Background to the conference

We are witnessing an ever-greater reliance on digital technologies in the aviation sector, especially as both hardware and software become more interconnected, sophisticated and automated. These new opportunities also bring increased vulnerabilities. Digital technologies are essential for aviation operations as they are of vital importance in Communication, Navigation and Surveillance (CNS). Therefore, protecting these systems via cybersecurity has become a crucial aspect of ensuring the safety, security and efficiency of aviation operations around the world.

Cyberattacks are becoming more prevalent – indeed they are the 'new normal' – with the potential to cause accidents and incidents, reputational damage, loss of data, and/or cost money to resolve. Cybersecurity threats facing the aviation sector can include data breaches, malware infections, ransomware attacks, Distributed Denial-of-Service (DDoS) Attacks, and other forms of cyber intrusions that have the potential to disrupt services, compromise safety, or steal sensitive information. Further, no stakeholder is immune, whereby all are facing cyber-risks and must take measures to protect against them.

Cybersecurity in aviation is a serious issue that all aviation stakeholders must consider in seeking to not only to ensure safe transport of passengers and cargo but also to protect contractual partners, third parties and the stakeholders themselves. To increase cybersecurity, regulators at all levels must react to the threat of cyberattacks. The high safety and security standards practised by all stakeholders are essential to the expansion of the aviation sector, which with time is becoming ever more reliant on technology. However, these aviation rules were not drafted with cybersecurity in mind and general cybersecurity rules may not appropriately account for the specifics found within the aviation sector.

As the aviation industry continues to evolve with the adoption of emerging technologies like the Internet of Things (IoT), Artificial Intelligence (AI), and automation, cybersecurity will remain a critical area of focus to ensure the safety and security of aviation systems. Aviation cybersecurity requires a multi-layered and proactive approach to identify, assess, and mitigate cybersecurity risks, thereby safeguarding critical aviation operations and maintaining the trust of passengers and stakeholders, whereby law is a core element of this. As a result, the Leiden IIASL conference was a timely and important contribution to leading dialogue and moving the agenda forward.