avenir dibattito

Politica di sicurezza: quali prospettive per la Svizzera?

Strategie concrete a salvaguardia del Paese

Gli spostamenti sullo scacchiere geopolitico e gli sviluppi sia sociali che tecnologici stanno generando nuove incertezze ovunque nel mondo, e pertanto anche in Europa. Il clima è esacerbato anche dalla guerra della Russia contro l'Ucraina nell'Europa dell'est. L'ultima pubblicazione di Avenir Suisse tenta di inquadrare quali siano le ripercussioni degli attuali avvenimenti per la politica di difesa svizzera. Gl'investimenti nella sicurezza vanno definiti con maggior precisione in funzione dei nuovi modelli di minaccia. La collaborazione transazionale deve essere rafforzata e bisogna migliorare le capacità di contrastare gli attacchi informatici.

L'invasione dell'Ucraina da parte della Russia e lo scoppio di un conflitto armato tra due Nazioni rappresentano una cesura nell'ordine europeo del dopoguerra. Già da tempo, tuttavia, si assiste a una forma «ibrida» di conflitti, affrancata dallo schema bellico vero e proprio. L'effetto protettivo del contesto geografico e politico della Svizzera si sta indebolendo.

I rischi cui è esposto il nostro Paese oggi non possono essere controllati con il solo impiego di mezzi militari: stiamo parlando di cyberattacchi (di origine criminale), pandemie, situazioni critiche nell'approvvigionamento di energia elettrica, un crollo della rete di telefonia mobile o attacchi terroristici (con droni). Gli scenari non convenzionali come la pirateria informatica a infrastrutture militari o comunque critiche assumono crescente importanza rispetto alle minacce armate di carattere tradizionale. Questo è quanto evidenzia l'ultimo studio di Avenir Suisse sulle prospettive della politica svizzera di sicurezza, firmato da Lukas Rühli e Lisa Rogenmoser.

Indirizzare in modo più mirato gl'investimenti nella difesa alle nuove minacce

A dispetto delle nuove minacce che si stanno profilando, nel quadro del rinnovo completo del materiale in dotazione, per il decennio a venire la gran parte degl'investimenti dell'esercito è destinata all'acquisto di mezzi convenzionali. Per incrementare la difesa informatica è invece prevista una parte relativamente modesta del budget.

Considerate la complessità e l'eterogeneità delle minacce, in qualità di piccolo Stato la Svizzera deve affrontare la sfida di prepararsi in modo adeguato a difendersi da ogni pensabile tipo di attacco. Invece di richiedere unicamente un aumento degli stanziamenti, occorre anche adottare un atteggiamento più pragmatico verso gl'inevitabili compromessi. Assumono crescente importanza la valutazione lucida della situazione e un'allocazione delle risorse che tenga maggiormente conto delle priorità in termini di minacce attuali e verosimili per il futuro.

Un conflitto convenzionale su suolo elvetico rimane poco plausibile. Se si arrivasse a tanto, la minaccia interesserebbe quasi sicuramente tutto il centro Europa, e non soltanto la Svizzera. Bisogna quindi annettere un'accresciuta importanza all'aspetto della cooperazione transnazionale.

Rotbuchstrasse 46
CH-8037 Zurigo
T + 41 44 445 90 00
kommunikation@avenir-suisse.ch
www.avenir-suisse.ch

Esponiamo di seguito le nostre cinque tesi sull'ulteriore sviluppo della difesa nazionale svizzera:

- Per quanto riguarda gl'investimenti previsti nel rinnovo e potenziamento delle forze terrestri la Svizzera dovrebbe considerare con maggior coerenza le probabili minacce future. Non vanno trascurati mezzi leggeri e mobili per contrastare minacce non convenzionali.
- Gli aerei da combattimento del tipo F-35A sono concepiti specificatamente per essere impiegati all'interno di un'alleanza (la Nato). Per sfruttare appieno il loro potenziale occorre rafforzare la cooperazione militare transnazionale, ad esempio partecipando ad esercitazioni della Nato. Gli aspetti legati alla nostra politica di neutralità vanno pertanto chiariti.
- La cybersicurezza in Svizzera dev'essere aumentata, sia nell'esercito che nelle infrastrutture critiche. Nella difesa da attacchi informatici non bellici, le forze armate dovrebbero mantenere un ruolo sussidiario. Per la gestione delle infrastrutture critiche la Confederazione dovrebbe prescrivere ridondanze di sistema, soluzioni di backup e obblighi di notifica (in caso di cyberattacchi).
- Le eventuali carenze a livello di competenze, ad es. nelle unità meccanizzate, potrebbero essere compensate con un'accresciuta cooperazione militare transazionale.
- Per il previsto dialogo sulle capacità con il Parlamento, l'esercito dovrebbe creare maggior trasparenza nella valutazione della situazione e presentare le ipotesi di minaccia nel modo più dettagliato possibile.

Modelli internazionali

In termini di politica di sicurezza, le strategie adottate da altri Paesi europei potrebbero fornire spunti interessanti per la Svizzera. Il Regno Unito prevede ad esempio di spostare le priorità dai mezzi robusti come i carri armati pesanti verso tecnologie come la difesa informatica e i droni dotati di intelligenza artificiale. La Finlandia e la Svezia mostrano che per contrastare le minacce di tipo convenzionale i Paesi piccoli e neutrali, rispettivamente non allineati, devono impostare le proprie strategie di difesa su una maggior cooperazione transazionale. In caso di emergenza, la difesa più efficiente è prodotta all'interno di un'alleanza, per cui queste capacità vanno esercitate e rafforzate in anticipo.

Mediante una strategia che assegna le risorse agli strumenti di politica della sicurezza secondo le necessità e in base alle minacce e ai rischi effettivi, la Svizzera sarà in grado di garantire una protezione efficace della popolazione anche in un futuro segnato da maggiori incertezze.

Conferenza stampa con live-streaming: venerdì 25 marzo 2022, ore 10.00.

Pubblicazione: Perspektiven der Sicherheitspolitik – Realitätsbezogene Strategien zum Schutz der Schweiz. Lukas Rühli e Lisa Rogenmoser, 72 pagine, consultabile online a partire dalle ore 6.00.

Ulteriori informazioni: Lukas Rühli, *lukas.ruehli@avenir-suisse.ch*, (+41 76 211 23 50); Lisa Rogenmoser, *lisa.rogenmoser@avenir-suisse.ch*, (+41 79 530 61 31)