ICB

Industry Consultation Body

POSITION PAPER

Regulatory Response to ATM Cyber-Security

Increasing reliance on inter-connected ATM systems, services and technologies increases the risk of cyber-attacks. Such risks undermine the vision of a safe, resilient and trustworthy European aviation sector, and would incur costs on the response to and recovery from cyber-attacks. Member States and operators are increasingly dependent on each other for their security, as cyber-attacks can easily propagate or be replicated across international borders. If information about previous attacks is not exchanged then neighbours cannot protect themselves and the industry cannot accurately assess the probability of a future attack.

The ICB supports a European response that first understands the risks and then establishes mitigating measures. Such a European response must support equivalent activity at national and operator levels. The ICB considers that the regulation may need to be extended and/or streamlined, but at the moment efforts should be focused on understanding the risks and building a holistic, coherent, affordable and adaptable response. Greater clarity is required in the allocation of responsibilities for these tasks.

This paper was adopted at ICB/57 on 10th September 2015.

1 CONTEXT

As part of the 2015 ICB Work Programme, the ICB committed to advise the European Commission on the regulatory response to ATM cyber-security. Cyber-security is an emerging topic in ATM, and the industry must address growing concerns about the risks from increased automation, connectivity and reliance on digital information and systems. However, at present there is little by way of vision or consensus on what is an appropriate response, particularly in terms of new or revised regulation. This paper summarises ATM cyber-risks as currently understood, the required response to these risks, the current regulatory response and how further regulation should be approached.

2 CYBER-RISKS

Whilst cyber-security has no universally accepted definition, the central concept concerns preventing, detecting and responding to malicious attacks aimed at adversely impacting the confidentiality, accuracy, integrity or availability of digital systems and services. Resilience – the ability to return to operations following a cyber-attack – is increasingly seen as important because the prevention of attacks cannot be guaranteed. Sometimes, particularly when widened to information security, the scope of cyber-security also includes accidental system failures and sabotage. The range of potential attackers is broad, including state-sponsored parties, organised crime groups, individual hackers and staff within the industry (the 'insider' threat). There is a clear link with safety, but the impact from cyber-attacks is not limited to safety of life, and may more commonly be economic and reputational.

To date ATM, being a closed system consisting of mostly proprietary systems, has been well-isolated from cyber-attacks. However, a combination of factors means that the risk of significant cyber-attacks is increasing:

- Increasing automation and dependence on digital systems
- Growing need for interoperability (including between ground and air)
- Moving to a network-centric architecture
- Increasing use of common and COTS components, as well as open standards
- Mixing legacy and new systems
- Extending to new end users
- Increasing capabilities of threat actors

Importantly, increasing interconnectivity and potential shared use of common components means that Member States and operators will be more reliant on each other for their own cyber-security. Attacks are likely be targeted to enter via weak points in a network before propagating across the network, and thus there is a risk of cascade failures of the network. Questions of trust and assurance will be paramount.

There is a particular concern in ATM given that the suspicion of a cyber-attack may be sufficient to close the skies for prolonged periods until a system can be demonstrated to be 'clean'. Such a demonstration is very hard to achieve without advanced data and system 'health' monitoring capabilities.

Work to assess the specific risks has started, but there is neither a complete nor common understanding of European ATM's current and foreseeable-future

vulnerabilities, threats and risks. Similarly, ICAO and some operators have made some headway, but no common and complete understanding has emerged. Establishing effective mechanisms for the exchange of comparable data on previous attacks is essential as the probability of an attack on a network cannot be accurately assessed if attacks on neighbouring networks are unknown. Under-reporting leads to an under-estimate of the risks.

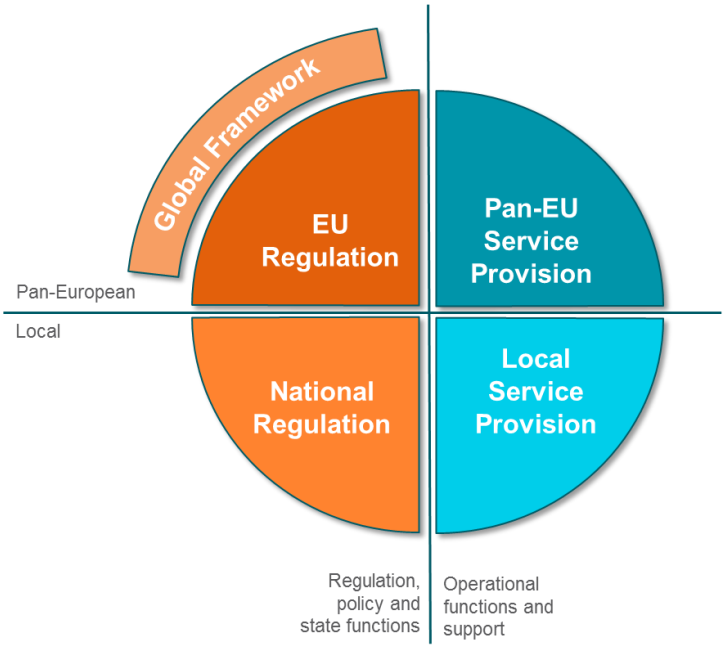
Furthermore, vulnerabilities and threats change regularly, and cannot be predicted too far ahead. Regular review of risk assessments will be necessary.

A common and robust understanding of cyber-risks is vital to inform policy and regulatory decisions on appropriate responses. Risk tolerances, risk containment and the potential cost of specific responses also need to be better understood.

3 ATM'S RESPONSE TO CYBER-RISKS

The response needs to be proportionate to the risk posed and adaptable as the risks change. The response also needs to be multi-level, coherent, holistic, affordable and, of course, effective. ATM can make use of good practices from other industries, but these will need to be tailored to ATM.

To improve ATM cyber-security there is a need to strengthen all parts of the EATMS – pan-European, regional and national; regulation, operations and supply chain. All actors have some responsibility for ensuring sufficient mitigations are in place.



A coherent response is needed from regulators and industry

Many of the required mitigations need to happen at the operational stakeholder level. Thus ANSPs, airports, airspace users and other service providers need to develop individual, but coherent, responses. The supply chain under each provider's responsibility also has to establish a response that further engenders trust.

The EU Cyber-Security Strategy[1] acknowledges that it is predominantly the task of Member States to deal with security challenges in cyber-space. Member States are sovereign in cyber-defence and are best-placed for understanding particular threats according to their geopolitical context. However, because of the inter-dependence of ATM stakeholders, and because of pan-EU service provision, a common and harmonised response is also necessary. The European regulatory environment for ATM is therefore crucial. Of course a European response, in turn, needs to be guided by the global response and requirements for cyber-security, including coordination with the ICAO Aviation Security Panel.

The response must be holistic. Addressing the issue purely at a technical level is insufficient. A holistic response includes institutional policies, human factors (training, expertise, culture, etc.) and (pan-)organisational processes. A holistic approach also includes through-life concerns, so that the response starts from the design stage and ends with decommissioning for technical systems, and is a continual improvement cycle for management. For example, the industry needs to consider how best to secure legacy systems that were designed when cyber-security was not a significant concern.

The response should include both short-term actions and longer-term programmes to establish the standards and security management systems that ultimately provide integrated protection for Europe. In the short term, actions could be taken to improve cyber-security and resilience – for example incorporating elements into ATCO / ATSEP training (there are a number of air traffic simulators in Europe which could be used extensively in order to build operational expertise and to train ATCOs and ATSEPs), developing guidance material for security management systems, further testing of European contingency mechanisms, and integrating cyber-security into new concepts such as SWIM and i4D. Safety and security standards need to be made compatible, if not combined as part of an integrated approach to risk.

Cyber-security needs to be affordable for the industry but engineering cyber-security retrospectively is expensive, difficult and slow. Starting work early will reduce costs in the long term. A Cost Benefit Analysis (CBA) is needed to inform the scale and scope of the industry response. However, since security breaches are expected to be high impact but rare, such a CBA will be challenging. A true understanding of cost may come iteratively over time. Costs that are passed onto others (eg to airspace users) should be determined transparently and agreed with those affected.

ATM is not alone in facing cyber-risks and can build on the guidance and services available to other industries. However, ATM, as a regulated safety-critical industry, does have some specific requirements that may run counter to other industries' good practice. Therefore tailoring guidance to the ATM environment is crucial.

4 CURRENT REGULATORY RESPONSE

ICAO Annex 17 considers security as a whole (rather than specifically cyber-security), and recommends that each State develops functions to protect systems used for civil aviation purposes from interference that may jeopardise the safety of civil aviation, as well as implement procedures to share threat information. The ICAO Aviation Security Manual (Doc 8973) assists in Annex 17 implementation, and has been revised to contain minimum measures to protect critical information systems. The ICAO ATM Security

[1] European Commission (2013) The Cyber-security strategy of the EU - An Open, Safe and Secure Cyberspace.

Manual (Doc 9985) provides guidance to assist States and service providers to meet security requirements, and covers controls to ensure confidentiality, integrity and availability of information. Finally, the ICAO Aviation Security Panel, is actively furthering the ICAO response to cyber-security. However, these are high-level documents and there is an urgent need for more specific guidance that can be applied by operators across Member States.

The European Commission has developed a general Cyber-Security Strategy for the European Union setting out key roles and responsibilities and emphasising information sharing and coordination. The EU Cyber Defence policy framework[2] has been developed to assist in cyber-defence aspects of the EU Cyber-Security Strategy. Whilst these are not specific to ATM they do help to inform a regulatory framework.

DG CONNECT have produced a draft directive, the Network and Information Security (NIS) Directive, designed to ensure a high common level of network and information security across Europe. This reflects considerable diversity at the Member State level, but, as a directive, will not guarantee a harmonised approach across States. The NIS Directive is applicable to critical infrastructures, but the extent to which ATM will be classified as a critical national infrastructure is unclear.

Core SES regulation (e.g. (EC) No 549/2004, as amended) states that security governance is a Member State matter and States have the power to implement appropriate measures to safeguard the public. ANS common requirements legislation ((EU) No 1035/2011) sets out high-level requirements for a security management system. EASA's draft ATM IR strengthens these requirements. Some regulations, for example the ADQ IR ((EU) No 73/2010), are more specific on security requirements, including cyber-security. There is no specific European regulation for airspace users and airports.

EN 16495:2014 defines guidelines and general principles for the implementation of an information security management system in organisations supporting civil aviation operations. As a European Standard it is automatically a national standard across Europe. EUROCAE ED-201 (in development) will provide framework guidance for aeronautical information system security and address ground systems.[3]

Coordinating the multitude of activities and bodies on this topic is crucial.

5 ICB POSITION ON REGULATORY RESPONSE

The European regulatory environment provides a means to mandate minimum ATM standards, and more generally provides mechanisms for harmonisation across Member States. A harmonised approach to cyber-security is vital. The ANS common requirements legislation could be a suitable way to mandate cyber-security requirements for ANSPs, although the airport and airspace user response should also be considered.

However, at the moment the regulatory response on cyber-security is fragmented and constantly evolving. Therefore the ICB makes five recommendations:

[2] European Commission (2014) EU Cyber Defence Policy Framework.

[3] EASA's airworthiness rule and EUROCAE ED-202A go some way to support operators to address cyber-security from an airborne perspective. Further EUROCAE standards (e.g. ED-203) are in development and will further support efforts at the aircraft level.

1. The ICB recognises that cyber-attacks pose real risks to European ATM. A suitably scoped risk assessment, using a standard assessment method and reflecting real data on previous attacks, would inform the regulatory response. **As a first step, the ICB urges the Commission to ensure that a detailed cyber-risk assessment is undertaken.**

2. Retrospectively engineering cyber-security will be expensive, difficult and slow, but a mature understanding of the costs is needed. An initial CBA should be undertaken to understand the risk-cost trade-offs and the expected costs to stakeholders. Furthermore, to achieve a coherent response, it needs to be considered in a harmonised manner for all ATM initiatives. Coordination and governance mechanisms should be established to support a coherent approach. **In further developing the response, the ICB considers it necessary to ensure cyber-security is addressed early on in all current and future ATM initiatives in a coordinated and coherent approach.**

3. Over regulation must be avoided, but if further regulation is necessary it must be flexible, fit for purpose, implemented at the right time and driven by a robust understanding of the cyber-risks. At present there are poorly coordinated 'flows' of regulation that can apply to ATM: that which targets critical infrastructure (national and European) and that which targets civil aviation. Aligning these would make requirements clear and compliance easier. Piecemeal regulation should be avoided in favour of a coherent framework. **The ICB recommends continued monitoring of the regulatory environment and that the principles of Better Regulation[4] are applied, by regulators competent in cyber-security, to ensure that appropriate measures are taken in agreement with the industry.**

4. Regulation needs to be accompanied by clear Means of Compliance (MoC) and Guidance Material (GM) such that stakeholders can demonstrate compliance in a cost-effective manner against standard levels of assurance. **The ICB supports, as a crucial step, the development of MoC and GM for existing and proposed regulation on cyber-security.**

5. Enforcement needs to be proportionate to risk and could provide a common approach to support industry in assessing and responding to interdependent risks between operators. Such an approach needs to respect national laws and regulations. **The ICB supports a common approach to incident reporting and auditing, provided measures are established to protect sensitive information.**

Overall, the ICB considers that the regulation may need to be extended and/or streamlined, but at the moment efforts should be focused on understanding the risks and building a holistic, coherent, affordable and adaptable response.

The ICB must continue to be engaged in a carefully planned regulatory response because there is a danger that the industry may be compelled to meet requirements that are uneconomic or impractical within an operational context, or are so general as to provide little assurance against threats to the Single European Sky.

[4] See http://ec.europa.eu/smart-regulation/index_en.htm