

Conclusions for the ESCP High Level Meeting

Toulouse, 14-15 November 2018

Co-organised by EASA and DGAC France

Representatives from National Aviation, Security and Military Authorities, EU institutions, ICAO, ECAC, EDA, Eurocontrol, ETF and other key European associations engaged in cybersecurity as well as representatives from airline operators, service providers and industry participated to a two days round table for the development of a comprehensive EU Cybersecurity Strategy for Aviation which should be published at the beginning of 2019. This meeting was a follow-up of the High Level Conference on Cybersecurity held in Krakow in November 2017.

Role of the ESCP and its members

- The ESCP has been and still is a key platform in the development of a pan-European comprehensive approach to address cybersecurity risks open to neighbours.
- It was created following the mandate of the High Level Meeting on Cybersecurity held in Bucharest in November 2016.
- Furthermore, the work of the ESCP is being essential in the development of regulatory requirements, guidance and industry standards aimed at ensuring that organisations across all aviation domains appropriately manage the impact on aviation safety of cybersecurity risks. This work should involve ECAC and contribute to ongoing ICAO work.
- An essential element supporting the implementation of these future requirements is the work being done within the ESCP in order to achieve a common risk management approach (STORM – Shared Trans-Organisational Risk Management).
- Awareness was identified as a key ESCP objective as well as the development of aviation cybersecurity skills.
- Each ESCP member must be the interface with its own organisation

Cybersecurity strategy for Europe

- The ESCP has developed during the last year a Strategy Paper which should be published at the beginning of 2019.
- This strategy aims at ensuring that the future aviation system is a trustworthy and dependable environment, leading to an Aviation system-of-systems capable to adapt and withstand new threats without significant disruptions.

- One of the main challenges is the coexistence of 2 main communities: the one dealing with security and the one dealing with safety.
 - Security: Reduce the manifestations of threats from intentional acts. However, effects are not directly addressed.
 - Safety: Reduce the effects of the residual threats (those not being stopped) passengers, crew and people on ground.

Their different perspectives need to be understood, so the knowledge of each party enters into the decision making of the other party.

- Another key challenge is to enable the sharing of information between all the affected parties, by creating a trustworthy environment based also on appropriate information control and confidentiality.
- It will be essential to monitor the progress being done, and on that basis, further refine the strategy being developed.
- ESCP can also be an instrument to liaise with other sectors in particular the transports modes.
- Additional work streams should be considered to deal with oversight requirements and process as well as research needs.
- The Conference agreed on the proposed strategy considering it as a first step to be reviewed after some collective return of experience.

Regulatory activities

- An essential element of the comprehensive cybersecurity strategy being developed is the introduction of a robust and flexible regulatory system, supported by adequate guidance and industry standards.
- This includes not only the aspects related to aircraft design and production, but also requirements for organisations so they properly manage the impact on safety of cybersecurity risks.
- Although there are already other regulatory frameworks addressing information security matters, such as the NIS Directive and Regulation 2015/1998, they may not be sufficient to address in a comprehensive manner the impact of cybersecurity risks on aviation safety.
 - They have other objectives (such as preventing disruption of essential services to society, or addressing aviation security issues).
 - They do not always cover all aviation stakeholders.

- Their implementation may not be fully consistent and standardized since they depend on the approach taken by each Member State.
- It is essential to ensure consistency of regulatory requirements between the different frameworks and to ensure adequate coordination between the different authorities (European, NAAs, security authorities, etc).
- To this end, EASA is already working with the relevant services of the European Commission and ENISA, in order to ensure that all the necessary coordination is in place, for regulatory, reporting and, oversight purposes.
- The conference did welcome the extensive regulatory efforts developed under the auspices of the ESCP but recalled the necessity to consider the regulatory framework stemming from the various European bodies from the point of view of operators and their capacity to implement it in an efficient and optimal way.

Shared Trans-Organisational Risk Management (STORM)

- STORM is currently laying only the first stone for Risk Management coordination among aviation stakeholders, which is the risk assessment toolset. Other activities have to be started to pave the road to a common risk management approach and achieve cybersecurity maturity.
- The reference model that will result from the ongoing STORM activities should become the foundation for the measurement and monitoring of organisations. This is essential both for organisations and authorities.
 - Organisations will be able to consistently identify and measure their risks taking into account not only their internal risks but also those identified by other organisations with whom they interface.
 - Competent authorities will have a reference model to assess those organisations under their oversight.
- The outputs of the STORM activities will be also the basis for creating guidelines for the ATM/ANS service providers community. Those guidelines will help building their strategy to elaborating action plans towards achievement of cybersecurity maturity.
- STORM will be a fundamental support element for the implementation of the New Basic Regulation, establishing a common understanding of cybersecurity risk management that will now involve not only the aircraft and its manufacturers but also all the other parts of the aviation system.
- The debate to the potential synergies between Global, Regional and National initiatives to better assess trans-organisational risk management. It considered it as a productive first step to be combined with the critical need to facilitate information-sharing.

French Council for Cybersecurity in Air Transport

- French initiatives for Cybersecurity in Aviation were presented to the Conference in the form of the recently created Council for Cybersecurity in Air Transport.
- The Conference learned with interest about the various French initiatives encompassing all the French Aviation Ecosystem, as well as the French National Information Security Agency.
- The Conference considered the French example as a good practice that could be followed in some other States to foster Coordinated Aviation Cybersecurity developments.

Conclusion: Drive ESCP Objectives for 2019

- Toulouse ESCP Conference marked a new milestone in the Pan European Aviation Cybersecurity Strategic Roadmap after the approval of EASA Basic Regulation which entered in force on 11th of September.
- Future steps will be
 - The publication of the ESCP Cybersecurity Strategy after endorsement by the ESCP Executive Committee
 - The issuance of the Part AISS (Aeronautical Information System Security) NPA before summer 2019.
 - The development of standards and means of compliance stemming from the AISS Horizontal Rule
 - The development of Trans Organisational Risk Assessment Methodologies to support Part AISS implementation
- The Conference identified the need to coordinate new areas under the ESCP:
 - Coordination between State Authorities (Aviation Safety, Aviation Security, National Information Security,...) for Aviation Cybersecurity Oversight
 - Research and Development activities
 - Outreach to all European Stakeholders
 - Education and Capacity Building