CAMPUS CYBER

Catalogue de financement

01. APPELS A PROJET EUROPEENS TOUT GUICHET.

AAPS Juin – Décembre 2022

Cluster	Topic	Title	Deadline
HORIZON EUROPE 2 / CLUSTER 3 SECURITY	HORIZON-CL3-2022-CS-01-01	Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures	16/11/2022
	HORIZON-CL3-2022-CS-01-02	Trustworthy methodologies, tools and data security "by design" for dynamic testing of potentially vulnerable, insecure hardware and software components	16/11/2022
	HORIZON-CL3-2022-CS-01-03	Transition towards Quantum-Resistant Cryptography	16/11/2022
	HORIZON-CL3-2022-CS-01-04	Development and validation of processes and tools used for agile certification of ICT products, ICT services and ICT processes	16/11/2022
HORIZON EUROPE PILLAR 2 / CLUSTER 5 CLIMATE, ENERGY AND MOBILITY	HORIZON-CL5-2022-D2-01-03	Furthering the development of a materials acceleration platform for sustainable batteries (combining AI, big data, autonomous synthesis robotics, high throughput testing) (Batteries Partnership)	06/09/22
	HORIZON-CL5-2022-D3-02-01	Digital solutions for defining synergies in international renewable energy value chains	27/10/22
	HORIZON-CL5-2022-D3-03-04	Integrated wind farm control	10/01/23
	HORIZON-CL5-2022-D3-03-08	Development of digital solutions for existing hydropower operation and maintenance	10/01/23
EUROPEAN DEFENSE FUND	EDF-2022-DA-CYBER-CSIR	Cybersecurity and systems for improved resilience	24/11/22
	EDF-2022-RA-CYBER-CSACE	Adapting cyber situational awareness for evolving computing environments	24/11/22
	EDF-2022-DA-CYBER-CIWT	Cyber and information warfare toolbox	24/11/22
INTERNAL SECURITY FUND	ISF-20226TF1-AG-CYBER	Call for proposals on Cybercrime and Digital Investigations	15/09/22
DG FOR COMMUNICATIONS NETWORK, CONTENT & TECHNOLOGY	CNECT/2022/OP/0033	Cybersecurity Community Support	16/09/22
INTERREGIONAL INNOVATION INVESTMENTS INSTRUMENT (I3)	I3-2022-INV1	Innovation investments Strand 1 - DIGIT	18/10/22

02. CLUSTER 3 - SECURITY.

Destination 4 – Increased Cybersecurity (CS)

Topic	Title	Type	Budget per project	# of projects
HORIZON-CL3-2022-CS-01-01	Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures	IA	4-6	4
HORIZON-CL3-2022-CS-01-02	Trustworthy methodologies, tools and data security "by design" for dynamic testing of potentially vulnerable, insecure hardware and software components	RIA	3-5	4
HORIZON-CL3-2022-CS-01-03	Transition towards Quantum-Resistant cryptography	IA	3.5 - 6	2
HORIZON-CL3-2022-CS-01-04	Development and validation of processes and tools used for agile certification of ICT products, ICT services and ICT processes	IA	3-5	4

03. CLUSTER 3 - SECURITY.

Destination 4 – Cybersecurity

Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures.

+ **BUDGET :** 4 à 6 M€ par projet

+ **DEADLINE :** 16 Nov. 2022

+ **TYPE OF ACTION :** Innovation Action

+ **APPLIANCE :** Consortia > 3 legal entitites from 3 member States

+ **OBJECTIVE :**

- Improved **disruption preparedness** and **resilience of digital infrastructure** in Europe
- Improved **capacity building** in digital infrastructure security including **organisational and operational capabilities**
- **Robust evidence** used in cybersecurity decisions and tools
- Better **prediction of cybersecurity threats** and related risks
- Improved **response capabilities** […] including **holistic incident reporting** and enabling **coordinated cyber-incident response**

+ **PROFILES :**

- **SMEs** (encouraged) **/ Industry / RTOs**
- **Communications or Network** providers
- **Software / hardware providers** e.g. 5G, IoT, medical devices, SCADA systems
- **Service providers** e.g. cloud-based ICT services
- **Technology providers** e.g. logging, categorisation, and aggregation of data, information extraction, incident analysis, network traffic analysis, machine learning / artificial intelligence to penetrate testing methods
- **End user partners** e.g. to validate intrusion detection & incident monitoring

04. CLUSTER 3 - SECURITY.
Destination 4 – Cybersecurity

Trustworthy methodologies, tools and data security “by design” for dynamic testing of potentially vulnerable, insecure hardware and software components

+ **BUDGET :** 3 à 5 M€ par projet

+ **DEADLINE :** 16 Nov. 2022

+ **TYPE OF ACTION :** Reasearch and Innovation Action

+ **APPLIANCE :** Consortia > 3 legal entitites from 3 member States

+ **OBJECTIVE :**

- Effective **access control to system components** and management of **trustworthy updates**
- Modelling of **security and privacy properties** and frameworks for validating and integration on the **testing process**
- Integrated process for testing, formal verification, validation and consideration of **certification aspects**
- **Tools** providing assurance that **third-party and open source components** are free from vulnerabilities, weaknesses and/or malware
- Data security “by design” e.g. via **secure crypto building blocks**
- Instrumentation and **secured communication with system components** for dynamic testing
- **Methods and environments** for secured **coding by-design** and by-default and secure hardware and software construction
- Effective **audit procedures** for cybersecurity testing
- **Methods or procedures** to make **supply chains** secure

+ **PROFILES :**

- **SMEs** (encouraged) **/ Industry / RTOs**
- **System providers:** Operating systems, Application Programming Interfaces (APIs)
- **Hardware & software providers:** device manufacturers, backend clouds and virtualisation, service functionality software, virtualisation environments, accountability tools for audit

05. CLUSTER 3 - SECURITY.

Destination 4 – Cybersecurity

Transition towards Quantum-Resistant Cryptography

+ **BUDGET :** 3.5 à 6 M€ par projet

+ **DEADLINE :** 16 Nov. 2022

+ **TYPE OF ACTION :** Reasearch and Innovation Action

+ **APPLIANCE :** Consortia > 3 legal entitites from 3 member States

+ **OBJECTIVE :**

- Measuring, assessing and standardizing/certifying **future-proof cryptography**
- Addressing gaps between the **theoretical possibilities** offered by **quantum resistant cryptography** and its **practical implementations**
- **Quantum resistant cryptographic primitives and protocols** encompassed in security solutions
- **Solutions and methods** that could be used to migrate from current cryptography towards **future-proof cryptography**
- **Preparedness for secure information exchange and processing** in the advent of **large-scale quantum attacks**

+ **PROFILES :**

- **SMEs** (encouraged) / **Industry / RTOs**
- **System providers:** Operating systems, Application Programming Interfaces (APIs)
- **Hardware & software providers:** device manufacturers, backend clouds and virtualisation, service functionality software, virtualisation environments, accountability tools for audit

06. CLUSTER 3 - SECURITY.

Destination 4 – Cybersecurity

Development and validation of processes and tools used for agile certification of ICT products, ICT services and ICT processes

+ **BUDGET :** 3 à 5 M€ par projet

+ **DEADLINE :** 16 Nov. 2022

+ **TYPE OF ACTION :** Innovation Action

+ **APPLIANCE :** Consortia > 3 legal entitites from 3 member States

+ **OBJECTIVE :**

- Availability of **applicable tools and procedures** for partial and continuous assessment and lean re-certification of ICT products, ICT services and ICT processes;
- Reduction of time and efforts spent for **(re-) certification**
- Improved **stakeholder collaboration** on cybersecurity certification information
- Efficient (re-)use of information and evidence relevant to certification and in support of **multi-scheme (re-)use;**
- **Integration of certification on the whole system** modelling, verification, testing and verification process
- Increased **comparability of assurance statements** arising from certification schemes and the standards used therein; avoidance of multi-certification;
- Advancing **test and simulation facilities**, including incident and threat analysis;
- Increased **Digital Twin capabilities** for continuous assessment and integration of new solutions.

+ **PROFILES :**

- **SMEs** (encouraged) **/ Industry / RTOs**
- **Manufacturers and end users**
- **ICT providers:** products, services, processes
- **Simulation and testing facilities**

Topic	Title	Date	Budget per project	# of projects
HORIZON-CL5-2022-D2-01-03	Furthering the development of a materials acceleration platform for sustainable batteries (combining AI, big data, a utonomous synthesis robotics, high throughput testing) (Batteries Partnership)	06/09/22	20	1
HORIZON-CL5-2022-D3-02-01	Digital solutions for defining synergies in international renewable energy value chains	27/10/22	3	3
HORIZON-CL5-2022-D3-03-04	Integrated wind farm control	10/01/22	6	3
HORIZON-CL5-2022-D3-03-08	Development of digital solutions for existing hydropower operation and maintenance	10/01/23	3-4.5	3

08. CLUSTER 5 – CLIMATE, ENERGY AND MOBILITY.

Destination 2 – Cross-sectorial solutions for the climate transition

Furthering the development of a materials acceleration platform for sustainable batteries (combining AI, big data, autonomous synthesis robotics, high throughput testing)

+ **BUDGET :** 20 M€ par projet

+ **DEADLINE :** 06 Sept. 2022

+ **TYPE OF ACTION :** Research and inovation Action

+ **APPLIANCE :** Consortia > 3 legal entitites from 3 member States

+ **OBJECTIVE :**

- Develop **new tools and methods** for significantly accelerating the development and optimisation of **battery materials and interfaces**
- Demonstrate a **fully autonomous battery-MAP** capable of integrating **computational modelling, materials synthesis & characterisation** of both Li-ion & beyond Li-ion chemistries.
- Scale-bridging, multi-scale battery interface models capable **of integrating data from embedded sensors** in the **discovery and prediction process**
- Community wide state-of-the-art collaborative environment to **access data and utilise automated workflows for integrated simulations and experiments** on heterogeneous sites,
- Demonstrate a **robotic system** that is capable of material synthesis
- Deploy predictive **hybrid physics & data-driven models** for the spatio-temporal evolution of battery interfaces & demonstrate **inverse design** of a battery material/interface.

+ **LINK TO CYBERSECURITY :**

- **SMEs** (encouraged) / **Industry / RTOs**
- **Manufacturers and end users**
- **ICT providers:** products, services, processes
- **Simulation and testing facilities**

09. CLUSTER 5 – CLIMATE, ENERGY AND MOBILITY.

Destination 3 –Sustainable, secure and competitive energy supply

Digital solutions for defining synergies in international renewable energy value chains.

+ **BUDGET :** 3 M€ par projet

+ **DEADLINE :** 10 Oct. 2022

+ **TYPE OF ACTION :** Research and inovation Action

+ **APPLIANCE :** Consortia > 3 legal entitites from 3 member States

+ **OBJECTIVE :**

- Advance the European and global scientific basis, European leadership and global role in the area of **renewable energy** and **renewable fuels** and **related energy value chains** while creating evidence for policy making by developing **novel digital solutions**.
- Provide **digital breakthrough solutions** for promoting the increase of the **global renewable energy share.**
- Reinforce the European scientific basis through **international collaboration** while increasing the potential to **export European renewable energy technologies** and ensuring political priorities in the context of **sustainable global energy value chains**.
- **Improve reliability of system components**, advanced and automated functions for **data analysis, diagnosis and fault detection**, **forecasting & model-predictive control frameworks, ancillary services** for the stability of the network; **maintenance** planning and/or reporting.

+ **LINK TO CYBERSECURITY :**

- Focus on smart and **cyber-secure** energy grids and **optimisation the interaction** between producers, consumers, networks, infrastructures and vectors.

10. CLUSTER 5 – CLIMATE, ENERGY AND MOBILITY.

Destination 3 –Sustainable, secure and competitive energy supply

Integrated wind farm control

+ **BUDGET :** 6 M€ par projet

+ **DEADLINE :** 10 Oct. 2022

+ **TYPE OF ACTION :** Research and inovation Action

+ **APPLIANCE :** Consortia > 3 legal entitites from 3 member States

+ **OBJECTIVE :**

- Development of **open source data-driven tools to decrease energy costs** on operation, while increasing total wind farm output, and a parallel evaluation of **operational risks** arising from the chosen solution
- Development of **digital and physical tools**, as well as interoperable **frameworks and controls**, for enhanced data collection, analysis, and operation aimed at an **improved performance at farm level.**
- Allow operators to make **better informed decisions** on farm-wide system optimisation, lifetime extension, decommissioning and/or recycling of components.
- Contribute to **LCOE reduction** in line with the **SET Plan targets**

+ **LINK TO CYBERSECURITY :**

- **High levels of cybersecurity** expected from digital innovation for wind farm control.

11. CLUSTER 5 – CLIMATE, ENERGY AND MOBILITY.

Destination 3 –Sustainable, secure and competitive energy supply

Development of digital solutions for existing hydropower operation and maintenance

+ **BUDGET :** 3 à 4.5 M€ par projet

+ **DEADLINE :** 10 Janv. 2023

+ **TYPE OF ACTION :** Research and inovation Action

+ **APPLIANCE :** Consortia > 3 legal entitites from 3 member States

+ **OBJECTIVE :**

- Advance the European scientific basis, technology base, technology leadership in the area of **hydropower in the context of digital transition and energy markets** while creating evidence for policy making;
- Increase the **technology competitiveness** of the existing hydropower fleet in changing European power markets by increasing **hydropower flexibility** and decision-making in modern power markets;
- Facilitate **market penetration of renewables** and getting closer to the European Green Deal and climate and energy targets for 2030 by **increasing the flexibility, sustainability and predictability of existing hydropower;**
- Improve **environmental and socio-economic sustainability** of the existing hydropower fleet.

+ **LINK TO CYBERSECURITY :**

- Focus on smart and **cyber-secure energy grids** and optimisation the interaction between producers, consumers, networks, infrastructures and vectors.

12. CLUSTER 5 – CLIMATE, ENERGY AND MOBILITY.

Destination 5 – Climate, Energy and mobility

Programme	Call topic	Call title	Deadline	Budget
European Defense Fund: Development Actions	EDF-2022-DA-CYBER-CSIR	Cybersecurity and systems for improved resilience	24/11/22	27
European Defense Fund: Research Actions	EDF-2022-RA-CYBER-CSACE	Adapting cyber situational awareness for evolving computing environments	24/11/22	10
European Defense Fund: Development Actions	EDF-2022-DA-CYBER-CIWT	Cyber and information warfare toolbox	15/09/22	33
Internal Security Fund: ISF-PJG-ISF Project Grants	ISF-20226TF1-AG-CYBER	Call for proposals on Cybercrime and Digital Investigations	16/09/22	8
DG for Communications Networks, Content & Technology: Call for Tender	CNECT/2022/OP/0033	Cybersecurity Community Support	16/09/22	30
Interregional Innovation Investments Instrument (I3): I3-PJB I3 Project Grants	I3-2022-INV1	Innovation investments Strand 1 - DIGIT	18/10/22	36

13. EUROPEAN DEFENSE FUND

Cybersecurity and systems for improved resilience

+ **BUDGET FOR CALL TOPIC :** 27 M€

+ **DEADLINE :** 24 Nov. 2022

+ **TYPE OF ACTIVITIES :** Study Design (+up/down)

+ **APPLIANCE :** Consortia > 3 legal entitites from 3 member States

+ **OBJECTIVE :** (…) **military operations** increasingly rely on computers and networked communications (…) as the dependencies on digital technologies rapidly grows, so does the **potential threats and vulnerabilities.** (…) Furthermore, the **Internet of Things (IoT)** has become widely integrated into a variety of sectors and industries, offering "readymade" solutions (…) Many IoT solutions are designed primarily for functionality, **without being properly secured.** As a result, attacks on IoT environments have gained momentum due to the increased attack surface. Therefore, the **need for cybersecurity services, including ensuring an appropriate level of control and prevention** (…) must be addressed.

14. EUROPEAN DEFENSE FUND

Adapting cyber situational awareness for evolving computing environments

+ **BUDGET :** 27 M€ for call topic

+ **DEADLINE :** 24 Nov. 2022

+ **TYPE OF ACTIVITIES :** Study Design (+upstream)

+ **APPLIANCE :** Consortia > 3 legal entitites from 3 member States

+ **OBJECTIVE :** (…) New or improved **solutions, technologies and applications for enhanced cyber situational awareness (CSA)** are essential to counter these [malicious] threats. To address evolving and more complicated activities in cyberspace (…) **decision makers** and **Security Operation Centre (SOC) operators** need the most **updated CSA related to cyber threats, in real time, gathering internal and external cyber information** (…) in order to be able to **make informed decisions and adequately respond to incidents.**

15. EUROPEAN DEFENSE FUND

Cyber and information warfare toolbox

+ **BUDGET :** 33 M€ for call topic
+ **DEADLINE :** 24 Nov. 2022
+ **TYPE OF ACTIVITIES :** Design, prototyping (+up/down)
+ **APPLIANCE :** Consortia > 3 legal entitites from 3 member States

+ **OBJECTIVE :** The continuously and rapidly **increasing flow of information** in the information environment, facilitated through **cyber capabilities**, is a well-established fact. We are witnessing an **increasing number of malicious actions** targeting the information environment. In the more and more **digitalized battlespace**, the **Cyber and Information domains become decisive to anticipate and manage conflicts in the full spectrum of threat activities from sub-threshold interference to open warfare.**

16. INTERNAL SECURITY FUND
Cybercrime

Cybercrime and Digital investigations

+ **BUDGET :** 8 M€ for call topic

+ **DEADLINE :** 15 Sept. 2022

+ **APPLIANCE :** Consortia > 2 legal entitites from 3 member States

+ **OBJECTIVE :**

- Developing **operational capacity and expertise** of law enforcement and judicial authorities and supporting cross-border cooperation in the field of Cybercrime
- Development of **investigative and forensics tools** to address the challenges posed by the use of encryption by criminals and its impact on criminal investigations and supporting law enforcement authorities' engagement in the area of Internet governance;
- Contributing to the **implementation of EU law**
- Fostering **cross-border cooperation** between law enforcement/ judicial authorities and private entities.

+ **SCOPE :**

- Enhancing the **operational capacity of law enforcement** and/or judicial authorities to **investigate cyber-attacks and cyber enabled crime**
- Enhancing the operational capacity of law enforcement and/or judicial authorities to address the challenges posed **by 5G and application level communication** in the area of lawful interception, with a focus on relevant **standardisation activities.**
- Enhancing the operational capacity of law enforcement and/or judicial authorities to address the challenges posed by the **use of encryption by criminals** and its impact on criminal investigations
- Enhancing the operational capacity of law enforcement and/or judicial authorities to **cooperate across borders**
- Enhancing the cooperation between private entities and/or authorities in the area of **cybersecurity and law enforcement** and/or judicial authorities
- Providing public authorities with an accurate picture of the **real (i.e. included unreported)** extent of cybercrime.

17. CALLS FOR TENDER

DG for communications Networks, Content and technology

Cybersecurity Community Support

+ **BUDGET :** 3 M€ par projet

+ **DEADLINE :** 16 Sept. 2022

+ **PROCEDURE TYPE :** Open procedure

+ **APPLIANCE :** All natural and legal persons coming within the scope of the Treaties

+ **DESCRIPTION :** In line with the regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) and the Network of National Coordination Centres (NCCs), **one project is foreseen to support community building and capacity building in cybersecurity research, technology, and industrial policy at EU level**. The goal of the project is to support the ECCC and the European Cybersecurity Competence Community. This action will support the activities necessary to **develop, promote, coordinate and organize** the work of the Cybersecurity Competence Community at European Level, within the scope and operations of the ECCC and NCC Network. This tender notice complements the information provided in the chapter 'Actions for Cybersecurity and trust – Support to implementation of EU legislation – Cybersecurity Community Support' of the Digital Europe programme, WP 2021-2022.

+ **MAIN ACTIVITIES :**

- Analyse the European Cybersecurity Competence Community
- Stimulate collaboration within the European Cybersecurity Competence Community
- Link the European Cybersecurity Competence Community with the ECCC and the NCCs network

18. INTERREGIONAL INNOVATION INVESTMENTS INSTRUMENT (I3)

I3-PJB Project Grants

Cybersecurity Community Support

+ **BUDGET :** 4 à 10 M€ par projet

+ **DEADLINE :** 18 Oct. 2022

+ **APPLIANCE :** Consortia > 5 legal entities from 3 member States

+ **OBJECTIVES :** Digital technologies present an enormous growth potential for Europe. According to the Europe fit for the digital age strategy, this call for proposals **targets investments in businesses and administrations**. In order to unlock digital growth potential and deploy **innovative solutions** (both for businesses and citizens), to improve the **accessibility and the efficiency** of services and bridge the **persisting digital divide**, the present call under this topic will support interregional investments projects in the following areas:

- Digital economy and innovation
- Digitalisation of the public administration
- Digitalisation of healthcare

+ **PRIORITIES :**

a) **Digital economy and innovation:** Companies reinforcing **EU cybersecurity value chain** and protecting from hacking, ransomware and identity theft;

b) **Digitalisation of the public administration:** New or significantly upgraded services for **e-government**, including the take-up of Europe wide interoperable services which improve the **efficiency of services** delivered by public administrations to citizens, companies and other public bodies by using information and communication **technologies such as artificial intelligence and cybersecurity**;

c) **Digitalisation of healthcare:** Innovative investments in security of health data across borders (**including cybersecurity**)

CAMPUS CYBER