La Russa: “Meloni presidente della Repubblica? Lo diventerà, magari non stavolta…”

(Adnkronos) – Giorgia Meloni presidente della Repubblica? “Secondo me lo diventerà presidente della Repubblica, magari la prossima volta e non questa”. Ignazio La Russa, presidente del Senato, vede un futuro al Quirinale per l’attuale presidente del Consiglio. “Quando, non lo so. Ma se un giorno Meloni diventasse presidente della Repubblica sarebbe un grande bene per l’Italia. Non credo voglia farlo adesso ma non c’è nessuna ragione che possa suonare come allarme”, dice La Russa all’Estate del principe a Viareggio. Secondo il presidente del Senato, “anche una fetta del centrosinistra” ne sarebbe felice. L’esponente di Fratelli d’Italia non si considera un candidato alla successione di Sergio Mattarella. La presidenza della Repubblica “non è una cosa che io potrei reggere”, è un ruolo, “mi perdoni il presidente della Repubblica, un po’ ingessato, un po’ chiuso”.

Capitolo legge elettorale: “Immaginare che arriva una norma” come la legge elettorale “e nessuno presenta gli emendamenti non è mai capitato. Quello che capita di frequente è che poi alla fine il primo testo licenziato viene riconfermato, ma in questo caso il primo testo confermato è passato per un voto con gravi disattenzioni della maggioranza”, dice La Russa facendo riferimento alla bocciatura dell’emendamento sulle preferenze. “Alcuni ministri addirittura non hanno votato, presiedeva uno di centrodestra, non presiedeva uno di sinistra, non presiedeva il presidente della Camera” facendo in modo che “il vicepresidente di centrodestra votasse”. “Io sono convinto che se ripresenteranno” l’emendamento sulle preferenze “è possibile che questa volta senza voto segreto,

il che costringe tutti a metterci la faccia, si vede chi è favorevole e chi è contrario veramente. Bocciare una legge non è come bocciare un emendamento”, conclude La Russa.

_

politica

webinfo@adnkronos.com (Web Info)

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/la-russa-meloni-presidente-della-repubblica-lo-diventera-magari-non-stavolta/582701/

Attentato Berlino, il sospettato è morto: Abdul Ballout ucciso dalle forze

speciali

(Adnkronos) –
Abdul Ballout, ricercato per l'attacco al Pride di Berlino, è morto. Il 21enne è stato ucciso oggi domenica 26 luglio in un'operazione delle forze speciali nella capitale tedesca è in particolare nel quartiere di Spandau. La polizia di Berlino ha reso noto su X che l'uomo è stato colpito da un proiettile ed è morto nonostante i tentativi di rianimazione. Le forze speciali sono intervenute in un orto dove sarebbe stato individuato un capanno, a quanto pare di proprietà del padre del sospettato. L'operazione è iniziata alle 15: gli agenti hanno isolato l'area, controllata dall'alto dagli elicotteri, e verso le 18 sono entrati in azione.

Il giovane ha affrontato gli agenti con un'arma da taglio, le forze speciali hanno aperto il fuoco e ucciso il 21enne. La ricostruzione di Bild evidenzia che Ballout, individuato grazie alle informazioni fornite da persone a lui vicine, è deceduto alle 18.34. Testimoni hanno riferito di aver sentito due raffiche ravvicinate di 4 colpi ciascuna. Secondo l'agenzia di stampa tedesca Dpa, l'uomo è stato colpito da un proiettile ed è deceduto.

Anche il ministro federale degli Interni Alexander Dobrindt (CSU) ha riferito alla ZDF di un'operazione delle forze speciali durante la quale è stato esploso un colpo d'arma da fuoco e nella quale una persona è morta a seguito dello sparo.

La morte di Ballout non pone fine all'inchiesta sull'attentato, che nella serata di sabato 25 luglio ha provocato la morte di una donna e il ferimento di 29 persone. Gli investigatori hanno raccolto testimonianze secondo cui, a bordo del van utilizzato per l'attacco, sarebbe stata presente una seconda persona. Secondo informazioni ottenute da Bild, gli inquirenti hanno fermato e interrogato tre persone vicine

al sospettato. Due di loro sono state rilasciate, mentre una rimane in custodia. “Dobbiamo arrivare ad avere elementi concreti nei confronti di questi individui. Se non ci riusciamo, dovranno essere rilasciati dopo 48 ore”, ha spiegato Florian Nath, portavoce della polizia.

–

internazionale/esteri

webinfo@adnkronos.com (Web Info)

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/attentato-berlino-il-sospettato-e-morto-abdul-ballout-ucciso-dalle-forze-speciali/582703/

Lega, Salvini spende 30mila euro mensili per Via

Bellerio: solo sede Pd costa di più. Sorride Vannacci, la sua è gratis

(Adnkronos) –
Nella ‘speciale’ classifica degli affitti più onerosi per le casse dei partiti italiani, dopo il Nazareno per il partito democratico, c’è la storica sede di via Bellerio, a Milano, della Lega. Che, secondo l’ultimo bilancio del Carroccio, chiuso al 31 dicembre 2025, è costata a Matteo Salvini la bellezza di 370mila 523 euro l’anno, poco più di 30mila euro al mese – per la precisione 30.876 euro. A conti fatti circa 10 mila euro meno di quanto costa ai democratici appunto il Nazareno (42mila di canone mensile). Come spiega, però, il tesoriere dei leghisti Alberto Di Rubba, il contratto d’affitto, registrato alle Agenzie delle entrate, è di 320mila euro all’anno, ovvero 26mila 666 euro al mese. La differenza, dice ancora all’Adnkronos il deputato, è nelle spese straordinarie – manutenzione, restauri e quant’altro – e nel 2024 era stata ben più elevata, tanto che il costo era lievitato a oltre 390mila euro.

Quartier generale della Lega già dai tempi di Umberto Bossi, che nel 1993 acquistò quei 7600 metri quadrati all’estrema periferia Nord della città lombarda come simbolo di diversità rispetto agli altri partiti romanocentrici, che avevano le loro sedi nei palazzi storici del centro della Capitale, la sede di via Bellerio è da tempo di proprietà della Pontida finanziaria e partecipata dalla Lega Nord.

In comodato d’uso e, quindi tendenzialmente gratis, è invece per Roberto Vannacci la sede di Futuro nazionale. Lo stabile – 80 metri quadrati in via san Lorenzo in Lucina 17, a pochi passi da Montecitorio – è stato ‘offerto’ all’ex generale della Folgore dal leader di Patto Italia, Stefano Ruvolo,

anche presidente di Confimprenditori. Il canone mensile, a quanto risulta all'Adnkronos, è di circa 7500 euro al mese al netto delle spese condominiali.

Inaugurata in pompa magna a fine marzo, si trova di fronte a dove ha casa Forza Italia, tanto che, almeno al momento, futuristi e azzurri si possono ritrovare di tanto in tanto a lavorare gomito a gomito, e non è l'unica sede per cui le truppe vannacciane non spendono un euro. Come ammette lo stesso Vannacci parlando con l'Adnkronos: "Noi non spendiamo nulla, c'è concessa in comodato d'uso gratuito, come tutte le nostre altre sedi". Anche se, precisa il presidente del gruppo alla Camera e tesoriere Edoardo Ziello, "tutte le sedi ufficiali di Futuro nazionale sono state aperte con regolare contratto di comodato d'uso a titolo gratuito, il cui valore rappresenta una donazione indiretta che è stata oggetto di pubblicazione sia sul sito Internet del partito sia dalla presidenza della Camera dei deputati con dichiarazione congiunta redatta ai sensi dell'art. 4 della legge n.659/1981".

Tra le altre sedi di cui Futuro nazionale usufruisce gratis c'è anche quella del Centro studi nazionale, ovvero il Castello Sforzini di Castellar Ponzano, che è stato messo a disposizione di Vannacci dal proprietario Luca Sforzini e che da ieri lancia ogni giorno il mattutino.

–

politica

webinfo@adnkronos.com (Web Info)

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/lega-salvini-spende-30mila-euro-mensili-per-via-bellerio-solo-sede-pd-costa-di-piu-sorride-vannacci-la-sua-e-gratis/582697/

L’illusione di Burnham si scontra con il muro del debito: perché Londra è condannata all’austerità

Il Regno Unito si trova a un passo da una profonda paralisi finanziaria. Il nuovo Primo Ministro Andy Burnham è appena arrivato a Downing Street con grandi promesse di spesa, ma si è ritrovato subito prigioniero di un debito gigantesco. Con i tassi sui titoli di Stato schizzati sopra il 5%, l’intero bilancio pubblico rischia il collasso sotto il peso degli interessi, e anche i media britannici, come il Telegraph, se ne sono resi conto.

Per approfondire:

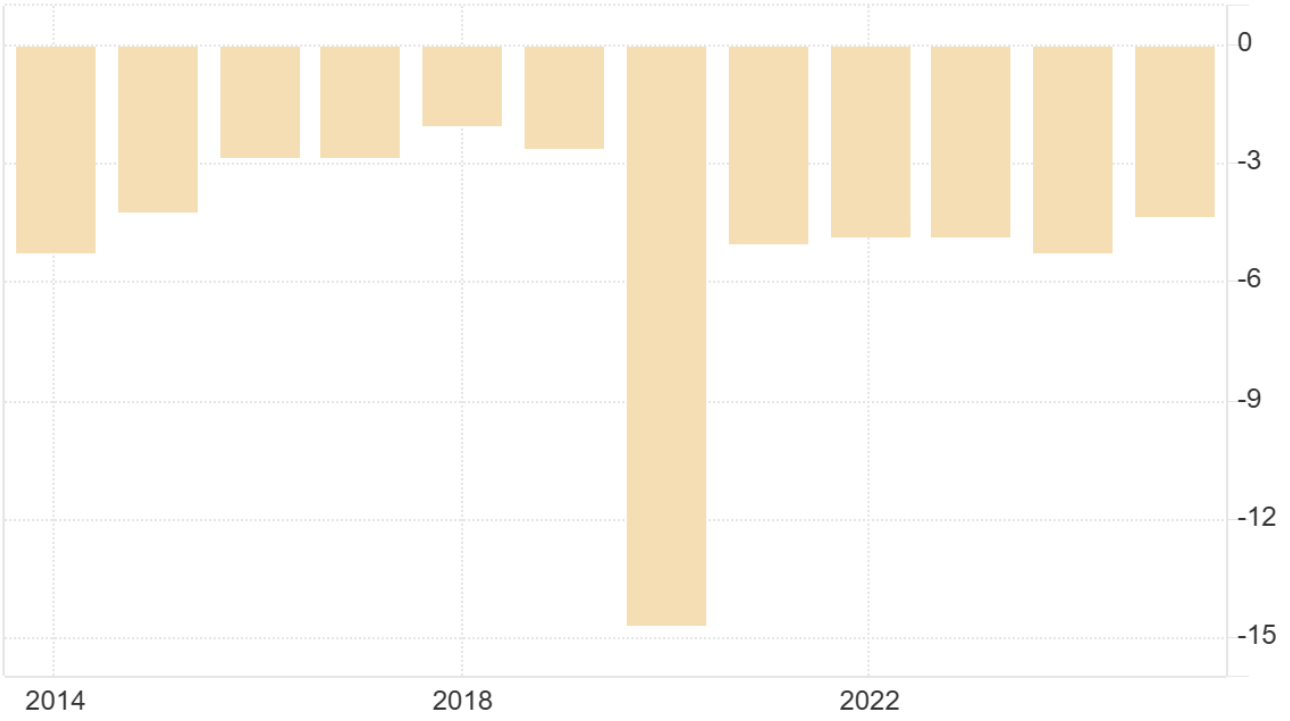
I primi giorni di governo sono stati una vera doccia fredda per il nuovo Premier laburista. Ogni volta che Burnham ha annunciato una misura popolare – dai trasporti locali a basso costo fino al taglio dell'IVA sulle bollette elettriche – i mercati finanziari non hanno applaudito. Al contrario, hanno risposto con una pioggia di interrogativi pesanti sulla copertura finanziaria. I tassi d'interesse sui Gilt, i titoli di stato decennali stanno correndo allegramente verso l'alto…





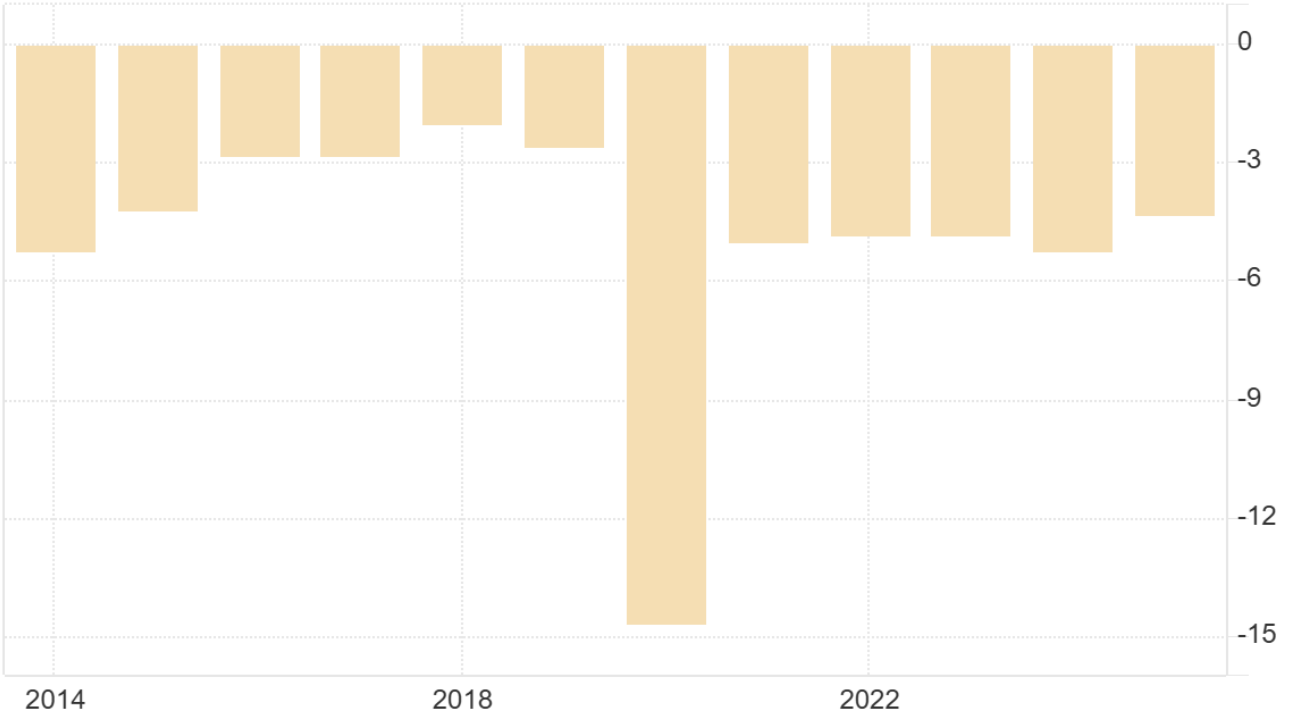
Il problema è che i conti pubblici britannici sono ormai sull'orlo del precipizio. Il debito nazionale sta per toccare la cifra astronomica di 3.000 miliardi di sterline, arrivando a superare il 95% del Prodotto Interno Lordo. Allo stesso tempo, il deficit annuale continua a correre alla **cifra di 115 miliard**i. Il 2025 si è chiuso con un deficit al 4,3% del PIL. Per fortuna che non sono nella UE, altrimenti la solerte Commissione avrebbe iniziato la solita procedura d'infrazione.

United Kingdom Government Budget (percent of GDP)



Source: tradingeconomics.com | Office for Budget Responsibility, UK

United Kingdom Government Budget (percent of GDP)



Source: tradingeconomics.com | Office for Budget Responsibility, UK

Ciò che stritola davvero le decisioni economiche di Londra è la spesa annuale per interessi sul debito. Questa voce ha raggiunto la cifra record di 130 miliardi di sterline all'anno. Si tratta di una somma immensa, superiore a quanto lo Stato spenda per la gran parte dei servizi pubblici primari.

I rendimenti dei titoli di Stato decennali inglesi hanno superato nuovamente la soglia critica del 5%. Questa dinamica colloca il Regno Unito come maglia nera per costo del debito tra tutte le grandi economie avanzate del G7, il che è curioso: la BCE ha una politica monetaria perfino più restrittiva della Bank of England, ma i tassi d'interesse pagati dai paesi europei sono più bassi.

Ecco come si confrontano i costi di indebitamento del Regno Unito rispetto agli altri principali Paesi:

Paese	Rendimento Titolo di Stato a 10 Anni
Regno Unito	**5,1%**
Stati Uniti	4,7%
Italia	4,0%
Francia	4,0%
Germania	3,2%

Per provare a finanziare la propria agenda di investimenti, Burnham vorrebbe sfruttare la cosiddetta "flessibilità" delle regole fiscali. Tra i corridoi del Ministero del Tesoro e della City si valutano diverse scorciatoie contabili per racimolare risorse fresche:

- **Consumare i margini di sicurezza:** Utilizzare il ridotto cuscinetto finanziario rimasto nel bilancio, che tuttavia le recenti tensioni internazionali hanno già assottigliato a soli 10 miliardi di sterline.
- **Spostare gli investimenti fuori dal bilancio statale:** Usare la banca di investimento pubblica e il National

Wealth Fund per attrarre capitali privati senza far figurare le somme come debito diretto.

- **Allungare le tempistiche di rientro:** Estendere gli orizzonti di previsione della spesa da 5 a 10 anni, promettendo un rigore futuro per spendere di più nel presente.
- **Lanciare i "War Bonds":** Emettere titoli di Stato dedicati esclusivamente al finanziamento della spesa militare, isolandoli formalmente dal resto del bilancio.

Tuttavia, queste acrobazie di ingegneria finanziaria non convincono gli investitori. Ogni sterlina aggiuntiva richiesta a prestito dal governo genera un immediato aumento dei rendimenti pretesi dai mercati, trasformando ogni nuova spesa in un boomerang economico.

Sullo sfondo emerge con chiarezza il vero problema di fondo che paralizza non solo il Regno Unito, ma l'intera impostazione economica moderna**. In assenza di una seria politica monetaria al servizio del Paese, il costo elevato degli interessi finisce per condizionare e infine cancellare del tutto la politica fiscale dei governi.**

Per decenni si è inseguito il dogma della totale "indipendenza" della banca centrale. Un principio che ha separato completamente la gestione della moneta dai governi eletti e dagli obiettivi concreti di piena occupazione, sviluppo e crescita industriale.

Quando una banca centrale opera in un vuoto isolato e mantiene i tassi alti per rispondere unicamente ai propri parametri interni, il risultato per lo Stato è devastante. Gli interessi sul debito schizzano verso l'alto e finiscono per divorare le entrate fiscali prodotte da cittadini e imprese.

Nessun piano politico, per quanto ambizioso o ben intenzionato, può reggere a lungo contro questo meccanismo. La spesa per interessi azzera la sovranità fiscale e trasforma i

ministri dell’Economia in semplici esecutori contabili dei mercati obbligazionari.

Andy Burnham vorrebbe rilanciare la produzione nazionale, finanziare la transizione energetica e avviare un piano massiccio di edilizia popolare. E**ppure, senza un raccordo concreto tra politica monetaria e bilancio statale, ogni sua promessa elettorale rimarrà pura utopia.**

L’esperienza britannica dimostra che i trucchi contabili hanno terminato la loro corsa. Senza rimettere in discussione il ruolo della banca centrale e il suo distacco dalla crescita reale, anche Burnham è destinato al fallimento come chi lo ha preceduto. Prima o poi, anche la classe politica dovrà prenderne atto.

 Rimani aggiornato seguendoci su Google News!

SEGUICI

https://scenarieconomici.it/lillusione-di-burnham-si-scontra-con-il-muro-del-debito-perche-londra-e-condannata-allausterita/

X Live-Tweets Its Fight Against Chatbot Spam In Real-Time via @sejournal, @martinibuster



Nikita Bier, head of product at X (formerly known as Twitter) posted a series of extraordinary tweets about spam on Twitter, explaining the motivation of some of the spammers, they described types of spam and mentioned that some spammers were using Grok to auto-post spam responses at scale.

Nikita Bier spent 24 hours tweeting anti-spam actions in real time, revealing details about how how automated and fast-paced AI-assisted platform spamming has become.

42,000 Accounts In One Sweep

Bier started their series of tweets describing the scope of the chatbot problem, saying that providing authenticity on X is a core value that's central to the company's core values.

Bier tweeted:

> *"We found 42,000 accounts automating replies using chatbots and have removed them from the platform.*
>
> *X's core value is providing an authentic pulse on humanity — and using AI to programmatically engage with users without a human in the loop runs counter to our mission."*

Chatbot Spam Is Motivated By Money

Bier followed up the next day with a clarification about what the chatbot spamming was about. They explained that the spam wasn't ideologically driven, it was not political nor a a state-run influence operation. It was purely about monetization. Apparently the spammers were trying to grow an audience in order to leverage that for paid promotion deals from AI companies looking to extend their influence.

Companies don't normally post about their spam issues and the real-time posting by Bier offered a behind-the-scene look at the scale and motivations.

Bier tweeted:

> *Perhaps you should find a different app pic.twitter.com/z9Qv0vbpZj*
>
> *— Nikita Bier (@nikitabier) July 24, 2026*

And also posted an explanation:

> *"For transparency, the bulk of them were spamming thought-leadership slop about artificial intelligence — to grow accounts and receive paid promotion offers from AI tech companies.*
>
> *99.99% of spam on X is economically-motivated.*
>
> *Just plain old grifters."*

The Status Update: A Fix in Hours, Not Days

After a day Bier posted a quick update about a timeline for when to see the X feed improve, again showing how these kinds

of anti-spam actions work in real-time.

Bier tweeted:

> *“This spam attack was mitigated tonight. Your feed will improve in the next 6-12 hours.”*

X Fights Back Against AI Chatbot Spammers

Bier’s tweets served as an open statement to spammers to show how serious they are about fighting inauthentic behavior on the platform, calling the spammers criminals.

Bier tweeted:

> *“We will clean this place. I don’t care how many enemies I create. X will not be manipulated by criminals.”*

The Spammer Who’s Pivoted 40 Times

The most eye-opening part of the thread wasn’t a short exchange between Bier and one of the X members. Bier described one spam operator that was so persistent and adaptive (40 method changes in six months), that the spammer behaves less like a bot farm and more like someone who’s sitting right next to them tracking all their responses and rapidly coming up with a countermeasure.

A reply from an X member called attention to the fact that some of these spammers have started using Grok, X’s own AI product, to generate their replies. Bier confirmed that the Grok-based method had already been caught and blocked. In their response, Bier revealed that X’s response time of 12-18 hour turnarounds was an improvement over how long the same problem used to linger under the old Twitter.

Bier tweeted:

> *“There are a few spammers on X that have been pivoting their strategy for the last 6 months.*
>
> *One of the them (“This guy is a great trader ⬇”) has pivoted a total of 40 times after each method has been blocked.*
>
> *Some of the techniques are so creative and fast that it feels like they’re sitting right next to us.*
>
> *At this point, we might as well hire them because they are just as familiar with the X codebase as us.”*

@CryptoParadyme responded:

> *“please do not encourage them*
>
> *a lot of them have been using some kind of grok reply recently.”*

Bier tweeted:

> *“We blocked the Grok one yesterday.*
>
> *Our team is standing by waiting for their next move. We are 10x more proactive than before.*
>
> *This would fester for months at Twitter but our turnaround time now is 12-18 hours.”*

False Positive Reported And Dealt With

Another interesting result of this thread about spam actions in real-time is that one person posted about their false-positive experience with the spam actions. A false positive is when a machine makes a mistake, labeling something as spam

when in fact it’s not. In real life, these kinds of algorithms rely on a multitude of signals in order to pinpoint spam with a high level of accuracy but false positives can still happen, ideally a low percentage of time.

@the_defi_dad tweeted:

> *“I gotta be honest. I was surprised to get a notice for my account being spam. I clicked the request review button and about 12 hours later I was reinstated. I did complain about grass app being a scam and immediately got a notice. Not sure the link there but glad to see the algorithm or whatever decides spam or no spam made the right call.”*

Bier’s posts received a positive response from X users, some of whom expressed that some of these engagement chatbots must be generating engagement numbers but that their inauthentic nature makes them a scourge.

@RandomPerson242 tweeted:

> *“On one hand, people clearly like this rubbish somehow. On the other hand, I agree you can’t let that be the site’s content, even if people follow it. It can’t be a race to the bottom.”*

Social Media Is Best When Authentic

Many were happy to see that X was fighting back against inauthentic AI chatbot spam. It ruins the experience because people come to social media platforms like X to read and share human experiences.

Featured Image by Shutterstock/Naumova Marina

https://www.searchenginejournal.com/x-live-tweets-its-fight-against-chatbot-spam-in-real-time/583572/

Quishing: il QR code che scavalca la sicurezza email



Il quishing, cioè il phishing veicolato da un QR code, ha smesso di essere una curiosità e nel 2026 è diventato, nella telemetria di Microsoft, il vettore email in più rapida crescita. Non è un dettaglio di forma, un phishing con un'immagine al posto di un link: è un attacco costruito apposta per aggirare i controlli che difendono la posta aziendale e per portare la vittima là dove quei controlli non arrivano. I numeri lo confermano. Il rapporto Microsoft sulle minacce email del primo trimestre 2026 registra un balzo del phishing via QR da 7,6 a 18,7 milioni di attacchi tra gennaio e marzo, più 146%, il volume mensile più alto da almeno un anno, su circa 8,3 miliardi di minacce di phishing via email rilevate nel trimestre. ESET, nel suo Threat Report del primo semestre 2026 (dicembre 2025-maggio 2026), rileva che ormai l'11% delle email di phishing contiene un QR code, con una media di centomila rilevamenti al mese: è un livello record, sia pure su una serie storica breve, dato che ESET lo traccia come categoria distinta solo da settembre 2025. Per il lettore italiano conta la geografia dei bersagli: in testa Stati Uniti (19%) e Spagna (17%), seguiti da Messico (6%) e Regno Unito (5%), con l'Italia al 3% insieme a Cechia, Canada e Polonia; il fenomeno non risparmia il nostro Paese.

La ragione di questa crescita non è la novità della tecnica, che esiste da anni, ma la sua efficacia contro le difese attuali. Il QR sposta l'attacco in un punto cieco, e lo fa sfruttando due debolezze insieme: una tecnica, nei gateway di posta, e una umana, nella fiducia quasi automatica che le persone ripongono in un quadratino da inquadrare. Una

precisazione di perimetro, prima di procedere: qui si parla del quishing via email, ma lo stesso inganno vive anche nel mondo fisico, con QR fraudolenti su parcometri, bike sharing e finti avvisi di multa o di pedaggio. A Pesaro, nel maggio 2026, la società dei parcheggi controllata dal Comune ha denunciato la comparsa di QR fraudolenti su alcuni parcometri cittadini, che rimandavano a pagine non autorizzate dove veniva chiesto l'inserimento dei dati della carta: cambia il canale, non il meccanismo. Capire perché funziona è la premessa per difendersi in modo diverso dal solito richiamo a "non fidarsi delle email".

Perché il quishing, o QR code phishing, scavalca i controlli dell'email

I filtri di sicurezza della posta sono costruiti per analizzare testo e link: seguono gli URL, ne valutano la reputazione, riscrivono i collegamenti, confrontano il contenuto con schemi noti di truffa. Un QR code, per quei filtri, è un'immagine, e l'indirizzo che nasconde non è leggibile come testo. Il collegamento malevolo viaggia dentro un disegno che il gateway, se non è attrezzato a decodificarlo, non ispeziona. È lo scarto che rende il quishing efficace: non c'è un link da bloccare, c'è una figura che supera i controlli perché quei controlli guardano altrove.

Gli attaccanti hanno affinato anche la consegna. Il canale dominante resta l'allegato PDF, che anzi cresce dal 65% delle campagne QR di gennaio al 70% di marzo, mentre i documenti Office scendono dal 31% al 24%. Accanto a questo, nel marzo 2026 Microsoft ha osservato un aumento del 336% dei QR piazzati direttamente nel corpo dell'email: un volume ancora minoritario, il 5% del totale, ma un segnale di sperimentazione. È la conferma che la tecnica non solo cresce, ma cerca di continuo la superficie che i sistemi testuali non

sanno leggere.

Il salto sul telefono, fuori dal perimetro

C’è un secondo motivo, più insidioso del primo, ed è dove finisce la vittima. Un QR non si clicca dalla postazione di lavoro, si inquadra con il telefono. Nel momento in cui il dipendente prende lo smartphone per scansionare il codice, esce dall’ambiente protetto del computer aziendale ed entra su un dispositivo che le difese dell’organizzazione, di norma, non presidiano. Se poi il telefono è personale, come accade nella maggior parte dei casi, l’attacco si completa interamente fuori dal perimetro gestito, lontano dall’*endpoint detection* e dai proxy che filtrano il traffico dei portatili.

È un trasferimento di terreno prima ancora che di vittima: l’attacco parte in un canale sorvegliato, la posta, e si conclude in uno che quasi nessuno sorveglia, il browser di un telefono privato. A questo si aggiunge la fiducia implicita nel formato. Un URL sospetto mette in guardia, un QR no, perché è illeggibile all’occhio umano e associato a usi quotidiani e legittimi, dal menu del ristorante al pagamento. La vittima non vede l’indirizzo verso cui sta andando finché non ci è già arrivata, spesso su uno schermo piccolo dove i segnali d’allarme di un sito falso sono più difficili da cogliere.

Dove porta davvero: non un’immagine, una catena

Sarebbe un errore fermarsi al QR come se fosse l’attacco. Il codice è solo la consegna; la pagina di destinazione è quasi sempre una trappola per le credenziali, e nelle campagne più evolute non un semplice sito clone ma una pagina adversary-in-the-middle che si frappone tra la vittima e il servizio reale.

Una pagina di questo tipo non ruba solo la password, ma intercetta anche il codice del secondo fattore e il *token* di sessione, così l'attaccante entra come se avesse superato l'autenticazione forte. È la ragione per cui il quishing non va derubricato a truffa da utente distratto: è l'anello iniziale di una catena che può arrivare a un account takeover completo. Che non sia roba da dilettanti lo conferma chi lo usa: a gennaio 2026 l'FBI ha diffuso un'allerta sui QR malevoli impiegati nello spearphishing del gruppo nordcoreano Kimsuky contro obiettivi statunitensi, descrivendo attacchi che si chiudono con il furto e il riuso del token di sessione, così da scavalcare l'MFA senza generare un allarme di "autenticazione fallita". E le pagine AiTM a valle non sono artigianali, ma servite da kit di *phishing-as-a-service*: un ecosistema in continuo rimescolamento: Tycoon 2FA è stato smantellato a inizio marzo 2026, ma un kit rivale come Starkiller era già documentato due settimane prima del takedown.

Letto così, il vettore QR e il furto di sessione non sono due problemi distinti, ma lo stesso attacco visto da due estremi. Il QR serve a far attraversare indenne la posta e a spostare la vittima su un dispositivo scoperto; la pagina AiTM, all'altro capo, monetizza quel varco rubando l'accesso. Difendere solo un estremo lascia l'altro aperto.

Come difendersi: l'awareness non basta, serve struttura

La prima reazione, formare le persone a diffidare dei QR, è utile ma insufficiente, e per un motivo strutturale: il QR è nato per essere inquadrato senza pensarci, e un livello di sospetto abbastanza alto da bloccarlo bloccherebbe anche gli usi legittimi. La security awareness resta un tassello, ma va affiancata a controlli che non dipendono dall'attenzione del singolo. Sul piano della posta significa dotare i gateway

della capacità di decodificare i QR nelle immagini e di analizzare la destinazione prima della consegna, invece di trattarli come figure innocue. Sul piano del dispositivo significa estendere la protezione ai telefoni che accedono alle risorse aziendali, perché è lì che l'attacco si consuma.

Ma la difesa che chiude davvero la catena agisce all'ultimo anello, l'autenticazione. Se l'accesso è protetto solo da fattori resistenti al phishing, come le passkey basate su FIDO2, senza fallback su OTP o SMS, la pagina AiTM a cui il QR conduce non ha nulla da rubare: non esiste un codice da intercettare né un token riutilizzabile, perché la credenziale è legata al dominio legittimo e non funziona altrove. È lo spostamento decisivo, dal cercare di impedire alla vittima di arrivare sulla pagina falsa al rendere inutile il fatto che ci arrivi. Le altre misure riducono la probabilità dell'attacco; questa ne annulla il guadagno.

Cosa aspettarsi, senza illusioni

Il quishing non è una moda passeggera ma un vettore destinato a restare, perché sfrutta un divario reale e duraturo: quello tra la posta aziendale, sorvegliata, e il telefono personale, che non lo è. Finché l'attacco potrà partire in un canale controllato e concludersi in uno scoperto, il QR resterà uno strumento comodo per gli aggressori, e i numeri del 2026 lo dicono già con chiarezza. La risposta efficace non è un cartello che invita a non inquadrare i codici, ma una difesa a strati che unisce l'ispezione dei QR nella posta, la protezione dei dispositivi mobili e, soprattutto, un'autenticazione che regge anche quando la vittima finisce sulla pagina sbagliata. Trattare il quishing come una questione di distrazione individuale è il modo più sicuro per continuare a subirlo; trattarlo come ciò che è, un bypass architetturale, è il primo passo per neutralizzarlo.

Condividi sui Social Network:

https://www.ictsecuritymagazine.com/articoli/quishing-qr-code-phishing/

Memory safety: la classe di vulnerabilità che i governi vogliono estinguere



La memory safety è uno dei problemi di sicurezza più antichi del software, e nel 2026 è tornata in cima all'agenda con la spinta delle agenzie governative. Si tratta dell'assenza di una intera famiglia di difetti, quelli che nascono quando un programma gestisce a mano la memoria e sbaglia: un *buffer overflow* che scrive oltre i confini di un'area, un *use-after-free* che accede a memoria già liberata, una lettura fuori dai limiti. Non sono bug esotici, sono i mattoni con cui si costruiscono da decenni gli *exploit* più gravi, e continuano a esserlo. Secondo la guida di CISA e agenzie alleate del dicembre 2023, due terzi delle vulnerabilità segnalate nei linguaggi non *memory-safe* restano legate proprio alla gestione della memoria.

Il punto di svolta non è tecnico ma di prospettiva. Per anni questi difetti sono stati trattati come errori da correggere uno per uno; oggi l'idea che si sta affermando è che siano una classe da eliminare alla radice, scegliendo strumenti che non li rendano possibili. È lo spostamento dal "programmare con più attenzione" al "programmare in un linguaggio che non lascia commettere quell'errore", e ha smesso di essere una preferenza accademica per diventare una richiesta esplicita di chi regola il mercato.

Che cos’è la memory safety, e perché C e C++ non ce l’hanno

Un linguaggio è *memory-safe* quando impedisce, per costruzione, gli accessi scorretti alla memoria: non si può leggere oltre la fine di un array, usare un puntatore a memoria già liberata o dimenticare di controllare un limite, perché il linguaggio non lo consente o lo verifica al posto dello sviluppatore. Rientrano in questa categoria linguaggi molto diversi tra loro, da Java e C# a Go, Swift, Python e Rust, che ci arrivano per strade differenti: alcuni con un *garbage collector* che gestisce la memoria automaticamente, Rust con un sistema di proprietà verificato dal compilatore che ottiene lo stesso risultato senza rinunciare al controllo di basso livello.

C e C++, i linguaggi su cui poggia gran parte del software di sistema, non offrono questa garanzia: lasciano allo sviluppatore la gestione manuale della memoria, e con essa la possibilità di sbagliare. La conseguenza è quantificata da chi ha più codice al mondo. Microsoft ha stimato nel 2019 che circa il 70% delle proprie vulnerabilità con CVE derivasse ogni anno da problemi di memory safety, e in Chrome, su un’analisi di 912 bug di gravità alta o critica segnalati dal 2015 in poi, Google ne ha ricondotto alla stessa classe circa il 70%. Non è una questione di programmatori distratti: è che una classe di errori, su basi di codice enormi, si ripresenta comunque, a prescindere dalla bravura di chi scrive.

Da problema tecnico a richiesta delle autorità

La novità è che la memory safety è entrata nei documenti delle autorità. La stessa guida di CISA, NSA, FBI e delle agenzie di Australia, Canada, Regno Unito e Nuova Zelanda chiede ai produttori di software di pubblicare una *roadmap* memory-safe, cioè un piano concreto per ridurre nel tempo la dipendenza dai

linguaggi non sicuri. Con il documento Product Security Bad Practices, arrivato alla versione 2.0 nel gennaio 2025, il tono si è fatto più netto: sviluppare nuove linee di prodotto in linguaggi non *memory-safe*, per il software che sostiene funzioni critiche, viene indicato come una cattiva pratica, e ai produttori si chiede di pubblicare la propria roadmap entro la fine del 2025, scadenza ormai alle spalle, con l'eccezione dei prodotti la cui fine del supporto è prevista prima del 2030. Lo stesso documento precisa di non imporre alcun obbligo: non è una legge, ma una guida; sposta però le attese, e con esse la responsabilità di chi continua a ignorare il problema.

L'orientamento è confermato e dettagliato dal documento congiunto NSA e CISA sui linguaggi memory-safe del giugno 2025. In Europa la spinta è meno esplicita ma va nella stessa direzione, per la via del security by design: il Cyber Resilience Act, i cui requisiti essenziali di cybersicurezza si applicheranno dall'11 dicembre 2027, imporrà sicurezza fin dalla progettazione e gestione delle vulnerabilità per i prodotti con elementi digitali, mentre l'obbligo di segnalare le vulnerabilità attivamente sfruttate scatta già dall'11 settembre 2026. Il regolamento non nomina i linguaggi memory-safe, e il collegamento resta quindi inferenziale, ma un difetto di memoria evitabile alla radice è proprio il tipo di rischio che quell'obbligo mira a comprimere. La memory safety, insomma, sta migrando dal terreno delle buone pratiche a quello delle aspettative di mercato e, in prospettiva, degli obblighi.

La lezione di Android: non riscrivere tutto, cambiare il nuovo codice

La domanda ovvia è come si applichi tutto questo a basi di codice che contano decine di milioni di righe in C e C++. La

risposta più convincente arriva da Google, che sul codice di Android ha ottenuto un risultato netto senza una riscrittura di massa. La serie storica è eloquente: la quota di vulnerabilità dovute a problemi di memoria è passata dal 76% del 2019 al 24% del 2024, e nel 2025, secondo la rilevazione di novembre, è scesa sotto il 20% per la prima volta. Google non ha riscritto il vecchio codice, ha spostato sui linguaggi memory-safe il codice nuovo, e la differenza si legge nella densità dei difetti: una stima prudente colloca il codice Rust di Android intorno a 0,2 vulnerabilità di memoria per milione di righe, contro le circa mille del C e del C++, oltre mille volte in meno.

Funziona perché le vulnerabilità non si distribuiscono in modo uniforme nel tempo: il codice appena scritto ne contiene molte di più di quello che è invecchiato ed è stato ripulito a forza di correzioni. Concentrare i linguaggi sicuri dove nasce il rischio, cioè nelle nuove funzionalità, fa crollare la quota complessiva senza il costo proibitivo di rifare ciò che già funziona. E smonta anche l’idea che la sicurezza costi in produttività: sempre su Android, sulle modifiche medie e grandi il tasso di *rollback* delle modifiche in Rust è circa quattro volte più basso che in C++, e le modifiche in Rust passano in generale circa il 25% di tempo in meno in revisione. Non bisogna migrare tutto, insomma: bisogna smettere di aggiungere il problema.

Rust non risolve tutto: i limiti e la strada realistica

Sarebbe però un errore trasformare la memory safety in un tifo per un linguaggio. Anche il codice memory-safe ha i suoi confini: Rust prevede blocchi *unsafe* per le operazioni di basso livello e per il dialogo con il codice C, che riaprono in parte i rischi che il linguaggio altrove elimina. Il peso di questi blocchi, però, va misurato e non esagerato: nel

codice Rust circa il 4% sta dentro blocchi *unsafe*, e *unsafe* non disattiva la maggior parte dei controlli del linguaggio. E soprattutto la sicurezza della memoria non elimina le altre categorie di bug, dalla logica errata alle vulnerabilità di iniezione: un programma memory-safe può essere insicuro in mille altri modi. Ciò che si guadagna è la scomparsa della classe più numerosa e più sfruttata, non la sicurezza assoluta.

Resta poi l'enorme patrimonio di software che non si può realisticamente riscrivere, dai kernel al mondo *embedded* e industriale, dove C e C++ domineranno ancora a lungo. Per quel codice la risposta non è il linguaggio ma l'irrobustimento a più livelli: mitigazioni del compilatore, analisi statica lungo la pipeline di DevSecOps con strumenti come i SAST, fuzzing sistematico e architetture che confinano i danni. Che le difese a più livelli funzionino lo mostra un caso reale, arrivato peraltro dal versante opposto: una vulnerabilità del 2025 in un decoder Rust di Android (CVE-2025-48530), annidata in un blocco *unsafe*, non è mai arrivata in un rilascio pubblico, e il codice CVE le è stato assegnato solo per tracciarne la correzione con la giusta priorità. Il postmortem ha stabilito che l'allocatore *hardened* Scudo la rendeva comunque deterministicamente non sfruttabile grazie alle sue *guard pages*, che anzi hanno contribuito a scoprirla trasformando un overflow silenzioso in un crash rumoroso. Scudo è l'allocatore predefinito di Android, benché Google stia ancora lavorando con i partner per renderlo obbligatorio ovunque. È la difesa in profondità che fa il suo lavoro, e la conferma che la strada realistica è duplice: linguaggi memory-safe per il nuovo, difese a più livelli per il vecchio.

La pressione, del resto, si sente anche fuori da Android. Il mondo C++ ha reagito ai richiami delle agenzie scegliendo la via dei Profiles, un insieme di regole di sicurezza opzionali, dopo aver di fatto accantonato la proposta più radicale di un *borrow checker* in stile Rust, una scelta che diversi critici

giudicano insufficiente a garantire una sicurezza stretta. Dentro Microsoft, un *distinguished engineer* ha reso pubblico a fine 2025 il proprio obiettivo, eliminare C e C++ dal codice dell'azienda entro il 2030, usando AI e algoritmi per tradurre i *codebase* più grandi, come da strategia del gruppo di ricerca di cui fa parte. L'autore ha poi precisato che si tratta di un progetto di ricerca e non di una strategia aziendale, ma la sola circolazione dell'idea dice quanto si sia spostato il baricentro del dibattito. E un argomento nuovo rende tutto più urgente: quando la generazione di codice assistita dall'AI produce software più in fretta di quanto gli umani riescano a rivederlo, conviene che quel codice nasca in un linguaggio che certi errori non li permette nemmeno.

Cosa aspettarsi, senza illusioni

La memory safety non è una bacchetta magica e non renderà sicuro il software di colpo, ma è probabilmente l'intervento con il miglior rapporto tra costo e beneficio disponibile oggi: rimuove alla radice la classe di vulnerabilità più numerosa e più sfruttata, e lo fa nel punto più economico, cioè prima che il difetto esista. Per chi sviluppa significa adottare una disciplina di secure coding che parte dalla scelta del linguaggio per il codice nuovo; per chi compra software significa iniziare a chiedere ai fornitori la loro roadmap memory-safe, esattamente come oggi si chiede un SBOM. Il messaggio che arriva dalle agenzie è che continuare a produrre nuovi difetti di memoria, avendo gli strumenti per non farlo, non sarà più considerato normale. La memory safety, da nicchia per specialisti, è diventata il modo più concreto per ridurre la superficie d'attacco alla fonte.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/memory-safety-linguaggi-sicuri/

Iran-Usa, Trump ferma gli attacchi: chance per dialogo con Teheran

(Adnkronos) –
Donald Trump congela gli attacchi contro l'Iran e punta sul dialogo. Il premier israeliano Benjamin Netanyahu, però, si appresta a volare a Washington e fornirà al presidente americano informazioni relative al programma nucleare che Teheran non avrebbe abbandonato. Il meeting in programma martedì alla Casa Bianca può segnare una svolta nella crisi che infiamma da mesi il Medio Oriente. Dopo quasi 2 settimane di raid ininterrotti, Trump ha fermato le operazioni. Il presidente degli Stati Uniti ha ordinato alle forze armate di non condurre raid contro l'Iran nella notte tra venerdì 24 e sabato 25 luglio, interrompendo quindi la striscia di 13 giorni consecutivi di attacchi.

La decisione riflette la volontà di dare più spazio alla diplomazia ma anche il riconoscimento che l'attuale livello di attacchi ha raggiunto il limiti di efficacia, come evidenzia Axios, citando due fonti informate. Non è chiaro se lo stop sia destinato a durare a lungo o se rappresenti un'eccezione. Lo stesso Trump, d'altra parte, nelle ultime uscite pubbliche ha evidenziato due opzioni differenti: "Potremmo lanciare un maxi attacco. Stiamo parlando con l'Iran, vuole un accordo ma non è ancora pronto".

Le informazioni raccolte dai media americani delineano un quadro secondo cui le forze Usa preparano ancora piani per un ritorno ad operazioni di combattimento in larga scala, ma il presidente non avrebbe ancora dato l'ordine. Nelle ultime due

settimane, secondo la ricostruzione di Axios, ogni pomeriggio i militari hanno chiesto e ottenuto da Trump l'approvazione per la lista di obiettivi che avrebbero colpito nel giro di poche ore. Nella giornata di venerdì, invece, il presidente non ha dato la luce verde, spiegano ancora le fonti.

Axios ricorda come l'ordine di Trump di fermare i raid sia stato dato poche ore dopo l'arrivo a Teheran di una delegazione dell'Oman per negoziati tesi a raggiungere un nuovo accordo per la riapertura dello Stretto di Hormuz. Nei colloqui sarebbero stati fatti progressi, rivelano fonti regionali, con la possibilità di raggiungere un'intesa tra Oman e Iran nel weekend.

In un quadro estremamente precario, si inserisce il viaggio di Netanyahu a Washington. Il premier israeliano, secondo l'emittente Channel 12, presenterà a Trump nuove informazioni di intelligence sugli sforzi che l'Iran sta compiendo per riprendere il programma nucleare. In particolare, il primo ministro illustrerà come i vertici della sua intelligence credano che sotto la leadership del leader supremo Mojtaba Khamenei siano stati accelerati gli sforzi per ottenere l'arma nucleare. L'emittente cita infine un alto funzionario israeliano che afferma che "le possibilità che si raggiunga un accordo tra Iran e Stati Uniti sono praticamente inesistenti", definendo "inevitabile" arrivare alla fine all'escalation del conflitto.

—

internazionale/esteri

webinfo@adnkronos.com (Web Info)

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Add as a preferred source on Google

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/iran-usa-trump-ferma-gli-attacchi-chance-per-dialogo-con-teheran/582673/

Ucraina-Russia, Zelensky: “Putin vuole 30mila soldati nordcoreani”

(Adnkronos) –
Vladimir Putin ha bisogno di soldati e la Corea del Nord può tornare protagonista della guerra tra Ucraina e Russia. Così afferma il presidente ucraino Volodymyr Zelensky. “La Russia vuole accogliere altri 30.000 soldati dalla Corea del Nord”, dice. “Disponiamo di rapporti di intelligence approfonditi sui piani della Russia per l’autunno. Ciò che non è previsto nei piani della Russia è la pace. Purtroppo, non ancora”, dice il leade di Kiev. “Putin sta creando le condizioni per un’ulteriore mobilitazione”, dice, delineando un quadro nel quale il Cremlino sarebbe pronto a rinforzare l’apparato militare per compensare le perdite sul campo. “Le cifre parlano da sole. In meno di sette mesi quest’anno, 221.000 persone si sono arruolate nelle Forze Armate russe. Nello stesso periodo, le perdite russe ammontano a quasi 225.500 unità: 131.000 morti e quasi 93.000 feriti. Una parte significativa di questi feriti è grave, poiché l’assistenza medica in prima linea in Russia è catastroficamente carente”,

afferma Zelensky.

“Putin si sta preparando a mandare semplicemente più russi in guerra. Lo nasconde a parole, ma si sta preparando a farlo. È fondamentale che, insieme ai nostri partner, esercitiamo una pressione sufficiente sulla Russia affinché l’idea di porre fine a questa aggressione diventi prevalente. Deve imporsi l’idea di pace, non di un’altra mobilitazione russa”, dice Zelensky.

L’asse tra Mosca e Pyongyang ha già prodotto risultati nel conflitto, iniziato ormai 4 anni e mezzo fa. La Corea del Nord ha inviato migliaia di soldati, che sono stati schierati nel corso del 2025 in particolare nella regione russa del Kursk, invasa per mesi dalle truppe di Kiev. Ora, Putin chiederebbe nuovamente la collaborazione di Kim Jong-un e il dialogo sarebbe già ad un livello avanzato. Per Zelensky, da giugno sarebbero “in corso i preparativi nella regione russa di Voronez per accogliere” i soldati nordcoreani.

La collaborazione tra Mosca e Pyongyang, da tempo, si basa sulle forniture militari nordcoreane. Il regno eremita ha garantito da tempo munizioni all’esercito russo. Ora, dice Zelensky, si prospetta un salto di qualità: “La Corea del Nord si sta anche preparando a trasferire alla Russia ulteriori lanciatori di missili balistici. Questa è una minaccia non solo per l’Ucraina”, dice il presidente ucraino, convinto che la Russia stia ‘ricambiando la cortesia’ fornendo alla Corea del Nord informazioni e capacità per “acquisire una reale esperienza di combattimento. Questo rappresenta una minaccia per chiunque in Asia si trovi nel raggio d’azione dei missili nordcoreani”.

—

internazionale/esteri

webinfo@adnkronos.com (Web Info)

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui



Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/ucraina-russia-zelensky-putin-vuole-30mila-soldati-nordcoreani/582675/

Terrore al Pride di Berlino, furgone sulla folla: un morto e 15 feriti

(Adnkronos) –
Un furgone ha travolto diversi pedoni a Berlino nella serata di oggi, sabato 25 luglio. Secondo la Bild, una persona è morta e altre 15 sono rimaste ferite. Il veicolo si è lanciato sulla folla durante il Christopher Street Day (CSD), il Pride della capitale della Germania, nel parco Tiergarten.

L'incidente è avvenuto intorno alle 22:00. Il furgone bianco si è lanciato a forte velocità – a circa 80 km orari – sulla folla e ha concluso la sua corsa contro un albero. Altri testimoni citati dal quotidiano hanno riferito di aver visto un uomo uscire dal veicolo: il sospetto, armato di coltello, avrebbe aggredito alcune persone.
Per il Berliner Kurier, un uomo è stato arrestato. Un secondo individuo sarebbe in fuga. Nelle operazioni della polizia è coinvolta l'unità speciale Gsg 9, reparto antiterrorismo.

Gli organizzatori del CSD hanno annunciato la cancellazione dell'evento. La parola "evacuazione" è apparsa a caratteri cubitali sul grande schermo della Porta di Brandeburgo. Poco dopo, un post su Instagram ha invitato i partecipanti a lasciare la zona "con calma e in modo ordinato". "Si prega di evitare la Colonna della Vittoria e il Tiergarten. Lasciate la zona in direzione della stazione ferroviaria principale", il post.

"È un attacco alla nostra società libera e cosmopolita: dopo una pacifica e vivace parata del Christopher Street Day (CSD), la manifestazione per una Berlino tollerante e pacifica è stata attaccata nel modo più brutale. Berlino è la città della libertà e la nostra libertà è stata oggi orribilmente attaccata", scrive su X il sindaco Kai Wegner. "Il mio pensiero va alle vittime, alle loro famiglie e ai loro amici. Ringrazio i servizi di emergenza che sono intervenuti immediatamente e hanno fatto tutto il possibile. E ho fiducia nella polizia e nelle autorità di sicurezza, che indagheranno con la massima urgenza".

"Attualmente è in corso un'operazione di polizia su larga scala nel Tiergarten – spiega la polizia di Berlino sull'account di X – L'area è stata transennata dalle nostre forze di intervento". "Siamo sul posto con numerose forze di polizia nonché con i soccorritori del Corpo dei Vigili del Fuoco di Berlino", ha detto in un video su X un portavoce della polizia.

–

internazionale/esteri

webinfo@adnkronos.com (Web Info)

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui



Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/terrore-al-pride-di-berlino-furgone-sulla-folla-un-morto-e-15-feriti/582677/