ICAO

SECURITY AND FACILITATION

Cyber Information Sharing

Published under the Authority of the Secretary General
2024, Version 1

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Table of Contents

ACRONYMS

ANSP	Air Navigation Service Providers
CAA	Civil Aviation Authority
CERT	Computer Emergency Response Team
CIShP	Cyber Information Sharing Policy
CSIRT	Cyber Security Incident Response Team
CTI	Cyber Threat Intelligence
FIRST	Forum of Incident Response and Security Teams
ICAO	International Civil Aviation Organization
IoC	Indicators of Compromise
IPR	Intellectual Property Rights
ISAC	Information Sharing and Analysis Center
ISMS	Information Security Management System
IT	Information Technology
OSINF	Open Source Information
OSINT	Open Source Intelligence
SOC	Security Operations Center
TLP	Traffic Light Protocol
TTP	Tactics, Techniques, and Procedures
UAS	Unmanned Aircraft System(s)

EXECUTIVE SUMMARY

Best practices established in aviation safety and aviation security demonstrate the importance of information sharing and its role in reducing threats and risks to civil aviation. Cyber information sharing is equally important.

Cyber information sharing is crucial for managing cyber risks in civil aviation. It fosters a robust cybersecurity culture by promoting collaboration and trust. It also supports situational awareness, operational and tactical cyber risk management, and strategic planning.

This document provides guidance to States and industry stakeholders on developing a plan to share cyber information, including recommendations on setting policy, resources and practical steps towards the implementation and continuous improvement of sharing practices.

The pre-requisites for sharing cyber information in the aviation industry are also described. Various types of cyber information that can be shared are listed. The analysis and assurance aspects of sharing cyber information are also discussed, emphasizing the need for evaluating the trust in the source and the credibility of the information.

This document supersedes the previously published ICAO guidance on using Traffic Light Protocol (TLP) in civil aviation. It provides rules for sharing cyber information in the aviation industry based on the updated TLP standard, the type of information being shared, date/time when information is shared, and recipients (e.g. State agencies, operators, service providers).

Overall, the document highlights the importance of sharing various types of cyber information in the civil aviation sector while considering analysis, assurance, and proper marking for effective dissemination of information among relevant stakeholders.

This guidance aligns with the International Civil Aviation Organization (ICAO) Aviation Cybersecurity Strategy[1] and its associated Cybersecurity Action Plan[2], and responds to the need for cyber information sharing. The information in this document is aligned with the general principles of ICAO guidance on aviation safety and aviation security information sharing included in the *Aviation Security Manual* (Doc 8973 – Restricted) and the *Safety Management Manual* (Doc 9859).

[1] https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx
[2] https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx

DEFINITIONS

Assurance. The planned and systematic actions necessary to provide adequate confidence that a product or process satisfies given requirements.

Attack Vector.The means of access which an attacker used to begin an attack.

Authentication. Measure that verifies the claim over the identity of an individual, user, programme, process, system or device.

Availability. Property of being accessible and usable upon demand by an authorized individual, user, programme, process, system or device.

Aviation Cybersecurity. The body of technologies, controls and measures, processes, procedures and practices designed to ensure confidentiality, integrity, availability, and overall protection and resilience of cyber assets from attack, damage, destruction, disruption, unauthorized access, and/or exploitation.

Confidentiality. Property that an asset is not being made available or disclosed to unauthorized individual, user, programme, process, system or device.

Cyber Asset. Digital and physical items which have value in terms of business, operations, aviation safety, aviation security, efficiency and/or capacity, such as systems, information, data, networks, devices, software, hardware, processes, firmware, relevant/certified personnel, and other electronic resources.

Cyber-attack. The intentional use of electronic means to interrupt, alter, destroy, or gain unauthorized access to cyber assets.

Cyber Event. Any observable occurrence in a network or system.

Cyber Incident. A single, or a series of cyber event(s) that adversely impacts aviation safety, aviation security, efficiency, and/or capacity.

Cyber Mitigation. Security control(s) that aim at lowering the cyber risk associated with a specific cyber threat or vulnerability, taking into account their impact on aviation safety, aviation security, efficiency, and/or capacity.

Cyber Resilience. The ability of a cyber asset to maintain critical functions under adverse conditions or stress, and to recover from those adverse conditions.

Cyber Risk. Potential for an unwanted outcome resulting from a cyber event.

Cyber Risk Assessment. Continuous process of cyber risk identification, analysis, and evaluation.

Cyber Risk Management. The continuous process of identifying, mitigating, treating and monitoring cyber threats and risks, according to a risk assessment.

Cyber Threat. Any potential cyber event that might adversely impact aviation safety, aviation security, efficiency, and/or capacity.

Information Security. Preservation of confidentiality, integrity and availability of information.

Information Sharing. The process through which information is provided by one entity to one or more other entities to facilitate risk-based decision-making and promote best practices.

Integrity. Property of accuracy and completeness of an asset, supporting what the asset claims to be.

Severity. Qualitative indication of the magnitude of the adverse effect of a threat condition.

Threat Actor. Entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact – an organization or system.

1. INTRODUCTION

1.1 Rationale for cyber information sharing

Information sharing is critical to support the management of aviation cyber risks. In today's interconnected world, cyber threats pose significant risks to the civil aviation sector. Cyber-attacks can target any aspect of the aviation system, from air traffic management systems to passenger data systems, which can lead to operational disruptions and potentially endanger passengers' safety and security. Therefore, effective cyber risk management requires a collaborative approach that involves sharing information among stakeholders.

Lessons learned from aviation safety and aviation security emphasize that a culture of information sharing will significantly reduce risks to civil aviation posed by malicious actors. In the aviation sector, information sharing has been proven to be a valuable tool in managing aviation safety and security risks. The same principle applies to aviation cybersecurity. By sharing cyber information, stakeholders can gain a better understanding of the cyber threats they face, identify vulnerabilities, and take appropriate measures to prevent or mitigate cyber-attacks against civil aviation.

Information sharing is also an essential aspect of a robust cybersecurity culture. A robust cybersecurity culture supports the effective recognition and response to cyber threats. Information sharing is an integral part of this culture as it promotes transparency, collaboration, and trust among stakeholders. Effective cyber information sharing ensures that all stakeholders have the necessary inputs to make informed decisions, take appropriate actions, mitigate cyber threats and/or respond to, and recover from, cyber incidents.

Cyber information is not only about actionable cyber-specific information, but any type of intelligence that has a potential impact on cyber risks to civil aviation. Cyber information sharing is not limited to cyber-specific intelligence. It includes any relevant information that can contribute to identifying and mitigating cyber risks in the civil aviation sector. For example, information about physical security breaches, insider threats, geo-political context, technology, or supply chain vulnerabilities can also support stakeholders in better understanding and mitigating cyber threats and risks.

Cyber information sharing supports:

- **Strategic planning** to build aviation cybersecurity capabilities. By sharing information, stakeholders can identify gaps in their cybersecurity capabilities and develop appropriate strategies to improve their cyber resilience. Strategic planning ensures that the aviation sector remains protected and resilient to cyber threats, and that stakeholders are prepared to respond to, and recover from, potential cyber incidents.
- **Situational awareness** in both day-to-day operations and during a cyber incident. By sharing cyber information, stakeholders can gain a better understanding of their cybersecurity posture, the cyber threat landscape, and potential vulnerabilities (weaknesses) in their systems. This enables stakeholders to identify potential risks and take appropriate measures to prevent or mitigate the impact of cyber incidents.
- **Operational and tactical cyber risk management** in anticipation of, and in response to, a cyber threat. By sharing information, stakeholders can identify cyber threats and develop appropriate risk management strategies.
- **Crisis management** during a cyber incident, where effective information sharing enables stakeholders to coordinate their response and take appropriate measures to mitigate the impact of an incident.

It is essential to acknowledge that effective information sharing is based on trust among participants. This guidance aims to support building the trust required to encourage a group of participants to overcome their natural hesitations when sharing information. This involves establishing a set of common rules and procedures that everyone within the sharing group understands, agrees upon, and adheres to. Reaching a consensus on what cyber information is shared, how it is shared, and the methods of distribution will facilitate effective information sharing among participants.

This guidance complements the holistic work of ICAO on aviation cybersecurity. It supports pillar 5, Information Sharing, of the ICAO Aviation Cybersecurity Strategy, and the Cybersecurity Action Plan item CyAP 5.1, which requests ICAO to develop guidance for cyber information sharing.

This document integrates within it, and supersedes, the previously published ICAO standalone guidance material on using Traffic Light Protocol (TLP) in civil aviation. Guidance on using the updated version 2.0 of the TLP standard[3], developed by FIRST (Forum of Incident Response and Security Teams), as a means for sharing cyber information in civil aviation, is included in this document.

1.2 Context of cyber information sharing

Before addressing cyber information sharing, it is necessary to first address the overall cyber intelligence life cycle.

The cyber intelligence life cycle is a fundamental iterative process used in the field of intelligence analysis. Each step in the cycle serves a critical purpose in ensuring that information is transformed from raw data into meaningful intelligence that can support decision-making, enhance cybersecurity, and support various organizational strategic objectives.

Information sharing (also called “Dissemination” in Figure 1 below) is part of the cyber intelligence life cycle, which includes the following steps:

1. Planning and Direction: The first step in collecting and analysing cyber information is to plan and direct the process. This involves defining the objectives of the collection and analysis effort, determining its scope and scale, and identifying the stakeholders who need to be involved. Planning and direction also involve developing policies and procedures for collecting and analysing information, as well as defining the roles and responsibilities of those involved in the different steps.

2. Collection: The second step is the actual collection of cyber information. This involves gathering data from various sources (see Section 3). Collection can be done manually or through automated processes. It is essential to ensure that the data collected is relevant, accurate, and timely.

3. Processing: The third step is to process the collected information. This involves converting the collected data into a usable format, analysing it, and identifying patterns or anomalies that may indicate a cyber threat, for instance. This step can involve the use of data processing tools, algorithms, and other analysis techniques to help identify potential cyber threats or vulnerabilities, for example. Processing also involves identifying the significance and urgency of the information and prioritizing the response accordingly.

[3] https://www.first.org/tlp/

4. Analysis and Production: The fourth step is to analyse and produce reports based on the processed data. This involves interpreting the data, identifying patterns or trends, and determining the cyber risks on the aviation system, for instance. It may lead to reject the information if the quality and level of detail are not sufficient to analyse it. Analysts use their knowledge and experience to make sense of the data and produce intelligence reports that are relevant for their intended audience, accurate, and actionable. The analysis and production step may also include developing recommendations for mitigating or preventing cyber threats, for example.

5. Dissemination (cyber information sharing) and Feedback: The final step is to disseminate the intelligence reports to the relevant stakeholders. This can include sharing cyber information with internal stakeholders, such as Information Technology (IT) teams, cybersecurity teams, and/or aviation safety/security teams, as well as with external stakeholders, such as other aviation organizations or State agencies. Dissemination involves ensuring that the cyber information is shared in a timely and secure manner, and that stakeholders have the necessary context and understanding to act on it. Effective dissemination helps build a culture of cyber information sharing in the civil aviation sector and enables stakeholders to take appropriate actions that could allow, for example, the prevention or mitigation of cyber threats.

Feedback is also collected in this step to assess the effectiveness and relevance of the cyber intelligence life cycle, with the objective to enhance it in future iterations.

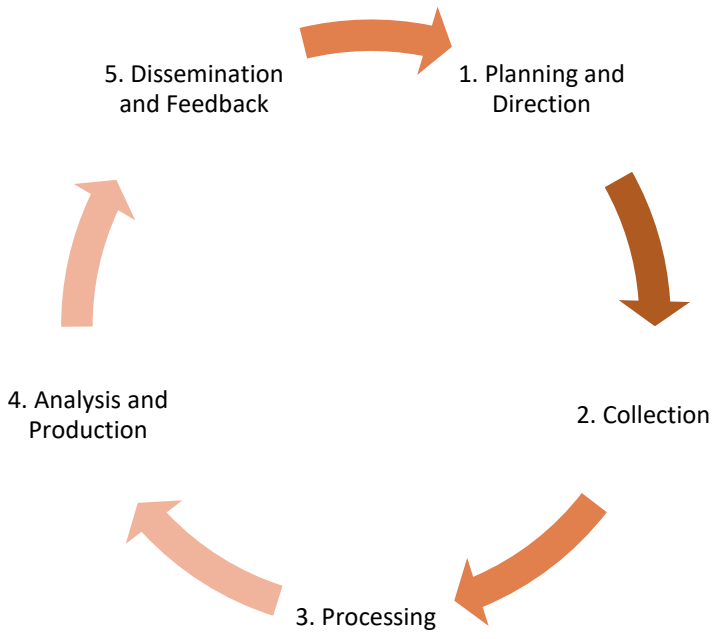

Figure 1. Cyber Intelligence Life Cycle

2. CYBER INFORMATION SHARING POLICY (CIShP)

This section provides guidance on how to develop and implement a cyber information sharing policy at the organizational level (e.g. among aviation stakeholders).

The guidance can also be used by States to develop their cyber information sharing plans. However, it is worth noting that national cyber information sharing schemes may be cross-sectoral and not specific to aviation.

2.1 Cyber Information Sharing Policy (CIShP)

The CIShP should define:

- The reason for cyber information sharing;
- Scope of applicability, context and limitations (e.g. cyber information sources, limitations related to intellectual property rights (IPR), privacy laws);
- Members of the cyber information sharing community within the organization and their respective responsibilities;
- Distribution rules (including further distribution[4]) of cyber information inside and outside of the organization, based on the information classification/categorization rules and taking into account relevant regulatory and legal requirements;
- Operational procedures:
  - information gathering;
  - de-identification, if needed;
  - content validation; and
  - distribution; and
- Review cycle of the CIShP and document control (i.e. recording significant changes and validation procedures).

The CIShP should be approved by the organization as part of the information security management system (ISMS)[5]. It should be reviewed periodically (e.g. annually), after any significant change to the policy, or after any cyber incident to take into consideration relevant lessons learned.

2.2 Regulatory and contractual requirements[6]

The CIShP should comply with all applicable regulations and existing agreements related to cyber information sharing such as:

- Cross-sectoral national, regional and/or international regulations.
- Aviation-specific national, regional and/or international regulations.
- Agreements with national and/or international Information Sharing and Analysis Centers (ISACs) and Computer Emergency Response Teams/Cyber Security Incident Response Teams (CERTs/CSIRTs) (e.g. Aviation ISAC, European Air Traffic Management Computer Emergency Response Team (EATM-CERT), national CERTs/CSIRTs).

[4] Further sharing of information is discussed in Section 5 of this document.
[5] ISO 27001, chapter A.5.14 *Information transfer*
[6] Additional information (cross-sectoral) can be found in:
NIST.SP.800-150 – Guide to cyber threat information sharing
ENISA Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches
https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

2.3 Resources

The organization should identify the resources needed to ensure the proper implementation of the CIShP, including:

- Human resources: leverage existing cybersecurity teams such as the Security Operations Center (SOC) team, hire new people as necessary;
- Technical resources: website, email, telephone, text messages, as well as secured and/or trusted sharing platforms; and
- Financial resources: costs related to procuring and/or developing systems, training of human resources, etc.

2.4 Implementation

The implementation of the CIShP includes the following phases:

- Scoping: identifying the sources of information and the cyber information to be shared through the CIShP;
- Identifying the tools to be used for cyber information sharing;
- Identifying a Point of Contact (POC) of the cyber information sharing network and developing processes to maintain the POC information;
- Testing the systems and processes for cyber information sharing, and adjusting them as needed;
- Launching the cyber information sharing scheme (going live);
- Continuous monitoring and control; and
- Continuous review and improvement.

3. MANAGING CYBER INFORMATION AND ITS SHARING

3.1 Types of cyber information

The following cyber information can be shared.

CYBER INTELLIGENCE

- **Cyber Threat Intelligence (CTI)**: it includes cyber threat landscape, intelligence about hackers' appetite, etc.
  - **Strategic:** strategic information helps an organization understand the type of cyber threats, and the capabilities and motivations of attackers.
    - Supports formulating an overall picture of the intent and capabilities of malicious cyber threats.
    - Informs decision making and/or provides early warnings.
    - It can include trends (e.g. targets, attackers' behaviours), statistics, cyber threat-related information (e.g. Advanced Persistent Threats (APTs), cyber incident reports, policy documents, white/research papers), etc.
    - *An example of Strategic CTI is a comprehensive report on emerging cyber threats to a State's critical infrastructure, outlining potential vulnerabilities and attack vectors. This report is typically used by high-level decision-makers to shape long-term cybersecurity policies and strategies.*
  - **Operational:**
    - Provides context to cyber incidents, enabling defenders to identify any possible dangers.
    - Allows to identify potential impacts of cyber incidents on operations (e.g. Tactics, Techniques, and Procedures (TTPs), motives, impact, timing).
    - Helps to allocate resources and prioritize tasks.
    - *An example of Operational CTI is information about an ongoing phishing campaign targeting aviation. This includes details such as the TTPs used by threat actors. This information is valuable for security operations teams to detect and respond to immediate cyber threats.*
  - **Tactical:** intelligence used by organizations to help with proactively developing a security posture that can withstand attacks (e.g. Indicators of Compromise (IoCs), TTPs, vulnerabilities).
    - *An example of Tactical CTI is IoCs related to a specific malware variant. This includes specific IP addresses, file hashes, and patterns of behaviour associated with the malware. This tactical information is used by frontline cybersecurity analysts to identify and mitigate cyber threats in real time.*
- **Indicators of Compromise (IoCs)**: IoCs are, for example, malicious IP addresses, malicious URL, malicious domain names, or malware hash.
  - Sharing this information will help the receiving parties better protect their systems/services.
  - When sharing IOCs, there is no need to disclose who discovered them.
- **Tactics, Techniques, and Procedures (TTPs)**: TTPs are scenarios of attacks and preferred methods used by hackers[7].

[7] MITRE ATT&CK has developed and is maintaining a taxonomy of TTPs which can be found on their website: https://attack.mitre.org/

- **Vulnerabilities**:
  - **As user of a cyber asset:** the cyber information to be shared is mainly related to the cyber asset (e.g. Hardware, Software, Service, Protocol, standard) for which the vulnerability was found. Information related to the identity of the cyber asset's user would not be useful to be shared.
    - This information can be shared with others to help them protect themselves.
    - There is no need to further disclose who discovered the vulnerability.
    - With regards to responsible disclosure of vulnerabilities, the vulnerability management programme of the organization may propose a "hall of fame" or a similar process to recognize researchers' contributions in the identification of vulnerabilities.
  - **As owner of a cyber asset:** the owner of the cyber asset should share the vulnerabilities with the users of the asset.
    - The owner of the cyber asset should also propose a patch/fix.
    - Best practices include sharing these vulnerabilities with CERTs/CSIRTs (national or sectoral) to support them in the response to any cyber incidents related the cyber asset in question.
  - A difference can be considered between potential, confirmed and exploited vulnerabilities in terms of how to deal with sharing information related to those vulnerabilities.

CYBER INCIDENT REPORT

- Contains information about a cyber incident affecting an organization.
- The following information should be included, to the extent possible, in cyber incident reports: summary, type, exact date and time of occurrence, location of occurrence, duration, chronology (i.e. sequence of events), IOCs, TTPs, context, vulnerability(ies), impacts (safety, security, efficiency, capacity, business, financial, reputation), severity, motivation, target, threat actor, impacted services and organization(s), etc.
- As a general rule, the more information provided, the more actionable the report will be.

CYBER MITIGATIONS

- Contains information on methods for:
  - remedying vulnerabilities;
  - mitigating cyber threats; and
  - responding to and recovering from cyber incidents.
- Common forms of such information include patches to address vulnerabilities, antivirus updates to stop exploits, and directions for purging malicious actors from networks.

SITUATIONAL AWARENESS

- Contains information that provides decision-makers with real-time telemetry of exploited vulnerabilities, active threats, and cyber-attacks that may be required to respond to a cyber incident.
- It could also contain information about the targets of attacks and the state of critical public or private computer networks.

BEST PRACTICES

- Contains information related to how software and services are developed and delivered, such as security controls, development and incident response practices, and software patching or effectiveness metrics.

3.2 Senders, recipients and sources of cyber information

- Sharing cyber information requires a sender, a receiver, and a source of information (if the information does not originate from the sender).
- The table below includes examples of senders, receivers, and sources of cyber information in civil aviation.

Senders/recipients	• Airspace users (e.g. airlines, general aviation, unmanned aircraft system (UAS) operator) • Air navigation service providers (ANSP) • Airport operators • Authorities (e.g. civil aviation authority (CAA)) • Aviation service providers • Manufacturers • Aviation and non-aviation supply chain • Others
Sources	• Senders/recipients as listed above • Aircraft (e.g. UAS, airplanes) • Open Source Intelligence (OSINT) sources • CTI vendors • International associations and organizations (e.g. airline/airport/ANSP associations) • International/national/regional aviation cybersecurity centres and aviation CERTs/ISACs • Others

- Appendix A includes the recommended flow of the different types of cyber information that can be shared between the different aviation stakeholders.

3.3 Assessment, analysis and TLP marking of cyber information to be shared as a sender

3.3.1 Assessment and analysis

Before sharing cyber information, the sender should undertake an analysis in order to:

- assess the trustworthiness of the source (see 3.3.1.1 and Appendices B and D);
- analyse the plausibility/credibility of the information (see 3.3.1.2 and Appendices C and D); and
- analyse the relevance of the information to its organization, the information sharing community (receiving organization(s)), and to the aviation ecosystem.

This step is critical in cyber information sharing. Without it, the information becomes a collection of data/findings without context.

When conducting the above analysis, it is important to recall that:

- different analytical problems require different approaches; and
- analysts should be aware of their natural biases, and make as much effort as possible to overcome them to conduct an objective analysis by using appropriate methods and tools.

To illustrate the role of assessment and analysis of cyber information, Figures 2 and 3 below describe the difference between Open Source Information and Open Source Intelligence, where it becomes evident that the usability of information significantly increases with proper analysis and assurance before dissemination.

- **OSINF (Open Source Information)** where information collected is shared as is.

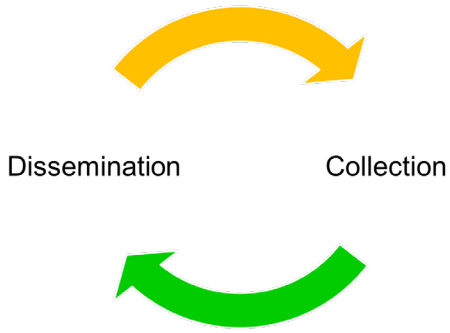

Figure 2. OSINF - Open Source Information

- **OSINT (Open Source Intelligence)** where information is subjected to the process below after its collection.

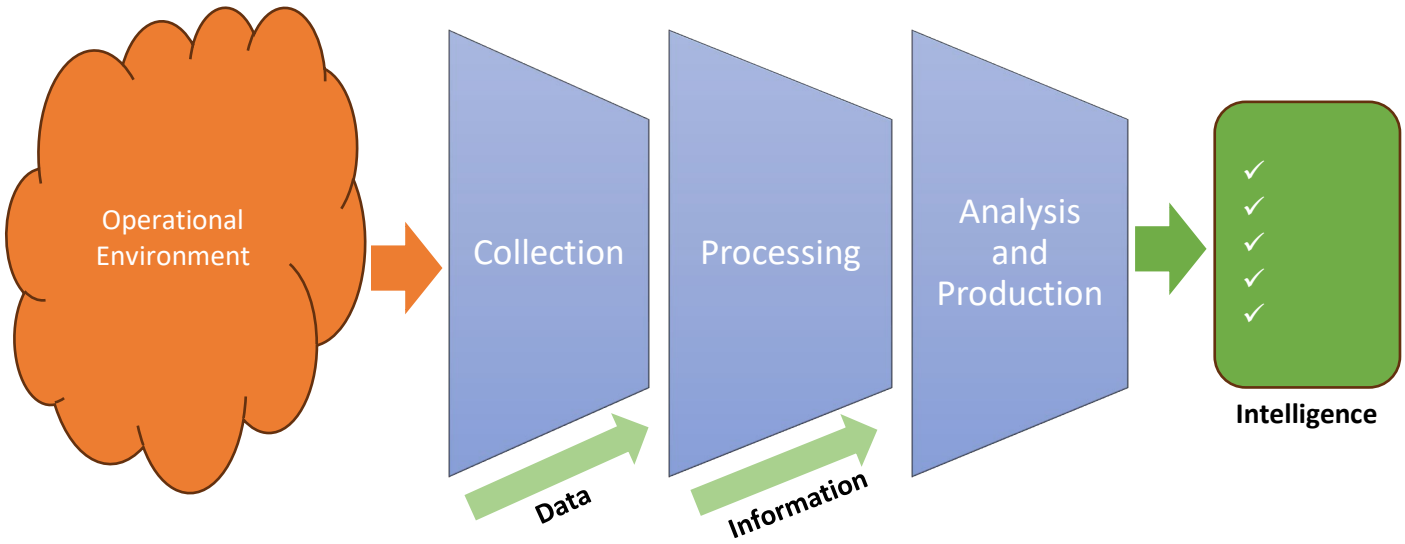

Figure 3. Cyber Intelligence Production[8]

3.3.1.1 Assessment of the trustworthiness and reliability of the source

Assessing the level of trustworthiness and reliability of the source of cyber information/intelligence is crucial for making informed decisions.

Appendix B includes an example of a framework for defining criteria and proposes an assessment scheme to measure the trustworthiness and reliability of a source of cyber information/intelligence.

The weights and scoring scale used in Appendix B can be adjusted to align with the organization's specific requirements and its risk tolerance.

Appendix D provides another example of an information trust scheme to assess both the trustworthiness of the source and the credibility of information (see 3.3.1.2 below) using a different method: the Admiralty Scale (or the NATO system).

Organizations should regularly reassess and update trust scores as the cyber threat landscape and sources of threat intelligence evolve over time.

3.3.1.2 Analysis of the plausibility/credibility of the cyber information

Assessing the level of plausibility/credibility of cyber information/intelligence is essential.

Appendix C includes an example of a framework for defining criteria and proposes an assessment scheme to measure the plausibility/credibility of cyber information/intelligence.

The weights and scoring scale used in Appendix C can be adjusted to align with an organization's specific requirements and its risk tolerance.

[8] Adapted from Joint Publication 2-0, *Joint Intelligence* (2013).

Organizations should regularly reassess and update plausibility/credibility scores as new cyber threat information/intelligence becomes available, and the cyber threat landscape evolves over time.

Appendix D provides another example of an information trust scheme to assess both the trustworthiness of the source (see 3.3.1.1 above) and the credibility of information using a different method: the Admiralty Scale (or the NATO system).

3.3.2 Traffic Light Protocol (TLP)[9,10] marking:

3.3.2.1 Using TLP in aviation

The TLP standard encompasses five markings: RED, AMBER, AMBER+STRICT, GREEN, and CLEAR.

As the **TLP:CLEAR** marking does not constraint the dissemination of the received information to anyone through any medium, and as the **TLP:RED** marking limits disclosure of the information to the specific recipient(s) with no further distribution at all, these two markings are not discussed in this section. The three markings which would require some clarification about how to apply them in an aviation context are:

- **TLP:GREEN**
- **TLP:AMBER**
- **TLP:AMBER+STRICT**

TLP:GREEN	- Information marked TLP:GREEN can be shared within the aviation community. - The recipient of TLP:GREEN information can further distribute it to any aviation organization (CAA, ANSP, airport operators, airspace users, manufacturers, aviation service providers, etc.). - It can be also shared with cybersecurity organizations having a role in aviation (national cybersecurity centres, national/regional/international aviation CERTs/CSIRTs, aviation ISACs, etc.). - It can further be shared with non-aviation organizations using similar technologies (e.g. information related to Operational or Information Technologies), sharing similar cyber threats or providing services to aviation (e.g. telecommunication systems or services, energy systems or services). Those non-aviation organizations can be actors of other sectors (e.g. operators, authorities, manufacturers) or cyber-related organizations (national cybersecurity centres, other sectors' related CERTs/CSIRTs, other sectors' ISACs).

[9] The Traffic Light Protocol (TLP) is a standard developed by FIRST (Forum of Incident Response and Security Teams) to facilitate sharing of information with the appropriate audience. This document provides guidance on the use of version 2.0 of the TLP standard which can be found on this link: https://www.first.org/tlp/.

[10] The guidance in this document supersedes the "Guidance on Traffic Light Protocol" that was published by ICAO in 2021.

TLP:AMBER	- Information marked TLP:AMBER can be shared on a **need-to-know basis** within the organization of the recipient and its clients. - Though the meaning of organization is straightforward, in aviation the meaning of "clients" having a **need-to-know basis** should be interpreted as follows: o CAAs can share such kind of information: ▪ within their State with: • national aviation stakeholders; • national cybersecurity centre(s); and • national aviation CERT/CSIRT(s) and ISAC(s). ▪ outside their State with: • other CAAs; and • national/regional/international aviation CERTs/CSIRTs and ISACs. o Aviation stakeholders (ANSP, airport operators, airspace users, aviation service providers) can share this kind of information with: ▪ their national CAAs; ▪ organizations supporting their service provision; ▪ national/regional/international aviation CERTs/CSIRTs and ISACs; and ▪ their customers excluding passengers (e.g. travel agents, duty-free outlets). o Manufacturers can share this kind of information with: ▪ national CAAs; ▪ their customers (e.g. airlines, airports); ▪ national/regional/international aviation CERTs/CSIRTs and ISACs; and ▪ their sub-contractors.
TLP:AMBER+STRICT	- Information marked TLP:AMBER+STRICT can be shared on a **need-to-know basis** only within the organization of the recipient.

3.3.2.2 Recommended TLP marking of different cyber information

It is recommended to use the following guidelines when marking cyber information, for aviation purposes. Some considerations may result in deviating from the below recommendations, including but not limited to:

- TLP marking might evolve over time: cyber information may be marked more restrictive when it is first shared, then its marking may be downgraded over time as the risk associated with the information has decreased with wider disclosure.
- State vs. industry perspectives on markings: a State can have different rules to mark cyber information than an aviation stakeholder due to different considerations (for example national security constraints).
- National constraints applicable to industry: a State may have a specific marking for some type of information that applies to national critical infrastructures (for example initial disclosure of IOCs such as suspicious IP addresses).

CYBER INTELLIGENCE

- **Cyber Threat Intelligence (CTI)**:
  - **Strategic:** depends upon the nature of the strategic CTI and of the audience (e.g. Board of Directors (BoD), C-level, CTI analyst, blue team)
    - TLP:RED: specific and very sensitive intelligence about a specific cyber threat targeting an organization. A limited number of specific decision makers need to be aware.
    - TLP:AMBER: senior management, BoD members or decision making committee members need to be aware of a specific cyber threat either targeting the organization, relevant to aviation (e.g. supply chain, connected stakeholder), and/or relevant to national critical infrastructure.
    - TLP:GREEN: intelligence that should be shared with a community to ensure that it is widely known and acted upon (e.g. policy documents, whitepapers, trends, statistics).
  - **Operational:**
    - TLP:RED: for specific operational, technical and security staff who need to act upon specific intelligence about a specific cyber threat or incident targeting a relevant aviation stakeholder or a national critical infrastructure (e.g. supply chain, connected stakeholder).
    - TLP:AMBER: for operational, technical and security staff who need to be aware of a specific cyber threat or incident either targeting the organization or relevant to aviation or to national critical infrastructure.
    - TLP:GREEN: intelligence that should be shared with a community to ensure that it is widely known and acted upon.
  - **Tactical:**
    - TLP:RED: for specific security and technical staff who need to act upon a specific cyber threat targeting the organization or need to be aware of an ongoing cyber incident.
    - TLP:AMBER: for security and technical staff who need to be aware of a cyber threat or an ongoing cyber incident or vulnerability targeting the organization, or relevant to aviation or to national critical infrastructure.
    - TLP:GREEN: intelligence that should be shared with a community to ensure that it is widely known and acted upon.

- **IOCs**: TLP:GREEN
- **TTPs**: TLP:GREEN
- **Vulnerabilities**:
  - Exploited vulnerability: TLP:RED
  - Confirmed vulnerability (with or without patch): TLP:AMBER
  - Potential vulnerability without patch: TLP:AMBER
  - Potential vulnerability with patch: TLP:GREEN

CYBER INCIDENT REPORT

- No recommendation as it depends upon the nature, the context, and the timing of the incident (i.e. time between the cyber incident and the sharing of information). TLP:CLEAR may be excluded at the early stages, though it may become applicable after some time.

3.4 Assessment and analysis of information as a recipient

The recipient of cyber information should analyse the received information to ensure that it is:

1. **Trusted/assured/quality:** the level of trust[11] in the cyber information may not be sufficient to consider that the information should trigger some actions on the recipient's side.
2. **Relevant:** an example of relevance is if the recipient cannot act upon the information (e.g. does not have a need to know) whereas the information is relevant to another personnel in the organization. This can be a hindrance if the information received is TLP:RED. In this case, the recipient should engage with the sender to either seek the consent of the sender to forward the information to the concerned recipient(s) through receiving a lower marking version of the information, or to provide the sender with another point of contact in the organization to receive the TLP: RED version of the information.
3. **Actionable:** the TLP marking may prevent the recipient from acting upon the information, which would require further discussion between the sender and the recipient to allow taking action based on the information received. For example:
   - If the information is marked TLP:RED and the recipient needs to engage with others in the organization to act upon it, but those concerned have not received the same information.
   - If the information is TLP:AMBER+STRICT and the recipient needs to engage with another organization to act in accordance with the content being shared.

The analysis should also include the following activities:

- The recipient should combine the cyber information received with available intelligence (for example correlate and/or complement it with other information). This will help to increase or decrease the level of trust in that information.
- The recipient should contextualize the information in relation to their duties, which would address questions related to the meaning of the information to the recipient in a political, strategic, operational, technical and/or cybersecurity context.

[11] See 3.3.1.1, 3.3.1.2, and Appendices B, C and D.

3.5 Trusted relationship between parties

Trust is a dynamic and multifaceted concept that is essential for the secure sharing and exchange of sensitive information. It is not an absolute measure, but a relative one that varies according to context, relationships and behaviours.

Establishing trusted relationships between the sending and receiving parties is crucial for effective cyber information sharing.

Trusted relationships with non-traditional partners or stakeholders may also be necessary. It is important to identify key parties for proactive and/or reactive cyber information sharing to ensure timely and relevant dissemination.

Trusted relationships can be with a variety of partners and stakeholders. Examples of trusted relationships include:

- Within aviation:
  - Between State agencies (nationally and/or internationally)
  - From State agencies to aviation organizations and vice-versa
  - Between industry organizations
  - From State agencies or aviation organizations to international organizations (e.g. ICAO) and vice-versa
- With non-aviation partners and stakeholders:
  - Non-governmental organizations
  - Non-profit organizations
  - International organizations (e.g. relevant United Nations agencies)
  - International Criminal Police Organization – INTERPOL (ICPO–INTERPOL))

Building trust typically takes time. States and stakeholders can establish, nurture and foster trusted relationships through:

- Alliances with like-minded partners.
- Regular activities: participation in periodic meetings or conferences.
- Agreements: the following two sections provide guidance on the types of agreements that can be developed for cyber information sharing.

States and stakeholders should also consider the benefits (see Section 1.1) and costs associated with establishing and maintaining trusted relationships, in order to justify and decide on the investment needed for such endeavours. Considerations should include:

- Time: what is the time commitment to set up and develop a relationship.
- Resources: including human and financial resources.
- Benefits: what does each party receive from the relationship.
- Liabilities: potential losses for each party by having a relationship.
- Maintenance: the ongoing cost of maintaining a relationship in terms of time and resources should also be taken into consideration.

Maintaining trusted relationships involves activities such as:

- Face-to-face and virtual meetings: the meeting frequency is to be agreed upon between the parties. It is recommended to be conducted as needed, and at least annually for face-to-face meetings, taking into account the level of personnel involved (senior, middle or technical level).
- Proactive cyber information sharing: frequent information sharing based on needs and priorities. This information can include:
  - Changes to policies and procedures that could affect the recipient(s).
  - Products: spot reports, strategic analysis, etc.
  - Raw information: source codes, logs, etc.

- Reactive cyber information sharing: this can include sharing information related to the response to a cyber incident:
    - During a cyber incident: real-time and consistent information sharing as the incident is ongoing.
    - After a cyber incident: sharing of findings, root causes, lessons learned, etc.

Trusted relationships can potentially end when the trust element is broken. Examples of actions that could lead to such result are:

- Unauthorized disclosure of classified information: the accidental or deliberate disclosure of classified information to unauthorized individuals or organizations that may be of national security or proprietary significance.
- Deliberate sharing of sensitive information: intentionally sharing sensitive security information or sensitive proprietary information with individuals or organizations to expose vulnerabilities or damage creditability, especially if done in the public domain.

3.5.1 Formal agreements

Cyber information sharing between parties can be formalized through bilateral or multilateral, binding or non-binding agreements.

Such agreements include different types of parties. For example, agreements can be developed between States, between State agencies (for example between a civil aviation authority and national cybersecurity agency in the same State), between governmental agencies in different States (for example between civil aviation authorities of different States), between a State agency and aviation stakeholder(s) within the same State, between a State agency and industry stakeholder(s) in another State, and/or between aviation stakeholders.

Appendix E provides a recommended list of sections to be covered in a formal cyber information sharing agreement to ensure clear roles and responsibilities of the parties sharing cyber information, which will reflect positively on the trust level between the parties over time.

3.5.2 Informal agreements

Informal agreements are often used when trust between the exchanging parties is already established or implied. These types of agreements should be used carefully as they have no legal implications on the signatory parties. They should not be the primary or sole mechanism for cyber information sharing.

Such agreements include limited information that is needed for the parties to share information, for example:

- the technical means to be used to share information; and
- respective points of contact (individual and team details).

The rigorous and consistent use of TLP marking is emphasized in importance when sharing cyber information using informal agreements, in order to maintain and foster the existing trust between the parties.

4. STRUCTURING, COMMUNICATING AND ARCHIVING SHARED CYBER INFORMATION

4.1 Structuring cyber information to be shared

Cyber information should be structured based on defined taxonomies or through a defined structure in order to ensure that it is shared with adequate context as well as with useful and actionable details.

This is an example of how to structure cyber information to be shared:

- Title: high-level description of the cyber information
- Reference number: to support the sender track the information
- TLP marking
- Main aspects, including but not limited to:
    - Category (e.g. cyber-espionage, cybercrime, information operation)
    - Type (e.g. vulnerability, botnet, surveillance, personal data, social media, credential leak, phishing, DDoS, malware)
    - Cyber threat level (e.g. Critical, High, Medium, Low)
    - Domain/sector
    - Trust and reliability of the source of information (see 3.3.1.1)
- Key points: list of bullet points that explains the information
- Summary
- Attribution: threat actor(s) that might have been potentially or actually identified as the perpetrator(s)
- Assessment of impacts, targets, victims, etc.
- Recommendations for actions to be taken by the recipient(s)
- Actionable information
    - Affected cyber assets
    - Timeline
    - IoCs
    - Detection rules
    - TTPs
- Mitigations
    - Generic mitigations
    - Specific mitigations
- References

4.2 Communicating cyber information

This section provides guidance on the advantages and disadvantages of using various media to share cyber information.

4.2.1 Telephone

This type of communication suits a TLP:RED marking to ensure a synchronous communication with the person intended to receive the information. It also helps communicate critical information that requires an immediate response.

If using telephone to share cyber information, it is recommended to consider controls that assure the identity of both parties (e.g. to avoid AI generated audio injections).

Overall, this medium has limited usability (used mainly to share high urgency and/or TLP:RED cyber information), and therefore should be considered in conjunction with other mediums of cyber information sharing.

4.2.2 Plain email

Cyber information can be shared in plain text in an email.

Using this medium to share cyber information means that:

- The recipient has to open the email and read the information.
- There is a need for an analysis of the content by a CTI analyst to assess its relevance to the recipient.
- The information will initially be processed manually.

Below are some limitations for the use of plain email messages to share cyber information:

- This medium suits short and text-based content.
- Some email systems may block the email as it may contain IOCs, which would trigger IT security controls.
- Up-to-date lists of emails are difficult to maintain. The use of individual and generic email addresses is recommended.
- Information marked TLP:RED cannot be sent to generic emails (e.g. groupmailbox@company.com), but only to individual emails (e.g. someone@company.com).
- Some types of email addresses may not be considered as trusted recipients (e.g. non-professional email addresses hosted on commercial email hosting services such as gmail/hotmail/yahoo/etc.)
- There is a risk of email impersonation. As such, it is recommended to use adequate authentication methods, such as email digital signature, to manage that risk.

4.2.3 Email with attachment

Cyber information can be shared in a document attached in an email. The attachment can be encrypted with a password that can be sent to the recipient via another trusted means (e.g. text messages, secure messaging application).

Using this medium to share cyber information means that:

- The recipient has to open the attachment and read the information.
- There is a need for an analysis of the content by a CTI analyst to assess its relevance to the recipient.
- The information will initially be processed manually.

Below are some limitations for the use of email messages with attachment to share cyber information:

- There is a risk of clicking on a malicious attachment – thus the attachment has to be sanitized first.
- Some email systems block some types of attachments (e.g. compressed files such as files with .zip, .rar, and .7z extensions).
- Some email systems may block the access to the document as it may contain IOCs which would trigger the IT security controls.
- The size of the attachment may prevent its transmission via email.
- Up-to-date lists of emails are difficult to maintain. The use of individual and generic email addresses is recommended.
- Information marked **TLP:RED** cannot be sent to generic emails (e.g. groupmailbox@company.com), but only to individual emails (e.g. someone@company.com).

4.2.4 Private repository

Cyber information can be shared via access to a private repository that contains the information to be shared.

In such scheme, notification methods should be put in place to notify the recipient(s) that new cyber information is available to be accessed.

This notification can be automated to be done via email or other means (e.g. text messages, secure communication application).

The access to the repository must be protected and maintained:

- Security controls/protections should be deployed in accordance with the sensitivity of information shared on the repository. Controls could include repository hosting (e.g. private/shared server, cloud hosting), access control/rights, user authentication methods (e.g. single sign-on (SSO), two/multi-factor authentication (2FA/MFA)), etc.
- The list of organizations/individuals authorized to access the repository should be continuously maintained to ensure its currency and authenticity.
- Access rights, such as *Read and Write* privileges, should be provided to individual accounts and maintained.
- All accesses and actions taking place on the repository should be logged and analysed.
- Cyber information posted on the repository should be carefully catalogued into folders as not all participants have the same access to information. Moreover, there is a need to move information between folders as classification (e.g. TLP marking) of the information changes over time (e.g. may be accessible to a larger audience if the classification/TLP marking is lowered). This can become a complex process as the number of members of the community and the information shared on the repository grows with time.

4.2.5 Applications

Various software applications (open source or commercial) can be used to share cyber information (for example MISP, OpenCTI, CyWare, etc.).

It is not possible to provide a generic list of considerations for applications in general, as this depends on the nature of the application (e.g. open source or commercial), who is responsible for developing and updating security controls, access rights, cataloguing of the information (e.g. manual or automatic through rules), storage of sensitive information (e.g. secure/private

or public servers), etc. Therefore, it is recommended to assess all these aspects, and others as required, when considering the use of applications for cyber information sharing.

Among existing applications, Appendix F provides information about MISP - Open Source Threat Intelligence and Sharing Platform, as the platform provides interesting features that would support the aviation sector's efforts to share cyber information.

4.3 Archiving cyber information

Shared cyber information should be archived by both sender and recipient for record keeping and quality control purposes.

The following aspects should be considered when archiving information:

- Regulations: consideration should be given to regulations that may apply to archiving information (for example, privacy laws and their requirements for archiving specific types of information and the maximum allowed duration of keeping that information in archives).
- Storage media: the use of storage media depends on the type of information. Different types of media may be used to archive cyber information. For example, cyber incident reports can be stored in a specific stand-alone database, cyber threat intelligence reports can be stored as a file on a computer disk, etc.
- Access control and rights: access to archived cyber information should be defined in a policy that defines who can access what type of information. This goes in line with the TLP marking of the information (for example **TLP:AMBER+STRICT** does not mean everybody in an organization, only those having a need to know).
- Local versus remote accessibility: some cyber information may not be allowed to be accessed from outside the organization (through intranets for example) but only internally. This also includes defining access right privileges based on roles and responsibilities of the personnel which can be used for auditing/assurance purposes.
- Security controls/protection: depending on the type of information, different levels of security controls and protection should be deployed. For example, more stringent controls should be implemented to protect cyber incident reports than those implemented to protect already patched vulnerabilities.
- Relevance: some cyber information may become obsolete due to some developments. For example, vulnerabilities of systems not used anymore by the organization, strategic cyber threat intelligence related to geo-political events that don't exist anymore, etc.
- Usability: various categories of archives should be defined to support the continued usability of the information. For example:
    - "Hot": includes recent data that is stored without compression to the files, allowing maximum performance for retrieval and processing;
    - "Warm": includes data that is stored with slight compression, allowing very good performance for retrieval and processing if needed; and
    - "Cold": includes data that has been archived and fully compressed, and which requires manual retrieval and decompression to be made available.
- Duration: the duration for which cyber information is archived should be considered depending on the type of information. For example, archiving rules can be defined to keep IOCs not older than [X] years. In addition, actions related to deleting outdated information should be implemented as part of the processes to manage cyber information archiving.

5. FURTHER SHARING CYBER INFORMATION

5.1 Why to further share cyber information

Further sharing of cyber information received from an external source may be necessary to ensure the information is known by the broadest audience that has a need to know. However, careful consideration should be taken before further sharing cyber information.

As an example scenario, a State agency receives information from an originator which only allows further sharing with entities with which the originator has a formal agreement. The State agency assesses that other State agencies, which do not have a formal agreement with the originator of the information, have a need to know the information. In this case, the recipient of the information should contact the originator of the information and seek their consent to share the information further with the other agencies that have a need to know.

To determine whether and with whom to further share cyber information, the recipient of the information should consider factors such as:

- Limitations of further sharing: can or should this information be shared further? In case of doubt (e.g. doubt of potential misuse of the TLP marking), the recipient may seek permission of the sender to further share the information.
- The purpose of further sharing the information and the role of the considered recipient.

The purpose of further sharing cyber information is related to what action is expected from the recipient:

- For information/awareness: the considered recipient has a need to know and the information is shared for informational purposes only.
- For action: the considered recipient has a need to know, and the cyber information is further shared for a specific action to be performed by the recipient. Such actions can include:
  - Allocating or mobilizing resources to address a particular issue.
  - Allocating or mobilizing resources to mitigate a particular cyber threat or vulnerability.
  - Allocating or mobilizing resources for response assistance purposes.

The role of the considered recipient may be a factor in deciding whether to further share cyber information. Roles that might have a need to know include for example:

- **Technical experts**: an expert or specialist who oversees the protection of networks, systems, services, applications, IT/OT infrastructures, etc., from unauthorized access.
- **Policy maker**: an individual who drafts aviation, or relevant non-aviation, cybersecurity strategies, policies, procedures and/or processes to be implemented by aviation stakeholders.
- **Decision maker**: a senior staff member who approves the implementation of aviation, or relevant non-aviation, cybersecurity strategies, policies, procedures and/or processes.
- **Coordinator**: a cybersecurity expert or specialist tasked with effectively channelling shared information to the right personnel.
- **Aviation Safety Officer**: an aviation safety expert who can further determine a possible impact on aviation safety, efficiency, and/or capacity.
- **Aviation Security Officer**: an aviation security expert who can further determine a possible impact on aviation security.

5.2 Rules to further share cyber information

The rules to further share cyber information include many areas that should be carefully considered:

- The organization the information is further shared with (e.g. State/aviation stakeholder/non-aviation stakeholder, national/international entity).
- The role of the recipient with whom the cyber information is further shared.
- What will be shared: the full cyber information or an extract (e.g. entire document or just relevant paragraphs).
- Under what circumstances the information will be shared: proactive or reactive.
- Frequency of sharing: routine or as needed.
- Why the cyber information is shared (e.g. for information or action).
- Handling of cyber information: all original classifications and caveats must remain on the appropriate channels of communication (i.e. classified and unclassified channels of communication).
- The TLP marking of the cyber information cannot be changed when it is further shared.

5.3 Method and media to further share information

The method/medium to further share cyber information should be secure and simple, as appropriate.

Physical information: Information that is provided in hard copy. The information should be properly packaged (e.g. in a folder) and secured (e.g. a folio that zips or latches closed) during transit to the meeting location and before providing the hard copy(ies). Any handling reminders or caveats should be noted on the information itself or on a coversheet (e.g. handling caveats of Sensitive Security Information (SSI)[12] are usually included in a coversheet with instructions).

Electronic information: The same means of sharing cyber information discussed in Section 4.2 are applicable to further sharing information. However, consideration should be given to the fact that the intended recipient with whom the cyber information is shared further may not have access to some electronic means that the sender has access to (e.g. white-listed email, access to the portal/repository where the information resides).

There are additional rules for handling classified information that varies by State or organization. Those rules should be strictly followed in accordance with applicable rules and procedures.

— — — — — — — —

[12] Guidance on handling Sensitive Aviation Security Information in Section 2.3 of the ICAO *Aviation Security Manual* (Doc 8973 – Restricted) provides useful information that can be used in a cyber information sharing context.

Appendix A
Recommended Cyber Information to be Shared in Aviation According to the Information Type

CYBER INTELLIGENCE

- **Cyber Threat Intelligence (CTI)**:
  - **Strategic**:
    - From State agencies (national cybersecurity centre, CAA, etc.) to aviation stakeholders within the State
    - From national cybersecurity centre to aviation CERTs/ISACs
    - From aviation CERTs/ISACs to aviation stakeholders
    - Amongst trusted national cybersecurity centres
    - Amongst trusted States
  - **Operational**:
    - From aviation stakeholders to aviation stakeholders
    - From aviation CERTs/ISACs to aviation stakeholders
    - From aviation stakeholders to State agencies (national cybersecurity centre, CAA, etc.) within the State
  - **Tactical**:
    - From aviation stakeholders to aviation stakeholders
    - From aviation CERTs/ISACs to aviation stakeholders
    - From national cybersecurity centre to aviation CERTs/ISACs
    - From national cybersecurity centre to aviation stakeholders within the State
    - From aviation stakeholders to State agencies (national cybersecurity centre, CAA, etc.)

- **IOCs**:
  - From aviation stakeholders to aviation stakeholders
  - From aviation CERTs/ISACs to aviation stakeholders
  - From national cybersecurity centre to aviation CERTs/ISACs
  - From national cybersecurity centre to aviation stakeholders within the State
  - From aviation stakeholders to national cybersecurity centre in the State

- **TTPs**:
  - From aviation stakeholders to aviation stakeholders
  - From aviation CERTs/ISACs to aviation stakeholders
  - From national cybersecurity centre to aviation CERTs/ISACs
  - From national cybersecurity centre to aviation stakeholders in the State
  - From aviation stakeholders to national cybersecurity centre in the State

- **Vulnerabilities**:
  - From aviation stakeholders to aviation stakeholders
  - From aviation stakeholders to their supply chain providers
  - From researchers to aviation CERTs/ISACs
  - From researchers to State agencies (national cybersecurity centre, CAA, etc.)
  - From researchers to aviation stakeholders
  - From researchers to supply chain
  - From aviation CERTs/ISACs to aviation stakeholders
  - From national cybersecurity centre to aviation CERTs/ISACs
  - From national cybersecurity centre to aviation stakeholders in the State
  - From aviation stakeholders to relevant State agencies (national cybersecurity centre, CAA, etc.) in the State

CYBER INCIDENT REPORT

- Mandatory cyber incident reports (through applicable national laws and/or regulations):
  - From aviation stakeholders to relevant State agencies (national cybersecurity centre, CAA, etc.) (for aviation safety and/or security incidents)
  - From aviation stakeholders to law enforcement authorities (for specific incidents related to cybercrime such as fraud or to specific laws such as privacy laws)
  - From State to ICAO (for cyber incidents related to acts of unlawful interference)

- Voluntary cyber incident reports:
  - From aviation stakeholders to national cybersecurity centre
  - From aviation stakeholders to aviation stakeholders (especially if they are interacting)
  - From aviation stakeholders to aviation CERTs/ISACs

— — — — — — — —

Appendix B
Example Framework for Assessing and Ranking the Trustworthiness and Reliability of a Source of Cyber Information/Intelligence

1. Reputation and track record:
   - Assess the source's history and reputation in the cybersecurity community.
   - Look for past successes, contributions, and their involvement in industry organizations.
   - Evaluate their track record in providing accurate and timely cyber threat information/intelligence.

2. Credibility and expertise:
   - Evaluate the qualifications, certifications, and expertise of the individuals or teams behind the source.
   - Consider their experience in the specific domain of cyber threat information/intelligence.

3. Data sources and collection methods:
   - Examine the source's data collection methods and sources.
   - Determine if they have access to diverse and reliable data feeds.
   - Assess the rigor of their data collection processes.

4. Data sharing and collaboration:
   - Determine if the source shares cyber threat information/intelligence with trusted organizations or industry peers.
   - Collaboration with other cybersecurity entities can enhance credibility.

5. Transparency:
   - Assess the level of transparency in their reporting and methodologies.
   - Evaluate if they disclose their data sources, analysis techniques, and update frequency.

6. Timeliness and accuracy:
   - Evaluate the source's ability to provide timely and accurate cyber threat information/intelligence.
   - Consider their historical performance in predicting and detecting cyber threats.

7. Analysis and context:
   - Analyse the depth and quality of their cyber threat analysis.
   - Assess their ability to provide context around cyber threats, including attribution and potential impacts.

8. Alignment with industry standards:
   - Determine if the source follows industry standards and best practices in cyber threat information/intelligence, for example adherence to frameworks like STIX/TAXII and common data formats.

9. Legal and ethical compliance:
   - Ensure that the source complies with legal and ethical standards regarding data collection and sharing.

To measure the level of trust in a source of cyber information/intelligence, one can use a scoring system based on the above criteria.

Below is an example of an assessment scheme.

1. Assign a weight to each criterion based on its importance to an organization's specific needs and risk profile.
2. Rate the source on a scale (e.g. 1-5) for each criterion, with 5 being the highest level of trust.
3. Calculate an overall trust score by summing up the weighted scores for each criterion. A higher score indicates a more trustworthy source.

Here is a simplified example of how to calculate an overall trust score:

- Reputation and track record: 4/5
- Credibility and expertise: 5/5
- Data sources and collection methods: 3/5
- Data sharing and collaboration: 4/5
- Transparency: 4/5
- Timeliness and accuracy: 4/5
- Analysis and context: 5/5
- Alignment with industry standards: 4/5
- Legal and ethical compliance: 5/5

The overall Source Trust Score could be:

(4*0.1) + (5*0.15) + (3*0.1) + (4*0.1) + (4*0.1) + (4*0.1) + (5*0.15) + (4*0.1) + (5*0.1) = **4.30**

— — — — — — — —

Appendix C
Example Framework for Assessing the Plausibility/Credibility of Cyber Information/Intelligence

1. Corroboration from multiple sources:
   - Assess whether the cyber threat information/intelligence is corroborated by multiple independent sources, for example multiple sources reporting the same information can increase plausibility.

2. Consistency with known threats and tactics:
   - Determine if the cyber threat information/intelligence aligns with known cyber threats, attack techniques and tactics, for example inconsistencies may indicate a lower level of plausibility.

3. Technical details and evidence:
   - Examine the presence of technical details and evidence supporting the cyber threat information/intelligence, for example strong technical evidence increases plausibility.

4. Attribution and motivation:
   - Evaluate the attribution of the cyber threat to specific actors or groups.
   - Consider the motivation of these actors and whether it aligns with the reported cyber threat.

5. Timing and context:
   - Analyse the timing of the cyber threat and its context within the cybersecurity landscape.
   - Consider if the cyber threat aligns with current events or trends.

6. Historical accuracy:
   - Assess the source's historical accuracy in reporting cyber threats, for example a consistent record of accurate reporting increases plausibility.

7. Peer validation and trust groups:
   - Determine if the cyber threat information/intelligence has been validated or endorsed by trusted peers or industry groups, for example peer validation can enhance plausibility.

8. Red flags and anomalies:
   - Look for red flags, anomalies, or suspicious elements in the cyber threat information/intelligence; addressing and explaining such issues can improve plausibility.

To measure the level of plausibility/credibility in cyber information/intelligence, one can use a scoring system based on the above criteria.

Below is an example of a scoring system.

1. Assign a weight to each criterion based on its importance and relevance to an organization's cyber risk assessment.
2. Rate the threat intelligence on a scale (e.g. 1-5) for each criterion, with 5 indicating the highest level of plausibility.
3. Calculate an overall plausibility score by summing up the weighted scores for each criterion. A higher score indicates a more plausible threat intelligence report.

Here is a simplified example of how to calculate an overall plausibility/credibility score:

- Corroboration from multiple sources: 4/5
- Consistency with known threats and tactics: 3/5
- Technical details and evidence: 5/5
- Attribution and motivation: 4/5
- Timing and context: 4/5
- Historical accuracy: 4/5
- Peer validation and trust groups: 4/5
- Red flags and anomalies: 3/5

The overall Plausibility/Credibility Score could be:

(4*0.15) + (3*0.15) + (5*0.15) + (4*0.1) + (4*0.15) + (4*0.1) + (4*0.1) + (3*0.1) = **3.90**

— — — — — — — —

Appendix D
Example Cyber Information Trust Scheme

This appendix describes the Admiralty Code[13], as another example of a method for evaluating collected items of intelligence.

The scale can be used when sharing information to provide a sense of the reliability of the source and credibility of the information. The method consists of a two-character notation (a letter and a number), the letter evaluates the reliability of the source and the number reflects assessed level of trust on the information.

Reliability of source

A source is assessed for reliability based on a technical assessment of its capability, or in the case of Human Intelligence sources, their history. The notation uses alphabetical coding from A to F to score the reliability of the source as follows.

Reliability Code	Reliability	Explanation
A	Completely reliable	No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability.
B	Usually reliable	Minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time.
C	Fairly reliable	Doubt of authenticity, trustworthiness, or competency but has provided valid information in the past.
D	Not usually reliable	Significant doubt about authenticity, trustworthiness, or competency but has provided valid information in the past.
E	Unreliable	Lacking in authenticity, trustworthiness, and competency; history of invalid information.
F	Reliability cannot be judged	No basis exists for evaluating the reliability of the source.

[13] Details of the method can be found on pages 59 – 60 of the Joint Doctrine Publication 2-00, Intelligence, Counter-intelligence and Security Support to Joint Operations (Fourth Edition), available here: https://www.gov.uk/government/publications/jdp-2-00-understanding-and-intelligence-support-to-joint-operations

Credibility of information

An item is assessed for credibility based on likelihood and levels of corroboration by other sources. The notation uses a numeric coding from 1 to 6 to score the credibility of the source as follows.

Credibility Score	Credibility	Explanation
1	Confirmed by other sources	Confirmed by other independent sources; logical in itself; consistent with other information on the subject.
2	Probably True	Not confirmed; logical in itself; consistent with other information on the subject.
3	Possibly True	Not confirmed; reasonably logical in itself; agrees with some other information on the subject.
4	Doubtful	Not confirmed; possible but not logical; no other information on the subject.
5	Improbable	Not confirmed; not logical in itself; contradicted by other information on the subject.
6	Truth cannot be judged	No basis exists for evaluating the validity of the information.

The above tables can be combined into the below table.

Reliability of the Source		Credibility of the Cyber Information	
A	Completely reliable	1	Confirmed by other sources
B	Usually reliable	2	Probably True
C	Fairly reliable	3	Possibly True
D	Not usually reliable	4	Doubtful
E	Unreliable	5	Improbable
F	Reliability cannot be judged	6	Truth cannot be judged

These are two examples of ratings of cyber information shared:

- *C4 which is translated to: fairly reliable source and doubtful information.*
- *A1 which is translated to: source completely reliable and information confirmed by other sources.*

Although the assessment is subjective, the rating provides a useful tool that supports the recipient of the cyber information in conducting their own assessment and analysis of the cyber information.

— — — — — — — —

Appendix E
Recommended Structure of a Formal Cyber Information Sharing Agreement

A formal cyber information sharing agreement should include the following sections:

- ✓ Preamble that includes the names and the description of the parties.
- ✓ Definitions and acronyms.
- ✓ Scope: describes the scope of the document and refers to Appendix 1 that covers the type of cyber information to be shared.
- ✓ Rights and obligations of the information receiver (recipient).
- ✓ Sources of information: who will provide what information to whom and based on what sources, and whether the source of the information is required to be shared.
- ✓ Limitations on what and with whom information can be shared, taking into consideration existing laws, intellectual property rights, commercial-in-confidence information, definition of TLP markings, etc.
- ✓ Format of information exchanged and frequency.
- ✓ Means of information transmission (such as letters, telephone, text messages, email, repository, etc.), including protection and assurance of confidentiality, integrity, and availability of digitally transmitted information.
- ✓ Quality requirements: describes actions to be performed by the sender before transmitting information. It also describes means to ensure the integrity and quality of information being shared, including for example its de-identification and/or sanitization.
- ✓ Storage and record keeping: describes archiving policies and procedures of shared information. It also describes the minimum time for which information sent/received should be archived for quality control purposes of the agreement and the relationship between parties.
- ✓ Cost: describes which party bears the cost of sharing information. It is recommended that each party bears its own cost related to the implementation of the agreement.
- ✓ Governance and change management procedures of the agreement.
- ✓ Correspondence and notices related to the agreement.
- ✓ Liability: where respective liabilities are described. It is recommended to indemnify the sending party from liability related to the shared information.
- ✓ Processing of personal data: describes how personal data is to be treated, including applicable laws and regulations.
- ✓ Dispute settlement: how and under which laws disputes related to the agreement will be addressed. It is recommended that parties try to resolve disputes amicably first, then if unsuccessful by mediation in an agreed upon jurisdiction.
- ✓ Entire agreement and amendments: where the precedence of the various parts of the agreement is described.
- ✓ Date for the agreement's entry into force, its duration, and procedures for its renewal and termination.
- ✓ Assignment: signatures of authorized individuals for each party.
- ✓ Appendices:
  - Appendix 1 - information to be provided: describes the type of information to be shared by each party.
  - Appendix 2: definition of TLP markings, including reference to the FIRST TLP standard.

— — — — — — — —

Appendix F
MISP - Open Source Threat Intelligence and Sharing Platform

MISP[14] is a platform for sharing, storing and correlating Indicators of Compromises (IoCs) of targeted cyber-attacks, as well as cyber threat intelligence such as threat actor information, financial fraud information, etc.

It is a free, open source cyber threat intelligence and sharing platform that allows organizations to create communities to share information such as cyber threat intelligence, indicators, threat actor information, or any kind of cyber threat which can be structured in MISP.

MISP users benefit from the collaborative knowledge about existing malware or cyber threats. MISP is used through the creation of "communities". The information sharing occurs within a user community. The aim of this trust-based platform is to help improve the counter-measures used against targeted cyber-attacks and the implementation of preventive actions and detection.

MISP, as well as any equivalent platform, is recommended to be considered by States and aviation stakeholders as a medium/method to share cyber information as the platform:

- helps automate the use of the information received to update various security systems, such as Security Information and Event Management/Security Operation Centers (SIEM/SOC), firewalls, antivirus software, and Intrusion Detection and Prevention System/Intrusion Prevention Systems (IDPS/IPS);
- allows to share cyber information rapidly as time might be a critical factor in case of sharing information related to an ongoing response to a cyber incident;
- allows the update of cyber information related to a cyber incident with additional related information as it becomes available; and
- all types of TLP marked information may be shared via MISP. However, information marked **TLP:RED** is shared on MISP only when the community is composed of a limited number of people who agree to share such information. Generally, **TLP:RED** information is not shared on MISP, but through alternative means (such as telephone, text messages and email communication).

— END —

[14] For further information on the use of MISP: https://www.circl.lu/services/misp-malware-information-sharing-platform/