03-NOV-2026
da pag. 1-10 /foglio 1 / 2

la Repubblica

Quotidiano - Dir. Resp.: Stefano Cappellini
Tiratura: 109075 Diffusione: 123028 Lettori: 1320000 (Data Stampa 0006901)

DATA STAMPA
45° Anniversario

Data Stampa 6901 Data Stampa 6901

Sabotaggi e guerra psicologica la strategia usata dai russi

di **GIANLUCA DI FEO**

a pagina **10**

Sabotaggi e guerra cognitiva così lo zar usa il conflitto ibrido contro infrastrutture fragili

La rete di sicurezza in Europa è piena di falle Pioggia di falsi messaggi di allerta anche sulle app ucraine: panico a Kiev

L'ANALISI

di **GIANLUCA DI FEO**
ROMA

I messaggi sulla app degli allarmi aerei che hanno seminato il panico nucleare a Kiev e le celle frigorifero mandate in tilt sono due capitoli della stessa guerra. La si può chiamare ibrida, cognitiva o psicologica ma l'obiettivo è lo stesso: diffondere la paura e incrinare la coesione delle società, che si tratti dell'Ucraina o dei Paesi europei che la sostengono. In entrambi i casi, però, lo scopo non è stato raggiunto attraverso strumenti di propaganda: sono stati colpiti i computer, dimostrando così che la sicurezza di una nazione oggi dipende completamente da quella delle sue reti cibernetiche. Sono il cardine della nostra vita e sono terribilmente fragili, perché cresciute senza tenere conto della minaccia non di predatori o sabotatori, ma di manovre gestite da entità statali con risorse e capacità tecnologiche superiori a qualunque azienda privata e spesso pure delle istituzioni.

Tutti parlano da anni di difesa cyber. Quello che sta accadendo dimostra che l'Europa è piena di falle, dove si riesce a penetrare con facilità. Se un singolo supermarket paralizzato non fa notizia, l'offensiva su larga scala in più Paesi trasmette un brivido e mette in discussione la reperibilità degli alimenti fondamentali: come se venissimo rimandati indietro di mezzo secolo, all'epoca in cui non esistevano i surgelati e la conservazione al freddo dei cibi.

Anche nei server ucraini è stata realizzata una breccia, facendo recapitare comunicati sui cellulari della popolazione che annunciavano di allerte atomiche, chimiche e persino di combattimenti nelle strade della capitale. Lì però è scattata subito la reazione, rispondendo con la stessa arma: nel giro di tre ore è stato hackerato il sistema del ministero delle Emergenze di Mosca e sugli smartphone russi sono comparsi messaggi praticamente identici. È l'applicazione concreta della deterrenza: far comprendere che ogni aggressione provocherà una ritorsione di uguale forza, in modo da dissuadere dall'osare altre incursioni.

A Kiev sanno chi è il nemico. La guerra ibrida contro l'Europa invece avviene nell'ombra, cercando di nascondere la matrice dietro una coltre di nebbia: sono azioni studiate per non lasciare tracce che abbiano valore in un tribunale e alimentare il dubbio sulle responsabilità. Le celle frigorifere sono state spente da antagonisti che contestano la grande distribuzione o da criminali che poi chiederanno soldi per non ripetere le irruzioni? Oppure c'è una regia che coalizza i pirati informatici di differenti estrazioni mettendoli al servizio di uno Stato come i corsari di una volta?

Nel caso degli attacchi contro i depositi del freddo, prima di quelli avvenuti in Francia c'è stata una serie di hackeraggi contro soggetti che escludono la possibilità di estorsioni per denaro. Tra il 26 e il 27 agosto quattordici celle frigorifero dei supermarket interni di altrettante basi militari statunitensi hanno smesso di funzionare: c'era persino quello dell'aeroporto di Holloman nel New Mexico, il nido dei droni Reaper che vanno in missione in tutto il mondo. Sono tutti punti vendita gestiti dalle forze armate, lasciati senza un'adeguata protezione cyber. L'inchiesta del Pentagono è ancora in corso e gli investigatori Usa ora collaborano con i colleghi francesi nel sospetto di un unico disegno.

In quel momento la Casa Bianca non aveva ancora ripreso i rapporti con il Cremlino, anzi sembrava più ricettiva verso le istanze ucraine. A far ipotizzare una connessione tra questi arrembaggi digitali e Mosca c'è un altro precedente: l'estradizione e l'arresto nello scorso dicembre di una donna con cittadinanza ucraina accusata esplicitamente di agire per conto di due collettivi manovrati dall'intelligence russa. Sarà processata pure di avere sabotato i frigoriferi di un centro di macellazione. Tra le sigle per cui avrebbe lavorato c'è NoName057(16): quella che ha rivendicato "l'Operazione Mattarella" scagliata contro i computer del nostro Paese dopo le parole del presidente sull'invasione dell'Ucraina.

Al momento, non ci sono elementi per sostenere che ci sia un solo mandante: ogni apparato connesso a internet è vulnerabile e i guastatori del web si scambiano le informazioni, come fanno ad esempio i corsari dello zar e quelli degli ayatollah iraniani. Ma è indubbio che l'Europa sia oggi il campo di battaglia del nuovo modo di combattere la guerra, ibrida e soprattutto cyber, che rende indispensabile trovare forme di risposta all'altezza della minaccia.

©RIPRODUZIONE RISERVATA



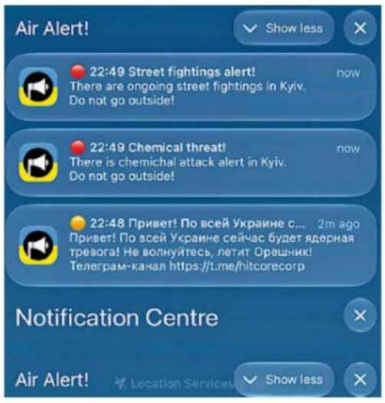
ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - DS6901 - S.30524 - L.1603_smart - T.1619

la Repubblica
Quotidiano - Dir. Resp.: Stefano Cappellini
Tiratura: 109075 Diffusione: 123028 Lettori: 1320000 (Data Stampa 0006901)

DATA STAMPA
45° Anniversario

IL CASO

E sui cellulari degli ucraini finti avvisi di combattimenti a Kiev





Le notifiche arrivate sui cellulari ucraini di falsi allarmi per attacchi chimici, atomici e che avvisavano di combattimenti per le strade di Kiev: un atto di guerra ibrida dalla Russia

ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - DS6901 - S.30524 - L.1603_smart - T.1619