Mitigare le nuove minacce e adattare le strategie investigative nell'era dell'Internet delle cose

Mitigating new threats and adapting investigation strategies in the era of Internet of Things

TOPIC ID:
HORIZON-CL3-2024-FCT-01-01

Ente finanziatore:
Commissione europea
Programma quadro Horizon Europe (HORIZON)

Obiettivi ed impatto attesi:
I risultati dei progetti devono contribuire a tutti i seguenti risultati:
- Maggiore comprensione da parte delle autorità di polizia delle minacce emergenti (digitali e soprattutto fisiche) dell'ambiente in rapido sviluppo dell'Internet degli oggetti;
- Alle autorità di polizia europee e agli altri operatori della sicurezza vengono forniti strumenti moderni per affrontare le forme di criminalità nuove ed emergenti legate allo sviluppo dell'Internet degli oggetti, che tengono conto delle norme giuridiche ed etiche di funzionamento, dei diritti fondamentali dell'UE come la privacy e la protezione dei dati personali, nonché di considerazioni di tipo costi-benefici;
- L'accesso e lo sfruttamento lecito delle prove nell'ambiente dell'Internet degli oggetti sono rafforzati;
- Le migliori pratiche (legali, organizzative, tecniche) per accedere e sfruttare l'Internet degli oggetti nel corso delle indagini sono rafforzate, anche attraverso lo sviluppo di strumenti e materiali di formazione pertinenti.
Ambito di applicazione:
L'Internet delle cose (IoT) connette praticamente tutto e rende tutto più vulnerabile. I dispositivi IoT beneficiano sempre più della convergenza e dell'integrazione di tecnologie come l'apprendimento automatico, l'analisi in tempo reale e il 5G, che fornirà connessioni più veloci e affidabili per tutti i dispositivi.
I ricercatori e le autorità di polizia hanno evidenziato una serie di implicazioni specifiche dei dispositivi IoT. Ad esempio, la vulnerabilità dei dispositivi IoT può essere sfruttata da criminali che cercano di raccogliere dati personali, compromettere le credenziali degli utenti o spiare organizzazioni o persone. Inoltre, i dispositivi IoT possono rappresentare una minaccia che va oltre il mondo digitale, ossia possono diventare una minaccia sempre più fisica, poiché trovano applicazione, ad esempio, nell'industria e nelle infrastrutture, nonché nella costruzione di città intelligenti. Anche le azioni malevole contro i dispositivi connessi con un impatto fisico diretto (ad esempio, comunicazione tra auto, hacking di veicoli, ospedali, impianti nucleari) sono una preoccupazione crescente.
Pertanto, la proposta vincente dovrà aiutare le autorità di polizia a comprendere le implicazioni dell'ambiente IoT in rapido sviluppo, al fine di tenere il passo con l'evoluzione delle sue applicazioni, riconoscere e affrontare le minacce emergenti (digitali e soprattutto fisiche) che questo può comportare. Allo stesso tempo, la proliferazione dell'IoT offrirà alle autorità di polizia e ad altri operatori della sicurezza

l'opportunità di raccogliere una nuova gamma di dati in relazione alle attività criminali. Per le autorità di polizia sono necessari nuovi schemi di indagine per accedere e sfruttare le prove dell'IoT, nel rispetto dei valori dell'UE. A tal fine, la proposta dovrebbe esaminare in che misura, ad esempio, i moderni modelli di veicoli europei, le smart TV, i sistemi di sorveglianza privata, gli assistenti virtuali o i sistemi di controllo vocale possano essere considerati fonti di prova per la raccolta e l'analisi dei dati, nonché come tali dati possano essere utilizzati per ricavare indicatori di una minaccia imminente.
La ricerca dovrebbe valutare le implicazioni legali, organizzative e tecniche dello sviluppo dell'IoT nel contesto delle indagini, comprese, ad esempio, le questioni relative alla privacy, e proporre strategie, tra cui materiali di formazione, strumenti e percorsi verso standard che favoriscano "by design" l'accesso lecito alle prove pertinenti.
In questo argomento l'integrazione della dimensione di genere (analisi del sesso e del genere) nei contenuti della ricerca e dell'innovazione dovrebbe essere affrontata solo se rilevante in relazione agli obiettivi dello sforzo di ricerca.
La proposta vincente dovrà basarsi sui risultati e sulle scoperte pubblicamente disponibili di precedenti progetti nazionali o finanziati dall'UE, nonché creare sinergie con analoghi progetti di ricerca sulla sicurezza in corso nell'ambito dei bandi 2021-2022 per la lotta alla criminalità e al terrorismo e per una maggiore sicurezza informatica, al fine di evitare duplicazioni e sfruttare le complementarietà e le opportunità di un maggiore impatto. Dovrebbero essere analizzate anche le possibilità di coordinamento con le attività correlate del Programma Europa Digitale .
Le proposte finanziate nell'ambito di questo tema devono impegnarsi con l'Europol Innovation Lab durante la durata del progetto, compresa la convalida dei risultati, con l'obiettivo di facilitare la futura adozione delle innovazioni per la comunità delle forze dell'ordine.
Condizioni specifiche dell'argomento:
Si prevede che le attività raggiungano il TRL 5-6 entro la fine del progetto - si veda l'Allegato generale B.

Criteri di eleggibilità:
Qualsiasi soggetto giuridico, indipendentemente dal suo luogo di stabilimento, compresi i soggetti giuridici di Paesi terzi non associati o di organizzazioni internazionali (comprese le organizzazioni internazionali di ricerca europee) può partecipare (indipendentemente dal fatto che sia ammissibile o meno al finanziamento), a condizione che siano state soddisfatte le condizioni stabilite dal regolamento Horizon Europe e qualsiasi altra condizione stabilita nel tema specifico del bando. Per "soggetto giuridico" si intende qualsiasi persona fisica o giuridica costituita e riconosciuta come tale ai sensi del diritto nazionale, del diritto dell'UE o del diritto internazionale, dotata di personalità giuridica e che può, agendo in nome proprio, esercitare diritti ed essere soggetta a obblighi, oppure un soggetto privo di personalità giuridica.
I beneficiari e gli enti affiliati devono registrarsi nel Registro dei Partecipanti prima di presentare la domanda, per ottenere un codice di identificazione del partecipante (PIC) ed essere convalidati dal Servizio centrale di convalida prima di firmare la convenzione di sovvenzione. Per la convalida, durante la fase di preparazione della sovvenzione, verrà chiesto loro di caricare i documenti necessari che dimostrino il loro status giuridico e la loro origine. Un PIC convalidato non è un prerequisito per presentare una domanda.
Questo tema richiede il coinvolgimento attivo, in qualità di beneficiari, di almeno 3 autorità di polizia di almeno 3 diversi Stati membri dell'UE o Paesi associati.

Se i progetti utilizzano dati e servizi di osservazione della terra, posizionamento, navigazione e/o tempistica correlati basati su satelliti, i beneficiari devono utilizzare Copernicus e/o Galileo/EGNOS (possono essere utilizzati anche altri dati e servizi).

Contributo finanziario:
Contributo UE previsto per progetto La Commissione ritiene che un contributo UE di circa 5 milioni di euro consentirebbe di affrontare adeguatamente questi risultati. Tuttavia, ciò non preclude la presentazione e la selezione di una proposta che richieda importi diversi. Budget indicativo Il budget totale indicativo per il tema è di 5,00 milioni di euro. Tipo di azione Azioni di ricerca e innovazione

Scadenza:
20 novembre 2024 17:00:00 ora di Bruxelles

Ulteriori informazioni:
wp-6-civil-security-for-society_horizon-2023-2024_en.pdf (europa.eu)