SPOTME

Spoof-Detection and Location Estimation using Deep Learning

Programm / Ausschreibung	FORTE, FORTE, FORTE - Kooperative F&E-Projekte KFE 2024	**Status**	laufend
Projektstart	01.09.2025	**Projektende**	31.08.2027
Zeitraum	2025 - 2027	**Projektlaufzeit**	24 Monate
Keywords	Resilience of military platforms and critical infrastructure; automated spoof detection; deep learning application;		

Projektbeschreibung

Die zunehmenden GNSS-Störattacken in Krisenregionen wie der Ukraine, Israel und Syrien bedrohen sowohl kritische Infrastrukturen als auch die Auslandseinsätze des österreichischen Bundesheeres (z. B. UNIFIL, UNTSO). Angesichts des globalen Anstiegs solcher Vorfälle ist es plausibel, dass auch Österreich in Zukunft mit ähnlichen Bedrohungen konfrontiert sein könnte. GNSS-Störungen oder -Ausfälle haben das Potenzial, erhebliche persönliche, materielle und finanzielle Schäden zu verursachen. Vor diesem Hintergrund zielt dieses Forschungsprojekt darauf ab, die Resilienz militärischer Plattformen und kritischer Infrastrukturen gegen GNSS-Störattacken durch den Einsatz fortschrittlicher Methoden der künstlichen Intelligenz (KI) zu verbessern.

Abstract

The increasing number of GNSS jamming attacks in crisis regions such as Ukraine, Israel, and Syria threaten both critical infrastructures and the Austrian Armed Forces' missions abroad (e.g. UNIFIL, UNTSO). Given the global increase in such incidents, it is plausible that Austria could also be confronted with similar threats in the future. GNSS disruptions or failures have the potential to cause considerable personal, materia,l and financial damage. Against this background, this research project aims to improve the resilience of military platforms and critical infrastructures against GNSS jamming attacks through the use of advanced artificial intelligence (AI) methods.

Projektkoordinator

- Technische Universität Graz

Projektpartner

- Bundesministerium für Landesverteidigung
- DriveMinds Technologies GmbH