AUSSCHREIBUNG SPRIND FUNKE: ANTI-DRONE RESPONSE

Wer ist die SPRIND?

SPRIND ist die Bundesagentur für Sprunginnovationen. SPRIND ist eine Gesellschaft des Bundes und hat die Aufgabe, bahnbrechende Innovationen zu identifizieren, zu finanzieren und zu skalieren. Inspiriert von der amerikanische DARPA ist ihr Hauptziel, agile und proaktive Unterstützung zu leisten, um Innovationen hervorzubringen, die unser Leben verändern.

Die Challenges und Funken sind die Innovationswettbewerbe der SPRIND. Sie sind ein Instrument, mit dem die SPRIND bahnbrechende Innovationen aufspürt. Im Wettbewerb miteinander demonstrieren die teilnehmenden Teams, welche Lösung das Zeug zur Sprunginnovation hat.

Worum geht es im SPRIND Funken?

Die zunehmende Verfügbarkeit und Leistungsfähigkeit von Kleinst- und Mikro-Unmanned-Aerial-Vehicles (UAV) stellen eine wachsende sicherheitstechnische Herausforderung dar sowohl in zivilen als auch in militärischen Szenarien. Besonders im militärischen Kontext, etwa im Ukrainekrieg, lassen sich prominente Beispiele finden, die diese Entwicklung eindrücklich verdeutlichen. Dort werden täglich große Mengen handelsüblicher oder modifizierter Drohnen für Aufklärungszwecke und Angriffe eingesetzt. Ihr Einsatzpotenzial reicht von der Überwachung bis hin zur Störung oder Sabotage. Sie sind kostengünstig, hochmanövrierfähig, schwer zu entdecken und in der Lage, durch Schwarmtaktiken oder Täuschungsmanöver selbst komplexe Abwehrsysteme zu überwinden. Moderne Drohnensysteme verfügen zunehmend über Fähigkeiten wie Navigation ohne GNSS-Unterstützung, autonome Flugformationen, automatische Zielklassifikation oder kaum detektierbare Signaturen.

Obwohl in der medialen Berichterstattung insbesondere Herausforderungen im militärischen Kontext skizziert werden, sind auch und vor allem zivile Einrichtungen wie Flughäfen, Stadien, Demonstrationen oder kritische Infrastrukturen in erhöhtem Maße anfällig für gezielte oder unkoordinierte Drohneneinsätze. Die Gefahr liegt dabei nicht nur in den Systemen selbst, sondern auch in ihrer niedrigen Eintrittsschwelle. Eine Weiterentwicklung hin zu größeren, schnelleren und autonom agierenden Flugobjekten zeichnet sich ab. Diese reichen von 3D-gedruckten Low-Cost-UAVs bis hin zu selbstgebauten Marschflugkörpern oder ungelenkten Raketen. Dadurch wächst der Druck auf bestehende Abwehrsysteme weiter. Um Drohnen effektiv abwehren zu können, ist es notwendig, auch gegen Raketen, Schwarmmunition oder Überschallziele vorbereitet zu sein. Ein zukunftsfähiger Abwehransatz muss deshalb skalierbar, autonom, selektiv und deeskalierend sein. Benötigt werden Systeme, die zwischen potenziellen Bedrohungen unterscheiden können, flexibel auf neue Angriffsformen reagieren und situationsgerechte

Gegenmaßnahmen treffen, die von sanftem Abfangen über gezielte Umleitung bis hin zur vollständigen Neutralisation reichen.

Zivile Schutzmaßnahmen sind damit nicht länger nur ein ergänzender Teil der Sicherheitsarchitektur, sondern werden zu einer zentralen Säule gesamtgesellschaftlicher Resilienz. Bestehende Abwehrmaßnahmen stoßen insbesondere bei autonomen, vernetzten oder im Schwarm agierenden Drohnen an ihre Grenzen. Es reicht nicht mehr, nur gegen klassische Drohnen vorzugehen – vielmehr müssen auch komplexere Bedrohungen wie Schwarmangriffe, improvisierte Flugkörper oder gar Überschallziele adressiert werden. Neue, innovative Lösungen werden benötigt, um solchen Bedrohungen schnell, autonom, skalierbar, mit minimalem Risiko für Dritte und ohne Kollateralschäden zu begegnen.

Der SPRIND Funke „Anti-Drone Response“ schließt diese Lücke und ruft zu einem Paradigmenwechsel auf: Gesucht sind nichtdestruktive, skalierbare, vollautonome Abwehrlösungen, die Bedrohungen zuverlässig erkennen, rasch reagieren und Drohnen neutralisieren, ohne den umgebenden Luftraum oder Dritte zu gefährden. Das Ziel ist nicht die kinetische Vernichtung des Flugsystems, sondern die Eindämmung durch intelligente Effekte, Umleitung, Blockade oder andere reversible Maßnahmen.

Langfristig soll so eine neue technische Schutzinfrastruktur entstehen, die Drohnenangriffe nicht eskaliert, sondern deren Erfolg systematisch verhindert sowohl operativ, wirtschaftlich und taktisch. Eine Lösung, die zeigt: Jeder Angriff wird wirkungslos. Der Funke richtet sich daher an visionäre Teams, die Verteidigungsüberlegenheit durch Präzision, Resilienz und intelligente Systemintegration verwirklichen wollen.

Das Ziel

Ziel des Funken ist die Entwicklung und Erprobung eines vollständig autonomen Gesamtsystems zur präzisen und kollateralfreien Neutralisierung von Kleinst- und Mikro-UAVs in Echtzeit, das ohne klassische Waffenwirkung wie Explosivstoffe oder kinetische Projektile auskommt, keine externe Kommunikation oder menschliches Eingreifen erfordert und ein hohes zivil-militärisches Transferpotenzial bietet.

Gesucht ist ein adaptives Gesamtsystem, das Bedrohungen erkennt, eindeutig klassifiziert und situationsgerecht mit nicht-kinetischen, reversiblen Maßnahmen wie Fangen, Umlenken oder Blockieren reagiert. Dabei sollen ergänzend innovative Ansätze zum Einsatz kommen, wie etwa richtwirkungsbasierte Interventionen durch gezielte Impulse, Steuerung oder Effekte zur Desorientierung oder rückführfähige Abfang- und Transportlösungen. Letztere sollen ein gefasstes UAV sicher aus dem Gefahrenbereich entfernen und sie gegebenenfalls polizei- und nachrichtendienstlich auswertbar machen.

Ebenso denkbar sind koordinierte Schwarmlösungen, bei denen mehrere mobile Plattformen ein dynamisches Schutznetz bilden, sowie Softkill-KI, welche UAVs durch gezielte Manipulation von Sensorik, Signalführung oder Flugpfaden neutralisiert. Multimodale Frühdetektionsverfahren, bei denen beispielsweise optische, akustische und thermische

Daten fusioniert werden, sollen zudem eine zuverlässige Erfassung auch bei geringen Signaturen und autonomen Flugprofilen ermöglichen.

Die Detektions- und Wirkkomponenten sollen dabei technisch klar getrennt, aber funktional aufeinander abgestimmt sein.

Die Leistungsfähigkeit wird in zwei Stufen nachgewiesen:

- **Stufe 1** demonstriert die Grundfunktionalität mit einem selbst gewählten, einfach agierenden Ziel-UAV
- **Stufe 2** testet das System unter Realbedingungen gegen bereitgestellte UAVs mit realistischen Bedrohungsprofilen

Der Fokus liegt auf skalierbaren und wirtschaftlich tragfähigen Lösungen, die in sicherheitskritischen zivilen oder urbanen Kontexten einsetzbar sind, ohne dass dabei Gefahr für Menschen, Infrastruktur oder den Luftraum entsteht. Systeme, die auf Jamming, Spoofing, Explosivwirkungen oder proprietären, nicht nachvollziehbaren Closed-Source-Technologien basieren, sind ausgeschlossen.

Das Ziel besteht darin, ein möglichst positives Verhältnis zwischen den Kosten für Abwehrmaßnahmen gegen UAVs und den Kosten für Angriffe zu erreichen. Dabei sollten die Kosten für die Abwehr deutlich unter denen für die Angriffe liegen. Damit wird ein Beitrag zur operativen, ethischen und ökonomischen Nachhaltigkeit in sicherheitsrelevanten Szenarien geleistet.

Langfristig soll so eine technische Schutzinfrastruktur entstehen, die UAV-Angriffe nicht eskaliert, sondern ökonomisch und operativ entwertet.

Technische Zielvorgaben:

- Gegenmaßnahme muss spätestens nach 1/3 der Flugstrecke zwischen Detektion und Zielpunkt eingeleitet werden
- Kein Einsatz von Jamming, Spoofing oder Explosivwirkungen
- Nachweis der Konformität mit luftfahrtrechtlichen Vorgaben (z. B. LBA für Betriebsgenehmigungen und UAS-Zulassungen, DFS für Freigaben im kontrollierten Luftraum und Koordination im Flughafenbereich, unter Beachtung von LuftVG, LuftVO und der EU-Drohnenverordnung)
- Softkill-Ansätze und Schwarmabwehrlösungen ausdrücklich erwünscht
- System muss vollständig autonom operieren, Notabschaltung zulässig
- Wiederverwendbarkeit und zivile Anwendbarkeit als Ziel

Einzureichende Unterlagen

- Technisches Kurzprofil
- Funktionsbeschreibung

— Sicherheitskonzept
— Konformitätsnachweis

Stufe 1: Technologiedemonstration mit eigener Ziel-UAV

Wie reagieren autonome Abwehrsysteme auf definierte Bedrohungsszenarien durch Kleinst- und Mikrodrohnen? In dieser ersten Demonstrationsphase präsentieren die Teams ihre Systeme unter kontrollierten Bedingungen, wobei sie eine selbst gewählte, eigenständig geflogene Ziel-UAV einsetzen. Diese darf keine aktiven Gegenmaßnahmen (z. B. GPS-Spoofing-Resistenz oder eine Fluglogik zur Täuschung des Gegners) nutzen, um eine möglichst saubere Bewertung der Grundfunktion zu ermöglichen.

Die Flugbahn soll reproduzierbar sein und entweder linear verlaufen oder auf vordefinierten Wegpunkten basieren. Im Fokus stehen die Detektion, Klassifizierung und Initiierung einer Gegenmaßnahme unter Zeitdruck. Das Gelände entspricht dem späteren Realsetup (Stufe 2), womit die Übertragbarkeit gesichert ist.

Technische Rahmenbedingungen

— Reaktionsauslösung spätestens nach 1/3 der Flugdistanz zwischen Erkennungspunkt und Ziel
— Nur nicht-destruktive Abwehrmaßnahmen zulässig
— Keine Störsender und Spoofing
— Einhaltung aller Auflagen für Flughafensicherheit
— Klar getrennte Sensorik- und Wirkungslogik
— Autonom oder teilautonom

Bewertungskriterien (u.a.)

— Nachweis der Zielerkennung und Tracking-Fähigkeit
— Demonstration eines funktionalen Interzeptionsprozesses
— Time-to-Intercept
— Interzeptionszeit & Erfolgsquote
— Robustheit bei Falschzielen
— Einhaltung aller Sicherheits- und Flugfeldregularien

Meilenstein-Ziel: Zwischen-Demo-Event (**voraussichtlich 18. und 19.09.2025**)

Stufe 2: Finale Demonstration gegen Ziel-UAV

Wie zuverlässig und sicher reagieren autonome Abwehrsysteme unter realistischen, taktisch anspruchsvollen Drohnenangriffen? In dieser finalen Demonstration treffen die Systeme auf bereitgestellte Drohnen mit variabler Signatur, Geschwindigkeit und Flugverhalten. Die Drohnen starten aus größerer Entfernung und führen realitätsnahe Profile aus, darunter Loitering-Flug, Kamikaze-Ansätze oder Wegpunktnavigation mit unvorhersehbarer

Kursänderung. Ziel ist der Schutz eines definierten Objekts (z. B. markierte Box mit Fahne). Die Teams dürfen keine Informationen zum Flugmuster vorab erhalten und müssen vollständig automatisiert reagieren, inkl. Detektion, Klassifizierung und neutraler Abwehr.

Technische Rahmenbedingungen

- Echtzeitreaktion (< 1/3 der Flugstrecke)
- Keine aktive Kommunikation mit Steuerpersonal während der Reaktion
- Keine klassischen Waffenwirkungen erlaubt
- Maßnahme muss reversibel sein oder keine Folgeschäden erzeugen
- Schutzradius mindestens 100 Meter um Zielobjekt
- Abwehr muss auch bei mehreren Bedrohungen gleichzeitig funktionieren
- Optionaler Bonus bei erfolgreicher Analyse und Rückführung der abgefangenen Drohne

Bewertungskriterien

- Detektion & Klassifikation bei wechselnden Profilen
- Reaktion auf Täuschungsdrohnen oder Schwärme
- Täuschungsresistenz
- Verhinderung erfolgreicher Anflüge
- Interzeptionsradius: 100 m um das Ziel
- Reaktionsdistanz und -zeit
- Autonomer Betrieb mit dokumentierter Entscheidungskette
- Systemrobustheit bei schwankenden Umweltbedingungen
- Sicherheit, Integrität und Skalierbarkeit der Lösung
- Unbedenklichkeitsnachweis & Regeltreue
- Innovationsgrad der Maßnahme

Meilenstein-Ziel: Abschluss-Event (**04. und 05. November 2025**)

Ablauf

Der Funke läuft über einen Gesamtzeitraum von **vier Monaten** (für Details siehe Tabelle 1: Zeitplan).

Interessierte Teams werden gebeten, ihre Bewerbung zur Teilnahme am Funken online bis zum **29. Juli 2025**, 23:59 Uhr CEST, über das Einreichungsformular einzureichen. Eine Fachjury bewertet die Bewerbungen und wählt im Rahmen einer Auswahlsitzung am **11. Und 12. August 2025** bis zu **20 Teams** aus, die zur Teilnahme an **Stufe 1** zugelassen werden.

Der Funke besteht aus zwei Stufen, in denen jeweils definierte Meilensteine erreicht werden sollen. Die erste Stufe mit einer Laufzeit von **einem Monat** startet am **15. August 2025** und endet am **19. September 2025**.

Am Ende von Stufe 1 bewertet die Jury den Fortschritt der Teams im Rahmen eines Zwischen-Demo-Events und wählt bis zu **zehn Teams** für die zweite Stufe des Funken aus. Die zweite

Stufe mit einer Laufzeit von rund **sechs Wochen** startet am **20. September 2025** und endet voraussichtlich am **05. November 2025**.

Die zweite Stufe und damit der gesamte Funke mündet in einem Abschlussevent am **04. und 05. November 2025**, bei dem die autonomen Systeme unter Realbedingungen einen definierten Parcours absolvieren müssen. Die Teilnahme an Stufe 2 verpflichtet zur aktiven Teilnahme am Abschlussevent. Auf Grundlage der praktischen Demonstration im Rahmen des Abschlussevents und des gesamten Entwicklungsprozesses kürt die Jury ein Siegerteam.

Der unten abgebildete Zeitplan (Tabelle 1 „Zeitplan“) fasst den gesamten voraussichtlichen Verlauf des Funken zusammen. SPRIND behält sich vor, die Termine zu ändern. Die Teilnehmer werden hinsichtlich etwaiger Änderungen rechtzeitig informiert.

Datum	Ereignis
08.07.2025	Veröffentlichung der Ausschreibung
29.07.2025	Bewerbungsfrist
15.08.2025	Start der Stufe 1
18. und 19.09.2025	Zwischen-Demonstration und Jury-Entscheidung Stufe 2
20.09.2025	Start der Stufe 2
04. und 05.11.2025	Finale Demonstration und Ende Stufe 2

Tabelle 1: Zeitplan

Wie profitiert mein Team?

Die SPRIND stellt über zwei Stufen bis zu 52.000 Euro pro Team zur Verfügung, abhängig von den finanziellen Anforderungen, welche die Teams mit ihrer Bewerbung einreichen. Diese Finanzierung erfolgt in Form eines individuellen Festpreises, der auf einer Kostenschätzung des Teams basiert. Die Preisobergrenze für die erste Stufe liegt bei 22.000 Euro; die Preisobergrenze für die zweite Stufe liegt bei voraussichtlich 30.000 Euro. Die SPRIND nutzt für diese Finanzierung das Instrument der vorkommerziellen Auftragsvergabe (siehe Teilnahmevereinbarung).

Um den Teams zu helfen, ihr volles Potential zu erreichen, stellt die SPRIND unterschiedliche Unterstützungsmöglichkeiten über den gesamten Zeitraum des Funke bereit. Die SPRIND erleichtert außerdem den Zugang zu neuen Kooperationspartner und Expert:innen. Es ist ebenfalls möglich, dass die SPRIND die teilnehmenden Teams auch nach dem Ende der Challenge finanziell unterstützt, wenn sie – auch gemeinsam mit der Jury und ggf. weiteren Expert:innen – ausreichend Sprunginnovationspotential sieht.

SPRIND erwartet von erfolgreichen Bewerber:innen, dass sie offen für Kollaborationen sind, um erfolgreiche Teams zu bilden.

Wer ist berechtigt, sich zu bewerben?

Bewerben können sich Teams in allen Rechtsformen wie Universitäten, außeruniversitären Forschungseinrichtungen, etablierten Unternehmen, Start-ups und Inkubatoren. Gründerzentren können die Aufforderung zur Einreichung von Bewerbungen gerne an ihre

Netzwerke weiterleiten. Eine Ausgründung ist während der Laufzeit des SPRIND Funkens grundsätzlich möglich, sollte allerdings in Anbetracht kurzer Fristen genau geprüft werden. Eine entsprechende Absicht sollte aus der Bewerbung des Teams hervorgehen.

Teams sind antragsberechtigt, wenn sie ihren Hauptsitz in der Europäischen Union, in der Europäischen Freihandelszone (EFTA), Israel oder dem Vereinigten Königreich haben. Einzelne Teammitglieder oder Kollaborationspartner können ihren Sitz außerhalb dieser Region haben.

Die Bewerber:innen müssen sicherstellen, dass die Arbeit an ihrem Beitrag zum Funken nicht bereits mit anderen öffentlichen Fördermitteln finanziert wird.

Mit der Bewerbung ist das Formblatt "ERKLÄRUNG ZU RUS-SANKTIONEN“ ausgefüllt einzureichen. Für die Teilnahme an diesem Funken ist das Ausfüllen des Formblatts obligatorisch. Es sind nur solche Bewerber:innen zugelassen, die keinen Bezug zu Russland gemäß dieser Erklärung aufweisen.

Wie funktioniert der Bewerbungsprozess?

Bewerber:innen sind eingeladen, online unser Bewerbungsformular auszufüllen, um sich für diesen SPRIND Funken zu bewerben:

https://sprind.org/taten/challenges/submissions/funke-anti-drone-response?

Wie werden die Teams ausgewählt?

Die SPRIND wird bei der Auswahl von Expert:innen unterstützt. Ausgewählte Bewerber:innen werden zu einem Pitch vor einer Jury eingeladen. Die Bewerbungen werden hinsichtlich

— ihres Potentials eine Sprunginnovation zu werden (Ansatz),
— der Effektivität des vorgeschlagenen Arbeitsplans (Umsetzung),
— der Fähigkeit des Teams, diesen Plan umzusetzen (Team)
— sowie ihrer wirtschaftlichen Strategie (Wirtschaftlichkeit) und
— der Umsetzung der Konditionen, wie sie hier vorgestellt wurden

bewertet. Tabelle 2 zeigt, wie diese Kriterien beurteilt werden können.

Die Kategorien Ansatz, Umsetzung und Team fließen zu gleichen Teilen in die Bewertung der Teams ein, wobei die Teams relativ zueinander bewertet werden. Die Kategorie Wirtschaftlichkeit ist ausschlaggebend sollten zwei Bewerbungen anhand der anderen Kriterien gleich bewertet sein.

Aussagen sind durch wissenschaftliche Daten zu belegen. Falls es für bestimmte Punkte noch keine Daten gibt, bitten wir dennoch um eine (als solche deklarierte) Abschätzung.

Tabelle 2: Auswahlkriterien

Ansatz
Hat der Ansatz das Potenzial, eine Sprunginnovation zu werden?

Lässt der Ansatz erwarten, dass standardisierte Bedrohungsszenarien (Stufe 2) in Echtzeit autonom erkannt und neutralisiert werden können?
Unterscheidet sich der Ansatz deutlich von bereits bestehenden Lösungen oder klassischen C-UAS-Systemen?
Wie effektiv reagiert das System auf unvorhersehbare Ereignisse im Betriebskontext (z. B. Schwärme, Täuschdrohnen, Richtungswechsel)?
Kann die Technologie auf andere sicherheitsrelevante Anwendungen übertragen werden (z. B. Veranstaltungsschutz, Flughäfen, Behörden)?
Wie hardwareunabhängig ist das System (z. B. kein GPS-Zwang, keine proprietären Closed-Source-Abhängigkeiten)?
Umsetzung
Basiert der Arbeitsplan auf realistischen Annahmen und einem strukturierten Zeitplan?
Sind der Finanzplan und die geplanten Schritte plausibel und stimmen überein?
Ist eine Demonstration der Kernfunktionen unter realistischen Bedingungen bis zur Zwischen- und Abschlussdemo zu erwarten?
Sind notwendige Arbeitspakete, externe Partner oder Subunternehmer sinnvoll eingebunden?
Besteht eine Skalierungsstrategie über den Funken hinaus (z. B. Industrieüberführung, NATO-Anschlussfähigkeit)?
Team
Verfügt das Team über relevante Expertise (z. B. Robotik, autonome Systeme, Sensorfusion, Echtzeitverarbeitung, C-UAS-Erfahrung)?
Verfügt das Team über Erfahrung mit sicherheitskritischen oder militärisch/zivilen Anwendungen?
Hat das Team Zugang zu geeigneter Testinfrastruktur (z. B. Flugplätze, sichere Testgebiete, Drohnensysteme)?
Ist das Team grundsätzlich in der Lage, das System perspektivisch zu industrialisieren oder weiterzuentwickeln?
Wirtschaftlichkeit
Stehen die angebotenen Gesamtkosten im Verhältnis zum angebotenen Leistungsumfang?
Leistet die SPRIND-Förderung einen entscheidenden Beitrag zur Realisierung des Vorhabens? | Förderrelevanz

Besteht ein tragfähiger Plan zur Weiterentwicklung oder Anschlussförderung (z. B. SPRIND, HTGF, BMVg, BAAINBw, VC, NATO, EU)?
Wie entwickeln sich die Kosten pro erfolgreicher Interzeption bei breitem Einsatz oder Serienfertigung? Ist ein wirtschaftlich tragfähiges Verhältnis von Abwehr- zu Angriffskosten realistisch erreichbar?

Vertraulichkeit

Die SPRIND wird alle Einreichungen vertraulich behandeln. Informationen über die Einreichungen werden nur an die Jury, Gutachter und die Challenge-Coaches weitergegeben. Auch diese Personen sind zur Verschwiegenheit verpflichtet.

Die ausgewählten Teams des Funke werden öffentlich bekannt gegeben. Mit der Einreichung der Bewerbung erklären die Teams sich damit einverstanden.

An wen kann ich mich bei weiteren Fragen wenden?

Bewerber:innen werden gebeten, einen Blick in die Teilnahmevereinbarung und die FAQs zu werfen. Sollten Sie Ihre Frage dort nicht beantwortet finden, wenden Sie sich bitte zur weiteren Klärung an *challenge@sprind.org*.