Blog-Entry for EU Project Resonant

Link: https://resonantproject.eu/articles-2

G*(emeinsames)* ***A****(bwehr)* ***Z****(entrum)* ***Hybrid*** *– What the new German centre for countering hybrid threats is meant to deliver*

The Federal Republic of Germany is increasingly confronted with a security environment that can no longer be clearly and neatly distinguished between espionage, cyberattacks, disinformation, sabotage and economic pressure.

With the “Joint Centre for Countering Hybrid Threats”, abbreviated as **GAZ Hybrid**, Federal Minister of the Interior Alexander Dobrindt opened in Berlin on June 16th, 2026 a new cross-agency coordination unit that is intended to detect infiltration and (subversive) attacks by foreign states at an early stage and to coordinate necessary countermeasures more effectively and efficiently. The newly established centre complements the existing national, specialist security and defense centres.

The crucial point is this: **GAZ Hybrid** is not a new super-authority, but a joint working format of existing security authorities at the federal and state (“Länder”) level. Represented are:

- Bundesamt für Verfassungsschutz (Federal Office for the Protection of the Constitution)
- Bundespolizei (Federal Police)
- Bundesamt für Sicherheit in der Informationstechnik (BSI – Federal Office for Information Security)
- Bundesamt für den Militärischen Abschirmdienst (Federal Office of Military Counterintelligence)
- Bundesnachrichtendienst (Federal Intelligence Service)
- Generalzolldirektion (General Customs Directorate)
- Verfassungsschutz der Bundesländer (Constitution Protection authorities of the single federal states)

Organisationally, the centre is located at the *Bundesamt für Verfassungsschutz* in Berlin, which primarily assumes organisational responsibilities according to public statements, rather than acting as the sole decision-maker.

Why hybrid threats require a dedicated situational picture

Hybrid threats appear initially so inconspicuous and yet so dangerous because they link and exploit several layers simultaneously. A cyberattack on a public authority, a disinformation campaign in the run-up to an election, a drone flight over critical infrastructure or an attempted sabotage in logistics may at first glance look like isolated, unrelated incidents – but they are not.

Taken together, they can cause significantly more damage and form part of a strategy that undermines trust in the government, the economy and the liberal democratic order. Minister of the Interior Alexander Dobrindt described the objective of such attacks with the words: “Es geht schlicht darum, unser Land zu destabilisieren” (“The simple aim is to destabilise our country”)[1].

GAZ Hybrid has the task of making precisely these lines of connection visible for the security authorities and enabling them to take appropriate countermeasures.

What tasks/competencies will be assigned to GAZ Hybrid?

The most important task of GAZ Hybrid is a professional coordination. It is intended to collect, assess and consolidate information and translate it into a common situational picture. To this end, five working groups are envisaged:

1. Situation
2. Operational information exchange
3. Disinformation and influence operations
4. Economy
5. Analysis and reporting

This structure clearly shows that hybrid threats are not understood merely as a policing or intelligence problem, but also as a challenge relevant to economic security, democracy and cybersecurity.

The working group on the “Situation” is likely to be particularly important, as it must bring together indications from different organisational logics: Police forces primarily think in terms of threat prevention and law enforcement; intelligence services focus on pre-emptive intelligence gathering; the German Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security) concentrates on technical resilience and the cyber situation. If these perspectives are evaluated not only one after another but simultaneously, isolated suspicions can more quickly form a robust pattern, and reactive countermeasures can be initiated.

The working group on “Disinformation and influence operations” is directly linked to European debates on the increasingly important concept of *Foreign Information Manipulation and Interference* (**FIMI**).

The European Commission understands the fight against information manipulation as a combination of situational awareness, platform regulation, media freedom, societal resilience, digital literacy and cooperation with national authorities, fact-checkers, civil society, media and academia. This is precisely where an interface between internal security and the liberal democratic order lies: Government agencies must be able to detect and explain manipulation without politicising, for example, legitimate expressions of opinion or journalistic work.

---

[1] Alexander Dobrindt, Federal Minister of the Interior, at the opening of the Joint Counter-Hybrid Threats Centre, quoted in Antenne Münster/dpa: „Was soll das Gemeinsame Abwehrzentrum Hybrid bringen?“ (“What is the Joint Counter-Hybrid Threats Centre supposed to achieve?”)

The EU-funded Horizon project **RESONANT** fits seamlessly into this picture. **RESONANT** examines how state and non-state actors employ tactics, techniques and procedures of information suppression and **FIMI**, particularly targeting diaspora communities - an issue that has already been addressed in several other blog contributions in this forum.

Among other things, the **RESONANT** project aims to develop evidence based, methodological tools, policy recommendations, table-top exercises and a handbook on countering information suppression and **FIMI**.

From a normative perspective, an objective for Germany - using the newly established *Joint Centre for Countering Hybrid Threats* as an example - would be that **GAZ Hybrid** does not merely process national security information, but systematically incorporates European basic research, situational pictures and best practices.

Implications for cooperation among security authorities

The most immediate implication arises directly from the existing need: in the first instance, a denser exchange of information between the security authorities. Germany already has several joint defence centers, for example for terrorism, extremism and counter-drone measures; **GAZ Hybrid** now complements this architecture with a cross-cutting topic touching many areas of responsibility. The political ambition is summed up in the formula “Koordinierung statt Kompetenzgerangel” (“coordination instead of turf wars”)[2]. In practice, success will depend on whether authorities share findings early enough, whether the single federal states of Germany and the federal government use the same indicators, and whether joint assessments are translated into concrete protective measures.

A detailed catalogue of criteria does not exist yet. However, the federal government and the federal states have committed themselves, in their decisions on hybrid threats, to establishing central coordination and contact points (“Single Points of Contact”) and to aligning measures against disinformation and hybrid threats. **GAZ Hybrid** works in working groups that identify and assess espionage, sabotage, disinformation, transnational repression and state terrorism. Obvious indicators are used for this purpose; these are anchored primarily in internal situational pictures and specialist documents rather than in a publicly available criteria catalogue.

Second, the newly formed center will increase pressure to link technical, police and intelligence data more closely. This can improve response capabilities, for example when cyber indicators, travel movements, financial traces, social-media campaigns and physical sabotage hints fit together. At the same time, legal and data-protection tensions arise. Precisely because **GAZ Hybrid** is not an independent authority, it must remain clear for each piece of information which legal basis applies, who contributed it, who may further process it and when it must be deleted. Coordination

[2] Deutschlandfunk: „Gemeinsames Zentrum zur Abwehr hybrider Bedrohungen nimmt Arbeit in Berlin auf“ („Joint Centre for Countering Hybrid Threats begins operations in Berlin”), news broadcast of 16 June 2026, available online at www.deutschlandfunk.de (accessed 28 June 2026).

must not result in de facto erosion of clear delineations of responsibilities, wherever those are still required, and purpose limitations.

Third, cooperation with the private sector and operators of critical infrastructure is becoming increasingly important. The working group “Economy” within **GAZ Hybrid** is intended to progressively network authorities with companies, business-related actors and associations and to systematise joint work. This is both consistent and targeted, since many hybrid attacks initially hit private operators, platforms, logistics companies and critical infrastructures such as energy firms, research institutions or media organisations. Where reporting thresholds, contact points and situational formats are clearly defined, an incident at company level can more quickly become a national warning signal.

For critical infrastructures, sector-specific guidelines and strategies are already in place (for example, the “KRITIS strategy” of the Federal Ministry of the Interior, which addresses critical infrastructures whose disruption would severely affect essential services and public order). These documents outline threat scenarios and corresponding protective measures and, in some cases, define specific indicators, such as characteristic patterns of cyberattacks, sabotage, or disinformation.

Fourth, **GAZ Hybrid** is likely to change the culture of security authorities in the long term. Success will be measured less by whether a single authority concludes a case, and more by whether Germany identifies patterns early, clarifies responsibilities quickly and reacts in a coordinated, concerted way. This requires trust, common standards, robust IT interfaces and a culture that shares early-stage warnings before a case escalates publicly.

The challenge is therefore not only organisational, but also directed individually at every single employee. Security authorities and their staff must increasingly be made aware of the need to address hybrid threats as a cross-agency process rather than as isolated incidents.

Conclusion

GAZ Hybrid is certainly not a panacea against hybrid threats, but it is unquestionably a necessary step in a current situation in which attacks on democracy, infrastructure and public opinion interlock. Its strength does not lie in new powers, but in faster situational awareness, better information exchange, the use of already existing rules and laws, and a coordinated - or even concerted - response of all government(security) authorities. It will therefore be crucial whether the centre communicates findings to authorities at an early stage and establishes clear processes, transparent responsibilities and data-protection-compliant information flows.

This requires a shared framework of indicators and criteria that ensures that the resulting assessments are actually translated into concrete protective measures.

At the same time, experience shows that the weakness of such arrangements can lie precisely where many security institutions, many legal bases and many organisational logics generate new friction losses.

If coordination succeeds, **GAZ Hybrid** can become an important node in a more resilient and sustainable German security architecture.