ICB
Industry Consultation Body

Industry Developments in ATM Cyber-Security

October 2016

Issue

Information Paper

Industry Developments in ATM Cyber-Security

In Q3 2015 the ICB's position paper on the regulatory response to ATM Cyber-Security was formally adopted at the plenary of ICB/57. The ICB stressed that, at the moment, efforts should be focused on understanding the risks and building a holistic, coherent, affordable and adaptable response. It was acknowledged that a European response is needed, and must support equivalent activity at national and operator levels.

ATM cyber-security is a fast moving topic, with many actors, and TSG members have a keen interest in its developments. Therefore, this information paper summarises the latest developments in terms of legislative and regulatory changes, standardisation activities, pan-European research and development, etc. A short summary of each known development is given. It was discussed at TSG/44 in September 2016 and has been updated in October 2016. It is important to stress that this is a dynamic area – with strong political and technical concerns that mean the shelf life of any analysis is limited.

CONTENTS

1. INTRODUCTION

In Q3 2015 the ICB's position paper on the regulatory response to ATM Cyber-Security was formally adopted at the plenary of ICB/57. The paper notes that the increasing reliance on inter-connected ATM systems, services and technologies increases the risk of cyber-attacks. Such risks undermine the vision of a safe, resilient and trustworthy European aviation sector, and would incur costs during the response to and recovery from cyber-attacks. The potential threat strikes at the heart of the Single European Sky. Member States and operators are increasingly dependent on each other for their security, as cyber-attacks can easily propagate or be replicated across international borders. If information about previous attacks is not exchanged, then neighbours cannot protect themselves and the industry cannot accurately assess the probability of a future attack.

The ICB, therefore, supported a European response that first understands the risks and then establishes mitigating measures. Such a European response must support equivalent activity at national and operator levels. The ICB considers that the regulation may need to be extended and/or streamlined, but at the moment efforts should be focused on understanding the risks and building a holistic, coherent, affordable and adaptable response. Greater clarity is required in the allocation of responsibilities for these tasks.

Since the adoption of the position paper there have been many developments, proposed and actual, by many players. This information paper summarises the latest developments, including legislative and regulatory changes, standardisation activities, pan-European research and development, etc. It should be noted that whilst some focus entirely on ATM, many are broader and address aviation or are even cross-sector. Similarly, some focus entirely on cyber-security and others address security more generally, including cyber.

Information for the summaries comes from a combination of public source and updates from key actors. The paper has been updated following TSG/44 (September 2016) to reflect additional and revised information.

It is important to stress that this is a dynamic area – with strong political and technical concerns that mean the shelf life of any analysis is limited.

2. LEGISLATIVE AND REGULATORY DEVELOPMENTS

2.1 ICAO

ICAO's Annex 17 to the Convention on International Civil Aviation, Security – Safeguarding International Civil Aviation against Acts of Unlawful Interference, sets minimum standards for aviation security worldwide and creates a global policy and legal framework. ICAO Aviation Security Manual (Doc 8973) provides guidance, including on minimum measures to protect critical information systems against unauthorised access and use. The last updates to these were in 2014.

The 39th ICAO Assembly, held in September/October 2016, was scheduled (Item 16) to include a progress report on the global aviation security policy framework and implementation of the ICAO Comprehensive Aviation Security Strategy (ICASS), including developments in risk assessment, innovation and cyber-security. Cyber-security was also expected to be addressed in other relevant items, such as RPAS (Item 33). The General Assembly passed a high-level resolution on cyber.

As outlined at SSC/59, the Commission, in coordination with ECAC, presented the European position at the 39th ICAO Assembly. This position emphasises the need for Europe to present concrete proposals, with a view to gather support from other delegations and to prevent potentially more prescriptive views. It also encourages ICAO to raise the general awareness of States on cyber-security and to encourage States to take into account cyber-security aspects in their safety and security programmes.

The Working Group on Threat and Risk has added cyber-security to the Risk Context Statement which should be used by all ICAO members to inform their national risk assessments. This includes a specific risk matrix for ATM which will be updated in 2017.

2.2 European Parliament and Council of the EU

2.2.1 General Data Protection Regulation (GDPR)

The GDPR (Regulation (EU) 2016/679) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data entered into force in May 2016 and shall apply from May 2018. The Regulation applies to personal data and imposes additional legal obligations on data processors, placing significantly more liability on organisations responsible for a breach. The scope of the EU data protection law is extended to all foreign companies processing data of EU residents, and a single set of rules is introduced for all EU Member States.

The Regulation stipulates that Data Protection Impact Assessments must be conducted when specific risks occur to the rights and freedoms of data subjects. Risk assessment and mitigation is required, along with prior approval of the DPA for high risks.

2.2.2 Network and Information Security (NIS) Directive

In July 2016 the Network and Information Security (NIS) Directive (2016/1148) was adopted. It is aimed at establishing minimum standards for Member States and operators of critical national infrastructure, noting that this is a much broader scope than ATM-specific regulation. The Directive entered into force in August 2016 and Member States have 21 months to transpose the Directive into their national laws and 6 months more to identify operators of essential services. ANSPs (and airports) are very likely to be included.

Organisations will be required to assess the risks and adopt appropriate measures to ensure a secure and trustworthy environment. Mandatory reporting of any incident seriously compromising the networks and information systems will be required from operators. Member States shall establish effective Computer Emergency Response Teams (CERT) and designate one or more competent authorities, which will be part of a secure European-wide electronic data interchange network to allow the sharing of cybersecurity related information especially for incident reporting.

2.3 European Commission

A new unit in DG MOVE dealing with all security aspects in transport has been established in October 2016. The A5 unit combines Maritime Security (former A4) and Aviation Security (former A2).

2.4 EASA

One of the elements of the EASA cyber-security roadmap is cross-domain regulatory oversight. This aims both to create a level playing field for all aviation stakeholders, and to initiate integration of cyber-security into Security Management Systems.

2.4.1 'New' Common Requirements: "Requirements for service providers and oversight thereof"

The Common Requirements for Provision of Air Navigation Services regulation (1035/2011) sets out general requirements for a variety of areas, including security management. This regulation, and others, will be repealed, while aligning the requirements for service providers and the oversight thereof into a single regulation ('CR-O'). The text of the CR-O IR includes an explicit requirement relating to cyber-security that has, so far, remained the same across different draft versions. It is: "Air navigation services and air traffic flow management providers and the Network Manager shall take the necessary measures to protect their systems, constituents in use and data and prevent compromising the network against information and cyber security threats which may have an unlawful interference with the provision of their service." This regulation will be applicable from 2020.

2.4.2 Amendments to the Basic Regulation

Negotiations on the Basic Regulation is on-going and it is noteworthy that the:

- Council proposal does not address cyber-security
- Parliament proposal considers cyber-security as one additional source of concern for Safety

Therefore, depending on its passage to law, the new BR may give EASA the competency to address cyber-security.

2.4.3 Gap analyses

EASA is undertaking a gap analysis of all Implementing Rules. These are started to identify areas of action.

2.4.4 Rulemaking links with the FAA

EASA has also joined the FAA in the information-security Aviation Rulemaking Advisory Committee (ARAC). The FAA tasks the ARAC to provide advice and recommendations concerning a full range of aviation-related issues, in this case information/cyber-security. However, this is focused on aircraft cyber-security and does not address ATM, since in the US ATM systems are of federal interest only.

3. STANDARDISATION ACTIVITIES

3.1 CEN

3.1.1 EN 16495

EN 16495 Information security for organisations supporting civil aviation is an existing European Standard, published at the start of 2014, defining guidelines and general principles, structured in line with ISO 27002, for the implementation of an information security management system. However, with the latest versions of the ISO 27000 series of standards, EN 16495 is no longer fully aligned with ISO 27002. Work to re-align EN 16495 has started.

3.2 EUROCAE

3.2.1 WG-72 ED-205

A sub-group from WG-72 (Aeronautical Information Systems Security) is producing a Process Specification for the security accreditation of ATM systems. The target date for publication is Q4 2017. The Statement of Work is as follows: ED-205 will target information security throughout the lifecycle of data exchanged between aircraft and ATM systems: this includes the creation, origination, storage, transmission, processing and decommissioning of data. It will address the design of a security accreditation method for ground ATM systems analogous to airworthiness certification. The scope will have a broad approach focusing on safety, operational and economic impact.

3.3 ECAC

3.3.1 Update to Doc. 30

An ECAC Study Group on Cyber Threats to Civil Aviation is updating Document 30 ('Doc. 30') to better address cyber-risks. Doc. 30 builds upon ICAO Annex 17 and can define higher standards. Amendments to the overarching principles in Chapter 14, and prescriptive annexes, as well as supporting guidance material are expected to be developed and included within the ECAC Aviation Security Handbook within the next couple of years.

3.4 EUROCONTROL

3.4.1 ATM Security Policy and Implementation Guidelines

The NEASCOG (NATO EUROCONTROL ATM Security Coordinating Group)[1] approved these two documents in Summer 2016. Further, both documents have been endorsed by the EUROCONTROL Civil Military Interface Standing Committee (CMIC) and the NATO Aviation Committee. Though implementation is not mandatory, or even audited, such endorsement essentially means that Member States 'commit' to implement it at national level. Further points to note are:

- The Policy has been developed as the framework for further development and implementation of ATM security, including cyber-security.
- The Guidelines for Implementation complements the ATM Security Policy by providing guidance in support of its implementation.
- Future work includes developing further different parts of the Policy. In 2017 it is expected to reach out an agreed ATM security baseline.

3.4.2 Manual for National ATM Security Oversight

The manual covers the full spectrum of ATM security, so cyber is included, and is complementary to the Policy above. Edition 2 of the manual, published in 2013, is now under review as a consequence of workshops/seminars organised in different Member States and lessons learnt from its implementation. Edition 3 is expected by 2017 Q3.

4. FUNCTIONS AND SERVICES

NB: Only International and European institutional activities are included, not individual operator level activities.

[1] The former EUROCONTROL ATM Security Team has been closed down and merged into the NEASCOG as the Air Navigation Security Working Group.

4.1 EASA

4.1.1 European Centre for Cyber Security in Aviation

One of the enablers identified in the EASA Cyber-Security in Aviation project, and roadmap, is a European Centre for Cyber Security in Aviation (ECCSA). This will help meet the roadmap's four identified objectives: Situational Awareness, Readiness & Resilience, Reactiveness, and Cyber-Security Promotion. This Aviation Computer Emergency Response Team (CERT) will both establish an aviation-focused cross-sectorial risk landscape and coordinate prevention of threat scenarios and response to future attacks. It is currently being set up, with ENISA's CERT-EU platform being used, and the start of pilot operations is planned for January 2017. Full operation is expected from November 2017. It is intended as a clearing house for (confidential) incident information that builds on existing safety reporting. Note that the scope of this is all of aviation.

4.2 EUROCONTROL

4.2.1 Centralised Services CS6-6

CS6-6 – a Security Certificate Service - is currently in procurement, specifically undertaking technical appraisal of proposals, with the intent of being operational in 2018. It will provide a Public Key Infrastructure (PKI) for European ATM stakeholders, effectively a technical foundation for trusted relationships. EUROCONTROL will be the Root Certification Authority (CA) and Policy Management Authority. Certificates will be issued to EUROCONTROL and Network Manager applications/users/systems, and other CAs (eg local ANSPs). There will also be cross-certification with US and could be extended to other ICAO regions.

EASA's ECCSA and EUROCONTROL's CS6-6 facilities will be linked, collaborating on ATM-related information and sharing any analyses.

4.2.2 Centralised Services CS6-7

CS6-7 is also currently in procurement, specifically undertaking technical appraisal of proposals, with an intent of being operational in mid-2017. It will provide two functions:

- **European ATM CERT**: this collects, generates and distributes ATM relevant cyber intelligence, and coordinates pan-European ATM responses to ATM relevant cyber-security events/incidents. This may provide the ATM element of EASA's AV-CERT and, similarly, uses ENISA's CERT-EU and guidance materials.

- **Security Operations Centre (SOC)**: this provides a SOC for all Centralised Services, specifically monitoring and assessing Centralised Services related cyber-security events and providing recommendations to the relevant CS Contractors. It also performs the role of a SOC for ANSPs wishing to entrust such role to CS6-7 based on specific bilateral agreements.

4.2.3 Training

The former GEN-SEC Course delivered twice a year at the EUROCONTROL Institute of Air Navigation Services (IANS) has been upgraded and split into three courses (Legislation, Security management systems and Cyber). At the same time, and as a consequence of the nomination of the IANS as a Regional Training Centre of Excellence, it will deliver ATM security training on behalf of ICAO. Development is ongoing; delivery is expected mid-2017.

4.3 Aviation-ISAC

The Aviation Information Sharing and Analysis Center (A-ISAC) is a US / Boeing led membership group for relevant security information sharing for the aviation sector. It combines both industry and government participants to share timely and actionable information pertaining to threats, vulnerabilities, incidents, etc. In addition, it aims to foster cooperation and provide best practices and educational awareness. Membership is open to

European organisations, and Airbus will be an “anchor” member to address European issues and engagement with the government, when needed.

4.4 EU-Aviation ISAC (EA ISAC)

A similar initiative to the Aviation-ISAC has been proposed by Airbus and Lufthansa, with informal discussions considering its formal launch. Discussions between the US and European efforts on potential collaboration are ongoing with a meeting held in September 2016 on the Aviation-ISAC’s European strategy. NDA and MoU are being drafted to frame the EA-ISAC activities.

5. RESEARCH AND DEVELOPMENT ACTIVITIES

5.1 SESAR 2020

The SESAR 2020 multi-annual work programme identified cyber-security as a research topic to address. It is therefore expected that the members’ proposals, and project plans, will address cyber-security and that work will start with the launch of projects in Q4 2016 / Q1 2017. One specific role of PJ19 (Content Integration) is to coordinate cyber-security activities and guidance provided across all projects, and this should be facilitated by the appointment of Security/Cyber-Security ATM Focal points in each project. Each SESAR solution shall develop a security case to demonstrate that self-protection and collaborative support has been correctly addressed. As part of this, projects will undertake security risk assessments and identify resulting security requirements – both include the cyber dimension.

In addition, the SJU are currently developing a cyber-security strategy. Its purpose is to clarify what will be delivered as part of SESAR's output regarding cyber-security and the securability of SESAR solutions. It will define the responsibilities of the SJU in the frame of the whole system - and service - lifecycle. Topics such as the role of operational mitigations to system vulnerabilities are likely to be addressed. The strategy is expected to be published in Q4 2016.

5.2 ACARE Security Sub-Group

In June 2015, at the request of the EC, a dedicated security sub-group was created within the WG/4 (Safety & Security) of the Advisory Council for Aviation Research and Innovation in Europe (ACARE). Its purpose is to update ACARE’s Strategic Research & Innovation Agenda (SRIA), which is a strategic roadmap for aviation research, development and innovation. It accounts for both the evolution of technology as well as radical changes or 'technology shocks'. It is expected to do this for cyber-security by mid-2017. SRIA impacts on Horizon 2020.

5.3 EASA

Another of the enablers identified in the EASA Cyber-Security in Aviation project, and roadmap, is research and studies. This aims both to encourage aviation industry to intensify research on vulnerabilities and strategic means, and to identify research needs and promote cyber-security as priority area at European level. At the moment there is nothing specifically on ATM.

5.4 GAMMA

The Global ATM Security Management Project (GAMMA) is a European research project (2013-2017) whose goal is to develop solutions to emerging air traffic management vulnerabilities backed up by practical proposals for the implementation of these solutions. During 2016 the focus has moved towards translating the GAMMA concept into a set of prototypes to validate in exercises. The Security Management Platform (SMP) prototype represents the central instantiation of the GAMMA concept as it is the security information sharing platform which lies at the heart of the GAMMA proposal for managing ATM security in Europe.

5.5 EUROCONTROL Agency Research Team (ART)

A dedicated ART Workshop on ‘ATM Security and Cybersecurity’ was held in Q1 2016, giving a broad overview of different areas of activities within the field.

6. WORKING GROUPS

6.1 Industry High-Level Group (IHLG)

In 2014, ICAO, ACI, CANSO, IATA and the International Coordinating Council of Aerospace Industry Associations (ICCAIA) signed a Civil Aviation Cybersecurity Action Plan aimed at more effective coordination across all stakeholders to effectively respond to cyber challenges. Since then there has been progress with:

- **Sharing of best practices**: IHLG organisations has identified key practices and guidance, to be held on an ICAO-based dedicated cyber security web-page. There is a recognition that specific guidance for different entities may be appropriate, with overarching guidance at the ICAO level (drawing on international standards such as ISO/IEC 27002).
- **Developing a common set of terms**: The IHLG identified a number of existing glossaries and have facilitated sharing those among the aviation community through the cyber portal established by ICAO.
- **Preparing civil aviation against future challenges**: The IHLG agreed a common set of key messages such that a consistent view could be presented publicly. Many efforts were also made to promote the cyber-security topic as a priority.
- **Proposing a declaration for the ICAO 39th Assembly**: The IHLG proposed a declaration intended to consolidate and align cyber-related policy statements and directions to facilitate defining general objective. This was scheduled for the end of September 2016.

6.2 ACI World Cybersecurity Task Force

The Task Force was initially set up with the focus of enhancing cyber-security information-sharing between airports and industry partners; educating airport management and information technology staff on cyber-security issues; representing ACI's interests with other organisations who are also concerned with the growing risks posed by cyber-terrorism in the air transport industry.

The taskforce has also developed the IT Airport Cybersecurity Benchmark, a web-based system addressing the specific information security needs of the airport community. It is aligned to ISO/IEC 27002 controls.

6.3 ASD Civil Aviation Cyber Security Task Force

The Task Force was launched in October 2015 with the goals of developing an ASD position on civil aviation cyber-security and coordinating ASD inputs to external bodies on the subject. International work has been through the ICCAIA and has contributed to ICAO's Assembly and AVSEC Panel, including the IHLG declaration (see above). European work to-date has centred on coordinating with, and providing input to, EASA (especially on the Basic Regulation and cyber-security roadmap) and ECAC. High-level objectives for the manufacturing industry and for operators have been developed. The Task Force was set up as a temporary entity so in Autumn 2016 decisions will be taken on whether to extend and on any future work programme.

6.4 CANSO ATM Security Working Group

CANSO has an ATM Security Working Group (ASWG) that address all aspects of security, including cyber-security. The third ASWG meeting was held in December 2015. CANSO participates in the IHLG (see above) and is fully committed to the 2014 ICAO Civil Aviation Cyber Security Action Plan (2014). A working paper on cyber-security was presented to the fifth ICAO EURNAT EUR/NAT Aviation Security Group (ENAVSECG) in May 2016. Ongoing activities within CANSO Vision 2020+ include:

- Security promotion, awareness and Just Culture
- ATM security human factors in the whole ATM lifecycle
- Identification of Security standards and best practices applicable to ATM environment in the light of sustainability and regulatory compliance
- Audit and oversight issues
- ADS-B Working Group activities for secure surveillance

2016 has also seen cooperation between CANSO and NEASCOG (NATO-EUROCONTROL Security Coordination Group).

7. INDUSTRY PLANNING AND WHITE PAPERS

7.1 Aviation Strategy for Europe

The December 2015 strategy noted that aviation is 'digitalising' at a fast pace and that, whilst this brings benefits, it does also make aviation more vulnerable to cyber-security risks. It states that the Commission will ask the EASA to address cyber-risks, in order to foster security by design and to establish the necessary emergency response capability, working with other competent bodies to achieve this.

7.2 European ATM Master Plan

The 2015 Edition of the Master Plan makes explicit reference to cyber-risks to ATM, noting that it is essential that the development of cyber-security is performed in parallel with the development of technical enablers. A risk identified within the Master Plan is that the deployment of SESAR solutions leads to unaddressed cyber-security vulnerabilities. The mitigations identified were to (a) ensure efforts on ATM cyber-security are coordinated, and assess policy options for strengthening cyber-security and resilience, and (b) establish principles and processes for ensuring cybersecurity and resilience are included appropriately within the SESAR R&D work programme.

7.3 Deployment Programme

The draft 2016 Deployment Programme both refines the specific Families related to SWIM cyber-security and reports on the identified cyber-security requirements to be considered in the deployment of each Family, having specific regard to the potential cyber-threats linked to the increased connectivity associated to the full PCP deployment. The SDM is of the opinion that some components of some families are particularly exposed to cyber-security risks and that stakeholders should take appropriate action to mitigate them.

The Commission also requested to the SESAR Deployment Manager to consider cyber-security requirements at project level in the Deployment Programme by proposing guidance material.

7.4 IFATCA

Early consideration is being given to the impact of cyber-security issues on controllers, and the required response, with a formal policy anticipated in the first half of 2017.

7.5 IFATSEA

A comprehensive document is being developed to provide IFATSEA’s global perspective on a range of issues, including cyber-security, integration of RPAS and remote towers. It will provide an IFATSEA position on cyber-security as well as pointing towards future solutions. It should be available by end of 2016.