POLICY BRIEFING

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

Author: Karl Licht
As of: June 2026

EXECUTIVE **SUMMARY**

- *The maritime security landscape is increasingly shaped by hybrid threats targeting ports, offshore energy assets, and critical undersea infrastructure (CUI). Fleet size and naval tonnage alone are no longer decisive for maritime power.*
- *The Baltic Sea has become a hotspot for sabotage, espionage, and cyberattacks linked to Russian hybrid activity. Conflicts in the Red Sea, Eastern Mediterranean, and Gulf region demonstrate how maritime disruptions can threaten global trade and energy security.*
- *The use of autonomous maritime systems in the Russo-Ukrainian War demonstrates how relatively low-cost unmanned systems can threaten or destroy high-value naval assets, creating significant cost asymmetry.*
- *Germany and Israel are expanding cooperation in submarines, autonomous systems, drones, cyber defense, and port security.*
- *Israeli operational experience and innovation in autonomous systems, counter-drone technology, drones, and cybersecurity complement Germany's industrial and naval capabilities.*
- *Deeper Israeli integration within NATO and EU maritime security frameworks could significantly strengthen resilience against hybrid threats, improve protection of CUI, and accelerate innovation in autonomous maritime and cyber defense technologies.*

In February 2026, the German Navy took delivery of the Blue Whale unmanned underwater vehicle (UUV), a system jointly developed by Germany's Thyssenkrupp Marine Systems (TKMS), via ATLAS Elektronik, and Israel Aerospace Industries (IAI).[1]

This marks a new phase of bilateral naval cooperation, which stretches back several decades. While the Dolphin-class submarines, developed since the 1990s, have become its most visible symbol, the origins of this relationship go back much longer. As early as the 1960s, German engineers contributed to the design of Israel's first missile boats, underscoring a long-standing, if at times discreet, collaboration in the maritime domain.[2]

Today, maritime security is no longer measured solely in terms of fleet size or tonnage. Instead, it is increasingly shaped by hybrid threats, including acts of sabotage against critical undersea infrastructure (CUI) and cyberattacks against ports. At the same time, the rapid emergence of autonomous systems is transforming naval warfare. Recent developments in the Black Sea, where Ukrainian forces have successfully deployed unmanned maritime systems (UMS) to sink strategic Russian naval assets, including the Caesar Kunikov in February 2024, illustrate

the disruptive potential of such technologies.[3] These shifts amount to a fundamental transformation of maritime security, challenging traditional concepts of naval power. For German–Israeli cooperation, this evolution presents both new challenges and significant opportunities, particularly in leveraging complementary strengths across their respective defense and security ecosystems.

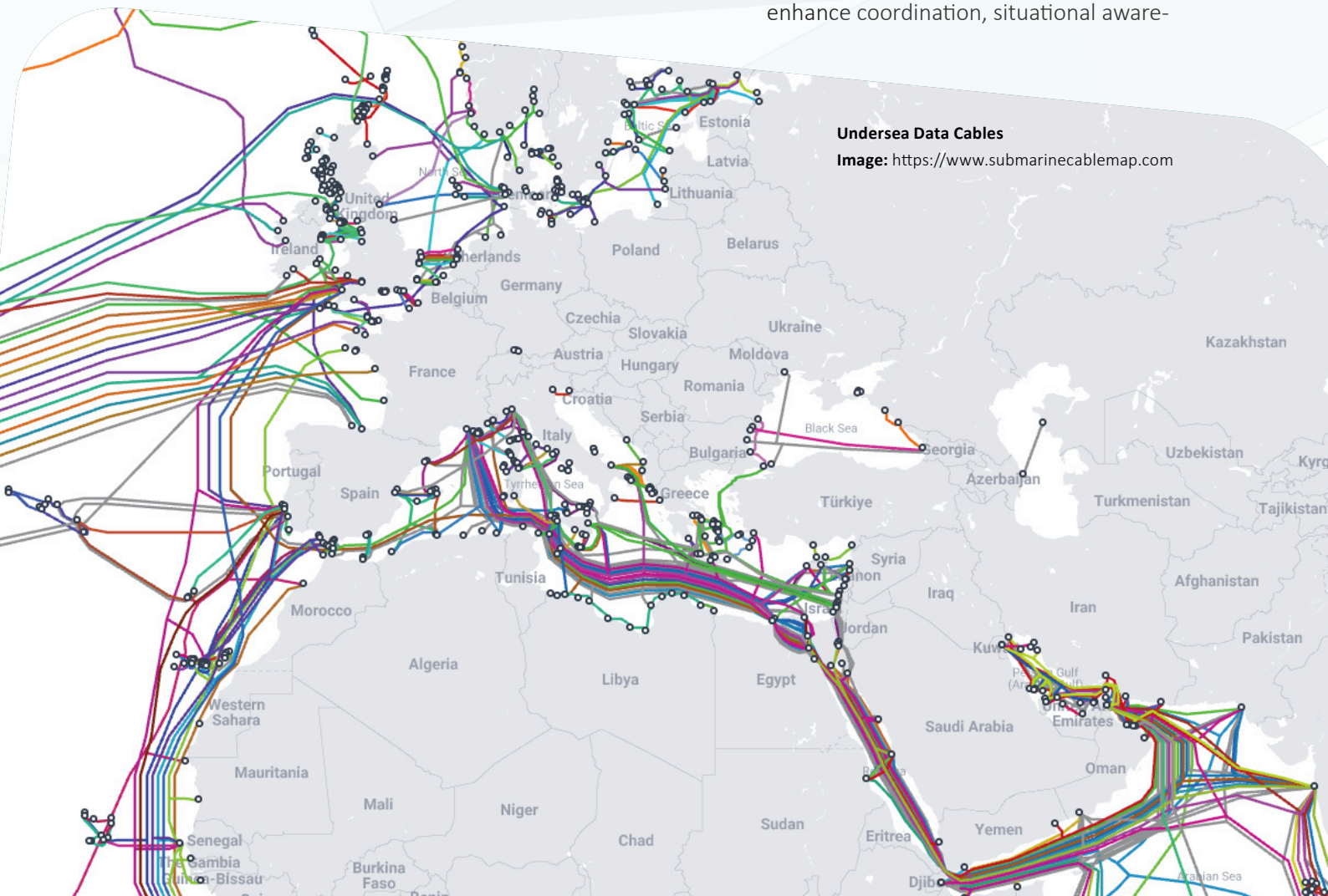
The Transformation of Maritime Threats

The transformation of maritime security outlined above is already visible across multiple theaters and at different levels of intensity. Rather than being confined to traditional naval confrontation, contemporary maritime threats increasingly manifest through hybrid activities and the weaponization of economic interdependence by disrupting Sea Lines of Communication (SLOC). From covert sabotage and cyber operations to direct kinetic attacks on critical assets, the maritime domain has become a contested space in which state and non-state actors operate across the full spectrum of conflict.

The Baltic Sea as a Theatre of Hybrid Maritime Conflict

The Baltic Sea has become a focal point of security concerns in Europe. In a potential future large-scale conflict between NATO and Russia, control of this maritime space would be of critical strategic importance, particularly regarding the sustainment of allied forward-deployed troops in the Baltic states.[4] In the hybrid domain, this contest has already begun. This is illustrated by recent incidents involving sabotage attacks on critical maritime infrastructure such as in October 2023, when the Balticconnector gas pipeline and a parallel telecommunications cable between Finland and Estonia were damaged, raising concerns about deliberate sabotage. Another incident in the same month that involved damage to cables between Sweden and Estonia. Although attribution remains contested, the incidents are widely discussed in connection with hybrid activities of the Russian Federation (Table 1).[5]

In response, NATO established the Critical Undersea Coordination Cell at NATO Headquarters in Brussels and founded the Maritime Centre for CUI in 2024 to enhance coordination, situational aware-



Undersea Data Cables
Image: https://www.submarinecablemap.com

ness, and the protection of subsea assets across the Alliance.[6] At the operational level, NATO has translated these concerns into action through the launch of Operation Baltic Sentry in 2025, which aims to increase military presence, improve surveillance, and deter sabotage against CUI in the Baltic Sea.[7]

Acts of sabotage are not limited to maritime infrastructure alone but also to German Navy vessels. In one instance, oil hoses were deliberately cross-connected with the freshwater system; in another, critical cables were intentionally damaged during maintenance work.[8/9] In a further case, several kilograms of scrap metal were reportedly thrown into a ship's engine.[10] These acts were fortunately detected in time. However, the potential consequences for operational readiness would have been significant, given the already operationally stretched German Navy.

All this underlines the assessment by European security experts and intelligence services of a broader pivot from espionage to sabotage on the side of the Russian Federation. However, espionage activities remain a critical challenge. As incidents involving illegal drone activities have been rising across Europe, Germany's domestic intelligence service (Bundesamt für Verfassungsschutz) has reported a significant increase in such activities over naval facilities.[11]

A prominent example occurred in November 2024, when a drone operated over a restricted military area while the British aircraft carrier HMS Queen Elizabeth was anchored in Hamburg. German forces could not neutralize it, and the signal was reportedly lost near a China-operated port section, raising broader concerns about critical port infrastructure security.[12]

Table 1: Selected CUI Incidents

Date	Incident	Location	(Suspected) Actor
26 Sep 2022	Detonation of Nord Stream 1 and Nord Stream 2 pipelines.[13]	Baltic Sea	Suspected: Ukrainian sabotage team
8 Oct 2023	Damage to Balticconnector gas pipeline and communication cables. Anchor recovered at the damage site.[14]	Gulf of Finland	Vessel Newnew Polar Bear (Hong Kong flag, Chinese owner, departing from Russian port)
17–18 Nov 2024	Severing of BCS East-West Interlink and C-Lion1 communication cables within 24 hours.[15]	Baltic Sea	Suspected: Yi Peng 3 (Chinese bulk carrier, Russian captain)
25 Dec 2024	EstLink 2 and four telecom cables destroyed. Vessel dragged anchor approx. 90 km across the seabed[16]	Gulf of Finland	Suspected: Eagle S (Cook Islands flag, Russian shadow fleet)

Cyber threats further expand the spectrum of hybrid maritime risks. A recent NATO policy brief warns of a surge in state-linked cyberattacks targeting civilian ports across Europe and the Mediterranean, many attributed to actors from Russia, China, and Iran. Hacktivist groups such as NoName057 have repeatedly targeted major European ports through Distributed Denial-of-Service (DDoS) attacks. In one instance in June 2023, the Port of Rotterdam experienced disruptions to its website and digital services following an attack attributed to the group. A similar incident affected Poland's Port of Gdynia in August 2023.

Drone ban sign at German shipyard

Image: Ein Dahmer / CC BY-SA 4.0 / via Wikimedia Commons

These attacks frequently target access control and vessel traffic management systems, exposing critical vulnerabilities.[17]

At the same time, insufficient coordination between civilian port operators and military actors further increases the risk to maritime logistics and NATO's operational readiness. Improving civil–military coordination constitutes a key pillar of the European Union's European Maritime Security Strategy (EUMSS), which was revised in 2023 to address these developments and strengthen the resilience against hybrid and cyber threats.[18] The protection of CUI is also being addressed through specific initiatives such as the PESCO project Critical Seabed Infrastructure Protection (CSIP), led by Italy with participation from Germany.[19] This highlights that both the European Union and NATO increasingly recognize the strategic importance of protecting CUI and are taking coordinated steps to address these challenges.

While public debate has focused on Nord Stream sabotage, Germany's maritime vulnerabilities extend beyond gas pipelines. Offshore wind farms in the North and Baltic Seas are becoming central to energy security, making their cables, substations, and logistics critical infrastructure increasingly exposed to hybrid threats. Protecting these assets is therefore becoming a key priority of Germany's maritime security strategy.[20]

Sa'ar-6-Class Corvette
Image: ELNET

Maritime Security Challenges in the Middle East

Israel's offshore gas infrastructure has already been exposed to repeated security threats in recent years. In July 2022, Hezbollah launched multiple drones toward the Karish gas field, which were intercepted by Israeli forces.[21] More recently, regional escalation as a result of the war in Iran has directly affected offshore energy security, as production at the Leviathan gas field was temporarily halted for 33 days beginning from 28 February 2026 due to missile and drone threats.[22]

While much of the attention surrounding the protection of maritime infrastructure within NATO is focused on the Baltic and North Sea regions, critical vulnerabilities to CUI have also become visible in the Mediterranean and the Red Sea. In October 2022, multiple fiber-optic cables on southern France's shore were deliberately cut in what authorities treated as a coordinated act of sabotage, disrupting internet connectivity and data traffic between Europe, Asia, and the United States.[23]

Similar concerns have emerged in the Eastern Mediterranean and Red Sea corridor, where dense networks of submarine cables linking Europe with the Middle East, Africa, and Asia pass through relatively shallow waters, increasing their exposure to accidental damage, anchoring incidents, and potential hostile interference.[24]

While undersea data cables form the backbone of global digital connectivity, maritime trade routes remain equally critical to the functioning of the global economy. Maritime ports handle 80 percent of global trade.[25] The ongoing war involving Iran has already led to a de facto blockade of one of the world's most critical energy transit routes, the Strait of Hormuz. Since early 2026, maritime traffic through the Strait had dropped by 90 percent, with vessels being intercepted, seized, or turned back amid a dual blockade. The growing threat of naval mines is particularly significant, as even limited mine-laying operations can severely disrupt commercial shipping.[26]

While international missions such as EU NAVFOR Somalia (Operation Atalanta) successfully contributed to safeguarding maritime trade routes during the peak of piracy off the Horn of Afri-

ca, the ongoing attacks by the Houthi movement in the Red Sea highlight the persistent challenges of securing these routes.[27] This remains the case even in the presence of international naval forces, such as those deployed under Operation Aspides, which was launched in February 2024.[28]

Considering these developments, the prioritization of securing sea lines of communication in the first comprehensive military strategy of the Bundeswehr, published only in April 2026, can be seen as a particularly ambitious objective.[29]

> "Protecting international (sea and other) lines of communication: The freedom of sea lines of communication and other lines of communication in all domains is crucial to the rules-based international order. The Bundeswehr will implement this military-strategic priority by, for example, allocating appropriate forces and contributing to protection of defence-critical infrastructure."
>
> -First Military Strategy of the Bundeswehr, April 2026

Vessels in the Crosshairs of Spoofing Attacks

Beyond large-scale disruptions of maritime chokepoints and infrastructure, cyberattacks on individual vessels have emerged as an additional layer of vulnerability in the maritime domain. Modern commercial ships rely heavily on digital navigation, communication, and cargo management systems, making them potential targets for cyber interference. In several documented cases, Global Navigation Satellite System (GNSS) spoofing and electronic interference have affected vessels in contested regions, leading to navigation errors and operational disruptions. Single ships can become entry points for broader disruption, with potential cascading effects on supply chains, port operations, and maritime safety.[30]

The scale and geographic concentration of GNSS interference in the Baltic region illustrates this threat concretely. Lithuania's air navigation service provider Oro Navigacija documented a roughly tenfold increase in GNSS interference between January 2024 and January 2025 alone.[31]

Attribution points consistently toward Russia. Estonian, Latvian, and Lithuanian authorities have each independently identified Russian origins: Lithuania has pinpointed more than ten sites in Kaliningrad as interference sources.[32] A Polish study further provides evidence that Russia-linked vessels operating in the Baltic Sea were likely responsible for maritime-domain GNSS interference – suggesting that shadow fleet tankers serve not only as sanctions-evasion tools but potentially as mobile electronic-warfare platforms.[33]

Several shadow fleet vessels have already been found to carry equipment consistent with intelligence-gathering or electronic surveillance: the tanker Eagle S, seized by Finland in December 2024 on suspicion of cable sabotage, as well as the Swiftsea Rider, were reportedly fitted with transmitting and receiving devices abnormal for a merchant ship.[34]

Shadow Fleets

The growing prevalence of so-called shadow fleets introduces an additional challenge. These vessels, often operating under flags of convenience, with opaque ownership structures and limited regulatory oversight, are used to circumvent international sanctions, particularly those imposed on Russia and Iran. By disabling tracking systems such as the Automatic Identification System (AIS), conducting covert ship-to-ship transfers, and operating outside established monitoring frameworks, they not only facilitate illicit

Table 2: Drone Incursions and the Russian Shadow Fleet

Date	Incident	Location	Actor
Early May 2025	Following unidentified drones over a military site in Kiel, the Dutch Coast Guard intercepted the freighter Dolphin (Antigua and Barbuda flag, all-Russian crew). Dutch boarding found no evidence that drones had been operated from the vessel.[36]	Kiel (drones); North Sea (boarding)	Suspected: Dolphin freighter; Russian crew
17 May 2025	Unidentified drones followed the German Federal Coast Guard patrol boat Potsdam for three hours, while it was shadowing the Russian freighter Luga. The ship was subsequently boarded by Belgian authorities, but no traces of drone activity were found.[37]	German EEZ, North Sea	Suspected: Luga freighter; Russian crew
21 May 2025	Shadow fleet tanker Sun (Antigua and Barbuda flag) observed loitering around a 600 MW undersea power cable connecting Sweden and Poland. Polish aerial patrol scared the vessel off. Suspected reconnaissance of critical undersea infrastructure.[38]	Baltic Sea, between Sweden and Poland	Sun Tanker (Russian shadow fleet)
22–24 Sep 2025	Wave of unidentified drone incursions closed multiple Danish airports and Oslo Airport. Danish authorities identified three vessels of interest with Russian links: the cargo vessels Astrol-1 and Oslo Carrier-3, and the oil tanker Pushpa. Danish PM Frederiksen described the incidents as the "most serious attack" on Danish infrastructure to date.[39]	Off Copenhagen and other Danish airports; Pushpa near Zealand	Suspected: Astrol-1, Oslo Carrier-3 and Pushpa; launch attribution unresolved

trade, but also create opportunities for covert activities, including intelligence gathering and potential interference with critical maritime infrastructure (Table 2).[35]

Beyond the smuggling of sanctioned oil, these networks are also used for the illicit transfer of weapons and other sensitive goods. This challenge is further exacerbated by the increasingly blurred lines between state adversaries, proxy actors, and organized crime, which complicates attribution and response. In this context, ports themselves become critical nodes in both vulnerability and resilience.[40]

The Port of Haifa, the largest of three major ports in Israel, followed by the Port of Ashdod and the Port of Eilat, and operating under constant security pressure, has developed some of the most advanced systems for container inspection, biometric access control, radiation detection, and intelligence supported risk profiling.[41] While Germany's largest port, the Port of Hamburg, Europe's third largest container port, handling around 8.3 million TEU (Twenty Foot Equivalent Units) annually, processes more than twice the combined volume of all Israeli ports, which together handle roughly 3.5 million TEU, the scale of operations is fundamentally different. Nevertheless, the core security challenges, including smuggling, sanctions evasion, and hybrid attacks on critical infrastructure, are increasingly similar.[42/43]

German–Israeli Maritime Security Cooperation

Taken together, these developments show that the maritime threat environment has become increasingly complex and multifaceted. Hybrid interference, cyberattacks, strikes on offshore infrastructure, and disruptions to critical sea lines of communication

demonstrate that maritime security challenges now span the full spectrum of conflict. Although these threats differ between the Baltic Sea and the Eastern Mediterranean, they reveal similar vulnerabilities and underline the growing need for technological adaptation.

Their hybrid character also requires close coordination among military, law enforcement, and civilian actors. This is especially relevant in Germany, where legal and political constraints limit military deployment, while responsibilities such as countering drones or protecting civilian infrastructure often fall to law enforcement. Germany's federal structure further complicates coherent responses across jurisdictions.

The long-standing German-Israeli partnership offers strong potential to address these challenges, combining complementary maritime experience, technological capabilities, and strategic perspectives. Germany contributes industrial capacity, European institutional integration, and naval manufacturing expertise, while Israel contributes operational experience, rapid defense innovation, and advanced capabilities in autonomous and cyber systems, as the cooperation in the following areas demonstrates.[44]

Naval Platforms and Industrial Cooperation

The backbone of German–Israeli defense cooperation lies in the shipyards of Kiel, particularly at Thyssenkrupp Marine Systems (TKMS), where the second batch of the Dolphin-class submarines were built. The latest contract for three additional, more capable Dakar-class submarines was signed in 2022 valued at around 3 billion EUR, underscores the durability of this partnership.

Blue Whale UUV
Image: Swadim, CC0 1.0 (Public Domain Dedication)

These submarines are widely considered nuclear-capable and form a key pillar of Israel's strategic deterrence.[45]

All four of Israel's latest Sa'ar 6 corvettes were built in Germany in a joint project between German Naval Yards Holdings and TKMS. Based on the Braunschweig-class design, they are equipped with Israeli systems, including the Barak-8 air defense system and the naval variant of Iron Dome. Germany covered roughly one third of the construction costs. The vessels now constitute the backbone of Israel's protection of its exclusive economic zone, including offshore gas infrastructure.[46]

TKMS and Elbit Systems opened a new production line for glass-fiber reinforced underwater components in Israel in February 2026. This step strengthens Israel's industrial base in submarine construction and illustrates the growing potential for reciprocal value creation within the partnership.[47]

In July 2024, Germany and Israel signed a two-year naval cooperation work plan, formalizing knowledge exchange, joint exercises, and coordinated operational planning aimed at regional stabilization. This institutional framework moves beyond a purely procurement-based relationship and lays the foundation for deeper operational cooperation.[48]

This cooperation directly addresses the growing vulnerability of offshore energy infrastructure and critical sea lines of communication described above. Platforms such as the Sa'ar 6 corvettes and Dakar-class submarines strengthen deterrence, maritime domain awareness, and the protection of critical infrastructure against hybrid threats, sabotage, and hostile interference in the Eastern Mediterranean.

Autonomous Systems

In February 2026, Germany received its first Blue Whale Large Unmanned Underwater Vehicle at the naval base in Eckernförde. Developed by IAI ELTA in cooperation with Atlas Elektronik, the system is designed for long-endurance, covert reconnaissance and acoustic in-

telligence gathering, operating autonomously for up to three weeks at depths of up to 300 meters.[49]

The procurement of eight US-made MQ-9B SeaGuardian drones by Germany recently made headlines due to their role in strengthening naval surveillance capabilities.[50] However, Israeli-made Heron TP drones had already been used by the Bundeswehr during NATO's Baltic Sentry mission to monitor and protect critical infrastructure in the Baltic Sea.[51]

The operational lessons from Ukraine's use of unmanned maritime systems demonstrate how autonomous platforms are reshaping naval warfare and critical infrastructure protection. German–Israeli cooperation in UUVs, drones, and maritime surveillance directly responds to the growing threat posed by sabotage, covert reconnaissance, and low-cost autonomous attacks against naval assets and subsea infrastructure (Table 3).

Port Security, C-UAS and Cyber Resilience

During the visit of Alexander Dobrindt, German Federal Minister of the Interior, to Israel in January 2026, both countries agreed to further strengthen their security cooperation, including enhanced collaboration on counter-drone capabilities (C-UAS) and cyber defense.[52] In this context, Israel's Cyber Dome concept, which integrates advanced cyber defense, real-time threat detection, and AI-supported response mechanisms, offers a relevant model for the protection of maritime critical infrastructure. Applied to ports, shipping, and CUI such an approach could enhance the resilience of digital systems that underpin port operations, vessel traffic management, and subsea networks, thereby addressing a key vulnerability in the evolving maritime threat environment.

Already in 2023, the Hamburg Chamber of Commerce launched an innovation and tech-scouting partnership with Israeli institutions focused on sectors including cybersecurity, logistics, and the maritime economy.[53]

Table 3: Prevalence of UMS in the Russo–Ukrainian War

Date	Incident	Location	System
4 Aug 2023	USV strike on the landing ship Olenegorsky Gornyak (Ropucha class). Severe hull breach; ship towed to dry dock, non-operational.[54]	Off Novorossiysk, Black Sea	UKR, Sea Baby
5 Aug 2023	USV strike on the sanctioned fuel tanker SIG. Significant damage to hull.[55]	Near Kerch Strait, Black Sea	UKR, Sea Drone
17 July 2023	USV strike on Kerch bridge.[56]	Kerch Strait, Black Sea	UKR, Sea Baby
Feb 2024	Sinking of Tarantul-III-class corvette Ivanovets and of the landing ship Caesar Kunikov (Ropucha class) by a swarm of USVs. First confirmed sinkings of warships by unmanned surface vehicles worldwide.[57]	Black Sea	UKR, Magura V5
31 Dec 2024, 2 Jan 2025	Two Mi-8 helicopters shot down (a third damaged) by an R-73 air-to-air missile fired from a Magura V5. First-ever destruction of an aerial target by an unmanned surface vehicle.[58]	Black Sea	UKR, Magura V5 with R-73
5 Jan 2025	Ukrainian Navy launched deep strikes on Russian Pantsir-S1 air defense systems, using USVs as mobile drone-launch platforms.[59]	Black Sea	UKR, USVs
2 May 2025	Two Su-30 fighter jets shot down by AIM-9M Sidewinder missiles fired from three Magura V7 drones. First-ever destruction of fighter aircraft by USV.[60]	Black Sea	UKR, Magura V7 with AIM-9M Sidewinder
Dec 2025	UUV strike on a Kilo-class submarine (Varshavyanka) using a Sub Sea Baby underwater drone. SBU claimed critical damage to stern and effective disablement; satellite imagery confirms a pier explosion at the attack site. First claimed combat use of a UUV against a submarine worldwide.[61]	Port of Novorossiysk	UKR, Sub Sea Baby

This cooperation is particularly relevant given the increasing cyberattacks, drone incursions, and hybrid operations targeting European ports and maritime infrastructure. Israeli experience in integrated cyber defense, counter-drone systems, and intelligence-supported port security can help strengthen the resilience of German and European ports against sabotage, espionage, and disruptions to maritime logistics chains.

Strategic Outlook

The transformation of the maritime domain through hybrid threats, cyber operations, and autonomous systems creates a strong rationale for deepening German–Israeli maritime cooperation within broader European and Transatlantic security frameworks. The successful collaboration on platforms such as the Dolphin- and Dakar-class submarines, the Sa'ar 6 corvettes, and most recently the Blue Whale unmanned underwater system demonstrates the complementary strengths of both countries in naval technology and maritime security innovation. For the Bundeswehr, it is important to make use of newly established structures such as the Maritime Innovation Center in Kiel to position itself more strongly as an innovation partner rather than solely as a procurement organization.[62]

Beyond the bilateral dimension, these technological and operational synergies also carry growing strategic relevance for the wider Euro-Atlantic security architecture, particularly in regions where maritime competition and hybrid threats are intensifying. The North- and Baltic Sea are of strategic importance for NATO but so are the (Eastern) Mediterranean and the Red Sea. The announced expansion of NATO's CUI activities into the Mediterranean should include mechanisms to integrate Israeli operational experience and intelligence expertise.[63]

At the European level, cooperation with Israel could increasingly be integrated into initiatives such as the PESCO project Critical Seabed Infrastructure Protection (CSIP), in which Germany already participates. This would align with broader European efforts to enhance maritime domain awareness and resilience against hybrid threats.

Germany's coalition agreement emphasizes the promotion of research and development in autonomous and underwater systems.[64] Building on the success of the Blue Whale project, both countries could institutionalize this cooperation through a dedicated German–Israeli Defense Tech Hub focused on maritime security, bringing together industry, research institutions, and naval operators to advance innovation in autonomous systems, maritime cyber defense, and the protection of critical maritime infrastructure. Research within this hub should explicitly embrace a dual-use approach, recognizing that these advances generate civilian spillovers in areas such as environmental monitoring, offshore energy, and port logistics. Civil-military cooperation could therefore be named an explicit innovation policy goal, anchored in the hub's founding mandate.[65]

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

REFERENCES

1. **Bundeswehr:** "Blue Whale: Marine Erhält Neues Unterwassersystem", 25.02.2026, in *https://www.bundeswehr.de/de/organisation/marine/aktuelles/marine-erhaelt-neues-unterwassersystem-blue-whale-6073570.*
2. **Luttwak, Edward N; Shamir, Eitan:** The Art of Military Innovation - Lessons from the Israel Defense Forces, *Harvard University Press, 2023, S.73*
3. **Rhys, John:** "Ukraine Forces Sink Russian Landing Ship with Huge Explosion in Black Sea", 14.02.2024, in *https://www.independent.co.uk/tv/news/russia-ukraine-caesar-kunikov-landing-ship-crimea-b2495964.html.*
4. **Bundeswehr:** "Northern Coasts: Germany's Invite to Baltic Sea Exercises", 26.02.2025, in *https://www.bundeswehr.de/en/organization/navy/news/northern-coasts-germany-baltic-sea-exercise.*
5. **Arts, Sophie;Ondraskove, Jana; Rintakumpu, Frida:** "Tensions Under the Baltic Sea", 10.01.2025, in *https://www.gmfus.org/news/tensions-under-baltic-sea.*
6. **NATO-MARCOM:** "NATO Officially Launches New Maritime Centre for Security of Critical Undersea Infrastructure", 28.05.2024, in *https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui.*
7. **NATO:** "NATO launches ‚Baltic Sentry' to Increase Critical Infrastructure Security", 14.01.2025, in *https://www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-securityl.*
8. **Bewarder, Manuel; Flade, Florian; Kempermann, Antonius:** "Neuer Sabotageverdachtsfall bei der Marine", 21.02.2025, in *https://www.tagesschau.de/investigativ/marine-kriegsschiff-sabotageverdacht-100.html.*
9. **Dittmer, Marco:** "Kabelstränge Durchtrennt: Sabotageverdacht auf Kriegsschiff", 19.02.2025 in *https://www.bild.de/regional/rostock/kabelstraenge-durchtrennt-sabotageverdacht-auf-kriegsschiff-67b57b5e1aeb2534badd0919.*
10. **Bewarder, Manuel; Flade, Florian:** "Hafenarbeiter nach Sabotage an Kriegsschiff Festgenommen' ?", 03.02.2026, in *https://www.tagesschau.de/investigativ/ndr-wdr/sabotage-marine-emden-haftbefehle-100.html.*
11. **Siebold, Sabine** "Drone sightings over German military bases hit record high in October, says official", 28.11.2025, in *https://www.reuters.com/world/drone-sightings-over-german-military-bases-hit-record-high-october-says-official-2025-11-28/.*
12. **Arts, Sophie; Ondraskove, Jana; Rintakumpu, Frida:** "Tensions Under the Baltic Sea", 10.01.2025, in *https://www.gmfus.org/news/tensions-under-baltic-sea.*
13. **Breuner, Frank:** "Nord Stream Explosionen: Neues Buch enthüllt Hintergründe", 27.04.2026, in *https://www.ndr.de/kultur/buch/sachbuecher/nord-stream-explosionen-neues-buch-enthuellt-hintergruende,nordstream-buch-100.html.*
14. **ERR** "China Admits Container Ship Newnew Polar Bear Damaged Undersea Gas Pipeline", 12.08.2024, in *https://news.err.ee/1609422658/china-admits-container-ship-newnew-polar-bear-damaged-undersea-gas-pipeline.*
15. **Lott, Alexander:** "The Baltic Sea Cable-Cuts and Ship Interdiction: the C-LION1 Incident", 26.11.2024, in *https://lieber.westpoint.edu/baltic-sea-cable-cuts-ship-interdiction-c-lion1-incident/.*
16. **Martin, Alexander:** "Finland' Trial of Men Charged over Baltic Sea Cable Damage Hits Choppy Waters", 10.10.2025, in *https://therecord.media/finland-court-decision-undersea-cable-breaks-eagle-s-crew.*
17. **NATO Cooperative Cyber Defence Centre of Exelence:** "Addressing State-Linked Cyber Threats to Critical Maritime Port Infrastructure"; 07.2025, in *https://ccdcoe.org/uploads/2025/07/CCDCOE_Policy_Brief.pdf.*
18. **European Commission:** "Maritime Security Strategy (EUMSS)", 2023, in *https://oceans-and-fisheries.ec.europa.eu/maritime-security/maritime-security-strategy_en.*
19. **PESCO:** "Critical Seabad Infrastructure Protection (CSIP)", in *https://www.pesco.europa.eu/project/critical-seabed-infrastructure-protection-csip/.*
20. **Federal Ministry of Research, Technology and Space:** "Maritime Sicherheit", in *https://www.sifo.de/sifo/de/projekte/schutz-kritischer-infrastrukturen/maritime-sicherheit/maritime-sicherheit_node.html.*
21. **Raydan, Noam:** "The Gaza War's Impact on Energy Security in the East Mediterranean", 01.11.2023, in *https://www.washingtoninstitute.org/policy-analysis/gaza-wars-impact-energy-security-east-mediterranean.*
22. **ZACKS Equity Research:** "Chevron Ordered to Halt Leviathan Gas Production Amid Rising Tensions,"04.03.2025, in *https://finance.yahoo.com/news/chevron-ordered-halt-leviathan-gas-152000778.html.*
23. **Wilkens, Andreas:** "Renewed Sabotage of Fiber Optic Networks in France", 29.07.2024, in *https://www.heise.de/en/news/Renewed-sabotage-of-fiber-optic-networks-in-France-9816918.html.*
24. **Darrah, Michael; Jakobsen, Eskil; Monaghan, Sean; Svendsen, Otto:** "Red Sea Cable Damage Reveals Soft Underbelly of Global Economy", 07.03.2024; in *https://www.csis.org/analysis/red-sea-cable-damage-reveals-soft-underbelly-global-economy.*
25. **World Bank:** "Shipping and Ports", in *https://www.worldbank.org/ext/en/topic/transport/shipping-and-ports.*
26. **Canal, Allie; Lorsch, Emily; Steinberg, Kayla:** "Shipping Slows to a Crawl through Strait of Hormuz, Threatening to Snarl International Trade", 04.03.2026, in *https://www.nbcnews.com/business/economy/shipping-slows-crawl-strait-hormuz-threatening-snarl-international-tra-rcna261797.*
27. **European Council:** "Rotes Meer: Rat Verlängert Mandat der Operation ASPIDES zur Wahrung der Freiheit der Schifffahrt", 23.02.2026, in *https://www.consilium.europa.eu/de/press/press-releases/2026/02/23/red-sea-council-extends-the-mandate-of-operation-aspides-to-safeguard-freedom-of-navigation/.*
28. **Chaix, Shannon:** "Beyond Catch and Release: An Analysis of the EU Naval Force's Disruption and Deterrence of Somalian Piracy", 02.08.2025, in *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3221447.*
29. **Federal Ministry of Defence:** "The Overall Concept of Military Defence", 04.2026, in *https://www.bmvg.de/resource/blob/6093998/678875025812878cfa657f9801f62ffc/dl-gesamtkonzeption-der-verteidigung-eng-data.pdf.*
30. **McCombie, Stephen, Pijpker; Stephen:** "Cyber Attacks on Vessels: a Review for the Last 20 Years", 12.2025, in *https://researchers.mq.edu.au/en/publications/cyber-attacks-on-vessels-a-review-for-the-last-20-years/.*
31. **Šilobritas, Žygimantas:** "Po pasipylusių žinių apie GPS ryšio trukdžius", 28.01.2025, in *https://www.lrytas.lt/verslas/rinkos-pulsas/2025/01/28/news/po-pasipylusiu-ziniu-apie-gps-rysio-trukdzius-ramina-nerimaujancius-skristi-saugu-36228716.*
32. **Euronews:** "Lithuania Blames Russia for Large Rise in GPS Jamming Incidents?", 22.07.2025, in *https://www.euronews.com/2025/07/22/lithuania-blames-russia-for-large-rise-in-gps-jamming-incidents.*
33. **The Maritime Executive:** "Polish Researchers Detect Ship-Based GPS Jammers in Baltic Seas", 03.03.2025, in *https://maritime-executive.com/article/polish-researchers-detect-ship-based-gps-jammers-in-baltic-sea.*
34. **Wiese Bockmann, Michelle:** "Russia-Linked Cable-Cutting Tanker Seized by Finland 'was Loaded with Spying Equipment", 27.12.2025, in *https://www.lloydslist.com/LL1151955/Russia-linked-cable-cutting-tanker-seized-by-Finland-was-loaded-with-spying-equipment.*
35. **Braw, Elisabeth:** "The Shadow Fleet is Undermining the Maritime Order more Brazenly than ever", 22.04.2026, in *https://www.atlanticcouncil.org/in-depth-research-reports/the-shadow-fleet-is-undermining-the-maritime-order-more-brazenly-than-ever/.*
36. **NL-Times:** "Freighters with Russian Crew Deployed Drones in European

Airspace: Report", 10.06.2025, in *https://nltimes.nl/2025/06/10/freighters-russian-crew-deployed-drones-european-airspace-report.*

37. Ibid.

38. **Erling,Barbara; Strzelecki, Marek:** "Poland Says Russian Ship Performed Suspicious Manouvres Near Cable", 21.05.2025, in *https://www.reuters.com/world/europe/poland-says-russian-ship-performed-suspicious-manoeuvres-near-cable-sweden-2025-05-21/.*

39. **Seibt, Sebastian:** "Denmark Drone Incursions: All Signs Point to Russia?", 26.09.2025, in *https://www.france24.com/en/europe/20250926-denmark-drone-incursions-all-signs-point-to-russia-suspect-ships.*

40. **Braw, Elisabeth:** "The shadow fleet is undermining the maritime order", 22.04.2026, in *https://www.atlanticcouncil.org/in-depth-research-reports/the-shadow-fleet-is-undermining-the-maritime-order-more-brazenly-than-ever/.*

41. **Haifa Port:** "Drive-through Security Screening of Empty Sea Containers Request for Information (RFI)", 23.10.2019 in *https://www.haifaport.co.il/wp-content/uploads/2019/10/RFI-DRIVE-THROUGH-SECURITY-SCREENING-OF-EMPTY-SEA-CONTAINERS.pdf.*

42. **Port of Hamburg:** "Hamburger Hafen: Umschlagszahlen 2025 auf einen Blick", 19.02.2026, in *https://www.hafen-hamburg.de/de/presse1/news/hamburger-hafen-umschlagszahlen-2025-auf-einen-blick/.*

43. **Port2Port:** "Supply Chain Resilience: Israel Ports Break Records Despite Red Sea Tensions", 27.01.2026 in *https://en.port2port.co.il/article/Sea-Transport/Ports/Supply-Chain-Resilience-Israel-Ports-Break-Records-Despite-Red-Sea-Tensions/.*

44. **Licht, Karl:** "The German-Israeli Defense Cooperation - Tacking Stock", 12.2025, in *https://elnet-deutschland.de/wp-content/uploads/2025/12/Online_Policy-Briefing-ESDI_EN.pdf.*

45. **Mergener, Hans Uwe:** "Die Taufe der INS Drakon – Ein diskretes Ereignis von großer Bedeutung", 13.11.2024, in *https://esut.de/2024/11/meldungen/54733/die-taufe-der-ins-drakon-ein-diskretes-ereignis-von-grosser-bedeutung/.*

46. **Linnemann, Navid:** "Israelische Marine: Vierte und letzte Korvette der Sa'ar-6-Klasse in Dienst gestellt", 14.12.2023, in *https://defence-network.com/letzte-korvette-der-saar-6-klasse-in-dienst/.*

47. **Bob, Yonah Jeremy:** "What Elbit's new deal with TKMS means for submarine manufacturing independence - analysis", 19.02.2026, in *https://www.jpost.com/defense-and-tech/article-887300.*

48. **Israel Defense Forces:** "Israeli and German Navies Sign a Two-Year Work Plan", 04.07.2024, in *Israeli and German Navies Sign a Two-Year Work Plan.*

49. **Bundeswehr:** "Blue Whale: Marine erhält neues Unterwassersystem", 25.02.2026, in *https://www.bundeswehr.de/de/organisation/marine/aktuelles/marine-erhaelt-neues-unterwassersystem-blue-whale-6073570.*

50. **Bundeswehr:** "Bundeswehr bestellt Drohnen zur Seefernaufklärung und U-Boot-Jagd", 12.01.2026, in *https://www.bundeswehr.de/de/meldungen/bundeswehr-mq-9b-drohnen-seefernaufklaerung-u-boot-jagd-6057512.*

51. **Bundeswehr:** "German Heron TP überwacht Ostsee", 09.04.2025, in *https://www.bundeswehr.de/de/organisation/luftwaffe/aktuelles/drohnen-ueberwachung-ostsee-5921548.*

52. **Federal Ministry of the Interior:** "Zusammenarbeit zur Cybersicherheit mit Israel wird ausgebaut", 12.01.2026, in *https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2026/01/israel-dobrindt.html.*

53. **Hamburg Chamber of Commerce:** "Hamburg and Israel launch Innovation Partnership", 21.02.2023, in *https://hamburg-business.com/en/news/hamburg-and-israel-launch-innovation-partnership.*

54. **Wertheim, Eric:** "Ukraine's Magura Naval Drones: Black Sea Equalizers", 09.2025, in *https://www.usni.org/magazines/proceedings/2025/september/ukraines-magura-naval-drones-black-sea-equalizers.*

55. **Newdick, Thomas:** "Image Of Russian Warship's Hull Torn Open By Ukrainian Drone Boat Emerges", 11.08.2023, in *https://www.twz.com/image-of-russian-warships-hull-torn-open-by-ukrainian-drone-boat-emerges.*

56. **Cook Ellie:** "Ukraine's 'Sea Baby' Drones Target Russia's Black Sea Fleet, Crimea Bridge", 16.08.2023, in *https://www.newsweek.com/ukraine-sea-baby-naval-drones-usv-kerch-bridge-russia-black-sea-fleet-1820137.*

57. **Wertheim, Eric:** "Ukraine's Magura Naval Drones: Black Sea Equalizers", 09.2025, in *https://www.usni.org/magazines/proceedings/2025/september/ukraines-magura-naval-drones-black-sea-equalizers.*

58. **Kushnikov, Kyrylo:** "Ukrainian Naval Drone Hits Russian Mi-8 for First Time", 31.12.2024, in *https://militarnyi.com/en/news/ukrainian-naval-drone-hits-russian-mi-8-for-first-time/.*

59. **Howard Altman:** "Two Russian Su-30 Flankers Downed By AIM-9s", 03.05.2025, *https://www.twz.com/news-features/two-russian-su-30-flankers-downed-by-aim-9s-fired-from-drone-boats-ukrainian-intel-boss.*

60. **Defence Intelligence of Ulraine (GUR):** "The Era of Magura", 15.05.2025, in *https://gur.gov.ua/en/content/era-maury-komanda-hur-vpershe-prezentuvala-novitni-morski-drony-zdatni-nyshchyty-vorozhi-korabli-ta-litaky.*

61. **Zoria, Yuri:** "Another Russian shadow fleet tanker wrecked by Sea Baby", 11.12.2025, in *https://euromaidanpress.com/2025/12/11/another-russian-shadow-fleet-tanker-wrecked-by-sea-baby-drones-in-the-black-sea/.*

62. **NDR:** "Kiel bekommt maritimes Innovationszentrum der Bundeswehr", 21.05.2026, in *https://www.ndr.de/nachrichten/schleswig-holstein/kiel_neumuenster_ploen_rendsburg-eckernfoerde/kiel-bekommt-maritimes-innovationszentrum-der-bundeswehr,regionkielnews-2162.html.*

63. **NATO:** "NATO expands its engagement on critical undersea infrastructure in the Mediterraneanr", 21.11.2025, in *https://www.nato.int/en/news-and-events/articles/news/2025/11/21/nato-expands-its-engagement-on-critical-undersea-infrastructure-in-the-mediterranean.*

64. **Coalition Agreement 2025 CDU/CSU and SPD:** "Verantwortung für Deutschland", 06.05.2026, in *https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav_2025.pdf.*

65. **Ovens, Carsten:** "Die deutsch-israelische Militärkooperation muss ausgebaut werden", 18.05.2025, in *https://table.media/security/tablestandpunkt/die-deutsch-israelische-militaerkooperation-muss-ausgebaut-werden.*

ELNET

berlin@elnetwork.eu

elnet-deutschland.de

@ElnetD

@elnet_D

The European Leadership Network (ELNET) is a think tank and network dedicated to European-Israeli relations. Founded in 2007, ELNET operates independently and across party lines, with offices in Berlin, Brussels, Jerusalem, London, Paris, Rome, and Warsaw. Its work focuses on foreign and security policy, combating antisemitism, and innovation.