Part-IS

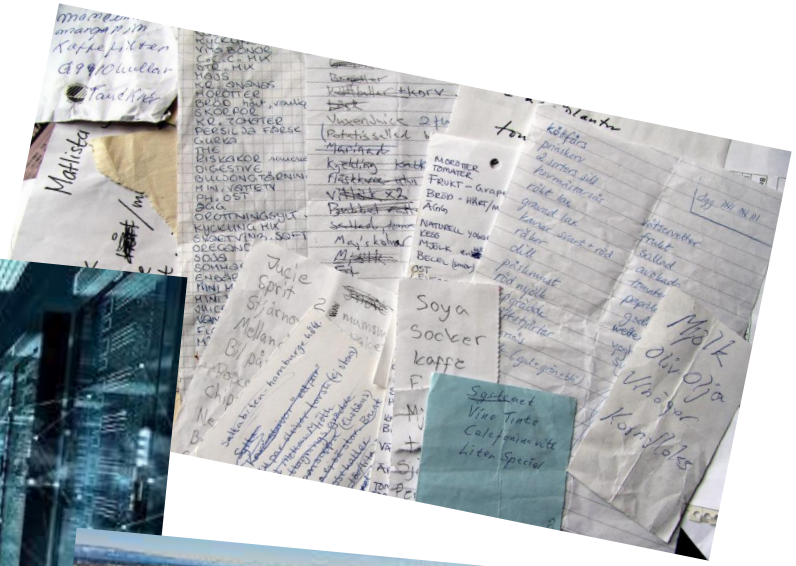
IT & informationssäkerhet

Johan Harter,
chef sektionen för cybersäkerhetstillsyn

Michael Andersson,
senior cybersäkerhetsinspektör

TRANSPORT STYRELSEN

Vad är information värd?



Agenda

- Omvärldsläget på IT-arenan
- Hotbilden mot transportsektorn
- Vad är Part-IS och varför nu
- Part-IS vs traditionell it/info-säkerhet
- Vad krävs av vår organisation? (grundkraven)
- Vad tar jag med mig?

TRANSPORT STYRELSEN


Minskad risk för konventionellt angrepp mot Sverige
Resursområde och styrkeuppbyggnad
Fortsatt stor risk för långräck-viddig bekämpning, cyber-angrepp, sabotage m m
Högintensiv och uthållig markstrid
Styrketillförsel
REAR
FRONT
DEEP

Hotaktörer mot transporter

- Cyberkriminella
- ”Hackers-for-hire”
- Hacktivister eller ”hacktivister”
  - NoName057 36.4% (2025)
  - DarkStorm Team 15.4%
  - Mysterious Team Bangladesh 6.2%
  - Stöd till Ukraina är en trigger
- Insiders

Nyheter

Sverige, ett av hacktivismens huvudmål under 2023

presenterar nu sin årliga säkerhetsrapport, Security Navigator 2024. Bland resultaten framkommer att Sverige är ett av de mest attackerade länderna.

Trafikverkets skydd mot it-attacker brister

Trafikverkets it-säkerhet och skydd mot cyberattacker har stora brister, visar en intern rapport som Ekot tagit del av.

Under granskningen lät man Totalförsvarets forskningsinstitut (Foi) försöka bryta sig in i myndighetens system, och testet visade på flera sårbarheter som kan utnyttjas av främmande makt.

Enligt Trafikverkets biträdande it-direktör Magnus Dalersand jobbar myndigheten regelbundet med it-säkerhet och åt

– Att vara hundraprocent

Nationalmuseum i Stockholm har blivit hackat och mejl skickas ut från en officiell e-postadress. **Foto: Pontus Lundahl/TT**

Nationalmuseum hackat – skickar ut phishingmejl

Attacker mot Sverige väntas när ryska hackare erbjuder botnet som tjänst

Fördubbling av it-angrepp mot myndigheter i fjol

Uppgifter till salu på darknet efter attacken mot Sophiahemmet

Bland annat patientuppgifter ligger ute till salu på darknet för en milion dollar efter cybera

att det

024-02-0

Robert Gallusson, kommunikationschef på Statens servicecenter, säger att myndigheten använder sig av hr-systemet Primula – men kan inte bekräfta att det ligger nere.

Däremot säger han att myndigheten har reservrutiner när it-system fallerar, vilket betyder att de kommer kunna betala ut lön i tid oavsett.

Instructure hacker claims data theft from 8,800 schools, universities

By Lawrence Abrams

May 5, 2026 05:20 PM 0

Nya it-attacker mot myndigheter – Polisen och Skatteverket drabbade

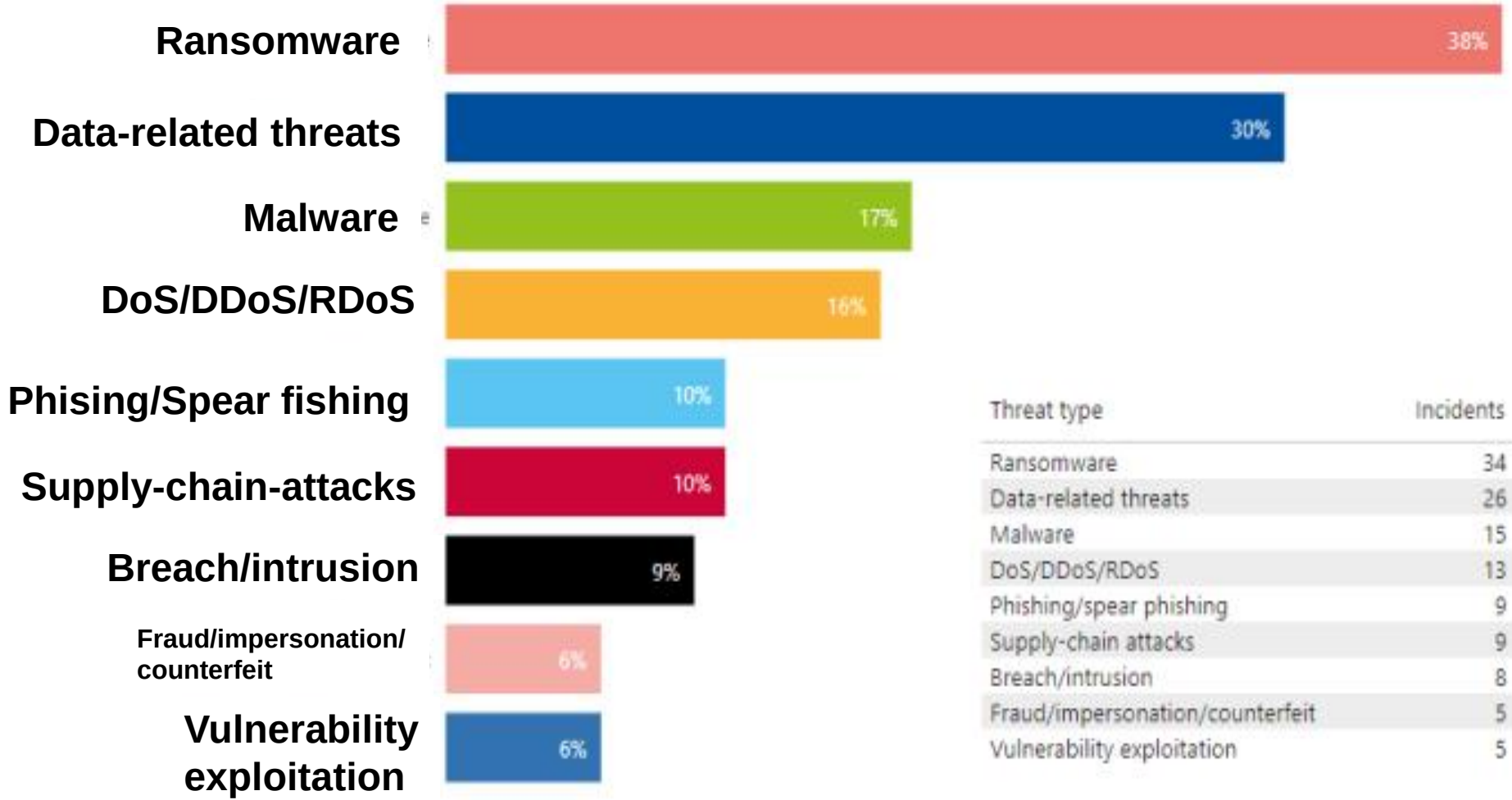
Säkerhet och beredskap

Flera kommuner och regioner drabbade av it-attacken

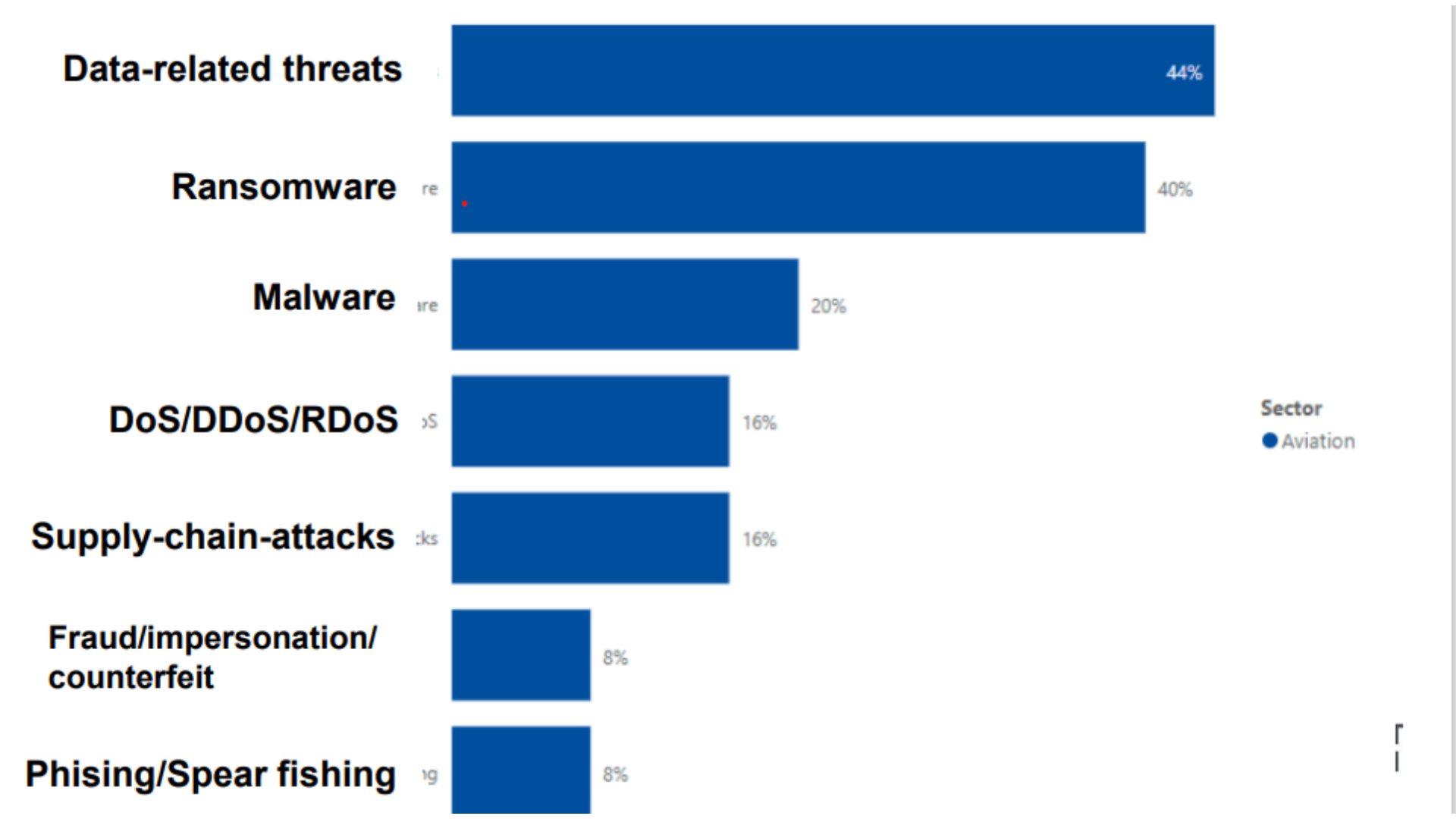
Publicerad: 22 januari 2024, 08:59

Hotbilden mot transportsektorn

TRANSPORT STYRELSEN



Threat type	Incidents
Ransomware	34
Data-related threats	26
Malware	15
DoS/DDoS/RDoS	13
Phishing/spear phishing	9
Supply-chain attacks	9
Breach/intrusion	8
Fraud/impersonation/counterfeit	5
Vulnerability exploitation	5


Data-related threats
44%
Ransomware
40%
Malware
20%
DoS/DDoS/RDoS
16%
Supply-chain-attacks
16%
Fraud/impersonation/ counterfeit
8%
Phising/Spear fishing
8%
Sector
Aviation

Cyberangrepp mot flyg & stödsystem

Flyget är extremt digitaliserat. Själva flygsäkerhetskritiska systemen är ofta separerade och hårt reglerade, men stora störningar kan ändå uppstå i kringliggande system: incheckning, boarding, bagage, gate-planering, crew scheduling, betalning, lojalitetsprogram, appar, webbplatser och leverantörsportaler.

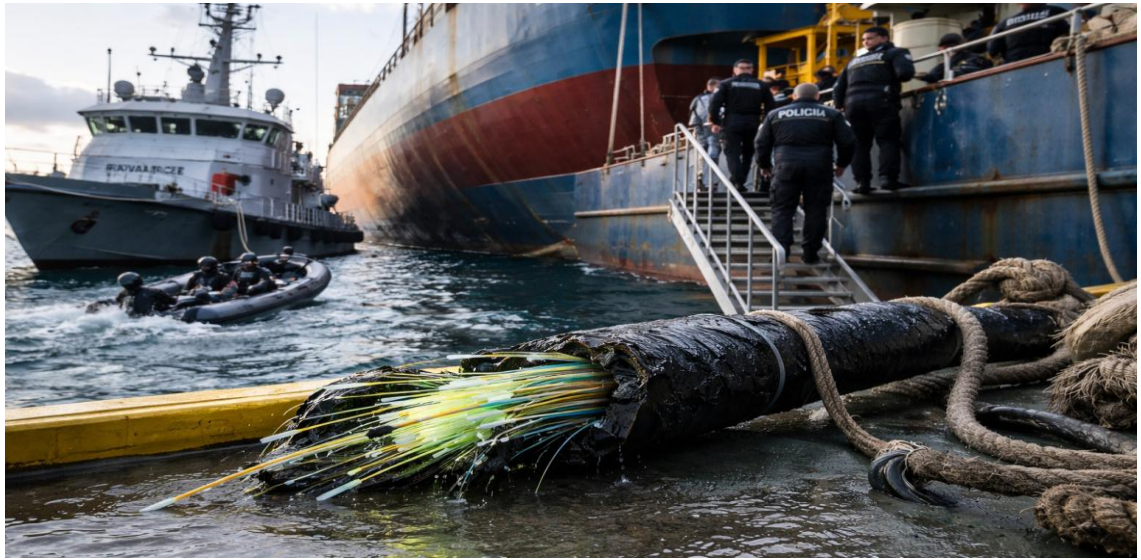
Ett praktiskt exempel är ransomware mot gemensamma flygplats och passagerarhanteringssystem.
Under 2025 rapporterades en ransomware incident mot Collins Aerospace ARINC cMUSe,
som påverkade in-checkning och boarding vid flera europeiska flygplatser, bland annat Heathrow, Bryssel och Berlin.

TRANSPORT STYRELSEN

Sabotage och fysisk påverkan

För flygets gäller detta inte bara flygplan.
Mer realistiska mål är:

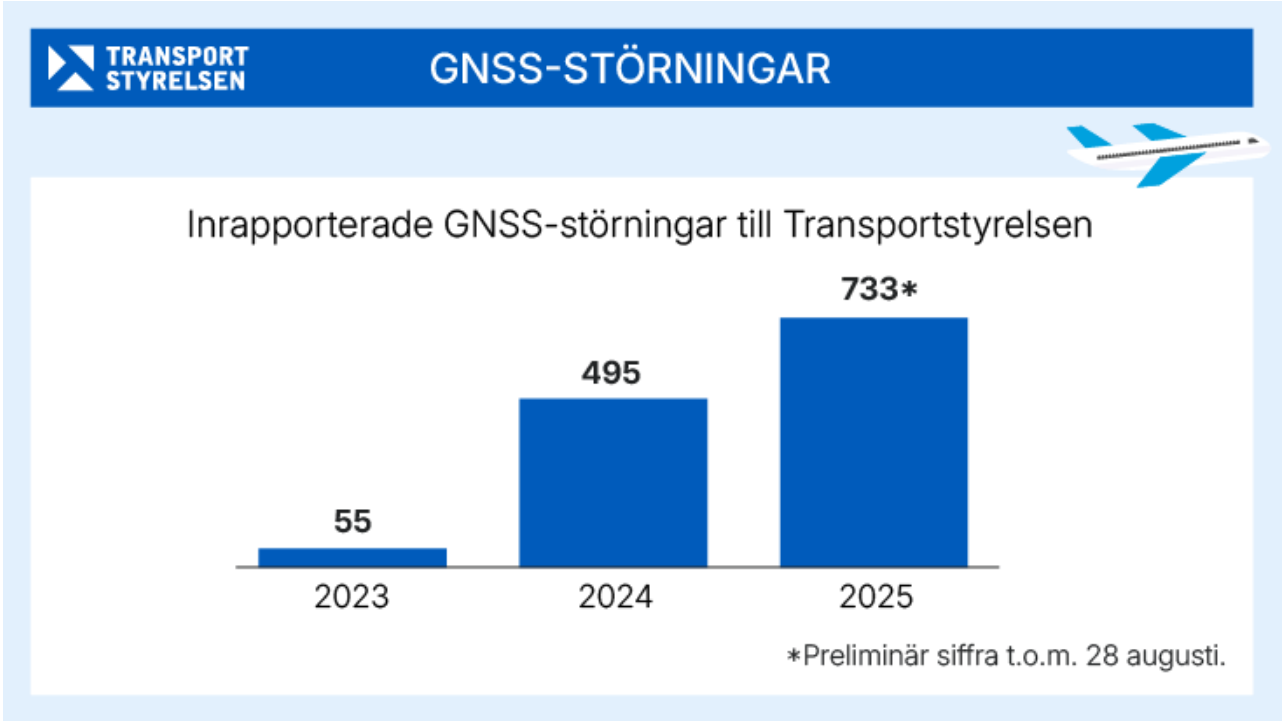
- kablar och kommunikationsnoder
- bränsleförsörjning
- markfordon och utrustning
- perimeterskydd och tillträdeskontroll
- underhållsdepåer
- fraktterminaler
- elförsörjning och reservkraft
- drönarstörningar nära flygplatser



Effekten blir större när ett mindre fysiskt sabotage görs i samband med ett cyberangrepp, GPS störning eller informationspåverkan.

TRANSPORT STYRELSEN

Sabotage och fysisk påverkan



TRANSPORT STYRELSEN

De största hoten mot flyget just nu

Högst sannolikhet:
GPS/GNSS-störningar, DDoS, phishing/social engineering, ransomware mot stödsystem, leverantörsstörningar.

Störst konsekvens:
Koordinerad hybridoperation mot flygplatsdrift, kommunikation och navigation; större ransomware mot gemensamma leverantörer; sabotage mot el/telekom/bränsle; insiderangrepp i säkerhetskritisk miljö.

Mest underskattat:
Beroenden till externa leverantörer, äldre reservsystem, identitetshantering/helpdesk och kombinationen cyber + fysisk påverkan + desinformation.

Särskilt för Sverige:
Östersjöregionens GPS-störningar, Nato-relaterad hybridhotbild, beroenden till flygplatsernas externa system och behovet av robust reservnavigering framstår som centrala.

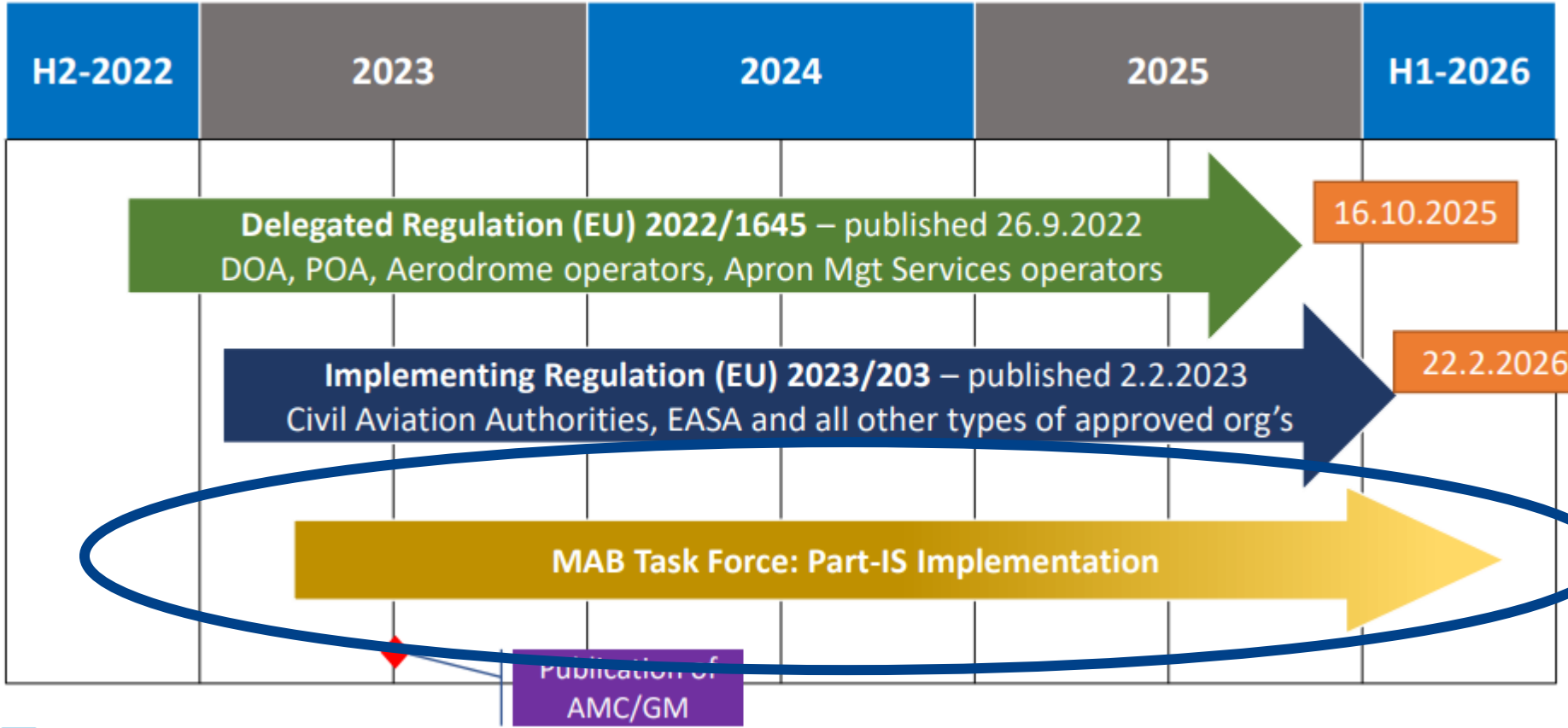
EASA and IATA outline comprehensive plan to mitigate GNSS interference risks | EASA

Aviation prepared for GPS interference: It is safe to fly in and to Finland | Traficom

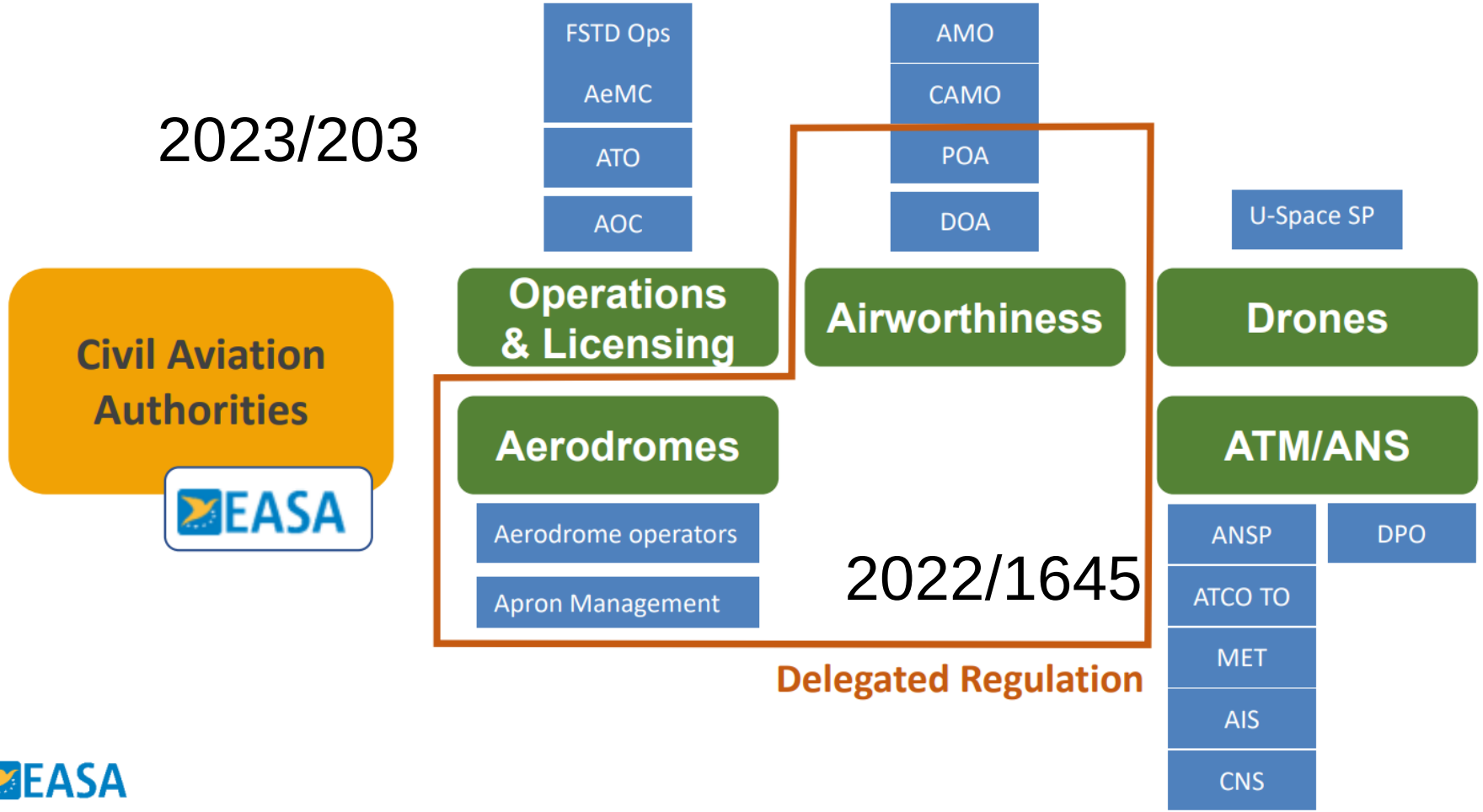
TRANSPORT STYRELSEN

Part-IS

Part-IS implementation journey



Applicability of Part-IS



Vad är EASA Part-IS?

Part-IS = krav på att identifiera, skydda, upptäcka, hantera och återhämta sig från informationssäkerhetshändelser som kan påverka flygsäkerheten.

Governance
roller, ansvar, policy

Riskhantering
tillgångar, hot, konsekvenser

Incidenter
detektera, rapportera, återhämta

Kontinuitet
motståndskraft, återhämtningsförmåga och övning

Part-IS är safety-driven informationssäkerhet: skyddsvärdet omfattar konfidentialitet, integritet, tillgänglighet och operationell säkerhet, där autenticitet används för att stödja dessa värden

Varför kommer Part-IS nu?

Uppkopplade system
Data, nätverk och fjärråtkomst är del av den operativa miljön.

Komplex leverantörskedja
MRO, CAMO, flygplatser, ANSP och IT-leverantörer är sammanlänkade.

Regulatoriskt skifte
EASA ställer krav på hantering av informationssäkerhetsrisk med potentiell safety-effekt.

TRANSPORT STYRELSEN

Det viktiga skiftet: från security till safety

TRANSPORT STYRELSEN

När informationssäkerhet blir Aviation Safety

Underhållsdata

Felaktig eller manipulerad data kan leda till fel beslut om luftvärdighet.

Flight planning

Otillgänglig eller manipulerad data kan påverka bränsle, rutt, väder eller prestandaberäkningar.

Airport/ATM integration

Avbrott i kommunikation eller systemsamverkan kan påverka kapacitet och säkerhetsmarginaler.

Cyberincidenten är inte alltid “hacking” – ibland är det den operativa konsekvensen som behöver styras.

TRANSPORT STYRELSEN

Grundkraven i praktiken

Organisation & ansvar
Definierade roller, resurser, policy och integrering i management system.

Riskbedömning
Identifiera informationssäkerhetsrisker med potentiell safety-effekt.

Åtgärder & kontroller
Tekniska, organisatoriska och processmässiga skyddsåtgärder.

Incidenthantering
Upptäcka, klassificera, rapportera, utreda och återhämta.

Kompetens & kultur
Awareness och rollbaserad kompetens.

Övervakning & förbättring
Internrevision, KPI:er, lärande och management review.

TRANSPORT STYRELSEN

Vad tar jag med mig?

- Part-IS är **safety-driven** informationssäkerhet.
- **IT, safety, compliance** och **operation** måste ha ett gemensamt språk gällande riskhantering.
- **Framtagning** och **träning** av processer är lika viktiga som policydokument.
- Bygga **säkerhetskultur** är A & O!

TRANSPORT STYRELSEN

TRANSPORT STYRELSEN

Tack för oss!

TRANSPORT STYRELSEN