Hackathon

ADIC26
Cognitive Security & Resilience Hackathon: Securing Minds, Strengthening Society

Für den Hackathon ist nur einer der unten angeführten drei Punkte zu bearbeiten.

Es wird nur ein Siegerprojekt ermittelt.

Der Hackathon steht im Kontext der Verteidigungsforschungsstrategie 2032+, deren Ziel es ist, Österreichs Innovationskraft und Resilienz im europäischen Umfeld zu stärken. Dazu sollen Forschungsthemen mit militärischer wie auch gesamtgesellschaftlicher Relevanz aufgegriffen und in Form konkreter Pilotprojekte für den praktischen Einsatz nutzbar gemacht werden.

Aktuelle sicherheits- und verteidigungspolitische Herausforderungen sind dabei zunehmend durch drei Faktoren geprägt: hohe Komplexität, die nur durch interdisziplinäre Ansätze bewältigt werden kann; ethische und rechtliche Fragestellungen, die beim Einsatz neuer Technologien unvermeidbar sind; sowie die Notwendigkeit, Menschen und Systeme effektiv zu verbinden und zu schützen, damit Einsatzfähigkeit und gesellschaftliches Vertrauen erhalten bleiben.

Vor diesem Hintergrund beschäftigt sich der heurige Hackathon mit der Frage, wie Menschen und Gesellschaften widerstandsfähig bleiben können. Im Zentrum steht daher die Entwicklung von Innovationen, die Resilienz fördern, Risiken abwehren und die Handlungs- und Entscheidungsfreiheit sichern, mit Lösungen, die Sicherheit sowohl für Streitkräfte als auch für zivile Einsatzbereiche stärken und demokratischen Werten und Prinzipien entsprechen.

Punkt 1: Allgemeiner Wehrwille

Thema: Innovative Ansätze zur Stärkung des allgemeinen Wehrwillens[1] und zur Abwehr manipulativer Informationsoperationen

Aufgabe: Gesucht werden Lösungsansätze, die Gesellschaften widerstandsfähiger gegen manipulative Medienmechanismen (z. B. Clickbait, soziale Netzwerke, algorithmische Verstärkung) machen. Der Wehr- und Verteidigungswille soll als Ausdruck von Vertrauen,

[1] Darunter wird die die Bereitschaft verstanden, sein/ihr Land, dessen Bevölkerung und seine/ihre Werte mit der Waffe zu verteidigen und dabei im Extremfall auch die persönliche Sicherheit aufs Spiel zu setzen.

Solidarität und Zusammenhalt „geschützt“ werden, auch wenn gezielte Informationsoperationen versuchen, diesen zu untergraben. Denkbar sind technologische, organisatorische oder gesellschaftliche Innovationen, die die Cognitive Security als Grundlage demokratischer Handlungsfähigkeit sichern und dem europäischen Werte- und Rechtsverständnis entsprechen.

Ziel: Umsetzungsansätze für Konzepte, die Vertrauen stärken, Transparenz fördern und kollektive Widerstandskraft gegenüber Desinformation schaffen. Dadurch soll die Basis für den Wehrwillen und gesellschaftliche Kohäsion als Voraussetzung einer wehrfähigen Demokratie erhalten bleiben.

Einsatzszenario: Das Einsatzszenario ist frei wählbar, aber im Fokus soll die für die Wehrpflicht relevante Personengruppe stehen (Alter 15-25 Jahre). Beispiele sind die Abwehr von Desinformationskampagnen vor politischen Entscheidungen, der Schutz des Zusammenhalts in Krisenzeiten, die Sicherung von Vertrauen in Informationsquellen oder die Stärkung von Einsatzorganisationen gegenüber gezielten Informationsangriffen sowie Stärkung der Einstellung zu den europäischen Werten und die Bereitschaft, für diese einzustehen. Die Erweiterung des Kontextes, etwa hybride Angriffe im internationalen Rahmen, ist denkbar.

Punkt 2: Schutz vor neurophysikalischen Stressoren

Thema: Innovative Ansätze zum Schutz vor neurophysikalischen Stressoren in Einsatzumgebungen

Aufgabe: Gesucht werden tragbare, neuroergonomische Schutzsysteme, die Soldat:innen in Einsatzumgebungen vor akustischen, elektromagnetischen und sensorischen Belastungen bewahren und so ihre kognitive Gesundheit und Entscheidungsfähigkeit sichern. Unsichtbare Stressoren wie extreme Lärmbelastung, elektromagnetische Einwirkungen oder dauerhafte Reizüberflutung können Aufmerksamkeit, Gedächtnisleistung und Entscheidungsqualität erheblich beeinträchtigen. Dabei geht es nicht allein um die reale Exposition: Bereits die Vorstellung einer potenziellen Bedrohung kann Angstreaktionen auslösen und die Einsatzfähigkeit deutlich beeinträchtigen. Daher gilt es, bestehende Technologien zur Dämpfung, Abschirmung und zum Monitoring gezielt weiterzuentwickeln und für den praktischen Einsatz nutzbar zu machen.

Ziel: Umsetzungsansätze für tragbare Systeme, die die kognitive Leistungsfähigkeit unter Belastung erhalten und unmittelbar den Bedürfnissen von Einsatzkräften entsprechen. Darüber hinaus sollen Konzepte entstehen, die auch auf zivile Hochrisikoberufe übertragbar sind.

Einsatzszenario: Das Einsatzszenario ist im militärischen Kontext frei wählbar. Beispiele sind Operationen in lärmintensiven urbanen Umgebungen oder Missionen mit hoher sensorischer Reizdichte. Auch Anwendungen für Einsätze in (unmittelbar) durch Waffenwirkung zerstörten Gebieten im Zusammenwirken mit den zivilen Einsatzkräften sind denkbar.

Punkt 3: Risk Assessment & Cognitive Security

Thema: Innovative Ansätze für Risk Assessment und den Schutz kognitiver Sicherheit im Umgang mit Neurotechnologien und algorithmischen Systemen

Aufgabe: Gesucht werden Werkzeuge und Rahmenwerke, die den Einsatz von Neurotechnologien und algorithmischen Systemen so bewerten und begleiten, dass Risiken frühzeitig erkannt und die kognitive Sicherheit geschützt werden. Risiken können sowohl durch eigene Entwicklungen entstehen, etwa durch unerwartete Nebenwirkungen im Praxiseinsatz, als auch durch fremde Technologien, sei es durch gegnerische Systeme oder Dual-Use-Produkte, die missbraucht werden. Erforderlich sind deshalb Konzepte, die einerseits Responsible Innovation unterstützen (z. B. Risk-Assessment-Tools, Governance-Frameworks) und andererseits keine Entwicklungsnachteile gegenüber potentiellen Konkurrenten oder Gegnern bedeuten.

Ziel: Umsetzungsansätze für innovative Risk-Assessment- und Schutzsysteme, die verantwortungsvolle technologische Entwicklung absichern, Manipulation vorbeugen und so unmittelbar zur Resilienz von Streitkräften wie auch der Gesellschaft beitragen. Dabei sollen insbesondere flexible Ansätze erarbeitet werden, die das hohe Entwicklungstempo in diesem Feld berücksichtigen.

Einsatzszenario: Das Einsatzszenario ist frei wählbar. Beispiele sind die Bewertung neuer Neuro-Interfaces vor dem Einsatz in kritischen Missionen, die Abwehr gegnerischer algorithmischer Systeme im Rahmen hybrider Konflikte oder die Detektion manipulativer Dual-Use-Technologien in zivilen Anwendungen. Auch Szenarien mit hoher regulatorischer Relevanz, etwa beim Einsatz von KI-gestützten Entscheidungswerkzeugen in Armeen und Operationen sowie durch Behörden oder bei Einsatzorganisationen, sind denkbar.

Bewertungskriterien

- Innovationsgrad & Exzellenz – Neuartigkeit, wissenschaftlich-technische Qualität, Potenzial zur Disruption
- Verteidigungsnutzen – Anwendbarkeit im verteidigungspolitischen und militärischen Kontext
- Technologische Souveränität & Resilienz – Beitrag zur Stärkung der nationalen Wertschöpfung und europäischen Autonomie
- Adressierung ethischer und werteorientierter Herausforderungen
- Umsetzbarkeit & Entwicklungsperspektive – technische Realisierbarkeit, TRL, Zeit- und Ressourcenplanung

Kooperation & europäische Anschlussfähigkeit – Einbindung von Partnern, Synergien mit EU-Programmen, Interoperabilität

Unsere Partner und Sponsoren:

Das Tagungsprogramm mit den Keynote Speakern und die geplanten Aktivitäten bei der ADIC 2026 finden Sie laufend aktualisiert unter: www.inno4def.at

[contact@inno4def.at]
[www.inno4def.at]

Bundesministerium für Landesverteidigung/Sektion I - Generaldirektion Verteidigungspolitik in Zusammenarbeit mit der Wirtschaftskammer Österreich (Kärnten), BABEG GmbH/LakeSideLabs, Lakeside Science & Technology Park GmbH, führenden österreichischen und internationalen Innovationspartnern.

Für Fragen steht ihnen der Projektleiter Mag. René CERNE, MBA Oberstleutnant des höheren militärfachlichen Dienstes zur Verfügung.

Bundesministerium Landesverteidigung