ATM is changing rapidly. The industry already makes great use of information and communication technology but continuing innovation, the need for greater cost-efficiencies while improving safety and initiatives like SESAR and NextGen are promoting the spread of network-based technologies and integrated approaches.

The planned introduction of system-wide information management (SWIM) will see even greater exchange of data and information, with the various systems becoming more closely integrated. There are clear operational benefits to these developments but also risks in the form of greater security vulnerabilities. Cyber security threats range from simple acts of digital vandalism to major cyber attacks.

Cyber security threats should not be seen as a new phenomenon that does not yet need a sophisticated defence, agrees Steve Daniels, Aviation Security Strategist at HP Enterprise Security Services. “Cyber security and information security are a spectrum, a continuum, demanding a more complete response,” he says.

ATM must tackle cyber security by assessing the vulnerability of processes, assets and, particularly, IT infrastructure to criminal activities and attacks, whether these involve staff or outside parties. The wide range of potential cyber threats and the integrated nature of modern ATM demands a holistic approach and the involvement of all ATM stakeholders.

Challenges in cyber security
CANSO is actively engaged in cyber security issues affecting ATM. At the March meeting of the ICAO Aviation Security Panel, CANSO argued successfully that risk assessments for ATM systems should take account not only of terrorist related attacks but also include attacks perpetrated by hackers to gain access to systems or cause disruption for non-terrorist purposes, or attacks carried out for espionage or commercial purposes or activities by State actors. These can be equally disruptive and compromise the safety, security and integrity of the aviation system. The Panel agreed and recommended that ICAO should develop best practices guidance for States and ANSPs against cyber attacks.

Barnabas Kis, Chief Technology Officer, HungaroControl – who took part in a panel discussion on the subject organised by Frequentis at World ATM Congress 2014 – believes cyber security has yet to become an established part of ATM culture. Unlike safety, cyber security has yet to become embedded into daily operations. “That has to change,” he insists. “Designers, developers, operators, decision-makers and regulators need to have a good understanding of the context of cyber security risks and how to mitigate them during everyday work.”

The industry and its customers have benefited enormously from the development of a safety culture: an awareness of safety issues and priorities that pervade the thoughts and actions of all staff within an organisation. The industry needs to equally develop a security culture.

Cyber threats should not be seen as a new phenomenon that does not yet need a sophisticated defence, agrees Steve Daniels, Aviation Security Strategist at HP Enterprise Security Services. “Cyber security and information security are a spectrum, a continuum, demanding a more complete response,” he says.

Multiple actors
Clarifying the role of regulation, including cross-border issues, and the potential for collaborative security policy approaches is equally crucial.

Promotion of cyber security requires work on a number of fronts including public awareness campaigns and strengthening cross-border cooperation and information exchange. For example, in 2013 the European Commission proposed a Network and Information Security (NIS) Directive to ensure a uniform level of cyber security across the EU, and has set up a permanent Computer Emergency Response Team (CERT-EU) for the EU institutions, agencies and bodies. And, some governments such as the UK have introduced critical national
infrastructure (CNI) legislation and regulations to protect infrastructure.

“Standards capture today’s best practice,” notes Daniels. “But they have often been watered down or undermined by governments and by procurement departments. We need more of them specified in programmes and true compliance and/or formal certification delivered following good ‘secure and privacy by design’ practices that take security and privacy into account as part of a systems engineering approach.

As cyber security represents a new area in ATM, Michael Standar, Chief Strategies and International Relations, SESAR Joint Undertaking, agrees that cyber security would probably need to be further regulated and standardised to harmonise appropriate skills, training and security management. He notes that policies and guidelines are available for joint cross-border operations in the functional airspace block context but the implementation of these guidelines offers an opportunity for further enhancement and harmonisation.

Multiple actors have a role to play in protecting and defending critical aviation systems against cyber security threats. It would be beneficial for aviation security regulators and stakeholders to establish clarity on the areas where they could take on a leading role and responsibility for ensuring the cyber security of critical aviation systems. A joined up or “system of systems” approach to aviation security is needed, both to thoroughly understand the threats and to enable effective mitigation.

Understanding the risk
For now, work continues on protecting the confidentiality, integrity and availability of ATM systems and services. “When we talk about cyber security we have to consider not only system-related perspectives but processes and human-related factors as well,” Kis says.

An obvious first step is analysing system-wide technical vulnerabilities and potential threats. This includes internal and external threat actors, sabotage, data theft, denial of services and natural hazards. Once the probability of a potential security incident is understood, it becomes possible to prioritise the necessary mitigating actions and develop risk-based proportional security safeguards.

Standar points to SESAR as a mechanism to understand and develop requirements and system solutions together. SESAR deployment will allow all stakeholders to understand the requirements needed to handle cyber security threats to ATM in general. CANSO’s recently established ATM Security Workgroup (ASWG) has also taken on the task of developing guidance material to address the cyber threat. This will include development of industry policy positions based on lessons learned and recognised best practices; advocacy for risk-based regulations that will support information sharing; communications to raise awareness of cyber security; and collaborative approaches to sharing threat information, incidents and mitigation strategies across the industry. Through such a comprehensive strategy and collaborative approach, it is expected that the ANSP community will be well-positioned in dealing with the cyber threat in a proactive manner.

Cyber security demands continual attention. Protective mechanisms need developing, monitoring and adjusting, based on robust practical testing, and on awareness and assessment of relevant developments and threats. In the final analysis, there is a clear link between the security and safety of the aviation system.

The recently published CANSO Cyber Security and Risk Assessment Guide provides air navigation service providers with an introduction to cyber security in air traffic management. It includes an analysis of the cyber threats and risks and motives of threat actors; some considerations for managing cyber risks; and suggestions for implementing a cyber security programme.