

# The Fine Memo 5



## Understanding Hybrid War

# Introduction — A War That Doesn't Speak Its Name

Hybrid warfare has become one of the central forms of contemporary conflict. It is based neither on an official declaration of war, nor on massive and visible military confrontations, but on a **combination of coordinated actions**, carried out below the threshold of armed conflict, aimed at weakening an adversary without triggering a frontal response.

In this type of war, **perception, confusion and attrition** matter as much as military might. Russia has made this approach a structuring pillar of its strategy, particularly against Western democracies, which it considers to be vulnerable in informational, social and political terms.

## 1. What is Hybrid Warfare? An operational definition

Hybrid warfare can be defined as the **simultaneous and coordinated** use of military, non-military and paramilitary means in order to create a favourable balance of power, without crossing the classic thresholds of declared war.

It combines in particular:

- **indirect or covert** military actions,
- **cyber operations** (espionage, sabotage, pre-positioning),
- informational **campaigns** (disinformation, manipulation, propaganda),
- **economic and energy pressures**,
- **acts of sabotage or intimidation** that are difficult to attribute.

The objective is not necessarily territorial conquest, but the **gradual disorganization** of the adversary.

## 2. Why democracies are prime targets

Democratic regimes have several structural vulnerabilities:

- a strong dependence on **public trust**,
- an open information space,
- regular election cycles,
- increased sensitivity to social and economic crises.

Hybrid warfare exploits precisely these characteristics. It seeks less to convince than to **disorient**, less to impose a narrative than to **undermine all certainty**, by installing permanent doubt.

In this logic, truth matters less than confusion, and the repetition of contradictory narratives becomes a weapon in itself.

## 3. The main tools of hybrid warfare

### Cyberspace

- Long-term strategic espionage
- Prepositioning in critical networks
- Potential sabotage of infrastructure (energy, health, transport)
- Difficulty of attribution that limits traditional deterrence

### Information

- Dissemination of polarizing narratives
- Exploitation of existing social divides

- Artificial amplification of controversies
- Saturation of the media space

### **Economy and energy**

- Blackmail on supplies
- Market destabilization
- Instrumentalization of structural dependencies

### **Collective psychology**

- Installation of a feeling of powerlessness
- Erosion of trust in the state
- Democratic fatigue and civic disengagement

## **4. The grey zone: the heart of hybrid warfare**

Hybrid warfare is part of what is known as the **grey zone**, i.e. the intermediate space between peace and war.

In this area:

- the aggression is real but legally unclear,
- the response is politically risky,
- The attribution is often questionable.

It is precisely this ambiguity that allows the aggressor to retain the strategic initiative.

## **5. Why Naming Hybrid War Is Already a Strategic Act**

Not naming hybrid warfare amounts to:

- to endure it passively,
- let the opponent impose his tempo,
- delay institutional responses.

Conversely, **explaining, documenting and making visible** this form of conflict makes it possible to:

- to raise the level of collective vigilance,
- strengthen democratic resilience,
- reduce the effectiveness of hostile operations.

Pedagogy then becomes a defence tool in its own right.