Hybrid Threats from the Perspective of Municipalities: a Lost Battle?

Didier Raffin *+
Emmanuel Muller *+°

* University of Applied Sciences Kehl (Germany)
+ Université de Strasbourg (France)
° Fraunhofer ISI, Karlsruhe (Germany)

May 2026

evoREG Research Note #60

evoREG Research Notes Series' editor: Emmanuel Muller (Fraunhofer ISI)

The aim of this research note is to analyse hybrid threats from the perspective of local authorities, principally municipalities, and to assess the extent to which they can withstand such threats. It emphasises the pivotal role municipalities play in preserving social cohesion and public trust. Short scenario-based examples illustrate typical hybrid threat vectors. From these vignettes, the note derives a set of key dimensions for countering hybrid threats at the local level. Finally, drawing notably on lessons from Ukraine since the onset of the Russian war of aggression in 2022, the note highlights three principal factors that can strengthen municipal resilience.

Hybrid threats are characterised by a combination of conventional and non-conventional means, as well as by a predominantly non-military approach. This makes them particularly difficult to detect, classify and counter effectively. Typical tools of hybrid strategies include disinformation, cyberattacks, sabotage, espionage, and economic and logistical influence. Their danger and effectiveness are further amplified by the targeted use of AI technologies. Developing appropriate institutional, societal and economic countermeasures is therefore a significant challenge.

At present, government institutions, public administration, business, academia and society in Europe are not yet sufficiently prepared for the complexity and dynamics of hybrid threat scenarios (European Union, 2024). This is particularly true at the local level, where there is often a lack of both expertise and resources. Consequently, there is a significant need, particularly at the local authority level, for effective solutions to strengthen institutional, societal and economic resilience against hybrid threats.

Indeed, against this backdrop, local authorities occupy a unique strategic position. On the one hand, they are potentially particularly vulnerable due to limited human, financial and technical resources. On the other hand, their integration into the political and administrative system, as well as their central importance for social, psychological and economic stability, make them a key lever in addressing hybrid threats in Germany.

As the level of government closest to the public, municipalities engage with a wide range of stakeholders and areas of activity, ranging from individuals, schools, local service providers, associations and private businesses. At the same time, they take on coordination tasks in relation to other levels of government, as well as emergency services and the police. In this role, they play a key part in safeguarding social cohesion and public trust. The COVID-19 pandemic has also shown that, at local level, public trust often remains particularly stable in crisis situations (Seker and Muller, 2023). This proximity, combined with the ability to develop ad hoc solutions, makes local authorities a key factor in resilience to hybrid threats.

Box 1 presents as an illustration some examples of thinkable hybrids threats municipalities could be confronted to (based on previous activities related to the development of crises scenarios, cf. Muller et al., 2024; Djuricic et al., 2025).

BOX 1: A few examples of possible hybrid attacks targeting local authorities

Example 1: Disinformation campaign in the health sector

A small local authority becomes the target of a coordinated campaign to spread false information on social media regarding the quality of drinking water. The aim is to undermine trust in local institutions, cause anxiety among the population and place an excessive burden on administrative services.

Example 2: Targeted sabotage of local infrastructure

A large municipality is confronted with a series of coordinated incidents affecting public transport and key local energy infrastructure. The aim is to disrupt daily life, test inter-institutional responsiveness and undermine trust in the authorities.

Example 3: Destabilisation campaign during a flood

A municipality is confronted with false reports during a flood, claiming that certain areas should not be evacuated. The aim is to complicate crisis management, increase public anxiety and overload the emergency services.

Example 4: Manipulation in connection with a local infrastructure project

A local authority is influenced by the dissemination of disinformation regarding the health and environmental consequences of a municipal construction project. The aim is to polarise public debate, block political decision-making processes and fuel mistrust of local authorities

Example 5: Deepfake of the mayor to mobilise the population

A local authority is confronted with a deceptively realistic deepfake video: the mayor appears to be calling for an unauthorised gathering or announcing discriminatory measures. Citizens are mobilised via social media and fake official emails. The aim is to undermine trust, paralyse the administration and provoke confrontations.

Public authorities at national and European level are aware of the challenge that hybrid threats pose to the civil society, to the economy and more generally to the defense of democratic values (Council of the European Union, 2016). From this background, a number of key aspects of the fight against hybrid threats are emerging, which clearly need to be applied at local authority level as well. These key aspects can basically summarized along the seven following dimensions (which does not constitute an exhaustive list of thinkable measures).

1. **Detection**: Detection involves the early identification of indicators of hybrid threats in order to be able to initiate countermeasures promptly.

2. **Analysis:** Analysis involves contextualising hybrid incidents and assessing their effects, particularly with regard to the combination of different forms of attack and the underlying objectives.

3. **Defence:** Defence involves measures to contain and disrupt ongoing hybrid attacks through coordinated technical, organisational and communicative responses.

4. **Risk and crisis management:** Risk and crisis management involves establishing structures to prepare for hybrid threats and enables a coordinated, prioritised response with clear lines of responsibility in the event of an incident.

5. **Communication and information strategies:** Communication and information strategies include measures to counter disinformation and to ensure transparency, trust and the ability to act in crisis situations.

6. **Awareness-raising and training for relevant stakeholders**: Awareness-raising and training involve strengthening the awareness of the issue and the capacity to act among relevant stakeholders, so that warning signs of hybrid threats can be identified at an early stage and addressed appropriately.

7. **Organisational protective measures**: Organisational protective measures include increasing the resilience of structures and processes, for example through clear responsibilities, robust procedures, contingency plans and coordinated communication channels.

Nevertheless, municipalities confronting hybrid threats face acute constraints. Compared with better-resourced higher-level authorities, local governments frequently lack sufficient human and financial resources, possess limited experience and specialised skills, and sometimes do not have access to the legal instruments required at critical moments. These shortfalls are often magnified by structural factors: municipal administrations operate under tight budgetary ceilings and short political cycles that discourage long-term resilience investments; responsibilities can be fragmented across departments with weak coordination; and local authorities frequently depend on external information flows that are neither timely nor tailored to the multi-vector nature of hybrid threats.

So, is the battle lost and should only “higher” levels of government be in charge of the defence against hybrid threats knowing that often the fight is to be done at the local level?

Not necessarily; an examination of recent studies and simulations reveals certain factors that mean local authorities have a role to play beyond the measures mentioned above. In particular, Russia’s war of aggression in Ukraine has demonstrated the extreme resilience of political, administrative and local authorities. This resilience also extends to countering hybrid attacks. In this regard, three key lessons can be drawn that are detailed below.

Ukraine's recent wartime experience exemplifies this form of "hybrid resilience," as societal self-organization and decentralized governance have enabled communities to withstand and adapt to multifaceted hybrid threats (Darkovich et al., 2023). Their findings indicate a positive association between urbanity and local preparedness as well as overall resilience capacity. This may reflect the greater availability of resources, particularly financial resources, in more prosperous areas. However, other factors are likely to contribute as well. The analysis of preparedness highlights notably the positive role of networks, as reflected in cooperation agreements, and of democratic practices, as indicated by higher voter turnout. The first key lesson is that resilience depends not only on material resources, but also on civic engagement and governance.

A second key lesson is that effective crisis response depends on cross-sector collaboration and shared decision-making. This point is supported by Danylenko and Zagorodsky (2025), whose analysis of Ukrainian local communities' responses to hybrid threats highlights the importance of institutional resilience programs and cross-sector communication for safeguarding democratic procedures during crises, especially in wartime.

Third, and more broadly beyond the Ukrainian case, social cohesion emerges as a crucial component of resilience. As Kunce (2025) argues, societal resilience rests on the individual, the community, and their collective cohesion. These elements are not only foundational to domestic resilience, but also represent primary targets of hybrid tactics, which often seek to erode trust both horizontally among citizens and vertically between citizens and institutions. Such erosion weakens collective unity and undermines the social fabric required for effective planning, equipping, and training within a resilience framework. A key lesson, therefore, is that social cohesion is essential to countering this type of threat.

In conclusion, national and regional authorities generally possess greater resources, technical expertise, and legal authority; however, an exclusively top-down approach risks overlooking the highly localized nature of hybrid operations. Municipal actors, by contrast, often have granular situational awareness, direct channels of communication with citizens, and immediate operational control over essential public services. As a result, they play an indispensable role in detection, mitigation, and recovery.

This is why further research is needed. Future studies should build on comparative analyses of crisis networks, combining simulation-based exercises with observations from real cases. They should also develop a metric specifically adapted to the local governance level, especially municipalities, in order to better assess preparedness and response capacity. In addition, research should work toward typologies that link different local contexts with specific hybrid threat patterns. Such an approach would improve understanding of how local conditions shape resilience and would support more effective, context-sensitive responses to hybrid threats.

References

Council of the European Union (2016): Joint Framework on countering hybrid threats: a European Union response. https://data.consilium.europa.eu/doc/document/ST-7688-2016-INIT/en/pdf

Danylenko, S., Zagorodsky, A. (2025): Cross-sectoral resilience: lessons from Ukrainian local communities' response to hybrid threats. Social Sciences & Humanities Open. https://doi.org/10.1016/j.ssaho.2025.102278

Darkovich, A., Savisko, M., Rabinovych, M. (2023): Explaining Ukraine's resilience to Russia's invasion: The role of local governance and decentralization reform. Memo. https://decentralization.ua/en/news/17176#:~:text=In%20this%

Djuricic, K., Cuhls, C., Muller, E. (2025): TOSA: A Backcasting Tool for Dystopian Scenarios. evoREG Research Note #51.https://doi.org/10.24406/publica-5603.

European Union (2024): Progress Report on the Implementation of the Strategic Compass for Security and Defence. https://www.eeas.europa.eu/sites/default/files/documents/2024/StrategicCompass_2ndYear_Report_0.pdf

Kunce, B. (2025): Beyond the tornado: Strengthening societal resilience against hybrid warfare. DKI APCSS. https://dkiapcss.edu/wp-content/uploads/2025/01/CH21_SocietalResilience_JNMB4928.pdf

Muller, E., Jülicher, M., Gnamm, M-B, Héraud, J-A, Martins Nourry, L., Raffin, D. (2024): Crisis Scenarios Strasbourg-Kehl 2050. evoREG Research Note #47. https://doi.org/10.24406/publica-3908.

Seker, M., Muller, E. (2023): Municipalities, Innovation and Resilience. Open Journal of Business and Management 11: 3332-42. https://doi.org/10.4236/ojbm.2023.116181