International Civil Aviation Organization

A39-WP/175
EX/64
09/08/16

WORKING PAPER

ASSEMBLY — 39TH SESSION

EXECUTIVE COMMITTEE

Agenda Item 16: Aviation Security – Policy

CIVIL AVIATION CYBER-SECURITY: POSSIBLE ACTIONS BY REGULATORS AND STAKEHOLDERS

(Presented by Argentina, Belgium, France, Guyana, Lao People's Democratic Republic, Namibia, Nauru, Nepal, Netherlands, Nigeria, Republic of Moldova, Russian Federation, Saint Lucia, Saudi Arabia, Senegal, Sierra Leone, Singapore, South Africa, Switzerland, The former Yugoslav Republic of Macedonia, Trinidad and Tobago, United Arab Emirates, and United Kingdom)

EXECUTIVE SUMMARY

Cyber-threats to the civil aviation system are a major concern for all stakeholders globally. It is crucial that the ICAO, aviation security authorities, aviation industry, and other civil aviation stakeholders collaborate to raise awareness of the threats, and develop practical and sustainable policies, approaches and measures, including in the area of training and capacity-building, to protect against them and mitigate their impact. Given the interdependence of the various parts of the global civil aviation eco-system, close coordination is essential to address these challenges.

Action: The Assembly is invited to:

a) note the contents of this paper, especially the possible actions by regulators and stakeholders to address cyber-threats to civil aviation operations;
b) urge the ICAO to establish a global framework for cyber-security for civil aviation stakeholders; and
c) identify a body within the ICAO to work on the global framework and for coordination with other relevant ICAO bodies and other stakeholders.

Strategic Objectives:	This working paper relates to Strategic Objectives A – *Safety*, B – *Air Navigation Capacity and Efficiency*, and C – *Security and Facilitation*
Financial implications:	No additional financial implications.
References:	A39-WP/14, *ICAO Comprehensive Aviation Security Strategy (ICASS)* A39-WP/15, *Establishment of a Global Aviation Security Plan* A39-WP/16, *Consolidated statement of continuing ICAO policies related to aviation security* A39-WP/17, *Addressing Cyber-security in Civil Aviation* Assembly Resolution A38-15, *Consolidated statement of continuing ICAO policies related to aviation security* AVSECP/27 Restricted (Yellow Cover) Report (*English only*)

1. INTRODUCTION

1.1 Cyber-threats to the civil aviation system have been recognised as a major concern, as in other sectors. There are numerous pathways for terrorists and persons with malicious intent to conduct cyber-attacks against civil aviation service stakeholders and their infrastructure. They can cripple civil aviation operations, including by hacking into aircraft navigation and control systems; interfering with radar and communications systems; and corrupting various airport systems. Although most such attacks against the aviation sector to-date have been low-level with limited impact, a cyber-attack against civil aviation operations could potentially be catastrophic with significant casualties, disruption to civil aviation services, and/or damage to critical infrastructure. These concerns are compounded by the fact that airlines, airports, air navigation service providers, and other stakeholders (e.g., ground handling companies; maintenance providers; security service providers; fuel companies; cargo agents; etc.) are increasingly reliant on information communications and technology (ICT) systems for their operations.

2. EFFORTS TO ADDRESS CYBER-THREATS

2.1 Civil aviation stakeholders have been paying more attention to cyber-threats in recent years. In 2014, the ICAO, International Air Transport Association (IATA), Airports Council International (ACI), Civil Air Navigation Services Organization (CANSO), and International Coordination Council of Aerospace Industries Associations (ICCAIA) issued a joint action plan to address these challenges. The IATA also developed a cyber-security tool kit for airlines, while many airports, air navigation service providers, and aircraft manufacturers undertook various measures to strengthen the security of their operations against cyber-threats.

2.2 At the international level, civil aviation security regulators have addressed cyber-security issues at the ICAO Aviation Security Panel (AVSECP). The AVSECP Working Group on Threat and Risk (WGTR) has presented a series of assessments and advice to the Panel on the risk of cyber-attacks, and coordination between the AVSECP and the relevant ICAO Safety Panels was initiated in order to streamline efforts on this horizontal topic.

2.3 Despite these actions, many stakeholders are still trying to grapple with the challenges. Raising awareness and promoting dialogue among stakeholders on cyber-threats would be useful in helping to increase understanding. Conducting detailed risk assessments will allow stakeholders to identify the security gaps so that the necessary steps can be taken to plug them. In July 2015, Singapore organised a cyber-security conference in partnership with the ICAO and IATA and supported by various States and industry stakeholders, which brought together experts across the civil aviation eco-system to discuss cyber-threats. The participants included airport operators, airlines, aircraft engine manufacturers, ground handlers, security service providers, security equipment providers, international civil aviation related organizations, and regulators. Some key issues discussed were:

a) The threats and risks posed by cyber-attacks to the global civil aviation system: the periodic assessments by the WGTR of these threats and risks can be used by the ICAO and stakeholders to develop effective preventive and response measures;

b) Considerations regarding preventive measures, response, as well as contingency and recovery actions in the event of a cyber-attack against civil aviation operations;

c) Actions that some stakeholders had undertaken to address cyber-threats;

d) That the civil aviation sector is particularly at risk, because cyber-attacks are more likely to be successful in a sector whose component parts are highly interdependent, and also because the cyber-defence mechanisms currently possessed by the civil aviation sector are not yet adequate to deal with this rapidly evolving threat; and

e) The need for a horizontal approach encompassing the entire aviation sector to ensure coordinated, proportionate, and effective implementation.

3. POSSIBLE ACTIONS BY REGULATORS AND STAKEHOLDERS

3.1 A number of possible actions by regulators and stakeholders were identified, including:

a) Urgently assigning responsibility for the issue, starting at the **global level**, where it would be useful for the **ICAO to establish a global framework for civil aviation stakeholders to address cyber-threats**. This framework, which should be based on existing best practices in information security and developed in close consultation with aviation security and aviation safety experts, could contain a set of principles, guidelines, and approaches for regulators and industry.

b) **At the State level, it is important for aviation security authorities (in coordination with other authorities responsible for cyber-security at a national level) to develop and provide regulatory oversight to deal with cyber-threats**. The regulatory oversight regime should cover the civil aviation sector and all players in the civil aviation eco-system from a holistic perspective, given their interdependence.

c) **At the individual stakeholder level, each stakeholder needs to establish its own set of actions to protect its operations against cyber-threats, especially for systems with relevance to aviation safety and security**.

d) Stakeholders need to respond to cyber-threats as early as possible. It is therefore important for the civil aviation sector **to develop measures for early detection, coordination, and swift remediation**. Reporting of cyber-security incidents to computer emergency response teams (CERTs) or information sharing and analysis centres (ISACs) would provide early warning to other stakeholders, and should be encouraged nationally with international coordination led by the ICAO.

e) As cyber-security is driven by both threat evolution and new technology trends, **people, process, technology, and systems must be brought together to ensure that there is capability in each of these for identifying and mitigating the threats**.

f) **Sharing of information and best practices amongst agencies on civil aviation cyber-security is essential**. This will help States and stakeholders to jointly and collectively detect trends, identify threats, and develop effective counter-measures. It is also important for intelligence and other relevant agencies to continue efforts to develop a better understanding of cyber-threats to civil aviation.

g) Given the interconnected nature of civil aviation information systems, **a common understanding of which systems and data are critical or essential for the safety, security, and continued operation of the civil aviation system is needed**. Aviation regulators should jointly determine criteria for systems to be deemed critical (from the global, regional, and/or national perspectives), in order to guide implementation.

h) **Training civil aviation personnel across the civil aviation eco-system to be aware of the threats and risks posed by cyber-attacks, and to respond quickly and appropriately, is important**. Detecting anomalies and raising the alert early on any suspicious developments or activities could prevent or contain a cyber-attack and help minimise disruption to operations. Including cyber-security challenges in aviation security training programmes, as well as recruiting aviation security specialists and auditors who are familiar with cyber-security, is important.

i) **Enhancing the aviation security culture to include a greater appreciation of cyber-threats will also be important**. If top management embraces the need to address these threats and lends strong support for training of personnel and investment in resources to deal with them, the civil aviation sector will be able to address them more effectively.

— END —