MOLIT
Ministry of Land,
Infrastructure and Transport

[ICAO APAC Regional Cybersecurity Seminar]

Current State of Aviation Cyber Threats in the Republic of Korea

Donghwan Yoon
(Expert nominated by Republic of Korea)

12-14, Mar. 2025

KIAST Korea Institute of Aviation Safety Technology

MOLIT
Ministry of Land, Infrastructure and Transport

Contents

- Global Cyber Threats
- Cyber Threats in Republic of Korea
- Aviation Cybersecurity Strategy of ROK

Global Cyber Threats (1/4)

- ICAO GCRC(Global Cyber Risk Considerations)(1st ,2024)
  - HIGH: 1, MEDIUM-HIGH: 4

Theft of Intellectual Property Rights (IPR)

Ransomware

Corruption of Electronic Flight Bag (EFB) Data

Using an Unmanned Aircraft System to Collide with an Aircraft

Spoofing of Global Navigation Satellite System (GNSS)

Global Cyber Threats (2/4)

- ICAO GCRC(Global Cyber Risk Considerations)(1st ,2024)
  - MEDIUM: 8

Distributed Denial of Service (DDoS)

Theft of Personally Identifiable Information (PII)

Unavailability of Heating Ventilation Air Conditioning (HVAC) in Operational or Data Centre

Unavailability of Power Supply in Operational or Data Centre

Intrusion to Aviation Dedicated Airspace by UAS

Corruption of Meteorological (MET) Data

Corruption/Spoofing of Surveillance Data

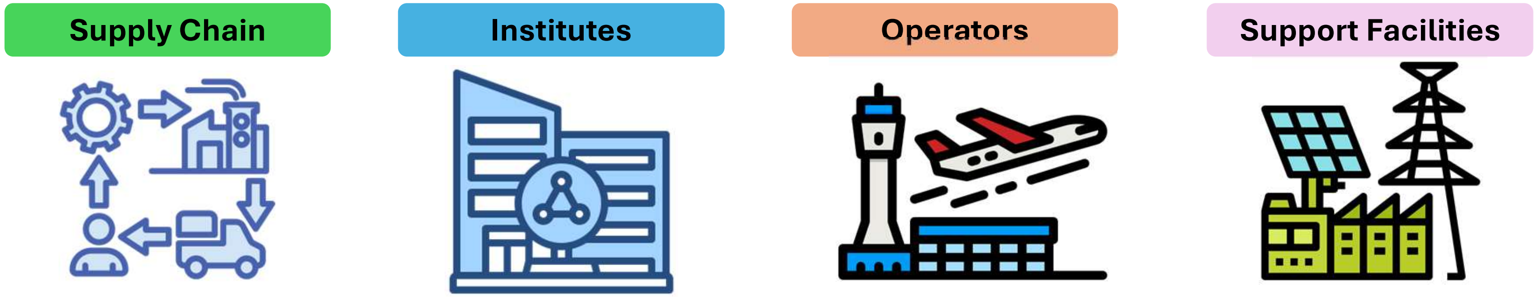
Corruption of Flight Plan

Global Cyber Threats (3/4)

- Occurrences of Cyber Threats in Aviation
  - Cyber Crime
    - Actions that compromise the **Integrity, Confidentiality, or Availability** of **Aviation Systems**
      - Unauthorized access to systems
      - Loss of devices with confidential information
      - Brute force attacks
  - Cyber Terrorism
    - Disruptive attacks by terrorist organizations against computer systems
    - The goal is to cause alarm, panic, or physical disruption
    - Used to cause harm for political, religious, or ideological reasons

Global Cyber Threats (4/4)

- Occurrences of Cyber Threats in Aviation
  - Cyber Terrorism → Cyber Attacks
    - **Cyber espionage**, which is when an unauthorized user accesses sensitive data for economic or political reasons
    - **Phishing attacks**, which use email to collect information that can be used to access systems or steal identities
    - **Ransomware attacks**, which are often compared to terrorism
  - Targets



Supply Chain

Institutes

Operators

Support Facilities

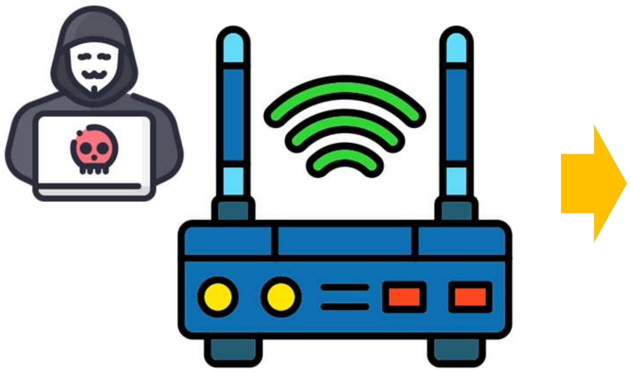
Cyber Threats in Republic of Korea

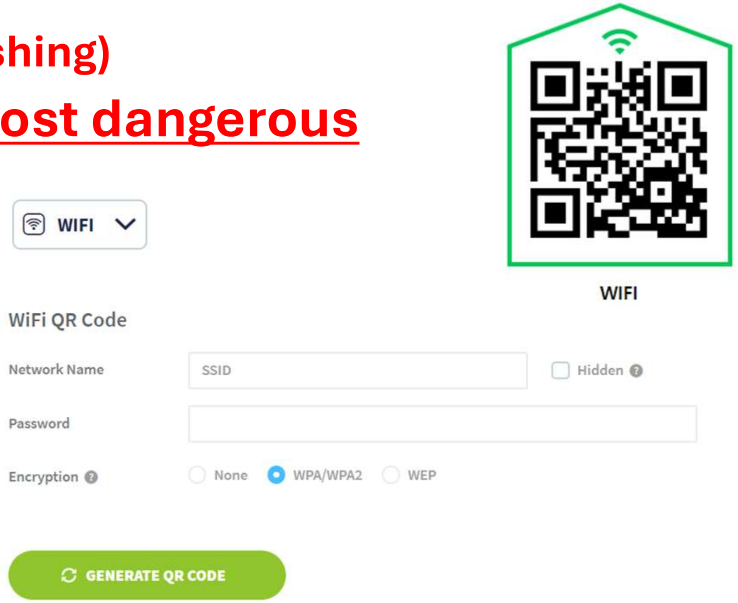
- Main Cyber Threats (2024)
  1. Phishing Attacks (ex: Mails, Messages, QRs)
  2. Supply Chain Compound Attacks
  3. Advanced Ransomware Attacks
- Expected Cyber Threats (2025)
  1. Evolving Attacks supported by Generative AI
  2. Vulnerabilities Attacks of Digital Convergence Technology(ex: Smart ITS)
  3. Critical Infrastructure Attacks by Cyber Terrorists
  4. Brute DDoS attacks

Reviews of Main cyber threats (2024)

1

- Phishing Attacks
  - Various methods
    - Spam(illegal) Mails, Messages
    - Smishing
    - **Qshing (QR code + Phishing)**
  - Especially, **Qshing is most dangerous**





WIFI ⌄

WiFi QR Code

Network Name: SSID □ Hidden

Password:

Encryption: ○ None ● WPA/WPA2 ○ WEP

Reviews of Main cyber threats (2024)

- Supply Chain Compound Attacks
  - Vulnerabilities
    - Software Updates
    - Each Stage of SW Supply chain (Especially, Open Source)
  - Emerging Methods
    - Convergence between Injection of Malicious code(1) and hacking(2)
      1. Watering Hole Attack → Malware infection targeted by the attack
      2. Theft of a valid digital certificate → Change the security SW installation file (so that the target installs the security software that contains the backdoor to the logged-in user)
    - Zero-day Attack/Exploit
      - Example: Internet Explorer has reached the end of support

Reviews of Main cyber threats (2024)

3

RANSOMWARE
Ooops, your files have been encrypted!
Your files will be lost
Time left:
59:59:59
Send $600 worth of bitcoin to this address:

- Advanced Ransomware Attacks
  - Methods of attack
    1. Data Encryption
    2. Leaking confidential materials and Threatening disclosure
    3. DDoS Attacks
  - LoTL(Living off the Land) <Latest>
    - Inability to distinguish between legitimate and attack traffic
    - Bypass security device detections → **Increase attack duration**

Expected Cyber Threats in Republic of Korea

- Evolving Attacks supported by Generative AI
  - Malicious generative AI models
    - FruadGPT(fraud)
    - WormGPT(Malware)
  - Deepfake
    - Synthetic technology that manipulates videos or images with artificial intelligence technology to make them look true

❖**Countermeasures**

✓ **'Secure by Design'**

✓ **Management of generative AI using monitoring system**

Expected Cyber Threats in Republic of Korea

2

- Vulnerabilities Attacks of Digital Convergence Technology
  - **Smart Airport**, Smart Grid, Smart Building, Smart Transport Systems, …
    - Target(s) : Various IoT devices
    - Attack Procedures
      - Malware infection on vulnerable devices → DDoS attacks + Botnet exploits

❖Countermeasures

✓**Secure by Design**

✓**ASM(Attack Surface Management)**

Expected Cyber Threats in Republic of Korea

3

- Critical Infrastructure Attacks by Cyber Terrorists
  - Hacktivist(Hacking + Activist)
    - Deepening global issues, wars, and political conflicts
    - Messaging through cyberattacks → **Social Disruption**
  - Theft of Intellectual Property Rights (IPR)
    - Quantum, Artificial Intelligence, Semiconductor, Battery, etc.
    - Primarily, it targets **Supply Chains** with a lot of security vulnerabilities

❖**Countermeasures**

- **Cybersecurity Management System / Cyber Risk Management Framework**
- **Cooperations between Civil and Military**

Expected Cyber Threats in Republic of Korea

4

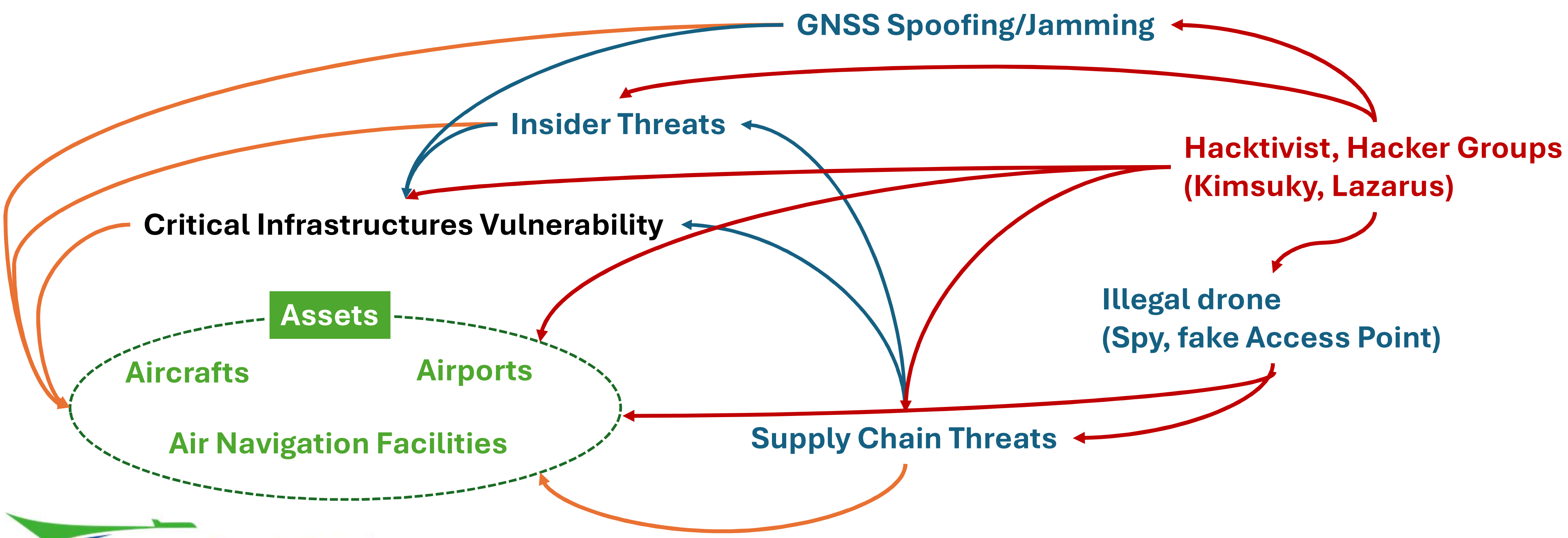
- Brute DDoS attacks
  - Generate network traffic at scale → **Service Outage**
    - Loss of confidence in the event of a
    - Economical damage
  - DDoS as a Service tool on sale on the dark web

❖Countermeasures

✓Operating DDoS cyber shelters

Aviation Cyber Threats in Republic of Korea

- Republic of Korea is **at the Forefront of Aviation Cyber Threats**



GNSS Spoofing/Jamming

Insider Threats

Hacktivist, Hacker Groups (Kimsuky, Lazarus)

Critical Infrastructures Vulnerability

Assets

Aircrafts

Airports

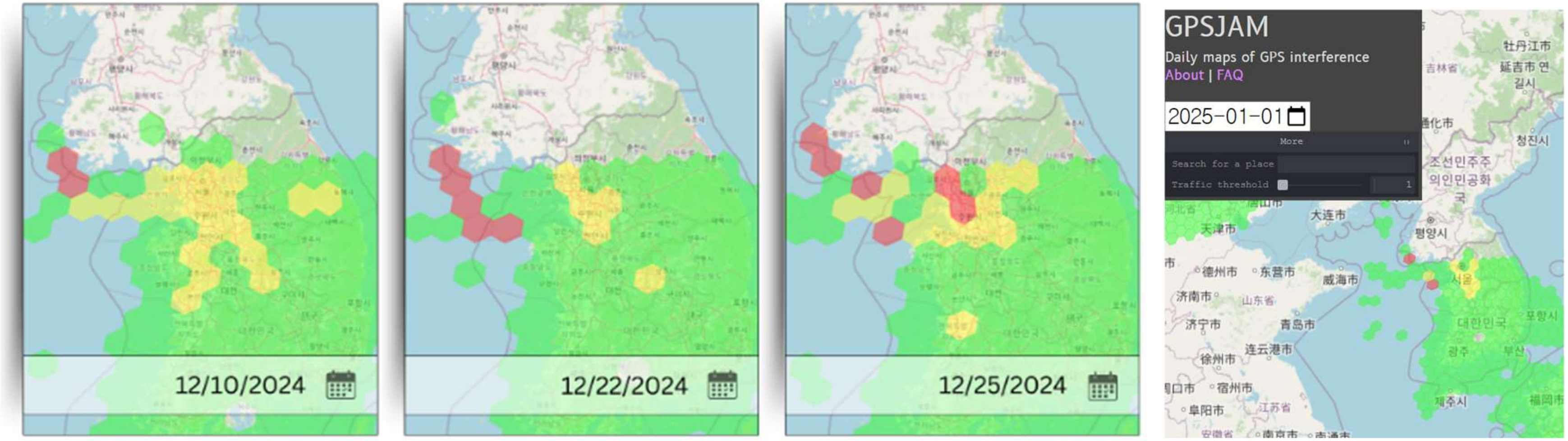
Air Navigation Facilities

Illegal drone (Spy, fake Access Point)

Supply Chain Threats

Aviation Cyber Threats Cases (2024)

- GNSS Spoofing/Jamming
  - Republic of Korea has been a **representative conflict zone** since 1950
  - GNSS jamming still occurs and has a weak impact on air navigation



12/10/2024

12/22/2024

12/25/2024

GPSJAM

Daily maps of GPS interference

About | FAQ

2025-01-01

More

Search for a place

Traffic threshold 1

Recurring jamming in the Korean Peninsula. Image source: gpsjam.org

Aviation Cyber Threats in Republic of Korea

- Theft of Intellectual Property Rights (Global Risk Score: High)
  - **Ransomware attack** impersonating a national aviation research institute
  - Many small and medium-sized companies have **been victims of theft of UAV design data (Supply Chain Attack)**
- Illegal drone and trash Balloon
  - Threat type: Using an Unmanned Aircraft System to Collide with an Aircraft (Global Risk Score: Medium-High)

Number of illegal drones detected (first half year)

2021	2022	2023
92	67	59

Fortunately, it is decreasing

North Korean balloons that landed in South Korea on May 29, 2024 (L) and South Korean authorities analyzing items that fell onto the streets of Seoul from North Korean balloons on June 1, 2024 | Image: ROK JCS | Images: ROK JCS

National Cybersecurity Strategy 2024

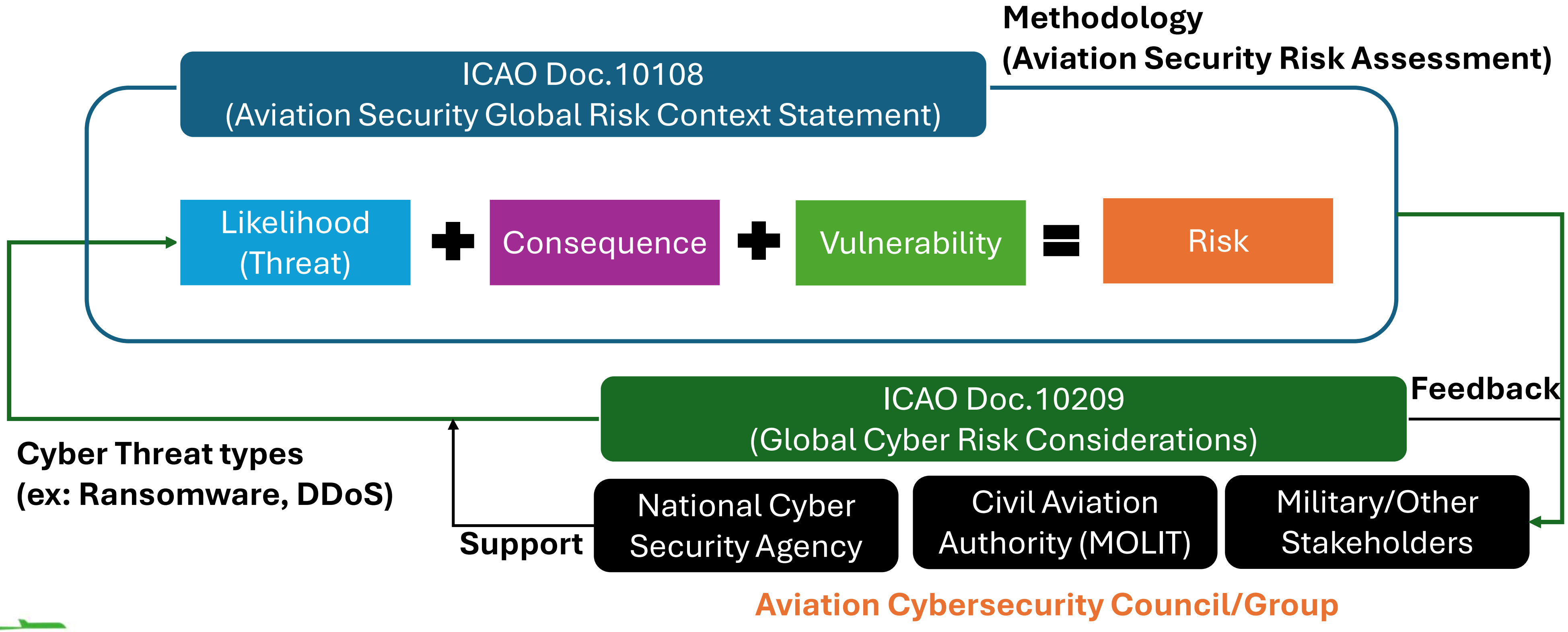
- Strengthening Offensive Cyber Defense Activities
- Establishing a Global Cyber Cooperation Framework
- Enhancing Cyber Resilience of Critical Infrastructure
- Securing a Competitive Edge in Critical and Emerging Technologies
- Strengthening the Operational Foundation

Aviation Cybersecurity Strategy in ROK

- **National Aviation Cybersecurity Strategy and Action Plan**
  - Harmonization between ICAO Aviation Cybersecurity and National Cybersecurity => **National Aviation Cybersecurity Strategy**
  - Developing Our Best Practices in Aviation Cybersecurity
  - Sharing case studies with ICAO, and supporting the development of ICAO guidelines, etc. (support to ICAO CyAP)

Aviation Cybersecurity Risk Assessment Framework

- Main flow



Methodology
(Aviation Security Risk Assessment)

ICAO Doc.10108
(Aviation Security Global Risk Context Statement)

Likelihood (Threat) ✚ Consequence ✚ Vulnerability = Risk

Feedback

ICAO Doc.10209
(Global Cyber Risk Considerations)

Cyber Threat types
(ex: Ransomware, DDoS)

Support

National Cyber Security Agency

Civil Aviation Authority (MOLIT)

Military/Other Stakeholders

Aviation Cybersecurity Council/Group

MOLIT
Ministry of Land,
Infrastructure and Transport

Thank you

Korea Institute of Aviation Safety Technology

KIAST will renew itself as a specialized institute dedicated to aviation safety that values the sky, people, and future.

[Q&A]

Donghwan Yoon (KIAST, Republic of Korea)

dh.yoon@kiast.or.kr

KIAST Korea Institute of Aviation Safety Technology