International Civil Aviation Organization
North American, Central American and Caribbean Office

INFORMATION PAPER

NACC/DCA/09 — IP/10
18/06/19

Ninth Meeting of the North American, Central American and Caribbean Directors of Civil Aviation (NACC/DCA/09)

Port-of-Spain, Trinidad and Tobago, 25 to 27 June 2019

Agenda Item 7 NAM/CAR Regional Aviation Security/Facilitation Implementation
7.2 Aviation Security/Facilitation Implementation Matters

CYBERSECURITY IN FRENCH GENERAL DIRECTION OF CIVIL AVIATION (DGAC)

(Presented by France)

EXECUTIVE SUMMARY

French DGAC has tackled early on the increasing cyber threats on its systems and has defined a Policy on Security for Information Systems (PSIS). It was defined within a national regulatory framework that gives a central role to the national cybersecurity agency (ANSSI) in preventing cyber threats, informing and protecting information systems.

The PSIS of DGAC is defined through 3 components: a strategy regarding cybersecurity, a governance component and an operational component (the cyber information system).

Due to the sensitivity of cybersecurity for civil aviation, DGAC chairs since 2018 the National Committee on Cybersecurity in Air transport in charge of the coordinatation of the strategy on cybersecurity for civil aviation with all the stakeholders. This National Committee is attended by aircraft manufacturers, airlines, airports, service providers, cyber expertise… in France.

This cyber information system has been implemented following a pragmatic step-by-step approach relying on internal skills and external skills in high level state-of-the-art cyber security aspects. The cyber information system provides 6 security services: access management, cartography, collect and log, detection of incidents, processing of incidents.

Strategic Objectives:	• Security & Facilitation
References:	• ICAO Annex 17 (Security) • Assembly Resolution A39-19 – Addressing Cybersecurity in Civil Aviation

1. Introduction

1.1 Cyber-attacks appear as an increasing threat worldwide in relation with the development of digitalization and the interconnection of systems. Civil aviation is particularly sensitive to this emerging

threat with widely interconnected systems. Moreover, any disruption of systems due to a cyber-attack can seriously impact the safety and the security of flights but also the image of civil aviation in the public eye. ICAO has taken into account this emerging threat to civil aviation through the resolution A39-19 “addressing cybersecurity in civil aviation” during the 39th Assembly.

1.2 Following is explained the way that DGAC tackles cyber security in this context to ensure the protection of its sensitive infrastructures within the framework of the French national and international regulations.

2. A regulatory framework at national level

2.1. National regulations

2.1.1 The question of cybersecurity is addressed in France at national level as a major threat on the national sovereignty. Therefore, the national, and general, framework on cybersecurity in France is based on the law on Critical Information Infrastructures Protection (CIIP) of December 2013.

2.1.2 Following the national law, a decree was published in March 2015 regarding the security of information systems for operators of vital importance (OVI). An OVI is defined as an operator whose unavailability could strongly threaten the economical or military potential, the security or the resilience of the Nation. Critical operators were identified within 12 critical sectors including civil aviation. This decree was followed in October 2016 by a more specific decree for OVI in Air transport.

2.1.3 The French government defined its first State Policy on Security of Information Systems (PSIS) in July 2014.

2.2. ANSSI, national cybersecurity agency and its support to civil aviation

2.2.1 Created in 2009, the Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI) is France’s national cybersecurity agency and also the national authority for information systems security (2009) and defence (2011). It is a body attached to the Prime Minister’s services. To ensure its missions, the staff of the ANSSI went from 100 in 2009 to more than 500 today.

2.2.2 The ANSSI’s three main missions are:

- **To prevent threats** by anticipating modes of attack through scientific expertise, defining protective measures and by certifying trusted IT products and services;
- **To inform target audiences** by raising awareness on the necessary protection of digital environments, promoting best practices for cybersecurity and by issuing technical recommendations;
- **To defend information systems** by detecting weaknesses and incidents and by reacting as early as possible in case of a cyberattack, including by providing technical assistance and expertise (CERT-FR included) to administrations and operators.

2.2.3 The CIIP law defines four sets of measures where ANSSI play a key role:

- **Security requirements:** ANSSI will impose to the operators a set of technical and organisational rules;

- **Inspection:** ANSSI can trigger security audits led by itself, another State authority or a Trust service provider;
- **Incident notification:** ANSSI shall be notified directly by operators of incidents occurring on their critical information systems;
- **Major crisis:** ANSSI can impose cybersecurity measures in case of major crisis, declared by the Prime Minister.

2.2.4 ANSSI cooperates with ministries to ensure consistency of specific regulations with the national regulation framework. It also qualifies cybersecurity service providers that can offer services to operators. The ANSSI also ensures that national regulations are applied within critical sectors by critical operators as is the case with DGAC for civil aviation. ANSSI supports and controls the DGAC in its implementation of a cybersecurity information system and DGAC informs and reports to ANSSI, on incidents for example.

3. Cybersecurity in DGAC

3.1. DGAC's Policy on Security for Information Systems (PSIS)

3.1.1 Within the national regulatory framework, DGAC has tackled the matter of cybersecurity following a standard methodology. As required by the CIIP law, DGAC has defined its own Policy on Security for Information Systems (PSIS). The PSIS of DGAC relied on a risk analysis on the existing systems based on DGAC requirements for:

- System availability,
- Data integrity,
- Data confidentiality,
- Traceability,
- Conformity.

3.1.2 The PSIS is defined through 3 components (i) the strategy of DGAC regarding cybersecurity, (ii) how the organisation monitors the implementation of the cybersecurity information system and (iii) the operational procedures of the cybersecurity information system.

3.2. Organisation of DGAC in cybersecurity

3.2.1 The PSIS defines the governance on cybersecurity at different levels within the organisation.
The Director General of DGAC stands as the Empowered authority for the Security of Information Systems (SIS) supported by the DGAC national manager of SIS that coordinates the implementation of the PSIS within the DGAC with the managers on SIS of DSNA (ANSP), DSAC (CAA), SSIM (Information Systems Management). The managers of these 3 directions will coordinate the implementation of the PSIS within their own direction and will be part of the operational management of the cybersecurity information system in their direction.

3.2.2 The sensitivity of civil aviation to cyber threats led to the creation in 2018 of the national committee for cybersecurity in Air transport. This national committee chaired by the Director General of DGAC coordinates the strategy on cybersecurity for all stakeholders in aviation like aircraft manufacturers, airlines, airports, service providers with the support of cybersecurity expertise (ANSSI...).

3.2.3 The committee heads three subgroups:

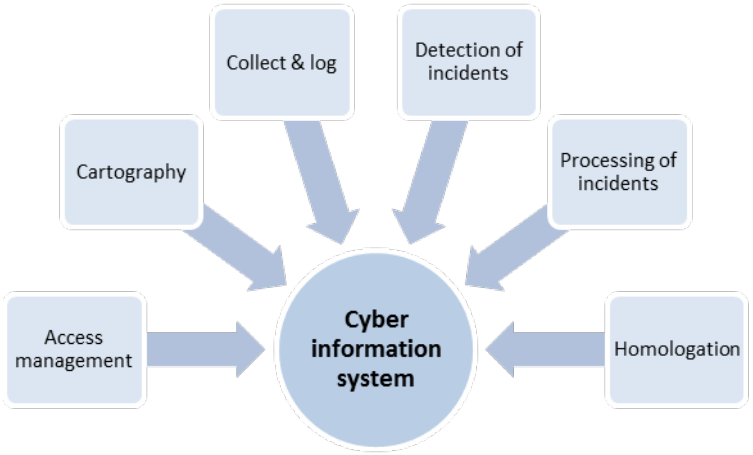
- **Emerging threats:** this subgroup takes into account emerging threats and scenarios that could impact activities in air transport;
- **Impact on air transport:** this subgroup analyses the impact of threats and scenarios on air transport activities and proposes protecting measures;
- **Regulation amendments:** this subgroup evaluates the needs to amend regulations at national and international level

3.2.4 The third subgroup coordinates the participation of France that was already active on the issue of cybersecurity at EU and ICAO level.

3.3. The DGAC cyber information system

3.3.1 DGAC decided on a pragmatic step-by-step approach in the monitoring and implementation of the cybersecurity information system.

3.3.2 The cyber information system provides 6 security services as shown below.



3.3.3 Each service relies on:

- A defined organisation and a set of operations,
- A technical infrastructure and tools,
- Engineering rules.

3.3.4 Following the risk analysis on its systems, DGAC decided to tackle first, thanks to the cyber information system, the more sensitive issues regarding the protection of its systems and to plan a progressive implementation of a more complete set of protection measures, relying on:

- its own competencies and skills on software and networks, that DGAC had always developed for safety and efficiency purpose, and that DGAC is developing further for cyber aspects;
- external competencies and skills in high level state-of-the-art cyber security aspects.

3.3.5 As a matter of fact, DGAC remains in charge of the management of cybersecurity on its systems and relies on external support only in matters of expertise on cybersecurity.

3.3.6 This pragmatic approach enables DGAC to integrate its cybersecurity policy within its organisation and culture, and the existing processes.

4. At international level

4.1. The EU framework

4.1.1 The EASA (European Union Aviation Safety Agency) cybersecurity roadmap presented in 2015 has been considered as basis for implementing a cybersecurity framework for aviation. Through the regulation 2018/1139 of the European Parliament and of the Council, EASA has fully taken into account the issue of cyber security. The objective of the Agency is to incorporate cybersecurity in the existing safety notion through promotion (training sessions or awareness campaigns), regulatory activities as well as international cooperation.

4.1.2 EASA established the European Strategic Coordination Platform for Cybersecurity in Aviation (ESCP). The European aviation community, both civil and military, join through this platform in a co-operative partnership to define and coordinate the implementation of a European strategy for Cybersecurity in Aviation. France takes part in the ESCP as member state along with other member states, European institutions, key stakeholders from industry, and airspaces users. As an active member of ESCP, France organised with EASA the ESCP high level meeting on cybersecurity in civil aviation in November 2018.

4.1.3 Furthermore, DGAC was able to verify its ability to deal with cyber incidents in 2018 through the large scale exercise Cyber Europe 2018. 'Cyber Europe' exercises are simulations of large-scale cybersecurity incidents that escalate to EU-wide cyber crises. The exercises offer opportunities to analyse advanced cybersecurity incidents, and to deal with complex business continuity and crisis management situations. Organised by the European Union Agency for Network and Information Security (ENISA) in collaboration with cybersecurity authorities and agencies from all over Europe, Cyber Europe 2018 focused on the aviation sector and enabled the European cybersecurity community to strengthen their capabilities in identifying and tackling large-scale threats, as well as to provide a better understanding of cross-border incident contagion.

4.2. The ICAO framework

4.2.1 The Assembly Resolution A39-19 – Addressing Cybersecurity in Civil Aviation in October 2016 established the framework for ICAO in tackling cybersecurity. France has actively participated to meetings and workgroups established by ICAO to promote its approach regarding cybersecurity. France designated a focal point to take part in ICAO Secretariat Study Group on Cybersecurity (SSGC) France also promotes its approach on cybersecurity in ICAO workgroup at regional level.

— END —