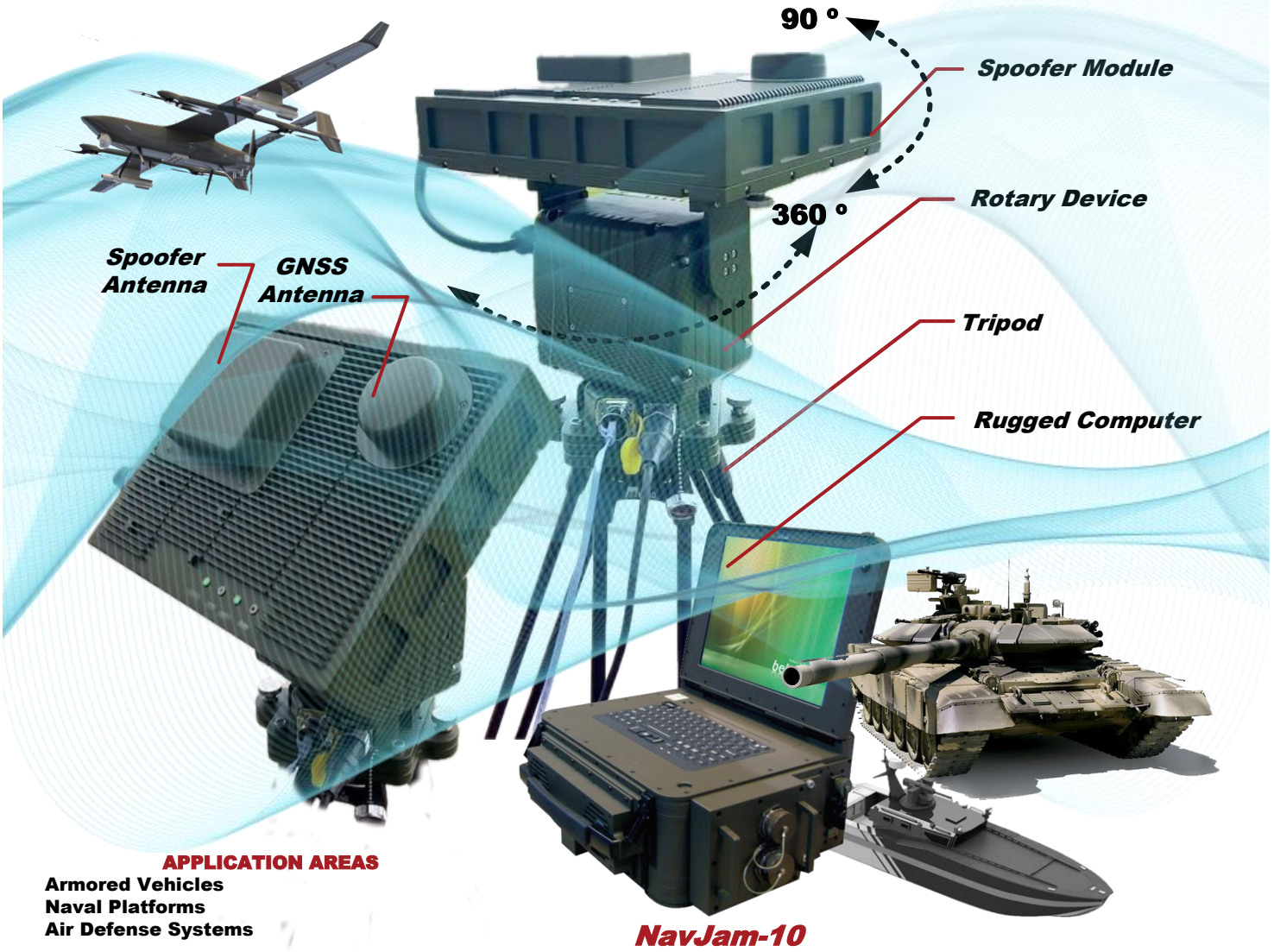
RIMCO JSC
NavJam-10

www.rimco.ru

Navigation Spoofing System

Electronic Warfare Equipment for Air Defense Systems



APPLICATION AREAS

Armored Vehicles
Naval Platforms
Air Defense Systems

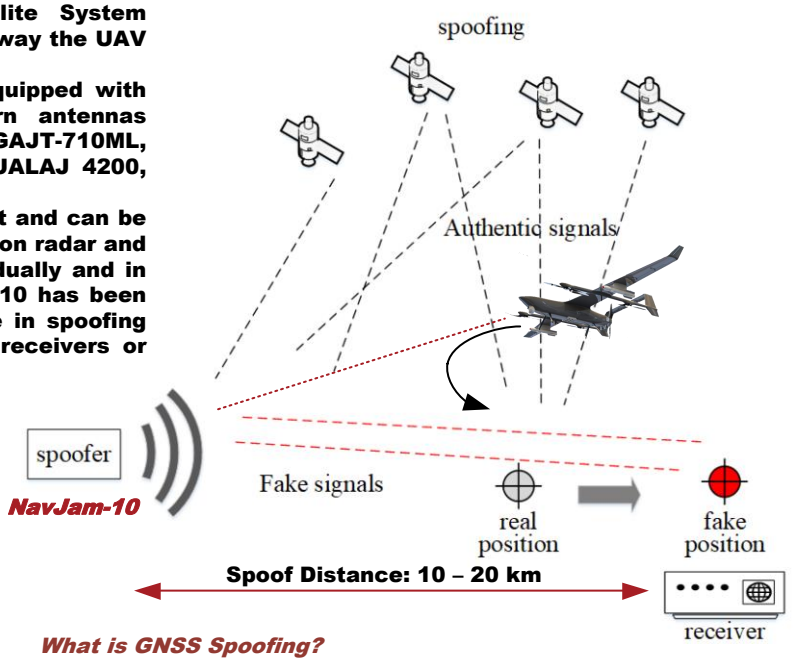
RIMCO JSC the NavJam-10 Navigation Spoofing System (NSS) uses advanced satellite navigation simulation technology to generate launch navigation deception Global Navigation Satellite System (GNSS) signals, enabling the UAV to land in place, drive away the UAV or guide the UAV to land at a designated location.

The NavJam-10 allows for spoofing attacks on UAVs equipped with anti-jamming antennas or controlled reception pattern antennas (CRPA), for example Hexagon/NovAtel GAJT-410ML/GAJT-710ML, ATIS AJ-2A/AJ-3R, Kosminis Vytis KV-AJx, TUALCOM TUALAJ 4200, InfiniDome GPSdome2, Calian's CR8894SXF+ and others.

The NavJam-10 is related to electronic warfare equipment and can be used alone or in conjunction with UAV low altitude detection radar and UAV detection countermeasures. Can be deployed individually and in vehicles deployment and fixed deployment. The NavJam-10 has been tested on the battlefield and has proven highly effective in spoofing attacks on enemy combat UAVs with embedded GNSS receivers or CRPA.

Specification

Spoofing GNSS Receiver and CRPA:
GPSL1 1575.42MHz + GPS L2 1227.6MHz
BDS B1 1561.098MHz + BDS B2 1207.14MHz
Glonass L1 1602MHz + Glonass L2 1246MHz
Galileo 1575.42MHz.....and others.
Spoof Distance: 10 – 20 km
Coverage: 360° whole airspace (Directional 90° optional)
Simultaneous Deception Quantity: 10 UAV
Weight: 30 kg
Size: 410×300 ×44 mm
Temperature: -40°C to +85°C
Environmental Tests: MIL-STD-810G
EMI / EMC: MIL-STD-461F
Performance (Actual performance for specific threat environments varies and is classified. Contact us for more information)



What is GNSS Spoofing?

Spoofing involves broadcasting fake GNSS signals to deceive a receiver into calculating an incorrect position, potentially causing a UAV or missile to deviate from its intended path. Unlike jamming, which disrupts signals, spoofing is more insidious as it can go undetected without proper countermeasures.