REPORT

GERMAN–ISRAELI COOPERATION IN MARITIME SECURITY: SAILING AHEAD IN AN ERA OF HYBRID THREATS

Author: Karl Licht
As of: June 2026

POLICY **RECOMMENDATIONS**

#1 Strengthen Sovereignty in Critical Maritime Infrastructure *through closer German-Israeli cooperation on maritime cybersecurity, supply-chain security, and the reduction of strategic technological dependencies in ports, vessels, and communication networks.*

#2 Develop a Shared Understanding of Maritime Threat*s by integrating military, intelligence, law-enforcement, and commercial actors to improve maritime domain awareness, attribution, and critical infrastructure protection, particularly in the Eastern Mediterranean and in support of NATO initiatives.*

#3 Develop a Maritime System-of-Systems Approach *by integrating autonomous systems, underwater sensing, command-and-control networks, and sensor networks at critical maritime infrastructure.*

#4 Establish a German-Israeli Defense Tech Hub for Maritime Security *to accelerate technology transfer, support defense and dual-use startups, and strengthen cooperation among industry, government, academia, and investors.*

#5 Foster a Culture of Initiative, Adaptability, and Readiness *through joint exercises, personnel exchanges, and operational learning formats that strengthen resilience, decentralized decision-making, and the ability to operate under degraded conditions.*

Maritime security is undergoing a significant transformation. Fleet size and naval tonnage alone no longer determine outcomes at sea. Instead, a growing range of hybrid threats is reshaping the maritime domain. These include the sabotage of critical undersea infrastructure (CUI), drone incursions over ports and naval facilities, cyberattacks on vessels, and the weaponization of shadow fleets. Furthermore, the proliferation of unmanned maritime systems demonstrates that the cost asymmetries already visible in aerial warfare are now extending to the maritime domain. As seen with Shahed loitering munitions and low-cost FPV drones, relatively inexpensive platforms can impose disproportionate costs on far more sophisticated systems, potentially altering the established balance of power at sea.

In this increasingly unstable environment, German-Israeli cooperation in maritime security is becoming ever more important. This partnership can build on a long-standing tradition, ranging from the transfer of missile boat designs in the 1960s and the submarines built in Kiel since the 1990s to the modern autonomous underwater system Blue Whale. The latter illustrates the transformation of German-Israeli maritime cooperation. Israel is no longer merely a recipient of German naval capabilities; it is increasingly emerging as a contributor to joint technological development and maritime defense innovation. This convergence was the subject of the ESDI Roundtable, “Maritime Security: From Decades of Cooperation to

Sailing the Seas Ahead," convened in partnership with the Hamburg Chamber of Commerce in mid-June 2026 under the framework of the ELNET Security & Defense Initiative (ESDI), a platform dedicated to strengthening strategic and security cooperation.

Building on the *ESDI Policy Briefing "German–Israeli Cooperation in Maritime Security: Sailing Ahead in an Era of Hybrid Threats"*, the event brought together representatives from industry, law enforcement, academia, the military, and other relevant authorities. The goals were to assess the current threat environment and develop joint approaches to emerging maritime security challenges.

The following report summarizes the roundtable's key findings and policy recommendations.

#1 Strengthen Sovereignty in Critical Maritime Infrastructure

Maritime security increasingly depends on control over critical technologies. Ports, vessels and other critical maritime infrastructure rely on systems that are vulnerable to cyberattacks, supply-chain dependencies, and foreign-made hardware. The growing use of Chinese-manufactured port equipment demonstrates that strategic vulnerabilities often emerge through technology rather than the often discussed ownership structures of ports alone.

Just as the proliferation of drones has democratized access to military capabilities on the battlefield, advances in artificial intelligence are democratizing the capacity to execute complex cyber operations. As a result, even highly secured systems, including naval platforms, are likely to become increasingly exposed to cyber threats from a broader range of actors.

Germany and Israel should expand cooperation on protection against cyberattacks and reducing technological dependencies. Israel's approach to Chinese-built rail infrastructure provides a useful model: retaining physical assets while replacing networked and digital components with nationally controlled systems. Similar concepts could be applied to port infrastructure and maritime communications. The announcement by Federal Minister Dobrindt to expand German-Israeli cooperation in the field of cybersecurity ("Cyberdome") in January 2026 should consequently also encompass the maritime domain.

#2 Develop a Shared Understanding of Maritime Threats

Maritime threats are increasingly hybrid, cross-domain, and difficult to attribute. Activities that begin with surveillance by drones or suspicious vessels can gradually escalate into sabotage of critical infrastructure, as demonstrated by recent incidents involving undersea cables, energy infrastructure, and navy vessels. Russia's incremental approach in European waters illustrates how adversaries test vulnerabilities below the threshold of open conflict before moving toward more disruptive actions. Germany and Israel should deepen cooperation on maritime domain awareness and threat assessment as disruptions at key chokepoints such as the Red Sea or Strait of Hormuz can rapidly generate global consequences.

A shared threat picture should integrate military, intelligence, law-enforcement, and commercial actors while covering both the physical and digital maritime domain. Particular attention should be given to CUI, ports, energy assets, and communication networks. Israel's experience protecting offshore gas fields and Germany's role as a major European logistics hub offer complementary expertise that can strengthen resilience against emerging maritime threats.

In this context, NATO's announcement to expand its newest initiatives for the protection of CUI into the Mediterranean should also be accompanied by closer cooperation and information exchange with Israel, given its strategic position in the Eastern Mediterranean.

#3 Develop a Maritime System-of-Systems Approach

The future maritime battlespace will be shaped by unmanned/autonomous systems, artificial intelligence, and cross-domain operations. Recent conflicts have demonstrated that low-cost technologies can impose disproportionate costs on high-value assets. Advances in autonomy and AI are increasingly enabling coordinated swarm and mesh attacks, allowing large numbers of interconnected systems

to overwhelm traditional defenses through speed, scale, and distributed decision-making, suggest that the offense is increasingly becoming stronger than the defense.

As naval platforms and critical maritime infrastructure become increasingly exposed to sophisticated physical and cyber threats, operational success will depend less on individual platforms and more on the ability to integrate sensors, effectors, autonomous systems, and command-and-control architectures into a coherent system of systems.

Protecting critical maritime infrastructure will require persistent underwater awareness. Existing subsea cables, communication links, and other undersea networks could be leveraged as distributed sensor systems to detect and monitor underwater activity across large maritime areas, strengthening the protection of CUI and sea lines of communication (SLOC).

The Blue Whale autonomous underwater vehicle demonstrates the potential of German-Israeli cooperation in this area. Building on this foundation, bilateral cooperation should focus on autonomous maritime systems, CUI protection, underwater sensing technologies, cyber resilience, and integrated battle-management capabilities that strengthen deterrence, improve situational awareness, and enhance operational effectiveness across the maritime domain.

Germany and Israel should also deepen cooperation in drawing lessons from Ukraine's experience in protecting critical port infrastructure, e.g. in integrated drone defense, and the employment of unmanned systems, including hard-kill capabilities demonstrated in the Black Sea. While Ukraine offers valuable lessons in asymmetric maritime warfare, Israel's experience integrating naval, air, cyber, and unmanned capabilities in recent conflicts remains essential for future maritime concepts. As an operator of German-built platforms, Israel offers operational insights that are necessary to collaborate on future concepts of naval warfare such as manned-unmanned teaming, the coordinated employment of crewed and autonomous maritime systems.

#4 Build a German-Israeli Defense and Dual-Use Innovation Ecosystem

Maintaining a technological edge in maritime security requires not only new capabilities but also a stronger innovation ecosystem. Across Europe, numerous startups are developing promising technologies in areas such as autonomous systems, maritime surveillance, artificial intelligence, cyber resilience, and critical infrastructure protection. However, many struggle to secure the early-stage funding and procurement opportunities necessary to scale their solutions and transition from prototypes to operational capabilities. Germany, Israel, and European partners should strengthen funding mechanisms for defense and dual-use startups while creating frameworks that encourage closer cooperation among entrepreneurs, established defense companies, investors, academia, and government stakeholders.

Israel's innovation ecosystem demonstrates the benefits of close interaction between operational users, industry, investors, and startups. Programs run by the Israeli Ministry of Defense's Directorate of Defense Research and Development (MAFAT) have shown how targeted support, accelerator programs, and early-stage funding can help transform innovative concepts into deployable military capabilities. Similar approaches could serve as a valuable model for Germany as it develops new Bundeswehr innovation structures, including the Innovation Center of the Bundeswehr in Erding.

To institutionalize this cooperation, Germany and Israel should establish a German-Israeli Defense Tech Hub for Maritime Security as a permanent platform for defense and dual-use innovation. The hub would connect startups, established industry, research institutions, investors, and government stakeholders to accelerate technology transfer, joint ventures, and capability development.

#5 Foster a Culture of Initiative, Adaptability, and Readiness

Success will depend not only on advanced capabilities but also on the ability of organizations and personnel to adapt quickly, make decisions under

uncertainty, and operate effectively when systems are disrupted, degraded, or denied.

Future conflicts will reward organizations that can learn and adapt faster than their adversaries. At the institutional level, keeping pace with the speed of change requires overcoming bureaucratic barriers, accelerating decision-making processes, and fostering a greater sense of urgency. Given the scale and complexity of critical infrastructure, comprehensive protection is impossible; organizations must therefore assume they will be targeted and prioritize resilience, redundancy, and rapid recovery.

While Israel's constant exposure to security threats has fostered a deeply ingrained culture of preparedness, Germany, despite being increasingly targeted by hybrid threats, has yet to develop a comparable sense of urgency. Through regular exchanges with Israel among military, government, industry, and academic stakeholders, German institutions can cultivate a stronger culture of resilience. Exercise series such as Red Storm in Hamburg also provide valuable opportunities to strengthen not only interoperability but also a culture of initiative, adaptability, and operational readiness.

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)

ELNET

berlin@elnetwork.eu

elnet-deutschland.de

@ElnetD

@elnet_D

Image: ELNET/Tobias Koch