An Aviation Security View on RPAS

Steven R. Berti
Chief Aviation Security Policy
What will the warrior-guardian of the future look like?

Yo! Dude... Back here.
A World of Challenges

Is our recent experience with “multidiscipline” areas such as ATM and cybersecurity relevant?

Where should we focus our efforts?

Who are the right players?

What is the appropriate forum to address security aspects of RPAS?

Known vs. unknown: are we identifying all possible threats posed by the use of RPAS?
ANNEX 17 — SECURITY

- 9th Edition of Annex 17 incorporates Amendments 1 to 14
- Amendment 12 introduced ATM and cybersecurity provisions
- Amendment 14 became applicable in Nov. 2014
  - ensure a risk-based cybersecurity regime
A Brief History of Time – Part I: Policy

- **ATM security to be included in next Amendment to Annex 17**
  AVSECP/18 (Sept 2006)

- **Working Group on Threat and Risk established**
  AVSECP/19 (May 2008)

- **Amendment 12 to be developed**
  AVSECP/20 (April 2009)

- **ATM and Cybersecurity provisions!**
  (applicable July 2011)

- ✓ Implementation of security measures by air traffic service providers
- ✓ Protection of ICT systems used for civil aviation purposes
A Brief History of Time – Part II: Guidance

Cross-reference approach

Security Manual
- Physical protection
- Access control
- Security control for staff
- Basic cybersecurity measures

ATM Sec Manual
- Protection of ATM systems
- Support of the ATM system to others engaged in aviation security

Common elements

Doc 8973
Aviation Security Manual

Doc 9985
Air Traffic Management Security Manual

Doc 10019
MANUAL ON REMOTELY PILOTED AIRCRAFT SYSTEMS (RPAS)
A Collaborative Endeavour

Ongoing work on cybersecurity capitalizes on collaboration between WGTR, ANB Technical Panels, AVSEC Panel, ECAC Task Force and IHLG (ACI, CANSO, IATA, ICAO, ICAO)…more?

For example: IHLG Action Plan
The Way Forward

• Continuous collaboration with all entities involved in RPAS matters (and ATM and cybersecurity?) - to enable ICAO to create synergy and develop further standards, guidance material, and training.

• Technical panels of ANB and AVSECP can be used for communication, cooperation and collaboration by all entities involved (coordination mechanism).

• Duplication of work by different entities should be avoided.