HANGAR 901
AIRCRAFT MAINTENANCE

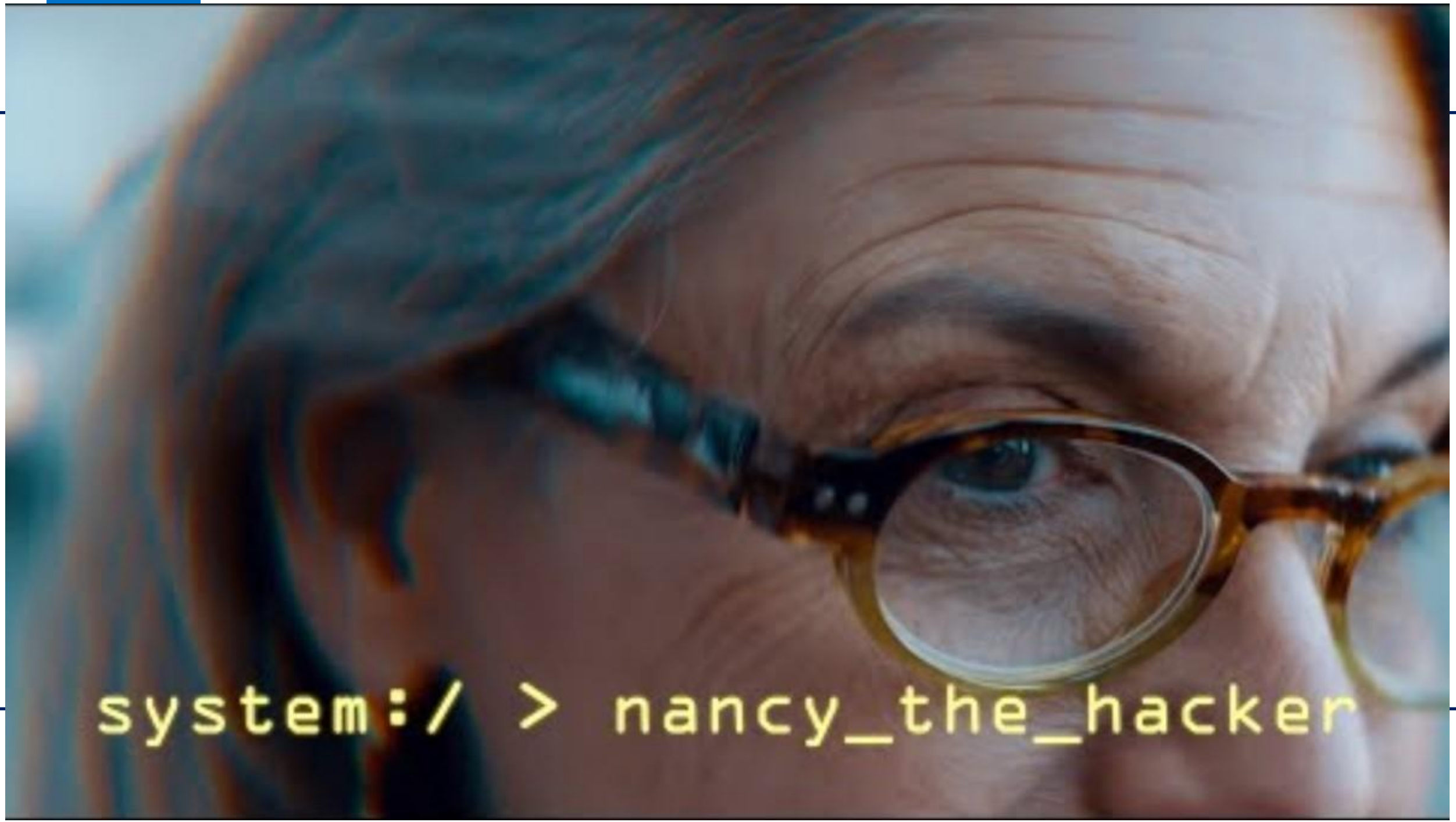
# CYBERSECURITY & CONFLICT ZONES: CASH, TRUST, COCKPIT

Santo Domingo, 5 May 2025 —
ICAO NACC/SAM Seminar

FLORIAN WAGNER, HEAD OF IT — HANGAR 901 AIRCRAFT MAINTENANCE

# Questions ?

- For any Questions during the Presentation Please scan the following QR Code


system:/ > nancy_the_hacker

# AGENDA

Hangar 901
05-05-2025

# Agenda

- Hook & context
- Examples Demo
- Background
- Bridge to Aviation
- Mitigations
- End

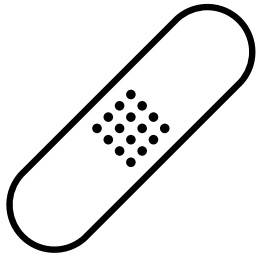
# HOOK & CONTEXT

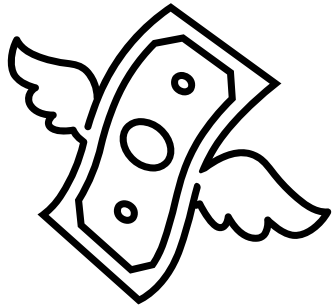
# From Wrenches to Wireless

- Yesterday’s toolbox:
  - paper logbooks
  - torque wrenches
  - slide rules
- In 2025 toolbox:
  - wireless **ACARS** uploads
  - predictive-maintenance dashboards
  - dashboards and digitally signed release certificates

# Why Everyone Should Care

- **$9.5 TRILLION**
  - Estimated global cyber-crime damage in 2024 (Cybersecurity Ventures)
- **$10.5 TRILLION**
  - Projected yearly damage by 2025
- **$4.88 M**
  - Average cost of a single data breach in 2024 (IBM)
- **+29 %**
  - Increase since 2015 when the average was $3.79 M (Inflation 2015-2025 30.79%)
- **One KPI**
  - Every dollar lost to cyber is a dollar not spent on safety – cash-flow & flight-safety now share the same metric



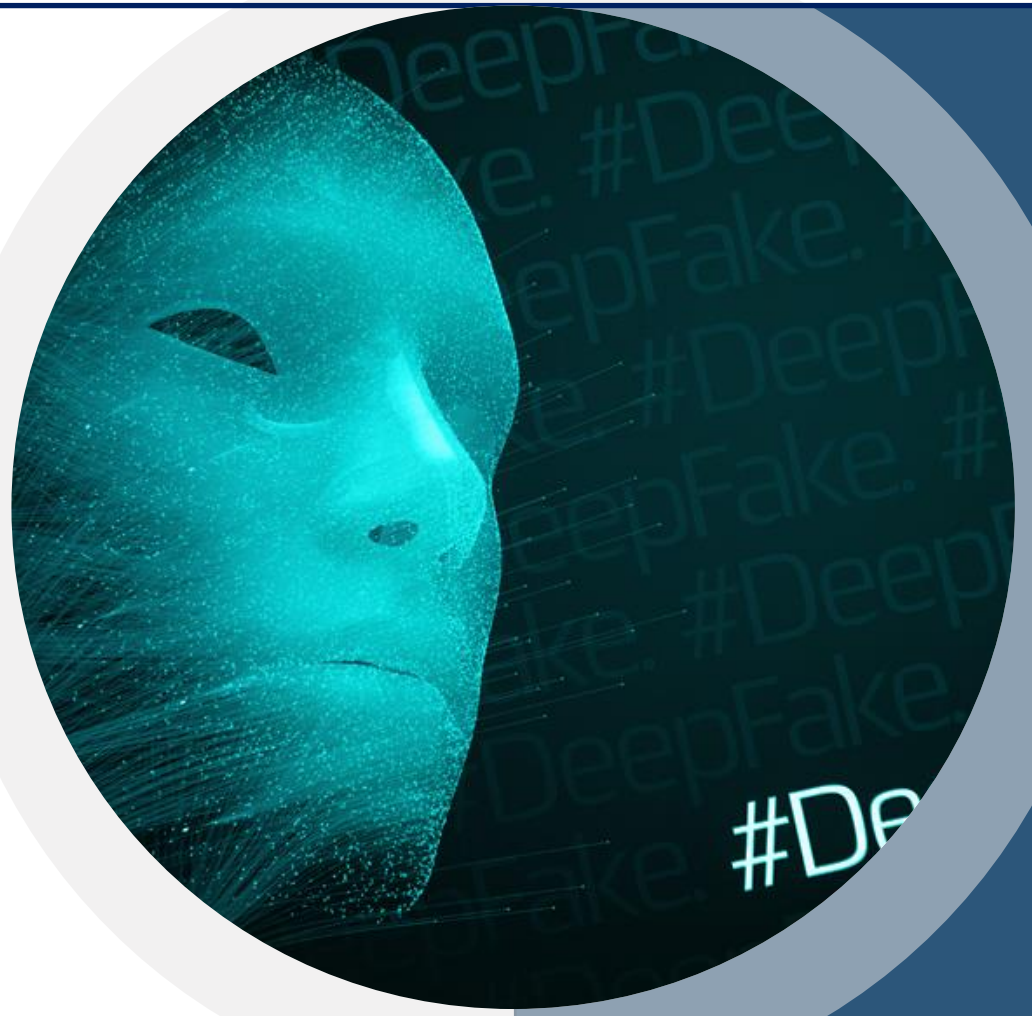


# Phishing & Business-E-mail Compromise

- Fake emails from someone pretending to be executives or trusted partners
- Employees tricked into sending money or sensitive data
- Often uses urgency and authority to bypass suspicion
- Many Different Specializations
  - Spear Phishing
  - Clone Phshing
  - Smishing (SMS Phishing) ……

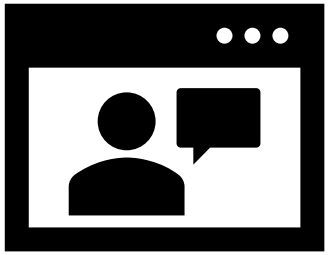
# Deep-fake Voice &Video

- Attackers use AI to create realistic fake voices and videos
- AI trained to mimic speech, mannerisms, and even writing style
- Growing rapidly as AI technology becomes widely accessible
- Gets more and more Difficult to detect



# Minimal Data Required for Deepfakes

- Voice Deepfakes:
  - **1–5 minutes** for a simple voice Clone
  - **15–30 minutes** for high quality for a convincing high-quality clone
- Video Deepfakes:
  - A single **photo or screenshot** from LinkedIn or other public profiles is enough for a basic video deepfake.
  - **1–2 minutes** of good video footage from platforms like Facebook or Instagram enables highly realistic deepfake videos



# Fake Vendor Invoices  Compromise

- Criminals send invoices that look like trusted supplier bills
- Carefully timed to coincide with expected payments or orders
- Employees inadvertently approve fraudulent payments
- Often includes subtle changes (e.g., bank account details)

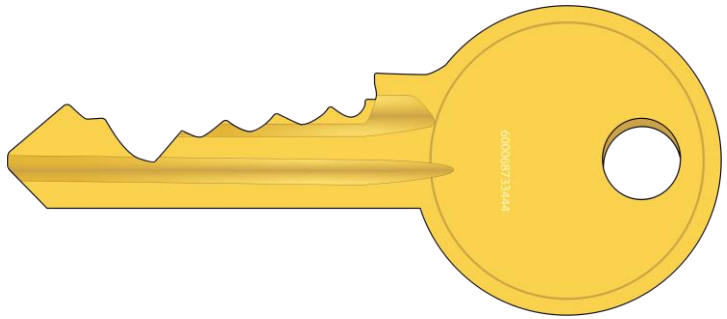
# Barrier to Entry for Deepfake Technology

- Easy Access:
  Deepfake software is freely available via open-source platforms like GitHub
- Low Cost for Voice Cloning:
  Effective AI voice-cloning hardware/software setup can cost as little as **$1,000 – $2,000**.
- Affordable High-Quality Video:
  Powerful, convincing video deepfake capabilities achievable for **$5,000 – $20,000**.



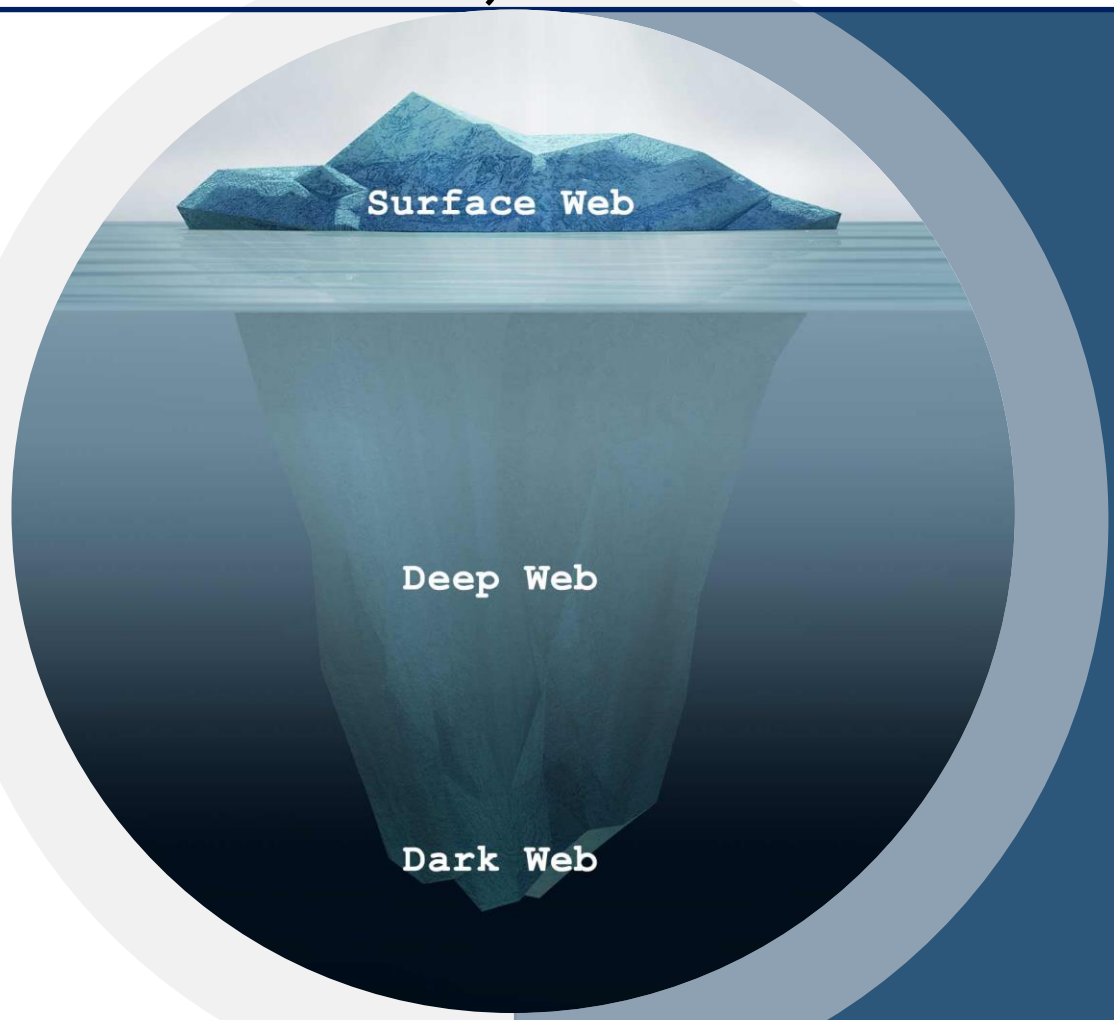

# Easy-to-use, "Turnkey" Deepfake Solutions

- E.g. User-Friendly Public Solutions (easy, widely accessible):
  - Cloud:
    - FakeYou
    - ElvenLabs
    - Synthesia
  - Mobile apps:
    - Reface
    - FaceApp
    - Zao



# Turnkey Professional Solutions (Accessible to Criminals Public &Dark Web):

- Dedicated Software Tools:
  - e.g. Deepfacelab (Pulblic Open Source)
  - e.g. Deepfacelive  (Public Open Source)
  - …….
- Criminal App / Services (Public / Dark Web):
  - Deepfake-as-a-Service
  - Marketplaces for Customized Impersonations Video and Voice Clips
  - Pre-trained AI models for specific celebrities or public figures (Public & Dark Web)



# EXAMPLE DEMOS

# Demo Osint

## Performed by Philippe Morio Icao

# Demo Fake Document

**Raising Awareness with Illustrative Fake Document Generation**

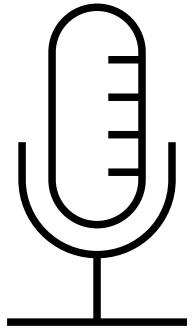
**Potential Counterfeit Documents**

- B1 / Form 1
- Certificates
- Invoices

- \+ Prompt Injection

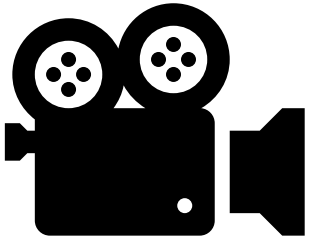
# Demo Voice Deepfakes & Training

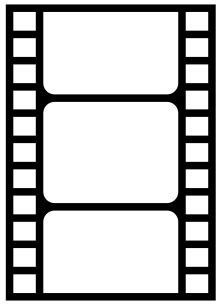
- Start with Source Material
- To Training Data
- To Training
- And Application
- Example Model
- Ussually a lot more Epochs are required



# Demo Visual Deepfakes & Training

- Start with Source Material
- To Training Data + Linked in
- To Training
- And Application
- Different ways that are possible
- Depends on your goal if you need a lot of Training or just one Screenshot





# Demo Deepfake Video Call

- Start a Demonstation wit a Fake video call via OBS Combination of
- Ussually you set the Settings so its lipp sinked (e.g. Teams Cal)


# HANGAR 901 AIRCRAFT MAINTENANCE

# Hangar 901 Aircraft Maintenance

- **Founded:**
  2008 (Originally HAITEC)
- **Certification:**
  EASA Part-145 Approved MRO
  - Line & Base Maintenance Services
  - And Wide Range of Approvals
- **Employees**: 500+
- **Main Facility:**
  Frankfurt-Hahn Airport (HHN)

# Hangar 901 Aircraft Maintenance

## Our Approvals

| | | |
|---|---|---|
| Cayman Islands<br>CAY-AMO-061219 | Aruba (DCA)<br>DL-ACC-170 | Sri Lanka (CAASL)<br>CAASL.145.254 |
| Bermuda (BCAA)<br>BDA/AMO/373 | USA (FAA)<br>HAIY901D | Kazakhstan<br>Recognition Letter |
| Azerbaijan<br>AZ.145R.0002 | Guernsey<br>2-REG.145.210 | UK (CAA)<br>UK.145.01406 |
| San Marino (CAA)<br>Information Circular No.1 | EASA (LBA)<br>DE.145.0427 | Canada (TCCA)<br>TCCA Approval 823-06 |
| Korea (MOLIT)<br>2025-AMO F01 | | |

# My Workplace & Job Role

- **Interests:**
  Aviation Space
  and Emerging IT Technologies
- **Current Role:**
  Head of Information Technology
  (Working in Hangar 901
  in different Roles since 2014 )
- **Education:**
  Bachelor's Degree in IT Business
  Management

# BRIDGE TO AVIATION

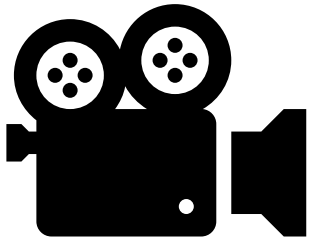
# From Cyber Fraud to Aviation Risk

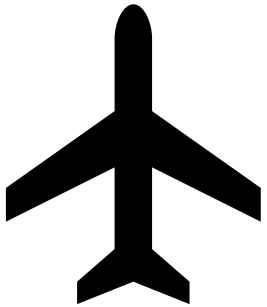
- Cyber incidents start with everyday office actions (emails , phone & video call, payments)
- Fraud creates initial trust breaches
- Trust breaches escalate into operational vulnerabilities
- Vulnerabilities lead directly into aviation safety risks

# How Cyber Fraud Enters Aviation

## Deepfake to Hangar — A Modern Attack Path

- A deepfake video call impersonates the Head of Maintenance or Quality:
  “Urgent situation—please fast-track this technician into the rotation for night shift.”
- HR sees a familiar face and voice, and grants access to a contractor based on the deepfake call
- The individual arrives with **forged B1 credentials** and is given MRO access
- He performs "authorized" work—potentially installing **counterfeit or tampered parts**

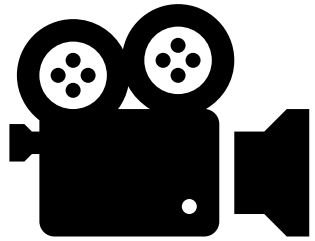


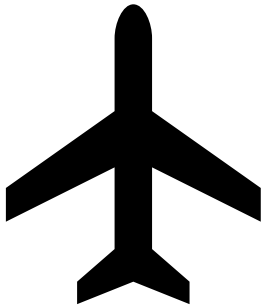


# How Cyber Fraud Enters Aviation

## Deepfake to Hangar — A Modern Attack Path

- The defect goes undetected, only to surface **mid-flight** or **during final approach**, especially critical near **conflict zones or complex airspace**
- **Root cause?** A deepfake bypassed all normal hiring and safety protocols by manipulating human trust



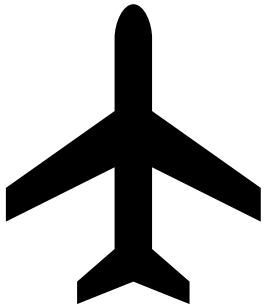


# Aviation-Specific Cyber Threats

## Cyber Threats Unique to Aviation

- Fake Aircraft Maintenance Licenses:
  Attackers can create realistic fake EASA B1 licenses using publicly available templates and identity data
  - These licenses are used to gain access and illegally sign off maintenance tasks
    Forged EASA B1 licenses used
    to sign off unauthorized maintenance
- Counterfeit EASA Form 1 Certificates:
  Digitally altered or cloned documents enable the installation of unapproved or tampered parts



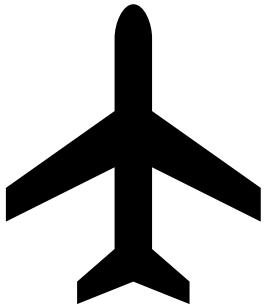



# Aviation-Specific Cyber Threats

## Cyber Threats Unique to Aviation

- Navigation Data Poisoning:
  - Malicious updates can be introduced via **legacy media** such as CDs, USB drives, or floppy disks—still used on older aircraft
  - These updates may contain **altered or corrupt navigation data**, undetected until flight
  - Attack vectors include:
    - **Manipulation during data delivery** – USB stick or media swap.
    - **Man-in-the-Middle attacks** – altering navdata files during upload or transfer
    - **Compromise of customer-facing update portals** – attackers tamper with data packages in supplier or OEM systems



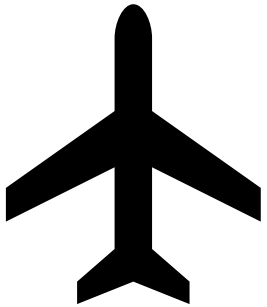



# Direct Safety Impact

## Realistic Aviation Risk Scenarios with Real Life Impact

- **Structural integrity compromised:**
  latent defects from fake licensed technicians
- **Flight path deviations:**
  navigation data tampering increases risks, especially near conflict zones
- **Operational chaos:**
  fleet groundings and mandatory inspections following fake parts discoveries
- **Physical threats:**
  targeted ADS-B tracking combined with public information leads to planned attacks



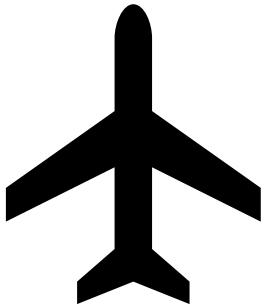




# MITIGATIONS

# Cybersecurity in Aviation: Not Optional !

- Cyber threats are not just IT problems — they impact flight safety and compliance
- ICAO and EASA have both published mandatory guidance:
  - ICAO Cybersecurity Strategy (2020)
  - EASA Part-IS
    (Information Security requirements for national authority's, operators and MROs)
- These are about protecting people, not just protecting data

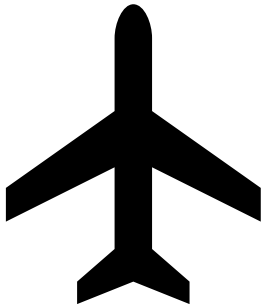


# Framework 101: What is EASA Part-IS?

- EASA Part-IS defines how aviation organizations manage information security risks and its impact on Aviation Safety
- It applies to airlines, maintenance orgs, and manufacturers in Europe
- It includes:
  - Staff clearance and training (IS.A.220)
  - Supplier oversight (IS.A.230)
  - Secure data exchange and storage (AMC1.IS.A.250)
- Think of it as the aviation version of a cybersecurity management system

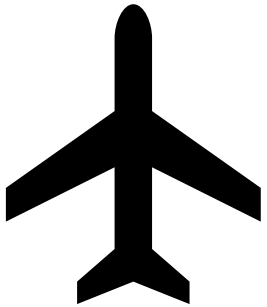


# Mitigation 1: Verify the Human

- Deepfakes can mimic voices and faces convincingly.
- Implement call-back procedures for any unusual or high-impact requests.
- Never approve access, hiring, or payments from an email or video call alone
- Frameworks:
  - ICAO Cybersecurity Principle 2: Human-Centric Defense
  - EASA IS.A.220 (Personnel Security)

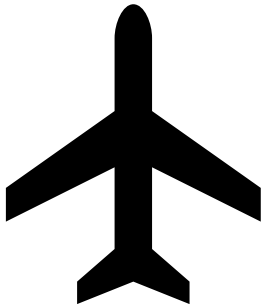


# Mitigation 2: Secure Documents and Data

- Use digital signatures and hashes to verify authenticity of:
  - Nav-data packages
  - Release documents (e.g., Form 1)
  - Work instructions or software updates
- Prevent media tampering during delivery (CD, USB, Lineflash)
- Frameworks:
  - ICAO Cybersecurity Action Plan
    Objective A3 – Enhance Protection of Critical Aviation Information and Systems

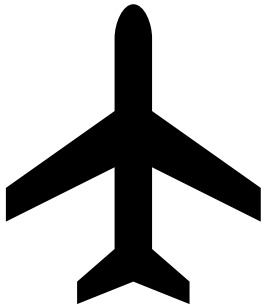


# Mitigation 3: Secure the Supply Chain – Trust, but Verify

- Revalidate all suppliers yearly — don’t trust old credentials
- Inspect digital certificates and contact lists
- Use separate VLANs and audit logs for maintenance access
- Frameworks:
  - ICAO Cybersecurity Principle 5: Collaboration
  - EASA IS.A.230 (Supplier Oversight)



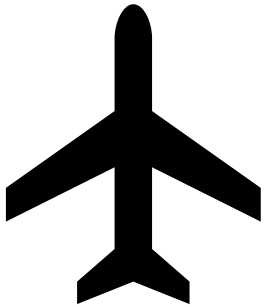



# Takeaway: What You Can Do

- **Raise cybersecurity awareness across all departments**, not just IT...
- Run interactive phishing simulations and deepfake response drills to strengthen awareness
- Offer classroom-based security training tailored to aviation-specific scenarios (e.g., ground ops, MRO, HR)
  (Integration into Onboarding Process)
- Leverage trusted guidance from:
  - ICAO Cybersecurity Strategy
  - EASA Part-IS regulations
  - National and regional aviation cybersecurity frameworks

Cybersecurity is no longer optional — it's a core part of safety culture in aviation



# END

# THANK YOU
# ANY QUESTIONS ?

HANGAR 901
AIRCRAFT MAINTENANCE

Hangar 901
05-05-2025