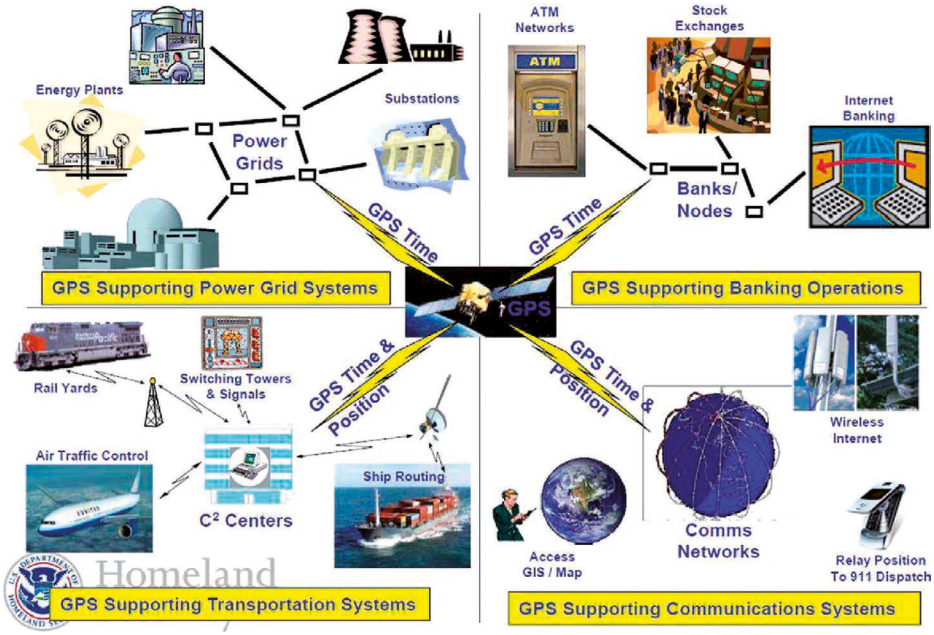
# Was ist GNSS-Spoofing?

*Spoofing ist der Versuch, einen GNSS-Empfänger zu täuschen, sodass er gefälschte Signale empfängt und verfolgt.*




Sobald der Empfänger die gefälschten Signale empfängt, kann der Spoofer die erforderliche Anzahl an Fehlern einfügen und so die Kontrolle über die vom Empfänger berechnete Position erlangen. Durch Spoofing werden also irreführende Navigationsinformationen in den GNSS-Empfänger eingespeist. Die gefälschten Signale können so verändert werden, dass der Empfänger seine Position anders einschätzt, als sie tatsächlich ist, oder dass er seine Position zwar richtig einschätzt, aber zu einem anderen Zeitpunkt, als tatsächlich festgelegt. Die Größe des eingeführten Fehlers kann zwischen wenigen Metern und tausenden von Kilometern liegen. Das Bild zeigt ein Schiff, das durch Spoofing seines GNSS-Navigationssystems von seinem vorgesehenen Kurs abgelenkt wird.

*Quelle:*
*Spoofing Detector - Accord's Anti-Spoofing Solution for GNSS*

*Accord Software & Systems*
*www.accord-soft.com*

*übersetzt und leicht gekürzt von FS*

### Anfälligkeit von GNSS-Empfängern

GNSS-Empfänger, die auf zivilen Signalen basieren, sowohl stationäre als auch mobile, sind am anfälligsten für Spoofing. Diese Empfänger akzeptieren einfach ein Signal mit höherer Leistung und überprüfen nicht die Authentizität.

Bei stationären Empfängern, die am häufigsten für Zeit-/Referenzstationen ohne Anti-Spoofing-Prüfungen verwendet werden, kann man die Genauigkeit der Zeitmessung und der Positionsmessungen erheblich beeinträchtigen. Selbst schnell bewegliche Empfänger, deren Bewegung genau bestimmt werden kann, sind anfällig, wenn der Spoofer ihren Standort dynamisch schätzen kann.

### Fälle von GNSS-Spoofing

In den letzten Jahren sind viele Berichte über Vorfälle in der Öffentlichkeit erschienen, die auf GNSS-Spoofing zurückgeführt werden. Nachfolgend sind einige dieser Vorfälle aufgeführt. Im Dezember 2011 behauptete der Iran, die Drohne RQ-170 Sentinel gespooft und das Flugzeug zur Landung auf seinem Boden getrickst zu haben. Im Januar 2016 kaperte der Iran zwei Flusspatrouillenboote der Vereinigten Staaten. Im Juni 2017 wurden offenbar rund 20 russische Schiffe im Schwarzen Meer gefälscht.

### Auswirkungen von Spoofing auf militärische Systeme

In militärischen GNSS-Anwendungen kann Spoofing, wenn es unentdeckt bleibt, schwerwiegende Folgen haben:

- Wirksamkeit von Waffen verringern, da diese ihr beabsichtigtes Ziel verfehlen könnten
- Soldaten, die mit GNSS-Geräten navigieren, durch Positionsfehler verwirren, sie auf eine falsche Route locken und sie zu leichten Zielen für den Feind machen.
- luftgestützte Lenkflugkörper zu einem anderen Ziel lenken und es dem Feind ermöglichen, kritische Infrastrukturen und Anlagen zu schützen
- die synchronisierte Funktion von GNSS-basierten luft- und seegestützten Zeitmesssystemen stören

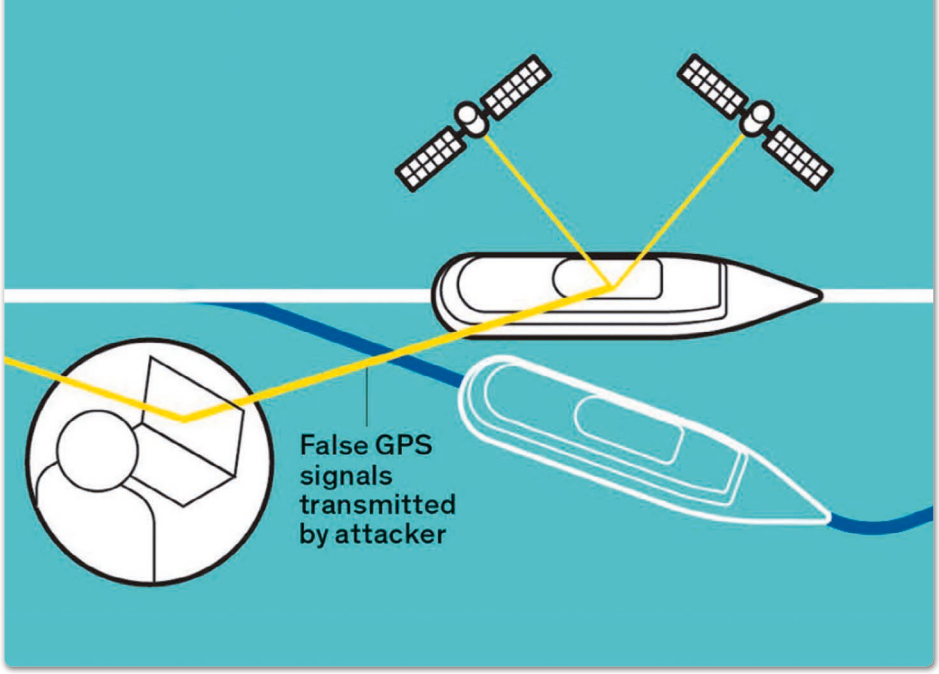
Die einzige Schutzmaßnahme besteht darin, über eine Infrastruktur zu verfügen, die alle Bedrohungen umfassend identifiziert und rechtzeitig Warnungen ausgibt. Diese Infrastruktur wird kontinuierlich benötigt, um Empfänger vor Spoofing und Störungen zu schützen, da die Einführung neuer Satelliten, die militärische Signale unterstützen, mehrere Jahre dauern kann. Daraus folgt:

Die Realisierung von Empfängergeräten, die militärische Signale unterstützen, und die Aufrüstung bestehender Anlagen wird lange dauern. Möglicherweise sind nicht alle Empfänger mit militärischen GNSS-Signalen kompatibel.

### Auswirkungen von Spoofing auf zivile Einrichtungen

Spoofing kann verschiedene zivile Infrastrukturen beeinträchtigen, da diese alle auf zivilen GNSS-Empfängern basieren und GNSS in die Geräte integriert ist: Stromnetze, Banken, Börsen, Eisenbahnen, Flugzeug-Landesysteme, Schiffe, Mobilfunknetze, Rettungsdienste, Börsen.

Denn beispielsweise die Überwachung des Stromnetzes basiert auf GNSS-Zeitstempeln, mit denen die Effizienz der Stromverteilung im gesamten Netz durch Echtzeitmessungen der Spannung und Stromphasen verbessert wird. Spoofing kann zu irreführenden Zeitstempeln




*Ablenkung eines Schiffes © spectrum.ieee.org*

führen, die falsche Abweichungen in den gemessenen Phasenwinkeln verursachen können, was zu unnötigen Kontrollmaßnahmen seitens der Netzbetreiber führt, wie z.B. das Abschalten von Generatoren.

### Was bedeutet ein Spoofing-Vorfall?

Spoofing könnte ein Hinweis auf feindliche Aktivitäten in Grenzregionen sein, kann von Feinden genutzt werden, um UAVs, Flugzeuge, Truppen usw. in die Irre zu führen.

Spoofing könnte ein Hinweis auf einen Terroranschlag sein. Denn Spoofing könnte genutzt werden, um Rettungsdienste, Armee- und Polizeifahrzeuge, die sich auf GNSS-basierte Karten verlassen, um zum Ort des Terroranschlags zu gelangen, abzulenken.

### Der GNSS-Spoofing-Detektor

Der beste Weg, Anlagen vor der Gefahr von GNSS-Spoofing zu schützen, ist die frühzeitige Erkennung des Spoofers mit einem externen Spoofer-Detektor. Accord Software & Systems hat ein solches Produkt namens Spoofer Detector entwickelt. Es erkennt das Vorhandensein von Spoofern und warnt den Benutzer sofort über das Vorhandensein von Spoofer-Signalen. Diese Warnung kann entweder dazu verwendet werden, das HF-Signal zu blockieren, oder um das Gerät zu warnen, das HF-Signal nicht zu verwenden. Die Lösung kann angepasst werden für Militär, Industrie, Avionik, Schifffahrt und andere Anwendungen, sowohl stationäre als auch bewegliche.

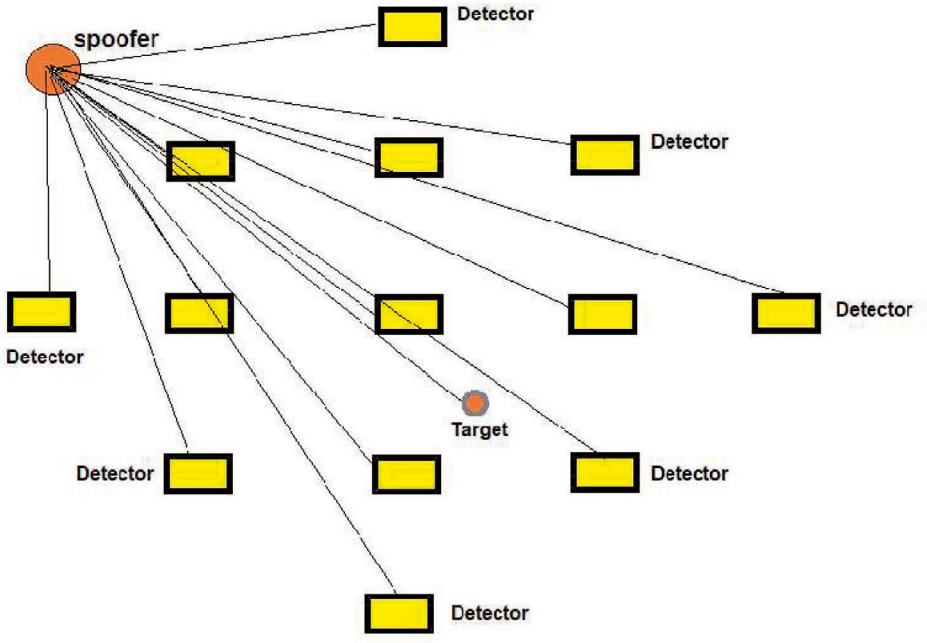
### Spoofing-Erkennungsnetzwerk

Um eine umfassende Abdeckung zu gewährleisten, kann ein Netzwerk von Spoofing-Detektoren sehr einfach in dem gesamten zu schützenden Bereich installiert werden durch die Installation einer Reihe von Spoofer-Detektoren in einem bestimmten geografischen Gebiet. Bei Auftreten von Spoofing können zeitnahe Navigations-EW-Warnungen an Geräte und Personal in der Region ausgegeben werden. Jeder Detektor ist mit einem dedizierten sicheren drahtlosen Netzwerk verbunden, um EW-Informationen an einen Server zu übermitteln.

Dies würde dabei helfen, geeignete Maßnahmen zur Abwehr der Bedrohung zu ergreifen oder einen Auslöser zu generieren, um bei Bedarf eine geeignete alternative Navigationshilfe auszuwählen. Die von mehreren solchen Geräten gesammelten Eingaben können von einem Server verarbeitet werden, um die Quelle des Spoofings/Meaconings ungefähr zu lokalisieren.

### Vorteile des Detektornetzwerks

- kontinuierliche Überwachung von Spoofing-/Jamming-/Meaconing-Angriffen
- Alarmierung der Einsatzkräfte bei solchen Vorfällen, damit sie auf alternative Navigationsmittel zurückgreifen können
- versorgt die Einsatzkräfte mit den entsprechenden Informationen, um fundierte taktische Entscheidungen zu treffen
- liefert Input für Empfängersysteme, die eingesetzt werden, um auf andere Konstellationen umzuschalten und die Navigation fortzusetzen.
- In Verbindung mit elektronischen Angriffssystemen ermöglicht es den Empfängern, zwischen freundlichen und feindlichen Störungen zu unterscheiden.
- hilft Kommandeuren zu Lande, in der Luft und auf See, die notwendigen Maßnahmen zu ergreifen, z.B. die Verfügbarkeit von Gegenmaßnahmen sicherzustellen, bevor eine Mission gestartet wird ◄




***Schutz indischer Flughäfen durch ein Netzwerk von Spoofing-Detektoren. Flughäfen können durch GNSS-Spoofing funktionsunfähig gemacht werden***