

## REPORT

**DEUTSCH-ISRAELISCHE ZUSAMMENARBEIT IN DER MARITIMEN SICHERHEIT: AUF KURS IN EINER ÄRA HYBRIDER BEDROHUNGEN**

*Autor: Karl Licht  
Stand: Juni 2026*

**HANDLUNGSEMPFEHLUNGEN**

- #1 Stärkung der Souveränität über kritische maritime Infrastruktur** durch eine vertiefte deutsch-israelische Zusammenarbeit in den Bereichen maritime Cybersicherheit, Lieferkettensicherheit sowie der Verringerung strategischer technologischer Abhängigkeiten in Häfen, an Bord von Schiffen und in maritimen Kommunikationsnetzen.
- #2 Entwicklung eines gemeinsamen Verständnisses maritimer Bedrohungen** durch die engere Einbindung militärischer, nachrichtendienstlicher, polizeilicher und kommerzieller Akteure zur Verbesserung der maritimen Lagebilderstellung, Attribution und des Schutzes kritischer Infrastruktur – insbesondere im östlichen Mittelmeer sowie zur Unterstützung von NATO-Initiativen.
- #3 Entwicklung eines maritimen System-of-Systems-Ansatzes** durch die Integration autonomer Systeme, moderner Unterwasser-Sensorik, leistungsfähiger Command-and-Control-Strukturen sowie vernetzter Sensorsysteme zum Schutz kritischer maritimer Infrastruktur.
- #4 Einrichtung eines deutsch-israelischen Defense-Tech-Hubs für maritime Sicherheit** zur Beschleunigung des Technologietransfers, zur gezielten Förderung von Startups im Verteidigungs- und Dual-Use-Bereich sowie zur Stärkung der Zusammenarbeit zwischen Industrie, Staat, Wissenschaft und Investoren.
- #5 Förderung einer Kultur der Eigeninitiative, Anpassungsfähigkeit und Einsatzbereitschaft** durch gemeinsame Übungen, Personalaustausch und innovative Formate zur Stärkung von Resilienz, dezentraler Entscheidungsfindung sowie der Fähigkeit zum Handeln unter anspruchsvollen Einsatzbedingungen.

Die maritime Sicherheit befindet sich in einem tiefgreifenden Wandel. Flottengröße und Tonnage allein entscheiden nicht mehr über den Ausgang von Auseinandersetzungen auf See. Vielmehr prägt ein wachsendes Spektrum hybrider Bedrohungen die maritime Domäne. Dazu zählen die Sabotage kritischer Unterwasserinfrastruktur (Critical Undersea Infrastructure, CUI), Drohnenüberflüge über Häfen und Marinestützpunkten und Cyberangriffe auf Schiffe. Darüber hinaus zeigt die Verbreitung unbemannter maritimer Systeme, dass sich die bereits in der Luftkriegführung sichtbaren Kostenasymmetrien nun auch auf die maritime Domäne erstrecken. Wie das Beispiel der Shahed- und kostengünstiger FPV-Drohnen verdeutlicht, können vergleichsweise günstige Systeme weitaus komplexeren Plattformen unverhältnismäßig hohe Kosten aufzwingen und damit das etablierte Kräftegleichgewicht auf See verschieben.

In diesem zunehmend instabilen Umfeld gewinnt die deutsch-israelische Zusammenarbeit weiter an Bedeutung. Diese Partnerschaft kann auf einer langen Tradition aufbauen – von der Übergabe von Konstruktionsplänen für Schnellboote in den 1960er-Jahren über die seit den 1990er-Jahren in Deutschland gebauten U-Boote bis hin zum modernen autonomen Unterwassersystem Blue Whale. Letzteres veranschaulicht den Wandel der deutsch-israelischen maritimen Kooperation: Israel ist nicht länger bloß Empfänger deutscher Marinefähigkeiten, sondern tritt zunehmend als Mitgestalter gemeinsamer technologischer Entwicklung und maritimer Verteidigungsinnovation hervor.

Diese Entwicklung stand im Mittelpunkt des ESDI-Roundtables „Maritime Security: From Decades of

Cooperation to Sailing the Seas Ahead“, der Mitte Juni 2026 in Partnerschaft mit der Handelskammer Hamburg im Rahmen der ELNET Security & Defense Initiative (ESDI) – einer Plattform zur Stärkung der strategischen und sicherheitspolitischen Zusammenarbeit – ausgerichtet wurde.

Aufbauend auf dem [ESDI-Policy-Briefing „German-Israeli Cooperation in Maritime Security: Sailing Ahead in an Era of Hybrid Threats“](#) brachte die Veranstaltung Vertreterinnen und Vertreter aus Industrie, Wissenschaft, Militär, Polizei und weiteren relevanten Behörden zusammen. Ziel war es, das aktuelle Bedrohungsumfeld zu bewerten und gemeinsame Ansätze für neue Herausforderungen der maritimen Sicherheit zu erarbeiten.

Der vorliegende Bericht fasst die zentralen Erkenntnisse und Handlungsempfehlungen des Roundtables zusammen.

### #1 Souveränität über kritische maritime Infrastruktur stärken

Maritime Sicherheit hängt zunehmend von der Kontrolle über kritische Technologien ab. Häfen, Schiffe und andere kritische maritime Infrastrukturen sind heute in hohem Maße von digitalen Systemen abhängig, die durch Cyberangriffe, verwundbare Lieferketten oder im Ausland entwickelte und gefertigte Hardware angreifbar werden. Der zunehmende Einsatz chinesischer Technologien in Hafenanlagen verdeutlicht, dass strategische Verwundbarkeiten häufig weniger aus den Eigentumsverhältnissen von Häfen als vielmehr aus der eingesetzten Technologie selbst entstehen. So wie Drohnen den Zugang zu militärischen Fähigkeiten auf dem Gefechtsfeld grundlegend verändert haben, erleichtern Fortschritte im Bereich der Künstlichen Intelligenz einer wachsenden Zahl von Akteuren die Durchführung komplexer Cyberoperationen. Dadurch werden künftig selbst hochgeschützte Systeme – einschließlich maritimer Plattformen – einem breiteren Spektrum von Cyberbedrohungen ausgesetzt sein.

Deutschland und Israel sollten ihre Zusammenarbeit beim Schutz kritischer maritimer Systeme vor Cyberangriffen sowie beim Abbau strategischer technologischer Abhängigkeiten deutlich vertiefen. Ein mögliches Vorbild bietet Israels Umgang mit chinesisch errichteter Bahninfrastruktur: Während die physische Infrastruktur erhalten bleibt, werden digitale und vernetzte Komponenten durch eigene Systeme ersetzt. Ein vergleichbarer Ansatz ließe sich auch auf Hafeninfrastrukturen und maritime Kommunikationsnetze über-

tragen. Die von Bundesminister Dobrindt im Januar 2026 angekündigte Ausweitung der deutsch-israelischen Zusammenarbeit im Bereich der Cybersicherheit („Cyberdome“) sollte daher ausdrücklich auch die maritime Dimension einbeziehen.

### #2 Ein gemeinsames Verständnis maritimer Bedrohungen entwickeln

Maritime Bedrohungen sind heute zunehmend hybrid, domänenübergreifend und oft schwer zuzuordnen. Was mit der Aufklärung durch Drohnen oder verdächtigen Schiffsbewegungen beginnt, kann schrittweise bis zur Sabotage kritischer Infrastruktur eskalieren – wie die jüngsten Vorfälle im Zusammenhang mit Unterseekabeln, Energieinfrastruktur und Marineschiffen verdeutlichen. Russlands schrittweises Vorgehen in europäischen Gewässern zeigt, wie staatliche Akteure gezielt Verwundbarkeiten unterhalb der Schwelle eines offenen Konflikts ausloten, bevor sie zu weitergehenden disruptiven Maßnahmen übergehen. Deutschland und Israel sollten deshalb ihre Zusammenarbeit bei der maritimen Lagebilderstellung und Bedrohungsanalyse ausbauen. Denn Störungen an strategischen Engpässen wie dem Roten Meer oder der Straße von Hormus können innerhalb kürzester Zeit erhebliche Auswirkungen auf globale Lieferketten und die internationale Sicherheit entfalten.

Ein gemeinsames maritimes Lage- und Bedrohungsverständnis sollte militärische, nachrichtendienstliche, polizeiliche und wirtschaftliche Akteure zusammenführen und sowohl die physische als auch die digitale Dimension des maritimen Raums berücksichtigen. Besonderes Augenmerk sollte dabei auf den Schutz kritischer Unterwasserinfrastruktur, von Häfen, Energieanlagen und maritimen Kommunikationsnetzen gelegt werden. Israels Erfahrungen beim Schutz seiner Offshore-Gasfelder und Deutschlands Rolle als zentraler europäischer Logistikstandort ergänzen sich in besonderer Weise und bieten eine solide Grundlage, um die Resilienz gegenüber neuen maritimen Bedrohungen gemeinsam zu stärken.

Vor diesem Hintergrund sollte die angekündigte Ausweitung der NATO-Initiativen zum Schutz von CUI auf den Mittelmeerraum durch eine engere Zusammenarbeit mit Israel flankiert werden. Aufgrund seiner strategischen Lage im östlichen Mittelmeer und seiner operativen Erfahrungen kann Israel einen wichtigen Beitrag zum Informationsaustausch, zur gemeinsamen Lagebilderstellung und zum Schutz kritischer maritimer Infrastruktur leisten.

### #3 Einen maritimen System-of-Systems-Ansatz entwickeln

Der maritime Gefechtsraum der Zukunft wird durch unbemannte und autonome Systeme, Künstliche Intelligenz sowie domänenübergreifende Operationen geprägt sein. Die jüngsten Konflikte zeigen, dass kostengünstige Technologien hochpreisige Plattformen mit geringem Mitteleinsatz erheblich unter Druck setzen können. Fortschritte in den Bereichen Autonomie und Künstliche Intelligenz ermöglichen zudem koordinierte Schwarm- und Mesh-Angriffe, bei denen eine Vielzahl vernetzter Systeme klassische Verteidigungsmechanismen durch Geschwindigkeit, Masse und dezentrale Entscheidungsfindung überwinden kann. Dadurch verschieben sich die Kräfteverhältnisse zunehmend zugunsten der Offensive.

Mit der wachsenden Bedrohung für Marineplattformen und kritische maritime Infrastruktur durch hochentwickelte physische und digitale Angriffe wird der operative Erfolg künftig weniger von der Leistungsfähigkeit einzelner Plattformen abhängen als von der Fähigkeit, Sensoren, Wirkmittel, autonome Systeme sowie Führungs- und Informationssysteme zu einem integrierten System of Systems zu vernetzen.

Der wirksame Schutz kritischer maritimer Infrastruktur setzt eine kontinuierliche Unterwasserlageerfassung voraus. Bestehende Seekabel, Kommunikationsverbindungen und weitere Unterwasserinfrastrukturen könnten dabei als verteilte Sensorsysteme genutzt werden, um Aktivitäten unter Wasser über große Seegebiete hinweg frühzeitig zu erkennen und zu überwachen. Dadurch ließen sich sowohl kritische Unterwasserinfrastrukturen als auch die Sicherheit maritimer Versorgungs- und Handelsrouten (Sea Lines of Communication, SLOC) nachhaltig stärken.

Das autonome Unterwasserfahrzeug Blue Whale verdeutlicht das Potenzial einer vertieften deutsch-israelischen Zusammenarbeit. Darauf aufbauend sollte sich die bilaterale Kooperation auf autonome maritime Systeme, den Schutz kritischer Unterwasserinfrastruktur, Unterwasser-Sensortechnologien, Cyberresilienz sowie integrierte Führungs- und Gefechtsführungssysteme (Battle Management) konzentrieren. Ziel sollte es sein, Abschreckung und Lagebild zu verbessern sowie die operative Handlungsfähigkeit in der maritimen Domäne insgesamt zu erhöhen.

Darüber hinaus sollten Deutschland und Israel ihre Zusammenarbeit beim Austausch operativer Erfahrungen ausbauen. Dazu gehören insbesondere die Lehren der Ukraine aus dem Schutz kritischer Hafeninfrastruktur, etwa bei der integrierten Drohnenabwehr und dem Einsatz unbemannter Systeme einschließlich der im Schwarzen Meer erfolgreich eingesetzten Hard-Kill-Fähigkeiten. Während die Ukraine wichtige Erkenntnisse für die asymmetrische Seekriegführung liefert, verfügt Israel über umfangreiche Erfahrungen bei der Integration maritimer, luftgestützter, cybergestützter und unbemannter Fähigkeiten in gemeinsamen Operationen. Als Betreiber deutscher Marineplattformen bietet Israel zudem wertvolle operative Erkenntnisse für die gemeinsame Weiterentwicklung künftiger Konzepte der Seekriegführung – insbesondere im Bereich des Manned-Unmanned Teaming, also des integrierten Zusammenwirkens bemannter und autonomer maritimer Systeme.

### #4 Ein deutsch-israelisches Innovationsökosystem für Verteidigung und Dual-Use aufbauen

Die Sicherung des technologischen Vorsprungs im Bereich der maritimen Sicherheit erfordert nicht nur die Entwicklung neuer Fähigkeiten, sondern auch ein leistungsfähiges Innovationsökosystem. Überall in Europa entwickeln Startups vielversprechende Technologien – etwa für autonome Systeme, maritime Überwachung, Künstliche Intelligenz, Cyberresilienz oder den Schutz kritischer Infrastruktur. Häufig scheitert der Übergang von der Entwicklung zur Anwendung jedoch an fehlender Frühphasenfinanzierung oder komplexer Beschaffungsprozesse. Deutschland, Israel und ihre europäischen Partner sollten daher die Finanzierungsinstrumente für Startups im Verteidigungs- und Dual-Use-Bereich gezielt ausbauen und zugleich Rahmenbedingungen schaffen, die eine engere Zusammenarbeit zwischen Startups, etablierter Industrie, Investoren, Wissenschaft und staatlichen Akteuren ermöglichen.

Israels Innovationsökosystem zeigt, wie ein enges Zusammenspiel von Streitkräften, Industrie, Investoren und Startups technologische Innovationen beschleunigen kann. Die Programme der Forschungs- und Entwicklungsdirektion des israelischen Verteidigungsministeriums (MAFAT) verdeutlichen, wie gezielte Förderung, Acceleratorprogramme und Frühphasenfinanzierung dazu beitragen, innovative Ideen zügig in einsatzfähige militärische Fähigkeiten zu überführen. Diese Erfahrungen können Deutschland als Vorbild dienen, während die Bundeswehr ihre Innovationsstrukturen

weiter ausbaut – etwa mit dem neuen Innovationszentrum der Bundeswehr in Erding.

Um diese Zusammenarbeit dauerhaft zu verankern, sollten Deutschland und Israel einen gemeinsamen German-Israeli Defense Tech Hub für maritime Sicherheit schaffen. Als zentrale Innovationsplattform im Verteidigungs- und Dual-Use-Bereich könnte er Startups, etablierte Unternehmen, Forschungseinrichtungen, Investoren und staatliche Akteure zusammenbringen, den Technologietransfer beschleunigen, gemeinsame Entwicklungsprojekte und Joint Ventures fördern sowie die gemeinsame Fähigkeitsentwicklung vorantreiben.

### #5 Eine Kultur der Eigeninitiative, Anpassungsfähigkeit und Einsatzbereitschaft fördern

Der Erfolg militärischer Operationen und der Schutz kritischer Infrastrukturen werden künftig nicht allein von technologischer Überlegenheit abhängen, sondern ebenso von der Fähigkeit von Organisationen und ihrem Personal, sich schnell anzupassen, unter Unsicherheit Entscheidungen zu treffen und auch dann wirksam zu handeln, wenn Systeme gestört, beeinträchtigt oder ausgefallen sind.

Künftige Konflikte werden jene Organisationen begünstigen, die schneller lernen und sich rascher anpassen

können als ihre Gegner. Auf institutioneller Ebene bedeutet dies, mit der Geschwindigkeit des Wandels Schritt zu halten, bürokratische Hemmnisse abzubauen, Entscheidungsprozesse zu beschleunigen und ein ausgeprägtes Bewusstsein für Dringlichkeit zu entwickeln. Angesichts des Umfangs und der Komplexität kritischer Infrastrukturen ist ein vollständiger Schutz nicht realisierbar. Organisationen müssen daher davon ausgehen, selbst Ziel von Angriffen zu werden, und ihre Anstrengungen auf Resilienz, Redundanz sowie die schnelle Wiederherstellung ihrer Handlungsfähigkeit ausrichten.

Während Israels anhaltende Konfrontation mit vielfältigen Sicherheitsbedrohungen eine tief verankerte Kultur der Resilienz hervorgebracht hat, hat Deutschland – obwohl es zunehmend hybriden Bedrohungen ausgesetzt ist – bislang kein vergleichbares Dringlichkeitsbewusstsein entwickelt. Ein regelmäßiger Austausch zwischen militärischen, staatlichen, industriellen und wissenschaftlichen Akteuren beider Länder kann dazu beitragen, in deutschen Institutionen eine stärkere Kultur der Resilienz und Anpassungsfähigkeit zu fördern. Übungsseerien wie Red Storm in Hamburg bieten hierfür wertvolle Gelegenheiten, indem sie nicht nur die Interoperabilität verbessern, sondern zugleich Eigeninitiative, dezentrale Entscheidungsfähigkeit und operative Einsatzbereitschaft stärken.

## Info

### DIE ELNET SECURITY & DEFENSE INITIATIVE (ESDI)

*Die sicherheitspolitische Zusammenarbeit zwischen Deutschland und Israel blickt auf eine lange Entwicklung zurück. Die ELNET Security & Defense Initiative (ESDI) wurde im Juli 2025 ins Leben gerufen, um angesichts globaler Bedrohungslagen und technologischer Umbrüche neue Wege der Kooperation zu begehen. Ziel der Initiative ist es, den strategischen Dialog zu vertiefen, gemeinsame Innovationspotenziale zu erschließen und die deutsch-israelische Partnerschaft auf eine nachhaltige, strukturell tragfähige Basis zu stellen.*

**European Leadership Network (ELNET)**



berlin@elnetwork.eu

 elnet-deutschland.de

 @ElnetD

 @elnet\_D