International Civil Aviation Organization

HLCAS/2-WP/2
23/8/18

**WORKING PAPER**

**SECOND HIGH-LEVEL CONFERENCE ON AVIATION SECURITY (HLCAS/2)**

**Montréal, 29 to 30 November 2018**

**Agenda Item 2: Future approaches to managing aviation security risks**

# IMPROVING AVIATION SECURITY RISK MANAGEMENT

(Presented by the Secretariat)

**SUMMARY**

In order to improve aviation security risk management throughout the international system, a comprehensive approach is required which ensures the promotion of an effective security culture across all aviation entities, appropriate risk reduction strategies and crisis response plans, mechanisms to address evolving threats, and the sharing of threat information by States to improve their security posture.

Action by the High-level Conference on Aviation Security is in paragraph 4.

## 1. INTRODUCTION

1.1 Aviation security faces an increasingly complex risk environment, and aviation systems remain a high risk target for terrorists. With increasing security measures, it may be more difficult to execute certain types of attacks, but terrorists still aim to achieve as high levels of death and destruction as possible.

1.2 For the purpose of this paper, aviation security "risk" is the probability of an act of unlawful interference being successfully carried out on a specific target, based on an assessment of threat, consequence, and vulnerability; and "risk management" is a systematic approach to determining the best course of action in an uncertain environment and making decisions based on cost-benefit considerations in an acceptable way. Both risk assessment and risk management help identify potential threats to civil aviation and prioritize actions to address these threats. In particular, a strong risk management aims at risk reduction strategies by: identifying risks to an airport and its operations; ensuring that mitigating actions and capabilities are addressed nationally and locally; and developing operational requirements that will mitigate the risk.

## 2. ENHANCING RISK MITIGATION STRATEGIES

### Promoting security culture

2.1 Criminals and terrorists seek to exploit the weakest link in the aviation system and benefit from existing vulnerabilities in an organization. Some of the principal vulnerabilities in the aviation sector are found at the employee level. In order to mitigate a broad variety of threats related to human factors, it is essential for States to establish and sustain a robust security culture within all aviation organizations.

2.2 Security culture can be described as a set of customs shared by a community, both as a mindset and the general application of operational processes to maintain security. Its intent is to capitalize on shared resources and avoid the need to develop individual problem-solving methodologies. A successful security culture will encourage best practices, break down operational silos, and facilitate the sharing of information, where practical. A robust security culture will also contribute to the prevention of acts of unlawful interference.

2.3 Every actor in the aviation security system needs to understand their role within the system and the associated requirements and responsibilities. A general understanding of security risks, risk assessments and management, combined with sector and function-specific training, will lead to greater awareness of existing and developing vulnerabilities. This can only be achieved through continuous and structured training that acknowledges and recognizes individual roles and responsibilities. Also important is a top-down promotion of an appropriate security culture.

2.4 Establishing an effective security culture, especially among those engaged in security-sensitive functions, is particularly crucial for mitigating insider threats. Personnel can be informed of risks through regular briefings on threats and wider security issues, can be trained to identify anomalous or suspicious behaviours, and should have access to a clear process for reporting any concerns. Employees are a valuable source of information on vulnerabilities and how to address them, and their input should be sought and used whenever possible in the assessment and management of insider risks.

**Tools to manage aviation security risk**

2.5 ICAO's Working Group on Threat and Risk (WGTR) assesses current risks and evolving and emerging threats to aviation based on analysis from reported incidents, intelligence and law enforcement sources, and transforms such risk data into information contained in the ICAO Aviation Security Global Risk Context Statement (RCS) to help decision-making by States and entities. The information in the RCS and from other sources also provides the basis for the development of new or amended Standards and Recommended Practices (SARPs) and guidance material and provides a description of the methodology used by the WGTR that States can implement for local risk assessments.

2.6 In addition, the following tools are made available by ICAO to assist States in assessing aviation security risks: ICAO *Aviation Security Manual* (Doc 8973, Restricted); ICAO MANPADS Information and Airport Vulnerability Assessment Guide (MANPADS Toolkit); ICAO Acts of Unlawful Interference Database (AUID); and ICAO Aviation Security Risk Management Workshop. The ICAO Aviation Security Risk Management Workshop is an intensive capacity-building activity that operationalizes the aviation security risk assessment methodology promoted both in the RCS and the ICAO *Aviation Security Manual* (Doc 8973, Restricted).

2.7 Furthermore, open-sourced information gathering is based on the analysis of available data from a vast array of sources, including from government, private and public sources, and may be structured or unstructured in its format. Smart data analysis (automated data analysis) combines the different types and source of data and can provide an analyst with the tools to appropriately manipulate the data in order to detect anomalies at an early stage, before they may even become a real threat.

2.8 ICAO has begun to implement data-driven risk management in the safety domain (such as iStars and the Safety Information Monitoring System) as it has been a long standing practice in Safety Management Systems. Law enforcement, security and intelligence services around the world have started to adopt similar approaches of data driven security risk management. An appropriate application and implementation of smart data security management would greatly contribute to a variety of ICAO internal initiatives, and help ICAO to support Member States in similar aspects.

**Fostering resilience of aviation security systems**

2.9 Resilience in aviation security can mean ensuring appropriate countermeasures are in place when an incident takes place and recognizing the value that exercises can bring to ensuring well-executed recovery plans. A major transition in the international community's response to incidents is a shift from a culture of reaction to one of prevention. The intent is to facilitate the vital role of civil aviation in responding to emergencies; to assist States in taking a more proactive role to identify risks and vulnerabilities in their civil aviation infrastructure; and provide assistance to States in building resilience into their aviation systems.

2.10 Resilience building of the aviation security system is based on the proactive identification of threats and vulnerabilities to support the development of appropriate mitigation mechanisms. It must be recognized that effective resilience further lies in the capability to isolate an affected system, and continue with normal, or close to normal, operation in the remainder of the aviation system. Such capability may need to include aspects of risk communication strategies and building of redundancy and contingency mechanisms.

## 3. ADDRESSING NEW AND EVOLVING THREATS

***Chemical, Biological and Radiological***

3.1 Addressing new and evolving threats to civil aviation such as those posed by Chemical, Biological and Radiological (CBR) agents presents unique challenges. First, most current aviation security measures are not specifically aimed at the detection or prevention of CBR attacks. Second, while banning the carriage in the aircraft cabin of certain substances is an option that could be considered, effective detection is likely to be challenging given the wide range of agents that could be used and considering that only small amounts are required to inflict mass fatalities and/or economic damage. Third, it is critical that States, international organizations and industry share with ICAO any information on viable and effective measures capable of mitigating the CBR threat, as it would greatly facilitate the development of a global and harmonized framework of mitigation measures – an approach that proved to be successful in addressing the liquids, aerosols and gels (LAGs) issue in 2006.

3.2 In scenarios where prevention of CBR attacks with current baseline measures may be unlikely, emergency procedures are important in limiting the consequences of the attack. Accordingly, ICAO has recently published new guidance material on the response to CBR incidents on civil aviation facilities, via the ICAO-NET as per Electronic Bulletin 2018/27, dated 11 June 2018. This document will continue to be refined, in consultation with experts from other disciplines, and will subsequently include response mechanisms to CBR incidents on board aircraft.

***Remotely-piloted aircraft systems***

3.3 The ICAO WGTR continues to assess risks related to remotely piloted aircraft systems (RPAS). Smaller RPAS are now widely used for both commercial and recreational purposes. To date, the major concern for civil aviation arises from the reckless use of drones in airspace around airports, which, although it may cause safety and operational implications, is more likely to occur through ignorance than for malicious reasons. The risk continues to evolve as the technology develops, including possible mitigation methods. To date, the WGTR has assessed only attacks using smaller RPAS, which are freely available and now very widely used, whereas larger RPAS are currently much more difficult to acquire – though these may create significantly higher risks if they were to become available to terrorist organizations.

***Cyber***

3.4 ICAO established the Secretariat Study Group on Cybersecurity (SSGC) in August 2017. The SSGC has formed several working groups (Current and Future Air Navigation Systems, Airworthiness, Aerodromes, and Legal Aspects) with a view to addressing all elements of the international aviation framework that may be affected by cyber incidents. The SSGC will coordinate the work of these groups so that any required cybersecurity provisions they propose are developed in a harmonized and coordinated fashion to ensure global interoperability and compatibility while maintaining required levels of safety and security.

3.5 Besides the in-depth work needed to address all issues in relation to cybersecurity, there is an urgent need to establish a high-level framework that raises States' awareness of cybersecurity and enables coordinated and harmonized action towards cybersecurity management. This notion was reinforced through the Dubai Declaration of 2017 and the Bucharest Communique of 2018.

3.6 Central to developing a cybersecurity strategy for the 40th Session of the ICAO General Assembly is the possible creation of a Cybersecurity Panel to bring together expertise from States, regional and international organizations, as well as industry. This structure would enable States to assign appropriate resources and make experts available in the relevant field.

3.7 Furthermore, the cybersecurity strategy will be based on the following elements, which will be integrated appropriately:

- Recalling States' responsibility to address system-wide cybersecurity at the legislative level;
- Providing and promoting existing guidance material developed by States and industry aimed at improving cybersecurity in all domains; and
- Reinforcing the need for the exchange of cybersecurity relevant information and best practices among States and industry.

## 4. ACTION BY THE HIGH-LEVEL CONFERENCE

4.1 The High-level Conference on Aviation Security is invited to:

a) urge States to continue to promote a security culture to foster effective national aviation security systems;

b) recognize the importance of increasing resilience of, and maintaining public confidence in, the aviation system;

c) endorse the ICAO strategies in addressing threats such as RPAS and CBR;

d) request States to share with ICAO cybersecurity best practices and cyber threat information, including indicators of compromise, techniques and procedures used by threat actors as well as incident analyses in order to better identify, assess, monitor, and respond to such threats; and

e) recognize the usefulness of data driven security risk management and requests ICAO to start exploring the possible implementation of such systems.

— END —