

GINA

GNSS Interference Sensor Network Austria

| | | | |
|---------------------------------|---|------------------------|------------|
| Programm / Ausschreibung | FORTE, FORTE, FORTE - Kooperative F&E-Projekte KFE 2024 | Status | laufend |
| Projektstart | 01.01.2026 | Projektende | 30.06.2027 |
| Zeitraum | 2026 - 2027 | Projektlaufzeit | 18 Monate |
| Projektförderung | € 312.950 | | |
| Keywords | GNSS; Sensornetzwerk; Navwar-Lagebild; Electronic Order of Battle | | |

Projektbeschreibung

Motivation/Bedarf: Blickt man auf aktuelle Krisensituationen weltweit, so ist zu beobachten, dass die gezielte Störung (RFI - Radio-Frequency Interference) der geschützten GNSS Frequenzbänder durch sogenanntes Jamming und Spoofing zum Stand der Technik gehört. Gleichzeitig nimmt auch die Anzahl an GNSS-abhängigen (globale Satellitennavigationssysteme, zur Positions- und Zeitgebung) Systemen und Anwendungen im Militär zu. Beim gezielten Angriff auf das für GNSS-relevante elektromagnetische Spektrum (EMS) spricht man von Navigation Warfare (NavWar), welches zum Ziel hat, den Gegner in seinen Handlungen einzuschränken. Um bspw. gezielte Störungen der Navigation von Truppen oder von Kommunikationssystemen bestmöglich zu verhindern, ist es essentiell, ein stets aktuelles NavWar-Lagebild als Beitrag zur Electronic Order of Battle zur Verfügung zu haben. Dies ermöglicht, entsprechende Vorkehrungen und Gegenmaßnahmen treffen zu können. Ein solches NavWar-Lagebild inklusive zugrundeliegendem GNSS Sensornetzwerk fehlt aktuell dem österreichischen Verteidigungsministerium (BMLV). Die Grundlage für ein NavWar-Lagebild ist ein GNSS Sensornetzwerk bestehend aus stationärer und verlegbarer Sensorik am Boden, Sensorik in der Luft (z.B. Drohnen) und am Satellit. Auf nationaler Ebene muss dieses grobmaschig das gesamte Bundesgebiet abdecken und an neuralgischen Punkten (Fliegerhorste, BMLV Radarstationen, Kasernen, grüne Grenze im Osten, etc.) das Netz verdichten. Zusätzlich benötigt es verlegbare Sensorik zur Netzverdichtung für Einsätze und für Regionen mit Schwergewicht wie z.B. der Auslandseinsatz im Libanon, das Sicherheitsforum Davos, etc.

Ziel: Mit dem Projekt Gina soll nun der erste wesentliche Schritt Richtung NavWar-Lagebild umgesetzt werden, indem ein BMLV GNSS Sensornetzwerk (Ausschreibungsschwerpunkt unter Punkt 2 Weltraumtechnologie für militärische Anwendungen) basierend auf in Österreich vorhandener GNSS Sensorik umgesetzt wird. Zu Beginn wird die Ist-Situation (wer betreibt GNSS Sensoren) analysiert und mit dem BMLV die Use Cases und Anforderungen diskutiert. Anschließend wird ein GNSS Sensornetzwerk konzipiert und umgesetzt, indem vorhandene Sensorik ans Netzwerk angebunden wird. Die Sensordatenanalyse und Netzwerkdatenanalyse wird durch KI-unterstützte Algorithmik erfolgen, um Störsignale (Jamming, Spoofing) zu detektieren, zu charakterisieren, bestmöglich zu lokalisieren. Am Ende des Projekts liegt ein Mockup eines NavWar-Lagebilds vor, das in Echtzeit die Daten des GNSS Netzwerks darstellt. Dies ermöglicht die Ausarbeitung einer Roadmap zur Definition der notwendigen Schritte und Investitionen hin zu einem operationellen System und gibt dem BMLV

eine Entscheidungsgrundlage.

Innovation: Der Ansatz der größtmöglichen Einbindung bereits vorhandener GNSS Infrastruktur ermöglicht es, Steuergelder von voraussichtlich mehreren Millionen Euro einzusparen. Ein Netzwerkaufbau rein mit spezifischer Sensorik würde viel mehr Zeit und Geld (typischerweise 10-30 kEUR pro Sensor) kosten. Der Beginn der Umsetzung darf nicht weiter verschoben werden, da bereits die weiteren Aktivitäten zur Befüllung des NavWar-Lagebilds initiiert wurden (z.B. EDA LEO2VLEO).

Mehrwert: Das Projekt Gina ist somit ein wichtiger erster Schritt Richtung Verfügbarkeit eines NavWar-Lagebild und liefert einen wesentlichen Beitrag zur Landesverteidigung und zum Schutz unserer Streitkräfte gegen moderne aktuelle Bedrohungslagen.

Abstract

Motivation/needs: Looking at current crisis situations worldwide, it can be observed that intentional jamming (RFI - Radio-Frequency Interference, e.g. jamming or spoofing) of the protected GNSS frequency bands is state of the art. At the same time, the number of GNSS-dependent (Global Navigation Satellite Systems, for positioning and timing) systems and applications in the military is also increasing. Intentional attacks on the GNSS-relevant electromagnetic spectrum (EMS) are called Navigation Warfare (NavWar), the aim of which is to restrict the enemy's actions. In order to prevent targeted disruption to the navigation of troops or communication systems, for example, it is essential to always have an up-to-date NavWar situation picture available as a contribution to the Electronic Order of Battle. This enables appropriate precautions and countermeasures to be taken. The Austrian Ministry of Defense (BMLV) currently lacks such a NavWar situation picture, including the underlying GNSS sensor network. The basis for a NavWar situation picture is a GNSS sensor network consisting of stationary and deployable sensors on the ground, sensors in the air (e.g. drones) and on satellites. At the national level, this network must cover the entire federal territory in a coarse-meshed manner and densify the network at neuralgic points (air bases, BMLV radar stations, barracks, the green border in the east, railway stations, etc.). In addition, it requires deployable sensor technology for network densification for missions and for regions with a heavy focus, such as foreign missions in Lebanon, the Davos Security Forum, etc.

Goal: With the Gina project, the first major step towards NavWar situational awareness is to be realized by implementing a BMLV GNSS sensor network (tender focus under point 2, Space technology for military applications) based on GNSS sensor technology available in Austria. To begin with, the current situation (e.g. who is operating GNSS sensors) will be analyzed and the use cases and requirements discussed with the BMLV. A GNSS sensor network is then designed and implemented by connecting existing sensors to the network. The sensor data analysis and network data analysis will be carried out using AI-supported algorithms to detect interference signals (jamming, spoofing), characterize and localize them in the best possible way. At the end of the project, a mockup of a NavWar situation picture will be available, which shows the data of the GNSS network in real-time. This enables the development of a roadmap to define the necessary steps and investments towards an operational system and provides the BMLV with a basis for decision-making.

Innovation: The approach of maximizing the integration of existing GNSS infrastructure makes it possible to save millions of euros in taxpayers' money. Building a network purely with specific sensor technology would cost much more time and money (typically 10-30 kEUR for each sensor). The start of implementation must not be postponed any further, as further activities to fill the NavWar situation picture have already been initiated (e.g. EDA LEO2VLEO).

Added value: The Gina project is therefore an important first step towards the availability of a NavWar situation picture and makes a significant contribution to the national defense and protects our armed forces against current modern threats.

Projektkoordinator

- JOANNEUM RESEARCH Forschungsgesellschaft mbH

Projektpartner

- Bundesministerium für Landesverteidigung
- BRIMATECH Services GmbH