Opinions on Security

DAG – Number 05 – 13.12.2021

Hybrid Threats – Is Germany prepared?

Theresa Caroline Winter
Manager for security and defence politics;
extended board member WIIS.de
(Women in International Security)

No, Germany is not prepared and it cannot be. The terminology is too broad and combatting hybrid threats (via the comprehensive approach) not sufficiently institutionalized.

Ever since the Ukraine crisis, the terms „hybrid threats" and „hybrid warfare" have become fashionable. In 2016 and for the first time, hybrid threats were mentioned in the German government's White Paper as a central security policy challenge, along with the response to it: the comprehensive approach. Hybrid threats can destabilize our liberal democracies in a wide variety of ways. The required response (better yet, *prevention*) must be interdisciplinary and involve interagency agreement; it requires civil-military cooperation, institutionalized rules and processes, and resilience among the population.

The spectrum of hybrid threats is enormously broad. Within cyberspace, it involves hacking attacks, online propaganda and radicalization, and the spread of disinformation. The actors are difficult to track, and influence and scope of the action often become clear only late. The methodological breadths and targeted population are so diverse that the distinction between autonomous social development and specific, actor-driven tactic often remains unclear and can blend fluidly. Much more overt is the instrumentalisation of refugees (consider the most recent example at the Belarusian-Polish border), where the actor, tactic and target are quickly identifiable, but the handling is politically sensitive and complex. Likewise complex are investments and thus (partial) control of foreign states over critical infrastructure such as energy supply, (air-)ports and cellular networks. Economic policy plays just as important a role as does foreign, security and defence policy in combatting hybrid threats.

This dynamic requires a comprehensive approach, meaning the participation of different actors from the military, politics, civil society and academia. Mobilizing these and coordinating them across ministries is intricate, especially when it comes to defining processes, structures and responsibilities and the exact details of the comprehensive approach. Prevention, response, and resilience building require scientific analysis of societal and security developments, interagency risk assessment, national and multilateral agreements and information sharing, securing infrastructure, regulating sanctions, political education, and promoting civil courage.

Since introduction to the federal government's White Paper, ministerial lead management for hybrid threats has changed several times and now resides with the Federal Ministry of the Interior (previously, the Federal Chancellery and the Federal Ministry of Defence were, separately, in charge). The comprehensive approach is anchored in the Federal Ministry of Defence. There is a lack of processes that make interdepartmental as well as overarching ministerial cooperation transparent and reduce redundancy: Analysis and assessment sometimes take place in parallel and in an uncoordinated manner, and recommendations for action are often implemented with delay.

For a more efficient and effective fight against hybrid threats, both the terminology and the approach must be operationalized. Actors, means and impact need classification and modular options for action need to be developed. Also, cultural and structural deficits in the exchange between the military and civil society at eye level urgently need to be addressed. One example is the exchange of information, which in the military is traditionally based on a hierarchically structured *Need-to-Know* principle. In civil society, processes and decisions are questioned much more often – the more information, the better. Rethinking *Need to Know* to *Dare to Share* still has long ways to go. Ultimately, the civilian population must be much more involved - especially when it comes to recognizing hybrid threats as such.