

A short, solid orange horizontal line.

FACHTAGUNG FORTISSIMO NAVWAC

ASPEKTE UND ANFORDERUNGEN AN EIN NAVIGATION WARFARE CENTER IN ÖSTERREICH (FORTE)
SASCHA BARTL

AGENDA



- 1 Projektübersicht NavWaC
- 2 Navigation Warfare
- 3 Ergebnisse
- 4 NavWar TüPI Seetaler Alpe

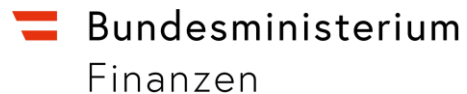
ECKDATEN

- Projektstart: 2019
- Laufzeit: 18 Monate
- Projektleitung: OHB Digital Solutions GmbH (vormals TeleConsult Austria GmbH)
- Projektpartner: Brimatech Services GmbH, Institut für militärisches Geowesen
- gefördert im Rahmen des österr. Verteidigungsforschungsprogramms FORTE des BMF



FORSCHUNGSFRAGE

- Welche technischen Fähigkeiten muss ein **Navigation Warfare Center** in Österreich bieten und wie können diese technisch, ökonomisch und organisatorisch umgesetzt werden?



■ Definition

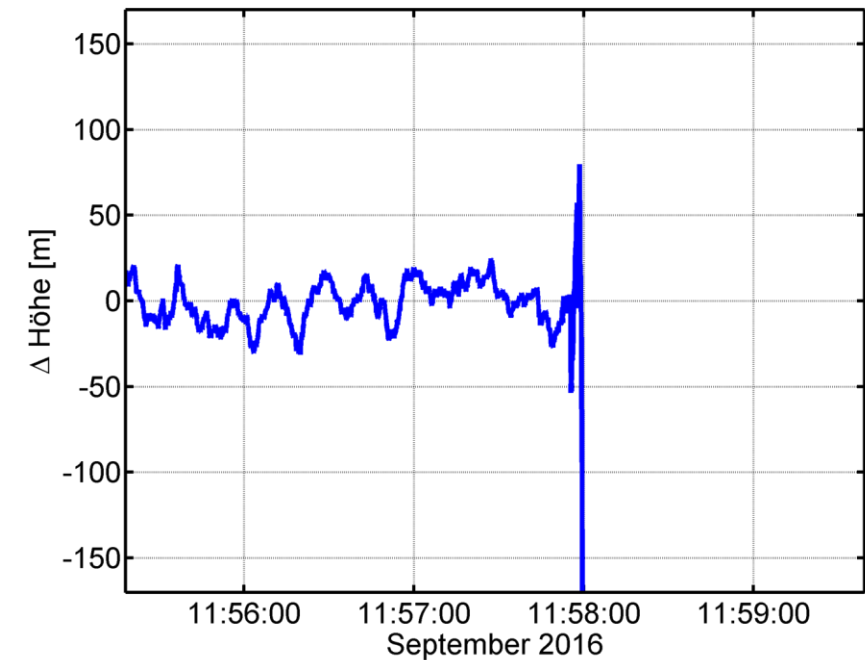
- geographisch begrenzte Störung von PNT-Informationen eines Gegners
- gleichzeitige Gewährleistung der Resilienz der eigenen Systeme

■ Möglichkeiten

- Stören → keine PNT-Information
- Täuschen → verfälschen der PNT-Information

■ Komponenten

- Defensiv → Auswirkung auf Truppe, Resilienz, Gegenmaßnahmen, etc.
- Offensiv → Aktives Stören (& Resilienz der eigenen Systeme)



FRAGESTELLUNGEN

WICHTIGSTE FRAGESTELLUNGEN UND INNOVATIONEN FÜR DAS PROJEKT

FRAGESTELLUNGEN

- Wie können unterschiedliche Störkomponenten zusammenwirken und welche Angriffsszenarien ergeben sich dadurch?
- Wie können Navigation Warfare Szenarien und deren Auswirkungen objektiv und qualitativ getestet und bewertet werden?
- Welche PNT-Services (satellitengestützt, terrestrisch, Cyberspace, hybrid) sollen/können dabei abgedeckt werden?



INNOVATIONEN

- Erprobungs- und Testmöglichkeiten für Navigation Warfare Szenarien sowie unterschiedlicher Truppen- und Waffengattungen in Realität
- Berücksichtigung von satellitengestützten, terrestrischen und hybriden Positionierungs-verfahren sowie passiver und aktiver NavWar Strategien und Einbeziehung von Cyberangriffen auf PNT-Informationen.
- NavWaC wird gemäß den Anforderungen und Spezifikationen des BMLV konzipiert.
- Österreich gibt international das Signal, dass man sich aktiv mit dem Thema beschäftigt und an Gegenmaßnahmen arbeitet. Durch Aufbau eines der ersten Navigation Warfare Center in Europa wird eine internationale Vorreiterrolle erreicht.

TECHNISCHE ASPEKTE

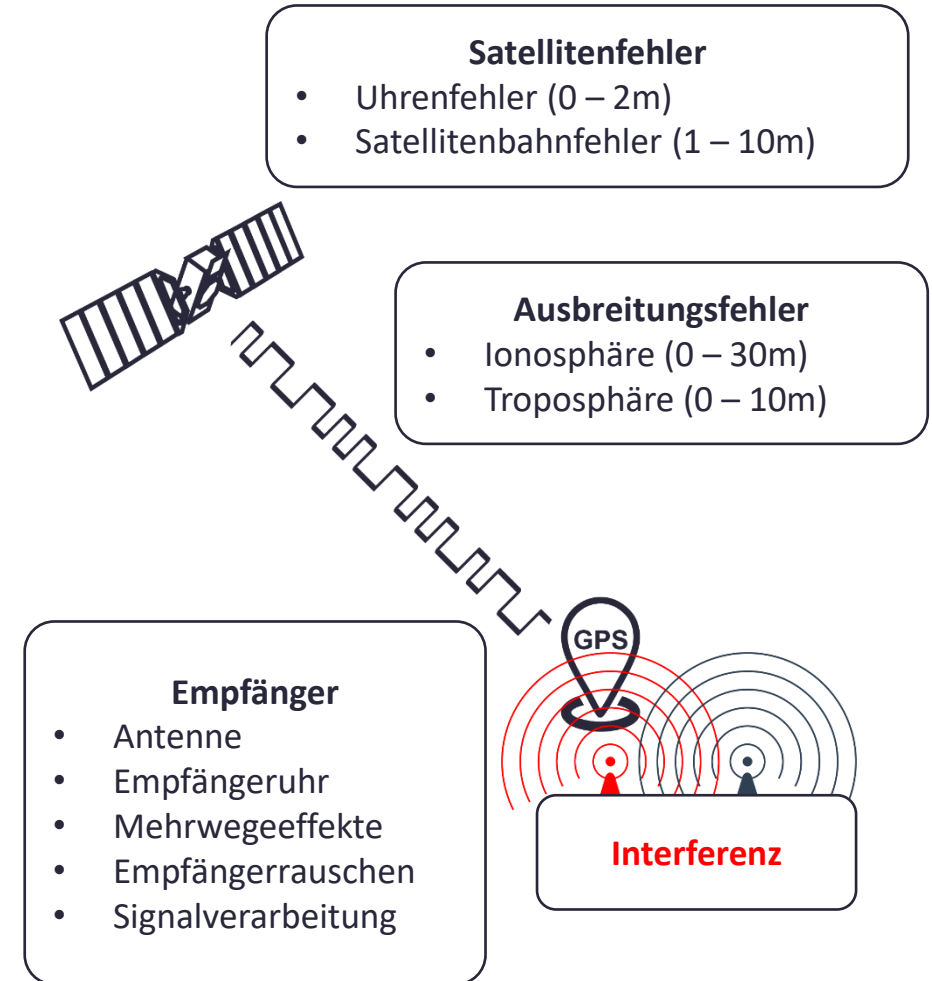
STÖRUNG VON GNSS SIGNALEN

GRUNDSÄTZE

- GNSS sind hoch komplexe Systeme → zahlreiche Fehlerquellen
- Die empfangenen GNSS-Signale sind sehr schwach
 - Leistung entspricht einer 50-Watt-Glühbirne in einer Entfernung von 20.000 km
 - GNSS Signalbänder sind von weißem Rauschen dominiert
- GPS Signaldesign stammt aus den 70er/80er Jahren
 - Design der zivilen Signale bekannt
 - Beabsichtigte Interferenz war damals kein Thema

ABSICHTLICHE STÖRUNGEN (INTERFERENZ)

- Jamming
- Spoofing

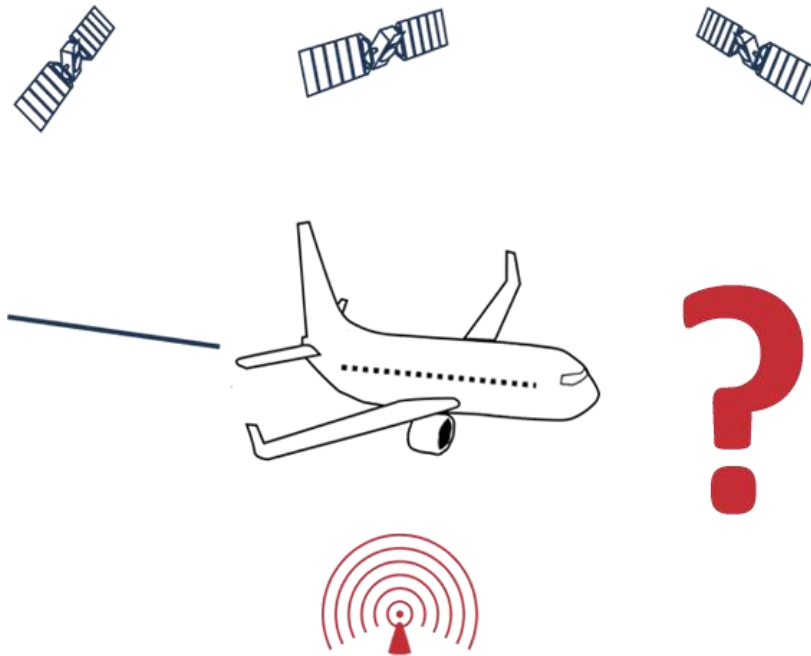


ABSICHTLICHE GNSS STÖRUNGEN

WAS IST JAMMING UND SPOOFING

JAMMING

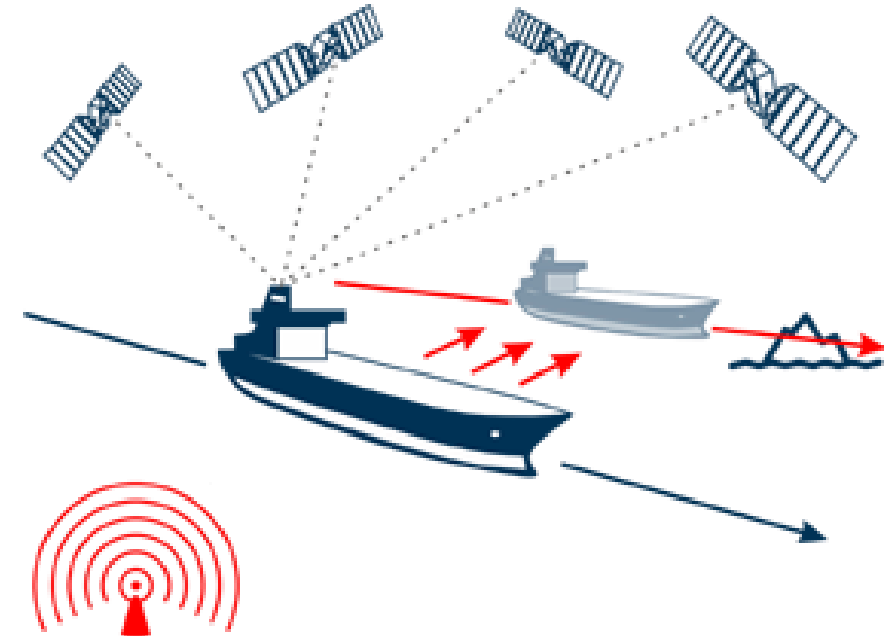
Der absichtliche Versuch, durch das Aussenden von leistungsstarken Störsignalen, GNSS-Dienste zu stören. Aufgrund der Unterbrechung der GNSS-basierten Positions- und Zeitinformation muss das on-board System auf alternative PNT-Methoden zurückgreifen.



Jammed plane

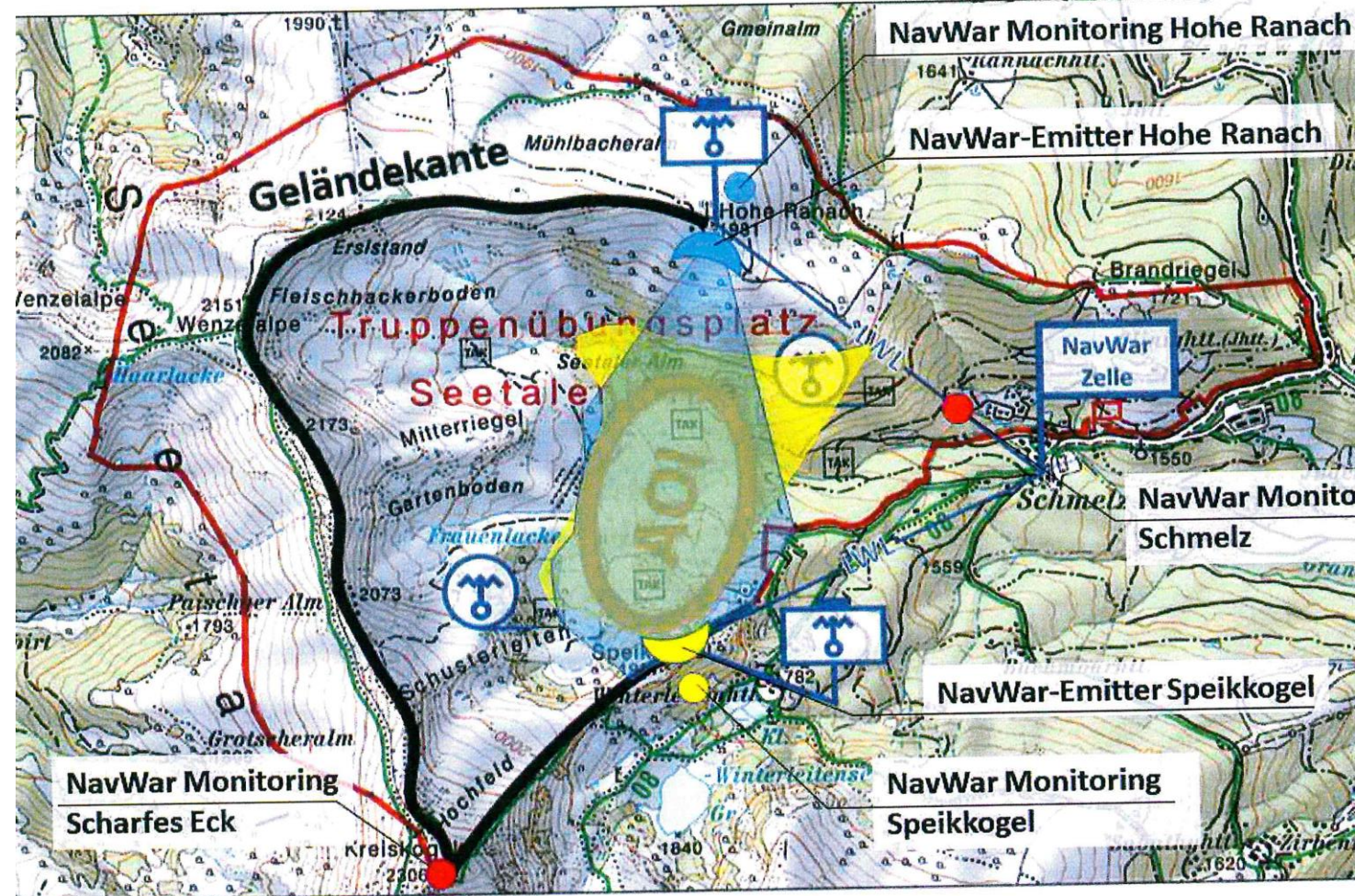
SPOOFING

Der absichtliche Versuch, einem GNSS-Empfänger, durch das Aussenden von gefälschten GNSS-Signalen, eine fehlerhafte Position bzw. Zeit vorzutäuschen. Gespoofte Empfänger zeigen bewusst manipulierte PNT-Informationen an.



Spoofed vessel

- Definition einer Area of Interest
 - Reichweite
 - Abdeckung
 - Zugänglichkeit
 - Nebeneffekte / Störungen
 - uvm.
- Definition von Monitoring Stationen zur Überwachung der Störsignale
- Definition von Anforderungen
 - Technisch
 - Organisatorisch
 - Finanziell



STÖRUNG UND MONITORING

JAMMING/SPOOFING UND INTERFERENCE MONITORING

AJ+S – Jamming und Spoofing Transmitter

Test und Analyse von Verwundbarkeiten bestehender System gegenüber Jamming und Spoofing von GNSS.

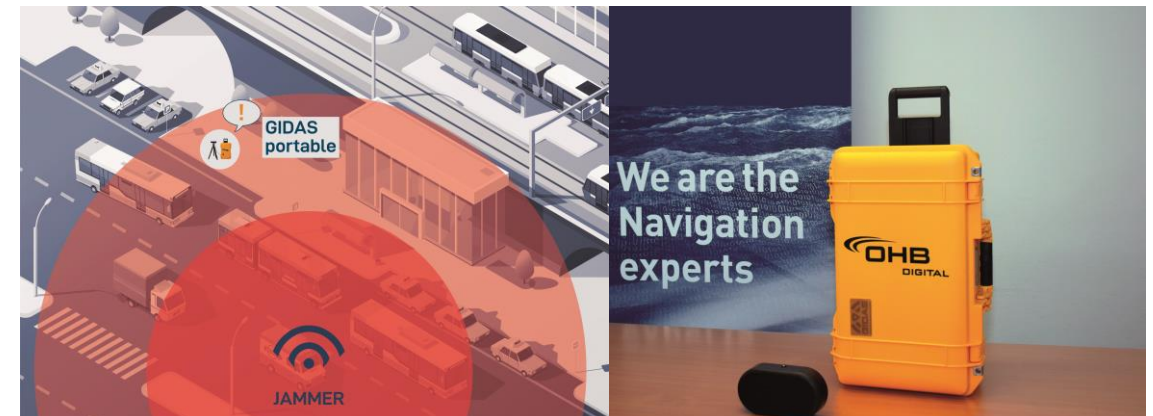
- Portables und integriertes System zum Erzeugen von Jamming und Spoofing Signalen
- Ermöglicht realistische Tests von militärischer Ausrüstung unter kontrollierten Bedingungen



GIDAS – GNSS Quality Assurance

Monitoring von GNSS Signalen zur Detektion und Alarmierung im Falle von Interferenzen durch Jamming und Spoofing.

- Autonomes System zur temporären oder dauerhaften Überwachung der GNSS Signalqualität
- Automatische Alarmierung im Falle von Störungen durch Jamming oder Spoofing



TESTS UND DEMONSTRATIONEN

NUTZUNG DES TÜPL SEETALER ALPE FÜR NAVWAR TESTS UND ÖA-AKTIVITÄTEN

BEWUSSTSEIN SCHAFFEN

- The need for GNSS resilience - European Forum Alpbach 2018
- Fachvortrag IKT Sicherheitskonferenz 2018 / Critical Infrastructure
- PRSAustria ÖA-Tag on 24. Mai 2017 at TÜPI Seetaler Alpe
- Showcase Seetaler Alpe am 25. September 2018
- Testmessungen mit NATO @ TÜPI-S
- Regelmäßige “Seetaler Festspiele” am TÜPI-S



ÖA-Tag auf der Seetaler Alpe



Live-Spoofing beim Forum Alpbach



Gemeinsame Tests mit NATO NCIA



Bewusstseinsbildung zu Jamming, Spoofing, PRS

CONCLUSIONS

ERGEBNISSE UND ZUKÜNFTIGE AKTIVITÄTEN

TECHNISCHE ERGEBNISSE

- Konzeptionierung eines Navigation Warfare Test Center am TÜPL-S
- Weiterentwicklung von geeigneter Ausrüstung zum Stören und Monitoring
- Analyse des Einfluss von GNSS-Störungen auf unterschiedliche Systeme durch Labortests und Feldtests

AWARENESS IS KEY

- ÖA-Aktivitäten und gemeinsame Tests und Demonstrationen am TÜPL
- Einbindung von unterschiedlichen Stakeholdern und Zusammenarbeit zwischen Ministerien und Industrie
- Europäische Zusammenarbeit
- Kommunikation der Ergebnisse auch über Ländergrenzen hinweg





DANKE

Sascha BARTL
OHB Digital Solutions GmbH
Kärntner Straße 7b/1
8020 Graz
ÖSTERREICH

Tel.: +43 316 890971 10
Mail: sascha.bartl@ohb-digital.at
Web: www.ohb-digital.at