Il caos nella quotidianità è la nuova arma strategica

Luca Longo

Un frigorifero industriale impostato a una temperatura anomala può compromettere tonnellate di alimenti. Un falso allarme bomba può bloccare un aeroporto, evacuare una scuola e impegnare forze di sicurezza. Non si tratta di guerra convenzionale, ma di come un attacco relativamente semplice può produrre conseguenze estese su servizi essenziali e attività economiche. Gli episodi registrati nelle ultime settimane nei supermercati europei e nel traffico aereo mostrano una vulnerabilità sempre più evidente: la possibilità di colpire un Paese attraverso il funzionamento della sua vita quotidiana. Il campo di battaglia ora scavalca le frontiere e attraversa reti informatiche, aeroporti, centri logistici, sistemi di distribuzione alimentare, infrastrutture sanitarie e scolastiche. La dimensione digitale si sovrappone a quella fisica, economica e sociale, rendendo sempre più difficile distinguere tra sicurezza militare e sicurezza civile.

La novità consiste nella possibilità di ottenere risultati strategici senza impiegare arsenali o distruggere obiettivi. Non è necessario colpire fisicamente un supermercato: può bastare alterarne la catena del freddo. Una scuola può essere bloccata per un'intera giornata da una falsa segnalazione. Un aereo può essere fermato sulla pista o dirottato verso un altro aeroporto. Lo stesso principio si osserva nello Stretto di Hormuz, dove anche la sola minaccia della presenza di mine può scoraggiare il traffico marittimo e produrre conseguenze economiche. È una strategia caratterizzata da una forte asimmetria dei costi: l'attaccante impiega risorse limitate, a volte basta una ben fatta e-mail minacciosa, mentre il bersaglio deve mobilitare personale, tecnologie e apparati di sicurezza per ripristinare la normalità. Un'intrusione informatica può richiedere pochi mezzi, ma le sue conseguenze possono coinvolgere imprese, amministrazioni, forze di polizia e protezione civile. Il vantaggio consiste nel trasferire sull'avversario il costo della gestione dell'emergenza: può essere sufficiente rendere più difficile garantire i servizi, amministrare le risorse e mantenere la fiducia dei cittadini. Queste operazioni acquistano maggiore efficacia quando si inseriscono in società già in tensione. Inflazione, caro energia, difficoltà negli approvvigionamenti e riduzione del potere d'acquisto possono amplificare gli effetti di un'interruzione dei servizi essenziali. Un problema circoscritto alla distribuzione alimentare o ai trasporti diventa così un ulteriore fattore di instabilità.

Alla dimensione materiale si aggiunge quella informativa. Notizie false, allarmi non verificati e campagne di manipolazione possono amplificare la percezione del pericolo e trasformare un episodio isolato in una generalizzata crisi di fiducia. Il sabotaggio produce il danno, la disinformazione ne estende le conseguenze e il disagio sociale può diventare il risultato politico. Per queste attività possono essere utilizzati gruppi informatici, intermediari e soggetti non direttamente riconducibili a uno Stato. Il ricorso a questi proxy rende più difficile individuare i responsabili e dimostrare eventuali collegamenti con attori governativi. È tuttavia necessario distinguere le ipotesi strategiche dalle responsabilità accertate: la somiglianza tra gli episodi non dimostra automaticamente l'esistenza di una regia comune. Il nemico può non essere sempre e solo l'odiato (ma apparentemente onnipotente) Putin.

La vulnerabilità raggiunge anche le abitazioni. I dispositivi domestici connessi, compresi i frigoriferi smart, possono diventare punti d'accesso alle reti private. Tra la fine del 2013 e l'inizio del 2014, oltre 100.000 dispositivi compromessi inviarono più di 750.000 e-mail malevole. Password robuste e differenti, aggiornamenti del software, reti separate per gli elettrodomestici e disattivazione degli accessi remoti non necessari sono alcune delle principali misure di protezione.

La risposta non può limitarsi alla difesa informatica tradizionale: occorre progettare infrastrutture capaci di continuare a funzionare anche quando una parte dei sistemi viene compromessa. Le architetture Zero Trust, che verificano continuamente identità e autorizzazioni, rappresentano uno strumento importante, così come la presenza di sistemi ridondanti e procedure analogiche di emergenza. Altrettanto decisivo è il controllo delle catene di fornitura tecnologiche e dei servizi affidati a operatori esterni. La sicurezza di un'infrastruttura strategica non può dipendere esclusivamente dalle logiche commerciali o dalla protezione dei singoli fornitori.

Esiste infine un rischio politico. Se l'obiettivo dell'aggressore è indebolire le democrazie, una risposta basata su restrizioni permanenti, sorveglianza indiscriminata e limitazioni delle libertà potrebbe contribuire proprio a ottenere il risultato desiderato. La deterrenza deve quindi comprendere non soltanto la capacità di prevenire e contrastare gli attacchi, ma anche quella di assorbirne gli effetti senza compromettere il funzionamento della società. La coesione sociale, la continuità degli approvvigionamenti e la fiducia nelle istituzioni sono ormai elementi della sicurezza nazionale. Nella nuova dimensione del conflitto, proteggere un Paese significa anche impedire che un frigorifero, un aeroporto, una scuola o una rete logistica diventino strumenti per destabilizzarlo. Il bersaglio è non solo l'infrastruttura, ma anche la normalità che essa garantisce.

Sì, anche l'Italia è in guerra tra hacker e filoputiniani



Mauro Del Bue

Inutile nascondercelo perché ci faremmo male, molto male, da soli. Anche noi, in Italia, siamo in guerra. Non si tratta della guerra tradizionale che per essere estrema dovrebbe essere atomica. E Dio ci ha regalato l'atomica come strumento di inibizione della guerra armata. Non ci attaccheranno con l'atomica e forse neanche coi missili e le bombe e i droni. Ma ormai di un nuovo genere di guerra tutti i Paesi europei, e anche gli stessi Stati Uniti, sono consapevoli e si stanno attrezzando. Si tratta di una guerra informatica che può bloccare, è successo a noi, il congelamento degli alimenti nei supermercati o deviare il regolare corso dei voli aerei. Dietro questi attacchi, secondo il ministro degli Esteri italiano, c'è la Russia; secondo quello francese, c'è l'Iran. Poco cambia, dal momento che Mosca e Teheran sono alleati.

Dal Regno Unito alla Svezia, dalla Francia agli Stati Uniti, si moltiplicano i manuali distribuiti alla popolazione per affrontare blackout, sabotaggi e interruzioni dei servizi essenziali (anche in caso di calamità e persino di guerra). Scorte di acqua e cibo, radio, contanti e medicinali: le istruzioni dei governi ai cittadini per prepararsi alle emergenze. Il ministro Crosetto non ci ha ancora riferito il piano italiano, e il suo finanziamento, da portare in Parlamento. Mi auguro che anche le forze di opposizione convergano sulla necessità di affrontare questa delicata emergenza. E non recitino la tiritera del "mettiamo i miliardi della Difesa su scuola a sanità". Ritornello che non si può sentire, visto che un trasferimento simile non può neanche avvenire essendo le spese per la Difesa fuori dal Patto di Stabilità.

Intanto vengono diffusi dallo Stato russo i dati sui decessi di soldati al fronte: sarebbero 450mila, che sommati ai 150mila ucraini fanno 600mila. E in Italia il numero non sconcerta. Non si alzano bandiere e barricate contro gli aggressori, e si parla genericamente di pace. Di pace con chi aggredisce. Di pace con chi si difende. Di pace con gli opposti guerrafondai. Non si può accettare. Il governo Draghi approvò quattro pacchetti di aiuti militari alla resistenza ucraina, il primo del 2026 del governo Meloni è contestato dalla Lega, mentre Vannacci, che a Mosca ha svolto l'incarico di addetto militare presso l'ambasciata italiana, e non nasconde simpatie putiniane, rifiutando di votare qualsiasi aiuto militare a Kyiv, è stato definito da Calenda "un traditore della patria", e Conte, che si trova sulle sue identiche posizioni, come Fratoianni, è stato citato come "un vile" nel corso del convegno di Bologna. La guerra informatica che si regge su informazioni e posizioni deformate e utili alla Russia può servirsi di interpreti dei campi politici opposti. Utili idioti che, coscientemente o no, fanno il gioco del nemico dell'Italia. Da destra e da sinistra. Iniziative per orientare elezioni politiche, come quelle in Georgia e in Romania, sono all'ordine del giorno. E mentre in Israele Eisenkot vacilla tra un'alleanza con i partiti arabi e una con gli ortodossi, Netanyahu lancia la sfida dell'unità nazionale.

Resta massima la tensione in tutti i Paesi che aiutano la resistenza ucraina e oggetto di attacchi mirati e sempre più pericolosi, mentre sull'Iran - con la sconfitta di Trump e l'avvento di un nuovo governo israeliano - soffiano venti di pace. O almeno di negoziato. Un tassello di speranza in un mosaico cupo.

Un Indice di invisibilità per inaugurare una politica del capitale umano tra università, imprese e mobilità sociale

Misurerebbe il tempo tra il momento in cui una persona ha qualcosa da dare e quello in cui qualcuno se ne accorge

Valentina Boddi

Sappiamo contare i cervelli che partono. Molto meno quelli che abbiamo davanti e non riusciamo a vedere. C'è una statistica che ancora non esiste. Potremmo chiamarla Indice di invisibilità. Non misurerebbe quanti giovani lasciano l'Italia: quelli, prima o poi, riusciamo a contarli. Né quanti laureati le imprese cercano senza trovarli o quanti finiscono in lavori lontani dalla propria formazione. Misurerebbe qualcosa che accade prima: il tempo che passa tra il momento in cui una persona ha qualcosa da dare e quello in cui qualcuno se ne accorge. Forse scopriremmo che l'Italia non ha soltanto un problema di fuga dei cervelli. Ha un problema di vista.

I numeri, messi uno accanto all'altro, producono un piccolo cortocircuito. Secondo il Rapporto CNEL 2025 sull'attrattività dell'Italia per i giovani, il capitale umano associato agli italiani espatriati tra il 2011 e il 2024 vale 159,5 miliardi di euro. Non PIL perduto né tasse volatilizzate: investimento incorporato nelle persone, fatto di scuola, università, formazione e competenze. Capitale costruito qui che mette altrove una parte della propria vita produttiva. Contemporaneamente, secondo Unioncamere-Excelsior, nel 2025 le imprese italiane prevedevano circa 670mila contratti destinati a laureati e, nel 50,9% dei casi, dichiaravano difficoltà nel reperirli. Per l'area ingegneristica, la domanda programmata era nell'ordine di 127mila persone. Formiamo persone. Le perdiamo. Poi diciamo di non trovarle.

C'è anche chi rimane, ma non necessariamente nel posto giusto. AlmaLaurea rileva che, tra i laureati di secondo livello, il mismatch tra studi e lavoro riguarda il 31,9% a un anno dalla laurea e resta al 25,4% dopo cinque. Sono fenomeni diversi, e sarebbe scorretto sommarli come se dimostrassero un'unica causa. Ma la domanda viene quasi da sola: e se il problema non fosse soltanto quanto talento produciamo o perdiamo, ma quanto siamo capaci di riconoscerlo, collegarlo, utilizzarlo? L'invisibilità, oltretutto, comincia molto prima della valigia per Londra o Berlino. In Basilicata, nell'anno accademico 2023-24, studiava fuori Regione l'85,6% degli immatricolati residenti nella provincia di Matera e il 68,3% di quelli di Potenza. E la possibilità di muoversi non è socialmente neutrale: tra i laureati meridionali, la mobilità universitaria verso il Centro-Nord riguardava il 34,3% di chi proveniva dai contesti familiari più favoriti, contro il 23% dei meno favoriti.

Prima di domandarci perché un talento se ne vada, dovremmo allora chiederci chi può permettersi di raggiungere il luogo nel quale quel talento verrà visto. C'è chi parte perché può, chi perché deve. Chi resta perché sceglie di farlo e chi semplicemente rimane fuori dal radar. Conosco, per ragioni familiari, uno di questi casi. Mio fratello Marco, ingegnere e ricercatore, nel 2023 partecipò a un lavoro scientifico premiato con uno Young Scientist Best Paper Award in ambito NATO. Fece una cosa piuttosto eccentrica nell'economia contemporanea dell'attenzione: praticamente non lo disse a nessuno. In famiglia lo scoprimmo molto dopo. Il caso, naturalmente, non dimostra nulla. Vale uno. Ma suggerisce una domanda che i numeri non riescono ancora a contenere: quante persone stanno facendo qualcosa di difficile, utile o semplicemente molto bene mentre nessuno le guarda?

Siamo diventati bravissimi a misurare ciò che è già visibile: ranking, citazioni, retribuzioni, migrazioni, engagement, follower. Molto meno ciò che accade prima: il talento silenzioso, la competenza fuori posto, la ricerca senza riflettori, la persona perfetta per quel posto che un'impresa dichiara di non riuscire a coprire. L'Indice di invisibilità dovrebbe misurare questa distanza. Non quella tra successo e insuccesso, ma quella tra valore e riconoscimento. Perché una parte della cosiddetta fuga dei cervelli potrebbe iniziare ben prima dell'aeroporto: quando qualcuno capisce che, per essere visto, deve cambiare città, rete, lingua. Qualche volta Paese. È lì che dovrebbe cominciare una politica del capitale umano: università capaci di attrarre, ricerca finanziata, imprese capaci di cercare davvero, mobilità sociale, collegamenti fra competenze e territori. E qualcosa di molto più difficile da inserire in una Legge di Bilancio: la curiosità per ciò che ancora non fa rumore. Perché forse i segnali ci sono già. Il rumore lo misuriamo benissimo. È il segnale che, qualche volta, ci sfugge.