DIGITAL EUROPE

Cybersecurity

Work programme 2021-2022

DRAFT

 *16 November 2020*

DISCLAIMER

All the budget figures in this document are purely indicative and
DO NOT REPRESENT the final budget allocation

Introduction

Digital technologies are profoundly changing our daily life, our way of working and doing business, the way we understand and use our natural resources and environment and the way people interact, communicate and educate themselves. The von der Leyen’s Commission has presented an ambitious strategy in its digital package of February 19th 2020. The [Council conclusions on shaping Europe’s digital future adopted on the 9th of June 2020](https://www.consilium.europa.eu/register/en/content/out?typ=SET&i=ADV&RESULTSET=1&DOC_TITLE=&CONTENTS=&DOC_ID=8711%2F20&DOS_INTERINST=&DOC_SUBJECT=&DOC_SUBTYPE=&DOC_DATE=&document_date_from_date=&document_date_from_date_submit=&document_date_to_date=&document_date_to_date_submit=&MEET_DATE=&meeting_date_from_date=&meeting_date_from_date_submit=&meeting_date_to_date=&meeting_date_to_date_submit=&DOC_LANCD=EN&ROWSPP=25&NRROWS=500&ORDERBY=DOC_DATE+DESC) confirmed this ambition.

The COVID-19 crisis has further highlighted the critical role of digital technologies and infrastructures in our lives and demonstrated how our societies and economies rely on digital solutions. The crisis confirmed how important it is for Europe not to be dependent on systems and solutions coming from other regions of the world.

The efforts needed are not limited to Research and Development. The EU must drastically improve its digital capacities. This includes digital technologies, as well as the necessary digital skills for EU workers. Europe must also develop key digital infrastructures and strengthen its industrial base, enhance its resilience and flexibility both in terms of technologies and supply chains. Delivering this will require massive public and private investment and common efforts that no Member State alone could secure. In that context, the European data strategy has announced a High Impact project on European data spaces, encompassing data sharing architectures and governance mechanisms, as well as the European federation of energy-efficient and trustworthy cloud infrastructures and related services.

This document sets out the Cybersecurity work programme for part of the actions implemented in the first two years of the Digital Europe Programme.

The work programmes follows the extensive consultation with Member States, stakeholders and the public on drafts of the strategic orientations for the programme. It uses as reference point the Annex1 of the Digital Europe Programme’s regulation.

The Digital Europe programme objectives

The Digital Europe programme will reinforce EU critical digital capacities by focusing on the key areas of artificial intelligence (AI), cybersecurity, advanced computing, data infrastructure, governance and processing, and their deployment and best use for critical sectors like energy and environment, manufacturing, agriculture and health. The programme also targets upskilling to provide a workforce for these advanced digital technologies. It supports industry, SME’s, and public administration in their digital transformation with a reinforced network of European Digital Innovation Hubs. Digital Europe will accelerate the recovery and drive the digital transformation of Europe.

The twin transitions to a green and digital Europe remain the defining challenges of this generation. This is reflected throughout the Commission’s proposals. Digital Europe will deliver on the goals set out in the European Data strategy of creating a true European data economy. It will help bring European human centred AI-solutions as set out in white paper on AI and it will unleash the powers of digital to reach Europe’s common goal of being climate neutral in 2050 as set out in the European Green Deal.

With the actions contained in this work programme, Digital Europe will deploy a European quantum communication infrastructure, and build up advanced cybersecurity equipment, tools and data infrastructures. It will support the development and best use of European knowledge and skills related to cybersecurity, promote the sharing of best practices and ensure a wide deployment of the state of the art cybersecurity solutions across the European economy to guarantee the resilience, integrity and trustworthiness of the Digital Single Market.

Indicative Budget and implementation

At the time of drafting this document the final budget is not decided yet. The budget brackets per topic are indicative, adding up to the amount included in the overall MFF agreement of 10 November 2020 (based on EUCO July 2020 agreement i.e. with a cut of 17,4 % to the original Commission proposal of EUR 8,2 billion in 2018 prices). The cut is applied linearly to the Strategic Objectives. However, as MFF negotiations are still ongoing the budget figures in this document might be subject to change.

Digital Europe is implemented by means of multiannual work programmes. There are independent work programmes for those parts which are implemented under indirect management (High Performance Computing and Cybersecurity), and for the European Digital Innovation Hubs (EIDH). Activities in this work programme are implemented under indirect management by the Cybersecurity Competence Centres Network as foreseen in the legislative proposal. Synergies and complementarities of the activities in the various work programmes will be ensured.

Participation in selected calls funded from the budget lines of Specific Objective 1, 2, and 3 may be restricted on the basis of art 12 of the Digital Europe Programme Regulation.

Contents

[1 Cybersecurity and Trust 5](#_Toc56439971)

[1.1 A secure quantum communication infrastructure for the EU (the EuroQCI) 5](#_Toc56439972)

[1.1.1 Create a European Industrial Ecosystem for Secure QCI technologies and systems 6](#_Toc56439973)

[1.1.2 Deploying advanced national QCI systems and networks 8](#_Toc56439974)

[1.1.3 A large-scale testing and support to certification infrastructure for QKD devices, technologies and systems enabling their rollout in EuroQCI 9](#_Toc56439975)

[1.2 Joint Preparedness, Situation awareness and Response 10](#_Toc56439976)

[1.2.1 EU cyber resilience and coordination; cyber ranges 10](#_Toc56439977)

[1.2.2 Security Operation Centres (SOCs) 11](#_Toc56439978)

[1.2.3 Strengthening of GovSatCom network 12](#_Toc56439979)

[1.3 Support to Implementation of relevant EU Legislation 13](#_Toc56439980)

[1.3.1 Deploying the network of national coordination centres with Member States 13](#_Toc56439981)

[1.3.2 Structural support and community building for EU Cybersecurity 14](#_Toc56439982)

[1.3.2.1 Cyber Security Community support 14](#_Toc56439983)

[1.3.2.2 European Cybersecurity Atlas 16](#_Toc56439984)

[1.3.3 Supporting the NIS Directive implementation and national cyber security strategies 17](#_Toc56439985)

[1.3.4 Testing and certification capabilities 18](#_Toc56439986)

[1.4 Support to market players and skills 20](#_Toc56439987)

[1.4.1 Securing 5G and other strategic digital infrastructures and technologies 20](#_Toc56439988)

[1.4.2 Uptake of innovative cybersecurity solutions and skills 20](#_Toc56439989)

[1.4.3 Support to the health sector 22](#_Toc56439990)

[2 Programme Support Actions [SECTION IS WORK IN PROGRESS] 23](#_Toc56439991)

[3 Implementation [SECTION IS WORK IN PROGRESS] 24](#_Toc56439992)

[3.1 Main implementation measures and EU financial contribution 24](#_Toc56439993)

[3.2 Procurement 24](#_Toc56439994)

[3.3 Grants – Calls for proposals 24](#_Toc56439995)

[3.3.1 Evaluation process 24](#_Toc56439996)

[3.3.2 Selection of independent experts for evaluation and reviews 25](#_Toc56439997)

[3.3.3 Indicative implementation calendar 25](#_Toc56439998)

# Cybersecurity and Trust

Cyber security is at the heart of the digital transformation of the European Union. Digital Europe Programme will strengthen the capabilities of the Union to protect its citizens and organisations aiming –amongst others- to improve the security of digital products and services. In the first two years of implementation, the activities could focus on the proposed three main work strands, but the Governing Board of the Implementing body (i.e. the European Cybersecurity Industrial, Technology and Research Competence Centre) will take the final decision on the activities to be supported once the relative Regulation will entry into force.

The focus in the first Work Programme is on:

* Support the deployment of cyber infrastructures (including EuroQCI);
* Strengthening the unions joint preparedness, situation awareness and response
* Support the implementation of relevant EU legislation and political initiatives: namely the NIS Directive, the Cyber Security Act, the European Cybersecurity Competence centre and network, the cyber Blueprint and Joint Cyber Unit, the 5G security toolbox;
* Support the capacity building, in particular for SME and sectors particularly affected by the Covid-19 pandemic and the ensuing economic crisis.

Indicative budget envelope

The budget share proposed is only indicative and subject to discussion and refinement.

* For actions leading to the setup of a secure quantum communication infrastructure for the EU (the EuroQCI): a budget of EUR 165-185 million
* For actions related to Cybersecurity Joint Preparedness, Situation awareness and Response: a budget of EUR 80-100 million
* For actions supporting the Implementation of relevant EU Legislation: a budget of EUR 100-120 million
* For actions supporting market players and improving skills: a budget of EUR 50-70 million

## A secure quantum communication infrastructure for the EU (the EuroQCI)

The security of current encryption technologies relies on computational hardness assumptions. In the near future advances in computing-enabled, combined with ever more insidious “brute force” and hardware-layer attacks, could put at risk the security of telecom and data communication networks. As a result, Europe’s communications networks and the sensitive data that they transmit could become extremely vulnerable.

In order to find solutions to these issues, the Commission is working with Member States as well as the European Space Agency, towards the deployment of a secure quantum communication infrastructure (EuroQCI) spanning the whole of the EU, including its overseas territories.

The EuroQCI will provide an unprecedented way of securing communications and data, supplementing current software-based security systems with physical security that makes use of the latest developments in quantum communication technologies. Its aim will be to secure the EU's public communication assets, in particular critical infrastructure and encryption systems, against cyber threats.

In several EU Member States, initiatives to build local/national quantum communications infrastructures are already underway. However, there is a strong case for EU-level coordination: joint efforts by Member States are needed to match the significant advances in quantum communication being made elsewhere in the world. Not all EU Member States have strong know-how and industrial capability in quantum communication technology. The first service to make use of the EuroQCI will be quantum key distribution (QKD), a highly secure form of encryption that makes use of the principles of quantum mechanics. The EuroQCI will allow Europe’s research excellence to form a base for industrial and commercial use, providing a strong supply- and demand-side stimulus for European industry. It will encourage the EU’s industrial ecosystem development, creating a large market pull and helping the EU’s quantum industry develop new, innovative systems and technologies critical for European open strategic autonomy and digital sovereignty.

The EuroQCI infrastructure will consist of a terrestrial component building on existing fibre communication networks linking strategic sites at national and cross-border level, complemented by a space component to cross-link and cover the whole EU. In order to preserve European sovereignty and autonomy, it will be built with European technology.

The actions supported by the Digital Europe programme are complemented by those developed through other EU programmes such as Space, Horizon Europe and the Connecting Europe Facility, and by activities carried out by the ESA, complemented by national, regional and private funds.

In the first two years of the EuroQCI’s implementation, the activities funded by the Digital Europe programme will focus on the following four main areas:

* preparation for industrialisation of European QKD systems with improved performance, and contributing to the development of Europe's industrial ecosystem for quantum communication technologies and systems;
* early deployment of advanced quantum networks supporting national quantum communication initiatives and their integration with existing communication networks;
* deployment of a pan-European “testing and validation” infrastructure to assess the compliance of different European technologies, accelerating solution development, and ensuring trust in the EuroQCI;
* preparation and coordination of the large-scale deployment of the EuroQCI infrastructure.

Subsequent activities will focus on the full deployment of the terrestrial network infrastructure, the full deployment of the space network infrastructure, and the operationalisation and support of the full EuroQCI network infrastructure.

The EuroQCI is part of an ambitious and long-term vision for Europe, brought together by the work of the EU-funded Quantum Technologies Flagship. The ultimate goal is for the EuroQCI to become the backbone of a future “quantum internet”, which would connect quantum computers, simulators and sensors to radically enhance their performance and enable a new technological revolution.

### Create a European Industrial Ecosystem for Secure QCI technologies and systems

Objective

To prepare for industrialisation and for deployment quantum communications infrastructure (QCI) technological capabilities and advanced QCI networks essential for European cybersecurity, and contribute to the development of a European industrial QCI ecosystem.

Scope

The action will focus on the following two priorities:

* **Industrialisation of EU QKD devices, technologies and systems**: prepare for industrialisation and for deployment (i.e. reaching TRL 8-9) quantum technology components for quantum key distribution that are stable, miniaturised and have competitive performance (e.g. cost-effective, exhibiting higher key exchange rates, link distances). QKD systems should enable scalability to multi-user network architectures and upgradability to future quantum information networks. Examples of such core technology components include QRNG, photon sources, application and control software, etc. Work should also cover the integration of individual components and devices to larger, standalone QKD systems and their full testing and thus compliance to EU (ETSI/CENELEC) standards (including independent device protocols) in view of their potential deployment in the EuroQCI initiative[[1]](#footnote-2). Work should also include an exploitation plan covering all the industrialisation and fabrication aspects of such devices, technologies and systems underpinning the creation of an EU QKD supply chain.
* **QKD-based Telecom Network System production**: Develop the full run system integration from EU QKD system (level 1) to Telecom network systems (level 2), key management (level 3) until cyber security system level (level 4). The level 4 quantum cybersecurity systems will then be integrated in traditional communication networks, assuring interoperability in a full multi-user end-to-end architecture. Upgradability to quantum information networks should be considered. Work could also cover the testing and certification/standards compliance of the complete QKD-based Telecom System in view of its deployment in the EuroQCI initiative.

Individual proposals should cover one of the above priorities. Overall, the proposals selected for EU funding shall cover both priorities.

Outcomes and deliverables

* Mature QKD-based systems ready for integration and deployment in an operational telecom infrastructure;
* First fully functional telecom network systems managing quantum keys and assuring the interoperability between quantum and traditional cybersecurity systems, that ensure the secrecy and integrity of sensitive communications digital data in Europe;

|  |  |
| --- | --- |
| Type of action | SME support grant (75% co-funding rate for SMEs and 50% for all the other beneficiaries) |
| Indicative Budget | [ 40 -50 MEUR ] |
| Indicative time of call opening  | First call |
| Indicative duration of the action | 24-30 months |
| Indicative budget per grant (EU contribution) | 5-15 MEUR  |

### Deploying advanced national QCI systems and networks

Objective

To deploy advanced national quantum systems and networks for testing quantum communication technologies and for integrating them with existing communication networks. Use these quantum systems and networks to develop and experiment use cases in support of national QCI initiatives in the context of the EuroQCI initiative. These quantum systems and networks will have to be managed by national authorities or their representatives.

Scope

In each Member State, activities will focus on the following priorities:

* Deploying advanced experimental quantum systems and networks combining the best of quantum and classical security technologies. Making them widely available for undertaking and testing, in a number of real use cases, the functioning and the provision of very high security QKD components and systems, their interoperability and the end-to-end secure functioning of the system architecture. The aim is to prepare the large-scale uptake and use of such systems and technologies, operating in traditional telecommunications networks, by national stakeholders and their first use in advanced use cases in different application scenarios:
	+ targeting firstly public use cases by linking public authorities within the country;
	+ making these quantum networks available to industries operating the network’s different layers contributing to developing national-based production chains for supplying critical quantum communication components and systems. This includes the integration of quantum and traditional cybersecurity systems in communication systems and networks (possibly also supported by post-quantum algorithms), which will be used to prepare for the future large-scale deployment of EuroQCI;
	+ making these quantum systems and networks available for educational purposes providing a training environment for technical staff and national users from public authorities or other organisations.
* Demonstrating first long-distance quantum communication networks compatible with the overall EuroQCI system architecture to prepare the large-scale deployment of a QCI spanning the EU;
* Where relevant, testing the interface between the QCI’s space and terrestrial systems.
* Cooperating and participating with other Member States in the deployment plan and strategic efforts towards designing and building an overall EuroQCI system architecture, including by exchanging lessons learned and experiences in building robust and fully secure QKD systems and networks.

Outcomes and deliverables

* First deployed QKD experimental networks integrated and operating with existing communication networks in several Member States and addressing different advanced use cases, contributing to prepare for the full deployment of the EuroQCI;
* A large number of trained users in quantum communication technologies and Member States ready for the design and deployment of next generation highly secure communication and data networks.

|  |  |
| --- | --- |
| Type of action | Grant for Support to Third Parties – *cascading grants* (*50% co-funding rate to be finalised*) up to 1 million euros  |
| Indicative Budget | [ 100 - 120 MEUR ] |
| Indicative time of call opening  | Second call |
| Indicative duration of the action | 24 to 30 months |
| Indicative budget per grant (EU contribution)  | Up to 8 MEUR |

### A large-scale testing and support to certification infrastructure for QKD devices, technologies and systems enabling their rollout in EuroQCI

Objective

To deploy a flexible large-scale testing and certification QKD infrastructure that is in the service of all relevant actors of the Member States, to assess the full-scale compliance of different EU technologies, i.e. compliance with standards (architectures, protocols, etc.), compliance with security specifications (certification); and compliance with product specifications (features, performance, reliability, etc.) with a view to their later integration in EuroQCI.

Scope

Preparation for procurement (including coordination of national efforts)

* Support discussions on user requirements and use cases, national deployment plans and strategic efforts with the aim of increasing networking between national QCI projects, achieving an overall EuroQCI system architecture by setting an overall roadmap for EuroQCI;
* coordinate standardisation and certification initiatives (which include the definition of mutual recognition criteria in security) enabling the development of a European-based supply chain for quantum communication components and systems, ensuring interoperability of QKD technologies and systems;

Procurement of a testing and experimentation infrastructure facility

* provide a large-scale testing and experimentation infrastructure facility that is used for thorough testing of different QKD technologies and system aspects, including the integration of quantum and traditional cybersecurity systems in communication networks and their interoperability with QKD networks (in terms of suppliers, application level, and at the key management layer, possibly also supported by post-quantum algorithms). It will also be used for testing compliance with user and security requirements (including cyber penetration attempts). These activities will be used to prepare for the large-scale deployment of EuroQCI;
* develop a testbed to simulate the EuroQCI architecture based on the existing EuroQCI system studies and service portfolio with the flexibility to be enhanced according to future EuroQCI developments and needs;
* test the interface between the EuroQCI’s space and terrestrial components, including the validation and certification of systems and components, and test the technology in ground and lower-altitude experiments.

Expected outcomes and deliverables

* An fully operational QKD infrastructure facility covering EU needs in terms of testing, experimentation, validation and certification of QKD devices, technologies and systems. The facility will be interoperable and integrated with traditional communication networks, and open to service operators and cybersecurity business actors, enabling them to develop standardised and certified EU technology solutions.
* Fully interoperable quantum-based technologies between ground stations, (simulated or real) satellite systems and terrestrial systems.

Preparation for procurement (including coordination of national efforts)

|  |  |
| --- | --- |
| Type of action | CSA |
| Indicative Budget | [3 MEUR] |
| Indicative time of call opening  | Second call |
| Indicative duration of the action | 12 months |

Procurement of a testing and experimentation infrastructure facility

|  |  |
| --- | --- |
| Type of action | Procurement – open call  |
| Indicative Budget | [ 12 – 22 MEUR ] |
| Indicative year of procurement | 2022 |
| Indicative duration of the action | 48 months |

## Joint Preparedness, Situation awareness and Response

### EU cyber resilience and coordination; cyber ranges

Objective

To strengthen in the Union the capacity to monitor cyber-attacks and threats, to react jointly against large incidents, and to improve knowledge, skills and training. This objective will be pursued in particular through the implementation of the Blueprint and the future Joint Cyber Unit.

To create, interconnect and strengthen Cyber ranges at national and regional level, in view to share knowledge and intelligence between stakeholders in the Member States, better monitor cyber threats, and respond jointly to cyber-attacks.

Scope

Proposals addressing this objective should achieve one or more of the following actions:

* support capacity building, deployment and operation in preparedness and response to cybersecurity threats and attacks; this can include automated knowledge acquisition based on cyber threat intelligence (CTI) reports and incident responses, AI based tools to help discover threats and response strategies. As threats may span across multiple sectors and countries, actions may possibly include mutual assistance between Member States (before, during and after cyber crisis).
* provide Member States bodies with shared coordination and operational capabilities to anticipate and respond to cyber attacks, notably in the framework of the Blueprint/CyCLONe and the Joint Cyber Unit.
* improve common situational awareness, including through collaboration with and between Security Operation Centres.
* bridge cooperation between various cyber communities, e.g. civilian cyber resilience, law enforcement, defence.
* support the creation, operation, capacity increase and/or uptake of cyber ranges, as well as foster networking between them in view to develop cybersecurity skills and expertise in key technologies (e.g. 5G, IoT, Cloud, AI, ICS) as well as application sectors (e.g. health, energy, finance). This action will aim to exchange knowledge between cyber ranges and create common data repositories; support large-scale and cross-sector scenarios covering a wide range of adversaries and attack strategies, including for example cross centre serious gaming exercises; allow realistic traffic simulation that reflect network conditions; support structured training and cyber exercises to prepare cyber defenders at both public and private organisations to protect critical infrastructures, enterprises and communications networks; provide additional services to stakeholders such as structured test methodologies, vulnerability database and forensic tools; develop of automated content delivery options supporting specific job profiles.

Outcomes and deliverables

The expected outcomes will be a strong capacity in the Member States to react in a coordinated way to large scale incidents, as well as top level cyber ranges offering advanced skills, knowledge and testing platforms.

|  |  |
| --- | --- |
| Type of action | SME support grant (75% co-funding rate for SMEs and 50% for all the other beneficiaries) |
| Indicative Budget | [30 - 40 MEUR] |
| Indicative time of call opening  | Third call |
| Indicative duration of the action | 36 months |
| Indicative budget per grant (EU contribution) | 5 - 15 MEUR |

### Security Operation Centres (SOCs)

Objective

The objective will be to create, interconnect and strengthen national and regional Security Operation Centres (SOCs).

Scope

Proposals addressing this objective should improve cyber resilience with faster detection and response to cybersecurity incidents at EU level though one or more of the following actions:

* establishing regional or sectoral EU SOCs serving private and/or public organisations with real-time monitoring and analysis of network traffic to detect malicious activities and information sharing agreements with public authorities.
* leveraging state of the art Artificial Intelligence, Machine Learning techniques and computing power to improve the detection of malicious activities.
* dynamically learning about the changing threat landscape, sharing actionable cyber threat intelligence based on detected activities across broad regions, notifying affected entities enabling them to take swifter action.[[2]](#footnote-3)

Outcomes and deliverables

The expected outcome will be the deployment of world-class SOCs across the Union.

|  |  |
| --- | --- |
| Type of action | SME support grant (75% co-funding rate for SMEs and 50% for all the other beneficiaries) |
| Indicative Budget | [30 - 40 MEUR] |
| Indicative time of call opening  | Third call |
| Indicative duration of the action | 36 months |
| Indicative budget per grant (EU contribution) | 7 – 10 MEUR |

### Strengthening of GovSatCom network

Objective

A strategic overarching framework for secure and resilient communications considering satellite and terrestrial convergence for pan-European and global coverage, security, resilience, and mobility.

Scope

Build on, and integrate the GOVSATCOM[[3]](#footnote-4) project with cybersecurity activities. This would be achieved through the initial deployment of a multipurpose space-based satellites constellation, integrated with terrestrial networks, to be designed, produced, deployed and operated by MS legal entities, established and controlled by MS and/or nationals of MS;

This activity should build on the best available technologies, using them where they are the most effective, relying on a network of terrestrial and satellite secured channels using the most adapted technologies (including quantum and conventional). This includes using the strongest cryptography and cutting-edge threat detection capabilities as a cornerstone for cybersecurity.

Depending on the type of information handled and the security analysis, the infrastructure may need to undergo security accreditation to assure the delivery of secure services. The cybersecurity certification of IT products, services and processes involved in this regard will also play a key role.

Outcomes and deliverables

Deployment of key services capable to support security critical missions and exchange sensitive information in a hybrid threats environment and, to serve the needs for secured communication of various actors: civil protection agencies, those responsible for crisis management operations, operators of critical infrastructures and essential services, and other governmental and private sector users with similar security needs.

Prepare the relevant European stakeholders to counter the most harmful cyber attacks and risks (such as quantum-powered cyber threats) against secure communications.

|  |  |
| --- | --- |
| Type of action | Simple grant (50% co-funding rate) |
| Indicative Budget | [15 – 25] MEUR |
| Indicative time of call opening  | Fourth call |
| Indicative duration of the action | 36 months |
| Indicative budget per grant (EU contribution) | [15 -25 ] MEUR |

## Support to Implementation of relevant EU Legislation

### Deploying the network of national coordination centres with Member States

Objective

With the creation of the European Cybersecurity Industrial, Technology and Research Competence Centre, National Coordination Centres – working together through a network – will contribute to achieving the objectives of the regulation and foster the Cybersecurity Competence Community in each Member State to acquire the necessary capacity. National Coordination Centres will support cybersecurity capacity building at national and, where relevant, regional and local level. They shall aim at fostering cross-border cooperation and the preparation of joint actions as defined in the Cybersecurity Competence Centre and Network regulation.

Scope

The National Coordination Centre may provide the following services:

* acting as contact points at the national level for the Cybersecurity Competence Community to support the European Cybersecurity Competence Centre in achieving its objectives and missions, in particular by coordinating the Cybersecurity Competence Community;
* providing expertise and actively contributing to the strategic planning activities of the European Cybersecurity Competence Centre, taking into account relevant national and regional challenges for cybersecurity in different sectors;
* facilitating the participation of industry, research institutions and other actors at Member State level in cross-border projects;
* seeking to establish synergies with relevant activities at national and regional level, such as addressing cybersecurity in national policies on research, development and innovation in the area of, and in particular in those policies stated in the national cybersecurity strategies;
* implementing specific actions for which grants have been awarded by the European Cybersecurity Competence Centre, including through provision of financial support to third parties in line with Article 204 of Regulation (EU, Euratom) 2018/1046 under the conditions specified in the grant agreements concerned;
* promoting and disseminating the relevant outcomes of the work of the Network, the Cybersecurity Competence Community and Competence Centre at national or regional level;
* assessing requests by entities established in the same Member State as the National Coordination Centre for becoming part of the Cybersecurity Competence Community;
* advocating and promoting involvement by relevant entities in the activities arising from the Centre, Network and Community, and monitoring, as appropriate, the level of engagement with actions awarded for cybersecurity research, developments and deployments.

Proposals are expected to further specify the activities listed above and possibly other relevant activities. The funding can cover capacity building and the functioning of the National Coordination Centres for up to 3 years.

Outcomes and deliverables

Setup and operation of National Coordination Centres in Member States.

|  |  |
| --- | --- |
| Type of action | Simple grant (50% co-funding rate) |
| Indicative Budget | [ 45 – 55 MEUR ] |
| Indicative time of call opening  | First call |
| Indicative duration of the action | 36 months |
| Indicative budget per grant (EU contribution) | 2 MEUR |

### Structural support and community building for EU Cybersecurity

#### Cyber Security Community support

Objective

In line with the regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, one project is foreseen to support community building in cybersecurity research, technology, and industrial policy at EU level.

Scope

The community activities may include activities such as:

* Support to Cybersecurity start-ups and scale-ups, including with a view to attract investment fto the EU;
* Support to the development and growth of an internal market in Cybersecurity products and services in the EU. Where relevant, activities shall be in line with the JRC Cybersecurity taxonomy and Atlas[[4]](#footnote-5);
* Support the Competence Centre and the Network in fostering knowledge-sharing and networking between regional and local ecosystems specialised in cybersecurity;
* Support to education, training, and gender balance in cybersecurity, in line with relevant actions promoted by organisations, including ENISA;
* Awareness raising.

All activities are to be carried out in support and under the supervision of the Commission and the European Cybersecurity Competence Centre once established.

Activities shall build on, complement, and provide additional value to the activities previously carried out in the framework of the contractual Public Private Partnership on Cybersecurity[[5]](#footnote-6) and the four pilot projects on cybersecurity competence networks. [[6]](#footnote-7)

Activities shall be geographically balanced and inclusive towards members of the Community created by the Cybersecurity Competence Centre and Network regulation.

Outcomes and deliverables

Strengthened Cyber security Community to support the European Cybersecurity Industrial, Technology and Research Competence Centre.

|  |  |
| --- | --- |
| Type of action | Coordination and Support Action  |
| Indicative Budget | [3 MEUR] |
| Indicative time of call opening  | First call |
| Indicative duration of the action | 24 months |
| Indicative budget per grant (EU contribution) | 3 MEUR |

#### European Cybersecurity Atlas

Objective

To complement the community support, sharing cybersecurity expertise is essential to foster the cooperation and collaboration among EU cybersecurity institutions.

The definition of an EU cybersecurity taxonomy aims to align cybersecurity definitions and terminologies to support the categorization of existing institutions and expertise across Europe. This taxonomy is based on a comprehensive set of standards, regulations and best practices, and has been validated by different EU cybersecurity stakeholders, such as the European Cyber Security Organization (ECSO). Furthermore, it was enhanced based on the feedback provided by the 4 cybersecurity research and competence network pilot projects3 (CONCORDIA, ECHO, SPARTA and CyberSec4Europe), which embrace over 160 partners including companies, SMEs, universities and research institutes. A taxonomy and the atlas are necessary to organise and better understand knowledge.

Scope

The Atlas will collect information needed for the support, structuring and understanding of the community and its needs. Furthermore, it should address the needs of the cyber community. Examples of such needs to be addressed by the Atlas may include:

* Who in Europe is working on which cybersecurity domains, subdomains, sectors, technologies and use cases?
* Who are the key researchers?
* What is the funding allocated by EU and national initiatives for each knowledge domain and research context?
* How does the funding allocated translate to publications and patents?

This work will contribute to the deployment, the maintenance and the improvement of an online platform that will enable European cybersecurity actors to register and describe their expertise.[[7]](#footnote-8)

All activities are to be carried out in support and under the supervision of the Commission and the European Cybersecurity Competence Centre once established. The funding will support the maintenance, upgrade and operation of the Atlas for a duration of up to 3 years.

Outcomes and deliverables

Enhancement of a platform supporting the Community, mapping all the cyber security stakeholder in the European Union.

|  |  |
| --- | --- |
| Type of action | Administrative Agreement with JRC |
| Indicative Budget | [1 MEUR] |

### Supporting the NIS Directive implementation and national cyber security strategies

Objective

The action focuses on Member States and European capacity building and the enhancement of cross-border cooperation on cybersecurity at technical, operational and strategic levels. It is a continuation of work currently supported under the CEF Telecom programme. Proposals should contribute to achieving these objectives:

* Development of trust and confidence between Member States;
* Effective operational cooperation of organisations entrusted with EU or Member State’s national level Cybersecurity, in particular cooperation of CSIRTs (including in relation to the CSIRT Network) or cooperation of Operators of Essential Services including public authorities;
* Better security and notification processes and means for Operators of Essential Services and for digital service providers in the EU;
* Improved security of network and information systems in the EU;
* More alignment and harmonisation of Member States’ implementations of the NIS Directive.

Scope

The action will focus on the support of at least one of the following priorities:

* User-centred implementation, validation, piloting and deployment of technologies, tools and IT-based solutions for monitoring, preventing, detecting and handling cybersecurity incidents (including in the context of cross-border cybersecurity threats and cross sector context) in EU Member States;
* Collaboration, communication, knowledge exchange and training, including through the use of cyber ranges, of public and private organisations working on the implementation of the NIS Directive;
* Twinning schemes involving originator and adopter organisations from at least 2 different Member States to facilitate the deployment and uptake of technologies, tools, processes and methods for effective cross-border collaboration preventing, detecting and countering Cybersecurity incidents.

The support will target relevant Member State competent authorities, which play a central role in the implementation of the NIS Directive, Computer Security Incident Response Teams (CSIRTs), Security Operation Centres (SOC), operators of essential services (OES), digital service providers (DSP), industry stakeholders (including Information Sharing and Analysis Centres- ISACs), and any other actors within the scope of the NIS Directive. In essence, the NIS Directive applies to OES (subject to national transposing legislation) in the following sectors considered as “critical”:

* Energy (electricity, oil, gas);
* Transport (air, rail, water, maritime);
* Banking and Financial market infrastructures;
* Health;
* Drinking water supply and distribution;
* Digital Infrastructure (IXPs, DNS service providers, TLD name registries);
* Online marketplace;
* Online search engine;
* Cloud computing service.

However, Member States can define additional critical sectors, including public administrations, and identify operators for their countries.

On top of that, the NIS Directive applies to providers of the following types of digital services (DSP):

* Online marketplace;
* Online search engine;
* Cloud computing service.

The action may support amongst other the continuation of the kind of cybersecurity activities funded through the CEF Telecom programme, building where relevant on the results from the CEF projects. Furthermore, synergies with actions from other relevant topics, e.g. 3.2 Joint preparedness, situational awareness and response, should be explored.

Support will be provided amongst other for the on boarding to the CEF Cybersecurity Core Service Platforms of public and private organisations working on the implementation of the NIS directive and are potential users of the CEF Cybersecurity Core Service Platforms.

Outcomes and deliverables

Proposals are expected to deliver on at least two of the following results:

* enable the Member States to limit the damage of cyber incidents, including economic, social, environmental, or political damage, while reducing the overall costs of cybersecurity for individual Member States and for the EU as a whole.
* improve compliance with the NIS Directive, higher levels of situational awareness and crisis response in Member States.
* contribute to enhanced cooperation, preparedness and cybersecurity resilience of the EU.

The action will result also in the interconnection of the centres in charge of guarantee the cyber security of the operator of important service.

|  |  |
| --- | --- |
| Type of action | SME support grant (75% co-funding rate for SMEs and 50% for all the other beneficiaries) |
| Indicative Budget | [30 – 40 MEUR] |
| Indicative time of call opening  | Fourth call |
| Indicative duration of the action | 36 months |
| Indicative budget per grant (EU contribution) | 1 - 5 MEUR |

### Testing and certification capabilities

Objective

The objective of this topic is to increase and facilitate security testing and certification of connected ICT systems. This aims improve the capabilities and cooperation of cybersecurity certification stakeholders in line with the objectives of Regulation (EU) 2019/881 (“Cybersecurity Act”).

Scope

Funding will be available for activities aiming to:

1. Support capacity building for national cybersecurity certification authorities, conformity assessment bodies and accreditation bodies; e.g. for the acquisition of certification testbeds; exchange of best practices and staff trainings; deploy innovative evaluation methods for specific ICT products or components; support standardisation actions (e.g. creation of protection profiles or adoption/improvement of standards used in certification schemes). This shall take into account activities in National Coordination Centres where relevant.
2. Support SMEs to test and certify ICT products, ICT services or ICT process they sell. The priority will be given to sectors affected by the COVID-19 crisis;
3. Provide support for SME users of ICT equipment to audit their infrastructures in term of cyber security resilience;
4. Support standardisation actions (e.g. creation of protection profiles or adoption/improvement of standards used in certification schemes), taking into account activities by European and international standardisation organisations as appropriate.

Where relevant, support will focus on certification schemes under the Cybersecurity Act, while it could also be available for technical areas not yet covered by schemes under the Cybersecurity Act.

 Outcomes and deliverables

The funding is expected to:

* Improve the cybersecurity testing capabilities in all Member States;
* Support SMEs to audit their infrastructure in view of improving their cybersecurity protection.

Type of action

It is planned to use Simple grant (50% co-funding) for the capacity building, standardisation and piloting call and SME support grants (75% co-funding for SME and 50% for all other beneficiaries) for the other actions.
Possibility for National Coordination Centres to apply with a view to allocating financial support to third parties (“cascading funding”). *The use of lump sums is being considered*.

|  |  |
| --- | --- |
| Type of action | Grants |
| Indicative Budget | [15 – 20 MEUR] |
| Indicative time of call opening  | Third call |
| Indicative duration of the action | 36 months |
| Indicative budget per grant (EU contribution) | 1 to 2 MEUR |

## Support to market players and skills

### Securing 5G and other strategic digital infrastructures and technologies

Objective

The digital transformation of the economy requires the highest protection of key digital infrastructures. The objective will be to support relevant entities in Member States’, such as regulators of electronic communications or security agencies, in the implementation of their national cyber security strategies and legislation, in line with policy European on cybersecurity protection of key digital infrastructures, notably 5G security policy. This will support capacity building for relevant national authorities regarding e.g. exchange of best practices; staff trainings; deployment of innovative evaluation methods; support standardisation actions; procurement of specialised services (e.g. audit and technical assessments). This shall take into account activities in National Coordination Centres where relevant.

Scope

* Support to 5G security, notably to contribute to the goals and measures of the Recommendations on 5G security of the 5G security “toolbox”, as well as follow-up initiatives in that context;
* Implement security measures in other strategic interconnected infrastructures such as IoT or cloud.

Activities shall take into account relevant outcomes of projects funded under Horizon 2020 and complement support from other EU or national programs.

Outcomes and deliverables

* Trusted and secure key digital infrastructures, notably 5G.
* Increased technical and organizational resilience in interconnected infrastructures.

|  |  |
| --- | --- |
| Type of action | Simple grant (50% co-funding rate) |
| Indicative Budget | [15 – 25 MEUR] |
| Indicative time of call opening  | Third call |
| Indicative duration of the action | 12 – 36 months |
| Indicative budget per grant (EU contribution) | 1 to 2 MEUR |

### Uptake of innovative cybersecurity solutions and skills

Objective

To support the market uptake and dissemination of innovative cybersecurity solutions (notably from SMEs, as well as results from public-funded research in the EU), skills, and auditing of cyber preparedness.

Scope

The focus will be on improving cybersecurity capabilities across the EU, notably for SMEs and public organisations, through both supply and demand support measures. This may include skills development and awareness raising measures (where relevant in line with activities promoted by ENISA), or market place platforms supporting interaction between suppliers and adopters of cybersecurity solutions and training.

The types of tools and skills covered must include at least one of the following:

* Cyber protection services;
* Auditing of cyber resilience of equipment and services;
* Security testing tools including static-analysis code scanning tools;
* Cyber investigation tools, tracing the origins of cybersecurity threats;
* Incident responding tools that fit into general operational security strategies;
* Innovative cyber training and skills development to fit the needs of the market;
* Support to Coordinated Vulnerability Disclosure, in line with national policies where relevant.
* Funding and support for projects which improve and/or audit open source software, with regard to cyber security;
* Support for hackathons and conferences, and for engaging with relevant stakeholders including software development communities.
* Support to cybersecurity entrepreneurship programmes, incubators, or accelerators.
* Support to awareness, prevention, education, training, and gender balance in cybersecurity.

Outcomes and deliverables

The funding will amongst other:

* Support the adoption of market-ready innovative cyber security solutions, including solutions developed in the framework of EU-supported research and innovation projects;
* Provide up to date tools and service to organisations (in particular SMEs) to protect themselves against cyber threats;
* Improve the security of open source solutions (establishment of bug bounty programmes);

|  |  |
| --- | --- |
| Type of action | SME support grant (75% co-funding rate for SMEs and 50% for all the other beneficiaries) |
| Indicative Budget | [25 – 35 MEUR] |
| Indicative time of call opening  | Second and fourth call |
| Indicative duration of the action | Up to 36 months |
| Indicative budget per grant (EU contribution) | [2 to 5 MEUR] |

### Support to the health sector

Objective

The action will support cybersecurity resilience in the healthcare domain, which has been put under particular stress over the recent years, especially further to the COVID-19 crisis, in view of limiting the damage of safety-critical cyber incidents which have affected hospitals and health services providers.

Scope

The focus will be on improving the cybersecurity capabilities of health institutions across the EU, including cybersecurity services and products, skills and training, awareness raising, and exchange of information, and others. Cross-border solutions will be promoted where appropriate.

The types of tools intervention covered must include at least one of the following:

* Implementation of objectives and requirements under the NIS Directive in relation to the health sector;
* Support for SMEs, and in particular the uptake of software tools, methods, best practices, and training material dedicated to cybersecurity and data protection in hospitals and care environments;
* eID and data management solutions contributing to data security in the health sector;
* Cybersecurity education, awareness and skills in hospitals and care environments.

Outcomes and deliverables

The funding will:

* Support the adoption of market-ready innovative cyber security solutions, including solutions deloped in the framework of EU-supported research and innovation projects.
* Provide up to date tools to health organisations (in particular SMEs) to protect themselves against cyber threats.
* Contribute to data sharing in view to improve security collectively.

|  |  |
| --- | --- |
| Type of action | SME support grant (75% co-funding rate for SMEs and 50% for all the other beneficiaries) |
| Indicative Budget | [5 – 15 MEUR] |
| Indicative time of call opening  | Third call |
| Indicative duration of the action | Up to 24 months |
| Indicative budget per grant (EU contribution) | 5 MEUR |

# Programme Support Actions [SECTION IS WORK IN PROGRESS]

Programme support actions aimed at maximising the impact of the EU intervention. Horizontal actions will cover costs including preparation, evaluation, monitoring and studies. An amount of funding will be set aside to cover awareness and dissemination as it is crucial to effectively communicate about the value and benefits of the Digital Europe Programme.

|  |  |
| --- | --- |
| Category of expenditure | Indicative budget |
| Studies |  |
| Communication and events |  |
| Proposals evaluation and project reviews |  |
| Other support measures |  |
| Events |  |
| Total |  |

# Implementation [SECTION IS WORK IN PROGRESS]

## Main implementation measures and EU financial contribution

The different nature and specificities of the actions in section above, require distinctive implementation measures. Each of these will therefore be achieved through various implementation modes as follow.

Proposers are strongly encouraged to follow green public procurement principles and take account of life cycle costs[[8]](#footnote-9).

## Procurement

Procurement actions will be carried out in compliance with the applicable EU public procurement rules. The procedures will be implemented either through direct calls for tenders or by using existing framework contracts.

## Grants – Calls for proposals

### Evaluation process

The evaluation of proposals will be based on the principles of transparency and equal treatment. It will be carried out by the Commission services and one Executive Agency with the assistance of independent experts. The award and selection criteria will be applied to each submitted proposal. The three sets of criteria are described in detail in Annex 2 of this Work Programme.

Only proposals meeting the requirements of the eligibility criteria in the call text will be evaluated further.

Each of the eligible proposals will be evaluated against the award criteria, while each individual applicant must demonstrate their financial and operational capacity to carry out the proposed action or work programme.

Proposals responding to a specific topic as defined in the chapters of this Work Programme will be evaluated both individually and comparatively. The comparative assessment of proposals will cover all proposals responding to the same topic.

Proposals that achieve a score greater than or equal to the threshold will be ranked within the objective. These rankings will determine the order of priority for funding. Following evaluation of award criteria, the Commission establishes a Selection Decision taking into account the scores and ranking of the proposals, the programme priorities and the available budget. In case it is specified in the call text that only one proposal per Member State will be selected, only the proposal with the higher ranking will be selected in case more proposals from a same Member State have passed the threshold. The Selection Decision will include proposals to be invited to prepare the Grant Agreement.

The coordinators of all submitted proposals will be informed in writing about the outcome of the evaluation for their proposal(s).

### Selection of independent experts for evaluation and reviews

The Commission and the Executive Agency will select independent experts to assist with the evaluation of proposals and with the review of project results as well as for other purposes where specific expertise might be required for implementation of the Programme. Experts are invited to apply using the mechanisms and tools provided for in the H2020 Framework Programme[[9]](#footnote-10) and a list of experts appropriate to the requirements of the Digital Europe Programme and each addressed area will be established. Experts will be selected from this list on the basis of their ability to perform the tasks assigned to them, taking into account the thematic requirements of the topic, and with consideration of geographical and gender balance.

### Indicative implementation calendar

The indicative calendar for the implementation of the Digital Europe calls for proposals in 2021 and 2022 is shown in the table below.

More information about these calls will be available on: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home.

| Date | Milestone |
| --- | --- |
| Q1 2021 | WP published, 1st call opens |
| Q2 2021 |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60090> [↑](#footnote-ref-2)
2. Activities should give due consideration to fundamental values associated with privacy and data protection with implementation of Security Incident and Event Monitoring by a wider variety of stakeholders arising from judgements including Breyer from the EU Court of Justice. [↑](#footnote-ref-3)
3. The High Level Civil Military User Needs for Governmental Satellite Communications (GOVSATCOM) funded under the European Defence Fund [↑](#footnote-ref-4)
4. See following topic

[Insert link once atlas is launched.] [↑](#footnote-ref-5)
5. Contractual arrangement setting up a public-private partnership in the area of cybersecurity industrial, research and innovation between the EU and ECSO. [↑](#footnote-ref-6)
6. CONCORDIA, ECHO, SPARTA and CyberSec4Europe are the four winning pilot projects of the 2018 Horizon 2020 cybersecurity call "establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap". [↑](#footnote-ref-7)
7. Including for instance institution contact information, cybersecurity knowledge, researcher profiles, projects and collaborations, courses and training offered. [↑](#footnote-ref-8)
8. <http://ec.europa.eu/environment/gpp/index_en.htm> [↑](#footnote-ref-9)
9. http://ec.europa.eu/research/participants/portal/desktop/en/experts/index.html [↑](#footnote-ref-10)