La resilienza delle infrastrutture alla luce della nuova normativa europea: metodi e tecnologie

By **Vittorio Rosato & Maurizio Pollino** On **Apr 14, 2026**

La normativa europea sulle infrastrutture critiche sta evolvendo rapidamente, con l'introduzione di nuovi soggetti oltre che strutture fisiche nell'ottica della resilienza dei sistemi-Paese.

Il termine "Soggetto Critico", introdotto dalla Direttiva (UE) 2022/2557[1] (CER), segna un cambio di paradigma: non ci si riferisce più solo a "oggetti" (infrastrutture), ma a "soggetti" che erogano servizi essenziali – energia, acqua, trasporti, telecomunicazioni, finanza e sanità – che costituiscono l'ossatura portante delle società moderne. La loro nuova accezione di *entità*[2] ("Entità Critiche") riconosce una corrispondenza tra la componente fisica, materiale (strada, condotta idrica, rete di interconnessione, rete elettrica) e quella immateriale, di controllo (sistemi di sicurezza, *management*), sancendo la convergenza – ormai ineludibile – tra la sfera della protezione fisica e quella della protezione *cyber* definita dalla Direttiva (UE) 2022/2555[3](NIS2). Le due direttive sono state recepite in Italia nel 2024[4],[5].

La resilienza non è solo "resistere", ma la capacità di un'entità di prevenire, proteggere, rispondere e recuperare da incidenti che interrompono i servizi essenziali. In quest'ottica, il termine *resilienza* deve essere necessariamente declinato in una accezione *sistemica*. Un singolo sistema, se perturbato o parzialmente distrutto, trova supporto per il ritorno alla normalità non solo grazie alle sue proprie risorse (struttura, ridondanze, strategie di ripristino) ma anche, e soprattutto, grazie al supporto di altri sistemi in grado di fornire, a quello perturbato, servizi per il corretto ripristino delle funzioni. In questo senso, il termine resilienza è più che mai sinonimo di *adattività* e *collaborazione*. Questo fatto dipende dalla forte interdipendenza esistente tra le diverse "Entità Critiche" dato che queste usano per il loro funzionamento i servizi erogati dalle altre. Solo grazie a tale complesso insieme di collaborazioni, i singoli "Soggetti Critici" sono in grado di erogare correttamente e con continuità i loro servizi essenziali. . Ciò implica che, le interruzioni nell'erogazione dei vari servizi essenziali può avvenire sia perché una perturbazione colpisce *direttamente* il soggetto in questione (cioè danneggia o inibisce il funzionamento di una infrastruttura) ma anche *indirettamente*, a causa della mancanza di servizi attesi provenienti da una infrastruttura perturbata (effetti "a cascata").

Le Entità Critiche devono confrontarsi con minacce provenienti da ambiti molto diversi. Se in passato le sorgenti del rischio erano concentrate prevalentemente sugli eventi naturali[6] — che hanno dominato lo scenario delle minacce negli ultimi cinquant'anni — il panorama delle minacce sta cambiando drasticamente e le proiezioni per i prossimi decenni indicano una sequenza di rischi profondamente diversa (Fig. 1), in termini di rilevanza e probabilità, includendo alcune minacce che non hanno precedenti nella storia delle società. Sebbene i cambiamenti climatici e i rischi geodinamici rimangano prioritari per il territorio italiano, emergono minacce legate alla polarizzazione sociale e al confronto geoeconomico.

In questo scenario in trasformazione, sono state sviluppate soluzioni *sistemiche* che, da un lato, consentono di monitorare e analizzare con una prospettiva olistica lo stato di rischio di tutte le infrastrutture e, dall'altro, di predire e prevenire (laddove possibile) gli impatti provenienti da tutti i *driver* di rischio (in una cosiddetta visione "*all hazards"*).

I Cambiamenti Climatici (e i fenomeni indotti), oltre alla specifica situazione geodinamica del nostro Paese, richiedono una intensificazione del monitoraggio e dell'analisi del rischio delle infrastrutture che insistono su un territorio continuamente sottoposto a eventi naturali estremi e spesso non in grado di rispondere adeguatamente a tali perturbazioni. Per questo motivo l'utilizzo di strumenti ad hoc per il monitoraggio del territorio e delle infrastrutture in esso contenute assume una caratteristica di indifferibilità, in particolare in relazione a quanto i Paesi EU si sono impegnati a fare nell'ambito della richiamata Direttiva CER.

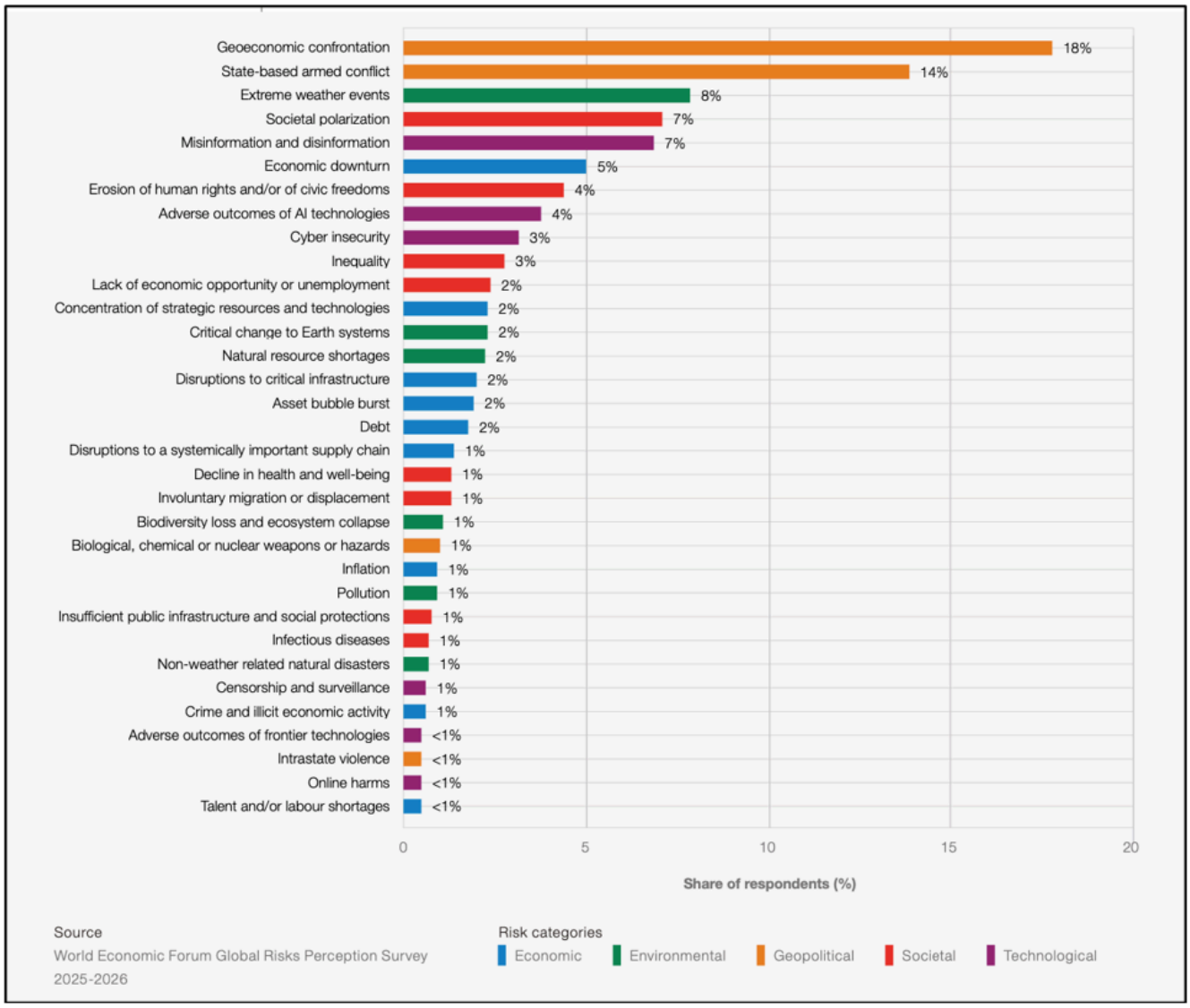

Fig. 1. Scenario attuale dei rischi globali, come stimato dal WEF Global Risk Report[5]. In ascissa è riportata la quota di rispondenti che hanno indicato la minaccia (in ordinata) nella propria lista di rischi futuri rilevanti per le entità critiche.

La resilienza di un sistema non è una proprietà statica, ma il risultato di una strategia integrata e dinamica, supportata da strumenti tecnologici adeguati e coerenti con la complessità dei contesti operativi.

In primo luogo, tale strategia deve garantire continuità operativa, assicurando il funzionamento dei sistemi di analisi, monitoraggio e supporto decisionale su base permanente (h24), così da intercettare tempestivamente segnali di degrado o di crisi.

In secondo luogo, è essenziale un approccio pervasivo e su larga scala, capace di operare su aree geografiche estese e di considerare le interdipendenze tra diverse Entità Critiche (energia, trasporti, telecomunicazioni, risorse idriche), che possono amplificare gli effetti di una perturbazione locale. Ciò richiede l'impiego di sistemi di monitoraggio distribuiti sul territorio, basati su reti di sensori, piattaforme di raccolta dati e architetture digitali interoperabili.

La strategia di resilienza deve inoltre adottare una prospettiva "*all hazards*", integrando tutte le componenti di rischio, siano esse naturali, tecnologiche o antropiche, e valutandone gli effetti combinati.

Infine, un elemento centrale è lo spostamento del focus dalla sola gestione dell'emergenza verso una fase previsionale e predittiva, orientata all'anticipazione degli eventi naturali e alla stima dei loro impatti potenziali. In questo quadro, modelli predittivi, analisi avanzate dei dati e strumenti di simulazione rappresentano fattori chiave per rafforzare la capacità adattiva e decisionale dei sistemi infrastrutturali critici.

Volendo, dunque, identificare le proprietà e le capacità che strumenti tecnologici debbano avere per svolgere un ruolo di supporto alla realizzazione di una strategia moderna per creare sistemi infrastrutturali resilienti possiamo identificare

- Copertura geografica di ampie aree e monitoraggio di infrastrutture o di loro elementi specifici;
- Continuità operativa del servizio (h24);
- Analisi predittiva di tutte le sorgenti di pericolo (eventi naturali, *cyber*, antropici) a supporto delle azioni di *preparedness*[7]
- Supporto alla definizione di strategie di resilienza.

La tecnologia ha contribuito alla costruzione di strumenti adatti per il monitoraggio e l'analisi del rischio operativo (h24) delle infrastrutture utilizzando, in particolare, la grande quantità di dati (statici e dinamici) riguardanti il territorio e degli eventi che lo caratterizzano attraverso sistemi di monitoraggio pervasivo che sfruttano sia tecnologie di *ground sensing* che di *remote sensing****[8]***. Tali strumenti, possono fornire, inoltre, un adeguato supporto alle *policy* di valutazione del rischio e definizione delle strategie di resilienza previste dalla Direttiva CER e dalle successive implementazioni nazionali[1-4].

In Italia vi è stato uno sforzo rilevante, effettuato da ENEA negli ultimi 15 anni, che ha portato alla realizzazione di un complesso sistema di Supporto alle Decisioni (DSS, *Decision Support System*) in grado di: (a) realizzare il monitoraggio degli asset critici del Paese, (b) valutare l'impatto di eventi naturali estremi in grado di ridurre o interrompere la funzionalità operativa delle EC, (c) valutare anche potenziali effetti a cascata, (d) effettuare una stima dell'impatto sulla popolazione (sia in temini di ampiezza geografica della perturbazione, sia in termini della rilevanza delle EC potenzialmente più compromesse nella loro funzionalità. Il sistema di supporto, denominato CIPCast[9], espone i propri risultati tramite una interfaccia (in Fig.2 un esempio del sinottico del DSS), che consente la mappatura e rappresentazione di problematiche e di possibili impatti di eventi sulle specifiche Entità Critiche[10].

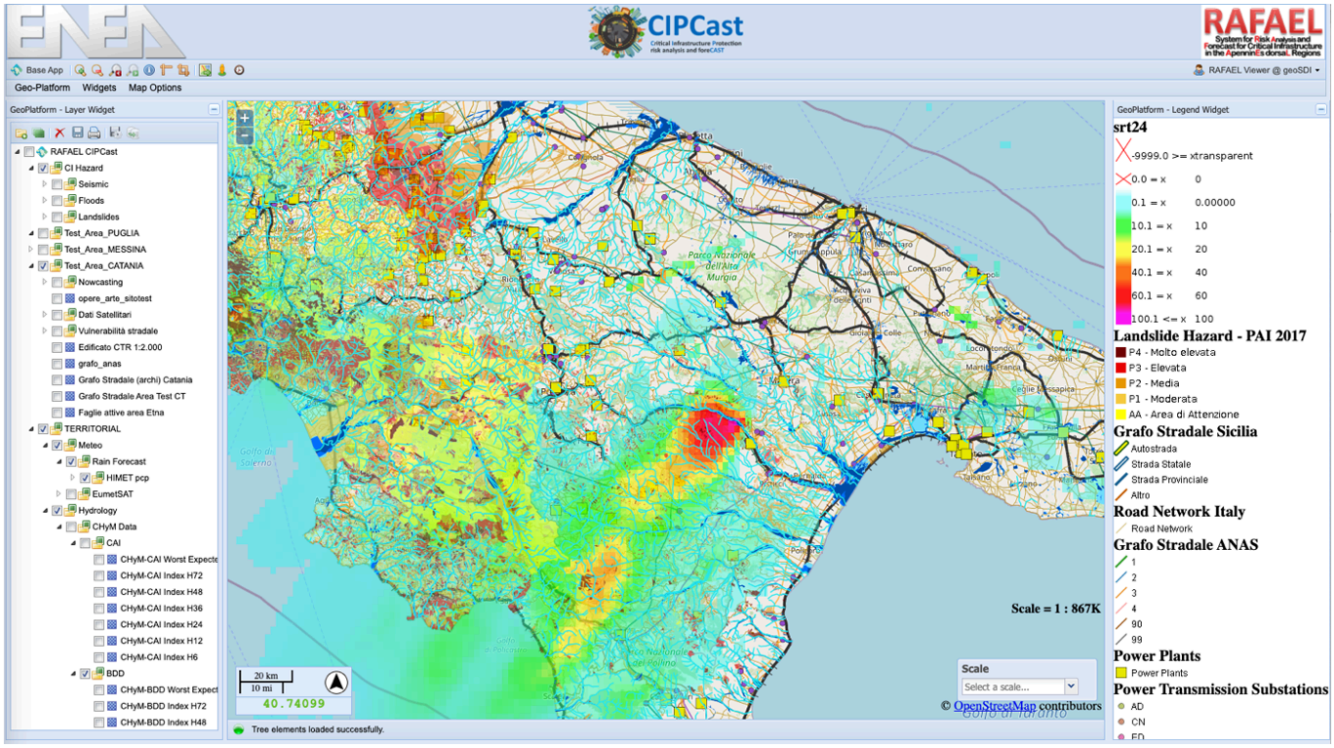

Fig. 2. Immagine del DSS che riporta il passaggio di una rilevante perturbazione piovosa con l'indicazione di alcune EC potenzialmente impattate dalla perturbazione con la visualizzazione di aree ad elevata pericolosità per esondazione.

Uno schema operativo che rende comprensibile l'azione di questi strumenti può essere riassunto illustrando quanto questi sistemi siano in grado di compiere per effettuare previsioni/valutazioni (e quindi fornire segnalazioni) di impatti in situazioni meteorologiche avverse sulle infrastrutture. La protezione delle infrastrutture utilizza le previsioni meteorologiche non solo per reagire a precipitazioni intense, inondazioni o ondate di calore, ma anche per pianificare l'allocazione preventiva delle risorse, implementare modificazioni strutturali temporanee per migliorare la robustezza, rafforzare i segmenti vulnerabili delle infrastrutture e coordinarsi con le autorità di gestione delle emergenze. Fondamentalmente, questo approccio si basa su tre principi fondamentali:

1. monitoraggio continuo
2. analisi predittiva

- localizzazione geospaziale del rischio.

Un moderno centro operativo di Entità Critica monitora i rischi che minacciano le prestazioni dell'infrastruttura prodotti da:

- eventi meteorologici (precipitazioni intense, ondate di calore)
- eventi idrologici/idraulici (alluvioni, esondazioni di corsi d'acqua)
- eventi geologici (terremoti, frane)
- incidenti informatici (a volte integrati)
- Eventi dolosi o accidentali
- problematiche indotte da fornitori e terze parti (interdipendenze)

Accanto alla gestione dei rischi materiali, è essenziale considerare il cosiddetto “rischio informativo”, capace di produrre impatti misurabili e talvolta paralizzanti sulle Entità Critiche. Le minacce informative non si limitano alla dimensione digitale, ma si traducono in criticità operative concrete.

In un moderno sistema di monitoraggio, la protezione fisica e quella informativa devono essere integrate in un unico modello operativo. I pericoli fisici possono infatti innescare “pericoli informativi” a catena: ad esempio, gli effetti di un’alluvione possono essere esasperati da notizie false su presunti crolli di dighe o contaminazioni idriche, provocando congestioni stradali che ostacolano i soccorsi. Le infrastrutture di pubblica utilità (energia, acqua, ospedali) sono le più vulnerabili agli *shock* della domanda generati da tali *rumors*.

Per ottenere una previsione a cascata realistica e accurata, è necessario che il modello di analisi includa:

- Monitoraggio OSINT (*Open Source Intelligence*): Una scansione automatizzata e costante della sfera informativa per rilevare anomalie, narrazioni distorte, tentativi di impersonificazione dell’operatore o chiamate alla mobilitazione.
- Modulo Hazard Informativo (IHM): Un sistema che, una volta accertata l’anomalia, applichi “moltiplicatori di rischio” al modello fisico per raccomandare azioni protettive tempestive.

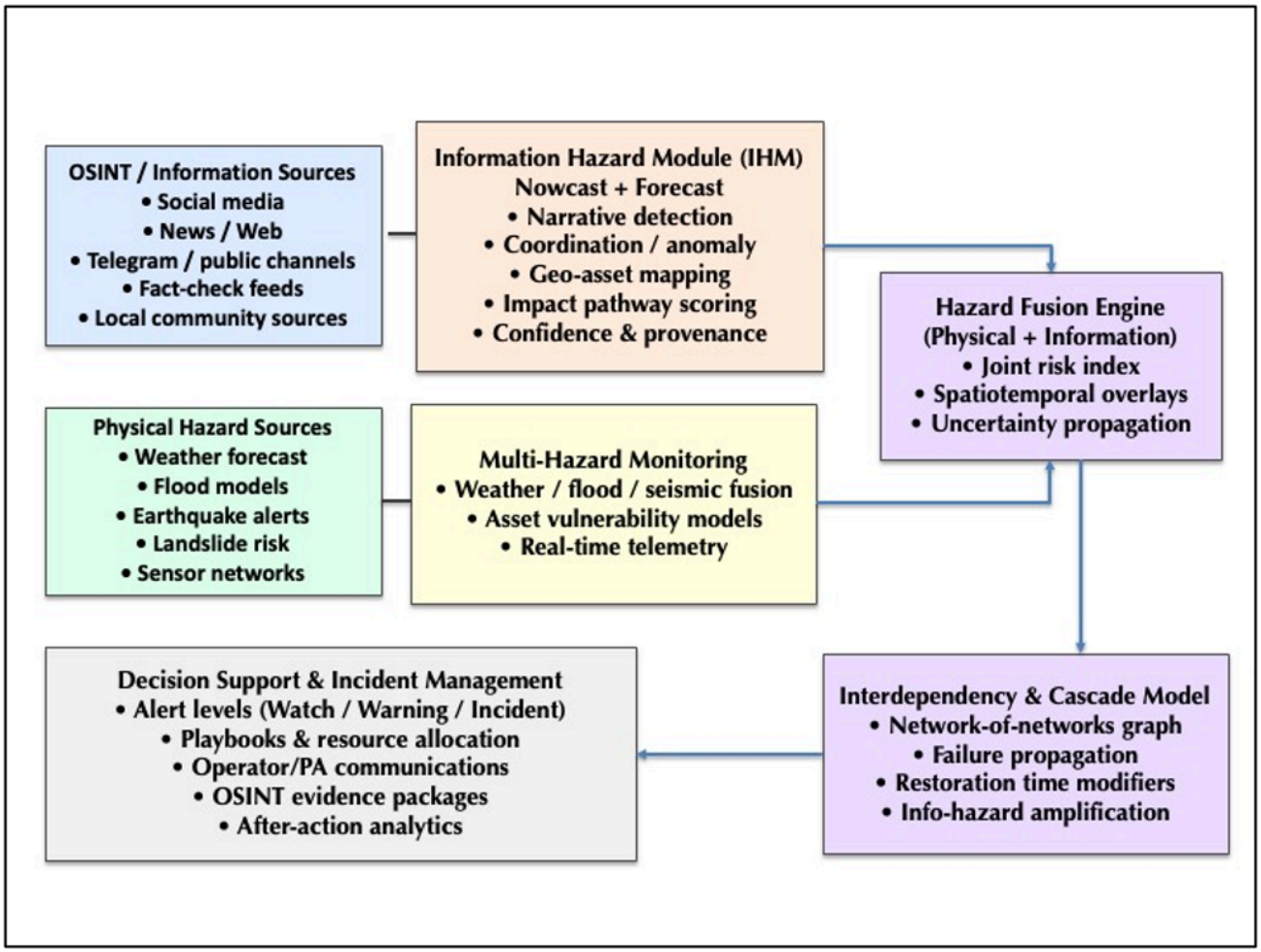

Fig. 3. Architettura del sistema di integrazione del monitoraggio dei rischi informativi in un centro operativo multi-rischio

Questo approccio risponde alla moderna filosofia di approccio "*all-hazards*", in cui l'ambiente informativo non è più considerato un elemento esterno, ma parte integrante del perimetro operativo che le Entità Critiche devono difendere h24.

In conclusione, la protezione delle Entità Critiche richiede oggi un superamento definitivo della visione settoriale a favore di un approccio sistemico, dinamico e proattivo. La resilienza non può più essere intesa come una semplice resistenza passiva, ma come una capacità adattiva alimentata dall'integrazione di tecnologie avanzate di monitoraggio e modelli di analisi previsiva. L'attuazione delle Direttive europee CER e NIS2 rappresenta il quadro normativo necessario per sancire la convergenza, ormai ineludibile, tra sicurezza fisica e logica. In questo scenario, strumenti di supporto alle decisioni come CIPCast si rivelano *asset* strategici per il Paese, permettendo di trasformare la complessità delle interdipendenze da fattore di vulnerabilità a elemento di forza attraverso la conoscenza e la cooperazione. La sfida futura risiederà nella capacità di integrare stabilmente la gestione dei rischi ibridi e della sfera informativa nei processi operativi, garantendo che la protezione dei servizi essenziali resti solida dinanzi a minacce globali sempre più imprevedibili e interconnesse.

Note:

[1] https://eur-lex.europa.eu/eli/dir/2022/2557/

[2] Il termine Entità è utilizzato come sinonimo di Soggetto, conservandone una accezione astratta.

[3] https://eur-lex.europa.eu/eli/dir/2022/2555

[4] Decreto legislativo 4 settembre 2024, n. 134

[5] Decreto legislativo 4 settembre 2024, n. 138

[6] World Economic Forum. Global Risk Report 2026; See for instance Sadhana Nirandjan et al. *Physical vulnerability database for critical infrastructure hazard risk assessments – a systematic review and data collection,* Natural Hazards and Earth System Sciences, **24**(12) (2024) 4341

[7] La preparatività (*preparedness*) è un insieme di azioni intraprese come misure precauzionali di fronte a potenziali eventi impattanti (su territorio, infrastrutture). Essere ***preparati*** aiuta ad evitare che gli eventi producano impatti molto negativi, riducendo quanto possibile i danni e consentendo, pertanto, di riguadagnare la situazione iniziale prima di quanto potrebbe essere fatto se l'evento, non predetto, non fosse stato contrastato.

[8] Belenguer-Plomer, M.A. et al., *Remote Sensing as a Sentinel for Safeguarding European Critical Infrastructure in the Face of Natural Disasters*. Appl. Sci. 2025, **15,** 8908.

[9] V. Rosato, F. Pistella, S. Stramondo, P. Clemente, D. Righini, M. Pollino & R. Setola (2024). *Decision Support System for the Monitoring and Risk Analysis of National Critical Entities*. In: Pickl, S., Hämmerli, B., Mattila, P., Sevillano, A. (eds) Critical Information Infrastructures Security. CRITIS 2023. Lecture Notes in Computer Science, vol 14599. Springer, Cham. https://doi.org/10.1007/978-3-031-62139-0_10; A. Di Pietro et al., *Design of DSS for Supporting Preparedness to and Management of Anomalous Situations in Complex Scenarios* in Managing the Complexity of Critical Infrastructures, eds. Roberto Setola, Vittorio Rosato, Elias Kyriakides and Erich Rome, Studies in Systems, Decision and Control Volume 90, Springer Open DOI 10.1007/978-3-319-51043-9; S. Taraglio et al., *Decision support system for smart urban management: resilience against natural phenomena and aerial environmental assessment*, Int. J. Sustainable Energy Planning and Management **24** (2019) 135 DOI: https://doi.org/10.5278/ijsepm.3338

[10] https://www.corriere.it/pianeta2030/26_marzo_11/piattaforma-analizza-rischi-terremoti-ondate-di-calore-enea-cipcast-6a3a62a4-1d35-11f1-91a3-5509096e603a.shtml

EU environment innovation science infrastructures Italy Europe technology

Vittorio Rosato & Maurizio Pollino

Vittorio Rosato is a Consultant at the Department of Engineering of the University Campus Bio-Medico in the area of Infrastructure Security and Risk Analysis.

Maurizio Pollino is Head of the Laboratory for the Analysis and Modelling of Critical Infrastructures and Essential Services (ICS) at ENEA, the Italian National Agency for New Technologies, Energy and Sustainable Economic Development.