Participation Handbook

Cyber Resilience Tabletop Exercise (TTX)

Exercise Overview

Cyber Resilience Tabletop Exercise is a useful tool to test existing air navigation cyber resilience and communication procedures.

Exercise Date: 09-12 October 2023
Location: Lima, Peru.
Hosted by: ICAO South American (SAM) Regional office
Point of Contact:

- *Sosa, Roberto, REGIONAL OFFICER, ATM/SAR OSG/SAM. rsosa@icao.int*

Facilitators:

- *Da Silva, Saulo, CHIEF, GLOBAL INTEROPERABLE SYSTEMS, ANB/AN/GIS. sdasilva@icao.int*
- *Kornetskiy, Anton, TECHNICAL OFFICER, GLOBAL INTEROPERABLE SYSTEMS, ANB/AN/GIS. AKornetskiy@icao.int*

Exercise Objectives:

1. Reduce confusion and streamline decision-making during air navigation cyber emergencies, enabling prompt and proactive actions by the personnel involved.
2. Develop awareness and promote a common understanding of air navigation systems cyber vulnerabilities, and resultant risks affecting operations.
3. Empower participants with measures to mitigate the exploitation of systems by identifying and promoting mechanisms for information sharing.
4. Introduce the International Aviation Trust Framework (IATF) and promote global benefits for the aviation Ecosystem by being part of the (IATF).
5. Provide actionable guidance on how to develop and run State/Organization tailored Tabletop Exercises.

Exercise Themes:

- **Expectations, skills & experience**
  - Role, responsibilities, authorities & interactions with others
- **Policies and procedures**
  - Current plans and procedures & significant inconsistencies, if any
- **Risks to the safety of flight operations**
  - Hazards, & vulnerabilities that could be impactful
- **Role of International Aviation Trust Framework.**

Preliminary Exercise Schedule

DAY 1 (9 OCTOBER 2023)		
Time	**Activity**	**Speaker/Moderator**
0800 - 0900	Registration	
0900 - 0930	Opening Session	ICAO RO
0930 – 1015	Introduction	ICAO HQ
1015 - 1045	*Group Photo & Coffee/Tea*	
1045 - 1115	The regional perspective and activities	ICAO RO
1115 - 1215	Setting the cyber scene	ICAO HQ
1215 - 1315	*Lunch*	
1315 - 1415	International Aviation Trust Framework (IATF) Facilitated discussion (part 1)	ICAO HQ
1415 - 1430	*Coffee/Tea Break*	
1430 - 1530	International Aviation Trust Framework (IATF) Facilitated discussion (part 2) + Q&A	ICAO HQ
DAY 2 (10 OCTOBER 2023)		
0900 – 0930	Summary of the previous day work	ICAO HQ
0930 - 1030	TTX exercise introduction	All
1030 - 1100	*Coffee/Tea Break*	
1100 - 1200	TTX exercise: Scenario 1	All
1200 - 1300	*Lunch*	
1300 - 1430	TTX exercise: Scenario 1 (to be cont'ed)	All
1430 - 1445	*Coffee/Tea Break*	
1445 - 1530	TTX exercise: Scenario 2	All
DAY 3 (11 OCTOBER 2023)		
0900 – 0930	Summary of the previous day work	ICAO HQ
0930 - 1030	TTX exercise: Scenario 2 (to be cont'ed)	All
1030 - 1100	*Coffee/Tea Break*	
1100 - 1200	TTX exercise: Scenario 3	All
1200 - 1300	*Lunch*	
1300 - 1400	TTX exercise: Scenario 3 (to be cont'ed)	All
1400 - 1430	*Coffee/Tea Break*	
1430 - 1530	Review of TTX, lessons learned and round-table Q&A	ICAO HQ
	DAY 4 (12 OCTOBER 2023)	
0900 – 0915	Summary of the previous day work	ICAO HQ
0915 - 1045	Fundamentals of Communication Strategy and Stakeholder Management Workshop	ICAO HQ
1045 - 1115	*Coffee/Tea Break*	
1115 - 1245	How to create and run State/Organization tailored Tabletop Exercise workshop	ICAO HQ
1245 - 1345	*Lunch*	
1345 - 1430	Workshop summary and wrap-ups	ICAO

Terms and Definitions

The terms and definitions herein are specific to this exercise and may differ from those presented in other ICAO documents. They are purely to clarify the terms in the context of these exercises.

Aviation-related:

- ***Aviation Domain V. Aviation Ecosystem***
    - **Aviation Domain:** The global airspace, including domestic, and international, as well as all manned and unmanned aircraft operating in that airspace, people and cargo present in that airspace, and all aviation-related infrastructures.
    - **Aviation Ecosystem**: A multi-layered network of intersecting elements with integral roles in the Aviation Domain and involves six primary entities: Airports, Airlines, Airlift, Aircraft, Actors, and Aviation Management.
- **Other Aviation Terms and Definitions**
    - **ANSP**: Used generically for all air navigation service providers
    - **Airline**: Used generically for all flagged air carriers (passengers, cargo)
    - **AIRAC**: Aeronautical Information Regulation and Control synchronization process
- **Communications Networks**: Responsible for the circuits, networks, and equipment supporting voice and data (email, surveillance, flight plans, etc.)
- **Drone pilot license:** A certificate that drone pilots must carry at all times while operating their drone.
- **Executive Stakeholders**: Senior leadership responsible for making policy, "non-routine" decisions.
- **International Aviation Trust Framework (IATF):** A set of policies, requirements and best practices that will enable trusted, resilient and secured ground-ground, air-ground, and air-air exchange of digital information among all current and prospective aviation stakeholders.
- **Operations Stakeholders**: Provide air traffic services and air traffic flow, responsible for making "routine" decisions based on existing policy and procedures.
- **Remote drone ID:** The ability of a drone in flight to provide identification and location information that can be received by other parties through a broadcast signal or a network-based system.
- **Remote pilot:** A person charged by the operator with duties essential to the operation of a remotely piloted aircraft and who manipulates the flight controls, as appropriate, during flight time.
- **State of Registry:** The State on whose register the aircraft is entered.
    - All unmanned aircraft (UA) should be registered according to part 101 of ICAO Model UAS Regulations.
- **Unmanned aircraft system (UAS)**: An aircraft and its associated elements which are operated with no pilot on board.
    - *Discussion will feature a small drone (251 g -25 kg) equipped with a professional digital single-lens reflex (DSLR) quality camera

Cyber-related

- **Cyber Hygiene:** Practices and steps to maintain computer and device system health and improve online security.
- **Cyber threat:** A potential negative action or event facilitated by a vulnerability that could result in an unwanted impact on a computer system or application.

- **Distributed Denial of Service:** A denial of service technique that uses numerous systems simultaneously to impair the authorized use of information system resources or services, typically by flooding the network with packets of huge amounts of data.
- **Event:** An observable occurrence in a system or network (e.g. a user sending email).
- **Incident:** An adverse event in an information system or network, or the threat of such an event.
- **Incident Response Plan:** A series of pre-planned actions that includes the processes, procedures, and documentation related to how your organization detects, responds to, and recovers from incidents.
- **Malware:** Software that compromises the operation of a system by performing an unauthorized function or process.
- **Phishing**: A digital form of social engineering to deceive individuals into providing sensitive information.
- **Resilience:** Capacity to maintain the system's ability to deliver the intended outcome continuously at all times, even when regular delivery mechanisms have failed.
  Spoofing: Faking the sending address of a transmission to gain illegal [unauthorized] entry into a system; the deliberate inducement of a user or resource to take incorrect action. Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing.
- **Zero trust:** Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

Participant's roles and responsibilities

The term participant encompasses many groups of people, not just those playing in the exercise. At a minimum, a Moderator and Players are required. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Moderator**: Directs the overall flow during the conduct of the exercise.
- **Subject Matter Experts (SME):** As requested, assist by providing relevant information, analysis, and recommendation in their area of expertise or providing subject matter expertise.
- **Players:** Active in discussing or performing their regular roles and responsibilities during the exercise.
- **Recorders**: Monitor the overall flow of exercise & help document actions and decisions, in support of post-exercise information/documents.
- **Observers:** Observe the overall flow of the exercise in a manner that does not directly affect its conduct.

Exercise structure

1. **IATF Facilitated discussion** scenario will be based on the safety of UAS operations internationally and domestically. The intent of this discussion is to highlight global benefits for the aviation ecosystem by being part of an International Aviation Trust Framework**.**

    - Players are encouraged to actively interact in accordance with their real-world actions, responsibilities, policy, and expertise.

2. **The Cyber Resilience TTX scenario** will be based on the **Flight Plan Management process** and presented in three parts (3 scenarios plus several injects). The intent of these injects is to highlight the interconnectedness of cyber systems with physical infrastructure and to exercise coordination

and communication between stakeholders. Following each part, players will have a set time to review the module and debate the discussion questions. **Cyber Resilience TTX scenario** has three major adversarial objectives:

- To disrupt specifically targeted systems through cyber events (critical or otherwise)
- To compromise systems for financial gain
- To undermine public confidence in air travel

- The moderators will present the situation and players will engage in a discussion of appropriate response actions and issues that arise from the scenario at hand.
- Participants may form teams to facilitate discussions.
- The situation will have a number of injected parameters throughout the narrative. The goal of the injections is to change one or more variables in the presented situation or to advance the story.
- The scenario will conclude when the storyline is finished or when the objectives of the situation have been met.
- The next situation will then be introduced (as applicable). Subsequent situations may build upon previous situations or may be completely unrelated.

3. **Fundamentals of Communication Strategy and Stakeholder Management Workshop.**

   - The moderators will utilize scenarios previously discussed during the TTX, along with various project management tools, to provide participants with practical guidance in developing a tailored communication strategy as part of their incident response plan.
   - Players will be engaged in group activities.
   - Players are encouraged to respond to the scenario using their awareness of current communication plans, strategies, and knowledge received during the TTX

4. The **'How to Create and Run a State/Organization-Tailored Tabletop Exercise Workshop'** will assist ICAO Member States and other aviation ecosystem stakeholders in creating and conducting exercises to assess their ability to plan for, respond to, and recover from cyber incidents.

   - This workshop equips participants with measures to prevent the exploitation of critical air Navigation systems, enhances awareness of cyber issues in aviation, and promotes the secure and resilient use of cyberspace.
   - The moderators will present a set of best practices and examples to provide players with a solid roadmap for initiating, planning, designing, conducting, evaluating, and improving TTXs.

Important Remarks

Players have no advanced knowledge of the scenarios and will receive all information at the same time. Although based on a plausible scenario, this TTX is not intended to replicate a real attack or simulate a full response; the goal is to examine and debate incident coordination and communications issues rather than determine a “best” response.

Although general terms are used in the scenario, players should emerge themselves in the exercise as if this is happening in their region and in their airspace. Players should always note that the scenario

presented is fictitious and any names mentioned are only used for context or as examples. Players should also note that the scenarios presented are based on certain assumptions that might be different from their own State or region. If this is the case, please feel free to point out the differences and discuss them.

This exercise will be held in an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected and even encouraged.

During all activities:

- Respond to the scenario using your own knowledge of current plans, policies, and capabilities (i.e., you may use only existing assets) and insights. No other resources are required for players to actively participate in the TTX.
- Actively use the **Slido.com** tool when prompted by moderators to provide your answers/ideas.
- Think outside the box. There is no right or wrong answer. Players are strongly encouraged to participate in in-depth discussions, as the primary purpose of the exercise is to exchange knowledge and share experiences between players.
- Discuss and present multiple options and possible solutions. Decisions are not precedent-setting and may not reflect your final position on a given issue.
- Identify issues but also suggest and recommend actions that could improve cyber efforts. Problem-solving efforts should be the focus.

There should not be the dissemination of exercise materials or discussion; *communication should remain in-room*. The outcomes of the discussion will be distributed to all participants and observers and may be freely shared. No State, organization, or person will be directly attributed to the discussion outcomes.