economia
Cybersicurezza: Ciardi (Acn) 'questo mondo è figlio dell'iperconnessione tra dati'

289 words
5 March 2026
15:35
Adnkronos - General News
GENNEW
Italian

Roma, 5 mar. (**Adnkronos**) -

"L'esempio della Jaguar Land Rover" vittima di un cyberattacco lo scorso agosto "ci dà l'opportunità di riflettere su come colpire un'azienda economica produttrice di automobili, e che incide sul pil di un paese con 5000 aziende di indotto, significhi andare a colpire, a cascata, il tessuto economico di altri paesi, essendo l'indotto non limitato ad un unico territorio. In sostanza si tratta di una crisi sistemica da affrontare in modo multifattoriale, poiché questo mondo è figlio dell'iperconnessione tra dati che assumono un valore in base alla relazione tra loro, delineando così il contesto". Lo ha detto Nunzia Ciardi, vicedirettrice generale Acn - Agenzia cybersicurezza nazionale - nel suo intervento a **Cybersec**, la conferenza internazionale in corso a Roma, organizzata dal quotidiano Cybersecurity Italia e giunta alla sua 5^ edizione.

"Sono partita da quest'esempio nel Regno Unito - spiega Ciardi - perché è la prova plastica di quanto ormai lo scenario digitale impatti su ogni aspetto della vita quotidiana di ciascuno di noi, oltre che sulla vita economica e sociale di un paese; in pratica ricade sulla trama che avvolge ogni aspetto della vita digitale e reale".

Fondamentale, però, la capacità umana nella gestione dello scenario: "Ci garantisce un'enorme possibilità di progresso e di performance produttiva, ma allo stesso tempo di limitare i rischi". E ancora: "Dobbiamo mettere l'uomo al centro, ma la capacità umana non può fare a meno di essere qualificata per controllare la costante sollecitazione al dominio cognitivo della persona, una sollecitazione che avviene tramite agenti automatici dell'intelligenza artificiale e che impattano, appunto, sulla capacità cognitiva delle persone, sulla loro opinione e sulle democrazie".

(Redazione/**Adnkronos**)

Document GENNEW0020260305em3500tph

economia
Cybersicurezza: Rizzi (Dis) 'Cambiato il concetto di dominio: oggi spazio oltre l'atmosfera'

420 words
5 March 2026
12:45
Adnkronos - General News
GENNEW
Italian

Roma, 5 mar. (**Adnkronos**) -

"Fino a qualche anno fa i domini che costituivano la sovranità erano ben individuati, oggi questo concetto di dominio si è espanso enormemente sia a livello Nato, con l'identificazione del dominio cyber, sia nel riconoscimento dello spazio oltre l'atmosfera". Esordisce così Vittorio Rizzi, direttore generale Dis - Dipartimento delle informazioni per la sicurezza, alla 5^ edizione di **Cybersec**, la conferenza internazionale in corso a Roma e organizzata dal quotidiano Cybersecurity Italia. Il suo articolato intervento poi prosegue: "Alla luce di ciò, è evidente che il concetto di minaccia si fa molto più esteso e ne parliamo in ottica di multidominio e multidimensione. Basti pensare all'esempio dell'opera di jamming su un satellite di qualche tempo fa: faceva backup dei dati in un gasdotto che passava sotto il mare a centinaia di metri e quindi distante dallo spazio, ma nonostante ciò creava il cosiddetto 'deep blue', una minaccia a qualcosa che invece si trovava sotto il mare".

E aggiunge ancora: "Quest'esempio è la fotografia plastica di quello che è il concetto di multidominio e multidimensione della minaccia stessa. Oggi viviamo in un tempo in cui l'intelligence ha l'obbligo, previsto dalla legge 124, di fare una relazione, e proprio questa relazione fotografa la minaccia in un'ottica prospettica, guardandola attraverso la lente di quello che è il motore che sta incidendo sull'intimidazione, ovvero l'innovazione". "L'innovazione - continua Rizzi - è uno dei principali fattori che incidono sulla sicurezza del paese, accelerando il ritmo e la portata di ogni minaccia".

Il direttore generale di Dis fotografa anche l'epoca attuale: "Ogni stagione dell'umanità ha una sua grammatica del potere, quella che noi oggi dobbiamo seguire ci impone una postura come intelligence a protezione della sovranità e dell'integrità degli interessi del nostro paese, guardando a due profili". E ancora: "Da un lato il cambiamento dell'ordine mondiale liberale. Non possiamo non tenere conto di ciò che è successo a Davos con il discorso divenuto virale del leader canadese che racconta di come il mondo sia cambiato in uno spazio temporale molto ridotto, ed io stesso l'ho visto e vissuto nella mia vita. Questo significa che il nostro spazio su questo pianeta è contenuto: siamo passati dalla caduta del muro di Berlino all'era della globalizzazione, che ci è parsa un'era di benessere in cui le catene del valore si integravano costituendo progresso per tutti".

(Redazione/**Adnkronos**)

Document GENNEW0020260305em3500izg

economia
Cybersicurezza: Gabrielli (Polizia postale), 'no limiti tecnici rispetto a capacità investigative'

273 words
4 March 2026
18:21
Adnkronos - General News
GENNEW
Italian

Roma, 4 mar. (**Adnkronos**) - "Bisogna far crescere responsabilità e competenze sia nel settore pubblico sia in quello privato e non bisogna avere paura di affrontare temi come il bilanciamento tra privacy e investigazione. Non possiamo permetterci limiti tecnici rispetto alle capacità investigative: una comunicazione che passa in chiaro è intercettabile se autorizzata da un giudice, una che passa su una piattaforma spesso non lo è. La tecnologia non può essere un limite, il limite deve essere giuridico" Lo ha dichiarato Ivano Gabrielli, direttore del Servizio Polizia postale e della sicurezza cibernetica, intervenendo a **Cybersec** 2026, la conferenza internazionale promossa e organizzata dal quotidiano Cybersecurity Italia in collaborazione con la Polizia di Stato, nel panel dal titolo 'Cybercrime e cyberwar: norme, geopolitica e cybersecurity per una Difesa comune'.

"Oramai – sottolinea Gabrielli - la cybersicurezza è diventata un fattore geopolitico al pari di altri settori come quello energetico o delle materie prime pregiate. Avere capacità autonoma di costruire sistemi adeguati di cybersicurezza significa mettere al sicuro buona parte della nostra economia, della nostra democrazia e del nostro sviluppo futuro. Il fattore digitale è un fattore abilitante per qualsiasi tipo di evoluzione e oggi va visto in tale ottica".

Gabrielli ha sottolineato come il Paese si sia dotato di una vera e propria architettura per la sicurezza cibernetica. "Il Paese si sta organizzando, esiste un'architettura per la sicurezza che vede quattro componenti fondamentali: la Polizia di Stato, l'Acn (Agenzia per la cybersicurezza nazionale), l'intelligence e la Difesa. Queste strutture oggi collaborano per elevare il livello di sicurezza dell'intero Paese".

(Redazione/**Adnkronos**)

Document GENNEW0020260304em340116y

cronaca
Cybersicurezza: Gabrielli (Polizia Postale), 'tecnologia e privacy non siano limiti a indagini'

161 words
4 March 2026
14:49
Adnkronos - General News
GENNEW
Italian

Roma, 04 mar. - (**Adnkronos**) - "Non bisogna avere paura di affrontare alcuni temi per esempio legati al bilanciamento tra privacy e investigazione. Non possiamo permetterci oggi di avere un limite tecnico rispetto a quelle che sono le capacità investigative. Una comunicazione che oggi passa in chiaro su un telefono è intercettabile qualora ricorrano i requisiti, qualora un giudice l'autorizzi, mentre una comunicazione che passa su una piattaforma non lo è". Lo ha detto il direttore del Servizio polizia postale e per la sicurezza cibernetica Ivano Gabrielli a margine del **CyberSec**. "Bisogna dare tutela effettiva ai nostri diritti: quando siamo oggetto di attacchi informatici o quando i nostri bambini vengono adescati online bisogna permettere di poter aggredire a livello investigativo spazi e ambiti che oggi sono preclusi soltanto dal punto di vista tecnologico - ha aggiunto - La tecnologia non può essere un limite, il limite deve essere giuridico".

(Sod/**Adnkronos**)

Document GENNEW0020260304em3400ob1

cronaca
Iran: Frattasi (Acn), 'no segnali pericoli cyber imminenti per Italia'

154 words
4 March 2026
14:33
Adnkronos - General News
GENNEW
Italian

Roma , 4 mar. - (**Adnkronos**) - "Nell'immediatezza del conflitto scoppiato sabato abbiamo costantemente monitorato la minaccia per scorgere anche i segnali più deboli che potessero indicare un attacco contro il nostro paese. In questo momento dobbiamo pesare le parole ma non abbiamo segnali che ci dicano che c'e' un pericolo grave e imminente per l'Italia anche dal punto di vista cibernetico, però sono dati che possono cambiare anche nel giro di poche ore o di pochi giorni". Lo ha detto il direttore generale dell'Acn Bruno Frattasi a margine del **CyberSec**. "Noi comunque continuiamo a osservare con grande attenzione ciò che accade nel web e ciò che può accadere anche con riguardo alla nostra superficie digitale - ha aggiunto - lo facciamo attraverso una cooperazione stretta con tante amministrazioni, innanzitutto con quella dell'intelligence, poi naturalmente con la Polizia e la Difesa".

(Sod/**Adnkronos**)

Document GENNEW0020260304em3400n85

politica
Referendum: Piantedosi, 'tempi ancora non maturi per voto elettronico'

49 words
4 March 2026
14:16
Adnkronos - General News
GENNEW
Italian

Roma , 04 mar. - (**Adnkronos**) - Sul voto elettronico "abbiamo fatto delle sperimentazioni, ma ancora i tempi non sono maturi, quindi abbiamo mantenuto i sistemi tradizionali".Lo ha detto il ministro dell'Interno Matteo Piantedosi nel corso del **CyberSec**.

(Sod/**Adnkronos**)

Document GENNEW0020260304em3400mau

cronaca
Referendum: Piantedosi, 'pronti a contrastare elementi destabilizzazione discussione pubblica'

178 words
4 March 2026
14:13
Adnkronos - General News
GENNEW
Italian

Roma , 04 mar. - (**Adnkronos**) - "E' importante che non ci siano nell'immediatezza dell'apertura delle urne, compromissioni, alterazioni, quindi elementi di disturbo, fatti magari anche volontariamente per creare formule di destabilizzazione della discussione pubblica. Su questo ci siamo organizzati, più che altro ho creato dei sistemi di doppio binario in modo da rendere meno attaccabile l'intero sistema". Lo ha detto il ministro dell'Interno Matteo Piantedosi nel corso del **CyberSec**, rispondendo a una domanda sulla sicurezza del voto del Referendum.

“Quando ci sono le tornate elettorali tra i temi che sono meno sostanziali, ma di grande importanza, c'è la comunicazione immediata del dato - ha aggiunto - I sistemi di comunicazione, per esempio dei dati dalla periferia al centro, transitano su reti digitali e quindi noi ci siamo preoccupati di garantire che ci fosse una corretta tenuta di questi dati, seppur non ci sia la possibilità di alterare il dato sostanziale in quanto tale perché la proclamazione dei risultati verrà fatta sempre con dei sistemi tradizionali”.

(Sod/**Adnkronos**)

Document GENNEW0020260304em3400m59

cronaca
Iran: Piantedosi, 'monitoriamo ripercussioni su piazze'

88 words
4 March 2026
13:23
Adnkronos - General News
GENNEW
Italian

Roma , 04 mar. - (**Adnkronos**) - Dopo l'attacco all'Iran "dovremo monitorare come si assesteranno i posizionamenti di tipo ideologico rispetto a quelli che sono i temi che emergeranno nel protrarsi del conflitto con ripercussioni sui movimenti di piazza". Lo ha detto il ministro dell'Interno Matteo Piantedosi nel corso del al **CyberSec**, la Conferenza promossa dal giornale Cybersecurity Italia, quest'anno organizzata in collaborazione con la Polizia, e che si svolge, fino a domani, alla Scuola superiore di Polizia.

(Sod/**Adnkronos**)

Document GENNEW0020260304em3400jll

cronaca
Ia: Melillo, 'ormai utilizzata da criminalità organizzata e terrorismo'

119 words
4 March 2026
13:14
Adnkronos - General News
GENNEW
Italian

Roma , 04 mar. - (**Adnkronos**) - "L'intelligenza artificiale è ormai quotidianamente utilizzata sia dalla criminalità organizzata che dal terrorismo. Nel campo del riciclaggio, algoritmi di intelligenza artificiale automatizzano da tempo i processi di layering, rendendo quasi impossibile tracciare i flussi finanziari illeciti non solo agli organi investigativi, ma anche ai fini della prevenzione del rischio di utilizzo del sistema finanziario a scopi di riciclaggio e finanziamento del terrorismo". Lo ha detto il procuratore nazionale Antimafia e Antiterrorismo, Giovanni Melillo, al **CyberSec**, la Conferenza promossa dal giornale Cybersecurity Italia, quest'anno organizzata in collaborazione con la Polizia, e che si svolge, fino a domani, alla Scuola superiore di Polizia.

(Sod/**Adnkronos**)

Document GENNEW0020260304em3400ize

economia
Cybersicurezza: Michelini (Telsy), 'Sovranità digitale per competitività industriale e sicurezza nazionale'

286 words
4 March 2026
13:02
Adnkronos - General News
GENNEW
Italian

Roma, 4 mar. (**Adnkronos**) - "La sovranità digitale non è solamente un tema tecnologico, ma un tema di competitività industriale e di sicurezza nazionale che il paese può avere nell'ambito del panorama geopolitico mondiale". Queste le parole di Alessandra Michelini, amministratore delegato e Presidente di Telsy, società del gruppo Tim, intervenuta nella 5^ edizione di **Cybersec**, la conferenza internazionale in corso a Roma e organizzata dal quotidiano Cybersecurity Italia. "Riteniamo che ridurre la dipendenza da tecnologie extra UE sia assolutamente necessario ma non sufficiente se non combinato con un quadro di governance italiana ed europea che possa darci la garanzia di una giurisdizione e regolamentazione chiara", aggiunge.

E la competenza umana? Michelini risponde così: "È un elemento chiave, direi imprescindibile. La tecnologia, per quanto avanzata e all'avanguardia, non è sufficiente. Il fattore umano è indispensabile. Oggi molto spesso lo consideriamo solo in un'accezione negativa, ma rimane l'unico in grado di fare la differenza nel contrasto con il cybercrime. È importante investire in competenze, formazione, e rendere le aziende un luogo attrattivo per i nostri talenti". A questo sta contribuendo, nel settore privato, anche Telsy: "È molto attenta all'investimento nel capitale umano. E poi fa parte di un grande gruppo, come il gruppo Tim, da sempre un motore dell'innovazione per il paese. Noi lo facciamo insieme, nel nostro piccolo, per la cybersecurity".

L'amministratore delegato sottolinea, infine, l'importanza dell'evento: "Eventi di questo tipo sono fondamentali. Credo sia emerso in modo chiarissimo, nel corso degli interventi, quanto sia importante far parlare industria, istituzioni ed i rappresentanti degli organismi dedicati alla cybersecurity e alla protezione del nostro paese".

(Redazione/**Adnkronos**)

Document GENNEW0020260304em3400iaf

english
Cybersecurity, Tito (IBM): "Attacks initiated with public applications increase by 44%"

297 words
4 March 2026
12:54
AKI - Adnkronos International
AKIEN
English

Rome, March 4. (**Adnkronos**) - "The increasing frequency and sophistication of cyberattacks forces organizations to radically rethink their approach to digital security. In the X-Force Threat Intelligence Index 2026 report, IBM recorded a 44% increase in attacks initiated by exploiting public applications, largely caused by a lack of authentication controls and the discovery of vulnerabilities enabled by AI." This was stated by Cristiano Tito, Cybersecurity Services Portfolio Lead IBM Italy, during the fifth edition of **Cybersec**, the international conference currently underway in Rome and organized by the daily newspaper Cybersecurity Italia.

Tito then illustrates the solutions to address the situation: "To face this challenge, security must evolve on two fronts: AI for security, which leverages artificial intelligence to automate tasks, analyze threats, and generate responses, and security for AI, aimed at protecting models, data, and workflows from sophisticated attacks, such as malicious prompts or deep fakes. A structured framework based on zero-trust principles and emerging technologies like AI firewalls and MLDR (Machine Learning Detection and Response) is therefore necessary."

"Another challenge then looms on the horizon: Quantum Computing. This technology promises unprecedented computing power, but risks rendering traditional cryptographic algorithms obsolete, exposing sensitive data to 'harvest now, decrypt later' attacks. The European Union has suggested a plan for the transition to Post-Quantum Cryptography (PQC) by 2035, emphasizing the importance of a timely, complete, and coordinated transition. It is clear that the future of cybersecurity will be hybrid, dominated by two transformative forces: AI and Quantum Computing. Threats and opportunities intertwine in a global race where those who can integrate these technologies as allies will have a decisive strategic advantage, not only in data protection - he concludes - but in geopolitical and technological leadership."

(Redazione/**Adnkronos**)

Document AKIEN00020260304em34001xk

english
Cybersecurity, Portaluri (Magnet Forensic): "AI accelerator in cybercrime investigations"

119 words
4 March 2026
12:52
AKI - Adnkronos International
AKIEN
English

Rome, March 4. (**Adnkronos**) - "Artificial intelligence is becoming a fundamental enabler in cybercrime investigations, allowing for the acceleration of digital evidence analysis and the identification of increasingly complex criminal patterns. The real challenge today is to integrate these technologies in a reliable, scalable, and compliant manner with regulatory frameworks, while strengthening cooperation between public and private actors." With these words, Luigi Portaluri, Director South Europe of Magnet Forensic, spoke today in Rome at the international conference **Cybersec** 2026, promoted and organized by the newspaper Cybersecurity Italia in collaboration with the State Police. The meeting focused on 'Cybercrime and cyberwar: norms, geopolitics and cybersecurity for a common Defense'.

(Redazione/**Adnkronos**)

Document AKIEN00020260304em34001xi

english
Cybersecurity, Pisano (Almaviva): "Accelerate prevention processes"

155 words
4 March 2026
12:51
AKI - Adnkronos International
AKIEN
English

Rome, 4 Mar. (**Adnkronos**) - "In the cyber domain, we face an asymmetric challenge: hostile actors operate with relentless speed and flexibility, while our responses risk being slowed down by organizational and procedural complexities. It is therefore essential to strengthen the synergy between institutions, industry, and the technological community, accelerate threat prevention and response processes, and promote greater cooperation between the public and private sectors. Only through a proactive and multi-domain approach will it be possible to foster greater resilience in the digital ecosystem, making it more secure and better able to face emerging challenges." Antonio Pisano, Chief Security Officer of Almaviva Group, said this today in Rome, on the occasion of **Cybersec** 2026, the international conference promoted and organized by the newspaper Cybersecurity Italia in collaboration with the State Police.

The meeting focused on 'Cybercrime and cyberwar: norms, geopolitics, and cybersecurity for a common Defense'.

(Redazione/**Adnkronos**)

Document AKIEN00020260304em34001xh

cronaca
Cybersicurezza: Pisani, 'crittografia end to end ostacola indagini'

158 words
4 March 2026
12:42
Adnkronos - General News
GENNEW
Italian

Roma, 4 mar. - (**Adnkronos**) - "La crittografia end to end favorisce determinati illeciti ed è uno strumento impeditivo per l'attività ordinaria investigativa". Lo ha detto il capo della Polizia Vittorio Pisani nel corso del al **CyberSec**, la Conferenza promossa dal giornale Cybersecurity Italia, quest'anno organizzata in collaborazione con la Polizia, e che si svolge, fino a domani, alla Scuola superiore di Polizia. "I provider che forniscono la crittografia end-to-end purtroppo, non sono sottoposti alla legislazione italiana, quindi non si riescono a sottoporre alle cosiddette prestazioni obbligatorie che invece riusciamo a imporre chiaramente alle nostre compagnie telefoniche - ha sottolineato- Questa difficoltà va affrontata anche da un punto di vista politico-giuridico: noi già da un paio d'anni nelle riunioni che vengono fatte a livello europeo tra i capi della Polizia abbiamo sollecitato affinché il problema venga affrontato da un punto di vista politico-istituzionale".

(Sod/**Adnkronos**)

Document GENNEW0020260304em3400gz7

cronaca
Cybersicurezza: Pisani, 'attacchi da Cina e Russia, tarare rapporti'

133 words
4 March 2026
12:27
Adnkronos - General News
GENNEW
Italian

Roma , 04 mar. - (**Adnkronos**) - “Il progresso tecnologico segna la differenza sul piano della competizione, non soltanto economica ma soprattutto geopolitica, e in mano ad alcuni Paesi che possiamo definire ‘non amici’, costituisce uno strumento di attacco. È inutile negare che gli attacchi informatici che subiamo da Paesi come Cina e Russia colpiscono direttamente le infrastrutture critiche del nostro Paese e, quindi, i rapporti con questi Stati vanno tarati anche in base al loro approccio nei confronti della nostra sicurezza nazionale”. Lo ha detto il capo della Polizia Vittorio Pisani nel corso del al **CyberSec**, la Conferenza promossa dal giornale Cybersecurity Italia, quest’anno organizzata in collaborazione con la Polizia, e che si svolge, fino a domani, alla Scuola superiore di Polizia.

(Sod/**Adnkronos**)

Document GENNEW0020260304em3400g4m

economia
Cybersicurezza: Momola (Engineering), 'è politica industriale, con la nostra la si rafforza ruolo nazionale'

373 words
4 March 2026
11:57
Adnkronos - General News
GENNEW
Italian

Roma, 4 mar. (**Adnkronos**) - “Viviamo in una fase in cui i confini tra dominio militare e civile si sono progressivamente dissolti. La guerra non è più solo militare: è economica e informativa. È una guerra ibrida che non colpisce confini, ma infrastrutture essenziali — energia, finanza, trasporti, sanità — e che si manifesta con blackout, reti bancarie rallentate, campagne di disinformazione. Negli ultimi anni l’Italia e l’Europa hanno investito sempre di più in cybersecurity, ma è arrivato il momento di un cambio di prospettiva: non possiamo più limitarci a essere consumatori di tecnologia per la nostra sicurezza. Dobbiamo diventare produttori". Ad affermarlo è Fabio Momola, Ceo DHub e Cybertech del Gruppo Engineering, intervenendo oggi al **Cybersec** 2026 sul tema 'Il digitale come leva strategica tra Hybrid Warfare e Cybersecurity'.

L’Intelligenza Artificiale, sottolinea, "è un moltiplicatore di potenza in entrambe le direzioni, sia per chi attacca sia per chi difende. Proprio per questo dobbiamo orchestrare l’AI, non esserne orchestrati. Non serve inseguire modelli sempre più grandi e generici. Servono modelli di AI specializzati, agili e verticalizzabili: un’intelligenza artificiale sovrana, di cui abbiamo la governance totale — su quali dati è addestrata, chi la governa, chi ne risponde".

La cybersecurity, rileva, "non è solo protezione tecnica. È politica industriale. E una resilienza senza sovranità tecnologica è fragile. L’Italia ha le competenze per costruire questa autonomia strategica: campioni nazionali, decine di aziende specializzate e PMI innovative in ambito cyber, un capitale umano fatto di grandi professionisti ed esperti. Noi di Engineering ci stiamo muovendo in questa direzione, investendo su un’architettura concreta che parte da modelli proprietari e aperti, li specializza attraverso piattaforme dedicate, li orchestra in flussi operativi governati e ne garantisce osservabilità e controllo continuo in ogni fase. Lo facciamo nella consapevolezza di agire in un ecosistema dinamico e ricco di eccellenze. Ci sono tutti i presupposti per un approccio sistemico in cui la partnership pubblico-privato non sia un’opzione, ma un requisito strutturale: condivisione sicura delle informazioni sulle minacce, integrazione tra grandi player e Pmi, rafforzamento di una difesa comune. Nel dominio cyber non vince chi compra meglio. Vince chi costruisce meglio".

(Redazione/**Adnkronos**)

Document GENNEW0020260304em3400dyu

economia
Cybersicurezza: Palermo (Fortinet), 'perdite milionarie per 41% aziende'

331 words
4 March 2026
11:49
Adnkronos - General News
GENNEW
Italian

Roma, 4 mar. (**Adnkronos**) - "Aumentano gli investimenti, ma cresce anche l'impatto economico degli attacchi. A livello globale, nell'ultimo anno i budget destinati alla sicurezza dei dati sono cresciuti nel 72% delle organizzazioni. Tuttavia, il 41% delle aziende ha comunque subito perdite milionarie a causa di incidenti cyber interni. In questo dato c'è un'incidenza importante del fattore umano, a ulteriore conferma della stretta relazione tra le violazioni e la carenza di conoscenze di sicurezza informatica nelle imprese". Lo ha spiegato oggi a Roma Massimo Palermo, VP & Country Manager Italy & Malta di Fortinet, alla **Cybersec** 2026, la conferenza internazionale promossa e organizzata dal quotidiano Cybersecurity Italia in collaborazione con la Polizia di Stato. Al centro dell'incontro i temi legati a 'Cybercrime e cyberwar: norme, geopolitica e cybersecurity per una Difesa comune'.

"Nel contesto internazionale oggi si registra una mancanza di oltre 4,7 milioni di professionisti di cybersecurity: un gap che coinvolge anche l'Italia e che diviene fondamentale colmare con urgenza, diffondendo una cultura della sicurezza informatica accessibile a tutte e tutti, sin dall'istruzione di base. Per innalzare il livello di difesa collettivo, ridurre il gap di competenze e alzare il livello di consapevolezza è ormai una priorità strategica nel processo di gestione del rischio che ogni organizzazione deve considerare per la protezione dei dati, delle infrastrutture e del mondo digitale".

Palermo si sofferma poi sul contributo di Fortinet: "Fortinet ha deciso di rendere disponibile, a titolo gratuito, il proprio servizio di Security Awareness and Training, personalizzato per il mondo dell'istruzione e degli istituti di formazione, per tutte le scuole primarie e secondarie del Paese, pubbliche e private. Il progetto, che nella sua fase pilota ha visto anche il coinvolgimento dell'Agenzia per la Cybersicurezza Nazionale (Acn) e della Polizia Postale, rientra nell'impegno globale di Fortinet volto a formare un milione di persone entro la fine del 2026, partendo proprio dalle nuove generazioni", conclude.

(Redazione/**Adnkronos**)

Document GENNEW0020260304em3400dfg

economia
Cybersicurezza: Tito (Ibm), 'attacchi iniziati con applicazioni pubbliche aumentano del 44%'

313 words
4 March 2026
11:14
Adnkronos - General News
GENNEW
Italian

Roma, 4 mar. (**Adnkronos**) - "La crescente frequenza e sofisticazione degli attacchi informatici impone alle organizzazioni di ripensare radicalmente il proprio approccio alla sicurezza digitale. Nel report X-Force Threat Intelligence Index 2026, Ibm ha registrato un aumento del 44% degli attacchi iniziati con lo sfruttamento di applicazioni pubbliche, in gran parte causati dalla mancanza di controlli di autenticazione e dalla scoperta di vulnerabilità consentita dall'Ai". Lo ha dichiarato Cristiano Tito, Cybersecurity Services Portfolio Lead Ibm Italia, in occasione della quinta edizione di **Cybersec**, la conferenza internazionale in corso a Roma e organizzata dal quotidiano Cybersecurity Italia.

Tito illustra poi le soluzioni per affrontare la situazione: "Per affrontare questa sfida la sicurezza deve evolvere su due fronti: Ai per la sicurezza, che sfrutta l'intelligenza artificiale per automatizzare compiti, analizzare minacce e generare risposte, e sicurezza per l'Ai, volta a proteggere modelli, dati e flussi di lavoro da attacchi sofisticati, come prompt malevoli o deep fake. È necessario quindi un framework strutturato basato su principi zero trust e tecnologie emergenti come firewall Ai e Mldr (Machine Learning Detection and Response)".

"All'orizzonte si profila poi un'altra sfida: il Quantum Computing. Questa tecnologia promette potenza di calcolo senza precedenti, ma rischia di rendere obsoleti gli algoritmi crittografici tradizionali, esponendo dati sensibili ad attacchi harvest now, decrypt later. L'Unione Europea ha suggerito un piano per la transizione alla Crittografia Post-Quantistica (Pqc) entro il 2035, sottolineando l'importanza di un passaggio tempestivo, completo e coordinato. È chiaro che il futuro della cybersecurity sarà ibrido, dominato da due forze trasformative: AI e Quantum Computing. Minacce e opportunità si intrecciano in una corsa globale dove chi saprà integrare queste tecnologie come alleate avrà un vantaggio strategico decisivo, non solo nella protezione dei dati - conclude - ma nella leadership geopolitica e tecnologica".

(Redazione/**Adnkronos**)

Document GENNEW0020260304em3400b6u

economia
Cybersicurezza: Portaluri (Magnet Forensic), 'la acceleratore in indagini per cybercrime'

122 words
4 March 2026
11:14
Adnkronos - General News
GENNEW
Italian

Roma, 4 mar. (**Adnkronos**) - "L'intelligenza artificiale sta diventando un abilitatore fondamentale nelle indagini sul cybercrime, permettendo di accelerare l'analisi delle evidenze digitali e individuare pattern criminali sempre più complessi. La vera sfida oggi è integrare queste tecnologie in modo affidabile, scalabile e conforme ai quadri normativi, rafforzando al tempo stesso la cooperazione tra attori pubblici e privati". Con queste parole Luigi Portaluri, Director South Europe di Magnet Forensic, è intervenuto oggi a Roma alla conferenza internazionale **Cybersec** 2026, promossa e organizzata dal quotidiano Cybersecurity Italia in collaborazione con la Polizia di Stato. Al centro dell'incontro 'Cybercrime e cyberwar: norme, geopolitica e cybersecurity per una Difesa comune'.

(Redazione/**Adnkronos**)

Document GENNEW0020260304em3400b6v

economia
Cybersicurezza: Pisano (Almaviva), 'accelerare processi di prevenzione'

155 words
4 March 2026
11:04
Adnkronos - General News
GENNEW
Italian

Roma, 4 mar. (**Adnkronos**) - "Nel dominio cibernetico affrontiamo una sfida asimmetrica: gli attori ostili operano con implacabile rapidità e flessibilità, mentre le nostre risposte rischiano di essere rallentate da complessità organizzative e procedurali. È quindi essenziale rafforzare la sinergia tra istituzioni, industria e comunità tecnologica, accelerare i processi di prevenzione e risposta alla minaccia e promuovere una maggiore cooperazione tra il settore pubblico e quello privato. Solo attraverso un approccio proattivo e multi dominio sarà possibile indirizzare una maggiore resilienza dell'ecosistema digitale, rendendolo più sicuro e maggiormente capace di affrontare le sfide emergenti". Lo ha detto oggi a Roma Antonio Pisano, Chief Security Officer di Almaviva Group, in occasione di **Cybersec** 2026, la conferenza internazionale promossa e organizzata dal quotidiano Cybersecurity Italia in collaborazione con la Polizia di Stato.

Al centro dell'incontro 'Cybercrime e cyberwar: norme, geopolitica e cybersecurity per una Difesa comune'.

(Redazione/**Adnkronos**)

Document GENNEW0020260304em3400aq6

economia
Cybersicurezza: Ferretti (Protiviti), 'con la rivoluzione in investigazioni cyber'

100 words
4 March 2026
11:04
Adnkronos - General News
GENNEW
Italian

Roma, 4 mar. (**Adnkronos**) - "L'Ai sta rivoluzionando le investigazioni cyber: non è un supporto, è un amplificatore strategico che permette di scoprire ciò che gli attaccanti cercano di rendere invisibile. Oggi non indagare rapidamente significa lasciare che il nemico detti le regole". Lo ha detto oggi a Roma Enrico Ferretti, Managing Director di Protiviti, alla **Cybersec** 2026, la conferenza internazionale promossa e organizzata dal quotidiano Cybersecurity Italia in collaborazione con la Polizia di Stato. Titolo dell'incontro: 'Cybercrime e cyberwar: norme, geopolitica e cybersecurity per una Difesa comune'.

(Redazione/**Adnkronos**)

Document GENNEW0020260304em3400aq5

economia
Cybersicurezza: Mugnano (Gyala), 'unire le forze per un'Italia hub di eccellenza'

145 words
4 March 2026
11:03
Adnkronos - General News
GENNEW
Italian

Roma, 4 mar. (**Adnkronos**) - "Il **Cybersec** 2026 propone una nuova visione: far evolvere l'ecosistema nazionale della cybersecurity verso il modello collaborativo CyberHub Italia, spinto dalla volontà di portare innovazione. In questo contesto, imprese come Gyala, che integra Threat Intelligence avanzata con strategie di resilienza condivise, possono dare un importante contributo. Sono convinto che solo unendo le forze tra pubblico e privato potremo contrastare le minacce evolute, trasformando l'Italia in un hub europeo di eccellenza". Queste le parole di Nicola Mugnato, Co-Founder di Gyala, oggi a Roma alla **Cybersec** 2026, la conferenza internazionale promossa e organizzata dal quotidiano Cybersecurity Italia in collaborazione con la Polizia di Stato che quest'anno, alla quinta edizione, si concentra sui temi 'Cybercrime e cyberwar: norme, geopolitica e cybersecurity per una Difesa comune'.

(Redazione/**Adnkronos**)

Document GENNEW0020260304em3400and

economia
Cybersicurezza: Fasano (Ermetix), 'la diventa superficie di attacco'

139 words
4 March 2026
11:00
Adnkronos - General News
GENNEW
Italian

Roma, 4 mar. (**Adnkronos**) - "L'intelligenza artificiale non è più soltanto uno strumento in mano ai cybercriminali. Sta diventando essa stessa parte della superficie d'attacco delle nostre organizzazioni. Il vero cambio di prospettiva è capire che l'intelligenza artificiale non è un semplice tool, ma un attore operativo inserito nei nostri sistemi: se un avversario riesce a orientarlo, non ha più bisogno di bucare un server perché può direttamente pilotare un processo". Sono le parole di Diego Fasano, Ceo di Ermetix, partecipando oggi a Roma alla **Cybersec** 2026, la conferenza internazionale promossa e organizzata dal quotidiano Cybersecurity Italia presso la Scuola Superiore di Polizia a Roma, in collaborazione con la Polizia di Stato per discutere di 'Cybercrime e cyberwar: norme, geopolitica e cybersecurity per una Difesa comune'.

(Redazione/**Adnkronos**)

Document GENNEW0020260304em3400af3

economia
Cybersicurezza: Aceti (Hwg Sababa), 'cyber resilienza per proteggere infrastrutture critiche'

217 words
4 March 2026
10:59
Adnkronos - General News
GENNEW
Italian

Roma, 4 mar. (**Adnkronos**) - "Oggi la priorità è creare un ecosistema nazionale della cyber resilienza, mirato a proteggere le infrastrutture critiche, quali i settori energy, health, finanza e trasporti. Stiamo infatti vivendo un contesto geopolitico sempre più teso e instabile, caratterizzato da attacchi ogni giorno più frequenti e sofisticati. Le minacce non colpiscono solo il singolo operatore, ma l'intera supply chain, con effetti sistemici su servizi essenziali e continuità operativa del Paese". Così Alessio Aceti, Chief Executive Officer di Hwg Sababa, partecipando oggi a Roma alla quinta edizione di **Cybersec**, la conferenza internazionale promossa dal quotidiano Cybersecurity Italia presso la Scuola Superiore di Polizia a Roma, in collaborazione con la Polizia di Stato che, attraverso il Servizio della Polizia Postale e della Sicurezza Cibernetica, è in prima linea nel contrasto al cybercrime e nella protezione delle infrastrutture critiche informatiche nazionali.

Aceti indica poi la via per fronteggiare i rischi legati ai cyber attacchi: "Creare allarmismi e panico è inutile e controproducente: è necessario far fronte comune tra attori della cybersecurity, istituzioni e aziende per saper prevenire i danni e rispondere in maniera efficace. Questo garantirebbe la resilienza strutturale delle infrastrutture critiche, tutelando la sicurezza, l'economia e la stabilità sociale del Paese", conclude.

(Redazione/**Adnkronos**)

Document GENNEW0020260304em3400a9h

economia
****Cybersicurezza: Boggio (Kyndryl), 'Italia bersaglio del 10% degli attacchi globali'****

267 words
4 March 2026
10:58
Adnkronos - General News
GENNEW
Italian

Roma, 4 mar. (**Adnkronos**) - "La cybersecurity è un'infrastruttura strategica per la competitività del Paese. I dati più aggiornati mostrano un'Italia particolarmente esposta: nel 2024 si sono registrati 357 attacchi gravi (+15,2% sul 2023) e nel primo semestre 2025 si rilevano 280 incidenti critici, pari a oltre il 10% degli attacchi mondiali". Lo ha detto Andrea Boggio, Director, Security Customer Technical Advisor di Kyndryl, in una nota prodotta in occasione del **Cybersec** 2026, la due giorni organizzata presso la Scuola Superiore di Polizia a Roma dal quotidiano Cybersecurity Italia in collaborazione con la Polizia di Stato. Temi di questa edizione: 'Cybercrime e cyberwar: norme, geopolitica e cybersecurity per una Difesa comune'.

Boggio si sofferma poi sui dati diffusi da Acn, l'Agenzia per la Cybersicurezza Nazionale: "Nel 2025 gli incidenti gestiti dalla Polizia Postale hanno superato quota 55mila e il 54% degli attacchi è attribuito all'hacktivism, contro l'8% del resto del mondo. Un fenomeno che colpisce infrastrutture, pubblica amministrazione e industria italiana in modo unico nel panorama europeo. Quando un attacco blocca un'azienda il costo si misura in milioni di euro al giorno: produzione ferma, servizi paralizzati, dati esfiltrati. Con il nuovo Security Briefing Center, integrato con il nostro Soc (Security operation center), offriamo alle aziende italiane un hub dove confrontarsi su scenari reali e co-progettare strategie di resilienza seguendo un approccio strutturato e pienamente allineato alle normative nazionali ed europee. In Italia - conclude - non basta più parlare di sicurezza, serve costruirla con competenze, metodo e trasparenza".

(Redazione/**Adnkronos**)

Document GENNEW0020260304em3400a6p

cronaca
Cybersicurezza: Viola (Polizia), 'minacce incidono su qualità democrazia'

118 words
4 March 2026
10:56
Adnkronos - General News
GENNEW
Italian

Roma , 04 mar. - (**Adnkronos**) - "La dimensione digitale non è più un ambito separato dalla realtà, ma ne costituisce una componente strutturale. Le minacce informatiche incidono sulla sicurezza delle Istituzioni, sull'economia, sulle infrastrutture critiche e, in definitiva, sulla qualità della nostra democrazia". Lo ha detto Mario Viola, direttore della Scuola Superiore di Polizia, al **CyberSec**, la Conferenza promossa dal giornale Cybersecurity Italia, quest'anno organizzata in collaborazione con la Polizia, e che si svolge, fino a domani, alla Scuola superiore di Polizia. "A queste sfide - ha aggiunto - si risponde solo con una visione condivisa, con competenze solide e con una cooperazione convinta tra tutti gli attori coinvolti".

(Sod/**Adnkronos**)

Document GENNEW0020260304em3400a15

cronaca
Cybersicurezza: Butti, 'nel 2025 +36% incidenti'

191 words
4 March 2026
10:30
Adnkronos - General News
GENNEW
Italian

Roma , 04 mar. - (**Adnkronos**) - “Nel 2025 gli incidenti cyber sono aumentati del 36% rispetto al 2024 quando l'incremento era stato notevole già rispetto anche all'anno precedente”. Lo ha detto il sottosegretario alla presidenza del Consiglio con delega all’Innovazione, Alessio Butti, al **CyberSec**, la Conferenza promossa dal giornale Cybersecurity Italia, quest’anno organizzata in collaborazione con la Polizia, e che si svolge, fino a domani, alla Scuola superiore di Polizia. "Quello che con l’Agenzia per la Cybersicurezza nazionale, con gli altri colleghi di governo, stiamo cercando di focalizzare è che l'Italia risulta essere uno degli oggetti dell’attenzione della criminalità cyber, nonostante non abbia uno straordinario potere di natura economica", ha aggiunto.

Butti ha poi ricordato che si sta “investendo parecchio anche in termini di conoscenza, in infrastrutture digitali ad altissima affidabilità, nella migrazione verso ambienti cloud che consentono quindi di custodire i nostri dati soprattutto per quanto riguarda la pubblica amministrazione centrale e locale nel modo migliore”. "Lo stiamo facendo per contrastare la frammentazione e la vulnerabilità che altrimenti sono ovviamente due serie minacce”, ha sottolineato.

(Sod/**Adnkronos**)

Document GENNEW0020260304em34008hl

cronaca
Roma: il 4-5 marzo torna CyberSec, la 5° conferenza su cybercrime e guerra digitale

526 words
23 February 2026
12:57
Adnkronos - General News
GENNEW
Italian

Roma, 23 feb. (**Adnkronos**) - "Cybercrime e cyberwar: norme, geopolitica e cybersecurity per una Difesa comune" è il titolo della 5° edizione di **CyberSec**, la conferenza internazionale promossa ed organizzata dal quotidiano Cybersecurity Italia che si terrà il 4 e 5 marzo prossimi alla Scuola superiore di polizia. L'edizione 2026 è in collaborazione con Polizia di Stato, che attraverso il servizio della polizia postale e della sicurezza cibernetica è in prima linea sia nel contrasto al cybercrime sia nella protezione delle infrastrutture critiche informatiche nazionali. La conferenza si terrà il 4 e 5 marzo 2026 a Roma presso la Scuola superiore di polizia.

Il direttore di Cybersecurity Italia Luigi Garofalo afferma: "Siamo orgogliosi della collaborazione con polizia di Stato, è un riconoscimento per **CyberSec**, che si posiziona sempre di più nel nostro Paese come il principale momento di confronto sulla cybersicurezza tra tutti gli stakeholder rilevanti sia istituzionali sia aziendali con l'obiettivo di proporre, in modo collaborativo, come affrontare e vincere le sfide del cybercrime e della cyberwar nell'attuale contesto geopolitico. Il cyberspazio non può più essere trattato solo come silos, perché è uno dei domini della guerra ibrida, combattuta quotidianamente. Infatti, dal nostro punto di vista la cybersicurezza è sicurezza nazionale". Per il direttore della conferenza Eliana D'Aquanno, "la cybersicurezza è una sfida sistemica che richiede cultura, tecnologie, visione, coordinamento, capacità di governance e formazione. **CyberSec**, con la 5° edizione presso la prestigiosa scuola superiore di polizia, continua ad essere la piattaforma in cui questa consapevolezza si consolida ed evolve. **CyberSec** è nata proprio con questa ambizione: favorire un confronto di alto livello che non si esaurisca nel dibattito, ma contribuisca alla definizione di una strategia condivisa per la resilienza del Paese e la tutela del benessere collettivo".

I relatori di CyberSec2026 saranno i rappresentanti delle Istituzioni e i top manager delle aziende più strategiche della cybersecurity, provenienti dall'Italia e dall'estero. Tra gli speaker confermati il ministro dell'Interno Matteo Piantedosi, il ministro delle Imprese e del Made in Italy Adolfo Urso, il capo della polizia, direttore generale della Pubblica Sicurezza Vittorio Pisani, il direttore generale del Dis Vittorio Rizzi, la vicepresidente della Commissione Henna Virkkunen, il direttore generale dell'Agenzia per la cybersicurezza nazionale Bruno Frattasi, il comandante del comando per le operazioni in rete Sandro Sanasi, il direttore del servizio della polizia postale e della sicurezza cibernetica Ivano Gabrielli, il direttore del centro nazionale anticrimine (Cnaipic) Riccardo Croce, il dirigente superiore della polizia di Stato e direttore del servizio per la sicurezza cibernetica del ministero dell'Interno Gianpaolo Zambonini, il direttore del comando cyberspazio del ministero dell'Interno francese (ComCyberMi) Patrick Touak, il direttore generale dell'Agenzia per l'Italia digitale Mario Nobile, la vicedirettrice dell'Acn Nunzia Ciardi, il generale Paolo Aceto comandante del III reparto del comando generale dell'Arma dei carabinieri, l'executive director dell'Eccc Luca Tagliaretti, il direttore generale per le questioni cibernetiche del ministero degli Affari Esteri e della Cooperazione Internazionale Alessandro De Pedys, il direttore della scuola superiore di polizia Mario Viola.

(Red-Cro/**Adnkronos**)

Document GENNEW0020260223em2n00fwa

Search Summary

Text	Adnkronos and Cybersec
Date	In the last 3 months
Source	All Sources
Author	All Authors
Company	All Companies
Subject	All Subjects
Industry	All Industries

Region	All Regions
Language	English Or Italian
Results Found	61
Timestamp	9 March 2026 14:53

