



NCC-AT Community Event 2025

Innovation in der Cybersicherheit:
Von der Forschung in den Markt

Wien, 15. Mai 2025

Programm I

- 09:00 - 10:00* *Eintreffen & Meet the Experts*
- 10:00 – 10:15 Begrüßung und Eröffnung durch NCC-AT
- 10:15 – 11:15 Session 1: Funding to Impact – Förderprogramme und erfolgreich Förderanträge stellen
- 11:15 – 11:45* *Kaffeepause*
- 11:45 – 12:45 Session 2: Cyber Innovation in Action – Erfolgreiche Projekte aus Forschung & Praxis
- Session 3: Cyber Connect – Gemeinsam Innovationen für Cybersicherheit entwickeln
- 12:45 – 14:00* *Mittagspause*

Programm II

- 14:00 – 14:30 Begrüßung und Eröffnung Nachmittagsprogramm
- 14:30 – 14:45 Keynote 1: Strategische Autonomie durch europäische Innovationen in der Cybersicherheit
- 14:45 – 15:00 Keynote 2: EU Best Practice: Innovation in der Cybersicherheit – Schlüssel zur technologischen Souveränität
- 15:00 – 15:15 NCC-AT Service & Community
- 15:15 – 16:00 Paneldiskussion: Von der Forschung in den Markt: Cybersicherheitsstrukturen in Österreich
- 16:00 – 17:00 *Networking & Ausklang*



NCC-AT Community Event 2025

Innovation in der Cybersicherheit:
Von der Forschung in den Markt

Mag. Hanna Wilhelmer, BA, BKA
DI Thomas Zergoi, FFG

Funding to Impact – Förderprogramme und erfolgreich Förderanträge stellen

Session 1

DI Lydia Lindner, BSc (NCC-AT & FFG)

Polina Wilhelm (FFG)

Cybersecurity-relevante EU-Förderprogramme

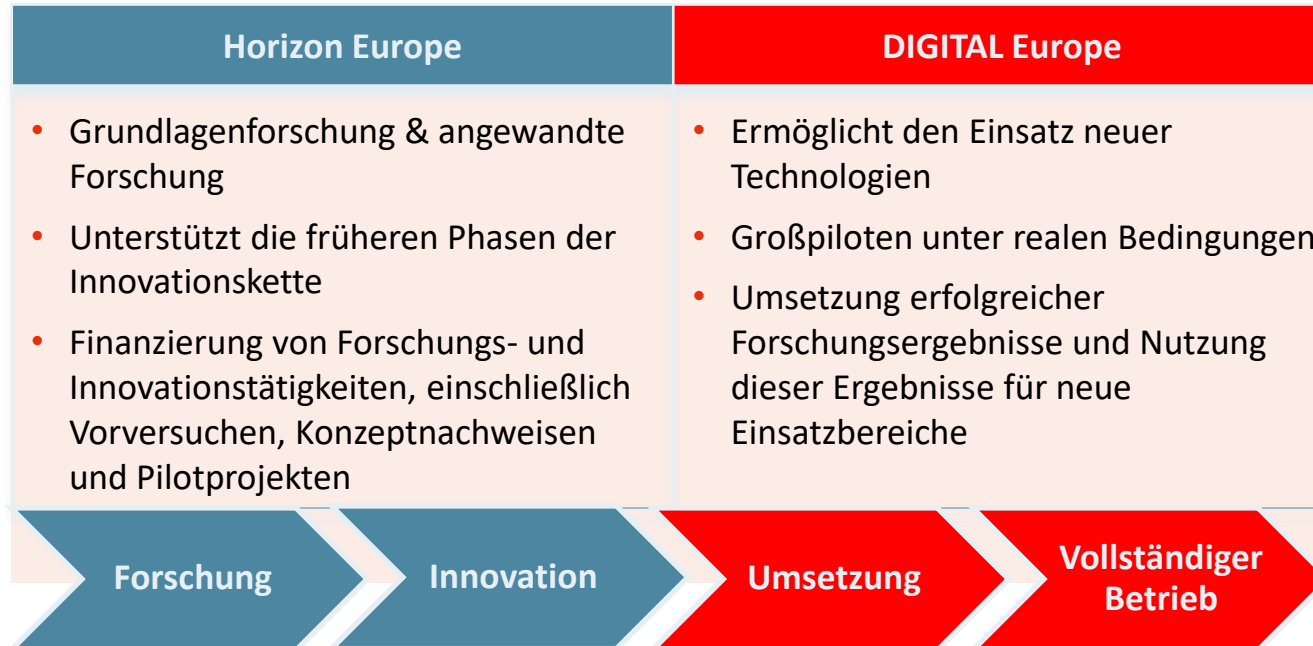


© European Commission



© European Commission

Vergleich Horizon Europe & DIGITAL Europe Programm



Das Horizon Europe Programm

- **Rahmenprogramm der Europäischen Union für Forschung und Innovation** für den Zeitraum **2021–2027**.
- Es ist das **größte Forschungsförderprogramm der EU**, mit einem Gesamtbudget von rund **€95,5 Milliarden**.
- **Ziel:** Wissenschaftliche und technologische Exzellenz in Europa zu stärken und zugleich die Wettbewerbsfähigkeit sowie Innovationskraft der EU nachhaltig zu fördern.
- **Komplementär zum Digital Europe Programm**
- **Zielgruppe:** Universitäten, Forschungseinrichtungen, Unternehmen, öffentliche Institutionen

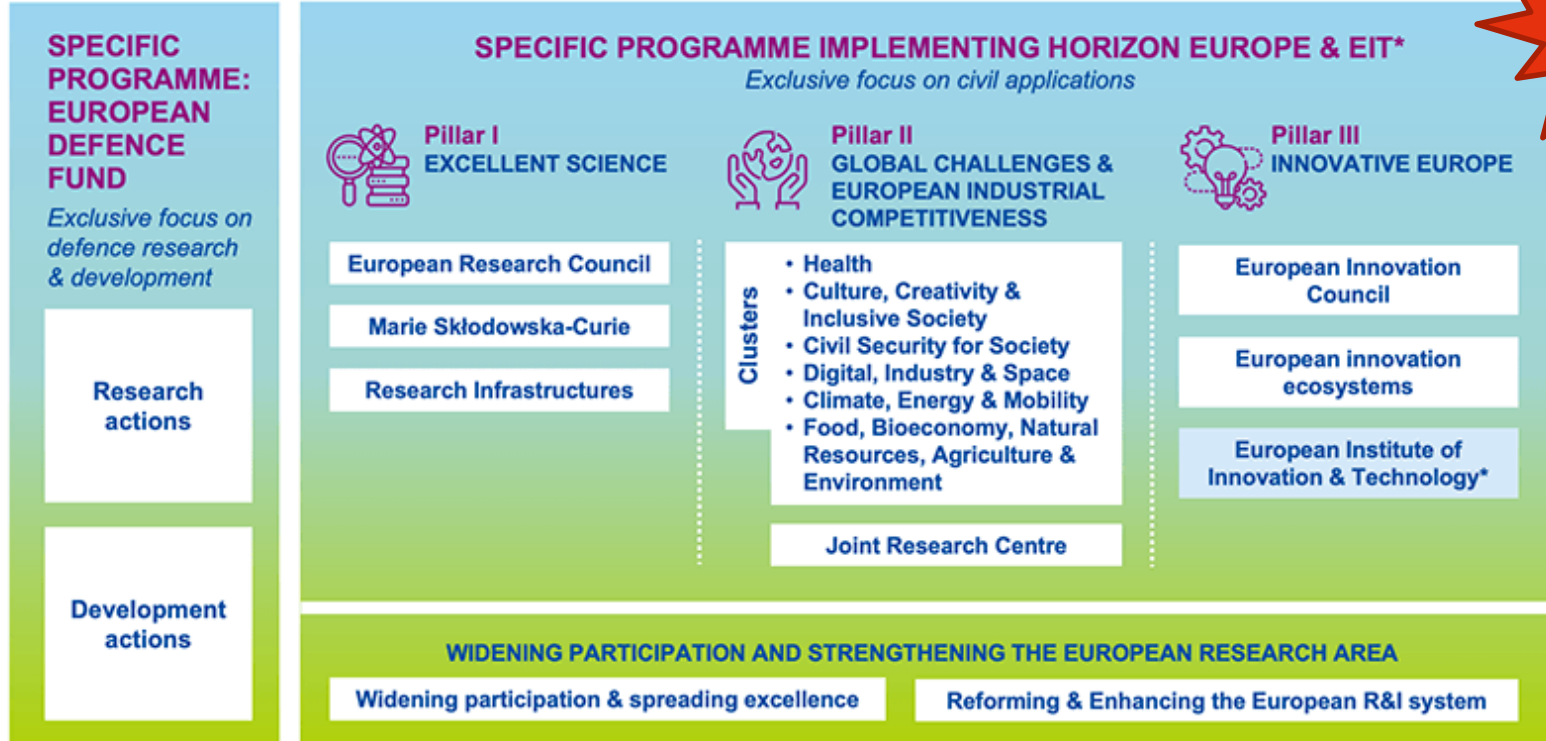


© European Commission

© European Commission

HORIZON EUROPE

~ 95
Mrd €

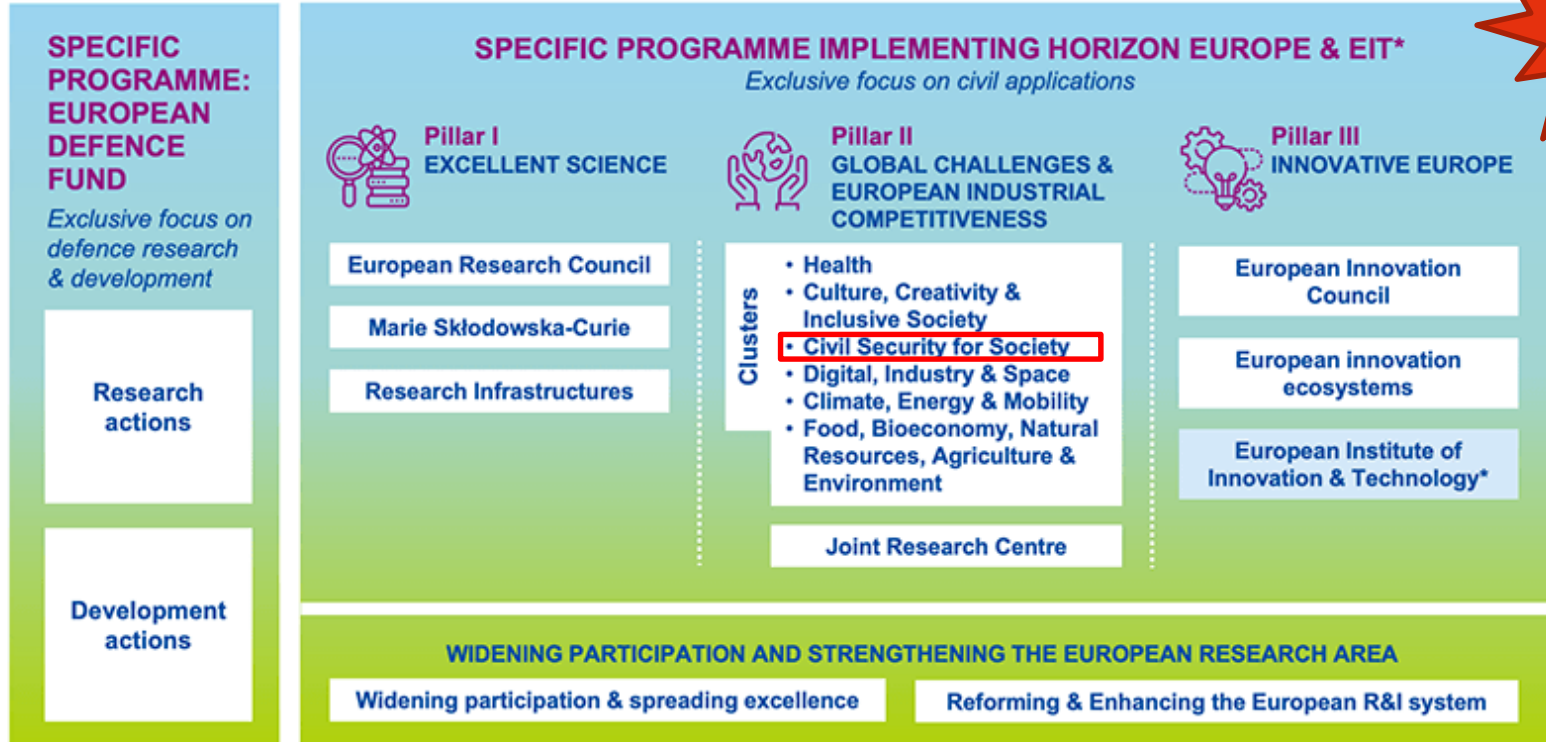


* The European Institute of Innovation & Technology (EIT) is not part of the Specific Programme

© European Commission

HORIZON EUROPE

~ 95
Mrd €



* The European Institute of Innovation & Technology (EIT) is not part of the Specific Programme

Horizon Europe - Cluster 3 „Civil Security for Society“

>> Destinationen und Synergien



Fight against Crime and Terrorism (FCT)

4 Topics, 43.5 Mio. €

Internal Security Fund, Cluster 2



Border Management (BM)

3 Topics, 28 Mio.€

Border Management and Visa Instrument



Resilient Infrastructure (INFRA)

2 Topics, 22 Mio. €

European Defence Fund, Digital Europe Programme, Cluster 5



Increased Cybersecurity (CS)

6 Topics, 90,5 Mio. €

Digital Europe Programme, European Defence Fund, Cluster 1, Cluster 4



Disaster Resilient Society (DRS)

4 Topics, 41 Mio. €

European Defence Fund, Union Civil Protection Mechanism, Cluster 5

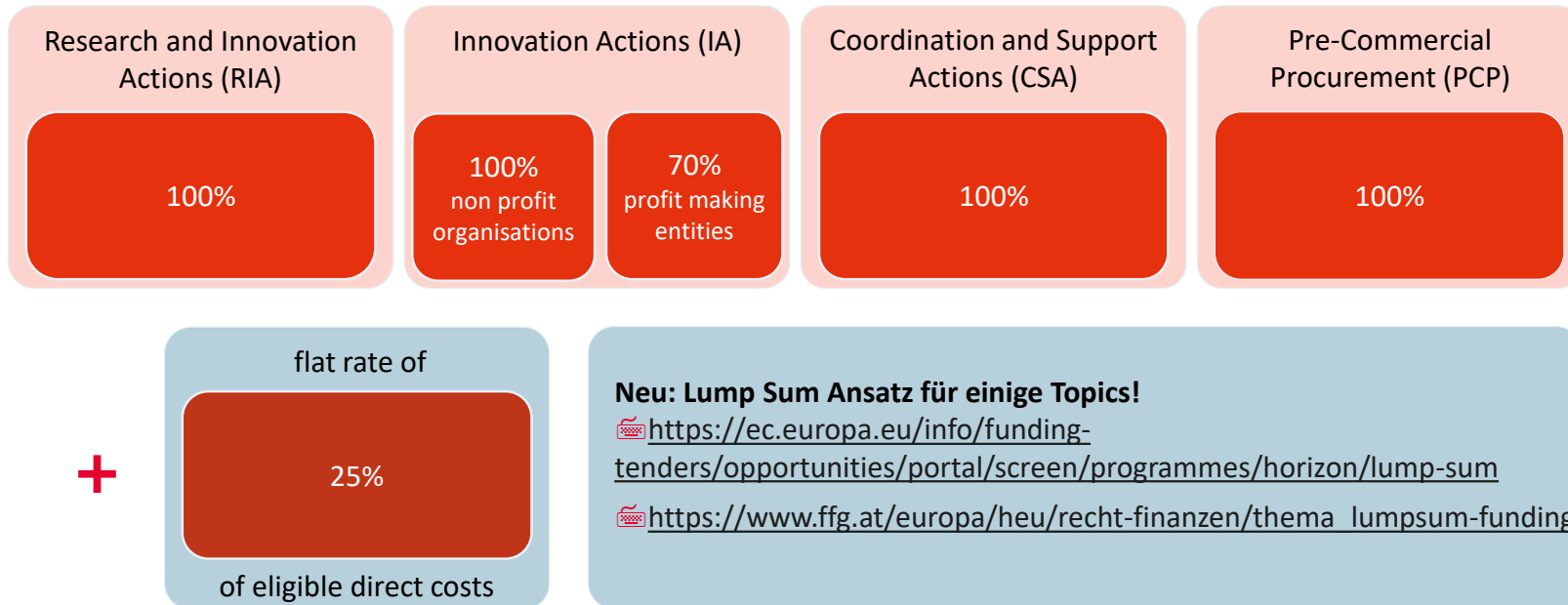


Strengthening Security Research and Innovation (SSRI)

6 Topics, 21.5 Mio. €

DRAFT!

Instrumente und Förderraten: Horizon Europe – Cluster 3



Teilnahmebedingungen Horizon Europe

Standardregel

- mindestens 3 voneinander unabhängige Rechtspersonen aus 3 unterschiedlichen EU-Mitgliedsstaaten oder assoziierten Staaten,
NEU! davon mindestens 1 Rechtsperson aus einem EU-Mitgliedsstaat

darüber hinaus

- mehrere Partner pro Land möglich,
- auch Teilnahme aus nicht-assozierten Drittstaaten möglich (sofern keine spezifischen Ausschlusskriterien festgelegt sind); ohne EU-Förderung,
- nicht-industrialisierte Länder bekommen auch EU Förderung,
- für bestimmte Themenbereiche (insbesondere im Bereich Cybersicherheit) gelten zusätzliche Einschränkungen.

Horizon Europe - Cluster 3: Increased Cybersecurity



Topics 2025

DRAFT!

Topic ID	Topic	Restrictions
HORIZON-CL3-2025-02-CS-ECCC-01	Generative AI for Cybersecurity applications	Restricted to MS + AC
HORIZON-CL3-2025-02-CS-ECCC-02	New advanced tools and processes for Operational Cybersecurity	Restricted to MS + AC
HORIZON-CL3-2025-02-CS-ECCC-03	Privacy Enhancing Technologies	
HORIZON-CL3-2025-02-CS-ECCC-04	Security evaluations of Post-Quantum Cryptography (PQC) primitives	Restricted to MS + AC + OECD
HORIZON-CL3-2025-02-CS-ECCC-05	Security of implementations of Post-Quantum Cryptography algorithms	Restricted to MS + AC + OECD
HORIZON-CL3-2025-02-CS-ECCC-06	Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols	Restricted to MS + AC + OECD

Horizon Europe – Cluster 3: Tipps und Tricks



Kooperation und Einbindung von Stakeholdern wie Betreiber von Infrastrukturen, regionale oder Behörden, Industriepartnern, Multiplikator:innen



Auseinandersetzung mit relevanten Policies , z.B. Cybersecurity Strategy, NIS-2 Directive, Directive on the Resilience of Critical Entities (CER), AI Act, Digital Skills etc.



Kompabilität mit geförderten/laufenden Projekten, z.B. in Cluster 3, Cluster 4 und im Digital Europe Programm, Teil Cybersecurity, EDF (Dual-Use!) und mit nationalen Initiativen (z.B. K-PASS)!



Vernetzung und Austausch mit Initiativen wie ENISA, ECCC, NCCs, ECSO, EDIHs, CS Competence Community, Cyber Skills Academy ...



Darstellung des Nutzen für die Gesellschaft und Berücksichtigung ethischer Aspekte, insbes. Datenschutz, Privatsphäre, etc.

KONTAKT: HORIZON EUROPE – CLUSTER 3

DI Jeannette Klonk

Nationale Kontaktstelle „Zivile Sicherheit für die Gesellschaft“

Österreichische Forschungsförderungsgesellschaft
Sensengasse 1, A-1090 Wien

T +43 (0) 5 77 55 – 4401

M +43 (0) 664 88 963003

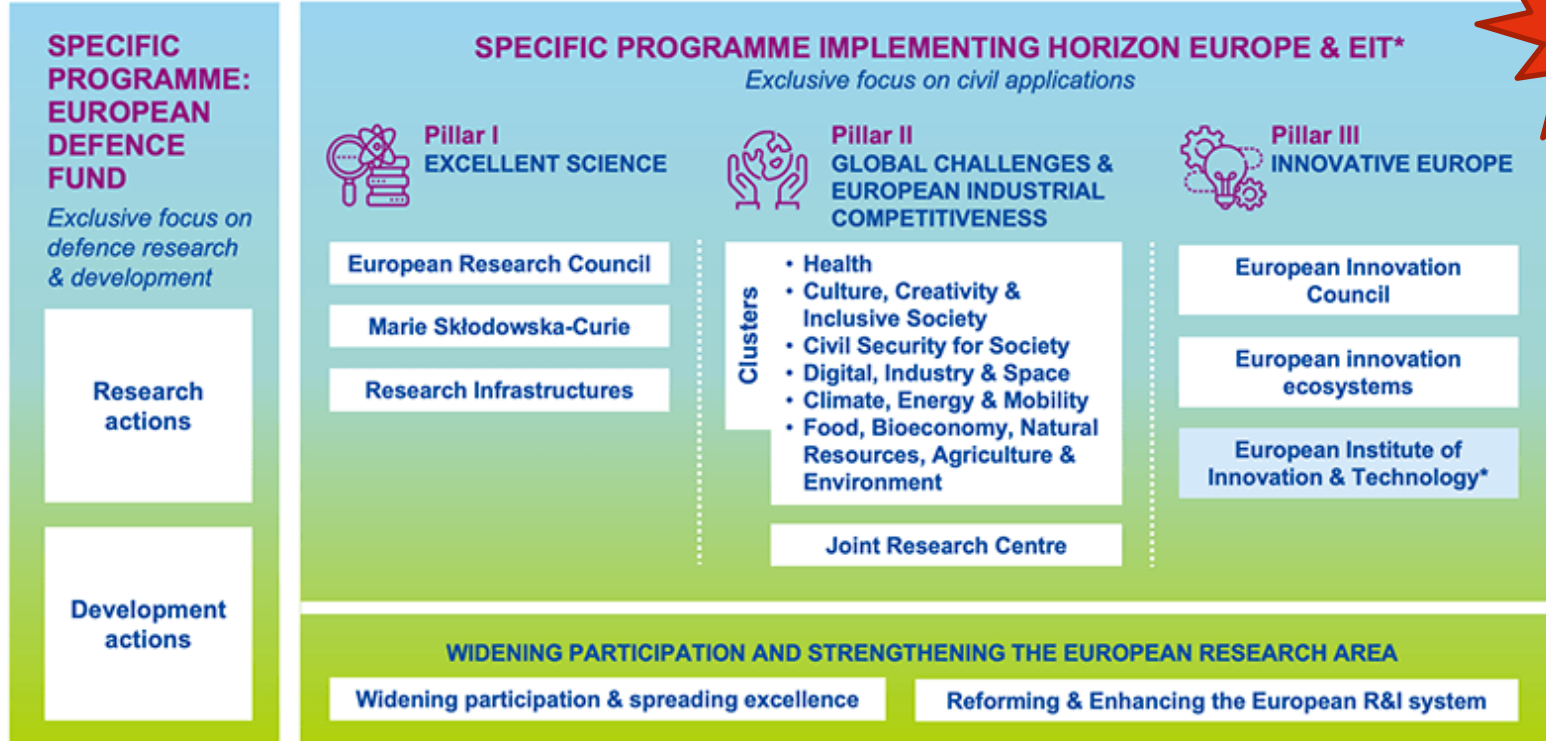
jeannette.klonk@ffg.at

www.ffg.at

© European Commission

HORIZON EUROPE

~ 95
Mrd €



* The European Institute of Innovation & Technology (EIT) is not part of the Specific Programme

© European Commission

HORIZON EUROPE

~ 95
Mrd €



* The European Institute of Innovation & Technology (EIT) is not part of the Specific Programme

Der „European Defence Fund“ (EDF)



© European Commission

- **EU-Förderprogramm für den Verteidigungssektor**
- Gefördert wird **Forschung zu innovativen Verteidigungstechnologien** und **Entwicklung von Prototypen**
- Kein Fokus auf Grundlagenforschung, sondern auf technologische Reife
- **Gesamt Budget:** 7,9 Milliarden €
 - Forschung: 2,651 Milliarden €
 - Entwicklung: 5,302 Milliarden €
- **Zielgruppe:** Start-ups, KMU, Forschungseinrichtungen und Großunternehmen
- **Ziele:**
 - Förderung gemeinsamer Verteidigungsforschung & -entwicklung
 - Stärkung der strategischen Autonomie Europas
 - Förderung der Wettbewerbsfähigkeit der europäischen Rüstungsindustrie

Instrumente und Förderraten: European Defence Fund (EDF)

Research Action (RA) - Forschung

- Wissen generieren
- Wissen integrieren
- Studien
- Design



- 100%

Development Action (DA) - Entwicklung

- Wissen integrieren
- Studien
- Design
- Prototypisierung
- Testen
- Qualifizierung
- Zertifizierung
- „Lebenszyklus“ des Produkts



- 20-90%
- Bonus bis max. 35%
- Ko-Finanzierung

Teilnahmebedingungen und Sicherheitsvorgaben EDF

Konsortialpartner

- Min. drei unabhängige Rechtspersonen aus drei verschiedenen EU-Mitgliedstaaten oder assoziierten Ländern (derzeit nur Norwegen).
- Bei bestimmten Ausschreibungen zu disruptiven Technologien genügt ein Konsortium mit mindestens zwei Rechtspersonen aus zwei Ländern.
- Keine „**Drittstaatenkontrolle**“. Teilnehmende und deren Ressourcen müssen in den Mitgliedsstaaten sein.
- Drittstaatenkontrolle besteht (BMLV).

Projektergebnisse

- Kein Transfer des IP außerhalb der EU erlaubt

Klassifizierte Informationen

- Eventuell **Facility Security Clearance** und **Personal Security Clearance** benötigt!
- Zuständigkeit BMLV und BKA
- Beachten Sie die Bearbeitungsdauer!

Cybersecurity-relevante Ausschreibungen im EDF



Topics 2025

Topic ID	Topic	Restrictions
EDF-2025-LS-RA-SI-CYBER-3RAV-STEP	Risk, robustness and resilience for autonomous vehicles in military operations	EDF Lump Sum Grant (Development Action)
EDF-2025-DA-CYBER-CDOC-STEP	Improved cyber defence operations capabilities	EDF Development Actions

KONTAKT: EUROPEAN DEFENCE FUND (EDF)

DI Thomas Leithner
National Focal Point EDF

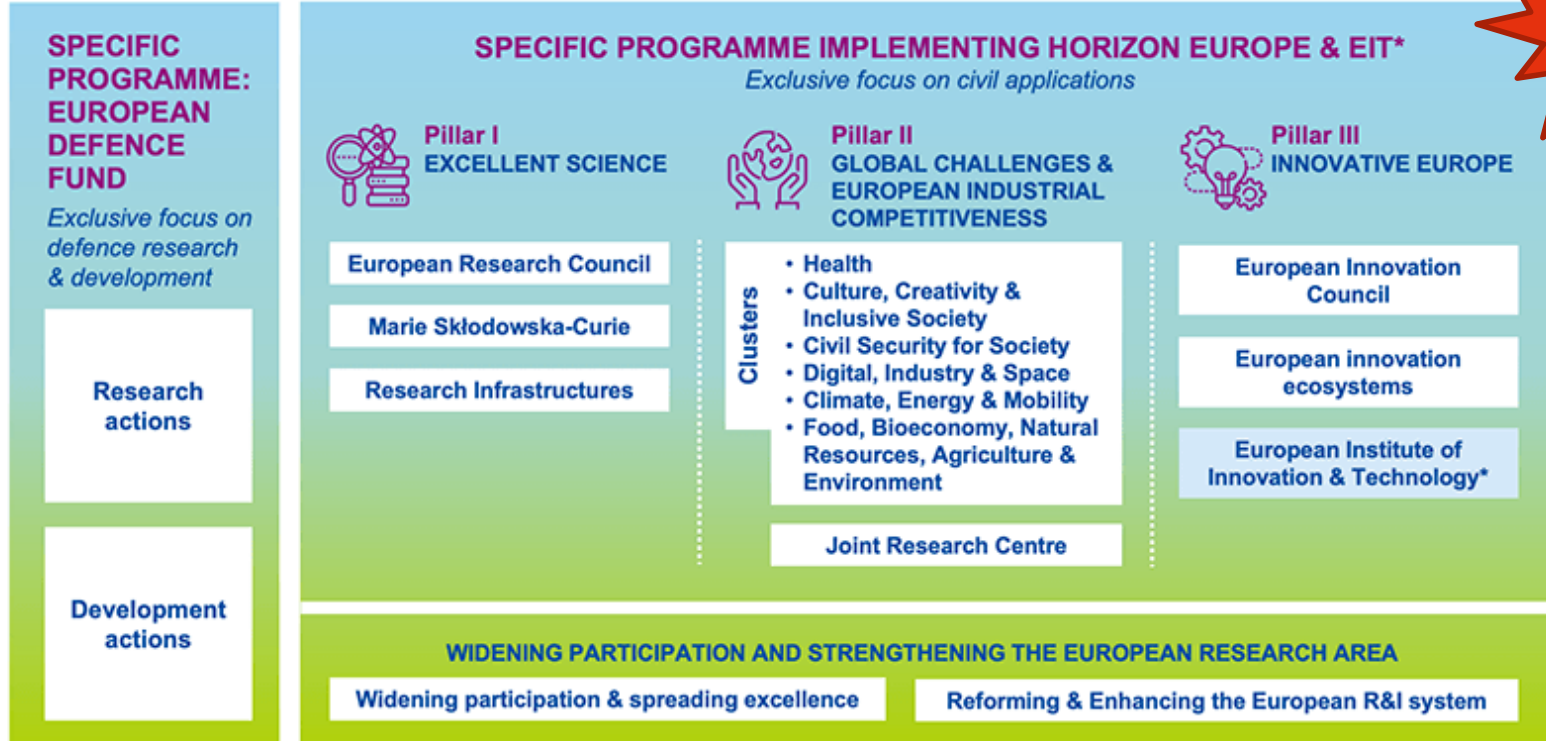
Österreichische Forschungsförderungsgesellschaft
Sensengasse 1, A-1090 Wien

T +43 (0) 5 77 55 – 4212
thomas.leithner@ffg.at
eudefence@ffg.at
www.ffg.at

© European Commission

HORIZON EUROPE

~ 95
Mrd €

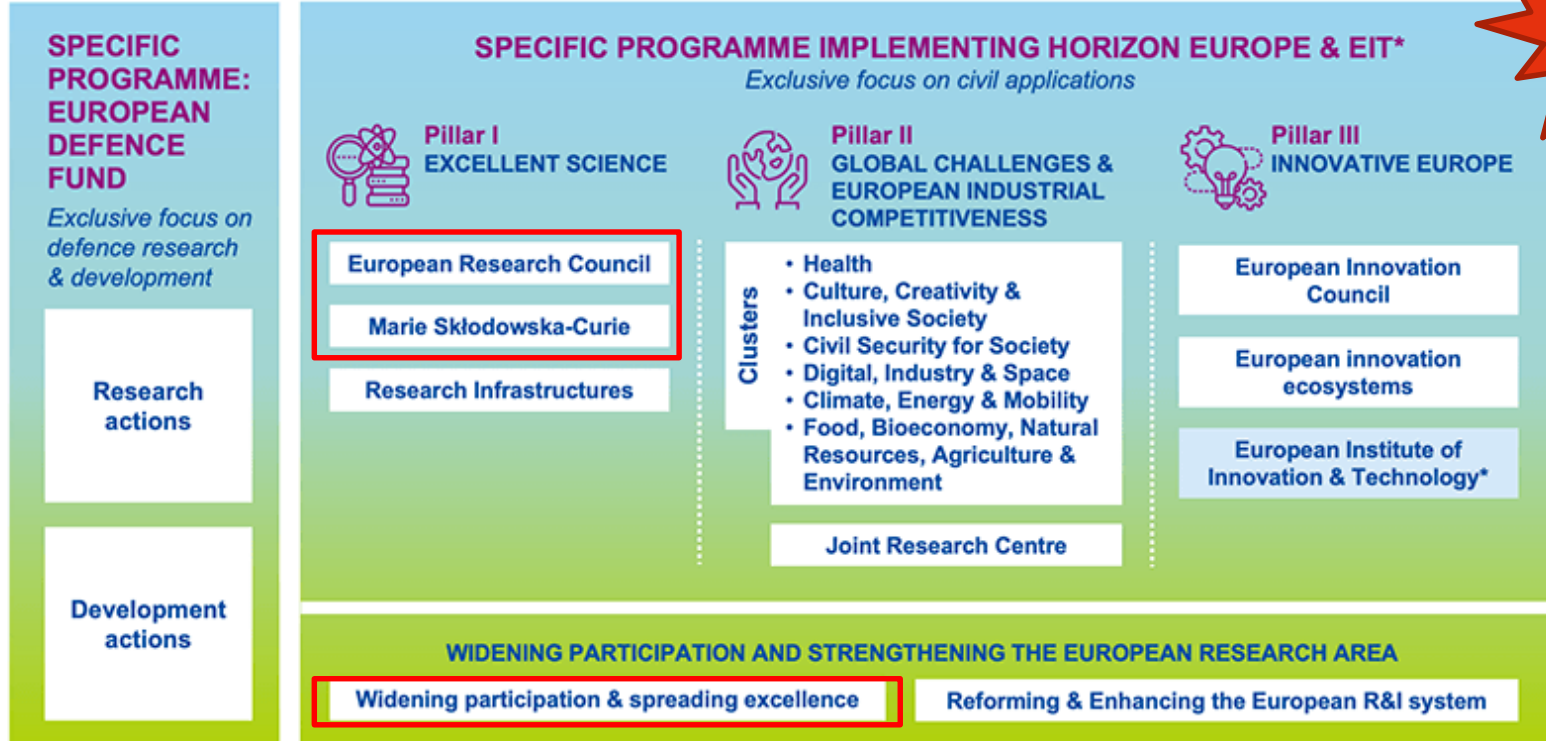


* The European Institute of Innovation & Technology (EIT) is not part of the Specific Programme

© European Commission

HORIZON EUROPE

~ 95
Mrd €



* The European Institute of Innovation & Technology (EIT) is not part of the Specific Programme

Themenoffene Förderungen in Horizon Europe



European Research Council (ERC)

*Förderungen für exzellente Einzel Forscher*innen und ihre Teams*

- **Starting Grant** 2-7 Jahre nach Diss
- **Consolidator Grant** 7-12 Jahre nach Diss
- **Advanced Grant** über 12 Jahre nach Diss
- **Synergy Grant** offen für alle Karrierestufen

jährliche Ausschreibungen

per Grant zwischen 1,5 und 10 Millionen Euro

sowie **Proof-of-Concept Grants**: eine Zusatzförderung für die vier Hauptgrants, um die Ergebnisse aus diesen Projekten zu verwerten, Förderhöhe: 150.000 Euro

www.ffg.at/europa/heu/erc

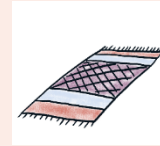


Marie Skłodowska-Curie Maßnahmen

Exzellente Forschungsprojekte und Unterstützung der Karriereentwicklung von Forscher:innen

- **Postdoctoral Fellowships**
Einzel Forschungsprojekte für Postdocs, die dafür nach AT kommen (Dauer 2-3.5 Jahre, je nach Laufzeit ca. 220.000 Euro / Projekt)
- **Doctoral Networks** Internationale Netzwerke zur Ausbildung von Doktorand*innen
→ 15 Dissertationen pro Projekt
- **COFUND** für Prä- und Postdoc-Programme, zur Förderung von Dissertations- und Postdoc-Projekten
- **Staff Exchange**: Wissenstransfer durch Personalaustausch

www.ffg.at/europa/heu/msca



COST Actions

Lebende Netzwerke für Forschung, Innovation und Karrieren

- **Thematisch offen & niederschwellige Beteiligungsmöglichkeiten**
- Fördert Trainingsformate, z.B. Training Schools, Forschungsaufenthalte, Treffen von Arbeitsgruppen
- Verschiedene Aktivitäten und Stipendien speziell für **junge Forschende und Innovator:innen**
- Laufende COST-Netzwerke, z.B. im Bereich Sicherheitsforschung:
<https://www.cost.eu/cost-actions-event/browse-actions/>

www.ffg.at/cost

KONTAKT: ERC, MARIE SKŁODOWSKA-CURIE MAßNAHMEN UND COST ACTIONS

Dr. Lil REIF
**ERC und Marie Skłodowska-
Curie Maßnahmen**

+43 577 55-4608
lil.reif@ffg.at

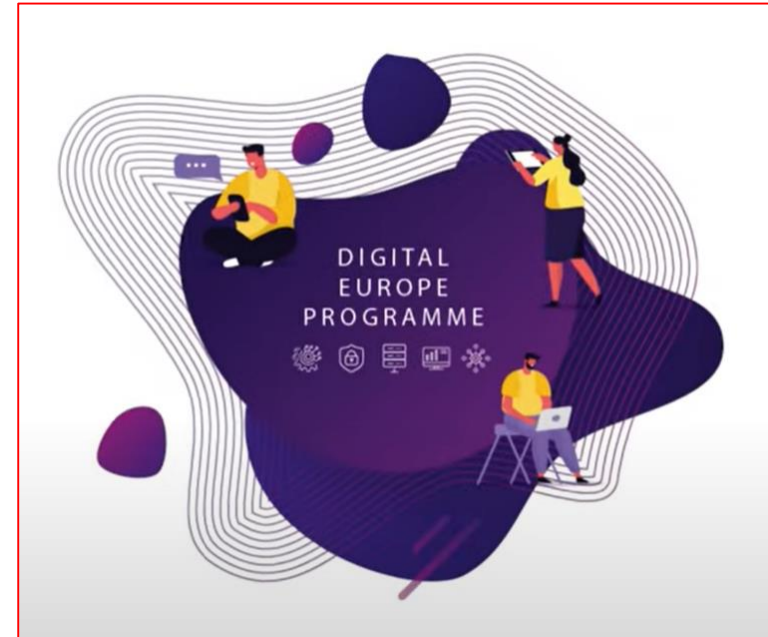
Mag. Pauline OBERTHALER
COST Actions

+43 577 55-4110
pauline.oberthaler@ffg.at

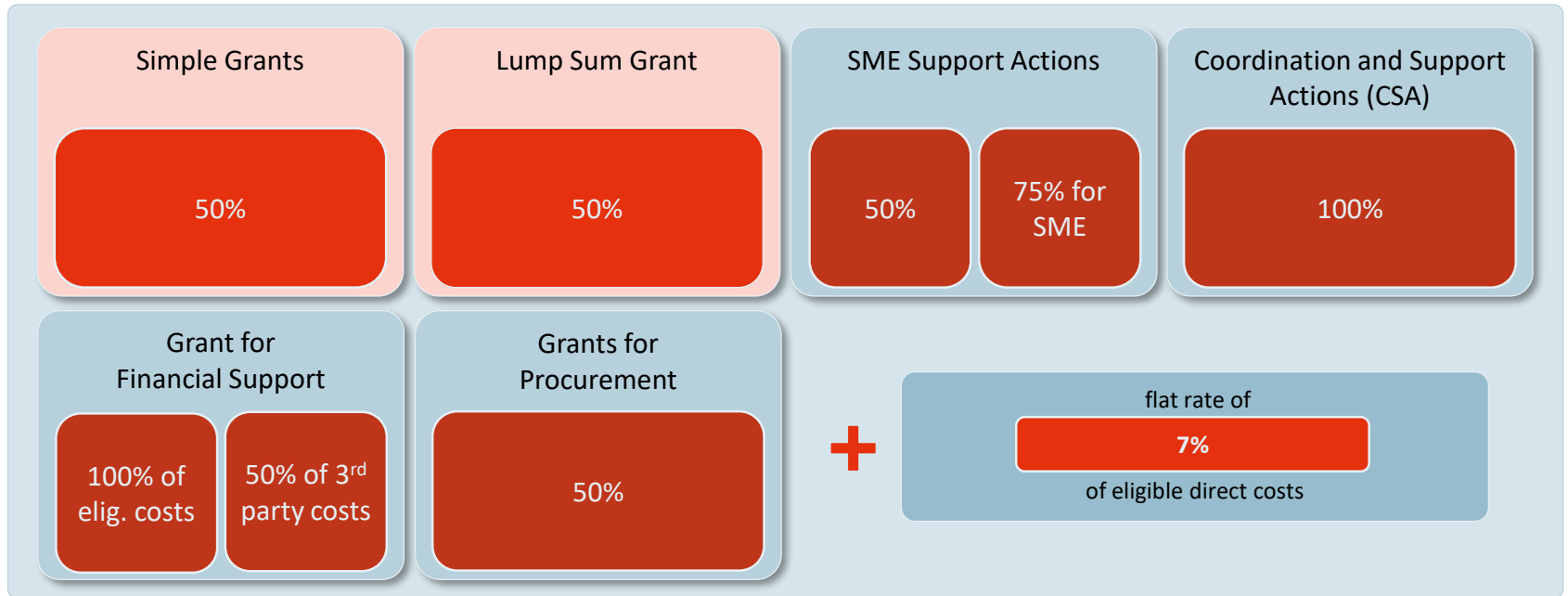
Österreichische Forschungsförderungsgesellschaft
Sensengasse 1, A-1090 Wien

Das DIGITAL Europe Programm

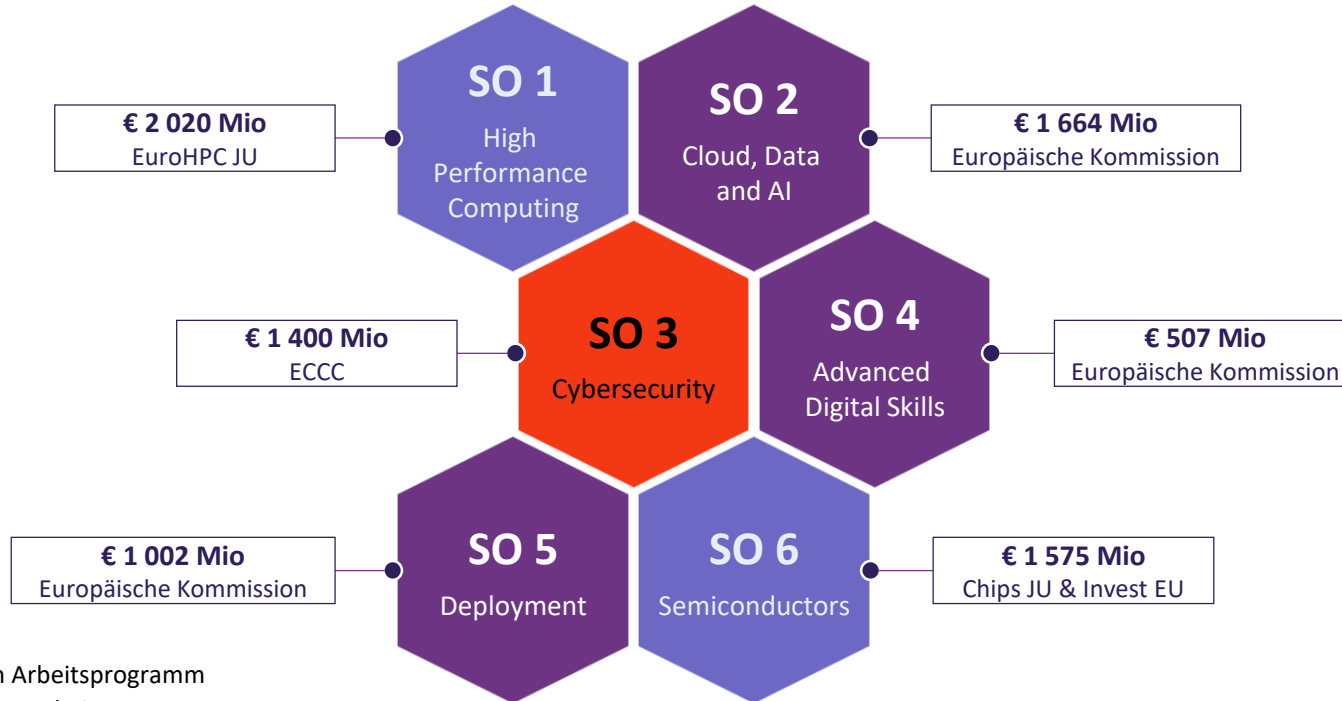
- Überbrückung der Lücke zwischen digitaler Forschung und Markteinführung
- **Ziel des Programms:** Verbindung von digitaler Forschung mit Markteinführung zugunsten europäischer Bürger und Unternehmen (insbesondere KMU)
- Beitrag zur grünen und digitalen Transformation sowie zur Stärkung der Resilienz und digitalen Souveränität der EU



DIGITAL Europe - Instrumente und Förderraten



DIGITAL Europe - Programmschwerpunkte 2021-2027



- Digital Main Arbeitsprogramm
- Cybersecurity Arbeitsprogramm
- Joint Undertaking

TOTAL BUDGET € 8 168 MIO

Teilnahmebedingungen DIGITAL Europe

Keine Standardregel bzgl. Konsortium wie in Horizon Europe:

- Keine grundsätzliche Konsortialspflicht
 - Auch Einzelanträge möglich
- Keine einheitliche Mindestanforderung → abhängig vom jeweiligen Ausschreibungsthema
- Für sicherheitsrelevante Themen (z. B. Cybersicherheit) gilt:
 - Teilnahme meist auf in der EU ansässige und kontrollierte Organisationen beschränkt
 - Beschränkung durch Art. 12(5) – DEP Reg. (EU) 2021/694
- Immer die spezifischen Bedingungen des jeweiligen Ausschreibungsthemas prüfen!

DIGITAL Europe – Cybersecurity Arbeitsprogramm



Cybersecurity

Implementiert durch ECCC

Calls restricted per
Art. 12(5) – DEP
Reg. (EU) 2021/694



Cyber Resilience Act

Cyber Solidarity Act

NIS2 Directive

New Technologies: AI & Transition to Post-Quantum

Development and
Implementation of AI Tools,
SME Support, Post-Quantum
Transition

Cyber Solidarity Act Implementation

National and Cross-Border
Cyber Hubs, Ecosystem &
Information Sharing,
Preparedness Testing

Additional Actions for Improving EU Cyber Resilience

NCC Network, Healthcare,
Legislative Compliance, Dual-
Use Technologies

DIGITAL EUROPE - CYBERSECURITY PROGRAMM

>> AUSSCHREIBUNGEN 2025

Timeline 2025	
Opening Call 1 2025	Juni 2025
Closing Call 1 2025	Oktober 2025
Opening Call 2 2025	September 2025
Closing Call 2 2025	Jänner 2026

Call Topics DEP CS 2025	Budget in Mio Eur	Call	Type	Funding Rate
New technologies. AI & transition to post quantum				
Cybersecure tools, technologies and services relying on AI	15	2	Simple Grant	50%
Transition to post-quantum Public Key Infrastructures	15	1	Simple Grant	50%
Uptake of innovative cybersecurity solutions for SMEs	15	2	SME support action	50-75%
Cyber Solidarity Act Implementation				
National Cyber Hubs	20	2	Joint procurement / Simple grant	50-75%
Cross-Border Cyber Hubs	20	2	Joint procurement / Simple grant	50-75%
Coordinated preparedness testing and other preparedness actions	5	1	Simple grant	50%
Additional actions improving EU resilience				
Enhancing the NCC network	10	1	Simple grant	50%
Dedicated action to reinforcing hospitals and healthcare providers	30	1	Simple grant	50%

KONTAKT: DIGITAL EUROPE CYBERSECURITY

DI Lydia Lindner, BSc.
Programmmanagerin NCC-AT

lydia.lindner@ffg.at

Anja Klauzer, MSc
Programmmanagerin NCC-AT

anja.klauzer@ffg.at

Mag. Nina Thomann, MA
Programmmanagerin NCC-AT

nina.thomann@ffg.at

Österreichische
Forschungsförderungsgesellschaft
Sensengasse 1, A-1090 Wien

ncc@ffg.at
www.ncc.gv.at

KONTAKT: DIGITAL EUROPE MAIN

DI Max Arends
Digital Europe NCP

+43 5 7755 4206
max.arends@ffg.at

Patricia Trinkl, MSc
Digital Europe NCP

+43 5 7755 4213
patricia.trinkl@ffg.at

Mag. Daniela Hackl
Digital Europe NCP

+43 5 7755 4209
daniela.hackl@ffg.at

Österreichische Forschungsförderungsgesellschaft
Sensengasse 1, A-1090 Wien

NCC-AT Services



NCC-AT Website

- Förderatlas
- Veranstaltungsspiegel



Webinare & Infosessions



Financial Support to Third Parties



Community Events



Teilnahme in Working Groups



Cybersecurity in the DIGITAL Europe Programme

- Beratung zu Ausschreibungen
- Proposal Checks
- Webinare
- Matchmaking



Newsletter






Kontakt



ncc@bka.gv.at

ncc@ffg.at

Förderatlas auf der NCC-AT Webseite

Förderprogramm	Ausschreibung	Zielgruppe	Kurzbeschreibung	Einreichfrist
Horizon Europe - Cluster 3: Zivile Sicherheit	 PQ-REACT: Open Call 2 - IMPLEMENT (Kaskadenfinanzierung)	KMU, Start-ups, Universitäten, Forschungseinrichtungen, NGOs, Vereine	Das EU-Projekt PQ-REACT unterstützt den Übergang zu quantensicheren Verschlüsselungen. In der aktuellen Ausschreibung werden Konsortien gesucht, in denen mindestens ein KMU beteiligt ist. Gefördert werden innovative Lösungen zur Post-Quantum Cryptography. Zur Auswahl stehen vier Use Cases: Smart Grid Meters, 5G/6G-Architekturen, PQC-Benchmarking und Eclipse-Qrisp. Ziel ist es, klassische kryptographische Verfahren durch quantensichere Alternativen zu ersetzen.	27.5.2025
FFG - Skills Scheck	 Skills Scheck 2025	Unternehmen mit Niederlassung in Österreich	Mit den Skills Checks soll Unternehmen mit einer Niederlassung in Österreich ein niederschwelliger Zugang zu einem Zuschuss für Qualifizierungsmaßnahmen ermöglicht werden. Die Weiterbildung muss inhaltlich dem Aufbau digitaler und/oder ökologisch nachhaltiger Kompetenzen dienen	Laufende Einreichung.
FFG - Diversity Scheck	 Diversity Scheck 2024	KMU mit Bedarf an Menschen in F&E, im Bereich Naturwissenschaften und Technik, mit Betriebsstätte oder Niederlassung in Österreich	Vielfalt unter den Mitarbeitenden und eine inklusive Kultur gehören zu den wichtigsten Treibern für Innovation im Unternehmen. Der Diversity Scheck zielt darauf ab, mit einzelnen, klein dimensionierten Maßnahmen schnelle eine positive Veränderung hin zu mehr Vielfalt im Unternehmen zu bewirken. Sie können aus folgenden Themen wählen: Diversity Analyse, Aufbau von Diversity Kompetenz, Recruiting & Human Resources, Mentoring, Gender Equality Plan. In einer offenen Kategorie können Sie entscheiden, was für Ihr Unternehmen am sinnvollsten wäre.	31.10.2025



Veranstaltungsübersicht auf der NCC-AT Webseite

Veranstaltung	Datum Start	Datum Ende	Ort
Privacy Symposium 2025 (supported by ECSO)	12. Mai 2025	16. Mai 2025	Venedig, Italien
Security Forum 2025	13. Mai 2025	14. Mai 2025	Hagenberg
NCC-AT Community Event: Innovation in der Cybersicherheit - Von der Forschung in den Markt	15. Mai 2025	15. Mai 2025	Wien
Lagebild Cyber Security 2025	20. Mai 2025	20. Mai 2025	Neuhaus, Kärnten
Cybersec Europe 2025	21. Mai 2025	22. Mai 2025	Brüssel, Belgien
The ECSO Award Finals 2025	21. Mai 2025	22. Mai 2025	Den Haag, Niederlande
Information Security Day 2025 - Strengthening Cyber Resilience in SMEs	28. Mai 2025	28. Mai 2025	Hybrid (Turku, Finnland und Online)
Invest4Cyber Networking Night 2025	4. Juni 2025	4. Juni 2025	Berlin, Deutschland
IDSF - International Digital Security Forum Vienna	4. Juni 2025	6. Juni 2025	Wien
IT-S NOW Konferenz 2025	5. Juni 2025	6. Juni 2025	Wien
CYBERSEC Expo & Forum 2025 (kostenpflichtig)	11. Juni 2025	12. Juni 2025	Krakau, Polen
Cybercrime Forum Wien	12. Juni 2025	12. Juni 2025	Wien
IKT-Sicherheitskonferenz 2025	25. Juni 2025	26. Juni 2025	Dornbirn
The ECSO Days 2025	25. Juni 2025	26. Juni 2025	Brüssel, Belgien
CyberWizards 2025 - Cybersecurity Camp für Mädchen im Alter von 13-16 Jahren	11. August 2025	16. August 2025	Kehtna, Estland
Cybercrime Forum Salzburg	18. September 2025	18. September 2025	Salzburg



Vielen Dank für Ihre Aufmerksamkeit!



K-PASS CYBERSICHERHEIT

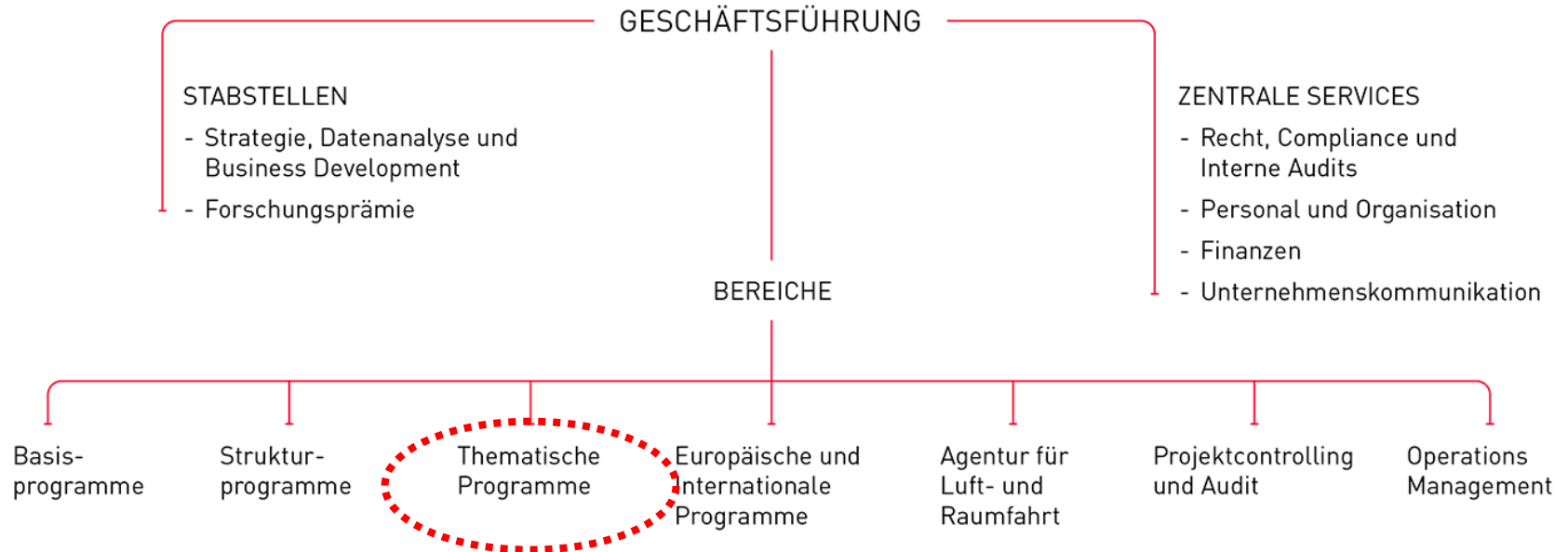
P. Wilhelm, J. Scheer

NCC-AT-Community Event 2025 | 15.05.2025 | Wien




FFG » WIRKT DURCH STANDARDS » DIE AUFTRAGGEBER FFG





SICHERHEITSKLAMMER – DREI PROGRAMME



 **Bundesministerium**
Finanzen



SICHERHEITSKLAMMER – EIN AUFTRAG

- Die Unterstützung (primär) österr. Unternehmen und Forschungseinrichtungen bei der Entwicklung neuer Technologien und der Schaffung des erforderlichen Wissens, um die Sicherheit Österreichs zu erhöhen und Wertschöpfung zu generieren
- Durch die staatliche Beihilfe sollen marktnahe Forschungsergebnisse für Sicherheitsanwender geschaffen werden, die in einem weiteren Schritt als Produkte und Dienstleistungen von den Bedarfsträgern beschafft werden können
- Programmeigentümer seit 2022 ist das BMF (finanziell und organisatorisch)
- Strategische Abstimmung erfolgt im Rahmen eines Lenkungsausschusses
- Das Programm-Management wird durch die FFG durchgeführt

SICHERHEITSKLAMMER – DREI PROGRAMME

Budget
ca. 20 Mio.
EUR/Jahr



Zivile Sicherheitsforschung

Zivile Sicherheitsthemen inkl. Dual-use; Seit 2006



Cybersecurity

Erstmalige Etablierung eines vollständig auf Cybersicherheit ausgelegten Forschungsförderungsinstrumentes in Österreich; Seit 2023



Verteidigungsforschung

Militärische Sicherheitsthemen (kein Dual-Use!); Seit 2018

SICHERHEITSKLAMMER – K-PASS

Budget
ca. 5 Mio.
EUR/Jahr




Cybersecurity

Erstmalige Etablierung eines vollständig auf Cybersicherheit ausgelegten Forschungsförderungsinstrumentes in Österreich; Seit 2023

K-PASS - CYBERSICHERHEIT

K-PASS Sonderrichtlinie

- K-PASS: „Kybernet-Pass“
- Unter der Programmverantwortung des Bundesministeriums für Finanzen (BMF)
- Unterstützt nationale Forschungsvorhaben mit dem Ziel der Erhöhung der digitalen Sicherheit Österreichs und seiner Bevölkerung
- Erstmalige Etablierung eines vollständig auf Cybersicherheit ausgelegten Forschungsförderungsinstrumentes in Österreich

 Bundesministerium
Finanzen

Sonderrichtlinie Kybernet-Pass für die Österreichische Forschungsförderungsgesellschaft mbH zur Förderung von digitaler Sicherheitsforschung (Kybernet-Pass-Sonderrichtlinie)

des Bundesministers für Finanzen

Laufzeit 1.8.2023 bis 31.12.2026

Wien, Juli 2023

K-PASS ZIELE

K-PASS Sonderrichtlinie

- Ziel 1: Erhöhung der Cyber-Sicherheit und des digitalen Sicherheitsbewusstseins der Bürgerinnen und Bürger
- Ziel 2: Generierung der für die Erreichung der sicherheitspolitischen Ziele Österreichs erforderlichen F&E-Ergebnisse im digitalen Bereich
- Ziel 3: Erzielung von Wissens-, Verfahrens- und Technologiesprüngen in der digitalen Sphäre
- Ziel 4: Wachstum der heimischen Sicherheitswirtschaft
- Ziel 5: Auf- und Ausbau von Exzellenz im Bereich der digitalen Sicherheitsforschung
- Ziel 6: Berücksichtigung gesellschaftlicher Fragestellungen in allen Aspekten digitaler Sicherheitsforschung

SCHWERPUNKT DER FÖRDERAKTIVITÄTEN IN K-PASS

K-PASS Sonderrichtlinie

- Sicherheit von „security“-relevanter Software
- Sicherheit von „security“-relevanter Hardware
- Schutz für IoT-Anwendungen und Netze
- Cyber Crime und Digitale Forensik
- E-Government-Schutz (inkl. Aufrechterhaltung des Vertrauens in der Bevölkerung)
- Steganografie und digitale Datenanalyse (z.B. Post-Quantenverschlüsselung)
- Der User als Teil der digitalen Dimension (inkl. Datensicherheit, Cyber-Stalking, Cyber-Mobbing)
- Sicherheit und Künstliche Intelligenz
- Hybride Bedrohungen
- Schutz für IKT-Systeme als „smarte“ kritische Infrastruktursysteme (z.B. autonome Mobilität, smarte Strom- und sonstige Versorgungsnetze) inkl. Resilienz, Versorgungssicherheit und Vertrauensüberprüfung (vor allem Themen für Breitbandausbau und 5G/6G-Netze)

K-PASS UND DIE FFG INSTRUMENTE

Kooperative F&E Projekte

- Kooperationen mehrerer Konsortialpartner, die in einem gemeinsamen Projekt mit definierten F&E Zielen zusammenarbeiten
- Das Vorhaben wird im Bereich der Forschungskategorie industrielle Forschung oder experimentelle Entwicklung durchgeführt
- Wettbewerbsverfahren
- Beantragte Förderung bis max. 2 Mio. EUR
- Förderungsquote: max. 85%
- Laufzeit: max. 24 Monate (und 12 Monate max. kostenneutrale Fristerstreckung)
- [Leitfaden für Kooperative F&E-Projekte \(v5.0\)](#)

F&E-Dienstleistungen

- Definiert durch die Erfüllung eines vorgegebenen Ausschreibungsinhaltes in einem bestimmten Zeitraum
- Das Angebot muss die ausgeschriebenen Leistungsinhalte adäquat darstellen und mittels plausiblen Kostenplan unterlegen
- Wettbewerbsverfahren
- Finanzierung: 100 000-300 000 EUR inkl. ev. Ust
- Finanzierungsquote: 100%
- Laufzeit: max. 24 Monate (und 12 Monate max. kostenneutrale Fristerstreckung)
- [Leitfaden für Forschungs- und Entwicklungsdienstleistungen \(v5.0\)](#)

KOOPERATIVE F&E PROJEKTE

Was sind die Anforderungen an das Konsortium?

- Voraussetzung Konsortium (mindestens 1+1+1(+1))
 - mindestens ein Bedarfsträger aus dem öffentlichen oder privaten Bereich als Konsortialteilnehmer
 - mit mindestens einem Partner aus der Wissenschaft (universitäre oder außeruniversitäre Forschungseinrichtung) als Konsortialteilnehmer und
 - einem Partner aus der Wirtschaft als Konsortialteilnehmer sowie
 - einem Vertreter der Geistes-, Sozial- und Kulturwissenschaften (GSK) als Konsortialteilnehmer oder Subauftragnehmer des Konsortiums

Ausländische Partner können bis zu 20% der Gesamtförderung gefördert werden.

KIRAS/K-PASS KMU-INITIATIVE INNOVATION AKUT

F&E-Dienstleistung mit folgenden Einschränkungen:

- Einreichungen im Bereich TRL 6-8
- Maximale Vertragssumme EUR 100.000.- inkl. ev. UST
- Laufzeit max. 12 Monate
- Konsortialvorschrift: Die BIEGE/ARGE muss aus mindestens einem österreichischen KMU und mindestens einem Bedarfsträger bestehen
- Ausländische Partner können im Konsortium teilnehmen, allerdings keine Finanzierung erhalten
- Ausländische Partner im Antrag als Drittleister: eine Teilnahme ist möglich (max. 20% der Kosten)
- Finanzierungsquote 100 %

Budget
max. 1 Mio. EUR

mehrmals im Jahr
(nächste Ausschreibung
in Planung, Juni 2025)

WEITERFÜHRENDE LINKS

- FFG Sicherheitsforschung: <http://www.ffg.at/sicherheitsforschung>
- BMF Website: <https://www.bmf.gv.at/themen/Sicherheit-Technologie.html>
- FFG: <https://www.ffg.at/>
- KIRAS Webseite: <https://www.kiras.at/>
- Cybersecurity K-PASS: <http://www.ffg.at/k-pass>
- Projektpartnersuche: KIRAS Sicherheitsforschungslandkarte: <https://www.kiras.at/landkarte/>
- Suche nach thematisch verwandten Projekten: <https://www.kiras.at/geofoerderte-projekte/>
- eCall: <https://ecall.ffg.at>
- eCall Tutorial: <https://ecall.ffg.at/Cockpit/Tutorial.aspx>
- KIRAS/K-PASS KMU Initiative Innovation AKUT: <https://www.ffg.at/kiras-k-pass-innovation-akut>
- Kostenleitfaden (Version 3.1):
<https://www.ffg.at/sites/default/files/downloads/Kostenleitfaden%20Version%203.1%20%28barrierefrei%29.pdf>

ALLGEMEINE INFORMATION

- **KIRAS/K-PASS Ausschreibung 2025: in Planung**
- **KIRAS/K-PASS Informationsveranstaltung zu der Ausschreibung 2025: in Planung**
- Beratungsgespräche
- Terminvereinbarungen: in schriftlicher Form an sicherheit@ffg.at
- Projektskizzen an Bedarfsträger, spätestens November-Dezember 2025

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!



 **Bundesministerium
Finanzen**

GENIEßEN SIE DIE KAFFEPAUSE

Cyber Innovation in Action – Erfolgreiche Projekte aus Forschung & Praxis

Session 2

Maria Eichlseder, TU Graz

Gabriel K. Gegenhuber, Universität Wien, SBA Research

DI Dr. René Heinzl, CyberTrap GmbH

Lukas Helm, zero 3

Cyber Connect – Gemeinsam Innovationen für Cybersicherheit entwickeln

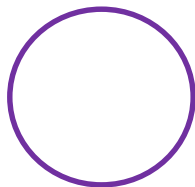
Session 3

Themen und Tisch-Hosts

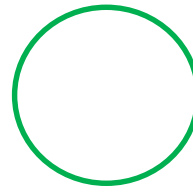
- **Artificial Intelligence** – Lydia Lindner
- **Digital Europe Programm** – Patricia Trinkl
- **Zivile Sicherheit & EDF** – Jeannette Klonk
- **Cybersicherheitsforschung Kybernet-Pass (K-PASS)** – Polina Wilhelm
- **Offene Themen** – Andrea Kindler, Annika Endres
- **Start-ups & Enterprise Europe Network** – Thomas Röblreiter

Tauschen Sie sich aus, lernen Sie sich kennen und finden Sie Ihre:n nächste:n Projektpartner:in!

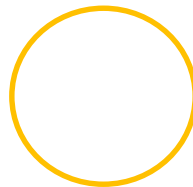
Artificial Intelligence



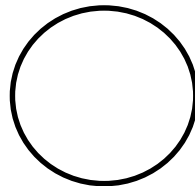
Zivile Sicherheit & EDF



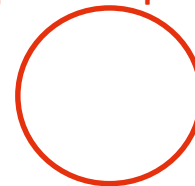
Digital Europe



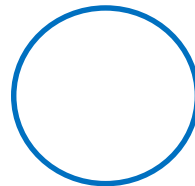
Offene Themen



**Start-ups &
Enterprise Europe Network**



**Cybersicherheitsforschung
& Kybernet-Pass (K-PASS)**



Eingang

GENIEßEN SIE DIE MITTAGSPAUSE



NCC-AT Community Event 2025

Innovation in der Cybersicherheit:
Von der Forschung in den Markt

Wien, 15. Mai 2025

Programm

- 14:00 – 14:30 Begrüßung und Eröffnung Nachmittagsprogramm
- 14:30 – 14:45 Keynote 1: Strategische Autonomie durch europäische Innovationen in der Cybersicherheit
- 14:45 – 15:00 Keynote 2: EU Best Practice: Innovation in der Cybersicherheit – Schlüssel zur technologischen Souveränität
- 15:00 – 15:15 NCC-AT Service & Community
- 15:15 – 16:00 Paneldiskussion: Von der Forschung in den Markt: Cybersicherheitsstrukturen in Österreich
- 16:00 – 17:00 *Networking & Ausklang*



NCC-AT Community Event 2025

Innovation in der Cybersicherheit: Von der Forschung in den Markt

Mag. Gernot Goluch, stv. Leiter der Abteilung für Netz- und Informationssystemssicherheit im BMI
Dr. Henrietta Egerth, Geschäftsführerin FFG

Strategische Autonomie durch europäische Innovationen in der Cybersicherheit

Svetlana Schuster

Leiterin des Referats Cybersicherheitstechnologie und Kapazitätsaufbau in der
GD CONNECT der Europäische Kommission

EU Best Practice: Innovation in der Cybersicherheit – Schlüssel zur technologischen Souveränität

Caroline Schmidt

Programmdirektorin für die Umsetzung des EU-Cybersicherheitspakets 2020 & 2023
im Innenministerium

NCC-AT Service & Community

Mag. Hanna Wilhelmer, BA (BKA)

Strategische Ziele



Mission

- Nutzbarmachung von Forschung, Technologie und Innovation fördern & Anwendung voranbringen
- Community
- Beitrag zur Strategischen Autonomie

NCC-AT Services



NCC-AT Website

- Förderatlas
- Veranstaltungsspiegel



Newsletter



Webinare & Infosessions



Financial Support to Third Parties



Community Events



Teilnahme in Working Groups



Cybersecurity in the DIGITAL Europe Programme

- Beratung zu Ausschreibungen
- Proposal Checks
- Webinare
- Matchmaking



Beitrag bei nationalen und internationalen
Veranstaltungen



Umfrage



Organisation von Roundtables

Förderatlas

Förderprogramm	Ausschreibung	Zielgruppe	Kurzbeschreibung	Einreichfrist
Horizon Europe - Cluster 3: Zivile Sicherheit	PQ-REACT: Open Call 2-IMPLEMENT (Kaskadenfinanzierung)	KMU, Start-ups, Universitäten, Forschungseinrichtungen, NGOs, Vereine	Das EU-Projekt PQ-REACT unterstützt den Übergang zu quantensicheren Verschlüsselungen. In der aktuellen Ausschreibung werden Konsortien gesucht, in denen mindestens ein KMU beteiligt ist. Gefördert werden innovative Lösungen zur Post-Quantum Cryptography. Zur Auswahl stehen vier Use Cases: Smart Grid Meters, 5G/6G-Architekturen, PQC-Benchmarking und Eclipse-Qrisp. Ziel ist es, klassische kryptographische Verfahren durch quantensichere Alternativen zu ersetzen.	27.5.2025
FFG - Skills Scheck	Skills Scheck 2025	Unternehmen mit Niederlassung in Österreich	Mit den Skills Schecks soll Unternehmen mit einer Niederlassung in Österreich ein niederschwelliger Zugang zu einem Zuschuss für Qualifizierungsmaßnahmen ermöglicht werden. Die Weiterbildung muss inhaltlich dem Aufbau digitaler und/oder ökologisch nachhaltiger Kompetenzen dienen	Laufende Einreichung.
FFG - Diversity Scheck	Diversity Scheck 2024	KMU mit Bedarf an Menschen in F&E, im Bereich Naturwissenschaften und Technik, mit Betriebsstätte oder Niederlassung in Österreich	Vielfalt unter den Mitarbeitenden und eine inklusive Kultur gehören zu den wichtigsten Treibern für Innovation im Unternehmen. Der Diversity Scheck zielt darauf ab, mit einzelnen, klein dimensionierten Maßnahmen schnelle eine positive Veränderung hin zu mehr Vielfalt im Unternehmen zu bewirken. Sie können aus folgenden Themen wählen: Diversity Analyse, Aufbau von Diversity Kompetenz, Recruiting & Human Resources, Mentoring, Gender Equality Plan. In einer offenen Kategorie können Sie entscheiden, was für Ihr Unternehmen am sinnvollsten wäre.	31.10.2025

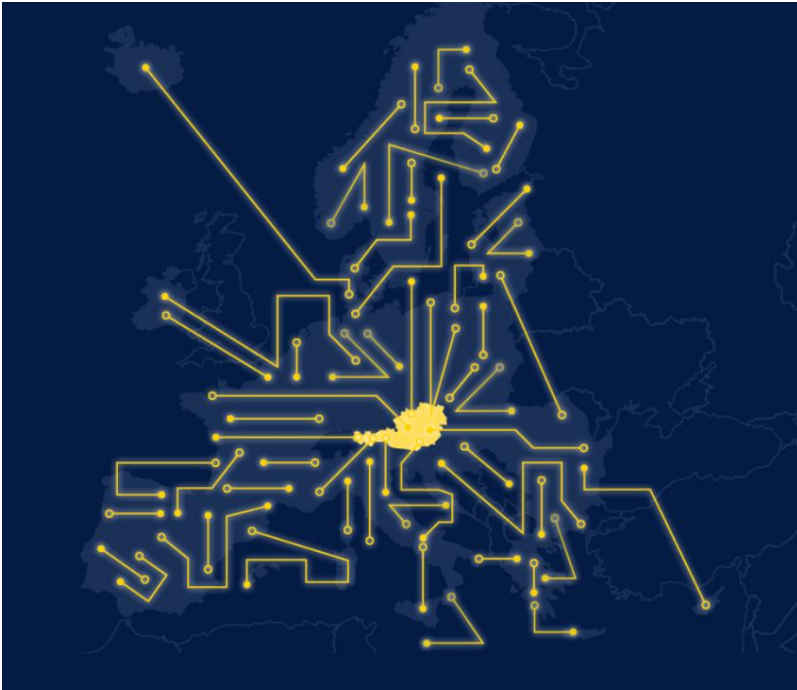


Veranstaltungsspiegel

Veranstaltung	Datum Start	Datum Ende	Ort
Privacy Symposium 2025 (supported by ECOSO)	12. Mai 2025	16. Mai 2025	Venedig, Italien
Security Forum 2025	13. Mai 2025	14. Mai 2025	Hagenberg
NCC-AT Community Event: Innovation in der Cybersicherheit - Von der Forschung in den Markt	15. Mai 2025	15. Mai 2025	Wien
Lagebild Cyber Security 2025	20. Mai 2025	20. Mai 2025	Neuhaus, Kärnten
Cybersec Europe 2025	21. Mai 2025	22. Mai 2025	Brüssel, Belgien
The ECOSO Award Finals 2025	21. Mai 2025	22. Mai 2025	Den Haag, Niederlande
Information Security Day 2025 - Strengthening Cyber Resilience in SMEs	28. Mai 2025	28. Mai 2025	Hybrid (Turku, Finnland und Online)
Invest4Cyber Networking Night 2025	4. Juni 2025	4. Juni 2025	Berlin, Deutschland
IDSF - International Digital Security Forum Vienna	4. Juni 2025	6. Juni 2025	Wien
IT-S NOW Konferenz 2025	5. Juni 2025	6. Juni 2025	Wien
CYBERSEC Expo & Forum 2025 (kostenpflichtig)	11. Juni 2025	12. Juni 2025	Krakau, Polen
Cybercrime Forum Wien	12. Juni 2025	12. Juni 2025	Wien
IKT-Sicherheitskonferenz 2025	25. Juni 2025	26. Juni 2025	Dornbirn
The ECOSO Days 2025	25. Juni 2025	26. Juni 2025	Brüssel, Belgien
CyberWizards 2025 - Cybersecurity Camp für Mädchen im Alter von 13-16 Jahren	11. August 2025	16. August 2025	Kehtna, Estland
Cybercrime Forum Salzburg	18. September 2025	18. September 2025	Salzburg



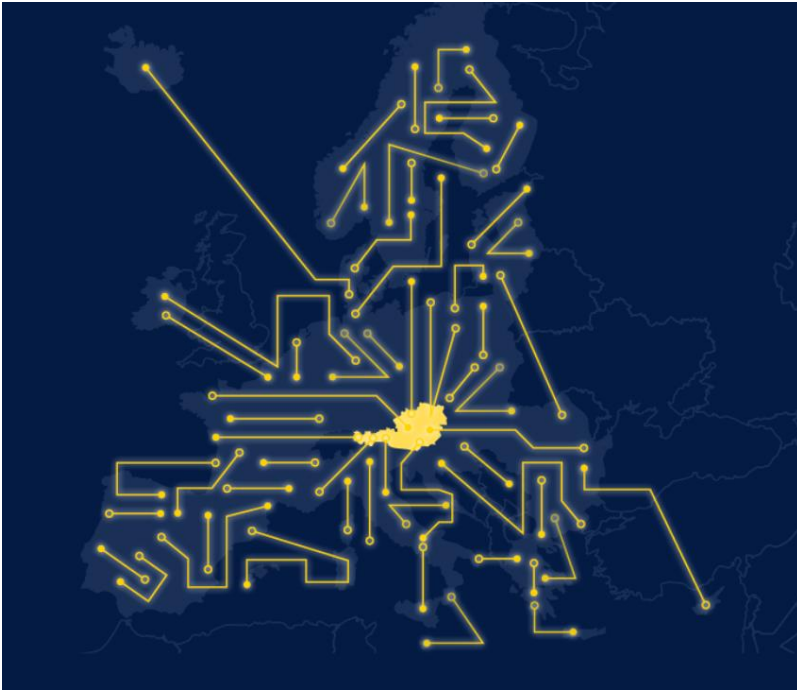
Community



NCC und ECCC

- Vernetzung
- Europäische *Kompetenzgemeinschaft für Cybersicherheit*
- Expertise für strategische Entscheidungen

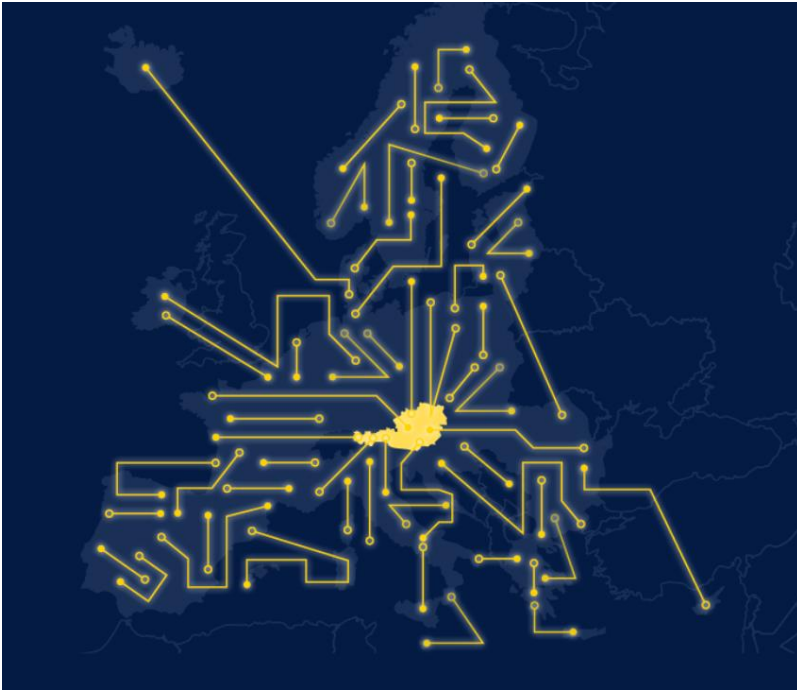
Kompetenzgemeinschaft für Cybersicherheit



Vorteile

- Internationale Sichtbarkeit
- Netzwerk- und Kooperationsmöglichkeiten
- Mitwirkung an strategischen Entscheidungen
- Zugang zu Fachwissen

Kompetenzgemeinschaft für Cybersicherheit



Aufnahmekriterien (Auswahl)

- Einrichtung (nicht Einzelpersonen)
- Niederlassung in Österreich
- Fachwissen in Cybersicherheit



Werden Sie Mitglied!
Schreiben Sie uns unter
ncc@bka.gv.at

Kontakt & Newsletter



Kontaktieren Sie uns unter

- ncc@bka.gv.at
- ncc@ffg.at

Von der Forschung in den Markt: Cybersicherheitsstrukturen in Österreich

Paneldiskussion

Von der Forschung in den Markt: Cybersicherheitsstrukturen in Österreich

Dr. Isabell Claus

thinkers.ai, Geschäftsführerin

MR Dr. Ralph Hammer

Bundesministerium für Finanzen, AL Stabstelle für Sicherheitsforschung und Technologietransfer

Dipl.sc.pol.Univ. Carolin Desirée Töpfer

Cytraction, Gründerin

Dipl.-Ing. Helmut Leopold, PhD

AIT Austrian Institute of Technology, Head of Center for Digital Safety & Security

Moderation: Marlies Hofmann, LL.M. M.Jur., Bundeskanzleramt (NCC-AT)

↓ Fragen aus dem Publikum ↓



Feedback

Wir bitten Sie um Ihr Feedback zur Veranstaltung über diesen QR-Code:





Danke für Ihre Aufmerksamkeit!

...und genießen Sie jetzt Getränke und Snacks!