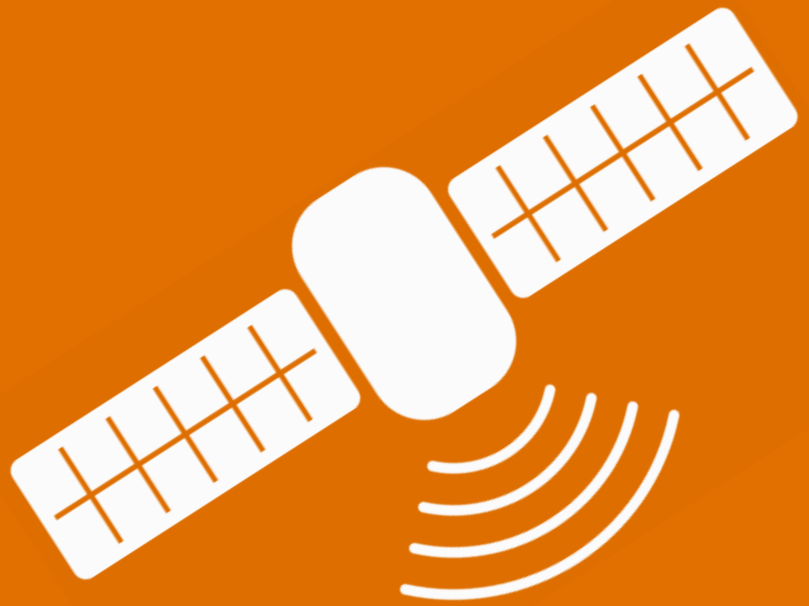


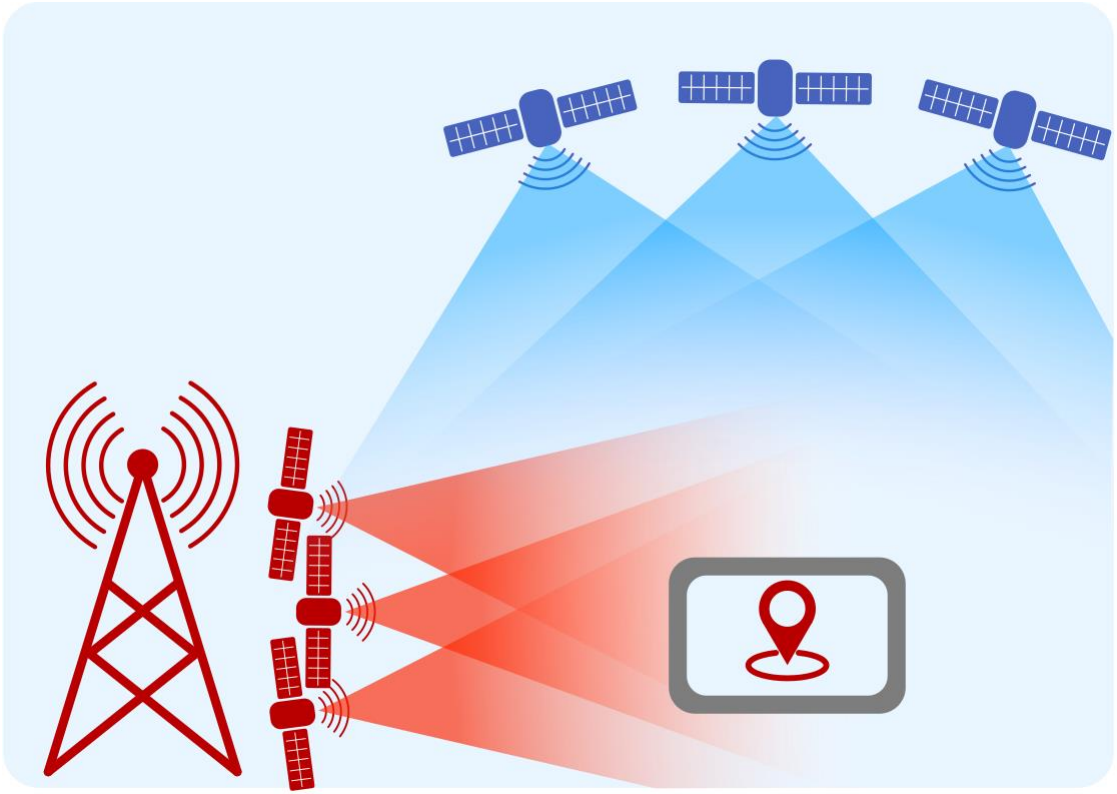
GNSS Spoofing en Detectie

Workshop GNSS Interferentie en Spoofing

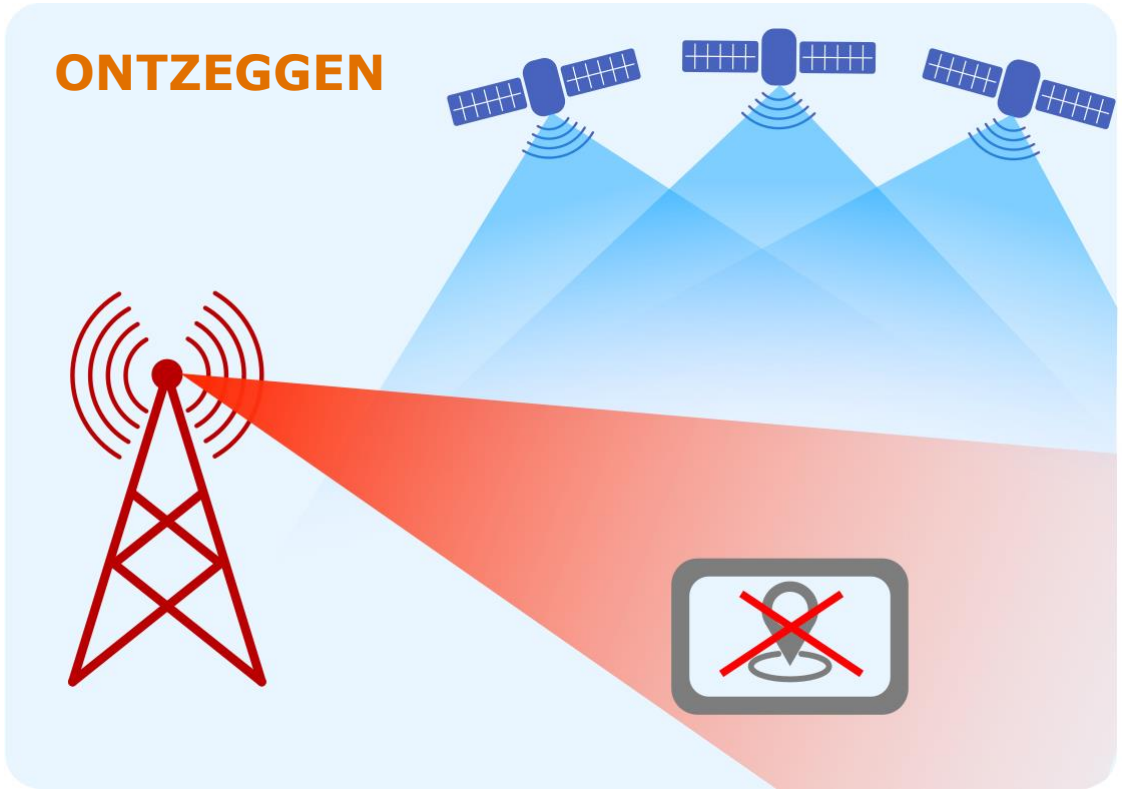
Barend Lubbers

Spoofing

To assume or emulate the identity of another user or device in order to gain access to a system



Doel Opzettelijke interferentie



Onderwerpen

- Hoe werkt een GNSS spoofer
- Welke types spoofers bestaan er
- Hoe kan spoofing worden gedetecteerd?
- Van spoofing naar jamming

GNSS Spoofing: from fiction to reality

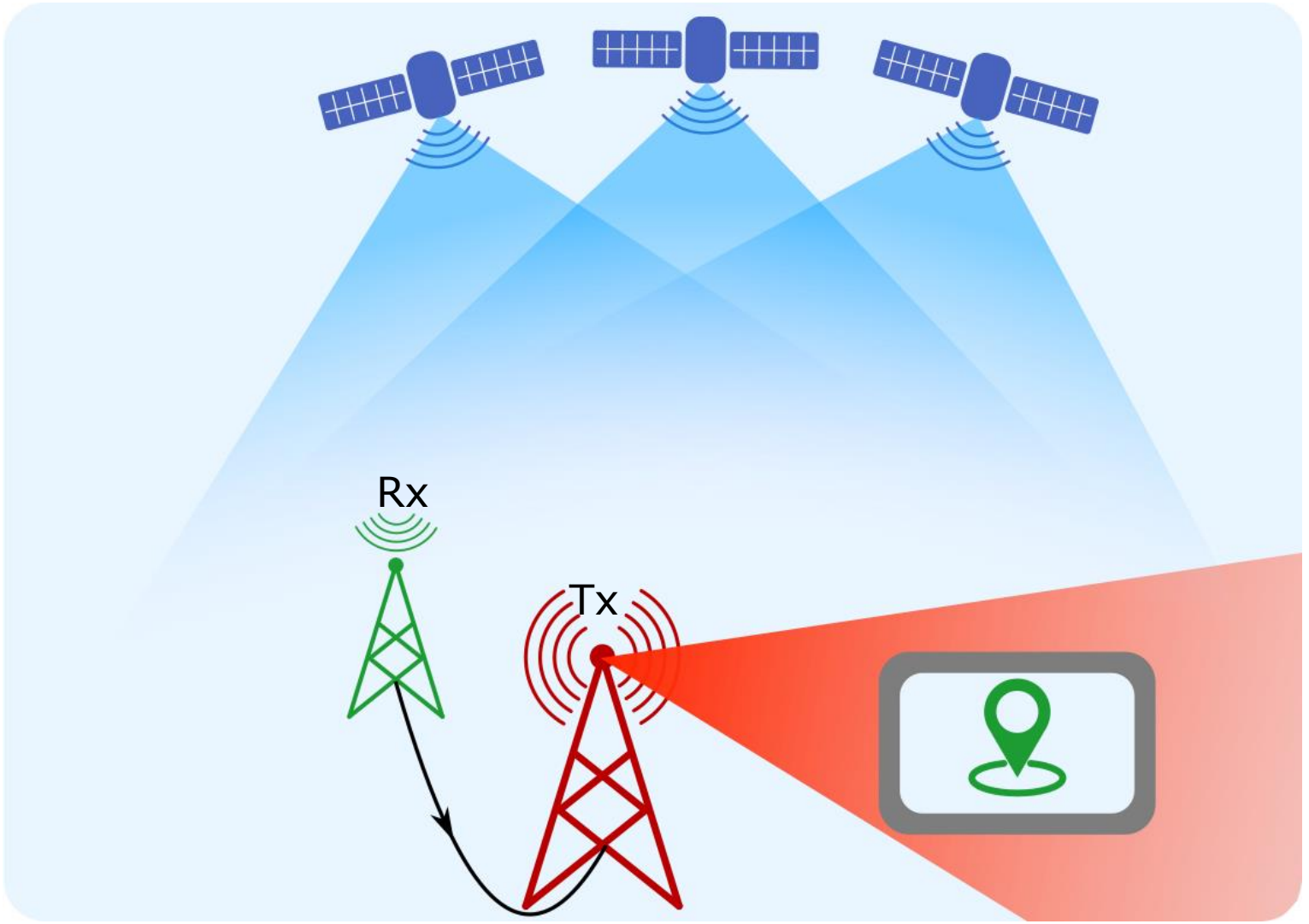
James Bond: Tomorrow Never Dies: Villans spoof HMS Devonshire into Chinese waters

GPS Risk Assessment Study, John Hopkins University: There is no credible spoofing threat

Portable spoofer by T.D. Humpreys et al. Article in GP World

1995 2000 2005 2010 2015 2020 2025

Meaconing



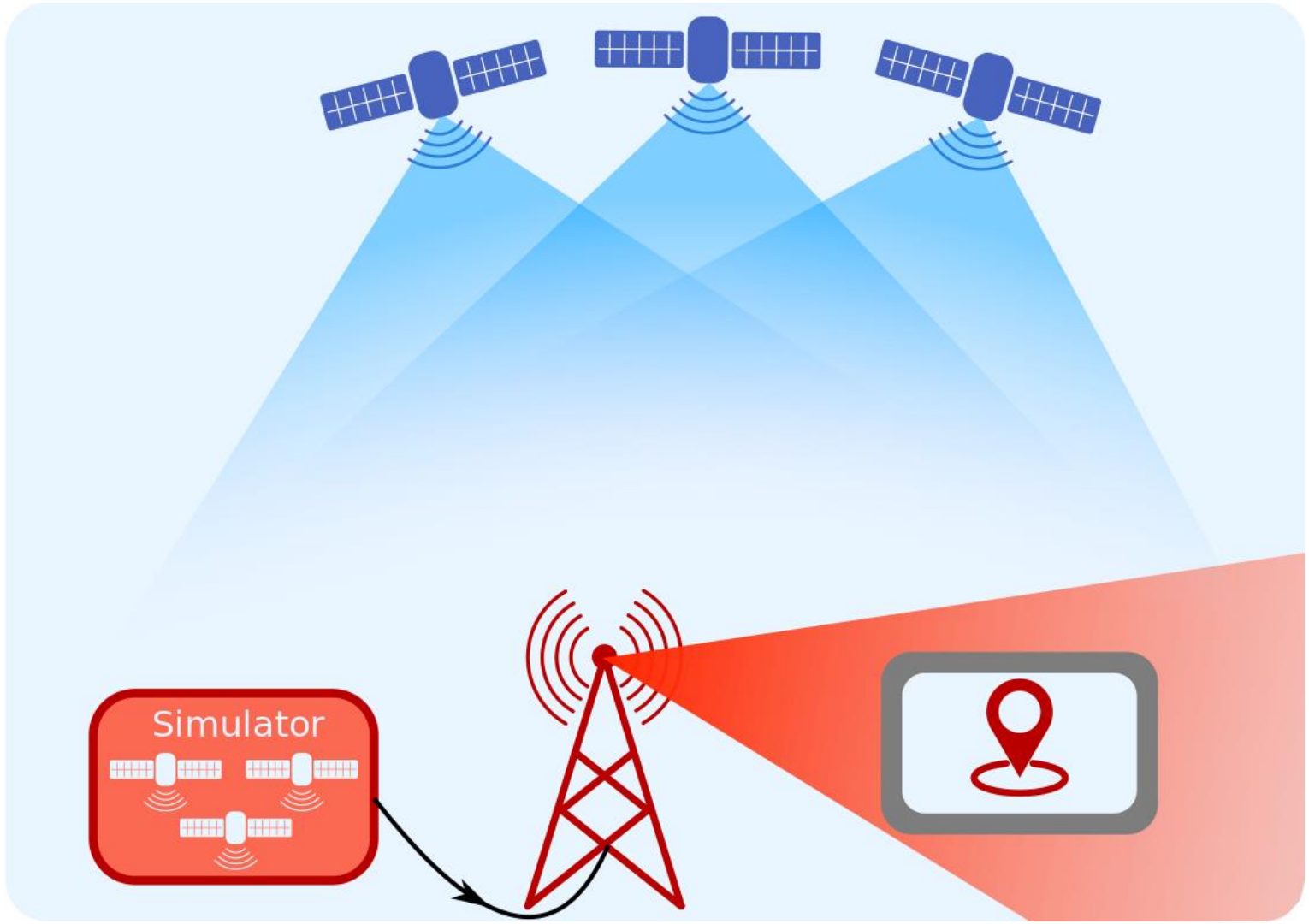
GPS signaal

Het civiele GPS signaal bestaat uit:

- Draaggolf
- Spreading code
- Data bericht

De beschrijving van het signaal is volledig openbaar en vrij verkrijgbaar op internet

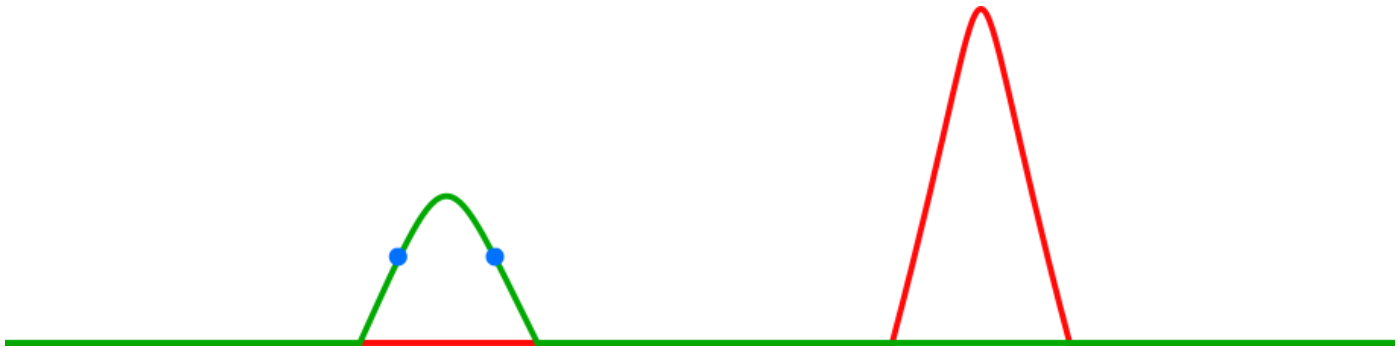
GNSS signaal simulator



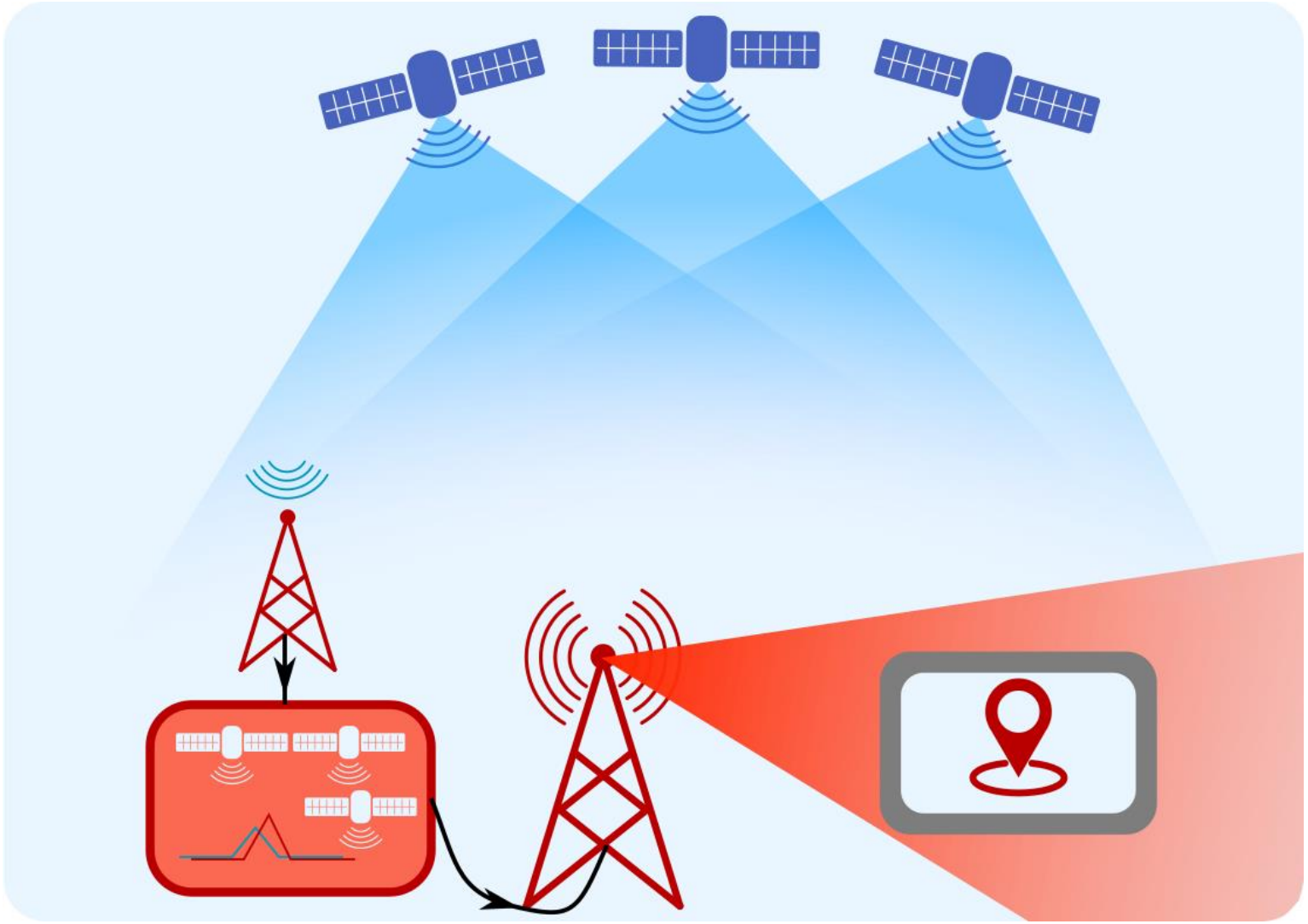
Meaconing en signaal simulator spoofers

- Consistente metingen
  - Niet te detecteren met conventionele RAIM technieken

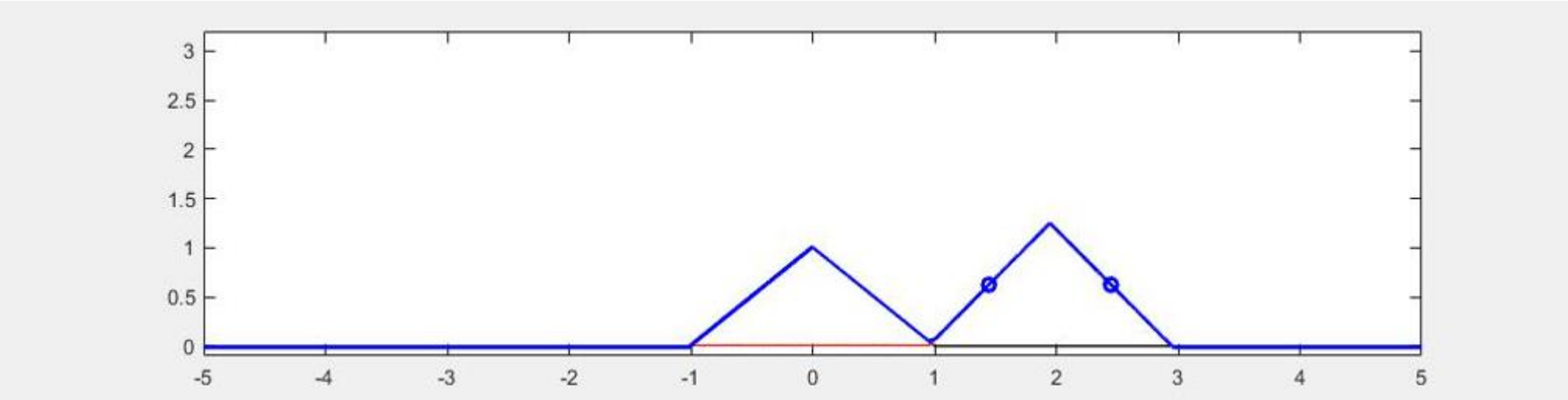
- Ontvanger alleen kwetsbaar in acquisitie fase
  - Combineren met jammer
  - Loss of Lock



Seamless take-over



Seamless take-over spoofer



GNSS Spoofing: from fiction to reality

James Bond: Tomorrow Never Dies: Villans spoof HMS Devonshire into Chinese waters

GPS Risk Assessment Study, John Hopkins University: There is no credible spoofing threat

Portable spoofer by T.D. Humpreys et al. Article in GPS World

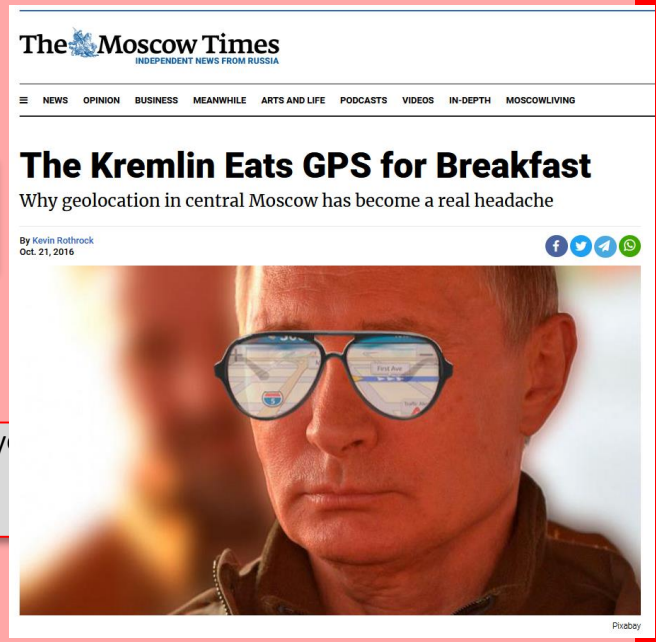
Demonstration of spoofing on a helicopter drone (2012) and a 80M$ super yacht (2013) by T.D. Humpreys

Iran hijacks US RQ-170 (GPS Spoofing??)

US patrol boat strayed into Iranian waters (GPS spoofing??)

Reports of spoofing in Moscow

DEFCON 23 & 24 DIY GPS spoofing & Drone attack



1995 2000 2005 2010 2015 2020 2025

Spoofing detectie

RECEIVER AUTONOMOUS INTEGRITY MONITORING (RAIM)

- Controleert de consistentie van de metingen
- Niet effectief tegen de meeste spoofing aanvallen

ONTVANGEN VERMOGEN

- Signaal sterkte van het ware signaal is bekend
- Automatic gain control
- Realistische C/N_0

Spoofing detectie

CONTROLE DATABERICHT

- Is het bericht complete? Almanak etc.
- Word Error Rate (WER)
- Navigation Message Authentication (NMA)

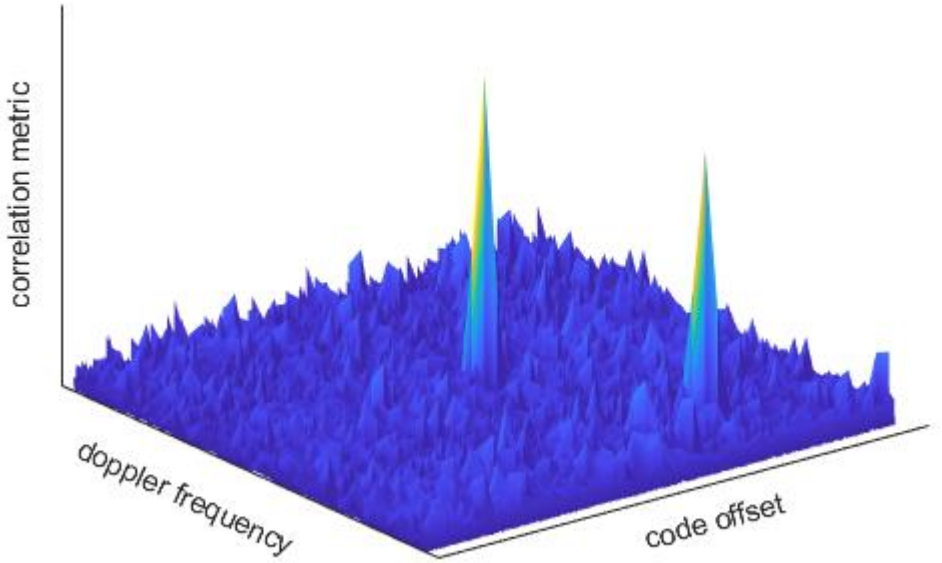
DRIFT DETECTIE

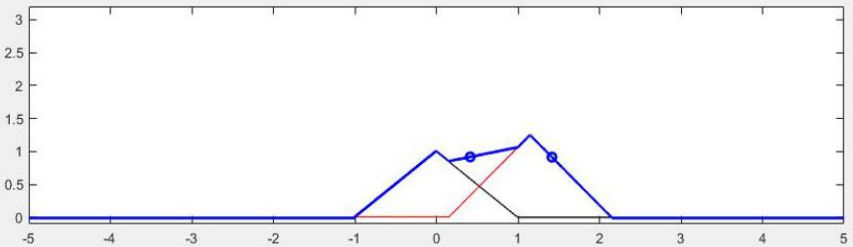
- Sprong in positie of tijd
- Onrealistische dynamica
- Inconsistentie met andere sensoren (IMU, log, etc)

Spoofing detectie

AUTOCORRELATIEFUNCTIE

- Tijdens overname => vervorming van autocorrelatiefunctie
- Na overname => meerdere correlatie pieken zichtbaar
- Multipath

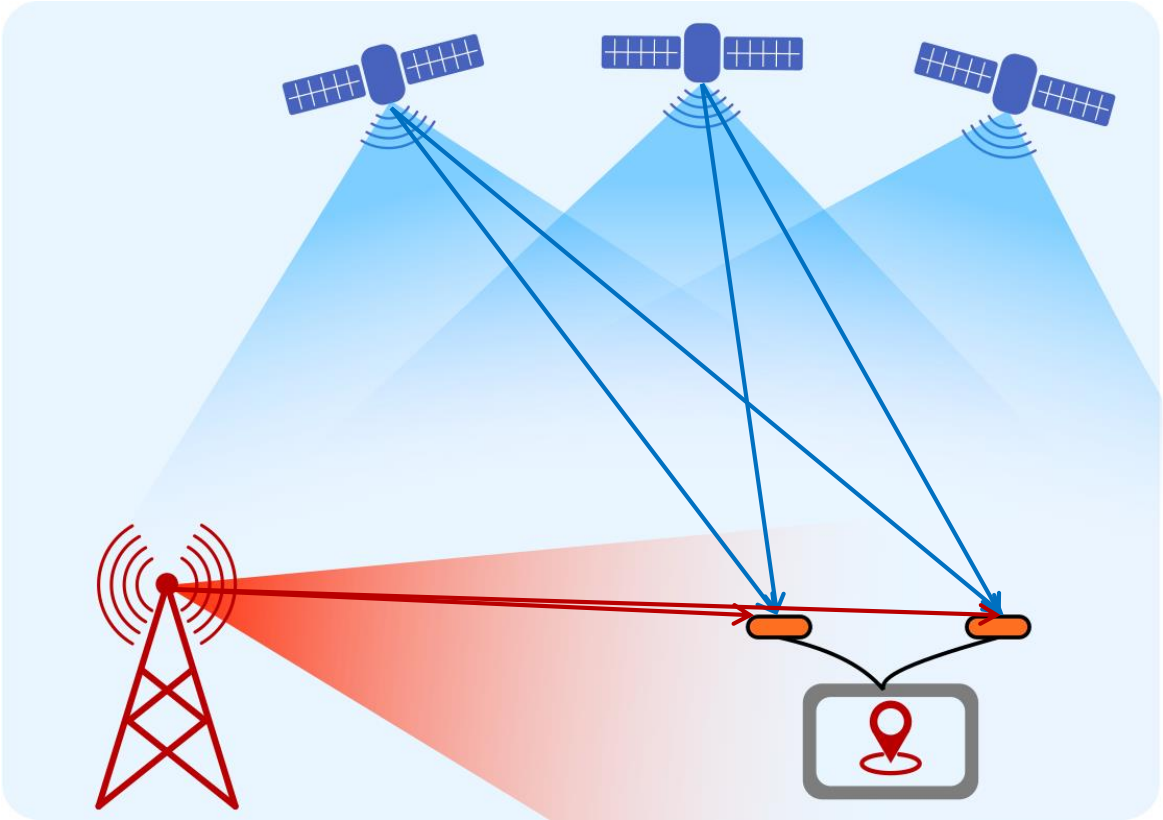




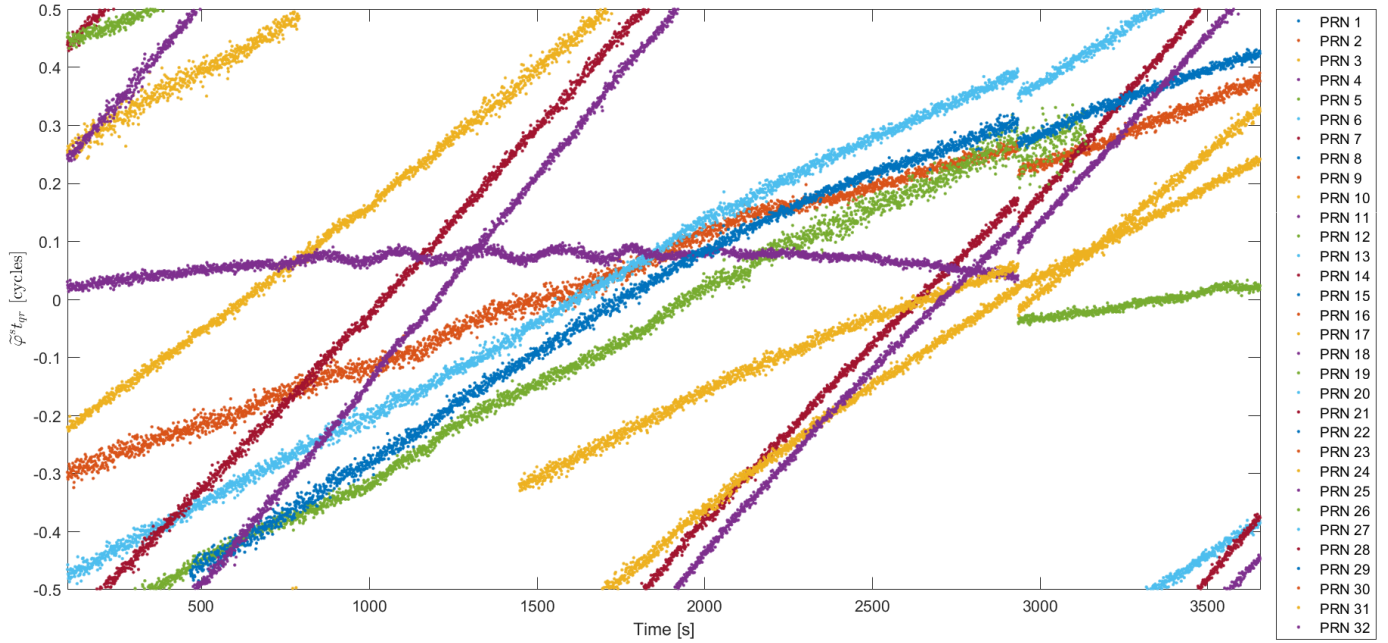
Spoofing detectie

ONTVANGER SATELLIET GEOMETRIE

- Meerdere antennes => angle of arrival
- Komen de signalen uit de te verwachten richting?
- Alle signalen uit dezelfde richting => spoofing



NIET GESPOOFED



GESPOOFED

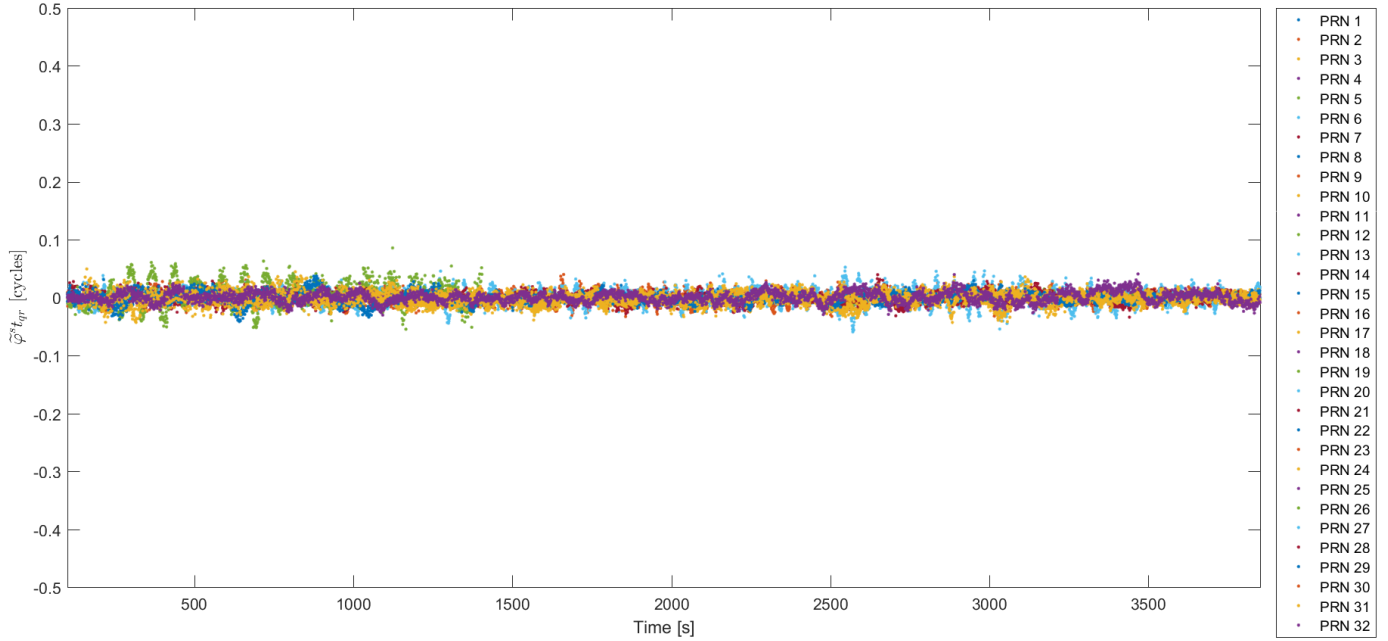


TABLE I: Cost-Ranked Matrix of GNSS Spoofing Attack and Detection Techniques

Detection	Attack Techniques												
Techniques	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13
D1	X	X	X	X	X	X	X	X	X	X	X	X	X
D2	∼	✓	X	X	∼	X	X	X	X	X	X	X	X
D3	∼	∼	∼	∼	∼	X	X	∼	∼	∼	∼	X	X
D4	∼	✓	∼	∼	∼	∼	∼	∼	∼	∼	∼	∼	∼
D5	✓	✓	✓	✓	✓	∼	∼	✓	✓	✓	✓	∼	∼
D6	X	✓	✓	X	X	✓	X	✓	✓	X	X	✓	X
D7	X	✓	✓	∼	X	✓	∼	✓	✓	∼	X	✓	∼
D8	X	✓	✓	∼	X	✓	∼	✓	✓	∼	X	✓	∼
D9	∼	✓	✓	✓	∼	✓	✓	✓	✓	✓	∼	✓	✓
D10	✓	✓	✓	✓	✓	✓	✓	✓	∼	∼	∼	∼	∼
D11	✓	✓	✓	✓	✓	✓	✓	X	∼	∼	∼	∼	∼
D12	X	✓	✓	∼	X	✓	∼	✓	✓	∼	X	✓	∼
D13	X	✓	✓	∼	X	✓	∼	✓	✓	∼	X	✓	∼

Detection probability matrix keys: ✓ – high, ∼ – intermediate or case-dependent, X – low

	Detection Techniques Key		Attack Techniques Key
D1	Pseudorange-based RAIM	A1	Meaconing, single RX ant., single TX ant.
D2	Observables and RPM	A2	Open-loop signal simulator
D3	Correlation function distortion monitoring	A3	RX/SP, single TX ant., no SCER
D4	Drift monitoring (clock offset, IMU/position)	A4	RX/SP, single TX ant., SCER
D5	Observables, RPM, distortion, and drift monitoring	A5	Meaconing, multi. RX ants., single TX ant.
D6	NMA*	A6	Nulling RX/SP, single TX ant., no SCER
D7	NMA* and SCER detection	A7	Nulling RX/SP, single TX ant., SCER
D8	Delayed symmetric-key SSSC*	A8	RX/SP, single TX ant., sensing of victim ant. motion
D9	NMA*, SCER detection, RPM, and drift monitoring	A9	RX/SP, multi. TX ants., no SCER
D10	Multiple RX antennas	A10	RX/SP, multi. TX ants., SCER
D11	Moving RX antenna	A11	Meaconing, multi. RX ants., multi. TX ants.
D12	Dual-RX keyless correlation of unknown SSSC codes	A12	Nulling RX/SP, multi. TX ants., no SCER
D13	Symmetric-key SSSC* [e.g., P(Y) equiv.]	A13	Nulling RX/SP, multi. TX ants., SCER

* Detection techniques requiring changes to the Signal In Space (SIS); TX: Transmitter; RX: Receiver; RX/SP: Receiver-Spoofer

Mark L. Psiaki and Todd E. Humphreys, "GNSS Spoofing and Detection"

GNSS Spoofing: from fiction to reality

James Bond: Tomorrow Never Dies: Villans spoof HMS Devonshire into Chinese waters

GPS Risk Assessment Study, John Hopkins University: There is no credible spoofing threat

Portable spoofer by T.D. Humpreys et al. Article in GPS World

Demonstration of spoofing on a helicopter drone (2012) and a 80M$ super yacht (2013) by T.D. Humpreys

Iran hijacks US RQ-170 (GPS Spoofing??)

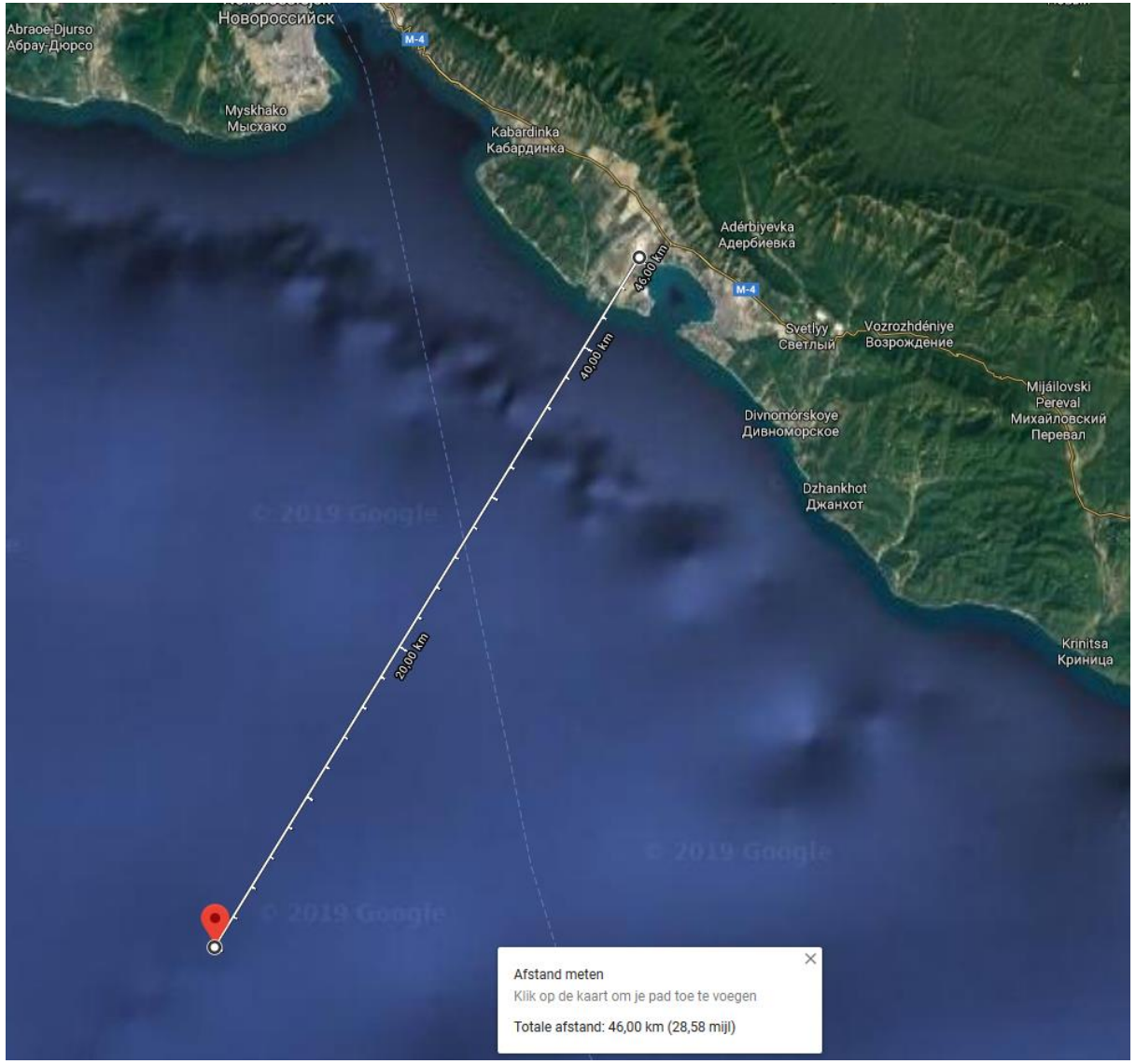
DEFCON 23 & 24 DIY GPS spoofing & Drone attack

Reports of spoofing in Moscow

Black Sea incident

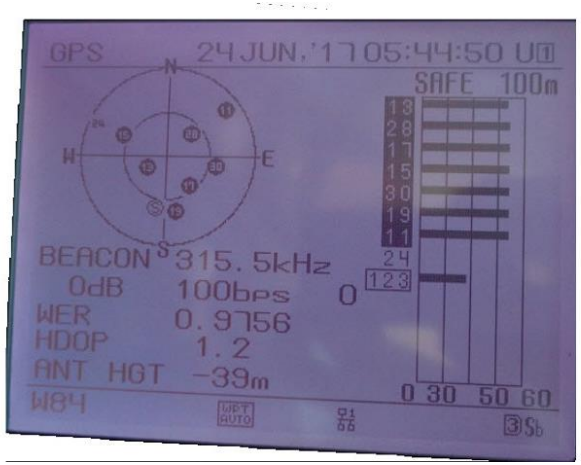
US patrol boat strayed into Iranian waters (GPS spoofing??)

1995 2000 2005 2010 2015 2020 2025



AIS data showing multiple ships on top of each other during their time in the Black Sea

Credit **Gurvan Le Meur**



Zwarte zee, 22 juni 2017

GNSS Spoofing: from fiction to reality

James Bond: Tomorrow Never Dies: Villans spoof HMS Devonshire into Chinese waters

GPS Risk Assessment Study, John Hopkins University: There is no credible spoofing threat

Portable spoofer by T.D. Humpreys et al. Article in GPS World

Demonstration of spoofing on a helicopter drone (2012) and a 80M$ super yacht (2013) by T.D. Humpreys

Iran hijacks US RQ-170 (GPS Spoofing??)

DEFCON 23 & 24 DIY GPS spoofing & Drone attack

C4ADS report: Above us only stars

Black Sea incident

Reports of spoofing in Moscow

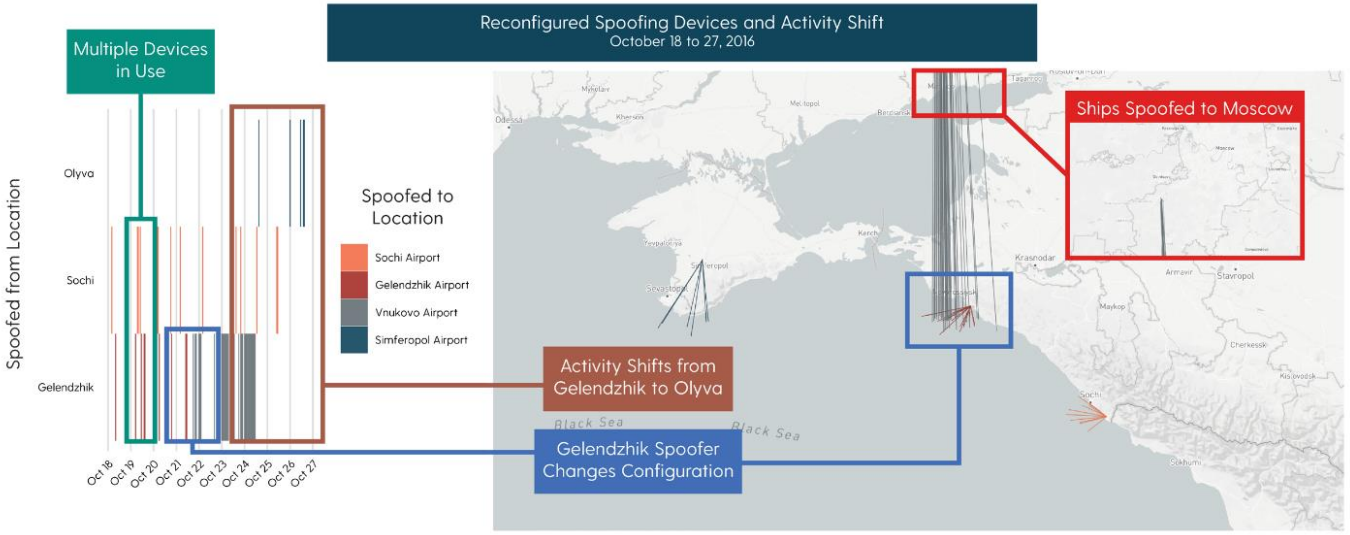
US patrol boat strayed into Iranian waters (GPS spoofing??)

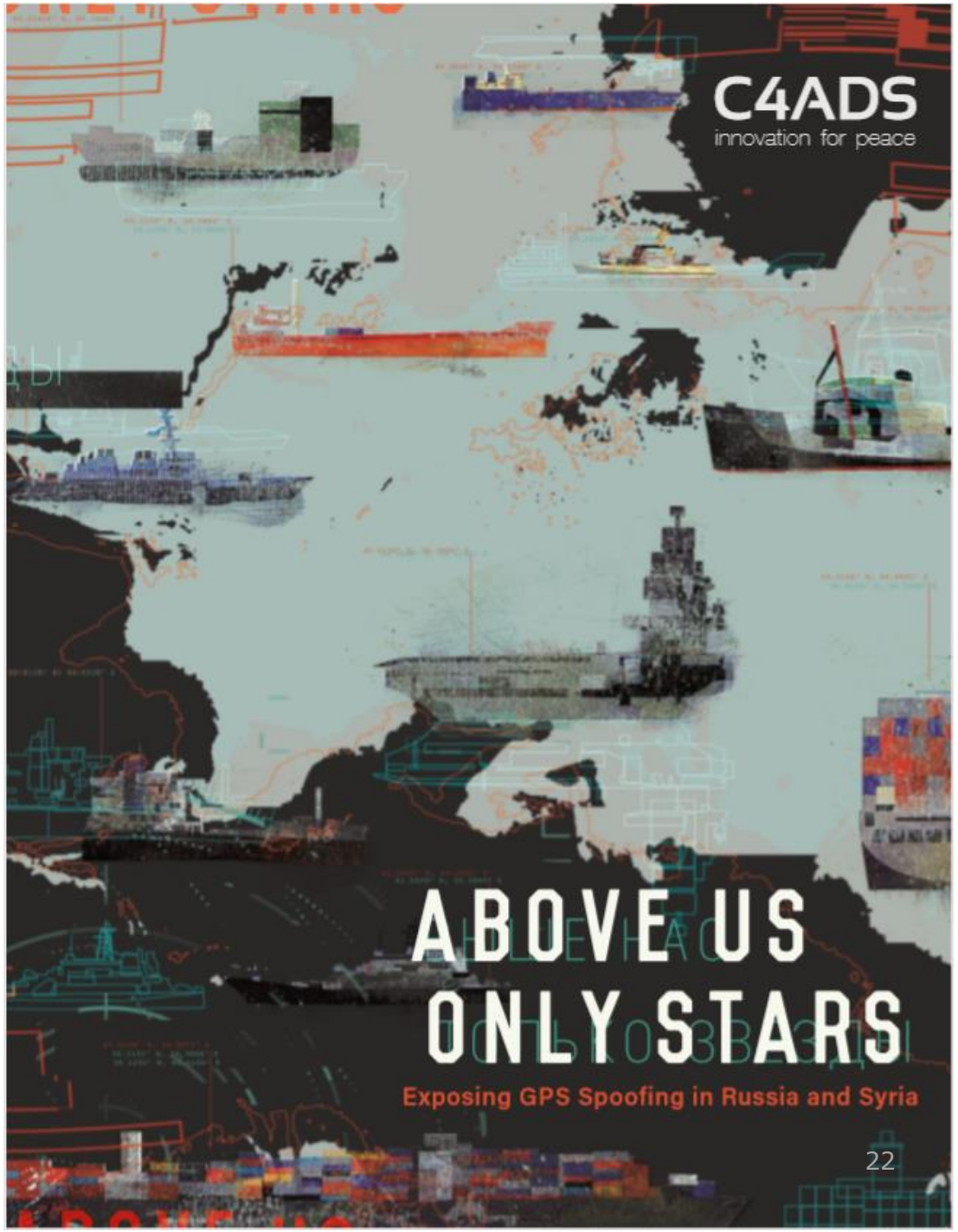
1995 2000 2005 2010 2015 2020 2025

Above us only stars

Exposing GPS Spoofing in Russia and Syria

www.c4reports.org/aboveusonlystars





GNSS Spoofing: from fiction to reality

James Bond: Tomorrow Never Dies: Villans spoof HMS Devonshire into Chinese waters

GPS Risk Assessment Study, John Hopkins University: There is no credible spoofing threat

Portable spoofer by T.D. Humpreys et al. Article in GPS World

Demonstration of spoofing on a helicopter drone (2012) and a 80M$ super yacht (2013) by T.D. Humpreys

Iran hijacks US RQ-170 (GPS Spoofing??)

DEFCON 23 & 24 DIY GPS spoofing & Drone attack

Reports of spoofing in Moscow

US patrol boat strayed into Iranian waters (GPS spoofing??)

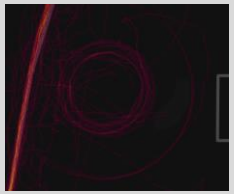
C4ADS report: Above us only stars

Black Sea incident

US UAV shot down in Iranian airspace according to Iran. (GPS spoofing??)

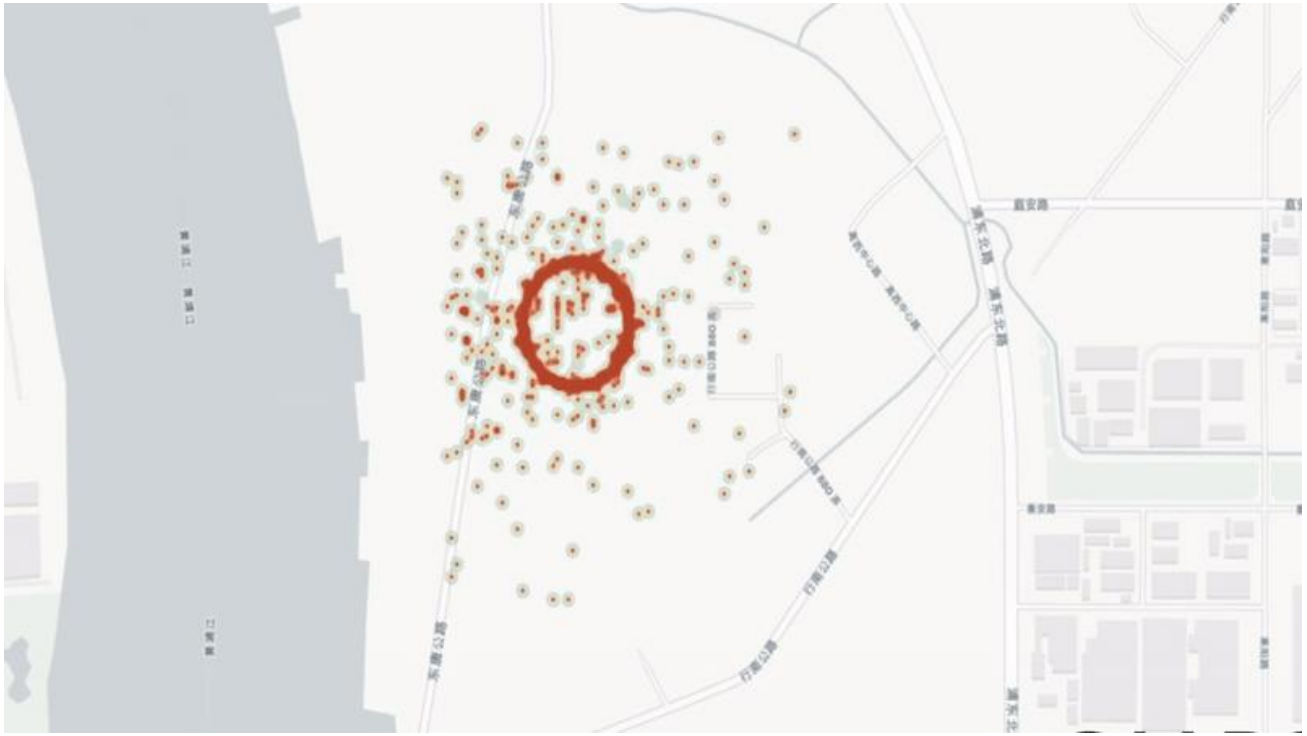
British oil tanker seized by Iran after wandering in Iranian waters

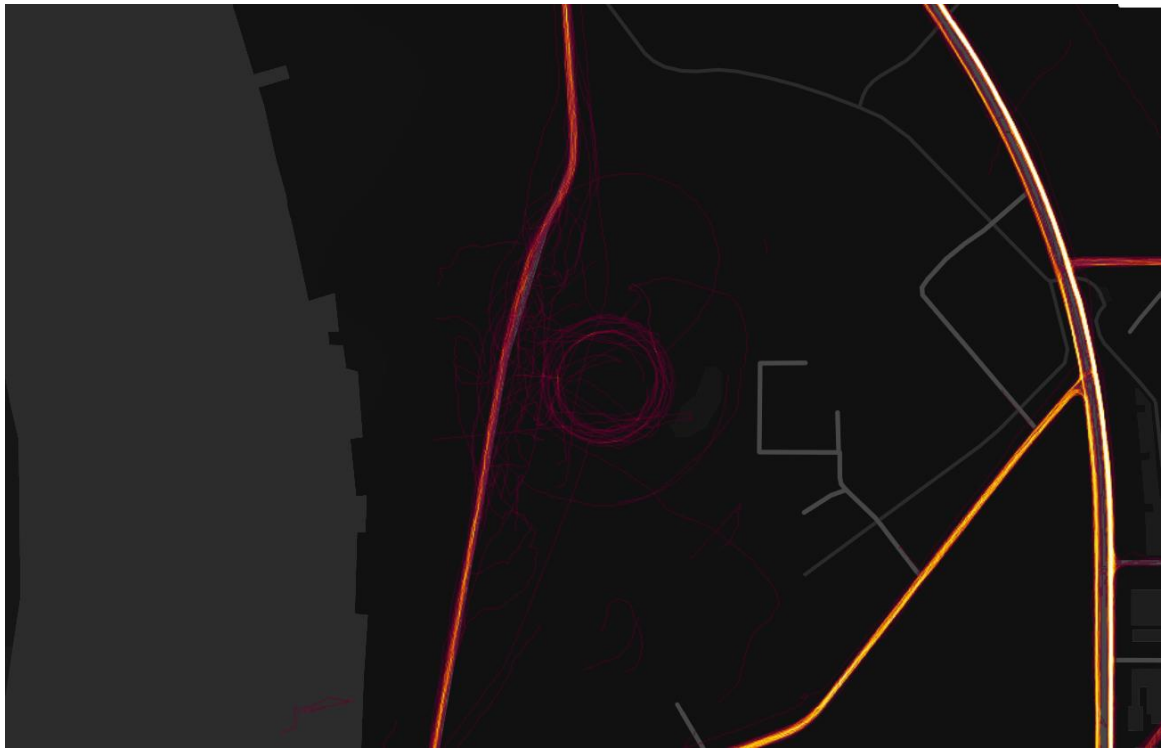
Shanghai incident

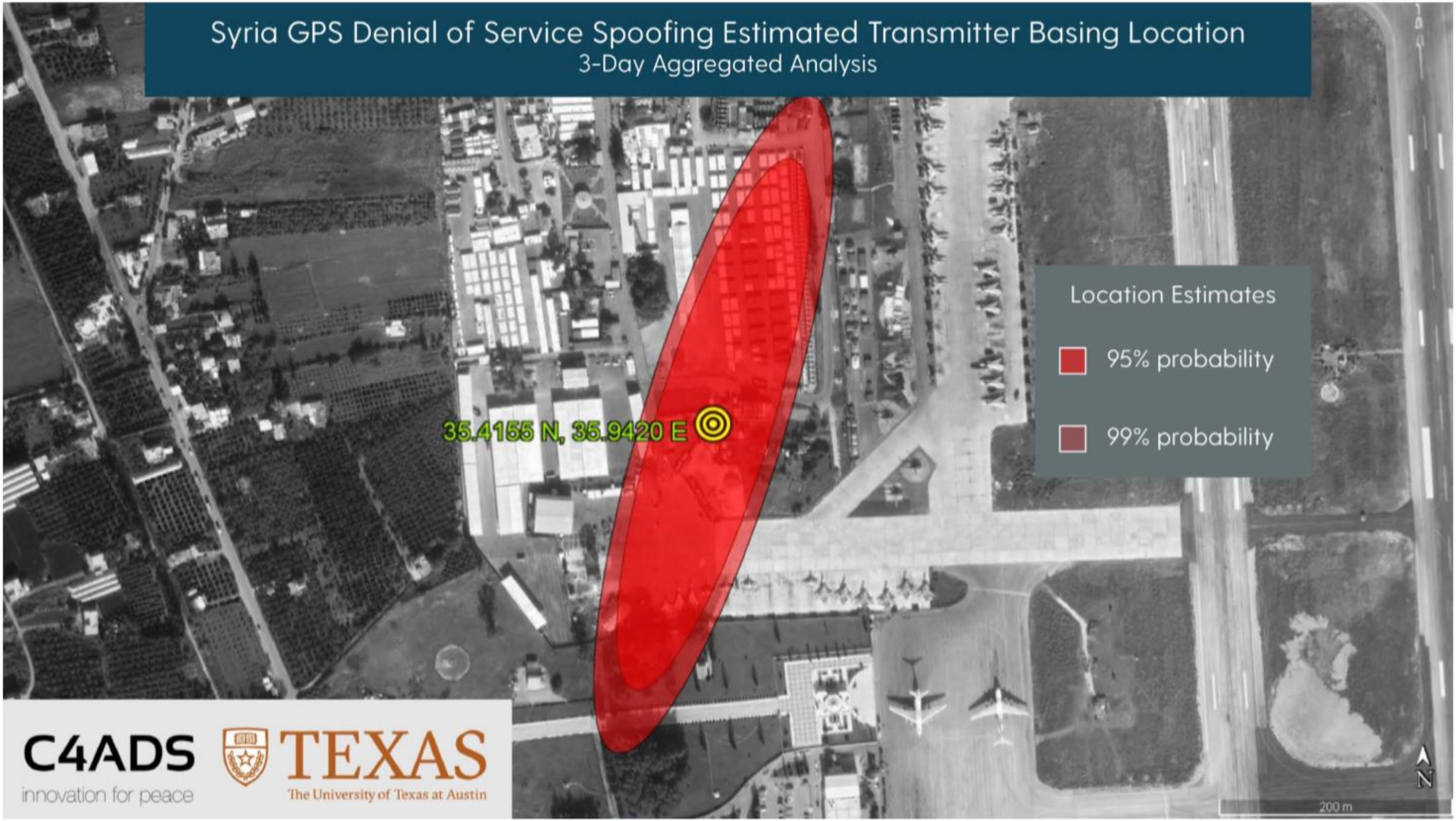


1995 2000 2005 2010 2015 2020 2025

Shanghai GPS spoofing






Syria GPS Denial of Service Spoofing Estimated Transmitter Basing Location
3-Day Aggregated Analysis
35.4155 N, 35.9420 E
Location Estimates
95% probability
99% probability
C4ADS
innovation for peace
TEXAS
The University of Texas at Austin
N
200 m

Jamming meets spoofing

CONVENTIONELE JAMMER

- 2 Watt
- 2 MHz bandbreedte
- Ontvanger
  - $\left(\frac{C}{N_0}\right)_{\min track} = 25\ \mathrm{dB\ Hz}$

Bereik ~15 km (~700 km² !!!)

GECODEERDE JAMMER

- Jammer genereerd GNSS signalen zonder data
- Bereik 15 km => 1mW
- Alleen effectief in acquisitie fase

GNSS Spoofing: from fiction to reality

James Bond: Tomorrow Never Dies: Villans spoof HMS Devonshire into Chinese waters

GPS Risk Assessment Study, John Hopkins University: There is no credible spoofing threat

Portable spoofer by T.D. Humpreys et al. Article in GPS World

Demonstration of spoofing on a helicopter drone (2012) and a 80M$ super yacht (2013) by T.D. Humpreys

Iran hijacks US RQ-170 (GPS Spoofing??)

DEFCON 23 & 24 DIY GPS spoofing & Drone attack

Reports of spoofing in Moscow

US patrol boat strayed into Iranian waters (GPS spoofing??)

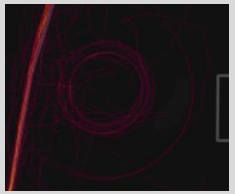
C4ADS report: Above us only stars

Black Sea incident

US UAV shot down in Iranian airspace according to Iran. (GPS spoofing??)

British oil tanker seized by Iran after wandering in Iranian waters

Shanghai incident



?

1995 2000 2005 2010 2015 2020 2025

www.rntfnd.org

b.lubbers.02@mindef.nl