


Cyber-SHIP Lab
SECURING MARITIME



Gary Kessler Associates
Training • Consulting • Research

Geopolitical Implications of the Weaponization of GPS and AIS in the Maritime Domain

Gary C. Kessler, Ph.D., CISSP

Gary Kessler Associates
Ormond Beach, Florida, USA
26 October 2022

0


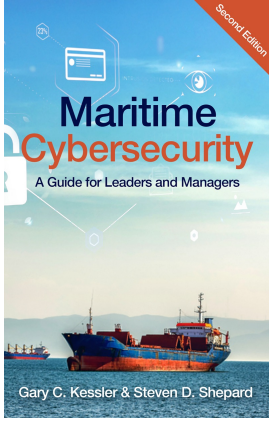
About Me...

Gary C. Kessler, Ph.D., CISSP
Gary Kessler Associates

Principal Consultant, Fathom5
Non-Resident Senior Fellow, Atlantic Council
Chief, Cyber Augmentation Branch, USCG Auxiliary
Visiting Faculty, USCG Academy
Board of Advisors, Cydome

50GT Master/Assistance Towing
Master SCUBA Diver Trainer

mobile: +1 802-238-8913
e-mail: gck@garykessler.net
<https://www.garykessler.net>

(c) Gary C. Kessler, 2022

1

1

Overview

- Evolution of GPS spoofing
- AIS, information leakage, and the evolution of AIS spoofing
- Why spoof AIS and GPS?
- Are we prepared?



(c) Gary C. Kessler, 2022

2

2

Global Positioning System (GPS)

- Most widely used satellite-based positioning, navigation, and timing (PNT) system
- GPS constellation has 37 satellites, 29 set healthy, and requires 24 for operation
 - On average, provides 1.6' (0.5 m) accuracy
- GPS is the timing source for most of our critical infrastructures
 - Power grid, telecommunications and data networks, financial networks, transportation systems, and more

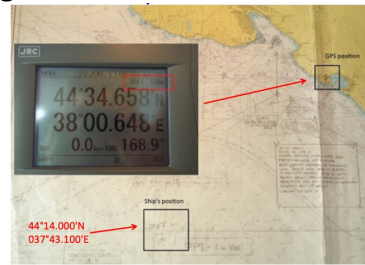
(c) Gary C. Kessler, 2022

3

3

Evolution of GPS Spoofing

- GPS signals jammed in 1991, even before full system deployment
- Demonstration of capability: Disorient a single vessel (2013)
- M/V ATRIA and mass GPS spoofing in the Black Sea (2017)
- C4ADS (2019) and CSIS (2020) report widescale episodes of GPS spoofing
 - Largely caused by China, North Korea, and Russia



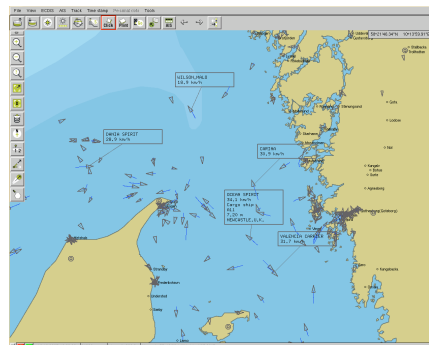
(c) Gary C. Kessler, 2022

4

4

Automatic Identification System

- AIS is a tracking system used by ships and VTMS
 - Designed to provides ships and maritime administrations with situational awareness about area vessel traffic
 - Vessel's data — e.g., identifier, position, COG, SOG, destination — meant to be ephemeral
- Defined in 2002 SOLAS; required on:
 - All vessels ≥ 300 gross tons travelling internationally
 - Commercial power vessels ≥ 65 ft (20 m)
 - Commercial towing vessels ≥ 26 ft (8 m) or >600 horsepower
 - Power vessels certified to carry >150 passengers
 - Warship exemption



(c) Gary C. Kessler, 2022

5

5

AIS Information Leakage

"[The Committee] agreed that the publication on the world-wide web or elsewhere of AIS data transmitted by ships could be detrimental to the safety and security of ships and port facilities and was undermining the efforts of the Organization and its Member States to enhance the safety of navigation and security in the international maritime transport sector.

The Committee condemned the regrettable publication on the [web] of AIS data transmitted by ships and urged Member Governments, subject to the provisions of their national laws, to discourage those who make available AIS data to others for publication on the [web] from doing so.

In addition, the Committee condemned those who irresponsibly publish AIS data transmitted by ships on the [web], particularly if they offer services to the shipping and port industries."

IMO Maritime Safety Committee, December 2004

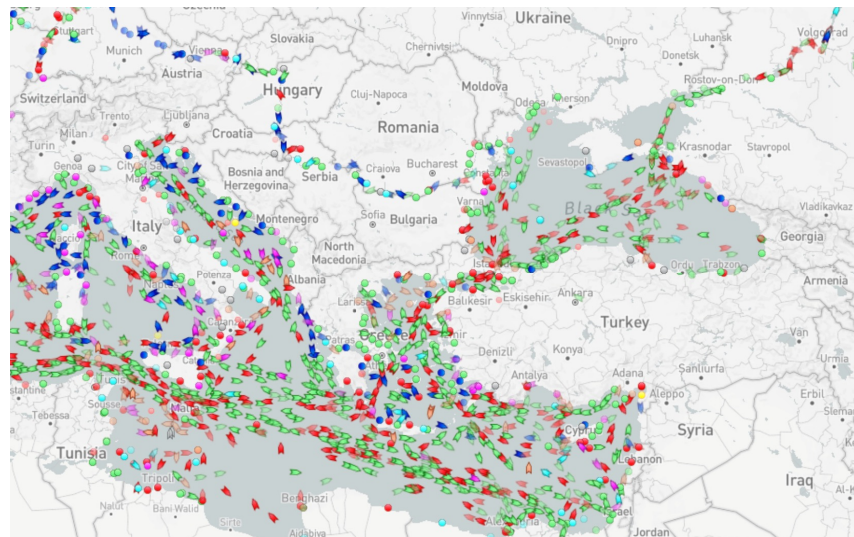
<http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx>

(c) Gary C. Kessler, 2022

6

6

Data Aggregation Sites

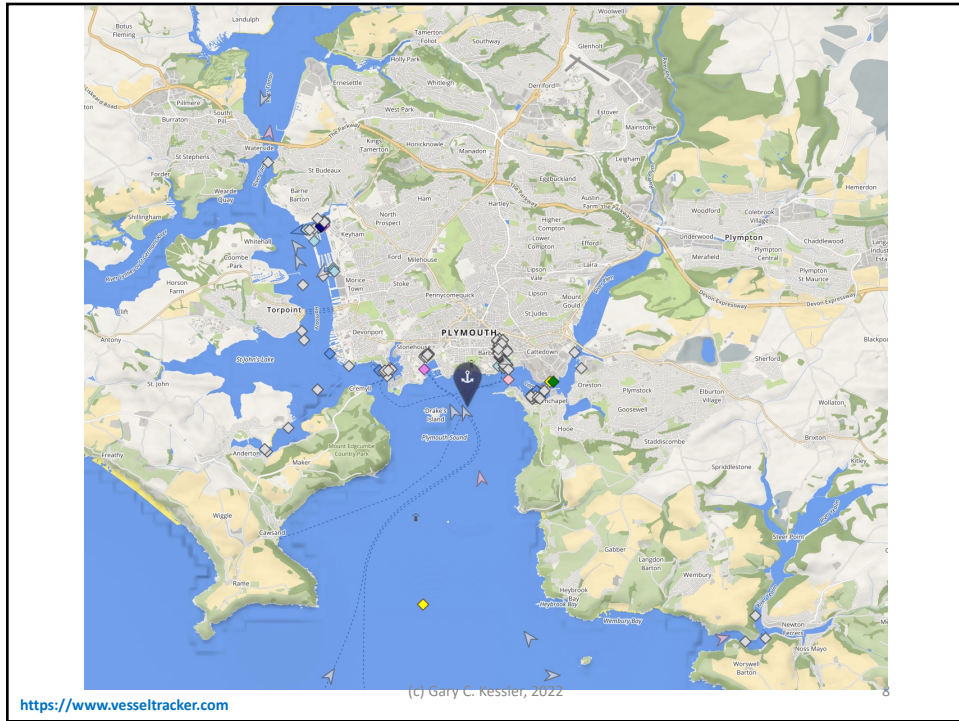


<https://www.marinetraffic.com>

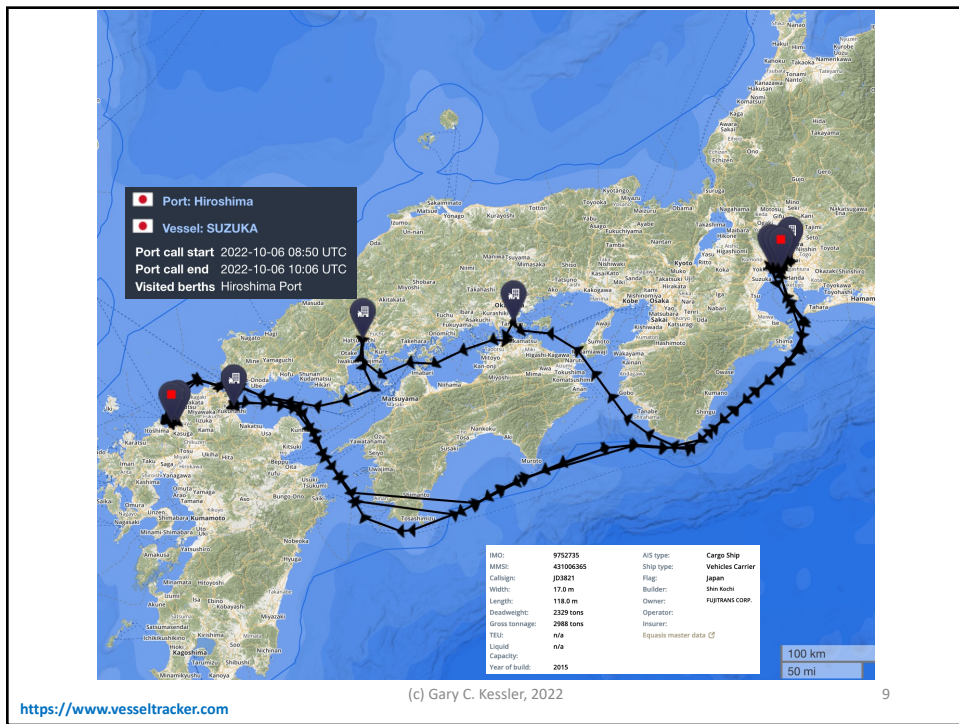
(c) Gary C. Kessler, 2022

7

7



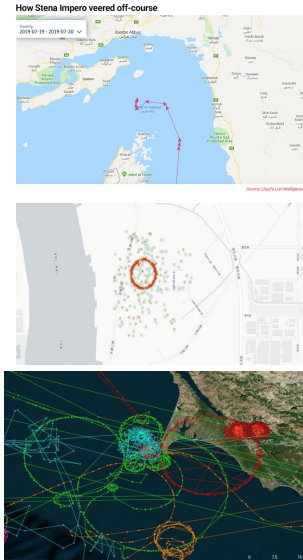
8



9

Evolution of AIS Spoofing

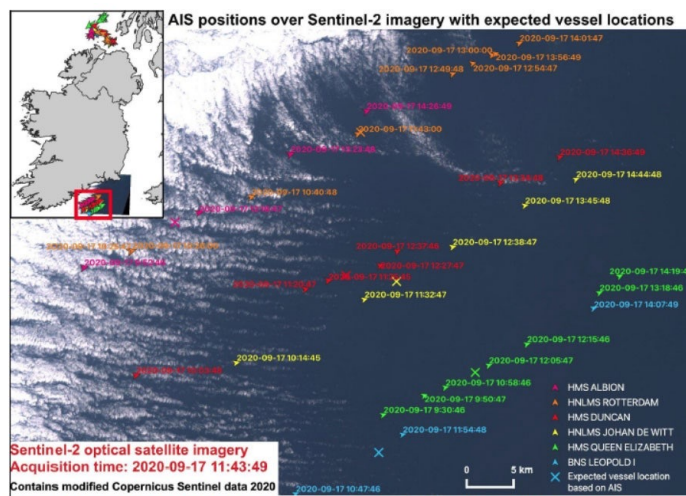
- TrendMicro reports AIS security vulnerabilities (2013)
 - Lack of timestamp, authentication, integrity checks, and validity checks
- STENA IMPERO seized by Iran (2019)
- Circle spoofing in Port of Shanghai (2019)
- Circle spoofing off Pt. Reyes (2019)



(c) Gary C. Kessler, 2022

10

Warship Position Spoofing (2020)

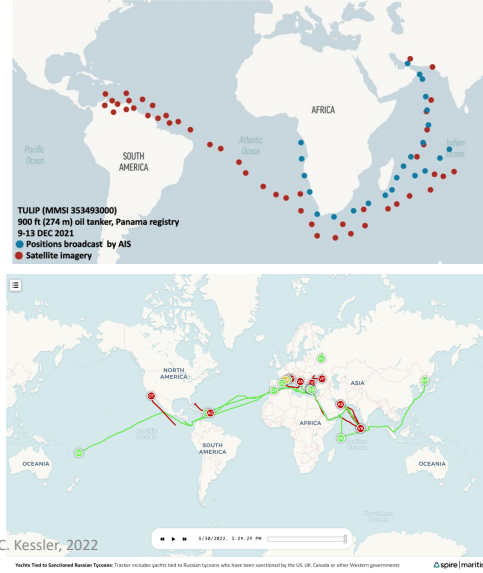


11

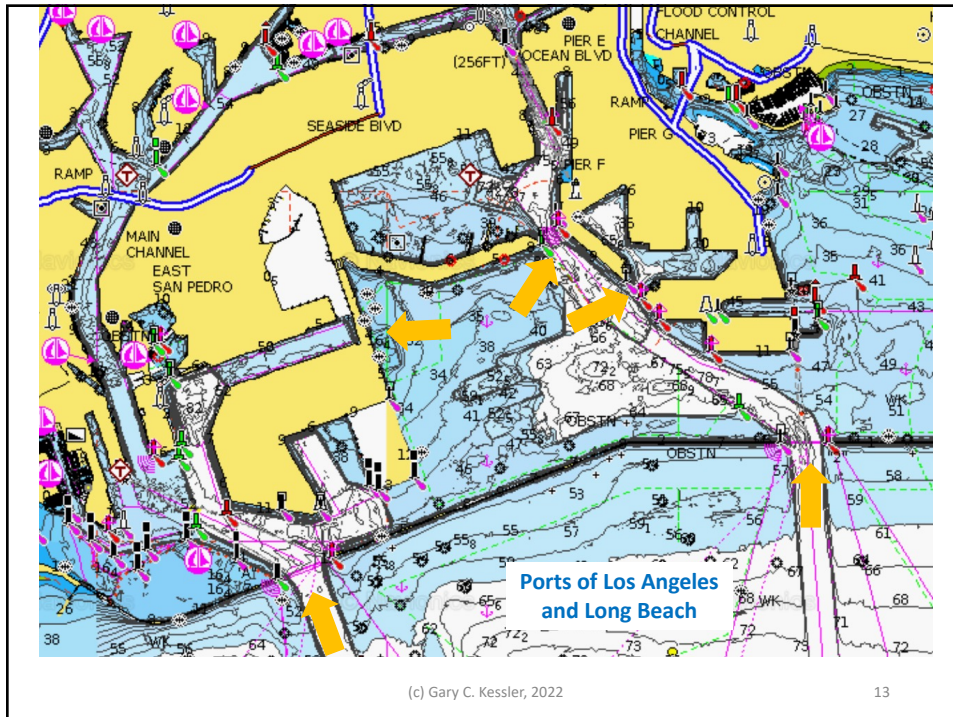
11

Why Spoof AIS and GPS?

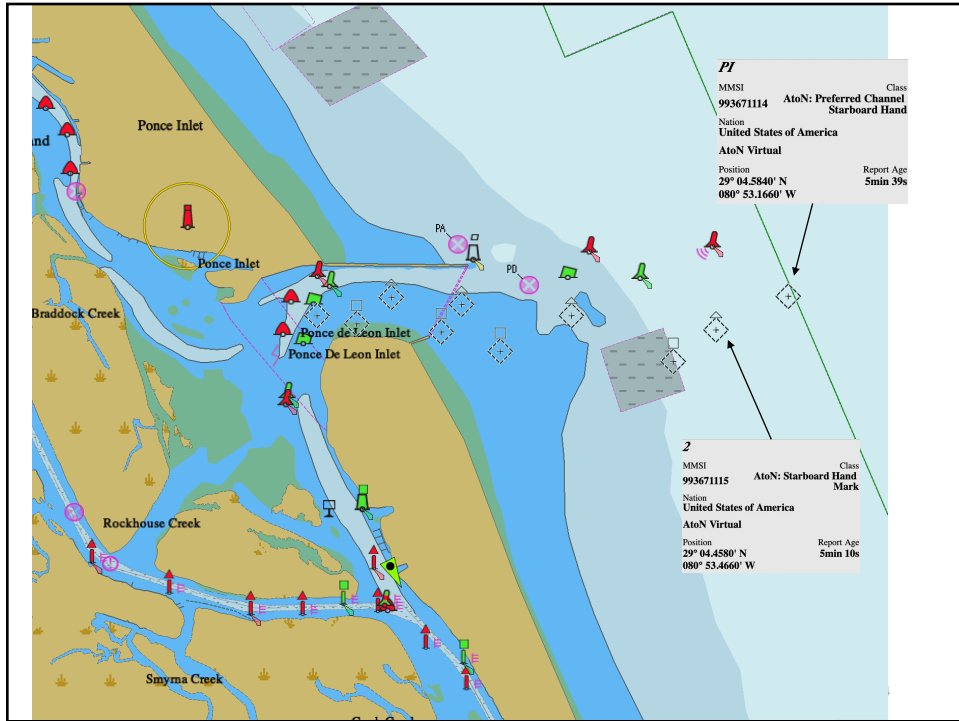
- IUU fishing
 - Impacts economy, food supply, environment
- Sanction avoidance
 - Criminal and civil
- Identity laundering
 - Masks criminal and smuggling operations
- "Dark operations"
- Physical attack



12



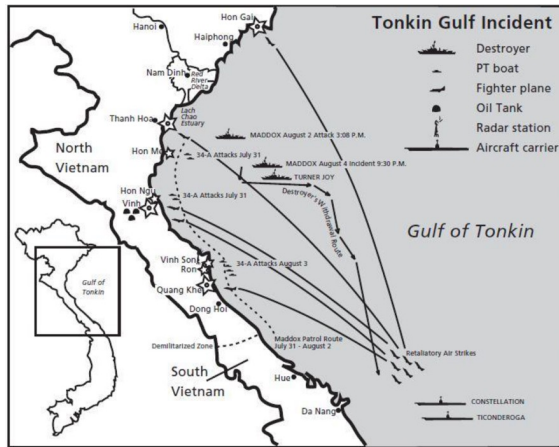
13



14

Why Spoof AIS and GPS? (2)

- Military offense and defense
- Manufactured pretext...
- *Case Study: Gulf of Tonkin (1964)*



(c) Gary C. Kessler, 2022

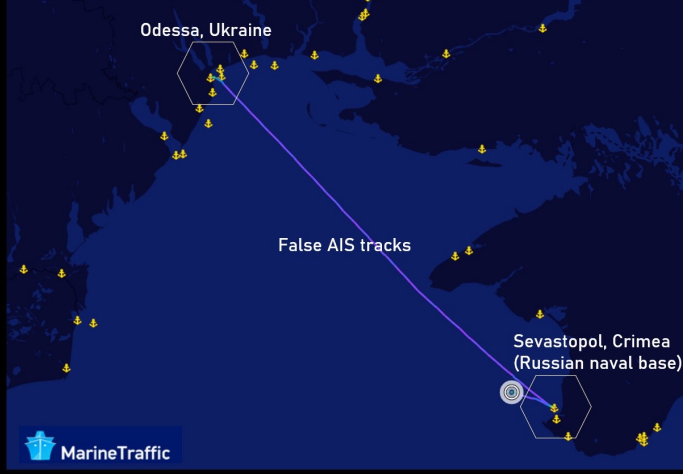
15

15

Black Sea AIS Spoofing (2021)

Falsified AIS (Automated Identification System) appearing to show HMS Defender and HNLMS Evertsen approaching Sevastopol, Crimea, On June 19 2021

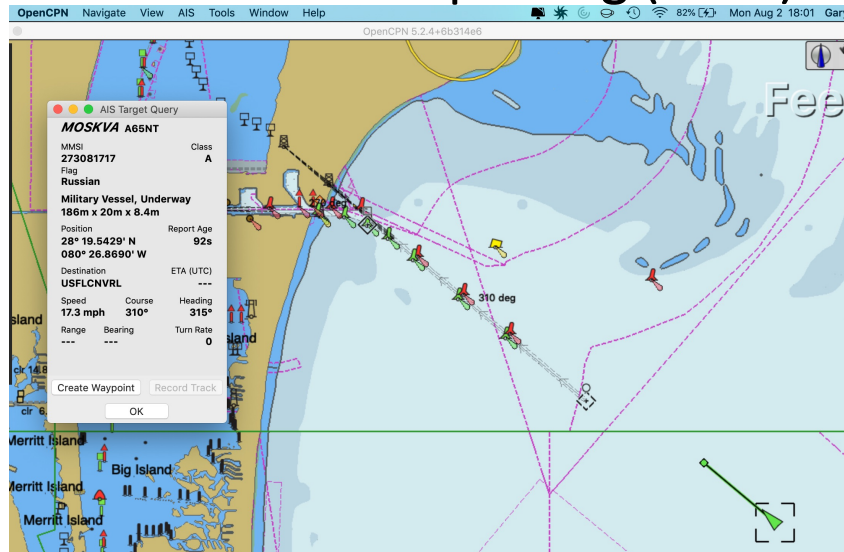
Webcams showing HMS Defender (A) and HNLMS Evertsen (B) in Odessa



(c) Gary C. Kessler, 2022

16

Port Canaveral Spoofing (2021)

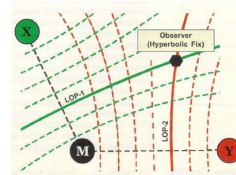


(c) Gary C. Kessler, 2022

17

And Yet...

- GPS is most widely used PNT around the world
 - Resilient against nature but not to a direct attack
 - No backup and no augmentation, particularly for timing services
 - How many of us can use a sextant or LORAN?
- AIS is reliable if used as designed
 - Not meant for permanence of information
 - Not intended to be used by authorities for long-term surveillance, enforcement, and historical purposes
 - Users can easily misuse AIS
 - There are no efforts to secure the underlying protocols



(c) Gary C. Kessler, 2022

18

18

Acronyms and Abbreviations

AIS	Automatic Identification System
C4ADS	Center for Advanced Defense Studies
COG	Course over ground
CSIS	Center for Strategic and International Studies
GPS	Global Positioning System
IMO	International Maritime Organization
IUU	Illegal, unreported and unregulated
LORAN	Long range navigation
PNT	Positioning, navigation, and timing
SOG	Speed over ground
SOLAS	Safety of Life at Sea
VTMS	Vessel traffic management system

(c) Gary C. Kessler, 2022

19

19