Ministero dell'Università e della Ricerca

APRE
Agenzia per la Promozione della Ricerca Europea

LA SETTIMANA HORIZON EUROPE 2021

INFO WEEK

Data 14-07-2021

Aurelia Sole

Rappresentante nazionale nel Comitato di Programma di Horizon Europe Cluster 3 "Civil Security for Society" - Università degli Studi della Basilicata

#HorizonEU #2021horizoneurope

CLUSTER 3 – Civil Security for Society

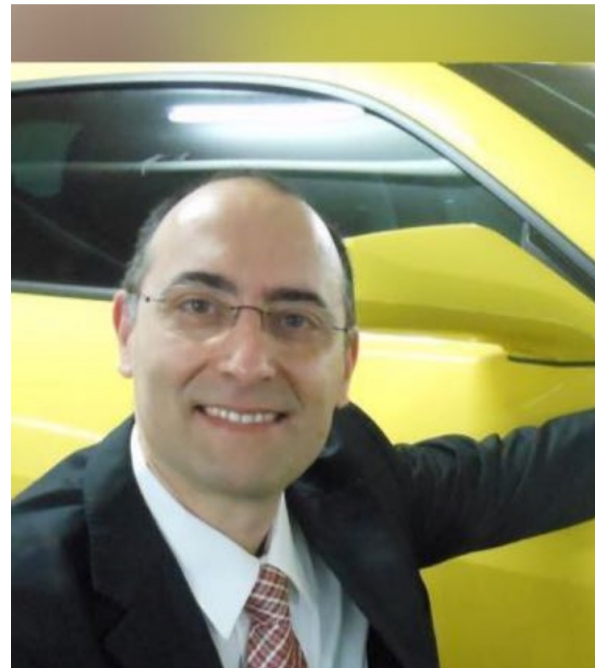
Il programma di lavoro del cluster 3 sosterrà l'attuazione delle priorità politiche dell'UE relative alla **sicurezza**, compresa la **sicurezza informatica, la sicurezza delle frontiere, terrorismi e crimini in generale** a questo cluster è stata assegnato anche il tema **della riduzione del rischio di catastrofi e della resilienza**. Inoltre, si baserà sugli insegnamenti tratti dalla crisi COVID-19 in termini di **prevenzione, mitigazione, preparazione e sviluppo di capacità per contrastare le crisi** (comprese le crisi sanitarie) **e nel miglioramento degli aspetti di gestione intersettoriali di tali crisi.**

Gruppo Italiano Esperti:

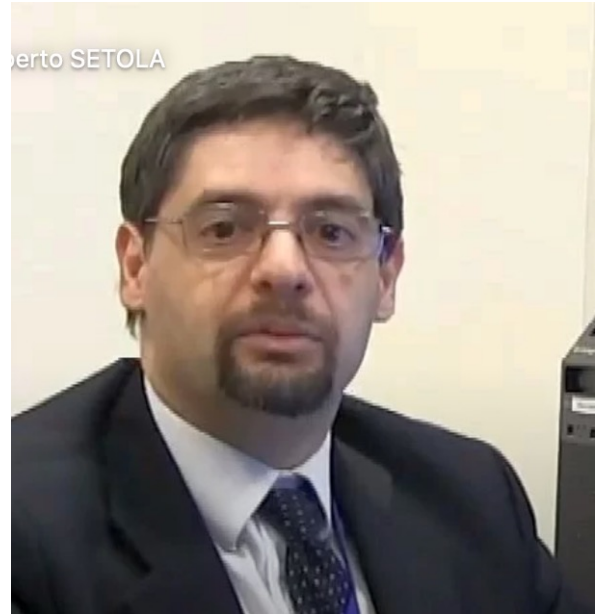
Angelo Masi – Prof. Ordinario di Tecnica delle Costruzioni presso l'Università della Basilicata. Componente del Consiglio Direttivo del Consorzio Interuniversitario ReLUIS. Coordinatore del gruppo di lavoro PNR su Sicurezza delle strutture, infrastrutture e reti. Esperto nominato dal Comitato Europeo delle Regioni per la preparazione dei Pareri "Una politica europea per la riqualificazione sismica di edifici ed infrastrutture" e "Resilienza delle entità critiche".

Paolo Prinetto Prof. Ordinario di Sistemi di Elaborazione delle Informazioni, Politecnico di Torino, esperto di Cybersecurity. Presidente del consorzio CINI (CINI Cybersecurity National Lab) (un consorzio di 44 università italiane per lo sviluppo di ricerca nel campo dell'Informatica e dell'Ingegneria Informatica

Gruppo Italiano Esperti:



Francesco Scialla Capitano di Vascello, ingegnere, è stato capo del reparto "Sistemi di comando, controllo e comunicazioni" della direzione Informatica, Telematica e Tecnologie Avanzate del ministero della Difesa e rappresentante del direttore nazionale degli Armamenti presso l'Unione Europea.



Roberto Setola Prof. Ordinario di Automatica presso presso l'Università Campus Bio-Medico. Direttore Laboratorio Sistemi Complessi e Sicurezza. Direttore del Master in Homeland Security. Esperto presso la Presidenza del Consiglio dei Ministri in tema di Infrastrutture Critiche.

Orientamento Strategico, Impatti e contributi specifici dei cluster 3 principalmente coinvolti

Promuovere un'autonomia strategica aperta

Orientamento strategico	Impatti	Contributi Cluster 3
OPEN STRATEGIC AUTONOMY	• Un'economia dei dati competitiva e sicura • Leadership industriale nelle tecnologie chiave ed emergenti utili per I cittadini • Tecnologia digitale sicura e cybersecurity • Servizi digitali di alta qualità per tutti	➢ Contribuire a creare/rendere infrastrutture (critiche) fisiche e digitali resilienti ➢ Rafforzare le capacità industriali europee nel campo della Cybersecurity (in cui i principi di sicurezza e rispetto della privacy siano presenti già in fase di progettazione) per creare una maggiore autonomia strategica che possa portare all'Europa vantaggio competitivo e leadership nei mercati globali nei confronti delle tecnologie straniere. ➢ Difendere gli standard elevati dell'UE (privacy, protezione dei dati personali, ecc.) ➢ Contribuire alla sicurezza e all'incolumità del Sistema economico e degli utenti

Orientamento Strategico, Impatti e contributi specifici dei cluster 3 principalmente coinvolti

Ripristinare gli ecosistemi e la biodiversità dell'Europa e gestire le risorse naturali in modo sostenibile per garantire la sicurezza alimentare e un ambiente pulito e sano.

Strategic Orientation	Impatti	Contributi Cluster 3
SUSTAINABLY NATURAL RESOURCES	• Migliorare gli ecosistemi e la biodiversità sulla terra e nelle acque • Aria, acqua e suolo puliti e sani • Sistemi alimentari sostenibili dalla fattoria alla tavola su terra e mare	- Interventi Natur-based contro I rischi naturali - Sicurezza nel cibo (food defence)

Orientamento Strategico, Impatti e contributi specifici dei cluster 3 principalmente coinvolti

Economia circolare, climaticamente neutra e sostenibile abilitata digitalmente

Strategic Orientation	Impatti	Contributi Cluster 3
FIRST DIGITALLY ENABLED CIRCULAR ECONOMY	• Mitigazione e adattamento ai cambiamenti climatici • Energia pulita e conveniente • Trasporti intelligenti e sostenibili • Economia circolare e pulita	• Rischi naturali (abbiamo introdotto la prevenzione) • Società resiliente ai disastri • Riduzione della perdita di vite umane

Orientamento Strategico, Impatti e contributi specifici dei cluster 3 principalmente coinvolti

Creare una società europea più resiliente, inclusiva e democratica, preparata e reattiva alle minacce e ai disastri, affrontare le disuguaglianze e fornire un'assistenza sanitaria di alta qualità e responsabilizzare tutti i cittadini ad agire per le transizioni verdi e digitali.

Strategic Orientation	Impatti	Contributi Cluster 3
A MORE RESILIENT, INCLUSIVE AND DEMOCRATIC EUROPEAN SOCIETY (1/3)	• Un'Europa resiliente preparata a combattere nuove e antiche minacce • Una società dell'UE sicura, aperta e democratica • Una assistenza sanitaria accessibile di alta qualità • Una crescita inclusiva e nuove opportunità di lavoro	➢ Sostenere le risposte dell'UE alle sfide in materia di sicurezza, garantendo al contempo la libera circolazione e proteggendo l'integrità dello spazio Schengen: ➢ contribuire a una migliore gestione delle frontiere aeree, terrestri e marittime sia per i flussi di persone che per le merci (rispondendo ai requisiti individuati da Frontex) e dalle autorità doganali dell'UE . ➢ Incrementare la capacità per la sicurezza marittima dell'UE. ➢ Occuparsi di prevenzione, Indagine e mitigazione degli impatti di atti criminali, anche di tipo nuovo / emergente (comprese le capacità di analizzare in tempo quasi reale grandi volumi di dati per prevenire eventi criminali o per combattere la disinformazione e le notizie false con implicazioni per la sicurezza.

Orientamento Strategico, Impatti e contributi specifici dei cluster 3 principalmente coinvolti

Creare una società europea più resiliente, inclusiva e democratica, preparata e reattiva alle minacce e ai disastri, affrontare le disuguaglianze e fornire un'assistenza sanitaria di alta qualità e responsabilizzare tutti i cittadini ad agire per le transizioni verdi e digitali.

Strategic Orientation	Impatti	Contributi Cluster 3
A MORE RESILIENT, INCLUSIVE AND DEMOCRATIC EUROPEAN SOCIETY (2/3)	• Un'Europa resiliente preparata a combattere nuove e antiche minacce • Una società dell'UE sicura, aperta e democratica • Una assistenza sanitaria accessibile di alta qualità • Una crescita inclusiva e nuove opportunità di lavoro	➢ Incrementare la sicurezza degli spazi pubblici (smartcity). ➢ Migliorare la sicurezza e la resilienza delle funzioni sociali di base (sanità, forze dell'ordine, energia, mobilità, servizi pubblici, servizi finanziari, infrastrutture e reti di comunicazione e logistica) ➢ Sostenere un'Europa resiliente e più stabile che protegge, passando da un approccio reattivo alla sicurezza a un approccio proattivo ➢ Ridurre le perdite dovute a catastrofi naturali, accidentali e provocate dall'uomo (maggiore riduzione del rischio di catastrofi naturali e antropiche, migliore preparazione, resilienza e ripristino della società; soluzioni intersettoriali e governance multilivello)

Orientamento Strategico, Impatti e contributi specifici dei cluster 3 principalmente coinvolti

Creare una società europea più resiliente, inclusiva e democratica, preparata e reattiva alle minacce e ai disastri, affrontare le disuguaglianze e fornire un'assistenza sanitaria di alta qualità e responsabilizzare tutti i cittadini ad agire per le transizioni verdi e digitali.

Strategic Orientation	Impatti	Contributi Cluster 3
A MORE RESILIENT, INCLUSIVE AND DEMOCRATIC EUROPEAN SOCIETY (3/3)	• Un'Europa resiliente preparata a combattere nuove e antiche minacce • Una società dell'UE sicura, aperta e democratica • Una assistenza sanitaria accessibile di alta qualità • Una crescita inclusiva e nuove opportunità di lavoro	➢ Supportare l'implementazione di: ✓ Strategia dell'Unione sulla sicurezza, ✓ Agenda antiterrorismo, ✓ dimensioni della sicurezza del nuovo patto sulla migrazione e l'asilo, ✓ Politiche dell'UE per la riduzione del rischio di catastrofi ✓ Strategia per la sicurezza marittima dell'UE

WP 2021-22 Corrispondenze obiettivi PNR- CLUSTER 3

WP-2021-22	PNR Ambito tematico Sicurezza per i Sistemi Sociali :
• **Resilient Infrastructure**	• **Sicurezza delle Strutture, Infrastrutture e Reti**
• **Disaster-Resilient Society for Europe**	• **Sicurezza Sistemi Naturali**
• Increased cybersecurity	• Cybersecurity

In termini generali gli impatti attesi dell'area PNR 2021-2027

- **"Sicurezza delle strutture, infrastrutture e reti" (organizzata in 4 articolazioni)**
- **«Sicurezza sistemi naturali» (organizzata in 4 articolazioni)**

rientrano tra quelli del cluster 3 di Horizon Europe, in particolare:

i) Riduzione delle le perdite dovute a disastri naturali, accidentali e provocati dall'uomo attraverso una migliore resilienza della società e una migliore gestione del rischio di catastrofi;

ii) Migliorare la resilienza e l'autonomia delle infrastrutture fisiche e digitali e le funzioni sociali vitali attraverso l'uso dell'innovazione tecnologica, nonché una migliore cooperazione tra le parti interessate;

iii) Affrontare Le minacce alla sicurezza in modo più efficace grazie a: una migliore conoscenza trasversale tra i diversi settori della sicurezza (approccio sistemico), una migliore attuazione del ciclo di ricerca e innovazione e una migliore diffusione dei risultati.

WP 2021-22 Corrispondenze obiettivi PNR- CLUSTER 3

Ambito tematico PNR CYBERSECURITY (presenta 6 articolazioni) :
Ambito tematico EU-CL3: Increased cybersecurity
Corrispondenze nelle Call 2021
Articolazione 4: Sicurezza dei servizi al cittadino e alle imprese

A. Trasparenza nel controllo di processi complessi
C. Privacy dei Dati

Articolazione 3: Tecniche e metodologie per la protezione delle risorse

C. IA per Cybersecurity e Cybersecurity per IA
D. Hardware Security e Hardware-based Security

WP 2021-22 Corrispondenze obiettivi PNR- CLUSTER 3

Ambito tematico PNR : CYBERSECURITY (presenta 6 articolazioni) :
Ambito tematico EU-CL3: INCREASED CYBERSECURITY
Corrispondenze nelle Call 2022

Articolazione 1: Intelligence and Incident response

A. *Metodologie e tecnologie per l'Intelligence*
B. *Offensive Security per finalità di difesa*
C. *Processi di incident response*
D. *Miglioramento delle capacità di difesa rispetto al malware*

Articolazione 2: Sicurezza dei sistemi cyber-fisici e delle infrastrutture di rete

A. *Standard, best practice e certificazioni cyber*
B. *Security, safety e privacy nei sistemi cyber-fisici*
C. *Security, safety e privacy in ambito industriale*

Articolazione 3: Tecniche e metodologie per la protezione delle risorse

A. *Crittografia*

Articolazione 5: Ecosistema della Cybersecurity

B. *Analisi e di gestione del rischio cyber*
C. *Security e privacy by design*

Articolazione 6: Infrastrutture di Ricerca per la Cybersecurity

A. *Rete Nazionale di Laboratori di Ricerca in Cybersecurity*

European Commission

Gender dimension in R&I content

Gender Dimension

Affrontare la dimensione di genere nella ricerca e nell'innovazione implica tenere conto del sesso e del genere nell'intero processo di ricerca e innovazione.

L'integrazione della dimensione di genere nei contenuti di ricerca e innovazione è obbligatoria, a meno che non sia esplicitamente dichiarato nella call

Centri di Ricerca ed Università dovranno avere un proprio GENDER EQUALITY PLAN – Pubblico da esporre sul sito con un programma di azioni e finaziamenti per ridurre il gender gap.

Security scrutiny

New in Horizon Europe

Le questioni di sicurezza saranno verificate sistematicamente in tutte le proposte di Horizon Europe (in Horizon 2020 sono state controllate solo le proposte presentate su argomenti contrassegnati come "sensibili alla sicurezza").
I controlli si basano su un'autovalutazione inclusa nella proposta.

Focus su:

- **Se la proposta utilizza o genera informazioni classificate UE**
- **Potenziale di abuso dei risultati (che potrebbe essere incanalato in criminalità o terrorismo, spionaggio industriale di modelli, progetti, brevetti, software ecc…)**
- **Se le attività comportano informazioni o materiali soggetti a restrizioni di sicurezza nazionale**

I controlli basati sull'autovalutazione possono innescare un esame di sicurezza approfondito

Security Appraisal Procedure

Security: Legal Basis

Regolamento Horizon Europe art. 20 sulla sicurezza:

Art. 20 (1): "Le azioni ... devono essere conformi ……alle norme sulla protezione delle informazioni classificate contro la divulgazione non autorizzata, compreso il rispetto di qualsiasi pertinente diritto nazionale e dell'Unione."

Art. 20 (2): »….., le proposte includono un'autovalutazione della sicurezza che identifichi eventuali problemi di sicurezza e specifichi come tali problemi saranno affrontati al fine di soddisfare il pertinente diritto nazionale e dell'Unione."

Art. 20 (3): "Se del caso, la Commissione o l'organismo di finanziamento effettua un controllo di sicurezza per le proposte che presentano problemi di sicurezza".

Horizon Europe Model Grant Agreement- Art. 13 e Allegato 5 su Riservatezza e Sicurezza:

Security Appraisal in HE: novelties!

- **Legal basis** in HE Regulation (Art. 20); valutare i problemi di sicurezza nelle proposte di ricerca non è solo una necessità, **ma anche un obbligo legale**!
- Avere un processo standardizzato per tutte le attività in **HE**..
- **Autovalutazione sulla sicurezza da parte dei partecipanti per tutte le proposte HE**. (presente nel modello di proposta)
- Possibilità di contrassegnare un **topic come sensibile alla sicurezza nel Work Programme**, (influenza l'iter del processo).
- **Set di materiale di orientamento** per tutti gli attori coinvolti (richiedenti, beneficiari, esperti nazionali).

Security Appraisal in HE: overview of the process

La procedura di valutazione della sicurezza **riguarda tutte le attività finanziate nell'ambito di Horizon Europee** comprende tre fasi principali:

- L'autovalutazione della sicurezza da parte del richiedente – **tutte le proposte;**
- La revisione della sicurezza da parte dell'autorità concedente, della Commissione e di esperti di sicurezza nazionale –attraverso **una selezione di proposte**;
- I controlli di sicurezza, da parte della Commissione o dell'ente finanziatore competente, se del caso, durante o dopo l'iter del progetto.

Al momento, i temi sensibili alla sicurezza riguardano Civil Security for Society e Space

Security Scrutiny

Composto da **esperti nominati in accordo con l'Autorità Nazionale per la Sicurezza** con l'obiettivo di **affrontare il potenziale uso improprio dei risultati del progetto** (ad esempio risultati che potrebbero essere incanalati in criminalità o terrorismo o risultati che potrebbero influire negativamente sulle infrastrutture critiche,o risultati che possono minare la produzione/furto di tecnologie di un dispositivo oggetto della ricerca)

Il controllo di sicurezza sarà effettuato nei seguenti casi:

Automaticamente, quando una proposta è stata presentata su un argomento sensibile alla sicurezza (nel nostro caso Civil security e Space) In altri casi, quando lo screening di sicurezza ha concluso che è molto probabile che la proposta contenga/sollevi problemi di sicurezza per i quali dovrebbero essere adottate misure di mitigazione.

Security Appraisal Scheme