CYBER- UND
INFORMATIONSRAUM

JAMMING & SPOOFING IN THE CONTEXT OF ELECTROMAGNETIC WARFARE

Henning Lübbers

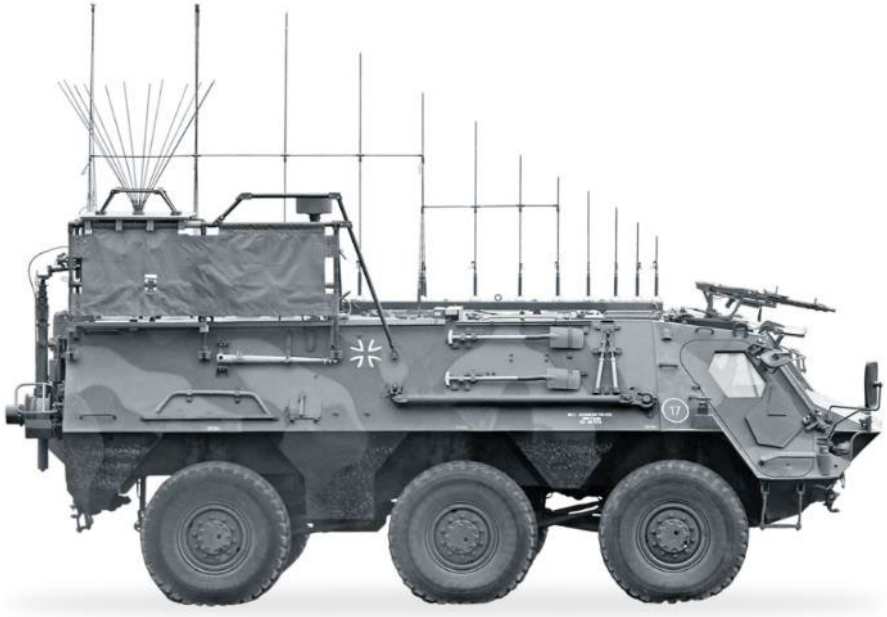
(NARFA DEU / German Cyber and Information Domain Service Headquarters)

BUNDESWEHR

DIFFERENT PERSPECTIVES

When Regulators think about Jammers

When the Military thinks about Jammers



SOME DEFINITIONS

Jamming

Deliberate interference, caused by emissions intended to render unintelligible or falsify the whole or part of a wanted signal.

Source: NATO Terminology Database

Spoofing #1 (Quite specific)

In electronic warfare, creation of false radar targets primarily used for deception.

Source: NATO Terminology Database

Spoofing #2 (More general)

The act of fooling a legitimate user into believing that he is interacting with the intended data processing system or network when, in fact, he is not.

Source: NATO Terminology Database

THE MILITARY VIEW ON JAMMING AND SPOOFING

THE MILITARY VIEW ON JAMMING AND SPOOFING

Context: Electromagnetic Warfare (EW)

- General approach in military mission planning (applies also to EW)
  - Step 1: Determine the effect that needs to be achieved
  - Step 2: Choose and deploy a suitable asset to achieve the effect
- Definition of EW: Military action that exploits electromagnetic energy to provide situational awareness and create offensive and defensive effects.
- Every military operation in the “real world” (Surveillance / Defense / Attack) has a counterpart in the electromagnetic environment
- EW operations can be missions in their own right, but usually support or enable more complex missions involving a variety of assets

THE MILITARY VIEW ON JAMMING AND SPOOFING

THE AVIATIONIST | Home | Military Aviation | Helicopters | Drones | Global Hotspots | Explore | Advertise with us | Subscribe to Newsletters

Home > Drones > Captured Stealth Drone > Captured U.S. stealthy drone was hijacked exploiting GPS vulnerability. But hack description does not solve the mystery

CAPTURED STEALTH DRONE | DRONES | INFORMATION SECURITY | INFORMATION WARFARE | IRAN | MILITARY AVIATION

Captured U.S. stealthy drone was hijacked exploiting GPS vulnerability. But hack description does not solve the mystery

Military Jamming and Spoofing Operations

- Typical uses of EW by the military
  - Conceal own activities → Jamming
  - Disrupt the opponent's communication → Jamming
  - Set hostile vehicles off-course → Jamming/Spoofing
  - Eavesdrop on the opponent's communication → Spoofing

- Current Focus: Navigational Warfare

THE MILITARY VIEW ON JAMMING AND SPOOFING

Navigational Warfare

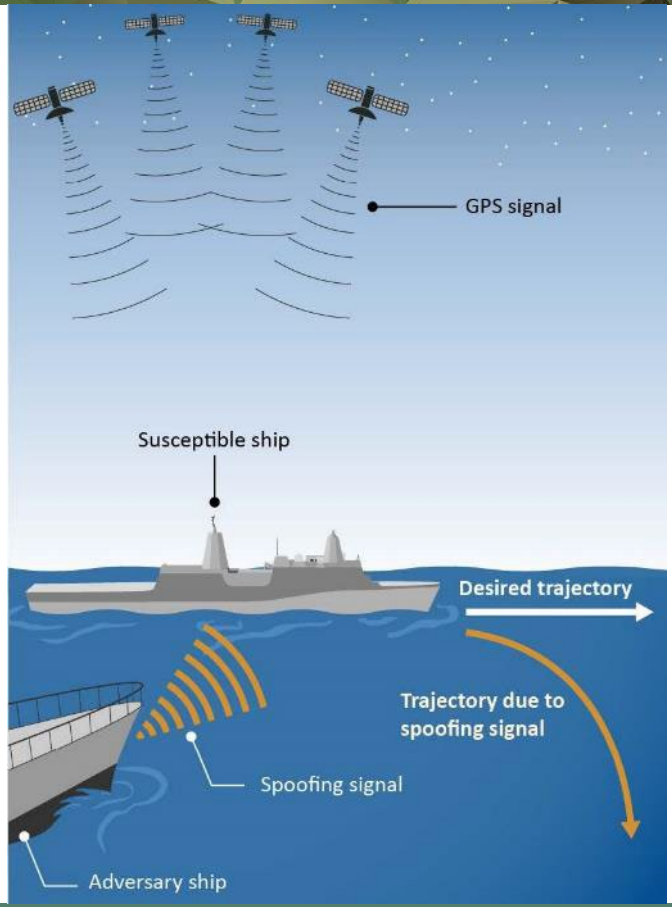
- Big Challenge for Civil Sectors and Military
- Mitigation possible, but tedious and pricy
- Alternative means of navigation required

BBC

Home News Sport Business Innovation Culture Arts Travel Earth Audio Video Live

Sweden accuses Russia of GPS jamming over Baltic Sea

4 September 2025



Example of EW Surveillance from the Past

- Generalized, but based on real events
- Military naval vessel operates in open waters
- All of a sudden: Private devices connect to a base station that just “appeared”
- Unaware soldiers start to exchange unencrypted messages with their friends and family
- Assumed hostile intention: Gathering intelligence to put pressure on soldiers, e. g. by threatening their families
- Potential Countermeasure: Awareness and restrictions on the use of private devices

Is this even Spoofing? Depends on the definition!

Characteristics of Military Jamming and Spoofing

- During training and exercise
  - Limited to a previously known area
  - Times of jamming/spoofing are somewhat predictable
  - Prior coordination with other spectrum users is possible
  - Jamming/spoofing can be interrupted or stopped if necessary („Stop Buzzer“)
- During operations
  - (Public) Disclosure of planned jamming/spoofing may compromise mission (Example: Jamming as a means of protecting a convoy)
  - Need for jamming/spoofing may arise on very short notice (Example: Defense against missiles/drones)

„Jamming“ Airspace without EW

- Weather Balloons from Belarus
- Obvious Intention: Smuggling Cigarettes
- Side Effect: Shutdown of Vilnius Airport
- At least 11 balloons, 2 directly over the airport
- 30 flights / 6000 passengers affected

Food4Thought

A desired effect can often be achieved by many different means

BBC

Home News Sport Business Innovation Culture Arts Travel Earth Audio Video Live

Balloons used to smuggle cigarettes shut Lithuanian airport

6 October 2025

Share Save

Dearbail Jordan

KEY TAKEAWAYS

Attempt of a Summary

- Electronic Warfare is an integral part of military activities
- Military jamming/spoofing is a means of achieving necessary effects
- In the context of training and exercise jamming/spoofing can be coordinated
- In the context of military operations it is usually not possible to coordinate jamming/spoofing

THANK YOU!

QUESTIONS?

COMMENTS?