

Drone Day 2025

Bitkom Defense Tech Briefing

Ausgangslage

Im Zuge aktueller Entwicklungen ist das Thema »Drohnen« so aktuell wie selten zuvor. Am 3. Juli 2025 fand zum ersten Mal der »Bitkom Drone Day« statt. Ziel der Veranstaltung war es, aktuelle technologische Entwicklungen im Bereich Unmanned Aerial Systems (UAS), also Drohnensysteme (die Drohne selbst plus alles, was man zum Steuern und Betreiben benötigt), aus erster Hand vorzustellen und den Austausch zwischen Behörden, Industrie und Forschung zu stärken.

Bitkom-Bewertung

Mit dem »Bitkom Defense Tech Briefing – Drone Day 2025« möchten wir zentrale Herausforderungen, bestehende technologische Lösungsansätze und notwendige nächste Schritte festhalten – als Nachlese und Impulsbeitrag. Zudem machen wir Vorschläge, um Deutschland wirksamer vor Bedrohungen durch Drohnen zu schützen und den Drohnensektor als strategische Industrie zu stärken.

Das Wichtigste

Wir schlagen u.a. vor:

- Umsetzung von **vernetzten und smarten Drohnenlagebildern** für kritische Bereiche, wie z.B. an Flughäfen
- Einrichtung von niedrighschwelligen **Testumgebungen** zur Erprobung von Drohnerdetektion und -abwehr unter realen Bedingungen – auch für die kommerzielle Nutzung von Drohnen
- Gemeinsame Erarbeitung durch Industrie und Behörden von **Beschaffungswegen für »Drohnen as a Service«**, um Drohnen unkompliziert für Sicherheitsbehörden nutzbar zu machen
- Anerkennung von Hardware- und Softwareherstellern von Drohnensystemen als **Schlüsselindustrie für Deutschland** und gezielte Förderung dieser; Berücksichtigung der Dual-Use-Potenzialen
- Berücksichtigung von **Low-SWaP-Kriterien** (Size, Weight, Power, Cost) als Innovationskriterien in Förderungen und Beschaffungsprozessen

Einleitung

Zielsetzung der Veranstaltung/des Tech-Briefings

Am 3. Juli 2025 fand zum ersten Mal der »Bitkom Drone Day« statt. Ziel der Veranstaltung war es, aktuelle technologische Entwicklungen im Bereich Unmanned Aerial Systems (UAS), also Drohnensysteme (die Drohne selbst plus alles, was man zum Steuern und Betreiben benötigt), aus erster Hand vorzustellen und den Austausch zwischen Behörden, Industrie und Forschung zu stärken. Der Drone Day brachte Vertreterinnen und Vertreter aus Sicherheitsbehörden, Verteidigung, Wissenschaft sowie der Tech-Industrie zusammen, um sich über Einsatzszenarien, technologische Trends und bestehende Herausforderungen auszutauschen.

Mit dem »**Bitkom Defense Tech Briefing – Drone Day 2025**« möchten wir zentrale Herausforderungen, bestehende technologische Lösungsansätze und notwendige nächste Schritte festhalten – als Nachlese, Impulsbeitrag und Grundlage für die weitere Diskussion. Dazu zeigt das Papier Herausforderungen und Lösungspotenziale in den Bereichen Einsatz, Detektion, Abwehr und Forensik. In diesem Papier wird insbesondere auf UAS Bezug genommen, also Fluggeräte, die ohne Piloten an Bord betrieben werden. Meistens werden diese durch einen Menschen über eine Funkverbindung ferngesteuert. Inzwischen gibt es auch UAS, die durch GPS-Navigation, Sensorik und Künstlicher Intelligenz teils autonom agieren können. Die Arten von UAS reichen von kleinen kommerziellen Drohnen, über militärische Drohnen (für die Aufklärung oder bewaffnete Einsätze) zu industriellen Drohnen (z. B. für den Transport) bis hin zu Freizeitdrohnen. Jede dieser Drohnentypen kann sowohl Nutzen als auch Bedrohung für die innere und äußere Sicherheit darstellen. Da die technischen und operativen Entwicklungen rasant sind, versucht dieses Papier, einen ersten Überblick und Anknüpfungspunkt der Herausforderungen und Lösungspotenziale auf den folgenden Gebieten mit dem Stand Sommer 2025 zu bieten.

1 Einsatz von Drohnen

Was sind aktuelle Entwicklungen beim Einsatz von Drohnen?

Herausforderungen

Moderne Drohnenoperationen, wie sie etwa im Ukraine-Konflikt beobachtet werden, stellen konventionelle militärische Strukturen vor erhebliche Herausforderungen. Zwar bieten insbesondere sogenannte First Person View Drones (FPVs) durch ihre Modularität, geringe Kosten und schnelle Anpassbarkeit Chancen für einen hochflexiblen Einsatz. Jedoch gibt es bei genauerer Betrachtung auf der technischen Ebene strukturelle Defizite, den Drohneneinsatz effektiv in die Fähigkeiten von Streitkräften zu integrieren. Ein zentrales Problem ist die mangelnde Interoperabilität verschiedener Systeme. Derzeit bestehen erhebliche Kompatibilitätsprobleme zwischen UAS unterschiedlicher Hersteller, was die Bildung koordinierter Aufklärungs- oder Einsatzverbünde – etwa im Rahmen von NATO-Missionen – erschwert. Auch die Bedienung der Drohnen ist bislang wenig skalierbar: Fast alle Systeme werden einzeln von jeweils einem Operator gesteuert (»one on one«), was den taktischen Einsatz stark limitiert. Eine intuitive Handhabbarkeit, vergleichbar mit konventionellen Waffen, fehlt bislang weitgehend.

Dem gegenüber steht die schnelle Einführung von Drohnen, von innovativen Einsatzmitteln, wie z. B. bei Loitering Munition oder autonom agierender Drohnensysteme, in die Fähigkeiten der Streitkräfte. Gerade im Bereich der Drohnen führen langwierige Beschaffungsprozesse und starre rüstungspolitische Vorgaben dazu, dass technologische Entwicklungen nicht in adäquater Geschwindigkeit in den operativen Betrieb überführt werden können. Der Rückstand westlicher Partner bei der Einführung und Nutzung solcher Systeme wird besonders deutlich im Vergleich zur Ukraine, die zehntausende hoch adaptive Drohnensysteme einsetzt – und zunehmend auch gegenüber Russland, das zum Beispiel den Einsatz und die Fertigung der Drohnen vom Typ »Shahed« in den Stückzahlen stark hochgefahren hat. Während gegnerische Systeme in Masse verfügbar, verlusttolerant und schnell adaptierbar sind, ist der aktuelle Ansatz in Deutschland und der EU zu schwerfällig und kleinteilig.

Die eigentliche Herausforderung für westliche Streitkräfte ist es, die schnelle Einführung von Drohnen sowie Interoperabilität und Standardisierung zusammen, z. B. auf Basis von offenen Standards wie Pixhawk für die Hardware-Architektur, PX4 für Flight Control, MAVLINK für Kommunikation, QC Ground Control für die Software der Bodenkontrollstation oder Embedded LINUX für ein On-Board-Betriebssystem zusammen zu denken. Gemeinsam mit der Industrie sollten Wege gefunden werden, kurzfristig schnell einsatzfähige Systeme bereitzustellen, ohne die mittelfristig notwendige Standardisierung gemeinsam zu verlieren.

Neben diesen strukturellen Defiziten kommt hinzu, dass unbemannte Systeme im Einsatz besonders anfällig für elektromagnetische Störungen und Jamming sind.

Während gegnerische Akteure zunehmend elektronische Kriegsführung einsetzen, verfügen westliche Systeme bislang nur über begrenzte Schutzmaßnahmen. Damit rücken Resilienzstrategien in der elektromagnetischen Dimension neben Cyberabwehr in den Vordergrund.

Lösungspotenziale

Ein erster zentraler Ansatzpunkt ist die Entwicklung standardisierter Schnittstellen und Protokolle, die eine reibungslose Integration unterschiedlicher Systeme ermöglichen. Hier ist die Industrie gefordert. Auf einer strategischen Ebene müssen skalierbare, modulare und offene Systemarchitekturen geschaffen werden, die durch kurze Entwicklungs- und Produktionszyklen ständig an aktuelle Anforderungen angepasst werden können. Diese Offenheit und Modularität sind Voraussetzung für eine industrielle Massenfertigung. Dies bedarf nicht nur einer zentralen Standardsetzung, sondern auch einer engen Kooperation zwischen Hardware-Herstellern und Software-Lieferanten. Ein weiterer Erfolgsfaktor liegt in der Entwicklung Low-SWaP-fähiger Technologien (Size, Weight and Power). Nur wenn Lösungen kompakt, energieeffizient und kostengünstig sind, können sie auf breiter Front – auch in kleineren Plattformen oder mobilen Einheiten – eingesetzt werden.

Entscheidend für die Zukunftsfähigkeit ist außerdem eine Anpassung der rechtlichen und politischen Rahmenbedingungen. Schnelle Innovationszyklen erfordern vereinfachte Beschaffungsverfahren, flexible Vorhaltekonzpte und eine politische Bereitschaft, sich von überkommenen Prinzipien der klassischen Rüstungspolitik zu lösen. Eine engere Verzahnung von Industrie, Militär und Gesetzgebung ist notwendig, um die Dynamik moderner Konflikte auch auf technologischer Ebene wirksam abzubilden.

Des Weiteren sollte die Steuerung der Systeme so vereinfacht werden, dass einzelne Operatoren mehrere UAS gleichzeitig führen können. Hierzu bedarf es intuitiver Benutzeroberflächen und automatisierter Unterstützungsfunktionen, die eine schnellere und flexiblere Bedienung ermöglichen. Die Rolle eines »Drohnenoperators« hat zudem andere Anforderungen als die eines infanteristisch kämpfenden Soldaten. Dies sollte bei der zukünftigen Personalstrategie einbezogen werden.

2 Drohnendetektion

Wie können Drohnen aufgespürt werden?



Herausforderungen

Die Drohnendetektion stellt die zentrale Voraussetzung für jede Form der Schutz- oder Abwehrmaßnahme dar und ist gleichzeitig mit erheblichen Schwierigkeiten verbunden. In urbanen Räumen und an besonders sensiblen Orten wie Flughäfen, Kraftwerken oder Offshore-Infrastrukturen erweist sich die frühzeitige Erkennung von Drohnen als anspruchsvoll. Technische Begrenzungen, schlechte Sichtverhältnisse, immer kleinere Systeme und die Vielfalt der verwendeten Frequenzen erschweren eine zuverlässige Identifikation.

Allein am Flughafen Berlin-Brandenburg wurden im Jahr 2024 bis zu 700 Drohnensichtungen pro Woche gemeldet. Dabei reicht die Bedrohungspalette von bloßer Annäherung bis hin zur konkreten Gefahr durch Kollisionen mit Flugzeugen. Gleichzeitig existieren offene Fragen bei den Zuständigkeiten zwischen Luftfahrtbehörden, Polizei, Flugsicherung und Betreibern, wodurch eine koordinierte Reaktion auf Bedrohungen erheblich erschwert wird.

Auch in anderen Bereichen wie Offshore-Windparks zeigen sich erhebliche Schwachstellen. Diese kritischen Infrastrukturen stehen zunehmend im Fokus hybrider Angriffsformen – darunter auch die Spionage und möglicherweise Sabotage mit Hilfe von Drohnen. Die Detektionskapazitäten auf See sind bislang begrenzt, was die Reaktionsfähigkeit im Ernstfall einschränkt. In all diesen Fällen besteht ein grundlegendes Problem darin, aus abstrakten Bedrohungslagen ein konkretes, handhabbares Risikobild zu erzeugen.

Darüber hinaus gibt es weitere Herausforderungen durch fortschrittlichere Drohnentechnologien:

Wegpunkt Navigierte Drohnen ermöglichen autonome Flugrouten ohne permanente Funkverbindung zum Piloten. Dadurch lassen sie sich schwer durch Funk- oder GPS-Störungen beeinflussen und operieren unabhängig von typischen Steuerungssignaturen. Ihre Erkennung wird zusätzlich erschwert, da sie keine kontinuierliche Kommunikation benötigen und somit klassische Detektionsverfahren wie Radiofrequenz (RF)-Scanning umgehen können.

Drohnen über LTE nutzen das Mobilfunknetz zur Steuerung, was sie weitreichender und schwerer lokalisierbar macht. Sie können große Entfernungen überwinden und sind durch dynamische IP-Zuweisungen schwer zu verfolgen. Zudem entziehen sie sich der Kontrolle klassischer Funkfrequenz-Scanner, da sie reguläre Mobilfunkfrequenzen verwenden, was die Unterscheidung von normalem Netzverkehr erheblich erschwert.

Kabelgebundene Drohnen, die über eine physische Verbindung (z. B. zur Energieversorgung oder Datenübertragung) betrieben werden, können stundenlang oder sogar dauerhaft in der Luft bleiben. Ihre stationäre oder semi-stationäre Nutzung

etwa zur Beobachtung macht sie besonders für Überwachung und Spionage geeignet. Gleichzeitig sind sie durch die fehlende Funkkommunikation nur schwer zu detektieren und werden von vielen Sensoren, die auf elektromagnetische Signale angewiesen sind, gar nicht erfasst.

Es gibt heute bereits Lösungen, welche jede für sich Teile der vorab genannten Herausforderungen abdecken können, aber insgesamt steht die Drohnerdetektion noch am Anfang ihrer technologischen Entwicklung. Speziell im Bereich RF-Technologie gibt es Systeme, welche erstaunliche Reichweiten und Präzision erzielen, aber die Integration der verschiedenen Technologien zu einem gemeinsamen Lagebild stellt nach wie vor eine große Herausforderung dar. Zudem fehlt es oft an verlässlicher rechtlicher Grundlage, an standardisierten Bewertungsverfahren sowie an strukturierten Verfahren zur Einbindung in operative Entscheidungsprozesse.

Lösungspotenziale

Zur wirksamen Behebung dieser Defizite bedarf es eines vernetzten Ansatzes. Die Kombination verschiedener Sensoren – darunter Hochfrequenztechnik, Radar, Video- und Audiotechnik – schafft eine Grundlage, die auch bei komplexen äußeren Bedingungen eine zuverlässige Detektion erlaubt. Zur Anwendung kamen solche Lösungen bereits bei internationalen Großveranstaltungen und städtischen Sicherheitsszenarien, wie etwa in Singapur oder bei der EURO 2024. Die Integration in ein zentrales Lagebild, die Nutzung der Daten für forensische Beweissicherung und die rechtssichere Nutzung personenbezogener Daten bilden die Grundlage künftiger Lösungsansätze. Sehr interessant, aber auch besonders herausfordernd ist die Detektion über LTE- und 5G-Netze. Erste Tests hierzu werden zusammen mit weiteren Projektpartnern an der Universität der Bundeswehr Hamburg durchgeführt. Ergänzend werden externe Systeme erprobt und in behördliche Lagebilder eingebunden. Ein weiterer Ansatz ist die systematische Auswertung und Integration von Detektionsdaten mit anderen sicherheitsrelevanten Informationen – etwa Abgleich von Seriennummern, IP-Adressen, Fernsteuerungsdaten oder Bewegungsprofilen. Dadurch werden eine umfassende Risikoanalyse und Bedrohungszuordnung möglich.

Für Flughäfen wird die Umsetzung strukturierter Hotspot-Analysen empfohlen, ergänzt durch die Übertragung bewährter Verfahren aus dem Wildlife-Management auf die Drohnerdetektion. Dies soll helfen, Bewegungsmuster frühzeitig zu erkennen und entsprechende Präventionsmaßnahmen einzuleiten. Für kritische Infrastruktur, wie z. B. Offshore-Anlagen wiederum werden die enge Verzahnung ziviler und militärischer Akteure als notwendige Schritte zur Steigerung der Resilienz gesehen.

Die Entwicklung eines Drohnen-Gefährdungsindex stellt ein potenzielles Werkzeug dar, das eine standardisierte Bewertung erlaubt und bestehende Datenquellen systematisch zusammenführt. Die zentrale Erkenntnis lautet: Detektion allein ist nicht ausreichend. Erst durch die nahtlose Integration in Entscheidungsprozesse, rechtssichere Dokumentationsketten und die Verknüpfung mit Kontextdaten wie Wetter, sozialen Medien oder temporären Flugzonen entsteht ein wirkungsvoller Sicherheitsmechanismus. Lösungspotenziale liegen nicht nur in der technischen Umsetzung, sondern auch in der operativen Anwendung – also in der Fähigkeit, aus der Vielzahl verfügbarer Daten konkrete Handlungsoptionen abzuleiten.

3 Drohnenabwehr

Wie können Drohnen abgewehrt werden?



Herausforderungen

Die Detektion von Drohnen ist lediglich der erste Schritt – eine weitere Herausforderung beginnt mit der Frage, wie man auf identifizierte Bedrohungen effektiv und situationsgerecht reagiert. Auf der militärischen Seite sehen sich Truppeneinheiten zunehmend mit schwer auffindbaren FPV-Drohnen konfrontiert, gegen die auf Zug- oder Kompanieebene bislang kaum taktische Mittel verfügbar sind. Auch die steigende Anzahl gleichzeitig agierender Systeme – etwa Schwärme mit dutzenden Drohnen – überfordert viele bestehende Abwehrlösungen, insbesondere im Hinblick auf Rechenkapazität und Reaktionsgeschwindigkeit. Ein zentrales Problem liegt in der technischen und operativen Fragmentierung der verfügbaren Systeme. Es gibt kein Abwehrsystem, das sich auf alle Bedrohungstypen anwenden lässt. Unterschiedliche Drohnentypen, Flughöhen, Steuerungsmethoden und Zielprofile erfordern jeweils spezifische Sensorik und Eingriffsmechanismen. Die Maxime »No one size fits all« trifft hier in vollem Umfang zu. Viele verfügbare Lösungen sind komplex, schwer zu integrieren oder erfordern hohes Ausbildungsniveau – was insbesondere unter Zeitdruck und bei geringer Personalverfügbarkeit zum Ausschlusskriterium werden kann.

Auf der zivilen Seite der Drohnenabwehr sind vor allem infrastrukturelle Einschränkungen, fehlende klare Rechtsgrundlagen und sensible Abwägungen der Verhältnismäßigkeit eines Eingriffs die größten Herausforderungen. Die sensorische Abdeckung, Detektionssicherheit bei ungünstigen Lichtverhältnissen sowie das Risiko von Fehleinschätzungen stellen wesentliche technische Limitierungen dar.

Lösungspotenziale

Innovative Konzepte wie autonome Abfangdrohnen und andere automatisierte Systeme haben hohes Potenzial. Diese Systeme können verdächtige Flugobjekte selbstständig identifizieren, verfolgen und mit Netzwerfern unschädlich machen. Gleichzeitig erweisen sich Systeme als wirkungsvoll für die taktische Abwehr, die optische Sensoren mit Tag- und Nachtsichtfähigkeit sowie akustischer Voralarmierung kombinieren. Die visuelle Verifikation durch Kamerasysteme schafft darüber hinaus eine Entscheidungsgrundlage. Inzwischen bieten einige Hersteller Plug-and-play-fähige Lösungen, die schnell adaptierbar sind und Künstliche Intelligenz wirkungsvoll einbinden. Damit können diese Systeme aus Echtdaten lernen, Muster erkennen und sogar Schwärme detektieren. Was für den Einsatz von Drohnen gilt, gilt auch für Systeme für die Abwehr von Drohnen. Entscheidend ist nicht nur die technische Fähigkeit zur Abwehr, sondern deren operative Nutzbarkeit. Systeme müssen einfach bedienbar, skalierbar und in bestehende Strukturen integrierbar sein. Nur wenn Technik,

Automatisierung und Benutzerfreundlichkeit ineinandergreifen, entsteht eine praxisfähige Lösung, die sowohl in urbanen Sicherheitslagen als auch im militärischen Feld Bestand hat.

4 Drohnenforensik

Wie können Drohnen ausgelesen werden?

Herausforderungen

Die forensische Analyse von Drohnen gewinnt zunehmend an Bedeutung, da sie eine Schlüsselrolle in der Strafverfolgung, der Gefahrenabwehr und der Aufklärung von sicherheitsrelevanten Vorfällen spielt. Das Sammeln von Daten, die forensisch ausgewertet werden können, beginnt jedoch bereits vor der eigentlichen Sicherstellung. Zwar lassen sich digitale Signale während des Fluges erfassen, jedoch bleibt ein direkter Zugriff auf die Hardware unmöglich. Eine fundierte Beweissicherung muss daher mit der präzisen Erfassung und Archivierung dieser »Live-Daten« in Echtzeit beginnen – eine Anforderung, die technisch wie organisatorisch hohe Anforderungen stellt.

Nach der erfolgreichen Abwehr oder Sicherstellung einer Drohne verlagert sich die Herausforderung in den Bereich der detaillierten Laboranalyse. Die große Vielfalt an Drohrentypen – von Spielzeug über kommerzielle bis hin zu spezialisierten militärischen Systemen – verlangt eine hohe Expertise und ein breites Methodenspektrum. Viele Systeme sind manipulationssicher, verschlüsselt oder verfügen über Sicherheitsmechanismen. Zudem ist die forensische Verwertung oft nur dann rechtssicher möglich, wenn eine lückenlose Dokumentation und Asservierung gewährleistet ist. Die schnelle technische Entwicklung sowie der internationale Charakter vieler Drohnenimporte erschweren zudem die Klassifizierung und Rückverfolgung, insbesondere bei modifizierten oder anonym betriebenen Systemen. Ein weiteres Problem besteht in der fehlenden Standardisierung der forensischen Auswertung. Ohne einheitliche Protokolle, Analysewerkzeuge und Schulungskonzepte bleibt die Qualität der Ergebnisse stark vom Einzelfall abhängig. Gerade in sicherheitsrelevanten Kontexten – etwa bei Terrorismusabwehr oder Industriespionage – stellt dies ein erhebliches Risiko dar.

Lösungspotenziale

Die Detektion von Drohnen eröffnet die Möglichkeit, Drohnen bereits im Einsatz eindeutig zu klassifizieren und erste Rückschlüsse auf Steuerung und Absicht zu ziehen. Nach der Sicherstellung der Drohne (ggf. nach einer erfolgreichen Abwehrmaßnahme) erfolgt eine systematische Auswertung physischer und digitaler Komponenten. Diese werden im Labor auf gespeicherte Daten, Verbindungsprotokolle und Nutzerprofile hin analysiert. Dabei entsteht ein forensisches Gesamtbild, eine sogenannte »DNA der Drohne«. Dieses kann dann Aufschluss über Herkunft, Einsatzmuster und mögliche Täterstrukturen geben. Zudem können die Informationen mit bestehenden Datenbanken und digitalen Identitäten verknüpft werden, um rechtssichere Beweise zu generieren.

Ein entscheidender Faktor ist die Entwicklung standardisierter Verfahren zur Sicherstellung, Auswertung und Dokumentation, welche die Voraussetzung für eine belastbare



Strafverfolgung liefern. Gleichzeitig sollten forensische Ausbildungsmodule in die Schulungskonzepte für Polizei, Militär und Sicherheitsbehörden eingebunden werden, um die Analysekompetenz flächendeckend zu verbessern. Langfristig eröffnet die Drohnenforensik auch strategische Perspektiven: Eine systematische Drohnenforensik würde es erleichtern, Bedrohungslagen frühzeitig zu erkennen und Akteursnetzwerke leichter zu identifizieren. Damit wird die forensische Arbeit zu einem integralen Bestandteil moderner Sicherheitsarchitektur – nicht nur als Reaktion auf Vorfälle, sondern auch als Werkzeug zur aktiven Gefahrenanalyse und strategischen Lageeinschätzung.

5 Bitkom-Vorschläge

- Für kritische Bereiche schlagen wir vor, vernetzte und smarte Drohnenlagebilder umzusetzen. Sie sind der Schlüssel zur Handlungsfähigkeit von Sicherheits- und Strafverfolgungsbehörden. Dies dient nicht nur der Spionageabwehr und dem Sabotageschutz, sondern auch der Flugsicherheit an deutschen Flughäfen.
- Für die Erprobung von Detektion, Abwehr, aber auch von eigenen Fähigkeiten – etwa im Bereich Aufklärungs- und Wirkdrohnen – schlagen wir vor, mehr und niedrigschwellige Testumgebungen unter realen Bedingungen einzurichten – auch für die kommerzielle Nutzung von Drohnen. Dafür müssen auch gesetzliche Regularien vereinfacht werden.
- Wir schlagen vor, dass Beschaffungswege für »Drohnen as a Service« unkompliziert für Sicherheitsbehörden nutzbar sein müssen. Für die Erarbeitung von gemeinsam getragenen Lösungen zwischen Industrie und Behörden bieten wir als Bitkom eine neutrale Plattform im vorwettbewerblichen Dialog.
- Als Bitkom regen wir an, dass Drohnen als neue Schlüsselindustrie für Deutschland erkannt werden müssen. Beispielsweise ist die Batterieproduktion für Drohnen auch ein entscheidender Faktor für die technologische Souveränität. Neben Anwendungen im Bereich innere und äußere Sicherheit stecken hohe Potenziale in kommerziellen Anwendungsfällen, wie Transportdrohnen.
- Wir schlagen vor, bei der Förderung von Drohnentechnologien das Dual-Use-Potenzial stärker mitzudenken, da viele Lösungen gleichermaßen im militärischen Bereich wie auch in Katastrophenschutz, kritischer Infrastruktur und industriellen Anwendungen genutzt werden können.
- Wir regen an, dass Low-SWaP-Kriterien (Size, Weight, Power, Cost) als Innovationsmaßstäbe in Förderungen und Beschaffungsprozessen berücksichtigt werden. Nur so können Technologien skalierbar in großen Stückzahlen auch auf kleineren Plattformen eingesetzt werden.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Nemo Buschmann | Referent Öffentliche Sicherheit & Verteidigung
T +49 30 27576-101 | n.buschmann@bitkom.org

Verantwortliches Bitkom-Gremium

AK XXX

Copyright

Bitkom 2025

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom oder den jeweiligen Rechteinhabern.