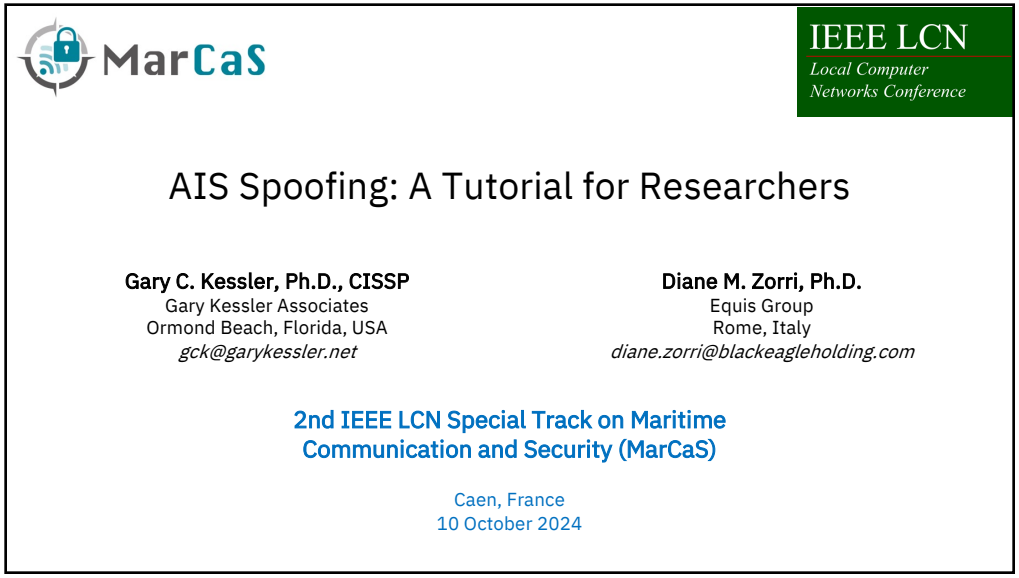
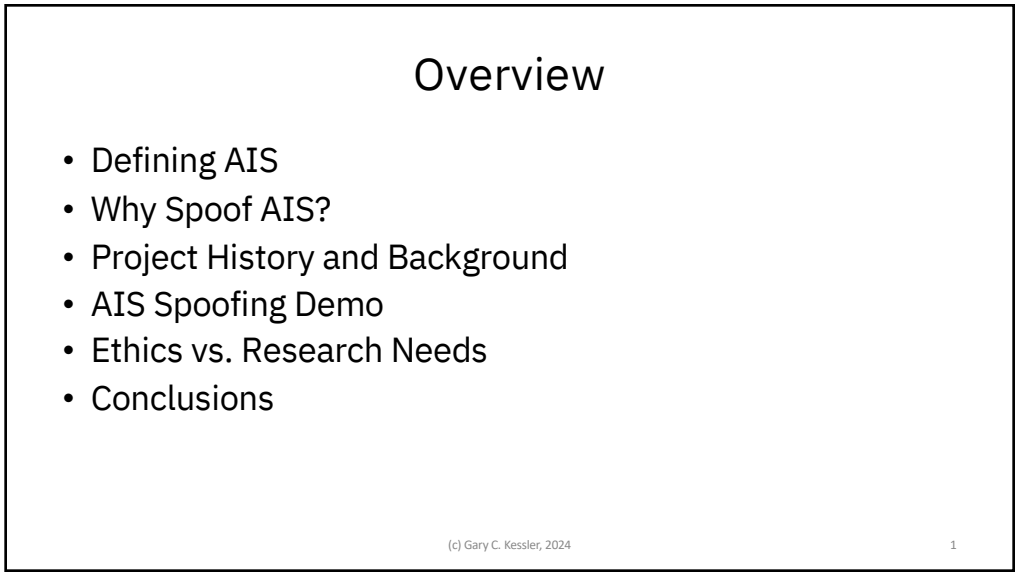
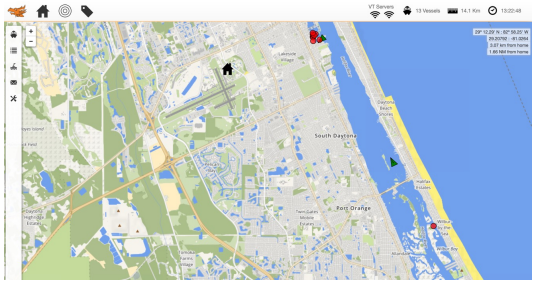

MarCaS
IEEE LCN
Local Computer
Networks Conference
AIS Spoofing: A Tutorial for Researchers
Gary C. Kessler, Ph.D., CISSP
Gary Kessler Associates
Ormond Beach, Florida, USA
gck@garykessler.net
Diane M. Zorri, Ph.D.
Equis Group
Rome, Italy
diane.zorri@blackeagleholding.com
2nd IEEE LCN Special Track on Maritime
Communication and Security (MarCaS)
Caen, France
10 October 2024

0


Overview
• Defining AIS
• Why Spoof AIS?
• Project History and Background
• AIS Spoofing Demo
• Ethics vs. Research Needs
• Conclusions
(c) Gary C. Kessler, 2024
1

1

# Defining AIS

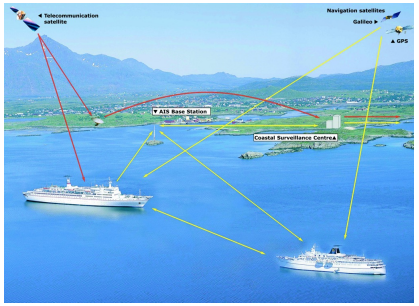


2

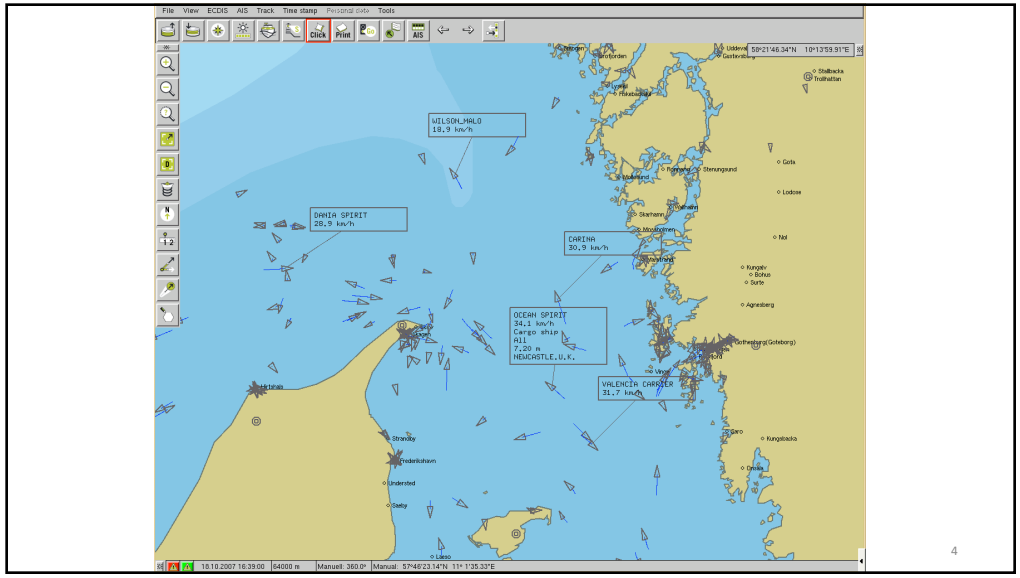
# Automatic Identification System

- AIS is a tracking system used by ships and VTMS
  - Provides a ship and maritime administration with situational awareness about area vessel traffic
- AIS provides sender's name, identifier, position, course, heading, speed, ROT, cargo, destination, and more
- Data can be displayed on a screen, ECDIS, or mobile app
- AIS design initiated by USCG after 1989 oil spill when EXXON VALDEZ ran aground



3




4

## *Side Note:* AIS Requirements

- Defined in 2002 SOLAS, Chapter V, Regulation 19 and 33 CFR 164.46
- In general, AIS is 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

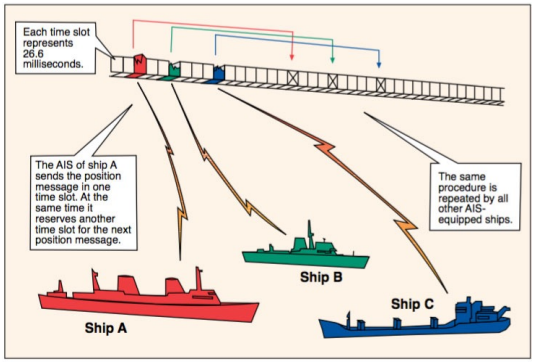


5

5

# AIS Communication Protocol

- Over-the-air AIS defined in ITU-R Rec. M.1371
  - Transmits on VHF channels 87B (161.975 MHz, AIS1) and 88B (162.025 MHz, AIS2), using various time division multiple access schemes, for terrestrial AIS (T-AIS)
  - Employs NMEA 0183 sentence format at 9,600 bps
  - Transmits Type 27 messages on VHF channels 75 (156.775 MHz, AIS3) and 76 (156.825 MHz, AIS4) for satellite AIS (S-AIS)



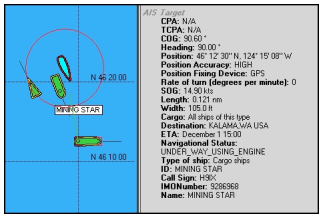

Self-Organized Time Division Multiple Access (SOTDMA)



6

# AIS Security Weaknesses

- TrendMicro (11/2013, 02/2017) reported a number of vulnerabilities in the AIS protocol
  - Lack of message integrity
  - Lack of timing integrity
  - Lack of authentication
  - Lack of validity






7

# Why Spoof AIS?




8

# AIS Spoofing Scenarios

- Closest point of approach (CPA) spoofing
- AIS Search and Rescue Transmitter (AIS-SART) spoofing
- Fake weather forecasts
- Denial-of-service (DoS)
  - Overwhelm VTMS *or* shrink AIS cell
- Frequency-hopping attack
- Ghost vessel or ATON spoofing
- Data diddling
  - Avoid sanctions; mask IUU fishing, human trafficking, or other illegal activity; hide source of environmental impact; identity laundering



9

# Why Spoof AIS (and GNSS, for that matter)?

- IUU fishing*
  - Impacts economy, food supply, environment
- Sanction avoidance
  - Criminal and civil
- Identity laundering
  - Masks criminal and smuggling operations
- "Dark operations"
- Physical attack
- Criminal activity
- Military offense and defense
  - Misinformation and disinformation about fleet location, size, and movement
- Manufactured pretext
  - Plant a false flag as a pretext to some political or military action

*"Hot Spots of Unseen Fishing Vessels"

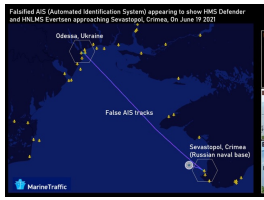


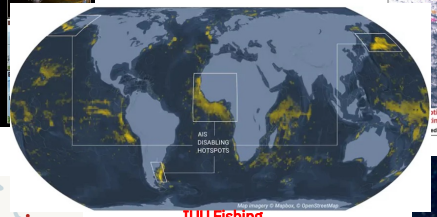


10

# Not Just Theory Anymore...

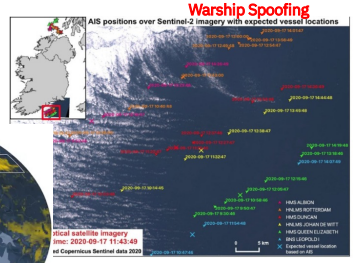
Pretext Setting?




IUU Fishing

Warship Spoofing



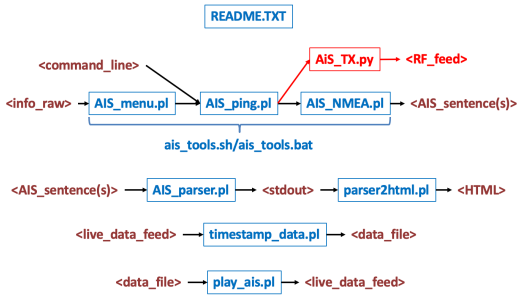

Sanction Avoidance


Illegal STS Transfer of Oil



11

# Project History and Background




 12

12

# AIS Tool Development

- Study vulnerabilities in AIS protocols
- Develop proof of concept to provide timestamp, authentication, and message integrity to AIS messages, including backward compatibility (protected AIS)
  - Required development of message generation and parsing software
- Developed tool with which to easily spoof the route of any vessel in any location
- Supporting research monitoring ghost and dark fleets

 13

13

# AIS Messages Necessary for Spoofing

- Type 1: Position Report Class A Message
  - Contains MMSI, nav. status, ROT, speed, latitude/longitude, course, heading
  - Transmission rate*: every 2-180 sec
- Type 5: Static and Voyage Related Data Message
  - Contains MMSI, IMO number, call sign, vessel name, ship type, length, beam, draft, destination and ETA
  - Transmission rate*: every 360 sec
- Type 18: Standard Class B CS Position Report
  - Contains MMSI, speed, latitude/longitude, course, heading
  - Transmission rate*: every 5-180 sec
- Type 27: Long Range AIS Broadcast Message
  - Contains MMSI, nav. status, speed, latitude/longitude, course
  - Transmission rate*: every 180 sec

* Rate depends upon navigation status, SOG, and ROT





14

# Some Useful Mariner Algebra

- Distance
  - 1° latitude = 1° longitude at the Equator* = 60 nm [1° = 60']
  - 1' latitude = 1' longitude at the Equator* = 1 nm [1' = 60"]
  - 1 nm = 1.151 statute miles = 1.852 km
- Speed
  - 1 knot (nm/hour, kn) = 1.67 ft/s = 0.51 m/s
- Distance, speed, time calculations
  - 60 x D = S x T
    - where D = distance (nm/mi/km)
    - S = speed (kn/mph/km/h)
    - T = time (min)

* The linear length of a degree of longitude depends upon the cosine of the latitude.





15

# Great Circle Navigation I

Because maps and charts generally use a Mercator Projection, the shortest distance between two points isn't always what appears to be a straight line on paper, particularly as distances get larger.

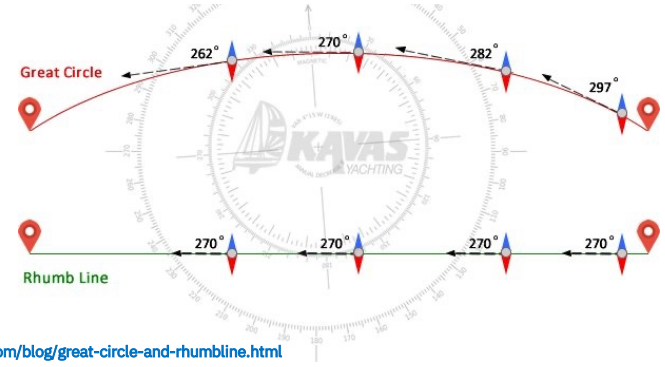

https://www.kavas.com/blog/great-circle-and-rhumbline.html




16

# Great Circle Navigation II

When you travel on the shortest route (i.e., along a great circle) from one point to the next, your course will be changing all of the time.




https://www.kavas.com/blog/great-circle-and-rhumbline.html




17

# AIS Spoofing Demo




18

# DEMO: USS LAKE CHAMPLAIN in the Port of Rotterdam

- U.S. Navy guided missile cruiser (CG-57)
  - Max. speed: 32.5 kn (37.4 mph, 60 km/h)
  - Length: 567 ft (173 m)
  - Beam: 55 ft (16.8 m)
  - Draft: 34 ft (10.2 m)
- Port of Rotterdam
  - Largest seaport in Europe, 10th largest in the world
  - 41 $mi^2$ (106 $km^2$) in area

https://en.wikipedia.org/wiki/USS_Lake_Champlain_(CV-39)




19

# apate

- *apate* simplifies the creation of a complete set of real-time AIS messages in order to prepare a spoofed vessel track*
- In Greek mythology, Apate (/ˈæpəti:/; Ancient Greek: Απάτη Apátē; "AH-puh-Tee") was the personification of deceit, and the goddess of fraud and guile

* A companion program can create a spoofed virtual channel.

20

```
Bishop:ais-prototype gck$ ./apate.pl

         Apate -- An AIS Spoofing Tool (Build: 08/07/2023 Version: 1.4.5)
                  [[Apate is the goddess of fraud and deception]]

Enter base name of file set (e.g., 'odyssey' or 'data/odyssey'): KML/USS_LAKE_CHAMPLAIN

Read from existing parameter file (R) or write a new parameter file (W)? w

Writing parameters to KML/USS_LAKE_CHAMPLAIN_parameters.txt...

--- Get vessel information for AIS Type 5 message ---

Enter MMSI (9 decimal digits): 338951000

Enter vessel name (1-20 characters); Encoder default = NaN:
USS LAKE CHAMPLAIN

Enter vessel call sign (0-7 characters):
NCPN

Enter vessel type (0-99) from the following list, or null:
  0. Not available, AIS default    1-19. Reserved
 20-29. Wing in ground (WIG)
 30. Fishing                      31. Towing
 32. Towing: length exceeds 200m or breadth exceeds 25m
 33. Dredging or underwater ops    34. Diving ops
 35. Military ops                  36. Sailing
 37. Pleasure Craft                38-39. reserved
 40-49. High speed craft (HSC)     50. Pilot Vessel
 51. Search and Rescue vessel      52. Tug
 53. Port Tender                   54. Anti-pollution equipment
 55. Law Enforcement               56-57. spare
 58. Medical Transport             59. Noncombatant ship
 60-69. Passenger ship             70-79. Cargo
 80-89. Tanker                     90-99. Other ship type
 >>> 35
```

21

```
===== Summary information for vessel: 'USS LAKE CHAMPLAIN' (Apate V3.1.3) =====

MMSI: 338951000   =====   IMO number: --   =====   Call sign:'NCPN'
Vessel type: 35 (Engaged in military operations)
Length: 159.0 m (521.7 ft)   =====   Beam: 18.0 m (59.1 ft)   =====   Draft: 10.2 m (33.5 ft)

Start route at:
   51.991808∞N ( 51∞59.508'N)
  004.042953∞E (004∞02.577'E)

Information for leg 1...
   This leg ends at:
      51.976642∞N ( 51∞58.599'N)
     004.118607∞E (004∞07.116'E)
   Approx. course: 108∞     Speed:  6 kn     Distance: 2.94 nm
   AIS Type 1 messages sent every 10 sec     Duration of leg: 1,707 sec (28.45 min)
   170 segments on this leg, each approx. 0.0173 nm (32.0 m)
            ::
            ::
Information for leg 9...
   Vessel has arrived at:
      51.910650∞N ( 51∞54.639'N)
     004.250620∞E (004∞15.037'E)

Course summary: Total distance: 9.28 nm    Total time: 89.8 min [1 hour(s) 29.8 min]
                Total number of AIS Type 1 messages: 534
                Total number of AIS Type 5 messages: 15
                Total number of AIVDM sentences: 564
```

22

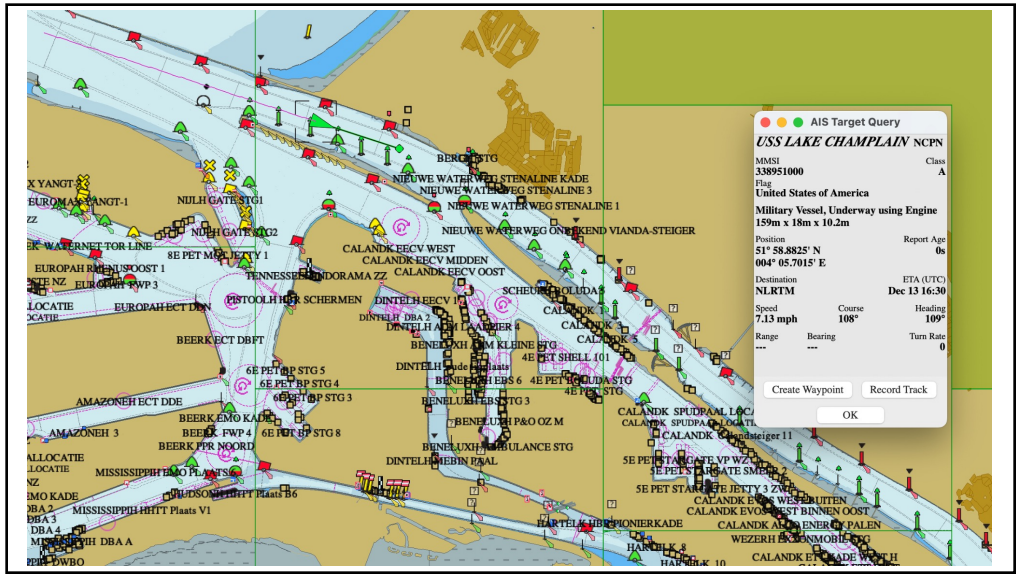
Type 5 message, sent ever 360 sec.

Type 1 messages, sent every 10 sec. (6 kn, ROT = 0)

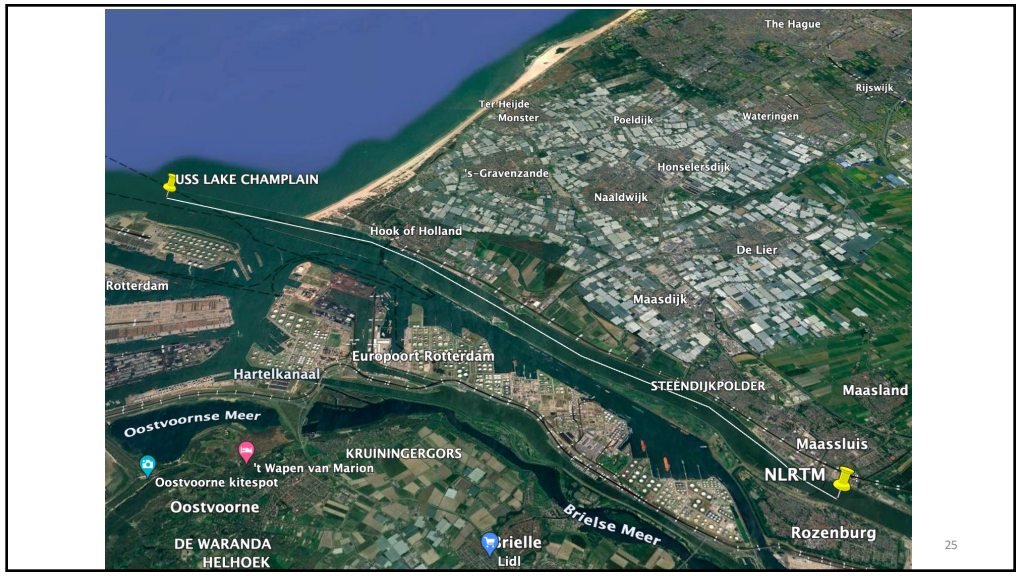
```
Bishop:ais-prototype gck$ perl play_ais.pl -f=KML/USS_LAKE_CHAMPLAIN_replay.txt -s=- -ais=1 -time=0
-v -pro=tcp -port=8888 -ip=127.0.0.1

AIS Play (Version 2.3.2, Build date: 05/24/2022)
Connection success to 127.0.0.1:8888/tcp.
Reading file KML/USS_LAKE_CHAMPLAIN_replay.txt, using '\-' as a field separator.
Timestamps are in field 0 and AIS data in field 1.

Record 1 -- Timestamp = 0; waited 0 second(s) to send...
 !AIVDM,2,1,2,A,553?sF800000p=0p001E=>0h4dF0<P4m0h4Tp00S6ab993GhNISS4U3@0000,0*41
Record 2 -- Timestamp = 0; waited 0 second(s) to send...
 !AIVDM,2,2,2,A,00000000008,2*2E
Record 3 -- Timestamp = 0; waited 0 second(s) to send...
 !AIVDM,1,1,,A,153?sF000v0BPMFMgwk4>3J00000,0*01
Record 4 -- Timestamp = 10; waited 10 second(s) to send...
 !AIVDM,1,1,,A,153?sF000v0BPUdMgwUl>3FD0000,0*25
Record 5 -- Timestamp = 20; waited 10 second(s) to send...
 !AIVDM,1,1,,A,153?sF000v0BPf4MgwHD>3H`0000,0*59
Record 6 -- Timestamp = 30; waited 10 second(s) to send...
 !AIVDM,1,1,,A,153?sF000v0BPnJMgw;4>3Ht0000,0*38
Record 7 -- Timestamp = 40; waited 10 second(s) to send...
 !AIVDM,1,1,,A,153?sF000v0BPvhMgvul>3E@0000,0*2C
Record 8 -- Timestamp = 50; waited 10 second(s) to send...
 !AIVDM,1,1,,A,153?sF000v0BQ76MgvhD>3ET0000,0*13
Record 9 -- Timestamp = 60; waited 10 second(s) to send...
 !AIVDM,1,1,,A,153?sF000v0BQ?lMgvS4>3J00000,0*41
Record 10 -- Timestamp = 70; waited 10 second(s) to send...
 !AIVDM,1,1,,A,153?sF000v0BQGjMgvET>3FD0000,0*11
Record 11 -- Timestamp = 80; waited 10 second(s) to send...
 !AIVDM,1,1,,A,153?sF000v0BQP8Mgv8D>3F`0000,0*1D
Record 12 -- Timestamp = 90; waited 10 second(s) to send...
 !AIVDM,1,1,,A,153?sF000v0BQ`NMgurl>3Jt0000,0*22
Record 13 -- Timestamp = 100; waited 10 second(s) to send...
 !AIVDM,1,1,,A,153?sF000v0BQhlMgueT>3E@0000,0*1C
Record 14 -- Timestamp = 110; waited 10 second(s) to send...
 !AIVDM,1,1,,A,153?sF000v0BQq:MguP4>3MT0000,0*1A
Record 15 -- Timestamp = 120; waited 10 second(s) to send...
 !AIVDM,1,1,,A,153?sF000v0BR1PMguBl>3H00000,0*18
Record 16 -- Timestamp = 130; waited 10 second(s) to send...
```

23


AIS Target Query
USS LAKE CHAMPLAIN NCPN
MMSI
338951000
Class
A
Flag
United States of America
Military Vessel, Underway using Engine
159m x 18m x 10.2m
Position
51° 58.8825' N
004° 05.7015' E
Report Age
0s
Destination
NLRTM
ETA (UTC)
Dec 13 16:30
Speed
7.13 mph
Course
108°
Heading
109°
Range
---
Bearing
---
Turn Rate
0
Create Waypoint
Record Track
OK

24


The Hague
Rijswijk
Ter Heijde
Monster
Poeldijk
Wateringen
Honselersdijk
's-Gravenzande
USS LAKE CHAMPLAIN
Naaldwijk
Hook of Holland
De Lier
Rotterdam
Maasdijk
Europoort-Rotterdam
Hartelkanaal
STEENDIJKPOLDER
Maasland
Oostvoornse Meer
Maassluis
KRUININGERGORS
't Wapen van Marion
Oostvoorne kitespot
NLRTM
Oostvoorne
Brielse Meer
Rozenburg
DE WARANDA
HELHOEK
Lidl
25

25

# Ethics vs. Research Needs



26

# USS LAKE CHAMPLAIN Route

| TIME | MMSI | LATITUDE | LONGITUDE | COURSE | HEADING | SPEED |
|---|---|---|---|---|---|---|
| 0 | 338951000 | 51.991808 | 004.042953 | 108.000000000005 | 105 | 6.48109841331924 |
| 10 | 338951000 | 51.9917189295626 | 004.04339817538945 | 108.000350763597 | 111 | 5.48412927506457 |
| 20 | 338951000 | 51.991629857447 | 004.04384334900782 | 108.000701525365 | 111 | 4.9732326791633 |
| 30 | 338951000 | 51.9915407836531 | 004.0442885208551 | 108.001052285317 | 107 | 6.85981723393238 |
| 40 | 338951000 | 51.9914517081812 | 004.04473369093127 | 108.001403043431 | 112 | 6.65881905341224 |
| 50 | 338951000 | 51.991362631031 | 004.0451788592363 | 108.001753799728 | 112 | 6.81652204863216 |
| 60 | 338951000 | 51.9912735522027 | 004.04562402577019 | 108.002104554208 | 112 | 5.60363122015949 |
| 70 | 338951000 | 51.9911844716962 | 004.04606919053289 | 108.002455306849 | 105 | 6.88778968462048 |
| 80 | 338951000 | 51.9910953895117 | 004.0465143535244 | 108.002806057683 | 112 | 5.78415454794434 |
| 90 | 338951000 | 51.991006305649 | 004.0469595147447 | 108.003156806696 | 110 | 6.28611960867065 |
| 100 | 338951000 | 51.9909172201082 | 004.04740467419376 | 108.003507553868 | 111 | 4.98597299248656 |
| 110 | 338951000 | 51.9908281328893 | 004.04784983187156 | 108.00385829923 | 109 | 5.34859182668098 |
| 120 | 338951000 | 51.9907390439924 | 004.04829498777808 | 108.004209042773 | 107 | 5.71560610580343 |
| 130 | 338951000 | 51.9906499534173 | 004.0487401419133 | 108.004559784494 | 106 | 6.89952743049913 |
| 140 | 338951000 | 51.9905608611643 | 004.04918529427721 | 108.004910524396 | 105 | 6.25914757306529 |
| 150 | 338951000 | 51.9904717672332 | 004.04963044486977 | 108.005261262478 | 105 | 4.99172056803862 |
| 160 | 338951000 | 51.990382671624 | 004.05007559369098 | 108.005611998733 | 107 | 6.36624682305762 |
| 170 | 338951000 | 51.9902935743369 | 004.0505207407408 | 108.00596273318 | 104 | 5.73946157469408 |
| 180 | 338951000 | 51.9902044753717 | 004.05096588601922 | 108.00631346578 | 106 | 5.69003549981676 |

D = 0.104 nm & T = 1 min → S = 6.25 kn



27

# Case Study: Poisoning AIS Data

D = 0.765 nm & T = 5 min → S = 9.18 kn

| Time stamp | MMSI | Latitude | Longitude | Speed | IMO | Name | Destination |
|---|---|---|---|---|---|---|---|
| 05/01/2021 06:04 | 209504011 | 26.33928 | −79.92229 | 14.75792 | 9517411 | CONTSHIP ICE | USMIA |
| 05/01/2021 06:10 | 209504011 | 26.32417 | −79.92317 | 14.65792 | 9517411 | CONTSHIP ICE | USMIA |
| 05/01/2021 06:15 | 209504011 | 26.31133 | −79.92383 | 14.85792 | 9517411 | CONTSHIP ICE | USMIA |
| 05/01/2021 06:20 | 209504011 | 26.29667 | −79.92483 | 14.65792 | 9517411 | CONTSHIP ICE | USMIA |
| 05/01/2021 06:25 | 209504011 | 26.28433 | −79.92533 | 14.75792 | 9517411 | CONTSHIP ICE | USMIA |
| 05/01/2021 06:30 | 209504011 | 26.269 | −79.926 | 14.85792 | 9517411 | CONTSHIP ICE | USMIA |
| 05/01/2021 06:35 | 209504011 | 26.256 | −79.92667 | 14.85792 | 9517411 | CONTSHIP ICE | USMIA |
| 05/01/2021 06:40 | 209504011 | 26.24117 | −79.92717 | 14.85792 | 9517411 | CONTSHIP ICE | USMIA |
| 05/01/2021 06:45 | 209504011 | 26.227 | −79.92767 | 14.65792 | 9517411 | CONTSHIP ICE | USMIA |
| 05/01/2021 06:50 | 209504011 | 26.21433 | −79.92817 | 14.55792 | 9517411 | CONTSHIP ICE | USMIA |
| 05/01/2021 06:55 | 209504011 | 26.19967 | −79.92883 | 14.75792 | 9517411 | CONTSHIP ICE | USMIA |
| 05/01/2021 07:00 | 209504011 | 26.09457 | −79.99955 | 14.65792 | 9517411 | CONTSHIP ICE | USMIA |

D = 7.37 nm & T = 5 min → S = 88.44 kn




28

# Why Distribute this Tool?

- Ethical considerations
  - Should we be distributing "hacker" tools?
- Needs of the research community
  - Better understand the higher-layer AIS protocols
  - Examine ways to better manipulate — and secure — AIS
- Some research needs
  - Securing AIS (VDES will not be enough)
  - Understand the AIS message patterns of commercial vessels




29

## The Role of Artificial Intelligence

- Researchers need to use clean, verified routes in order to build ML models so that fake routes can be detected
  - Differentiate normal anomalies from spoofing syndromes
  - Different spoofing tools will most likely leave different "signatures"
- Defensive AI methods can assist in detecting spoofed AI routes in near real-time
  - But might not be able to detect a replay attack
- Offensive AI methods can likely create detection-resistant spoofed routes

30

## This is Like Herding… Fish

31

# Acronyms and Abbreviations

| | |
|---|---|
| AI | Artificial intelligence |
| AIS | Automatic Identification System |
| ATON | Aid-to-navigation |
| CFR | Code of Federal Regulations (U.S.) |
| ECDIS | Electronic Chart Display and Information System |
| ETA | Estimated time of arrival |
| GNSS | Global Navigation Satellite System |
| IMO | International Maritime Organization |
| ITU-R | International Telecommunication Union, Radiocommunication sector |
| IUU | Illegal, unreported, and unregulated (fishing) |
| kn | Knot (nm/hour) |
| ML | Machine learning |
| MMSI | Maritime Mobile Service Identity |
| nm | Nautical mile |
| NMEA | National Maritime Electronics Association |
| ROT | Rate-of-turn |
| SOLAS | International Convention for the Safety of Life at Sea |
| USCG | United States Coast Guard |
| VDES | VHF Data Exchange System |
| VHF | Very high frequency |
| VTMS | Vessel traffic management system |