militär AKTUELL

05.11.2025

PREVENZIONE INVECE DI PANICO: COME UNA DIFESA COMPLETA

In caso di attacco, non sono solo le qualità militari a determinare il successo della difesa. Almeno altrettanto importanti sono la resilienza e la volontà di difendersi della popolazione.

RAFFORZARE LA RESILIENZA

In "Deutschland im Ernstfall" (La Germania in caso di emergenza), Ferdinand Gehringer e Johannes Steger analizzano come la politica e la società possono reagire alle minacce militari. In un'intervista con Militär Aktuell affermano: l'importante non è il panico, ma la prevenzione e una comunicazione aperta con la popolazione.

Intervista: MARKUS SCHAUTA

La guerra in Ucraina costringe l'Europa a prepararsi all'emergenza. Numerosi scenari ipotizzano che un possibile attacco da parte della Russia inizi come una guerra ibrida: disinformazione, attacchi informatici e sabotaggio di infrastrutture critiche come le reti elettriche e di telecomunicazione sono considerati uno scenario iniziale realistico. La conseguenza: un'interruzione di corrente su larga scala. Supermercati e stazioni di servizio chiudono, i frigoriferi smettono di funzionare. Senza scorte di cibo e acqua, si verificano saccheggi. Il panico e il caos si diffondono, facilitando l'avanzata delle forze armate russe.

Ferdinand Gehringer e Johannes Steger analizzano come la Germania, e con essa altri Stati dell'UE, possano prepararsi a tali scenari nel loro libro "Deutschland im Ernstfall" (La Germania in caso di emergenza), pubblicato a settembre. Una conversazione sui punti deboli, la prevenzione e la comunicazione politica.

Signor Gehringer, lei descrive scenari di un attacco alla Germania. Quali punti deboli nella vita quotidiana – ad esempio nell'approvvigionamento, nella comunicazione o nelle infrastrutture – emergerebbero per primi secondo lei? I problemi in Austria sarebbero simili?

Gehringer: Quale punto debole nella vita quotidiana emergerebbe per primo dipende dalla situazione concreta. L'approvvigionamento, la comunicazione e le infrastrutture non sono di per sé punti deboli, ma lo diventano se ci affidiamo ciecamente alla loro disponibilità. I rischi maggiori risiedono solitamente in ciò che diamo per scontato, come la comunicazione digitale e l'approvvigionamento. Se Internet, i cellulari o l'approvvigionamento di merci smettono di funzionare, se ne avverte subito l'effetto.

Quanto tempo ci vorrebbe?

Gehringer: Le reti di comunicazione possono crollare in poche ore, così come le catene di approvvigionamento. Se poi si aggiunge il panico, la situazione si aggrava. Per questo è importante essere

preparati: concordare in famiglia i punti di incontro, l'assistenza ai bambini o la cura dei familiari se la comunicazione digitale non funziona. Siamo abituati al “su richiesta”: supermercato dietro l'angolo, cellulare sempre a disposizione. Ma sono proprio le prime 72 ore a essere decisive: una buona preparazione dei cittadini alleggerisce il carico delle autorità, che possono così concentrarsi sui compiti più urgenti.

E l'Austria...

Gehringer: ...avrebbe problemi simili: forte digitalizzazione, catene di approvvigionamento interconnesse, elevata dipendenza dalle reti energetiche e di dati. Le differenze riguardano piuttosto la scala: le dimensioni della Germania rendono le strutture più complesse, mentre l'Austria è più compatta e forse più facile da controllare. In linea di principio, le vulnerabilità sono simili in entrambi i paesi.

Nel suo libro lei scrive di un possibile sabotaggio dell'apparato politico, che potrebbe essere attaccato nel corso di una guerra (ibrida) e subire un guasto totale. Come si svilupperebbe uno scenario del genere?

Gehringer: Uno scenario del genere potrebbe svilupparsi gradualmente. Inizialmente, ad esempio, gli attacchi informatici colpirebbero l'infrastruttura digitale dei ministeri, del parlamento e delle autorità, mentre parallelamente campagne di disinformazione potrebbero minare la fiducia nella capacità di azione della politica. Informazioni riservate verrebbero rese pubbliche e singoli decisori potrebbero essere messi alla gogna. Si diffonderebbe una maggiore sfiducia nelle decisioni del governo. Informazioni sensibili potrebbero anche essere rese pubbliche da autori interni all'apparato politico. Queste potrebbero avere un effetto simile.

E nella fase successiva?

Gehringer: Le reti governative centrali potrebbero essere disturbate. La comunicazione crollerebbe e i processi decisionali si bloccherebbero. Soprattutto a livello regionale e comunale verrebbero prese decisioni contraddittorie. Ciò causerebbe ulteriore incertezza nella popolazione, probabilmente anche all'interno dell'apparato politico, e potrebbe infine avere un impatto negativo sui nostri alleati.

Quale sarebbe, secondo lei, il passo più importante che la Germania dovrebbe intraprendere immediatamente per non essere colta di sorpresa e sopraffatta in caso di emergenza?

Steger: La sorpresa è un concetto molto importante in questo contesto. Chi è sorpreso è colui o colei che non si aspettava affatto una determinata cosa. Ne consegue logicamente, nella maggior parte dei casi, una sensazione di sopraffazione. La grande difficoltà consiste nel riconoscere o accettare l'emergenza come tale e, cosa molto importante, comunicarla immediatamente. Esistono scenari con attacchi diretti ai soldati tedeschi in cui l'emergenza diventa ovviamente “realtà”. Ma ci sono anche sviluppi che non rendono immediatamente chiara l'emergenza. Molti attacchi ibridi diversi, combinati e in parte sovrapposti. La nostra architettura di sicurezza in Germania probabilmente non sarebbe in grado di collegare rapidamente questi elementi.

Ciò significa che spetta alle autorità e alla politica garantire una maggiore resilienza in questo ambito?

Steger: In ogni caso, un primo passo deve essere una comunicazione coerente e consistente da parte della politica e delle autorità. Chi sa come viene valutata una situazione di sicurezza, ad esempio, è meno sorpreso quando si verifica un incidente. Inoltre, in questo modo le persone sono messe in grado di prendere decisioni informate e responsabili. I rapporti annuali di servizi come l'Ufficio federale per la

protezione della Costituzione o l'Ufficio federale di polizia criminale sono documenti eccellenti per affrontare la questione. Purtroppo la loro portata rimane limitata, quindi sono necessari nuovi formati per informare la popolazione in modo sereno e tempestivo. A tal fine, occorre dare più fiducia ai cittadini: le risposte che non vengono fornite perché potrebbero creare insicurezza nella popolazione dovrebbero diventare l'eccezione.

Ma come si può promuovere la resilienza in un'UE i cui Stati membri non hanno vissuto la guerra da quasi otto decenni?

Steger: La Finlandia, la Svezia e i Paesi baltici non hanno vissuto la guerra per molto tempo. Tuttavia, la resilienza della società finlandese nel suo complesso viene spesso citata come esempio. Il Paese non ha dimenticato la guerra d'inverno del 1939/40 contro l'Unione Sovietica. La situazione è simile nelle nazioni baltiche. Non dobbiamo cadere nella trappola, come nel caso dell'amministrazione digitale, di fare confronti che ricordano un po' la metafora delle mele e delle pere. L'Estonia non è la Germania, ma è comunque possibile imparare e tradurre alcuni approcci. Lo scambio mirato di best practice sarebbe in questo caso un approccio paneuropeo. Standard, sostegno reciproco e condivisione delle risorse possono costituire le basi della resilienza europea.

In che misura gli Stati confinanti sarebbero colpiti da un attacco alla Germania e quali dinamiche potrebbe innescare a livello europeo?

Gehringer: Un attacco alla Germania sarebbe automaticamente un attacco alla stabilità europea. Un'emergenza per e in Germania avrebbe conseguenze immediate per tutti i paesi confinanti. Non rimarrebbe limitata al territorio tedesco, poiché le interconnessioni geografiche, economiche e infrastrutturali creano strette dipendenze. La NATO e l'UE sarebbero immediatamente coinvolte, con aree di schieramento e rifornimento nei paesi confinanti. La logistica verrebbe militarizzata e diventerebbe essa stessa bersaglio di ricognizione, attacchi informatici e sabotaggi. Molti Stati dell'UE stanno discutendo la creazione di un Consiglio di sicurezza nazionale o di strutture simili.

Sarebbe ipotizzabile un equivalente europeo che mantenga una visione d'insieme in caso di crisi?

Gehringer: L'idea di un Consiglio di sicurezza europeo sembra interessante a prima vista, proprio perché gli attacchi ibridi e, in alcuni casi, anche le escalation militari nell'UE non avrebbero confini chiari. Tuttavia, è necessario distinguere tra gestione operativa delle crisi e capacità decisionale strategica.

In che modo?

Gehringer: Esistono già strutture UE come il meccanismo di risposta politica integrata alle crisi (IPCR), il Centro europeo di raccolta e analisi delle informazioni (EU INTCEN) o il Centro di risposta alle crisi del Servizio europeo per l'azione esterna. Queste piattaforme raccolgono informazioni e creano quadri della situazione. Tuttavia, manca loro qualcosa di fondamentale...

Vale a dire?

Gehringer: Il potere politico necessario per prendere decisioni vincolanti in caso di emergenza. Un Consiglio di sicurezza europeo toccherebbe quindi la questione centrale: gli Stati membri sono disposti a cedere a Bruxelles la loro sovranità in materia di sicurezza e difesa? Un tale organo sarebbe in grado di agire solo se prendesse decisioni giuridicamente vincolanti in caso di crisi. Si potrebbe ipotizzare un modello a più livelli:

un Consiglio come piattaforma di coordinamento con valutazione costante della situazione e collegamento con la NATO, nonché un “gabinetto di crisi dell'UE” con competenze di emergenza chiaramente definite.

Quanto è realistico questo scenario secondo lei?

Gehringer: Al momento non è realistico. Non mi aspetto che si prendano decisioni in tal senso nel prossimo futuro. Forse un giorno l'Europa riorganizzerà la sicurezza, e allora tali impulsi sarebbero degni di discussione.