Brussels, 12.9.2018
SWD(2018) 403 final

PART 2/4

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 404 final}

Annex 1: Procedural information

1. Lead DG, Decide Planning/CWP references

This Impact Assessment report was prepared by Directorate H "Digital Society, Trust and Cybersecurity" of the Directorate General "Communications Networks, Content and Technology" (DG CONNECT).

The Decide Planning reference of the initiative "Proposal to create a Cybersecurity Competence Network with European Cybersecurity Research and Competence Centre" is PLAN/2017/1743.

The present initiative has been included in the Commission Work Programme 2018 by way of amendment to the text. The Programme Committee unanimously voted for the amendment of the Work Programme on 18 January 2018.

2. Organisation and timing

Several services of the Commission with an interest in this initiative have been associated in the development of this analysis. DG CONNECT worked closely with the Joint Research Centre (JRC) to gather evidence for the Impact Assessment. The initiative has been also regularly presented at the meetings of the cybersecurity sub-group of the Security Union Task Force, which gathers all relevant DGs. DG CONNECT has also engaged in bilateral exchanges with other DGs relevant for the initiative, notably DG GROW, DG HOME as well as the European External Action Service (EEAS).

On 26 March 2018, a meeting of the ISG was held on the draft of the Impact Assessment and on the results of the targeted consultation of relevant stakeholders, before the submission to the Regulatory Scrutiny Board (RSB). The representatives of all relevant DGs, including DG CONNECT, JRC, DG DIGIT, DG RTD, DG HOME and SG were present.

Should the RSB issue a positive opinion, a final Fast Track ISG meeting is expected to be held in early to mid-May 2018 on the legal proposal and on the final version of the Impact Assessment. DG CONNECT will have updated the Impact Assessment Report by taking into account the comments received at-and following-the ISG meeting. The meeting was chaired by SG, and DG CONNECT was flanked by DG GROW, DG HOME, JRC, DG BUDG, DG MOVE, DG REGIO, DG HR DS, DG FISMA, DG COMP, DG ENER, DG JUST, DG EAC, DG EMPL) as well as European External Action Service

3. Exceptions to the Better Regulation Guidelines

DG CONNECT has identified one exception to the Better Regulation guidelines. Specifically, a *dedicated* open public consultation has not been conducted. However, stakeholders were given the opportunity to express their views on this initiative and the overall thematic in the following open and targeted public consultations:

- A general open public consultation on the topic of security in relation to the next MFF. For results see Annex 2, section 3.1.1.
- A general open public consultation on the topic of investment, research & innovation, SMEs and the single market. For results see Annex 2, section 3.1.2.
- A self-registration survey open to all cybersecurity centres of expertise across Europe, giving them the opportunity to register their competence and domains of expertise within the remit of the cybersecurity taxonomy developed by the Commission prior to opening the Survey (see Annexes 4 and 5)
- A series of targeted workshops and meetings:

  - **Consultation workshop with competence centres** - on 23 February 2018 the Commission organised a full-day consultation workshop with cybersecurity expertise centres from across Europe to exchange views on, among others, possible ways of reinforcing the EU cybersecurity research capabilities; better coordinating research and innovation efforts with the industry partners; and promoting industrial innovation and competitiveness. Given the big number of cybersecurity expertise centres across the EU, a list of executive-level invitees to the workshop was prepared taking into consideration the activities of the cybersecurity centres (scientific criteria such as e.g. publications and patents), geographical balance and results of the mapping of the cybersecurity expertise centres across the EU conducted by the Joint Research Centre (JRC). Last but not least, Member States were asked to provide additional suggestions of possible participants.

  - **Consultation with the Management Board of the European Cybersecurity Organisation** – the European Commission's counterpart in the contractual Public Private Partnership during a meeting held on 21 March 2018. The representatives of the Board include high-level representatives of cybersecurity companies and SMEs, cybersecurity associations across the EU, representatives of users/operators community, representatives of public administration, research and technology organisations, universities as well as of regional structures e.g. cybersecurity clusters.

  - **Consultation workshop with industry, research community and Member States -** on 22 March 2018 the Commission organised a full-day consultation workshop with the representatives of industry (supply and demand side), competence centres as well as Member States to discuss current challenges, gaps and best ways to mitigate them to ensure that the EU has the capacity to autonomously secure its economy, society and democracy against cyber threats. The workshop also identified the areas where the Network and the Centre would provide added-value to the work already done at the national level.
  - **Consultation with the Management Board of ENISA** (15 March 2018) as well as a request for targeted contribution, which ENISA provided in April 2018.
  - **Consultation with European Defence Agency** through a request for contribution, which EDA provided in April 2018.
- Consultation activities with Member States:
  - A high-level workshop with Member States on 5 December 2017
  - Discussions at the Horizontal Working Party on Cyber (08 March 2018)
  - Member States were also invited to the consultation workshop on 22 March 2018

4. CONSULTATION OF THE REGULATORY SCRUTINY BOARD (RSB)

The Regulatory Scrutiny Board has been consulted as per the procedural rules for the submission of new proposals. The Impact Assessment Report was submitted to the Board on 11 April 2018. The RSB examined the Impact Assessment and issued its Opinion on 07 May. The Board gave a positive opinion with reservations. The Impact Assessment was subsequently reviewed in light of the Board's comments.

The table below presents and overview how these comments were addressed. As point C of the Opinion includes specific considerations detailing the main considerations included under point B of the Opinion, the table below focuses on specific consideration to provide thorough explanation while avoiding duplication.

Board's Recommendations in the Opinion	Implementation of the recommendations into the revised IA Report
(1) The report should better describe what has already been decided and which aspects of coordinating cybersecurity research at EU level are still open. In particular, it should clarify whether the principle of the establishment of the network and the European centre has already been agreed in the Council. Additionally, on the basis of the results of the consultations, it should identify the remaining sensitive points for stakeholders, in particular for the Member States.	Section 1 ***Political and legal context*** has been updated to further illustrate the political and legal context. It now spells out more clearly the feedback from the Member States, the decisions taken as well as remaining sensitive points – all creating basic strategic assumptions guiding the Impact Assessment analysis. In particular, the report makes now a clearer reference to: • The consultation with Member States at the time of reviewing the 2013 EU Cybersecurity Strategy as well as following the announcement of the initiative in the September 2017 Cybersecurity Package, which indicated that any efforts in cybersecurity field need to take advantage of and be complementary with the existing capacities at the national level; • The Council Conclusions, in which Member States welcomed the intention to set up a network of cybersecurity competence centres to stimulate the development and deployment of cybersecurity technologies, stressing the need to be inclusive towards all Member States and their existing centres of excellence and competence and to pay special attention to complementarity of European and national level efforts – these two elements being the key sensitive issues from the Member States' perspective mentioned throughout the consultation process. • Explanation why the option of creating a fully centralised structure (as opposed to the network with the European centre) has been discarded at an early stage of the process and is now mentioned in the section "Options discarded at an early stage".
(2) The report should more clearly spell out what makes the sector special. What specific characteristics of the cybersecurity sector justify a particular solution that differs from other sectors facing similar challenges? Additionally, it should clarify the prominent role of the public sector as this significantly shapes the character of the initiative. In this context, the report should also expand on the envisioned limited role of industry and the reasons for that. Finally, the report should describe the state of existing competence centres.	Section 1 ***Political and legal context*** has been updated and spells out more clearly now what makes the cybersecurity sector special. In particular, the report now mentions that: • Over the last decade, cybersecurity has become a cross-cutting, horizontal issue, which concerns not only IT sector but virtually any part of our economy and society, including also the critical sectors our societies depend on – from energy, through transport, financial services, public services and healthcare, to mention just a few. • Europe must be therefore in a position to autonomously secure its digital assets and to do so it needs to ensure its competitiveness in the field of cybersecurity. At the same time for most sectors cybersecurity is not part of their core business so they need to have easy access to

	knowledge and support to make their own products secure. • Despite the fact that a wealth of expertise and experience in cybersecurity exists - more than 660 organisations from across the EU registered to the recent mapping of cybersecurity centres of expertise conducted by the European Commission.[1] Yet, the efforts of research and industrial communities are fragmented, lacking alignment, and a common mission, which hinders EU's competitiveness in this domain as well as its ability to secure its digital assets. Despite Europe's potential to cover the full cybersecurity value chain, the relevant cybersecurity sectors (e.g. energy, space, defence transport) and sub-domains are today insufficiently supported.[2] • Synergies between the civilian and defence cybersecurity sectors are not fully exploited in Europe either. • The specificities of the area of cybersecurity, in which considerations of national security and of European strategic autonomy play an important role justify different approach compared to other, less sensitive sectors. The initiative has to find the right arrangements to work with and support industry (both the supply and demand side), academia, and the public sector - from both civilian and defence sectors - while giving a clear role to Member States' authorities in key areas. In addition ***section 2.2.1***. now points to the fact that public authorities have multiple roles in supporting cybersecurity industrial development. They are users of cybersecurity solutions themselves as they are responsible for securing a wide range of public services. The role of public sector is also crucial in e.g. ensuring that researchers and industries from different economic sectors have access to necessary testing and experimentation infrastructure. In case of cybersecurity such facilities (e.g. quantum test beds) are often too large/costly for a single entity - be it private or public - to acquire alone so the public authorities' intervention is needed.
(3) The report should present the differences between the two options in a more accessible way (e.g. in a table). It should discuss how each option would set up the interaction with non-civilian stakeholders and industry. The report should also include a discussion of the pros and cons of the alternative options with regard to the envisaged division of responsibilities between the European competence centre and national competence centres. The report should detail the reasons for selecting the preferred option, for example in terms of avoiding conflicts of interest of industry and anticipating demand from non-civilian	Following the recommendation of the Board, Section 7 of the report ***How do the options compare,*** in addition to the standard comparison of the assessment against the core criteria of effectiveness, efficiency and coherence, has now been supplemented with an overview table summarising the differences between the two options in terms of possible scope of activity. The relation and possible interactions with civilian and non-civilian stakeholders and industry are outlined in Section 5.2.1 and 5.5.2 as well as in the section 6 analysing the impacts of the option. The table

[1] JRC Technical Reports: European Cybersecurity Centres of Expertise, 2018

[2] JRC Technical Report: Outcomes of the Mapping Exercise (See Annex 4 and 5 for details)

stakeholders.	summarising the differences between the options described above now makes clearer the difference between the Options in terms of possible interactions with non-civilian stakeholders. In addition, the section 4.3 ***Functionalities and governance of the Network and the Centre*** now makes it clear that the governing rules should allow the possibility to discuss cybersecurity defence-related topics in an appropriate setting (e.g. ensuring appropriate information security and confidentiality) and how the Centre should do this. In addition to explaining why the "network only" option has been discarded at an early stage, the Report provides now the explanation why the option of creating a fully centralised structure (as opposed to the network with the European centre) has been discarded as well. In addition, the section 4.3 ***Functionalities and governance of the Network and the Centre*** now provides a more detailed description of how the network would work, what would be the role of the National Coordination Centres vs the European Competence Centre. Following the recommendation of the Board, section 8 on preferred option has now been adapted, summarising all key arguments used throughout the report in the sections describing the options and assessing their impacts. In addition to the important aspect of finding synergies between civilian and defence communities, the section more clearly outlines the advantage of the Option in supporting cybersecurity industrial policy by conducting activities related not only to research and development but also to market deployment activities. This includes both providing infrastructure for research and innovation as well as undertaking efforts to bring innovations to the market (e.g. through joint procurement of cybersecurity products and solutions to shield critical sectors under the responsibility of the public authorities (the latter one with the exception of defence area). The Report also points to the fact that the public-public governance structure, while allowing for pro-active advisory engagement of the industry and other stakeholders, is better suited to reflect the sensitive nature of cybersecurity initiatives as well as to avoid potential conflicts of interest in case of e.g. joint procurement;
(4) The report should meticulously describe the envisioned implementation (alternatives) of both the European competence centre and the network of national competence centres. This should cover in particular, but not exclusively, their governance; the practicalities of the co-investment scheme; the degree of centralisation; and the link to other (research) bodies (existing competence centres, HPC JU, FP9, EIT, cPPP, the Innovation House, ENISA, etc.). Additionally, the report should explain the interaction with the education sector in order to build missing skills.	As mentioned above, in addition to explaining why the "network only" option has been discarded at an early stage, the Report provides now the explanation why the option of creating a fully centralised structure (as opposed to the network with the European centre) has been discarded as well. In addition, the section 4.3 ***Functionalities and governance of the Network and the Centre*** now provides a more detailed description of how the network would work, what would be the role of the National Coordination Centres vs the European Competence Centre. The report addresses and reinforces the message about the links with different structures (HPC, EIT, cPPP,

	innovation Hubs, ENISA) in a number of sections throughout the text (Section 1: Policy and legal Context as well as Section 4.3 on functionalities and governance of the Network and the Centre). In addition, an explanation on the relation with the education sector has been added in the sections describing possible tasks of the Centres both under Option 1 and 2.
(5) The report should upfront be clearer that this initiative is about cybersecurity research and innovation and not cybersecurity in general (a field with many more existing networks and pooling of resources at the EU level). Related to this, the report should set out that deployment, carried out in the process of implementing the Digital Europe Programme, in this context means providing hard- and software for research purposes. Finally, the report should clarify whether the initiative includes efforts to bring innovations to the market, and if so, how that would be done.	Section 1 on ***Political and Legal Context*** now makes it clearer that the aim of the initiative is to support cybersecurity industrial and technological development in the EU. The text also points out to most relevant existing cooperation mechanisms in the field of cybersecurity - the Cooperation Group and CSIRT Network under the NIS Directive and explains how this initiative is different. The preferred option would allow supporting cybersecurity industrial policy by conducting activities related not only to research and development but also to market deployment activities both in terms of providing infrastructure for research and innovation as well as undertaking efforts to bring innovations to the market (e.g. through joint procurement of cybersecurity products and solutions to shield critical sectors under the responsibility of the public authorities (the latter one with the exception of defence area). While this was mentioned already in the initial report, a summary point was added in the section "Preferred Option" to provide more clarity in this respect.

5. EVIDENCE, SOURCES AND QUALITY

The Commission gathered qualitative and quantitative evidence from various sources. Sources have been categorized according to the nature of the documents: EU official documents, Reports issued by EU institutions and bodies, Reports issued by other entities and online sources.

5.1. EU official documents

- JOIN(2013) 1 final: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace .
- COM(2015) 192: A Digital Single Market Strategy for Europe.
- COM(2015) 185: The European Agenda on Security (The European Agenda on Security)).
- COM(2016) 410 final: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry.
- JOIN(2017) 450 final: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.
- COM(2017) 477 final: Proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").
- Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

- Council Conclusions 14435/17 on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, adopted by the General Affairs Council on 20 November 2017.
- COMMISSION STAFF WORKING DOCUMENT, SWD(2016) 210 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).
- COMMISSION STAFF WORKING DOCUMENT, SWD(2018) 69 Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and the Council establishing a European Labour Authority.
- H2020 Work Programme 2018-2020 http://ec.europa.eu/research/participants/ portal/desktop/en/funding/reference_docs.html#h 2020-work-programmes-2018-20.
- Tallinn Digital Summit Conclusions, 29 September 2017; https://www.eu2017.ee/news/press-releases/tallinn-digital-summit-conclusions-published-creating-digital-continent.

5.2. Reports, position papers and other sources

- Synergies between the civilian and the defence cybersecurity markets, Final Report, June 2016: https://ec.europa.eu/digital-single-market/en/news/study-synergies-between-civilian-and-defence-cybersecurity-markets.
- Investing in the European Future we want, Report of the independent High Level Group on maximising the impact of EU Research & Innovation Programmes, European Commission, July 2017.
- Cybersecurity Industry Market Analysis Draft Final Report, Leaders in Security (KU Leuven) in collaboration with PriceWaterhouseCoopers, 2017.
- JRC Technical Report: European Cybersecurity Centres of Expertise Map, Cybersecurity Competence Survey, JRC, 2018 (see Annex 4).
- JRC Technical Report: European Cybersecurity Centres of Expertise Map, Definitions and Taxonomy, JRC, 2018 (see Annex 5).
- JRC, Technical Report: European Cybersecurity Centres of Expertise Map, Preliminary Mapping Exercise, JRC, 2018.
- "Position paper on European Cybersecurity Strategy: fostering the SME ecosystem", https://www.digitalsme.eu/digital/uploads/20170731-DIGITAL-SME-Cybersecurity-Position.pdf.
- Internet Organised Crime Threat Assessment (IOCTA), Europol, 2017, https://www.europol.europa.eu/iocta/2017/index.html.
- Supply Chain Attacks, ENISA, August 2017, https://www.enisa.europa.eu/publications/info-notes/supply-chain-attacks.
- Cyber Insurance: Recent Advances, Good Practices and Challenges, November 2016, ENISA: https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges/at_download/fullReport.
- The European Cybersecurity Market, Investment or necessity?, Cybersec Hub, http://cybersechub.eu/files/European-Cybersecurity-Market-Vol.1-Issue-1.pdf.
- ECSO suggestions on the future European Cybersecurity, ECSO, 2018.
- Healthcare Sector Report, ECSO Working Group on Sectoral Demand, March 2018.
- Industry 4.0, ECSO Working Group on Sectoral Demand: Industry 4.0., March 2018.
- Stratégie national sécurité numérique, France, https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf.
- Le livre blanc de la defense 2013, http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf.
- Les budgets nationaux de cyberdéfense en croissance constante, https://www.frstrategie.org/publications/defense-et-industries/les-budgets-nationaux-de-cyberdefense-en-croissance-constante-1-7.
- Selbstbestimmt und sicher in der digitalen Welt 2015-2020 Forschungsrahmenprogramm der Bundesregierung, Self-determined and secure in the digital world 2015-2020 The German Government's research framework programme on IT security https://www.bmbf.de/pub/IT_Security.pdf.
- De Nationale Cyber Security Strategie (NCSS), Slagkracht door samenwerking, The Netherlands, http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/02/28/nationale-cyber-security-strategie.html.

- National Cyber Security Strategy 2, From awareness to capability, The Netherlands, https://www.ncsc.nl/english/current-topics/national-cyber-security-strategy.html.
- "Dutch investments in ICT and cybersecurity: putting it in perspective", The Hague Centre for Strategic Studies, December 2016 https://hcss.nl/report/dutch-investments-ict-and-cybersecurity.
- "Recommendations on Cybersecurity in Europe", European Cybersecurity Industry Leaders, Page 11, https://ec.europa.eu/digital-single-market/en/news/commissioner-oettinger-receives-final-report-european-cybersecurity-industrial-leaders.
- "Net Losses: Estimating the Global Cost of Cybercrime", McAfee & Center for Strategic and International Studies, 2014.
- "Counting the cost – Cyber exposure decoded", Lloyd's and Cyence, 2017.
- "2015 Cost of Cyber Crime Study", Global, Ponemon Institute October 2015.
- "Global State of Information Security Survey", PwC, 2016, http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/.
- "National Cyber Testbed (NCT) Programme", https://www.thehaguesecuritydelta.com/projects/project/89-national-cyber-testbed.
- "Increased coherence and openness of European Union research and innovation partnerships", https://www.hm.ee/sites/default/files/eu_ri_partnerships_final_report.pdf.
- "Shifting Gears in Cybersecurity for Connected Cars", February 2017: https://www.mckinsey.com/~/media/mckinsey/industries/automotive%20and%20assembly/our%20insights/shifting%20gears%20in%20cybersecurity%20for%20connected%20cars/shifting-gears-in-cyber-security-for-connected-cars.ashx.
- "Study on synergies between the civilian and the defence cybersecurity markets" IPACSO (2015), https://ec.europa.eu/digital-single-market/en/news/study-synergies-between-civilian-and-defence-cybersecurity-markets.
- "DARPA Military Researchers ask Industry for new Cyber Security Tools for Large Computer Network", John Keller, 2017, http://www.militaryaerospace.com/articles/2017/06/cyber-security-computer-networks-military-researchers.html.
- "Automated Program Analysis for Cybersecurity (APAC)", DARPA, https://www.darpa.mil/program/automated-program-analysis-for-cybersecurity.
- "The Networking and Information Technology Research and Development Program", https://www.nitrd.gov/pubs/2018supplement/FY2018NITRDSupplement.pdfACEA.
- "Principles of Automobile Cybersecurity", http://www.acea.be/uploads/publications/ACEA_Principles_of_Automobile_Cybersecurity.pdf.
- "Cyber Security M&A Decoding deals in the global Cyber Security industry", IMAA, https://imaa-institute.org/cyber-security-ma-decoding-deals-in-the-global-cyber-security-industry/.
- "Cybercrime Report", Cybersecurity Ventures, 2016.
- "Increased coherence and openness of European Union research and innovation partnerships", Ministry of Education and Research of Estonia, 2017, https://www.hm.ee/sites/default/files/eu_ri_partnerships_final_report.pdf.
- 2017 Global Information Security Workforce Study Benchmarking Workforce Capacity and Response to Cyber Risk, A Frost & Sullivan Executive Briefing and The Center for Cyber Safety and Education partnered with (ISC)2: https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf.
- Europeans' attitudes towards cyber security, Special Eurobarometer 464a, 2017, https://www.cncs.gov.pt/content/files/ebs_464a_en.pdf.
- Europeans' attitudes towards cyber security, Special Eurobarometer 464b, 2017, http://data.europa.eu/euodp/en/data/dataset/S1569_87_4_464B_ENG.
- "The European Cybersecurity Market", Kosciuszko Institute, http://cybersechub.eu/files/European-Cybersecurity-Market-Vol.1-Issue-1.pdf .
- "A platform to experience the intelligent Cybersecurity for the real world", Report on Cisco Cyber Range Service, https://www.servicesdiscovery.com /en/article.php?idx=218 and https://www.servicesdiscovery.com/ download/Cyber_Range_At_a_Glance_2015.pdf.

5.3. International sources and international competence centres

- "The DoD Cyber Strategy", US Department of Defence, 2015: https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

- “IoT Cybersecurity Coalition Letter”, USA Chamber, https://www.uschamber.com/iot%26cybersecurity.
- “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”, President of the USA, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.
- Collegiate Cyber Defense Competition USA – attracting both public and private sectors, http://www.nationalccdc.org/index.php/competition/about-ccdc
- “Factsheet Cybersecurity National Action Plan”, White House.
- “Cybersecurity”, USA Homeland Security, https://www.dhs.gov/topic/cybersecurity.
- NIST Establishes National Cybersecurity Center of Excellence https://www.nist.gov/news-events/news/2012/02/nist-establishes-national-cybersecurity-center-excellence.
- Scalable Quantum Cryptography Network for Protected Automation Communication, US Department of Energy, https://www.energy.gov/sites/prod/files/2017/05/f34/Qubitekk_QKD_FactSheet.pdf.
- High Performance Computing Centre, Stanford University, https://hpcc.stanford.edu/.
- “Global Cybersecurity Index 2017”, ITU, the United Nations specialized agency for information and communication technology, https://www.itu.int/pub/D-STR-GCI.01-2017.
- “National Cyber Security Organisation: ISRAEL”, https://ccdcoe.org/sites/default/files/multimedia/pdf/IL_NCSO_final.pdf.
- “Structuring Israel’s Cyber Defense”, INSS, 2016, http://www.inss.org.il/publication/structuring-israels-cyber-defense/.
- “World Development Report 2016: Best Practices and Lessons Learned in ICT Sector Innovation: A Case Study of Israel”, http://pubdocs.worldbank.org/en/868791452529898941/WDR16-BP-ICT-Sector-Innovation-Israel-Getz.pdf.
- The Cybersecurity Sector in Israel, Preliminary Market Analysis, Embassy of India, Tel Aviv, 2015, http://www.indembassy.co.il/pdf/Report-on-the-Cybersecurity-Industry-in-Israel.doc.
- “6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry”, https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/#6e555ab3420a.
- “Israel accounts for 16 percent of global cybersecurity investment, second only to U.S.”, https://www.cyberscoop.com/israel-cybersecurity-venture-funding.
- Canada adds new cybersecurity center, hikes funding for electronic spy agency, https://www.defensenews.com/international/2018/02/28/canada-adds-new-cybersecurity-center-hikes-funding-for-electronic-spy-agency/.
- 2018 Federal Budget: Focus on Data and Data-Driven Technologies, https://www.canadiancybersecuritylaw.com/2018/03/2018-federal-budget-focus-on-data-and-data-driven-technologies/.
- The Australian Cyber Security Strategy 2016: Where is the money going? https://www.itsecuritytraining.com.au/articles/australian-cyber-security-strategy-2016-where-money-going.
- The Australian Cyber Security Centre (ACSC), website https://www.acsc.gov.au.
- Cybersecurity Strategy, Government of Japan, 2015, https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf.
- Defence programme and budget of Japan, Ministry of Defence, http://www.mod.go.jp/e/d_budget/.
- Japan Cyber Readiness at a Glance, Potomac Institute for Policy Studies, 2016, http://www.potomacinstitute.org/board-of-regents/150-cyber-readiness-index/cyber-readiness-translations/2437-japan-cyber-readiness-at-a-glance.
- Keio Establishes World's First InterNational Cyber Security Center of Excellence (INCS-CoE), https://www.keio.ac.jp/en/news/2016/Nov/15/48-18788/.
- “NUS launches shared national cybersecurity infrastructure to spur research and test innovations”, National university of Singapore, 2017, http://news.nus.edu.sg/press-releases/nus-launches-shared-national-cybersecurity-infrastructure-spur-research-and-test.
- Budget 2018-19: Government May Allocate Funds For Cyber Security, http://www.india.com/news/india/budget-2018-19-government-may-allocate-funds-for-cyber-security-2833070/,

5.4. Online Sources

- “A conversation with Jarno Limnéll on Cybersecurity and the Digital Summit”, Interview of Professor Jarno Limnéll by the Estonian Presidency, October 2017, https://e-estonia.com/a-conversation-with-jarno-limnell-on-cybersecurity-and-the-digital-summit.
- “The EU as a Coherent (Cyber) Security Actor?”, http://onlinelibrary.wiley.com/doi/10.1111/jcms.12575/pdf.
- How the Fraunhofer Institutes’ funding model contributes to success, https://www.eef.org.uk/campaigning/news-blogs-and-publications/blogs/2013/jul/fraunhofer-friday-part-2--how-the-fraunhofer-institutes-funding-model-contributes-to-success,
- CERN, Website, https://home.cern/about/structure-cern,
- Who funds CERN’s research, https://voisins.cern/en/en-bref/who-funds-cerns-research,
- ECSEL Joint Undertaking, Electronic Components and Systems for European Leadership, http://www.ecsel-ju.eu,
- JRC, Smart Grid Laboratories Inventory, JRC, 2016, http://ses.jrc.ec.europa.eu/smart-grid-laboratories-inventory,
- “FireEye Releases First Mandiant M-Trends EMEA Report”, https://www.fireeye.com/company/press-releases/2016/fireeye-releases-first-mandiant-mtrends-emea-report.html.
- “What Are The Biggest Challenges Facing The Cybersecurity Industry?”, https://www.forbes.com/sites/quora/2017/09/15/what-are-the-biggest-challenges-facing-the-cybersecurity-industry/#41f0e4372d62.
- “Key Reinstallation Attacks. Breaking WPA2 by forcing nonce reuse”, https://www.krackattacks.com/.
- “Spectre and Meltdown processor security flaws – explained”, https://www.theguardian.com/technology/2018/jan/04/meltdown-spectre-computer-processor-intel-security-flaws-explainer.
- “Ransomware’s history and evolution in facts and figures”, https://www.kaspersky.com/blog/ransomware-blocker-to-cryptor/12435/.
- “The MeDoc Connection”, http://blog.talosintelligence.com/2017/07/the-medoc-connection.html.
- The ACDC project launched by EU: https://www.acdc-project.eu/,
- The Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSOS, FP7) http://www.nessos-project.eu,
- Main Science and Technology Indicators, OECD, http://www.oecd.org/sti/msti.htm,
- “China’s ghost in Europe’s telecom machine”, https://www.politico.eu/article/huawei-china-ghost-in-europe-telecom-machine/.
- “Special Issue ‘Surviving the Valley of Death”, https://www.journals.elsevier.com/technovation/call-for-papers/special-issue-surviving-the-valley-of-death.
- “High Performing Aviation for Europe”, http://www.sesarju.eu/.
- “List of 200 cybersecurity startups that received venture capital in 2017”, Steve Morgan, CEO at Cybersecurity Ventures and editor in chief of the Cybersecurity Market Report.
- “Dragonfly: Western energy sector targeted by sophisticated attack group”, Dragonfly, 2017, https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks.
- The Cyber Security Body Of Knowledge, Project website, https://www.cybok.org

With regard to the quality of the evidence, the following points must be noted:

For the purpose of mapping the centres of expertise, the Commission developed a comprehensive taxonomy of cybersecurity. However, it is to be noted that such taxonomy is not universally agreed upon and may include or exclude areas that would otherwise be included or excluded in other taxonomies. However, the Commission went to great lengths to take into consideration all relevant standards and consult with stakeholders, including the research and industrial communities, which have either developed or are working on similar projects. This is one of the issues that this initiative itself would tackle.

The quality of this report is impacted by the overall scarcity of evidence in the field of cybersecurity as a whole.

Annex 2: Stakeholder consultation

1. Stakeholder consultation strategy

Cybersecurity is a broad, cross-sectoral topic. The Commission used different consultation methods in order to make sure that the Union's general public interest – as opposed to special interests of a narrow range of stakeholder groups – is well reflected in this initiative. This method ensures transparency and accountability in the Commission's work.

In order to identify the most appropriate mix of consultation methods, the first step has been to identify the relevant stakeholder groups (please see section 2.1 of this Annex).

The second step has been to identify the best way to consult them in order to gather relevant input. The Commission pays attention to differentiate data gathering tools and adapts them to different types of contributions the stakeholders might have.

While no open public consultation was conducted specifically for this initiative given its target audience (industrial and research community and Member States), the thematic was already covered by several other open public consultations:

- A general open public consultation carried out in 2018 on the topic of security in relation to the next MFF. For results, see section 4.1.1.
- A general open public consultation carried out in 2018 on the topic of investment, research & innovation, SMEs and the single market. For results, see section 4.1.2.
- A 12-week online public consultation launched in 2017 to seek views of the wider public (approx. 90 respondents) on ENISA evaluation and review.
- A 12-week online public consultation that was carried out in 2016 at the occasion of the launch of the contractual public-private partnership on cybersecurity (approx. 240 respondents).

The Commission also organised targeted consultations on this initiative including workshops, meetings and targeted requests for input (from ENISA and EDA).

The Commission also analysed the feedback to the Inception Impact Assessment published at "Have Your Say" website, which allows citizens and stakeholders to contribute to EU policy and law-making process.

The consultation period spanned over 6 months, starting in November 2017 until March 2018.

2. Identification of groups of stakeholders consulted, means of consultation, and consultation topics

2.1 Whom has the Commission consulted?

A list of stakeholders that have been consulted either directly, or through consultation efforts related to open public consultations on the thematic, includes the following bodies:

- The EU Member States national authorities;
- Member State's local and regional administrations taking part in public-private partnership on cybersecurity
- European Commission's services;
- Industrial community representing both supply and demand side of cybersecurity products and solutions, including SMEs – through European Cybersecurity Organisation, which includes a wide variety of stakeholders such as large companies, SMEs and Start-ups, end-users, operators, clusters and association

- Cybersecurity competence centres across Europe - apart from reaching to the members of the public-private partnership on cybersecurity, the Commission also conducted a mapping exercise of relevant centres of expertise across the EU. In addition to desktop research conducted by the Commission services, a self-registration survey allowing cybersecurity expertise centres across Europe to declare their know-how, activity and achievements was launched, to which 665 cybersecurity expertise centres registered by 08 March 2018
- Relevant EU agencies bodies, including targeted consultation activities with European Network and Information Security Agency (ENISA) and European Defence Agency (EDA);
- Citizens

2.2 How has the Commission consulted stakeholders?

Different tools and methods were used in order to conduct the consultation.

- **Mapping of centres of expertise** conducted jointly by DG CONNECT and JRC, which allowed to gather input from 665 cybersecurity expertise centres across Europe and Associated countries on their know-how, activity, working fields, international cooperation. The survey was launched in January and closed on 08 March 2018. (see Annex 4).
- **Targeted Consultations:**
    - A series of targeted workshops and meetings:
        - **Consultation workshop with competence centres** - on 23 February 2018 the Commission organised a full-day consultation workshop with cybersecurity expertise centres from across Europe to exchange views on, among others, possible ways of reinforcing the EU cybersecurity research capabilities; better coordinating research and innovation efforts with the industry partners; and promoting industrial innovation and competitiveness. Given the big number of cybersecurity expertise centres across the EU, a list of executive-level invitees to the workshop was prepared taking into consideration the activities of the cybersecurity centres (scientific criteria such as e.g. publications and patents), geographical balance and results of the mapping of the cybersecurity expertise centres across the EU conducted by the Joint Research Centre (JRC). Last but not least, Member States were asked to provide additional suggestions of possible participants.

        - **Consultation with the Management Board of the European Cybersecurity Organisation** – the European Commission's counterpart in the contractual Public Private Partnership during a meeting held on 21 March 2018. The representatives of the Board include high-level representatives of cybersecurity companies and SMEs, cybersecurity associations across the EU, representatives of users/operators community, representatives of public administration, research and technology organisations, universities as well as of regional structures e.g. cybersecurity clusters.

        - **Consultation workshop with industry, research community and Member States -** on 22 March 2018 the Commission organised a full-day consultation workshop with the representatives of industry (supply and demand side), competence centres as well as Member States to discuss current challenges, gaps and best ways to mitigate them to ensure that the EU has the capacity to autonomously secure its economy, society and democracy against cyber threats. The workshop also identified the areas where the Network and the Centre would provide added-value to the work already done at the national level.

- **Consultation with the Management Board of ENISA** (15 March 2018) as well as **a request for targeted contribution**, which ENISA provided in April 2018.

- **Consultation** with **European Defence Agency through a targeted request for contribution**, which EDA provided in April 2018.

- **Consultation activities with Member States:**

  - High Level Roundtable chaired by Vice President Ansip on the creation of Cybersecurity Network and Competence Centre (5 December 2017),
  - Bilateral meetings with Member States' national cybersecurity authorities
  - Discussions with Member States in the Programme Committee at the occasion of launching a Pilot Project
  - Discussions at the Council Horizontal Working Party on Cyber (08 March 2018)
  - Discussions at the 22 March 2018 workshop, where Member States were invited

3. HAVE THE COMMISSION STANDARDS BEEN MET?

The Commission standards as set in the Better Regulation Guidelines have been met. At the same time please see the exception to the Better Regulation Guidelines identified in Annex 1, Section 3.

4. LEARNINGS FROM THE CONSULTATION PROCESS

4.1 Learnings from Open Public Consultations on the next generation Multiannual Financial Framework

Both open public consultations presented below were launched in the context of the proposals for the next generation of financial programmes for the post-2020 Multiannual Financial Framework (MFF), which is the EU's long–term budget. These consultations are part of a careful assessment both of what has worked well in the past and what could be improved in the future and their objective is to collect the views of all interested parties on how to make the most of every euro of the EU budget. These consultations are highly relevant for the initiative covered by this Impact Assessment, given that it is meant to be the main implementation mechanism for cybersecurity funds under different MFF Programmes.

4.1.1 The general open public consultation on the topic of security in relation to the next MFF

This consultation ran from 10 January until 8 March 2018 and was open to all citizens, organisations and stakeholders with an interest and/or involvement in issues related to security.

This consultation collected the views of 153 respondents. 114 replies were sent on behalf of organisations while 39 were coming from individuals. Respondents were given a list of pre-identified policy challenges for the future of Europe, in which respondents had to identify which challenges were the most important in their opinion. “Promoting strong cybersecurity” comes as the second challenge[3] perceived to be “very important” by respondents, with 64.05% of respondents choosing this option. These results confirm the earlier results of the 2017 Eurobarometer, which identified cybercrime as one of the first forms of crime citizens are worried about. At the same time, 43.52%[4] of respondents consider that the current programmes/funds address only to some extent, or do not address at all the promotion of strong cybersecurity in the EU.

[3] The first policy challenge identified as “very important” was the fight against cross-border crime, including terrorism, with more cooperation between law enforcement authorities (73.20%).

[4] 41,83% of respondents believe that strong cybersecurity is addressed to some extent only, while 1,96 % believe they are not addressed at all.

4.1.2 The general open public consultation on the topic of investment, research & innovation, SMEs and the single market in relation to the next MFF

This consultation ran from 10 January until 8 March 2018 and was open to all citizens, organisations, SMEs and stakeholders with an interest and/or involvement in issues related to investment, entrepreneurship, research and innovation.

This consultation collected the views of 4052 respondents, including 2244 organisations and 1808 individuals. 81.10% of respondents identified the need to foster research and innovation across the EU as "very important". Thus making this the first policy challenge deemed very important by respondents in this consultation. This is particularly relevant to the present initiative as fostering research and development through the pooling of efforts and resources is one of the key objectives of the proposal for a network and Competence Centre.

This initiative also aims to support education, skills and training which is the second policy challenge deemed "very important", with 62.86% of respondents choosing this option. The Commission noted the recurrent mentioning of the cyber skills gap by stakeholders including the cybersecurity industry, which is lacking experts in the field[5], and aims to address this issue with the present initiative.

4.1.3 The online public consultation on ENISA evaluation

The open public consultation on the evaluation and review of ENISA took place between 18 January and 12 April 2017. The public consultation aimed to gather the views of stakeholders on evolving needs and challenges in the cybersecurity landscape and to evaluate ENISA's overall performance. The results of this consultation were insightful for the purpose of this impact assessment as they highlighted gaps and challenges in the current cybersecurity ecosystem identified by the stakeholders, and their perception on the progress achieved since the 2013 Cybersecurity Strategy.

Main results related to the questions on the broad cybersecurity ecosystem:

- Respondents identified a number of gaps and challenges for the future of cybersecurity in the EU; in particular the top 5 (in a list of 16) were: the cooperation across Member States in matters related to cyber security; capacity to prevent, detect and resolve large scale cyber-attacks; cooperation and information sharing between different stakeholders, including public-private cooperation; protection of critical infrastructure from cyber-attacks; skills development, education and training of professionals.
- Respondents were also asked if the current instruments and mechanisms at the European level are adequate to promote and ensure cybersecurity in relation to the needs previously identified. Only 6% of the respondents judged the current instruments and mechanisms at the European level (such as regulatory framework, cooperation mechanisms, funding programmes, EU agencies and bodies) to be "fully adequate" to promote and ensure cybersecurity. 83% of respondents regarded them as either "partially" or only "marginally adequate" and 5% found them "not at all adequate". National authority respondents appear to be more positive about the adequacy of these instruments and mechanisms in comparison with representatives of private enterprises or business associations and "other" respondents.

4.1.4 The online public consultation that was carried out at the occasion of the launch of the contractual Public Private Partnership on cybersecurity.

The public consultation on the contractual Public Private Partnership on cybersecurity took place from 18 December 2015 to 11 March 2016. Respondents represented a wide variety of organisations, with a good balance between big businesses (41), SMEs (33), microbusinesses (6) as well as other stakeholders e.g. research bodies (20), national public administrations (7) and regulators (1), NGOs

[5] These remarks were noted during bilateral meetings with stakeholders and during the first workshop organised for this initiative (summary of which can be found in Annex 2, section 4.2.1).

(13). While the first steps to tackle some of the challenges identified by the consultation were taken with the creation of the contractual public private partnership for which it was conducted, due to inherent limitations of this instrument as described in section 2.3.2 of the Impact Assessment the following challenges are still relevant:

- **Competitiveness and EU's technological dependency:** The majority of respondents to the survey saw Europe's cybersecurity market as insufficiently competitive in several areas. Among the reasons mentioned is technological dependency on security solutions (software and hardware) produced or supplied by vendors headquartered in other regions of the world. It was also observed that there is not a single EU company that offers integrated security solutions for the whole (IT) value chain. Instead, the EU market is described by respondents as being dominated by large global vendors from outside the EU, whereas European suppliers are operating in specific niches and the majority of them is small in size. More than 44.3% of respondents (78 out of 176) also stated that they experience barriers related to market access and export within the EU and/or beyond EU countries, particularly due to the fragmentation of the EU cybersecurity market along with EU internal borders. A large majority of respondents (60,8%) state that a shortage of supply in Europe jeopardize the security of the whole digital value chain.
- **Insufficient access to finance, especially for SMEs** - the majority of respondents (75%) felt access to finance for their cybersecurity initiatives or projects is a challenge.
- **Insufficient human capital at industry's disposal** - the large majority of respondents (73.3%) felt that ICT security and supply industry in Europe did not have enough skilled workforce at its disposal. There was a consensus among respondents on the lack of cybersecurity experts. One of the challenges mentioned in this context is that cybersecurity experts are not produced by Universities and other training institutes, but rather develop an extensive practical competence over time, both to become an expert and to keep their knowledge and skills up to date.

4.2 Learnings from workshop with Cybersecurity Centres of expertise

4.2.1. Workshop with national cybersecurity competence centres

On 23 February 2018 DG CONNECT organised **a full-day consultation workshop with cybersecurity expertise centres from across Europe** to exchange views on, among others, possible ways of reinforcing the EU cybersecurity research capabilities; better coordinating research and innovation efforts with the industry partners; and promoting industrial innovation and competitiveness.

Given the big number of cybersecurity expertise centres across the EU, a list of executive-level invitees to the first workshop was prepared taking into consideration the activities of the cybersecurity centres (scientific criteria such as e.g. publications and patents), geographical balance and results of the mapping of the cybersecurity expertise centres across the EU conducted by the Joint Research Centre (JRC). Last but not least, Member States were asked to provide additional suggestions of possible participants in case they felt that the list prepared by the Commission services should be complemented with other centres.

The workshop gathered therefore experts in cybersecurity with a broad overview of the cybersecurity research landscape, needs and challenges. The represented institutions included a number of leading cybersecurity centres across Europe.[6]

[6] **Belgium:** KULeuven; **Croatia:** University of Zagreb; **Estonia:** Tallinn University of Technology, Centre of Digital Forensics and Cyber Security **AND** Estonian Information System Authority; **Finland:** VTT Technical Research Centre of Finland **AND** Helsinki-Aalto Center for Information Security; **France:** INRIA Institut National de Recherche en Informatique et en Automatique **AND** TELECOM ParisTech, INFRES Network and Computer Science Department **AND** CEA - Commissariat for Atomic Energy and Alternative Energies; **Germany:** Fraunhofer Institute **AND** Ruhr University Bochum - Horst Görtz Institute; **Greece:** Department of Computer Science, University of Crete **AND** University of Pireaus Security Lab; **Ireland:** Centre for Cybersecurity and Cybercrime investigation, University College of Dublin; **Italy:** Institute for Informatics and Telematics, Consiglio nazionale della Ricerca **AND** National Laboratory for Cybersecurity; **Luxembourg:** SECURITYMADEIN.LU; **Netherlands:** The cybersecurity group, Delft University; **Poland:** Division of Cybersecurity, Warsaw University of Technology, Faculty of Electronics and Information Technology; **Portugal:** University

Summary of the workshop outcomes:

Though a full-day discussion a number of key challenges and related needs of the research community were identified by the participants, where the EU-action would be of added-value:

- ***Need to align resources & create lasting structures of cooperation/exchange and knowledge management***: Participants agreed with most of the initial conclusions of the cybersecurity expertise centres' mapping presented by the Joint Research Centre, which showed that:
  - The capacities in Europe are dispersed. While there are many teams working on cybersecurity issues, they are often quite small and scattered across Europe, which often does not allow deploying a critical mass of resources to solve cybersecurity challenges.
  - Many expertise centres do research across many cybersecurity domains but with small teams. Europe could have the potential to cover the whole cybersecurity value chain if Member States/centres would specialise in different domains and exchange knowledge and expertise.
  - There are important areas of cybersecurity which are not sufficiently covered by the current efforts. Participants agreed that this might be due to limited resources and inaccessibility to necessary infrastructure (e.g. experimentation/testing facilities).
- ***A strong need to gather industry, academia, government and users together:*** Participants have largely brought to light the need of creating a common place that would ideally fill a perceived gap between the academia and the industry. Europe needs to have a place that would become a real engine for research and investment, with the capacity of being an attractive working place with good conditions for its experts. Also, participants gave as a model an entity that would be the middle point between industry and academia and which would attract the best experts (e.g. the MITRE institute in the US). Participants also noted that there is a semantic gap between government, industry and academia with regard to expectations from each other. Creating a common platform to bring these communities together and exchange views on strategic challenges could help accelerate European progress in the cybersecurity field. In this context participants emphasised that collaboration does not necessarily happen spontaneously. It is important to have, apart from funds, human resources to animate and sustain it.
- ***Need for interdisciplinary approach*** - participants emphasised that the cybersecurity is a very broad and complex area, which requires a multidisciplinary approach. Europe should put in place mechanisms allowing researchers from different areas (e.g. ICT, engineering, psychology, legal) to work together as challenges cannot be resolved by experts of one discipline only. Participants emphasised that this very often boils down to having a place for all those people to come/meet to discuss challenges and work together on common projects. In this context, participants highlighted the need to provide access to widest possible set of skills and knowledge as one entry point/one shop stop across Europe. They mentioned that Europe needs a dedicated cybersecurity knowledge management space/expertise hub, where there is data and means, and where experts can meet and address common challenges. Participants underlined the current problem of small organisations to conduct broader research (e.g. sometimes it is even not possible to buy basic small standards for software).
- ***Need of "infrastructures"/"capacities" for researchers in Europe***: Participants highlighted the need to reinforce the access of European researchers to testing and experimentation infrastructure. The examples given included access to hardware (e.g. access to HPC), software (e.g. access to AI, creation of software testing platforms) or real time data sets. This was supported by a comparison with the opportunities available in the US, where researchers and industry have access to very large scale real time data and laboratories where these can be tested helping them to advance their

of Porto – Centro de Competencias em Ciberseguranca e privacidade; **Spain:** Centro nacional de Protección de Infraestructuras y Ciberseguridad **AND** INCIBE (Instituto Nacional de Ciberseguridad);

projects and get them to the market. Participants warned about the current state-of-play where innovation is led by large private companies from outside Europe. Participants encouraged collaborative co-investing in large scale experimentation, which could be then used by researchers from across Europe.

- ***Need to address deployment challenges*** – the participants emphasized the challenges related to getting the outcomes of the research projects to the market.
  - The misalignment in the supply-demand timeline was highlighted working as an obstacle to the translation of research, including EU-funded research, into marketable products. This in turn makes it difficult to compete with off-the-shelf products supplied by global players already present on the market (e.g. an operator will buy the product made elsewhere because the EU funded one takes too long to enter the market).
  - Participants accentuated the current challenge of the dissemination and communication on the entry onto the market of new EU products.
  - Finally, participants largely asserted that H2020 is a well-functioning instrument but evoked a paramount need to continue supporting projects after their completion to help them overcome the "*valley of death*". Europe should find an effective mechanism to support the full innovation cycle.
  - In addition, the H2020 framework was acknowledged as a good incentive for encouraging start-ups. However, participants mentioned the need of new mechanisms and category of project reviewers with a "venture capital type of approach", which would be mandated to take the risk to invest in promising start-ups/SMEs as they can yield great results. Further support mechanisms such as e.g. European incubator for cybersecurity start-up to leverage their solutions would be desirable.
- ***Cybersecurity skills gap and brain drain:*** Participants emphasized the current gap in cyber skills. Participants have largely called for more action in countering the actual "skills gap" and related "brain drain".
  - There is a strong need to increase the number of engineers and other profiles specialised in cybersecurity.
  - There is a need for more structural support to cyber skills that would go beyond providing funding to researchers (e.g. in FP9-projects) only.
  - The "skills gap" is currently linked not only to not having enough people specialising in cybersecurity but also to not losing the best of the educated and specialized ones, who in a highly competitive global market decide to leave Europe. There is an urgent need for creating an attractive work environment in order for the EU's best assets to remain. In this context the basic resource challenges in smaller institutes were mentioned. This is challenge, according to participants, is also very much linked to the access to testing/experimentation facilities.
  - In this context participants emphasised that there is a strong lack of instrument for continuous academic collaboration (not only on an ad-hoc, project basis). Additionally, some participants brought forward the need of considering the opportunity of offering more PhDs and MAs programmes for students in the EU.
- ***Dual use and possible link with defence***: Although a multi-dimensional approach is needed in the conceptualization of the competence centre, the defence sector deserves particular attention. On the one hand, some participants raised the challenge of the involvement of civilian entities in defence projects due to applicable law. On the other hand, other participants reported good and effective cooperation with the national Ministries in charge of Defence. The benefits of having additionally civil research on defence were highlighted. Besides emphasizing the currently limited synergies between civilian and military sectors, participants acknowledged that addressing dual-use synergies is necessary. At the same time, some participants emphasised that the issue of "mutual trust" is crucial in case of dual-use projects conducted by civilian and military sectors

(e.g. because of the need to access classified data). Therefore, trust building efforts will be essential for a good achievement of the cooperation.

- ***Added-value of creating the network and the Centre -*** participants welcomed the idea and emphasised that the Centre and the network could add value to the current efforts on the national level by:
  - Helping create Europe-wide cybersecurity ecosystem
  - Helping research and industries communities to work together
  - Helping the community work with a longer-time, strategic perspective
  - Ensuring access to key capabilities such as testing and experimentation facilities, which could be used by the network of expertise centres across Europe.
  - Helping achieve interdisciplinary approach to cybersecurity in Europe
  - Becoming a knowledge management platform, which could be used by the whole cybersecurity community
  - Helping close the cybersecurity skills gap and preventing brain drain by offering interesting research challenges for young researchers (e.g. large-scale, ambitious European projects attracting highly-skilled people)
  - Ensuring visibility of European cybersecurity know-how and competence both within the EU and globally;

At the same time, the participants emphasised that the key to success will be a well-defined role of the Centre and an inclusive, collaborative approach to the network to avoid creating new silos. Participants also emphasised the fact that the structure will have to be flexible to be easily adaptive as cybersecurity is a fast-moving and fast-pace environment.

Last but not least participants shared a number of challenges where aggregating efforts across the network and pulling European resources could bring added-value:

- Hardening software/hardware - building trustworthy systems on top of untrustworthy ones.
- Working towards "every device as a non-compromisable device". While this might be not totally feasible in practice, working towards a far-fetched goal brings often surprising side-results (e.g. an US research project, which managed to create a system which sustained attacks for 6 weeks compared to usual much shorter limits (measured in days if not hours))
- Vulnerabilities and certification of products
- Blockchain; Artificial Intelligence; Post-quantum encryption
- European projects (across different sectors) that are secure by design
- Tools to protect against massive malicious attacks (e.g. state-sponsored cyber-attacks)
- Resilience and recovery mechanisms (stress testing)
- Tools allowing to learn fast when the system was compromised
- Societal challenges with essential security aspects: e.g. digital identity, online voting, connected cars;

4.2.2. Workshop with Industry, Research community and Member States

On the 22th of March 2018, a full day high-level consultation workshop was organised. The workshop gathered about 100 stakeholders from industry (both supply and demand side, research community and national and public authorities. It allowed gathering stakeholders' views on whether there is a need for increased cooperation at the EU level as well as on possible priorities and strategic orientations for the network of the competence centres with the European Research and Competence Centre at its heart. The discussion generally confirmed the challenges identified during the workshop on 23 February and provided some practical suggestions for possible actions. During the workshop, the Commission also presented the preliminary results of the cybersecurity competence centres' mapping undertaken in the recent months (see point 4.3 of this Annex).

Workshop Conclusions:

Main challenges of the network and the Centre - The participants identified several needs and challenges existing in the area of cybersecurity that in majority were consistent with the ones identified during the workshop in February. Therefore, this part will highlight the main needs/challenges and summarise new challenges and findings:

- ***Need for alignment and connection of economic/industrial strategies and research goals***: The participants highlighted the need to create a clear connection between industry and research that should be supported by a strategic approach at the EU level. Such approach should involve a framework that would ensure possibility of planning not only in the medium but also in the long-term. The participants highlighted that there is a strong need for such strategic cooperation to focus on both priorities and ideas as well as on funding. It was also highlighted that while such cooperation is needed it should leave the space for the competition in a market and allow flexibility to address challenges from evolving cybersecurity environment. Some participants pointed out that there is a need to take into account and use existing competences and capacities of the Member States.

  The participants stressed as well the need of continuing the basic research for the years to come, as this will allow Europe to develop and innovate beyond the market needs at a given moment.

- ***Need for interdisciplinary approach:*** As during the previous workshop, the participants indicated the need for working together across different sectors, as well as along value-chain. Some participants pointed out to the necessity of interoperable solutions, as well as the need for raising awareness on cybersecurity among companies on the demand side and for addressing sectoral needs.

- ***Need of "infrastructures"/"capacities" in Europe***: participants from both industrial and research communities emphasised that there is a strong need for creating shared competences, infrastructure and testing facilities (a possibility could be considered to open current facilities to other users and fill in the gaps by creating the lacking ones);

- ***Need to address deployment challenges***: the participants stressed the need for developing a clear industrial strategy for the EU. At the same time, many participants highlighted the need to involve and give the opportunity to participate for the SMEs that could benefit from the economy of scale. In this context, the participants stressed the need for a more strategic approach to public procurement.

- ***Need to gather industry, academia, government and users together:*** similarly to the first workshop, the majority of participants raised this issue. The need to create a reliable system of trust in a digitalized world that would be based on two-way collaboration was highly visible. Some participants pointed out that while linking competences spread in the EU, there is also a need to allow the cooperation in smaller groups and ensure flexibility.

- ***Dual use and possible link with Defence***: the participants on one hand stressed the need for multidisciplinary approach which could include the civil and military initiatives but on the other hand special position and characteristics of the defence sector were also mentioned to be taken into account.

- ***Need to close the cybersecurity skills gap and preventing brain drain:*** the participants raised this issue similarly to the discussions during the first workshop and stressed that the EU should offer interesting research challenges for young people.

Recommendations - In response to these challenges, participants also formulated recommendations regarding the network and the Centre:

- Strategic <u>leadership</u> in the EU. A strategic plan developed at the EU level is recommended, together with coordination and leadership needed;

- Connection between <u>research and industry</u>, both on the demand as on the supply side (‘applied’ and ‘sectorial’ research);

- <u>Research</u> that serves the industry in the short term, but also funding and supporting the long-term research;

- The possibility to invest and fund bigger projects, also allowing to benefit from the economy of scale; need to develop testing facilities and build common infrastructure;
- Need to create a framework for a two-way collaboration;
- Help to include various stakeholders;
- Creation of common rules/principles of procurement;
- Improving education at early stages and ensuring reduction of skills gap. Creating a platform that offers interesting work and keeps young people in Europe;
- More efficient dialogue between industry and academia;
- Help to create trust for cross-border solutions, strengthening capacities in the EU;
- Creation of both the Centre and the network of competence centres to overcome fragmentation in the EU but allowing flexibility. The centres of the network must have their independence. The mission and mandate of the Centre must be clearly stated;
- Make use of smart tools, such as trade agreements;
- Create a place to share ideas and newest technology/tools.

4.3 Learnings from the EU Survey for the self-registration of Centres

The main learnings from this survey are presented below. For a full analysis of the mapping exercise and survey please refer to Annex 4. The survey was open for participation from middle January until middle March of 2018 and over 665 centres participated.

The preliminary analysis of the survey results and the desktop research mapping exercise[7] provides a detailed and complex picture of the situation of cyber-security research in Europe.

In general, the full picture provided by this analysis shows a European cybersecurity research community vibrant, productive and recognised at global level, which however has often difficulties in reaching the critical mass to truly make the difference, and which is not always able to tightly connect with the industry.

Answers of the survey related to the domains covered by the research centres in Europe show that there are competencies in all the domains identified in the EU Cybersecurity Taxonomy, however the analysis of research subdomains in fact shows that the real coverage of the subdomains is heavily jeopardised with the majority of the centres active in the reality only in a minor number of sub-fields. This means that a full coverage of the cybersecurity domains by European players is far from being complete. The same trend was observed at the country level.

The analysis of the sectors of application of cybersecurity research, as well as of the technological applications covered, shows again a heterogeneous landscape at Member State level, with some sectors developed in few countries, and poorly developed in all the others.

Looking at the distribution of the scientific production among European institutions, the scientific literature analysis per domain shows that each domain is dominated by a restricted number of institutions in term of number of publications, and that the numerical difference between the top 10 for each domain and the rest of the institutions publishing in that domains is not negligible. In other words, the picture that the analysis of scientific publications combined with the results provided by the survey gives, is that of a Europe where few institutions polarise the scientific production and are able make a difference in the domain.

Looking at the ratio between scientific publications and patents, the report concludes that it seems evident that to the relatively high scientific production does not automatically correspond an equal “innovation” push.

[7] JRC Technical Report “European Cyber Security Centres of Expertise, Preliminary Mapping Exercise”

For what concerns the collaborations between industry and academy, the H2020 programme had surely contributed to strengthen the relations between industry and academy but it also showed that few institutions were successful to access the H2020 funds continuously. This created polarisation with only institutions from some Member States benefiting while others benefiting more from national funding and limited international collaboration.

These last considerations call for the definition of new measures to:

- Strengthening and enlarging the collaboration of cyber-security research organisations across Member States;
- Streamline and stabilise the R&D cooperation between industry and academy;
- Better coordinate research funding across the Union;
- Co-design of research plans between funding bodies and recipients;
- Support the sharing of highly expensive infrastructures (in an Open Laboratory initiative fashion).

4.4 Learnings from the contributions from EU agencies and other bodies.

The EU agencies EDA and ENISA were requested to provide their contribution in the consultation process. The main points are presented below.

4.4.1 European Defence Agency contribution

The European Defence Agency drew attention to their work promoting capability development in the field of cyber defence through intergovernmental cooperation among Member States.

In their contribution, EDA pointed out that cross-sectoral research agendas, identification of areas where civil/military efforts and investments could be combined, development of common training and exercises curricula or conduct of coordinated or joint cyber activities could be some of the topics where a future Cybersecurity Competence Centre and Networkcould add value. The Network and Centre should build upon and seek for complementary efforts to the existing structures/mandates and competences (e.g. beyond EDA also of other entities which are active in similar fields such as the European Security and Defence College-ESDC) as well as to map and define the role of all actors. EDA stressed the need for synergetic approach with these actors.

The main issues from the defence perspective are: to reflect Member States armed forces' needs, to take into account the specificity of the defence sector (question of national sovereignty, differences in the cyber technologies application, the industry competencies should be addressed to fill the capability gaps of the Member States and prioritisation should follow this approach.) With regard to cyber defence funding priorities that have been identified with Member States and that cut across also the civilian sector, a coordinated action and co-funding could be elaborated. Such approach could be envisaged not only in the field of research but also in the field of capabilities.

EDA also sees a task for the Centre in development and maintaining an overview on cybersecurity related activities, raising awareness of all relevant national and EU entities' activities, support synergies and cross-fertilisation. A synergetic approach to testing on requirements and solutions between the cybersecurity network and Centre and EDA could promote effective solutions.

4.4.2 ENISA contribution

A discussion on the creation of the network of competence centres with a European Research and Competence Centre at its heart took place at the ENISA's Management Board on 15 March 2018. Additionally, ENISA provided a reply to the targeted consultation in April 2018 welcoming the Commission's proposal and strongly supporting its goal of increasing coordination and enhancing cybersecurity competencies within the European Union. According to ENISA, the proposal of the European Cybersecurity Competence Network Centres offers a great opportunity to supplement existing policy measures by specifically targeting the cybersecurity competencies that underlie these existing instruments.

ENISA identified the following priorities that the Centre and the network should focus on: developing of the strategy and governance system, identifying its short/long term objectives; developing and maintaining Digital Skills throughout the EU and prioritising technical work. The network and the Centre should cooperate with other important cybersecurity actors and networks (such as Europol EC3, EDA, CERT EU within the EU institutional framework and with established industry networks in the private sector), provide input to the relevant policy development. ENISA believes it could substantially contribute to the project being well position in the cybersecurity environment, among other through supporting networking activities and helping the Network and the Centre develop their strategies.

4.4.3 European Cybersecurity Organisation's contribution

The Management Board (MB) of the European Cybersecurity Organisation's – the Commission's counterpart to the contractual Public Private Partnership (cPPP) on cybersecurity provided a contribution to the targeted consultation in April 2018.

Within the network of cybersecurity competence centres, the cPPP MB envisions clusters of competence centres contributing to the development of a full trustworthy European value chain: standards, certification, trustworthy elements of the supply chain for different applications / vertical sectors (also transversal technologies used in different verticals).

Local / regional / national critical infrastructure / essential services would be used as platforms for introducing and validate trustworthy innovations. They would improve R&I approaches to better bring research to market based upon regional needs yet with an EU added value. They could also contribute to the creation of cybersecurity diploma in universities and skill development.

The European Cybersecurity Research and Competence Centre should provide, according to the cPPP MB overall "coordination" of the network providing support for exchange of information and coordinating funding for cybersecurity. It would support the definition and implementation of EU policies and legislations related to cybersecurity and could be the EU training centre on cybersecurity. If developed in a NIST-like approach (with seconded experts), such centre could also drive highly advanced research on special topics as well as provide specific operational support (upon request).

The above would be complemented by the evolution of the present cPPP, currently focused on research, towards a wider capability and competitiveness PPP, supporting also strategic capabilities development and initial procurement.

The cPPP MB concludes with a set of recommendations for future actions in the cybersecurity area including the definition of a European cybersecurity industrial policy, tackling not only R&D but also capability development, which could be done through an enhanced cPPP, allocating more resources to R&D and capability building, raising awareness of companies and citizens, harmonising security standards for IoT, and developing private EU Sectoral CERTs with rapid reaction capabilities to threats.

4.4.4. Feedback received to the Inception Impact Assessment

The Commission has also received feedback to the Inception Impact Assessment (IIA) published at "Have Your Say" website, which allows citizens and stakeholders to contribute to EU policy and law-making process (12 responses including private sector, research organisations, citizens as well as one association from a third country) .

Stakeholders providing feedback to IIA pointed to the fact that fragmentation and low level of coordination in between the EU cybersecurity experts groups in public and private sectors are undermining the impact of the efforts deployed in a field whereas other economical regions are strong and well-organized (examples of USA, Israel and China were provided). Stakeholders also pointed to the need of sharing investment as research requires equipment levels that are out of reach of many organisations - be it public or private. Most stakeholders providing feedback on the IIA supported the option, which would include both industrial support measures and research and development activities.

At the same time all stakeholders providing their views on core aspects of the IIA supported policy action going beyond baseline scenario only.

Other issues brought up by stakeholders concerned the need of interdisciplinary approach encompassing not only computer-science aspects of IT-security, but also humanities/social-science-based aspects of the challenge as well as the need to stimulate a dual approach where civil and military stakeholders interact in the development of a new security technology.

Annex 3: Who is affected and how?

6. PRACTICAL IMPLICATIONS OF THE INITIATIVE

This annex describes the practical implications of the preferred option identified in the Impact Assessment – the establishment of a Cybersecurity Competence Network with a European Cybersecurity Industrial and Research Competence Centre entity empowered to pursue measures in support of industrial technologies as well as in the domain of research and innovation (Option 1) – for stakeholder groups likely to be directly or indirectly affected by the initiative.

Member States

The EU Member States will have at disposal an effective mechanism to help them build their cybersecurity technological capabilities, support the scaling up of the cybersecurity industry and increase the protection of essential services (e.g. transport, health, banking and financial services) in their territories while strengthening the collective resilience of the EU.

The initiative will enable Member States to coordinate together with the Commission their investments in necessary cybersecurity infrastructure at the national and European levels. The mechanism will allow Member States to pool expertise as well as resources for tools and infrastructures which would otherwise be more costly or not affordable for individual Member States. Such approach would allow economies of scale and rationalisation.

The return from such investments would be also proportionally higher as the Member States would benefit from the access to upgraded capacities and facilities that could not be achieved through national efforts only.

The increased coherence and synergies between different funding mechanisms (Digital Europe Program, FP9, and possibly cyber defence under European Defence Fund) would also reduce the administrative burden of managing different cybersecurity funding programmes, with a positive impact on the EU budget to which Member State contribute.

The preferred option will also impact positively Member States' capability to deal with the wide range of issues related to education and skills. The functionalities of the Centre linked to the education paths, for example the development of cybersecurity curricula and the support to the cybersecurity certification programs, will complement the efforts of the Member States by providing appropriate input to education policy makers. At the same time, the access for researchers to cutting-edge projects will help contain the "brain drain" phenomenon and increase the chances of retaining the best talents in the EU and attracting foreign highly skilled professionals.

Businesses

European companies, both on the cybersecurity demand and the supply side will be among the most impacted stakeholder groups. The Network and the Centre under this option would ensure access for businesses to necessary testing and experimentation infrastructure helping them to ensure that their products are cyber-secure and turning cybersecurity into their competitive advantage. This should also help them cut research and development costs and speed up the development process, which would further reinforce their competitiveness.

In addition, the chosen mechanism will ensure coordination between research and industry and therefore direct the research efforts towards concrete industrial needs. The provision of cutting-edge expertise and tools in cybersecurity will indirectly support economic operators in complying with the NIS Directive.

In addition one of the key functionalities of the Competence Centre and the Network is to support the deployment of European cybersecurity leading-edge products and solutions across the market

SMEs

The European SMEs and micro-enterprises operating in the cybersecurity filed will experience direct and indirect economic benefits from the initiative as highlighted above. While the set-up of the Competence Centre and the Network does not impose regulatory obligations upon them, it will open up opportunities in terms of costs reduction for the design of new products and it will help them gaining easier access to the investors' community and attract the necessary funding to deploy marketable solutions. In the case of SMEs and micro-enterprises the access to publically funded testing and experimentation facilities is even more important as they are lacking resources to either purchase or to travel outside their market (and often outside the EU) to find necessary infrastructure. It is also hoped that this initiative would open up new markets for European SMEs and micro-enterprises active in the field of cybersecurity.

Research Community

Research and development organisations throughout the EU, both on the civilian and the defence side, will enjoy the benefits deriving from better coordination, resource pooling and increased availability of advanced methodologies and tools (such as testing and experimentation facilities). They will be able to achieve the critical mass to carry out projects of common interest with a longer-time, strategic perspective. In addition, the chosen mechanism will ensure coordination between research and industry and therefore direct the research efforts towards concrete industrial needs helping the process of turning the outcomes of the research into applicable and marketable solutions that could be then used by different industries and public authorities.

The hosting of several programmes under a common "umbrella" would also allow the research community to experience cross-fertilisation among the different stakeholder groups related to cybersecurity and increase the visibility of the EU excellence in research on the global scene.

Citizens

Stronger European know-how in cybersecurity should result in an overall higher level of protection for citizens in the Digital Single Market, e.g. in Internet of Things domains such as smart energy, medical devices, or connected automated vehicles. The initiative should result in an improved provision of products and services which reflect European values and are directly in line with European policies and regulations.

EU institutions, agencies and bodies

The EU institutions, agencies and bodies will benefit both from the outcome of the research and development and the procurement activities of the Competence Centre and the Network, and from the access to state-of -the art methodologies and tools to perform their operations as effectively as possible.

This is in particular true for the bodies in cybersecurity field, such as ENISA, the EU cybersecurity Agency, the European Cybercrime Centre at Europol, the European Defence Agency (interested in e.g. dynamic risk assessment and incident handling) and the several sectoral agencies with an interest in the area (for example the European Aviation Security Agency).

7. SUMMARY OF COSTS AND BENEFITS

II. Overview of costs – Preferred option							
		Citizens/Consumers		Businesses		Administrations	
		One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
Network of Competence Centres with European Industrial and Research Competence Centre	Direct costs	0	0	0	0	0	EUR 15-20 million EU budget
	Indirect costs	0	0	0	0	0	0

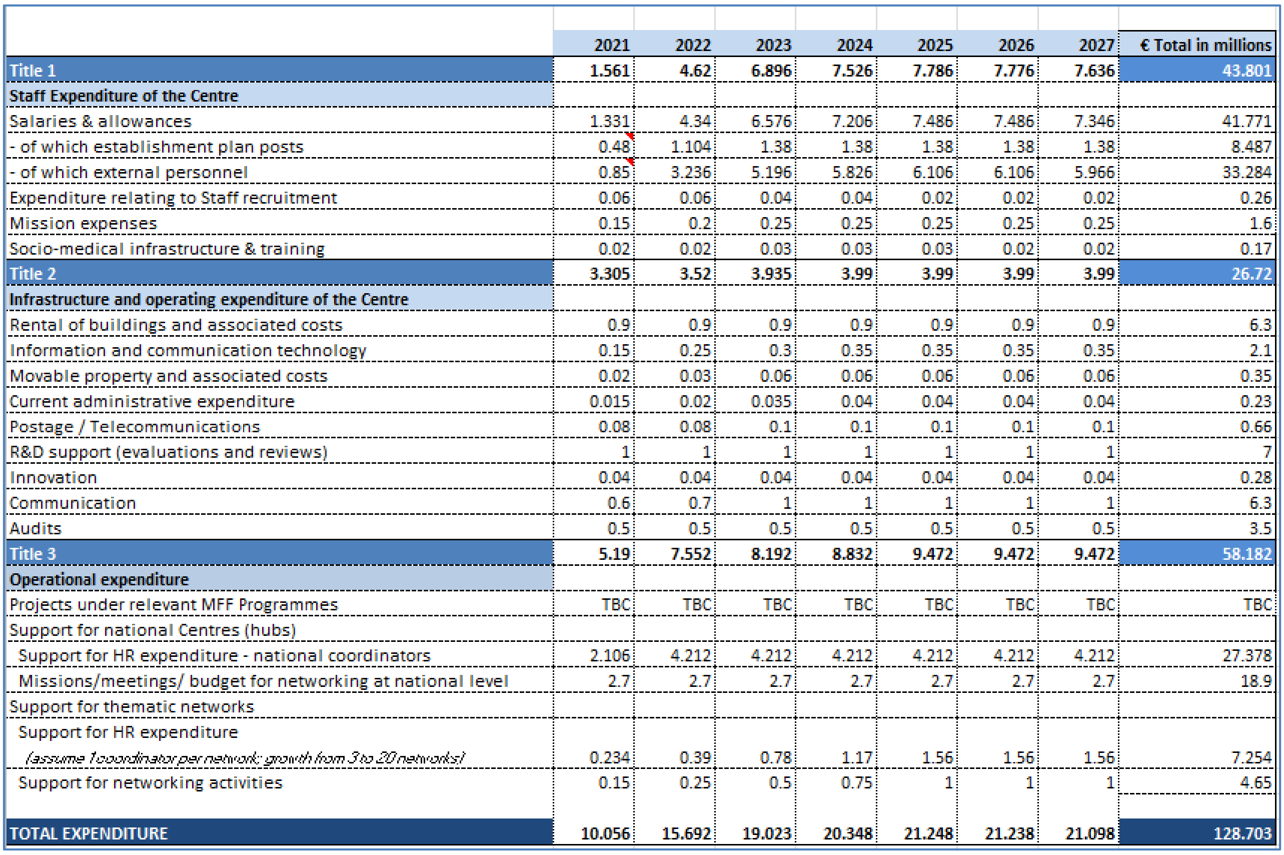
Comments:

Recurrent costs related to the functioning of the Centre itself as well as the financial support by the Centre to the Network (support for the national centres chosen by Member States to act as a national Competence Centre hub as well as for thematic networks) have been presented in the below budget overview[8]*. The overall amount dedicated to the Centre is very modest in comparison with the overall level of funding expected under the new Multiannual Financial Framework.*

The costs would be covered under the EU budget and are considered as additional as no such costs are incurred under the Baseline scenario.

Please note that this overview does not include the operational costs related to the implementation of different funding programmes, which are decided within separate processes.

[8] *The costs related to facilitation of the network cooperation by a central entity were base, to the extent possible, on comparable experiences e.g. The European Reference Network for Critical Infrastructure Protection.*



	2021	2022	2023	2024	2025	2026	2027	€ Total in millions
Title 1	**1.561**	**4.62**	**6.896**	**7.526**	**7.786**	**7.776**	**7.636**	43.801
Staff Expenditure of the Centre								
Salaries & allowances	1.331	4.34	6.576	7.206	7.486	7.486	7.346	41.771
- of which establishment plan posts	0.48	1.104	1.38	1.38	1.38	1.38	1.38	8.487
- of which external personnel	0.85	3.236	5.196	5.826	6.106	6.106	5.966	33.284
Expenditure relating to Staff recruitment	0.06	0.06	0.04	0.04	0.02	0.02	0.02	0.26
Mission expenses	0.15	0.2	0.25	0.25	0.25	0.25	0.25	1.6
Socio-medical infrastructure & training	0.02	0.02	0.03	0.03	0.03	0.02	0.02	0.17
Title 2	**3.305**	**3.52**	**3.935**	**3.99**	**3.99**	**3.99**	**3.99**	26.72
Infrastructure and operating expenditure of the Centre								
Rental of buildings and associated costs	0.9	0.9	0.9	0.9	0.9	0.9	0.9	6.3
Information and communication technology	0.15	0.25	0.3	0.35	0.35	0.35	0.35	2.1
Movable property and associated costs	0.02	0.03	0.06	0.06	0.06	0.06	0.06	0.35
Current administrative expenditure	0.015	0.02	0.035	0.04	0.04	0.04	0.04	0.23
Postage / Telecommunications	0.08	0.08	0.1	0.1	0.1	0.1	0.1	0.66
R&D support (evaluations and reviews)	1	1	1	1	1	1	1	7
Innovation	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.28
Communication	0.6	0.7	1	1	1	1	1	6.3
Audits	0.5	0.5	0.5	0.5	0.5	0.5	0.5	3.5
Title 3	**5.19**	**7.552**	**8.192**	**8.832**	**9.472**	**9.472**	**9.472**	58.182
Operational expenditure								
Projects under relevant MFF Programmes	TBC	TBC	TBC	TBC	TBC	TBC	TBC	TBC
Support for national Centres (hubs)								
Support for HR expenditure - national coordinators	2.106	4.212	4.212	4.212	4.212	4.212	4.212	27.378
Missions/meetings/ budget for networking at national level	2.7	2.7	2.7	2.7	2.7	2.7	2.7	18.9
Support for thematic networks								
Support for HR expenditure *(assume 1coordinator per network: growth from 3 to 20 networks)*	0.234	0.39	0.78	1.17	1.56	1.56	1.56	7.254
Support for networking activities	0.15	0.25	0.5	0.75	1	1	1	4.65
TOTAL EXPENDITURE	**10.056**	**15.692**	**19.023**	**20.348**	**21.248**	**21.238**	**21.098**	128.703

Benefits analysis:

1. With regard to creation of the Network and the Centre economic benefits can be assumed for MSs, industries and research communities as the services of the Centre will be free of charge and therefore the reduced investment from these stakeholders from their own resources is needed (e.g. on testing and experimentation infrastructure).
2. Other indirect economic impacts can be assumed as a result of the initiative as it could help MSs and industry to reduce the costs of cybersecurity/cybercrime incidents for which the estimated economic impact stands 0.41% of GDP (around 55 billion).
3. Additional indirect economic benefits are expected due to: 1) increased access for businesses to necessary testing and experimentation infrastructure helping them to ensure that their products are cyber-secure and turning cybersecurity into their competitive advantage thus increasing volumes of sales. This should also help them cut research and development costs and speed up the development process, which would further reinforce their competitiveness. 2) the increased market opportunities for businesses, including SMEs thanks to deployment support activities of the Centre and the Network.