UDC 629.7.045

Li Haoyang, PhD,
(National Aviation University, Ukraine)

The state of development of the security of the civil aviation network

ICAO believes that civil aviation, as an important infrastructure field, relies on network technology to improve the safety and efficiency of air transportation, and its safety and stability involve a great deal, which not only directly affects the development and efficiency of civil aviation enterprises, but also affects national security.

1. Civil aviation faces increased cyber security risks.

In recent years, cyber security incidents in the global civil aviation industry have shown a high incidence. The information infrastructure of airports, airlines, air traffic management and other departments continues to break out network security loopholes, and even lead to a large number of attacks in serious cases.

Cybersecurity firm Immuni Web published a report in 2020[1] on public websites, mobile apps, and basic security checks on public websites, mobile apps, and exposure of sensitive data on public code repositories and the dark web at the world's top 100 airports. The results showed that of the Top 100 international airports, only 3 passed basic security checks, while the other 97 had security risks related to vulnerable web and mobile applications, public cloud misconfigurations, dark web exposure or codebase leaks.

At present, security incidents related to the civil aviation industry are divided into the following categories:

- **Security incidents caused by software failures.** A software glitch led to two fatal crashes of Boeing's 737 Max plane in 2019, killing a total of 346 passengers and crew. According to the classification and classification guidelines of information security incidents (GB/T 20986-2007), equipment and facility failures belong to one of the seven basic categories of network security incidents [2].

- **Malicious attacks by outsiders or organizations.** In April 2020, the website of San Francisco International Airport in the United States was attacked, the website system was implanted with malicious code and user authentication information was leaked; in June 2020, the computer system of a well-known domestic airline was continuously attacked, resulting in a comprehensive external service network of the airline Paralyzed for nearly four hours, more than 50 million users were affected.

- **Supply chain attacks.** In July 2020, the aviation industry supplier giant Garmin Corporation crippled consumer and commercial aviation products Garmin Pilot, Connext and FlyGarmin due to ransomware. The Garmin Pilot app provides pilots with flight plan archiving, account synchronization and database functions, while Connext provides cockpit services and weather, unknown reports, and data from the aircraft's central maintenance computer (CMC).

- **Security vulnerabilities of equipment and facilities themselves.** In July 2019, DHS/CISA issued a warning about the unsafe implementation of the CAN bus network, a protocol that allows various devices within aircraft, cars and other machines to communicate with each other. The flaw could allow bad actors to inject fake data into the plane. In 2019, a buffer overflow vulnerability (CVE-2019-9109) targeting the IFE in-flight entertainment system was discovered, which crashes the entire in-flight entertainment system. At the same time, the emergence of this vulnerability proves the authenticity and danger of flight network security problems.

2. ICAO attaches great importance to cyber security work.

There are currently 5 valid international air law-related instruments or documents, namely:

- Convention for the Suppression of Unlawful Seizure of Aircraft (1970)
- Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971)
- Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation Supplementing the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971)
- Convention for the Suppression of Unlawful Acts Relating to International Civil Aviation (2010)
- Beijing Supplementary Protocol to the Hague Convention for the Suppression of Unlawful Seizure of Aircraft (2010)

ICAO also attaches great importance to the research work on cyber security and related regulations. In 2018, ICAO established a cyber security research group in the Secretariat and released a series of cyber security strategic plans. In Annex 17 to the Chicago Convention, ICAO requires Member States to develop and implement measures to protect their critical information and communication technology systems and data used for civil aviation purposes from unlawful interference.

In 2019, during the 40th session of the ICAO Assembly, the release of the ICAO Aviation Cybersecurity Strategy was widely recognized [3], proposing international cooperation, governance, effective laws and regulations, cybersecurity

policies, information sharing, Seven measures of incident management and contingency planning, capacity building, training and cybersecurity culture. The strategy calls for member states to rapidly conduct feasibility studies and gap analyses to identify the most appropriate cybersecurity governance structures and coordination mechanisms, ensure a multidisciplinary approach to cybersecurity, and facilitate information sharing.

In the coming period, ICAO will continue to promote the improvement of the cyberspace security strategy, formulate a set of global principles, and raise the cybersecurity activities to a certain level, and coordinate with the safety and security management regulations.

3. Recommendations for next steps.

- Strengthen the publicity and implementation of cybersecurity awareness, take cybersecurity as an important part of aviation safety, and establish the habit of all employees to understand, support and participate in cybersecurity. Strengthen the self-education of network security, establish the era of network security, everyone is a pilot, and the mouse in his hand is the concept of the flight joystick, and mobilize all staff to strengthen network security by themselves. Strengthen network security capacity building, adopt regular online training, and replace training with exams, etc., to achieve the goals of protecting privacy for all employees, protecting corporate network boundaries, and denying unnecessary APP and network access.

- Build an information sharing platform. Enhanced data sharing of cyber threat information. The high-quality cybersecurity of civil aviation needs to realize threat intelligence sharing and collaborative linkage in the whole industry. It is necessary to co-create and share cybersecurity information big data collaboration, obtain real-time threat intelligence and risk notification and solutions, and continuously expand and share the case base for threat handling. Strengthen the building of its own anti-risk capabilities.

Conclusions

With the gradual acceleration of the informatization construction process, the importance of civil aviation network security has become increasingly prominent, and it is closely related to economic construction, national defense security and public interests. At the same time, civil aviation network security has gradually become an important part of information security. Scientific and effective coping strategies. It has important practical significance for clarifying information strategic planning, creating a sound information security management system, and promoting the effective and comprehensive development of the civil aviation industry.

References

1. ImmuniWeb. State of Cybersecurity at Top 100 Global Airports. 2020. https://www.immuniweb.com/blog/state-of-cybersecurity-top-100-airports.html.
2. Guidelines for Classification and Classification of Information Security Events (GB/T 20986-2007)
3. ICAO Aviation Cybersecurity Strategy https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx
4. Hu Haifeng. (2015). Research on Civil Aviation Information Network Security Construction. Information and Computer: Theory Edition (24), 2.