THE EU CYBERSECURITY AGENCY

GOOD PRACTICES IN INNOVATION UNDER NCSS

GOOD PRACTICES IN INNOVATION ON CYBER SECURITY UNDER THE NATIONAL CYBER SECURITY STRATEGIES

NOVEMBER 2019

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu

AUTHORS
Anna Sarri, ENISA

Pinelopi Kyranoudi, ENISA

CONTACT
For contacting the authors please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

ACKNOWLEDGEMENTS
ENISA would like to thank and acknowledge all the experts that took part and provided valuable input for this report and especially:

Enterprise Ireland (Ireland)
Information System Authority (Estonia), Silja-Madli Ossip
INCIBE (Spain), Félix Antonio Barrio Juárez
Centre for Cybersecurity Belgium (Belgium)
NASK (Poland), Magdalena Wrzosek, Anna Felkner
CERT (Poland), Paweł Pawliński
Ministry of Transport, Innovation and Technology (Austria), Ralph Hammer and Lisbeth Mosnik
Department for Digital, Culture, Media and Sport (United Kingdom), Ben Shaps
Portuguese National Cybersecurity Centre (Portugal), Alexandre Leite
Inter-ministerial working party on cyber prevention and cybersecurity (Luxembourg)
TECNALIA (Spain), Leire Orue-Echevarria and Ana Ayerbe
Deutor Cybersecurity Solutions (Germany and Switzerland), Stefanie Frey
Ministry of Digital Affairs (Poland), Marcin Domagała
Università degli Studi di Milano (Italy), Claudio Agostino Ardagna,
Consorzio Interuniversitario Nazionale per l'informatica (Italy), Ernesto Damiani and Paolo Prinetto
Agence nationale de la sécurité des systèmes d'information, ANSSI (France)

ENISA would like to thank for their valuable contribution to this study, all the experts that provided input, but prefer to stay anonymous.

This study was also based on input and a preparatory study that was performed by ENISA colleagues Dr. Athanasios Drougkas and Ms. Christina Skouloudi. We would like to thank our ENISA colleagues for their valuable contribution.

ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

ISBN 978-92-9204-308-7, DOI 10.2824/01007

TABLE OF CONTENTS

GLOSSARY OF TERMS

ACRONYM	DEFINITION
CA	Competent Authority
CEF	Connecting Europe Facility
DSM	Digital Single Market Strategy
DSP	Digital Service Provider
EFTA	European Free Trade Association
GDPR	General Data Protection Regulation
ICT	Information and communications technology
INEA	Innovation and Networks Executive Agency
ISAC	Information Sharing and Analysis Centre
MS	Member State
NCSS	National Cyber Security Strategies
NIS	Network and Information Systems
OES	Operators of Essential Services
PPP	Public-Private Partnership
SME	Small and Medium-sized Enterprise
SPOC	Single Point of Contact

EXECUTIVE SUMMARY

The online Digital Single Market (DSM) is in increasing jeopardy from various forms of cyber-attacks. The need for a strong and effective EU Network and Information Security (NIS) Industry becomes two-fold; on the one hand the DSM needs NIS protection for commercial services, critical infrastructure and the everyday life of its citizens, who depend on online services. On the other hand, the DSM offers opportunities and tools that can facilitate the growth of the EU NIS Industry. Growth of the NIS industry can occur with direct benefits in terms of revenue for NIS suppliers, growth of the EU GDP and boost of employment in the cybersecurity sector; the latter is of particular importance considering that cybersecurity is one of the faster growing segments of the ICT industry. To achieve this, innovation in cybersecurity is a key enabler. ENISA supports the efforts aimed to enhance the overall level of cybersecurity in the Member States (MS) both at a national and EU level. This report supports that effort by analysing how Member States are approaching innovation as a strategic priority under National Cyber Security Strategies (NCSS).

The analysis is structured around several aspects of innovation such as: Innovation Priorities, Industrialisation and Collaboration and Market and Policy. Each of these aspects is at the same time divided into two dimensions. Innovation priorities can be divided into Innovation in technologies and services, and into economic incentives and investments. Industrialisation and collaboration can be divided into industrialisation processes and activities, and stakeholders' collaboration. Market and Policy can be divided into Market and Technology Alignment and Market regulation. Each dimension can be supported by several activities and mechanisms.

Moreover, this study identifies a set of challenges and good practices, as experts perceive them, across the different innovation dimensions. The identification of these challenges may help in identifying relevant actions for addressing them and also in drafting future innovation strategic objectives. Finally, this report identifies seven recommendations that can be taken into account both at National and EU level to support the development of cybersecurity innovation strategies and enhance their impact:

1. **Support and develop sector specific innovation priorities.**
2. **Support sufficient and adequate level of funding.**
3. **Involve stakeholders while developing and implementing innovation strategies.**
4. **Take into account the positive impact of regulatory frameworks on innovation.**
5. **Support industries in positioning new cybersecurity offerings in the market**
6. **Promote EU level certification of services/products**.
7. **Promote NIS training and educational measures.**

These recommendations form a roadmap for enhancing innovation on cybersecurity under NCSS.

Stakeholders who are involved in defining national cybersecurity strategies may take into account the results of this study, in particular, may take into account the identified challenges, good practices and suggested recommendations.

1. INTRODUCTION

According to the Network and Information Security (NIS) Directive[1], MS are required to develop National NIS Strategies to meet current and emerging cybersecurity threats. National NIS Strategies are considered by the MS the same policy documents as National Cyber Security Strategies (NCSS). The EU Member States need to constantly develop and adapt their cybersecurity strategies and cooperate effectively to counter network and information security risks. National cybersecurity strategies (NCSS) are the main documents of nation states to set strategic principles, guidelines, and important objectives. Key priorities (among others) of a National Cyber Security Strategy are critical information infrastructure protection, citizen's awareness, provision of incentives for the private sector to invest in cybersecurity, research and development as well as promoting innovation in the field of cybersecurity.

ENISA supports the efforts aimed to enhance the overall level of cybersecurity preparedness of EU Member States (MS) both at national and EU level. Innovation as a strategic priority under NCSS is a key enabler to achieve those efforts. The objective of this report is to analyse how Member States are approaching innovation as a strategic priority in terms of economic incentives and investments, industrialisation and collaboration activities, implementation methods, initiatives and all relevant aspects of innovation ecosystem building.

In the Commission proposal for establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, the Network and Information Security (NIS) industry is among the fastest growing segments of the ICT market[2]. In order to optimise the benefits for the EU economy in terms of jobs and competitiveness, it is necessary to create the right environment and ecosystems for the NIS industry to grow. The Digital Single Market needs NIS products and services for its own growth. It also provides opportunities for providers of NIS products and services. However, despite the presence of NIS technical knowledge, innovative ideas and entrepreneurial spirit in Europe, various factors may hinder the growth of NIS industry resulting in new companies following an early exit strategy, or seeking growth opportunities outside the EU.

In an ever-changing cybersecurity environment, EU Member States need to have flexible and dynamic cybersecurity strategies to meet new, global threats. ENISA is supporting the EU Member States since 2012 to develop, implement and evaluate their NCSS in order to help the Member States to enhance their level of cybersecurity preparedness.

1.1 POLICY CONTEXT

A NCSS is a plan of actions designed to improve the security and resilience of national infrastructures and services. It is a high-level top-down approach to cybersecurity that establishes a range of national objectives and priorities that should be achieved in a specific timeframe. Currently all countries in the European Union have a NCSS as a key policy feature, helping them to tackle risks which have the potential to undermine the achievement of economic and social benefits from cyberspace. Apart from tackling cybersecurity risks, a strategy builds on collaboration. Some of the most important settings to improve collaboration between stakeholders is Information Sharing and the creation of Public-Private Partnerships.

The NIS Directive reinforces NCSS's role and states that innovation should be a key element of a NCSS. The NIS Directive described NCSS as one element of the 'National Frameworks on the

[1] 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 (NIS Directive) http://data.europa.eu/eli/dir/2016/1148/oj
[2] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52018PC0630

security of network and information system'. Specifically, Article 7 of the NIS Directive states that each Member State shall adopt a national strategy on the security of network and information systems defining the strategic objectives and related measures with a view to achieving and maintaining a high level of security of network and information systems, covering at least the Operators of Essential Services and the Digital Service Providers.

The increase in cyber threats and the perception of cyber insecurity is causing a growing mistrust in citizens, potentially holding back the European economy as it increasingly becomes digital. Recognising its key importance to growth of the EU's digital economy, cybersecurity forms a key component in the European Commission's **Digital Single Market** (**DSM**) **strategy**.[3]

The DSM strategy recognises the need to protect the EU's communication networks and critical infrastructure and respond effectively to cyber threats, and the need to build on existing national and EU-level cybersecurity strategies and regulation.

The aim of the EU's Cybersecurity Strategy is to establish common minimum requirements for network and information security (NIS) among the Member States; to set up coordinated prevention, detection, mitigation, and response mechanisms; and to improve the preparedness and engagement of the private sector. The strategy seeks to stimulate demand for effective NIS ICT products and to certify these products by establishing a platform to identify good cybersecurity and by developing security standards for cloud computing.

In particular, the DSM strategy also highlighted one of the key priorities of the Cybersecurity Strategy, which is to **develop industrial and technological resources for cybersecurity**, acknowledging that gaps exist between the rapid development of technologies and solutions for online network security. It calls for "a more joined-up approach… to step up the supply of more secure solutions by EU industry and to stimulate their take-up by enterprises, public authorities, and citizens".

The Commission is now considering[4] key activities to protect the EU against cyber-attacks covering multiple aspects, such as supporting EU NIS R&D and innovation for increased competitiveness[5], prompting European cooperation for a series of **Sectoral Information Sharing and Analysis Centres** (sectoral ISACs), removing barriers that prevent market participants from sharing event information and more. The European Commission supports the model by exploring financial programmes such as the Connecting Europe facility[6] (CEF), discussing possibilities for cooperation, and suggesting further investment through procurement.

In terms of Data Privacy and Data Protection, the new **General Data Protection Regulation** (**GDPR**)[7] replaces the **Data Protection Directive 95/46/EC**[8] effective May 25, 2018. The GDPR is directly applicable in each member state and will lead to a greater degree of data protection harmonization across EU nations. The GDPR is an important step forward for enhancing privacy of EU citizens, harmonizing data protection rules across Member States, and promoting privacy and security as core aspects of the European industry.

Innovation priorities are also present in other initiatives. For example, the **EU Cybersecurity Act**[9], part of the Cybersecurity package, sets innovation as one of the priorities of the Digital Single Market strategy and mandates ENISA to support Member States in their innovation activities.

[3] A Digital Single Market Strategy for Europe {SWD(2015) 100 final}, http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf
[4] Communication on *Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry*, COM(2016) 410 final, 5 July 2016, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=16546.
[5] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=16545
[6] https://ec.europa.eu/inea/en/connecting-europe-facility
[7] http://ec.europa.eu/justice/data-protection/reform/index_en.htm
[8] http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex:31995L0046
[9] https://eur-lex.europa.eu/eli/reg/2019/881/oj

In addition, the Commission has also supported the creation of a **European Cybersecurity Industrial, Technology and Research Centre[10], and of a network of Cybersecurity Competence Centres[11]** to better target and coordinate available funding for cybersecurity cooperation, research and innovation. The Competence Centre will facilitate and help coordinate the work of the Network and foster the Cybersecurity Competence Community, driving the cybersecurity technological agenda and facilitating common access to the expertise of national centres. The overall mission of this new proposal is to help the Union retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market.

1.2 SCOPE AND OBJECTIVES

The main objective of this report is to analyse the landscape of innovation in cybersecurity in the EU Member States and to present the good practices and the challenges that Member States are facing when implementing innovation as a strategic priority of their National Cyber Security Strategies. More specifically, the objectives of this report focus on:

- Understanding the current landscape and mechanisms for supporting innovation in cybersecurity in the EU by mapping regional characteristics as well as sectoral demands.
- Understanding the financial supporting mechanism in each MS from the public sector (R&D funds) and how research results can end up as products on the market;
- Share good practices and propose recommendations to relevant stakeholders to foster the growth of innovation in cybersecurity in the EU.

1.3 METHODOLOGY

Error! Reference source not found. presents the methodology adopted for conducting the study. It consists of five different steps:

1. **Desktop research:** during this phase, relevant public documents and literatures have been collected and taken into account. In particular, the desktop research focuses on the analysis of the published NCSS. Different concepts, terminologies and usages provide a characterisation of the different understanding of innovation and of the different strategies that support innovation in cybersecurity.
2. **Collection of experts and stakeholders point of view:** Based on preliminary analyses and findings of the desktop research, this phase identified and invited for interviews (or online surveys) experts that have experience in relation to the development and implementation of NCSS and more specific in the implementation of Innovation as a strategic objective of a NCSS. For this reason, ENISA contacted its NCSS experts group and National Liaison Officers (NLOs) to find the relevant experts in each MS.
3. **Analysis:** The analysis presents an overview of the different dimensions to consider when EU Member States implement cybersecurity innovation priorities. It also presents the key practices used by the Member States to support innovation of cybersecurity in their counties.
4. **Conclusions and recommendations**: The discussion of good innovation practices for advancing innovative cybersecurity products and services in the EU allowed the presentation of recommendations that could benefit EU Member States both at a national level and at EU level.
5. **Validation with experts:** The results of the study have been validated by experts in the field.

[10] https://ec.europa.eu/digital-single-market/en/european-cybersecurity-industrial-technology-and-research-competence-centre
[11] https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-establishing-european-cybersecurity-industrial-technology-and-researchb

Figure 1: Methodology used during the study work

1.4 TARGET AUDIENCE

This report provides insights for the whole cybersecurity ecosystem. The specific target audience may benefit from the report's insights differently:

- National and EU Policy and Decision Makers, who are concerned with defining innovation strategic priorities for cybersecurity.
- Operators of Essential Services and Digital Service Providers, who are interested in innovative technologies, products and services.
- Public and private sector organisations, who need to collaborate in order to support the introduction of new technologies, products and services
- Research Organisations, who conduct research and innovation activities, and want to bring research results into the market.

1.5 STRUCTURE OF THE DOCUMENT

The remainder of this report is structured as follows:

- **Section 2** EU and National Initiatives describes the priorities that take place at EU and at National Level to support innovation as a strategic objective.
- **Section 3 Dimensions of Innovation** introduces the different dimensions that has been identified by analysing the existing NCSS. The section also includes an overview of the four categories of stakeholders that have been identified as playing a role in the implementation of innovation strategic objectives under NCSS.
- **Section 4 Key findings** provides a detailed account of the dimensions and elements underpinning innovation, including examples from the Member States.
- **Section 5Strengths and Weaknesses** presents a SWOT analysis for developing cybersecurity innovation strategies in the European Union.
- **Section 6 Recommendations** provides recommendations for the development of innovation strategies.

Examples of Member States' and EFTA practices are highlighted in the text within boxes, tables and/or italics.

2. EU AND NATIONAL INITIATIVES

This section provides an overview of the EU and National initiatives for innovation in cybersecurity. In particular, it provides an account of the major EU initiatives supporting innovation in cybersecurity. The European Commission supports innovation with different initiatives and dedicated programmes supporting innovation across the European Union. Among the EU programmes, the Connecting Europe Facility (CEF) programme and the Horizon 2020 (H2020) programme regarding EU Research and Innovation support innovation mechanisms and initiatives across different domains, including cybersecurity. This section also provides an overview of the key national initiatives supporting innovation in cybersecurity.

2.1 EU INITIATIVES

The Connecting Europe Facility (CEF) and the Horizon 2020 (H2020) programmes support different innovation mechanisms and initiatives in cybersecurity across sectors

The Innovation and Networks Executive Agency (INEA) has been responsible for the implementation of the CEF programme and parts of H2020 programme. The CEF programme promotes growth, jobs and competitiveness through targeted infrastructure investment at European level. The CEF programme covers three sectors: CEF Energy, CEF Telecom and CEF Transport. Since January 2014, INEA is responsible for the implementation of most of the CEF programme for a budget of €28.8 billion (out of €30.4 billion): €24.2 billion for Transport, €4.8 billion for Energy, and €1.5 billion for Telecom. The CEF Telecom has also supported cybersecurity projects and capability developments. In addition to grants, the CEF offers financial support to projects through innovative financial instruments such as guarantees and project bonds. These instruments create significant leverage in their use of EU budget and act as a catalyst to attract further funding from the private sector and other public sector actors.

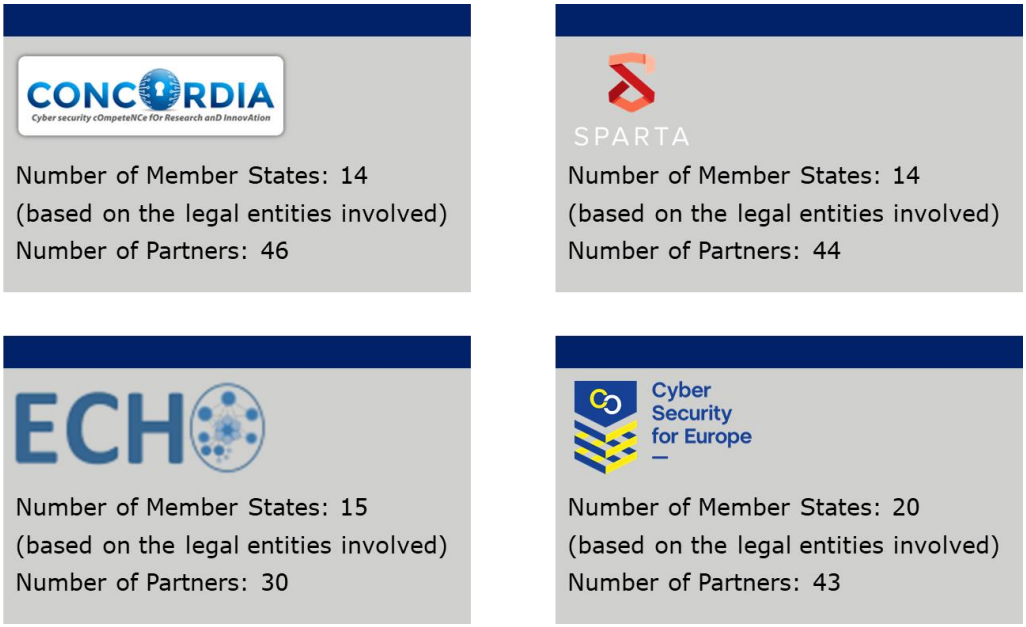
INEA has published a report on the achievements of the CEF programme[12]. The CEF programme, in alignment with the NIS Directive, supports cooperation among Member States in order to develop technical capabilities addressing emerging cyber threats, including potential cross-border and cross-sector propagation of cyberattacks to operators of essential services and digital service providers. The CEF's Cybersecurity Digital Service Infrastructure (DSI) supports the implementation of the Directive by increasing the cybersecurity capabilities of actors that are fundamental for a State's cybersecurity, such as National Computer Security Incident Response Teams (CSIRTs), operators of essential services, and national competent authorities. The DSI also puts in place cooperation mechanisms for information sharing and maturity development at the EU level. CEF Telecom has invested €29.4 million for the Cybersecurity DSI funding 58 different actions (that INEA managed).

H2020, the other major EU programme for cooperative Research and Innovation partially managed by INEA, has also provided supports to relevant cybersecurity research. H2020 funds mainly three different types of mechanisms: Research and Innovation Actions (RIA) with EU funding rate of 100% of the eligible project costs, Innovation Actions (RIA) with EU funding rate of 70% of the eligible project costs (except non-profit, which are still funded 100%), and Coordination and Support Actions (CSA). The European Commission maintains a H2020 dashboard, which prides an overview (by countries and beneficiaries) of the funded projects[13]. Up to date, H2020 has supported over 24K grants, involved over 116K participants for a total EU contributions exceeding €44 billion. Among the H2020 beneficiaries, over 23K SMEs have participated in more than 10K grants receiving an EU contribution of over €7 billion. The European Commission's proposal for Horizon Europe is an ambitious €100 billion research and innovation programme to succeed Horizon 2020.

[12] INEA (2019): Investing in European Networks. The Connecting Europe Facility: Five years supporting European Infrastructure.
[13] H2020 Dashboard:
https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-dashboard

At the European Level, the European Commission has launched four different EU pilot projects in order to prepare the European Cybersecurity Competence Network[14]. The Horizon 2020 (H2020), the EU Research and Innovation programme[15], is funding the four pilot projects addressing the overall objective of *"establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap"*. Which summarises key information of the four pilot projects: CONCORDIA[16], ECHO[17], SPARTA[18] and CyberSec4Europe[19]. These four EU pilot projects will support strengthening the EU's cybersecurity capacity and address emerging cybersecurity challenges for a safer European Digital Single Market[20].

Figure 2: EU Pilot Projects



The four Horizon 2020 pilot projects will support the development of a sustainable European Cybersecurity Competence Network. They will implement different activities (e.g. trainings, cybersecurity demonstration cases and cyber ranges in different sectors such as eHealth, finance, telecommunication, transportation, etc.) in order to address the cybersecurity-skill gab in EU and to deliver innovative solutions preparing EU for future cross-sector and cross-border cybersecurity challenges. These projects together with the European cybersecurity ecosystem will work towards advancing cybersecurity research and innovation in Europe. The projects' objectives are in alignment with the European Commission proposal for a European Regulation establishing a European Cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Cybersecurity Coordination Centres in 2021[21].

2.2 NATIONAL INITIATIVES

For the purposes of this study, a desktop research on 28 NCSS and a series of interviews with 14 responding MS have been carried out. In this subchapter, the analysis of those interviews and

[14] See: https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre
[15] See: https://ec.europa.eu/programmes/horizon2020/en
[16] See: https://www.concordia-h2020.eu/
[17] See: https://www.echonetwork.eu/
[18] See: https://www.sparta.eu/
[19] See: https://www.cybersec4europe.eu/
[20] See: https://ec.europa.eu/commission/priorities/digital-single-market_en
[21] See: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-establishing-european-cybersecurity-industrial-technology-and-research

NCSS highlight the strategic objectives that support innovation in cybersecurity across the Member States. Those objectives are the following:

Organise cybersecurity exercises

In this objective, awareness in cybersecurity, skills development, collaboration and new ideas are cultivated. All these could be a beginning for new products. Cybersecurity exercises are a great way for people to test and enrich their skills and for companies to discover new talents.

Citizen's awareness

Informing and advising citizens regarding cybersecurity threats and incidents help them understand the importance of cybersecurity in the everyday life. This helps in building a cybersecurity culture, shaped according to the needs and priorities of each country. After all, human dynamics is one of the key links of the cybersecurity chain.

Establish baseline security requirements

As internet is expanded far more than one country's borders, cybersecurity threats concern everyone. This is important for sectors and companies with different maturity levels to take specific actions that will help them grow in parallel. Establishing baselines security requirements for their information infrastructure is a first step in evolving and innovating.

Engage in international cooperation

This is a great way to collaborate, learn from each other, as well as adopt good practices. Moreover, by organising international events, MS support internal companies to present and promote their products, technologies and services.

Establish public-private partnerships

There is often a gap between public and private sector, making collaboration and trust difficult to be achieved. Establishing public-private partnerships can help in bringing stakeholders together to collaborate, understand the needs of the market and develop new products, technologies and services.

Foster R&D

As technology is growing faster and faster, research and development in cybersecurity needs to run at the same speed or even foresee further developments. In this way technologies and people will keep being secure and safe.

Provide incentives for the private sector to invest in security measures

One of the challenges the private sector usually faces is to choose between profit and investing in cybersecurity, as both are important for a company's continuity. Apart from this, companies' security measures may also relate to their people, products or customers, so it is essential for MS to provide incentives that could help the private sector in this dilemma. This will also help the growth of the cybersecurity market and the adoption of new technologies, products or services.

Strengthen training and educational programmes

Universities, most of the times, is the first environment that future professionals meet. The more trainings, conferences and workshops they organise, the more ready they will be to discuss, brainstorm and come up with new ideas that might grow into innovative products, services and technologies. Other initiatives such as private sector initiatives supported by the public sector could offer training and educational programs and discover new talents, new ideas and potential workforce for the cybersecurity domain.

In total 78.57% of the countries that participated in this study, organise cybersecurity exercises and 92.86% establish baseline security requirements. 85.71% engage in international cooperation and establish public-private partnerships. All participating countries confirmed that they provide citizen's awareness, foster R&D and strengthen training and educational programs and 78.57% provide incentives for the private sector to invest in security measures. Figure 3 below presents the above analogy in detail.

The table below is also a snapshot of national initiatives, which complement as well as often rely on EU initiatives.

A strategic coordination of EU and NCSS would enhance the efficiency and the contribution towards cybersecurity across the Union

Figure 3: National Strategic Objectives that support innovation in the Member States

Table 1: National Initiatives on Innovation

Member State	National initiatives
Austria	• Preparing a Cyber Security Communication Strategy • Strengthening Austria's research in the area of cybersecurity through national and EU security research programmes (e.g. National Research Development Programme KIRAS Austria) • Austrian Cyber Security Platform: The Cyber Security Platform launched by the Federal Chancellery in 2015 as a public-private partnership is Austria's central platform for cooperation between the private and public sectors in matters of cybersecurity and the protection of critical infrastructures • Supporting education in ICT, providing ICT security and media competence in early school Grades (National ICT Security Strategy) • Defining compulsory ICT training for all teacher training students (National ICT Security Strategy) • Improving training structures for ICT security specialists in the tertiary sector (National ICT Security Strategy) • Increasing awareness of ICT security as an important element of adult education/further training (National ICT Security Strategy) • Establishing ICT security research as a basis of national competence (National ICT Security Strategy) • Covering ICT security to a greater extent in applied ICT research (National ICT Security Strategy) • Supporting active theme leadership in international research programmes (National ICT Security Strategy)

Member State	National initiatives
Belgium	• Promoting certification schemes • Creating initiatives for control and homologation bodies (e.g. standardisation) • Contributing to the widening of expertise and knowledge in cybersecurity • Supporting the development of technologies
Bulgaria	• Establishing dedicated programmes in order to improve the competitiveness of SMEs and micro enterprises • Supporting R&D, academia, education: incubate resources and industry specialisation • Raising awareness, knowledge and competence and developing a stimulating environment for cybersecurity research and innovation
Cyprus	• Developing a comprehensive National Awareness Programme for cybersecurity matters, covering all users of electronic systems, from governmental workers to citizens of the State • Investigating the possibility of creating a dynamic PPP (Public-Private Partnership) in the area of critical information infrastructure protection and promoting active cooperation with international entities • Developing suitable human resources that will have the necessary technical know-how and certifications to implement the provisions of the national cybersecurity strategy to a high level, in the mid- and long-term, and inclusion of these skills and certifications into the job descriptions for related positions
Czech Republic	• Supporting investments in research and development in the cybersecurity (including cybersecurity technologies), as well as in training and education of the end users (i.e. the Czech Republic's population) • Designating the National Security Authority (NSA) as the main point of contact for cybersecurity research, contributing to coordination of research activities in cybersecurity in order to avoid duplications • Focusing cybersecurity research on substantive problems and on transfer of research outputs into practice
Denmark	• Supporting the Defence Agreement with funds tackling future cyber challenges through additional initiatives, including research and training – An allocation of DKK 10 million in the agreement period for cyber security research and education which the Centre for Cyber Security manages in collaboration with relevant research institutions • Allocating funds for technological research, including funding for research in cyber security, within the auspices of Innovation Fund Denmark
Germany	• Setting up a National Cyber Response Centre in 2011 (with the previous NCSS) and optimising the cooperation between others incident response teams and national authorities • Creating Cybersecurity Training centres - Fraunhofer and a select group of universities have created a Cybersecurity Training Lab, which focuses on different sectors • Supporting the use of reliable and trustworthy information technology, continuing and intensifying research on IT security and on critical infrastructure protection
Estonia	• Maintaining and improving cybersecurity capabilities in cooperation between the government, academia and private sector • Adopting independent cybersecurity solutions, which are backed by cybersecurity training opportunities, research & development and entrepreneurship • Supporting sustainability of existing and new cybersecurity solutions (both public and private sector) with strong focus on export and outreach • Supporting development of cybersecurity SMEs and startups through strategic planning and providing national assistance.

Member State	National initiatives
Spain	• Developing a Framework for Cyber Security Knowledge, extending and broadening talent recruitment, advancing research and training programmes in cybersecurity in cooperation with Universities and specialised centres • Promoting cybersecurity certification activities, models and techniques for analysing cyber threats and measures for protecting products, services and systems • Fostering industrial developments of cybersecurity products and services through instruments such as, among others, the State Plan for Scientific and Technical Research and Innovation and initiatives for supporting its internationalisation • Incorporating into the Spanish legal framework solutions to problems that arise in connection with cybersecurity in order to establish types of criminal offences and the work of the departments with responsibilities in this area
Finland	• Improving cyber expertise and awareness of all societal actors, including Non-Governmental Organisations (NGOs) which are critical to the vital functions of society. • Establishing a strategic cybersecurity centre of excellence under the existing ICT-SHOK (TIVIT) in order to provide an opportunity for top research teams and companies who utilise the results for engaging in an effective mutual cooperation over the long term
France	• Establishing a council dealing with disruptive innovation, including initiatives on securing and certifying systems using IA and on the role of automation in cybersecurity • Developing and accentuating the national and European offer of security products and services • Integrating cybersecurity requirements into public contracts • Supporting export and internationalisation of businesses in the sector
Greece	• Recording and improving the existing institutional framework • Supporting research and development programmes and academic educational programmes • Supporting the participation of the academic community to national, EU or other international research and development programmes • Supporting the adaptation of academic curriculum in order to address issues concerning the National Cyber Security Strategy • Establishing and supporting Public-private partnerships • Raising awareness to citizens, businesses through educational campaigns
Croatia	• Supporting Public-Private Partnerships (PPPs) connecting academia, government and economic sectors • Connecting educational institutions in order to systemise programmes and curricula, and avoid unnecessary paralleling or implementation of teaching programmes in information security of questionable quality • Defining strategic research sectors in the area of information security (from the point of view of defensive and offensive technologies, methods, algorithms, devices, software and hardware)
Hungary	• Integrating cybersecurity as a field in the information technology syllabus of primary, secondary and higher education, in training courses for government officials and in professional training courses • Ensuring that the quality of education, training as well as research and development meets the requirements of international best practices, thus contributing to the establishment of a world-class national knowledge pool • Supporting cooperation with university and scientific research centres which have achieved outstanding and internationally recognised results in cybersecurity research and development and helping to establish cybersecurity centres of excellence

Member State	National initiatives
	• Establishing a support framework for research and development, education and awareness-raising
Ireland	• Establishing the National Cyber Security Centre (NCSC) within the Department of Communications, Energy and Natural Resources • Supporting education and training for Industry/SMEs: ICT Skillsnet & Cyber Ireland. • Developing and deepening partnerships with third level institutions to aid the sharing of knowledge, experience and best practice, and to support the developing research agenda in cybersecurity
Italy	• Establishing Public-Private Partnerships (PPPs) in order to strengthen cyber-security preparedness • Conducting cyber security exercises • Supporting cooperation with universities and research centres in order to develop new methodologies and technologies aimed at detecting/analysing vulnerabilities and threats • Developing partnerships with universities and research centres to set up trainings and specific courses for Public Administration and private companies' personnel. • Enhancing bilateral and multilateral cooperation programs in order to improve national Research & Development at both EU and international level • Engaging research sector and Academia in developing performing risk management tools
Lithuania	• Supporting training initiatives for enhancing cyber awareness, increasing the percentage of Lithuanian population who is aware of cybersecurity principles • Promoting cybersecurity culture and innovation • Developing scientific research and activities that create high added value in the area of cybersecurity • Developing creativity, advanced capabilities and cybersecurity skills and competence that meet market needs • Promoting public, private, and academic partnerships while creating innovation in cybersecurity
Luxembourg	• Creating a Cybersecurity Competence Centre (C3) • Developing and implementing a model of "responsible disclosure", allowing the disclosure of a detected computer vulnerability, while giving the parties concerned a deadline to correct the vulnerability prior to its disclosure • Supporting research start-ups offering innovative solutions feature among the needs identified within the Luxembourg digital security ecosystem • Supporting a cross-cutting approach is required for the development of a cybersecurity training programme • Strengthening of cooperation in the development of cryptographic protocols and algorithms
Latvia	• Creating training centres for constantly and systematically developing and improving skills in the ICT sector and its security specialisation in order to protect against rapidly growing threats in the cyber space • Promoting innovation in the cybersecurity sector and develop a unified academic resource of high-capacity computing (supercomputer) • Creating an ICT security laboratory and to organise scientific conferences about topical issues concerning cybersecurity and cybercrime in cooperation with universities and scientific institutes • Developing academic studies and research in cybersecurity to train experts, promote innovation, establish public-private partnerships for the support of science and research, and to attract European funds, grants and financial instruments
Malta	• Fostering application of research and development in cybersecurity in order to ensure cybersecurity among key research priorities

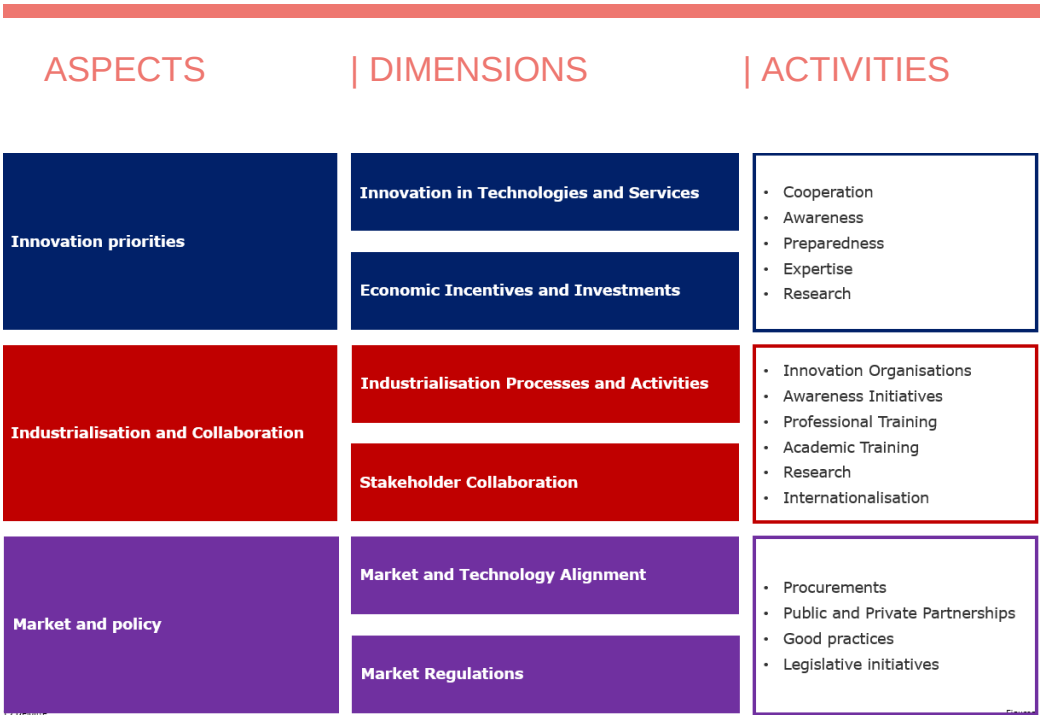
Member State	National initiatives
	• Supporting participations of government, academia and private sectors to research in any national and EU research projects and initiatives in cybersecurity
Netherlands	• Implementing the National Cyber Security Research Agenda III (NCSRA III) in order to pursue the development of cybersecurity research aimed at the development and commercialisation of innovative solutions • Encouraging open-source encryption by making additional resources available for this within the framework of NCSRA III • Establishing a Cyber Security Research Agency
Poland	• Developing industrial and technological resources for cybersecurity • Implementing the Cyberpark Enigma program in order to support participants in producing high quality hardware and software and strengthening their existing skills and knowledge • Stimulating research and development in the field of security of ICT systems • Jointly with the National Development Centre for Research and Development, launching a research programme for preparation and implementation of new methods of protection against novel threats from cyberspace • Developing a Centre for Research and Development
Portugal	• Supporting and enhancing scientific, technical, industrial and human capabilities in order to confirm national independence in cybersecurity • Supporting initiatives for internationalisation of companies offering cybersecurity services and products
Romania	• Stimulating research, development and innovation capabilities in cybersecurity • Developing educational and research programmes
Sweden	• Supporting initiatives for open access to research • Establishing five strategic innovation partnership programs to help meet a range of the societal challenges that Sweden is facing
Slovakia	• Developing the internal market with cybersecurity products and services by grants and EU funds • Supporting newly emerging projects and start-ups • Supporting research, development and innovation of industrial and technological resources in cybersecurity
Slovenia	• Implementing cyber awareness raising programmes • Promoting integration of academic and research sphere with the economy at both national and international levels • Creating public-private partnerships that will be able to develop innovative products and services with high added value to domestic and global markets
United Kingdom	• Supporting research developments and industrialisation through dedicated organisations and programmes such as Innovate UK and Catapult UK • Establishing a Cyber Growth Partnership • Establishing a Government Emerging Technology and Innovation Analysis Cell • Conducting a consultation on Cyber Science and Technology Strategy

The analysis of the national initiatives highlights that MS are investing a substantial effort in cybersecurity. The EU and national initiatives provide collectively a substantial investment in cybersecurity. A strategic coordination of EU and NCSS would enhance the efficiency as well as the potential contribution towards cybersecurity across the Union.

3. DIMENSIONS OF INNOVATION

The analysis is structured around several aspects of innovation, which were identified by analysing the NCSS across the EU. These aspects include: Innovation Priorities, Industrialisation and Collaboration and Market and Policy. Each of these aspects is at the same time divided into two dimensions. Innovation priorities can be divided into Innovation in technologies and services, and into economic incentives and investments. Industrialisation and collaboration can be divided into industrialisation processes and activities, and stakeholders' collaboration. Market and Policy can be divided into Market and Technology Alignment and Market regulation. Each dimension can be supported by several activities and mechanisms. In order to define the different dimensions of innovation, this study took into account and analysed the NCSS across EU Member States. The study also identifies the relevant mechanisms and activities that support the implementation of innovation in cybersecurity as a strategic priority under NCSS. It uses an integrated framework to analyse the different dimensions of innovation and to identify specific elements contributing to them. **Error! Reference source not found.** shows the Dimensions of Innovation in the context of NCSS.

Figure 4: Dimensions of Innovation in the context of National Cyber Security Strategies



The different dimensions are grouped on three different aspects: *Innovation Priorities*, *Industrialisation processes and collaboration*, and *Market and Policy.* The dimensions include a number of activities such as cooperation, awareness initiatives, research, etc.

3.1 INNOVATION PRIORITIES

Innovation priorities refer to the objectives that are pursued by a given Member State in the area of innovation. Innovation priorities can be divided in two categories: Innovation in technologies and services, and economic incentives and investments.

Innovation in technologies and services refers to those priorities focussed on growing existing technologies and organisations. It includes the following elements:

- **Cooperation:** Supporting collaboration between public and private sectors in enhancing cybersecurity and in dealing with emerging threats. *For example, in the French NCSS, this is described as the creation of an 'environment of digital technology businesses, industrial policy, export and internationalization'. In Ireland, this is described as: 'to build capacity across public administration and the private sector to engage fully in the emergency management of cyber incidents'.*
- **Awareness:** Informing citizens, businesses and professionals and raising awareness about the importance of cybersecurity and their abilities to deal with emerging cyber threats. This topic has different considerations, but overall the majority of NCSS, mention awareness raising and education activities.
- **Preparedness:** Development of cybersecurity expertise and capabilities in order to deal with emerging cyber threats. This is an element that some Member States identify as an ongoing activity. *For example, the Latvian NCSS states that it is possible to protect against rapidly growing threats in cyber space only by constantly and systematically developing and improving skills in the ICT sector and its security specialization.* Organising cybersecurity exercises are a way to increase MS preparedness to respond to cyber threats
- **Expertise:** Activities (including formal training programmes) contributing to development of skills and expertise in cybersecurity. This priority is not found in the NCSS of a lot of Member States. *As an example, the Netherlands has a long-term knowledge development program under which the academic community develops and improves high-quality knowledge in the area of cybersecurity.*
- **Research:** Activities supporting the development of new products, services and processes enhancing cybersecurity. Also, research is presented under different terms in the NCSS. These terms include 'research and development', 'stimulation of technology development', or 'capability development'. *An example of this category from the Member States comes from the Czech Republic: 'the Czech Republic shall strive to ensure maximum cyberspace security. In parallel, it shall support high technological production, research, development, and implementation. Thereby contributing to the technological advancement of the country.*

Economic incentives and investments refer to the relevant funding mechanisms that support innovation in cybersecurity. Such mechanisms include access to capital, sector specific investments, venture capitals, tax incentives, legal frameworks and insurance that might have an impact on the effective adoption of cybersecurity technologies and services. NCSS define funding mechanisms as research grants supporting studies and projects concerned with specific innovation areas. Such funding mechanisms provide alternative opportunities, which may complement EU research and innovation programmes. Funding mechanisms may also involve public-private partnerships for strategic areas of innovation.

3.2 INDUSTRIALISATION AND COLLABORATION

Industrialisation and collaboration refers to the challenge of transitioning from research to practice – with emphasis on stakeholder collaboration and industrialisation processes and activities. To support such priorities, MS have identified different mechanisms or activities. Although MS may implement such processes and activities differently, it is possible to cluster them according to the two specific above mentioned categories

Industrialisation Processes and Activities refers to those processes and activities supporting the integration of new cybersecurity technologies, products and services into the market. It covers five priorities:

- **Innovative Organisations:** Establishing organisations and formally mandating them with industrialisation processes and activities. *For example, following its NCSS, Spain has as*

an objective to 'develop a Framework for Cyber Security Knowledge and Extend and broaden talent recruitment, advanced research and training programmes in cybersecurity in cooperation with Universities and specialised centres'. In Hungary, its NCSS states that 'Hungary strives for strategic cooperation with universities and scientific research centres, which have achieved outstanding and internationally recognised results in cybersecurity research and development to help establish cybersecurity centres of excellence'.

- **Awareness Initiatives:** Activities oriented towards informing citizens of emerging threats and possible cybersecurity solutions. *The Spanish NCSS mentions that it will 'raise the awareness of citizens, professionals and companies about the importance of cybersecurity and the responsible use of new technologies and the services of the Information Society'.*
- **Professional Training:** Activities oriented towards providing formal training to professionals. *In Croatia there is a push for the 'development of human resources in the area of communication and information technology security'.*
- **Academic Training:** Activities oriented towards providing formal academic training either at schools or at the universities. *Hungary pays particular attention to integrating cybersecurity as a field in the information technology syllabus of primary, secondary and higher education, in training courses for government officials and in professional training courses.*
- **Internationalisation:** Activities supporting national stakeholders in international activities in order to facilitate commercial opportunities. *France supports export and internationalisation of the businesses in the [cybersecurity] sector.*

Stakeholder Collaboration refers to those initiatives and mechanisms supporting stakeholder collaboration fostering industrialisation. The priority under this category is R&D, which refers to activities oriented to the research and development of new products, services and processes to enhance cybersecurity. Research can take many forms, although overall, research is conducted with a combination of national and European funds. *This is the case of Austria, which mentions in its NCSS that 'to strengthen Austria's research in the area of cybersecurity through national and EU security research programmes. E.g. National Research Development Programme KIRAS Austria'.*

3.3 MARKET AND POLICY

From governance perspective, the analysis investigated occurrences of mechanisms or activities intended for shaping the cybersecurity market. In this section, two categories have been identified: Market and Technology Alignment and Market regulation.

Market and Technology Alignment refers to the alignment between cybersecurity market and innovative technologies, products and services. It covers:

- **Procurements**: Adoption of technologies, products and services in order to support National/EU industry. *France is a big proponent of this priority by supporting public procurement, the State will develop a favourable environment for French companies in the digital sector offering secure products and services*[22]*. . The country is developing and accentuating a national offer of cybersecurity products and services to create competitiveness for national businesses. The State will develop a favourable environment for French companies in the digital sector offering secure products and services by supporting investment, innovation and exports. Moreover, France is integrating cybersecurity requirements in public contracting. Croatia follows a similar approach, stating in its NCSS that the country will aim at 'Presenting and promoting the solutions developed in Croatia for cybersecurity on the global market'. Poland also develops industrial and technological resources for promoting cybersecurity.*
- **Public and Private Partnerships (PPPs):** Creation of PPPs focused on cybersecurity. A PPPs is a cooperative arrangement between two or more public and private sectors, typically of a long-term nature. They were primarily used for infrastructure provision, such

[22] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf

as the building and equipping of schools, hospitals, transport systems, water and sewerage systems. Less than half of the Member States have created PPPs focusing on cybersecurity. An example of a PPP is that of *the Austrian Cyber Security Platform, launched by the Federal Chancellery in 2015. It is Austria's central platform for cooperation between the private and public sectors in matters of cybersecurity and the protection of critical infrastructures.*

Market regulations refers to relevant policy initiatives shaping the national or the European internal market. The priorities under this category include:

- **Good Practices:** good practices are activities that have shown to work well by proving to succeed in achieving objectives and could be recommended as a model. They are activities oriented towards providing guidance to the different stakeholders.
- **Legislative Initiatives:** Activities oriented towards the establishment and maintenance of legal frameworks. In this regard, some Member States pledge in their NCSS to keep the legislative environment friendly to innovation in cybersecurity. *For example, Spain wants to 'incorporate into the Spanish legal framework solutions to problems that arise in connection with cybersecurity in order to establish types of criminal offences and the work of the departments with responsibilities in this area'[23]. Greece has a similar approach, stating in its NCSS that it aims at 'recording and improving the existing institutional framework'[24].*

All the above are the main dimensions of innovation (i.e. Innovation Priorities, Industrialisation and Collaboration, and Market and Policy) and their underpinning mechanisms in the context of NCSS.

3.4 NCSS STAKEHOLDERS

The analysis of the NCSS across Member States has identified the main stakeholders, who are involved in the implementation of cybersecurity strategies. The national strategies define relevant measures and mechanisms for the different stakeholders. shows the four main groups of stakeholders in the context of the NCSS: Governments, citizens and industries, service providers and research institutions.

[23] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/the-national-security-strategy
[24] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view

Figure 5: Identified stakeholders in the context of NCSS

Governments refer to institutions that belong to the public sector. In particular, it refers to governmental bodies such as ministries, military, police and institutions that compose the public sector and as identified in the NIS Directive such as: Single Point of Contacts (SPOCs), Computer Security Response Teams (CSIRTs) and Competent Authorities (CAs). Governments are the main stakeholder in charge of innovation under the NCSS, having both a leading/managerial role and an executive role. An example of governmental institutions refers to the Ministries of Interior for some Member States.

A governmental body that has an executive role is the State School for Public Administration of Croatia. This body provides training to Croatian public servants and plays a key role in ensuring that cybersecurity innovation happens in the public sector.

The French General Commission for Investment, following the guidance of the French Government allocates through public procurement public funds for promoting innovation of in the cybersecurity sector.

Service providers refer mainly to the Operators of Essential Services (OESs) and to the Digital Service Providers (DSPs), two stakeholders identified in the NIS Directive. Operators of essential services are private businesses or public entities with an important role to provide security in healthcare, transport, energy, banking and financial market infrastructure, digital infrastructure and water supply. Under the NIS Directive, identified operators of essential services will have to take appropriate security measures and to notify serious cyber incidents to the relevant national authority. DSPs refer to all entities meeting the definitions of online marketplaces, Cloud computing services and Search engines as presented in the NIS Directive. This category is provided because it is expected that, in order to comply with the NIS Directive, the stakeholders covered by the NIS Directive will be interested in innovative cybersecurity technologies, products and services.

Citizens and Industries refer to all relevant stakeholders, who may benefit directly and indirectly from NCSS. Strengthening cybersecurity as a whole as well as across all range ICT products, services and processes will have a positive impact for citizens, who are often the end users and principal beneficiaries. Industries form a complex ecosystem of stakeholders, who may depend on other stakeholders such as governments, service providers (both OES and DSPs) and research institutions too. Among such stakeholders are also industry associations across sectors (e.g.

manufacturing, machinery, etc.), which are becoming more and more dependent on ICT products, services and processes. These industries may often benefit from various initiatives under NCSS, including cyber awareness programmes and tailored cybersecurity solutions for their sectors. Besides such industry stakeholders are also vendors, which provides relevant cybersecurity solutions into the market. Due to the diversity of solutions, the resulting cybersecurity market is highly fragmented. Furthermore, there are also public and private stakeholders who are investing in cybersecurity with limited coordination with NCSS.

Research institutions refer to public and private academia and research organisations. Contrary to what could be expected, this category is not mainly composed by universities. This seems to suggest that there is a gap between universities and the NCSS. Instead, specific research centres compose mainly this category. These centres can take many forms.

Technology Ireland ICT Skillnet is a network of companies who collaborate to address skills needs within the technological sector. The network is a non-profit body which is co-funded by Skillnet Ireland, the national agency for workforce development learning, and member companies. Skillnet Ireland is funded from the National Training Fund through the Department of Education and Skills. Another example of these institutions is the Fraunhofer Society, a German research organization with 72 institutes spread throughout Germany, each focusing on different fields of applied science. Fraunhofer is Europe's largest application-oriented research organization. Around 70 percent of Fraunhofer's contract research revenue is derived from contracts with industry and from publicly financed research projects. Citizens and Industries refer to the broader private sector, including any institution that is not a part of the other categories. So far, no relevant institutions have been identified for this category.

4. KEY FINDINGS

4.1 INNOVATION IN TECHNOLOGIES AND SERVICES

In order to identify the main priorities in innovation, the analysis investigates the following questions:

Q1: Is innovation among the top priorities of the NCSS?
Q2: Are there policy related priorities that support innovation?
Q3: Are the mechanisms for collecting feedback from private sector regarding their access to new cybersecurity technologies and services?
Q4: Are there challenges affecting objectives and priorities in cybersecurity innovation?

The interviews and surveys with experts highlight the different approaches that Member States are following in order to support innovation in the context of the National Cyber Security Strategies.

Innovation is among the strategic priorities of National cybersecurity strategies in the EU

***In Portugal**, innovation was among the top priorities in the previous NCSS of 2015. It is also among the top priorities in the new strategy (published in the Official Journal in the 5th of June of 2019). Besides the vision defined in the new NCSS, one of the three established strategic objectives is to "promote innovation". There is also a specific axis of intervention: "Research, Development and Innovation". The specific activities planned in the next 5 years are yet unpublished. 120 days after publication, the government will define a specific action plan to operationalise these activities (with specified timeline, owners, etc.).*

In some cases, Member States create relevant institutions or networks of stakeholders giving them a mandate for specific aspects of innovation.

***In Ireland**, the Department of Communications and the National Cyber Security Centre (NCSC) have a mandate for leading the NCSS work and defining relevant innovation strategies in cyber security. However, innovation strategies often involve different stakeholders. The Industrial Development Authority (IDA) has created the Cybersecurity Cluster called Cyber Ireland. In some cases, such initiatives involve collaboration between the public and private sectors like a Public-Private Partnership (PPP). **In Spain**, the Spanish National Cybersecurity Institute (INCIBE), is involved in the development of such PPPs and other partnerships with other governmental agencies.*

Other initiatives support innovation in cybersecurity and especially the creation of new enterprises and new capabilities at national level.

***Belgium** is evaluating the creation of a "greenhouse" in order to support innovation in cybersecurity and to assess new business models and solutions. Similarly in UK, the "Cyber Growth Partnership" (CGP) is a Public-Private Partnership involving representatives from academia, industry and government. Among the strategic objectives of this PPP is to enhance innovation within the cybersecurity sector.*

***In Portugal**, there is a national integrated initiative aimed at enhancing digital competences: "InCoDe 2030". The objective of the initiative is to develop digital skills, focussing on the opportunities of adopting fast-paced technology. It goes in parallel to the content of the NCSS. Innovation is also a relevant priority in the Portuguese Digital Agenda.*

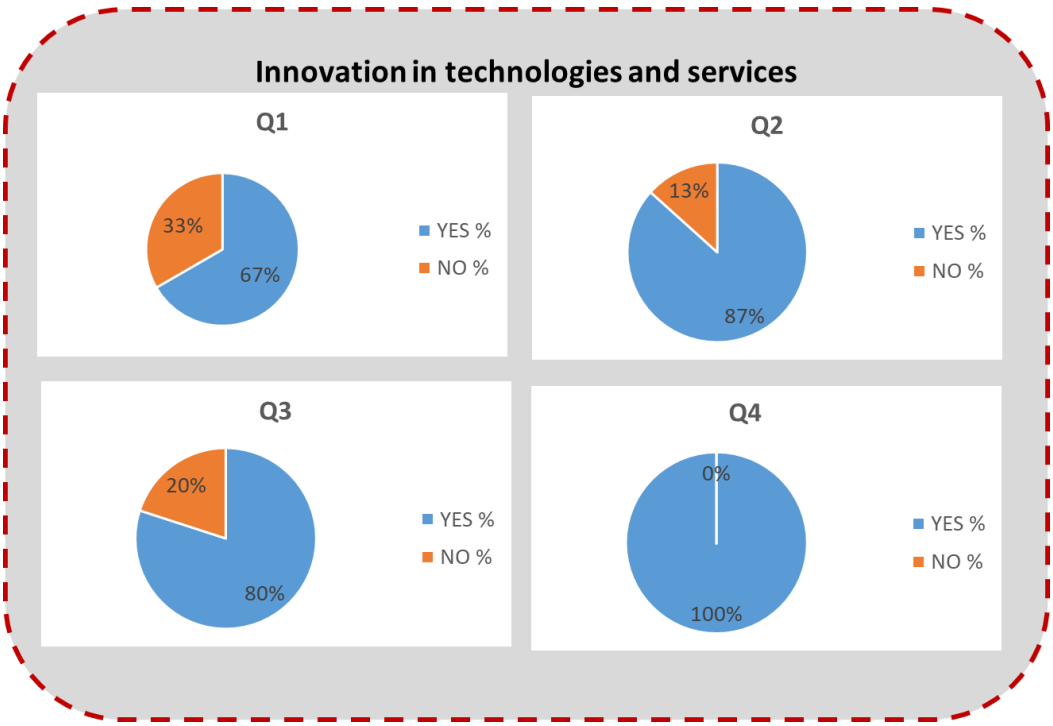
These are just few examples that highlight how Member States develop and prioritise innovation strategies.

Error! Reference source not found. provides an overview of how experts responded to these questions. The experts' opinions highlight that innovation is among the priorities of NCSS (Q1) and other policy related priorities (Q2). However, there are different accounts of innovation across the NCSS across Member States. In defining their innovation strategic priorities under NCSS, most Member States have mechanisms for consulting stakeholders' opinions and gathering their feedback regarding their positions in order to access new cybersecurity technologies, products and services (Q3).

> ***In Luxembourg**, there are multiple ways this feedback is organised:*
>
> - *Direct feedback for operators of critical infrastructures and operators of essential services. These companies are in relation with regulators and have to provide information about their cyber security capabilities. Either via providing policies, or risk assessments.*
> - *Indirect feedback for other companies by the governmental cooperation with the cyber insurance industry. The government closely collaborates with cyber insurance companies, as they become informal regulators for non-regulated SME, which represent a large part of the economy. The collaboration with cyber insurance is linked to the informed governance projects, which provides risk scenarios as well as metrics. The cyber insurance sector gives anonymous feedback to the government about the maturity of the insured companies. The cyber insurance industry also invests in the cyber security ecosystem and promotes private incident response capabilities and research.*

This is useful in order to facilitate the development of innovation in the industry. In addition, there is a complete agreement that many challenges exist affecting innovation in cybersecurity (Q4).

Figure 6: Innovation in technologies and services



Error! Not a valid bookmark self-reference. highlights that the mean ranking[25] has been given to critical factors such as lack of funding and misalignment between innovation and market are higher than the median values given to the other factors. Experts may have different views on the matter. Despite the observation that "lack of expertise" affects developments of competitive business models for new technologies and services, experts highlighted "lack of funding" and "misalignment between innovation and market" as the most critical factors (**Error! Not a valid bookmark self-reference.**). Whereas, they recognise the lack of expertise as critical as market fragmentation and scale. *One challenge is the so-called 'Time to Market' challenge in Germany. This challenge is related to the process of certifying products and services, which is very time consuming. This can often lead to the fact that when the product arrives to the market, it is already outdated.* Experts have also identified other challenges. For instance, it is often difficult for governments to understand the needs of the industry, as well as to develop expertise in dealing with PPPs. Often cybersecurity is addressed within other topics. Among other factors, compliance with relevant regulatory frameworks may according to some experts inhibit innovation. This is because lack of compliance is a business risk, which some organisations (in particular SMEs) may perceive as a barrier to innovation. For innovative companies such as start-ups it is very difficult to provide services or products to regulated public and private sectors. The European market remains somehow difficult and challenging for such innovative companies, which may try to develop their business outside Europe. Other organisations, such as universities and research centres, may have access to research funding. However, they usually have limited availabilities and capabilities (e.g. in terms of data for testing innovative solutions) for bringing their research results to the market.

Table 2: Factors affecting developments of competitive business models

Critical factors	Mean ranking (1 most important – 5 least important)
Lack of funding	2
Misalignment between innovation and market	2
Lack of expertise	3
Market fragmentation	3
Scale of market	3

Therefore, despite innovation is among the strategic priorities in NCSS, lack of funding and misalignment between innovation and market represent important barriers for achieving associated strategic objectives.

4.2 ECONOMIC INCENTIVES AND INVESTMENTS

To identify the main economic mechanisms supporting innovation, the analysis investigates the following questions:

Q6. Is there any access to capital to support innovation in cybersecurity technologies and services?
Q7. Are there sector specific economic incentives and investments supporting innovation in cybersecurity technologies and services?
Q8. Does the public sector support large enterprises to play a technical and economic role in delivering new cybersecurity technology and service ventures in the marketplace?

[25] The mean ranking is the weighted average of all interviewees feedback for each standard factor without taking into consideration other custom provided factors. Other factors are documented in the text but cannot participate in the total scoring.

Q9. Do factors such as, legal frameworks, insurance and taxation have an impact on the effective adoption of new cybersecurity technologies and services?

Interviews with experts and surveys highlighted an irregular situation regarding funding and innovation priorities. Member States have dedicated funding mechanisms and initiatives, which however are often focusing on different research and innovative objectives rather than being specific on cybersecurity.

***In Sweden**, the Swedish Innovation Agency currently allocates 200 Million Swedish Crowns for innovation on digital security during a three year period 2018-2020. There is also a private foundation, the Swedish Foundation for Strategic Research (https://strategiska.se/en/about-ssf/). The foundation was created by the government in 1994 and was given 6 billion SEK to administrate. It is independent and estimates that will be able to carry out its mission until 2025. It has recently allocated 300 Million Swedish Crowns (https://strategiska.se/en/research/ongoing-research/cyber-security-2017/) for cybersecurity research.*

However, eligibility criteria might limit access to public funding. Most funding mechanisms and incentives support SMEs. Large enterprises in the private sector often rely on their own investments. There are differences among regional, national and European funding initiatives. Lack of coordination creates a fragmented set of funding mechanisms, which organisations may perceive as lack of funding or strong competition. Some Member States have established and funded institutions for managing and running innovative programmes.

***The UK** Catapult centres, are networks of world-leading centres designed to transform the UK's capability for innovation in specific areas and to help drive future economic growth.*

*CyberSecIdent **in Poland** is a research and development program aimed at increasing the security of cyberspace of **the Republic of Poland** by increasing the availability of hardware and programming solutions.*

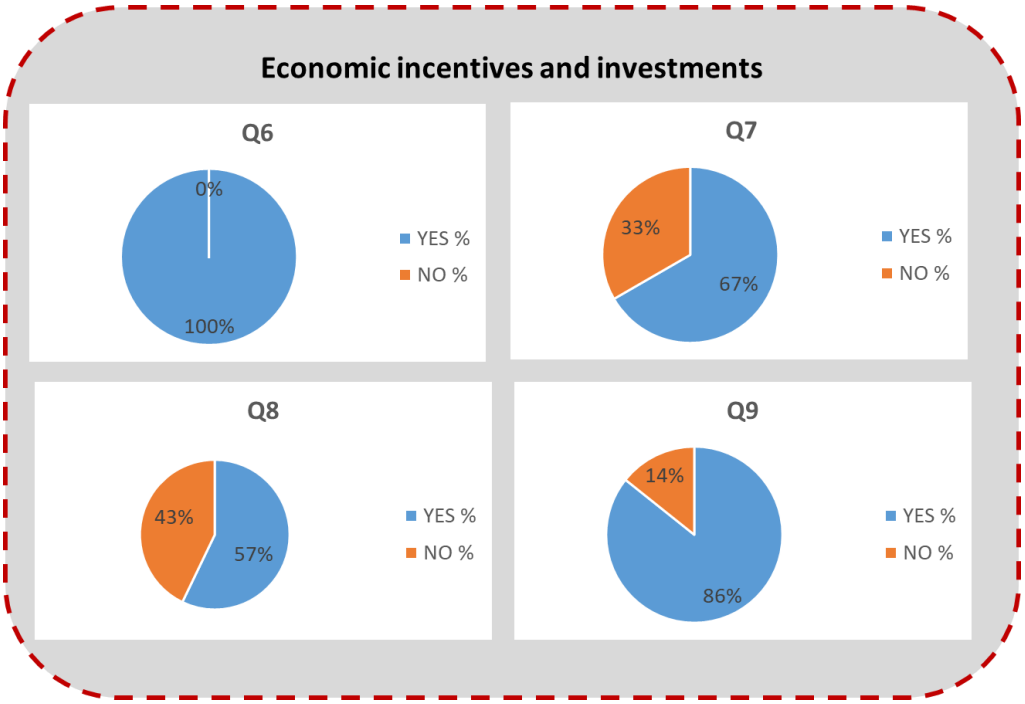
Error! Reference source not found. provides an overview how experts responded to the above questions regarding funding accessibility. The ability to access funding supporting innovation (even targeting specific sectors) is somehow in contradiction with the perception that lack of funding is a challenge affecting innovation. This is to a certain extent due to the misalignment between funding available for specific innovation objectives and market opportunities.

It emerges that different types of mechanisms (e.g. legal frameworks, insurance mechanisms, and taxation regimes) may have an impact on innovation and adoption of new technologies and services.

***In Italy**, some security incentives for enterprise digitalization and Nuova Sabatini supporting investments in big data, robotics, industry 4.0, cybersecurity.* It is however questionable to what extent the public sector and its relevant initiatives recognise the role of large enterprise in supporting innovation.

***In Luxembourg, t**he cyber security competence centre C3 (www.c-3.lu) identifies needs in cyber security services and tries to create public private collaboration with the private sector to create these services. The C3 operates on three main pillars: OBSERVE (threat intel, situational awareness), TRAINING (providing innovation training), TEST (testing of start-up technology in order to promote their services within larger companies). The government also enters into strategic partnerships with large enterprises (e.g. Cisco), for example via memoranda of understanding, seeking to address particular needs of the digital ecosystem, one of which is cybersecurity.*

Figure 7: Economic incentives and investments



4.3 INDUSTRIALISATION PROCESSES AND ACTIVITIES

To identify the main activities supporting industrialisation processes and activities, the analysis investigates the following questions:

Q10. Is there any support for effective marketing expertise, particularly in the context of cybersecurity and privacy?
Q11. Are there challenges effecting industrialisation processes and activities in cybersecurity?
Q12. Are Intellectual Property Rights (IPR) preventing the exploration of the full range of commercial options for new technologies and services in cybersecurity?

Error! Reference source not found. provides an overview how experts responded to these questions. Despite the support to marketing initiatives (e.g. promotion of adoption of technologies and services by the public sector and promotion of them alongside Member States' initiatives in international events), there are different challenges affecting the commercialisation of new cybersecurity technologies and services. Experts do not identify that Intellectual Property Rights (IPR) prevent industrialisation processes and activities (Q12). Most Member States support companies in positioning themselves internally. They may organise dedicated networking events or support them in establishing international relationships. However, there are various challenges affecting the commercialisation of innovative solutions in cybersecurity. Among the reported challenges are lengthily procurement processes. Thus, preventing in particular SMEs and innovative companies such as start-ups to offer their services to the public sectors.

In Austria, *the public sector relies on procurements. However, the government provides test beds and (financially) supports SMEs in order to present their products and services to foreign customers and investors. The government (and its initiatives including, for example, financial supports covering travel costs for networking alongside government's representatives) creates a platform for enhancing the visibility of services and products. The focus is on the internal market as well as on the international one*.

Furthermore, local market characteristics such as fragmentation and composition (e.g. small market with many SMEs) may affect industrialisation of new services and products.

Figure 8: Industrialisation processes and activities

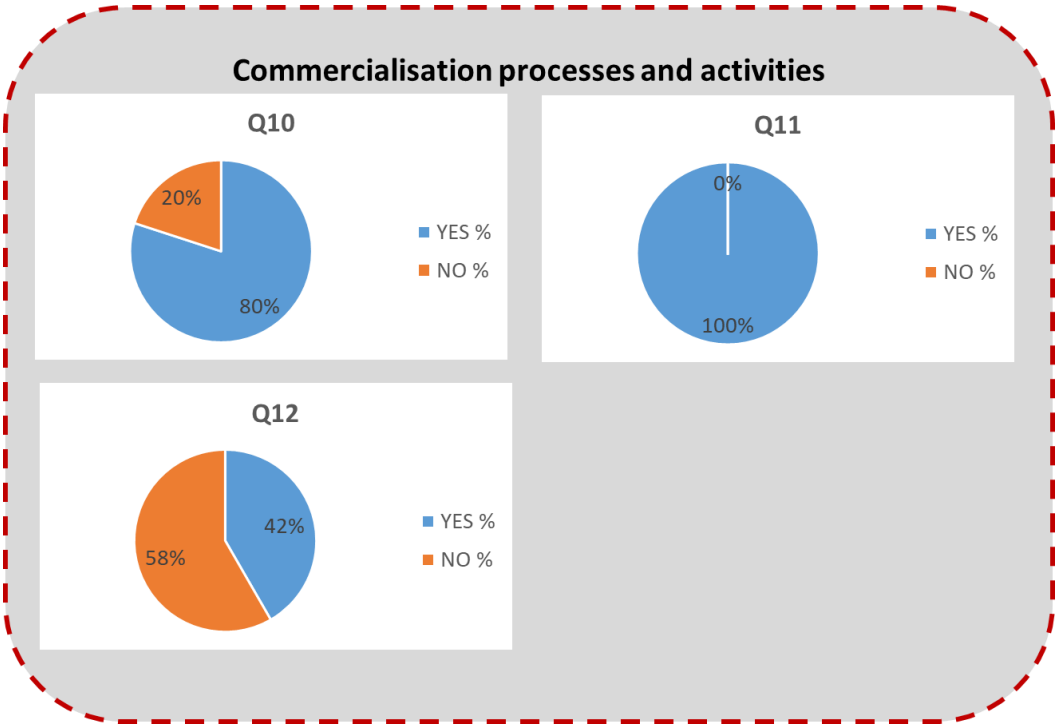


Table 3 provides further insights regarding factors affecting industrialisation of new technologies, products and services. Unsurprisingly, understating of technologies, products and services together with understanding buyers' needs are among the most important factors for industrialisation. Interestingly, experts recognise such factors to be as important as compliance with regulatory requirements. They recognise that understanding of business models and understanding of alternative propositions are less important than the other factors of industrialisation.

Table 3: Factors clarifying the value propositions of new technologies, products and services

Critical factors	Mean ranking (1 most important – 5 least important)
Understanding of technologies and services	2
Understanding of buyers' needs	2
Compliance with regulatory requirements	2
Clear business models	4
Understanding of alternative propositions	5

Therefore, industrialisation initiatives should focus of clarifying technologies and services, as well as needs of potential buyers. Furthermore, compliance with regulatory requirements (e.g. compliance with relevant security and data protection requirements drawn from relevant regulatory frameworks) is an important aspect of technologies and services for positioning them into the market.

4.4 STAKEHOLDER COLLABORATION

In order to assess the role of stakeholder collaboration in innovation activities, the analysis investigates the following questions:

Q14. Is there any support for geographical proximity by bringing together innovation stakeholders (e.g. universities, campuses clusters, start-ups, etc.)?
Q15. Are there any sector specific initiatives that support collaboration and fostering of innovative products and services?

Error! Reference source not found. provides an overview how experts responded to these questions. They identify that geographical clusters and collaborations are important mechanisms that support innovation.

*There are several initiatives bringing people together in **Brussels**, e.g. the Brussels Initiative on Cybersecurity and Innovation. Also, everything in Brussels is geographically close enough, which helps in bringing people together*.

However, collaboration mechanisms may support innovation differently.

***In Germany**, the BSI takes part and/or organises sector-specific working groups for cybersecurity products and services with industry and/or research institutes (e.g. Frauenhofer Gesellschaft) on encryption, Artificial Intelligence and others. There are also regional initiatives for fostering collaboration: competence centres in certain regions dealing with different topics, such as cybersecurity research, military purposes, or universities.*

Figure 9: Stakeholder collaboration

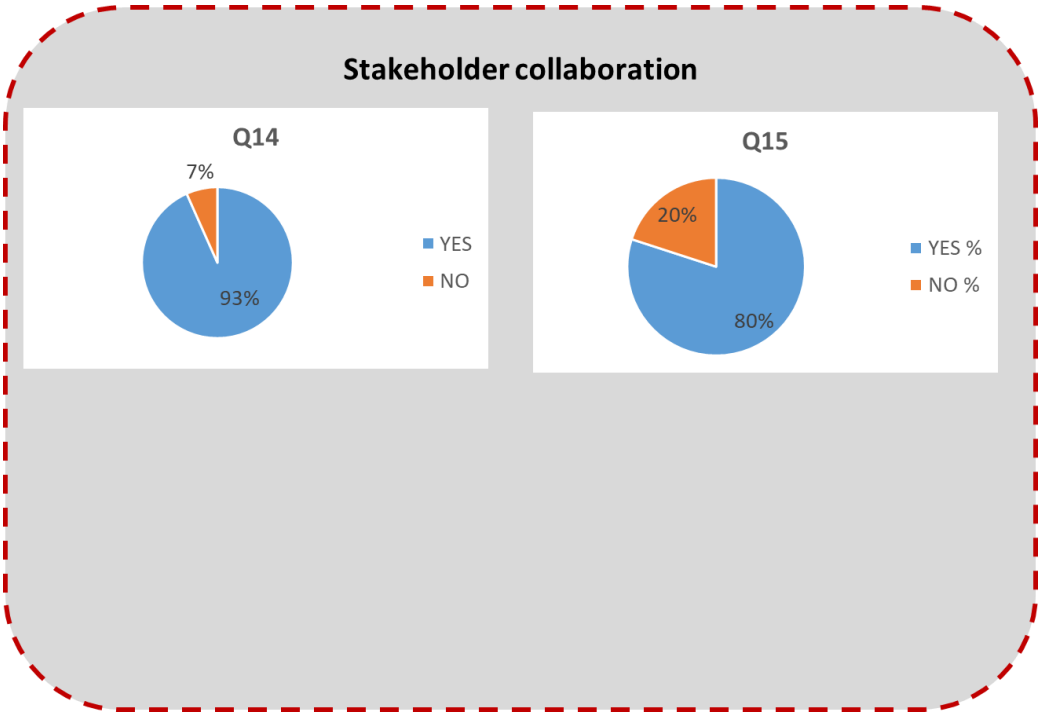


Table 4 highlights how experts recognise different collaboration mechanisms. Experts identify that the involvement of industry in research and innovation is the most important factor affecting industrialisation.

Table 4: Factors supporting industrialisation

Critical factors	Mean ranking (1 most important – 5 least important)
Involvement of industry in research and innovation	1,5
Industry secondments	3
Involvement of industry in education	3
Public-Private Partnerships	3
Conferences and Workshops	4

Industry takes an active role in conducting and shaping research and innovation. Other important mechanisms for industrialisation are industry secondments, involvement of the industry in education and Public-Private Partnerships (PPPs).

*The **Estonian** Information Security Association (EISA) was founded to boost cross-sectorial cooperation in Estonia between academia and private sector as well as with the government, including supporting the EU's contractual Public Private Partnership (cPPP) model on cybersecurity. The joint effort intends to formalise existing ties and enhance R&D activities in the information security and cybersecurity field in Estonia.*

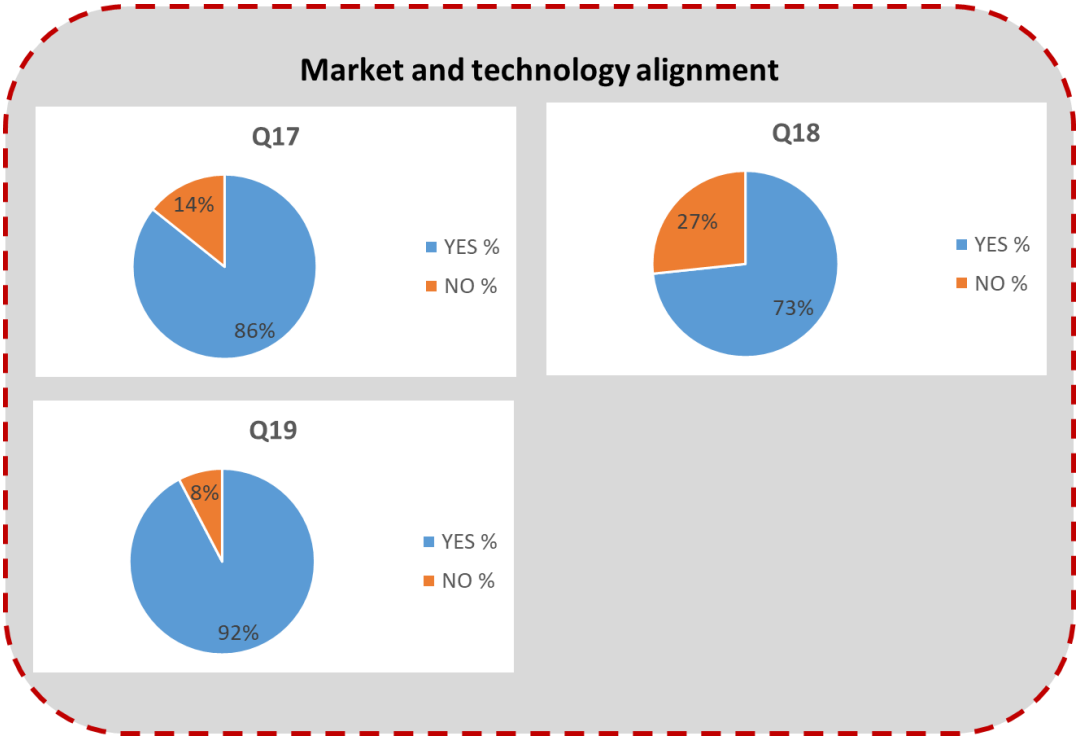
4.5 MARKET AND TECHNOLOGY ALIGNMENT

To assess the role of market and technology alignment in innovation, the analysis investigates the following questions:

Q17. Are there any barriers and challenges for creating alignments between markets and technologies/services?
Q18. Are publicly funded research and innovation effectively addressing current and future capability gaps of private and public services?
Q19. Are there any initiatives to build national talent base in cybersecurity research and innovation in order to produce game-changing technologies and services addressing current and future threats?

Figure 10 provides an overview how experts responded to these questions.

Figure 10: Market and Technology Alignment



Experts recognise that research and innovation initiatives are addressing future needs. Furthermore, Member States are taking various initiatives in order to support talent in cybersecurity research and innovation.

***In Austria**, the Ministry of Defence organises specific initiatives (e.g. Hackathons) supporting talent building and widening their recruiting strategies (e.g. internship opportunities for six months).*

However, experts recognise also the existence of barriers and challenges for supporting alignments of technologies and services with markets. Interviews with experts and surveys highlight that normal market dynamics create opportunities for bringing innovation in operations.

***In Belgium**, which is a small country, regional governments seek to invest where they can make a difference. They do not have the scale or budgets of international leaders, but they do have excellent research in relevant domains, such as AI, on which they thus seek to focus investment.*

In addition, there are differences across sectors. For example, the public sector depends on procurements, which require companies offering their services and products to follow necessary procedures and to comply with relevant requirements. Other sectors (e.g. cyber defence, critical infrastructures, etc.) may have additional market constraints due to the criticality of services offered at national level.

4.6 MARKET REGULATIONS

To assess the role of market regulations in innovation, the analysis investigates the following questions:

Q20. Do government's incentives accelerate the adoption of new technology in cybersecurity and privacy?
Q21. Are there sector specific incentives to help in the adoption of new cybersecurity technologies/services?

Error! Reference source not found. provides an overview how experts responded to these questions. It appears that governments' incentives have a positive impact in accelerating the adoptions of new technologies, products and services.

***In Germany**, there are different relevant national strategies supporting various objectives. Such strategies cover different topics and address different objectives: from applied cybersecurity to cybersecurity research. Talking specifically about the NCSS, it covers four (4) areas:*

1) Secure and autonomous acting in a digital environment

2) Joint mission of State and Economy

3) Efficient and sustainable cyber security architecture

4) Active positioning of Germany in European and international cyber security.

Within the activities concerned with 'Secure and autonomous acting in a digital environment', there are different measures including strengthening IT security research and innovation. The Ministry of Research and Innovation, in relation to the later, is providing direct funding through a programme called 'Being autonomous and secure in a digital world' (EUR 180 million). Moreover, BSI develops technical guidelines, which promote adequate cybersecurity standards in IT systems of different sectors/areas.

However, there are factors that may constrain markets and the adoption of new technologies, products and services.

Figure 11: Market regulations

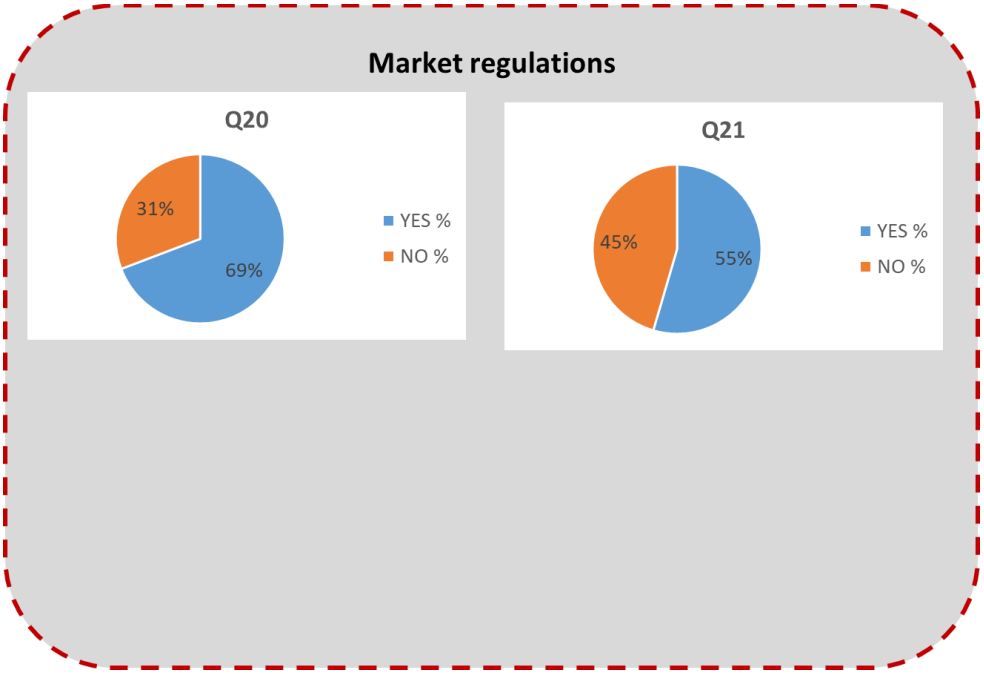


Table 5 highlights how experts perceive critical factors on policies and legislative frameworks that may stimulate innovation in cybersecurity. Regulatory stability and predictability as well as neutral technological regulation are important factors to support innovation. Similarly, experts recognise stakeholder involvement equally important. They recognise principle-based regulations and performance evaluations to be less critical than other factors. Experts perceive differently the impact of regulatory frameworks and initiatives. On one hand, they highlight that most regulatory frameworks and initiatives focus on compliance (rather than security). Such frameworks and initiatives may prevent the adoption of innovative solutions and services that innovative companies such as start-ups provide. On the other hand, regulatory frameworks and initiatives may drive innovation. Companies invest in compliance projects (e.g. compliance with GDPR) and cybersecurity capabilities (e.g. cybersecurity capabilities in alignment with security requirements and incident notification) in order to align with relevant regulatory frameworks.

Table 5: Factors of policies and legislative frameworks in innovation

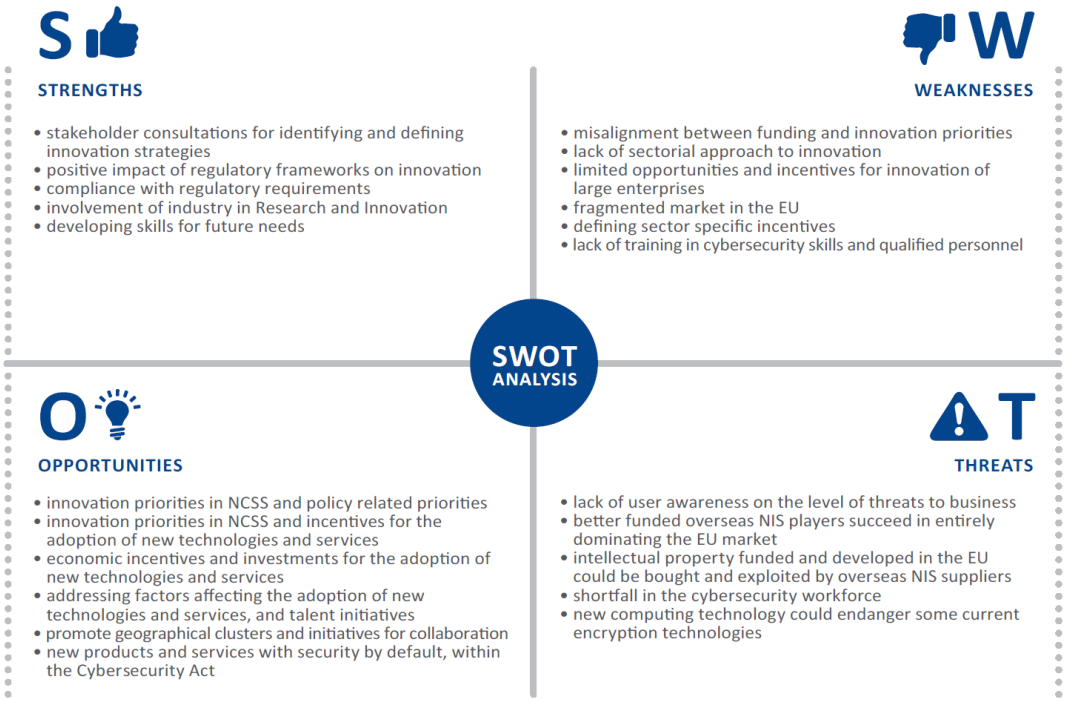
Critical factors	**Mean ranking** (1 most important – 5 least important)
Regulatory stability and predictability	2
Technology neutral regulations	2
Stakeholder engagements	2
Principle-based regulations	3
Performance evaluation	4

5. SWOT ANALYSIS

This section discusses strengths, weaknesses, opportunities and threats that influence the successful implementation of innovation priorities in the Member States. It also provides a strategic forward looking perspective, which provides insights for further developments of National Cyber Security Strategies. Figure 11 summarises the SWOT analysis of this chapter.

NIS Directive and the GDPR accelerated and incentivised innovation in relevant areas of security and data protection

Figure 12: SWOT that influence innovation priorities under NCSS



5.1 STRENGTHS

Stakeholder consultations for identifying and defining innovation strategies. The interviews with experts highlighted that some Member States may have both formal and informal means of engaging with and collecting feedback from innovation stakeholders. In particular, industry involvement provide insights in defining innovation strategies. Member States shall consider establishing and consolidating stakeholder involvements while identifying and specifying national cybersecurity innovation strategies.

Positive impact of regulatory frameworks on innovation. The experts highlighted how regulatory frameworks such as the NIS Directive and the GDPR accelerated and incentivised innovation in relevant areas of security and data protection. On the one hand, regulatory frameworks define governance regimes for new technologies and services. On the other hand, they may incentivised and accelerate innovation in the specific areas of interventions.

Compliance with regulatory requirements. Experts recognise that compliance with regulatory requirements is an important factor for commercialising and positioning cybersecurity services and technologies in the market. This is also in alignment with the EU Cybersecurity Act, which requires the development of a European Cybersecurity Certification Framework for ICT products, services and processes.

Involvement of industry in Research and Innovation. An important mechanism for supporting industrialisation is to involve directly industry in research and innovation activities. This helps research stakeholders (e.g. universities, research centres, etc.) to align with industry needs as well as industry stakeholders to identify opportunities for adopting or commercialising research outcomes.

Developing skills for future needs. Among the various innovation strategies, it was possible to identify different initiatives supporting development of cybersecurity skills. It is important to extend such initiatives in order to develop the necessary skills for emerging cybersecurity technologies and services.

5.2 WEAKNESSES

Misalignment between funding and innovation priorities. Among the identified challenges are lack of funding and misalignment between innovation and market. This is to a certain extent due to the fact that there is a lack of direct funding supporting innovation strategies. This may result in disconnects between national strategies and availabilities of funding for achieving and supporting the implementation of strategic objectives related to innovation under national cybersecurity strategies.

Lack of sectorial approach to innovation. Often the lack of funding in cybersecurity is due to limited opportunities supporting innovation across different sectors. Although cybersecurity is a critical factor, funding opportunities are often within generic topics (e.g. Artificial Intelligence, Automotive, Manufacturing, Industry 4.0, etc.). Furthermore, there is a lack of funding addressing cybersecurity across sectors without giving any priorities to critical sectors (for instance, the sectors of Operators of Essential Services that the NIS Directive identifies). More R&D financing of EU technical innovation is needed as well as funding of NIS projects in the critical sectors, which could use EU NIS products and services. Investing in R&D is expensive for small EU specialist NIS vendors, and participating in EU programmes is difficult. Switching to regional and national levels would need coordination.

Limited opportunities and incentives for innovation of large enterprises. There are various mechanisms at the European and national level supporting innovation for SMEs as well as emerging innovative entrepreneurships such as start-ups. Unfortunately, there are limited opportunities and incentives for innovation of large enterprises. Besides some Public-Private Partnerships (PPPs), large enterprises have to face most of the cost and investment in innovation. However, they may have a critical role in order to accelerate innovation as well as to provide access to markets for innovation at scale. Unfortunately, there is a lack of initiatives and incentives in order to support innovation collaboration between SMEs and large enterprises, besides normal market dynamics.

Fragmented market in the EU. Suppliers need to be able to cope with a fragmented EU market often divided by language and culture. NIS often requires a specific relationship of trust so customers may mandate that the vendor speak the same language to build this and then conserve it in a long-term relationship. It should result in a transfer from transactional selling to a service-based relationship of repeated sales. Marketing strategies may support companies in promoting their services to potential buyers, in particular, internationally. Procurement to the public sector may help companies in promoting themselves in the market.

Lack in defining sector specific incentives. Despite the positive impact of regulatory frameworks on innovation, there is still a lack of incentives and regulatory frameworks targeting specific sector interventions. Organisations have to deal with different frameworks, not necessary tailored to their market needs and specificities.

Lack of training in cybersecurity skills and qualified personnel stretches back through to university education in cybersecurity and even further into the introduction of computing and coding, at the level of secondary schools. This impacts awareness in general and is causing a shortage of staff with the qualifications and experience the NIS industry sorely needs.

5.3 OPPORTUNITIES

Innovation priorities in NCSS and policy related priorities: it is necessary to understand the relationships between innovation priorities in NCSS and other policy related priorities. In particular, policy related initiatives should follow and support innovation priorities in NCSS. As a marketing tool to promote EU NIS companies within the EU and internationally, **technical standards for NIS products and services** should be used, such as the Federal Office for Information Security in Germany, BSI, for ICT approvals but at EU level. An **EU-wide security label** would support European sales. Harmonised qualifications should be created through local national standards but **not as a centralised approach as the EU MS require sovereignty over NIS matters**. Moreover, such standards should be promoted overseas, so EU NIS providers gain global recognition, which is especially significant in the developing world. The standards setting and approvals initiative and its international promotion could be part of ENISA's responsibilities

Innovation priorities in NCSS and incentives for the adoption of new technologies and services: it is necessary to align innovation priorities in NCSS with relevant incentives for the adoption of new technology. There are a number of **European institutions and programs supporting NIS development[26] [27], etc** with the main goal to ensure cyber protection for all: citizens, companies (including SMEs) and public administration by supporting the development of an EU cybersecurity industry

Economic incentives and investments for the adoption of new technologies and services: economic incentives may accelerate the adoption of new technologies, products and services. Increased availability of national or regional funds and tax incentives. For example, start-ups can benefit from a cut on R&D costs, on social charges and on corporate taxes. Investors who invest in start-ups and innovation can also benefit from cuts in charges which can lead to turning the investment riskless, as the funds invested would have been otherwise spent in paying taxes[28].

Addressing factors affecting the adoption of new technologies and services, and talent initiatives: it is necessary to address factors affecting the adoption of new technologies and services as well as take into account relevant talent initiatives. Through early school education in secure software development plus development of new professional qualifications at degree and post graduate levels, create a stronger EU-based NIS industry with large numbers of qualified personnel for three areas requiring stronger NIS skills:

- CSIRT teams to work in SOCs
- Product development – both NIS and generally, especially for infrastructure
- Programming of all types – bespoke, embedded, product packages for the commercial market

Promoting geographical clusters and initiatives for collaboration: geographical clusters support collaboration initiatives. Leveraging existing European clusters specialized in cybersecurity will help to develop business in close proximity with other start-ups, incubators/accelerators, universities and big corporations.

Security by default, within the Cybersecurity Act will allow new NIS products and services to become more affordable and attractive to use, as they will be configured by default with the most secure setting possible. Security by default will not require specific technical knowledge and understanding of consumers.

5.4 THREATS

Lack of awareness of users of the level of threats to business is a common theme across the EU Member States. This lack of awareness is greatest in the EU's SME segment, where governments need to provide more support. Business and the public sector are not being sufficiently educated on

[26] https://ec.europa.eu/programmes/horizon2020/h2020-sections
[27] https://ec.europa.eu/digital-single-market/en/policies/start-up-europe
[28] https://www.enisa.europa.eu/publications/challenges-and-opportunities-for-eu-cybersecurity-start-ups

the need for security. Major fraud activities touch every level of the population every day, but continued low levels of sales of NIS services and products threaten the EU economy.

In terms of the global market, the **key threat to EU is** that **better funded overseas NIS players succeed in entirely dominating the EU market**. They could exploit the EU's fragmentation by acquiring the best local companies in each Member State, then expanding sales as a common brand across the EU, with major inward investment underpinned by their home markets' revenues (in the USA and China).

Similarly, it is conceivable that **intellectual property funded and developed in the EU could be bought and exploited by overseas NIS suppliers**, from China and the USA, so that EU investments in R&D may be lost to the EU. In this regard, promising EU suppliers may have little alternative because of the limited EU investment available to enable them to develop the more advanced tools required and bring them to market. Not only is EU funding for R&D and industrialisation too limited, given the scale of AI and large-scale data analytics required, but it is spread too thinly, making the creation of a major EU player less likely. Moreover, EU and national funding may be too burdensome to access in terms of costs and bureaucracy for start-ups and SMEs. Thus, any promising innovative or existing EU NIS supplier is often acquired by a global player, especially if major equity holders are anxious to realise their investments.

The **shortfall in the cybersecurity workforce** remains a critical vulnerability for the industry. Conventional education and training policies cannot meet demand. The lack of trained personnel exacerbates an already difficult task of managing cybersecurity risks. Professional certification in NIS is essential to increase the qualified workforce.

Sometime in the next decade, **new computing technology could endanger some current encryption technologies**. That would open more customer databases to attack for data theft. Confidence in online commerce, and in any business that stores customer or confidential data, could be compromised. Countering this will require further R&D investments in cryptography for new algorithms.

6. RECOMMENDATIONS

The analyses of National Cyber Security Strategies across Member States provide an overview of innovation challenges and good practices. Based on the results of this study, which also involved experts providing further insights and examples of innovation practices, this report draws some recommendations for enhancing innovation in cybersecurity. Stakeholders who are involved in developing and implementing NCSS, EU policy makers, National policy makers may take into account the results of this study, in particular, the identified challenges, good practices and suggested recommendations:

Support and develop sector specific innovation priorities both at National and EU level – Current level of funding is often perceived insufficient or misaligned with industry needs and expectations. This is also due to a certain extent to the fragmentation of funding mechanisms as well as to the lack of coordination between alternative funding mechanisms at regional, national or European level. In order to address the lack of funding as well as the misalignment between innovation strategies and industry needs, it is necessary to support an adequate level of funding for innovation priorities and to support coordination among alternative funding mechanisms. Moreover, most innovation priorities and funding mechanisms support general cybersecurity objectives (including development of new products, services and processes) or other generic objectives for which cybersecurity is only a part of them. Therefore, it is necessary to take into account different needs across sectors. Currently, there is a lack of cybersecurity initiatives tailored to specific sectors. Addressing this situation would help developing a sectorial approach to innovation in cybersecurity.

Provide adequate level of funding both at National and EU level - Most economic incentives and funding mechanisms support research organisations such as universities and research centres, and innovative enterprises such as SMEs and start-ups. However, economic incentives and funding mechanisms shall recognise the innovation contributions of all stakeholders, from SMEs to large enterprises and research institutions in the public and private sectors. Innovation stakeholders need different types of economic incentives and funding mechanisms depending on their specific contributions to innovation in cybersecurity.

Involve stakeholders while developing and implementing innovation priorities both at National and EU level. In order to address stakeholder's expectations and support their needs, it is necessary to establish both formal and informal channels of communication. A way is to achieve this is to support the creation of industrial clusters:

- To create clusters of start-ups, SMEs and post-start-up ecosystems, with geographic concentration of resources and cross EU links to smaller players of all kinds, possibly around a university as a centre of NIS excellence, or other permanent institution, such as a testing and certification lab.
- Clusters could be formed at various locations across the EU.
- With formation of clusters for vertical sectors also, where appropriate.

Take into account the positive impact of regulatory frameworks on innovation at national level and EU level – Regulatory frameworks may have a positive impact on accelerating innovation and adoption of new products, services and processes. Therefore, regulatory frameworks may positively support the achievement of specific innovation objectives. Emphasising compliance with regulatory requirements as a market differentiator may be perceived mainly in terms of obligations. However, compliance with specific regulatory requirements may clearly define market opportunities both in the public and private sectors.

Support industries in positioning new cybersecurity offerings in the market both at National and EU level – Innovative organisations such as SMEs and start-ups may face challenging market conditions (e.g. fragmentation, international competition, etc.) in order to offer and position their products, services and processes. It is therefore necessary to support them with specific initiatives such us effort towards internationalisation of offerings in order to help them to growth into the cybersecurity market.

Promote EU level certification of services/products both at National and EU level. That would engender trust for users within the EU and provide a stamp of approval for international markets that other regions do not have by enabling:

- Security certification of ICT products and services for software, hardware and firmware, ranging from apps for smartphones to data centre management utilities to real-time industrial control software to chip level security. Certification should be detailed and robust – not just a tick box exercise.
- Certification of NIS products should be in terms of efficiency, ease of use and effort needed across the product/service lifecycle.
- Approved centres of certification.
- EU security branding for certified products and services.
- Continuous certification processes to track developing products/services.

Promote NIS training and educational measures both at National and EU level:

- University level qualifications for a new NIS workforce, with a new emphasis on security as a basic computer science
- Support skill developments for current needs as well as future needs due to emerging cybersecurity technologies and services **–** Skill developments should take into account employability as well as innovation. It is necessary to support skill developments addressing current needs as well as competencies and capabilities needed for emerging innovative technologies, services and processes.
- Education at school level on the need for cybersecurity in using ICT devices and in writing software
- Support funds for training NIS service staff for cybersecurity incident response teams, e.g. six-month induction course for several thousand staff annually across the EU, with financial support for training courses and trainees. This would provide NIS service providers of all sizes with a solution to the gap in qualified personnel for the security operations centres (SOCs) that will be a key feature of the future EU NIS industry.

Some of these actions have already been put into motion, For example, the agreed approach of the Commission is already turning to maximise awareness in the cybersecurity community of financing opportunities at European, national and regional level, via existing instruments and channels such as the Enterprise Europe Network29 and also has initiated the contractual Cybersecurity Public Private Partnership (cPPP) for large-scale funding. Moreover the Commission may complement these efforts with inputs from the European Investment Bank (EIB) and the European Investment Fund (EIF) to accelerate access to finance with further measures.

[29] *Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry.* EC COM 410 Final, 05JUL2016,

TP-01-19-830-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

enisa.europa.eu

ISBN 978-92-9204-308-7
doi: 10.2824/01007