

BENVENUTI NELL'ERA DELLA PACE IBRIDA

Posted on 10 November 2026 by Danilo Breschi

Category: Pensare il pluriverso

Sin dai tempi antichi, oltre alla guerra intesa come scontro frontale in campo aperto, il conflitto ha conosciuto modalità parallele e alternative. Più di duemila anni fa il filosofo cinese Sun Tzu teorizzava che il massimo dell'abilità militare consiste nel piegare la resistenza del nemico senza nemmeno combattere: usa l'inganno, la propaganda e il sabotaggio. Non troppo dissimile il giudizio dello storico greco Tucidide, il quale descriveva come la destabilizzazione psicologica delle fazioni interne e l'uso di infiltrati potessero distruggere la coesione di una città molto più di una sconfitta in battaglia. Carl von Clausewitz, com'è noto, ci ha insegnato che la guerra è la continuazione della politica con altri mezzi. Se oggi la politica e l'economia globali si muovono sui flussi digitali, la guerra si sposta inevitabilmente su quelle stesse reti.

Con lo sviluppo delle moderne forme ibride di ostilità, noi cittadini europei dobbiamo abituarci a un fatto spietato: la guerra sta tornando prepotentemente in scena nella nostra vita quotidiana, sotto spoglie completamente diverse rispetto a quelle classiche. Dovremo cambiare radicalmente modo di pensare e di vivere?

Quella stabilità, quasi idilliaca, che l'Europa occidentale ha sperimentato dal secondo dopoguerra a oggi è di certo tramontata. Forse non ce ne siamo ancora resi conto. Almeno non a livello di consapevolezza collettiva. In parte è normale e comprensibile. Il passaggio è epocale. Siamo entrati in una nuova era, in cui la pace non è assenza di conflitto ma una sorta di tregua apparente,

intrisa di una conflittualità latente, sempre presente. È la dimensione della *grey zone*, quel limbo in cui la routine della vita quotidiana si trova costretta a convivere con un'ostilità potenziale sempre sul punto di colpire. Una vera e propria spada di Damocle che ogni tanto punzecchia, facendo più o meno male a seconda dell'occasione e dei malcapitati di turno. Nel momento in cui lo scontro geopolitico sceglie come bersaglio le reti digitali, le centrali energetiche e la logistica, la linea del fronte si sposta dentro la nostra stessa quotidianità. Se ti alzi la mattina, vai a prendere la metro e improvvisamente c'è un blackout dentro la galleria più buia, la tua percezione del pericolo cambia. Se rimani bloccato dentro l'ascensore di un grattacielo per un attacco informatico, o se i voli aerei vengono cancellati mentre sei in viaggio per andare in vacanza a causa di un allarme-drone, e tutto questo diventa routine, beh!, la tua forma *mentis* muta radicalmente.

I dati dell'ultima settimana: ben 35 segnalazioni coordinate di bomba hanno paralizzato e dirottato voli commerciali in tutta Europa, mentre una raffica di attacchi hacker ha colpito i sistemi di refrigerazione dei supermercati in Italia, Svezia, Belgio e Regno Unito, arrivando persino a minacciare le strutture di stoccaggio del sangue del servizio sanitario nazionale francese. Quando i termostati dei frigoriferi industriali vengono manipolati da remoto a 50 gradi, o quando si colpisce l'infrastruttura del cantiere del Tunnel di base del Brennero, la minaccia da virtuale si fa molto, ma molto concreta. Ci tocca e fa male.

L'incertezza cessa di essere una notizia lontana che ascolti distratto al telegiornale. Diventa una condizione psicologica con cui convivere ogni giorno. Questa strategia asimmetrica si basa sul principio della smentita plausibile, la cosiddetta *plausible deniability*: chi colpisce lo fa in modo invisibile, potendo sempre negare il proprio coinvolgimento diretto. Come emerge dalle ultime indagini investigative dell'Europol, i servizi di sicurezza russi, dopo essere stati scoperti per gli hackeraggi di unità militari ufficiali come Sandworm o Fancy Bear, utilizzano sempre più gruppi esterni in outsourcing e sigle

informali del dark web come NoName057 o Everest per condurre una massiccia info-war. È una strategia opportunistica, esasperata dall'uso dei modelli di frontiera dell'intelligenza artificiale, che gli esperti descrivono come un vero e proprio "momento Wuhan" per internet. L'intelligenza artificiale consente a gruppi criminali, autonomi o prezzolati da governi stranieri, di scovare le falle dei sistemi civili e di diffondere il caos a velocità mai viste prima. La guerra si fa interamente psicologica, vuole far saltare i nervi, letteralmente. Si tratta di uno scenario inquietante, che può essere approfondito grazie al recente studio di Gastone Breccia (*L'età della pace ibrida. Le democrazie alla prova*, Scholé, Brescia 2026).

Fino a oggi abbiamo vissuto in una comfort zone nell'idea che la sicurezza potesse essere delegata a pochi professionisti. In parte continuerà a essere così, anche se il concetto di difesa è destinato a estendersi parecchio così come il numero degli addetti a questo settore. Non solo: il cittadino qualunque dovrà acquisire maggiori informazioni e conoscenze in tema di sicurezza, personale e collettiva. Educazione allo spirito critico, di questo avremo sempre più bisogno, per saper scindere il necessario dal superfluo, il falso dal vero. Fatica improba, ma ineludibile. Se è la pace dei vivi e non dei cimiteri quanto davvero si pretende, allora ciascuno dovrà rendersi in qualche modo partecipe, vigile e responsabile. Delegare tutto è sinonimo di servitù.

Il virus più pericoloso dell'era della pace ibrida è il senso di completa vulnerabilità che rischia di contagiare la classe media, già resa inquieta da altri problemi. I governi di mezza Europa, d'altronde, non fanno niente per nasconderlo, tanto da consigliare ormai apertamente ai cittadini di fare scorte alimentari d'emergenza e tenere contanti in casa per far fronte a possibili blackout logistici. Alcuni diranno sia ingiustificato allarmismo. Secondo altri è il riconoscimento del fatto che nella nostra società iper-interconnessa basta un difetto di codice in un dispositivo periferico non protetto per mandare in tilt un'intera rete nazionale.

Le democrazie pluraliste sono strutturalmente fragili di fronte a queste

infiltrazioni. La trasparenza e la libertà di espressione, che sono i nostri valori più preziosi, vengono sistematicamente usate dagli avversari come varchi per diffondere disinformazione e disordine. Negare l'esistenza di questa minaccia strisciante è da ingenui, se non da complici, perché significa fare il gioco di un aggressore invisibile ma non per questo meno reale, e meno pericoloso. Sfruttando le nuove tecnologie cyber, il terrorismo postmoderno può seminare il panico e logorare la fiducia nelle istituzioni senza bisogno di sparare un colpo. Non per questo il suo impatto è inferiore. Tutt'altro.

Per questo motivo la crescente domanda di protezione e autodeterminazione che sale dalle nostre società non può più limitarsi alla sola difesa del potere d'acquisto. La cyber-sicurezza è il nostro presente e il nostro futuro. Di fronte a questo nuovo tipo di minacce lo Stato non può mostrarsi impotente. La protezione della base infrastrutturale della società e dei legami comunitari è ormai tutt'uno con la difesa nazionale dei nostri confini e del nostro vivere libero. La stessa cittadinanza, come detto, deve prendere atto della nuova situazione, mostrandosene all'altezza. Non sarà affatto facile, ma occorre dotarsi di una mentalità pronta a gestire l'emergenza, senza per questo modificare troppo abitudini proprie di una società aperta e dinamica. In una parola, libera.

Proprio per questo occorrerà, al contempo, guardarsi sempre da quel Leviatano che l'età della pace ibrida rischia di scatenare, liberando oltremisura l'autorità statale da quei limiti che la tradizione del costituzionalismo liberale e democratico ha faticosamente posto perché il monopolio dell'uso legittimo della forza non diventi alibi per abusi e soprusi del pubblico ai danni del privato. La sfida che attende la cittadinanza europea sta tutta qua, nel custodire con cura e intelligenza il delicato equilibrio tra libertà e sicurezza.