HERMES
AIR TRANSPORT ORGANISATION

POSITION PAPER

R20-PP/10
10/02/2020

Digitalisation, AI and the human factor in aviation security and ATM domains in particular

Presented by ERA

Historically, aviation security referred to unlawful acts including destruction of an aircraft, hostage-taking on board an aircraft or at airports and the carriage of weapons or other hazardous materials for criminal purposes. However, looking at the present (and future) most modern aircraft and airport systems are dependent on the reliable functioning of critical computer systems infrastructures (e.g. flight management systems, electronic flight bag, e-enablement of aircraft and extending to air traffic management). As a consequence, the aviation industry's vulnerability to cyber-attack has been significantly widened.

In the past terrorists or lone perpetrators with malicious intent may have attempted to smuggle a bomb into an airport or on board an aircraft, whereas computer system hacking now provides such individuals with an alternative means of causing disruption or even threat to life. Although there may be no loss of life during such events, they nonetheless demonstrate how vulnerable computer systems are to cyber- attack and aviation is a prime target. An important tool for the industry to combat the threat of cyber is to firstly recognise and understand the threats. Such threats are defined into two specific categories; either an attack that is designed to facilitate an event with the aim of causing risk to or loss of life, or an attack designed to cause disruption to airport or airline operations, principally around passenger facilitation.

The facilitation of an attack via cyber can be aimed at numerous aircraft and airport systems that are vulnerable due to them employing either computer software or digital communication devices. At an airport, this can include security checkpoints such as baggage and passenger scanning equipment or ID/entry-controlled gates to restricted areas (e.g. airside). Infecting such systems with malware will prevent the devices from functioning properly and thus afford the perpetrator(s) the opportunity to smuggle through a concealed weapon or explosive device. A cyber-attack aimed at disruption may not have the intent on causing physical harm to individuals but can still result in an enormous financial impact on airlines and/or airports. Malware in check-in, baggage handling and passport control systems can result in severe disruption to the flow of passengers, creating both a backlog in the terminal and potential delay of flights. For smaller, regional airlines that operate multi-sector days the impact would be enormous.

From an aircraft perspective, cyber-attack can have far more serious consequences. Pilots become more reliant on advanced digital glass cockpit displays powered by sophisticated computer systems. Consequently, such aircraft digital advancements accelerate, so does the vulnerability and attack surface from cyber widen. An Aircraft whilst on the ground or in flight is constantly transmitting various data across networks via both ground antennas and satellites. The more complex/modern the aircraft the greater number of antennas, with the Airbus A380 aircraft being a good example where in excess of 1000 applications are running when the aircraft is airborne.

To elaborate further, aircraft computerised control systems are classed into three specific categories, namely Flight Controls, Cabin Controls and Passenger Controls. Flight Controls operate such safety critical systems required to fly the aircraft including the elevators, flaps, rudder and outside temperature sensors. The systems used to operate/maintain the aircraft cabin will lighting, air conditioning and most importantly the fire suppression systems in the cargo compartment due to the

on-going concerns regarding lithium batteries. Finally, there are the passenger control systems governing in-flight entertainment, seat displays and the cabin crew control panel.

With the aviation industry gaining operational efficiency via the use of digitalisation and computer systems and their integration to optimise the management of their networks, the number of software systems, connectivity and entry points is thus constantly increasing. It is therefore critical that all industry stakeholders, particularly aircraft operators and airports are aware that although their systems and processes may be more convenient and efficient, they are also consequently increasingly vulnerable to a cyber-attack.

The Air Traffic Management domain has been slow to react to an ever faster evolving digital world. Fortunately a number of initiatives are now either in place, or will be in place over the next few years in order to modernise the ATM system which will, in turn, provide better granularity, predictability and hopefully deliver additional capacity and better Network performance in the airspace through automation. Indeed, delivery of SESAR initiatives are predicated on the timely realisation of digital services.

The cornerstone of a digitised environment is through the provision of harmonised information exchange. System wide information management (SWIM) provides infrastructure and related governance though several interoperable services as defined in ICAO Doc 10039. Through these open standard services, information access and exchange between all ATM stakeholder will reduce costs and increase competition, allowing all components of the ATM value chain to become more efficient.

We are already seeing the shift from Aeronautical Information Services (AIS) to Aeronautical Information Management (AIM), which will deliver dynamic, integrated and harmonised AIS to airspace users. Meteorological and flight information management services through SWIM must be delivered in order to address the demand vs airspace capacity gap that is starting to become critical.

On the ground, Airport Collaborative Decision Making (A-CDM) is a relatively mature concept - the first airport – Munich - going live in 2007 - improving efficiency and throughput by the optimisation of airport assets and resources whilst improving the quality of information provided to air traffic services at local and Network level. Full A-CDM is not for every airport, and to address this the advanced ATC tower concept was introduced which allows smaller airports to send a small subset of the A-CDM data to relevant stakeholders without having the financial or operational burden of full implementation. The evolution of the digital remote tower can provide huge savings for the airport ATM infrastructure as control towers can now be situated hundreds of miles away and centralised (a benefit for smaller regional airports with limited movements per day).

For the airspace users, digitisation can’t come soon enough in certain areas, as the airlines have embraced new technologies for some time both in the commercial and operational arenas. However, care needs to be taken particularly with regards to data services where we need to see positive cost benefit analysis, understand fully the controls and accessibility of data as well as safety oversight. There is also some nervousness around local and continental implementations in a global operating environment. It should be noted that users share a significant amount of information today whether it schedule information, flight planning information and enhanced equipage data however it is not fully clear how much of this is used to deliver maximum benefits.

One of the potential disruptive technologies that might radically influence or transform the aviation industry value chain (including ATM) is the Artificial Intelligence (AI). The business of all

incumbent and traditional industry players will be impacted by the products and services made possible by the use of AI, which will also open the market up to new entrants. A new ecosystem of players is already emerging and those new players will be important partners for traditional aviation companies. New players' technology expertise can be used by aviation/ATM actors to unlock value potential from AI, and the industry has to be also prepared for them claiming their share of the aviation and mobility markets (as Google, Tesla or Uber did in the automotive industry). The industry should take action to fully capture the AI-enabled value opportunities in both the short and long term whilst protecting / further enhancing the overarching value of the aviation safety.

Application of AI, introduced with the desirable performance outcome that the joint human-AI system performs better than human plus AI separately, will inevitably affect the human performance across the entire aviation industry. It will help airline/ANSP/airport management to take strategic decisions e.g. in terms of fleet management or infrastructure monitoring, in ATC it might substantially alleviate controller's workload, propose the best possible options to the human and solve complex trajectory situations using machine-to-machine communication with air vehicles.

However, if not appropriately managed, introduction of new technology might include the risk of adding new type of complexity, especially in ATM where the human operates in an already complex system. In a new human-machine partnership between the human and the AI, automation and people do not compete but have to coordinate as a joint system (Joint Human Machine System (JHMS) philosophy). Further, the human operator needs to develop trust in the AI assistant and also retain certain core skills to take back control safely in case the AI's analysis is judged erroneous or inadvisable, or in case of temporary AI unavailability or failure. In order to achieve this, the involvement of operational staff in early stages of systems development will be critical as it will provide a guarantee that the system complies with all user requirements. Hence this will increase its usability and acceptability as being seen as a useful tool instead of a competitor.

Overall, digital transformation of the industry, including ATM is a necessary and vital step in delivering improved performance and opening up new possibilities. However, with ATM already lagging someway behind other industries in adoption of new technologies, we must ensure that whatever is deployed in the next decade or so is future proofed so we don't find ourselves in out of date shortly after these new methods of operating are deployed.

- END -