Il Non-paper del Ministro della Difesa Guido Crosetto: l'Italia di fronte alla Guerra Ibrida (pdf)

Pubblicato il 19/11/2025

Durante la riunione del Consiglio Supremo di Difesa è stato presentato il "Non-paper sul contrasto alla guerra ibrida" redatto dal **Ministro della Difesa Guido Crosetto**, documento che evidenzia come l'Italia si trovi oggi in un contesto caratterizzato da attività multidominio condotte da attori ostili con modalità che non superano la soglia del conflitto armato tradizionale.

Alla riunione erano presenti il **Presidente della Repubblica Sergio Mattarella**, la **Presidente del Consiglio dei Ministri Giorgia Meloni**, il **Ministro degli Affari Esteri e della Cooperazione Internazionale Antonio Tajani**, il **Ministro delle Imprese e del Made in Italy Adolfo Urso** e il **Capo di Stato Maggiore della Difesa Generale di Corpo d'Armata Luciano Portolano**.

Nel corso della presentazione, il Ministro della Difesa Guido Crosetto ha illustrato un quadro in cui gli attacchi non riguardano esclusivamente infrastrutture e sistemi, ma interessano in modo significativo anche il dominio informativo e la percezione pubblica. Il documento sottolinea come la dimensione cognitiva rappresenti oggi un elemento essenziale della sicurezza nazionale, poiché attività mirate possono incidere sulla stabilità istituzionale e sulla fiducia collettiva.

Il “Non paper” riunisce analisi tratte da fonti aperte, contributi dell’intelligence e informazioni raccolte in ambito internazionale, ed è destinato ai Presidenti della Camera dei Deputati e del Senato della Repubblica.

Gli attori ostili e le vulnerabilità italiane: dal dominio cognitivo a quello cibernetico

Il documento individua quattro principali attori in grado di condurre attività ibride contro l’Italia e gli altri Paesi occidentali: **la Federazione Russa**, **la Repubblica Popolare Cinese**, **la Repubblica Islamica dell’Iran** e **la Repubblica Popolare Democratica di Corea**.

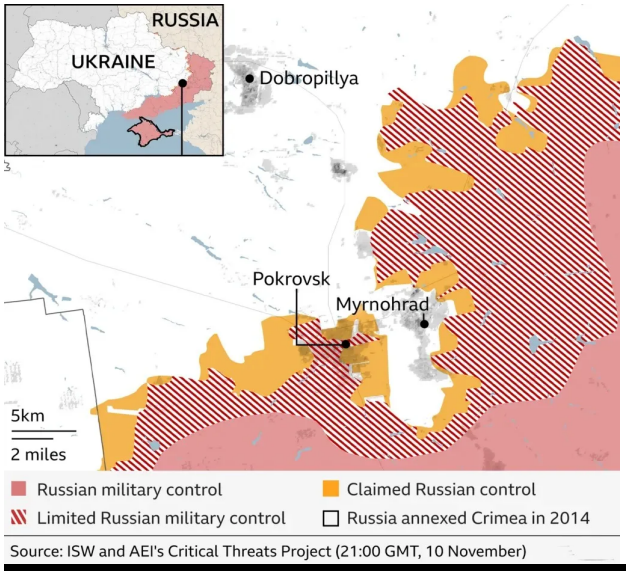
La **Federazione Russa** impiega un insieme articolato di strumenti, tra cui operazioni informative, pressione economica, attività nel cyberspazio e supporto a gruppi affiliati in grado di condurre azioni non direttamente attribuibili. Il conflitto in Ucraina ha consolidato l’uso di tecniche volte a influenzare il quadro europeo senza generare escalation militare.

La **Repubblica Popolare Cinese** adotta una strategia “multi-vettoriale”, basata sulla combinazione di leve economiche, tecnologiche e informative. Le dipendenze europee da materie prime strategiche — come terre rare, gallio e germanio — sono indicate come elementi particolarmente sensibili. L’Italia presenta un grado di dipendenza dall’importazione di tali materiali superiore alla media UE.

La **Repubblica Islamica dell’Iran** opera tramite una rete di attori regionali e attraverso iniziative che interessano aree ad alta rilevanza strategica, tra cui i principali choke points marittimi. La posizione geografica dell’Italia, fortemente legata ai traffici commerciali del Mediterraneo e del Canale di Suez, rende necessaria una sorveglianza continua delle dinamiche di sicurezza regionali.

La **Repubblica Popolare Democratica di Corea** mantiene un apparato cibernetico molto attivo, impiegato per attività di ransomware, spionaggio digitale e sottrazione di risorse nel cyberspazio.

Il documento evidenzia inoltre alcune vulnerabilità nazionali: la dipendenza energetica dall'estero, la concentrazione di infrastrutture critiche sul territorio italiano e la crescente esposizione ai fenomeni di disinformazione. Secondo i dati dell'Agenzia per la Cybersicurezza Nazionale, nel 2024 si sono registrati **1.979 eventi cyber** e **573 incidenti con impatto confermato**, con un aumento rispetto al 2023. Nel primo semestre 2025 è stato rilevato un ulteriore incremento. I settori sanitario e manifatturiero risultano tra i più interessati.



Vertice NATO Bruxelles (ottobre 2024), discussione sulle minacce ibride. Fonte: Ministero della Difesa.

Una sezione specifica del documento analizza anche le potenziali interferenze nei processi democratici, rese possibili dall'evoluzione delle tecniche di manipolazione informativa, tra cui deepfake e micro-targeting. Tale dinamica richiede un rafforzamento della cooperazione tra istituzioni nazionali ed europee, in particolare durante le consultazioni elettorali.

Costruire una postura proattiva: strumenti nazionali e cooperazione internazionale

Il "Non paper" propone di rafforzare la resilienza nazionale come elemento centrale nella risposta alle minacce ibride. La resilienza viene definita in un'accezione ampia, includendo aspetti tecnologici, istituzionali, economici e informativi.

Sul piano internazionale, il documento richiama le iniziative in corso in ambito **NATO**, **Unione Europea** e **G7**. La NATO ha aggiornato la propria strategia per il contrasto alle minacce ibride, potenziando gli strumenti di supporto cibernetico e rafforzando la presenza sul fianco Sud. L'Unione Europea ha ampliato il proprio quadro normativo in materia di sicurezza digitale grazie alla NIS2, al Cyber Resilience Act e al Digital Services Act, mentre organismi come ENISA ed ECCC contribuiscono al consolidamento delle capacità operative comuni. Anche il G7, estendendo il mandato del Rapid Response Mechanism alla coercizione economica, ha mostrato una crescente attenzione verso il carattere multidimensionale della minaccia.

Foto di gruppo del Vertice G7 dei Ministri della Difesa (Napoli, ottobre 2024). Fonte: Ministero della Difesa

Sul piano nazionale, il documento presentato dal **Ministro della Difesa Guido Crosetto** delinea una serie di interventi strutturali. Tra questi figurano:

- la creazione di una **Arma Cyber civile-militare**, attiva in modo continuativo e dotata di personale altamente qualificato;
- l'istituzione di un **Centro nazionale per il Contrasto alla Guerra Ibrida**, incaricato di coordinare analisi, risposte e cooperazione tra amministrazioni, imprese e mondo accademico;
- la promozione di una **cultura nazionale della sicurezza**, volta a consolidare la consapevolezza collettiva e a migliorare la capacità di riconoscere e mitigare le attività ibride.

Il documento conclude sottolineando come tali iniziative non rappresentino solo una risposta tecnica alle nuove forme di minaccia, ma costituiscano un passo decisivo verso una postura più moderna, integrata e preparata del sistema Paese. Le proposte avanzate dal Ministro della Difesa Guido Crosetto definiscono un percorso chiaro: consolidare la protezione delle infrastrutture critiche, rafforzare la capacità di prevenzione e risposta nel dominio cyber, migliorare il coordinamento istituzionale e ampliare le competenze specialistiche.

Nella visione delineata dal Ministro, l'Italia può dotarsi di uno strumento organico e altamente qualificato, capace non solo di fronteggiare le attività ibride, ma anche di anticiparle. Il progetto di una Arma Cyber e la creazione di un centro nazionale dedicato costituiscono, in questo senso, un investimento strategico a lungo termine, volto a garantire continuità operativa, deterrenza e un livello di protezione adeguato alla complessità dello scenario attuale.

Nel suo insieme, l'impianto proposto rappresenta un'evoluzione significativa della postura nazionale: un modello che integra prevenzione, analisi, risposta e cooperazione internazionale, offrendo al Paese una capacità di protezione più solida e coerente con le sfide emergenti.

non-paper_il_contrasto_alla_guerra_ibridaDownload

Link notizia: https://www.difesa.it/assets/allegati/83696/non-paper_il_contrasto_alla_guerra_ibrida.pdf