European Commission

INCEPTION IMPACT ASSESSMENT

Inception Impact Assessments aim to inform citizens and stakeholders about the Commission's plans in order to allow them to provide feedback on the intended initiative and to participate effectively in future consultation activities. Citizens and stakeholders are in particular invited to provide views on the Commission's understanding of the problem and possible solutions and to make available any relevant information that they may have, including on possible impacts of the different options.

TITLE OF THE INITIATIVE	Create a cybersecurity competence network with a European Cybersecurity Research and Competence Centre
LEAD DG (RESPONSIBLE UNIT)	DG CNECT, H1
LIKELY TYPE OF INITIATIVE	Legislative
INDICATIVE PLANNING	May/June 2018
ADDITIONAL INFORMATION	-

The Inception Impact Assessment is provided for information purposes only. It does not prejudge the final decision of the Commission on whether this initiative will be pursued or on its final content. All elements of the initiative described by the Inception impact assessment, including its timing, are subject to change.

A. Context, Problem definition and Subsidiarity Check

Context

In its Cybersecurity *Communication*[1]*, 13 Sept.2017,* the European Commission announced the intention to set up a network of cybersecurity centres of expertise with a European Research and Competence Centre at its heart with the aim to pool resources, overcome fragmentation of efforts across the EU and stimulate development and deployment of technology in cybersecurity. The Council Conclusions[2] following the Communication adopted in November 2017 called on the Commission to provide rapidly an impact assessment on possible options and propose by mid-2018 the relevant legal instrument for the implementation of the initiative establishing a Network of Cybersecurity Competence Centres and a European Cybersecurity Research and Competence Centre. The Commission has also launched a call for proposals under the Horizon 2020 Work Programme to pilot the creation of efficient networks of competence centres across the EU. The lessons learned from these projects will inform the process of building out the future network and Competence Centre.

Analyses[3] show that the aggregated number of experts working in competence centres in cybersecurity in the EU is comparable to, if not higher than the numbers in competing economies world-wide. Nevertheless, Europe's industrial and technology positioning, in terms of patents filed or market share is relatively limited. This is the case in particular in advanced and critical technologies such as cryptography. Fragmentation and redundancy in investments in knowledge and capacity building in cybersecurity is undermining the impact of the total effort. This is confirmed by the consultations with stakeholders[4] from academia, industry and public authorities. They converge on the need not only for higher and further coordinated efforts in the field but also for focused co-investments between Member States and the EU in shared capacities like complex equipment, software tools and data resources. In a nutshell, it is only through further cooperation and collective efforts that the EU can become a cybersecurity powerhouse, matching its economic weight, be it in terms of supply or uptake and best use.

The EU has been providing research and innovation funds under the Seventh Framework Programme and Horizon 2020 and strived to reinforce the links between research and industry through cross-institutional and cross-sectoral projects and by establishing the contractual public-private partnership on cybersecurity in 2016. The EU also provides, albeit at a very limited scale, support to pilot actions for the deployment of cybersecurity and trust solutions in areas of public interest within the Connecting Europe Facility programme.

---

[1] JOIN(2017) 450 final: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU;

[2] Council Conclusions 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.

[3] Ongoing research by the Commission's Joint Research Centre, based i.a. on a survey of cybersecurity expertise centres (https://ec.europa.eu/eusurvey/runner/cybersecurity-survey)

[4] Results of stakeholder engagements, including a Commission workshop with national cybersecurity competence centres (23 February 2018) and with the European Cybersecurity Organisation ECSO in the context of the contractual Public-Private Partnership on Cybersecurity.

Problem the initiative aims to tackle

Despite these efforts today the EU still lacks sufficient capacity to autonomously secure its economy and critical infrastructures and to become a global leader in cybersecurity field. For example, not only does Europe not manage entire value chains of Information and Communication Technology products and services – it is also a net importer of the cybersecurity know-how to secure these systems, This situation is driven by a number of underlying causes, which are closely linked to each other.

Fragmentation of the effort, lack of a dynamic EU-wide ecosystem: From the technology perspective including not only research and innovation but also and mainly the wide diffusion and uptake of latest cybersecurity solutions, the efforts across the EU, including notably the public sector, are fragmented, redundant on basic solutions and subcritical for leading-edge technologies. The links between the demand (both public and private from various sectors e.g. health, telecomm, energy, space, defence, finance, transport) and supply side of the cybersecurity market are not sufficiently well developed resulting in sub-optimal supply of European products and solutions adapted to different sectors' needs, as well as in insufficient levels of trust among market players.

Size of the effort: Today public and private investment in the field is not only dispersed but also sub-optimal compared to other global players (e.g. US, China, Israel). The research and industrial communities as well as the public sector struggle with insufficient capacities both in terms of human resources and also access to necessary facilities e.g. for experimentation and testing, which are often too large/costly for a single entity to acquire (e.g. infrastructure for post-quantum encryption, or large-scale databases). These conditions hamper ambition and the possibility to look collectively at the best solutions that reinforce our industries and the security of the Digital Single Market.

Difficulty to get access to latest cybersecurity capacities: While European cybersecurity companies tend to be innovative, their size and capacity is smaller in comparison to their global counterparts, making it difficult for them to face fierce global competition. This is due, among others, to the fragmentation of the European cybersecurity market, the limited availability of testing and experimentation facilities, and limited access to cutting-edge specific and interdisciplinary cybersecurity know-how.

Protecting the public sector as a major challenge but also an opportunity: Not only the business sector at large struggles to appropriately secure its existing products, services and assets or to design secure innovative products and services (e.g. due to lack of resources, skills, different business priorities). Also key cybersecurity assets with relevance to the public sector (e.g. blockchain-based solutions, infrastructures supporting quantum key distribution enabling highly-secure communications for critical assets and institutions) are too costly to be developed and set up other than jointly at the European level.

Dual use is not enough developed: The problem of insufficient interaction also concerns the civilian and defence communities, which share common challenges but do not cooperate effectively enough – both in terms of ideas and funding – to take advantage of their synergies.

The cybersecurity skills challenge: Last but not least, all these communities struggle to find skilled cybersecurity professionals for both research and business tasks. While there is a global shortage of skilled workforce in the field of cybersecurity, the current non-harmonised set-up of the cybersecurity research and industry ecosystem results also in the outflow of highly qualified specialists to other geographies/markets, which present better professional opportunities.

This situation has a number of serious consequences both in terms of Europe's economic development and security. It will be a missed opportunity for Europe to become a global leader in the field of cybersecurity – one of the fastest growing Information and Communication Technologies market segments. The EU risks to stay behind in the leadership race related to the next-generation digital technologies (e.g. artificial intelligence, quantum computing), innovative products and services. Innovative European companies face fierce global competition and, if we are not able to overcome the current obstacles, are likely to become the target of mergers and acquisitions by non-European actors – a trend that has already been observed in the past years. This is likely to further increase Europe's technological dependence on providers from other geographies and make the EU more vulnerable. A closely linked consequence is the potential lack of access for European citizens and businesses to security products and solutions based on European values.

Basis for EU intervention (legal basis and subsidiarity check)

The final legal basis for the EU intervention will be decided depending on the policy option chosen. Without prejudice to this analysis, the following basis for the EU intervention correspond to its objectives (see also the section on objectives, below);

- The Union is empowered to pursue the objective of strengthening its scientific and technological bases by achieving a European research area in which researchers, scientific knowledge and technology circulate freely to make the EU more competitive (Art 179 of the Treaty on the Functioning of the EU).

- The European Union is empowered to encourage an environment favourable to cooperation between undertakings and fostering better exploitation of the industrial potential of policies of innovation, research and technological development (Art. 173 of the Treaty on the Functioning of the EU).
- The European Union is also empowered to adopt measures with the aim of establishing or ensuring the functioning of the Internal Market, in accordance with the relevant provisions of the Treaties (Article 26 and Article 114 of the Treaty on the Functioning of the European Union). In view of the fragmentation of the cybersecurity internal market, EU action is needed to achieve a single market in this field, which is also a prerequisite for a well-functioning digital economy.

The objectives (see the section below) can be better achieved at the EU level, rather than by the Member States alone, in view of:

- The cross-border aspects of cybersecurity threats and the needs for standards and interoperable solutions in the digital single market,
- the large resource requirements related to certain essential capabilities in cybersecurity not only for research and development but also for the wide deployment, across the EU, that requires also access to interdisciplinary cybersecurity know-how (often only partially available at the Member State's level), and
- The global nature of industrial value chains, as well as the activity of global competitors working across the markets.

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

B. Objectives and Policy options

The strategic objective of the initiative is to ensure that the EU retains and develops the essential capacities to autonomously secure its digital economy, society and democracy while becoming a global leader in cybersecurity field. This is linked to the specific objectives of stimulating cooperation and synergies between research and industry communities to develop and deploy technology in cybersecurity and complement the capacity building efforts in this area at the EU and national level.

To reinforce cooperation, achieve critical mass and ensure leadership in key areas, Europe needs an effective mechanism to commonly invest in acquiring latest cybersecurity capacities, making them available notably for public sector and research across the EU as well as for partnerships with industry. Such a mechanism should play a key role in developing and implementing common technology and competencies agendas that reinforce the excellence of existing centres, strengthen industrial competitiveness and protect our businesses and citizens from cyber-threats.

At this stage of reflection, the Commission is considering the following preliminary policy options:

- **Option 0 – Baseline scenario (status quo) - Collaborative Option** - this scenario assumes the continuation of the current policy approach to managing cybersecurity research and industry policy in the European Union through the next framework research programme. This option assumes the continuation of the contractual Public Private Partnership and facilitating cooperation among expertise centres networks created through a Pilot Project[5] by the European Commission.
- **Option 1 – Joint Undertaking based on Art.187 of the Treaty on the Functioning of the EU** – this option assumes creating a European Cybersecurity Research & Competence Centre in the form of a Joint Undertaking to stimulate and ensure structural and sustainable cooperation between a new network of cybersecurity competence centres in the Member States and industrial communities. A Joint Undertaking is an independent EU legal entity, with its own staff, budget, structure, rules and governance that can be tasked to implement actions under the EU Framework Programmes for Research and Innovation. It can combine EU budget with non-EU sources of funding (national, private, etc.), allowing the implementation of research, technological development and demonstration programmes in an integrated way. This option assumes that the Centre could facilitate the cooperation within the network, help pool and shape research efforts and handle multinational projects. It could also serve the cybersecurity community as a testing and simulation resource helping to develop cyber secure products across different industrial sectors.
- **Option 2 – a Centre based on Art.173 of the Treaty on the Functioning of the EU and Art.58 and 208 of Regulation 966/2012 (Financial Regulation)** –such an entity would be capable of carrying out activities as under option 1. In addition, together with the network of cybersecurity competence centres in the Member States, such an entity would be able to support the large-scale deployment of new, security-relevant technologies and infrastructures. This option would also make it possible to seek synergies with

[5] https://ec.europa.eu/digital-single-market/en/news/commission-launches-call-proposals-eu50-million-pilot-support-creation-network-cybersecurity

relevant Union activities in the area of defence.

These preliminary options will be assessed against the usual criteria of effectiveness and efficiency but also against the need for a flexible solution that could be adapted to fast changing needs in the field of cybersecurity.

C. Preliminary Assessment of Expected Impacts

Likely economic impacts

The present initiative is likely to contribute to:

- Stimulating the development of the Digital Single Market and improve the functioning of the cybersecurity internal market
- Increasing the competitiveness of European cybersecurity businesses
- Increasing the competitiveness of European industries across different sectors, which will be able to appropriately secure their existing assets and design secure innovative products while reducing security related research and development costs;
- Allowing the EU to become a leader in the next-generation digital and cybersecurity technologies
- Enhancing cyber security investments and allow the EU cyber security market to grow internationally;
- Stimulating cybersecurity start-ups and Small and Medium-sized Enterprises by building synergies between civilian and military cybersecurity markets and attracting investment including venture capitals to support cybersecurity start-ups and Small and Medium-sized Enterprises;
- Avoiding double-spending in terms of funding and general resources.

Likely social impacts

This initiative is likely to positively impact the social sphere by supporting increased security and consequently the trust of EU citizens and businesses in the digital society and economy. This is in particular relevant for the protection of access to essential services (e.g. transport, health, banking and financial services) as well as the security of personal data. Increased capacity of the European Union to autonomously secure its products and services is also likely to help the citizens enjoy their democratic rights and values. Last but not least, the initiative is also likely to contribute to closing the cybersecurity skills gap.

Likely environmental impacts

No specific or major impact on the environment is expected at this stage of the analysis.

Likely impacts on fundamental rights

Increased capacity of the European Union to autonomously secure its products and services is also likely to help the citizens better protect their information-related rights enshrined in the Charter of Fundamental Rights, particularly the right to the protection of personal data and private life.

Likely impacts on simplification and/or administrative burden

Streamlining EU cybersecurity research development and implementation efforts is likely to reduce administrative burden of managing different cybersecurity funding programmes. Pooling resources from the EU, Member States and industry will also help to achieve the economies of scale and help avoid double-spending. The cybersecurity research in the EU will be also better monitored and its impact will be better assessed against industrial challenges and needs. None of the options foresee new regulatory obligations for businesses. At the same time, the businesses and especially Small and Medium-sized Enterprises are likely to reduce their costs related to their efforts in designing innovative cybersecure products. The administrative burden of establishing the network and the Centre will be explored in each policy option.

D. Evidence Base, Data collection and Better Regulation Instruments

Impact assessment

An impact assessment is being prepared to support the preparation of this initiative and to inform the Commission's decision. The Impact Assessment is likely to be available in the second quarter of 2018.

Evidence base and data collection

The following information and data already exists:

- 2017 Eurobarometer on Cybersecurity
- Civil-Military Capacities for European Security, Netherlands Institute of International Relations, 2017
- Commission Communication on Strengthening Europe's Cybersecurity Resilience System and Fostering Competitive and Innovative Cybersecurity Industry and related Council Conclusions
- Commission Staff Working Document, Contractual Public Private Partnership & Accompanying Measures
- Cybersecurity in the EU Common Security and Defence Policy (CSDP), European Parliamentary

Research Service Scientific Foresight Unit (STOA), 2017
- Cybersecurity in the European Digital Single Market No2/2017
- Dual Use Study
- European Parliament resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI))
- Evaluation of 2013 Cybersecurity Strategy of the European Union
- Existing evaluations of the Seventh Research and Innovation Framework Programme (FP7) and relevant cybersecurity projects as well as H2020 mid-term evaluation of contractual Public Private Partnerships (not covering the cybersecurity one but relevant for general conclusions)
- Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU and related Council Conclusions
- Ponemon's "2015 Cost of Cyber Crime Study: Global"
- Public consultation on the Contractual Public Private Partnership. The questionnaire included specific questions on the EU's future cybersecurity needs;
- PriceWaterhouseCoopers Cybersecurity Market Study initial results of the Draft final report 2018

The following additional evidence will be sought:

- Joint Research Centre Study mapping competence centres across the EU
- Stakeholders' consultations (see next section).

Consultation of citizens and stakeholders

In line with the Better Regulation Guidelines, the Commission wishes to consult stakeholders as widely as possible. Therefore, the consultation strategy aims at involving a broad set of stakeholders that include national authorities, competence centres and research community across the EU, industry, EU institutions and bodies, and others. Depending on the stakeholder group identified, different tools and methods will be used in order to conduct the consultation.

- During a 4-week period, all interested stakeholders will be able to provide feedback on this Inception Impact Assessment.
- Public Consultations: several online public consultation for the future Multiannual Financial Framework, including on the topics of "Security" and "Investments, research and innovation, Small and Medium-sized Entreprises and single market", sought views from the wider public (open from 10 January to 8 March 2018). [6]
- A self-registration survey[7] for the cybersecurity competence centres across the EU was launched on 09 January 2018 allowing them to register their expertise in the field of cybersecurity; until 8 March more than 660 entities registered;
- Stakeholder workshops: two workshops on 23 February and 22 March 2018 with the representatives of the competence centres across the EU, national authorities and the industry;
- Regular consultations with the Member States through the Council Horizontal Working Party on cybersecurity, the Network and Information Security Directive Cooperation Group;
- Targeted consultations of the main EU bodies concerned by the initiative - European Network and Information Security Agency, European Defence Agency;
- Targeted consultation with the European Cybersecurity Organisation and cybersecurity contractual Public-Private Partnership;
  Direct dialogue with individual stakeholders reaching out to the Commission on the initiative.

Will an Implementation plan be established?

Yes. The plan will list the various actions which are needed to implement the policy option chosen and identify the main implementation challenges in terms of compliance, technical challenges and timing. Specific mechanisms for Commission and Member States support action will be devised.

[6] Public consultation on EU funds in the area of investment, research & innovation, SMEs and single market: https://ec.europa.eu/info/consultations/public-consultation-eu-funds-area-investment-research-innovation-smes-and-single-market_en
Public consultation on EU funds in the area of security: https://ec.europa.eu/info/consultations/eu-funds-area-security_en
[7] https://ec.europa.eu/eusurvey/runner/cybersecurity-survey