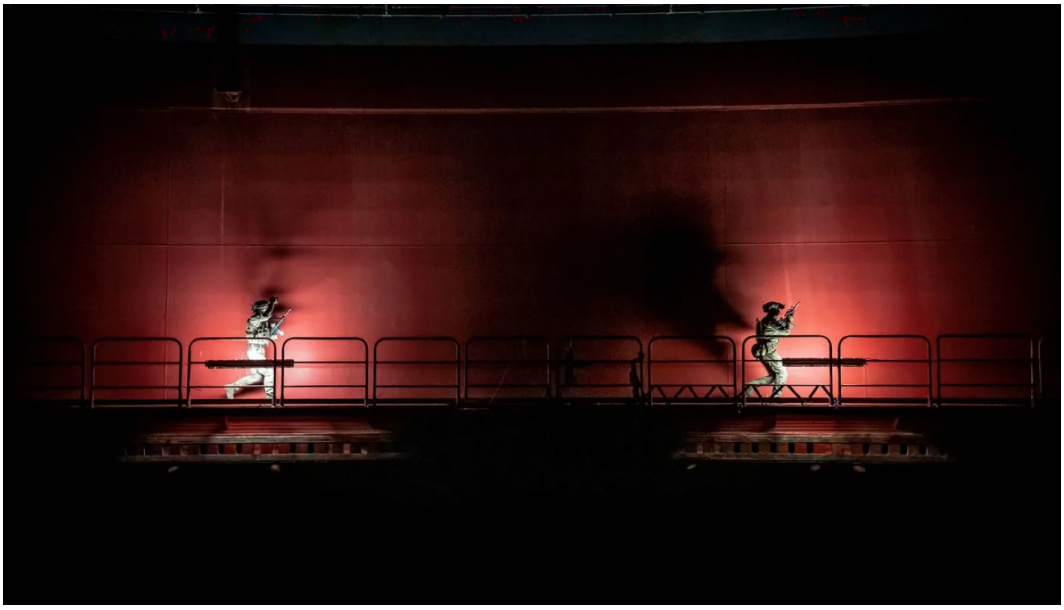


Hybrid Warfare Explained: Tactics, History, and the Challenge for NATO

Published on 13/12/2025

Hybrid Warfare has emerged as a defining feature of 21st-century conflicts, redefining how states pursue their strategic objectives. It is not a declared war, but a complex blend of conventional and unconventional tools aimed at exploiting an adversary's vulnerabilities, often remaining **below the threshold of open conflict**.

Definition and Objective

Hybrid Warfare refers to the **coordinated use of multiple power tools – both military and non-military – to achieve strategic objectives, making attribution difficult and delaying the adversary's response**.

- **The "Grey Zone":** Hybrid Warfare thrives in this space, the area between peace and declared conflict, where actions are ambiguous and do not automatically trigger formal defense mechanisms (such as NATO's Article 5).

- **Objective:** To destabilize and undermine the cohesion and trust in the institutions of a target society.

NATO defines hybrid threats as "**a broad, complex, and adaptive combination of conventional and unconventional means, including military force, cyberattacks, disinformation, economic coercion, and proxy operations**".

Fundamental Elements of Hybrid Warfare

This strategy relies on a vast toolkit, ranging from digital to physical:

Element	Description	Contemporary Examples
Disinformation and Information Operations	Spreading false or distorted narratives to manipulate public opinion, exacerbate social divisions, and undermine trust in democratic institutions.	Russian interference in elections, propaganda campaigns on social media.
Cyber Attacks	Cyberattacks targeting critical infrastructure (power grids, communications, transport) to create chaos and disrupt government operations.	Attacks on government networks or disruption of energy supplies.
Economic Coercion	Use of sanctions, trade embargoes, or energy dependencies (e.g., gas supply) to exert political pressure on adversaries.	Exploiting European energy dependencies on a specific supplier.
Proxy and Irregular Forces	Exploitation of militias, mercenary groups (like the Wagner Group), or rebel movements to act on behalf of a state, ensuring plausible deniability.	Support for armed separatists or the use of "little green men" without insignia.
Physical Sabotage	Targeted attacks on physical assets like warehouses, factories, or military infrastructure to punish or disrupt support for the adversary.	Attempted arson or sabotage acts against logistical and military infrastructure in Europe.

Case Study: Russia as a Key Actor

Russia is the most cited contemporary example in the use of Hybrid Warfare against NATO and Europe:

- **Annexation of Crimea (2014):** This operation is considered a textbook example of Hybrid Warfare, combining the use of undercover military forces ("little green men"), an intense disinformation campaign, and local political manipulation.
- **Campaign in Europe:** Russia maintains ties with **numerous far-right organizations** and provides them with financial support and encouragement. Additionally, it floods Europe with disinformation to:
    - Support pro-Russian parties.
    - Exacerbate pre-existing tensions (e.g., on immigration).
    - **Undermine trust in elections** and democratic institutions.

Hybrid Warfare Explained - Microsoft Threat Intelligence

The Challenges for NATO and the Response

Hybrid Warfare complicates collective security because it does not fit traditional military response models.

The Potential Threat

If conventional warfare in Ukraine were to slow down, **the Russian hybrid threat could increase**. With weakened conventional forces, the Kremlin might intensify hybrid methods –

such as sabotage, disinformation, and support for extremism – to retaliate against Western support for Ukraine.

Key Challenges

- **Attribution Dilemma:** The obscure nature of hybrid attacks makes it difficult to establish who is responsible, complicating retaliation.
- **Legal Ambiguity:** Hybrid attacks often do not reach the threshold to invoke NATO's Article 5 (collective defense), requiring responses that navigate legal grey areas.
- **Civil-Military Coordination:** Since Hybrid Warfare targets social cohesion and civilian infrastructure, a purely military response is insufficient.

Hybrid Warfare Explained: Tactics, History, and the Challenge for NATO

NATO Strategy: Preparedness, Deterrence, and Defense

NATO has a strategy to address these threats, centered on several pillars:

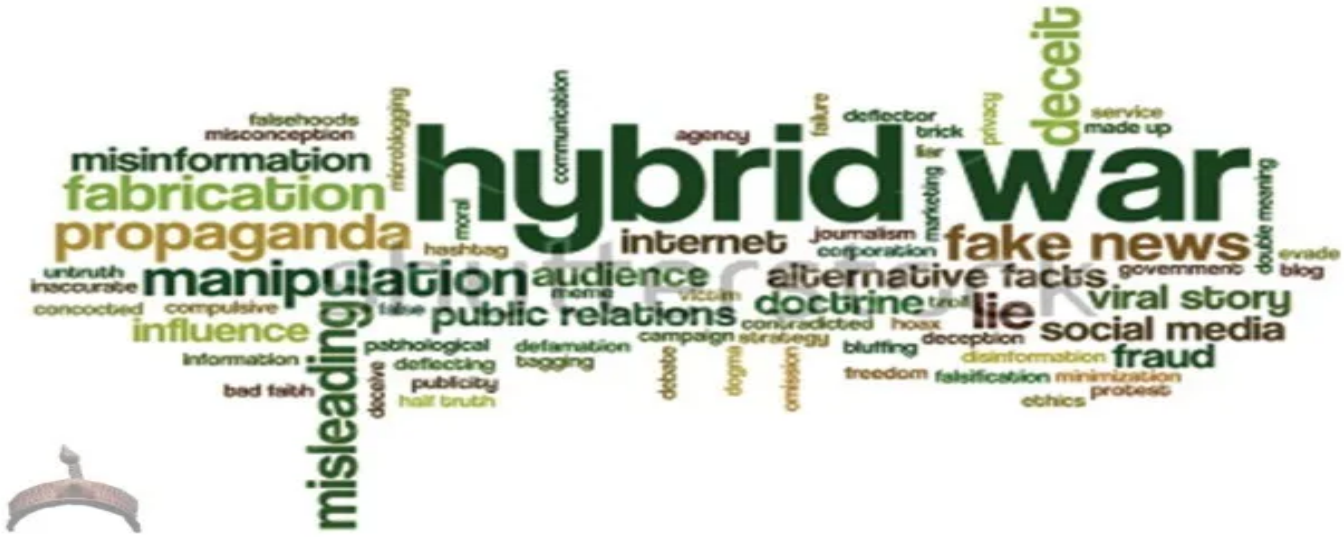
1. **Enhancing Situational Awareness:**
   - Better integration of national intelligence services within the Alliance for faster information sharing.
   - NATO's **Joint Intelligence and Security Division** and its hybrid analysis branches work to detect and attribute hybrid activity.
2. **Strengthening Resilience:**

- Investing in civil society preparedness for cyberattacks, power outages, and sabotage. Countries like **Finland**, for example, have extensive civil preparedness plans, including **50,500 shelters** scattered across the country.
- Improving cyber defense options and protection of critical infrastructure.

3. **Deterrence and Response:**
   - NATO has publicly stated that hybrid actions against one or more Allies **could lead to the invocation of Article 5**.
   - **Counter-Hybrid Support Teams** have been created to provide targeted assistance to Allies requesting it to prepare for and respond to hybrid activities.

4. **Cooperation with Partners:**
   - Strengthening cooperation with the **European Union** (EU) is vital, particularly in cyber defense, strategic communications, and exercises.
   - Centers of excellence, such as the **European Centre of Excellence for Countering Hybrid Threats** in Helsinki, provide expertise and specialist knowledge.

Hybrid Warfare will continue to evolve, integrating artificial intelligence (AI) and **deepfake** technologies to sow confusion and undermine command and control. It is essential that Western democracies remain adaptable and invest in a defense that is both military and civilian.



Hybrid Warfare Explained: Tactics, History, and the Challenge for NATO

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