HINWEIS: Frei übersetzt aus dem Englischen. Wir empfehlen als Referenz bei der Bewerbung den englischen Text zu nutzen.

Originaltext auf Englisch finden Sie in folgendem Dokument:

“Digital Europe Cybersecurity Work Programme 2025-2027“
Version 1, März 2025 herausgegeben vom ECCC

https://cybersecurity-centre.europa.eu/document/8af166e1-69c5-4ccd-b38f-5a3ffe43ad73_en

Förderbereich:	Cyber Solidarity Act implementation – European Cybersecurity Alert System
Förderthema:	2.8 Cross-Border Cyber Hubs
Seiten:	41-46

Deutsche Übersetzung des Förderthemas durch das NKCS/ NCC-DE als unterstützendes Informationsangebot erstellt:

2.8 Cross-Border Cyber Hubs

In früheren Ausschreibungen wurden die seinerzeit so benannten „Cross-Border SOC Plattformen“ gefördert. Eine ebensolche Zusammenarbeit ist für die Cross-Border Cyber Hubs vorgesehen. Diese sollen, aufbauend auf und ergänzend zu den existierenden SOCs/Cyber Hubs, Computersicherheits-Ereignis- und Reaktionsteams (Computer Security Incident Response Teams = CSIRTs), ISACs und anderen relevanten Akteuren, neue zusätzliche Kapazitäten schaffen.

2.8.1 Ziele

Diese Maßnahme richtet sich in erster Linie an neue Cross-Border Cyber Hubs. Unterstützende Maßnahmen für die SOCs, die bereits unter den früheren DIGITAL EUROPE-Ausschreibungen gefördert wurden (2021-2022 oder 2023-2024) können ebenfalls aufgenommen werden, sofern diese Maßnahmen zweckdienlich (Anm. d. Red.: Im Original wird hier das mehrdeutige Wort „relevant“ verwendet) sind, um die Zusammenarbeit mit den Cross-Border Cyber Hubs sicherzustellen.

Der Anwendungsbereich umfasst die Einrichtung von Prozessen, Tools und Dienstleistungen zur Prävention, Erkennung und Analyse von auftretenden Cyberattacken, sowie ergänzend die Akquise und / oder Einbindung üblicher (Automatisierungs-)Tools, Prozesse und gemeinsamer Dateninfrastrukturen für das Management und die EU-weite Verbreitung von kontextualisierten und umsetzbaren Cybersecurity-Einsatzinformationen.

Gut etablierte, offene Standards für CTI sharing (z.B. MISP Standard) oder Automatisierung von Warnmeldungen (z.B. CSAF) und

cybersicherheitsrelevanten Benachrichtigungen (z.B. IntelMQ) sollen berücksichtigt werden.

Die mögliche Überwachung unterseeischer Infrastruktur wie z.B. Unterseekabel könnte hierbei vorausschauend mitbedacht werden.

2.8.2 Umfang (oder Anwendungsbereich)

Die Cross-Border Cyber Hub Plattformen werden dazu beitragen, die gemeinschaftliche Lageerfassung, Detektionsfähigkeit und CTI zu verbessern und zu bündeln; sie unterstützen die Entwicklung von leistungsfähigeren Datenanalysen, Detektionen und Response-Tools, indem sie große Mengen an Daten bündeln (inklusive neuer Daten, die von den Konsortialpartnern intern generiert werden).

Die Plattformen sollen als Zentralstelle dienen, um relevante Daten und CTI breiter bündeln zu können und die höher skalierte Verbreitung von Bedrohungsinformationen innerhalb eines großen und breit aufgestellten Kreises von Akteuren (z.B. CERTs/CSIRTs, ISACs, Betreiber kritischer Infrastrukturen) zu ermöglichen.

Gemäß dem Cyber Solidarity Act sollen die Cross-Border Cyber Hubs und das CSIRT Netzwerk eng miteinander kooperieren, insbesondere zum Zweck des Informationsaustauschs. Hierfür sollen sie formale Abläufe bezüglich der Kooperation und der Verbreitung von relevanten Informationen, sowie die Art der zu verbreitenden Informationen vereinbaren.

Weiterhin könnten Cross-Border Cyber Hubs auch Lösungen für die Überwachung und den Schutz der kritischen unterseeischen Infrastruktur wie z.B. Unterseekabel und die Detektion von schädlichen Aktivitäten in deren Umfeld aufbieten, um die Resilienz und Sicherheit in dieser für die globale Kommunikation kritischen Infrastruktur zu erhöhen. Die Antwort auf diese hybriden Bedrohungen könnte zudem durch die Erfassung und Analyse von in-situ, im Meer erfassten Sensordaten sowie relevanten Satellitenbildern zur Erfassung des gesamten Lagebilds beitragen. Für diese Maßnahme werden operationale Synergien mit dem EU Copernicus Space Programme und insbesondere mit dessen Sicherheitsdienst vorausgesetzt.

Cross-Border Cyber Hubs sollen, u.a. zur Verbesserung des gemeinsamen Lagebildes, sicherstellen, dass bei potentiellen oder laufenden groß angelegten Cybersicherheitsvorfällen unverzüglich relevante Informationen sowie frühe Warnungen an die Behörden der Mitgliedsstaaten und die Kommission mittels EU-CyCLONe und CSIRT-Netzwerk herausgegeben werden.

Es wird einen Aufruf zur Interessensbekundung geben, anhand derer mehrere Entitäten in Mitgliedsstaaten ausgewählt werden, die die notwendige Ausstattung zur Verfügung stellen, um Cross-Border Cyber Hubs zur Bündelung von Daten zu Cybersicherheitsbedrohungen zwischen mehreren Mitgliedsstaaten zu betreiben.

HINWEIS: Frei übersetzt aus dem Englischen. Wir empfehlen als Referenz bei der Bewerbung den englischen Text zu nutzen.

Antragstellende auf den Aufruf zur Interessensbekundung sollten die Ziele und Zielvorgaben des Cross-Border Cyber Hubs darlegen, dessen Rolle und Verhältnis zu anderen Cybersecurity-Akteuren beschreiben sowie ggf. auf eventuelle Kooperationen mit anderen öffentlichen oder privaten Cybersecurity Stakeholdern eingehen.

Zudem sollten Antragstellende folgendes darlegen:

- Detaillierter Plan zu den angedachten Maßnahmen und Aufgaben des Cross-Border Cyber Hubs
- Informationen zur Vorgehensweise und Operationalisierung
- Hauptmeilensteine und -projektleistungen
- Informationen zu den geplanten angebotenen Dienstleistungen

Um die o.g. Aktivitäten eines Cross-Border Cyber Hubs zu fördern, sind die beiden folgenden Workstreams vorgesehen:

1. **[Procurement] Eine gemeinsame Beschaffungsmaßnahme**

   Eine gemeinsame Beschaffungsmaßnahme mit dem Mitgliedsstaat, welcher am Cross-Border Cyber Hub beteiligt ist: gefördert wird die Beschaffung von Infrastruktur, Tools und Dienstleistungen, welche für den Aufbau des Cross-Border Cyber Hubs notwendig sind.

2. **[Building up and running the Cross-Border Cyber Hub] Aufbau und Betrieb des Cross-Border Cyber Hubs**

   Zudem wird es folgende Förderungen geben:

   a) für die Vorbereitungen zur Einrichtung des Cross-Border Cyber Hubs, u.a.
      - für dessen Interaktion und Kooperation mit anderen Stakeholdern
      - sowie hierbei anfallende laufende (Betriebs-)Kosten

   b) um den effektiven Betrieb des Cross-Border Cyber Hubs zu ermöglichen, z.B.
      - die Nutzung von über gemeinsame Beschaffungsmaßnahmen erworbenen Infrastruktur-Tools und Dienstleistungen
      - Personalkosten

Hierbei sollten ebenfalls Meilensteine und Projektleistungen zur Fortschrittsanzeige benannt werden.

Bewerbungsanträge sollten für beide Workstreams gestellt werden. Bewerbungsanträge werden im Rahmen von Evaluierungsprozessen geprüft. Die Förderung wird ausschließlich für jene Anträge gewährt, für die zuvor die Evaluierung für die gemeinsame Beschaffungsmaßnahme erfolgreich verlaufen ist.

Diese Maßnahmen zielen auf die Errichtung oder Stärkung von Cross-Border Cyber Hubs, welche eine zentrale Rolle in der Gewährleistung der Cybersicherheit der nationalen Behörden, Anbieter kritischer Infrastrukturen und essentiellen Dienstleister einnehmen. Aufgrund dieser Rolle werden Cyber Hubs sensible Informationen verarbeiten.

HINWEIS: Frei übersetzt aus dem Englischen. Wir empfehlen als Referenz bei der Bewerbung den englischen Text zu nutzen.

Gemäß Artikel 22 Absatz (3) (a) der EU-Verordnung Reg (EU) 2025/38, welcher Artikel 12 der EU-Verordnung (EU) 2021/694 ergänzt, gilt:

Art 12 (5) der EU-Verordnung 2021/694 soll keine Anwendung finden, wenn alle Bedingungen des Art 12(5a) erfüllt sind. Diese lauten:

unter Berücksichtigung der Ergebnisse der gemäß Artikel 9 Absatz 4 der Verordnung (EU) 2025/38 erstellten Aufstellung besteht ein reales Risiko, dass die Instrumente, Infrastruktur oder Dienste, die erforderlich und ausreichend dafür sind, dass die betreffende Maßnahme angemessen zu den Zielen des europäischen Warnsystems für Cybersicherheit beitragen kann, von Rechtsträgern, die in einem Mitgliedstaat niedergelassen sind oder als dort niedergelassen gelten und die von einem Mitgliedstaat oder von einem Staatsangehörigen eines Mitgliedstaats kontrolliert werden, nicht zur Verfügung gestellt werden können;

das mit einer Beschaffung über solche Rechtsträger im Rahmen des europäischen Warnsystems für Cybersicherheit einhergehende Sicherheitsrisiko steht in einem angemessenen Verhältnis zu den damit verbundenen Vorteilen und steht den grundlegenden Sicherheitsinteressen der Union und ihrer Mitgliedstaaten nicht entgegen.

Derzeit laufen erste Kartierungsversuche. Bis zum Abschluss der Kartierung und im Einklang mit den Regelungen des Cyber Solidarity Act, wird die Teilnahme an den unter diesem Topic gewährten Ausschreibungen den Beschränkungen des Artikel 12(5) unterliegen, wie im Anhang 3 dieses Work Programmes dargelegt. Diese Sicherheitsvorkehrungen könnten später angepasst werden, wenn die Ergebnisse der Kartierung der Dienstleistungen nach Artikel 9(4) des Cyber Solidarity Act durch das ECCC vorliegen.

2.8.3 Zu erbringende Leistungen

- Cross-Border Cyber Hubs von Weltrang quer durch die Union wo Daten zu Cybersicherheitsbedrohungen innerhalb mehrerer Mitgliedsstaaten gebündelt werden, ausgestattet mit hochsicherer Infrastruktur und fortschrittlichen Datenanalysetools zur Detektion, Sammlung und Speicherung von Daten zu Cybersicherheitsbedrohungen, zur Analyse dieser Daten und zur Verbreitung und Berichterstattung von CTI, Prüfberichten und Analysen.
- Teilen von Threat Intelligence innerhalb der nationalen Cyber Hubs und verbindliche Vereinbarungen zur Informationsverbreitung mit kompetenten Behörden und Netzwerken, inklusive CSIRTs.

Art der Maßnahme	Aufruf zur Interessensbekundung – Call for Expression of Interest – workstream on Joint procurement with Member States
Vorläufiges Budget	*40 Mio. EUR – Die per Delegation autorisierte Behörde soll die Kontingente für die Maßnahmen nach Sektion 2.1.2 an die in den*

	erhaltenen Einsendungen angefragten Kontingente anpassen.
Vorläufige Ausschreibungsplanung	2025, 2027
Vorläufige Projektdauer	3 Jahre
Implementierung	ECCC
Zielgruppe	Körperschaften des öffentlichen Rechts, die als nationale Cyber Hubs dienen und als solche von den Mitgliedstaaten anerkannt wurden.
Sicherheit	Die Maßnahme unterliegt den Beschränkungen des Artikel 12(5) der Regulation (EU) 2021/694. Weitere Ausführungen zu den sicherheitsrelevanten Bedingungen für Fördermittel und Auftragsvergabe befinden sich in den Absätzen „third country participation“ und „procurement from non-EU entities“ dieses Dokumentes.

Art der Maßnahme	Aufruf zur Interessensbekundung – Call for Expression of Interest – workstream on Simple Grants
Vorläufiges Budget	*Wird noch definiert --. Die per Delegation authorisierte Behörde soll die Kontingente für die Maßnahmen nach Sektion 2.1.2 an die in den erhaltenen Einsendungen ange-fragten Kontingente anpassen.*
Vorläufige Ausschreibungsplanung	2025, 2027
Vorläufige Projektdauer	3 Jahre
Implementierung	ECCC
Zielgruppe	Erfolgreiche Antragstellende auf den Workstream “Joint procurement with Member States”
Sicherheit	Die Maßnahme unterliegt den Beschränkungen des Artikel 12(5) der Regulation (EU) 2021/694. Weitere Ausführungen zu den sicherheitsrelevanten Bedingungen für Fördermittel und Auftragsvergabe befinden sich in den Absätzen „third country participation“ und „procurement from non-EU entities“ dieses Dokumentes.

HINWEIS: Frei übersetzt aus dem Englischen. Wir empfehlen als Referenz bei der Bewerbung den englischen Text zu nutzen.

Das **Nationale Koordinierungszentrum für Cybersicherheit (NKCS/ NCC-DE)**

berät zu **EU-Fördermöglichkeiten in der Cybersicherheit**

und hilft bei der **Vernetzung mit EU-Partnern**.

Sie erreichen uns unter **nkcs@bsi.bund.de**