

Guerra ibrida, il peggio deve ancora venire. E lâ??Europa non sa come rispondere

Descrizione

default watermark

(Adnkronos) â?? Quello che abbiamo visto finora della guerra ibrida contro lâ??Europa rischia di essere soltanto un assaggio. Attori ostili (russi, iraniani, cinesi, nordcoreani, piÃ¹ un mare di realtÃ non incasellabili) dispongono delle capacitÃ necessarie a mettere seriamente in crisi interi sistemi da cui dipende il funzionamento delle nostre societÃ : sanitÃ , trasporti, telecomunicazioni, energia, logistica. Parlando solo del fronte russo, gli attacchi che si sono moltiplicati negli ultimi anni suggeriscono che Mosca stia mettendo alla prova â?? in modo costante e progressivo â?? le linee rosse occidentali, verificando fin dove puÃ² spingersi senza provocare una risposta significativa.

Il problema Ã¨ che lâ??Europa continua a ragionare soprattutto in termini di resilienza. Proteggere le infrastrutture, prepararsi alle emergenze, ridurre i danni, continuare a funzionare anche sotto attacco. Tutto indispensabile, naturalmente. Ma insufficiente. Imparare a incassare meglio non significa convincere lâ??avversario a smettere di colpire.

Secondo un esperto di sicurezza con decenni di esperienza, sentito dallâ??Adnkronos, davanti agli attacchi di queste settimane occorrerebbe un cambio di mentalitÃ , prima ancora che di strategia. Smettere di considerare ogni possibile contromisura come un rischio di escalation e riconoscere che lâ??escalation Ã¨ giÃ in corso, anche se lâ??Europa non ha fatto granchÃ© per alimentarla. Una guerra puÃ² essere combattuta anche da una parte sola, se lâ??altra vuole far finta di non esserne coinvolta. Ma questo non la mette al riparo dalle conseguenze.

La questione Ã¨ passare dalla sola
deterrence by denial
, cioÃ¨ rendere gli attacchi meno efficaci, a una credibile
deterrence by punishment
: far capire allâ??avversario che determinate aggressioni comporteranno costi superiori ai benefici che si aspetta. Senza rinunciare alla prudenza, alla proporzionalitÃ e al rispetto del diritto, ma senza nemmeno trasformare il timore dellâ??escalation in un vincolo che finisce per paralizzare qualsiasi risposta.

E gli strumenti non mancano. Dalle sanzioni economiche al congelamento dei beni, dalle operazioni di controspionaggio per individuare e smantellare le reti russe e filorusse alle misure di military signalling. Fino alle capacitÃ cyber offensive e alle covert operations , operazioni sotto copertura, che appartengono tradizionalmente allâ??arsenale degli Stati, da esercitare entro i limiti previsti dal diritto.

Non si tratta di rispondere indiscriminatamente a ogni provocazione, ma di costruire una scala credibile di contromisure. Con un obiettivo molto concreto: modificare il calcolo costi-benefici di chi decide di attaccare lâ??Europa.

Il vero ostacolo, a sentire chi conosce bene la materia, Ã¨ la volontÃ politica di utilizzare questi strumenti. E convincere lâ??avversario di essere pronti a farlo.

Le vicende degli ultimi giorni aiutano a comprendere quanto siano vulnerabili le societÃ europee.

Una mail non costa nulla, spedirla a migliaia di scuole Ã¨ questione di pochi minuti. Le conseguenze, invece, possono essere pesanti: studenti evacuati, genitori costretti ad abbandonare il lavoro, artificieri e forze dellâ??ordine mobilitati, lezioni interrotte, strade bloccate, cittÃ in allarme.

default watermark

Il secondo giorno di questa ondata, nonostante lâ??invio di oltre 3.700 email, solo 77 istituti hanno fatto uscire gli studenti, e la metÃ ha ripreso le lezioni dopo i controlli delle forze dellâ??ordine. La mossa del governo, evitare lâ??evacuazione â??automaticaâ?•, ha sottratto agli autori delle minacce buona parte del risultato che cercavano di ottenere. Ma dimostra anche il limite di un approccio esclusivamente difensivo: il sistema ha imparato a gestire meglio lâ??emergenza, senza necessariamente ridurre la capacitÃ o la volontÃ di chi lâ??ha provocata di tentare nuovamente.

Nelle ultime settimane lâ??Europa ha sperimentato un campionario quasi surreale di attacchi e intimidazioni.

Falsi allarmi bomba hanno coinvolto decine di voli, alcuni dei quali diretti in Italia. Il 3 novembre due Eurofighter dellâ??Aeronautica Militare sono stati fatti decollare per scortare un aereo Ryanair proveniente da Dublino. Due giorni dopo, unâ??altra raffica di minacce.

Poi ci sono i frigoriferi. In Francia, un attacco informatico ha manipolato i sistemi di refrigerazione di circa 700 supermercati, facendo salire le temperature, deteriorando gli alimenti e provocando, in alcuni casi, principi dâ??incendio, e colpendo anche i macchinari che conservano il sangue negli ospedali. Simili attacchi si sono verificati in diversi Paesi europei, eppure lâ??Italia Ã¨ stata colpita solo marginalmente. Sia perchÃ© gli impianti erano piÃ¹ protetti, sia per unâ??attivitÃ preventiva dellâ??Agenzia per la Cybersicurezza Nazionale, che giÃ il 13 ottobre aveva diramato unâ??allerta tecnica agli operatori del settore. Il direttore generale Andrea Quacivi ha confermato al Tg1 che lâ??Agenzia aveva provveduto a informare gli operatori.

La Francia ha attribuito gli attacchi di ottobre a unâ??unitÃ cyber dei Guardiani della Rivoluzione iraniani, mentre per quelli successivi le responsabilitÃ non sono state ancora accertate. Quanto alle email che hanno terrorizzato scuole e aeroporti, non esistono finora prove pubbliche sufficienti per ricondurle alla Russia. Le firme, spesso grottesche, e i riferimenti a organizzazioni russe o islamiste non dimostrano nulla. E non si puÃ² escludere che alla strategia di destabilizzazione si aggiungano mitomani ed emulatori.

Non tutto ha la stessa regia. PerÃ² Ã¨ chiaro che soggetti diversi hanno scoperto la stessa vulnerabilitÃ : le societÃ europee sono straordinariamente complesse, interconnesse e quindi esposte a perturbazioni anche minime.

E se oggi Ã¨ possibile ottenere questi risultati con mezzi relativamente semplici, Ã¨ legittimo domandarsi quali sarebbero le conseguenze di operazioni piÃ¹ sofisticate, coordinate e intenzionalmente distruttive.

Su un piano piÃ¹ ampio, il quadro Ã¨ ambiguo solo per chi non vuole vedere. Da anni la Russia conduce una campagna di sabotaggi, interferenze, cyberattacchi e operazioni clandestine contro i Paesi europei. Non Ã¨ una ricostruzione affidata a qualche analista particolarmente allarmista: Ã¨ la valutazione ufficiale dellâ??Unione europea.

Un rapporto dellâ??International Institute for Strategic Studies, pubblicato nellâ??agosto 2025, ha ricostruito la crescita delle operazioni di sabotaggio russe contro le infrastrutture europee dal 2022. Con un problema ricorrente: la difficoltÃ degli Stati occidentali di coordinare risposte capaci di scoraggiare nuove aggressioni.

default watermark

Ã? un conflitto che si svolge sotto la soglia della guerra convenzionale per logorare una societÃ : consumarne risorse, attenzione, fiducia. Per costringere le istituzioni a rincorrere continuamente emergenze piccole e grandi, ciascuna apparentemente insufficiente a giustificare una reazione significativa.

Câ??Ã¨ anche un equivoco culturale da superare. In Europa siamo abituati a pensare che una guerra cominci con una dichiarazione ufficiale, o almeno quando si sganciano le prime bombe. Ma il fatto che una parte non si consideri in guerra non impedisce allâ??altra di condurre operazioni ostili.

E câ??Ã¨ il rischio di un secondo errore: attribuire allâ??avversario le nostre stesse categorie. Supporre, per esempio, che Mosca condivida la nostra riluttanza allâ??escalation o che interpreti la prudenza europea come un segnale di moderazione da ricambiare. Non Ã¨ per forza cosÃ¬. Una risposta sistematicamente debole puÃ² essere letta come un invito a spingersi un poâ?? piÃ¹ avanti.

Ã? un problema che una parte della comunitÃ strategica internazionale sta affrontando con crescente preoccupazione.

In unâ??analisi pubblicata dallâ??European Policy Centre, Juraj Majcin e Jannik Hartmann sostengono che lâ??Europa debba rafforzare la deterrenza attraverso lâ??imposizione di costi alla Russia. Una strategia concentrata quasi esclusivamente sulla capacitÃ di assorbire gli attacchi rischia di lasciare a Mosca la possibilitÃ di procedere per piccoli passi, accumulando vantaggi senza mai oltrepassare una soglia che provocherebbe una risposta decisiva.

E in effetti la deterrenza europea, fondata perlopiÃ¹ su resilienza e strumenti normativi, non Ã¨ bastata a contenere le operazioni ibride russe.

Anche il problema dellâ??attribuzione, spesso invocato come ostacolo insuperabile, Ã¨ reale ma non assoluto. Prima della Francia con gli iraniani, câ??Ã¨ stata la Germania, che ha accusato la Russia (uno dei presunti esecutori era in possesso di visto turistico italianoâ?¦) di aver piazzato droni esplosivi allâ??aeroporto di Lipsia nel punto in cui partivano aerei cargo destinati allâ??Ucraina.

La necessitÃ di prove solide resta fondamentale. Sbagliare bersaglio, o adottare contromisure sproporzionate, significherebbe indebolire la credibilitÃ della stessa deterrenza.

La questione in Italia non Ã¨ nuova. Il 17 novembre 2025 Guido Crosetto ha presentato al Consiglio supremo di difesa un documento intitolato â??Il contrasto alla guerra ibrida: una strategia attivaâ?•. Tra le proposte figuravano la definizione di uno spazio cyber di interesse nazionale, la creazione di unâ??arma cyber civile e militare e di una riserva di specialisti, oltre a strutture di coordinamento dedicate al contrasto delle minacce ibride.

A un anno di distanza, gli allarmi bomba nelle scuole hanno dimostrato quanto sia ancora complicato tradurre la consapevolezza strategica in procedure operative uniformi. Le misure decise da Palazzo Chigi hanno corretto rapidamente la risposta iniziale, ma il problema piÃ¹ vasto resta aperto.

Anche a Bruxelles gli strumenti non mancano. Lâ??Unione europea ha giÃ introdotto un regime sanzionatorio specifico per le attivitÃ ibride russe e, nella propria strategia, prevede espressamente sia la deterrenza attraverso la resilienza sia quella fondata sullâ??imposizione di costi. Non Ã¨ che lâ??Europa non abbia pensato a una risposta. Eppure, nonostante questi strumenti, le operazioni ostili continuano. Ed Ã¨ legittimo chiedersi se la capacitÃ europea di dissuadere lâ??avversario sia allâ??altezza della minaccia.

default watermark

Il passaggio che manca non Ã¨ soltanto giuridico o tecnologico. Ã? politico e strategico: decidere quali comportamenti non possono essere tollerati, quali conseguenze devono produrre e chi Ã¨ disposto ad assumersi la responsabilitÃ di applicarle.

Câ??Ã¨ infine un aspetto che rende questa stagione particolarmente pericolosa. Quando gli attacchi diventano abituali, si rischia di normalizzarli. Ci si abitua alle email minatorie, ai voli deviati, ai servizi interrotti. Si impara a conviverci. Ã? esattamente il terreno su cui la guerra ibrida puÃ² prosperare: una successione di episodi che sembrano sopportabili se osservati singolarmente, ma che nel loro insieme consumano la capacitÃ di reazione di un Paese.

Con un rischio ulteriore. Quello che oggi Ã¨ un falso allarme potrebbe domani diventare un sabotaggio vero, magari contro unâ??infrastruttura dalla quale dipendono migliaia di persone. E non Ã¨ detto che le contromisure preparate per il primo siano sufficienti ad affrontare il secondo. Lâ??Europa non puÃ² permettersi di attendere che qualcosa di molto piÃ¹ grave accada per prendere atto della natura della minaccia. Deve certamente diventare piÃ¹ resiliente, ma anche piÃ¹ capace di deterrenza. PerchÃ© un avversario che non teme conseguenze puÃ² essere incoraggiato a colpire ancora, e piÃ¹ duramente.

Le scuole italiane hanno dimostrato che Ã¨ possibile imparare a non farsi paralizzare da una mail. Ã? un progresso importante. Ma la deterrenza comincia un passo piÃ¹ avanti: quando chi sta dallâ??altra parte del computer deve preoccuparsi delle conseguenze.

â??

politica

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione
Novembre 13, 2026
Autore
redazione

default watermark