# Role of Information Sharing in creating a resilient system

Gian Andrea Bandieri

*Section Manager – Cybersecurity in Aviation & Emerging Risks*

Paris, 10 May 2022

**Your safety is our mission.**

An Agency of the European Union

# Making EU aviation cyber resilient



## Products (Aircrafts, Engines, …)

- Transition from case by case approach to mandatory on all products now done.
- Positive change of mind set in industry: From defiance to full engagement.

## Organisations (People, Processes)

- EASA proposal for a rule (Part-IS) published in June 2021
- Adoption foreseen by end of 2022
- AMC/GM under development

## Information Sharing

- Create a community to
  - Share knowledge
  - Perform Analysis
  - Collaborate
  - Reinforce the system

## Capacity building & Research

- To have competent and well aware workforce
- To monitor the current Threat Landscape
- To understand the future Threat Landscape

EASA

# Why sharing Information - 1

**RESOLUTION A40-10**

- …

- e) Encourage government/industry coordination with regard to aviation cybersecurity strategies, policies, and plans, as well as <u>sharing of information to help identify critical vulnerabilities</u> that need to be addressed;

- f) <u>Develop and participate in government/industry partnerships and mechanisms</u>, nationally and internationally, <u>for the systematic sharing of information</u> on cyber threats, incidents, trends and mitigation efforts;
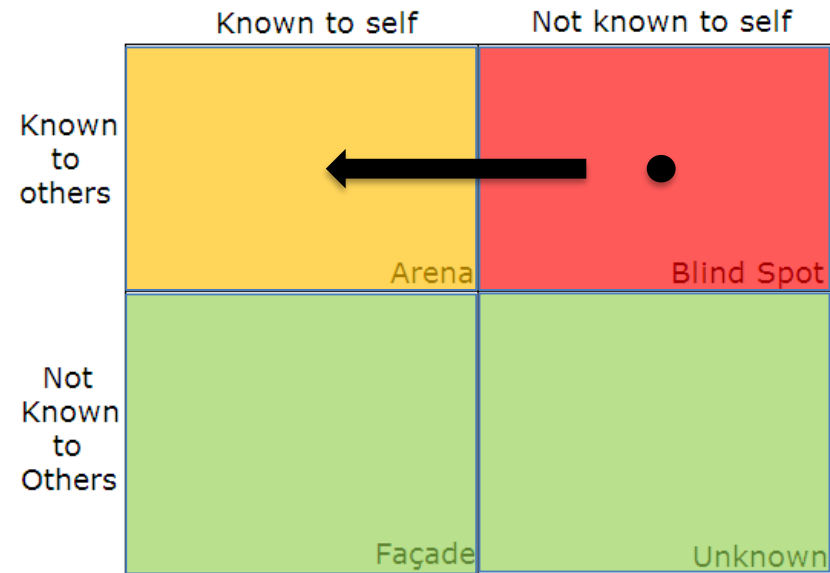
- …

**EASA**

# Why sharing Information - 2

## IN PRACTICE

- We may have some clue about the threat agents, vulnerabilities and exploits to perform a reasonable assessment

- New threats may appear without notice and it is practically impossible to know all the vulnerabilities of a system.

- It is essential to know elements that will emerge in the future and may change the risk picture.

- We need to be aware of "**unknown unknowns**".

The "unknown unknown" is safe until it becomes known to a threat source than turns into a "blind spot" for you

**Johari Window**

| | Known to self | Not known to self |
|---|---|---|
| Known to others | Arena | Blind Spot |
| Not Known to Others | Façade | Unknown |

If "others" with knowledge are "allies" there should be means in place to get to the Arena state

EASA

# What to share

**Vulnerabilities** | **Events** | **Incidents**

**Communicate threats and ensure situational awareness**
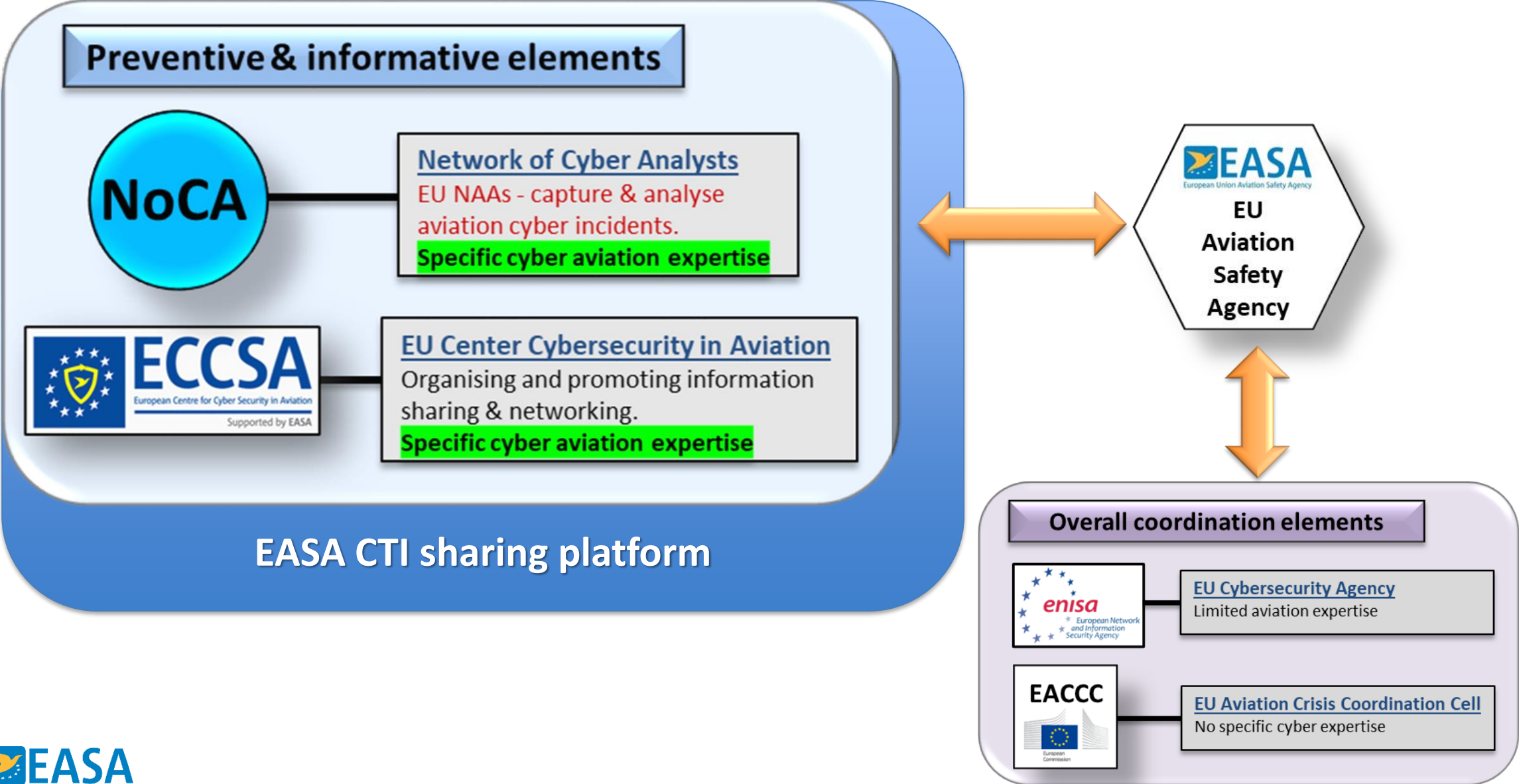
**Make the unknowns known**

**Mandatory** | **Voluntary**

Reg. 376/2014

- To ensure a common approach across all technical domains

EASA

# Network of Cyber Analysts to share and analyse information



**Preventive & informative elements**

**NoCA**

**Network of Cyber Analysts**
EU NAAs - capture & analyse aviation cyber incidents.
Specific cyber aviation expertise

**ECCSA** — European Centre for Cyber Security in Aviation — Supported by EASA

**EU Center Cybersecurity in Aviation**
Organising and promoting information sharing & networking.
Specific cyber aviation expertise

**EASA CTI sharing platform**

**EASA** — European Union Aviation Safety Agency

**EU Aviation Safety Agency**

**Overall coordination elements**

**enisa** — European Network and Information Security Agency

**EU Cybersecurity Agency**
Limited aviation expertise

**EACCC** — European Commission

**EU Aviation Crisis Coordination Cell**
No specific cyber expertise

**EASA**