ICAO Cyber Summit and Exhibition
Dubai 4th – 6th April 2017

The work of the ICAO Threat and Risk Working Group

Phil Williams
UK Department for Transport &
UK rep on the ICAO Threat and Risk Working Group
Contents

• Principles
• ICAO TRWG - background
• Definitions
• Formula and scoring
• Process
• 2016 Results - overview
• Cyber work
• Next steps
Principles

• Focus on terrorism
• Fundamental need to assess the size and nature of malicious threats
• Needs to be done logically, constantly, consistently and comprehensively
• Risk management approach (NOT elimination)
• Must consider Likelihood, Consequences, Mitigations & Vulnerabilities to assess Residual Risk
• Scenario (target, MO, perpetrator) based
• Inform “acceptability” debate and Av Sec response
Threat And Risk Working Group (TRWG)

- Established in 2009
- Open to all Member States to contribute
- Meets twice yearly
- Produces and maintains risk matrices
- Annual Risk Context Statement (RCS)
- Ad hoc reports e.g. on landside security as necessary
- Recommendations for possible amendments, mainly for Annex 17 – cyber may go wider
Formula

- Not precise mathematical exercise but relative ranking of risks
- Likelihood $\times$
  Consequences of that attack $\times$
  Mitigations against (Vulnerability to) that attack $=$
- Residual Risk $=$ the remaining problem
Scoring

• Each element scored on a 5 point scale of:
  – Low;
  – Medium-Low;
  – Medium;
  – Medium-High; and
  – High

• Definitions in the RCS – best fit applies

• Results available to all ICAO States in RCS

• Global ICAO view (methodology and results) for Member States to build upon
Concerns Identified
From the RCS, ICAO, and other intelligence sources

Threat Development
Identify targets and means and methods of attacks

Likelihood
of the threat occurring

Consequences
of the threat succeeding, including estimated economic, political, human, and psychological impacts. Estimate the reasonable worst case scenario

Current Countermeasures
Consider adequacy and appropriateness of current security measures in place

Remaining Vulnerabilities
Determine the vulnerability remaining when all existing countermeasures have been considered

Residual Risk

Adequately/Acceptable
Mitigated Risk
No action required until next review/risk assessment

Inadequately/Unacceptable
Mitigated Risk
Further evaluation of security measures required

Implementation
of revised security measures as proposed by:
- AVSEC Panel
- Other ICAO bodies
- Member States
General considerations

• What does “cyber” mean?
• Availability, integrity and/or confidentiality of data and therefore systems that carry that data
• Inadvertent impacts from attacks on other sectors
• Aims: disruption, destruction, distraction, degradation and/or denial of service
• Facilitation (for other types of attack)
• Links: physical and cyber security; external and internal perpetrators; safety and security; developers/ manufacturers, suppliers and operators
• Plausible scenarios – spoofing (covert, credible corruption) and jamming (overt denial)
• Likelihood – LOW (broad intent but capability lacking other than for limited, “basic” attacks)
• Consequences – HIGH (reasonable worse case in busy airspace of collisions and loss of aircraft)
• Vulnerabilities – MEDUM-LOW (technical, safety, human mitigations)
• Residual Risk - LOW
### Results – 2016

<table>
<thead>
<tr>
<th>THREAT TYPE</th>
<th>RESIDUAL RISK</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERSON-BORNE IED carried on the person or in cabin baggage</td>
<td>HIGH</td>
</tr>
<tr>
<td>ManPADS (in combat or proliferation zone)</td>
<td>MEDIUM-HIGH</td>
</tr>
<tr>
<td>IED In cargo</td>
<td>MEDIUM-HIGH</td>
</tr>
<tr>
<td>LANDSIDE THREATS</td>
<td>MEDIUM-HIGH</td>
</tr>
<tr>
<td>IED in hold baggage</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>VEHICLE-BORNE IED</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>ManPADS (non-proliferation or conflict zone)</td>
<td>MEDIUM-LOW</td>
</tr>
<tr>
<td>AIRBORNE THREATS – aircraft used as a weapon</td>
<td>MEDIUM-LOW</td>
</tr>
<tr>
<td>IED in services (catering, IFS etc)</td>
<td>MEDIUM-LOW</td>
</tr>
</tbody>
</table>
# Results – 2016

<table>
<thead>
<tr>
<th>THREAT TYPE</th>
<th>RESIDUAL RISK</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIRBORNE THREATS - Remotely Piloted Aircraft Systems</td>
<td>MEDIUM-LOW</td>
</tr>
<tr>
<td>AIRBORNE THREATS – conventional hijack</td>
<td>LOW</td>
</tr>
<tr>
<td>CYBER Attacks</td>
<td>LOW</td>
</tr>
<tr>
<td>Chemical, Biological, Radiological threats</td>
<td>LOW</td>
</tr>
</tbody>
</table>
Risk assessments never stay still

Greater awareness

Skilled insiders?

Increasing vulnerabilities:

- greater reliance on and criticality of information systems
- increasing inter-connectivity within the aviation sector
- Increasing use of external data sources e.g. internet, COTS equipment, remote software updates etc
- Greater connectivity of E-enabled aircraft
- Retro-fitting
Ongoing cyber work

Split into three areas:

1. Aircraft and ATM interface systems
2. “Other” aircraft systems
3. Airport systems
Aircraft and ATM interface

Three specific but interconnected areas

- Communications: data and voice;
- Navigation: GNSS/GPS, FMS, ILS/MLS, en route and terminal navigation systems; and
- Surveillance: consideration of systems based on 1030 and 1090 MHz – SSR, WAM, MLAT, ADS-B & ACAS which support ATC functions

Eurocontrol leading initial review of 2014 work
Other aircraft systems

- 3 domains;
  - Aircraft control systems – critical systems in the cockpit environment
  - Cabin operational systems
  - Cabin passenger systems e.g. in-flight entertainment
- Being arranged on the basis of air worthiness functionality e.g. provision and control of engine thrust. First draft being completed by Boeing, Airbus and EASA
Airport systems

Two broad categories:

• a potential facilitation activity e.g. bt degrading IT-based aviation security measures such as access control and screening; and

• disruption of operations (departure control, baggage handling etc) – part of operational resilience and business continuity rather than conventional aviator security
Next steps

• Further international SME meetings to be held in May and June
• ICAO TRWG next meeting 11\textsuperscript{th} – 13\textsuperscript{th} July in Paris
• Further TRWG meeting in November
• Aim to have first two blocks of work completed by 31\textsuperscript{st} December 2017 in time for 2018 RCS
Questions & comments?