QUOTIDIANO NAZIONALE

06-NOV-2026
da pag. 4 / foglio 1 / 3

Quotidiano - Dir. Resp.: Agnese Pini
Tiratura: 137439 Diffusione: 84577 Lettori: 903000 (Data Stampa 0006901)

DATA STAMPA
45° Anniversario

Data Stampa 6901-Data Stampa 6901
Data Stampa 6901-Data Stampa 6901




## L'impatto

# Il conto degli attacchi: dagli aerei ai frigoriferi mezzo miliardo di danni Solo far alzare un caccia costa 75mila euro all'ora

*di* **Alessandro Da Rold, ROMA**

Quanto costa agli italiani e agli europei la guerra ibrida? Quanto pesano gli allarmi bomba sugli aerei, i frigoriferi dei supermercati manomessi a distanza, gli attacchi informatici? Per capirlo non bastano neppure i rapporti economici pubblicati in questi anni di guerra tra Russia e Ucraina. «Non esiste un costo medio univoco associabile a un allarme bomba o al conseguente dirottamento di un volo», spiega a QN Luca Mantecchini, docente di Ingegneria dei trasporti all'Università di Bologna. Non esiste insomma un bilancio unico. Minacce, sabotaggi e spionaggio generano spese e danni difficili da separare.

Gli episodi di questi giorni raccontano un problema che potrebbe diventare presto quotidiano. Una mail anonima mobilita artificieri e caccia, provoca deviazioni e ritardi senza alcun esplosivo.

Nei supermercati gli aggressori hanno modificato da remoto le temperature dei frigoriferi, costringendo a buttare alimenti. Palazzo Chigi ha circoscritto l'impatto italiano a pochi punti vendita. In Francia


Quanto ci costa la guerra ibrida


L'Italia e il format Kiev «Parli una sola voce»

ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - DS6901 - S.30524 - L.1849 - T.1849

l'attacco di ottobre ha colpito centinaia di negozi. Thierry Cotillard, presidente del gruppo Intermarché, ha stimato perdite per decine di milioni di euro. Non c'è neppure certezza sulla copertura assicurativa delle merci deteriorate, perché molte polizze informatiche escludono i danni materiali.

Che cosa sia questa guerra senza soldati lo spiegano bene Norbert Metiu e Martin Völpel, economisti della Bundesbank, nello studio 'Geopolitical Hybrid Threats' di marzo. Un contesto bellico dove «sfuma il confine tra guerra e pace», scrivono. E parlano di attacchi informatici, sabotaggi, spionaggio, pressioni economiche e disinformazione. «Operano sotto la soglia del conflitto aperto». Non producono macerie, ma frenano consumi e investimenti. La finalità, spiegano gli autori, è una sola: «seminare paura e incertezza» tra la popolazione.

Gli economisti della Bundesbank hanno esaminato oltre dodici milioni di articoli di giornale, pubblicati dal 1985, per costruire un indicatore della diffusione delle minacce ibride, dagli attacchi informatici ai sabotaggi e allo spionaggio.

Hanno quindi simulato le conseguenze economiche di un aumento delle minacce paragonabile a quello registrato all'inizio dell'invasione russa dell'Ucraina, nel 2022. Secondo il loro modello, negli Stati Uniti il Pil reale pro capite potrebbe ridursi fino a quasi l'1,5 per cento e gli investimenti del 6,2 per cento nell'arco di un anno. Quando aumentano gli attacchi informatici, le famiglie diventano più prudenti negli acquisti, le imprese rinviano gli investimenti e l'economia rallenta.

Del resto aggressioni digitali possono fermare la produzione, interrompere i servizi e pesare sui bilanci delle imprese. Lo segnala anche la Banca d'Italia in una ricerca di gennaio, 'Il rischio cibernetico delle imprese non finanziarie'.

La ricerca esamina circa quattromila aziende, tra bilanci e rapporti di sicurezza. Nel campione gli attacchi documentati sono passati da 14 nel 2019 a 232 nel 2023. Dopo un incidente le difese richiedono tempo per funzionare, mentre la vulnerabilità aumenta subito. I ricercatori suggeriscono perciò di considerare il rischio informatico anche quando le banche valutano l'affidabilità di un'azienda. Un altro rapporto sulla stabilità finanziaria fotografa la dipendenza del sistema bancario dalla tecnologia. Gli intermediari finanziari, banche e altre società finanziarie sottoposte ai controllo di Bankitalia, hanno circa 100mila contratti con fornitori informatici, per 2,4 miliardi di euro di spesa annua. E il 40 per cento del valore è concentrato su appena cinque fornitori.

La risposta dello Stato passa anche dalle gare pubbliche. Il 15 ottobre Consip ha annunciato tre iniziative per oltre 1,2 miliardi di euro destinate a proteggere reti e dati delle amministrazioni: 826 milioni per servizi di sicurezza da remoto, 317 per sistemi di protezione e 112 per la gestione delle infrastrutture. Intanto le istituzioni sono nel mirino. Nella relazione sul 2024 Consob ricordava oltre 2,5 milioni di tentativi di attacco informatico contro i propri sistemi e denuncia ripetute offensive di soggetti filorussi. Le difese, precisa l'autorità di vigilanza sulla Borsa, hanno evitato conseguenze significative. Il numero comprende eventi di natura diversa da quelli a cui stiamo assistendo in questi giorni: non sono 2,5 milioni di violazioni riuscite, né tutti i tentativi sono attribuiti ai gruppi filorussi.

In Italia manca una cifra totale. Il 2 novembre scorso Hackmanac, piattaforma di intelligence sulle minacce informatiche, stimava nel nostro Paese 468,18 milioni di dollari di perdite associate a 407 incidenti informatici nel primo semestre 2026.

Non solo. Un recente rapporto della multinazionale Ibm sull'Italia indicava invece 3,55 milioni di euro come costo medio di una violazione dei dati nelle organizzazioni italiane esaminate, mentre nel settore energetico si sale a 4,65 milioni. Il Politecnico di Milano valuta in 2,78 miliardi il mercato italiano della cybersicurezza nel 2025, cresciuto del 12 per cento in un anno. Il 34 per cento delle grandi imprese ha sostenuto costi significativi di ripristino. Negli Stati Uniti l'Fbi registra per il 2025 quasi 21 miliardi di dollari di perdite denunciate per reati online, in gran parte frodi: non tutte legate a operazioni ostili o a intelligence straniere.

Quanto vale invece un falso allarme bomba su un aereo? Secondo i parametri di Eurocontrol, citati da Mantecchini, i ritardi possono costare indicativamente tra i 160 e 2.010 euro al minuto per singolo volo, considerando anche le ripercussioni sugli altri collegamenti. Ma il conto non si ferma qui. Un aereo costretto ad atterrare in un aeroporto diverso deve essere rifornito, riposizionato e riprogrammato. I passeggeri possono avere bisogno di assistenza. «Gli affetti indiretti possono propagarsi nella rete, coinvolgendo voli e aeroporti non direttamente interessati», ricorda Mantecchini.

C'è poi la spesa militare. Secondo dati della Difesa 75mila euro è il costo medio per l'utilizzo di un Eurofighter per solo un'ora di volo.

L'Aeronautica italiana ha registrato nel 2025 quindici intercettazioni reali, trenta minacce di dirottamento e 43 ore e 22 minuti di volo. «È ragionevole affermare che le conseguenze economiche di questi eventi possano verosimilmente essere significative e superiori ai soli costi immediatamente visibili», conclude Mantecchini.

I DATI INCROCIATI

**I voli interrotti dopo il cibo buttato via Dietro il conflitto senz'armi esborsi ingenti e danni per la collettività**

L'ANALISI

**Il docente di Ingegneria Luca Mantecchini «Conseguenze legate a offensive o spionaggio difficili da quantificare»**

**33,3%**

**L'aumento delle perdite in un semestre**
Il dato è stimato dal Global Cyber Loss Report calcolato su un totale di 407 incidenti informatici in Italia che sono stati registrati nel primo semestre dell'anno

ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - DS6901 - S.30524 - L.1849 - T.1849

QUOTIDIANO NAZIONALE

06-NOV-2026
da pag. 4 / foglio 3 / 3

Quotidiano - Dir. Resp.: Agnese Pini
Tiratura: 137439 Diffusione: 84577 Lettori: 903000 (Data Stampa 0006901)

DATA STAMPA
45° Anniversario

# 34%

**La quota delle grandi imprese vittime di attacchi**
Un dato che emerge considerando le intrusioni informatiche che hanno richiesto costi significativi di ripristino
Il 3% delle aziende ha registrato anche ripercussioni operative

# 623 milioni

**La dotazione Pnrr per la cybersicurezza**
Sono i fondi messi in campo nell'ambito del piano nazionale per rafforzare la sicurezza informatica nazionale le infrastrutture e la capacità di risposta agli attacchi

**Lorenzo Guerini (Pd)**

«Evidente minaccia ibrida Queste situazioni generano preoccupazioni e insicurezza Soglia d'allarme da elevare»



**Francesco Lollobrigida**

«Il cibo usato come arma impropria in una guerra ibrida sempre più complessa Il sistema è troppo fragile»



**Matilde Siracusano (Fi)**

«Sono attacchi non convenzionali che per noi comuni cittadini sono difficili da immaginare Ma il governo non sottovaluta»



ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - DS6901 - S.30524 - L.1849 - T.1849