Bundesministerium
für Bildung
und Forschung

NKS Digitale und Industrielle Technologien
Nationale Kontaktstelle zum
EU-Programm Horizont Europa

Chancen der Cyber-Sicherheitsforschung im Rahmen der EU-Förderprogramme „Horizont Europa“ und „Digitales Europa“

CODE-Jahrestagung 2022

Stefan Hillesheim
Dr. Marvin Richter
DLR-PT
Nationale Kontaktstelle - Digitale und Industrielle Technologien

Bundesministerium
für Bildung
und Forschung

NKS Digitale und Industrielle Technologien
Nationale Kontaktstelle zum
EU-Programm Horizont Europa

NKS DIT - Nationale Kontaktstelle Digitale und Industrielle Technologien

DLR Projektträger

ptj Projektträger Jülich
Forschungszentrum Jülich

Unteraufträge

VDI Technologiezentrum

PTKA
Projektträger Karlsruhe
im Karlsruher Institut für Technologie

Information und Beratung zum **Cluster 4** „Digital, Industry and Space“ in „Horizont Europa“ und zu den
„Cybersecurity“-F&I-Maßnahmen im **Cluster 3** „Civil Security for Society“ in „Horizont Europa“ und im Programm „Digitales Europa“

www.nks-dit.de

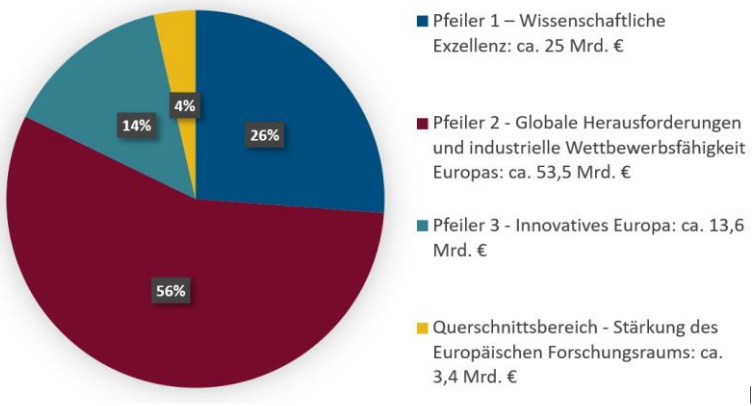
Agenda

EU-Rahmenprogramme

- Horizont Europa
  - Cybersicherheit in Horizont Europa
- Digitales Europa
  - Cybersicherheit in Digitales Europa

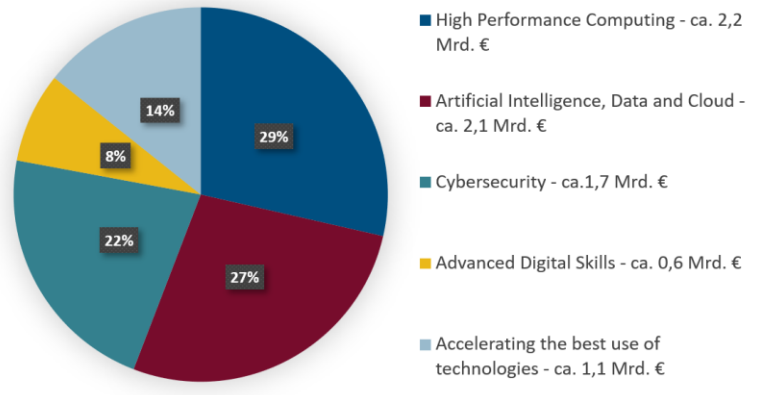
„Horizont Europa“ und „Digitales Europa“

Horizont Europa



95,5 Mrd. €

Digitales Europa



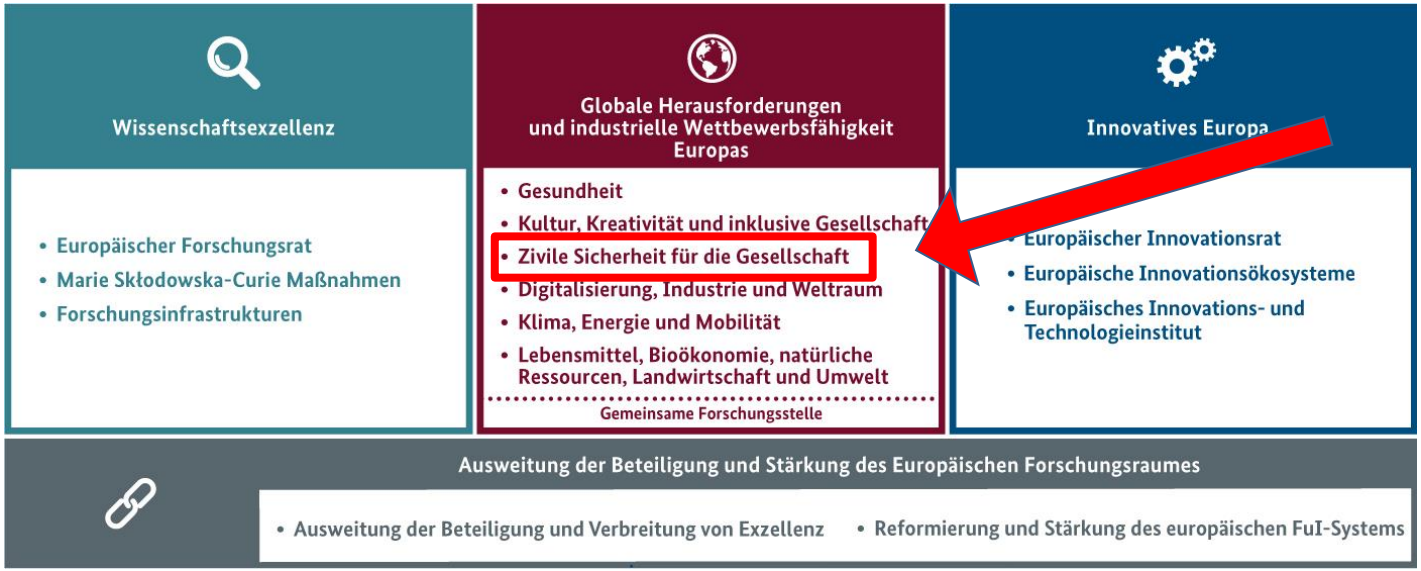
7,7 Mrd. €

Cybersecurity-Themen in „Horizont Europa“ und „Digitales Europa“

“HORIZONT EUROPA” Cluster 3 / Arbeitsprogramm 2021-2022	“DIGITALES EUROPA” Arbeitsprogramm 2021-2022
• Sichere und resiliente digitale Infrastrukturen	• Sichere Quantenkommunikationsinfrastruktur
• Hardware-, Software- und Lieferkettensicherheit	• Maßnahmen für Cybersicherheit und Vertrauen: – Europäisches „Cyber-Schutzschild“ – Unterstützung bei der Umsetzung von EU-Rechtsvorschriften
• Cybersicherheit und disruptive Technologien	
• Zertifizierung	
• Menschenzentrierte Sicherheit, Datenschutz und Ethik	

➢ Übersicht zu Cybersicherheit Ausschreibungen in „Horizont Europa“ und „Digitales Europa“2021-2022

Struktur von „Horizont Europa“



Cybersicherheits-Themen

Quelle: DLR Projektträger

Horizon Europa - Arbeitsprogramm 2021/2022 Cluster 3

Destinations	
Destination 1	Better protect the EU and its citizens against Crime and Terrorism
Destination 2	Effective management of EU external borders
Destination 3	Resilient infrastructure
Destination 4	Increased Cybersecurity
Destination 5	A Disaster-Resilient Society for Europe
Destination 6	Strengthened Security Research and Innovation

Horizont Europa - Destination 4: Increased Cybersecurity 2021-2022

- **Basis und Komplementarität**
  - Forschung und Innovation sollen auf den Ergebnissen von „Horizont 2020“ aufbauen
  - Komplementär zu den Cybersicherheitsmaßnahmen des Rahmenprogramms „Digitales Europa“ (DEP) und dem Arbeitsprogrammteil „Digital, Industrie und Raumfahrt“ in „Horizont Europa“ (HEU)
  - ausgerichtet an den künftigen Zielen des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und dem Netz nationaler Koordinierungszentren (ECCC)

Horizont Europa - Destination 4: Increased Cybersecurity 2021-2022

Themen unter “Gestärkte Cybersicherheit”

- Sichere und resiliente digitale Infrastrukturen
- Hardware-, Software- und Lieferkettensicherheit
- Cybersicherheit und disruptive Technologien
- Intelligente und quantifizierbare Sicherheit und Zertifizierung
- Menschenzentrierte Sicherheit, Datenschutz und Ethik

Horizont Europa - Destination 4: Increased Cybersecurity 2021-2022

Topic	Budget (Mio. Euro)	Open	Deadline
Secure and resilient digital infrastructures and interconnected systems			
HORIZON-CL3-2021-CS-01-01: Dynamic business continuity and recovery methodologies based on models and prediction for multi-level Cybersecurity (RIA)	21,5	30.06.2021	21.10.2021
HORIZON-CL3-2022-CS-01-01: Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures (IA)	**21,0**	**30.06.2022**	**16.11.2022**
Hardware, software and supply chain security			
HORIZON-CL3-2021-CS-01-02: Improved security in open-source and open specification hardware for connected devices (RIA)	18,0	30.06.2021	21.10.2021
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)	**17,3**	**30.06.2022**	**16.11.2022**
Cybersecurity and disruptive technologies			
HORIZON-CL3-2021-CS-01-03: AI for cybersecurity reinforcement (RIA)	11,0	30.06.2021	21.10.2021
HORIZON-CL3-2022-CS-01-03: Transition towards Quantum-Resistant Cryptography (IA)	**11,0**	**30.06.2022**	**16.11.2022**
Human-centric security, privacy and ethics			
HORIZON-CL3-2021-CS-01-04: Scalable privacy-preserving technologies for crossborder federated computation in Europe involving personal data (RIA)	17,0	30.06.2021	21.10.2021
Smart and quantifiable security assurance and certification shared across Europe			
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	**18,0**	**30.06.2022**	**16.11.2022**

Horizont Europa - Destination 4: Increased Cybersecurity 2021-2022

Themen unter “Gestärkte Cybersicherheit”

- Sichere und resiliente digitale Infrastrukturen
- Hardware-, Software- und Lieferkettensicherheit
- Cybersicherheit und disruptive Technologien
- Intelligente und quantifizierbare Sicherheit und Zertifizierung
- Menschenzentrierte Sicherheit, Datenschutz und Ethik

HORIZON-CL3-2022-CS-01-01: Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures

Expected Outcomes*

- gesteigerter Schutz vor Störungen und größere Widerstandsfähigkeit digitaler Infrastruktur
- Aufbau von Kapazitäten für die Sicherheit digitaler Infrastrukturen, einschließlich organisatorischer und operativer Fähigkeiten
- verlässliche Nachweise für Cybersicherheitsentscheidungen und –instrumente
- bessere Vorhersage von Bedrohungen und damit verbundenen Risiken
- verbesserte Reaktionsfähigkeit

Scope*

- Anwendungsszenarien z.B.: Kommunikationssysteme und -netze und ihre Komponenten, z. B. 5G-Netze, Internet der Dinge (IoT), medizinische Geräte, Überwachungs-, Kontroll- und Datenerfassungssysteme (SCADA) und ihre Dienste
- “state of the art technologies” zur Informationsextraktion und Analyse von Cybersicherheitsvorfällen
- Entwicklung von Prototypen zur Überwachung und Analyse von Cybersicherheitsvorfällen
- …

Financial support to third parties (FSTP)
Projekte können „Dritten“ finanzielle Unterstützung gewähren.

Instrument	Förderung je Projekt	Topic-budget	TRL Start/Ziel	Deadline
IA	4 – 6 Mio. €	21 Mio. €	-/7	16.11.2022

* Auszug aus dem Arbeitsprogramm 21-22

Horizont Europa - Destination 4: Increased Cybersecurity 2021-2022

Themen unter “Gestärkte Cybersicherheit”

- Sichere und resiliente digitale Infrastrukturen
- Hardware-, Software- und Lieferkettensicherheit
- Cybersicherheit und disruptive Technologien
- Intelligente und quantifizierbare Sicherheit und Zertifizierung
- Menschenzentrierte Sicherheit, Datenschutz und Ethik

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

Expected Outcomes

- wirksame Zugangskontrolle zu Systemkomponenten und Management
- Modellierung von Sicherheits- und Privatsphären-Eigenschaften und Frameworks zur Validierung und Integration in den Testprozess
- Werkzeuge, die sicherstellen, dass Open-Source-Komponenten und Komponenten von Drittanbietern frei sind von Sicherheitslücken und/oder Malware
- Datensicherheit "by design"
- Methoden und Umgebungen für sichere Kodierung „by-design" und „by default"
- ...

Scope:

- vertrauenswürdige Methoden und Werkzeuge zur Analyse und Überprüfung sowie dynamisches testen von potenziell anfälligen, unsicheren Hardware- und Softwarekomponenten
- F&I zur Entwicklung hybrider, agiler und hochsicherer Tools um Bewertungsprozesse zu automatisieren, isolierte Virtualisierungsumgebungen die eine sichere Inspektion und Orchestrierung von Anwendungen ermöglichen in heterogenen Hardware- und Software-Architekturen
- KPIs, Metriken, Verfahren und Werkzeuge für eine dynamische Zertifizierung
- ...

Beteiligung von KMU
wird ausdrücklich empfohlen

Instrument	Förderung je Projekt	Topic-budget	TRL Start/Ziel	Deadline
RIA	3 – 5 Mio. €	17,3 Mio. €	-/4	16.11.2022

*Auszug aus dem Arbeitsprogramm 21-22

Horizont Europa - Destination 4: Increased Cybersecurity 2021-2022

Themen unter “Gestärkte Cybersicherheit”

- Sichere und resiliente digitale Infrastrukturen
- Hardware-, Software- und Lieferkettensicherheit
- Cybersicherheit und disruptive Technologien
- Intelligente und quantifizierbare Sicherheit und Zertifizierung
- Menschenzentrierte Sicherheit, Datenschutz und Ethik

HORIZON-CL3-2022-CS-01-03: Transition towards Quantum-Resistant Cryptography

Expected Outcomes*

- Messung, Bewertung und Standardisierung/Zertifizierung zukunftssicherer Kryptografie
- Behebung der Lücken zwischen den theoretischen Möglichkeiten und ihrer praktischen Anwendung
- Lösungen und Methoden, für den Übergang von der derzeitigen Kryptographie zur zukunftssichere Kryptographie
- Vorbereitung auf einen sicheren Informationsaustausch und eine sichere Informationsverarbeitung im Hinblick auf groß angelegte Quantenangriffe
- ...

Scope*

- Entwicklung von kryptografischen Systeme, die gegen Angriffe mit Quanten- und/oder klassischen Computern sicher sind
- innovative Wege für den Entwurf, den Aufbau und die Bereitstellung der neuen quantenresistenten Infrastrukturen
- Implementierung von quantenresistenten Algorithmen in Software sowie spezifischer Hardware
- ...

Financial support to third parties (FSTP)
Projekte können „Dritten" finanzielle Unterstützung gewähren.
Teilnahmeregel: Teilnahme ist beschränkt auf Rechtspersonen mit Sitz in den Mitgliedstaaten und assoziierten Ländern.

Instrument	Förderung je Projekt	Topic-budget	TRL Start/Ziel	Deadline
IA	3,5 – 6 Mio. €	11 Mio. €	-/6	16.11.2022

* Auszug aus dem Arbeitsprogramm 21-22

Horizont Europa - Destination 4: Increased Cybersecurity 2021-2022

Themen unter “Gestärkte Cybersicherheit”

- Sichere und resiliente digitale Infrastrukturen
- Hardware-, Software- und Lieferkettensicherheit
- Cybersicherheit und disruptive Technologien
- Intelligente und quantifizierbare Sicherheit und Zertifizierung
- Menschenzentrierte Sicherheit, Datenschutz und Ethik

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

Expected Outcomes*

- Verfügbarkeit von anwendbaren Instrumenten und Verfahren für die partielle und kontinuierliche Bewertung und Re-Zertifizierung
- Reduzierung des Zeit- und Arbeitsaufwands für die (erneute) Zertifizierung
- Weiterentwicklung von Test- und Simulationseinrichtungen
- Verbesserte „Digital Twin"-Fähigkeiten
- ...

Scope*

- Harmonisierung, Bündelung und Verbreitung von Zertifizierungsverfahren für moderne IKT-Produkte, -Dienstleistungen und Prozesse
- Verbesserung der Zertifizierungsprozesse und der Instrumente
- Entwicklung von Konzepten für dynamische, kooperative Schwachstellentests in Echtzeit und für den Informationsaustausch
- ...

Instrument	Förderung je Projekt	Topic-budget	TRL Start/Ziel	Deadline
IA	3 – 5 Mio. €	18 Mio. €	-/7	16.11.2022

* Auszug aus dem Arbeitsprogramm 21-22

Horizont Europa - Destination 4: Increased Cybersecurity 2023-2024

Ausblick auf die Themenblöcke 2023-2024:*

- Systemsicherheit und „Security Lifetime Management“, sichere Plattformen, digitale Infrastrukturen
- Datenschutz- und Identitätstechnologien
- Sichere disruptive Technologien
- Kryptographie

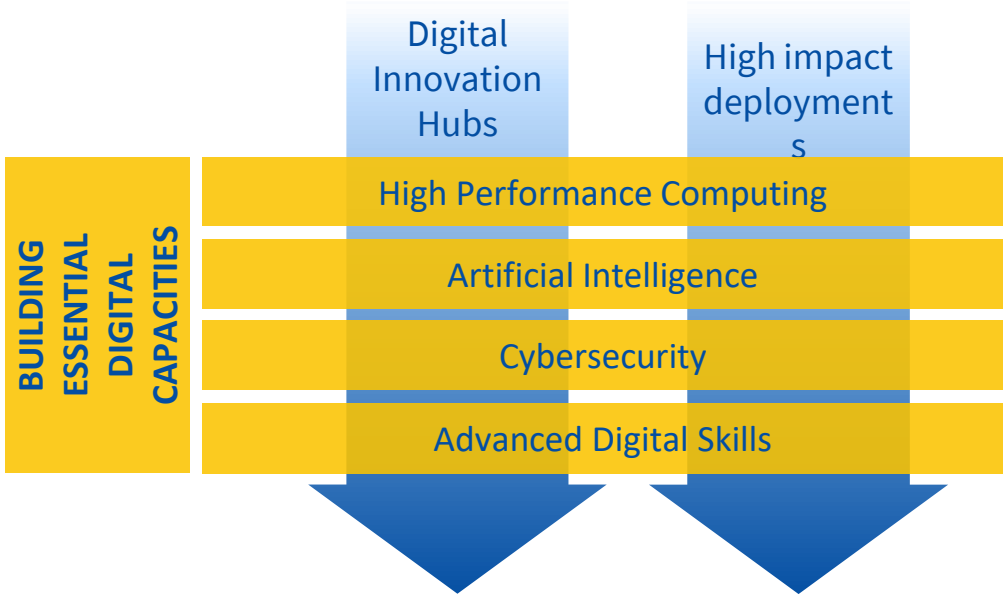
*Arbeitsprogramm 2023-2024 ist noch nicht angenommen! Änderungen sind nicht ausgeschlossen!!!

Agenda

EU-Rahmenprogramme

- Horizont Europa
  - Cybersicherheit in Horizont Europa
- **Digitales Europa**
  - Cybersicherheit in Digitales Europa

Struktur von „Digitales Europa“



Themen von „Digitales Europa“

High-performance computing

- Procure exascale machines
- Upgrade existing supercomputers,
- Quantum computing
- Widen the access to and use of supercomputing

Artificial intelligence

- Data4EU : common Data Spaces, cloud, platforms and infrastructure
- Large Testing and Experimentation Facilities in five areas
- Scale up the European AI platform to access tested AI technologies

Cybersecurity

- Deploy competence centres network
- Cybersecurity shield, quantum communication infrastructure - QCI
- Certification schemes
- Cybersecurity tools

Advanced digital skills

- Master courses
- Short term trainings
- Job placements
- Platform for Skills and Jobs

European digital innovation hubs

- At least one per MS
- At least one per MS on AI

Deployments : emphasis on

- Destination Earth
- Green and smart communities and mobility
- Continuation of investments (CEF – ISA2)
- Once-only principle
- Blockchain
- Enhancing confidence in the digital transformation

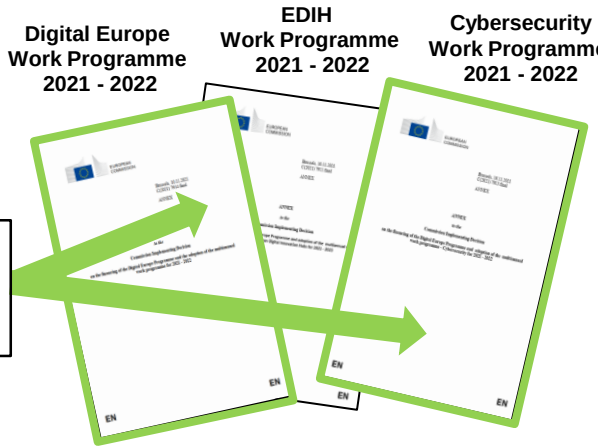
Quelle: EU Kommission

Arbeitsprogramme von „Digitales Europa“

„Digitales Europa“ wird derzeit in vier Arbeitsprogramme umgesetzt:

- DIGITAL Europe Work Programme 2021-2022
- *DIGITAL Europe - EDIH Work Programme 2021-2023*
- *DIGITAL Europe - Cybersecurity Work Programme 2021-2022*
- *HPC actions – Work Programme will be prepared by the EuroHPC Joint Undertaking*

Cybersecurity
462,5 Mio. €



„Digitales Europa“ - Arbeitsprogramm 2021 / 2022

Topic	Budget (Mio. Euro)	Open	Deadline
Cybersecurity / A secure quantum communication infrastructure for the EU (the EuroQCI)			
Create a European Industrial Ecosystem for Secure QCI technologies and systems (SME support grant)	44,00	17.11.2021	29.03.2022
Deploying advanced national QCI systems and networks (Simple grant)	108,00	17.11.2021	29.03.2022
Coordinate the first deployment of national EuroQCI projects and prepare the large-scale QKD testing and certification infrastructure (CSA)	2,00	17.11.2021	29.03.2022
Deploy a large-scale testing and certification infrastructure for QKD devices, technologies and systems enabling their accreditation and rollout in EuroQCI (procurement)	16,00	-	2022

Deploy a large-scale testing and certification infrastructure for QKD devices, technologies and systems enabling their accreditation and rollout in EuroQCI

Outcomes and deliverables*

- QKD-Infrastruktureinrichtung zur Deckung des EU-Bedarf in Bezug auf Tests, Erprobung, Validierung und Unterstützung bei der Akkreditierung von QKD-Geräten, Technologien und Systemen
- Vollständig interoperable quantenbasierte Technologien zwischen Bodenstationen (simulierten oder realen) Satellitensystemen und terrestrischen Systemen.

Scope*

- Bereitstellung von Test- und Zertifizierungsinfrastruktureinrichtung, für den Test von QKD-Technologien und Systemen
- Entwicklung einer Testumgebung zur Simulation der EuroQCI-Architektur auf der Grundlage bestehender EuroQCI-Systemstudien
- Schnittstellentest zwischen den Weltraum- und den terrestrischen Komponenten von EuroQCI

Procurement: Förderquote 50%; Teilnahme ist eingeschränkt auf der Grundlage von Artikel 12(5)

Instrument	Förderung je Projekt	Topic-budget	Deadline
Procurement	- €	16 Mio. €	2022

* Auszug aus dem Arbeitsprogramm 21-22

Bundesministerium
für Bildung
und Forschung

NKS Digitale und Industrielle Technologien
Nationale Kontaktstelle zum
EU-Programm Horizont Europa

„Digitales Europa“ - Cybersicherheits-Arbeitsprogramm 2021 / 2022

Topic	Budget (Mio. Euro)		Open 2022	Deadline 2022
Actions for Cybersecurity and Trust: European “Cyber-Shield”				
EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges	15		Q3	Q4
Capacity Building Of Security Operation Centres (SOC); (1) Capacity building activity & (2) Deployment and running of advanced tools and infrastructures	(1) 80	(2) 30	Q3	Q4
Securing 5G Strategic Digital Infrastructures And Technologies	10		Q3	Q4
Uptake Of Innovative Cybersecurity Solutions	32		Q3	Q4
Support To Cybersecurity In The Health Sector	10		22.02.2022	31.05.2022
Actions for Cybersecurity and Trust: Support To Implementation Of Relevant EU Legislation				
Deploying The Network Of National Coordination Centres With Member States	55		Q3	Q4
Cybersecurity Community support	3		21.06.2022	16.09.2022
Supporting The NIS Directive Implementation And National Cybersecurity Strategies	20		Q3	Q4
Testing and Certification Capabilities	5		Q3	Q4

Digitales Europa - Cybersicherheits-Arbeitsprogramm 2021 / 2022

Maßnahmen für Cybersicherheit und Vertrauen: Europäischer „Cyber-Schutzschild“

- EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges
- Kapazitätsaufbau von Sicherheitsoperationszentren
- Sicherung strategischer digitaler 5G-Infrastrukturen und -Technologien
- Einführung innovativer Cybersicherheitslösungen
- Unterstützung der Cybersicherheit im Gesundheitssektor

Digitales Europa - Cybersicherheits-Arbeitsprogramm 2021 / 2022

Maßnahmen für Cybersicherheit und Vertrauen:

Unterstützung bei der Umsetzung einschlägiger EU-Rechtsvorschriften

- Aufbau des Netzes der nationalen Koordinierungszentren mit den Mitgliedstaaten
- Unterstützung der Cybersicherheitsgemeinschaft
- Unterstützung der Umsetzung der NIS-Richtlinie und der nationalen Cybersicherheitsstrategien
- Prüf- und Zertifizierungskapazitäten

Digitales Europa - Cybersicherheits-Arbeitsprogramm 2021 / 2022

Maßnahmen für Cybersicherheit und Vertrauen: Europäischer „Cyber-Schutzschild“

- EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges
- Kapazitätsaufbau von Sicherheitsoperationszentren
- Sicherung strategischer digitaler 5G-Infrastrukturen und -Technologien
- Einführung innovativer Cybersicherheitslösungen
- Unterstützung der Cybersicherheit im Gesundheitssektor

EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges

Outcomes and deliverables*

- Starke Kapazität in den Mitgliedstaaten, um auf groß angelegte Cybersicherheitsvorfälle koordiniert zu reagieren
- Hochkarätige Cybersicherheitsbereiche, die fortgeschrittene Fähigkeiten, Kenntnisse und Testplattformen bieten

Scope*

- Die Schaffung, den Betrieb, den Kapazitätsausbau oder die Aufnahme von Cybersicherheitsbereiche unterstützen
- Förderung der Vernetzung zum Aufbau von Cybersicherheitskompetenzen
  - in Schlüsseltechnologien (z. B. 5G, Internet der Dinge, Cloud, künstliche Intelligenz, industrielle Kontrollsysteme)
  - sowie in Anwendungsbereichen (z. B. Gesundheit, Energie, Finanzen, Verkehr, Telekommunikation, Agrar- und Ernährungswirtschaft, Ressourcenmanagement)
- Austausch von Wissen zwischen Cybersecurity-Bereichen und Schaffung gemeinsamer Datenbestände
- Unterstützung groß angelegter und sektorübergreifender Szenarien: z.B. Serious-Gaming-Übungen, realistische Verkehrssimulationen

SME support grant
Zuschuss zur Unterstützung von KMU (75% Kofinanzierungssatz für KMU und 50% für alle anderen Begünstigten)

Instrument	Förderung je Projekt	Topic-budget	Deadline
SME support grant	2 – 4 Mio. €	15 Mio. €	Q4 - 2022

* Auszug aus dem Arbeitsprogramm 21-22

Digitales Europa - Cybersicherheits-Arbeitsprogramm 2021 / 2022

Maßnahmen für Cybersicherheit und Vertrauen: Europäischer „Cyber-Schutzschild“

- EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges
- Kapazitätsaufbau von Sicherheitsoperationszentren
- Sicherung strategischer digitaler 5G-Infrastrukturen und -Technologien
- Einführung innovativer Cybersicherheitslösungen
- Unterstützung der Cybersicherheit im Gesundheitssektor

Capacity Building Of Security Operation Centres (SOC): (1) Capacity building activity (Simple grant) & (2) Deployment and running of advanced tools and infrastructures (Joint procurement)

Outcomes and deliverables*

- Mehrere grenzüberschreitende Plattformen für die Zusammenführung von Daten über Bedrohungen der Cybersicherheit zwischen mehreren Mitgliedstaaten
- SOC von Weltklasse in der gesamten Union, verstärkt durch modernste Technologie in Bereichen wie KI
- Austausch von und Vereinbarungen über Bedrohungsdaten zwischen SOCs mitzuständigen Behörden

Scope*

- Verbesserung der Widerstandsfähigkeit im Bereich der Cybersicherheit durch
  - Schnellere Erkennung und Reaktion auf Cybersicherheitsvorfälle (auf nationaler und EU-Ebene)
  - Einrichtung von SOCs, insbesondere KMU (bzw. Unterstützung bestehender SOC) national, regional, sektoral, ...
  - Nutzung disruptiver Technologien und Austausch von Informationen
- Einsatz modernster KI (einschl. maschinelles Lernen) und Rechenleistung zur Erkennung bösartiger Aktivitäten: dynamisches Lernen

Anwendung von Artikel 12(5)
(1) Simple grant (50% Kofinanzierungssatz)
(2) Gemeinsame Beschaffung

Instrument	Förderung je Projekt	Topic-budget	Deadline
(1) Simple grant (2) Joint procurement	7 – 10 Mio. €	(1) 80 Mio. € (2) 30 Mio. €	Q4 - 2022

* Auszug aus dem Arbeitsprogramm 21-22

Digitales Europa - Cybersicherheits-Arbeitsprogramm 2021 / 2022

Maßnahmen für Cybersicherheit und Vertrauen: Europäischer „Cyber-Schutzschild“

- EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges
- Kapazitätsaufbau von Sicherheitsoperationszentren
- Sicherung strategischer digitaler 5G-Infrastrukturen und -Technologien
- Einführung innovativer Cybersicherheitslösungen
- Unterstützung der Cybersicherheit im Gesundheitssektor

Securing 5G Strategic Digital Infrastructures And Technologies (Simple grant)

Outcomes and deliverables*

- Vertrauenswürdige und sichere 5G-Dienste
- Unterstützung der Zusammenarbeit zwischen nationalen Behörden und privaten Anbietern von Technologiediensten oder -ausrüstungen, insbesondere innovativen europäischen KMU
- Unterstützung bei Erprobung, Prüfung und Integration von Sicherheits- und Interoperabilitätsaspekten von interoperablen, offenen und disaggregierten Lösungen

Scope*

- Unterstützung der 5G-Cybersecurity, insbesondere als Beitrag zu den Zielen und Maßnahmen der Empfehlung und der "Toolbox" zur 5G-Cybersicherheit
- Erprobung und Unterstützung des Aufbaus von Kapazitäten für Sicherheits- und Interoperabilitätsaspekte: Neue Kooperationsmodelle erforschen, innovative Ansätze integrieren (für europäischen KMU)

Simple grant (50% Kofinanzierungssatz)
Anwendung von Artikel 12(5)

Instrument	Förderung je Projekt	Topic-budget	Deadline
Simple grant	1 – 3 Mio. €	10 Mio. €	Q4 - 2022

* Auszug aus dem Arbeitsprogramm 21-22

Digitales Europa - Cybersicherheits-Arbeitsprogramm 2021 / 2022

Maßnahmen für Cybersicherheit und Vertrauen: Europäischer „Cyber-Schutzschild“

- EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges
- Kapazitätsaufbau von Sicherheitsoperationszentren
- Sicherung strategischer digitaler 5G-Infrastrukturen und -Technologien
- Einführung innovativer Cybersicherheitslösungen
- Unterstützung der Cybersicherheit im Gesundheitssektor

Uptake Of Innovative Cybersecurity Solutions (SME support grant)

Outcomes and deliverables*

- Unterstützung der Einführung marktreifer innovativer Cybersicherheitslösungen,
- Bereitstellung und Einsatz aktueller Instrumente und Dienste für Organisationen (insbesondere KMU)
- Verbesserung der Sicherheit von Open-Source-Lösungen

Scope*

- Verbesserung der Cybersicherheitskapazitäten in der gesamten EU, insbesondere für KMU und öffentliche Organisationen
  - Maßnahmen zur Sensibilisierung
  - Marktplattform-Unterstützungs-Interaktion zwischen Anbietern und Anwendern

SME support grant
Zuschuss zur Unterstützung von KMU (75% Kofinanzierungssatz für KMU und 50% für alle anderen Begünstigten)

Instrument	Förderung je Projekt	Topic-budget	Deadline
SME support grant	2 – 5 Mio. €	32 Mio. €	Q4 - 2022

* Auszug aus dem Arbeitsprogramm 21-22

Digitales Europa - Cybersicherheits-Arbeitsprogramm 2021 / 2022

Maßnahmen für Cybersicherheit und Vertrauen: Europäischer „Cyber-Schutzschild“

- EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges
- Kapazitätsaufbau von Sicherheitsoperationszentren
- Sicherung strategischer digitaler 5G-Infrastrukturen und -Technologien
- Einführung innovativer Cybersicherheitslösungen
- Unterstützung der Cybersicherheit im Gesundheitssektor

Support To Cybersecurity In The Health Sector

Call ist geschlossen!

Outcomes and deliverables*

- Unterstützung der Einführung marktreifer innovativer Cybersicherheitslösungen, einschließlich Lösungen, die im Rahmen von EU-geförderten Forschungs- und Innovationsprojekten entwickelt wurden
- Bereitstellung aktueller Instrumente für Einrichtungen des (öffentlichen) Gesundheitswesens (insbesondere KMU), um sich vor Cyber-Bedrohungen zu schützen
- Beitrag zur gemeinsamen Nutzung von Daten im Hinblick auf die kollektive Vebesserung der Sicherheit

Scope*

- Verbesserung der Cybersicherheitskapazitäten von Einrichtungen des (öffentlichen) Gesundheitswesens in der EU: Cybersicherheitsdienste und -produkte, Fähigkeiten und Schulungen, Sensibilisierung und Informationsaustausch, ...
- Umsetzung der Ziele und Anforderungen der NIS-Richtlinie in Bezug auf das Gesundheitswesen Sektor
- Elektronische ID (eID) und Datenverwaltungslösungen als Beitrag zur Datensicherheit im (öffentlichen) Gesundheitswesen

SME support grant
Zuschuss zur Unterstützung von KMU (75% Kofinanzierungssatz für KMU und 50% für alle anderen Begünstigten)

Instrument	Förderung je Projekt	Topic-budget	Deadline
SME support grant	1 – 3 Mio. €	10 Mio. €	31.05.2022

* Auszug aus dem Arbeitsprogramm 21-22

Digitales Europa - Cybersicherheits-Arbeitsprogramm 2021 / 2022

Maßnahmen für Cybersicherheit und Vertrauen:

Unterstützung bei der Umsetzung einschlägiger EU-Rechtsvorschriften

- Aufbau des Netzes der nationalen Koordinierungszentren mit den Mitgliedstaaten
- Unterstützung der Cybersicherheitsgemeinschaft
- Unterstützung der Umsetzung der NIS-Richtlinie und der nationalen Cybersicherheitsstrategien
- Prüf- und Zertifizierungskapazitäten

Bundesministerium
für Bildung
und Forschung

NKS Digitale und Industrielle Technologien
Nationale Kontaktstelle zum
EU-Programm Horizont Europa

„Digitales Europa“ - Cybersicherheits-Arbeitsprogramm 2021 / 2022

1/3

Topic	Budget (Mio. Euro)	Open 2022	Deadline 2022
Actions for Cybersecurity and Trust: European “Cyber-Shield”			
EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges	15	Q3	Q4
Capacity Building Of Security Operation Centres (SOC); (1) Capacity building activity & (2) Deployment and running of advanced tools and infrastructures	(1) 80 (2) 30	Q3	Q4
Securing 5G Strategic Digital Infrastructures And Technologies	10	Q3	Q4
Uptake Of Innovative Cybersecurity Solutions	32	Q3	Q4
Support To Cybersecurity In The Health Sector	10	22.02.2022	31.05.2022
Actions for Cybersecurity and Trust: Support To Implementation Of Relevant EU Legislation			
Deploying The Network Of National Coordination Centres With Member States	**55**	**Q3**	**Q4**
Cybersecurity Community support	**3**	**21.06.2022**	**16.09.2022**
Supporting The NIS Directive Implementation And National Cybersecurity Strategies	**20**	**Q3**	**Q4**
Testing and Certification Capabilities	**5**	**Q3**	**Q4**

Deploying The Network Of National Coordination Centres With Member States

Outcomes and deliverables*

- Einrichtung und Betrieb von nationalen Koordinierungsstellen in den Mitgliedstaaten

Scope*

- Fungieren als Kontaktstellen auf nationaler Ebene für die Cybersecurity Competence Community, als Unterstützung des Europäischen Kompetenzzentrums für Cybersicherheit (ECCC)
- Bereitstellung von Fachwissen und aktive Mitwirkung an den strategischen Aufgaben des ECCC, unter Berücksichtigung der relevanten nationalen und regionalen Herausforderungen für die Cybersicherheit
- Förderung, Ermutigung und Erleichterung der Beteiligung der Zivilgesellschaft, insbesondere der Industrie Start-ups und KMU, Hochschul- und Forschungsgemeinschaften und anderen Akteuren an grenzüberschreitenden Projekten und Maßnahmen zur Cybersicherheit
- Bemühen um Synergien mit einschlägigen Aktivitäten auf nationaler, regionaler und lokaler Ebene, im Bereich der Forschung, Entwicklung und Innovation, insbesondere in den nationalen Strategien für die Cybersicherheit

Simple grant (50% Kofinanzierungssatz)
FSTP möglich (50% Kofinanzierungssatz)
Teilnahmebedingung: Call richtet sich an NCC

Instrument	Förderung je Projekt	Topic-budget	Deadline
Simple grant	2 Mio. €	55 Mio. €	Q4 - 2022

* Auszug aus dem Arbeitsprogramm 21-22

Cybersecurity Community support (procurement)

Outcomes and deliverables*

- Gestärkte Cybersicherheitsgemeinschaft zur Unterstützung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschungskompetenzzentrum

Scope*

- Unterstützung von Start-ups und Scale-ups im Bereich der Cybersicherheit in allen Mitgliedstaaten, auch mit dem Ziel Investitionen in die EU anzuziehen
- Unterstützung der Entwicklung und des Wachstums eines Binnenmarktes für Cybersicherheitsprodukte und Dienstleistungen in der EU
- Unterstützung des ECCC und des Netzes der NCCs bei der Förderung des Wissensaustauschs und der Vernetzung
- Unterstützung von Bildung, Ausbildung und Chancengleichheit im Bereich der Cybersicherheit

Procurement (50% Kofinanzierungssatz)

Instrument	Förderung je Projekt	Topic-budget	Deadline
Procurement	3 Mio. €	3 Mio. €	16.09.2022

* Auszug aus dem Arbeitsprogramm 21-22

Supporting The NIS Directive Implementation And National Cybersecurity Strategies

Outcomes and deliverables*

- Die Mitgliedstaaten in die Lage zu versetzen, den Schaden von Vorfällen im Bereich der Cybersicherheit zu begrenzen
- Verbesserung der Einhaltung der NIS-Richtlinie
- Beitrag zu verstärkter Zusammenarbeit, Bereitschaft und Widerstandsfähigkeit der EU

Scope*

- Nutzerzentrierte Implementierung, Validierung, Erprobung und Einführung von Technologien, Werkzeugen und IT-gestützten Lösungen, zur Überwachung, Erkennung und Reaktion auf (grenzüberschreitenden) Cybersicherheitsvorfällen
- Zusammenarbeit, Wissensaustausch und Schulung von öffentlichen und privaten Organisationen, die an der Umsetzung der NIS-Richtlinie arbeiten
- Partnerschaftsprogramme, zur Einführung und Übernahme von Technologien, Werkzeugen, Verfahren und Methoden für eine wirksame grenzüberschreitende Zusammenarbeit bei der Prävention, Aufdeckung und Bekämpfung von Cybersicherheitsvorfällen

SME support grant (Kofinanzierung: KMU 75% und 50% für alle anderen)

Instrument	Förderung je Projekt	Topic-budget	Deadline
SME support grant	1 – 5 Mio. €	20 Mio. €	Q4 - 2022

* Auszug aus dem Arbeitsprogramm 21-22

Testing and Certification Capabilities

Outcomes and deliverables*

- Stärkung der nationalen Zertifizierungsbehörden, Konformitätsbewertungsstellen und Akkreditierungsstellen für Cybersicherheit
- Verbesserung der Kapazitäten für Cybersicherheits- und Interoperabilitätstests in allen Mitgliedstaaten, auch im Bereich der disaggregierten und offenen 5G-Lösungen
- Unterstützung von KMU bei der Prüfung ihrer Infrastruktur im Hinblick auf die Verbesserung ihres Cybersicherheitsschutzes
- Unterstützung von Maßnahmen im Bereich der Standardisierung / Normung

Scope*

- Unterstützung des Kapazitätsaufbaus bei nationalen Cybersicherheits-Zertifizierungsbehörden, Konformitätsbewertungsstellen und Akkreditierungsstellen
- Unterstützung von KMU bei der Prüfung und Zertifizierung von IKT-Produkten, IKT-Dienstleistungen oder IKT-Verfahren, die sie verkaufen. Vorrangig berücksichtigt werden Vorschläge, die sich positiv auf von der COVID-19-Krise betroffene Sektoren (z. B. das Gesundheitswesen) auswirken.
- Unterstützung von Normungsmaßnahmen, gegebenenfalls unter Berücksichtigung von Aktivitäten europäischer und internationaler Normungsorganisationen

Grant for Support to Third Parties (FSTP)
Teilnahmebedingung: an NCC gerichtet

Instrument	Förderung je Projekt	Topic-budget	Deadline
Grant for Support to Third Parties	0.5 – 1 Mio. €	5 Mio. €	Q4 - 2022

* Auszug aus dem Arbeitsprogramm 21-22

Bundesministerium
für Bildung
und Forschung

NKS Digitale und Industrielle Technologien
Nationale Kontaktstelle zum
EU-Programm Horizont Europa

Danke für Ihre Aufmerksamkeit!!!