



GAZ Hybrid - Germany: Hybrid Warfare Becomes a Strategic Priority

Published on 27/06/2026

Germany takes a decisive step in redefining its national security. With the official inauguration in Berlin of the **Gemeinsames Zentrum zur Abwehr hybrider Bedrohungen** (the [joint center GAZ Hybrid](#)), located at the facilities of the Bundesamt für Verfassungsschutz in Berlin-Treptow, the German government responds in a structured way to the growing threats in the "gray zone" of international confrontation.

The new platform will serve to coordinate intelligence, police forces (federal and state), cybersecurity (*BSI*), and territorial authorities. The goal? **"Coordination instead of competence conflicts"**, to timely address espionage, sabotage, disinformation campaigns, and the use of so-called "disposable agents" (*Wegwerf-Agenten*), often unaware pawns manipulated by foreign intelligence services, primarily Russian and Chinese.

Beyond Traditional Conflict: Network Protection

The initiative reflects an irreversible transformation in Western security strategies. Threats are no longer limited to the classic military level but affect civil society and the economy.

For Germany, the continent's main industrial power, the protection of critical infrastructures has become an essential component of national security:

- **Energy and water networks**
- **Logistics systems, ports, and railways**
- **Telecommunications and data centers**
- **Research centers and strategic industries**

Moscow observes these developments with great suspicion. Russian authorities have long claimed that the West uses economic and media tools as strategic pressure, interpreting the strengthening of European structures as part of a containment strategy. This deep divergence in perceptions continues to fuel a climate of growing mutual distrust.

The "Zeitenwende" and the Debt Brake Revolution

The establishment of the center is part of the broader process of strengthening European and NATO deterrence. But the real German turning point is of an economic-political nature.

After the extraordinary €100 billion fund announced in 2022, the Bundestag led by **Friedrich Merz** approved a historic reform of the *Schuldenbremse* (the constitutional debt brake), introducing a special exemption for national security expenses exceeding 1% of GDP. Thanks to this fiscal flexibility, sectors like military defense, civil protection, and cybersecurity now enjoy financial resources unimaginable until a few years ago.

The lesson from the conflict in Ukraine was clear: technological superiority alone is not enough if volumes are lacking. Modern wars consume ammunition, drones, and defense systems at a dizzying speed. For this reason, NATO is implementing a true **industrial revolution**.

*At the Hague summit, allies agreed on a new target of **5% of GDP allocated to security by 2035** (\$3.5%\$ for traditional military expenses and \$1.5%\$ for resilience, infrastructure, and cybersecurity). A shift accelerated by the partial strategic disengagement promoted by Donald Trump's United States.*

Vulnerability	Description and Impact
Dependence on Raw Materials	The production of advanced Western weapon systems still heavily depends on rare earths and components whose processing is monopolized by China .
Industrial Fragmentation	Unlike the standardized model of the United States, Europe continues to disperse billions of euros in numerous competing national programs, fragmenting research and development funds.
Political Sustainability	In Germany, the far-right party AfD consolidates support close to 30%. The growth of Eurosceptic and pro-Russian forces across the continent questions the political sustainability of long-term support for Ukraine and increased military spending.

The opening of the Berlin center marks the definitive farewell to decades in which Germany's strategic posture was based solely on export and commercial stability. Europe has steadily entered a new phase: the confrontation between powers is no longer played only with deployed armies but through the integrity of information flows, markets, and digital infrastructures.