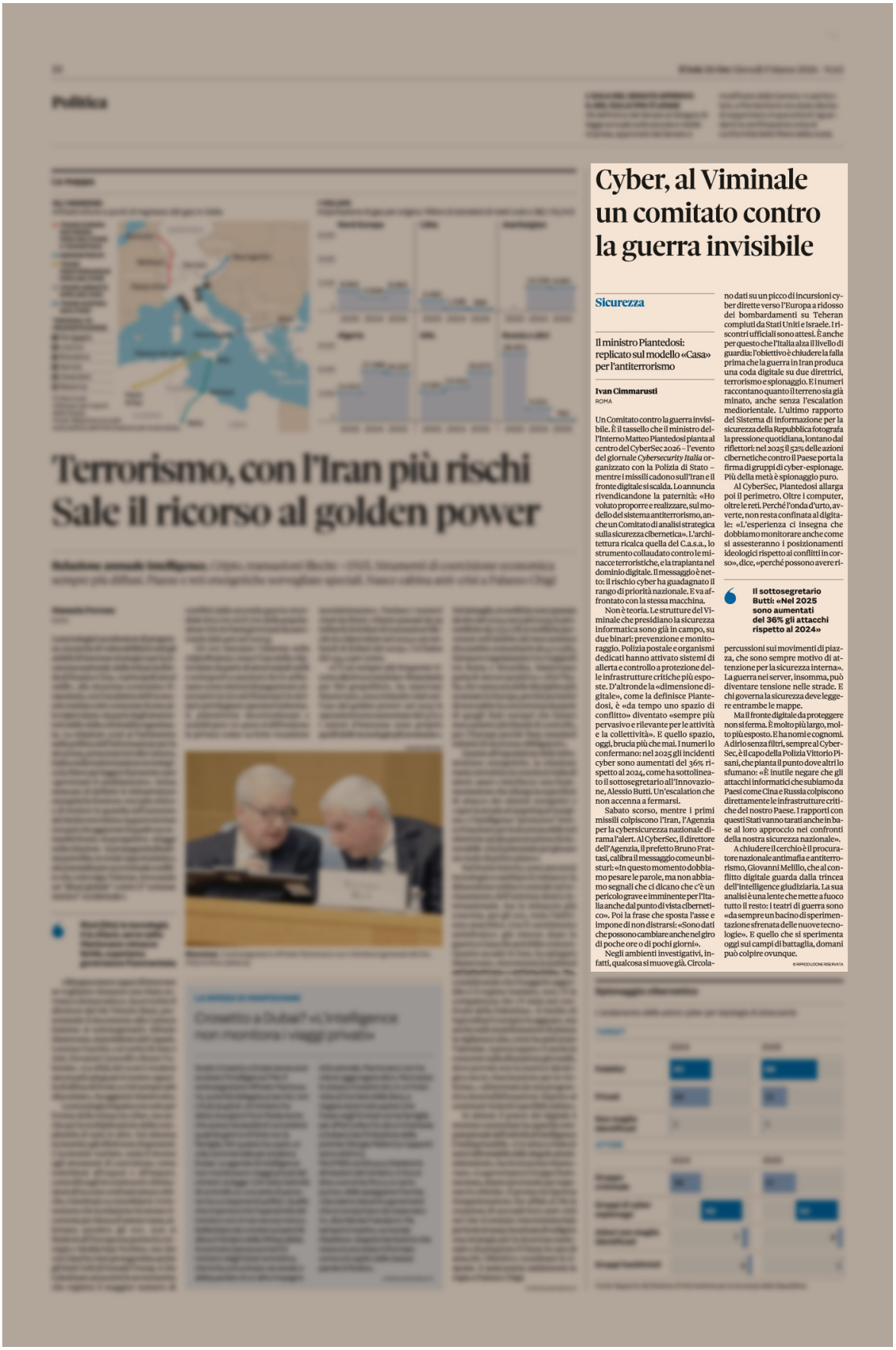

Cyber, al Viminale un comitato contro la guerra invisibile

Sicurezza

Il ministro Piantedosi: replicato sul modello «Casa» per l'antiterrorismo

Ivan Cimmarusti
ROMA

Un Comitato contro la guerra invisibile. È il tassello che il ministro dell'Interno Matteo Piantedosi pianta al centro del CyberSec 2026 – l'evento del giornale *Cybersecurity Italia* organizzato con la Polizia di Stato – mentre i missili cadono sull'Iran e il fronte digitale si scalda. Lo annuncia rivendicandone la paternità: «Ho voluto proporre e realizzare, sul modello del sistema antiterrorismo, anche un Comitato di analisi strategica sulla sicurezza cibernetica». L'architettura ricalca quella del C.a.s.a., lo strumento collaudato contro le minacce terroristiche, e la trapianta nel dominio digitale. Il messaggio è netto: il rischio cyber ha guadagnato il rango di priorità nazionale. E va affrontato con la stessa macchina.

Non è teoria. Le strutture del Viminale che presidiano la sicurezza informatica sono già in campo, su due binari: prevenzione e monitoraggio. Polizia postale e organismi dedicati hanno attivato sistemi di allerta e controllo a protezione delle infrastrutture critiche più esposte. D'altronde la «dimensione digitale», come la definisce Piantedosi, è «da tempo uno spazio di conflitto» diventato «sempre più pervasivo e rilevante per le attività e la collettività». E quello spazio, oggi, brucia più che mai. I numeri lo confermano: nel 2025 gli incidenti cyber sono aumentati del 36% rispetto al 2024, come ha sottolineato il sottosegretario all'Innovazione, Alessio Butti. Un'escalation che non accenna a fermarsi.

Sabato scorso, mentre i primi missili colpiscono l'Iran, l'Agenzia per la cybersicurezza nazionale diramal'alert. Al CyberSec, il direttore dell'Agenzia, il prefetto Bruno Frattasi, calibra il messaggio come un bisturi: «In questo momento dobbiamo pesare le parole, ma non abbiamo segnali che ci dicano che c'è un pericolo grave e imminente per l'Italia anche dal punto di vista cibernetico». Poi la frase che sposta l'asse e impone di non distrarsi: «Sono dati che possono cambiare anche nel giro di poche ore o di pochi giorni».

Negli ambienti investigativi, infatti, qualcosa si muove già. Circolano dati su un picco di incursioni cyber dirette verso l'Europa a ridosso dei bombardamenti su Teheran compiuti da Stati Uniti e Israele. I riscontri ufficiali sono attesi. È anche per questo che l'Italia alza il livello di guardia: l'obiettivo è chiudere la falla prima che la guerra in Iran produca una coda digitale su due direttrici, terrorismo e spionaggio. E i numeri raccontano quanto il terreno sia già minato, anche senza l'escalation mediorientale. L'ultimo rapporto del Sistema di informazione per la sicurezza della Repubblica fotografa la pressione quotidiana, lontano dai riflettori: nel 2025 il 52% delle azioni cibernetiche contro il Paese porta la firma di gruppi di cyber-espionage. Più della metà è spionaggio puro.

Al CyberSec, Piantedosi allarga poi il perimetro. Oltre i computer, oltre le reti. Perché l'onda d'urto, avverte, non resta confinata al digitale: «L'esperienza ci insegna che dobbiamo monitorare anche come si assesteranno i posizionamenti ideologici rispetto ai conflitti in corso», dice, «perché possono avere ri-

> **Il sottosegretario Butti: «Nel 2025 sono aumentati del 36% gli attacchi rispetto al 2024»**

percussioni sui movimenti di piazza, che sono sempre motivo di attenzione per la sicurezza interna». La guerra nei server, insomma, può diventare tensione nelle strade. E chi governa la sicurezza deve leggere entrambe le mappe.

Ma il fronte digitale da proteggere non si ferma. È molto più largo, molto più esposto. E ha nomi e cognomi. A dirlo senza filtri, sempre al CyberSec, è il capo della Polizia Vittorio Pisani, che pianta il punto dove altri lo sfumano: «È inutile negare che gli attacchi informatici che subiamo da Paesi come Cina e Russia colpiscono direttamente le infrastrutture critiche del nostro Paese. I rapporti con questi Stati vanno tarati anche in base al loro approccio nei confronti della nostra sicurezza nazionale».

A chiudere il cerchio è il procuratore nazionale antimafia e antiterrorismo, Giovanni Melillo, che al conflitto digitale guarda dalla trincea dell'intelligence giudiziaria. La sua analisi è una lente che mette a fuoco tutto il resto: i teatri di guerra sono «da sempre un bacino di sperimentazione sfrenata delle nuove tecnologie». E quello che si sperimenta oggi sui campi di battaglia, domani può colpire ovunque.

Sicurezza

Cyber, al Viminale un comitato contro la guerra invisibile

Il ministro Piantedosi: replicato sul modello «Casa» per l'antiterrorismo

Ivan Cimmarusti

ROMA Un Comitato contro la guerra invisibile.
È il tassello che il ministro dell'Interno Matteo Piantedosi pianta al centro del CyberSec 2026 - l'evento del giornale Cybersecurity Italia organizzato con la Polizia di Stato - mentre i missili cadono sull'Iran e il fronte digitale si scalda.
Lo annuncia rivendicandone la paternità: «Ho voluto proporre e realizzare, sul modello del sistema antiterrorismo, anche un Comitato di analisi strategica sulla sicurezza cibernetica».
L'architettura ricalca quella del C.a.s.a., lo strumento collaudato contro le minacce terroristiche, e la trapianta nel dominio digitale.
Il messaggio è netto: il rischio cyber ha guadagnato il rango di priorità nazionale.
E va affrontato con la stessa macchina.
Non è teoria.
Le strutture del Viminale che presidiano la sicurezza informatica sono già in campo, su due binari: prevenzione e monitoraggio.
Polizia postale e organismi dedicati hanno attivato sistemi di allerta e controllo a protezione delle infrastrutture critiche più esposte.
D'altronde la «dimensione digitale», come la definisce Piantedosi, è «da tempo uno spazio di conflitto» diventato «sempre più pervasivo e rilevante per le attività e la collettività».
E quello spazio, oggi, brucia più che mai.
I numeri lo confermano: nel 2025 gli incidenti cyber sono aumentati del 36% rispetto al 2024, come ha sottolineato il sottosegretario all'Innovazione, Alessio Butti.
Un'escalation che non accenna a fermarsi.
Sabato scorso, mentre i primi missili colpiscono l'Iran, l'Agenzia per la cybersicurezza nazionale dirama l'alert.
Al CyberSec, il direttore dell'Agenzia, il prefetto Bruno Frattasi, calibra il messaggio come un bisturi: «In questo momento dobbiamo pesare le parole, ma non abbiamo segnali che ci dicano che c'è un pericolo grave e imminente per l'Italia anche dal punto di vista cibernetico».
Poi la frase che sposta l'asse e impone di non distrarsi: «Sono dati che possono cambiare anche nel giro di poche ore o di pochi giorni».
Negli ambienti investigativi, infatti, qualcosa si muove già.
Circolano dati su un picco di incursioni cyber dirette verso l'Europa a ridosso dei bombardamenti su Teheran compiuti da Stati Uniti e Israele.
I riscontri ufficiali sono attesi.
È anche per questo che l'Italia alza il livello di guardia: l'obiettivo è chiudere la falla prima che la guerra in Iran produca una coda digitale su due direttrici, terrorismo e spionaggio.
E i numeri raccontano quanto il terreno sia già minato, anche senza l'escalation mediorientale.
L'ultimo rapporto del Sistema di informazione per la sicurezza della Repubblica fotografa la pressione quotidiana, lontano dai riflettori: nel 2025 il 52% delle azioni cibernetiche contro il Paese porta la firma di gruppi di cyber-espionage.
Più della metà è spionaggio puro.

Al CyberSec, Piantedosi allarga poi il perimetro.

Oltre i computer, oltre le reti.

Perché l'onda d'urto, avverte, non resta confinata al digitale: «L'esperienza ci insegna che dobbiamo monitorare anche come si assesteranno i posizionamenti ideologici rispetto ai conflitti in corso», dice, «perché possono avere ripercussioni sui movimenti di piazza, che sono sempre motivo di attenzione per la sicurezza interna».

La guerra nei server, insomma, può diventare tensione nelle strade.

E chi governa la sicurezza deve leggere entrambe le mappe.

Ma il fronte digitale da proteggere non si ferma.

È molto più largo, molto più esposto.

E ha nomi e cognomi.

A dirlo senza filtri, sempre al CyberSec, è il capo della Polizia Vittorio Pisani, che pianta il punto dove altri lo sfumano: «È inutile negare che gli attacchi informatici che subiamo da Paesi come Cina e Russia colpiscono direttamente le infrastrutture critiche del nostro Paese.

I rapporti con questi Stati vanno tarati anche in base al loro approccio nei confronti della nostra sicurezza nazionale».

A chiudere il cerchio è il procuratore nazionale antimafia e antiterrorismo, Giovanni Melillo, che al conflitto digitale guarda dalla trincea dell'intelligence giudiziaria.

La sua analisi è una lente che mette a fuoco tutto il resto: i teatri di guerra sono «da sempre un bacino di sperimentazione sfrenata delle nuove tecnologie».

E quello che si sperimenta oggi sui campi di battaglia, domani può colpire ovunque.