

La Guerra Ibrida Spiegata: Tattiche, Storia e La Sfida per la NATO

Pubblicato il 13/12/2025

La Guerra Ibrida (Hybrid Warfare) è emersa come una caratteristica distintiva dei conflitti del XXI secolo, ridefinendo il modo in cui gli stati perseguono i loro obiettivi strategici. Non è una guerra dichiarata, ma una complessa miscela di strumenti convenzionali e non convenzionali volti a sfruttare le vulnerabilità di un avversario, spesso rimanendo **al di sotto della soglia di un conflitto aperto**.

Definizione e Obiettivo

La Guerra Ibrida si riferisce all'**uso coordinato di molteplici strumenti di potere – sia militari che non militari – per raggiungere obiettivi strategici, rendendo difficile l'attribuzione e ritardando la risposta dell'avversario**.

- **Il "Grey Zone" (Zona Grigia):** La Guerra Ibrida prospera in questo spazio, l'area tra la pace e il conflitto dichiarato, dove le azioni sono ambigue e non innescano

automaticamente i meccanismi di difesa formali (come l'Articolo 5 della NATO).

- **Obiettivo:** Destabilizzare e minare la coesione e la fiducia nelle istituzioni di una società bersaglio.

La **NATO** definisce le minacce ibride come "**una combinazione ampia, complessa e adattiva di mezzi convenzionali e non convenzionali, inclusa la forza militare, gli attacchi informatici, la disinformazione, la coercizione economica e le operazioni per procura (proxy operations)**".

Elementi Fondamentali della Guerra Ibrida

Questa strategia si basa su un vasto kit di strumenti, che spaziano dal digitale al fisico:

Elemento	Descrizione	Esempi Contemporanei
Disinformazione e Operazioni di Informazione	Diffusione di narrazioni false o distorte per manipolare l'opinione pubblica, esacerbare le divisioni sociali e minare la fiducia nelle istituzioni democratiche.	Interferenza russa nelle elezioni, campagne di propaganda sui social media.
Cyber Attacchi	Attacchi informatici mirati alle infrastrutture critiche (reti elettriche, comunicazioni, trasporti) per creare caos e interrompere le operazioni governative.	Attacchi a reti governative o interruzione di forniture energetiche.
Coercizione Economica	Uso di sanzioni, embarghi commerciali o dipendenze energetiche (ad esempio, la fornitura di gas) per esercitare pressione politica sugli avversari.	Sfruttare le dipendenze energetiche europee da un fornitore specifico.
Forze Proxy e Irregolari	Sfruttamento di milizie, gruppi di mercenari (come il Gruppo Wagner) o movimenti ribelli per agire per conto di uno Stato, garantendo una plausibile negabilità.	Il sostegno a separatisti armati o l'uso di "omini verdi" senza insegne.
Sabotaggio Fisico	Attacchi mirati ad asset fisici come magazzini, fabbriche o infrastrutture militari per punire o interrompere il sostegno all'avversario.	Tentati incendi dolosi o atti di sabotaggio contro infrastrutture logistiche e militari in Europa.

Case Study: La Russia come Attore Principale

La Russia è l'esempio contemporaneo più citato nell'uso della Guerra Ibrida contro la NATO e l'Europa:

- **Annessione della Crimea (2014):** Questa operazione è considerata un libro di testo di Guerra Ibrida, che ha combinato l'uso di forze militari sotto copertura ("omini verdi"), una intensa campagna di disinformazione e manipolazione politica locale.

- **Campagna in Europa:** La Russia mantiene legami con **numerose organizzazioni di estrema destra** e fornisce loro supporto finanziario e incoraggiamento. Inoltre, inonda l'Europa di disinformazione per:
  - Sostenere partiti pro-russi.
  - Esacerbare tensioni preesistenti (ad esempio, sull'immigrazione).
  - **Minare la fiducia nelle elezioni** e nelle istituzioni democratiche.



La Guerra Ibrida Spiegata - Microsoft Threat Intelligence

Le Sfide per la NATO e la Risposta

La Guerra Ibrida complica la sicurezza collettiva perché non si adatta ai modelli tradizionali di risposta militare.

La Minaccia Potenziale

Se la guerra convenzionale in Ucraina dovesse rallentare, **la minaccia ibrida russa potrebbe aumentare**. Con le forze convenzionali indebolite, il Cremlino potrebbe intensificare i metodi ibridi – come sabotaggio, disinformazione e sostegno all'estremismo – per vendicarsi del supporto occidentale all'Ucraina.

Le Sfide Chiave

- **Dilemma dell'Attribuzione:** La natura oscura degli attacchi ibridi rende difficile stabilire chi sia l'autore, complicando la ritorsione.

- **Ambiguità Legale:** Gli attacchi ibridi spesso non raggiungono la soglia per invocare l'Articolo 5 (difesa collettiva) del Trattato NATO, richiedendo risposte che navigano in aree legali grigie.
- **Coordinamento Civile-Militare:** Poiché la Guerra Ibrida colpisce la coesione sociale e le infrastrutture civili, una risposta puramente militare è insufficiente.



La Guerra Ibrida Spiegata: Tattiche, Storia e La Sfida per la NATO

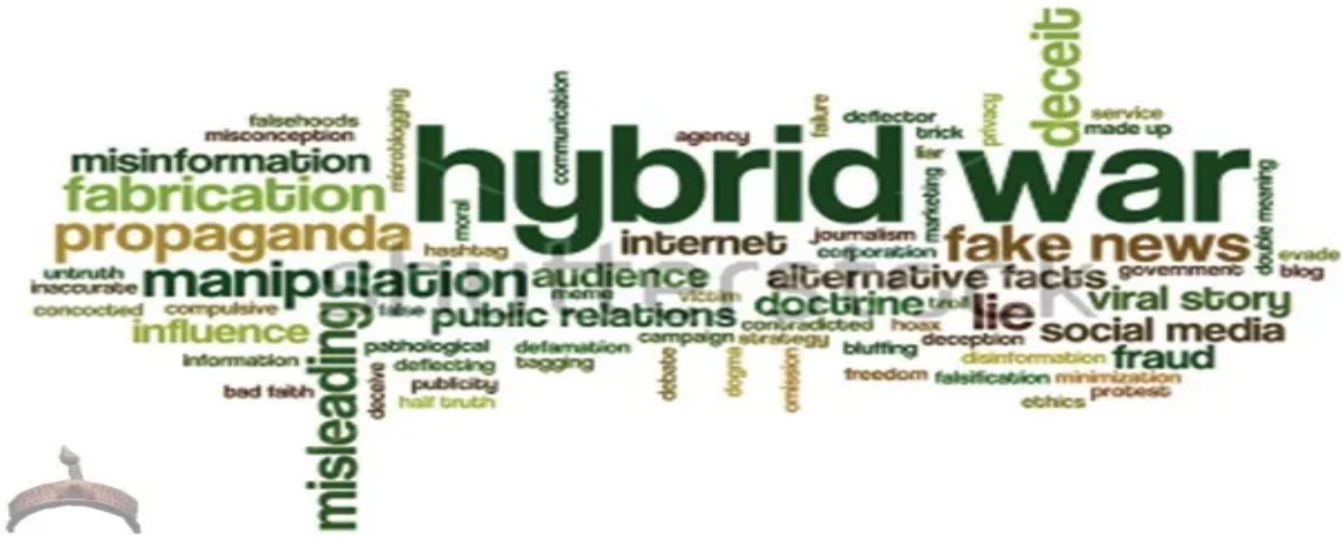
La Strategia NATO: Preparazione, Deterrenza e Difesa

La NATO ha una strategia per affrontare queste minacce, incentrata su diversi pilastri:

1. **Migliorare la Consapevolezza Situazionale:**
    - Migliore integrazione dei servizi segreti nazionali nell'Alleanza per una condivisione più rapida delle informazioni.
    - Il **Joint Intelligence and Security Division** della NATO e i suoi rami di analisi ibrida lavorano per rilevare e attribuire l'attività ibrida.
2. **Rafforzare la Resilienza (Resilience):**
    - Investire nella preparazione della società civile per attacchi informatici, interruzioni di corrente e sabotaggi. Paesi come la **Finlandia**, ad esempio, hanno estesi piani per la preparazione civile, inclusi **50.500 rifugi** sparsi per il paese.
    - Migliorare le opzioni di difesa informatica e la protezione delle infrastrutture critiche.

3. **Deterrenza e Risposta:**
    - La NATO ha pubblicamente dichiarato che le azioni ibride contro uno o più Alleati **potrebbero portare all'invocazione dell'Articolo 5**.
    - Sono stati creati **Counter-Hybrid Support Teams** per fornire assistenza mirata agli Alleati che ne fanno richiesta per prepararsi e rispondere alle attività ibride.
4. **Cooperazione con Partner:**
    - Il rafforzamento della cooperazione con l'**Unione Europea** (UE) è vitale, in particolare nella difesa informatica, nelle comunicazioni strategiche e nelle esercitazioni.
    - Centri di eccellenza, come il **Centro Europeo di Eccellenza per il Contrasto alle Minacce Ibride** a Helsinki, forniscono competenze e conoscenze specialistiche.

La Guerra Ibrida continuerà ad evolversi, integrando l'intelligenza artificiale (AI) e le tecnologie **deepfake** per seminare confusione e minare il comando e controllo. È essenziale che le democrazie occidentali rimangano adattabili e investano in una difesa che sia al tempo stesso militare e civile.



La Guerra Ibrida Spiegata: Tattiche, Storia e La Sfida per la NATO

Link notizia: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats