NCC-DE

GERMANY CYBERSECURITY COORDINATION CENTRE

Topic Booklet: Cybersecurity in the European funding programs “Horizon Europe” and “Digital Europe”

kiimoshi / stock.adobe.com

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

The project funded under Grant Agreement No. 101126787 is supported by the European Cybersecurity Competence Centre

Co-funded by the European Union

Table of content

1 Executive Summary

This topic booklet describes all call topics from 2024 of the 2023-2024 work programs on the overarching topic of cybersecurity, including the submission deadlines and budgets of the individual calls from the "Horizon Europe" and "Digital Europe" funding programs. Furthermore, an overview of the two funding programs "Horizon Europe" and "Digital Europe" is given by presenting the structure, term and budget. The topic booklet is rounded off with a summary of the funding forms and participation rules of the two funding programs.

2 Cybersecurity in “Horizon Europe“

2.1 Structure of “Horizon Europe”

“Horizon Europe” is structured in three pillars. The “Excellent Science” pillar contains programs for open-topic (individual) funding. The topic-specific pillar “Global Challenges and European Industrial Competitiveness” addresses a total of six areas (“clusters”). “Innovative Europe” with a focus on innovation and market uptake forms the third pillar. The overarching program area “Widening participation and strengthening the European Research Area” is aimed, among other things, at promoting the participation of Member States that have been less active in the field of research and innovation to date.

Cybersecurity is a sub-aspect of the entire program and is primarily represented in Cluster 3 “Civil Security for Society”.

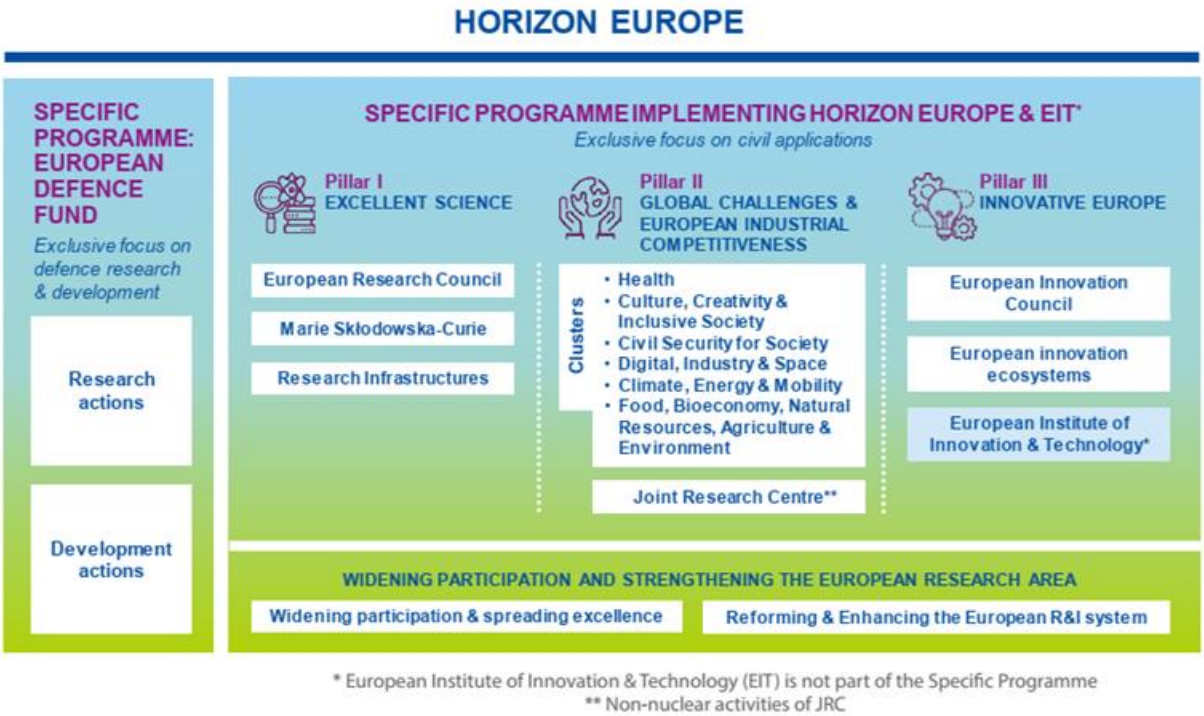

Figure 1: Structural organization of “Horizon Europe” *(1)*

2.2 Term and budget

The program runs for 7 years (01.01.2021 to 31.12.2027). The planned total budget amounts to around 95.5 billion euros and is distributed according to the diagram in Figure 2. The total budget earmarked for Cluster 3 amounts to EUR 1.6 billion for the seven-year duration of “Horizon Europe”.

For the second work program 2023-2024 in Cluster 3 “Civil Security for Society”, a total of EUR 332.89 million of this budget is earmarked, of which EUR 119.1 million is for the implementation of measures in the area of cybersecurity.

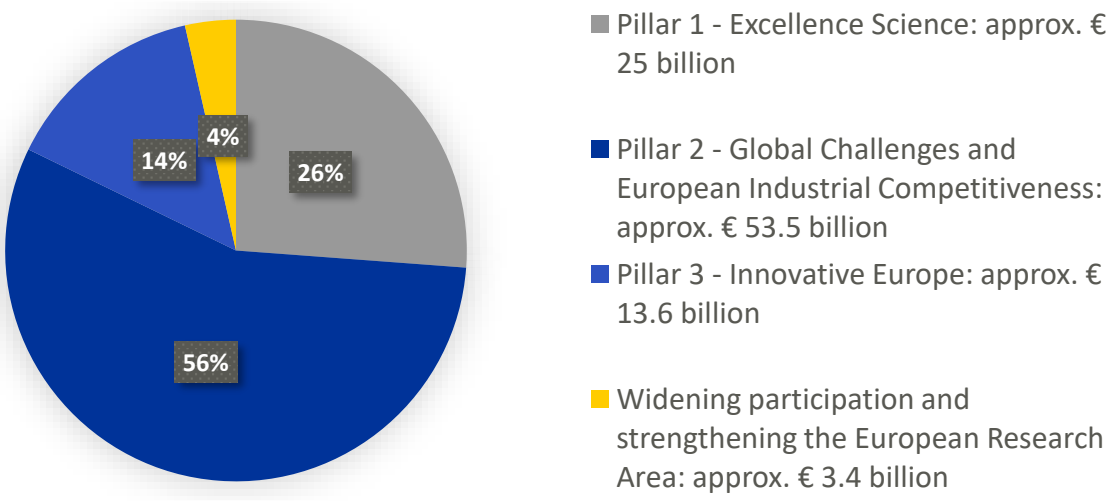

Figure 2: Budget allocation over the entire duration of the “Horizon Europe” program *(6)*

2.3 Cybersecurity topics in 2024 in the 2023-2024 work program of Cluster 3 “Civil Security for Society” of “Horizon Europe”

Table 1 lists all Cybersecurity topics in 2024 in the 2023-2024 work program of Cluster 3 “Civil Security for Society” of ”Horizon Europe” (2):

Section / Topic	Type of action	Budget (€ million)	Opening	Deadline
CS01 – Systems Security and Security Lifetime Management, Secure Platforms, Digital Infrastructures				
HORIZON-CL3-2024-CS-01-01: Approaches and tools for security in software and hardware development and assessment	IA	37.0	27.06.2024	20.11.2024
CS02 – Cryptography				
HORIZON-CL3-2024-CS-01-02: Post-quantum cryptography transition	RIA	23.4	27.06.2024	20.11.2024

All information is subject to change. Official information can always be found in the current work program or on the "Funding & Tenders" portal of the European Commission.

2.4 “Horizon Europe” funding forms and participation rules

The framework program for research and innovation ("Horizon Europe") provides for various forms of funding and defines the rules for participation. All forms of funding are subject to the participation rules of "Horizon Europe" (3). Special regulations regarding these participation rules may be defined in the calls for proposals. Detailed information on the various forms of funding can be found in the work program (2).

2.5 Overview of funding forms, funding rates and minimum number of participants

Table 2 provides an overview of funding forms, funding rates and minimum numbers of participants in Horizon Europe:

Type of action	Funding rate (Eligible costs)	Minimum number of participants**
Research and Innovation Actions (RIA)	100%*	3 partners from 3 different EU Member States or associated countries
Innovation Actions (IA)	60% or 70%* (100%* for non-profit organizations)	3 partners from 3 different EU Member States or associated countries
Coordination and Support Actions (CSA)	100%*	1 partner from 1 EU Member State or associated country
ERA-NET Cofund	Up to 33%*	3 partners from 3 different EU Member States or associated countries
Pre-commercial Procurement (PCP) Cofund Actions	Up to 90%*	3 partners from 3 different EU Member States or associated countries
Public Procurement of Innovative Solutions (PPI) Cofund Actions	Up to 35%*	3 partners from 3 different EU Member States or associated countries

All information is subject to change. Official information can always be found in the current work program or on the "Funding & Tenders" portal of the European Commission.

* Deviating funding rates are possible as an exception. Topics with a reduced funding rate are marked "[RF]" in the topic overview table; the reduced funding rate here is 60% in each case.

** With a minimum number of three participants, at least one participant must come from an EU Member State. Legal entities from third countries (i.e. the whole world) can also participate.

Within a funding measure, all partners receive the same funding rates for all activities (except for "Innovation Action"). In addition to the subsidy for direct costs, indirect costs are also reimbursed. The indirect costs are calculated as a flat-rate of 25% of the eligible direct costs (reduced e.g. through subcontracting).

3 Cybersecurity in “Digital Europe”

3.1 Structure of “Digital Europe”

The "Digital Europe" program aims to strengthen the European Union's critical digital capacities by focusing on the key areas of artificial intelligence, cybersecurity, advanced data processing and data infrastructures and their use for critical sectors such as energy, environment, manufacturing, agriculture and health.

Existing capacities are to be utilized and further expanded. A particular focus will be placed on the development of synergies between digital infrastructure stakeholders in Europe.

In the key area of cybersecurity under "Digital Europe", the capacities and capabilities of the European Union are to be expanded and strengthened in order to protect EU citizens, companies and organizations, expand digital sovereignty in Europe and improve the security of critical infrastructures and digital products and services.

3.2 Term and budget

The “Digital Europe” program will run for seven years (2021-2027). The total budget of the “Digital Europe” program amounts to approx. 7.68 billion euros for seven years, with a total of 1.7 billion euros earmarked for the key area of cybersecurity (see Figure 3).

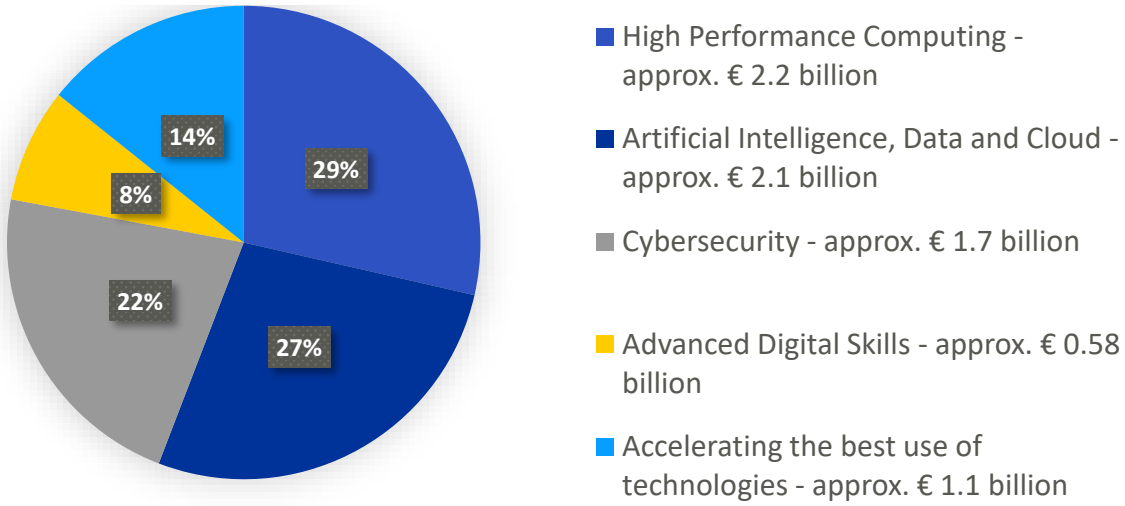

Figure 3: Budget allocation over the entire duration of the “Digital Europe” program (7)

3.3 Overarching objectives of the key area of cybersecurity

The overarching objectives of the key area of cybersecurity can be summarized as follows:

- Strengthening the coordination of Member States' cybersecurity tools and data infrastructures
- Strengthening European capabilities in the areas of optical communication and cybersecurity through quantum communication infrastructures
- Support the broad deployment of cybersecurity capabilities across the economy
- Strengthening advanced skills and capabilities in Member States and the private sector to achieve a uniformly high level of security for network and information systems

3.4 Cybersecurity topics in 2024 in the 2023-2024 Work Programs of “Digital Europe”

Table 3 lists all Cybersecurity topics in 2024 in the 2023-2024 Amended Main Work Programs of “Digital Europe”:

Topic	Budget (€ million)	Opening	Deadline
Incident Response Support and Preparedness for Key Sectors (Contribution agreement; Article 12(5)*) / Implementation by ENISA	20,0	2024	2024
Incident Response Support (Contribution agreement; Article 12(5)*) / Implementation by ENISA	15,0	2024	2024
Cybersecurity Skills Academy (Simple grant) / Implementation by Executive Agency HaDEA	10,0	21.11.2023	21.03.2024

All information is subject to change. Official information can always be found in the current work program or on the "Funding & Tenders" portal of the European Commission.

Table 4 lists all Cybersecurity topics in 2024 in the 2023-2024 Amended Cybersecurity Work Programs of “Digital Europe”:

Topic	Budget (€ million)	Opening	Deadline
Security Operation Centres			
National SOCs (Joint procurement and Simple grant; Article 12(5)*)	20,8	04.07.2024	27.03.2025
Enlarging existing or Launching New Cross-Border SOC Platforms (Joint procurement and Simple grant; Article 12(5)*)	22,0	04.07.2024	27.03.2025
Joint Acquisition of Infrastructure, Tools and Services with the Cross-Border SOC Platforms (Joint procurement; Article 12(5)*)	14,2	2024	2024
Novel applications of AI and Other Enabling Technologies for Security Operation Centres (Simple grant; Article 12(5)*)	30,0	16.01.2024	26.03.2024
Strengthening the SOC ecosystem (Coordination and support action grant; Article 12(5)*)	2,0	04.07.2024	27.03.2025
Development and Deployment of Advanced Key Technologies			
Development and Deployment of Advanced Key Technologies (SME support action grant; Article 12(5)*)	35,0	04.07.2024	27.03.2025

Support for the Implementation of the proposed Cyber Resilience Act			
Strengthen Cybersecurity capacities of European SMEs in line with CRA requirements and obligations (Grant for Support to Third Parties; Article 12(5)*)	22,0	16.01.2024	26.03.2024
Tools for compliance with CRA requirements and obligations (SME support action grant; Article 12(5)*)	8,0	16.01.2024	26.03.2024
Post-Quantum Cryptography			
Deployment of Post Quantum Cryptography in systems in industrial sectors (Simple grant; Article 12(5)*)	22,25	16.01.2024	26.03.2024
Standardisation and awareness of the European transition to post-quantum cryptography (Coordination and support action grant; Article 12(5)*)	1,0	16.01.2024	26.03.2024
Roadmap for the transition of European public administrations to a post-quantum cryptography era (Coordination and support action grant; Article 12(5)*)	0,75	16.01.2024	26.03.2024
Cybersecurity Emergency Mechanism			
Preparedness Support and Mutual Assistance, targeting larger industrial operations and installations (Grant for Financial Support; Article 12(5)*)	35,0	04.07.2024	27.03.2025
Support to EU Legislation			
Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024) (Simple grant; Article 12(5)*)	20,0	04.07.2024	27.03.2025
National Coordination Centres			
Deploying the Network of National Coordination Centres with Member States (Simple grant; Article 12(5)*)	65,0	29.02.2024	29.05.2024, 28.11.2024
Programme Support Actions	6,0		

All information is subject to change. Official information can always be found in the current work program or on the "Funding & Tenders" portal of the European Commission.

3.5 “Digital Europe” funding forms and participation rules

The “Digital Europe” program provides for various forms of funding and defines the rules for participation. All forms of funding are subject to the participation rules of “Digital Europe” (4). Special regulations regarding these participation rules may be defined in the calls for proposals. For detailed information on the various forms of funding, please refer to the work programs.

Table 5 shows an overview of funding forms and funding rates (5):

Type of action	Funding rate (Eligible costs)	Description
Simple grants	**50%** of total eligible costs for all beneficiaries.	The Simple Grants are used by a large variety of topics and can cover most activities. The consortium will mostly use personnel costs to implement action tasks, activities with third parties (subcontracting, financial support, purchase) are possible but should be limited.
SME Support actions	SMEs **75%,** others **50%** of eligible costs	The type of action primarily consists of activities directly aiming at supporting SMEs involved in building up and the deployment of digital capacities. This type of action can also be used if an SME needs to be in the consortium and make investments to access digital capacities.
Coordination and support actions (CSA)	**100%** of the eligible costs	Small grants with the primary goal to promote cooperation and/or provide support to EU policies. Activities can include coordination between different actors for accompanying measures such as standardisation, dissemination, awareness-raising and communication, networking, coordination or support services, policy dialogues and mutual learning exercises and studies, including design studies for new infrastructure. CSA may also include complementary activities of strategic planning, networking and coordination between programmes in different countries.
Grants for Procurement	**50%** of total eligible costs for all beneficiaries	Grants where most of the costs consist of buying goods or services and/or subcontracting tasks. Contrary to the grants for procurement of advanced capacities (PAC grants) (see below), for these there are no specific procurement rules (i.e. usual rules for purchase apply), nor is there a limit to “contracting authorities/entities”. Personnel costs should be limited in this type of action; they are used to manage the grant, coordinate between the beneficiaries and prepare the procurement.
Grants for Procurement of Advanced Capacities (PAC)	**50 %** of total eligible costs	Grants awarded only to beneficiaries that are “contracting authorities or contracting entities” as defined in the EU public procurement Directives (Directives 2014/24/EU, 2014/25/EU and 2009/81/EC) aiming at buying innovative digital goods and services (i.e. novel technologies on the way to commercialisation but not yet broadly available).

Grant for Financial Support	**100%** of eligible costs for the consortium, co-financing of **50%** of total eligible costs by the supported third party.	Grants with a particular focus on providing financial support to third parties. The majority of the grant will be distributed via financial support to third parties with special provisions in the grant agreement, maximum amounts to third parties, multiple pre-financing and reporting obligations. Annex 5 of the model grant agreements foresees specific rules for this type of action regarding conflict of interest, the principles of transparency, non-discrimination and sound financial management as well as the selection procedure and criteria. In order to assure the co-financing obligation in the programme, the support to third parties should only cover 50% of third-party costs.
Framework Partnership Agreement (FPA) and Specific Grant Agreement (SGA)	FPA: no funding SGA: **50%** of total eligible costs	FPAs: An FPA establishes a long-term cooperation mechanism between the granting authority and the beneficiaries of grants. The FPA specifies the common objectives (action plan), the procedure for awarding specific grants and the rights and obligations of each party under the specific agreements. The specific grants are awarded via identified beneficiary actions (with or without competition). SGAs: The SGAs are linked to an FPA and implement the action plan or part of the action plan. They are awarded via an invitation to submit a proposal (identified beneficiary action). The coordinator of the FPA has to be the coordinator of each SGA signed under the FPA and will always take to role of interlocutor with the granting authority. All the other partners of the FPA can participate in any SGA. There is no limit to the number of SGAs signed under one FPA.
Lump Sum Grant	**50 %** of total eligible costs	Lump Sum Grants reimburse a general lump sum for the entire project and the consortium as a whole. The lump sum is fixed ex-ante (at the latest at grant signature). The granting authority defines a methodology for calculating the amount of the lump sum. There is an overall amount, i.e., the lump sum will cover the beneficiaries’ direct and indirect eligible costs. The beneficiaries do not need to report actual costs, they just need to claim the lump sum once the work is done. If the action is not properly implemented only part of the lump sum will be paid.

All information is subject to change. Official information can always be found in the current work program or on the "Funding & Tenders" portal of the European Commission

3.5.1 *Restrictions based on Articles 12(5) and 12(6)

For duly justified security reasons, the participation of legal entities controlled by a third country (including those established in an eligible country but controlled by a third country or a legal entity from a third country) may be excluded from certain calls for proposals.

The assessment of foreign control will be dealt with at the eligibility stage of the evaluation of applications. To this end, participants will be asked to complete a self-assessment questionnaire to determine their control status when submitting the proposal. They will also be asked to provide supporting documents to enable the Commission to determine that the entities are not controlled by a third country. Entities classified as controlled by a third country may only participate in subjects to which Article 12(6) applies, provided that they meet certain conditions. These participants will be required to provide guarantees approved by the eligible country in which they are established. The validity of these guarantees will be subsequently verified by the European Commission.

Further information on this topic, such as conditions for foreign-controlled companies, can be found in Appendix 3 of the “Digital Europe Amended Work Programme 2023-2024” *(see* (5)*).*

List of Figures

List of Tables

References

1. **European Commission, Directorate-General for Research and Innovation, Publications Office, 2021, https://data.europa.eu/doi/10.2777/05.** *Horizon Europe, the EU research and innovation programme (2021-27): for a green, healthy, digital and inclusive Europe.* Publications Office of the European Union : s.n., 2021. https://data.europa.eu/doi/10.2777/052084.

2. **European Commission.** *Horizon Europe Work programme (2023-24) - Cluster 3.* Brussels : s.n., 31.03.2023. https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/horizon-europe-work-programmes_en.

3. **European Parliament, Council of the European Union.** *Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations.* [http://data.europa.eu/eli/reg/2021/695/oj] 28.04.2021.

4. **European Parliament, Council of the European Union**. *Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (Text with EEA relevance).* [http://data.europa.eu/eli/reg/2021/694/oj] 29.04.2021.

5. **European Commission.** *Digital Europe Amended Work Programme 2023-2024.* Brussels : s.n., 14.12.2023. https://digital-strategy.ec.europa.eu/en/activities/work-programmes-digital.

6. **European Commission, Directorate-General for Research and Innovation.** *Horizon Europe, budget – Horizon Europe - the most ambitious EU research & innovation programme ever.* Publications Office of the European Union : s.n., 2021. https://data.europa.eu/doi/10.2777/202859.

7. **European Commission.** *Digital Europe Programme: €7.5 billion of funding for 2021-2027.* 2020. https://digital-strategy.ec.europa.eu/en/library/digital-europe-programme-eu75-billion-funding-2021-2027.

Copyright and Disclaimer

The German National Coordination Center for Cybersecurity in Industry, Technology and Research is a joint virtual institution of the Federal Ministry of the Interior and Community, the Federal Ministry of Education and Research, the Federal Ministry of Economic Affairs and Climate Action and the Federal Ministry of Defence.

The operation of the NCC-DE is assigned to

- the Federal Office for Information Security (BSI) as head of the NCC-DE,
- the German Aerospace Center (DLR Projektträger) and
- the Research Institute CODE (RI Code) of the Bundeswehr University Munich.

This topic booklet has been edited by the German Aerospace Center (DLR Projektträger) as part of the NCC-DE.

www.nkcs.bund.de/en

Publication date: 09/01/2025

Co-funded by the European Union

DLR Projektträger

Bundesamt für Sicherheit in der Informationstechnik

FI CODE Forschungsinstitut Cyber Defence Universität der Bundeswehr München