AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Newsletter

ANNO 2025	n. 3/ 2025	marzo 2025

Quali saranno i rischi cyber nel 2025

L'obiettivo fondamentale per il 2025 del governo è posizionare l'Italia al vertice nella corsa globale verso l'innovazione tecnologica, creando un ecosistema fertile per la crescita di *start up* e imprese capaci di competere sul mercato globale. I finanziamenti rappresentano una leva cruciale per attirare talenti e investimenti nel settore, nonché per stimolare la ricerca e lo sviluppo di soluzioni innovative in ambiti-chiave per il futuro digitale del Paese.
L'allocazione dei fondi prosegue con politiche mirate a incentivare la ricerca e lo sviluppo nel campo delle nuove tecnologie. Con un occhio di riguardo verso l'IA, la sicurezza e il *cloud*, il governo intende non solo stimolare la nascita di nuove imprese ma anche consolidare la posizione di quelle già esistenti che si distinguono per capacità innovativa e potenziale di crescita.
Gli investimenti rappresentano un tassello fondamentale della strategia nazionale per la trasformazione digitale e per creare un ambiente fertile dove talenti e idee possano prosperare, generando un impatto positivo sull'economia e sulla società.
Nel 2025 gli attacchi alle infrastrutture critiche vedranno un ulteriore incremento di *ransomware* mirati a settori come energia, sanità e trasporti. Si prevede una crescita degli attacchi alle *supply chain* digitali, sfruttando *software* vulnerabili utilizzati nella gestione delle infrastrutture. L'interconnessione tra dispositivi IoT e sistemi OT sarà un altro vettore critico, poiché i *cyber*-criminali sfrutteranno sensori e controllori per compromettere operazioni essenziali.
L'IA verrà utilizzata sia dagli attaccanti per automatizzare azioni malevole, sia dai difensori per individuare anomalie e rispondere.
Gli Stati intensificheranno le loro campagne di *cyber-warfare*, puntando alle reti energetiche e alle telecomunicazioni. Per contrastare queste minacce, le organizzazioni devono adottare un approccio Zero trust, aggiornare sistemi OT e IoT e garantire segmentazione della rete per limitare i danni. È cruciale investire in tecnologie di *cyber-security* avanzate e nella formazione del personale per ridurre il rischio di compromissioni dovute a errori umani.
La collaborazione pubblico-privato sarà fondamentale per condividere informazioni sulle minacce e rispondere agli incidenti. Simulazioni di attacchi reali e piani di recupero testati ridurranno l'impatto delle intrusioni; mantenere aggiornati i sistemi e garantire *backup* sicuri saranno strategie essenziali per preservare la continuità operativa e la sicurezza delle infrastrutture critiche. Questa cooperazione è fondamentale per migliorare la sicurezza delle infrastrutture critiche, che dipendono da risorse, tecnologie e competenze distribuite tra i due settori. Queste sono gestite in gran parte da enti privati, ma la loro compromissione ha implicazioni per la sicurezza nazionale e il benessere pubblico, rendendo indispensabile un approccio collaborativo.
Il pubblico fornisce normative, Intelligence e coordinamento per affrontare le minacce, mentre il privato contribuisce con innovazione tecnologica, competenze operative e conoscenza diretta delle vulnerabilità dei sistemi. La condivisione tempestiva di informazioni sulle minacce, come indicatori di compromissione e strategie di mitigazione, è cruciale per prevenire attacchi e rispondere in modo efficace. Inoltre, attraverso questi partenariati, si possono sviluppare *standard* di sicurezza condivisi, simulazioni di attacco e strategie di ripristino che rafforzano la resilienza complessiva delle infrastrutture.

Questo tipo di collaborazione aiuta anche a ottimizzare le risorse, riducendo duplicazioni e lacune.

settore pubblico e privato.

Luisa Franchina
presidente dell'Associazione Italiana esperti in Infrastrutture Critiche

Luisa Franchina è stata Direttore Generale della Segreteria per le Infrastrutture Critiche (Presidenza del Consiglio dei Ministri 2010-2013). Ha pubblicato numerosi articoli e libri sulla sicurezza e sulla protezione delle infrastrutture critiche.

(*Airpress - gen. 2025 • n. 162)*

ATTIVITA' DELL'ASSOCIAZIONE

RINNOVO ASSOCIATIVO ANNO 2025

Il 31 dicembre 2024 è scaduto il periodo associativo. Invitiamo pertanto i signori soci a rinnovare per tempo l'iscrizione alla nostra associazione versando il relativo contributo.
La quota per il rinnovo individuale è di euro 50 e può essere versata con bonifico sul conto corrente presso Banca Intesa Business, IBAN IT17B0306909606100000114955, intestato a AIIC Associazione Italiana esperti in Infrastrutture Critiche, indicando come causale "rinnovo socio ordinario nome e cognome anno 2025".
Le quote e le modalità di rinnovo per i soci collettivi sono contenute nel sito AIIC www.infrastrutturecritiche.it. La nostra segreteria è a disposizione, per ogni informazione, alla mail segreteria@infrastrutturecritiche.it.

Ricordiamo agli associati che non hanno ancora rinnovato la quota: il socio rimane iscritto nel libro soci per tre mesi ma perde il diritto di partecipare alla vita sociale e il diritto di voto e viene cancellato dalle mailing list di distribuzione soci. Scaduti i tre mesi il socio decade per morosità e deve effettuare di nuovo l'iscrizione pagando anche la relativa quota una tantum.

PUBBLICAZIONE DI ARTICOLI DA PARTE DI SOCI E PARTECIPAZIONE AD EVENTI

Ricordiamo ai soci che nella pubblicazione di un articolo o di un libro **non è possibile** firmarsi qualificandosi come "Associazione Italiana esperti in Infrastrutture Critiche", in quanto solo chi ha la rappresentanza legale dell'Associazione può esprimersi a nome AIIC.
La stessa regola vale anche se si partecipa ad un evento in qualità di organizzatore, relatore o chairman.

La possibilità di pubblicare o partecipare ad eventi a nome AIIC deve essere approvata dal Consiglio Direttivo dell'Associazione su richiesta del socio che, pertanto, è pregato di contattare il CD con ragionevole anticipo.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

È invece raccomandato indicare, nel proprio profilo professionale, l'appartenenza ad AIIC, Associazione Italiana esperti in Infrastrutture Critiche, in qualità di socio.

NUOVO SITO WEB AIIC – FONTE UFFICIALE DELL'ASSOCIAZIONE

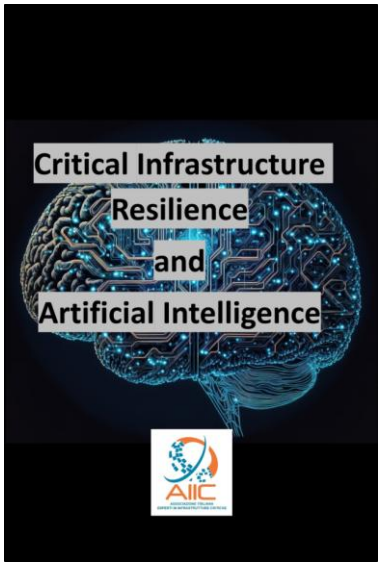
Ricordiamo che è attivo il nuovo sito dell'Associazione Italiana Esperti in Infrastrutture Critiche.
L'indirizzo è sempre **www.infrastrutturecritiche.it** ma il sito è stato completamente rinnovato, sia nelle veste grafica che nei contenuti e nelle funzioni a disposizione.
Vi invitiamo a consultarlo e anche a farci pervenire le vostre osservazioni: i vostri suggerimenti sono sempre preziosi e ci aiutano a migliorare il prodotto.

Vi ricordiamo inoltre che il sito web www.infrastrutturecritiche.it rappresenta la **fonte ufficiale dell'associazione**, accessibile a tutti, e contiene tutte le informazioni necessarie per un corretto svolgimento della vita associativa.

COLLABORAZIONE ALLE ATTIVITA' AIIC

Si invitano tutti i soci a partecipare alle attività sociali (newsletter, webinar, ecc.) inviando articoli, segnalazioni o dando la disponibilità a tenere webinar o seminari o a partecipare alla stesura e redazione della newsletter mensile.
La mail cui scrivere è segreteria@infrastrutturecritiche.it

NUOVO DOCUMENTO AIIC
"CRITICAL INFRASTRUCTURE RESILIENCE AND ARTIFICIAL INTELLIGENCE"



Il Gruppo di Lavoro AIIC dedicato all'analisi del ruolo e dell'impatto dell'Intelligenza Artificiale (IA) nelle infrastrutture critiche ha concluso i lavori ed ha pubblicato il relativo documento "Critical Infrastructure Resilience and Artificial Intelligence".

Questo documento è il risultato di un progetto congiunto coordinato da Sandro Bologna e realizzato con il contributo di *(in ordine alfabetico)* Silvano Bari, Glauco Bertocchi, Sandro Bologna, Luigi Carrozzi, Alberto Caruso DeCarolis, Raffaella D'Alessandro, Francesca Della Mea, Luisa Franchina, Adriana Peduto, Giorgio Pizzi, Alberto Stefanini, Maria Versaci.

Il rapporto esamina il ruolo e l'impatto dell'Intelligenza Artificiale (IA) nelle infrastrutture critiche, fornendo una panoramica globale di strategie, standard, considerazioni etiche e quadri normativi.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

L'obiettivo è identificare le best practice e offrire raccomandazioni per promuovere la resilienza e la sostenibilità delle infrastrutture critiche attraverso l'uso responsabile dell'IA.

Il documento è scaricabile dal sito www.infrastrutturecritiche.it

DOCUMENTI AIIC SU CAMBIAMENTO CLIMATICO

Vi informiamo che sono stati recentemente pubblicati alcuni documenti contenenti contributi del Gruppo di Lavoro AIIC su "Resilienza delle Infrastrutture Critiche e Cambiamenti Climatici".

Il Gruppo era costituito da
Silvano Bari, Glauco Bertocchi, Sandro Bologna, Luigi Carrozzi, Gianluca Cipriani, Elenio Dursi, Luisa Franchina, Andrea Agostino Fumagalli, Alberto Stefanini, Alberto Traballesi,

Il documento completo del Gruppo di Lavoro AIIC, pubblicato nel novembre del 2023, è disponibile per il download in formato PDF nel sito www.infrastrutturecritiche.it.
Il documento è in lingua italiana.

ONLINE IL NUOVO VOLUME DEL CNR-IRCRES "CAMBIAMENTO CLIMATICO E SOSTENIBILITÀ: UNA VISIONE MULTIDISCIPLINARE"

È uscito il nuovo volume "Cambiamento climatico e sostenibilità: una visione multidisciplinare", n. 21 dei Quaderni dell'Istituto di ricerca sulla crescita economica sostenibile (Cnr-Ircres) e disponibile online, che raccoglie otto contributi afferenti a diverse aree scientifiche che riescono a rappresentare in maniera articolata, inclusiva e aperta numerosi aspetti della questione ambientale, tema di ampio respiro e grande impatto etico, sociale ed economico.

Negli ultimi anni, il climate change ha assunto un'importanza trasversale nella cronaca quotidiana, nelle scienze e nelle arti. D'altronde, gli effetti del cambiamento climatico sono evidenti. La cronaca riporta con cadenza sempre più fitta disastri derivanti da cause climatiche – carestie, scioglimento dei ghiacci, inondazioni, frane – cui viene diffusamente attribuita un'origine antropogenica. Da qui, ne consegue che l'adozione di comportamenti di maggior sostenibilità ambientale sia il principale strumento di mitigazione e rallentamento di questa deriva.

Il volume, curato da Ugo Finardi, contiene contributi di **Silvano Bari**, **Glauco Bertocchi**, **Sandro Bologna**, Laura Bonato, Monica Cariola, **Luigi Carrozzi**, **Gianluca Cipriani**, Carmen Concilio, **Elenio Dursi**, **Luisa Franchina**, Chiara Franciosi, Filippo Fraschini, **Andrea Agostino Fumagalli**, Marta Giambelli, Antonio Gioia, Elena Melloni, Marina Morando, Anna Novaresio, Tommaso Pardi, Emanuela Reale, Andrea Orazio Spinello, **Alberto Stefanini**, **Alberto Traballesi**, Giampaolo Vitali, Isabella Maria Zoppi.

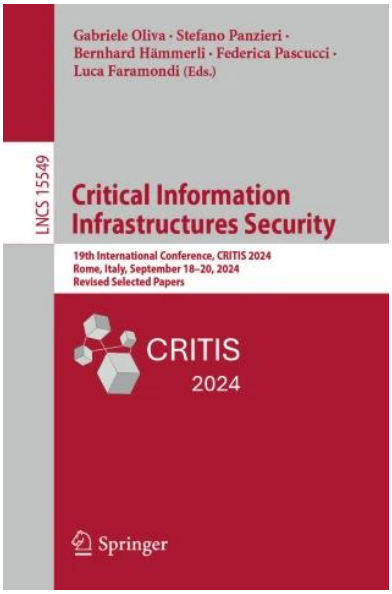
Questi i temi trattati all'interno dell'opera:

Resilienza delle Infrastrutture critiche e cambiamenti climatici
L'impatto dell'elettrificazione del settore automotive su lavoro, società e ambiente: un approccio olistico
Le certificazioni ambientali nelle industrie tessili, abbigliamento e pelletteria in Italia
Il ruolo dell'intelligenza artificiale e delle tecnologie robotiche nella transizione ambientale e nella governance climatica dei porti marittimi: il caso di studio di Genova
Cambiamento climatico: attività di ricerca e strategie delle università
Approcci basati sulla comunità per definire misure e strategie di adattamento al cambiamento climatico e di riduzione del rischio da disastri: un'analisi di letteratura grigia
Eco-music: rock per l'ambiente
«E sussurra canzoni tra le foglie». Cambiamento climatico e sostenibilità nella popular music italiana
Per informazioni:
Ugo Finardi - Cnr-Ircres
Area Ricerca di Torino - Strada delle Cacce, 73 TO
ugo.finardi@ircres.cnr.it

Il volume in formato pdf è disponibile al link

https://www.ircres.cnr.it/wp-content/uploads/2024/11/Q21_2024.pdf

PUBBLICAZIONE DEGLI ATTI DELLA CONFERENZA CRITIS 2024



Sono stati pubblicati, sotto forma di ebook e di volume cartaceo, gli atti del Convegno CRITIS 2024 su "Critical Information Infrastructures Security", tenuto a Roma nel periodo 18 - 20 settembre, 2024.

Uno dei Topics trattati è stato "Climate change implications in Critical Infrastructures and services" che riflette il tema trattato nel Rapporto AIIC pubblicato nel mese di Novembre 2023. La presentazione del nostro rapporto AIIC è stata effettuata dal dott. Sandro Bologna.

Il volume completo o il singolo capitolo "Resilience of Critical Infrastructures and Climate Change" possono essere acquistati nel sito di Springer Nature al link

https://link.springer.com/book/10.1007/978-3-031-84260-3

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

NEWS E AVVENIMENTI

Attuazione Direttiva (UE) 2022/2557 CER sulla resilienza dei soggetti critici: implicazioni per le imprese di sicurezza privata in Italia - La Direttiva (UE) 2022/2557 CER del Parlamento Europeo e del Consiglio relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio, adottata il 14 dicembre 2022, rappresenta un significativo avanzamento nel quadro normativo europeo per garantire la resilienza dei soggetti critici, ovvero quegli enti pubblici e privati che erogano servizi essenziali per il funzionamento delle società e delle economie moderne. L'Italia ha recepito questa Direttiva attraverso il Decreto Legislativo 134/2024, che mira a rafforzare la protezione delle infrastrutture critiche e a garantire la continuità operativa in caso di minacce fisiche, naturali o antropiche.
Il Decreto Legislativo 134/2024 definisce una serie di obblighi e misure che i soggetti critici e le autorità competenti devono adottare per migliorare la loro resilienza. Tra questi, spiccano

- la predisposizione di strategie nazionali,
- l'istituzione di un Comitato Interministeriale per la Resilienza (CIR) e
- l'adozione di strumenti di valutazione del rischio a livello nazionale e settoriale.

Questi elementi costituiscono il fulcro dell'adattamento italiano alla Direttiva CER *(Critical Entities Resilience)*, evidenziando un impegno verso un approccio integrato e coordinato alla protezione delle infrastrutture critiche.
La Direttiva si inserisce in un contesto più ampio di regolamentazione europea, integrandosi con la Direttiva (UE) NIS2 2022/20025, focalizzata sulla cybersicurezza, e con il Regolamento Delegato (UE) 2023/2450, che stabilisce un elenco di servizi essenziali per i soggetti critici. Mentre la Direttiva CER si concentra sulla resilienza fisica e operativa dei soggetti critici, la NIS2 si occupa della sicurezza dei sistemi informatici che supportano tali entità. Questo approccio integrato riflette l'interdipendenza tra sicurezza fisica e digitale, evidenziata da crescenti minacce ibride e transfrontaliere.
Il Regolamento Delegato (UE) 2023/2450 integra la Direttiva CER, stabilendo un elenco non esaustivo di servizi essenziali che gli Stati membri possono utilizzare per identificare i soggetti critici. Tale elenco aiuta a uniformare le metodologie di valutazione del rischio e a garantire una maggiore coerenza nell'attuazione delle norme in tutta l'Unione Europea.
(continua…)
https://www.snewsonline.com/attuazione-direttiva-ue-2022-2557-cer-resilienza-soggetti-critici-implicazioni-imprese-sicurezza-privata-italia/
S News - *Maria Cristina Urbano - 3 Febbraio 2025*

Energia 100% rinnovabili: mito o realtà? - Secondo Mark Jacobson, professore all'università di Stanford e uno dei massimi esperti globali in materia di energia, abbiamo già il 97% delle tecnologie necessarie. E non ci servono gas, nucleare, CCS e altre false soluzioni.
Quali tecnologie e quali politiche ci servono per una transizione verso 100% rinnovabili?
Una transizione globale dei sistemi energetici verso 100% rinnovabili è già possibile con le tecnologie esistenti. L'elettrificazione, combinata con l'energia eolica, solare e idroelettrica, può eliminare la dipendenza dai combustibili fossili. Senza dover ricorrere a soluzioni ipotetiche come il nucleare, compresi i reattori nucleari modulari di piccola taglia (Small Modular Reactors, SMRs), o la cattura e lo

stoccaggio del carbonio (Carbon Capture and Storage, CCS). Il tutto riducendo contemporaneamente i costi, le emissioni e i rischi ambientali.
Questo è il messaggio chiave che Mark Jacobson condivide nel suo libro del 2023 No Miracles Needed: How Today's Technology Can Save Our Climate and Clean Our Air, di cui è prevista una versione aggiornata nel 2025. Nel volume, il professore di ingegneria civile e ambientale della Stanford University analizza le tecnologie non necessarie, ma su cui molti governi e aziende stanno puntando.
Rinnovabili ha intervistato il professor Jacobson, uno dei massimi esperti globali in materia di energia e clima, sui suoi modelli di transizione energetica e sui piani per raggiungere un sistema basato al 100% sulle energie rinnovabili. (continua)
https://www.rinnovabili.it/energia/fotovoltaico/100-rinnovabili-possibile-mark-jacobson/
Rinnovabili - *Lorenzo Marinone – 11 febbraio 2025*

Le metropolitane urbane: un sistema di trasporto efficiente e sostenibile, ma con diverse sfide tecniche - L'Italia sta accelerando lo sviluppo delle metropolitane urbane, con 85 km di nuove linee previste in dieci anni, grazie a una crescente consapevolezza sull'importanza delle infrastrutture moderne. Durante le "Giornate Studio Fabre", il professor Chiaia ha evidenziato le sfide tecniche, come l'efficientamento dello scavo e la sicurezza, sottolineando il ruolo chiave della ricerca universitaria nell'innovazione del settore.
Nei prossimi 10 anni in Italia verranno realizzati 85 km di nuove metropolitane
Lo sviluppo delle infrastrutture urbane è un tema centrale per il futuro delle città italiane. Durante le "Giornate Studio Fabre", evento svoltosi a Perugia il 12 e 13 febbraio 2025, il professor Bernardino Chiaia del Politecnico di Torino ha affrontato il tema delle metropolitane urbane, mettendo in evidenza le sfide e le opportunità legate alla loro progettazione e realizzazione.
Negli ultimi anni, l'Italia ha visto un significativo aumento dell'interesse verso le metropolitane urbane come soluzione sostenibile ed efficiente per il trasporto pubblico. Chiaia ha sottolineato come nei prossimi dieci anni verranno costruiti circa 85 km di nuove linee metropolitane, una quantità che in passato ha richiesto oltre trent'anni per essere realizzata. Questo dato dimostra un'accelerazione nell'adozione di sistemi di trasporto sotterraneo, sintomo di una crescente consapevolezza da parte delle amministrazioni locali e della popolazione sull'importanza di infrastrutture moderne e funzionali. (continua)
https://www.ingenio-web.it/articoli/le-metropolitane-urbane-un-sistema-di-trasporto-efficiente-e-sostenibile-ma-con-diverse-sfide-tecniche/
Ingenio – *Bernardino Chiaia* ***-*** *19.02.2025*

Industrial System Cyberattacks Surge as OT Stays Vulnerable
Nearly a third of organizations have an operational system connected to the Internet with a known exploited vulnerability, as attacks by state and non-state actors increase.
Ransomware attacks on manufacturing, oil and gas, and other industrial sectors jumped significantly in 2024, as more groups emerged to target operational technology (OT); nearly a quarter of affected firms had to suspend operations.
Overall, nearly 1,700 ransomware attacks successfully breached industrial organizations last year, as measured by attackers' posts on dedicated leak sites. That's an increase of 87% over the previous year,

according to an OT/ICS report published by Dragos, an infrastructure security firm. The breaches led 25% of affected sites to halt operations, while 75% of attacks caused operational disruption to some degree, the company's report stated.

Those are conservative estimates, Robert Lee, CEO and co-founder of Dragos, said during a press call announcing the report. Overall, the number of ransomware attacks is underreported because of fear of reputational damage, he said.

"It's a much larger number than I think the public is aware of [because] there's not a huge incentive to report, and there's not a whole lot of value in reporting," Lee said. "Even if government wanted to get involved, it's like, what are you actually going to do?"

In tandem with the surge in attacker interest directed at OT systems, many of those systems remain vulnerable, according to a second report released last week by cyber-physical security firm Claroty. In a study of 1 million OT devices, the firm's researchers found that 40% of organizations have at least one asset insecurely connected to the Internet, and about a third (31%) have an asset connected to the Internet that also has a known exploited vulnerability

The vulnerabilities are often exposed because of expediency, says Grant Geyer, chief strategy officer at Claroty.

"A lot of why this happens is there's some emergency — there's a maintenance issue or production is down — and they need to connect their automation OEM to the asset to do maintenance troubleshooting or firmware upgrade," he says. "And so they will download TeamViewer or some other off-the-shelf remote access tool and implement it quickly, without multifactor authentication in place, so it's an open channel out to the Internet."

Manufacturing Attractive to Cyberattackers

The manufacturing sector stood out last year — and not in a good way, Geyer. says Forty-three percent of manufacturing organizations had a KEV linked to ransomware attacks; in contrast, the natural-resources sector had 22%, and the transportation sector had only 19%, according to Claroty.

"There's a higher propensity for manufacturing organizations to have cloud connectivity just as a way of doing business, because of the benefits of the public cloud for manufacturing, like for predictive analytics, just-in-time inventory management, and things along those lines," he says, pointing to Transportation Security Administration (TSA) rules governing pipelines and logistics networks as one reason for the difference.

"There is purposeful regulation to separate the IT-OT boundary — you tend to see multiple kinds of ring-fence layers of controls. ... There's a more conservative approach to outside-the-plant connectivity within logistics and transportation and natural resources," Geyer says.

The increased vulnerability of OT systems is not the only trend. (continua….)

https://www.darkreading.com/cyber-risk/industrial-system-cyberattacks-surge-ot-vulnerable

DarkReading- *Robert Lemos -February 25, 2025*

Cambiamenti climatici e alluvioni: perché è necessario cambiare modo di progettare le infrastrutture - I cambiamenti climatici impongono una radicale revisione delle strategie di progettazione e gestione delle opere idrauliche. Gli eventi alluvionali che hanno colpito l'Emilia-Romagna nel maggio 2023, seguiti da ulteriori episodi estremi nel settembre e nell'ottobre del 2024, rappresentano una chiara dimostrazione dell'urgenza di un nuovo approccio. Secondo **Armando Brath**, professore dell'Università di Bologna e presidente della Commissione tecnico-scientifica istituita

dalla Regione Emilia-Romagna, questi fenomeni mettono in crisi i modelli idraulici tradizionali e impongono una revisione profonda delle infrastrutture di difesa idraulica.
Gli eventi alluvionali registrati negli ultimi anni si sono rivelati di portata eccezionale, con tempi di ritorno stimati intorno ai 200 anni. La loro ripetizione in un arco temporale così ristretto – quattro eventi catastrofici in due anni sulle stesse aree – evidenzia l'inadeguatezza delle previsioni basate sulla statistica storica. Brath sottolinea come la probabilità di tali ricorrenze fosse estremamente bassa, pari a una su un milione, segnalando l'evidente necessità di riconsiderare le strategie di gestione del rischio idraulico.
La crescente frequenza di eventi meteorologici estremi richiede l'adozione di soluzioni più resilienti e sostenibili. Il rapporto della Commissione tecnico-scientifica, disponibile online, fornisce una serie di indicazioni per il miglioramento della gestione idraulica, tra cui la necessità di integrare modelli climatici aggiornati nei processi di progettazione delle opere.
Il dibattito si estende anche alle politiche di ripristino ambientale. La Direttiva per il ripristino della natura, approvata nell'estate del 2024, prevede la rimozione di opere idrauliche lungo circa 20.000 km di fiumi europei per ripristinare le condizioni naturali. Tuttavia, Brath evidenzia l'inapplicabilità di questa misura in contesti altamente antropizzati come l'Italia. Le aree colpite dalle alluvioni recenti erano storicamente paludi, ma la loro trasformazione in territori urbanizzati rende impensabile un ritorno alle condizioni originarie.
Piuttosto che la semplice eliminazione delle opere esistenti, la soluzione risiede in una progettualità innovativa, capace di coniugare sicurezza idraulica e sostenibilità ambientale. Occorre una pianificazione basata su dati scientifici aggiornati, che contempli interventi mirati, come l'adeguamento delle infrastrutture esistenti e la creazione di aree di espansione controllata delle acque. L'obiettivo è garantire una maggiore resilienza del territorio di fronte alle sfide poste dal cambiamento climatico.
(continua…)
https://www.ingenio-web.it/articoli/cambiamenti-climatici-e-alluvioni-perche-e-necessario-cambiare-modo-di-progettare-le-infrastrutture/
Ingenio - *Armando Brath | Redazione INGENIO- 26.02.2025*

Come usare al meglio gli applicativi di intelligenza artificiale - L'intelligenza artificiale viene utilizzata sempre più spesso nel mondo della tecnologia delle informazioni e questa tendenza potrà creare sia vantaggi che problemi, negli anni a venire. La norma UNI CEI ISO/IEC 42001 rappresenta un prezioso aiuto.
Questa norma è stata preparata dalla joint Technical committee ISO /IEC JTC 1 - information technology- sottocommissione SC42- intelligenza artificiale.
Questa norma, pubblicata in lingua inglese al dicembre 2023, è oggi disponibile anche in lingua italiana e ciò contribuirà in maniera determinante ad un utilizzo allargato.
L'obiettivo di questo documento è quello di aiutare le organizzazioni coinvolte a utilizzare al meglio applicativi di intelligenza artificiale, prendendo in considerazione questi aspetti:
l'uso dell'intelligenza artificiale per decisioni automatiche, talvolta non trasparenti e non chiaramente spiegabili, può richiedere l'adozione di sistemi specifici di gestione, che superano i sistemi tradizionali, l'uso della analisi dei dati e degli apprendimenti automatici, non basati su logiche umane, in fase di progettazione e sviluppo di sistemi, non solo aumenta le opportunità applicative dei sistemi di intelligenza artificiale, ma cambia anche le modalità con cui questi sistemi debbono essere sviluppati ed utilizzati, infine, molti applicativi di intelligenza artificiale modificano in continuazione il proprio comportamento, durante l'utilizzo normale. Occorre garantire che questa evoluzione automatizzata sia sempre rispettosa delle modalità di sviluppo inizialmente messe a punto.

Questa normativa, in particolare, illustra le modalità con cui è possibile utilizzare sistemi di gestione di applicativi di intelligenza artificiale, prendendo in considerazione il progetto iniziale, l'attuazione, la manutenzione ed il miglioramento continuo degli applicativi stessi.(continua…)
https://www.puntosicuro.it/sicurezza-informatica-C-90/come-usare-al-meglio-gli-applicativi-di-intelligenza-artificiale
Punto Sicuro - *Adalberto Biasiotti - 26/02/2025*

Former top NSA cyber official: Probationary firings 'devastating' to cyber, national security
Rob Joyce emphasized during a House hearing how important probationary employees are to NSA efforts to counter China and other threats in cyberspace.
The NSA's former top cybersecurity official told Congress on Wednesday that the Trump administration's attempts to mass fire probationary federal employees will be "devastating" for U.S. cybersecurity operations.
In testimony to the House Select Committee on the Chinese Communist Party, Rob Joyce, the former NSA cybersecurity director who retired from government service last year, warned lawmakers that countering Chinese hacking campaigns against critical infrastructure will require top-level cybersecurity talent at the NSA and other government agencies.
"Part of the defense is also having expertise and capacity in the government," Joyce said. "I want to raise my grave concerns that the aggressive threats to cut U.S. government probationary employees will have a devastating impact on the cybersecurity and our national security."
Probationary federal employees are those who have been in their current positions for less than a year, though in many cases those employees have worked other positions in the federal government over their careers.
Shortly after coming into office, the Trump administration, using the Office of Personnel Management, attempted to fire nearly all federal probationary employees en masse. A federal judge has temporarily blocked that order, citing a lack of authority by OPM to fire employees at other agencies.
OPM this week updated its guidance to reflect that firing decisions are made by individual departments and agencies, and many of those agencies have begun working to rehire or reinstate batches of fired workers in the weeks since they were dismissed.
Joyce, who spent 34 years at the NSA, emphasized how important those employees are in sustaining an aggressive stance against China in cyberspace.
"At my former agency, remarkable technical talent was recruited into developmental programs that provided intensive unique training and hands-on experience to cultivate vital skills," Joyce said. "Eliminating probationary employees will destroy a pipeline of top talent responsible for hunting and eradicating [Chinese] threats."
But he also lamented that the firings may have already harmed the NSA's ability to retain and attract top cybersecurity talent, as those affected seek more stable employment options. (continua…)
https://cyberscoop.com/joyce-china-probationary-firings-devastating-congress/
CYBERSCOOP - *Derek B. Johnson- March 5, 2025*

Massive botnet that appeared overnight is delivering record-size DDoSes
Eleven11bot infects video recorders, with the largest concentration of them in the US.

A newly discovered network botnet comprising an estimated 30,000 webcams and video recorders—with the largest concentration in the US—has been delivering what is likely to be the biggest denial-of-service attack ever seen, a security researcher inside Nokia said.
The botnet, tracked under the name Eleven11bot, first came to light in late February when researchers inside Nokia's Deepfield Emergency Response Team observed large numbers of geographically dispersed IP addresses delivering "hyper-volumetric attacks." Eleven11bot has been delivering large-scale attacks ever since.
Volumetric DDoSes shut down services by consuming all available bandwidth either inside the targeted network or its connection to the Internet. This approach works differently than exhaustion DDoSes, which over-exert the computing resources of a server. Hypervolumetric attacks are volumetric DDoses that deliver staggering amounts of data, typically measured in the terabits per second.
Johnny-come-lately botnet sets a new record
At 30,000 devices, the Eleven11bot was already exceptionally large (although some botnets exceed well over 100,000 devices). Most of the IP addresses participating, Nokia researcher Jérôme Meyer told me, had never been seen engaging in DDoS attacks.
Besides a 30,000-node botnet seeming to appear overnight, another salient feature of Eleven11bot is the record-size volume of data it sends its targets. The largest one Nokia has seen from Eleven11bot so far occurred on February 27 and peaked at about 6.5 terabits per second. The previous record for a volumetric attack was reported in January at 5.6 Tbps.
"Eleven11bot has targeted diverse sectors, including communications service providers and gaming hosting infrastructure, leveraging a variety of attack vectors," Meyer wrote. While in some cases the attacks are based on the volume of data, others focus on flooding a connection with more data packets than a connection can handle, with numbers ranging from a "few hundred thousand to several hundred million packets per second." Service degradation caused in some attacks has lasted multiple days, with some remaining ongoing as of the time this post went live. (continua…)
https://arstechnica.com/security/2025/03/massive-botnet-that-appeared-overnight-is-delivering-record-size-ddoses/
ARTECHINICA - Dan Goodin – 6 mar 2025

Reti terrestri e satellitari: l'integrazione con il 5G introduce nuove sfide
Il futuro della connettività globale dipende da un approccio integrato che sappia bilanciare innovazione e sicurezza. La protezione delle reti ibride Gnss Satcom-5G non può basarsi su singole tecnologie, ma deve essere il risultato di una strategia multilivello. Ecco vantaggi e rischi
L'integrazione tra reti terrestri e satellitari con il 5G sta rivoluzionando le telecomunicazioni, migliorando copertura e latenza, ma sta anche introducendo nuove sfide di sicurezza.
Gnss e Satcom evolvono con **tecnologie avanzate come crittografia quantistica e AI per contrastare spoofing e cyber attacchi**. Standard globali e **strategie multilivello** sono essenziali per garantire affidabilità e resilienza delle infrastrutture digitali.
Indice degli argomenti

- Come mitigare i rischi
- Il ruolo dell'AI
- L'interoperabilità tra Gnss, Satcom e reti terrestri

- **Prospettive future**

Reti di comunicazione: le sfide dell'integrazione con il 5G

L'integrazione tra reti di comunicazione terrestri e satellitari rappresenta una delle evoluzioni più rivoluzionarie della trasformazione digitale. Con l'avvento del 5G e la crescente domanda di connettività globale, la convergenza tra queste due tecnologie sta ridefinendo il panorama delle telecomunicazioni e della sicurezza informatica.

L'**Agenzia dell'Unione Europea per il Programma Spaziale (Euspa)** ha **pubblicato** il primo "Rapporto sulla tecnologia d'uso Gnss e Secure Satcom", che delinea le sfide e le opportunità di questa transizione, evidenziando come la fusione tra reti tradizionali e non terrestri (NTN) non sia più una visione futura, ma una realtà già in atto.

Questo processo pone **nuove questioni di governance, sicurezza e innovazione tecnologica, con implicazioni che spaziano dalla geopolitica alla vita quotidiana dei cittadini**.

I sistemi Gnss

Al centro di questa rivoluzione ci sono i **sistemi globali di navigazione satellitare (Gnss)**, infrastrutture essenziali per settori critici come i trasporti, la logistica, la gestione delle emergenze e le transazioni finanziarie.

Il **sistema Galileo** rappresenta il **pilastro della strategia spaziale europea e sta registrando significativi progress**i grazie all'introduzione del servizio di alta precisione (**Has**) e dell'autenticazione dei messaggi di navigazione (**Osnma**). Quest'ultima rappresenta una risposta diretta alle **crescenti minacce di spoofing e jamming**, attacchi sempre più sofisticati che possono compromettere la sicurezza e l'affidabilità dei segnali Gnss.

L'Osnma consente ai ricevitori di verificare l'autenticità dei dati trasmessi dai satelliti, riducendo il **rischio di manipolazioni** che potrebbero avere conseguenze disastrose, come **deviazioni di rotte di navi e aerei, frodi geolocalizzate o sabotaggi militari**.

Un approccio ibrido per integrare il Gnss con i sensori terrestri

Per garantire una navigazione affidabile in qualsiasi contesto, è sempre più necessario un **approccio ibrido, che integri il Gnss con sensori terrestri, dati inerziali e piattaforme di cloud computing**.

Questa strategia si rivela particolarmente utile in **ambienti urbani densamente popolati**, dove edifici alti e **interferenze elettromagnetiche** possono degradare il segnale, o in **scenari critici** come missioni di soccorso in zone colpite da disastri naturali.

La **resilienza delle infrastrutture di navigazione** si basa sempre più su architetture ridondanti e dinamiche, capaci di adattarsi in tempo reale alle condizioni operative e mitigare eventuali attacchi o guasti imprevisti. (continua…)

https://www.cybersecurity360.it/nuove-minacce/reti-terrestri-e-satellitari-lintegrazione-con-il-5g-introduce-nuove-sfide/

Cybersecurity360 *- Tommaso Diddi - 7 mar 2025*

Cybersicurezza dello Spazio: ecco i pilastri della strategia Ue

L'UE rafforza la sicurezza informatica con la Warsaw Call, stabilendo priorità per proteggere infrastrutture critiche e migliorare la cooperazione. Parallelamente, emergono strategie per garantire all'Ucraina alternative a Starlink, mentre avanza il progetto europeo IRIS2 per l'autonomia digitale

Il 5 marzo scorso, **Varsavia** ha **ospitato** un incontro dei ministri dell'UE responsabili della sicurezza informatica nel formato del Consiglio **"Trasporti, telecomunicazioni e energia"** (TTE), il primo in assoluto interamente dedicato alla **sicurezza informatica dell'Unione europea**.
L'incontro è culminato nell'adozione unanime del **Warsaw Call**, una dichiarazione che affronta le principali sfide della sicurezza informatica, quali il rafforzamento delle misure per il settore delle Tlc, inclusi i cavi sottomarini e le tecnologie emergenti, e la necessità di **accelerare l'impatto della Direttiva NIS 2 sulla cibersicurezza** delle reti e dei sistemi informativi.
Nel frattempo, il vice primo ministro polacco e ministro per gli Affari digitali, Krzysztof Gawkowski, ha **detto** che la Polonia – che sta finanziando l'uso militare e civile delle comunicazioni satellitari Starlink da parte dell'Ucraina – sta "cercando di diversificare" il suo accesso internet, in modo da garantire a Zelensky una copertura satellitare nell'eventualità in cui Elon Musk decidesse di interrompere l'accesso Starlink all'Ucraina. La dichiarazione di Gawkowski è stata rilasciata in merito all'annuncio, **riportato** per la prima volta dalla Reuters il 4 marzo, secondo cui l'UE sarebbe in trattative con la società di comunicazioni satellitari Eutelsat con sede a Parigi per fornire l'accesso Internet all'Ucraina.

Indice degli argomenti

Le priorità della Warsaw Call per la sicurezza informatica europea

Tra **i temi principali discussi dai ministri europei a Varsavia** rientravano la sicurezza informatica come fondamento della stabilità dell'UE, il rafforzamento della cooperazione civile-militare in risposta alle sfide emergenti e gli investimenti in una maggiore resilienza alle minacce su larga scala.
Per riaffermare il loro impegno verso una più stretta cooperazione in materia di sicurezza informatica, i membri del Consiglio, come detto, hanno adottato una dichiarazione ad hoc, la **Warsaw Call**. **Il documento funge da punto di riferimento fondamentale per i futuri sforzi dell'UE per proteggere lo spazio digitale e migliorare la resilienza in mezzo alle crescenti sfide geopolitiche**.
Esso stabilisce **tredici raccomandazioni, approvate dai ministri e dai rappresentanti degli stati membri.**

La necessità di meccanismi di coordinamento e risposta agli incidenti informatici più efficaci

Durante l'incontro, i partecipanti hanno concordato che investire nella resilienza digitale dell'Europa deve andare di pari passo con l'istituzione di meccanismi di coordinamento e risposta agli incidenti più efficaci a livello UE.
La Commissione europea era rappresentata da Henna Virkkunen, vicepresidente esecutivo per la sovranità tecnologica, la sicurezza e la democrazia, che ha sottolineato come **l'attuazione degli impegni delineati nell'appello di Varsavia sarà fondamentale per la futura resilienza digitale dell'UE**. Al dibattito hanno partecipato anche i direttori esecutivi dell'ENISA (l'Agenzia dell'UE per la

sicurezza informatica) e dell'ECCC (il Centro europeo di competenza per la sicurezza informatica), agenzie che svolgono un ruolo nel rafforzamento della resilienza informatica dell'UE.

Protezione dei cavi sottomarini e implementazione della direttiva NIS2

Il Warsaw Call delinea **sei aree chiave che dovrebbero guidare gli sforzi dell'UE in materia di sicurezza informatica: (**continua…)

https://www.agendadigitale.eu/mercati-digitali/cybersicurezza-e-spazio-i-pilastri-della-nuova-strategia-geopolitica-ue/

AGENDADigitale *- Gabriele Iuvinale, Nicola Iuvinale - 10 mar 2025*

Agenti AI, la verità oltre l'hype: potenzialità, rischi e miti da sfatare

Gli agenti AI superano i limiti del prompt engineering permettendo interazioni più complesse con gli LLM. Nonostante le potenzialità, persistono problemi di affidabilità e determinismo che rendono essenziale il controllo umano, suggerendo un approccio cauto alle applicazioni autonome

Il t**ema dell'Agentic AI** sta emergendo come un tema caldo dell'AI. Il passaggio da AgenticAI ad "AgenticHype" rischia di diventare molto breve. Ormai **aggiungere "AI" dietro a qualcosa** sta diventando una abitudine di marketing e ricorda molto quando negli '90 correva la moda di aggiungere "ware" perché questo dava quel "technical flavor" necessario a rendere tutto più "tecnologico".

Indice degli argomenti

Il fenomeno dell'agentic AI tra hype e realtà

Sono usciti molti articoli, post e perfino studi di alcune società di consulenza o entità varie che partono da alcune considerazioni condivisibili sugli agenti per poi spingersi verso narrazioni che superano di gran lunga la fantascienza senza nemmeno lo stile della Cerchiamo di capire in modo semplificato cosa sono realmente gli agenti AI, come possono essere utilizzati al meglio, cosa ci si può aspettare e soprattutto cosa non è realistico aspettarsi. Infine, quali sono i rischi e i limiti degli agenti che non risolvono i problemi posti dall'uso dell'intelligenza artificiale (che io preferisco chiamare intelligenza aumentata visto che da sola non è in grado di fare poco o niente).

Perché gli agenti AI sono stati creati: oltre i limiti del prompt engineering

Prima di andare a capire cosa sono gli agenti bisogna chiederci il perché siamo andati a creare cose complicate, non bastava la prompt engineering?

Il prompt riesce a risolvere molte cose, esistono tecniche molto sofisticate che consentono di modificare il comportamento degli LLM in modo da fargli eseguire compiti anche molto complessi. Tuttavia, per arrivare ad attività sofisticate sarebbe necessario creare prompt molto lunghi e complessi e questo, oltre ad essere particolarmente complesso, diventa anche inefficace. In questo ultimo anno i LLM sono cresciuti molto nella capacità di comprendere richieste ma ancora non abbastanza da soddisfare le nostre esigenze.

A questo punto nasce l'esigenza di creare degli agenti che sono delle integrazioni software e che consentono di scomporre le richieste all'LLM in modo che azioni più semplici possano essere eseguite

meglio. (in realtà le cose sono molto più complesse ma possiamo sintetizzarle per chiarezza e brevità in questo modo)

Caratteristiche fondamentali degli agenti AI e loro architettura

Partiamo da una definizione che può aiutarci a comprendere meglio di cosa parliamo:
Un agente è definito come un sistema in grado di interpretare e/o ragionare sulle intenzioni di un utente, cercando di soddisfare i desideri e le esigenze dell'utente, pur comprendendone capacità e limiti.
Per ottenere questo risultato abbiamo bisogno che vi siano almeno alcune di queste caratteristiche:

- **Percezione**

La capacità di percepire e interpretare l'ambiente circostante o flussi di dati rilevanti.

- **Interattività**

La capacità di interagire in modo efficace con il proprio ambiente operativo, inclusi utenti, altri sistemi di intelligenza artificiale e fonti di dati o servizi esterni.

- **Persistenza**

La capacità di creare, mantenere e aggiornare ricordi a lungo termine sugli utenti e sulle interazioni chiave.

- **Reattività**

La capacità di rispondere ai cambiamenti nel suo ambiente o ai dati in arrivo in modo tempestivo. Farlo bene dipende fortemente da solide capacità percettive.

- **Proattività**

Capacità di anticipare esigenze o potenziali problemi e di offrire suggerimenti o informazioni pertinenti senza essere esplicitamente sollecitati, rimandando comunque la decisione finale all'utente.

- **Autonomia**

Capacità di operare in autonomia e di prendere decisioni entro parametri definiti.
Ora già da qui dovrebbe risultare complicato estrarre queste cose da un LLM che, non dimentichiamolo mai, prevede parole sulla base di come è stato addestrato e dunque è una probabilità il fatto che prevedendo bene il linguaggio riesca a rispondere in modo sensato alle nostre richieste.
Questo risultato possiamo raggiungerlo in due modi principali, il primo **costruendo una catena di oggetti software concatenati nel quale ogni "oggetto" viene specializzato in qualcosa** e viene eseguito in una certa sequenza per produrre un risultato che può essere utilizzato da un altro oggetto (un workflow o processo con una serie di passi definiti e una certo grado di rigidità nei compiti) oppure creare agenti che a fronte di una richiesta sono in grado di elaborare una strategia partendo da un foglio bianco di eseguirla utilizzando dei tool software (molto flessibili e adattabili ad ogni evenienza). (continua…)
https://www.agendadigitale.eu/cultura-digitale/agenti-ai-la-verita-oltre-lhype-potenzialita-rischi-e-miti-da-sfatare/
AGENDADigitale *Paolino Madotto - 10 mar 2025*

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

NOTIZIE D'INTERESSE:

Le indicazioni per chi vuole iscriversi come nuovo socio sono contenute nel sito AIIC al link *http://www.infrastrutturecritiche.it/new/per-iscriversi/*

Preghiamo i soci che, per vari motivi, modificano la loro anagrafica (recapiti telefonici, indirizzo email o altro) di comunicare I nuovi dati a segreteria@infrastrutturecritiche.it. La mancanza di tali comunicazioni potrebbe impedire, al socio, la ricezione delle comunicazioni.

RIFERIMENTI DELL'ASSOCIAZIONE

AIIC è una associazione apolitica il cui scopo è promuovere attività e conoscenze nell'ambito delle infrastrutture critiche, della loro gestione, protezione e sicurezza.

Per maggiori informazioni sull'Associazione inviare una mail a

segreteria@infrastrutturecritiche.it

o visitate il sito

www.infrastrutturecritiche.it

ATTENZIONE

Per ricevere questa newsletter è necessario inviare una richiesta all'indirizzo
segreteria@infrastrutturecritiche.it

L'iscrizione alla newsletter NON comporta alcun onere e non è richiesta la comunicazione di alcun dato personale ad eccezione dell'indirizzo di posta elettronica.

Sede operativa e servizio di segreteria	AIIC c/o NITEL – via Urbino 31 – 00182 ROMA Tel. +39 06 64871209 E-mail: segreteria@infrastrutturecritiche.it
Gruppo di user all'interno della community	AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirsi al gruppo si può usare il link http://www.linkedin.com/ groups/96335
Versione stampabile della newsletter	Nella sezione "Newsletter"del sito http://www.infrastrutturecritiche.it è disponibile l'archivio delle Newsletter.
Comitato di Redazione	Glauco Bertocchi Silvano Bari *ai quali potete inviare suggerimenti e quesiti scrivendo a:* *segreteria@infrastrutturecritiche.it*

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

La NewsLetter ha lo scopo di rendere note le principali informazioni nell'ambito delle Infrastrutture Critiche e le attività dell'Associazione Italiana esperti in Infrastrutture Critiche (AIIC). Tutti i contenuti relativi alla sezione NEWS e Eventi sono pubblici on line e di proprietà dei rispettivi editori.