CONFINDUSTRIA

Horizon Europe

Work Programme 2021-2027

Cluster 3

Civil Security for Society

Nota di Aggiornamento

Horizon Europe

Horizon Europe è il programma dell'Unione europea per la ricerca e l'innovazione. A partire dal 2021 e fino al 2027, Horizon Europe supporterà progetti volti a raggiungere gli obiettivi individuati dagli orientamenti politici della Commissione per la programmazione 2021-2027:

- Un Green Deal europeo
- Un'Europa pronta per l'era digitale
- Un'economia al servizio delle persone
- Un'Europa più forte nel mondo
- Promuovere il nostro stile di vita europeo
- Un nuovo slancio per la democrazia europea

La struttura di Horizon Europe si articola principalmente in tre pilastri:

1) Eccellenza scientifica
2) Sfide Globali e Competitività Industriale Europea
3) Innovative Europe

Horizon Europe ha una dotazione finanziaria complessiva di 95,5 miliardi (a prezzi correnti), cifra che include i 5,4 miliardi provenienti dal piano per la ripresa Next Generation EU. Vengono finanziate attività di ricerca e innovazione attraverso inviti a presentare proposte (call for proposals) aperti e competitivi. Il programma è attuato direttamente dalla Commissione europea (gestione diretta) e dalle sue Agenzie esecutive.

Le attività di ricerca e innovazione finanziate da Horizon Europe devono concentrarsi esclusivamente su applicazioni civili.

Strutturazione del Programma di lavoro

Ogni Cluster del Pilastro 2 ha il proprio Programma di lavoro, articolato in **Destination**. Le Destination sono pacchetti di azioni coerenti tra loro (macroaree tematiche) che contribuiscono a raggiungere gli impatti attesi identificati nello Strategic Plan di Horizon Europe.[1] Ogni Destination offre una narrativa politica per le ***Call for proposals*** che propone al suo interno e che riflettono la modalità di implementazione delle Destination. All'interno di ogni Call abbiamo una lista di **Topic**, ossia argomenti specifici rispetto ai quali può essere presentato un progetto.

[1] Il piano strategico 2021-24 definisce quattro orientamenti strategici chiave (Key Strategic Orientations) per gli investimenti in ricerca e innovazione, supportati da 15 aree di impatto (impact areas), in linea con le priorità della Commissione europea. Link Strategic Plan.

Tipologie di azione e tassi di cofinanziamento

Le principali tipologie di azione in Horizon Europe sono le seguenti: [2]

RIA - Research and innovation actions: attività che mirano a sviluppare nuove conoscenze e/o esplorare la fattibilità di una tecnologia, prodotto, processo, servizio o soluzione nuovi o migliorati. Si tratta di azioni che comprendono la ricerca di base e applicata, lo sviluppo e l'integrazione della tecnologia, i test, la dimostrazione e la convalida su un prototipo su piccola scala in un laboratorio o in un ambiente simulato. Cofinanziamento al 100% dei costi eleggibili.

IA - Innovation actions: attività volte a sviluppare piani, disposizioni o progetti per prodotti, processi o servizi nuovi, alterati o migliorati, compresa la prototipazione, test, dimostrazione, pilotaggio, convalida del prodotto su larga scala e replica sul mercato. Cofinanziamento al 100% dei costi eleggibili per i soggetti no profit e 70% per i soggetti profit.

CSA - Coordination and support actions: attività generali che contribuiscono agli obiettivi del programma e che non sono attività di ricerca e innovazione in senso stretto. Cofinanziamento al 100% dei costi eleggibili.

Scheda Cluster 3 - Civil Security for Society

In questa Scheda potrete trovare una analisi riassuntiva delle Call e dei rispettivi Topic che si apriranno nei prossimi due anni all'interno del Cluster 3 "Civil Security for Society", appartenente al secondo pilastro di Horizon Europe. Il Cluster 3 si articola nelle seguenti 6 Destination:

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

Vi ricordiamo che per la presentazione dei progetti è necessario far riferimento ai Work Programme e a tutti i documenti ufficiali della Commissione europea.

[2] Sono poi identificate altre tipologie di azioni quali: Programme Co-fund Action; Innovation and Market Deployment; Training and Mobility Action; Pre-commercial procurement action; Public procurement of innovative solutions action.

SOMMARIO

Introduzione al Cluster 3

Il programma di lavoro del Cluster 3 si prefigge di sostenere le priorità politiche dell'UE in **materia di sicurezza e di riduzione del rischio di catastrofi e resilienza**. Inoltre, si baserà sugli insegnamenti tratti dalla crisi COVID-19 in termini di prevenzione, mitigazione, preparazione e sviluppo di capacità per le crisi e nel miglioramento degli aspetti intersettoriali di tali crisi.

Esso sosterrà le priorità politiche della Commissione europea "Promoting the European way of life", lo "European Green Deal" e "Europe fit for the digital age". In particolare, sosterrà l'attuazione della strategia dell'UE per l'Unione della sicurezza, l'agenda antiterrorismo, la gestione delle frontiere e la dimensione della sicurezza del nuovo patto sulla migrazione e l'asilo, le politiche dell'UE per la riduzione del rischio di catastrofi, la nuova strategia dell'UE per l'adattamento ai cambiamenti climatici, la strategia dell'UE per la sicurezza marittima e la strategia dell'UE per la cibersicurezza.

Nel quadro del piano strategico di Horizon Europe, gli impatti previsti del Cluster 3 contribuiranno in particolare alle aree d'impatto: *"Un'UE resiliente preparata alle minacce emergenti"* e *"Una società dell'UE sicura, aperta e democratica"* dell'orientamento strategico fondamentale (Key Strategic Orientation, KSO[3]) D "Creare una società europea più resiliente, inclusiva e democratica"; *"Tecnologia digitale sicura e cybersicura"* del KSO A "Promuovere un'autonomia strategica aperta guidando lo sviluppo di tecnologie, settori e catene del valore digitali chiave, abilitanti ed emergenti".

I progetti inoltre svilupperanno nuove conoscenze, tecnologie e/o altre soluzioni per soddisfare i requisiti identificati. I progetti coinvolgeranno gli utenti finali professionisti, ricercatori e industria. I progetti dovranno garantire risultati etici che siano sostenuti dalla società: è particolarmente importante che i progetti tengano conto dei fattori umani e del contesto sociale, e assicurino il rispetto dei diritti fondamentali, compresa la privacy e la protezione dei dati personali.

Per quanto riguarda la cooperazione internazionale, la ricerca sulla sicurezza nell'ambito del Cluster 3 richiede un approccio specifico per raggiungere il giusto equilibrio tra la necessità di scambio con i principali partner internazionali e allo stesso tempo garantire la

[3] Key Strategic Orientation: gli orientamenti strategici forniscono le linee guida ai programmi di lavoro di Horizon Europe e si pongono come base per costruire sinergie con altri programmi europei.

protezione, assicurando al tempo stesso la protezione degli interessi di sicurezza dell'UE e rispettando la necessità di un'autonomia strategica aperta nei settori critici.

In Horizon Europe si presterà particolare attenzione alla cooperazione tra le università, le comunità scientifiche e l'industria, nonché con i cittadini e i loro rappresentanti. Horizon Europe incoraggia le sinergie con altri programmi dell'UE rilevanti per la R&I.

Le sinergie con altri fondi dovrebbero anche essere articolate in modo da accelerare l'assorbimento da parte del mercato dei risultati positivi delle azioni di R&I. Le azioni nell'ambito di Horizon Europe dovrebbero concentrarsi esclusivamente sulle applicazioni civili, si dovrebbero cercare sinergie con le attività finanziate nell'ambito del Fondo europeo per la difesa, evitando la duplicazione. Inoltre, si possono cercare sinergie con il meccanismo di protezione civile dell'Unione (Union Civil Protection Mechanism, UCPM), anche attraverso opportunità come la rete di conoscenze della protezione civile dell'Unione (Union Civil Protection Knowledge Network), i progetti di prevenzione e preparazione (Prevention & Preparedness projects), lo sviluppo di ulteriori capacità di riserva nell'ambito di rescEU per le catastrofi gravi e simultanee, e cofinanziando il dispiegamento delle capacità di risposta nazionali degli Stati membri.

I progetti finanziati nell'ambito delle destinazioni di questo Cluster sono invitati a cooperare strettamente con altre iniziative presiedute o finanziate dalla CE nei settori pertinenti, come i Networks of Practitioners finanziati nell'ambito dei programmi di lavoro H2020 Secure Societies, i Knowledge Networks for Security Research & Innovation finanziati nell'ambito del programma di lavoro Cluster 3 di Horizon Europe (destinazione "Ricerca e innovazione rafforzate in materia di sicurezza"), o la Community of Users for Secure, Safe and Resilient Societies (futura CERIS - Community of European Research and Innovation for Security). Si incoraggiano le sinergie anche con altri gruppi di lavoro per la ricerca e l'innovazione in materia di sicurezza istituiti dalle agenzie dell'UE e con altre reti di conoscenze istituite dai servizi della Commissione europea.

Inoltre, le proposte di successo nell'ambito di questo Cluster dovrebbero essere complementari e non sovrapporsi con le azioni pertinenti finanziate da altri strumenti dell'UE, compresi i progetti finanziati dal programma Europa digitale, nonché dal Fondo europeo di difesa e dal programma europeo di sviluppo industriale della difesa, mantenendo un focus solo sulle applicazioni civili. Le conoscenze e tecnologie sviluppate nell’ambito di questo Cluster potranno essere riprese da altri strumenti, come il Fondo per la gestione integrata delle frontiere, che permetteranno lo sfruttamento dei risultati della ricerca e la consegna finale degli strumenti necessari agli operatori della sicurezza.

Le proposte che riguardano l'osservazione della terra sono incoraggiate a fare uso principalmente dei dati, dei servizi e delle tecnologie di Copernicus.

Inoltre, al fine di realizzare gli obiettivi delle destinazioni di questo cluster, sono state definite ulteriori condizioni di ammissibilità per quanto riguarda il coinvolgimento attivo dei professionisti della sicurezza o degli utenti finali interessati.

Questo programma di lavoro comprende sei destinazioni che si basano sulla struttura dei programmi di lavoro di Horizon 2020 per la ricerca sulla sicurezza.

1. Destination 1: Better protect the EU and its citizens against Crime and Terrorism

Uno degli scopi principali della presente destinazione è quello **di contribuire in modo significativo all'attuazione della strategia dell'Unione della sicurezza, ovvero utilizzare ricerca e innovazione come uno degli elementi chiave per raggiungere gli obiettivi politici generali**. Come tale, i topic di questa destinazione mirano ad affrontare pienamente tutte le questioni chiave sottolineate nella strategia. Inoltre, questa destinazione tocca l'agenda antiterrorismo e la dimensione della sicurezza del nuovo patto sulla migrazione e l'asilo, in particolare le questioni relative alle reti criminali. Più specificamente, questa destinazione comprende temi di ricerca che mirano a combattere il crimine e il terrorismo in modo più efficace, in particolare attraverso una migliore prevenzione del crimine e maggiori capacità investigative, una migliore protezione dei cittadini da attacchi violenti negli spazi pubblici. Questa destinazione svilupperà le conoscenze e le tecnologie che saranno riprese dal Fondo per la sicurezza interna, come uno strumento complementare che permetterà lo sfruttamento dei risultati della ricerca e la consegna finale degli strumenti necessari ai professionisti della sicurezza.

L'obiettivo di questa destinazione è quello di **migliorare la prevenzione, l'indagine e l'attenuazione degli impatti della criminalità, compresi i nuovi/emergenti modi di operare criminali** (come quelli che sfruttano la digitalizzazione e altre tecnologie). Tale approccio deve essere basato su una conoscenza più profonda degli aspetti umani e sociali delle sfide sociali rilevanti. La ricerca può inoltre contribuire a trasporre tali conoscenze nelle attività operative delle autorità di polizia e delle organizzazioni della società civile. La ricerca sosterrà le capacità di analizzare in tempo quasi reale grandi volumi di dati per prevenire le attività criminali, o per combattere la disinformazione e le fake news con implicazioni per la sicurezza. I progetti nell'ambito di questa destinazione forniranno strumenti operativi per migliorare le capacità di indagine criminale per le autorità di polizia e, se del caso, altri utenti finali pertinenti. Pertanto, questa destinazione copre una vasta gamma di attività, dalla scienza forense, alla gestione dei big data, alle indagini sulle attività dei criminali informatici, al miglioramento della cooperazione transfrontaliera e allo scambio di prove.

Per quanto riguarda le minacce CBRN-E (chimiche, biologiche, radiologiche, nucleari ed esplosive), la ricerca e l'innovazione all'interno di questa destinazione permette di generare conoscenze per l'antiterrorismo sui metodi in continua evoluzione relativi a sostanze chimiche pericolose, contaminanti e sostanze sconosciute, e lo sviluppo di tecnologie per contrastare e rispondere ai relativi incidenti.

Inoltre, questa destinazione mira a migliorare la sicurezza degli spazi pubblici e la sicurezza pubblica, preservando allo stesso tempo la natura aperta degli spazi pubblici urbani. Per raggiungere una maggiore sicurezza dello spazio pubblico, la ricerca in questa destinazione identificherà concetti per la prevenzione, la preparazione e la risposta degli attori urbani alle minacce di attacchi terroristici negli spazi pubblici. Le innovazioni possono essere usate per progettare spazi pubblici più sicuri e aumentare la capacità di proteggere gli spazi da attacchi con veicoli e rilevare armi da fuoco e altre armi, così come materiali CBRN-E che vengono portati negli spazi pubblici. Nel caso in cui gli attacchi non possano essere prevenuti, una maggiore efficacia delle misure di mitigazione ha il potenziale per ridurre gli impatti potenziali di tali attacchi. L'analisi avanzata dei dati in tempo reale può ridurre criticamente il tempo di reazione per i primi soccorritori.

Questa Destinazione promuoverà anche le proposte con:

- il coinvolgimento delle autorità di polizia nel loro nucleo,
- una chiara strategia su come si adatteranno all'ambiente in rapida evoluzione nell'area della lotta al crimine e al terrorismo,
- una piattaforma minimamente necessaria, cioè strumenti che sono modulari e possono essere facilmente inseriti in un'altra piattaforma,
- strumenti che sono sviluppati e validati rispetto ai bisogni e alle esigenze dei professionisti,
- un piano solido su come si costruiranno sui progetti precedenti,
- il coinvolgimento (attivo) di cittadini, organizzazioni di volontariato e comunità,
- aspetti di istruzione e formazione, specialmente per le autorità di polizia e altri operatori del settore, così come la condivisione delle informazioni e la sensibilizzazione dei cittadini,
- una chiara strategia sull'adozione dei risultati,
- un piano ben sviluppato sia su come saranno ottenuti i dati di ricerca per la formazione e i test, al fine di raggiungere i livelli di preparazione della tecnologia (Technology Readiness Levels, TRL) richiesti, sia su come sarà misurato il TRL specifico.

La Destinazione 1 creerà anche opportunità di collaborazione per la ricerca e l'innovazione tra diverse comunità di professionisti che operano nel settore della lotta al crimine e al terrorismo. La cooperazione internazionale è incoraggiata dove appropriato e pertinente.

In particolare, le proposte dovrebbero contribuire al raggiungimento di uno o più dei seguenti impatti:

- Analisi moderna delle informazioni per le autorità di polizia;
- Miglioramento della scienza forense e della raccolta di prove legali;
- Miglioramento della prevenzione, dell'individuazione e della deterrenza dei problemi sociali legati a varie forme di criminalità e al terrorismo;
- Maggiore sicurezza dei cittadini contro il terrorismo, anche negli spazi pubblici;
- Miglioramento del quadro di intelligence e maggiore prevenzione, individuazione e deterrenza delle varie forme di criminalità organizzata;
- Un cyberspazio più sicuro per i cittadini, attraverso una solida prevenzione, individuazione e protezione dalle attività cybercriminali.

I seguenti inviti in questo programma di lavoro contribuiscono a questa destinazione.

1.1 Call - Fighting Crime and Terrorism 2021

Destination Better protect the EU and its citizens against Crime and Terrorism

Call: HORIZON-CL3-2021-FCT-01

Topics	Tipologia di azione	Budget totale (milioni di euro) 2021	Contributo UE previsto per progetto (milioni di euro)[4]	Numero di progetti che si prevede di finanziare
Apertura: 30 giugno 2021 Deadline(s): 23 novembre 2021				
HORIZON-CL3-2021-FCT-01-01: Terrorism and other forms of serious	IA	16.00	Circa 5.00	1

[4] Tuttavia, questo non preclude la presentazione e la selezione di una proposta che richiede importi diversi.

crime countered using travel intelligence				
HORIZON-CL3-2021-FCT-01-03: Disinformation and fake news are combated and trust in the digital world is raised	IA		Circa 4.00	1
HORIZON-CL3-2021-FCT-01-04: Improved access to fighting crime and terrorism research data	IA		Circa 7.00	1
HORIZON-CL3-2021-FCT-01-02: Lawful interception using new and emerging technologies (5G & beyond, quantum computing and encryption)	RIA	5.00	Circa 5.00	1
HORIZON-CL3-2021-FCT-01-05: Modern biometrics used in forensic science and by police	IA	5.00	Circa 5.00	1
HORIZON-CL3-2021-FCT-01-06: Domestic and sexual violence are prevented and combated	IA	6.00	Circa 3.00	2
HORIZON-CL3-2021-FCT-01-07: Improved preparedness on attacks to public spaces	IA	3.00	Circa 3.00	1
HORIZON-CL3-2021-FCT-01-08: Fight against trafficking in cultural goods	RIA	5.00	Circa 5.00	1
HORIZON-CL3-2021-FCT-01-09: Fight against organised environmental crime	IA	10.00	Circa 5.00	1
HORIZON-CL3-2021-FCT-01-10: Fight against firearms trafficking	IA		Circa 5.00	1
HORIZON-CL3-2021-FCT-01-11: Prevention of child sexual exploitation	RIA	6.00	Circa 3.00	1
HORIZON-CL3-2021-FCT-01-12: Online identity theft is countered	RIA		Circa 3.00	1

Budget indicativo complessivo		56.00		

1.2 Call - Fighting Crime and Terrorism 2022

Destination Better protect the EU and its citizens against Crime and Terrorism

Call: HORIZON-CL3-2022-FCT-01

Topics	Tipologia di azione	Budget totale (milioni di euro) 2022	Contributo UE previsto per progetto (milioni di euro)[5]	Numero di progetti che si prevede di finanziare
Apertura: 30 giugno 2022 Scadenza: 23 novembre 2022				
HORIZON-CL3-2022-FCT-01-01: Improved crime scene investigations related to transfer, persistence and background abundance	IA	7.00	Circa 7.00	1
HORIZON-CL3-2022-FCT-01-02: Better understanding the influence of organisational cultures and human interactions in the forensic context as well as a common lexicon	RIA	3.00	Circa 3.00	1
HORIZON-CL3-2022-FCT-01-03: Enhanced fight against the abuse of online gaming culture by extremists	RIA	3.00	Circa 3.00	1
HORIZON-CL3-2022-FCT-01-04: Public spaces are protected while	CSA	3.00	Circa 3.00	1

[5] Tuttavia, questo non preclude la presentazione e la selezione di una proposta che richiede importi diversi.

respecting privacy and avoiding mass surveillance				
HORIZON-CL3-2022-FCT-01-05: Effective fight against corruption	IA	15.00	Circa 5.00	1
HORIZON-CL3-2022-FCT-01-06: Effective fight against illicit drugs production and trafficking	IA		Circa 5.00	1
HORIZON-CL3-2022-FCT-01-07: Effective fight against trafficking in human beings	IA		Circa 5.00	1
Budget indicativo complessivo		31.00		

2. Destination 2: Effective management of EU external borders

Questa destinazione affronta gli obiettivi identificati dalla strategia dell'Unione della sicurezza, nonché la gestione delle frontiere e le dimensioni della sicurezza del Nuovo Patto sulla Migrazione e l'Asilo. I topic inclusi nella destinazione mirano quindi a garantire la forza delle frontiere esterne terrestri, aeree e marittime dell'Europa. Ciò comprende lo sviluppo di forti capacità di controllo alle frontiere esterne e quindi la salvaguardia dell'integrità e del funzionamento dello spazio Schengen; essere in grado di effettuare controlli sistematici alle frontiere, pur facilitando il viaggio dei viaggiatori in buona fede e rispettando i diritti e le eventuali vulnerabilità degli individui; fornire sorveglianza integrata e continua alle frontiere, consapevolezza della situazione e supporto all'analisi; combattere le frodi in materia di identità e documenti; sostenere la tecnologia futura per la guardia di frontiera e costiera europea; sostenere l'interoperabilità e le prestazioni dei sistemi informatici di scambio e analisi dei dati dell'UE; sostenere una migliore individuazione dei rischi, la risposta agli incidenti e la prevenzione della criminalità; migliorare la preparazione dell'Europa e la gestione dei futuri cambiamenti in rapida evoluzione; e aggiornare la nostra gestione della sicurezza marittima.

Tenendo conto del ruolo centrale dell'Agenzia europea della guardia di frontiera e costiera (Frontex) nella definizione dei requisiti di capacità per la guardia di frontiera e costiera europea, essa sarà strettamente associata alla Commissione europea e la assisterà nell'elaborazione e nell'attuazione delle pertinenti attività di ricerca e innovazione. L'Agenzia

dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA), allo stesso modo, potrebbe assistere la Commissione europea sulle attività di ricerca e innovazione pertinenti e su topic specifici.

La ricerca contribuirà anche all'attuazione del sistema europeo di sorveglianza delle frontiere (European Border Surveillance System, EUROSUR) e allo sviluppo di strumenti e metodi per la gestione integrata delle frontiere.

Per quanto riguarda la sicurezza marittima, i topic di questa destinazione sosterranno anche l'attuazione delle azioni pertinenti nell'ambito dello sviluppo delle capacità, della ricerca e dell'innovazione del piano d'azione UE per la sicurezza marittima. Le attività di ricerca consentiranno pertanto di migliorare la sicurezza e la gestione delle frontiere marittime dell'UE, delle infrastrutture critiche marittime, delle attività marittime e dei trasporti, contribuendo altresì a migliorare le prestazioni e la cooperazione nelle funzioni di guardia costiera. La ricerca e l'innovazione nel settore della sicurezza marittima sosterranno anche lo sviluppo di capacità future per la protezione dei porti e delle linee di comunicazione marittima correlate. L'obiettivo delle attività di ricerca sulla sicurezza marittima a questo proposito riguarda la prevenzione, la preparazione e la risposta a eventi previsti e inaspettati. L'agenda di ricerca sulla sicurezza marittima dell'UE stabilisce a questo proposito aree specifiche da affrontare, tra cui la sicurezza informatica, l'interoperabilità e la condivisione delle informazioni, i sistemi autonomi, i sistemi di rete e di comunicazione e le piattaforme multiuso. La legislazione specifica dell'UE sulla sicurezza marittima pone anche l'accento sul trasporto marittimo di passeggeri e sulle minacce per i passeggeri. Capacità innovative e più efficienti per la sicurezza del trasporto marittimo di passeggeri potrebbero quindi essere un utile settore di ricerca.

Per quanto riguarda la sicurezza dei movimenti di merci attraverso le frontiere esterne, la ricerca risponderà alle esigenze individuate dalla Commissione europea e dalle autorità doganali dell'UE e dovrebbe contribuire alle capacità di individuare le attività illegali, sia ai punti di attraversamento delle frontiere esterne, sia lungo la catena di approvvigionamento. Le dogane hanno bisogno di innovazione per consentire il rilevamento e garantire la sicurezza senza interrompere o ostacolare inutilmente i flussi commerciali. Le capacità costruite attraverso la ricerca contribuiranno all'attuazione del nuovo piano d'azione dell'Unione doganale dell'UE per rafforzare la gestione del rischio doganale e i controlli efficaci. Le capacità includono quelle sul rilevamento delle minacce nei flussi postali; controlli automatizzati e rilevamento che riducono la necessità di aprire o fermare container, pacchetti, bagagli o merci; supporto decisionale; portabilità delle soluzioni di controllo; e tecnologie per tracciare il commercio illecito transfrontaliero.

Le proposte presentate nell'ambito di questa destinazione dovrebbero dimostrare come si costruiranno sui progetti precedenti pertinenti; di considerare le prospettive dei cittadini e

della società; di includere l'istruzione, la formazione e la sensibilizzazione dei professionisti e dei cittadini; di misurare il TRL raggiunto; e di preparare l'adozione dei risultati della ricerca.

Impatto previsto

Le proposte nell'ambito di questa destinazione dovrebbero definire un percorso credibile per contribuire al seguente impatto atteso del piano strategico di Horizon Europe 2021-2024: *"I passeggeri e le spedizioni legittime viaggiano più facilmente nell'UE, mentre i traffici illeciti, il traffico, la pirateria, il terrorismo e altri atti criminali sono prevenuti, grazie al miglioramento della gestione delle frontiere aeree, terrestri e marittime e della sicurezza marittima, compresa una migliore conoscenza dei fattori sociali".*

Più specificamente, le proposte dovrebbero contribuire al raggiungimento di uno o più dei seguenti impatti:

- Miglioramento della sicurezza delle frontiere terrestri e aeree dell'UE, così come delle frontiere marittime e dell'ambiente marittimo, delle infrastrutture e delle attività, contro incidenti, disastri naturali e sfide alla sicurezza;
- Una migliore esperienza di attraversamento delle frontiere per i viaggiatori e il personale delle autorità di frontiera, mantenendo la sicurezza e il monitoraggio dei movimenti attraverso le frontiere esterne dell'UE aeree, terrestri e marittime, sostenendo lo spazio Schengen, riducendo i movimenti illegali di persone e merci attraverso tali frontiere e proteggendo i diritti fondamentali dei viaggiatori;
- Miglioramento della sicurezza delle dogane e della catena di approvvigionamento attraverso una migliore prevenzione, individuazione, deterrenza e lotta contro le attività illegali che coinvolgono i flussi di merci attraverso i valichi di frontiera esterna dell'UE e attraverso la catena di approvvigionamento, riducendo al minimo le interruzioni dei flussi commerciali.

I seguenti inviti in questo programma di lavoro contribuiscono a questa destinazione.

2.1 Call - Border Management 2021

Destination Effective management of EU external borders

Call: HORIZON-CL3-2021-BM-01

Topics	Tipologia di azione	Budget totale (milioni	Contributo UE previsto	Numero di progetti

		di euro)	per progetto (milioni di euro)[6]	che si prevede di finanziare
		2021		
Apertura: 30 giugno 2021 Scadenza: 23 novembre 2021				
HORIZON-CL3-2021-BM-01-01: Enhanced security and management of borders, maritime environment, activities and transport, by increased surveillance capability, including high altitude, long endurance aerial support	IA	20.00	Circa 7.00	1
HORIZON-CL3-2021-BM-01-03: Improved border checks for travel facilitation across external borders and improved experiences for both passengers and border authorities' staff	IA		Circa 4.00	2
HORIZON-CL3-2021-BM-01-05: Improved detection of concealed objects on, and within the body of, persons	IA		Circa 5.00	1
HORIZON-CL3-2021-BM-01-02: Increased safety, security, performance of the European Border and Coast Guard and of European customs authorities	CSA	2.50	Circa 2.50	1
HORIZON-CL3-2021-BM-01-04: Advanced detection of threats and illicit goods in postal and express courier flows	RIA	8.00	Circa 4.00	2

[6] Tuttavia, questo non preclude la presentazione e la selezione di una proposta che richiede importi diversi.

Budget indicativo complessivo		30.50		

2.2 Call – Border Management 2022

Destination Effective management of EU external borders

Call: HORIZON-CL3-2022-BM-01

Topics	Tipologia di azione	Budget totale (milioni di euro) 2022	Contributo UE previsto per progetto (milioni di euro)[7]	Numero di progetti che si prevede di finanziare
Apertura: 30 Jun 2022 Scadenza: 23 Nov 2022				
HORIZON-CL3-2022-BM-01-01: Improved underwater detection and control capabilities to protect maritime areas and sea harbours	RIA	6.00	Circa 6.00	1
HORIZON-CL3-2022-BM-01-02: Enhanced security of, and combating the frauds on, identity management and identity and travel documents	IA	6.00	Circa 6.00	1
HORIZON-CL3-2022-BM-01-03: Better, more portable and quicker analysis and detection for customs	IA	6.00	Circa 3.00	2
HORIZON-CL3-2022-BM-01-04: OPEN TOPIC	RIA	3.50	Circa 3.50	1
HORIZON-CL3-2022-BM-01-05: OPEN TOPIC	IA	3.50	Circa 3.50	1

[7] Tuttavia, questo non preclude la presentazione e la selezione di una proposta che richiede importi diversi.

Budget indicativo complessivo		25.00		

3. Destination 3: Resilient Infrastructure

Il funzionamento affidabile, solido e resiliente delle infrastrutture è vitale per la sicurezza, il benessere e la prosperità economica delle persone in Europa. Le infrastrutture sono diventate più complesse per tenere il passo con lo sviluppo delle società moderne, assicurando allo stesso tempo la loro resilienza contro i disastri e gli impatti del cambiamento climatico e di altri fattori che influenzano la società, come i cambiamenti demografici. Le infrastrutture operano e funzionano in un ambiente socio-tecnologico e di minacce in rapida evoluzione, con reti sempre più interconnesse e altamente dipendenti l'una dall'altra. Devono quindi essere resilienti di fronte a diversi eventi previsti e inaspettati ed a rischi emergenti.

La strategia dell'Unione della sicurezza individua la protezione delle infrastrutture critiche come una delle principali priorità dell'UE e dei suoi Stati membri per i prossimi anni. La preparazione e la protezione delle infrastrutture è un settore tecnologicamente complesso, influenzato da vari sviluppi globali e quindi deve essere sostenuto da una ricerca mirata sulla sicurezza. Questo programma di lavoro mira a sostenere la protezione delle infrastrutture europee con progetti pertinenti, permettendo agli attori pubblici e privati di affrontare le sfide attuali ed emergenti.

Le applicazioni tecnologicamente complesse offrono la possibilità di una migliore prevenzione e preparazione, possono permettere una risposta efficiente alle diverse minacce e un recupero più veloce. Ma allo stesso tempo, creano nuove vulnerabilità. Il danno potenziale risultante dalla loro interruzione può aumentare rapidamente e influenzare negativamente parti più ampie delle funzioni vitali della società. Per esempio, questo è il caso dei sistemi di posizionamento e temporizzazione basati sui satelliti, che forniscono una ricchezza di servizi di posizionamento, navigazione e temporizzazione (Positioning, Navigation and Timing, PNT) di alta qualità che sono sfruttati da infrastrutture critiche come i trasporti e la logistica, le reti di energia, la rete di acqua potabile, le dighe, le reti di telecomunicazione o i mercati finanziari. L'interruzione o la negazione dei servizi del sistema globale di navigazione satellitare (Global Navigation Satellite System, GNSS) è riconosciuta come una rilevante minaccia economica e sociale.

Con la direttiva sull'identificazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione, l'UE e i suoi Stati membri hanno creato una base per un approccio comune alla protezione. La proposta di misure aggiuntive sulla protezione delle infrastrutture critiche, che fa parte del programma di lavoro della Commissione europea per il 2020, si avvale anche dei significativi risultati che la ricerca sulla sicurezza ha prodotto nell'ultimo decennio.

L'UE ha riconosciuto il forte ruolo della dimensione informatica nella protezione delle infrastrutture, in particolare nella direttiva sulla sicurezza delle reti e dei sistemi informativi e nella sua revisione, proposta nel dicembre 2020. L'estrazione di dati su larga scala di informazioni intersettoriali dovrebbe essere sostenuta da una ricerca mirata su tecniche e infrastrutture di IA appropriate.

Gli attacchi fisici sono meno frequenti, ma i casi nel vicinato dell'UE hanno mostrato il potenziale distruttivo delle nuove tecnologie utilizzate per gli attacchi, come gli Unmanned Aerial Vehicles (UAV), che possono essere utilizzati anche per interruzioni intenzionali che mettono in pericolo il funzionamento sicuro delle infrastrutture e creano perdite economiche significative.

Le minacce ibride sono di particolare rilevanza negli scenari di rischio complessivi, poiché sono progettate per colpire le vulnerabilità e mirano in molti casi a interrompere le infrastrutture e i loro servizi, facendo uso di metodi diversi. Le minacce ibride, le tecniche e i mezzi comprendono una combinazione di attacchi fisici e informatici o interruzioni, mezzi diplomatici, militari e politici ed economici. Gli effetti degli strumenti informatici e della disinformazione sono elementi cruciali di tali strategie e creano la necessità di una preparazione completa per evitare interruzioni su larga scala. Per questo motivo, sia il Quadro congiunto per contrastare le minacce ibride (2016), sia la Comunicazione congiunta sul rafforzamento della resilienza e potenziamento delle capacità di affrontare minacce ibride (2018) prestano particolare attenzione al ruolo delle infrastrutture e affermano che la ricerca dovrebbe fornire mezzi migliori per contrastare le minacce ibride.

L'Europa è esposta a una vasta gamma di pericoli naturali e le vulnerabilità delle infrastrutture devono essere affrontate anche da questa prospettiva. Vi è quindi la necessità di implementare soluzioni innovative per garantire il funzionamento continuo delle infrastrutture europee esposte. A questo proposito, la ricerca sulla sicurezza dovrebbe sostenere le misure di regolamentazione e cooperazione a livello europeo, come il meccanismo unionale di protezione civile e la nuova strategia di adattamento dell'UE. D'altra parte, le stesse nuove tecnologie delle infrastrutture possono rappresentare un rischio potenziale per la società a causa di incidenti. Pertanto, il ruolo della protezione civile deve essere riflesso in una ricerca mirata allo stesso livello di quella delle diverse autorità di sicurezza.

La crisi COVID-19 riguarda le infrastrutture in due dimensioni principali. Le pandemie sono uno stress-test estremo per il funzionamento di alcune infrastrutture (in particolare: sanità, trasporti e catene di rifornimento) in quanto sconvolgono le procedure stabilite, minacciano il funzionamento a causa del contagio della forza-lavoro e aumentano in modo massiccio la necessità di risorse. Inoltre, le infrastrutture stesse possono aumentare il rischio pandemico se non sono adatte a diverse misure di mitigazione e favoriscono la trasmissione del virus.

Quest'area si baserà sulle lezioni apprese dalla crisi COVID-19. Sarà essenziale per certi topic anche garantire sinergie e coordinamento delle azioni con il programma UE per la salute.

La maggiore complessità nel settore della protezione delle infrastrutture non è solo legata al ruolo amplificato della dimensione cibernetica, ma anche al mix di rischi naturali e artificiali e alla crescente interdipendenza. Lo sviluppo delle città europee in città intelligenti ha aperto un nuovo dominio nella protezione delle infrastrutture, espandendo la prospettiva oltre i settori classici delle infrastrutture, poiché nelle aree urbane vengono impiegati beni più complessi, connessi e vulnerabili. Questa considerazione svela gli elementi costitutivi ancora fragili delle caratteristiche tecnologiche delle città intelligenti e sottolinea la necessità di porre una maggiore enfasi su sfide ed esigenze sociali più ampie. La ricerca sulla sicurezza può contribuire a mettere a frutto le conoscenze acquisite in altri settori e a renderle utilizzabili dalle autorità locali per proteggere e potenziare persone e beni nelle città e nelle aree urbane.

Impatto previsto

Le proposte di temi nell'ambito di questa destinazione dovrebbero definire un percorso credibile per contribuire al seguente impatto atteso del piano strategico Horizon Europe 2021-2024: *"[...] la resilienza e l'autonomia delle infrastrutture fisiche e digitali sono rafforzate e le funzioni vitali della società sono garantite, grazie a una prevenzione, preparazione e risposta più potenti, a una migliore comprensione dei relativi aspetti umani, sociali e tecnologici e allo sviluppo di capacità all'avanguardia per [...] operatori di infrastrutture [...]".*

Più specificamente, le proposte dovrebbero contribuire al raggiungimento di uno o più dei seguenti impatti:

- Garanzia di resilienza delle infrastrutture di sistemi interconnessi su larga scala in caso di attacchi complessi, pandemie o disastri naturali e causati dall'uomo;
- Sistemi aggiornati di protezione delle infrastrutture consentono una risposta rapida, efficace, sicura e senza interventi umani sostanziali a minacce e sfide complesse, e valutano meglio i rischi garantendo la resilienza e l'autonomia strategica delle infrastrutture europee;
- Le città intelligenti resilienti e sicure sono protette utilizzando le conoscenze derivate dalla protezione di infrastrutture e sistemi critici caratterizzati da una crescente complessità.

I seguenti inviti in questo programma di lavoro contribuiscono a questa destinazione.

3.1 Call - Resilient Infrastructure 2021

Destination Resilient Infrastructure

Call: HORIZON-CL3-2021-INFRA-01

Topics	Tipologia di azione	Budget totale (milioni di euro) 2021	Contributo UE previsto per progetto (milioni di euro)[8]	Numero di progetti che si prevede di finanziare
Apertura: 30 giugno 2021 Scadenza: 23 novembre 2021				
HORIZON-CL3-2021-INFRA-01-01: European infrastructures and their autonomy safeguarded against systemic risks	IA	20.00	Circa 10.00	1
HORIZON-CL3-2021-INFRA-01-02: Ensured infrastructure resilience in case of Pandemics	IA		Circa 10.00	1
Budget indicativo complessivo		20.00		

3.2 Call - Resilient Infrastructure 2022

Destination Resilient Infrastructure

Call: HORIZON-CL3-2022-INFRA-01

Topics	Tipologia di azione	Budget totale (milioni	Contributo UE previsto	Numero di progetti

[8] Tuttavia, questo non preclude la presentazione e la selezione di una proposta che richiede importi diversi.

		di euro) 2022	per progetto (milioni di euro)[9]	che si prevede di finanziare
Apertura: 30 giugno 2022 Scadenza: 23 novembre 2022				
HORIZON-CL3-2022-INFRA-01-01: Nature-based Solutions integrated to protect local infrastructure	RIA	5.00	Circa 5.00	1
HORIZON-CL3-2022-INFRA-01-02: Autonomous systems used for infrastructure protection	IA	6.00	Circa 6.00	1
Budget indicativo complessivo		11.00		

4. Destination 4: Increased Cybersecurity

L'Europa è nel mezzo di una trasformazione digitale. La comunicazione digitale, l'interazione dei social media, l'intelligenza artificiale, l'e-government, il commercio elettronico e le imprese digitali stanno trasformando costantemente il nostro mondo e stanno generando una quantità sempre maggiore di dati che, se messi in comune e usati, possono portare a livelli nuovi di creazione di valore. Più siamo interconnessi, tuttavia, più siamo vulnerabili alle minacce informatiche.

Le perturbazioni digitali non solo minacciano le nostre economie ma anche il nostro stile di vita, le nostre libertà e i nostri valori, e minano la coesione e il funzionamento della nostra democrazia in Europa.

È necessario migliorare la nostra capacità di **proteggere l'UE dagli attacchi maligni e di affrontare le debolezze della sicurezza digitale in generale**. La trasformazione digitale richiede un miglioramento sostanziale della sicurezza informatica, in modo da garantire la protezione del crescente numero di dispositivi connessi e il funzionamento sicuro dei sistemi

[9] Tuttavia, questo non preclude la presentazione e la selezione di una proposta che richiede importi diversi.

di rete e di informazione. L'Europa deve costruire la resilienza ai cyber-attacchi e creare una deterrenza informatica efficace, assicurandosi allo stesso tempo che la protezione dei dati e la libertà dei cittadini siano rafforzate. Questi sforzi dovrebbero includere considerazioni per organizzazioni e cittadini particolarmente vulnerabili.

Gli strumenti tecnologici della sicurezza informatica sono risorse strategiche, oltre ad essere tecnologie chiave di crescita per il futuro. È nell'interesse strategico dell'UE garantire che l'UE mantenga e sviluppi le capacità essenziali per garantire la sua economia digitale, la società e la democrazia, per proteggere hardware e software critici e per fornire servizi chiave di cybersecurity.

Le attività di ricerca e innovazione sulla cybersecurity sosterranno un'Europa adatta all'era digitale, consentendo e sostenendo l'innovazione digitale, pur preservando altamente la privacy, la sicurezza e gli standard etici. Esse contribuiranno all'attuazione della politica digitale e della privacy dell'Unione, in particolare la direttiva sulla sicurezza delle reti e dei sistemi informativi nell'Unione, il regolamento sulla cibersicurezza, la strategia sulla cibersicurezza, il GDPR e il futuro regolamento sulla e-Privacy.

La ricerca e l'innovazione si baseranno sui risultati di Horizon 2020, come i progetti pilota finanziati nell'ambito di SU-ICT-03-2018 e su altri topic pertinenti di H2020 e sulle attività in materia di cibersicurezza. Le attività saranno allineate, se del caso, ai futuri obiettivi del centro di competenza sulla sicurezza informatica e della rete dei centri di coordinamento nazionali (proposta della Commissione COM(2018)630). Saranno complementari alle azioni nell'ambito del programma Europa digitale, obiettivi specifici 3 e 4, che rafforzeranno la capacità di sicurezza informatica dell'UE sostenendo la diffusione di infrastrutture e strumenti di sicurezza informatica in tutta l'UE, per le amministrazioni pubbliche, le imprese e i singoli individui, e sosterranno le competenze digitali, anche in materia di sicurezza informatica. In generale, la cybersecurity è una sfida orizzontale e non è limitata a Horizon Europe - Cluster 3. Oltre ai bandi di Horizon Europe del Cluster 3 - Civil Security for Society, altre attività rilevanti per la Cybersecurity saranno sostenute in particolare nella parte del programma di lavoro del Cluster 4 - Digital, Industry and Space.

I risultati della ricerca e dell'innovazione possono alimentare il lavoro operativo sulla preparazione e la risposta nella Joint Cyber Unit.

Impatto previsto:

Le proposte nell'ambito di questa destinazione dovrebbero definire un percorso credibile che contribuisca al seguente impatto del piano strategico 2021-2024: *"Maggiore sicurezza informatica e un ambiente online più sicuro sviluppando e utilizzando efficacemente le capacità dell'UE e degli Stati membri nelle tecnologie digitali a sostegno della protezione*

dei dati e delle reti che aspirano alla sovranità tecnologica in questo settore, nel rispetto della privacy e di altri diritti fondamentali; ciò dovrebbe contribuire a rendere sicuri servizi, processi e prodotti, nonché a solide infrastrutture digitali in grado di resistere e contrastare attacchi informatici e minacce ibride".

Più specificamente, le proposte dovrebbero contribuire al raggiungimento di uno o più dei seguenti impatti:

- Rafforzamento delle capacità di sicurezza informatica dell'UE e sovranità dell'Unione europea nelle tecnologie digitali;
- Infrastrutture, sistemi e processi digitali più resilienti;
- Maggiore sicurezza del software, dell'hardware e della catena di approvvigionamento;
- Tecnologie dirompenti protette;
- Garanzia di sicurezza intelligente e quantificabile e certificazione condivisa in tutta l'UE;
- Consapevolezza rafforzata e una gestione e cultura comune della sicurezza informatica.

I seguenti inviti in questo programma di lavoro contribuiscono a questa destinazione.

4.1 Call - Increased cybersecurity 2021

Destination Increased Cybersecurity

Call: HORIZON-CL3-2021-CS-01

Topics	Tipologia di azione	Budget totale (milioni di euro)	Contributo UE previsto per progetto (milioni di euro)[10]	Numero di progetti che si prevede di finanziare
		2021		
Apertura: 30 giugno 2021 Scadenza: 21 ottobre 2021				

[10] Tuttavia, questo non preclude la presentazione e la selezione di una proposta che richiede importi diversi.

HORIZON-CL3-2021-CS-01-01: Dynamic business continuity and recovery methodologies based on models and prediction for multi-level Cybersecurity	RIA	21.50	Da 3.00 a 5.00	5
HORIZON-CL3-2021-CS-01-02: Improved security in open-source and open-specification hardware for connected devices	RIA	18.00	Da 3.00 a 5.00	4
HORIZON-CL3-2021-CS-01-03: AI for cybersecurity reinforcement	RIA	11.00	Da 3.00 a 4.00	3
HORIZON-CL3-2021-CS-01-04: Scalable privacy-preserving technologies for cross-border federated computation in Europe involving personal data	RIA	17.00	Da 3.00 a 5.00	4
Budget indicativo totale		67.50		

4.2 Call - Increased cybersecurity 2022

Destination Increased Cybersecurity

Call: HORIZON-CL3-2022-CS-01

Topics	**Tipologia di azione**	**Budget totale (milioni di euro)**	**Contributo UE previsto per progetto (milioni di euro)[11]**	**Numero di progetti che si prevede di finanziare**
		2022		
Apertura: 30 giugno 2022				

[11] Tuttavia, questo non preclude la presentazione e la selezione di una proposta che richiede importi diversi.

Scadenza: 16 novembre 2022				
HORIZON-CL3-2022-CS-01-01: Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures	IA	21.00	Da 4.00 a 6.00	4
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	17.30	Da 3.00 a 5.00	4
HORIZON-CL3-2022-CS-01-03: Transition towards Quantum-Resistant Cryptography	IA	11.00	Da 3.50 a 6.00	2
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	IA	18.00	Da 3.00 a 5.00	4
Budget indicativo complessivo		67.30		

5. Destination 5: Disaster-Resilient Society for Europe

Questa destinazione sostiene l'attuazione dei framework politici internazionali (ad esempio, Sendai Framework for Disaster Risk Reduction, l'accordo di Parigi, gli obiettivi di sviluppo sostenibile), le politiche di gestione del rischio di catastrofi dell'UE che affrontano le minacce naturali e di origine umana, le priorità del Green Deal europeo, compresa la nuova strategia di adattamento dell’UE ai cambiamenti climatici, nonché la strategia dell’UE per l'Unione della sicurezza e l'agenda antiterrorismo.

Il mondo e le nostre società stanno affrontando rischi crescenti da pericoli antropogenici e naturali, che richiedono maggiori capacità nella gestione e nella governance del rischio e

della resilienza, compresi strumenti per una migliore prevenzione e preparazione, tecnologie per i primi e i secondi soccorritori e, se del caso, per i cittadini, e una resilienza generale della società. La crescente gravità e frequenza di eventi meteorologici estremi ed eventi associati derivanti dai cambiamenti climatici richiedono una ricerca specifica, mentre i pericoli geologici e le tendenze ad insorgenza lenta meritano un'attenzione costante. Le minacce antropogeniche richiedono anche capacità rafforzate di gestione delle crisi. Infine, la crisi COVID-19 ha dimostrato come le società siano diventate più esposte e vulnerabili ai rischi pandemici.

La riduzione del rischio di qualsiasi tipo di catastrofe è regolata da una serie di politiche e strategie internazionali, comunitarie, nazionali e locali. Le nostre società oggi devono affrontare crisi complesse e transfrontaliere all'interno delle quali è necessario un approccio più sistemico con una stretta interconnessione tra riduzione del rischio e sviluppo sostenibile. Le crisi complesse riguardano aree scientifiche, di governance, politiche e sociali e richiedono una cooperazione intersettoriale. Un'ampia gamma di ricerche e sviluppi tecnologici, così come progetti di formazione e sviluppo delle capacità, hanno sostenuto lo sviluppo e l'attuazione di politiche e strategie. Tuttavia, l'integrazione di ulteriori esigenze di ricerca e innovazione è spesso difficile a causa della complessità del quadro politico e dell'alto livello di frammentazione delle iniziative di ricerca e sviluppo delle capacità. Inoltre, una maggiore cooperazione e il coinvolgimento di diversi settori e attori sono essenziali.

Per quanto riguarda la risposta, la cooperazione internazionale su ricerca e innovazione con i partner chiave ha il potenziale per identificare soluzioni comuni e aumentare la rilevanza dei risultati. Come tale, l'International Forum to Advance First Responder Innovation (IFAFRI) e altre reti di esperti coinvolte in iniziative dell'ONU e/o della NATO hanno fornito una panoramica delle lacune esistenti e sono in grado di impegnarsi nella cooperazione con i partner all'interno e all'esterno dell'UE, i cui risultati possono fornire una fonte preziosa per identificare i bisogni più urgenti relativi alla gestione delle catastrofi.

Gli approcci integrati sono essenziali per collegare diverse aree politiche, tra cui la protezione civile, l'ambiente, l'adattamento al clima e la mitigazione, la salute e la protezione dei consumatori, e la sicurezza. I percorsi comuni di resilienza che emergono da diversi domini scientifici e operativi devono ancora essere esplorati in termini di potenziale di attuazione. In particolare, il cambiamento di paradigma dalla gestione dei "disastri" alla gestione dei "rischi" e al miglioramento della resilienza deve essere sostenuto da azioni di ricerca e innovazione, compresi metodi e soluzioni innovative rivolte ai decisori, per sostenere l'istruzione e la formazione complementari necessarie in tutti i settori di intervento, i cambiamenti procedurali e organizzativi complementari che hanno un impatto sulla società nel suo complesso, nonché sulle tecnologie, i processi, le procedure e i vari strumenti a sostegno delle operazioni di primo e secondo intervento. Un enorme corpo di conoscenze e tecnologie è stato sviluppato nel Settimo programma quadro e in Horizon 2020: questo

costituisce una forte eredità che aprirà la strada alla ricerca futura, e i risultati precedenti dovranno essere pienamente riconosciuti e utilizzati nei prossimi sviluppi della ricerca.

Le proposte per i topic di questa destinazione dovrebbero definire un percorso credibile per contribuire al seguente impatto atteso del piano strategico Horizon Europe 2021-2024: *"Le perdite dovute a catastrofi naturali, accidentali e provocate dall'uomo sono ridotte attraverso una maggiore riduzione del rischio di catastrofi basata su azioni preventive, una migliore preparazione e resilienza della società e una migliore gestione del rischio di catastrofi in modo sistematico."*

Più specificamente, le proposte dovrebbero contribuire al raggiungimento di uno o più dei seguenti impatti:

- Una maggiore comprensione e una migliore conoscenza e consapevolezza situazionale dei rischi legati alle catastrofi da parte dei cittadini;
- Un più efficiente coordinamento intersettoriale, interdisciplinare e transfrontaliero del ciclo di gestione del rischio di catastrofi (dalla prevenzione, preparazione alla mitigazione, risposta e recupero) dal livello internazionale a quello locale;
- Maggiore condivisione delle conoscenze e coordinamento per quanto riguarda la standardizzazione nell'area della gestione delle crisi e dei CBRN-E.
- Rafforzamento delle capacità dei primi soccorritori in tutte le fasi operative relative a qualsiasi tipo di catastrofe (naturale e causata dall'uomo) in modo che possano preparare meglio le loro operazioni, avere accesso a una maggiore consapevolezza della situazione, avere mezzi per rispondere agli eventi in modo più rapido, sicuro ed efficiente, e possano procedere più efficacemente all'identificazione, al triage e alla cura delle vittime.

I seguenti inviti in questo programma di lavoro contribuiscono a questa destinazione.

5.1 Call - Disaster-Resilient Society 2021

Destination Disaster-Resilient Society for Europe

Call: HORIZON-CL3-2021-DRS-01

Topics	Tipologia di azione	Budget totale (milioni di euro)	Contributo UE previsto per progetto	Numero di progetti che si prevede di finanziare
		2021		

			(milioni di euro)[12]	
Apertura: 30 giugno 2021 Scadenza: 23 novembre 2021				
HORIZON-CL3-2021-DRS-01-01: Improved understanding of risk exposure and its public awareness in areas exposed to multi-hazards	RIA	5.00	Circa 5.00	1
HORIZON-CL3-2021-DRS-01-02: Integrated Disaster Risk Reduction for extreme climate events: from early warning systems to long term adaptation and resilience building	IA	6.00	Circa 6.00	1
HORIZON-CL3-2021-DRS-01-03: Enhanced assessment of disaster risks, adaptive capabilities and scenario building based on available historical data and projections	RIA	5.00	Circa 5.00	1
HORIZON-CL3-2021-DRS-01-04: Developing a prioritisation mechanism for research programming in standardisation related to natural hazards and/or CBRN-E sectors	CSA	2.00	Circa 2.00	1
HORIZON-CL3-2021-DRS-01-05: Fast deployed mobile laboratories to enhance situational awareness for pandemics and emerging infectious diseases	IA	8.00	Circa 4.00	2
Budget indicativo totale		26.00		

[12] Tuttavia, questo non preclude la presentazione e la selezione di una proposta che richiede importi diversi.

5.2 Call - Disaster-Resilient Society 2022

Destination Disaster-Resilient Society for Europe

Call: HORIZON-CL3-2022-DRS-01

Topics	Tipologia di azione	Budget totale (milioni di euro) 2022	Contributo UE previsto per progetto (milioni di euro)[13]	Numero di progetti che si prevede di finanziare
Apertura: 30 giugno 2022 Scadenza: 23 novembre 2022				
HORIZON-CL3-2022-DRS-01-01: Enhanced citizen preparedness in the event of a disaster or crisis-related emergency	IA	10.00	Circa 5.00	1
HORIZON-CL3-2022-DRS-01-03: Improved quality assurance / quality control of data used in decision-making related to risk management of natural hazards, accidents and CBRN events	IA		Circa 5.00	1
HORIZON-CL3-2022-DRS-01-02: Enhanced preparedness and management of High- Impact Low-Probability or unexpected events	RIA	10.00	Circa 5.00	1
HORIZON-CL3-2022-DRS-01-04: Better understanding of citizens' behavioural and psychological reactions in the event of a disaster or crisis situation	RIA		Circa 5.00	1

[13] Tuttavia, questo non preclude la presentazione e la selezione di una proposta che richiede importi diversi.

HORIZON-CL3-2022-DRS-01-05: Improved impact forecasting and early warning systems supporting the rapid deployment of first responders in vulnerable areas	IA	10.00	Circa 5.00	1
HORIZON-CL3-2022-DRS-01-06: Improved disaster risk pricing assessment	IA		Circa 5.00	1
HORIZON-CL3-2022-DRS-01-07: Improved international cooperation addressing first responder capability gaps	RIA	5.00	Circa 5.00	1
HORIZON-CL3-2022-DRS-01-08: Enhanced situational awareness and preparedness of first responders and improved capacities to minimise time-to-react in urban areas in the case of CBRN-E-related events	IA	11.00	Circa 5.00	1
HORIZON-CL3-2022-DRS-01-09: Enhanced capacities of first responders more efficient rescue operations, including decontamination of infrastructures in the case of a CBRN-E event	IA		Circa 6.00	1
Budget indicative complessivo		46.00		

6. Destination 6: Strengthened Security Research and Innovation (SSRI)

Il quadro di ricerca e innovazione sulla sicurezza finanziato dall'UE è stato lanciato con il Preparatory Action for Security Research. Da allora, il programma ha contribuito in modo sostanziale alla conoscenza e alla creazione di valore nel campo della sicurezza interna e al consolidamento di un ecosistema meglio attrezzato per capitalizzare la ricerca e

l'innovazione a sostegno delle priorità dell'UE in materia di sicurezza, ma rimane la sfida del miglioramento nell'assorbimento dell'innovazione.

La misura in cui **le tecnologie innovative sviluppate grazie agli investimenti R&I dell'UE vengono industrializzate e commercializzate** dall'industria dell'UE, e successivamente acquisite e impiegate dagli utenti finali, potrebbe fornire una valida misura dell'impatto ottenuto con il programma. Tuttavia, ci sono fattori inerenti all'ecosistema di sicurezza dell'UE che ostacolano il pieno raggiungimento di questo impatto. Questi includono, tra gli altri, la frammentazione del mercato, le barriere culturali, le debolezze analitiche, le debolezze di programmazione, le considerazioni etiche, legali e sociali o la mancanza di sinergie tra gli strumenti di finanziamento. Vale la pena notare che tali fattori influenzano tutti i settori di sicurezza affrontati nel Cluster 3; che non c'è un fattore predominante con un'influenza sufficiente da solo a cambiare la dinamica generale di assorbimento dell'innovazione; e che presentano relazioni complesse tra di loro che sono difficili da distinguere.

È necessario creare un ambiente favorevole che sia progettato con lo scopo principale di aumentare l'impatto della R&I in materia di sicurezza, che sia visibile e riconoscibile per coloro che sono interessati a contribuire a questo obiettivo, e che fornisca strumenti su misura che servano ad affrontare i fattori che ostacolano l'adozione dell'innovazione.

La Destinazione SSRI è stata quindi progettata con questo scopo per servire allo stesso modo a tutti gli impatti attesi del Cluster 3. La ricerca applicata in questo settore contribuirà ad aumentare l'impatto del lavoro svolto nell'ecosistema di ricerca e innovazione sulla sicurezza dell'UE nel suo complesso e a contribuire ai suoi valori fondamentali, ovvero: 1) garantire che la R&I in materia di sicurezza mantenga l'attenzione sul potenziale uso finale dei suoi risultati; 2) contribuire a una pianificazione lungimirante delle capacità di sicurezza dell'UE; 3) garantire lo sviluppo di tecnologie di sicurezza che siano socialmente accettabili; 4) aprire la strada all'industrializzazione, alla commercializzazione, all'acquisizione e alla diffusione di risultati di R&I di successo; e 5) salvaguardare l'autonomia strategica aperta e la sovranità tecnologica dell'UE nei settori critici della sicurezza contribuendo a una base tecnologica e industriale di sicurezza dell'UE più competitiva e resistente.

Mentre le altre destinazioni del Cluster 3 supportano attività di ricerca e innovazione per sviluppare soluzioni che affrontino specifiche minacce alla sicurezza o esigenze di capacità, la destinazione SSRI contribuirà a raggiungere gli obiettivi con strumenti che aiuteranno a portare questi e altri sviluppi più vicini al mercato. Tali strumenti aiuteranno gli sviluppatori (compresa l'industria, le organizzazioni di ricerca e il mondo accademico) a migliorare la valorizzazione dei loro investimenti nella ricerca.

Inoltre, la destinazione SSRI offrirà un ambiente aperto per creare conoscenza e valore attraverso la ricerca in settori che non sono esclusivi di una sola area di sicurezza, ma trasversali a tutto il cluster. Questo contribuirà a ridurre la frammentazione tematica, avvicinando gli attori di diversi settori relativi alla sicurezza, ed espandendo il mercato oltre i tradizionali silos tematici.

Infine, la SSRI permetterà l'assegnazione di risorse allo sviluppo di strumenti e metodi per rafforzare il ciclo dell'innovazione dal punto di vista del processo, aumentando così la sua efficacia, efficienza e impatto. Questa destinazione contribuirà allo sviluppo di una capacità analitica adattata alle esigenze specifiche degli attori della sicurezza per la materializzazione di una pianificazione strutturata a lungo termine basata sulle capacità di ricerca e innovazione per la sicurezza.

Al fine di realizzare gli obiettivi di questa destinazione, sono state definite ulteriori condizioni di ammissibilità per quanto riguarda il coinvolgimento attivo dei professionisti della sicurezza o degli utenti finali.

Le proposte di topic nell'ambito di questa destinazione dovrebbero definire un percorso credibile per contribuire ai seguenti impatti:

- Uno sviluppo più efficace ed efficiente basato su evidenze scientifiche delle capacità di sicurezza civile dell'UE, costruito su un ciclo di ricerca e innovazione in materia di sicurezza più forte, sistematico e ad alta intensità di analisi;
- Una maggiore industrializzazione, commercializzazione, adozione e diffusione dei risultati positivi della ricerca in materia di sicurezza rafforza la competitività e la resilienza della tecnologia e della base industriale dell'UE in materia di sicurezza, e salvaguarda la sicurezza nell'approvvigionamento dei prodotti dell'UE nei settori critici della sicurezza;
- La conoscenza e il valore delle questioni trasversali, grazie alla R&I, riducono i pregiudizi settoriali e rompono i silos tematici che impediscono la proliferazione di soluzioni di sicurezza comuni.

I seguenti inviti in questo programma di lavoro contribuiscono a questa destinazione.

6.1 Call - Support to Security Research and Innovation 2021

Destination Strengthened Security Research and Innovation

Call: HORIZON-CL3-2021-SSRI-01

Topics	Tipologia di azione	Budget totale (milioni	Contributo UE previsto	Numero di progetti

		di euro) 2021	per progetto (milioni di euro)[14]	che si prevede di finanziare
Apertura: 30 giugno 2021 Scadenza: 23 novembre 2021				
HORIZON-CL3-2021-SSRI-01-01: A maturity assessment framework for security technologies	RIA	1.50	Circa 1.50	1
HORIZON-CL3-2021-SSRI-01-02: Knowledge Networks for Security Research & Innovation	CSA	4.00	Circa 2.00	2
HORIZON-CL3-2021-SSRI-01-03: National Contact Points (NCPs) in the field of security and cybersecurity	CSA	2.50	Circa 2.50	1
HORIZON-CL3-2021-SSRI-01-04: Demand-led innovation for situation awareness in civil protection	PCP	6.00	Circa 6.00	1
HORIZON-CL3-2021-SSRI-01-05: Security research technologies driven by active civil society engagement: transdisciplinary methods for societal impact assessment and impact creation	RIA	2.00	Circa 2.00	1
Budget indicativo totale		16.00		

6.2 Call - Support to Security Research and Innovation 2022

Destination Strengthened Security Research and Innovation

Call: HORIZON-CL3-2022-SSRI-01

[14] Tuttavia, questo non preclude la presentazione e la selezione di una proposta che richiede importi diversi.

Topics	Tipologia di azione	Budget totale (milioni di euro)	Contributo UE previsto per progetto (milioni di euro)[15]	Numero di progetti che si prevede di finanziare
		2022		
Opening: 30 giugno 2022 Scadenza: 23 novembre 2022				
HORIZON-CL3-2022-SSRI-01-01: Increased foresight capacity for security	CSA	1.50	Circa 1.50	1
HORIZON-CL3-2022-SSRI-01-02: Knowledge Networks for security Research & Innovation	CSA	4.00	Circa 2.00	2
HORIZON-CL3-2022-SSRI-01-03: Stronger grounds for pre-commercial procurement of innovative security technologies	CSA	2.00	Circa 1.00	2
HORIZON-CL3-2022-SSRI-01-04: Social innovations as enablers of security solutions and increased security perception	RIA	2.00	Circa 2.00	1
Budget indicativo totale		9.50		

7. Siti e documenti di riferimento

- Funding and Tender Portal – Cluster 3 Call 2021-2022
- Work Programme Cluster 3
- Horizon Europe Strategic Plan 2021-2024

[15] Tuttavia, questo non preclude la presentazione e la selezione di una proposta che richiede importi diversi.

- Le Partnership in Horizon Europe