EUROPEAN
COMMISSION

Brussels, 5.7.2016
COM(2016) 410 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Strengthening Europe's Cyber Resilience System

and Fostering a Competitive and Innovative Cybersecurity Industry

1. INTRODUCTION / CONTEXT

Every day, cybersecurity incidents cause major economic damage to European businesses and the economy at large. Such incidents undermine the trust of citizens and enterprises in the digital society. Theft of commercial trade secrets, business information and personal data, disruption of services - including essential ones - and of infrastructures result in economic losses of hundreds of billions of euros each year.[1] They can also have consequences for citizens' fundamental rights and for society at large.

The 2013 Cybersecurity Strategy of the European Union[2] (EU Cybersecurity Strategy), and its central deliverable – the soon-to-be adopted Network and Information Security (NIS) Directive[3] – as well as Directive 2013/40/EU on attacks against information systems form the core policy response so far of the European Union to these cybersecurity challenges. In addition, the EU also has specialised entities at its disposal such as the European Union Agency for Network and Information Security Agency (ENISA), the European Cyber Crime Centre (EC3) at Europol, and the Computer Emergency Response Team (CERT-EU). Recently, a number of sectoral initiatives have also been launched (e.g. in the energy and transport field) to increase cybersecurity in various critical sectors.

In spite of these positive achievements, the EU remains vulnerable to cyber incidents. This could undermine the digital single market and economic and social life as a whole. Their impact can also go beyond the economy. In the case of hybrid threats[4], cyberattacks can be used in a coordinated manner with other activities to destabilise a country or challenge political institutions.

Against this background, the handling of a large-scale cyber incident involving multiple Member States simultaneously could be challenging for the EU. In synergies with the Communications on countering Hybrid Threats as well as on Delivering the European Agenda on Security[5], the Commission is looking at ways to address the evolving cybersecurity reality and assess additional measures that may be necessary to improve the EU's cybersecurity resilience and incident response.

Furthermore, the Commission is also addressing cybersecurity industrial capacities in the EU. Even though the whole value chain of digital technologies may not be mastered in Europe, there is a need to at least retain and develop certain essential capacities. Supply of products and services that provide for the highest level of cybersecurity is an opportunity for the cybersecurity industry in Europe and it could become a strong competitive advantage. The global cybersecurity market is expected to be among the fastest growing segments of the ICT sector[6]. Making the EU a leading player in this field needs to be supported by a strong culture of data security, including for personal data, and an effective response to incidents. This will

[1] *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II; Center for Strategic and International Studies; June 2014.*
[2] JOIN(2013) 1.
[3] COM(2013) 48.
[4] JOIN(2016) 18.
[5] COM(2016) 230.
[6] See SWD(2016) 216.

be seen as a strong argument to invest in the EU, thereby helping to achieve the ambitious goals of the Digital Single Market to create growth and jobs.

A strong commitment is needed to achieve the above, notably through:

i) Stepping up cooperation to enhance preparedness and deal with cyber incidents

Existing and agreed cooperation mechanisms need to be strengthened to increase the EU's resilience and preparedness, including for a possible pan-European cybersecurity crisis. These cooperation mechanisms should be comprehensive, spanning the life cycle of an incident from prevention to prosecution. Effective cooperation among Member States and practical implementation of security requirements for critical operators will also demand robust technical solutions from the cybersecurity industry.

At the same time, ensuring resilience of critical cyber assets throughout the EU will require continuous efforts to find cross-sectoral synergies and to mainstream cyber requirements in all relevant EU policies. The Commission will consider the need to update the 2013 EU Cybersecurity Strategy in the near future.

ii) Addressing challenges facing Europe's cybersecurity Single Market

The Digital Single Market (DSM) strategy[7] recognised that specific gaps still exist in the fast-moving area of technologies and solutions for online network security. At the same time, market studies show that the EU internal market is still geographically fragmented as far as supply of cybersecurity products and services is concerned[8]. This Communication sets out a number of market-oriented policy measures to address these Single Market gaps and challenges.

iii) Nurturing industrial capabilities in the field of cybersecurity

In the EU Cybersecurity Strategy and in the DSM strategy, the Commission committed to promote increased supply of products and services by the EU cybersecurity industry. Consequently, the Commission is also adopting a decision paving the way to a contractual arrangement on Public Private Partnership (cPPP) on cybersecurity, which will seek to advance a cutting-edge European cybersecurity research and innovation agenda for increased competitiveness.

2. TAKING COOPERATION, KNOWLEDGE AND CAPACITY TO THE NEXT LEVEL

The EU Cybersecurity Strategy and in particular the forthcoming NIS Directive[9] will pave the way towards improved EU-level cooperation across Member States. The swift and effective implementation of the Directive will be key in view of the increasing digitalisation of economic and societal life (also taking into account the cloud, the Internet of things, and machine-to-machine communication), growing cross-border interconnection and the fast-

[7] COM(2015) 192.
[8] See SWD(2016) 216.
[9] The NIS Directive will require Member States to identify a range of operators of essential services in fields such as energy, transport, finance and health, to address cybersecurity risks, and also to ensure that certain digital service providers take appropriate measures to address such risks.

evolving cyber-threat landscape[10]. In this context, the EU needs to prepare itself for the possibility of a large-scale cyber crisis[11], including for instance simultaneous attacks on critical information systems in several Member States[12].

EU level cooperation is therefore essential for dealing with both smaller-scale but potentially proliferating cyber incidents, and a possible large-scale cyber-attack in multiple Member States. The EU needs to integrate cyber aspects into existing crisis management mechanisms. It also needs to ensure effective cooperation and swift information-sharing mechanisms among sectors and Member States to respond to, and contain, such incidents. Furthermore, these mechanisms should operate coherently, thus contributing to the fight against terrorism, organised crime and cybercrime. This would also increase the EU's ability to coordinate with its international partners in responding effectively to global threats and incidents.

2.1. Making the most of NIS cooperation mechanisms and moving towards ENISA 2.0

An essential part of national capabilities required by the NIS Directive are Computer Incident Response Teams (CSIRTs) responsible for rapid reaction to cyber threats and cyber incidents. They will form the CSIRTs Network to promote effective operational cooperation on specific cybersecurity incidents and sharing information about risks. Furthermore, the Directive will create a Cooperation Group to support and facilitate strategic cooperation among Member States and to build trust among them.

Given the nature and multitude of cyber threats, the Commission encourages Member States to make the most out of the NIS cooperation mechanisms and to enhance cross-border cooperation related to preparedness for a large-scale cyber incident. Such additional cooperation for a significant cyber incident would benefit from a coordinated approach to crisis cooperation across the various elements of the cyber ecosystem. Such an approach can be set out in a 'blueprint' that should also ensure synergies and coherence with existing crisis management mechanisms[13]. It should then be regularly tested in cyber and other crisis management exercises. It would include a role for EU-level bodies such as ENISA, CERT-EU and the European Cybercrime Centre (EC3) at Europol, and use tools developed in the context of the CSIRTs Network. In the first half of 2017, the Commission will present such a cooperation blueprint for consideration by the Cooperation Group, the CSIRTs Network and other relevant stakeholders.

Currently, knowledge and expertise on cybersecurity is available at the EU level, but in a dispersed and unstructured way. To support the NIS cooperation mechanisms, information should be pooled in an 'information hub' to make it easily available on request to all Member States. This 'hub' would become a central resource allowing the EU institutions and Member States to exchange information as appropriate. Easier access to better structured information on cybersecurity risks and potential remedies should help Member States to increase their capacities and align their practices, and thereby enhance overall resilience to attacks. The

[10] See SWD(2016) 216.
[11] See e.g. ENISA Report: Common practices of EU-level crisis management and applicability to cyber crises (April 2016).
[12] See SWD(2016) 216.
[13] Notably the Integrated Political Crisis Response Arrangements including the decision on the arrangements for the implementation by the Union of the solidarity clause (24 July 2014) and the Common Security and Defence Policy decision-making processes.

Commission, supported by ENISA, CERT-EU and with the expertise of its Joint Research Centre, will facilitate the creation and ensure the sustainability of the hub.

In addition, a regular high-level advisory group[14] on cybersecurity – composed of experts and decision-makers from industry, academia, civil society and other relevant organisations – should be set up at EU level. The group would enable the Commission to get external expertise and input, in an open and transparent way, for its cybersecurity strategy policies and on potential regulatory or other public policy actions. It would complement and connect with other structures on cybersecurity[15] .

Moreover, the Commission is required to evaluate ENISA by 20 June 2018 and the possible modification or renewal of ENISA's mandate must be adopted by 19 June 2020[16]. In view of the current cybersecurity landscape, the Commission aims to advance the evaluation and, subject to its results, present a proposal as soon as possible.

When assessing the possible need to change ENISA's mandate, the Commission will take into account the cybersecurity challenges described above and the overall effort to step up cooperation and knowledge sharing. This process will provide an opportunity to look into the possible enhancement of the Agency's capabilities and capacities to support Member States in a sustainable manner in achieving cybersecurity resilience. The reflection on ENISA's mandate would furthermore need to take into account the Agency's new responsibilities under the NIS Directive, new policy objectives to support cybersecurity industry (the DSM strategy and in particular the cPPP), evolving needs in securing critical sectors, and new challenges linked to cross-border incidents, including coordinated response to cyber crises.

The Commission will:

- submit for consideration a cooperation blueprint to handle large-scale cyber incidents on the EU level in the first half of 2017;
- facilitate the creation of an 'information hub' to support the exchange of information between EU bodies and Member States;
- create a high-level advisory group on cybersecurity; and
- finalise the evaluation of ENISA by end of 2017. Such evaluation will address the need to modify or extend the mandate of ENISA, aiming for a possible proposal as soon as possible.

2.2 Increase efforts in cybersecurity education, training and exercises

Adequate skills and training, related both to preventing cybersecurity incidents and to dealing with and mitigating their impacts, are some of the key aspects of achieving cybersecurity resilience.

[14] Commission expert groups are subject to the horizontal rules established by Commission decision C(2016)3301.
[15] E.g. the NIS Platform, cPPP on cybersecurity and sectoral platforms such as the Energy Expert Cyber Security Platform (EECSP). It should also link to the high-level roundtable announced in the Communication on Digitising European Industry: COM(2016) 180.
[16] Regulation (EU) No 526/2013 repealing Regulation (EC) No 460/2004.

Currently, ENISA, the European Cybercrime Training and Education Group (ECTEG), in cooperation with the European Cybercrime Centre at Europol and the European Police College (CEPOL) all play an important role in providing capacity-building support – including on cyber forensics – by developing manuals, and organising training and cybersecurity exercises.

At the same time, cyberspace is a rapidly developing domain where dual-use capabilities play an essential role. It is therefore necessary to develop civil-military cooperation and synergies in training and exercises to increase the resilience and incident response capabilities of the EU.

To respond to this need, and as a follow-up to the adoption of the NIS Directive and the EU Cyber Defence Policy Framework[17], the Commission services will cooperate with Member States, the European External Action Service (EEAS), ENISA and other relevant EU bodies[18] to establish a cybersecurity education, exercise and training platform that will promote synergies between civilian and defence training.

The Commission will:

- work in close cooperation with Member States, ENISA, EEAS and other relevant EU bodies to establish a cybersecurity training platform.

2.3. Addressing inter-sectoral interdependencies and key public network infrastructure resilience

An important factor in assessing the risk and impact of a large-scale cyber incident is the degree of cross-border and cross-sectoral interdependencies. A severe cyber incident in one sector or in one Member State may directly or indirectly have an effect on – or propagate to – other sectors, or to other Member States.

Cross-border and cross-sector cooperation facilitates the exchange of information and expertise and thus increased preparedness and resilience. The Commission has been supporting work in various sectors to better understand interdependencies through the implementation of the European Programme for Critical Infrastructure Protection[19].

At the same time, a necessary pre-requisite for addressing cross-sectoral risks is the ability of each individual sector to identify, prepare for and respond to cyber incidents. The Commission will assess the risk resulting from cyber incidents in highly interdependent sectors within and across national borders, in particular on the sectors covered by the NIS Directive, also taking into account developments at the international level[20]. Following this assessment, the Commission will consider if there is a need for further specific rules and/or guidance on cyber risk-preparedness for such critical sectors.

[17] Adopted by the Foreign Affairs Council of the European Union on 18 November 2014, Doc. 15585/14.
[18] Such as the European Security and Defence College, EC3, CEPOL and the European Defence Agency.
[19] SWD(2013) 318.
[20] E.g. cyber security roadmap adopted by the European Aviation Safety Agency, cybersecurity roadmap, work of International Civil Aviation Organisation, International Maritime Organisation.

At European level, Sectoral Information Sharing and Analysis Centres[21] (ISACs) and corresponding CSIRTs can play a key role in preparing for and responding to cyber incidents. To ensure effective information flows on evolving threats and to facilitate the response to cyber incidents, ISACs should be encouraged to engage with the CSIRTs Network under the NIS Directive, and with the European Cybercrime Centre at Europol, CERT-EU as well as with relevant law enforcement bodies.

Information exchange between stakeholders and with authorities throughout the life cycle of cyber risks requires confidence among participants that it will not expose them to liability. The Commission has noted a number of such concerns, which prevent businesses from sharing valuable threat intelligence with their peers, across sectors or with authorities, in particular across borders. The Commission will seek to address and allay such concerns in the interest of improved cyber-threat information exchange.

Trusted reporting channels ensuring confidentiality are also vital to encourage businesses to report on cyber theft of trade secrets. This would make it possible to monitor and assess the damage suffered by European industry (resulting also in loss of sales and jobs) and research bodies. This would also help in designing a proper policy response. With the support of ENISA, the European Union Intellectual Property Office (EUIPO) and EC3 at Europol, the Commission will — in dialogue with private stakeholders — set up trusted channels for voluntary reporting of cyber theft of trade secrets. This should make it possible to compile anonymised and aggregated data at EU level. This data can be shared with Member States to feed diplomatic efforts and awareness-raising actions to help protect the EU's intangible assets from cyber-attacks.

To support sectoral cybersecurity, the Commission will also promote embedding cybersecurity in the development of various EU sectoral policies with cybersecurity stake.

Last but not least, public authorities have a role to play in verifying the integrity of key internet infrastructures to detect issues, inform the party responsible for these networks and – wherever needed – provide assistance in fixing known vulnerabilities. National regulatory authorities could use the capacities of CSIRTs to conduct regular scans of public network infrastructures. Based on this, they could encourage operators to remedy gaps or address vulnerabilities that such scans could identify.

The Commission will therefore examine the necessary legal and organisational conditions in order to allow National Regulatory Authorities – in cooperation with national cybersecurity authorities – to request CSIRTs to conduct regular vulnerability checks of public network infrastructures. National CSIRTs should be encouraged to cooperate under the CSIRTs Network on best practices in monitoring networks, thus facilitating the prevention of large-scale incidents.

The Commission will:

- foster the emergence of European cooperation of Sectoral Information Sharing and

[21] See e.g. the European Energy ISAC (http://www.ee-isac.eu).

Analysis Centres, support their collaboration with CSIRTs and seek to address barriers that prevent market participants from sharing information;
- study the strategic/systemic risk resulting from cyber incidents in highly interdependent sectors within and across national borders;
- assess the need for and, if appropriate, consider additional rules and/or guidance on cyber risk-preparedness for critical sectors;
- set up with ENISA, EUIPO and EC3 trusted channels for voluntary reporting on cyber theft of trade secrets;
- promote the embedding of cybersecurity measures in European sectoral policies; and
- examine the necessary conditions to enable national authorities to request CSIRTs to conduct regular checks of key network infrastructures.

3. CONFRONTING CHALLENGES FACING EUROPE'S CYBERSECURITY SINGLE MARKET

Europe needs high-quality, affordable and interoperable cybersecurity products and solutions. However, the supply of ICT security products and services within the single market remains very fragmented geographically. On the one hand, this makes it difficult for European companies to compete on the national, European and global level; on the other, it reduces the choice of viable and usable cybersecurity technologies that citizens and enterprises have access to[22].

Indeed, the cybersecurity industry in Europe has developed largely on the basis of national governmental demand, including for the defence sector. Most European defence contractors have developed cybersecurity divisions[23]. In parallel, a myriad of innovative SMEs has also emerged both in specialty/niche markets (e.g. crypto systems) and in well-established markets with new business models (e.g. antivirus software).

However, companies have difficulties growing outside their domestic, national market. The lack of trust in the solutions offered 'cross-border' is the essential factor that clearly emerged from all the consultations undertaken by the Commission[24]. As a consequence, much procurement still takes place within a given Member State and many companies struggle to achieve the economies of scale that would enable them to be more competitive both within the internal market and globally.

The lack of interoperable solutions (technical standards), practices (process standards) and EU-wide mechanisms of certification are among other gaps affecting the single market in cybersecurity. In this context, cybersecurity was identified as one of the ICT Standardisation Priorities for the Digital Single Market[25].

[22] See SWD(2016) 216.
[23] See SWD(2016) 216.
[24] See SWD(2016) 215.
[25] COM(2016) 176/2.

The limited perspectives of growth for cybersecurity companies within the single market result in a multitude of mergers and acquisitions by non-European investors[26]. While this trend demonstrates the innovation capacity of Europe's entrepreneurs in cybersecurity, it also risks leading to the loss of European know-how and expertise, and to a brain drain.

Urgent action is needed to foster a more integrated single market for cybersecurity products and services that will facilitate the deployment of more practical and affordable solutions.

Barriers of trust among Europe's industrial and institutional actors can be overcome by fostering cooperation at the early stage of the innovation life cycle: within the cybersecurity industry itself, between suppliers and purchasers; and in a cross-sector dimension involving industries that already are or are likely to become customers of cybersecurity solutions.

At the same time, the development of dual-use products, services and technologies is becoming increasingly important in Europe. A growing number of solutions are being brought from the civilian to the defence market[27]. In the upcoming European Defence Action Plan, the Commission intends to identify measures to further boost civil-military synergies at the European level.

3.1 Certification and labelling

Certification plays an important role in increasing trust and security in products and services. This is also valid for those new systems that make extensive use of digital technologies and which require a high level of security, such as connected and automated cars, electronic health, industrial automation control systems (IACS) or smart grids.

National initiatives are emerging to set high-level cybersecurity requirements for ICT components on traditional infrastructure, including certification requirements. Albeit important, these bear the risk of creating single market fragmentation and interoperability issues. Only in a few Member States are there effective security certification schemes for ICT products[28]. An ICT vendor might therefore need to undergo several certification processes in order to sell in several Member States. In the worst case scenario, an ICT product or service designed to fulfil cybersecurity requirements in one Member State cannot be placed on the market in another.

In order to achieve a functioning single market in cybersecurity, a possible framework for security certification of ICT products and services should strive to achieve the following goals: (i) cover a wide range of ICT systems, products and services; (ii) ensure application in all 28 Member States; and (iii) address any cybersecurity level; while taking into account developments on the international level.

For this purpose, the Commission will set up a dedicated working group on security certification of ICT products and services, composed of experts from Member States and industry. Its aim will be to develop, in cooperation with ENISA and the Joint Research Centre, by end-2016 a roadmap exploring the possibility of creating such a European ICT

[26] See SWD(2016) 216.
[27] In 2013 the dual use export domain already represented about 20 % of EU total exports (in value). This includes intra-EU trade.
[28] See SWD(2016) 216 for Senior Officers Group for Information Systems agreement (Council Decision of March 31st 1992 (92/242/EEC)) and other existing schemes e.g. Commercial Product Assurance in the UK, Certification Sécuritaire de Premier Niveau in France.

security certification framework proposal by end-2017. In this context, the Commission will also consider Regulation (EC) No 2008/765 and certification provisions included in the General Data Protection Regulation 2016/679[29].

The process will include a broad consultation and impact assessment. This will enable the Commission to explore various options for the creation of the certification framework for ICT products and services. The Commission will also explore ICT security certification within infrastructure sectors (e.g. in aviation, railways, automotive), and within specific certification and validation mechanisms of ready-to-be-deployed technology (e.g. Cybersecurity of Industrial Automation Control Systems[30], Internet of Things, Cloud). It will also address identified gaps under the European ICT security certification scheme mentioned above.

As much as possible, certification efforts will build on internationally recognised standards and be developed with international partners.

The Commission will also explore options related to how best to integrate ICT security certification in future sector-specific legislation, also related to safety aspects.

Apart from possible regulatory options, the Commission will also explore the creation of a European, commercially oriented, voluntary and lightweight labelling scheme for the security of ICT products. Complementary to certification, it will aim to increase the readability of cybersecurity in commercial products so as to increase their competitiveness in the single market and globally. Due consideration will be given to ongoing sectoral and horizontal initiatives launched by industry, from both the supply and demand sides.

Public administrations will be closely involved to enable use of common specifications and reference to certification in public procurement. The Commission will also monitor and report on the usage of relevant certification requirements in public procurement, at national level, in particular for sectoral systems (energy, transport, health, public administration, etc.)

The Commission will:

- Develop by end-2016 a Roadmap towards a possible European ICT security certification framework proposal, to be presented by end-2017, and to assess the feasibility and impact of a European lightweight cybersecurity labelling framework;
- explore the need and, if appropriate, address gaps in ICT security certification within existing sector-specific certification/validation mechanisms;
- include, where appropriate, the integration of ICT product security certification in future sector-specific legislative proposals;
- stimulate involvement of public administrations to facilitate the use of certification and common specifications in public procurement; and
- monitor the usage of relevant certification requirements in public and business

[29] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, provides for both codes of conduct intended to contribute to the proper application of the data protection rules as well as for certification mechanisms covering all data protection principles, including in particular the data security of the personal data processing.

[30] See ERNCIP's Thematic group on "Cyber security of Industrial Control Systems", available at https://erncip-project.jrc.ec.europa.eu/download-area/category/16-case-studies-for-industrial-automation-and-control-systems.

procurement and report on the state of the market in three years.

3.2. Scale up cybersecurity investment in Europe and support SMEs

While innovation in cybersecurity sector is booming in Europe, the EU still lacks a sufficient culture of investing in cybersecurity. There are many innovative SMEs in the field but they are often unable to scale up their operations. This is, among others, due to the lack of easily available funding to support them in the early phases of development. Companies also have limited access to venture capital in Europe and their available budget for marketing to improve their visibility, or to deal with different sets of standardisation and compliance requirements, is inadequate.

At the same time, cooperation between cybersecurity players is quite patchy and further effort is needed to increase economic concentration and develop new value chains[31].

To scale up cybersecurity investment in Europe and support SMEs, it is necessary to ease access to finance. There must also be support for the development of globally competitive cybersecurity clusters and centres of excellence in favourable regional ecosystems for digital growth. This support needs to be linked to the implementation of smart specialisation strategies and other EU instruments so that the cybersecurity industry in Europe takes better advantage of them.

The approach of the Commission will be to maximise awareness in the cybersecurity community of financing opportunities at European, national and regional level (related to both horizontal instruments and specific calls[32]) by using existing instruments and channels e.g. the Enterprise Europe Network.

The Commission will supplement these efforts by exploring with the European Investment Bank (EIB) and the European Investment Fund (EIF) ways of easing access to finance. This can be in the form of equity and quasi-equity investments, loans, guarantees to projects or counter-guarantees to intermediaries, e.g. through the creation of a Cybersecurity Investment Platform under European Fund for Strategic Investment[33].

In addition, the Commission would also look into developing with interested Member States and regions a Cybersecurity Smart Specialisation Platform[34]. This would help coordinate and plan cybersecurity strategies and set up a strategic collaboration of interested parties in regional ecosystems. This approach should also help unlock the potential of existing European structural and investment funds for the cybersecurity sector.

More generally, the Commission will promote a security-by-design approach. It will seek to ensure that cybersecurity requirements are consistently addressed in all major infrastructure

[31] See SWD(2016) 216.

[32] See e.g. multi-sectoral 2016 call for proposals under the Connecting Europe Facility programme, 2016 COSMO calls related to Cluster Internationalisation Programme.

[33] In the framework of the European Fund for Strategic Investment individual projects can be supported either directly or indirectly through Investment Platforms. Such Platforms can help finance smaller projects and bundle funds from different sources to enable diversified investments with a geographic or thematic focus.

[34] See smart specialisation instruments (RIS3): http://s3platform.jrc.ec.europa.eu/.

investments that have a digital component and which are co-financed by the European funds. It will do this by gradually introducing relevant requirements in public procurement and programme rules.

The Commission will:

- use existing SME support tools to raise awareness about existing funding mechanisms among the cybersecurity community;
- further step up the use of EU tools and instruments to support innovative SMEs in exploring synergies between civilian and defence cybersecurity markets[35];
- explore with EIB and EIF the feasibility of easing access to investment e.g. through a dedicated Cybersecurity Investment Platform or other tools;
- develop a Cybersecurity Smart Specialisation Platform to help Member States and regions interested in investing in cybersecurity sector (RIS3); and
- promote a security-by-design approach in major infrastructure investments that have a digital component and are co-financed by EU funds.

4. STIMULATE AND NURTURE EUROPEAN CYBERSECURITY INDUSTRY THROUGH INNOVATION — ESTABLISHMENT OF THE CYBERSECURITY CPPP

To stimulate the competitiveness and innovation of Europe's cybersecurity industry, a contractual public private partnership (cPPP) on cybersecurity will be signed. The cPPP will gather industrial and public resources to deliver excellence in research and innovation.

The cPPP's aim is to build trust among Member States and industrial by fostering cooperation at early stages of the research and innovation process. It also aims to help align the demand and supply sectors. This should allow industry to obtain future requirements from end-users and sectors that are important customers of cybersecurity solutions (e.g. energy, health, transport, finance). It will facilitate their engagement in defining common digital security, privacy and data protection requirements for their sectors.

The cybersecurity cPPP will also help to maximise the use of available funds. This will be achieved firstly through greater coordination with Member States. Secondly, there will be a better focus on a few technical priorities to help the cybersecurity industry obtain technological breakthroughs and master key future cybersecurity technologies. In this context, the development of open source software and open standards can help foster trust, transparency and disruptive innovation, and should therefore also be a part of the investment made in this cPPP.

The work conducted under the cPPP on cybersecurity will also benefit from synergies with other European projects, notably where these address security aspects. These include

[35] For example, the Enterprise Europe Network and the European Network of Defence-related Regions will provide new opportunities for regions to explore cross-border cooperation in the area of dual use, including cybersecurity, and for SMEs to engage in matchmaking activities.

Factories of the Future, Energy Efficient Buildings, 5G and big data PPPs[36], and other sectoral PPPs[37] as well as the Internet of Things initiative[38]. Furthermore, a close alignment will be promoted with the European Open Science Cloud and the European supercomputing initiative for quantum cyber technologies (e.g. innovation in quantum key distribution, quantum computing research).

The cPPP on cybersecurity is launched under Horizon 2020[39], the EU's research and innovation framework programme for the period 2014-2020. It will leverage funding from two pillars of the programme: Leadership in Enabling and Industrial Technologies (LEIT-ICT) and Societal Challenge – Secure Societies (SC7). The total budget of the cPPP will be up to EUR 450 million with a triple leverage factor on the industry's side. Cybersecurity should also be addressed and coordinated with other relevant parts of Horizon 2020 (e.g. the energy, transport and health societal challenges and the Excellence part of Horizon 2020). This will contribute to the objectives of the cPPP on cybersecurity. This coordination should also happen upfront at the stage of designing sectoral strategies.

The cPPP will be implemented in a transparent manner, with open and flexible governance adapted to a fast-evolving environment of cybersecurity. It will take into account the need for Member States to discuss how changes in technology affect the secure operation of national and cross-border infrastructures. Equally, the partnership's output must be sustainable over several years to ensure that its objectives can be met.

The cPPP will be supported by the European Cyber Security Organisation (ECSO), whose membership will reflect the diversity of the cybersecurity market in Europe. It will also include national, regional and local public administrations, research centres, academia and other interested parties.

The Commission will:

- sign with industry a contractual Public Private Partnership on cybersecurity so that it becomes operational in the third quarter of 2016;
- launch Horizon 2020 calls for proposals related to the cybersecurity cPPP in the first quarter of 2017; and
- ensure coordination of the cybersecurity cPPP with relevant sectoral strategies, Horizon 2020 instruments and sectoral PPPs.

5. CONCLUSION

This Communication presents measures aiming to strengthen Europe's cyber resilience system and to foster a competitive and innovative cybersecurity industry in Europe, as announced in the EU Cybersecurity Strategy and in the Digital Single Market strategy. The Commission invites the European Parliament and the Council to support this approach.

[36] The 5G Infrastructure Public Private Partnership & the Big Data Value Public-Private Partnership.
[37] The SESAR or the Shift to Rail Public Private Partnership for instance.
[38] The Alliance for Internet of Things Innovation (AIOTI).
[39] http://ec.europa.eu/programmes/horizon2020/en/official-documents.