VULNERABILITY VERSUS THREAT: RISK-BASED MITIGATION

Session 2

VULNERABILITY VERSUS THREAT: RISK-BASED MITIGATION

Mr. Jean-Philippe Morange

Senior Legal Officer, Counter-Terrorism Committee
Executive Directorate, United Nations

Activity 2.1

The Unpredictability Game

Facilitator:

Mr. Florin Hungerbühler

Inspector, Security, Federal Office of Civil Aviation, Switzerland

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of the
Environment, Transport, Energy and Communications DETEC

Federal Office of Civil Aviation FOCA

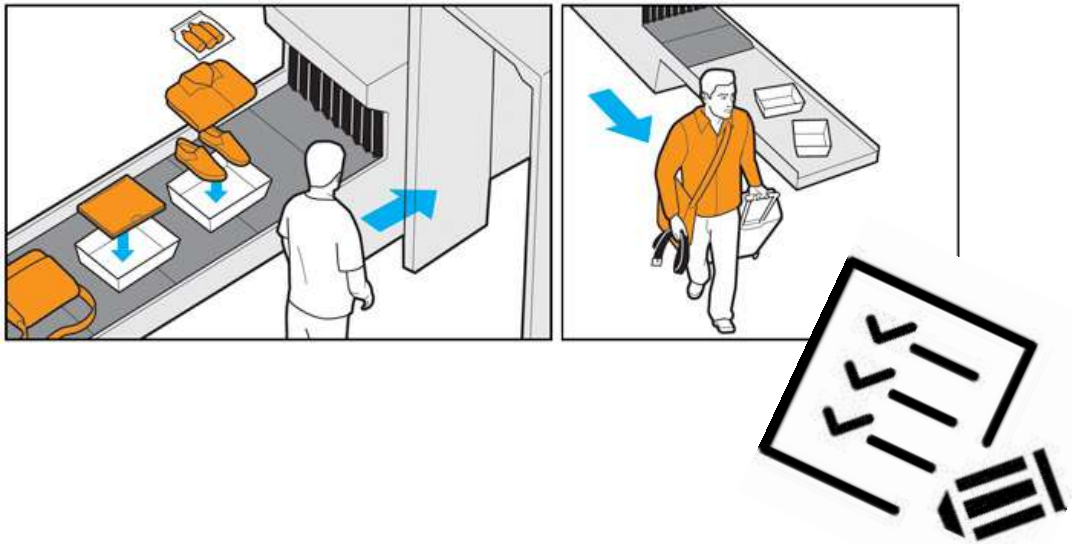
Unpredictability-Game

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of the
Environment, Transport, Energy and Communications DETEC

Federal Office of Civil Aviation FOCA

Predictability



- Uniform
- Harmonized
- Comparable
- Measurable

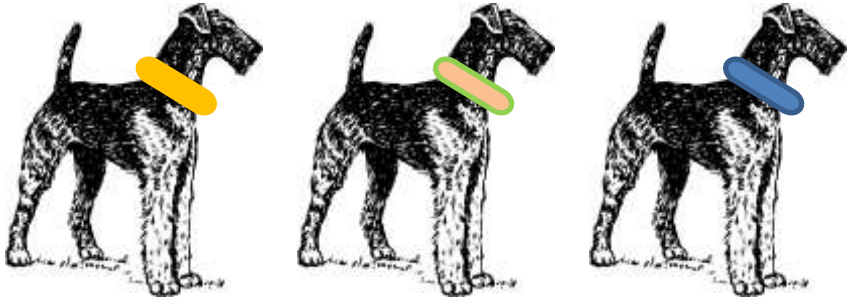
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of the
Environment, Transport, Energy and Communications DETEC

Federal Office of Civil Aviation FOCA

Unpredictability

- Randomness
- Alternation
- Different time, area / location, means
- Different stakeholders
- Surprises

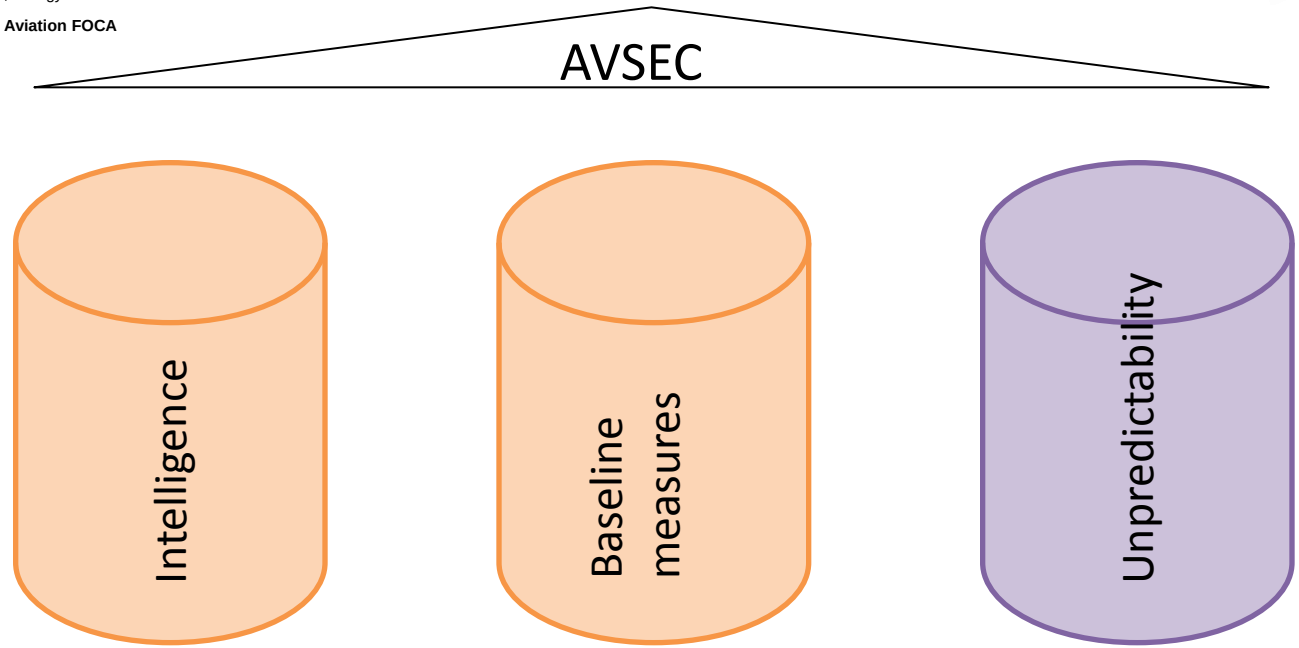


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of the
Environment, Transport, Energy and Communications DETEC

Federal Office of Civil Aviation FOCA

Unpredictability

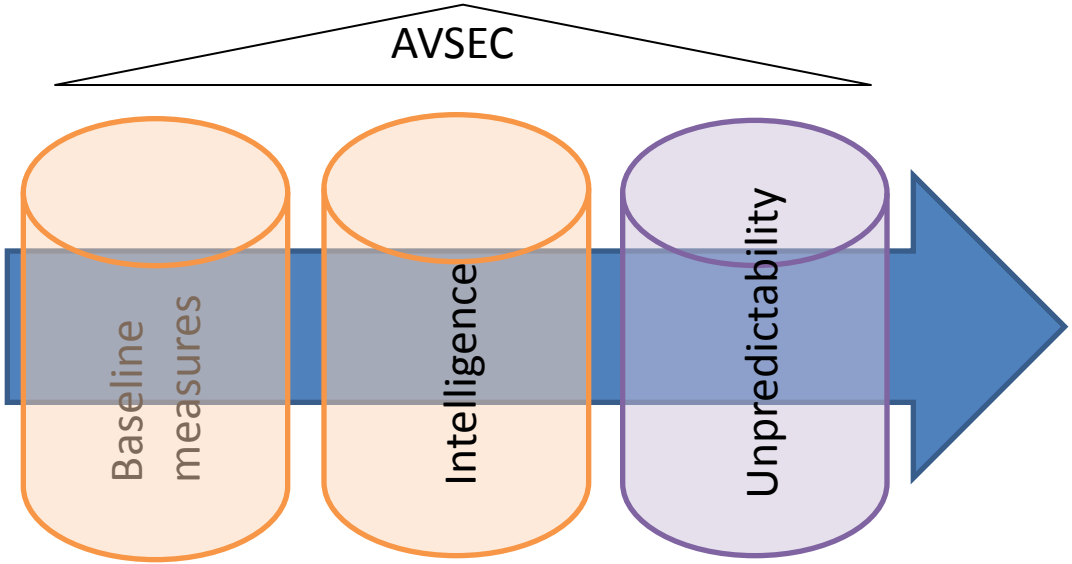


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of the
Environment, Transport, Energy and Communications DETEC

Federal Office of Civil Aviation FOCA

Unpredictability



Process-oriented security measures, often static and uniform

Outcome-oriented and risk-based security measures, flexible and adaptive

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of the
Environment, Transport, Energy and Communications DETEC

Federal Office of Civil Aviation FOCA

Unpredictability-Game

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of the
Environment, Transport, Energy and Communications DETEC

Federal Office of Civil Aviation FOCA

Unpredictability-Game

- Round 1: Predictable — Goal: 
- Round 2: Predictable — Goal: 
- Round 3: Unpredictable — Goal: 
- Round 4: Unpredictable + Compensation — Goal: 
- Round 5: Unpredictable + Countercompensation — Goal: 

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of the
Environment, Transport, Energy and Communications DETEC

Federal Office of Civil Aviation FOCA

Conclusions

- Predictable = Task can be solved easily

- Unpredictable = Heigthened complexity;
  more resources needed to solve the task;

  uncertain prospect of success.

Unpredictability

Advantages of applying unpredictable measures can include:

- flexible, effective and efficient use of resources
- possible synergies between different entities
- hostile reconnaissance and plotting disturbed; more complex and demanding
- addressing the «insider threat»
- staff motivation

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of the
Environment, Transport, Energy and Communications DETEC

Federal Office of Civil Aviation FOCA

Unpredictability

«… unpredictability as a way to guarantee and strengthen security.» [Nuclear security authority, Ministry of Energy, France]

«… malicious software assumes your computer will operate in a certain way, so why not confuse it and be unpredictable.» [University of Florida]

Activity 2.2

Risk Model

Mr. John Velho, Chief, Screening Oversight and International Operations, Transport Canada

Mr. Phil Williams, Risk Assessment and Incident Response Team, Department for Transport (DfT), United Kingdom

Content

- Principles
- ICAO TRWG
- Definitions
- Formula and scoring
- Threat Scenario
- Questions

Principles

- Fundamental need to assess the size and nature of malicious threats
- Needs to be done logically, consistently, comprehensively and constantly
- Risk management approach (NOT elimination)
- Must address Threat Likelihood, Consequences, Mitigations & Vulnerabilities to assess Risk
- Threat scenario based (target, adversary, MO)
- Inform “acceptability” debate and aviation security response

Threat and Risk Working Group (TRWG)

- Established in 2009
- Established risk assessment process
- 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

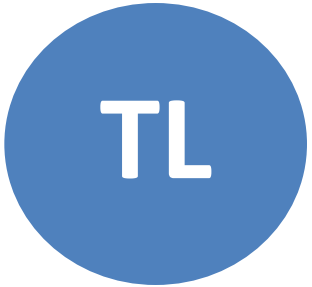
Risk Inputs

Threat scenario

- Identification and description of a credible act of unlawful interference comprising a target, the means and methods of an attack (modus operandi), and the adversary

Threat Likelihood

- The probability or likelihood that an act of unlawful interference is attempted, based on an adversary's intentions and capabilities but NOT taking into account current security measures



Consequence

- The reasonable worst case outcome of an act of unlawful interference, in human, economic, and disruption of services terms

Current Mitigating measures

- Measures in place to reduce the likelihood and consequences of successful attack
- Include all measures relevant to the scenario (international, national and local) to deter, detect, and prevent an attack and may be:
  - physical
  - procedural
  - personnel
  - IT/cyber security etc.

Vulnerability

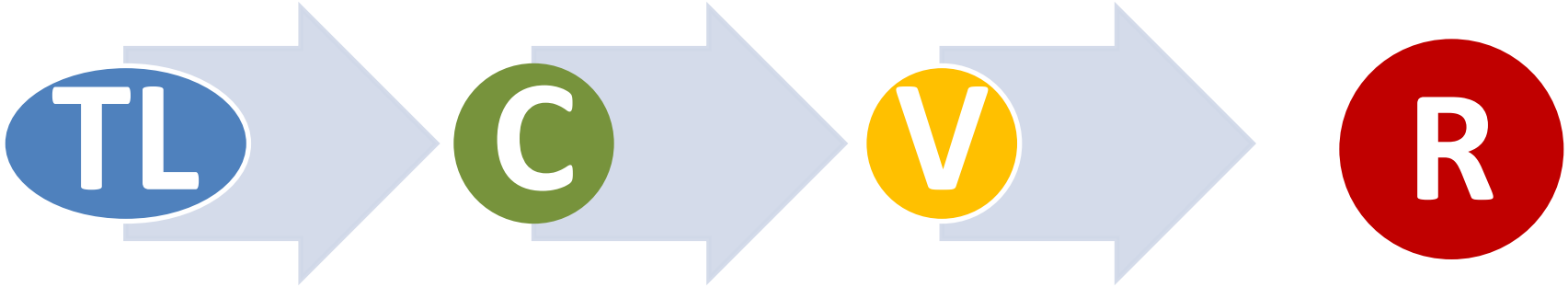
- Inadequacies and/or characteristics of a system/asset that could permit an act of unlawful interference
- Current mitigations must be identified and their effectiveness assessed in order to identify vulnerabilities

Risk

- Probability of an act of unlawful interference being successfully carried out on a specific target, based on an assessment of threat likelihood, consequence, and vulnerability

Formula

- Not precise mathematics but relative ranking of risks



Scoring

- Each element of the threat scenario (Threat Likelihood, Consequences and Vulnerabilities and therefore Risk) scored on a 5 point scale
- Definitions in the RCS – best fit applied
- This is the flexible element as other scoring systems can be used

Scoring:
High
Medium-high
Medium
Medium-low
Low

Threat Scenario Development

- Target: The location or objective where or against which an attack will take place (Ex: Aircraft, Landside)
- Adversary: The person or role that is attempting to conduct an attack (Ex: Passenger, Insider)
- Modus Operandi: How the adversary will instigate an attack (Ex: IED, Gun), and How the adversary gets the weapon to the target (Ex: On the Body, Hold Baggage, Accessible Property), and By which path an adversary reaches the intended asset (Ex: via Passenger Checkpoint, via Perimeter Breach)

Threat scenario example

Threat scenario	Methodology (description of methods)
Passenger-borne low, non-metallic Improvised Explosive Device (IED) detonated on a passenger aircraft	Target/Asset: passenger aircraft Adversary: Passenger Modus Operandi: IED concealed in an electrical item in cabin baggage, solid explosive, low metal content, reaching the target via normal passenger pathway (e.g., through security checkpoint)

Threat/Likelihood RCS scoring

For probability:	
High	A very plausible scenario, with an actual attack of this kind having occurred in the past few years, or strong evidence of capability, intent, and planning
Medium-high	A clearly plausible scenario, with relatively recent examples or evidence of early attack planning or hostile reconnaissance
Medium	An essentially plausible scenario, with some evidence of intent and capability and possibly some examples, but no evidence of current attack planning
Medium-low	A scenario for which there are no, or no recent, examples, but some evidence of intent, yet with a method apparently not sufficiently developed for a successful attack scenario or probably superseded by other forms of attack
Low	A theoretically plausible scenario but with no examples or signs of attack or attack planning, and a theoretical intent but no apparent capability

Consequence RCS scoring

Potential Consequences of the Event			
Consequence	**Human**	**Economic**	**Other**
Low	Possibly some deaths and injuries	Some economic impact	Some disruption to services and confidence in the aviation system
Medium-Low	Some but not all of the MEDIUM consequences below		
Medium	Tens of deaths	Tens or hundreds of millions of dollars	Substantial disruption to services and confidence in the aviation system
Medium-High	Some but not all of the HIGH consequences below		
High	Hundreds of deaths	Billions of dollars	Severe disruption to services and confidence in the aviation system

Vulnerability scoring

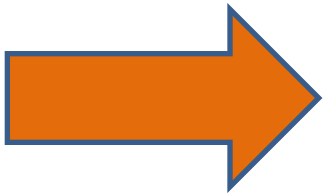
Vulnerability	
High	No mitigating measures are in general effect, either because there is no Annex 17/national programme requirement or because no realistic effective measures are available
Medium-high	Mitigation has a limited scope and that important areas and aspects of the risk are not covered by Annex 17/national programme requirements or measures in general effect
Medium	Features of both MEDIUM-HIGH and MEDIUM-LOW are present
Medium-low	Mitigating measures are generally in place, but they may be immature or only partially effective. For instance, the broad Annex 17/national programme requirements may be in place for all areas and aspects, but they are capable of being further developed or better implemented in practice
Low	Clear Annex 17/national programme requirements exist and that mitigating measures generally regarded as effective are in widespread use

Risk Scoring

T L
H
MH
M
ML
L

C
H
MH
M
ML
L

V
H
MH
M
ML
L

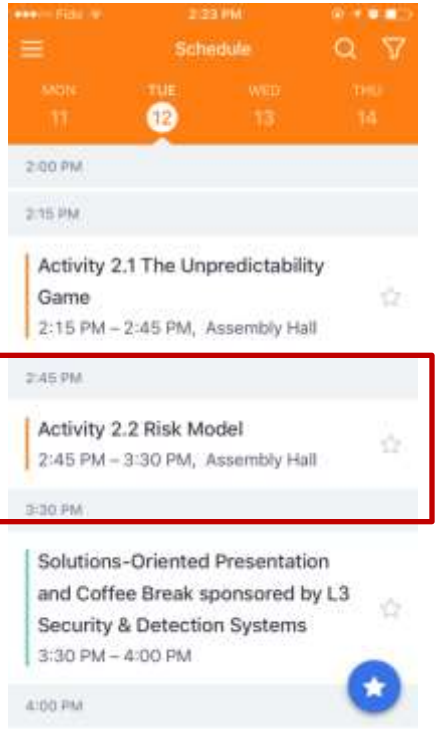


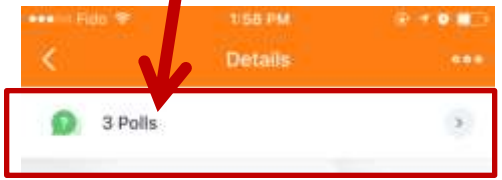
R
H
MH
M
ML
L


ICAO
AVSEC
2017

Conduct the Activity

- Scroll to and select “Activity 2.2 Risk Model”
- Select Polls and answer the questions





Plenary 2

Emerging Threats: Cybersecurity, RPAS, IEDs/PEDs and the Unknown

Moderator:
Mr. Mark Rodmell
Representative of the United Kingdom on the Council, ICAO

Panellists:

- **Ms. Leslie Cary**, Remotely Piloted Aircraft System (RPAS) Programme
- Manager, ANB, ICAO
- **Mr. Daniel Johnson**, Director, National Aviation Intel Integration Office, US
- **Ms. Sonia Hifdi**, Chair, ICAO AVSECP Task Force on Improvised Explosives Device and Head, Security, Directorate General for Civil Aviation (DGAC), France
- **Mr. Nico Voorbach**, Director, ICAO and Industry Affairs , Civil AirNavigation Services Organization
- **Mr. Yan Li**, Vice Director General, Aviation Security Bureau, Civil Aviation Administration, China

ICAO AVSEC 2017

ICAO Global Aviation Security Symposium

ICAO

In collaboration with ACI AIRPORTS COUNCIL INTERNATIONAL

RPAS and Security

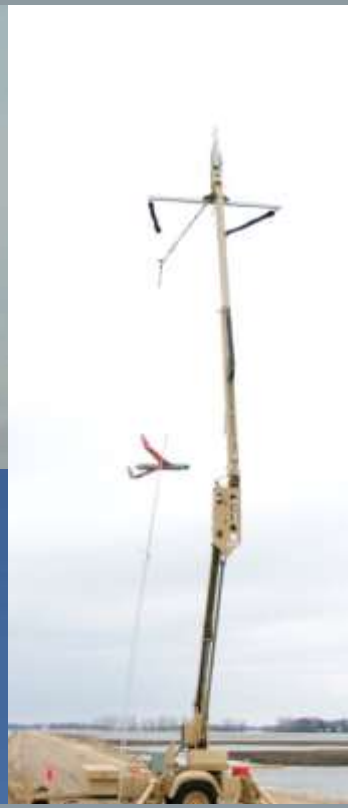
Leslie Cary
ICAO RPAS Programme Manager
12 September 2017

ICAO AVSEC 2017

ICAO Global Aviation Security Symposium

ICAO

In collaboration with ACI AIRPORTS COUNCIL INTERNATIONAL



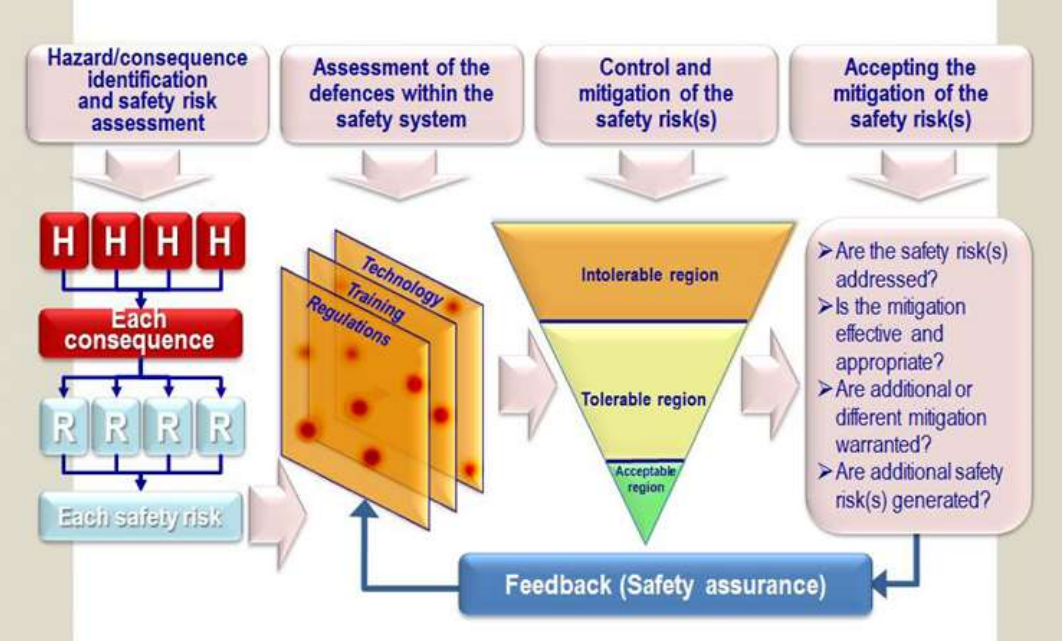

BDB


G-EZMB

The Drone Market Environment 2016

DRONEII.COM

Operation-centric, risk-based approach



Two Approaches – Two Streams of Work

RPAS

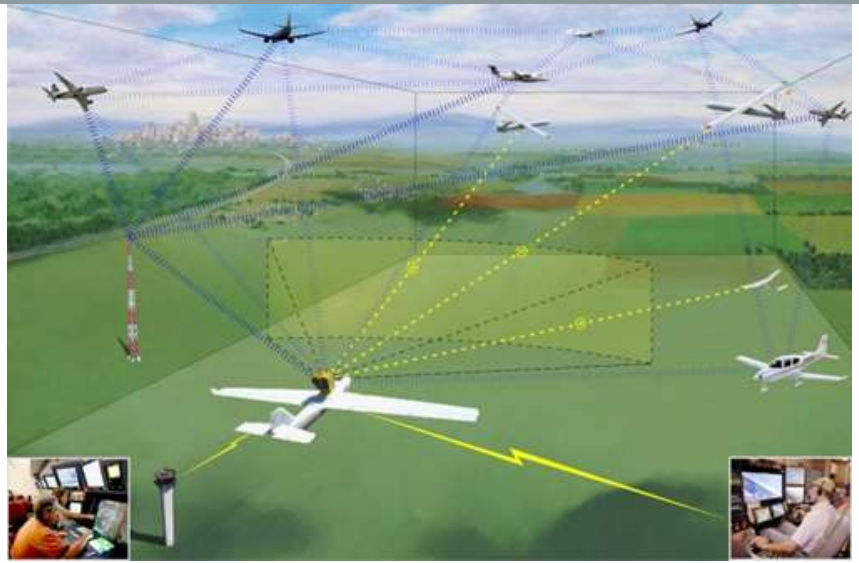
Full aviation regulatory approach

Other UAS

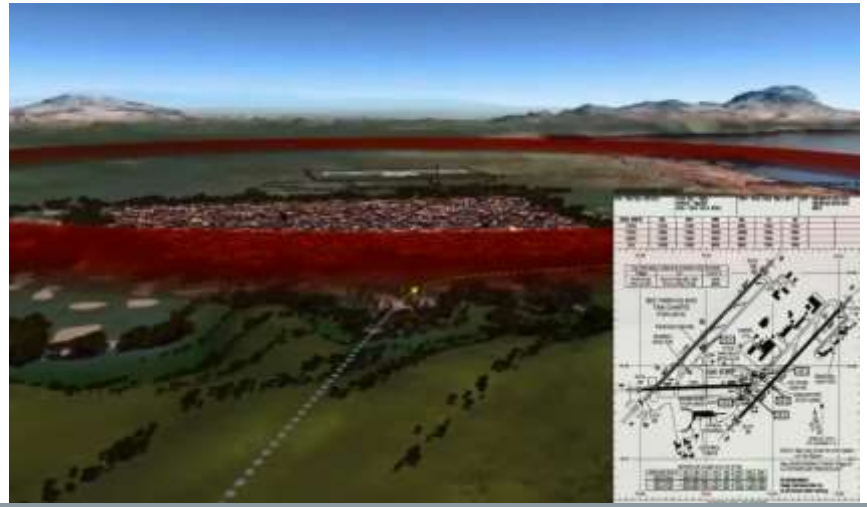
- UAS Toolkit
- UTM
- Registration
- Network deliveries

UA versus RPA

- Unmanned aircraft include:
  - Free balloons
  - Model aircraft
  - Remotely piloted aircraft
    - Airspace/aerodrome integration requires control
    - Control, in real time, provided by a licensed remote pilot
  - Drones



RPA vs Drone



Security challenges for RPAS

- RPAS are new actors in Civil Aviation World
- They have the same challenges as others users
- PLUS……

Security challenges for RPAS

- This new system is split in 3 parts RPA, RPS and C2 Link
- RPS may exist in various forms and types
- C2 Link conveys all data; disruption can pose serious risk

Security challenges for RPAS

- RPAS security challenges require:
  - holistic approach
  - cooperation and coordination with others bodies


THANK YOU!

Plenary 2

Emerging Threats: Cybersecurity, RPAS, IEDs/PEDs and the Unknown

Mr. Daniel Johnson
Director, National Aviation Intel Integration Office, USA

Plenary 2

Emerging Threats: Cybersecurity, RPAS, IEDs/PEDs and the Unknown

Ms. Sonia Hifdi
Chair, ICAO AVSECP Task Force on Improvised Explosives Device and Head, Security
Directorate General for Civil Aviation (DGAC), France

SWIM and security: CANSO perspective

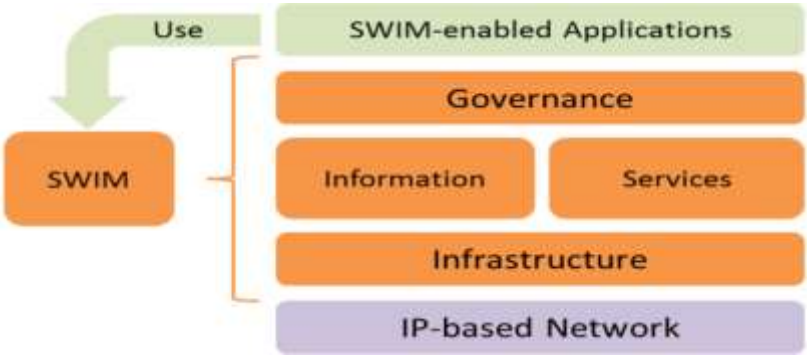
Nico Voorbach
Director, ICAO Affairs

TRANSFORMING
GLOBAL ATM PERFORMANCE

AVSEC2017 12-14 September 2017

FOREWORDS

"SWIM consists of standards, infrastructure and governance enabling the management of ATM-related information and it exchange between qualified parties via interoperable services" ***(ICAO DOC 10039 SWIM Manual)***



INTEROPERABILITY

A KEY ROLE FOR SECURITY

- Security will become a critical factor, therefore the global SWIM concept encompasses aspects such as authentication, authorization, encryption, intrusion detection, security policies, etc. ***(ICAO Doc 10039)***
- Information Security pillars: → confidentiality, Integrity and Availability must be addressed in the whole lifecycle
- "Security by design", in the light of Annex 17 Amd 16 standard 4.9.1 and RP 4.9.2

CANSO POSITION

- Security plays a transversal roles in any part of the SWIM concept, mainly in the “infrastructure” and “governance” layers
- Not a vaccine; it must be permanently addressed through the entire lifecycle:
  - to ensure the security of SWIM components (data and systems) so that they are protected from interference and access to them is restricted only to those authorized
  - to ensure the security management measures for SWIM are risk based, sustainable, appropriate and referred to existing yet standards/best practices in order to meet regulatory compliance, due diligence and to safeguard the continuity of service from acts of unlawful interference

CANSO POSITION – HOW TO?

- KEYWORD: → standardization: using the existing standards/best practices, do not reinvent the wheel. Security is a “globalized factor”
- Learning from our experiences;
- “Best practices” and “standards” are terms of reference for measuring **diligence, prudence and duty of care**;
- Harmonization;
- Common evaluation metrics;
- Meeting fair competition needs;
- Common language;

ESTABLISHING A COMMON «SECURITY POLICY»

- In the SWIM environment the “security policy” is a bit more than “what shall we do to protect the information stored on computers”
- In a multilayered scenario, with huge complexity and criticalities, an effort is required in order to:
  - declare the commitment and make it effective
  - define rules, responsibilities, and the main constituents of the architecture, encompassing human factor, procedures, technologies
  - set the appropriate objectives of the overall strategy fitted for SWIM purposes

URGING FOR A RISK BASED APPROACH

- Reflect on the needs for a risk based approach, to avoid useless effort, to determine what is the risk to manage and to orient the investment, the activities and the operations
- Provide a rationale for determining the actions of the security management system to be implemented
- Common agreed metrics
- Suitable for accountability

REQUIRING THE LEGAL FRAMEWORK ADAPTION

- Focus on the trans-boundary nature of SWIM;
- Consider the need to involve non-aviation actors (third parties such as TELCO services providers, outsourcers, etc.);
- Define roles, responsibilities and accountability;
- Coordinate with cybersecurity initiatives at Regional and Member States level;
- Avoid duplications

KEEPING IT SHORT AND SIMPLE

- Defining the need for a “SWIM Security Management System”, with a methodological and measurable approach (e.g. ISO 27001);
- Security is not only a matter of IT but involves the whole organisation;
- Select the appropriate measures aimed at protecting the relevant/critical assets (including information, systems and personnel);
- Means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be administrative, technical, management, or legal in nature;
- Focus on Human Factor.

CONCLUSIONS

CANSO believes:

- Security must be addressed in any phase of SWIM development and in operations
- SWIM is the future for aviation efficiency. A security Management System is mandatory
- Security is not only matter of technological improvements,
  - implies a holistic approach
  - including procedures
  - and human factor
- COMMITMENT REQUIRED

Thank you!

CANSO ICAO and Industry Affairs
1 Place Ville Marie (Suite 2901)
Montreal, QC
H2X 0E9 Canada

Tel: +1 514 448 5565
Cell: +1 514 449 6199
email: nico.voorbach@canso.org

Plenary 2

Emerging Threats: Cybersecurity, RPAS, IEDs/PEDs and the Unknown

Mr. Yan Li
Vice Director General, Aviation Security Bureau
Civil Aviation Administration, China