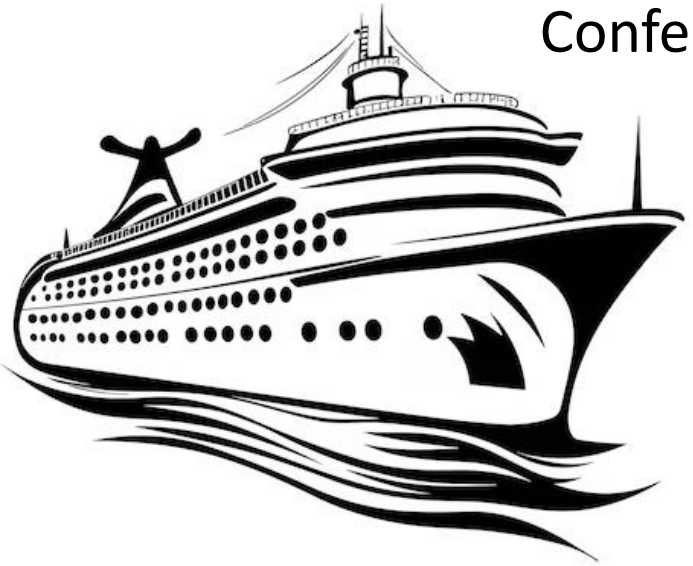
Sailing and Flying in a Vulnerable World

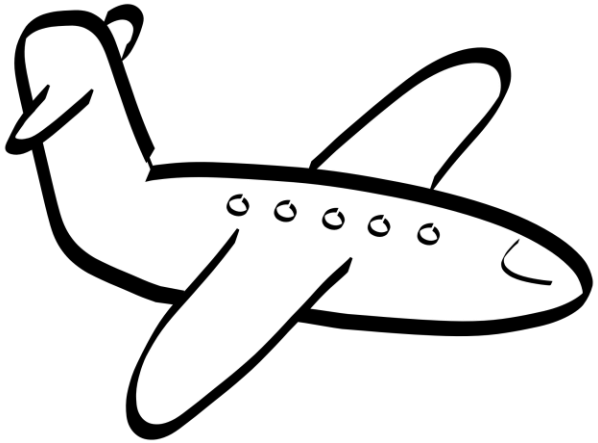
Alessio Merlo

Conferenza sulla sicurezza cibernetica e aerospaziale

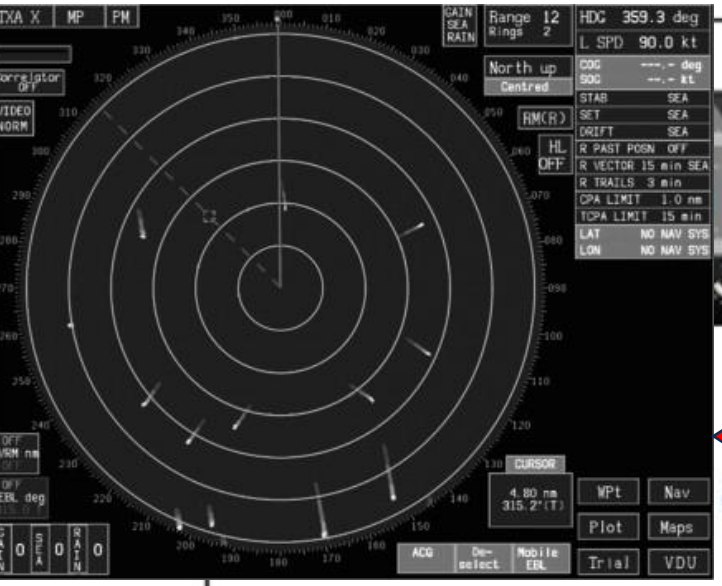
7 aprile 2025 – Palazzo Wedekind

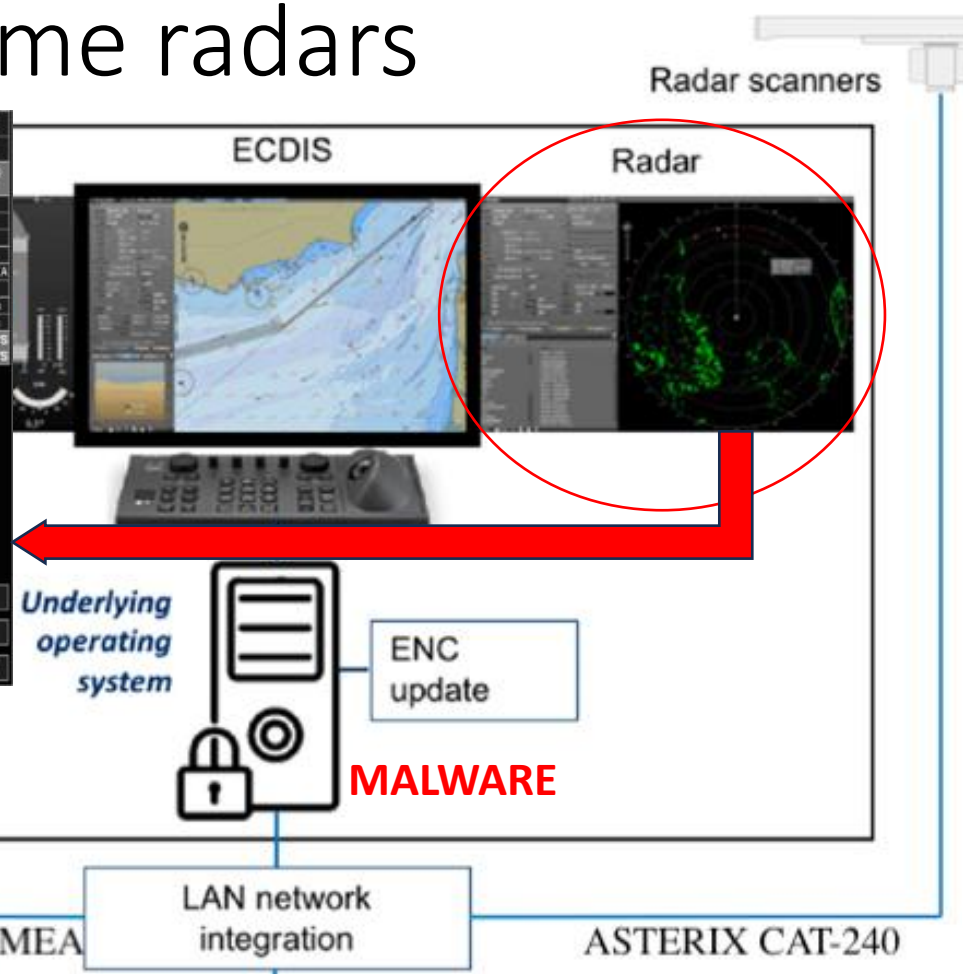
Piazza Colonna 366, Roma





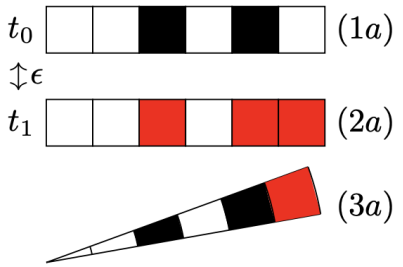
Attacking maritime radars



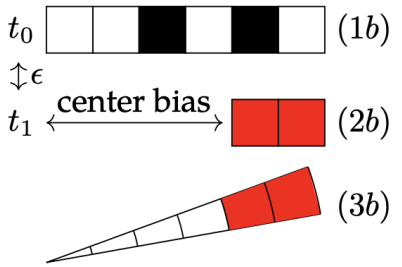


Aim: Reduce Situational Awareness

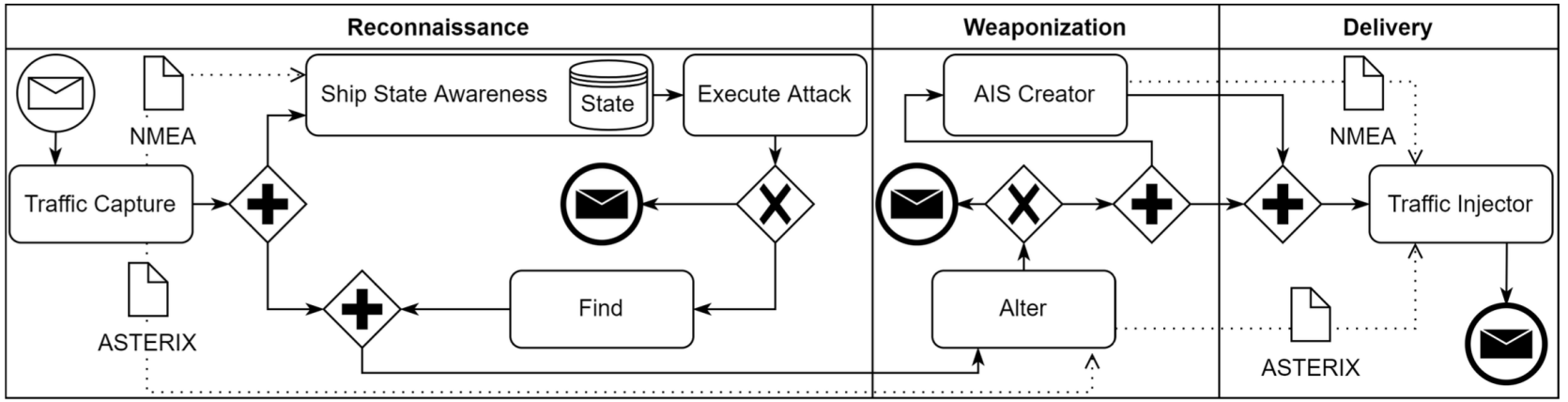
Attack: inject fake ASTERIX packets after legitimate ones from the antenna to ***add*** and ***delete*** targets on the PPI.

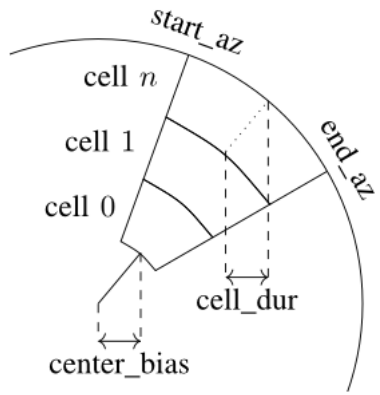


(a) Add.

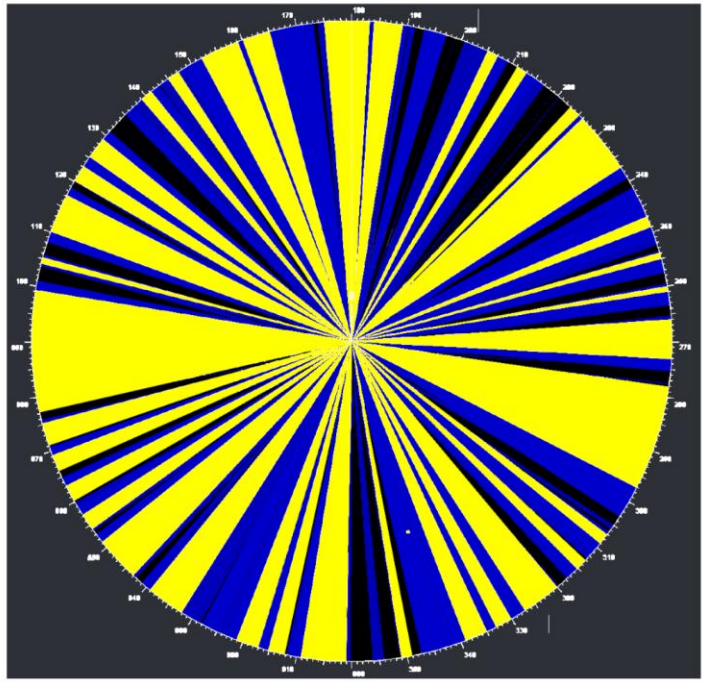


(b) Add and delete.

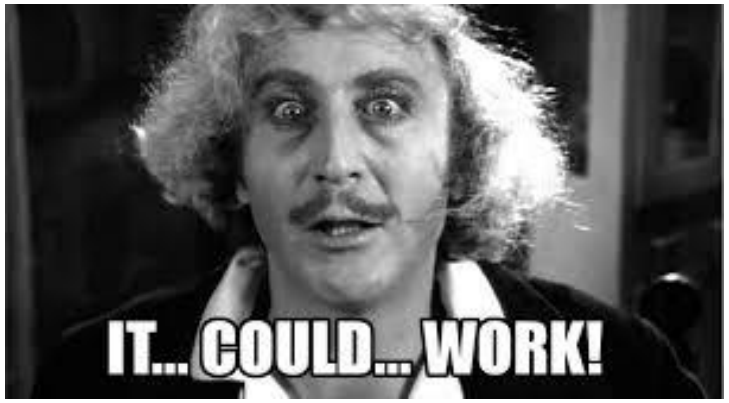


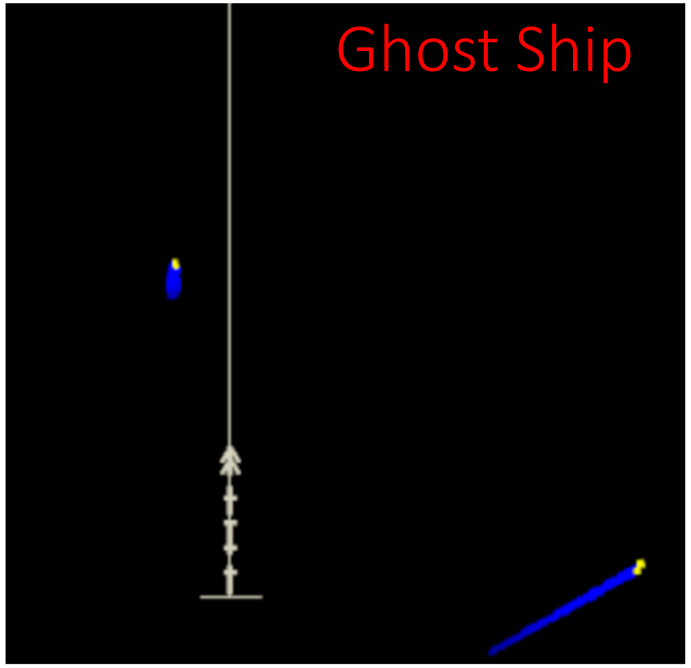


Radar Hijacking

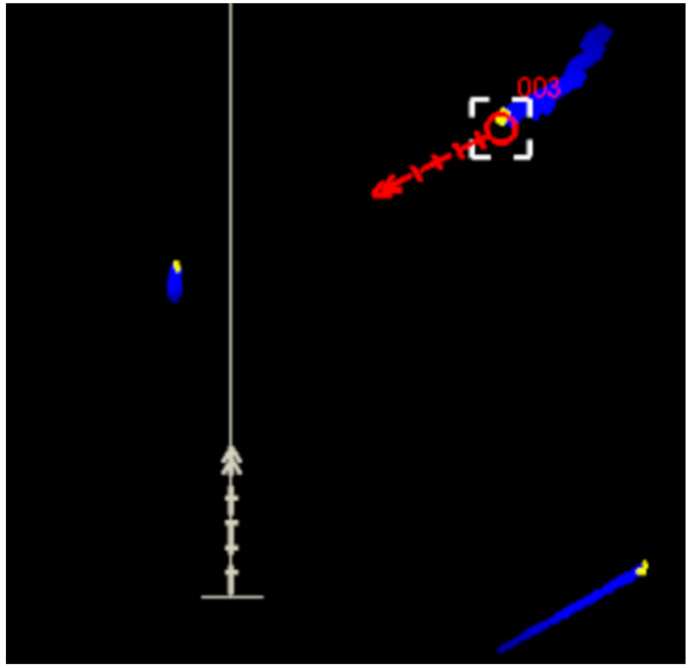


DoS Attack

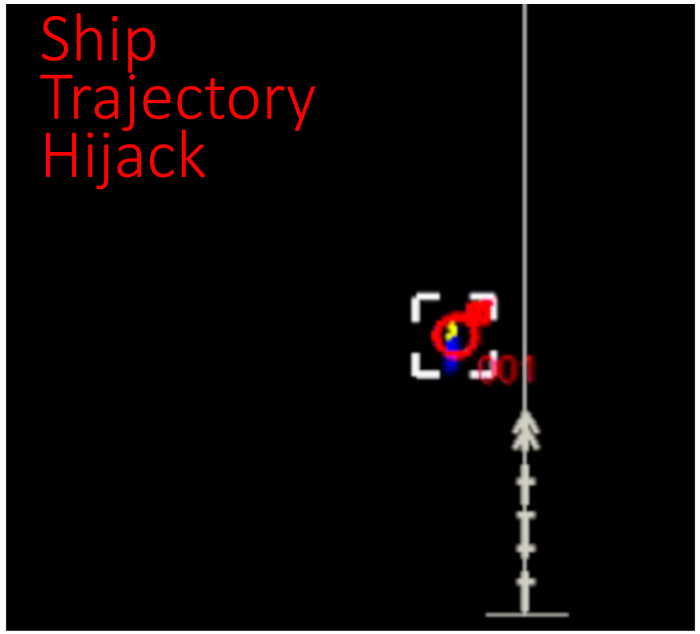




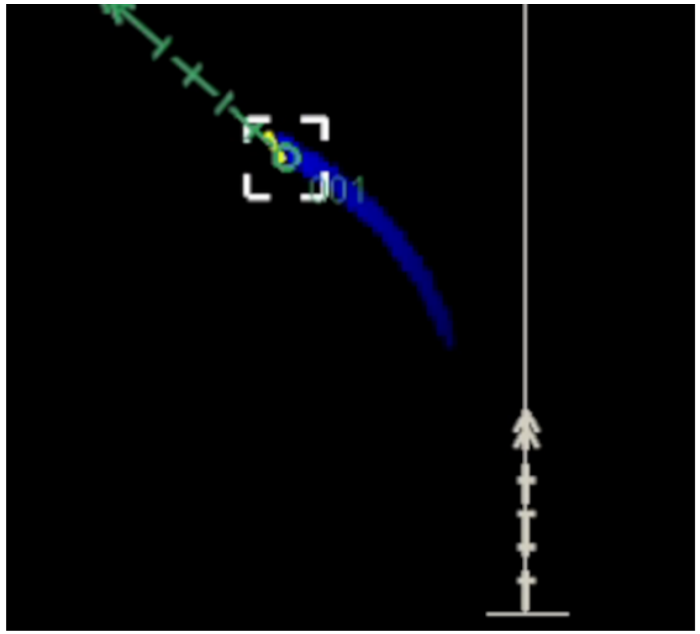
(a) Real



(b) Attacked



(a) Real



(b) Attacked

Remediation and Disclosure

- Remediation is based on anomaly detection, and a patent is coming.

METHOD AND SYSTEM FOR DETECTING ANOMALIES IN A RADAR SYSTEM ON BOARD OF A SHIP **Application**

Publication/Patent Number: WO2024009332A1 **Publication Date:** 2024-01-11

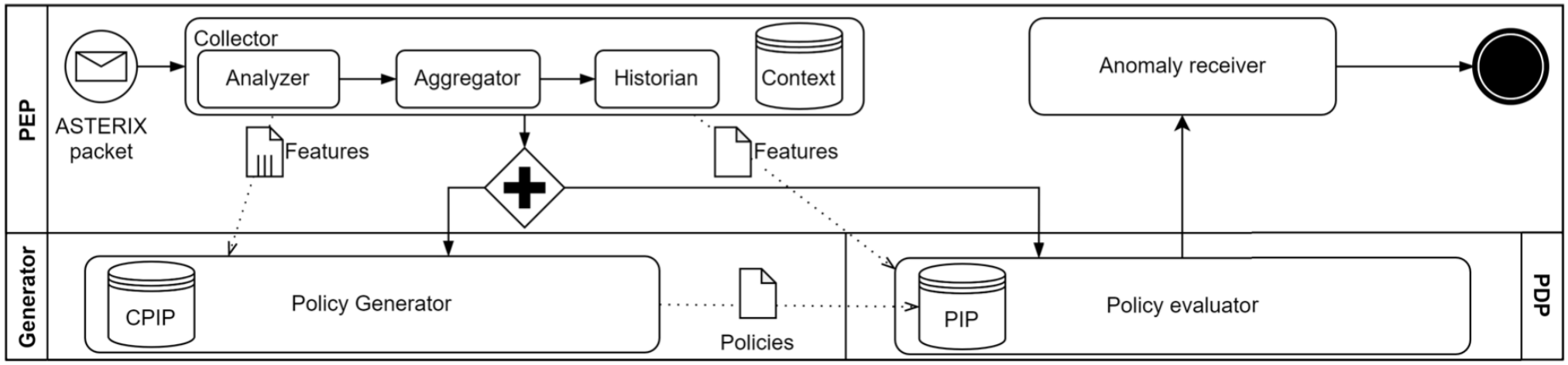
Application Number: IT2022/000036 **Filing Date:** 2022-07-08

Inventor: Russo, Enrico Armando, Alessandro Merlo, Alessio Longo, Giacomo

Assignee: E-PHORS S.P.A.

IPC: H04L9/40

- The idea:

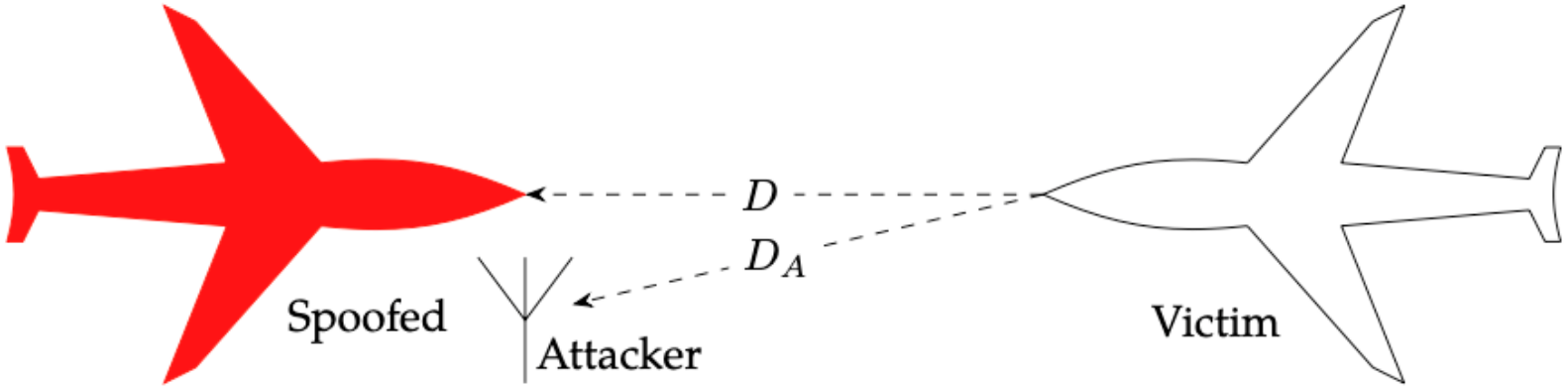


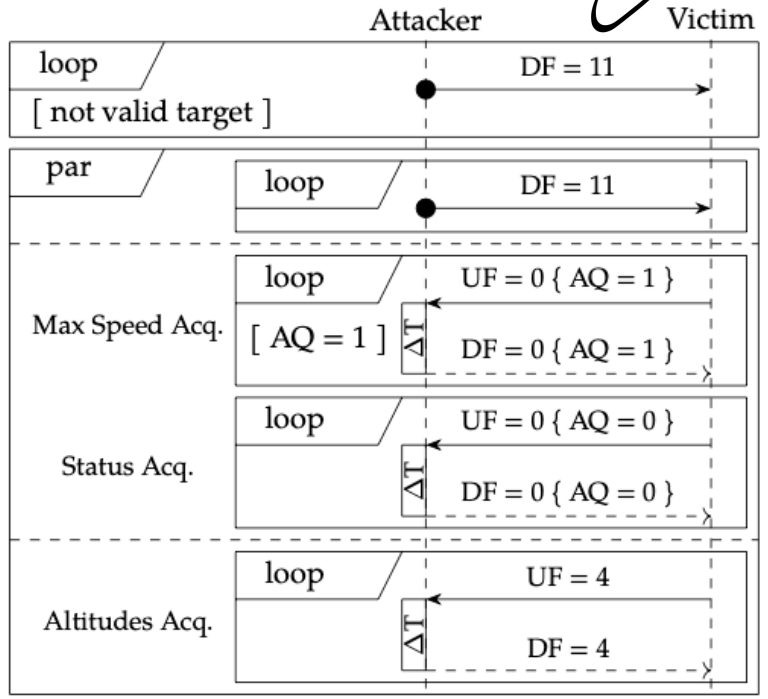
«Responsible disclosure» to radar manufacturers and several maritime stakeholders

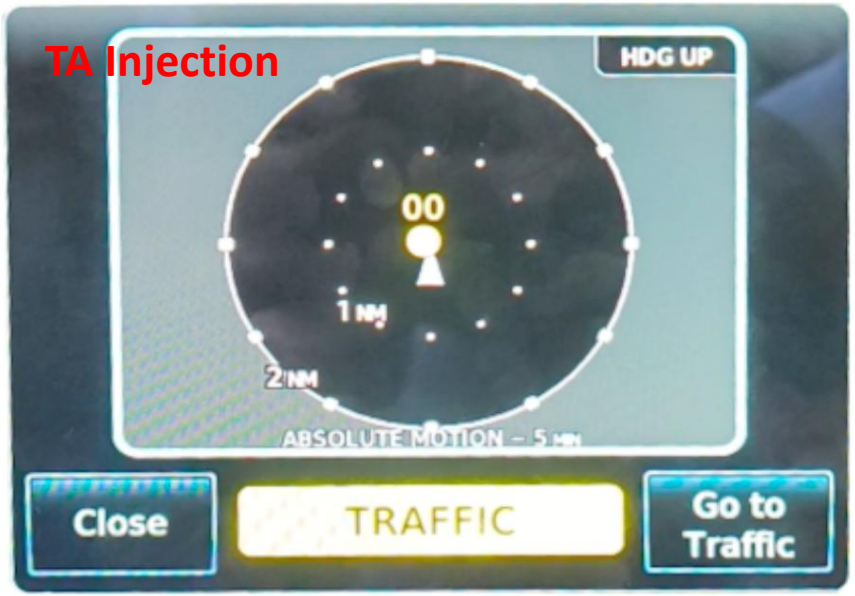
G. Longo, E. Russo, A. Armando, **A. Merlo**: Attacking (and defending) the maritime radar system, IEEE TIFS, 2023

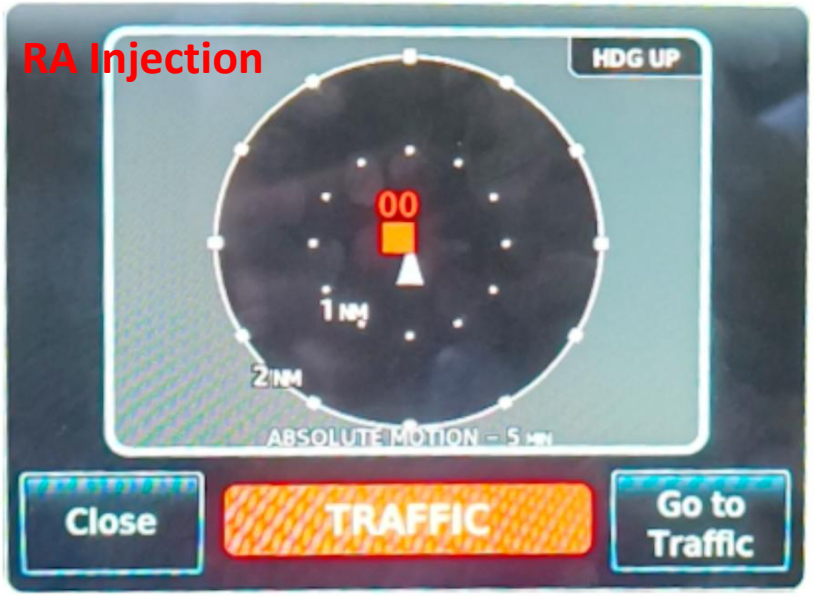
Attacking TCAS

Threat model: An attacker having moderated-price COTS hw (SDRs, signal amplifiers, antennas, computers) → ($10.000) → *terrorists, activists, and nation-state*









DoS on RA

(a) Before SLC (b) SLC receipt (c) After SLC

Found two vulnerabilities allowing to:

1. **Build up false targets on the radar**
2. **Disabling TCAS-RA**

Three RF-based attacks:

1. **Traffic Advisory (TA) Injection**
2. **Resolution Advisory (RA) Injection**
3. **Denial of Service on RA**

Validation, Mitigations, and Disclosure

Validation:

- Joint work with the Defense Campus, Armasuisse, Thun, Switzerland;
- Attacks tested in the lab, real aircraft at rest, and in-flight

Two CVEs:

- CVE-2024-9310: Reliance on Untrusted Inputs in a Security Decision
- CVE-2024-11166: External Control of System or Configuration Setting

Responsible disclosure:

- Agencies: FAA, EASA, Aviation ISAC, COR Difesa, ENAC, ENAV, ACN.
- Industries: Garmin, Leonardo, Airbus, Boeing, Pilatus Aircraft, Thales.

Potential Mitigations (anomaly detection, again):

- No «rewriting», relying on external data;
- Vertical angle (altitude) and Doppler effect (distance).

However, there is **NO FIXING** for the first vulnerability (display fake targets - CVE-2024-9310)

A TA Injection on a real aircraft

G. Longo, M. Strohmeier, E. Russo, A. Merlo, V. Lenders: "On a Collision Course: Unveiling Wireless Attacks to the Aircraft Traffic Collision Avoidance System (TCAS)", USENIX Security 2024.

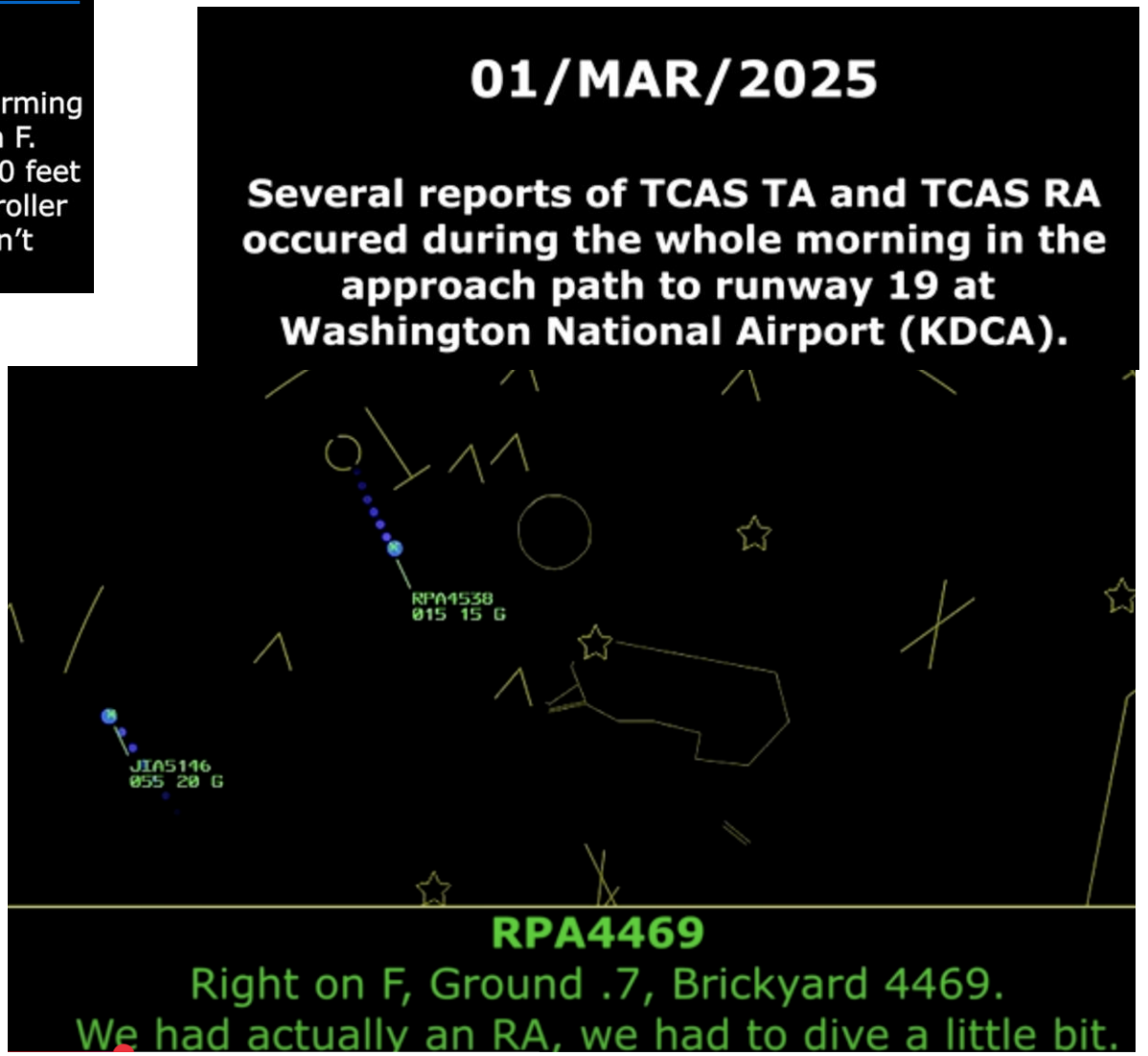
Two «incidents», any correlation?

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

On Jan. 21, 2025, CISA released a bulletin: https://www.cisa.gov/news-events/ics-advisories/icsa-25-021-01

Date: 11-DEC-2024 https://www.youtube.com/watch?v=YiGgKeEwW7U
Place: New York, NY, USA
Time of landing: 11:04 PM, local time.
Description: An American Airlines Boeing 737-800 (B738), registration N358PW, performing flight AAL578 / AA578 Dallas-Fort Worth International Airport, TX (USA) to New York John F. Kennedy International Airport, NY (USA) was on final approach at Kennedy Airport at 3000 feet when the flight crew started the climb to 3700 feet and later reported TCAS RA. The controller informed that there was no conflicting traffic. After that the flight crew said that they hadn't seen anything on their scope as well.

https://www.youtube.com/watch?v=pOXV3AjESVU



Thank you

Contacts:

Alessio Merlo

Professor of Computer Engineering

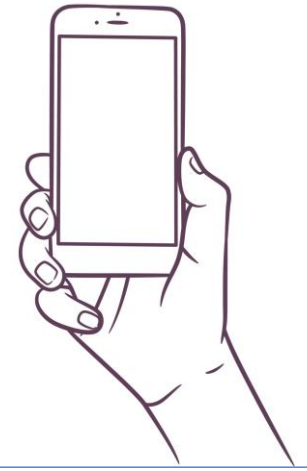
Director - CASD - School of Advanced Defence Studies

Email: direttore@unicasd.it

Mob. +39 3289199105

Android, Notify Me When It Is Time To Go Phishing

Antonio Ruggia*, Andrea Possemato†, Alessio Merlo*, Dario Nisi†, Simone Aonzo†
* *University of Genoa, Italy*
† *EURECOM, France*



IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 18, 2023 3575

Attacking (and Defending) the Maritime Radar System

Giacomo Longo, Enrico Russo, Alessandro Armando, and Alessio Merlo, *Senior Member, IEEE*

On a Collision Course: Unveiling Wireless Attacks to the Aircraft Traffic Collision Avoidance System (TCAS)

Giacomo Longo
DIBRIS
University of Genova, Italy
giacomo.longo@dibris.unige.it

Martin Strohmeier
Cyber-Defence Campus
armasuisse S + T, Switzerland
martin.strohmeier@armasuisse.ch

Enrico Russo
DIBRIS
University of Genova, Italy
enrico.russo@unige.it

Alessio Merlo
CASD
School of Advanced Defense Studies, Italy
alessio.merlo@ssuos.difesa.it

Vincent Lenders
Cyber-Defence Campus
armasuisse S + T, Switzerland
vincent.lenders@armasuisse.ch