STRATEGIA E INFRASTRUTTURE

Colpire i nervi del sistema

Cyberattacchi, falsi allarmi e strategia della disorganizzazione da Liddell Hart a John Boyd

7 novembre 2026

> *«C'è una guerra là fuori, amico mio. Una guerra mondiale. E non ha la minima importanza chi ha più pallottole, ha importanza chi controlla le informazioni. Ciò che si vede, si sente, come lavoriamo, cosa pensiamo, si basa tutto sull'informazione!»*
>
> Cosmo, *I signori della truffa* (*Sneakers*, 1992).[1]

La battuta porta in primo piano il rapporto fra informazione e condotta, dal quale dipende una parte crescente del funzionamento delle società contemporanee: un'apparecchiatura industriale modifica il proprio comportamento sulla base delle istruzioni ricevute, mentre chi è responsabile della sicurezza deve interpretare le segnalazioni che gli pervengono prima di decidere come intervenire. Poiché, in entrambi i casi, l'azione prende avvio da un segnale che la procedura è tenuta a considerare — come comando autorizzato oppure come rischio da accertare —, chi riesca ad alterarne il contenuto o a falsificarne la provenienza può provocare conseguenze che travalicano il proprio intervento iniziale, sfruttando attività già predisposte per garantire un servizio; quanto più numerose sono le apparecchiature e le persone chiamate a cooperare nell'eseguirle, tanto più ampio può diventare l'impiego di risorse sulle quali l'autore della perturbazione non esercita alcun controllo diretto.

Questa dipendenza emerge con particolare chiarezza negli episodi europei dell'autunno 2026, che coinvolsero due attività apparentemente lontane. A partire dall'11 ottobre, le autorità francesi documentarono compromissioni dei controllori remoti impiegati nella refrigerazione commerciale, alle quali seguì, fra il 1º e il 2 novembre, una nuova ondata di incidenti segnalata dalla Commissione europea e da ENISA; il 5 novembre, invece, una minaccia di bomba costrinse un volo diretto da Dublino a Roma a deviare verso la base francese di Évreux, mentre a Madrid altri avvertimenti, giunti a breve distanza, determinarono accertamenti su più aeromobili, senza che le ricerche riferite da Reuters portassero al ritrovamento degli ordigni annunciati. [5–7] Benché nel primo gruppo di episodi si sia intervenuti sui comandi di apparecchiature industriali e nel secondo sia stata sollecitata la valutazione di un pericolo da parte delle autorità responsabili, il confronto diventa possibile seguendo il lavoro imposto ai destinatari: l'impianto deve essere controllato e riportato a condizioni sicure, l'allarme deve essere verificato prima che il volo riprenda il proprio corso, e in entrambi i casi una parte delle risorse disponibili viene distolta dalla funzione cui era originariamente destinata. Da tale sottrazione discende il problema della *libertà d'azione*, che Basil Henry Liddell Hart collocò al centro dell'approccio indiretto; qualora le perturbazioni si succedano abbastanza rapidamente da ostacolare la verifica dei fatti e il coordinamento delle risposte, la stessa questione investe l'*orientamento* e la coesione delle organizzazioni, sui quali John Boyd avrebbe fondato la propria teoria del conflitto. [2, pp. 326–328] [4, capp. 5–7]

Quando un'istruzione raggiunge il mondo fisico

Per comprendere come una modifica informatica possa trasformarsi in una perdita di merci occorre considerare il funzionamento ordinario di un impianto frigorifero, nel quale la temperatura, soggetta a variare ogni volta che si aprono le porte, entrano prodotti o si modifica lo scambio di calore con l'ambiente, viene misurata da un sensore e confrontata da un controllore con un valore prestabilito, detto *setpoint*; sulla base di questo confronto, il controllore impartisce agli attuatori le istruzioni necessarie, mentre le misure successive gli consentono di stabilire se occorrano ulteriori correzioni. Il circuito, che prende il nome di *retroazione* o *feedback*, costituisce uno dei meccanismi fondamentali della *tecnologia operativa* (OT), categoria nella quale il NIST riunisce i sistemi informatici che sorvegliano o modificano direttamente i processi fisici. [9, § 2.3, pp. 10–11] [10] Se, attraverso un accesso abusivo, viene cambiato il valore verso il quale l'impianto deve tendere, la macchina può eseguire correttamente una sequenza di comandi che, essendo stata alterata la premessa, produce un risultato dannoso: ciò accade, per esempio, quando la funzione di sbrinamento, necessaria a eliminare il ghiaccio che ostacola lo scambio termico, viene programmata in modo da provocare riscaldamenti eccessivi o prolungati, eventualità richiamata nell'avviso congiunto delle autorità statunitensi sui sistemi di refrigerazione. [8, p. 1]

L'alterazione dei parametri, peraltro, costituisce soltanto uno dei punti sui quali si può intervenire, giacché per governare efficacemente il processo l'operatore deve anche disporre di misure attendibili: quando la temperatura anomala viene segnalata, il personale può accertare la causa e correggere il funzionamento, mentre una rappresentazione manipolata delle condizioni reali rischia di indurre una diagnosi falsa, ritardando l'intervento proprio quando sarebbe necessario. È utile, perciò, distinguere la modifica dei parametri operativi dalla manipolazione delle informazioni mostrate al gestore, due tecniche descritte separatamente da MITRE per i sistemi industriali. [11, 12] La prima incide sulle istruzioni eseguite dall'apparecchiatura, la seconda sulla conoscenza che l'operatore ha del suo comportamento; qualora si combinino, un impianto può deviare dalle condizioni prescritte mentre chi dovrebbe sorvegliarlo continua a ricevere dati rassicuranti. In entrambi i casi, l'effetto dipende dal posto che il dispositivo occupa in una catena di decisioni già predisposta per amministrare il mondo materiale: di qui la necessità di comprendere attraverso quali accessi un soggetto estraneo possa raggiungere il controllore o le informazioni da esso prodotte.

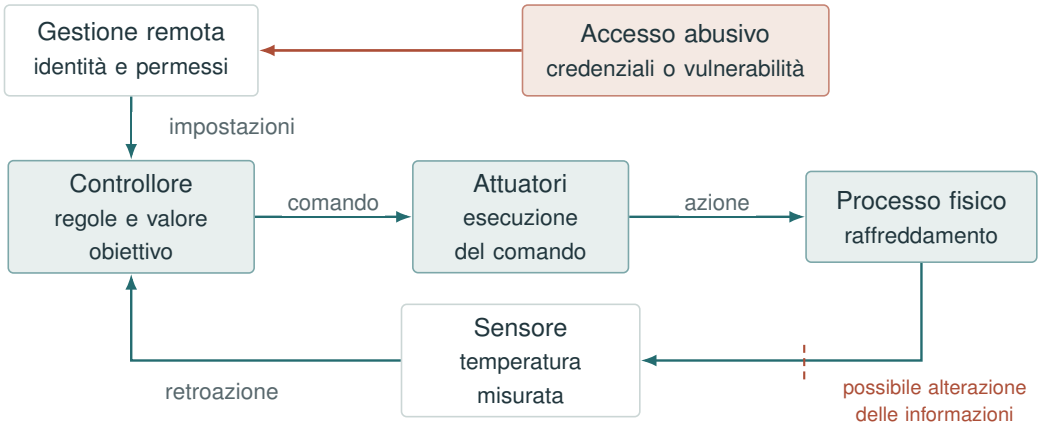


Figura 1. La misura torna al controllore, che stabilisce come intervenire. L'accesso abusivo ai parametri e la manipolazione delle informazioni destinate all'operatore riguardano due punti distinti del circuito di regolazione. [9, 11, 12]

Poiché la manutenzione di molti impianti distribuiti fra punti vendita diversi avviene a

distanza, un tecnico può raggiungere un'interfaccia di amministrazione senza recarsi fisicamente presso il frigorifero; perché tale comodità rimanga sicura, il sistema deve anzitutto riconoscere chi sta entrando, attraverso l'*autenticazione*, e quindi limitare le operazioni consentitegli, attraverso l'*autorizzazione*. Quando una password valida viene sottratta o quando rimangono utilizzabili credenziali predefinite e deboli, chi le possiede può ricevere dal sistema gli stessi privilegi attribuiti all'amministratore, sicché comandi perfettamente ordinari, come la modifica di una soglia o di un ciclo di funzionamento, possono essere impartiti per scopi estranei alla conservazione delle merci; MITRE documenta questa modalità d'accesso sotto la categoria degli *account validi*. [13] Una via diversa si apre qualora un'applicazione raggiungibile dalla rete presenti un difetto sfruttabile: in tal caso, l'*exploit*, ossia il procedimento che utilizza una *vulnerabilità* del programma, può consentire di oltrepassare una protezione senza conoscere la password, secondo una tecnica anch'essa registrata da MITRE per gli ambienti industriali. [14] L'allerta francese relativa alla refrigerazione richiama, proprio per ridurre queste possibilità, la protezione delle interfacce esposte a Internet, la sostituzione delle credenziali iniziali e l'aggiornamento del firmware. [7]

Dall'esistenza di più vie d'ingresso segue una conseguenza che il linguaggio giornalistico tende a trascurare: la gravità del danno non rivela, da sola, quanto fosse sofisticata la tecnica impiegata, poiché una password compromessa può conferire un'autorità operativa paragonabile a quella ottenuta sfruttando una falla complessa. Una volta raggiunto il controllore, il potere di alterarne i parametri deriva dai privilegi acquisiti e dalle funzioni cui questi danno accesso; per stabilire quanto fosse innovativo il mezzo occorre invece ricostruire il percorso attraverso il quale l'intruso è entrato. Fra le vulnerabilità software, inoltre, alcune presentano una particolare asimmetria temporale, perché chi le sfrutta può conoscere una debolezza prima che agli utilizzatori sia disponibile una correzione: è a questa circostanza che si riferisce il termine *zero-day*, il cui significato richiede di separare il momento della scoperta da quello della pubblicazione e da quello dell'effettiva protezione dei dispositivi.

Il tempo che separa la scoperta dalla protezione

Una vulnerabilità esiste nel programma anche quando nessuno l'abbia ancora individuata e può essere scoperta tanto da un ricercatore che intenda segnalarla al produttore quanto da un aggressore interessato a sfruttarla; pertanto il fatto che essa sia nota privatamente e che le informazioni tecniche non siano pubbliche non permette di dedurre, senza altri elementi, quale uso ne verrà fatto. Le linee guida di FIRST prevedono, nella *divulgazione coordinata*, che il ricercatore comunichi riservatamente il problema al produttore, affinché possa predisporre un rimedio prima della diffusione dei dettagli che faciliterebbero lo sfruttamento. [17] Quando però la falla viene utilizzata a fini malevoli prima che esista una correzione pubblicamente disponibile, Google Threat Intelligence la classifica, ai fini dei propri rapporti, come *zero-day*; il glossario del NIST insiste invece soprattutto sul fatto che la vulnerabilità fosse precedentemente sconosciuta. [15, 16] Le definizioni pongono l'accento su aspetti diversi, ma consentono di cogliere il medesimo problema operativo: mentre l'attaccante dispone già di un modo per intervenire, chi amministra il sistema può ignorare la debolezza oppure conoscerla senza possedere ancora gli strumenti specifici per eliminarla.

La disponibilità di una *patch*, vale a dire dell'aggiornamento che corregge il difetto, non coincide a sua volta con la scomparsa immediata del rischio, poiché negli impianti industriali la correzione deve spesso essere esaminata sotto il profilo della compatibilità, provata e installata su dispositivi che non possono essere fermati indiscriminatamente: il NIST considera per questo la gestione degli aggiornamenti un'attività continuativa, nella quale la preparazione tecnica si intreccia con le esigenze di esercizio. [18] Una volta pubblicata la patch, un dispositivo che non l'abbia ancora ricevuta resta vulnerabile a una falla ormai nota, benché non appartenga

più alla fase precedente alla disponibilità del rimedio; si comprende così perché la scoperta, l'eventuale divulgazione, la correzione e l'installazione costituiscano tempi distinti, durante i quali la posizione del difensore può cambiare senza che cambi subito il software in esecuzione. Gli avvisi relativi agli impianti frigoriferi attestano compromissioni e condizioni di esposizione, mentre la tecnica effettivamente utilizzata nelle singole intrusioni richiede accertamenti specifici: chiamare indiscriminatamente *zero-day* l'intera ondata attribuirebbe quindi agli episodi una caratteristica che i documenti citati non stabiliscono. [7, 8]

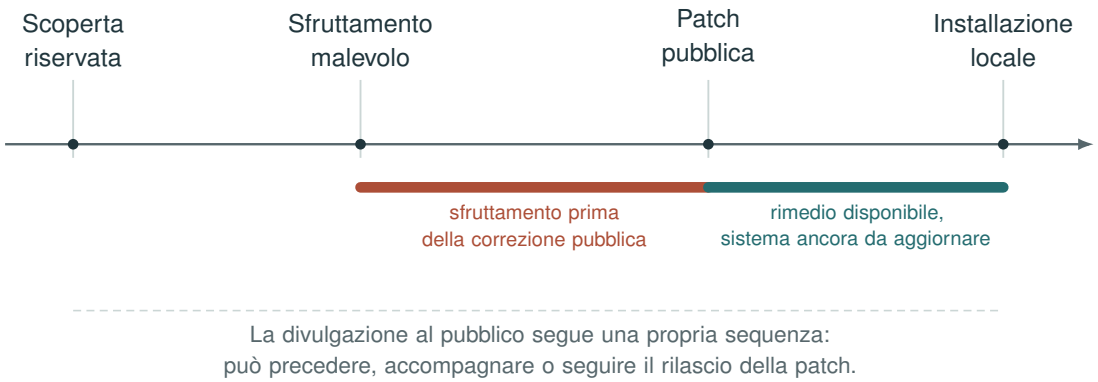


Figura 2. La scoperta privata, lo sfruttamento, l'eventuale divulgazione, la disponibilità della patch e la sua installazione appartengono a fasi differenti. Gli intervalli mostrano come una correzione già pubblica possa richiedere ancora tempo per raggiungere ogni impianto. [16–18]

Che si tratti di credenziali sottratte, di software esposto o di una falla ancora priva di rimedio, l'intrusione sfrutta dunque il divario fra la capacità di intervenire sul sistema e la preparazione di chi deve amministrarlo, divario che può protrarsi quando la difesa richiede verifiche e aggiornamenti distribuiti su molte apparecchiature. Gli allarmi bomba degli stessi giorni permettono di osservare una pressione sull'organizzazione che nasce per una via assai diversa, perché il mittente di un messaggio inventato conosce già l'infondatezza dell'avvertimento, mentre chi ne risponde deve accertarla senza poter escludere in partenza una minaccia autentica: la questione riguarda, in questo caso, il tempo e il lavoro necessari a decidere responsabilmente in condizioni d'incertezza, anziché l'accesso non autorizzato a un programma.

La verifica del pericolo e il costo della decisione

La responsabilità della sicurezza di un volo impone di valutare una minaccia ricevuta anche quando la sua provenienza sia oscura, poiché l'eventualità che una segnalazione autentica venga sottovalutata obbliga a ponderare il rischio prima di escluderlo; affinché la decisione sia giustificata, chi la assume deve confrontare le informazioni disponibili e, secondo le circostanze, disporre controlli e coordinare l'intervento di equipaggi, aeroporti e organismi di sicurezza. Nei casi riferiti da Reuters, questo dovere di verifica si tradusse in ispezioni, deviazioni e, per alcuni aeromobili, scorte militari, benché le ricerche non abbiano portato alla scoperta degli esplosivi annunciati. [5] Il mittente della falsa segnalazione può dunque esaurire la propria azione nella trasmissione di un messaggio, mentre il destinatario, al quale spetta tutelare persone e mezzi, deve far seguire una successione di attività reali: dall'analisi iniziale al contatto con il controllo del traffico aereo, dall'eventuale decisione di atterrare altrove all'organizzazione dei controlli, dell'assistenza ai passeggeri e della ripresa del servizio. L'onere non discende da un accesso abusivo ai sistemi dell'aeromobile, che una semplice minaccia inviata per email non dimostra, bensì dalla necessità istituzionale di distinguere il rischio effettivo dal pericolo dichiarato.

Il confronto con i controllori frigoriferi diventa pertinente una volta seguita, per ciascun episodio, la trasformazione dell'informazione in azione: mentre il controllore esegue l'istruzione perché al suo autore sono stati riconosciuti determinati permessi, la segnalazione di bomba

viene sottoposta al giudizio di persone che, prima di proseguire nelle operazioni ordinarie, devono determinarne l'attendibilità. Di conseguenza, gli obblighi sono differenti — ripristinare o verificare il controllo di un processo materiale, nel primo caso; accertare un pericolo e decidere come garantire la sicurezza, nel secondo — ma entrambi assorbono personale, mezzi e tempo altrimenti destinati allo svolgimento del servizio. Quanto più l'organizzazione deve impiegare le proprie risorse per verificare ciò che proviene dall'esterno, tanto meno può disporne liberamente per le attività già programmate; se sopraggiungono altre segnalazioni prima che le operazioni precedenti siano concluse, la difficoltà aumenta, perché lo stesso personale non può dedicarsi contemporaneamente a tutte le richieste e l'ordine delle priorità deve essere riconsiderato. L'effetto che interessa l'analisi strategica nasce dunque dal rapporto fra l'iniziativa di chi introduce la perturbazione e gli obblighi di chi ne affronta le conseguenze.

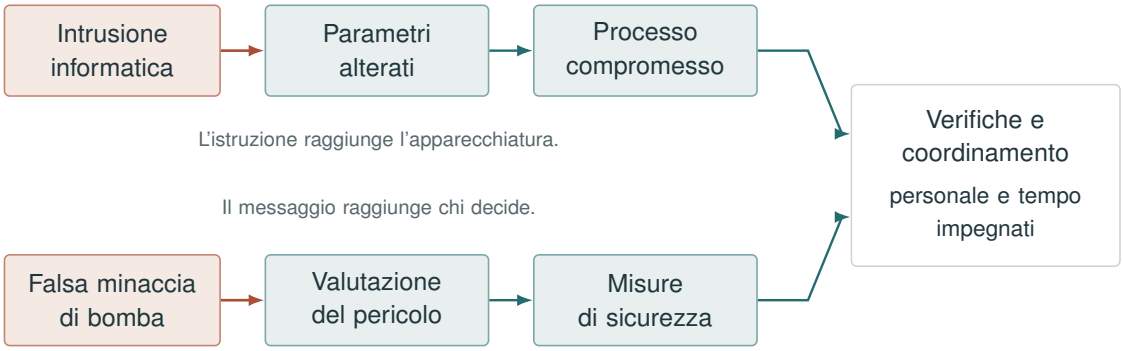


Figura 3. Un'istruzione abusiva entra nel circuito di controllo; una minaccia infondata entra nel processo di valutazione del pericolo. Le conseguenze convergono nel lavoro di verifica e ripristino richiesto al servizio interessato. [5, 8]

Supponiamo che un tecnico sia già impegnato a verificare le impostazioni di un impianto e che, mentre quel controllo resta aperto, debba occuparsi di un'altra anomalia; oppure che un equipaggio, dopo una deviazione, sia in attesa delle autorizzazioni senza le quali non può riprendere il programma di volo. In entrambe le situazioni la perdita consiste anche nelle attività rinviate, oltre che nel tempo impiegato direttamente per rispondere all'incidente, sicché il costo della perturbazione dipende dall'insieme dei compiti che essa rende necessari e dalle possibilità di assorbirli con le risorse disponibili. Il vincolo diviene strategicamente significativo quando le priorità dell'organizzazione, anziché essere stabilite soltanto in funzione dei suoi obiettivi ordinari, vengono determinate almeno in parte dagli eventi che un soggetto esterno ha provocato: la libertà di scegliere dove concentrare lo sforzo viene allora ridotta senza che sia indispensabile distruggere le risorse di cui l'organizzazione dispone. Proprio il rapporto fra un intervento relativamente circoscritto e la redistribuzione del lavoro che esso impone consente di comprendere perché Liddell Hart, riflettendo sulle guerre del passato, attribuisse tanta importanza alle minacce indirizzate contro i collegamenti e alle manovre capaci di costringere l'avversario a reagire prima dello scontro decisivo.

Liddell Hart: dislocare prima di combattere

La ricerca di Basil Henry Liddell Hart nacque dalla Grande Guerra, nella quale egli aveva prestato servizio come ufficiale della fanteria britannica e, nel luglio 1916, era rimasto vittima di un attacco con gas durante la battaglia della Somme; le lettere conservate presso il King's College London restituiscono l'esperienza di combattimenti nei quali il fuoco delle armi moderne poteva consumare intere formazioni per progressi territoriali minimi. [19] Negli anni successivi,

ripensando il rapporto fra il risultato ottenuto e le perdite sopportate, Hart si domandò quale valore potesse conservare una vittoria raggiunta dopo aver dissipato la forza umana e materiale necessaria a sostenere gli obiettivi politici della guerra. La sua risposta partiva dal principio secondo cui il successo sul campo, quando conduce una nazione a dissanguarsi, può compromettere proprio ciò che avrebbe dovuto garantire; in *Strategy* egli scrisse infatti che perfino la vittoria più decisiva perde valore qualora il paese debba pagarla consumando le proprie risorse essenziali. [2, p. 212] Se l'esito politico costituisce il criterio del risultato, ne segue che la strategia debba cercare, prima di ricorrere a combattimenti costosi, le condizioni nelle quali la resistenza nemica possa essere indebolita mediante movimenti, minacce e sorprese.

Da questa esigenza derivò la polemica che Hart rivolse alla tradizione militare da lui ricondotta a Clausewitz e ai suoi seguaci, ai quali imputava di avere attribuito alla battaglia decisiva, alla concentrazione delle masse e alla distruzione delle principali forze avversarie un primato tale da favorire lo scontro contro le difese più robuste. Nella sua interpretazione, la guerra di trincea aveva mostrato quanto potesse diventare onerosa una concezione della vittoria fondata sul logoramento diretto, soprattutto dove la potenza di fuoco rendeva difficilissimo avanzare senza pagare un prezzo sproporzionato; egli cercò pertanto una strategia che, invece di affrontare la resistenza nelle condizioni prescelte dal difensore, ne modificasse anticipatamente l'equilibrio. Osinga ricostruisce la formazione di questo orientamento nel capitolo dedicato all'*approccio indiretto*, seguendo anche l'influenza che la riflessione di Hart avrebbe esercitato su Boyd. [4, cap. 2, "The Indirect Approach"] Per Hart il comandante doveva dunque creare una situazione nella quale la forza avversaria, prima ancora di essere battuta, fosse costretta a ridisporsi e a impegnare energie in compiti diversi da quelli originariamente previsti, perché il combattimento, se ancora necessario, avrebbe allora trovato una resistenza già indebolita.

L'*approccio indiretto* traduceva questo criterio in un rapporto preciso fra movimento e aspettativa: aggirando un settore fortemente difeso per minacciarne i rifornimenti, i collegamenti o le retrovie, l'attaccante poteva costringere il comando avversario a mutare fronte e a impegnare risorse nella protezione di ciò che fino a quel momento considerava sicuro; se la manovra fosse stata imprevista, il tempo richiesto per comprenderla e adattarvisi avrebbe accresciuto l'effetto della minaccia. Hart affiancava pertanto alla «linea di minore resistenza», che riguarda la possibilità fisica di raggiungere un obiettivo, la «linea di minore aspettativa», che riguarda le previsioni del difensore, poiché la facilità del percorso avrebbe avuto scarso valore se l'avversario l'avesse anticipato e si fosse predisposto a fermarlo. [2, p. 327] La sorpresa agiva così in due direzioni: rendeva più agevole il movimento di chi aveva assunto l'iniziativa e, nello stesso tempo, obbligava l'altro a consumare parte della propria energia per correggere un assetto divenuto inadeguato; era quest'ultima conseguenza, più ancora del semplice aggiramento geografico, a determinare la dislocazione strategica.

I collegamenti cui Hart si riferiva erano anzitutto concreti: vie di rifornimento, linee di ritirata, rapporti fra unità e possibilità di far affluire rinforzi dove fossero necessari. Quanto più un esercito è grande e articolato, tanto più la sua forza dipende dalla continuità di quelle relazioni, sicché minacciare una linea di comunicazione può costringerlo a proteggere una parte del proprio sistema logistico impiegando uomini e mezzi che, altrimenti, avrebbe destinato a combattere. [2, p. 326] L'effetto fisico, tuttavia, rimane incompleto se non si considera ciò che accade nella mente del comandante, al quale spetta interpretare i movimenti nemici e decidere dove concentrare la risposta: quando la minaccia compare in una direzione inattesa, l'incertezza circa la sua gravità può indurlo a disperdere l'attenzione su obiettivi secondari, riducendo ulteriormente la possibilità di utilizzare lo schieramento in modo coordinato. È a questo processo che Hart attribuiva il nome di *distrazione*, spiegando che la perdita della libertà

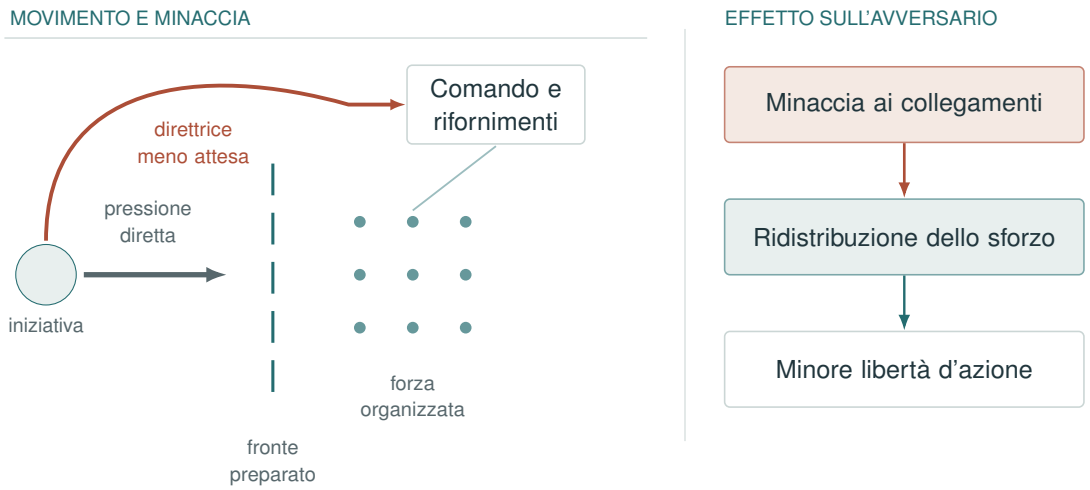


Figura 4. Una minaccia indiretta verso comando e rifornimenti può costringere l'avversario a ridistribuire il proprio sforzo; il diagramma sintetizza il rapporto fra movimento, sorpresa e perdita della libertà d'azione descritto da Hart. [2, pp. 326–328]

d'azione segue quella della libertà di concepire adeguatamente la situazione. [2, pp. 327–328][1]

La dimensione psicologica assume ancora maggiore importanza quando l'incertezza si accompagna alla paura, che può propagarsi attraverso le persone e modificare le decisioni anche al di fuori del punto in cui è sorta: per esprimere questa possibilità Hart descrive l'uomo scosso come un veicolo capace di diffondere un'«epidemia di panico», osservando poi che l'impressione prodotta sul comandante può neutralizzare la capacità combattiva di forze ancora materialmente disponibili. [2, p. 212] L'esercito, in altre parole, conserva uomini e mezzi, ma la loro efficacia dipende dal giudizio e dai collegamenti attraverso cui vengono diretti. Il medesimo rapporto aiuta a comprendere perché le perturbazioni civili interessino la strategia oltre la tecnologia impiegata: chi altera un comando o diffonde una minaccia infondata può costringere il destinatario a riorganizzare il lavoro e a sottoporre a verifica funzioni che prima procedevano normalmente, riducendone per un certo tempo la libertà di scegliere le proprie priorità. Hart chiarisce perché la reazione possa diventare parte dell'effetto; per capire come successive informazioni incerte possano rendere più difficile ristabilire una direzione comune, occorre però esaminare il processo attraverso cui le organizzazioni formano, correggono e condividono la propria rappresentazione degli eventi.

John Boyd: interpretare prima di reagire

John Boyd affrontò il problema muovendo dall'esperienza del combattimento aereo, nel quale la capacità di cambiare rapidamente manovra può mettere in difficoltà il pilota avversario, costretto ad adattarsi a una situazione che muta prima che abbia compreso la precedente. Ian T. Brown ricostruisce come Boyd, partendo dalle prestazioni dei caccia e dallo studio delle transizioni fra manovre, arrivasse a considerare la rappresentazione mentale dell'altro combattente quale elemento decisivo: il vantaggio acquistato nello spazio e nel tempo produce effetti maggiori quando l'avversario interpreta male ciò che vede e orienta le proprie decisioni verso una situazione ormai superata. [3, cap. 4] Nella testimonianza orale riportata da Brown, Boyd descrive il processo dal punto di vista di chi lo subisce, spiegando che l'ambiguità delle azioni altrui lo rende progressivamente incerto, poi confuso e disordinato, fino al panico. [3, p. 94, nota 17] La formulazione lascia riconoscere una sequenza causale: se l'informazione

[1] Nell'originale: «The loss of his freedom of action is the sequel to the loss of his freedom of conception»; B. H. Liddell Hart, *Strategy*, p. 328.

disponibile non consente più di costruire un quadro attendibile, anche la decisione presa con prontezza rischia di rispondere a un evento diverso da quello realmente in corso.

Per spiegare come individui e organizzazioni interpretino e correggano il proprio rapporto con l'ambiente, Boyd elaborò il processo indicato dall'acronimo OODA, dalle parole inglesi *Observe, Orient, Decide, Act*: osservare significa rilevare segnali e cambiamenti; orientarsi significa attribuire loro un significato alla luce dell'esperienza e delle conoscenze possedute; decidere significa scegliere un comportamento; agire permette infine di verificarne gli effetti, dai quali prendono avvio ulteriori osservazioni. La ricostruzione di Osinga insiste sul fatto che l'orientamento occupa il posto centrale, perché influenza ciò che viene notato e il modo in cui una possibilità d'azione viene giudicata: la cultura, le esperienze precedenti, le capacità apprese e le informazioni nuove concorrono a formare una rappresentazione che deve essere continuamente messa alla prova. [4, cap. 6, "The Essence of Winning and Losing", fig. 6.1] Boyd riassume questa centralità affermando che l'orientamento è lo *Schwerpunkt*, cioè il punto sul quale si concentra l'attività intellettuale dell'organizzazione, dal momento che persino un flusso abbondante e tempestivo di dati perde valore qualora non venga interpretato in modo adeguato alle circostanze. [4, cap. 6, "The big O: orientation", nota 13]

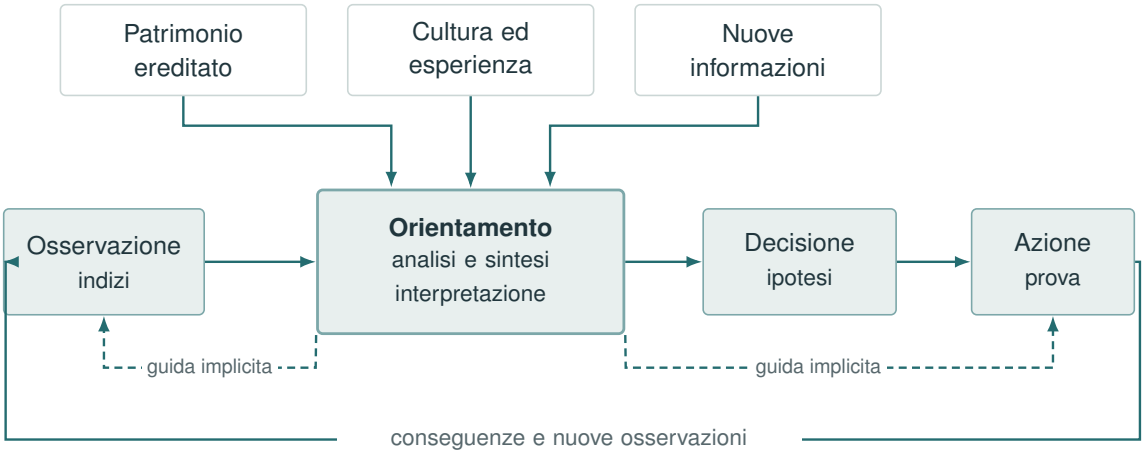


Figura 5. Il processo OODA nella lettura di Osinga: esperienza, cultura e nuove informazioni concorrono all'orientamento; l'azione produce conseguenze che tornano a modificare le osservazioni e la valutazione successiva. [4, cap. 6, fig. 6.1]

Quando il compito richiede l'intervento di più persone, la qualità dell'orientamento dipende anche dalla possibilità che osservazioni parziali vengano ricomposte in un giudizio condiviso: l'addetto alle merci può constatare una temperatura anomala senza conoscere le impostazioni del controllore, il tecnico può individuare un parametro alterato senza essere responsabile della destinazione dei prodotti, mentre chi dirige l'esercizio deve decidere se fermare l'impianto o proteggere le scorte. Affinché l'organizzazione agisca con coerenza, i diversi saperi devono potersi confrontare e produrre una rappresentazione comune, mentre messaggi contraddittori o incompleti possono ritardare proprio le decisioni che richiedono il concorso di più funzioni. Boyd attribuiva per questo grande importanza alla *guida implicita*: quando esperienza condivisa, fiducia e chiarezza degli obiettivi permettono ai membri di riconoscere l'intenzione generale, essi possono prendere iniziative compatibili fra loro senza attendere istruzioni particolareggiate per ogni circostanza; Osinga collega tale principio alla riduzione dell'attrito organizzativo e alla capacità di adattamento. [4, cap. 6, "Organic Design for Command and Control"]

La rapidità, in questa teoria, è utile nella misura in cui accompagna un'interpretazione capace di correggersi, perché agire immediatamente secondo una rappresentazione falsa può

aggravare l'errore, mentre comprendere tempestivamente che le ipotesi iniziali sono inadeguate permette di modificare le decisioni prima che le conseguenze diventino più gravi. Se a una perturbazione ne segue un'altra quando la prima non è stata ancora chiarita, il lavoro di verifica si sovrappone a nuove richieste e rende più difficile stabilire quali informazioni siano pertinenti, quali decisioni abbiano precedenza e chi debba assumersene la responsabilità. La dislocazione descritta da Hart si prolunga allora in un problema di orientamento, poiché le risorse già impegnate nella risposta non possono essere facilmente ridistribuite mentre il quadro degli eventi rimane incerto: Boyd ha analizzato questa circostanza attraverso il rapporto fra shock, tempo disponibile e capacità di adattamento.

Shock ripetuto, isolamento e capacità di recupero

Nel capitolo dedicato al conflitto di manovra, Osinga riferisce che Boyd considerava sorpresa e shock come forme di sovraccarico, prodotte da una successione di eventi minacciosi che superi la capacità mentale o fisica di rispondere, adattarsi o resistere. [4, cap. 5, "Maneuver conflict", nota 103] La gravità di tale sovraccarico dipende dal rapporto fra il ritmo con cui arrivano nuove richieste e il tempo necessario a comprenderle: quando una squadra sta ancora accertando il funzionamento di un impianto e sopraggiunge un'altra anomalia, oppure quando un'ispezione non è conclusa e una nuova segnalazione richiede una decisione, i compiti rimasti aperti competono per le medesime persone e informazioni. Poiché ciascuna valutazione deve essere coordinata con altre funzioni, l'accumulo può rendere meno agevole stabilire quali accertamenti siano urgenti e in quale ordine svolgerli; così, l'incremento dell'onere dipende anche dalla loro sovrapposizione, poiché ciascun nuovo episodio deve essere affrontato mentre il precedente continua ad assorbire risorse.

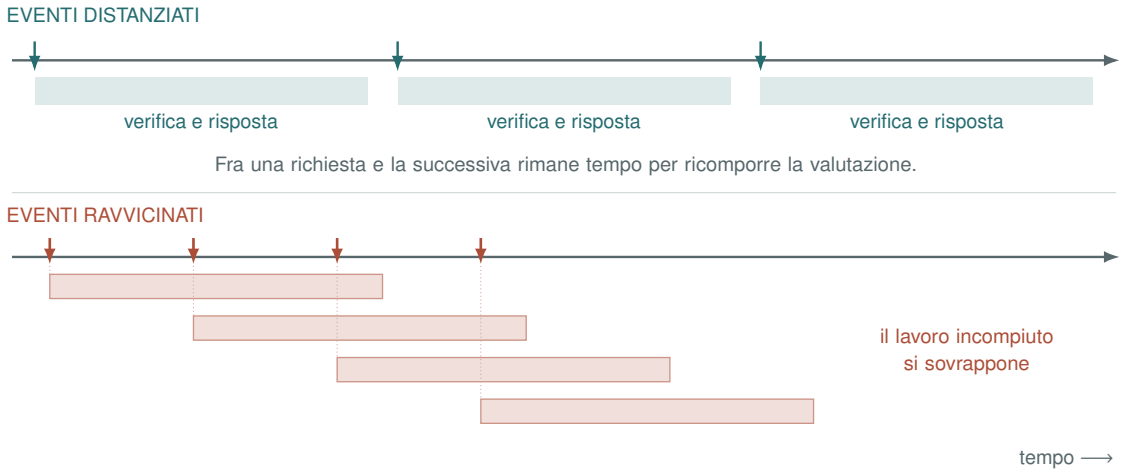


Figura 6. Una successione di richieste può creare lavoro simultaneo quando gli accertamenti precedenti rimangono aperti. Lo schema illustra la relazione fra intervallo degli eventi e tempo disponibile per la risposta, secondo il problema del sovraccarico discusso da Boyd. [4, cap. 5, "Maneuver conflict"]

Se i segnali riguardano rischi che non possono essere esclusi senza verifica, l'incertezza stessa impone ulteriori accertamenti, i quali riducono il tempo disponibile per comprendere gli eventi successivi; qualora, inoltre, i messaggi risultino contraddittori, chi deve decidere può trovarsi costretto a riesaminare giudizi già formulati mentre nuove attività sono state avviate sulla base di essi. In *Patterns of Conflict*, secondo il passo riportato da Osinga, Boyd associava la compromissione dei collegamenti dai quali dipendono comunicazioni, comando e sostegno alla produzione ripetuta di sorpresa e shock, «ancora e ancora e ancora», giacché l'effetto cercato era la perdita di coesione che impedisce a un avversario di reagire come un insieme

organizzato. [4, cap. 5, "The nucleus of victory", nota 92: *Patterns of Conflict*, diapositiva 98] Per comprenderne la portata, occorre intendere i collegamenti in senso ampio: Osinga mostra che, nello *Strategic Game of ? and ?*, Boyd distingue la relazione *fisica*, che assicura lo scambio di risorse e informazioni, da quella *mentale*, che consente una comprensione adeguata degli eventi, e da quella *morale*, che sostiene la cooperazione attraverso norme e fiducia; la strategia diventa così un confronto fra capacità di *interazione* e condizioni di *isolamento*. [4, cap. 6, "The Strategic Game of ? and ?"]

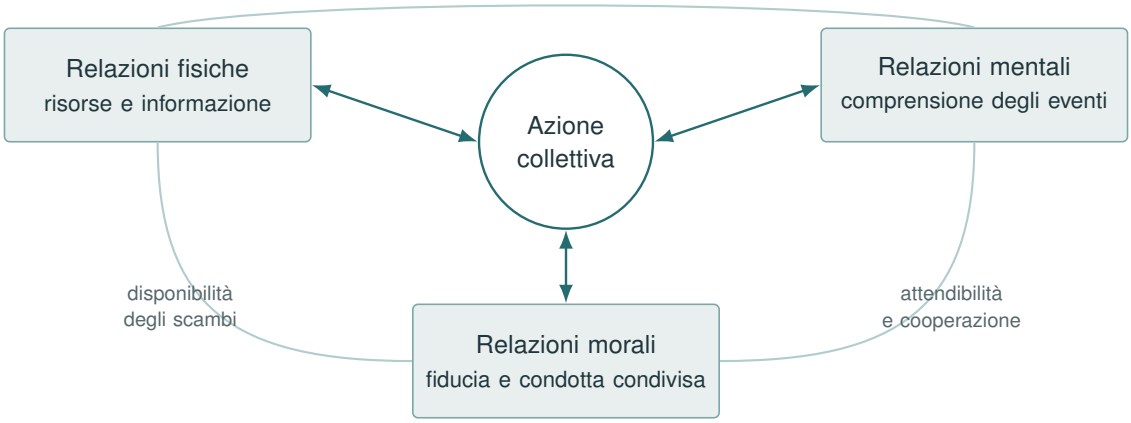


Figura 7. La capacità di agire insieme richiede che lo scambio delle risorse, la comprensione degli eventi e la fiducia nelle persone rimangano reciprocamente sostenuti. [4, cap. 6, "The Strategic Game of ? and ?"]

Una rete può continuare a trasmettere messaggi e, nondimeno, non garantire un'azione coordinata: se le informazioni sono inattendibili, le persone possono muoversi sulla base di interpretazioni incompatibili; se manca la fiducia nelle valutazioni altrui, anche comunicazioni tecnicamente corrette richiedono continue conferme e finiscono per appesantire la risposta. Quando il lavoro di verifica sottrae energie alle attività successive e queste, a loro volta, introducono ulteriori incertezze, la perturbazione iniziale può alimentare un circolo nel quale la difficoltà di comprendere il quadro generale accresce il ritardo delle decisioni, mentre il ritardo moltiplica i problemi ancora da chiarire. Nella teoria di Boyd, una simile progressione può sfociare nella paralisi qualora venga meno la capacità di ricostruire un orientamento collettivo; l'esito cambia, invece, se l'organizzazione conserva collegamenti affidabili, iniziativa dei propri membri e possibilità di apprendere dagli accertamenti, perché queste risorse consentono di interrompere il sovraccarico e recuperare una direzione comune. [4, capp. 5 e 7]

Il costo della perturbazione, dunque, comprende il lavoro necessario a ristabilire l'attendibilità dei segnali, la legittimità dei comandi e la continuità delle decisioni, anche quando il danno materiale immediato sia rimasto circoscritto. Quando tale lavoro assorbe risorse che sarebbero destinate all'attività ordinaria, la libertà di concentrare lo sforzo si riduce nel senso descritto da Hart; se poi l'incertezza si accumula e gli shock si succedono prima che l'organizzazione abbia recuperato una rappresentazione affidabile degli eventi, la teoria di Boyd spiega come alla perdita d'iniziativa possa aggiungersi il deterioramento dell'orientamento e della coesione. Per contenere questa progressione occorrono accessi protetti e sistemi aggiornati, come raccomandano le autorità di sicurezza, insieme alla capacità di verificare i dati, condividere le valutazioni e decidere secondo responsabilità chiare, affinché il ripristino del servizio coincida con il recupero della libertà d'azione dalla quale dipende la continuità delle attività ordinarie. [7, 8] [4, cap. 7, "Mental and organizational agility"]

Riferimenti

[1] Phil Alden Robinson (regia), *I signori della truffa* (*Sneakers*), Universal Pictures, 1992; battuta di Cosmo nella versione italiana. Trascrizione italiana della battuta.

[2] B. H. Liddell Hart, *Strategy*, seconda edizione riveduta, 1967; ristampa Meridian, New York, 1991. Edizione fornita: pp. 212, 324–328.

[3] Ian T. Brown, *A New Conception of War: John Boyd, the U.S. Marines, and Maneuver Warfare*, Marine Corps University Press, Quantico, 2018. Edizione fornita: cap. 4, p. 94, nota 17, che cita la testimonianza orale di Boyd, pp. 134–135.

[4] Frans P. B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd*, Routledge, 2007; edizione elettronica 2006 fornita. Cap. 2, "The Indirect Approach"; cap. 5, "The nucleus of victory: the themes of Blitzkrieg and guerrilla warfare", nota 92 (*Patterns of Conflict*, diapositiva 98), e "Maneuver conflict", nota 103 (diapositiva 117); cap. 6, "The big O: orientation", nota 13 (*Organic Design*, diapositiva 16), "The Strategic Game of ? and ?", nota 56 (diapositiva 33), e "The Essence of Winning and Losing", fig. 6.1; cap. 7, sezioni su orientamento, adattamento, agilità organizzativa e "Cyberwar and swarming". I rimandi per sezione identificano i passi nell'EPUB a impaginazione variabile.

[5] Reuters, *Bomb threats cause flight disruptions across Europe*, 5 novembre 2026, ripubblicato da *Internazionale*, 6 novembre 2026. Testo della ricostruzione.

[6] Commissione europea ed ENISA, *Joint statement on cyber incidents in refrigeration systems across the EU*, 4 novembre 2026. Comunicato ufficiale.

[7] ANSSI / CERT-FR, *Incident de sécurité ciblant les contrôleurs à distance des installations de réfrigération*, CERTFR-2026-ALE-012, 12 ottobre 2026, aggiornamento del 16 ottobre 2026. Allerta tecnica.

[8] CISA, FBI, HHS, USDA e DoT, *US Government Partners Urge Hardening Industrial Refrigeration and Cold Chain Monitoring Systems*, 5 novembre 2026, pp. 1–2. Avviso congiunto.

[9] Keith Stouffer et al., *Guide to Operational Technology (OT) Security*, NIST SP 800-82, revisione 3, settembre 2023, in particolare §§ 2–2.3 e pp. 10–11. doi:10.6028/NIST.SP.800-82r3.

[10] NIST, CSRC Glossary, voce *Operational technology*. Definizioni e fonti.

[11] MITRE, ATT&CK for ICS, *Modify Parameter*, tecnica T0836. Scheda tecnica.

[12] MITRE, ATT&CK for ICS, *Manipulation of View*, tecnica T0832. Scheda tecnica.

[13] MITRE, ATT&CK for ICS, *Valid Accounts*, tecnica T0859. Scheda tecnica.

[14] MITRE, ATT&CK for ICS, *Exploit Public-Facing Application*, tecnica T0819. Scheda tecnica.

[15] NIST, CSRC Glossary, voce *Zero-day attack*. Definizione e fonti.

[16] Google Threat Intelligence Group, Casey Charrier et al., *Look What You Made Us Patch: 2025 Zero-Days in Review*, 5 marzo 2026, sezione "Scope". Rapporto e criterio di classificazione.

[17] FIRST, *Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure*, versione 1.0, 2017, caso d'uso 2 e varianti. Linee guida.

[18] Murugiah Souppaya e Karen Scarfone, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*, NIST SP 800-40, revisione 4, aprile 2022. doi:10.6028/NIST.SP.800-40r4.

[19] Liddell Hart Centre for Military Archives, King's College London, presentazione a cura di Patricia Methven della lettera di Hart ai genitori del 15 luglio 1916 e del resoconto della Somme del 18 settembre 1916, 3 marzo 2014; segnatura Liddell Hart 7/1916/15a. Presentazione e materiali d'archivio.

Criteri delle fonti. L'argomento storico e teorico si fonda sui tre volumi forniti, che seguono la citazione cinematografica nell'elenco. Le spiegazioni informatiche utilizzano le fonti tecniche indicate, mentre la cronologia iniziale deriva dai comunicati istituzionali e da Reuters. Le applicazioni dei concetti agli episodi contemporanei sono sviluppate nel testo. Fonti online consultate il 7 novembre 2026.