

Tecnologie dual-use

Dual-use technologies

TOPIC ID:

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-DUALUSE

Ente finanziatore:

Commissione europea
Programma Europa Digitale

Obiettivi ed impatto attesi:

Le tecnologie dual use sono emerse come un elemento fondamentale per affrontare sia le minacce alla cibersicurezza sia le più ampie esigenze di ciberdifesa. L'integrazione di tecnologie civili e militari avanzate all'interno di un quadro unificato è fondamentale per rafforzare la resilienza delle infrastrutture critiche e garantire la sicurezza dei dati. Inoltre, affrontare la criminalità informatica e le minacce ibride contribuirà a mantenere la stabilità sociale.

Sulla base del Programma Europa digitale, di Orizzonte Europa e del Fondo europeo per la difesa, l'UE deve dare priorità a progetti pilota collaborativi. I risultati di tali progetti possono creare un ponte tra i settori civile e della difesa, promuovendo innovazioni in tecnologie chiave pertinenti quali la crittografia resistente agli attacchi quantistici, le architetture Zero Trust (ZTA) e i sistemi di rilevamento delle minacce basati sull'IA. Tali sforzi sono essenziali per affrontare le minacce informatiche emergenti, garantendo al contempo l'interoperabilità e la scalabilità tra i diversi settori.

L'obiettivo è rafforzare la cooperazione tra la sfera civile e quella della difesa per quanto riguarda progetti, servizi, competenze e applicazioni a duplice uso nel settore della cibersicurezza, in linea con l'articolo 6, paragrafo 1, lettera f), del Regolamento DEP e con l'articolo 5, paragrafo 3, lettera g), del Regolamento ECCC.

Ambito di applicazione

L'obiettivo è rafforzare la cooperazione operativa tra la sfera civile e quella della difesa attraverso lo sviluppo di prototipi funzionanti a duplice uso, prodotti pronti per il mercato e infrastrutture operative connessi a tecnologie, applicazioni e strumenti di cibersicurezza rilevanti sia nel contesto civile sia in quello della difesa.

Esempi di ambiti di interesse per il presente topic della call sono:

- Crittografia resistente agli attacchi quantistici (Quantum-Safe Cryptography): sviluppare metodi di cifratura resistenti agli attacchi effettuati mediante il calcolo quantistico. Tali soluzioni garantiranno comunicazioni sicure e protezione dei dati per le infrastrutture critiche civili e militari.
- Architetture Zero Trust (ZTA): implementare quadri ZTA per rafforzare la sicurezza degli endpoint e impedire l'accesso non autorizzato ai sistemi critici. Tali architetture possono essere utilizzate sia per applicazioni civili (ad esempio, sanità e finanza) sia per sistemi di difesa.
- Rilevamento e risposta alle minacce basati sull'IA: implementare strumenti avanzati di IA per il rilevamento, la mitigazione e la risposta alle minacce in tempo reale. L'IA può essere utilizzata per il rilevamento delle anomalie nelle reti critiche, per meccanismi di difesa adattivi e per valutazioni predittive dei rischi. I sistemi di rilevamento delle minacce basati sull'IA possono rafforzare la capacità dei portatori di interesse, comprese le autorità di contrasto, di analizzare grandi insiemi di dati e individuare modelli di attività dannose. Tali sistemi consentono inoltre di attribuire priorità in tempo reale alle informazioni utilizzabili e possono supportare le indagini in diversi settori. Considerazioni di natura etica, compresa la conformità al GDPR e all'AI Act, devono guidarne l'implementazione.
- Cyber Range, compresi i gemelli digitali per la cibersicurezza: utilizzare soluzioni Cyber Range e tecnologie Digital Twin per simulare potenziali attacchi informatici contro sistemi e reti civili e militari. Ciò consente l'individuazione proattiva delle vulnerabilità e lo sviluppo di strategie di risposta efficaci. Questo rafforzerebbe le capacità di un'ampia gamma di portatori di interesse, comprese le autorità di contrasto.
- Strumenti SOAR avanzati: sviluppare piattaforme di Security Orchestration, Automation and Response (SOAR) per razionalizzare la risposta agli incidenti nei diversi settori.

Rientreranno nell'ambito del presente topic della call anche altri settori della cibersicurezza nei quali la sfera civile e quella della difesa abbiano un interesse comune nello sviluppo congiunto di sistemi funzionanti.

Gli ambiti sopra indicati dovrebbero essere dimostrati e implementati per le seguenti finalità, a titolo non esaustivo:

- Protezione delle infrastrutture critiche: ad esempio, implementare strumenti a duplice uso basati sull'IA per monitorare e proteggere infrastrutture critiche quali le infrastrutture critiche sottomarine, le reti di trasporto, le reti di comunicazione, le reti energetiche e i sistemi sanitari contro minacce informatiche e fisiche, nonché per indagare sugli incidenti.
- Comunicazioni sicure: ad esempio, utilizzare protocolli di comunicazione resistenti agli attacchi quantistici per proteggere gli scambi di dati sensibili tra portatori di interesse civili e della difesa.
- Gestione delle minacce ibride: ad esempio, progettare sistemi in grado di contrastare minacce ibride, quali il jamming e lo spoofing del GPS, il sabotaggio dei cavi e gli attacchi ransomware combinati con campagne di disinformazione, garantendo la continuità operativa.
- Estensione delle funzionalità e delle operazioni dei SOC/CSIRT compatibili con i requisiti militari. La comunità della difesa può beneficiare di più solide capacità civili di rilevamento e di consapevolezza situazionale sviluppate per la protezione delle infrastrutture critiche.

- Prevenzione delle frodi digitali e della violenza digitale per la sicurezza pubblica: ad esempio, tecnologie a duplice uso per la prevenzione delle frodi digitali, della disinformazione e del furto d'identità attraverso il monitoraggio in tempo reale e tecniche avanzate di informatica forense digitale. Tali soluzioni possono rafforzare la capacità di raccogliere e analizzare prove digitali in diverse giurisdizioni, sostenendo la protezione delle vittime e le attività delle autorità di contrasto.

Su richiesta dell'ECCC, i consorzi di progetto parteciperanno ad attività di clustering volte a definire azioni comuni e a rafforzare le sinergie tra le comunità civile e della difesa.

Risultati attesi

- Quadro per la condivisione sicura dei dati: sviluppare meccanismi di comunicazione standardizzati e cifrati per facilitare uno scambio fluido di dati tra portatori di interesse civili e militari. Tali meccanismi dovrebbero essere conformi al GDPR e agli altri requisiti normativi dell'UE.
- Sistemi di allerta precoce (EWS): istituire un EWS a livello europeo per le minacce informatiche e ibride. Tali sistemi dovrebbero integrare strumenti di monitoraggio in tempo reale e analisi predittive al fine di individuare e neutralizzare preventivamente le minacce informatiche e ibride rivolte contro le infrastrutture critiche.
- Programmi di formazione collaborativi: progettare programmi di formazione congiunti che integrino scenari relativi all'IA e alla cibersecurity sia per il personale civile (comprese le autorità di contrasto) sia per il personale militare. Tali programmi dovrebbero affrontare le esigenze specifiche dei diversi settori e gli scenari di minaccia ibrida.
- Sistemi integrati di rilevamento delle minacce: implementare sistemi unificati di rilevamento delle minacce che utilizzino IA, ZTA e gemelli digitali per applicazioni intersettoriali, rivolti alle minacce informatiche e ibride attuali ed emergenti.
- Standard di sicurezza intersettoriali: sviluppare standard armonizzati di cibersecurity per le tecnologie a duplice uso, al fine di garantire l'interoperabilità e la scalabilità tra gli Stati membri dell'UE, e proporre quadri a livello dell'UE per l'armonizzazione degli standard di cibersecurity, garantendo un'integrazione fluida delle tecnologie civili e militari.
- Collaborazione e integrazione tra i portatori di interesse: facilitare partenariati tra diversi portatori di interesse, comprese le autorità nazionali, le PMI, il mondo accademico e gli operatori industriali, al fine di promuovere l'innovazione e l'implementazione di soluzioni a duplice uso.

Criteri di eleggibilità:

Ammissibilità delle candidature

Le candidature saranno considerate ammissibili solo se il loro contenuto corrisponde interamente (o almeno in parte) alla descrizione del topic per il quale sono presentate.

Partecipanti ammissibili (Paesi ammissibili)

Per essere ammissibili, i richiedenti (beneficiari ed entità affiliate) devono:

- essere entità giuridiche (organismi pubblici o privati);
- essere stabiliti in uno dei Paesi ammissibili, vale a dire:
 - Stati membri dell'UE (compresi i Paesi e territori d'oltremare – PTOM);
 - Paesi SEE (Norvegia, Islanda, Liechtenstein).

I beneficiari e le entità affiliate devono registrarsi nel Participant Register — prima della presentazione della proposta — e dovranno essere convalidati dal Central Validation Service (REA Validation). Ai fini della convalida, sarà loro richiesto di caricare documenti attestanti lo status giuridico e l'origine.

Altre entità possono partecipare ricoprendo altri ruoli all'interno del consorzio, quali partner associati, subappaltatori, terzi che forniscono contributi in natura, ecc. (cfr. sezione 13).

Si tenga presente che tutti i topic del presente invito sono soggetti a restrizioni per motivi di sicurezza; pertanto, le entità non devono essere direttamente o indirettamente controllate da un Paese che non sia un Paese ammissibile. Tutte le entità¹⁷ dovranno compilare e presentare una dichiarazione relativa alla proprietà e al controllo.

Inoltre

- la partecipazione a qualsiasi titolo (in qualità di beneficiario, entità affiliata, partner associato, subappaltatore o destinatario di sostegno finanziario a terzi) è limitata alle entità stabilite e controllate da Paesi ammissibili;
- le attività del progetto (compresi i lavori subappaltati) devono svolgersi nei Paesi ammissibili (cfr. la sezione relativa alla localizzazione geografica di seguito e la sezione 10);
- il Grant Agreement può prevedere restrizioni in materia di diritti di proprietà intellettuale (IPR) (cfr. sezione 10).

Contributo finanziario:

Budget disponibile 10.000.000 EUR.

La disponibilità del budget della call dipende ancora dall'adozione definitiva della modifica del Programma di lavoro 2025-2027.

Forma della sovvenzione, tasso di finanziamento e importo massimo della sovvenzione

I parametri della sovvenzione (importo massimo della sovvenzione, tasso di finanziamento, costi ammissibili totali, ecc.) saranno stabiliti nella Convenzione di sovvenzione (Grant Agreement) (Scheda dati, punto 3 e articolo 5).

Budget del progetto (importo della sovvenzione richiesta)

Il contributo UE richiesto dovrebbe essere compreso tra 3 milioni di EUR e 5 milioni di EUR per progetto.

Tuttavia, potranno essere prese in considerazione anche proposte che richiedano importi diversi, purché ciò sia debitamente giustificato.

La sovvenzione concessa potrà essere inferiore all'importo richiesto.

Forma della sovvenzione e costi ammissibili

La sovvenzione assumerà la forma di una sovvenzione basata sul budget a costi effettivi misti (budget-based mixed actual cost grant: costi effettivi, con elementi basati su costi unitari e tassi forfettari).

Ciò significa che saranno rimborsate ESCLUSIVAMENTE determinate tipologie di costi (costi ammissibili) e i costi effettivamente sostenuti per il progetto (NON i costi preventivati).

Per i costi unitari e i tassi forfettari, potranno essere imputati gli importi calcolati secondo le modalità indicate nella Convenzione di sovvenzione (cfr. articolo 6 e Allegati 2 e 2a).

Tasso di finanziamento

I costi saranno rimborsati secondo il tasso di finanziamento stabilito nella Convenzione di sovvenzione.

Tipo di azione e tasso di finanziamento Simple Grants — tasso di finanziamento del 50%

Divieto di profitto

Le sovvenzioni NON possono generare un profitto, vale a dire un'eccedenza dei ricavi + sovvenzione UE rispetto ai costi.

Le organizzazioni a scopo di lucro devono dichiarare i propri ricavi e, qualora si realizzi un profitto, questo sarà dedotto dall'importo finale della sovvenzione (cfr. articolo 22.3).

Riduzione dell'importo finale della sovvenzione

Si tenga inoltre presente che l'importo finale della sovvenzione potrà essere ridotto in caso di mancato rispetto della Convenzione di sovvenzione, ad esempio in caso di attuazione non corretta, violazione degli obblighi, ecc.

Scadenza:

14 Gennaio 2027 17:00:00 Brussels time

Ulteriori informazioni:

[8e1d6074-95ed-4b23-8bd3-2ca42b096411_en](#)