



Twenty Eighth Meeting of the Communications/Navigation and Surveillance Sub-group (CNS SG/28) of APANPIRG

WP/26

Strengthening Aviation Cybersecurity Through Organizing Attack-With-Defence Exercise

Presented by Hong Kong, China

Introduction

- **Alignment with the ICAO Aviation Cybersecurity Strategy – 7th Pillar**
- **“Capacity Building, Training and Cybersecurity Culture”**
 - Essential to raise awareness and emphasize that building cybersecurity culture is everyone’s responsibility

Introduction

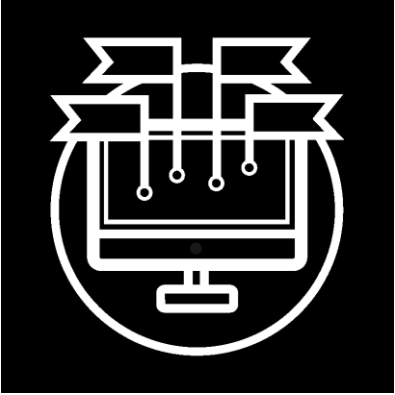
■ **Cybersecurity Landscape**

- Dynamic and evolving threats
- Importance of improving skills for emergency response

■ **Rationale for AWD Exercises**

- Provides real-world experience in handling actual cyber-attacks
- Strengthening cybersecurity personnel's understanding on attacker's mindset and skills

Introduction



Capture-the-Flag (CTF) competition

- ✓ Promote active participation and healthy rivalry
- ✓ Encourages taking timely action and decisive decision-making
- ✓ Active engagement lead to happy and productive learning process

AWD Exercise

- **March 2024 Event by Hong Kong CAD**
 - Collaboration with cybersecurity consultants



AWD Exercise

■ Team Composition and Competition

- Four teams from various divisions
- One-day pre-competition training on online platform utilising various tools



Competition Overview

Attack

Identify and exploit vulnerabilities in the virtual environments of other teams

Defence

Strengthen defences in your team's virtual environment

Earning points by capturing flags



Competition Question Types

■ Types of Challenges

Website Security Weaknesses

- Code injection
- File upload vulnerabilities
- Deserialisation problems

Program Manipulation

- PHP
- Java
- Python

Questions can be customised to match skill levels for effective learning.

Competition Stages

■ Stages of Competition

■ Reinforcement Stage

- Data backup, code auditing, vulnerability repair

■ Attack and Defence Stage

- Attacking other teams and defending own environment
- Importance of effective team coordination with duties segregated between attacking and defending

■ Visualisation and Engaging Engagement

- Real-time competition status and scoreboards



Conclusion

- With encouraging result, CAD plans to organise the AWD exercise regularly for both professional and general staff with different levels of complexity
- Participants feedback on AWD exercise benefits:
 - Bridging theory and practice
 - Preparing professionals for real-world cyber threats
 - Enhancing skills, adaptability, and teamwork
- Event Video

<https://www.cad.gov.hk/english/video/AWD.mp4>

ACTION BY THE MEETING

- Acknowledge the commendable efforts of Hong Kong, China in organizing the Attack-with-Defence (AWD) exercise in collaboration with cybersecurity consultants, to actively engage aviation professionals in offensive and defensive activities, helping participants develop critical skills, enhance incident response capabilities, and contribute to overall cybersecurity resilience;
- Seek assistance from ICAO APAC Office in organizing seminars/ workshops, bundled with similar AWD exercise, that facilitate the acquiring and sharing of experience in cybersecurity among States/Administrations and industry partners; and
- Encourage States/Administrations to collaborate effectively in addressing cybersecurity threats.



Thank you

