New Legislative Framework

Given the close relationship between ICT Security Certification and Conformity Assessment, it is particularly important to give an overview of the existing EU legislative instruments that address conformity assessment and market surveillance. The text below is taken from the "'Blue Guide' on the implementation of EU product rules"[70]:

Overview of Regulation 765/2008

Regulation (EC) No 765/2008 established the legal basis for accreditation and market surveillance and consolidated the meaning of the CE marking, thus filling an existing void. Decision No 768/2008/EC updated, harmonised and consolidated the various technical instruments already used in existing Union harmonisation legislation (not only in New Approach directives): definitions, criteria for the designation and notification of conformity assessment bodies, rules for the notification process, the conformity assessment procedures (modules) and the rules for their use, the safeguard mechanisms, the responsibilities of the economic operators and traceability requirements".

It is important to note that neither Regulation 765/2008 nor Decision 768/2008 define the requirements that products will have to meet. These requirements are defined in other product category specific legislative acts of which these are examples:

- Toys' safety (Directive 2009/48/EC)
- Machinery (Directive 2006/42/EC)
- Medical devices (Directive 93/42/EEC)

In each of the above directives, the legal text sets out the "essential requirements". Essential requirements define "the results to be attained, or the hazards to be dealt with, but do not specify the technical solutions for doing so. The precise technical solution may be provided by a standard or by other technical specifications at the discretion of the manufacturer. This flexibility allows manufacturers to choose the way to meet the requirements "[71].

The stakeholders in a conformity assessment procedure are the following:

The legislator who:

- sets out the legal requirements that products have to fulfil;

[70] 'Blue Guide' on the implementation of EU product rules http://ec.europa.eu/DocsRoom/documents/12661
[71] Ibid

- selects conformity assessment modules/procedures from the menu set out under Decision No 768/2008/EC.

The manufacturer who:

- designs, manufactures and tests the product or has it designed, manufactured or tested;
- draws up the technical documentation of the product;
- takes all measures necessary to ensure compliance of the products;
- upon positive assessment of the products, draws up the EU Declaration of Conformity and affixes the CE marking on the products if the legislation so requires;
- upon intervention of a notified body, affixes the notified body's identification number to the product if the legislation so requires.

It must be clear that it is always the manufacturer who takes responsibility for the conformity of his products with the relevant legislative requirements.

The (in-house or external) conformity assessment body that:

- performs checks and assessments, if the legislation so provides;
- upon positive assessment issues the approval certificate or attestation as required by the applicable legislation.

Standardization bodies: responsible for drafting the standards for communication and testing.

ICT Product security Requirements in Conformity Assessments as per 765/2008

Perhaps the first example of incorporating IT Security requirements in a legislative act based on the New Legislative Framework on Conformity Assessment is in the Proposal for a Regulation of the European Parliament and of the Council on medical devices and amending Directive 2001/83/EC (Medical Device Directive).

Cybersecurity aspects for software falling under the definition of a medical device have been a topic of discussion in the context of the ongoing negotiations. In particular, the introduction of two new "essential Requirements" for medical software is being considered[72] and may appear in the final text.

1. For devices that incorporate software or for standalone software that are devices in themselves, the software shall be developed and manufactured according to the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation.
2. The manufacturer shall describe minimum requirements on hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.

If adopted, this would entail, that, when the regulation becomes applicable, in the view of the placing of his/her product on the market, a medical software manufacturer would be requested (among other things) to demonstrate that such product is compliant with these two "Essential requirements".

[72] http://data.consilium.europa.eu/doc/document/ST-9769-2015-ADD-1/en/pdf