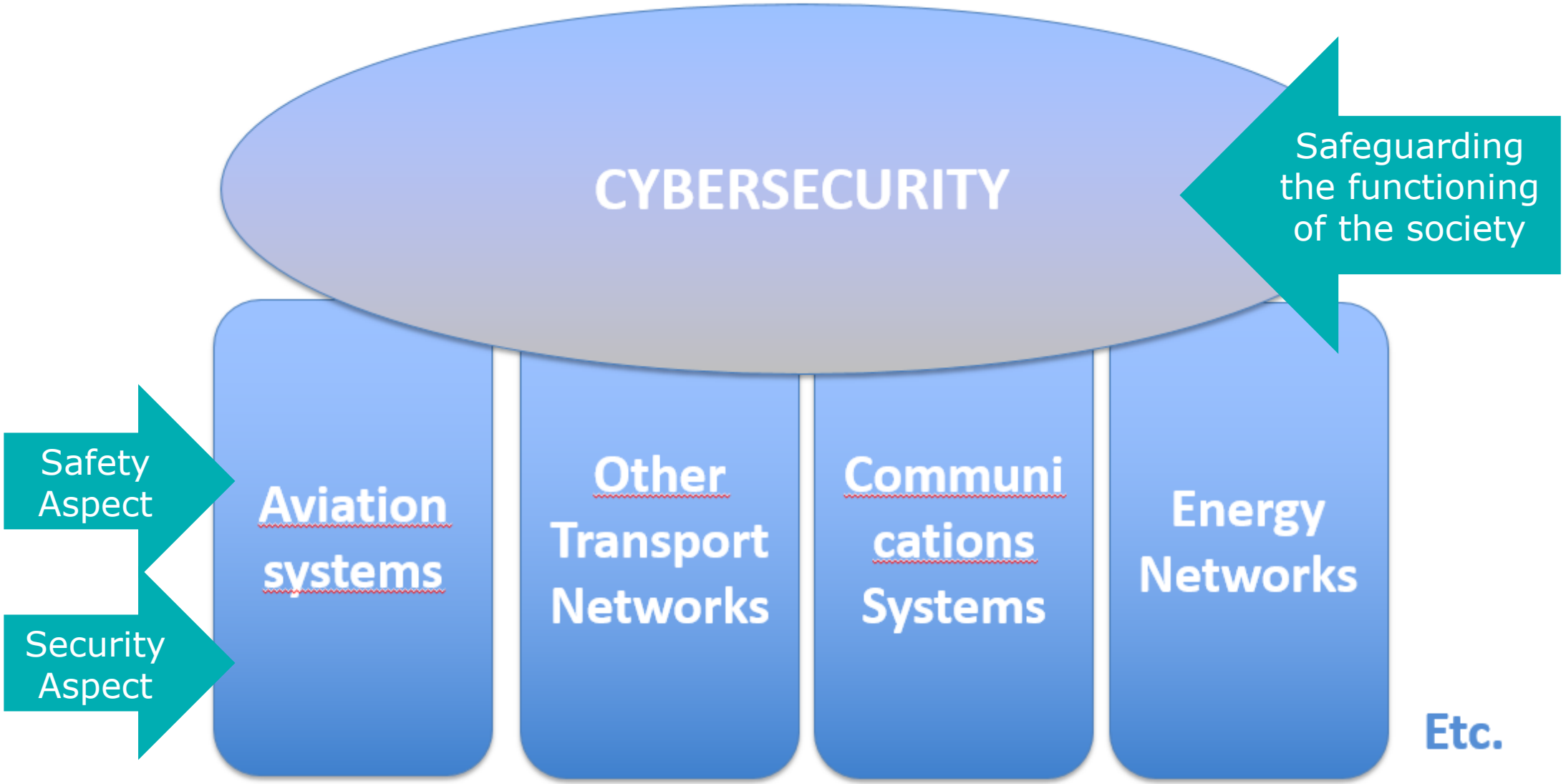
TRAFICOM
Finnish Transport and Communications Agency

Legal framework for dealing with cyber threats against civil aviation

ICAO Legal Seminar, Banjul, Gambia, 24 -25 February 2020

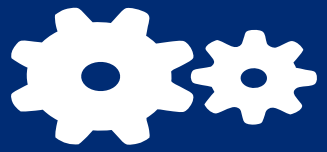
Susanna Metsälampi


CYBERSECURITY
Safeguarding the functioning of the society
Safety Aspect
Security Aspect
Aviation systems
Other Transport Networks
Communi cations Systems
Energy Networks
Etc.

National Cyber Security Strategy since 2013

1. Collaborative model

2. Situation awarness, NCSC-FI



3. Securing vital functions of society and continuity management

4. Cybercrime prevention

5. Cyber defence as part of the national defence capability

6. Active international cooperation

7. Expertise and shared awarness

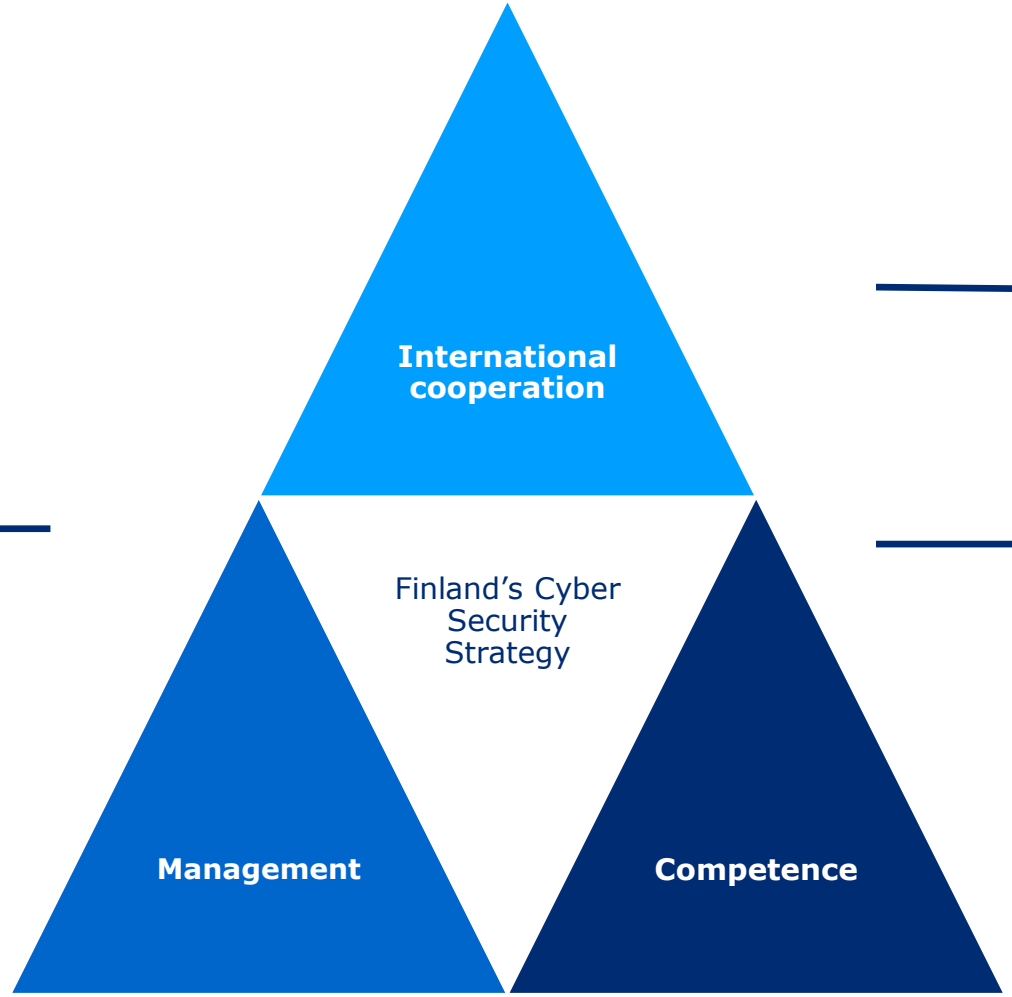
8. Modern legistlation supporting cyber security

9. Cyber security tasks and service models

10. Implementation and monitoring

Cyber Security Strategy 2019

Better coordination of **management**, **planning** and **preparedness** in cyber security



Developing international cooperation – borderless security in the cyber environment

Improving cyber security competence – everyday skills and top experts ensuring cyber security

General and Specific Rules 1/3

- **National Preparedness Act**
  - How to secure vital functions in the society in exceptional circumstances.
  - Allocates obligations and competencies
- **Act on Electronic Communications Services**
  - Regulates e.g. telecommunications operators
- **Legislation on how data should be handled in Finnish Administration**
  - E.g. on classification of data (Secret, Confidential)

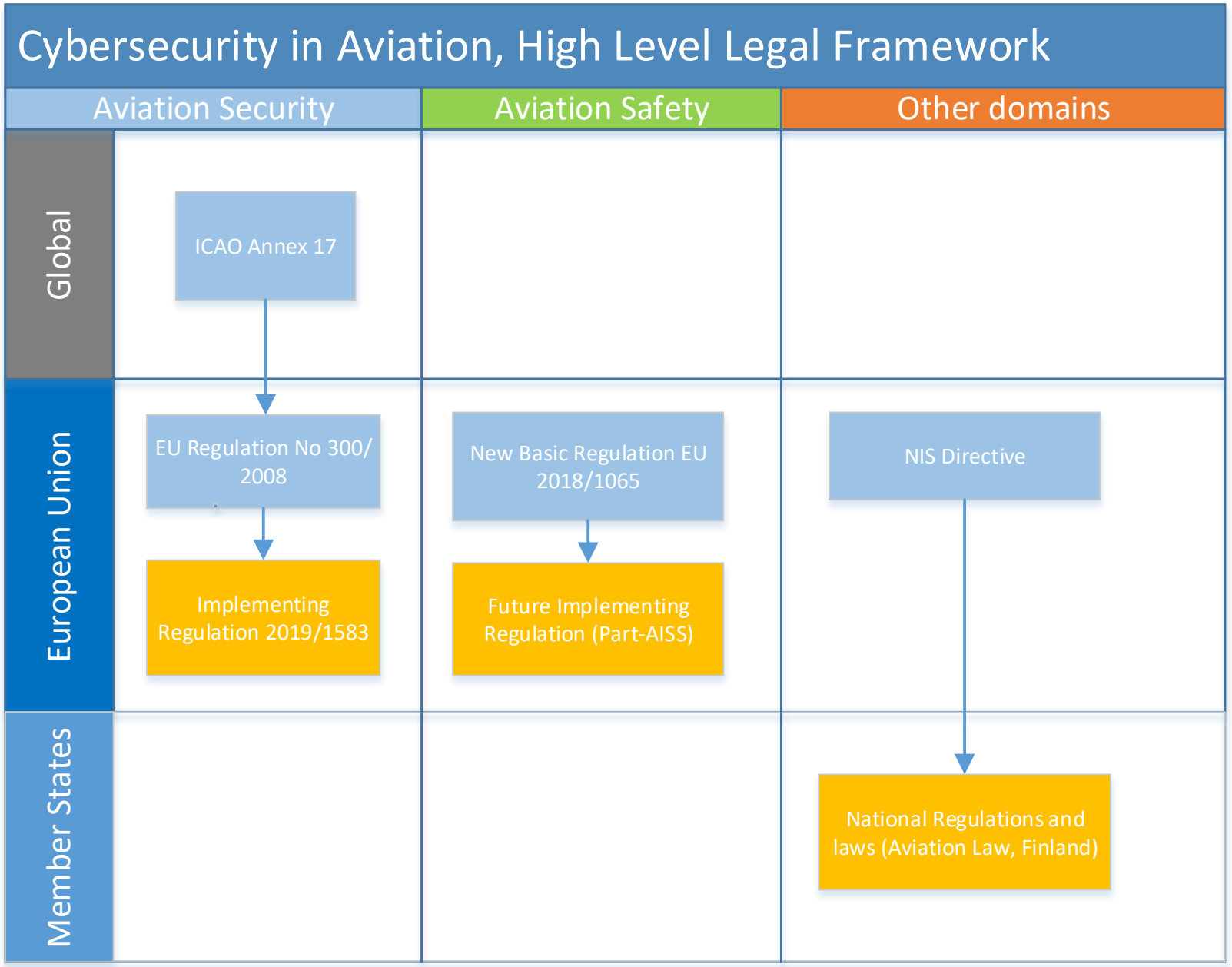
General and Specific Rules 2/3

- **European Union Directive on security of network and information systems (NIS Directive)**
  - Member States' preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority
  - Co-operation between Member States
  - a culture of security across sectors which are vital for the economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.
  - ➢ **This Directive has been implemented/transposed in several national laws, among others the Aviation Act**

EU legislation in EU Member States
- Regulations are directly applicable
- Directives need national transposition

General and Specific Rules 3/3

- **EU Commission Implementing Regulation** (EU) 2019/1583 amending Implementing Regulation (EU) 2015/1998 laying down **detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures**
  - Cybersecurity in Security
- **Aircraft Cybersecurity and Management of information security risks: 2 ongoing Rulemaking Tasks**
  - The first proposes amendments that are expected to contribute to updating the EASA Certification Specifications to reflect the state of the art of **protection of products and equipment against cybersecurity threats**. They are also expected to improve harmonisation with the Federal Aviation Administration (FAA) regulations.
  - The second proposes the introduction of provisions for the management of information security risks related to aeronautical information systems used in civil aviation. These provisions shall apply to competent authorities and organisations in all aviation domains (i.e. design, production, management of continuing airworthiness, maintenance, air operations, aircrew, air traffic management/air navigation services (ATM/ANS), and aerodromes), shall include high-level, performance-based requirements, and shall be supported by acceptable means of compliance (AMC), guidance material (GM), and industry standards.
  - Management System Approach


Cybersecurity in Aviation, High Level Legal Framework
Aviation Security
Aviation Safety
Other domains
Global
European Union
Member States
ICAO Annex 17
EU Regulation No 300/ 2008
Implementing Regulation 2019/1583
New Basic Regulation EU 2018/1065
Future Implementing Regulation (Part-AISS)
NIS Directive
National Regulations and laws (Aviation Law, Finland)

TRAFICOM

The “Trinity” in Information Security

- The Availability of Information
- The Confidentiality of Information
- The Integrity of Information

- Information should be available to those, but only those who need it, and it should be modified only by those who are entitled to do that.

National Cyber Security Centre Finland (NCSC-FI)

National information security authority, whose duties include

- **collecting information** on violations of and threats to information security
- **disseminating information** on security issues as well as performance of communications networks and services
- **investigating** violations of and threats to information security in respect of network services, communications services and added value services
- steering and monitoring telecommunications operators' **information security and preparedness**
- **audits and accreditation of systems and networks**
- monitoring obligations related to **privacy in electronic communications**

Collaborative networks

- Information Sharing and Analysis Centres (ISACs) exchange information on information security threats and phenomena.
- These centres allow for:
  - confidential discussion on information security issues
  - increasing information security expertise in organisations
  - improving situation awareness by the NCSC-FI
  - improving cyber security in the field and in society

NCSC-FI's cooperation networks promote security

Improving the cyber security of industries and society via Information Sharing and Analysis Centres (ISACs) for information security issues

- risk analyses
- guidelines
- research
- information exchange

TRAFICOM
Finnish Transport and Communications Agency

Susanna.metsalampi@traficom.fi
www.traficom.fi
@TraficomFinland