Dopo il corso: dalla guerra ibrida alla capacità di orientamento

Complessità, vulnerabilità sistemiche, decisioni e resilienza: una riflessione per il governo dei sistemi civili e militari

Guido Mastrobuono | Memo 03 | Revisione scientifica dell'11 novembre 2026

Nota personale di approfondimento per i partecipanti al corso di Alta Formazione in Project Management rivolto al Corpo degli Ingegneri dell'Esercito, svolto presso il CEPOLISPE.

Una tesi per iniziare

Una società può continuare a funzionare e diventare, nel frattempo, meno capace di governare le proprie funzioni essenziali. Le infrastrutture erogano ancora servizi, i programmi risultano formalmente in corso e le informazioni continuano ad arrivare. Eppure si stanno consumando le riserve, alcune interdipendenze non sono rappresentate, le ipotesi decisionali non descrivono più il contesto oppure le autorizzazioni necessarie arriverebbero oltre il tempo utile. La vulnerabilità più seria può dunque maturare prima che un indicatore convenzionale segnali una crisi.

Questo memo approfondisce una convinzione che ho maturato lavorando sul Risk Management e sui sistemi complessi: proteggere un'organizzazione non significa soltanto prevenire eventi avversi. Significa anche preservare la capacità di capire che cosa sta cambiando, distinguere una perturbazione da una trasformazione strutturale e utilizzare in tempo le leve effettivamente disponibili. È una questione che interessa la Difesa, ma anche chi governa infrastrutture critiche, servizi essenziali, programmi pubblici e grandi progetti.

La riflessione nasce dal confronto avvenuto durante il corso e da successivi approfondimenti sul governo dei progetti e dei sistemi complessi. È una nota personale di ricerca e confronto: non costituisce una dottrina militare né esprime una posizione ufficiale dell'Esercito, della Difesa, della Sapienza o di altre istituzioni. I due meccanismi integrati di destabilizzazione e la nozione di «caos operativo» sono proposte interpretative dell'autore, non risultati scientifici convalidati; i principi consolidati e le ipotesi originali sono tenuti distinti.

1. La domanda emersa dopo il corso

Durante il corso al CEPOLISPE abbiamo discusso di incertezza, progetti complessi, guerra ibrida, analisi di contesto, vulnerabilità e resilienza nazionale. A distanza di qualche tempo, tornando su questi temi, mi sono accorto che una domanda attraversava tutti gli altri: *come può un'organizzazione accorgersi che la rappresentazione sulla quale fonda le proprie decisioni non è più adeguata alla situazione reale?*

Non è un problema esclusivamente informativo. Un'organizzazione può disporre di dati corretti ma attribuire loro un significato sbagliato; può comprendere perfettamente ciò che sta accadendo ma non avere più le risorse, l'autorità o il tempo necessari per rispondere. I problemi di conoscenza e quelli di capacità d'intervento sono diversi. Confonderli può condurre a soluzioni inefficienti: più report quando servirebbe una riserva operativa, più mezzi quando occorrerebbe cambiare modello interpretativo, più procedure quando il collo di bottiglia è una decisione che nessuno può assumere in tempo.

Ho cercato di affrontare il problema integrando tre prospettive. La prima è sistemica: quali relazioni e dipendenze spiegano il comportamento dell'insieme? La seconda riguarda gli attori: come possono interessi, aspettative e azioni intenzionali trasformare il contesto? La terza è decisionale: quali capacità permettono di preservare le funzioni quando non possiamo prevedere con sufficiente affidabilità l'evoluzione del sistema? Il collegamento fra queste prospettive, più che la ricerca di una nuova etichetta, è il contributo che vorrei discutere.

2. La guerra ibrida non è soltanto un repertorio di minacce

Le espressioni «guerra ibrida» e «minacce ibride» vengono spesso associate a cyberattacchi, sabotaggi, manipolazione delle informazioni, coercizione economica, pressioni diplomatiche e impiego o minaccia della forza. Non sono però sinonimi in ogni quadro analitico: il primo termine rimanda a determinate modalità di conflitto, mentre il secondo è utilizzato dalle istituzioni europee e atlantiche per descrivere un insieme più ampio di attività ostili. Elencare gli strumenti aiuta a riconoscerli, ma non spiega da solo perché le azioni producano effetti differenti in sistemi con vulnerabilità e capacità di risposta diverse. (Consiglio dell'Unione europea, 2026; NATO, 2026)

Il Consiglio dell'Unione europea descrive le minacce ibride come attività dannose generalmente coordinate e intenzionali, condotte attraverso mezzi spesso combinati, per colpire istituzioni o Stati e rendere difficili individuazione e risposta. La NATO segnala la varietà di attori e metodi e la crescente rapidità, scala e intensità abilitate dall'interconnessione. Nelle conclusioni del 16 marzo 2026, il Consiglio richiama la protezione delle infrastrutture critiche e dei processi democratici e la cooperazione con soggetti pubblici e privati. Sono posizioni istituzionali e indicazioni di policy, non verifiche sperimentali dei meccanismi ipotizzati in questa nota. (Consiglio dell'Unione europea, 2026; NATO, 2026)

Il rapporto del Joint Research Centre e dell'Hybrid CoE organizza l'analisi delle minacce ibride intorno a quattro pilastri: attori e obiettivi strategici, domini, strumenti e fasi. Il documento collega tali elementi alle vulnerabilità, alle soglie di rilevabilità e attribuzione e alla risposta. Gli autori dichiarano di aver messo alla prova il modello mediante studi di caso, ma questi ultimi sono classificati e non compaiono nella versione pubblica: il lettore può verificarne l'impostazione concettuale, non replicare autonomamente il controllo sui casi. Il trasferimento di questo schema al governo di singoli progetti è quindi una nostra applicazione interpretativa, da valutare nel caso concreto. (JRC/Hybrid CoE, 2021)

Non tutte le perturbazioni sono ostili e non tutte le condotte ostili producono l'esito sperato. Una restrizione commerciale, un blocco logistico o una comunicazione falsa possono avere conseguenze serie anche senza un coordinamento fra gli eventi. Per sostenere l'ipotesi di una campagna intenzionale occorre ricostruire separatamente il fatto osservato, il meccanismo attraverso il quale gli effetti si sarebbero propagati, gli indizi dell'intento e gli elementi che consentono un'attribuzione. Il semplice vantaggio conseguito da un attore non prova che l'attore abbia progettato l'evento.

La prudenza nell'attribuzione non impone passività. La protezione di una funzione essenziale può essere necessaria anche quando la causa non è ancora accertata. Riconoscere una vulnerabilità e correggerla è una responsabilità gestionale; attribuire un'azione ostile e decidere eventuali risposte investigative o istituzionali è una questione ulteriore, affidata ai soggetti competenti.

3. Il problema sistemico: le relazioni contano quanto le componenti

Un'infrastruttura è spesso descritta attraverso le proprie componenti: impianti, opere, reti, mezzi, persone, contratti. È una rappresentazione necessaria, ma non sempre sufficiente. Ciò che rende

possibile il servizio è anche l'organizzazione delle relazioni fra gli elementi. La disponibilità di un gruppo elettrogeno, per esempio, non garantisce la continuità di una funzione se mancano il carburante, i controlli, le autorizzazioni all'impiego o le persone in grado di metterlo in esercizio.

Qui è utile distinguere *complicazione* e *complessità*. Un problema è principalmente complicato quando la sua difficoltà dipende dal numero delle parti e dalle competenze necessarie, ma le relazioni sono abbastanza stabili da poter essere analizzate. Diventa rilevante la complessità quando interazioni, retroazioni, comportamenti adattivi e vincoli condivisi possono modificare il comportamento complessivo. Il primo tipo di problema richiede scomposizione e competenza specialistica; il secondo può richiedere anche osservazione delle interdipendenze, ricostruzione dei feedback e aggiornamento dei modelli. I due caratteri possono coesistere nello stesso sistema. (Holland, 1992; Kurtz e Snowden, 2003)

È utile distinguere tre meccanismi che possono generare andamenti esteriormente simili. Una causa comune agisce su più elementi senza che il guasto dell'uno causi quello dell'altro. Una cascata propaga conseguenze lungo dipendenze effettive. Una retroazione riporta gli effetti di una variazione sulle condizioni che influenzano il processo successivo. La distinzione è una sintesi analitica: per verificarla occorrono cronologia, collegamenti e dati, non la sola coincidenza temporale degli scostamenti. Le possibili risposte sono diverse: proteggere una risorsa condivisa, interrompere una propagazione o modificare un circuito di feedback. (Rodrigues, 2001; NASA, 2016)

Si consideri un grande programma che utilizza gli stessi fornitori specializzati di altri programmi. Una difficoltà produttiva provoca ritardi; i responsabili reagiscono anticipando ordinativi o modificando le priorità; gli ordini concorrenti aumentano il carico sul medesimo collo di bottiglia. Il problema finale non è più soltanto il primo ritardo, ma l'interazione fra capacità limitata e comportamenti di risposta. È uno scenario esemplificativo, non un caso empirico presentato come dimostrato. Mostra perché una soluzione localmente razionale possa produrre un effetto collettivo indesiderato.

Non dobbiamo però trasformare «più interconnessione» in un sinonimo automatico di «più rischio». Collegamenti alternativi possono aumentare ridondanza e capacità di recupero. Il giudizio dipende da quali funzioni sono sostenute, dalla sostituibilità, dai tempi necessari e dall'eventuale presenza di dipendenze comuni. Una rete può amplificare la perturbazione oppure assorbirla: occorre descrivere il percorso causale concreto, non fermarsi alla sua topologia.

Per questo il confine dell'analisi non coincide necessariamente con il perimetro amministrativo o contrattuale. Un'organizzazione può dipendere da reti energetiche, filiere, sistemi digitali e attori istituzionali che non controlla. Un'analisi di contesto proporzionata deve includere le condizioni pertinenti alle funzioni e alle decisioni da sostenere, non l'intero universo dei fattori esterni. Le relazioni rappresentate restano ipotesi da motivare e, quando possibile, da controllare con evidenze indipendenti. (NASA, 2016; Rodrigues, 2001)



Figura 1 — Le dipendenze di una funzione essenziale possono attraversare più sistemi. Schema illustrativo.

4. Due meccanismi possibili di destabilizzazione

Da queste distinzioni propongo di ricavare due meccanismi interpretativi, utili a formulare domande differenti davanti a situazioni genericamente definite «caotiche». Il primo riguarda la trasformazione e l'amplificazione delle interazioni; il secondo l'adeguatezza dell'osservazione, dell'orientamento, delle decisioni e delle capacità d'intervento. Le opere citate documentano singoli concetti e approcci; nessuna delle fonti verificate dimostra che questa specifica integrazione costituisca una nuova teoria causalmente validata.

4.1 Primo meccanismo: la perturbazione si amplifica attraverso il sistema

Una perturbazione, intenzionale o spontanea, può attraversare dipendenze funzionali, temporali, informative e organizzative. Le risposte dei soggetti coinvolti possono modificarne la propagazione, introducendo nuove priorità, saturando risorse comuni oppure attivando retroazioni che aggravano il problema. In queste condizioni cresce la difficoltà di coordinare il sistema, anche quando l'evento iniziale è ben conosciuto.

Il passaggio decisivo non è il numero dei problemi segnalati, ma l'eventuale trasformazione delle interazioni rilevanti per le decisioni e dei tempi di risposta. L'amplificazione degli effetti non implica necessariamente un aumento misurabile della complessità intrinseca del sistema. Occorre domandarsi: quali collegamenti sono stati attraversati? Quali decisioni hanno cambiato la situazione? Quando sono state consumate le capacità di risposta? Quali alternative erano davvero indipendenti? Senza una ricostruzione temporale e un confronto con cause comuni o errori locali, l'ipotesi rimane plausibile, non accertata. (Rodrigues, 2001)

4.2 Secondo meccanismo: si deteriorano le capacità di governo

Un sistema può mantenere sostanzialmente immutate le proprie relazioni e diventare ugualmente difficile da governare. Le informazioni arrivano tardi; fatti nuovi sono interpretati attraverso assunzioni obsolete; le competenze decisionali sono distribuite fra unità che non si coordinano; una misura viene approvata quando non c'è più tempo per attuarla. La difficoltà riguarda allora il collegamento fra osservazione, orientamento, decisione e azione, senza che ciò dimostri un incremento della complessità del fenomeno. Il richiamo al ciclo OODA è tratto da Boyd; quello alla credibilità delle rappresentazioni è pertinente ai criteri NASA, non a una presunta validazione organizzativa di questo meccanismo. (Boyd, 2018; NASA, 2026)

Qui la distinzione sviluppata nel memo originario conserva tutta la sua importanza: *degradare l'orientamento* e *ridurre le opzioni di azione* non sono la stessa cosa. La prima difficoltà è conoscitiva e interpretativa; la seconda è materiale, temporale, organizzativa o di autorità. Possono presentarsi insieme, ma anche separatamente. Un'organizzazione può capire la situazione e non poter agire; può, viceversa, mantenere funzioni essenziali grazie a meccanismi protettivi anche quando la diagnosi è incompleta.

I due meccanismi integrati non devono essere confusi con la distinzione, interna al secondo, fra insufficienza dell'orientamento e insufficienza delle opzioni di intervento. Il primo interpreta il ruolo di dipendenze, propagazione e retroazioni; il secondo considera la capacità dell'organizzazione di comprendere e affrontare le richieste risultanti. Possono combinarsi oppure presentarsi separatamente. Per ciascun caso servono una funzione da preservare, una cronologia, nessi da verificare e spiegazioni concorrenti. Non è lecito dedurre né il meccanismo né l'intento ostile dalla gravità dell'esito.

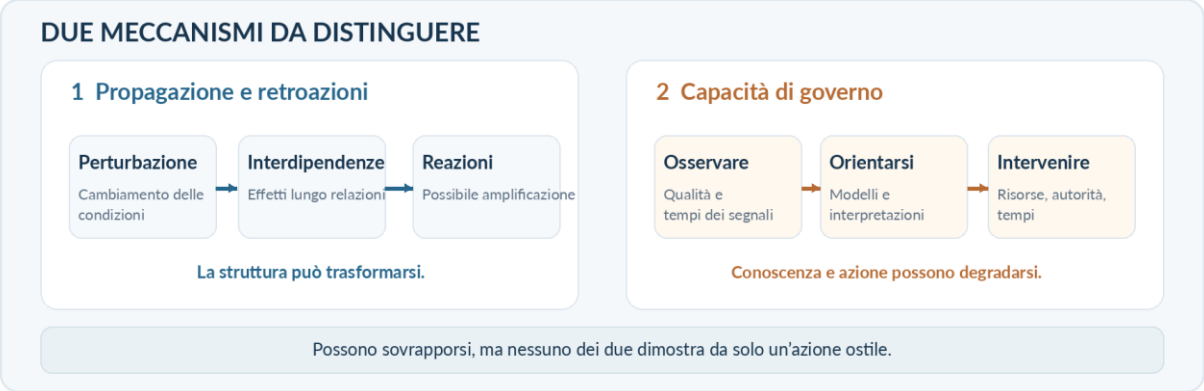


Figura 2 — Due possibili meccanismi di destabilizzazione, da verificare nel caso concreto.

5. Il «caos operativo»: una proposta da trattare con prudenza

Il caos deterministico ha un significato matematico: in particolari sistemi dinamici deterministici, piccole differenze nelle condizioni iniziali possono determinare traiettorie divergenti; ciò non autorizza a chiamare «caotica» ogni organizzazione in crisi. Il dominio chaotic del framework Cynefin è invece una categoria di sense-making per condizioni nelle quali i consueti nessi causa-effetto non possono orientare in tempo utile la decisione; in quel dominio può essere necessario agire inizialmente per stabilizzare e poi osservare. Nessuno dei due concetti dimostra la proposta di «caos operativo» formulata qui. (Lorenz, 1963; Kurtz e Snowden, 2003; Snowden e Boone, 2007)

Propongo di utilizzare, in via esplorativa, l'espressione «caos operativo» per una condizione nella quale, rispetto a una funzione identificata e a un intervallo di tempo definito, le capacità effettive di riconoscere la situazione e/o attivare risposte utili non risultano adeguate alle richieste che devono essere affrontate. Non basta un report mancante, una risorsa insufficiente o un esito sfavorevole: occorre documentare perché la funzione non possa più essere governata entro le soglie dichiarate. Vanno specificati prestazione minima, orizzonte temporale, perturbazioni, osservazioni disponibili, opzioni e relativi tempi di attivazione. È una definizione di lavoro, non una grandezza matematica, una metrica tarata o una categoria scientifica indipendentemente validata.

La proposta permette una distinzione che trovo operativamente importante. Un progetto può fallire pur essendo stato governato ragionevolmente rispetto alle conoscenze e alle possibilità disponibili; il mancato raggiungimento dell'obiettivo non prova di per sé una precedente perdita di governabilità. Per contro, un'organizzazione può continuare a conseguire risultati soddisfacenti mentre consuma riserve,

perde sostituibilità e non riesce più a rivedere tempestivamente le scelte. In questo secondo caso il problema può precedere il deterioramento visibile delle prestazioni.

Perché la proposta abbia un valore scientifico occorre mostrarne l'utilità discriminante rispetto a termini già consolidati, come «crisi», «saturazione», «incertezza profonda» o «fallimento organizzativo». Andranno cercati anche controesempi: sistemi molto interdipendenti che restano governabili, organizzazioni efficaci con conoscenza incompleta e fallimenti inevitabili nonostante giudizi e azioni adeguati. Un eventuale miglioramento delle decisioni dovrà essere confrontato con i costi di diagnosi e coordinamento. Una definizione che potesse essere assegnata retrospettivamente a qualsiasi esito negativo non sarebbe falsificabile.

6. Un esperimento mentale: un blackout e tre realtà che interagiscono

Riprendo un esempio discusso nel corso. Immaginiamo un'interruzione dell'alimentazione elettrica in una grande città, accompagnata dalla circolazione di informazioni contrastanti sulle cause e sui tempi del ripristino. Alcuni servizi passano a modalità di emergenza; altri dipendono da infrastrutture e fornitori che non si trovano nello stesso territorio. Nel frattempo si diffondono ricostruzioni, indiscrezioni e narrazioni che possono modificare la fiducia dei cittadini e le decisioni degli operatori. **È uno scenario didattico ipotetico**, non la descrizione di un evento storico determinato.

La prima realtà è *materiale*. Bisogna capire quali funzioni siano degradate, quali riserve esistano, quali sistemi siano effettivamente dipendenti dall'energia, quali soglie e tempi non siano superabili. Non tutti i servizi sono esposti allo stesso modo e non tutte le connessioni producono una cascata. Le alternative devono essere valutate rispetto alla loro reale attivabilità, non soltanto alla loro presenza nominale nei piani.

La seconda realtà è *organizzativa*. Soggetti diversi osservano segmenti del fenomeno: gestori delle reti, servizi essenziali, amministrazioni, operatori logistici, strutture sanitarie, forze di sicurezza. Le priorità possono essere legittimamente differenti e i poteri di intervento distribuiti. La qualità della risposta dipenderà anche dalle interfacce che collegano segnale, decisione, autorizzazione e azione. Avere un piano per ogni ente non equivale a possedere una capacità coordinata per l'insieme.

La terza realtà è *informativa e cognitiva*. Una notizia errata può alterare aspettative e comportamenti; una comunicazione tardiva può accrescere l'incertezza anche se è corretta; un annuncio troppo sicuro può minare la credibilità se il ripristino richiede più tempo del previsto. Ma non ogni voce falsa è una campagna ostile, né ogni cambiamento di comportamento è causato da disinformazione. Occorre osservare la catena concreta fra esposizione alle informazioni, interpretazione, condotta ed effetto operativo.

Proviamo ora a immaginare tre situazioni differenti. Nella prima le autorità dispongono di informazioni affidabili, ma le risorse disponibili non possono sostenere tutte le funzioni: domina il vincolo di capacità. Nella seconda esistono possibilità di intervento, ma una dipendenza critica non è stata riconosciuta e la risposta viene indirizzata al problema sbagliato: domina il limite di orientamento. Nella terza la perturbazione iniziale è contenibile, ma le reazioni simultanee di più soggetti assorbono le riserve condivise e moltiplicano le interferenze: è plausibile un meccanismo di amplificazione sistemica. I tre esiti richiedono diagnosi e rimedi differenti.

Potrebbe poi emergere un'azione intenzionale di manipolazione dell'informazione. L'ipotesi va esaminata senza anticipare la conclusione: quale contenuto è stato diffuso, da chi, attraverso quali canali, con quale coordinamento documentabile e con quali effetti effettivamente osservati? La protezione del servizio può procedere anche mentre tali domande restano aperte. Il valore

dell'esercizio non sta nell'indovinare un avversario, ma nel mostrare quanto cambino le decisioni quando separiamo il sistema fisico, la rete delle responsabilità e le rappresentazioni degli attori.

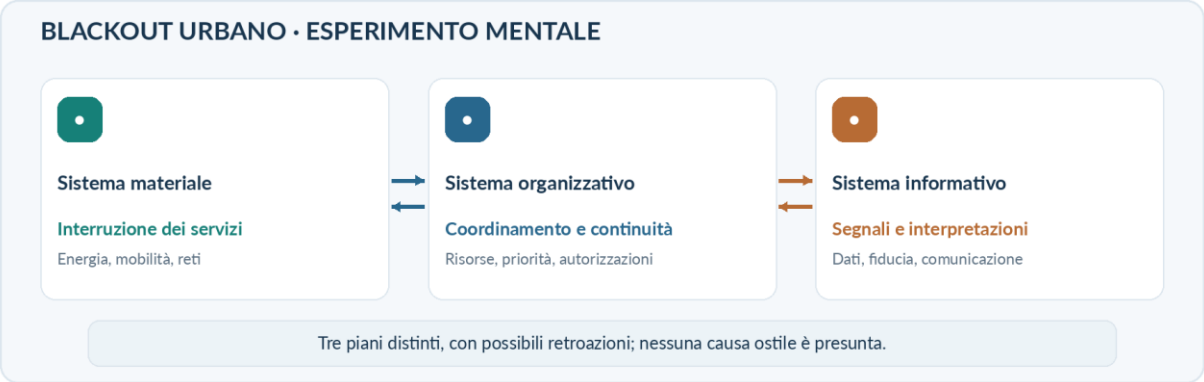


Figura 3 — Nel blackout ipotetico interagiscono dimensioni materiali, organizzative e informative.

7. Orientamento, OODA e autorità di agire

John Boyd ha elaborato una riflessione strategica sul rapporto fra Observe, Orient, Decide e Act, pubblicata anche nei materiali raccolti postumi nel volume curato da Grant T. Hammond. Non si tratta di una prescrizione semplicistica a percorrere quattro caselle il più rapidamente possibile. L'orientamento filtra ciò che osserviamo, come attribuiamo significato ai dati e quali opzioni riconosciamo. Un processo molto rapido, ma fondato su ipotesi errate, può aggravare il problema. Il trasferimento di questa lettura dalla strategia militare alla governance di organizzazioni civili è qui un'analogia metodologica, non un risultato sperimentale. (Boyd, 2018)

Nei sistemi organizzativi possiamo distinguere tre possibili colli di bottiglia. Il primo è nell'osservazione: un segnale rilevante è assente, poco affidabile o tardivo. Il secondo è nell'orientamento: il segnale esiste, ma il modello attribuisce al fatto una spiegazione inadeguata. Il terzo è nell'intervento: il problema è compreso, ma la sequenza di decisioni, autorizzazioni e mobilitazione delle risorse supera il tempo disponibile. Nella pratica questi problemi si combinano; il vantaggio analitico nasce dal non confonderli.

La distinzione richiama, per analogia, osservabilità e controllabilità nella teoria del controllo. Nei modelli matematici tali termini hanno definizioni tecniche dipendenti dalla rappresentazione adottata; qui li uso nel senso operativo di poter ricavare informazioni pertinenti e poter attivare azioni efficaci. Conoscere una condizione non implica possedere le risorse, l'autorità e il tempo per modificarla. La teoria della regolazione di Ashby ispira il ragionamento sui limiti della risposta, ma non fornisce direttamente un indice di «governabilità» delle istituzioni o dei sistemi sociali. (Ashby, 1956)

Questa lettura apre un raccordo con il Mission Command, discusso nel corso. La dottrina statunitense ADP 6-0 associa l'iniziativa disciplinata a intento del comandante, competenza, fiducia reciproca, comprensione condivisa, ordini orientati alla missione e assunzione consapevole del rischio. Richiamarla permette di discutere il rapporto fra autonomia e tempi di risposta, senza sovrapporre dottrine o attribuire a questo memo indicazioni ufficiali per l'Esercito italiano. In termini organizzativi, deleghe e autonomia hanno valore soltanto quando sono accompagnate da obiettivi, risorse, responsabilità e criteri d'intervento effettivamente chiari. (Department of the Army, 2019)

Le organizzazioni dovrebbero quindi esercitarsi non solo a «prendere la decisione corretta», ma anche a riconoscere il momento nel quale occorre cambiare domanda: non più «come eseguiamo il piano?», bensì «quale sua ipotesi non vale più, quali opzioni restano e chi può attivarle?». È qui che il governo del rischio diventa capacità di orientamento.

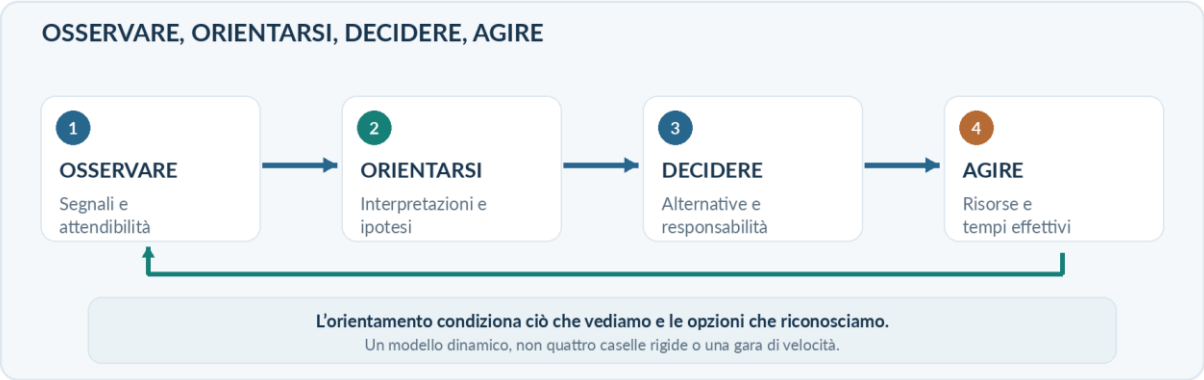


Figura 4 — Il ciclo OODA richiama la necessità di aggiornare continuamente l'orientamento.

8. Dalla previsione alla robustezza e all'adattamento

L'analisi del rischio tradizionale conserva pienamente la sua utilità quando le incertezze sono rappresentabili, le relazioni pertinenti sono sufficientemente conosciute e le stime possono essere motivate. La complessità non giustifica l'abbandono dei metodi probabilistici, né l'incertezza profonda è un alibi per rinunciare all'analisi. Cambia, piuttosto, la domanda da porre ai modelli. Se non possiamo stabilire con affidabilità quale futuro si realizzerà, possiamo cercare di capire in quali condizioni una scelta rimarrebbe accettabile e in quali fallirebbe. (Chapman e Ward, 2003; Marchau et al., 2019)

Per questa riflessione distinguo tre proprietà correlate ma non intercambiabili. La robustezza riguarda il mantenimento di prestazioni accettabili in condizioni differenti; la resilienza comprende, secondo la terminologia UNDRR, la capacità di resistere, assorbire, adattarsi, trasformarsi e recuperare preservando o ripristinando funzioni essenziali; l'adattabilità enfatizza la possibilità di modificare un percorso decisionale mentre il futuro si manifesta. La distinzione ha fini operativi, non introduce tre categorie universalmente disgiunte. Riserve e ridondanze possono comportare costi, il recupero non equivale sempre al ritorno allo stato iniziale e un'opzione adattiva può arrivare quando il tempo utile è già esaurito. (UNDRR, 2017; Marchau et al., 2019)

Il *Robust Decision Making* propone di esplorare una pluralità di futuri plausibili, individuare le condizioni nelle quali una strategia fallisce e cercare alternative meno vulnerabili. Il *Dynamic Adaptive Planning* collega il piano a ipotesi portanti, osservazioni e risposte contingenti. I *Dynamic Adaptive Policy Pathways* permettono di ragionare su percorsi alternativi e sui punti oltre i quali una politica o una scelta non soddisfa più i propri obiettivi. Sono approcci documentati, con presupposti e campi d'impiego propri: la loro applicazione a una specifica organizzazione deve essere proporzionata al problema. (Lempert, 2019; Walker, Marchau e Kwakkel, 2019; Haasnoot, Warren e Kwakkel, 2019)

È importante non confondere signpost, trigger e adaptation tipping point. Nella pianificazione adattiva i signpost sono variabili o segnali monitorati, mentre i trigger sono soglie o eventi associati all'attivazione di azioni preparate in anticipo. Un adaptation tipping point è una condizione oltre la quale l'attuale politica o strategia non soddisfa più gli obiettivi prefissati: non coincide necessariamente con un punto fisicamente irreversibile. Per essere efficace, un trigger deve consentire di decidere e agire prima che la prestazione diventi inaccettabile, tenendo conto del tempo necessario all'attivazione. (Walker, Marchau e Kwakkel, 2019; Haasnoot, Warren e Kwakkel, 2019)

Resilienza e adattamento hanno un costo. Ridondanze, scorte, fornitori alternativi, addestramento, deleghe e monitoraggi assorbono risorse oggi; il loro beneficio dipende dagli scenari futuri e dalla concreta possibilità di impiegarli. Non propongo di moltiplicare indiscriminatamente le riserve, né di

sottoporre ogni decisione a una modellazione complessa. Propongo di rendere esplicito che cosa stiamo proteggendo, contro quali condizioni, con quali costi e con quale possibilità di ripensare la scelta.



Figura 5 — Robustezza, resilienza e adattabilità rispondono a esigenze distinte e complementari.

9. Un metodo proporzionato: sette passaggi da integrare nei processi esistenti

Per tradurre queste distinzioni in una conversazione operativa propongo una sequenza di sette passaggi. Non è una procedura standardizzata, una norma di Project Management o una metodologia già validata; è una griglia di domande da confrontare con i processi di Risk Management, le responsabilità di comando e i piani di continuità esistenti. Il valore aggiunto deve essere misurato sui problemi che aiuta a riconoscere e sulle decisioni che modifica, considerando anche tempi, costi e risorse richiesti dall'analisi.

1. **Inquadrare.** Individuare le funzioni essenziali, gli obiettivi, le soglie non negoziabili, l'orizzonte temporale e la decisione che deve essere sostenuta. Senza una funzione definita, anche «vulnerabilità» e «resilienza» rimangono parole generiche.
2. **Rappresentare.** Ricostruire le dipendenze critiche, comprese quelle esterne; distinguere interfacce materiali, informative, istituzionali e decisionali; rendere esplicite le ipotesi su cui si fonda il quadro del contesto.
3. **Identificare.** Formulare scenari di rischio collegando perturbazioni, vulnerabilità del sistema esposto, percorsi di propagazione e conseguenze. Separare i fatti dall'ipotesi che una condotta sia intenzionale; considerare anche possibilità favorevoli quando pertinenti agli obiettivi.
4. **Valutare.** Scegliere tecniche e livelli di approfondimento proporzionati alla qualità delle informazioni, alla reversibilità delle scelte e alla gravità delle conseguenze. Esaminare spiegazioni alternative e condizioni nelle quali l'interpretazione potrebbe non valere.
5. **Progettare risposte.** Valutare prevenzione, protezione, ridondanza, capacità di recupero, flessibilità e adattamento; associare ogni risposta a risorse, tempi, autorizzazioni e responsabilità realmente disponibili.
6. **Monitorare e decidere.** Sorvegliare le assunzioni decisive e i segnali capaci di invalidarle, definendo in anticipo quali condizioni avviano un riesame, quale livello assume la decisione e quale azione può essere attuata prima della soglia critica.
7. **Apprendere.** Verificare che cosa hanno prodotto gli interventi, quali ipotesi erano errate, quali capacità hanno funzionato e quali modifiche concrete vadano apportate a piani, interfacce, deleghe, riserve o esercitazioni.

Per una prima applicazione possono essere sufficienti quattro prodotti: una mappa selettiva delle dipendenze; un registro dei rischi collegato alle vulnerabilità e ai nessi rilevanti; una scheda delle alternative e dei tempi di attivazione; un elenco delle assunzioni da monitorare con responsabili e

trigger. Non serve produrre documenti aggiuntivi se non modificano una decisione. Nel confronto con la gestione ordinaria bisogna misurare tanto il vantaggio — nuove vulnerabilità riconosciute, opzioni preservate, tempi di risposta migliorati — quanto il costo analitico e organizzativo.



Figura 6 — Schema sintetico dei sette passaggi proposti nel memo, da sperimentare e confrontare.

10. Resilienza nazionale: le interfacce sono una capacità strategica

Quando parliamo di resilienza nazionale, il livello di analisi cambia. Non consideriamo soltanto un progetto o un'organizzazione, ma un insieme di sistemi tecnici, istituzioni, comunità e operatori economici con autorità, vincoli e responsabilità differenti. Nessun soggetto possiede una rappresentazione completa dell'insieme né il potere di modificarne unilateralmente tutte le parti. La capacità di governo dipende allora anche dalla qualità delle interfacce fra sistemi autonomi.

Un'infrastruttura strategica può essere tecnicamente protetta ma dipendere da forniture specialistiche, comunicazioni, autorizzazioni esterne o capacità di riparazione concentrate. La continuità delle sue funzioni richiede quindi di ricostruire dipendenze pertinenti e possibili cause comuni, anche fuori dal perimetro dell'organizzazione. Il quadro JRC/Hybrid CoE aiuta a individuare i domini e le vulnerabilità potenzialmente coinvolti nelle minacce ibride; il NASA Systems Engineering Handbook sostiene l'attenzione a interfacce e confini di sistema. Nessuno dei due documenti fornisce, da solo, una stima della probabilità di crisi per il caso concreto. (JRC/Hybrid CoE, 2021; NASA, 2016)

La cooperazione civile-militare e interistituzionale presenta una sfida analoga: condividere informazioni non significa automaticamente condividere significato, priorità o possibilità d'azione. Può essere più utile concordare in anticipo quali funzioni devono essere preservate, quali soglie richiedono coordinamento, chi riceve i segnali e quali decisioni spettano a ciascuno, piuttosto che costruire un flusso informativo vastissimo privo di un destinatario operativo.

Le misure di resilienza devono inoltre rispettare legittimità, competenze e proporzionalità. Una soluzione tecnicamente efficace può non essere giuridicamente consentita; una scelta utile a un ente può trasferire conseguenze inaccettabili ad altri soggetti. Il problema non è cancellare le differenze di mandato, ma renderle visibili prima della crisi e verificare che i raccordi previsti funzionino davvero. Il linguaggio sistemico aiuta a riconoscere queste dipendenze senza pretendere di sostituire le regole e le responsabilità delle istituzioni.

11. Cinque domande che porterei in una esercitazione

Una riflessione diventa utile quando cambia ciò che un'organizzazione si domanda prima di prendere una decisione. Per questo, se dovessi trasformare il memo in un'esercitazione, partirei da cinque quesiti, ciascuno riferito a una funzione concreta e a un orizzonte temporale definito.

Quale funzione non possiamo permetterci di perdere? Non basta indicare «energia», «mobilità» o «comunicazioni». Dobbiamo precisare il servizio richiesto, la prestazione minima, il periodo nel quale deve essere assicurato e le persone o attività che ne dipendono. Gli indicatori devono descrivere anche le capacità residue, non soltanto la prestazione corrente.

Da che cosa dipendiamo senza governarlo? Occorre mettere alla prova le dipendenze esterne e le cause comuni: un secondo fornitore condivide in realtà il medesimo impianto? Una riserva dipende dalla stessa rete che dovrebbe sostituire? Le risorse sono disponibili entro il tempo utile? Una mappa può essere semplice, purché espliciti le interfacce che contano.

Quale ipotesi del nostro piano potrebbe smettere di valere? La domanda richiede di nominare le assunzioni, indicare un segnale che potrebbe smentirle e stabilire chi lo esaminerà. Un segnale non è utile se non esiste una decisione che possa essere rivista quando esso si manifesta.

Se vedessimo il problema in tempo, potremmo realmente agire? La risposta deve attraversare l'intera catena: riconoscimento, interpretazione, autorizzazione, mobilitazione, attuazione e verifica. Una misura prevista sulla carta, ma non attivabile entro la soglia critica, non costituisce una capacità di risposta effettiva.

Come sapremmo di avere imparato? Dopo una prova non basta raccogliere osservazioni. Occorre verificare se sono cambiate una delega, un'interfaccia, una riserva, una soglia di monitoraggio o una procedura, e ripetere la prova per accertare che la modifica abbia prodotto l'effetto atteso. Una *lesson learned* senza una capacità nuova rischia di essere soltanto un documento archiviato.

Le domande possono essere utilizzate in progetti civili, organizzazioni pubbliche e attività di preparazione alla crisi. Non attribuiscono al singolo responsabile poteri che non possiede: al contrario, rendono riconoscibili in anticipo i problemi che richiedono decisioni a un livello superiore.

12. Che cosa resta da dimostrare

La coerenza di una spiegazione non basta a renderla vera. Cibernetica, dinamica dei sistemi, gestione del rischio, strategia e decisioni in condizioni di incertezza profonda offrono contributi distinti e riconoscibili. Non esistono però, nelle fonti qui utilizzate, verifiche empiriche indipendenti della loro specifica integrazione nei due meccanismi proposti o della nozione di «caos operativo». La distinzione è essenziale in un ambito come la guerra ibrida, nel quale spiegazioni persuasive e attribuzioni di intenzionalità possono essere formulate con un grado di certezza superiore a quello consentito dalle evidenze.

La prima ipotesi da verificare è che la ricostruzione delle interdipendenze permetta, in alcuni casi, di identificare e trattare vulnerabilità non adeguatamente riconosciute da un'analisi dei rischi condotta separatamente per eventi. Servono cronologie, dati sulle relazioni, conoscenza delle alternative e confronti con metodi ordinari. Occorre cercare anche casi nei quali la prospettiva sistemica non abbia aggiunto informazioni decisive.

La seconda riguarda l'utilità di distinguere degrado osservativo, interpretativo e operativo per spiegare la perdita di governabilità. Bisognerebbe ricostruire quando i segnali erano disponibili, quando sono stati interpretati, chi disponeva dei poteri di risposta e quanto tempo restava prima della perdita della funzione. Non ogni decisione tardiva deriva da cattivo orientamento; non ogni fallimento poteva essere evitato con informazioni migliori.

La terza è l'eventuale utilità aggiuntiva del concetto di «caos operativo». Per giustificarne l'adozione dovremo mostrare che distingue fenomeni e condizioni decisionali che definizioni più semplici non

distinguono sufficientemente. Dovremo formulare osservazioni capaci di smentire il modello, non selezionare soltanto esempi favorevoli.

La quarta questione riguarda il valore concreto dell'integrazione metodologica. Su casi comparabili occorrerebbe stabilire prima dell'analisi quali vulnerabilità e decisioni valutare, applicare un processo ordinario di riferimento e confrontarlo con la griglia proposta. Il confronto dovrebbe considerare tempestività, qualità delle alternative riconosciute, prestazioni delle funzioni essenziali e costi aggiuntivi di informazione, coordinamento e analisi. Un maggior numero di rischi identificati o una ricostruzione retrospettiva più ricca non dimostrano, da soli, che siano state prese decisioni migliori. La sperimentazione dovrebbe comprendere anche casi nei quali il metodo non offre un beneficio riconoscibile.

Queste questioni non indeboliscono la riflessione: ne definiscono il confine di attendibilità. Una proposta aperta alla confutazione è più utile di una formula che pretenda di spiegare qualsiasi crisi. Condividere questo memo significa anche chiedere ai lettori di individuare errori, controesempi e condizioni nelle quali le distinzioni proposte non funzionano.

13. Una conclusione aperta

Se dovessi riassumere in una sola frase la lezione che porto con me dopo il corso, sceglierei questa: **non basta proteggere il funzionamento di un sistema; bisogna proteggere anche la capacità di comprenderlo e di intervenire quando cambia.** Gli eventi possono colpirne i componenti, le interdipendenze possono moltiplicarne gli effetti e le decisioni possono aggravare o contenere la perturbazione. Ma l'esito dipende anche dalla qualità del nostro orientamento e dalle opzioni che abbiamo avuto la lungimiranza di conservare.

La guerra ibrida rende particolarmente evidente questa esigenza, perché le pressioni possono attraversare domini differenti, sfruttare vulnerabilità pregresse e influenzare le rappresentazioni dei soggetti coinvolti. La stessa esigenza esiste però anche senza un avversario: ogni grande sistema interdipendente può perdere capacità di governo quando continua a ragionare con ipotesi superate o scopre troppo tardi di non possedere più alternative praticabili.

È su questo terreno che vedo un incontro fertile fra ingegneria dei sistemi, analisi di contesto, Risk Management, capacità organizzative e cultura della resilienza. Non credo serva sostituire i metodi consolidati con un lessico nuovo. Serve applicarli con consapevolezza dei loro limiti, integrarli dove il problema lo richiede e imparare a riconoscere quando bisogna cambiare rappresentazione e risposta.

Mi piacerebbe che questa nota diventasse un'occasione di confronto con chi ha esperienza diretta di sistemi, operazioni e decisioni in condizioni difficili. Le obiezioni più utili non saranno quelle rivolte alle parole, ma quelle fondate su casi concreti: situazioni nelle quali una dipendenza era stata sottovalutata, un segnale non era stato interpretato, una risposta non era realmente attivabile oppure, al contrario, un'organizzazione aveva mantenuto le proprie funzioni nonostante l'incertezza. Da quelle esperienze possiamo imparare a formulare domande migliori e, forse, a costruire sistemi più governabili.

Riferimenti scientifici e istituzionali

- Ashby, W. R. (1956). *An Introduction to Cybernetics*. Chapman & Hall.
- Boyd, J. R. (2018). A Discourse on Winning and Losing. A cura di G. T. Hammond. Air University Press. Fonte online
- Chapman, C., e Ward, S. (2003). *Project Risk Management: Processes, Techniques and Insights*. Wiley.

- Consiglio dell'Unione europea (2026). Conclusioni sul rafforzamento della capacità dell'UE di contrastare le minacce ibride, 16 marzo 2026, doc. 7349/26. Fonte online
- Department of the Army (2019). ADP 6-0, Mission Command: Command and Control of Army Forces, 31 luglio 2019, cap. 1. Fonte online
- Giannopoulos, G., Smith, H., e Theocharidou, M. (a cura di) (2021). The Landscape of Hybrid Threats: A Conceptual Model (Public Version). JRC123305, EUR 30585 EN. Joint Research Centre e Hybrid CoE, Commissione europea. DOI: 10.2760/44985. Fonte online
- Haasnoot, M., Warren, A., e Kwakkel, J. H. (2019). *Dynamic Adaptive Policy Pathways*. In Marchau et al. (a cura di), *Decision Making under Deep Uncertainty*. Springer. DOI: 10.1007/978-3-030-05252-2_4.
- Holland, J. H. (1992). *Complex Adaptive Systems*. *Daedalus*, 121(1), 17–30.
- Kurtz, C. F., e Snowden, D. J. (2003). *The New Dynamics of Strategy*. *IBM Systems Journal*, 42(3), 462–483. DOI: 10.1147/sj.423.0462.
- Lempert, R. J. (2019). *Robust Decision Making*. In Marchau et al. (a cura di), *Decision Making under Deep Uncertainty*. Springer. DOI: 10.1007/978-3-030-05252-2_2.
- Lorenz, E. N. (1963). Deterministic Nonperiodic Flow. Journal of the Atmospheric Sciences, 20(2), 130–141. DOI: 10.1175/1520-0469(1963)020<0130:DNF>2.0.CO;2.
- Marchau, V. A. W. J., Walker, W. E., Bloemen, P. J. T. M., e Popper, S. W. (a cura di) (2019). *Decision Making under Deep Uncertainty: From Theory to Practice*. Springer. DOI: 10.1007/978-3-030-05252-2.
- NASA (2016). NASA Systems Engineering Handbook. NASA/SP-2016-6105 Rev. 2. Fonte online
- NASA (2026). NASA Handbook for Models and Simulations: An Implementation Guide for NASA-STD-7009B. NASA-HDBK-7009B, 3 febbraio 2026. Fonte online
- NATO (2026). Countering Hybrid Threats, pagina istituzionale aggiornata il 29 gennaio 2026. Fonte online
- Rodrigues, A. G. (2001). Managing and Modelling Project Risk Dynamics: A System Dynamics-Based Framework. 4th European PMI Conference, London. Fonte online
- Snowden, D. J., e Boone, M. E. (2007). *A Leader's Framework for Decision Making*. *Harvard Business Review*, 85(11), 68–76.
- Walker, W. E., Marchau, V. A. W. J., e Kwakkel, J. H. (2019). *Dynamic Adaptive Planning*. In Marchau et al. (a cura di), *Decision Making under Deep Uncertainty*. Springer. DOI: 10.1007/978-3-030-05252-2_3.
- UNDRR (2017). Terminology on Disaster Risk Reduction — Resilience. United Nations Office for Disaster Risk Reduction. Fonte online