

REPORT

DIE REVOLUTION DER KLEINEN DROHNEN: DEUTSCH-ISRAELISCHE PERSPEKTIVEN AUF NEUE SICHERHEITSHERAUSFORDERUNGEN

Autor: Karl Licht
Stand: Februar 2026

HANDLUNGSEMPFEHLUNGEN

#1 Stärkung der zivil-militärischen Koordination durch klar definierte Zuständigkeiten zwischen zivilen und militärischen Akteuren, um Lücken bei Erkennung, Zuordnung und Reaktion zu schließen.

#2 Entwicklung eines Luftverkehrsmanagementsystems für niedrige Flughöhen, das autorisierte Drohnen von Bedrohungen aus der Luft unterscheiden kann und damit verhältnismäßige Reaktionen ermöglicht.

#3 Förderung von Interoperabilität und Standardisierung durch gemeinsame deutsch-israelische technische Standards, damit Sensoren, Effektoren und Führungsstrukturen nahtlos zusammenarbeiten können.

#4 Beschleunigung von Beschaffungs- und Innovationszyklen, indem langwierige Vergabeverfahren durch agile und anpassungsfähige Rahmenwerke ersetzt werden, die schnelle Tests, Einführung und kontinuierliche Weiterentwicklung von C-UAS-Technologien angesichts sich rasch wandelnder Bedrohungen erlauben.

#5 Einrichtung eines German-Israeli Defense Tech Hub, um die bilaterale Zusammenarbeit in Forschung, Prototyping und einsatznaher Weiterentwicklung zu institutionalisieren. Dabei soll Israels operative Erfahrungen mit Deutschlands industrieller und technologischer Infrastruktur verbunden werden, um einen qualitativen Vorsprung zu sichern.

Kleine Drohnen (sUAS) sind zu einem prägenden Merkmal moderner Konflikte und hybrider Sicherheitsherausforderungen geworden. Ihr Dual-Use-Charakter und die einfache Modifizierbarkeit ermöglichen es einer Vielzahl von Akteuren, sie für schädliche Absichten zu nutzen. Während des Besuchs des deutschen Bundesinnenministers in Israel im Januar 2026 vereinbarten beide Länder, ihre Zusammenarbeit nicht nur im Bereich der Cybersicherheit, sondern auch bei der Drohnenabwehr (C-UAS) zu intensivieren.

Diese Zusammenarbeit stand auch im Mittelpunkt des ersten virtuellen deutsch-israelischen Roundtables, der am 20. Januar 2026 im Rahmen der ELNET Security & Defense Initiative (ESDI) stattfand. ELNET brachte eine hochrangige Expertengruppe aus Politik, Ministerien, Forschung und Industrie zusammen, um die sicherheitspolitischen Herausforderungen, die von sUAS für Deutschland und Israel ausgehen, zu diskutieren und gemeinsame Lösungsansätze zu entwickeln. Das ESDI Policy Briefing *Die Revolution der kleinen Drohnen: Deutsch-Israelische Perspektiven auf neue Sicherheitsherausforderungen* bildete die Grundlage der Diskussion. Der folgende Report fasst die wichtigsten Erkenntnisse und Empfehlungen der Veranstaltung zusammen.

Das Bedrohungsumfeld in Europa und im Nahen Osten

Die Bedrohung durch sUAS hat sich in Europa und im Nahen Osten unterschiedlich entwickelt. Israel sieht sich seit Mitte der 2000er-Jahre mit der feindlichen Nutzung von Drohnen konfrontiert. Zu einer greifbaren sicherheitspolitischen Herausforderung wurden sie am Ende des Libanonkriegs 2006, als vier im Iran hergestellte Drohnen mit jeweils rund zehn Kilogramm Sprengstoff in den israelischen Luftraum eindrangen. Diese Erfahrung veranlasste Israel, operativ erprobte, mehrschichtige C-UAS-Fähigkeiten aufzubauen.

In Deutschland und in Europa insgesamt entwickelte sich die Wahrnehmung der Bedrohung durch sUAS schrittweise. Ein frühes Schlüsselereignis war 2013, als eine kleine Drohne während einer Wahlkampfveranstaltung in die Nähe von Bundeskanzlerin Angela Merkel flog. Der Vorfall legte erhebliche Schwachstellen der Luftraumsicherheit offen und löste erste politische und institutionelle Debatten aus. Dennoch blieben Gegenmaßnahmen über Jahre hinweg fragmentiert und reaktiv, da der politische Druck für eine koordinierte Entwicklung fehlte.

Eine entscheidende Zäsur brachte erst Russlands vollumfängliche Invasion der Ukraine im Jahr 2022. Der Krieg zeigte die militärische Wirksamkeit von sUAS bei Aufklärung, Zielerfassung und im direkten Angriff. Gleichzeitig nahm die Zahl drohnenbezogener Vorfälle, von denen viele Russland zugeschrieben werden können, über kritischer Infrastruktur (KRITIS) und militärischen Einrichtungen in Europa deutlich zu. Diese Entwicklungen veränderten die Bedrohungswahrnehmung in Deutschland grundlegend: sUAS wurden vom Nischenthema zur anerkannten strategischen Herausforderung für die innere Sicherheit und waren zugleich Fragen nach der künftigen Kriegsführung der NATO auf. Auch die Hamas setzte im Krieg gegen Israel sUAS ein, allerdings blieb der Umfang ihres Einsatzes begrenzt, und die israelischen Streitkräfte (IDF) konnten ihren traditionellen Ansatz der verbundenen Waffen wirksam umsetzen.

Während Israel in einem permanent umkämpften Sicherheitsumfeld agiert, sieht sich Deutschland einer neuen hybriden Bedrohungslage gegenüber, und bei-

de Länder stehen nun vor einer gemeinsamen Sicherheitsrealität, die durch sUAS geprägt ist. Während des Roundtables wurden die folgenden Empfehlungen für den Umgang mit der Revolution der kleinen Drohnen entwickelt.

#1 Stärkung der zivil-militärischen Koordination

Eine wirksame Drohnenabwehr erfordert die enge Verzahnung ziviler und militärischer Akteure. Deutschland passt derzeit seine Sicherheitsarchitektur, unter anderem durch Änderungen im Luftsicherheitsgesetz sowie durch den Aufbau spezieller Einheiten und eines dedizierten Abwehrzentrums, an. Dennoch bleiben Zuständigkeiten für Luftraumsicherheit und den Schutz kritischer Infrastrukturen auf viele Akteure verteilt, was zu Lücken im Lagebild und zu verzögerten Reaktionen führt.

Silodenken muss beendet und ein echtes zivil-militärisches Koordinierungsmodell geschaffen werden. Dazu gehören gemeinsame Führungsstrukturen, geteilte Bedrohungsanalysen und standardisierte Verfahren zur Erkennung, Identifizierung und Reaktion mit klar definierten Verantwortlichkeiten. Ein Echtzeit-Datenaustausch zwischen Polizei, Flugsicherung und Bundeswehr ist entscheidend für ein gemeinsames Lagebild. Regelmäßige Übungen und szenariobasiertes Training könnten zusätzlich Interoperabilität und Vertrauen stärken.

Israel hat Erfahrung mit der Verwaltung eines vollen und von Bedrohungen geprägten Luftraums und zeigt, dass die Wirksamkeit von C-UAS von nahtloser Koordination abhängt. Besonders im zivilen Umfeld müssen eingesetzte Technologien kontrollierbare und vorhersehbare Wirkungen gewährleisten, um Risiken für Bevölkerung und Infrastruktur zu minimieren. Deutschland kann hiervon lernen. Zugleich unterscheidet sich die Lage: Israels kritische Infrastruktur ist im Gegensatz zu Deutschlands stark zentralisiert – so hat das Land nur zwei große Kraftwerke, in Deutschland sind es über 70. Israel könnte von deutschen Ansätzen zum Schutz dezentraler Strukturen und darüber hinaus von regulatorischen und rechtlichen Rahmenbedingungen lernen.

#2 Entwicklung eines Luftverkehrsmanagementsystems für niedrige Flughöhen

Die rasche Verbreitung von sUAS erinnert an die Anfangszeit der Cybersicherheit, als der demokratisierte Zugang zu Technologie unerwartete Risiken schuf. Nicht jede Drohne stellt eine Bedrohung dar; viele werden legitim für kommerzielle und öffentliche Zwecke genutzt. Die meisten Vorfälle beginnen in einer Grauzone mit unklaren Absichten, können jedoch schnell eskalieren. Ein modernes System muss daher kooperative und autorisierte Dроhnen von potenziell feindlichen unterscheiden.

Deutschland sollte einen einheitlichen Rahmen entwickeln, der Registrierung, digitale Identifizierung und Echtzeit-Verfolgung von Dроhnen unterhalb des kontrollierten Luftraums integriert. Das erhöht Transparenz und ermöglicht es den Behörden, Anomalien rasch zu erkennen und verhältnismäßig zu reagieren. Gleichzeitig braucht es klare regulatorische Pfade, um Innovation und Investitionen im zivilen Dроhnensektor zu fördern und wirtschaftliche Potenziale zu heben. Die deutsch-israelische Zusammenarbeit kann hier insbesondere bei Sensorfusion und Datenverarbeitung wertvolle Beiträge leisten.

#3 Förderung von Interoperabilität und Standardisierung

C-UAS ist als „System von Systemen“ zu begreifen. Es braucht eine mehrschichtige Architektur, in der Sensoren, Effektoren und Führungssysteme (C2) verschiedener Anbieter reibungslos zusammenarbeiten. Derzeit ist die Landschaft jedoch von Fragmentierung, schnellen technologischen Veränderungen und inkompatiblen Verfahren geprägt – was die operative Wirksamkeit mindert.

Deutschland und Israel sollten daher gemeinsame technische Standards, Kommunikationsprotokolle und interoperable Schnittstellen priorisieren. Standardisierung ermöglicht die flexible Integration neuer Komponenten und sichert zugleich operative Kontinuität. Gerade in einem dynamischen Bedrohungsumfeld ist ein modularer Ansatz entscheidend.

Interoperabilität ist der Schlüssel zu einer resilienten und zukunftsorientierten C-UAS-Struktur, die sowohl auf aktuelle als auch auf neue Bedrohungen reagieren kann.

#4 Beschleunigung des Beschaffungs- und Innovationszyklus

Im Jahr 2024 wurden schätzungsweise 75 Prozent aller sUAS in der Ukraine durch elektronische Kriegsführung neutralisiert, wodurch sich diese Methode als scheinbarer Goldstandard etablierte. Dieser Vorteil schwand jedoch rasch, als die Konfliktparteien künstliche Intelligenz einsetzten und sogar zu fiber-glasgesteuerten Systemen zurückkehrten – Technologie aus der Zeit des Kalten Kriegs. Für Deutschland und Israel bleibt elektromagnetische Dominanz auf dem Schlachtfeld wichtig, doch kinetische („Hard-Kill“)-Fähigkeiten gewinnen im Rahmen eines mehrschichtigen Ansatzes an Bedeutung.

Der Krieg zeigt deutlich: Innovationszyklen verkürzen sich von Jahren auf Wochen. Daraus folgt die Notwendigkeit, auch in Friedenszeiten Beschaffung und Entwicklung drastisch zu beschleunigen. Deutschland sollte flexible Vertragsmechanismen, experimentelle Einsätze und kontinuierliche Rückkopplung zwischen Nutzern, Industrie und Forschung priorisieren. Die Lehren aus der Ukraine zeigen: Nicht eine einzelne Technologie entscheidet, sondern Anpassungsfähigkeit.

#5 Einrichtung eines German-Israeli Defense Tech Hub

Um einen qualitativen Vorsprung in der Dроhnenabwehr und anderen Zukunftstechnologien zu sichern, sollten Deutschland und Israel einen dauerhaften gemeinsamen Defense Tech Hub schaffen, um die bilaterale Zusammenarbeit in den Bereichen Forschung, Prototypenentwicklung und einsatznaher Weiterentwicklung zu institutionalisieren.

Gegner setzen zunehmend auf unbemannte Systeme, um Defizite in konventionellen Fähigkeiten auszugleichen. Russlands Vorgehen in der Ukraine verdeutlicht diesen Trend. Zugleich übernehmen auch nichtstaat-

liche Akteure und terroristische Organisationen – darunter Irans regionale Stellvertreter – kommerziell verfügbare Drohnen für Aufklärung und Angriffe.

Deutschland und Israel verfügen über komplementäre Stärken. Ein gemeinsamer Hub würde Israels operative Erfahrung mit Deutschlands industrieller Leistungsfähigkeit verbinden. Israel kann besonders von der Fähigkeit der deutschen Industrie profitieren, rasch zu skalieren. Deutsche Unternehmen haben außerdem aufgrund der Unterstützung der Ukraine wertvolle technologische und operative Erkenntnisse gesammelt, von denen auch Israel kann. Durch eine institutionalisierte Zusammenarbeit können beide Staaten ihren Vorsprung gegenüber staatlichen wie nichtstaatlichen Akteuren sichern und ihre exzellente wissenschaftliche und technologische Expertise gezielt mobilisieren.

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