REPORT

DEFENDING AGAINST THE SMALL DRONE REVOLUTION: GERMAN–ISRAELI PERSPECTIVES ON NEW SECURITY FRONTIERS

Author: Karl Licht
As of: February 2026

POLICY **RECOMMENDATIONS**

#1 Strengthen Civil-Military Coordination *with joint command-and-control mechanisms and clear responsibilities across civilian and military authorities to close gaps in detection, attribution, and response.*

#2 Develop a Low-Altitude Air Traffic Management System *to distinguish authorized drones from aerial threats while enabling proportional responses.*

#3 Promote Interoperability and Standardization *by establishing common technical standards to ensure that sensors, effectors, and command structures can operate seamlessly together.*

#4 Accelerate Procurement and Innovation Cycles *by shifting from lengthy acquisition processes to agile, adaptive frameworks that support rapid testing, fielding, and continuous upgrading of counter-drone technologies in response to fast-evolving threats.*

#5 Establish a German–Israeli Defense Tech Hub *for institutionalizing bilateral cooperation in research, prototyping, and operational adaptation by combining Israel's operational experience with Germany's industrial and technological base to maintain a qualitative edge.*

Small drones (sUAS) have become a defining feature of modern conflict and hybrid security challenges. Their democratized production, dual-use nature, and ease of modification allow a wide range of actors to exploit them for hostile purposes. During the visit of the German Minister of the Interior to Israel in January 2026, both countries agreed to strengthen their security cooperation including intensified colaboration on counter-drone capabilities (C-UAS).

This cooperation was also the focus of the first virtual German-Israeli Roundtable held within the framework of the ELNET Security & Defense Initiative (ESDI) on 20 January 2026. ELNET convened a high-level group of experts from politics, ministries, research and industry to discuss the security policy challenges posed by sUAS for Germany and Israel and to develop joint approaches to address them. The ESDI Policy Briefing *"Defending Against the Small Drone Revolution: German-Israeli Perspectives on New Security Frontiers"* served as a foundation for the discussions at the roundtable. The following report summarizes the event's key takeaways and recommendations.

Threat Environment in Europe and the Middle East

The threat posed by sUAS has evolved differently in Europe and the Middle East. Israel has confronted the challenge of hostile drone use since the mid-2000s. They emerged as a tangi-

ble security concern at the end of the Second Lebanon War in 2006, when four Iranian-made drones carrying approximately 10 kilograms of explosives each penetrated Israeli airspace. This long-standing exposure has driven Israel to develop operationally tested layered C-UAS.

In Germany and across Europe, the perception of the sUAS threat developed more gradually. A key early incident occurred in 2013, when a small drone flew close to Chancellor Angela Merkel during a public campaign event, exposing significant vulnerabilities in airspace security and triggering initial political and institutional debate. However, for several years, counter-drone capabilities remained largely fragmented and reactive, as no sufficient political pressure emerged to drive coordinated development.

The decisive shift came with Russia's full-scale invasion of Ukraine in 2022. The war demonstrates the military effectiveness of sUAS for reconnaissance, targeting, and strike missions. At the same time, Europe experienced a sharp rise in drone-related incidents at critical infrastructures and military facilities, many of which were attributed to Russia. These developments fundamentally altered threat perceptions in Germany, transforming sUAS from a niche security concern into a strategic challenge for homeland defense, while also raising questions about NATO's future warfighting approach. It is worth noting that Hamas employed sUAS against Israel during the Hamas–Israel war; however, the scale of their use was limited and the IDF was able to conduct its combined arms approach effectively.

While Israel operates in a permanently contested security environment, Germany faces an emerging hybrid threat landscape and both countries now confront a common security reality shaped by sUAS. During the roundtable, the following recommendations were developed for facing the small drone revolution.

#1 Strengthen Civil-Military Coordination

Effective C-UAS requires close integration between civilian and military actors. Germany is adapting its security architecture to address the challenges posed by drone threats, including amendments to the Aviation Security Act and the establishment of a counter-drone unit and a counter-drone center. Nevertheless, responsibilities for airspace security and critical infrastructure protection remain fragmented across multiple actors, resulting in gaps in situational awareness and delayed response times.

Stovepipe thinking must end, and a genuine civil–military coordination framework must be established including joint command-and-control mechanisms, shared threat assessments, and standardized procedures for detection, identification, and response, with clear responsibilities. Real-time data exchange between police, air traffic authorities, and the German Armed Forces is essential to ensure a shared operational picture. Frequent joint exercises and scenario-based training should further strengthen interoperability and trust between institutions.

Israel has experience in managing a congested and threat-prone airspace and demonstrates that C-UAS effectiveness depends on seamless coordination across civilian and military sectors. Especially in civilian environments, technologies used for detection and neutralization must ensure controlled and predictable outcomes to minimize risks to people and critical infrastructure. Germany can adapt these lessons; nevertheless, important differences characterize Israel's situation. Critical infrastructure in Israel is highly centralized, e.g. with only two major power plants compared to approximately 70 in Germany. Israel may benefit from insights drawn from Germany's C-UAS solutions for decentralized critical infrastructure, as well as regulation and advanced legal mechanisms.

#2 Develop a Low-Altitude Air Traffic Management System

The rapid proliferation of sUAS allows parallels to be drawn with the early days of cybersecurity, when democratized access to technology led to unforeseen threats. Not all drones pose a security threat; many are operated for legitimate commercial and public purposes, including agriculture and emergency services. Most drone incidents begin in a gray zone where intent is unclear, but consequences can escalate quickly. A modern low-altitude air traffic management system must therefore distinguish between cooperative, authorized drones and potentially hostile or uncooperative platforms.

Germany should develop a unified framework that integrates registration, digital identification, and real-time tracking of drones operating below conventional airspace levels. Such a system would enhance transparency while enabling security authorities to quickly detect anomalies and respond proportionally to emerging threats. At the same time, clear regulatory pathways are needed to support innovation and investment in civilian drone applications, unlocking significant economic potential. German–Israeli cooperation could contribute technical expertise in sensor fusion and data processing, to build a resilient and scalable model for future drone governance.

#3 Promote Interoperability and Standardization

C-UAS must be treated as a system of systems. It requires a multilayered defense architecture in which sensors, effectors, and command-and-control systems from different providers and actors operate seamlessly together. The current C-UAS landscape is characterized by fragmented solutions, rapidly changing technologies, and a wide range of civilian and military actors, often using incompatible systems and procedures. This fragmentation reduces operational effectiveness.

Germany should prioritize the development of common technical standards, shared communication protocols, and interoperable interfaces for C-UAS systems across relevant institutions. Standardization would allow flexible integration of new sensors and effectors as technologies evolve, while ensuring continuity of operations. A modular and interoperable approach is particularly important in a fast-changing threat environment, where adversaries constantly adapt tactics and platforms.

German–Israeli cooperation can contribute valuable operational insights into layered defense concepts, enabling both countries to align technical standards and operational doctrines. Interoperability will be essential to building a resilient and future-proof C-UAS posture capable of responding to both current and emerging threats.

#4 Accelerate Procurement and Innovation Cycles

In 2024 it was estimated that up to 75 percent of all sUAS in Ukraine were neutralized through electronic warfare/jamming, establishing it as a perceived gold standard. This advantage has since eroded as adversaries adopted artificial intelligence and returned to Cold War–era technologies such as fiber-optic–guided drones. While for Germany and Israel electromagnetic dominance will still have to remain a priority, hard-kill capabilities are becoming increasingly relevant as part of a layered defense approach.

The war in Ukraine demonstrates how rapidly adaptation occurs during wartime through synergetic government-civilian efforts. sUAS technologies evolve at unprecedented speed, rendering traditional procurement timelines increasingly obsolete: innovation cycles must accelerate from years to weeks.

These developments underline the necessity of shortening procurement and innovation cycles in peacetime institutional preparation. Authorities must move away from lengthy acquisition processes toward agile frameworks that enable rapid testing, fielding, and upgrading of systems in wartime speed. Germany should learn from Israel and prioritize flexible contracting mechanisms, experimental deployments, and continuous feedback loops between operators, industry, and research institutions. Lessons from Ukraine demonstrate that adaptability—rather than reliance on any single technology—is the key to sustaining operational effectiveness in a rapidly evolving threat environment.

#5 Establish a German–Israeli Defense Tech Hub

To maintain a qualitative edge in C-UAS and other emerging defense technologies, Germany and Israel should establish a permanent joint Defense Tech Hub for institutionalizing bilateral cooperation in research, prototyping, and operational adaptation. Such a hub would ensure technological superiority at a time when adversaries increasingly rely on unmanned systems to compensate for disadvantages in conventional military capabilities.

Russia's experience in Ukraine illustrates this trend and underscores the danger that the country aims to export its model of attrition warfare in case of a conflict with NATO. At the same time, non-state

actors and terrorist organizations, including Iran's regional proxies, are rapidly adopting commercially available drones for surveillance and attacks.

Germany and Israel bring complementary strengths. A German-Israeli Defense Tech Hub would combine Israel's operational experience with Germany's industrial and technological base to accelerate research, rapid prototyping, and field deployment of advanced defense solutions. Israel could especially benefit from the German industry's ability to scale up quickly. While Israel possesses two decades of experience in C-UAS, German companies, owing to Germany's role as one of Ukraine's principal supporters, have gained valuable technological and operational insights into the use of drones in high-intensity conflict — knowledge from which Israel could equally profit. By institutionalizing cooperation, both countries can stay ahead of state and non-state adversaries and make use of their countries' skilled human capital to preserve the qualitative edge.

Info

THE ELNET SECURITY & DEFENSE INITIATIVE (ESDI)

Security policy cooperation between Germany and Israel has a long history. The ELNET Security & Defense Initiative (ESDI) was launched in July 2025 to explore new avenues of cooperation in the face of global threats and technological upheaval. The initiative aims to deepen strategic dialogue, tap into joint innovation potential, and place the German-Israeli partnership on a sustainable, structurally sound footing.

European Leadership Network (ELNET)

Image: ELNET/Tobias Koch

ELNET

berlin@elnetwork.eu

elnet-deutschland.de

@ElnetD

@elnet_D