EGHD Expert Group on the Human Dimension of the Single European Sky

EGHD Paper | Issue | 13 March 2024

Human dimension aspects in ensuring a cyber-secure ATM environment

1 INTRODUCTION

1.1 Context

Modern Air Traffic Management (ATM) is based upon an ever-increasing degree of digitalisation to allow for improvements in operational efficiency, and to facilitate greater capacity whilst upholding existing safety standards and thereby supporting the policy objectives of the Single European Sky. At the same time, digitalisation and automation can contribute to the development of new tools in support of front-line actors.

A digital revolution in ATM is expected in the near future with the implementation of new digital concepts such as remote operating towers, ADSPs, virtual centres and ATM interaction with U-space. In addition, one can observe an increased use of space-based CNS services to provide surveillance, navigation and real time voice data communication services through Low Earth Orbit Satellites. The increased interconnectivity between different actors in ATM, driven by new concepts and technologies, alongside existing technologies requires a cyber-secure CNS/ATM environment that is reliable, effective and safe. As a result, cybersecurity is transversal to all ANS and is both a present and future challenge for the ATM system.

Cybersecurity plays a crucial role in ATM operations as it ensures the confidentiality, integrity, continuity and availability of critical systems and data information.

In recent years, the scale of cybersecurity attacks and threats within European aviation has grown exponentially, with a 530% year-on-year rise in reported cyber incidents from 2019 to 2020[1]. In 2020 EUROCONTROL's EATMCERT (European Air Traffic Management Computer Emergency Response Team) registered a total of 1260 cyber-attacks. The distribution of market segments impacted by cyber-attacks was heavily weighted towards airlines (61.5%), followed by the manufacturers (16.3%) and airports (14%), with around 6% of cyber-incidents impacting ANSPs[2]. However, a cyber-attack on an ANSP can have a wide-reaching impact, potentially leading to the closure of national airspace or even to the loss of life.

It is crucial for the safety and security of European aviation that cybersecurity within the ATM system evolves to cope with the increasing sophistication of cyber-attacks and that mechanisms for dealing with existing cyber threats remain effective. As the scope for digital and space-based applications increases within ATM, the same goes for the risk of exploitation of these new services.

The required approach for dealing with cybersecurity cannot only consider technology, but also the human factors, ensuring human operators can effectively help to prevent, avoid, and address a cyber-attack. This includes ensuring individuals can effectively identify when they are under a cyber-attack and have the necessary skills to respond to and recover from a cyber-attack.

EUROCONTROL's report 'Air Traffic Management A Cybersecurity Challenge' considers at a generic level the challenge to the ATM system of cyber-threats. However, with human operators of systems often targeted as points of weakness by attackers, the **EGHD in this position paper considers the human dimension aspects related to ensuring cybersecurity in ATM, in particular within the boundaries of the ATM functional system**. Whilst not a focus of the proposed position paper, the cybersecurity of the business organisation (which includes office computer systems, email platforms, file storage systems, etc) is addressed where this is necessary to support the analysis of cybersecurity aspects related to the ATM functional system.

The impact of cyber-threats on the day-to-day duties of front-line actors can be significant and should be appropriately managed to ensure the continuity of safe and secure operations. With the ATM functional system comprising of people, procedures and equipment, this position paper provides recommendations on the means (trainings, operational procedures) and the tools (technological solutions) to enable the human to handle existing and expected cybersecurity challenges.

---

[1] *https://www.eurocontrol.int/sites/default/files/2021-07/eurocontrol-think-paper-12-aviation-under-cyber-attack.pdf*

[2] *https://www.eurocontrol.int/sites/default/files/2021-12/eurocontrol-atm-cybersecurity-report.pdf*

The recommendations included in this paper are derived from EGHD members' inputs and experience of cybersecurity challenges and lessons learnt within ATM.

1.2 Scope

This position paper directly captures the views expressed by EGHD members on the **implications for human factors and human performance to ensure a cyber-secure ATM functional system.**

The three questions this paper seeks to address are as follows:

- How is the human in ATM currently impacted in their day-to day work by preventing and responding to cybersecurity attacks and by existing cybersecurity procedure requirements (e.g. to protect/avoid, detect, respond and recover)?
- What are the lessons learnt from existing cyber-incidents with implications on the HF/HP of the human in ATM?
- What additional human dimension implications are predicted in the immediate future? i.e. with the increasing digitalisation of the ATM sector, increased cybersecurity awareness, increased use of space-based CNS services and with the integration of new business models and concepts such as ADSPs, virtual centres, remote towers and U-space.

Based on these questions, the EGHD proposes pragmatic recommendations to address the challenges and to put in place the improvement measures identified.

This position paper focuses on the following front line actors in the ATM system currently affected by cybersecurity implications in their work:

- ATCOs;
- Manned aircraft pilots;
- ATSEP;
- AIS/AIM staff (e.g. AIS -PUB, NOF- NOTAM-Office, ARO, AIS AD, Chart staff);
- other ATS personnel such as: FDA, FDS, FDP, FMP, Flow Coordinator, Data Assistant, FISO and AFISO, Clearance Delivery, Apron Control, COM -AFTN, Aeronautical Radio Station – HF/VHF Freq. staff);
- frontline managers e.g. Supervisors (ATCO, ATSEP).

This paper only considers cybersecurity implications in the perimeter of operations undertaken by the human operators listed, when linked to the functional system as established in (EU) 2017/373. It seeks to address members' concerns related to cybersecurity implications for human operators in the short and medium term.

1.3 Structure of the paper

This paper is structured into three chapters, namely:

- **Section 1 Introduction –** introduces the context of this paper, its scope and provides a summary of the relevant regulatory framework.
- **Section 2 Human dimension challenges related to cybersecurity in aviation**Human dimension **–** presents the current and expected future human factor and human performance implications associated with ensuring a cyber-secure ATM environment.
- **Section 3 Recommendations to address human dimension challenges related to cybersecurity in aviation –** presents a series of recommendations proposed by the EGHD addressing the current and expected future of human factors and human performance implications associated with ensuring a cyber-secure ATM environment.

This paper is also supported by the following annex:

- **Annex A** - the acronyms table.

1.4 Regulatory framework

There have been many developments in European cybersecurity policy and regulation in recent years. Although the focus of the position paper is on exploring the practical cybersecurity experiences and lessons learned provided by members any recommendations and conclusions drawn take into consideration the existing regulatory environment. Consequently, for contextual purposes, a summary of existing European cybersecurity policy and regulatory activities is provided below:

- **Commission Implementing Regulation (EU) 2017/373** lays down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight. On the specific area of security management, it stipulates that air navigation services and air traffic flow providers take the necessary steps to protect their systems and take the necessary mitigations to prevent cybersecurity threats which may have an unlawful interference with the provision of their service. The regulation stipulates the processes to be followed by service providers to handle change management and safety assurance of their functional system defined as '*a combination of procedures, human resources and equipment, including hardware and software, organised to perform a function within the context of ATM/ANS and other ATM network functions*.' The regulation also defines air traffic safety electronics personnel (ATSEP) as the '*authorised personnel who are competent to operate, maintain, release from, and return into operations equipment of the functional system*'.
- EASA is working to establish regulation in the area of cybersecurity in ATM. **EASA released RMT.720** in 2019 to address high-level, performance-based requirements on the management of cybersecurity risks for organisations in all aviation domains. ATM/ANS providers are one of the domains that this Rule Making Task is applicable to. The RMT.720 led to publication of (EU) 2023/203.
- **EASA's Part-IS regulation**, **Commission Implementing Regulation (EU) 2023/203**, provides the regulatory framework for the regulation of information security in ATM. It introduces requirements for ANSPs in the identification and management of information security risks which could affect information and communication technology systems and data used for civil aviation purposes. It sets requirements for the detection of information security events, identifying those which are considered information security incidents, and then responding to, and recovering from, those information security incidents to a level commensurate with their impact on aviation safety. Part-IS provisions will be applicable from October 16, 2025, for organisations in the scope of the delegated act and from February 22, 2026, for all other organisations and competent authorities covered by the implementing act. EASA has also released NPA 2023-102, with proposed AMC and GM to Regulation 2023/203, subject to a focused consultation. The AMC and GM amongst other things look to address issues regarding the information security risks related to interfaces between organisations, identification of threat scenarios and risk assessment, and approaches to evaluating staff competency.
- EASA is also involved in the development of industry standards through EUROCAE Working Group 72 on information security, which is investigating various aspects of aeronautical systems security. Their work will eventually form the basis of regulation. The work of this group is complementary to Part-IS regulation.
- ICAO is currently investigating how to extend existing regulation to consider cyber. It has set up a study group called the Secretariat Study Group on Cybersecurity (SSGC) to conduct a review of ICAO annexes to consolidate standards and recommended best practices related to cybersecurity.

Alongside the above regulations which are focussed exclusively on aviation, generic security regulations applying to critical national infrastructures within EU member states have also been formulated. The context of these regulations is provided below:

- **NIS directive (EU) 2016/1148** covers network and information systems and services playing a vital role in society. It defines "OES" (Operators of Essential Services) and "DSP" (Digital Service Providers) and has a particular focus on OES for critical national infrastructure. The regulation defines the coverage of key sectors needed for the economic stability of the EU and it stipulates that enforcement measures for failing to comply are considered on a case-by-case basis. This regulation is managed via the European Union Agency for Cybersecurity (ENISA) and as an implementing rule, each state has a responsibility to pass it into state law.

2 HUMAN DIMENSION CHALLENGES RELATED TO CYBERSECURITY IN AVIATION

Following discussions with EGHD members, human factor and human performance (HF/HP) challenges related to ATM cybersecurity, which are not currently addressed by the regulatory framework and existing working arrangements, were identified. These challenges have been described under different topic areas in this section and summarised in section 2.3.

Proposed recommendations on how to address these challenges in the short to medium term are presented in section 2.3.

2.1 ATM cybersecurity: protect, avoid, detect, respond and recover

2.1.1 New policies and procedures

There are often different levels of procedural awareness across the various roles within an ANSP (senior management, ATCOs, ATSEP, etc) when a cyber-attack takes place. Procedures to deal with cybersecurity events are not yet sufficiently developed to take operational, tactical, technical and security aspects fully into account. For instance, where operational arguments deal with safety and stabilising a situation, from the technical point of view the focus will be on isolating and resolving the problem, and from a security perspective the focus will include evidence gathering for further investigation and forensic research.

These different perspectives impact the response to a cyber event, since the coordinated response has to follow a compromise between isolating or shutting down the system (and even potentially close the sky...), and the safety reaction being to avoid shutting down the system at all costs (or maintain the operations at all costs). The post cyber-incident period will also be a demanding process requiring compromise and coordination.

Even though there are procedures in place to respond to system outages these do not fully cover cyber-attacks/threats. This means that ATM staff may be unsure of how best to act when a cyber-attack takes place. It is therefore **critical to have a well-thought through approach with clear processes to drill reaction and recovery action to cyber-events**, **detailing the do's and don'ts in case of a specific cyber-event.** New procedures have to be developed with the involvement of ATM front-line operators (e.g. ATSEP, ATCOs, etc) and implemented together with new adapted training protocols and emerging cyber tools as noted in section 2.1.8.

The approach to be followed should include:

- **Implementation of cybersecurity management procedures in order to protect, detect, respond and recover from a cyber-attack**. Until now this has not been considered because detection and correlation capabilities did not exist. Once these capabilities are implemented (e.g. in a Security Operations Centre – SOC) the situation will evolve, allowing the "whole affected area" to be accessed when an event occurs as opposed to managing the affected area "locally/manually". It should be noted that sometimes cybersecurity events are "masked" by technical events and reported to the safety line.
- **Establishing a decision-making policy accounting for cyber-related events**. Cyber-events may require decisions that differ from the usual day-to-day business. Thus, the decision-making process must be redrafted accordingly, and must take into account operational aspects.
- **ATM stakeholders, in particular ANSPs, to create cyber-attack exercise scenarios and to develop related recovery plans, validate them, prepare to implement them**. This means reviewing cybersecurity measures, identifying the tools, training the different actors, and amend backup and contingency policies (for both hardware and software) as well as related operational procedures. Some important aspects to be considered in these plans are:
  - **Resilient contingency plans** to maintain essential services at any cost.
  - A minimal **set of regression tests for system patches**. The implementation of system patches because of a cyber-event needs to be done as soon as possible. Not only the patch application, but also the minimal set of regression tests to validate the system's functions. If the tests are not defined

beforehand, high stress levels and inexperience can subsequently lead to insufficient regression testing and unexpected system behaviour.

- **Methodology and tools to collect and record data related to the cyber-event**, since this data can support the forensic analysis and continuous improvement of the protection and response to these events, including safety investigations.

- **Develop the ANSP cybersecurity policy** according to the relevant regulations.
- **Implement** state of the art **cybersecurity tools**, such as detection tools for the ATSEP working position and wherever else is deemed necessary.
- **Intuitive Human-Machine Interfaces together with appropriate user training.** Intuitive interfaces displaying relevant information (such as system changes and potential risks) which support the operators in the detection and response to potential cyber-threats promptly.
- **Adaptation of the service level requirements in contractual and procurement procedures** to ensure external service providers and associates are aligned with the ANSP's cybersecurity policies. This aspect is particularly important with increasing externalisation of services and increasing interconnectivity. Outsourcing of infrastructure and system support requires additional arrangements for coordination and information provision in case of cyber-related events. This should be agreed between the parties involved, to prevent any misunderstanding or misalignment of expectations when a cyber-event occurs. The balance between information sharing and confidentiality should be clear.
- **Sharing of best practices and lessons learnt by the aviation community.** Collaboration among industry stakeholders, including ATM organisations, regulators, and cybersecurity experts, is essential. Sharing best practices, lessons learned, and threat intelligence can strengthen cybersecurity across the entire industry. Establishing forums, information-sharing platforms, and regular communication channels can foster collaborative efforts to address cyber-threats effectively. Lessons learned from past incidents should be used to continuously improve cybersecurity measures, adapt to emerging threats, and implement necessary updates to policies, procedures, and technologies. Coordination with all stakeholders is necessary to identify points of weakness. This is important for the human in ATM as a cyber-policy that is not aligned with the policy of other stakeholders that they work closely with may lead to a lack of clear understanding of their individual responsibilities.

2.1.2 Staffing, workload, and rostering for ATM cybersecurity

New cybersecurity policies and processes will have a strong impact on the staffing and workload of ATM front-line operators, in particular ATSEP, a category already undergoing challenges in relation to **staffing, workload, and rostering. These have a negative consequence on ANSPs' capacity to effectively facilitate innovation whilst continuing running the normal activities related to the maintenance of ATM/CNS functional systems**. This problem arises from a combination of factors:

- ANSPs' difficulties in attracting, recruiting and retaining new ATSEP at a time in which the existing ATSEP population is aging and moving towards retirement. The difficulties in recruiting are linked to competition with other more attractive industries combined with the increased responsibilities and liabilities connected with working on operational CNS/ATM systems and the lack of clearly defined career paths for young professionals (that you may find in other industries).
- Increased workload of ATSEP staff with introduction of cybersecurity related policies and tasks, and lack of understanding of the time and effort these will require. The increasing digitalisation of CNS/ATM systems usually results in an increase in cybersecurity related tasks, but currently it is unclear how exactly the workload will be affected. Since some cybersecurity related activities for the ATM/CNS functional system do not result in visible improvements in terms of functionality or system performance for the end users and management, during the planning phase the effort these require is often underestimated or not sufficiently accounted for.

Furthermore, since cybersecurity is still a relatively recent concern, **ATSEP would benefit from the expertise and support of cybersecurity experts** while preparing and addressing cyberattacks. This support could help to ease the workload and knowledge pressures on the ATSEP.

The staffing issues resulting from the increase in cybersecurity policies and processes are not solely a concern in the ATSEP domain. The **AIS/AIM workforce face similar workload and staffing pressures**. This has come about due to the increased cybersecurity demands coinciding with the transition from paper-based to digital AIS/AIM services, and is intensified by the current ageing of AIS/AIM staff.

These **staffing, workload and rostering challenges are aggravated by the introduction of urgent cybersecurity policies and demands and by the need to immediately address critical vulnerabilities in infrastructure or software. In parallel to this there are pressures in responding to modernisation (e.g. digitalisation) and to the continuous maintenance and operation of existing ATM/CNS functional systems.** Furthermore, as the current level of cybersecurity maturity in the ATM sector is still relatively low in comparison to other industries, additional effort is required to compensate so that cybersecurity is assured. This includes not only effort in preparing and implementing new processes, but **also effort in the preparation and attendance of additional trainings and simulations**. For example, it requires a considerable amount of time to train ATCO OPS supervisors in developing and maintaining high level competences. Staffing numbers might need to be revised to cover for the new activities and training needs. Moreover, front-line operators such as ATCO experts need to be involved in the decision-making process when defining cybersecurity procedures.

2.1.3 New competences and training requirements for ATM cybersecurity

Insufficient or inadequate training of ATM personnel in cybersecurity directly impacts the cybersecurity of the system. Human error, a lack of awareness, and complacency can significantly contribute to a successful cyber-attack. By prioritising training, education, and awareness, organisations can mitigate cybersecurity risks. The human in ATM needs to be competent and sufficiently trained to perform their role in defending the ATM system from cybersecurity threats.

New competency needs

As ATM/CNS technology evolves, cybersecurity will need to evolve as well. This means **entry qualifications and competency schemes for ATM personnel must be updated accordingly**. This applies in particular to ATSEP, ATCO OPS supervisors and FMP experts who will need to update their cybersecurity knowledge to keep pace with changes in technology. Proper expertise and understanding of cybersecurity will help ATSEP, ATCO supervisors, and other ATM staff, in their decision-making when defining and implementing adequate operational decisions to avoid or respond to cyberattacks. Cybersecurity experts alone would not be able to properly measure operational consequences.

Similarly, aeronautical information management is changing from paper-based to digital, and the ever-increasing demand for reliable information, leads to new cybersecurity risks that have to be handled by AIS/AIM staff. These aspects need **to be considered in the setting of competency requirements for AIS/AIM professionals**.

The advent of AI powered automation tools and the accelerated implementation of new systems increases the risk that ATM staff will have a reduced understanding of the systems they interact with. The proficiency of ATM staff in operating these new systems needs to be reflected in the competency requirements of ATM professionals.

New training needs

Cyber incidents emphasise the need for **robust training programmes that address the specific cybersecurity aspects that affect ATM professionals**.

Training should be undertaken by a whole range of ANSP staff, including front-line staff (e.g. ATSEP, ATCOs, FMPs, AIS/AIM staff), ATM instructors, and administrative/IT staff. Training should cover the best practices to identify, protect and avoid cybersecurity risks, as well as how to detect, respond and recover from cybersecurity incidents. The training should cover topics such as protection against phishing, secure password management, incident reporting procedures, best practices, and information sharing.

Regular refresher courses and updates on emerging threats are essential to maintain high levels of situational awareness and cybersecurity resilience.

Some important aspects to be considered in the development of cybersecurity training programmes include:

- Cross fertilization with other safety critical or transport industries (e.g. how is the rail or the nuclear industry addressing cybersecurity and related technical failures?)
- Playbooks for specific cyber events. These must be developed, validated, trained, and updated as the cybersecurity landscape evolves.
- Periodic simulation of cyber-crisis scenarios with all involved teams and departments. Different levels of familiarity with cyber-related events and the way to handle them can lead to misunderstanding and frustration between different teams. These scenarios should include management and corporate communication teams that deal with social media and external stakeholders. In such cybersecurity simulations, it will be important to understand the impact on the workload of the ATCO in the controller working position in scenarios using real life traffic samples.
- Collection and recording of cybersecurity issues/attacks data for posterior forensic investigation. Different cybersecurity issues/attacks require specific actions to ensure that not only the impact is minimised, but also that relevant data is not destroyed during the response. This data can support the criminal investigation and the continuous improvement of the protection and response to these events. Training is required on the methods and tools to collect and record this data (e.g. to replay the incident offline).

2.1.4 New roles and responsibilities for ATM cybersecurity

ATSEP are the sole authorised personnel to access and intervene ATM/CNS functional systems, thus they are the 'first responder' to cyber-attacks to the ATM/CNS functional system. This includes the responsibility to detect (a shared responsibility with the Security Operations Centre of a national cybersecurity centre) and contain the event, securing evidence for forensic analysis, and to restore the service delivery. When a malfunction due to a potential cyber-attack is identified, infected processes or servers would normally be taken offline or switched off, but it is only the ATSEP on duty in coordination with ATCO OPS supervisor who can decide what to do and which ATM/CNS configuration is the most appropriate. This involves deciding the safest means to guarantee optimum/maximum delivery of service (even if degraded) and to ensure that data relevant for a forensic analysis is not lost.

As systems become ever more interconnected, greater **cooperation between the ATSEP**, ATCO OPS supervisor and **the cyber-expert is crucial** during the handling of a cyber event since their expertise are complementary. For example, the **ATSEP can assess the impact of the event on the functional system** and perform the necessary actions to minimise the impact, the ATCO OPS supervisor understands the operational consequences, and **the cyber-expert can analyse the data and advise on how to handle the event**.

Moreover, the cooperation with the cybersecurity experts post incident phase (until the ATSEP expertise and knowledge further builds) will help to strengthen the resilience of ATM/CNS functional system from future cyber-attacks.

Where possible, administrative IT systems (IT) should remain isolated from the Operational Technology (OT) of the total ATM/ANS functional system. Where there are cases of shared components between the two areas, then the two technical teams (ATSEP and cyber-experts) must come to an agreement on how they cooperate in the case of cyber-attacks for safety-critical systems.

2.1.5 Asset management for new and legacy systems and authentication procedures

Asset management policy

One of the most undervalued tasks in the path to a cyber-secure environment is asset management. Asset management requires a manual, or in some cases an automated, process to continually update the inventory of hardware and software of all equipment within the ANSP's functional system. This inventory database is the basis for risk assessments (including cyber security risks and vulnerabilities), patch policies and overall life cycle management.

If the inventory is incomplete, incorrect or outdated these tasks cannot be conducted correctly. It is from this inventory that outdated and unsupported hardware and software has to be identified and located within the functional system.

The importance of the asset inventory to conduct **asset and lifecycle management** is still not sufficiently acknowledged and valued by **the ATM community** and represents an important risk for cybersecurity. For example, recently, a system used for routing the flight plan from an airline to an ANSP was not properly patched/upgraded (due to software certification issues) and many aircraft of a well-known airline were grounded as a result. This was aggravated as no ATSEP was available at the time of the incident. Subsequent investigation into the incident revealed that the system in question was not identified as a critical ATM functional system. This example demonstrates the importance of having a robust asset management policy and well-trained staff in the domain of asset management.

To overcome existing asset management shortcomings and improve its contribution to cybersecurity, the following actions should be considered:

- Implement a **complete and reliable configuration management database (CMDB)** with **automated processes** to update the ATM functional system inventory. For ANSPs with assets distributed across a variety of locations the CMDB should be the single source of truth for all hardware and software within the functional system and should be sufficient to assess the life-cycle status, vulnerabilities, and exposure of the equipment. The CMDB is a critical tool to support cybersecurity since functional system details and vulnerabilities are available when needed. To support it, in the future, all ATM functional systems should be able to feed into the CMDB automatically and not manually.
- **Ensure that a patch policy is in place,** updates should be made periodically to ensure hardware and software is up to date. This should be done in a proactive manner rather than a reactive one (when something stops working).
- **Train ATSEP** accordingly.

Making legacy systems cyber-secure

Many ATM/CNS legacy systems were never designed with a cybersecurity mindset. This means that cyber related features are not standard features of these systems, but instead add-ons that need to be implemented.

In the case of legacy systems without internet/external connectivity, the level of cybersecurity requirements is lower than for connected systems. It may be that physical protection, such as being in a secured location, together with basic password management and staff training is sufficient to keep them cyber-safe. For critical assets, a multi-layered security approach remains preferable.

Ensuring the cybersecurity of existing ATM/CNS legacy systems still requires a significant amount of work to implement new policies, address outdated software/firmware versions, conduct patching and to deal with currently unsupported hardware. There will even be cases where updating hardware or software is not an option, because the equipment will not work on a more recent platform and other security measures have to be considered. The handling of the cybersecurity of legacy systems should be conducted carefully to ensure safety functions are not compromised. This is particularly important since there is a network of different interoperable and complex systems, and changes in one system may impact the behaviour of the total system. **Methodical procedures should be made available to support these activities** and should include measures to revert the change to a previous working status, this is particularly important for safety critical environments.

The **workload of ATSEP can be seriously impacted** by activities to make legacy ATM/CNS systems cyber-secure, this can compromise other day-to-day activities. Therefore, it is advisable that **proportionality is adopted when considering the measures to safeguard the functional system perimeter, together with the operational staff.** This approach should consider the business impact, priorities, and pros and cons of implementing add-on options *versus* investing in new 'secure by design' systems.

Authentication procedures

Authentication procedures are essential to ensure the security of systems and safety of operations, but conversely, they add to the workload of ATSEP and other ATM staff.

ATM and CNS systems are gradually becoming better protected with more restrictive access (stricter password management, connections under surveillance by probe who record flow and connections, firewalls, etc) to the system management. As a result, the ATSEP daily work (maintenance, upgrade, test, installation and systems monitoring and control) is becoming increasingly more complicated and requires extra training (firewalls, probe, dedicated cyber-systems), and authentications (credentials).

Password policies often require personal login credentials and strong passwords that are renewed periodically. Every system usually has its own login credentials, and there is often no centralised authentication service. This can amount to tens of different login credentials for each individual ATSEP. Without a structured way of storing and maintaining these credentials, daily tasks can become frustrating and tend to diminish the strength of passwords used or tempt the use of the same password everywhere. Therefore, **implementing a centralised authentication services to ensure secure access** without the need for multiple passwords could reduce the cognitive workload of ATSEP. In addition, more modern authentication processes such as the use of biometrics or one-time tokens could help to reduce the reliance on passwords and reduce the cognitive workload on ATSEP.

Furthermore, the **authentication procedures should be adapted to the operational environment and to the safety implications**. As an example, less stringent authentication procedures could be applied on small tower units with a small number of staff and extremely limited rights in terms of changes that may affect the safety function[3].

2.1.6 Cybersecurity of space-based and other digital CNS services

The increasing use of space-based CNS creates new challenges from a cybersecurity perspective including jamming and spoofing[4]. These cyber-events are currently difficult to detect and require the establishment of clear protocols on how to detect and respond to them.

Other services such as Controller-Pilot Data Link Communications (CPDLC), transmitted via VHF or SatCom, are also vulnerable to interferences, both deliberate and unintentional. CPDLC uses unencrypted and unauthenticated messages which are vulnerable to unlawful interference. Additionally, although these services are part of the ATM system, they are often handled by third party companies. This increases the complexity in the case of a cyber-event impacting these services.

It is still unclear how best to detect and respond to interference to space-based and digital CNS services. This contrasts with an attack on other legacy systems for which there are clear protocols established. Crucially, it is yet to be determined how best to detect an interference, error, or attack in which the corruption looks credible (i.e. close enough to the truth or at least realistic enough that no pilot or ATCO is able to recognise it). **Protocols on how to detect and respond to these events are required to ensure humans can conduct their tasks** effectively.

2.1.7 Data assurance

The human in ATM needs to have confidence in the data they use. However, there are numerous hazards regarding **data discrepancies** (e.g. FDP/RDP interference) **that need to be detected in time for a proper response**. It is often assumed that ATCOs as well as FISOs, FMPOs, ATSEP and FDOs are usually connected to

---

[3] In general, tower units in a country usually have extremely limited rights, except for some Regional Centres (which have restricted rights to make only certain modifications). The ACC/APP routing centre is the only area that centrally manages modifications/upgrades of operational systems, IDS configurations/routers/etc.

[4] Potential sources of interference to GNSS include both systems operating within the same frequency bands as GNSS and systems operating outside those bands. Interference can be intentional or unintentional. GNSS spoofing is when a GNSS receiver is made to calculate a false position and jamming is when GPS signals are overpowered locally by other signals so that a GPS receiver can no longer operate.

secure internal networks, but connections to external networks are often necessary. This increases the vulnerability to cyber-attacks. Prevention is important, but situational awareness is also a top priority. Decision making is based on data, thus a digital trust framework is crucial to support it and is currently under development.

In terms of data assurance there are several key aspects which need to be considered:

- How does the human know that a cyber-attack is underway on ATM systems, particularly in the case of open or cloud-based solutions? The front-end users must know instantly when they are under a cyber-attack.
- How do all parties identify that the attack is over and that the data they are using is once again trustworthy. This is a complex issue as mechanisms need to be in place that allow the trust of the human operator to be regained.

Working with corrupted data and no situational awareness is a catastrophe waiting to happen in the ATM environment. Response and recovery times are crucial when it comes to conducting safe and efficient operations and each stakeholder has a role to play. **Guidelines that consider the network minimum requirements need to be developed and updated periodically**.

2.1.8 New standardised tools to support detection of cyber events

Automation of tasks and intuitive human-machine interfaces and tools could help ease ATSEP workload and aid the ATSEP with meaningful alert signalling integrated into the ATSEP working position for Systems Monitoring and Control (SMC).

The usual sequence of tasks for an ATSEP is that first they are informed of a technical failure/degradation/malfunction. The ATSEP then finds the root cause and distinguishes within a complex network of legacy and state of the art systems, whether it is a typical failure of hardware or software, or if it is due to a cyber-attack. The use of **standardised support tools for all interconnected CNS/ATM systems** could significantly simplify these tasks. **Automation and Artificial Intelligence** could play an important role here**, especially in the detection of cyber-attacks**. These new tools should not unduly increase cybersecurity risks, so that the benefit of implementing such tools is outweighed by new risks.

Manufacturers of CNS/ATM systems and architectures like remote towers, are already developing system specific cybersecurity tools for the ATSEP Working position for SMC, which support the distinguishing of technical failures from cybersecurity issues. However, these are generally too system specific. Greater harmonisation and standardisation of these tools is required.

2.1.9 Just Culture in cybersecurity

Reporting of cybersecurity incidents must be prompt. To facilitate this, ATC professionals need to be encouraged to be pro-active and transparent in this activity. Establishing a culture of reporting, without fear of blame or disciplinary actions, can help identify and respond to threats effectively. **Timely reporting and information-sharing contributes to early detection and mitigation of cyber incidents,** minimising **potential harm to the overall system.**

ATC staff already have a Just Culture mindset in the realms of aviation safety and security, this should be implemented in an identical, complimentary manner to the domain of cybersecurity incident reporting.

2.2 ATM cybersecurity evolution in the immediate future

As the ATM sector continues to evolve and adopt new technologies and operational concepts, several additional human dimension implications are predicted in the immediate future, linked to:

- the integration of new technologies and systems;
- the adoption of new business models;
- the evolution of cybersecurity needs.

These aspects will need to be monitored and continuous evolutions will be required in terms of:

- ATM cybersecurity policies and tools;
- ATM staffing, competences and training; and
- ATM change management.

In the following sections these changes and their potential impact on ATM human factors are discussed. These should be **considered by the European Commission and other European aviation bodies in their regulatory, standardisation, and operational activities**.

2.2.1 Integration of new technologies and systems

New technologies come with new procedures, regulations, and potential associated safety risks and may lead to the need for increased skill set requirements which means that ATC professionals need to acquire new skills and competencies. In relation to cybersecurity, new technologies are likely to lead to significant impacts on the day-to-day activities of the ATSEP in charge of ATM/CNS systems. Systems will be hardened (specific OS, software restriction, login, and password management), security requirements will certainly impact work habits, and procedures to react and recover from a cyberattack will have to be put in place. The use of advanced digital tools, data analysis, cyber-risk management, and the integration of new technologies into daily operations should be part of the training to keep the workforce's skills up to date. This means that all training programmes will need to be updated. In addition, new developments come with their own systems, protocols, and interfaces that are not necessarily well understood by ATSEP professionals and other front-line actors. This means it is not only application specific knowledge that is needed, but also background knowledge in applicable low level technological solutions and protocols, their vulnerabilities and security solutions.

Furthermore, new technologies require the correct change management processes to be implemented. The reliance on technology and increasing complexity of the ATC system, despite the intention of new technologies often being to reduce the workload on the ATC personnel, has the potential to increase mental workload and potentially stress. Providers of ATC services will need to provide support, promote work-life balance, and implement measures to mitigate stressors associated with these changes and attract new professionals to ensure continuity and the sharing of knowledge. These measures should include transparency of information, to better manage staff expectations, the maintenance of the safety culture and the evolution of the regulatory framework in support of the technological changes.

With many ANSPs having an ageing pool of ATM professionals including ATSEP, it should be acknowledged when attempting to integrate new technologies, that more experienced ATSEP may take more time to adjust to new technologies designed to support their role. This can be remedied by ensuring sufficient training and appropriate change management processes are put in place.

2.2.2 Introduction of new business models

New business models such as U-space, virtual centres and remote towers are likely to redefine traditional job roles and responsibilities. **ATC professionals may have to adapt to the new ways of cooperating and coordinating with remote teams.** Due to the new business models and distributed architectures as described in the SJU Airspace Architecture Study (AAS), CNS/ATM systems may exist in distributed geographical locations. The potential impacts of this are likely to be significant. For example, the potential introduction of (cross-border) ADSPs will effectively result in AIS/AIM staff being centralised to a much greater extent than under the current business model. Therefore, the damage done by a cyberattack would likely be much further reaching compared to the current business model where ANSPs have their own independent systems. A geographically distributed model is also likely to impact recovery processes, where coordination between ADSPs and different ANSPs is required as opposed to the current model, where communication is predominantly contained within ANSPs (in an environment where people know who to turn to for assistance and speak the same language).

2.2.3 Evolution of cyber security needs

Knowledge of the nature of future cyber-attacks is required to facilitate an understanding of the potential impacts on Air Traffic Services and potential mitigations. For example, in the future there are likely to be many more participants in the aviation ecosystem (with more digital connectivity to external entities). This will lead

to uncertainties around how these entities are used, what they are trusted for and the relevant assurances that will facilitate trust in them. The upcoming EACP (European Aviation Common Public Key Infrastructure) that has been mandated under CP1 regulation by 31/12/2024, may contribute to the mitigation of this challenge. A key component of this group of 30 partners is to develop a EACP Trust Framework, addressing uncertainties around trust between different aviation stakeholders as the number of aviation participants expands.

The capabilities of the cyber attackers are likely to improve, and existing and new technologies may come under increasing attack through new methods. New technologies will be required to help monitor and detect cyber-attacks to counteract this, including for example GNSS signal quality monitoring equipment in response to increasing deliberate GNSS interference from attackers.

Research institutions and industry must supply front-line users with the necessary technology and tools. These tools should have the capability to differentiate between a system malfunction/normal behaviour, as opposed to a cyberattack. An outstanding question remains: how can confidence be maintained to ensure that Air Traffic Service provision remains safe and resilient in this evolving environment?

2.3 Summary of related Human Factors and Human Performance aspects

The previous section described the operational and technical challenges that have an impact on the human dimension, associated with ensuring a cyber-secure ATM environment. This section shows how these challenges link to the human dimension by taking inspiration from the SESAR Human Performance Assessment Process[5] to identify the HP/HF implications related to each of the challenges described in section 2.2.

According to SESAR, Human Performance (HP) is used to denote the human capability to successfully accomplish tasks and meet job requirements. The capability of a human to successfully accomplish tasks depends on a number of variables that are usually investigated within the discipline of "Human Factors (HF)". These are: procedure and task design, design of technical systems and tools, the physical work environment, individual competences and training background as well as recruitment and staffing. HP also depends on the way in which social factors and issues related to change and transition are managed.

TABLE 1 : SUMMARY OF HF/HP IMPLICATIONS OF THE CHALLENGES CONTAINED IN SECTION 2.2

	New policies and procedures	Staffing, workload, and rostering for ATM cybersecurity	New competences and training requirements for ATM cybersecurity	New roles and responsibilities for ATM cybersecurity	Asset management for new and legacy systems and authentication procedures	Cybersecurity of space-based and other digital CNS services	Data assurance	New standardised tools to support detection of cyber events	Just culture in cybersecurity
Adequate decision-making team composition according to the requirements and responsibilities.	●			●					
Adequate standardised tools (hardware and software with intuitive human-machine interfaces) in supporting the tasks of human actors.	●				●			●	
ATM professionals' competences and training requirements to evolve in line with the changes in operating methods and/or tasks	●		●	●	●				

[5] *SESAR DES Human Performance Assessment Process TRL1-TRL8*

	New policies and procedures	Staffing, workload, and rostering for ATM cybersecurity	New competences and training requirements for ATM cybersecurity	New roles and responsibilities for ATM cybersecurity	Asset management for new and legacy systems and authentication procedures	Cybersecurity of space-based and other digital CNS services	Data assurance	New standardised tools to support detection of cyber events	Just culture in cybersecurity
Adequate team composition and clarity on the roles and responsibilities of the different human actors.	●	●		●					
Create a safe environment for reporting issues/incidents and promote exchange of the best practices and lessons learnt.	●								●
New demands, new roles and responsibilities together with a lack of recognition and appreciation might have a negative impact on acceptance and job satisfaction.		●	●						
Operating methods and/or tasks to evolve in supporting the human performance.	●			●	●	●	●		
Situation awareness might be decreased						●	●		
Staff might not have the adequate mental model of the machine behaviour, the flow of information and the roles and responsibilities of each player.	●					●	●	●	
The current urgency to act faster can lead to increased stress and workload		●							
The human capabilities and limitations can soon be surpassed due to additional training needs, excess workload and lack of adaptation of the working methods/tasks.		●	●		●				
The level of trust on the performance of the technical system and on the accuracy of the data might decrease.						●	●		
The team structure and team communication might not be adapted to the new needs and responsibilities.		●	●	●					

3 RECOMMENDATIONS TO ADDRESS HUMAN DIMENSION CHALLENGES RELATED TO CYBERSECURITY IN AVIATION

Considering the cybersecurity challenges in ATM, continued action and advances are needed to prevent negative impacts on ATM staff. In the previous sections the main HF/HP challenges are outlined by the EGHD across different areas of work. This section lays out specific recommendations directed mostly to the European

Commission to foster the adoption and implementation of mitigatory actions to ensure these challenges are addressed.

RECOMMENDATION 1

The European Commission to promote the inclusion of the ATM cybersecurity human factors aspects outlined in this paper in the work being developed by the European Centre for Cybersecurity in Aviation (ECCSA) and EUROCONTROL - European Air Traffic Management Computer Emergency Response Team (EATM-CERT)[6]. Furthermore, to promote and incentivise the reinforcement of the ECCSA and EATM-CERT activities in contribution to a harmonised ATM cybersecurity approach across Europe, based on strengthened coordination and best practices sharing across the ATM community.

ATM cybersecurity has network implications, but it is being managed in a fragmented manner by the different ATM stakeholders (ANSPs, airspace users, airports, USSPs, ADSPs, etc), which have different levels of cybersecurity readiness and different capacities to invest in the improvement of their cybersecurity readiness. The EATM-CERT work should be further disseminated and supported, taking into account human factors aspects, in particular to:

- Continue to promote Member States and ATM stakeholders' awareness, through workshops and information campaigns.

- Support or provide guidance to the ATM stakeholders in the assessment of cybersecurity related risks and identification of gaps (e.g. in terms of procedures, technology, staffing/roles and organisational structure, etc). Noting that cybersecurity related risks should include cyber-attacks, interferences to space-based and other digital CNS services and data corruption.

- Support or provide guidance to the ATM stakeholders in the definition and implementation of cybersecurity policies and procedures, whilst considering the operational specificities. These procedures should include best practices on how to timely detect information security incidents.

- Support or provide guidance to the ATM stakeholders in the definition and implementation of cyber-crisis scenarios for training exercises and in then assessment of the results of these exercises which should feed into the risk-assessment. These guidelines for exercises/simulations playbook, procedures could be inspired in the work developed by the Joint CNS Stakeholder Platform (JCSP) which is a combination of the EUROCONTROL CNS Team and the EASA CNS Experts Group.

- Support or provide guidance to the ATM stakeholders regarding the structure of their organisations, and on how to evaluate how their structure, contributes to their readiness for cybersecurity. As an example, should they have a Cybersecurity Incident Response Team (CSIRT) in place?

- Advise the Member States in the revision of national regulations with an impact on ATM cybersecurity.

- Continue to collect, generate, and distribute relevant cyber intelligence with the ATM stakeholders.

- Maintain a registry of entities which can support ATM stakeholders in the implementation of cybersecurity related actions.

RECOMMENDATION 2

The European Commission to promote collaboration between the EUROCONTROL EATM-CERT, ECCSA and ENISA (the European Union Agency for Cybersecurity), in particular the European cyber crisis liaison organisation network (EU-CyCLONe)[7],

This collaboration will contribute to an improved European ATM cybersecurity and overall European cybersecurity, which should take into consideration the ATM human factors outlined in this paper.

---

[6] https://www.eurocontrol.int/cybersecurity

[7] *The European cyber crisis liaison organisation network (EU-CyCLONe), is a cooperation network for Member States national authorities in charge of cyber crisis management. The network was launched in 2020 and formalized on 16th of January 2023 with entrance into force of NIS2 art 16.* https://www.enisa.europa.eu/topics/incident-response/cyclone

RECOMMENDATION 3

The European Commission to sponsor a study together with EASA, SESAR, the EUROCONTROL EATM-CERT team, ECCSA and the ATM operational stakeholders to investigate how ATM staffing will be impacted by the immediate needs related to cybersecurity and digital transformation. This should be followed by the production of a roadmap plan to address any forecasted gaps and risks that may impact the human factors and human performance.

This study and action plan should include:

- The expected evolution of ATM processes and workload, including planning and training workload.

- An analysis of how roles and responsibilities may evolve to account for new cybersecurity related processes.

- Guidance on how to conduct the ATM change management, to mitigate impacts on the human factors and human performance. This could include the use, temporary or not, of external cybersecurity services.

- Guidance on how to manage workload when staffing levels are lower than recommended, which can include guidance on how to define contingency plans and define tasks/activities prioritisation.

- Identification of regulatory gaps or the need for regulatory evolution (e.g. new security requirements, new roles and responsibilities, inspections, ATM staffing and training).

- Best practices and lessons learnt in ATM and other sectors of the economy.

RECOMMENDATION 4

The European Commission to review the rules to be applied to cybersecurity related costs/investments during the revision of the performance and charging scheme for RP5.

The implementation of urgent cybersecurity related measures can lead to high investment costs in staffing, new equipment, subcontracting of external services, implementation of new cybersecurity structures such as the safety and information security management systems (SMS/ISMS), amongst others. The performance and charging scheme for RP5 should take these aspects into consideration and should propose solutions that stimulate and support the ATM stakeholders in the realisation of the required investments towards a more cyber-secure European ATM.

RECOMMENDATION 5

The European Commission, together with EASA, to review and update existing competence and training regulations applicable to the European ATM. These updates should reflect the human factors outlined in this paper and the findings from the study to be developed together with EASA, SESAR, the EUROCONTROL EATM-CERT team and the ATM operational stakeholders, as proposed in RECOMMENDATION 3.

Examples of regulations in force and guidance material that would benefit from an update are listed hereafter:

- The guidance material published by EASA for the IR (EU) 2023/203[8], the First Easy Access Rules for Information Security, ANNEX II — INFORMATION SECURITY — ORGANISATION REQUIREMENTS [PART-IS.I.OR][9].

- GM1 IS.I.OR.240(g) Personnel requirements: In the AMC it is stated that personnel competence should be maintained, however in the GM there is no description on how to do it. Thus, it is advisable to review the GM to add that personnel competence has to be maintained at the individual and organisation level. This includes the technical handling of a cyber-event as well as communication. The EGHD proposal would be: '*The organisation shall have a process in place to ensure that the personnel referred to in point (f) have the necessary competence and confidence to perform their tasks.*'. The word confidence adds a requirement for human experience, which can then be elaborated in the AMC and GM to include periodical training, familiarity with

[8] *https://eur-lex.europa.eu/eli/reg_impl/2023/203*

[9] *https://www.easa.europa.eu/en/document-library/easy-access-rules/online-publications/easy-access-rules-information-security?page=6*

procedures/processes and hands on experience in real-life exercises and/or simulators. This proposal could be considered in other regulations.

- AMC1 IS.I.OR.240(g) Personnel requirements: In terms of 'Necessary Competence' under (a) it should be added a number (3) 'relevant stakeholders and their roles'. This would ensure that all stakeholders are included.

- GM1 IS.I.OR.220(b) Information security incidents — detection, response and recovery: This section describes three aims for a response action: activating predefined resources and course of action, contain the spread of an attack and control the failure mode of the affected elements. An additional aim should be proper internal and external communication and not only the technical aspects.

- During the ongoing revision of EU 2015/340[10] laying down technical requirements and administrative procedures relating to air traffic controllers' licences and certificates, consider the human factor aspects related to the implementation of cybersecurity procedures outlined in this paper, in particular in what refers to ATCO OPS supervisors since there is not a specific license applicable.

- Update and expand IR (EU) 2017/373[11], namely:

- ANNEX XIII Requirements for Service Providers Concerning Personnel Training and Competence Assessment, to consider ATSEP's human factor aspects related to the implementation of cybersecurity procedures outlined in this paper.

- ANNEX III Common Requirements for Service Providers (Part-ATM/ANS.OR), SUBPART B — Management (ATM/ANS.OR.B), to include a process to ensure that the personnel of the service provider are trained and competent in cybersecurity. This should be applicable not only to front-line operators, but also to management staff and communication departments.

RECOMMENDATION 6

The European Commission to promote the creation of an ATM Cybersecurity Community, potentially under the EUROCONTROL EATM-CERT umbrella and with EASA support, to promote the Continuous Personal Development (CPD) of ATM staff and the improvement of awareness and competences at the ANSP level in topics related to cybersecurity.

A community focused on the ATM cybersecurity topic will contribute to building knowledge, skills, competences and awareness of the ATM community.

RECOMMENDATION 7

The European Commission to work together with standardisation bodies, EASA and SESAR Deployment Manager in the development of guidance material for ATM system development and certification and for ATM asset management and maintenance, considering cybersecurity implications with repercussion on ATM human factors. This guidance material should be widely disseminated among ANSPs and ATM system manufacturers.

Updating and deploying asset management policies, authentication procedures and system configuration that ensure that systems monitoring, and maintenance are made easier and faster for ATSEP, and other ATM engineers/operators will have a strong positive impact on ATM cybersecurity.

Overall, systems interoperability and standardisation will be key and will facilitate the creation of common protection protocols, common regulations, training requirements, specifications, etc, contributing to the improved protection of the ATM functional system.

---

[10] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R0340*

[11] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0373*

RECOMMENDATION 8

The European Commission together with EASA to review existing regulations related to ATM systems and constituents and to update it, taking into consideration the need for improved human machine interaction which contribute to a more cyber-secure ATM.

As an example, Basic Regulation 2018/1139 (Annex VIII, Chapter 3. Systems and Constituents) should be updated to reflect and reinforce the need for proper documentation of ATM systems and information on how to make them more secure. Furthermore, the regulation should reinforce the requirement for an optimised human machine interaction:

- Paragraph 3.1: '*ATM/ANS systems and ATM/ANS constituents providing related information to and from the aircraft and on the ground shall be properly designed, produced, installed, maintained, protected against unauthorised interference and operated to ensure that they are fit for their intended purpose*.'. Proposal to add 'documented', so '…shall be properly designed, produced, **documented**, installed, maintained….'.
- Paragraph 3.3.5: *'Information needed for production, installation, operation and maintenance of the systems and constituents as well as information concerning unsafe conditions shall be provided to personnel in a clear, consistent and unambiguous manner*.'. Proposal to add 'securing', so 'Information needed for production, installation, operation, **securing** and maintenance of the systems….'.
- Paragraph 3.3.3:' *Systems and constituents, considered individually and in combination with each other, shall be designed taking into account limitations related to human capabilities and performance*.'. This paragraph is unclear and could be rephrased as follows 'Systems and constituents, considering individually and in combination with each other, shall be designed to optimise human machine interaction in production, installation, operation, securing and maintenance of the systems'.

RECOMMENDATION 9

The European Commission together with EASA to raise awareness among the ATM community (ANSPs, AUs, Airports, NM) of existing regulations and guidance material related to information security incidents which may have a potential impact on safety (such as cyberattacks, or interferences to space-based and other digital CNS services, or data corruption). **Additionally, to support, making use of ATM cybersecurity communities, the development and the implementation of protocols to detect and respond to these events.**

As an example, the GM and AMC published by EASA for the IR (EU) 2023/203, the First Easy Access Rules for Information Security, ANNEX II — Information Security — Organisation Requirements [PART-IS.I.OR], IS.I.OR.220 Information Security incidents, the text states 'the organisation shall implement measures' and the AMC1 IS.I.OR.220(a) says 'the organisation should define and implement a strategy to detect information security incidents which may have a potential impact on safety'. As part of these measures and strategies, the necessary protocols and technical solutions have to be developed and implemented, but it is still unclear which solutions already exist or are being developed. Coordinated work with the participation of technical experts and operational stakeholders would accelerate the development of the necessary protocols and technical solutions to avoid, detect, respond and recover from information security incidents.

Additionally, awareness initiatives, training and recycling courses will have to be conducted for ATM operational and management staff.

RECOMMENDATION 10

The European Commission together with EASA, with inputs from the ATM operational stakeholders including EUROCONTROL, to study and promote the development of contingency scenarios and procedures on how to respond and recover from an information security incident at a European level.

Today's European ATM is increasingly dependent on space-based and other digital CNS services and digital technologies, and it is unclear how the ATM network should respond and recover from an information security incident. Contingency procedures involving the different ATM stakeholders must be developed. These will need to address the role of the legacy systems, as a replacement for space-based CNS services, taking into account the costs associated to keep them operational, such as ensuring ATCOs and ATSEP remain proficient in their use and maintenance costs (including availability of spare parts).

RECOMMENDATION 11

The European Commission to encourage SESAR, EUSPA and the ATM manufacturers to research, develop and standardise authentication encryption and other technological solutions or services to protect communications and data sharing and to support the human in the timely detection of information security risks. These tools and services will contribute to ATM cybersecurity and to an increase in the trust of ATM front-line operators on the performance of the technical system.

Authentication and encryption services will be able to certify if a message is identical to the one transmitted at its origin and that it was generated by a trusted source. Encryption and authentication refer to two interrelated mechanisms to protect communications. New solutions and services are required to ensure interferences or data corruption are identified easily and in a timely manner. SESAR (e.g. through projects under the 'Virtualisation and Cyber-Security Data Sharing' flagship) and ATM manufacturers should put part of their efforts in the research and development of these type of solutions and services for ATM.

As an example, EUSPA together with the European Commission is currently testing the Galileo Open Service – Navigation Message Authentication (OSNMA) for GNSS, a service that may have an important contribution to aviation security.

Other standardised support tools for all interconnected CNS/ATM systems to support the detection of information security risks would also contribute positively to the ATM HF/HP. These tools can be adapted from other existing tools taking into account the ATM human factors. As an example, tools already available have unsatisfactory human-machine interfaces (e.g. information relevant for the ATSEP not clearly displayed).

RECOMMENDATION 12

The European Commission together with EASA should review and update the Regulation (EU) 2018/1139[12] on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency**, to include cybersecurity aspects.**

Cybersecurity tools for the ATSEP working position for SMC, which support the distinguishing of technical failures from existing cybersecurity issues, however, these are generally too system specific. Greater harmonisation and standardisation of these tools is required. Regulation (EU) 2018/1139 should include a chapter on cybersecurity and system validation, including procedures, staff training and system requirements. As an example, these aspects can be included in the 'relevant essential requirements' of Regulation (EU) 2018/1139, in the Annex VIII, Essential requirements for ATM/ANS and air traffic controllers, Chapter 3. Systems and Constituents, paragraph 3.3.5.

RECOMMENDATION 13

The European Commission, EASA, EUROCONTROL and Member States should continue their efforts to establish a Just Culture environment for all ATM-related stakeholders, as established in Regulation (EU) No 376/2014[13]**. All involved actors should be familiar with cybersecurity and be encouraged to report any information security incidents or risks. The European Commission should also encourage Member States to continue adjusting their national safety prosecution and criminal investigation policy to be in line with the Just Culture principles, confirming that only gross negligence and wilful misconduct should be prosecuted.**

Just Culture has been recognised as an important pillar of a good safety culture and can contribute to a good security culture as well.

---

[12] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1139*

[13] *https://www.easa.europa.eu/en/document-library/regulations/regulation-eu-no-3762014*

ANNEX A ACRONYMS

Acronyms	Full Term
(A) FISO	(Aerodrome) Flight Information Service Officer
AAS	Airspace Architecture Study
ADSP	ATM Data Service Providers
AFTN	Aeronautical fixed telecommunication network
AI	Artificial Intelligence
AIM	Aeronautical Information Management
AIS	Aeronautical Information Service
AMC	Acceptable Means of Compliance
ANS	Air Navigation Services
ANSP	Air Navigation Service Provider
ARO	Air Traffic Service Reporting Office
ATC	Air Traffic Control
ATCO	Air Traffic Control Officer
ATFCM	Air Traffic Flow and Capacity Management
ATM	Air Traffic Management
ATS	Air Traffic Services
ATSEP	Air Traffic Safety Electronics Personnel
CMDB	Configuration Management Data Base
CNS	Communications Navigation Surveillance
COM	Communications
CPD	Continuous Personal Development
CPDLC	Controller Pilot Data Link Communications
CSIRT	Cybersecurity Incident Response Team
DSP	Digital Service Providers
EACP	European Aviation Common Public Key Infrastructure
EASA	European Union Aviation Safety Agency
EATM-CERT	European Air Traffic Management Computer Emergency Response Team
EC	European Commission
ECCSA	European Centre for Cybersecurity in Aviation
EGHD	Expert Group on Human Dimension
ENISA	European Union Agency for Cybersecurity
EUROCAE	European Organisation for Civil Aviation Equipment
EUSPA	European Union Agency for the Space Programme
FDA	Flight Data Analysis

Acronyms	Full Term
FDO	Flight Data Officer
FDP	Flight Data Processing
FDS	Flight Data Services
FMP	Flow Management Position
FMPO	Flow Management Position Officer
GM	Guidance Material
GNSS	Global Navigation Satellite System
HF	Human Factors
HP	Human Performance
ICAO	International Civil Aviation Organisation
IR	Implementing Regulation
ISMS	Information security management system
JCSP	Joint CNS Stakeholder Platform
NIS	EU Network and Information Security Directive
NOF	International NOTAM office
NOTAM	Notice to Airmen
NPA	Notice of Proposed Amendment
OES	Operators of Essential Services
OS	Operating System
OSNMA	Open Service Navigation Message Authentication
OT	Operational Technology
RDP	Radar Data Processor
RMT	Rule Making Task
SESAR	Single European Sky ATM Research
SJU	SESAR Joint Undertaking
SMC	Systems Monitoring and Control
SMS	Safety Management System
SOC	Security Operations Centre
SSGC	Secretariat Study Group on Cybersecurity
VHF	Very high frequency