INTERPOL

PROJECT **STADIA**

Safe & Secure Major Events

STADIA PROTECTION AND MITIGATION FROM DRONE INCURSION AND THREATS

Case Study FIFA World Cup Qatar 2022

October 2023

Legal Disclaimer

This document (the "Guidelines") aims to provide actionable guidelines, insights and recommendations to INTERPOL Member Countries on the topic of developing Counter Unmanned Aerial Systems (C-UAS) processes, protocols, and testing for the protection of an asset, event, or public space in the context of criminal activities. The content draws upon the contributions provided by a select group of experts and organizations, as well as the FIFA World Cup Qatar 2022™ Red Teaming Operation, facilitated by the INTERPOL Project Stadia, INTERPOL Innovation Centre, and the Qatar Ministry of Interior. These Guidelines aim to support security practitioners, first responders and police officers by covering the identification of preparatory requirements, the development of operational procedures, and the design of an adversarial testing and evaluation framework to determine the effectiveness of defenses and reactions to threat capabilities.

These Guidelines are provided for the reference and knowledge of concerned authorities to illustrate the minimum requirements to prepare, test and defend an asset, event or public space from malicious threat actors, which relevant authorities can adapt and customize to comply with applicable legal requirements and meet the character and format of their national circumstances. These must be adopted at the discretion of the reader, with appropriate and adequate legal advice specific to his/her jurisdiction. Certain activities such as the adoption and implementation of flight permissions and parameters, no fly zones, threat modelling, ISR, if sought to be undertaken, may include the need for specific procedural steps to be taken, or legal bases under applicable laws. In case of any uncertainty, the reader's recourse is to consult the relevant law enforcement, legal and judicial authorities in his/her jurisdiction. INTERPOL does not and cannot provide legal basis for undertaking any of the actions mentioned herein. INTERPOL shall not be liable for any actions taken or omitted by any reader on the basis of the content of these Guidelines.

The legal, procedural and customary frameworks in respect to Unmanned Aerial Systems, Unmanned Vehicles System and Counter-Unmanned Aerial System differ widely by jurisdiction. These Guidelines do not provide any recommendations, advice or instructions in respect of requirements under such legal and procedural frameworks in any jurisdiction and any references seemingly suggesting as such should be read as being subject to domestic laws and procedures in this regard. Readers are advised to ensure, when taking any actions based on these Guidelines, to verify and be satisfied that such actions are in compliance with appropriate legal and procedural requirements or standards in their jurisdictions.

The content of these Guidelines may not constitute a complete overview of legislative resources. Readers are advised to contact competent national authorities if they require any further information regarding the applicable legal framework and relevant requirements. In addition, these Guidelines do not constitute legal or other professional advice or an opinion of any kind. These Guidelines are not mandatory in nature and have no enforceability. INTERPOL shall not be liable for any actions taken by any parties based on these Guidelines which is contrary to or inconsistent with or not in compliance with any relevant legal, regulatory, administrative, procedural, evidentiary, customary, or other requirements.

In relation to the Guidelines references to INTERPOL's support activities, in the execution of its mandate, INTERPOL is guided by four main principles enshrined in its Constitution: national sovereignty, respect for human rights, neutrality and constantly active cooperation. The Constitution (Article 3) explicitly forbids INTERPOL to undertake any intervention or activities of a political, military, religious or racial character. The national law enforcement authorities remain exclusive holders of executive and investigative powers for police activities.

All reasonable precautions have been taken by INTERPOL to verify the information contained in this document. However, the material is distributed without warranty of any kind, either express or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall INTERPOL be liable for damages arising from its use. INTERPOL takes no responsibility for the continued accuracy of the information contained herein or for the content of any external website referenced. No mention of commercial products, processes, or services in this report shall be construed as an endorsement or recommendation. Any reference to third party names is for appropriate acknowledgement of their ownership and does not constitute a sponsorship or endorsement of such owner.

The content of these Guidelines does not necessarily reflect the views or policies of INTERPOL, its Member Countries, its governing bodies, or contributory organizations, nor does it imply any endorsement.

INTERPOL General Secretariat
200, quai Charles de Gaulle`
69006 Lyon (France)
Telephone + 33 4 72 44 70 00 - Fax + 33 4 72 44 71 63

Table of Contents

Abbreviations: C-UAS Terminology

Terminology diversity within the C-UAS domain can cause issues with cross border communications; as such, our goal is to support standardised terminology. Below is a list of the more commonly encountered acronyms and terms within the C-UAS domain, which can be used within your own organization's documentation. By standardising terminology, we can improve knowledge exchange and international communications. These terms have been cross-referenced with international documentation with the aim of presenting standard terminology to member countries.

ABBREVIATION	DEFINITION
Adversarial testing	Known commonly as Red Teaming or Red/Blue Teaming. A war gaming scenario where one team (Red) acts as the attacker and the other team (Blue) the defender.
AGL	Above Ground Level
ANSP	Air Navigation Service Providers
APOC	Airport Operations Centre
ATC	Air Traffic Control
ATIS	Automatic Terminal Information
ATM	Air Traffic Management
ATS	Air Traffic Services
Attack vector	An attack vector is the single drone flight which is planned and flown by a Red Team drone operator in an adversarial testing scenario, also known as Red Teaming or Red/Blue Teaming
BVLOS	Beyond Visual Line of Sight
C2	Command and Control
CAA	Civil Aviation Agency/Authority
CBR	Chemical, Biological, and Radiological
CCOC	Command and Control Operations Centre
CID	Criminal Investigation Department (Forensic Recovery)
CNPC	Control and Non-Payload Communication
CONOPS	Concept of Operations
C-UAS	Counter Unmanned Aerial Systems
COTS	Commercial off-the-shelf
DJI	Da-Jiang Innovations
FIFA	Federation Internationale de Football Association
FOP	Forward Operating Procedure
ft	Feet

ABBREVIATION	DEFINITION
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMS	Electromagnetic System
GCS	Ground Control Station
GHz	Gigahertz
GPS	Global Positioning System
IED	Improvised Explosive Device
IOT	Internet of Things
ISR	Intelligence, Surveillance and Reconnaissance
kmph	kilometres per hour
LE	Law Enforcement
LEA(s)	Law Enforcement Agencies
NCC	National Control Centre
NFZ	No Fly Zone
NOTAMs	Notices to Air Missions
P2P	Peer to Peer
RAG	Red, Amber, Green
RF	Radio Frequency
RoE	Rules of Engagement
RSF	Responding Security Forces
RTH	Return To Home
SAR	Search and Rescue
SecOps	Security Operating Procedure
SOP	Standard Operating Procedure
TCC	Tournament Control Centre
TSCM	Technical Security Counter Measure
UAS	Unmanned Aerial Systems
UAS Technology Detection	Technological countermeasure detection of a UAS/UAV launching, landing, or flying.
UAV	Unmanned Aerial Vehicles
VLOS	Visual Line of Sight
VOC	Venue Operations Centre
WiFi	Wireless Fidelity
THIRA	Threat and Hazard Identification and Risk Assessment

1.Case Study: FIFA World Cup Qatar 2022

Below is a case study highlighting the elements of these Guidelines in practice, considering the numerous and varied avenues of threat mitigation, which can be applied to Stadia depending on the location and situational parameters.

This case study shows how procedures and protocols outlined for protection of stadia for the FIFA World Cup were tested during the World Cup Red Teaming Operation.

1.1 Introduction

An INTERPOL UAV Task Force in 2022 held a Red vs. Blue Teaming event delivered by INTERPOL in Doha, Qatar, for the UAS/C-UAS units of the Security and Safety Operations Committee (SSOC) for the FIFA World Cup 2022. INTERPOL undertook this exercise after receiving an official request from the Ministry of Interior (MOI), Qatar.

INTERPOL Project Stadia and INTERPOL Innovation Centre (IC) representatives were present with four external experts to provide C-UAS testing capability and expertise to implement Red Teaming and develop scenario building for further security exercise.

The Ministry of Interior (MOI) and their supporting team acted as the Blue Team. INTERPOL, external experts, and a selection of MOI drone pilots acted as the Red Team. INTERPOL and experts from the Red Team were also located in the Venue Operations Centre (VOC) during testing to observe Blue Team protocols, which aided in developing a cohesive picture of action and response mechanisms from both teams.

1.2 Operation Objectives & Requirements

The INTERPOL team discussed the scope of the operation with the stakeholders and that lead to defining the objectives and requirements that the operation needed to achieve. These are stated below.

1.2.1 Scope

Identify any gaps in C-UAS strategy and operations to ensure that mitigation measures can be put in place by Qatar and that Standard Operating Procedures (SOPs) can be modified accordingly. The Red Team's key focus will be on assessing the Blue Team operators' response capacity on the ground and in the VOC through the development of targeted penetration testing exercises.

1.2.2 Objectives

- Test the C-UAS operators' response to drones entering a protected stadium's vicinity, including assessment of neutralisation techniques and adequacy of Standard Operating Procedure (SOP).
- Test the detection, tracking, and identification capability of the C-UAS system and how this aids the response teams.
- Provide feedback on the command, control, and coordination processes when a drone enters a protected airspace.

1.2.3 Requirements

- Ensure a Peer-to-Peer (P2P) format allowing for full knowledge transfer.
- Allow a Red Team member into the Venue Operations Centre (VOC) during testing to observe Blue Team protocols to aid in developing a cohesive picture of action and response mechanisms from both teams.
- Design Red Team operations, which provide both confidence and training as well as fully testing response capacity.
- Qatar local drone pilots to work with experts to provide local context and insights into existing capacity.

1.2.4 Stakeholders and other requirements

Before the INTERPOL Team arrived in Qatar, their processes described in the guidelines were designed, as such, and where appropriate, these documents were shared with the Red Team. Sharing this information is valuable for the Red Team to understand what the status of processes and protocols is as these aids in planning how to breach these elements. In addition, the procedures, which have safety elements, are very important for the Red Team when developing their attack operations to ensure they remain within suitable parameters.

1.3 Red team Objectives & Assessment

The INTERPOL team discussed the scope of the operation with the stakeholders and that lead to defining the objectives and requirements that the operation needed to achieve. These are stated below.

1.3.1 Red Team Assessment

Red Team penetration tests should be shaped to offer cohesive responses to critical areas of question. As an example, the general objectives within these questions below would contribute to shaping the targeted operational Red Team objectives for planning attack vectors for the Red Team when developing their attack operations to ensure they remain within suitable parameters.

- **Drone Countermeasure System:** does the installed C-UAS system effectively detect, track and identify the drones employed by the Red Team during penetration testing? If so, at what distance from the stadium and where (if appropriate) are drones detected, tracked, and identified (DTI)?
- **Effective Use of Neutralisation:** when neutralisation was applied, did it prevent the drone from entering the protected airspace when engaged? What techniques were employed by the response team to remove the drone from the protected airspace?
- **Response to Drone Incursions:** how did the drone incursion teams/operators respond to drones? Did they engage with a drone? How far away from the stadium was the drone sighted, identified, and mitigated?
- **Command and Coordination:** how effective was command and coordination between the ground teams and the VOC? Were there any areas of improvement that can be suggested? Were response protocols adhered to, and if so, how long did it take to notify and seek approval from the VOC for incursion response (this was out of scope of the original request but due to the valuable insights that Red Team could provide this was included within the exercise)?

1.3.2 Targeted objectives of the Red Team

Below is an example of the targeted objectives, which were used by the Red Team for testing the Blue Team:

- Understanding of operator effector, operator spotter, or operator VOC roles.
- Understanding Unmanned Aerial Systems (UAS) threat vectors and possible threats to World Cup events and facilities.
- Identification of UAS, the airframes, modifications, and flight behaviour in order to provide observations, judgments, and potential risks, and communicate contact when drones were sighted with the assessment of risk.
- Communication between VOC and other response teams of contact with UAS with designation, position, and trajectory under the issued SOPs.
- Understanding of the SOPs, Rules of Engagement (RoE), and Concept of Operations (ConOps) issued by the MOI.
- Employment of the effector technology and ability to seek required authorizations.
- Capacity to risk assess necessity, proportionality, and collateral impact when using an effector.

The Red Team carried out Intelligence, Surveillance & Reconnaissance (ISR) on a selection of sites including stadiums, which would be used for hosting matches, and areas where large crowds of spectators would be present. This process took 1.5 days, when viewing three stadiums and two spectator sites.

With all the information gathered within the field, the Red Team designed a number of operation parameters and attack vectors. This process for this case, in total took two days, yet with further sites, would take longer, and the Red Team was operating under tight deadlines working irregular hours.

1.4 Red Team Operation Parameters

1.4.1 General parameters

There are different levels of operational parameters, below are the general parameters for the penetration test:

- During the tests, drones can only operate on a predefined range of frequencies.
- Only safe drones with a Return to Home (RTH) function are to be operated during the tests unless otherwise specified.
- Different attack vectors should be used to ensure that the drone response teams' engagement criteria are tested from drone pop-ups, short, mid, and long-range attack vectors are utilized to ensure variety in threat modelling.
- The sites that will be subjected to Red/Blue Teaming to be selected, and clear parameters for the testing and type of testing to be agreed upon prior to the execution of the operations.
- The exercise should test the drone response while instilling confidence building within the Blue Team.
- No encroachment of national infrastructure, sensitive areas, or transit of UAVs across residential areas.

1.4.2 Targeted flight Parameters

More targeted parameters were defined by the Red Team and approved by the Qatar Civil Aviation Authority.

- Hardtop altitude was set within provided flight plan volumes at 250 meters.
- All pilots are to remain within approved and authorized volumes.
- All pilots are to fly on TX/RX 2.4 GHz only.
- All pilots are to have a clear path for Return to Home (RTH) after effecting by jammers.
- All observers are to remain in radio contact with VOC.
- All reports of air proximity are to be reported to VOC.

The Red Team also followed general Civil Aviation Authority (CAA) drone rules where applicable:

- Not to fly higher than 120m / 400 feet unless authorized by the CAA to do so (see above list).

- Always keep the drone in Visual Line of Sight (VLOS).
- Keep clear of airspace restrictions, including around aerodromes, unless granted permission by the CAA to do so (see above list).
- Keep 50 meters away from uninvolved people to avoid endangering them.
- In most cases, unless flying a drone that is less than 250 grams, you must keep at least 150 meters distance horizontally away from parks, industrial, residential, and built-up areas.

The Red Team faced a lot of limitations and a lack of baseline data sets to work against during this pre-cursor exercise. Notably, the Blue Team could not provide Red Amber Green (RAG) maps or zones with allocated SOPs, which would have assisted the Red Team in localizing areas actioned for neutralisation.

1.5 Daily Brief & De-Brief

Reconnaissance , mission planning, penetration testing, analysis, stakeholder meetings, and report preparation should be planned prior to the exercise.
It is good practice to follow detailed focus areas, daily overviews, and remarks/lessons learned at the end of each day of the exercise. Below is an example of one day from the Red Team planning; it can be extrapolated as required.

1.5.1 Example - Remarks Template

<table>
<tr><th colspan="2">Day 1 – Introduction to Red/Blue Team Penetration Tests and Required Criteria. Recon Location</th></tr>
<tr><td>Key Focus Areas</td><td>• Overview of Red/Blue Team penetration testing
• Criteria of penetration tests and requirements of flight operations
• Identification of stadiums to be tested
• Assessment and application for drone flights approval
• Types of testing to be employed
• Scope and limitations of operations</td></tr>
<tr><td colspan="2">Helps establishing the rules of engagement (RoE), and what could/not be utilised during the tests through stakeholder discussion and reconnaissance activities. For example, the Red Team can only use drones with an RTH function for intrusion testing. In addition, if drones function unsafely, such as crashing to the ground, causing collateral damage, or gaining altitude, they cannot be employed within the scope of the exercise.</td></tr>
<tr><td>Remarks</td><td>• It is crucial for the Blue and Red teams to establish RoE and set the test parameters so that each party is aware of the scope and limitations of the exercise.
• Any areas of doubt should be discussed and resolved in compliance with the needs of both Blue and Red teams, i.e., the use of drones on set frequencies with the capability to RTH.</td></tr>
</table>

Remarks	• Any test that needs to take place that requires applications for permissions to fly etc. should be requested at the earliest possible to avoid delays and misinterpretation. • It is the responsibility of both the Red and Blue teams to ensure safety and understand the scope of the penetration testing. • Once areas have been selected for testing, access should be granted to the Red Team to conduct recon in and around the test site to identify potential vectors of attack and hazards or obstacles they may face during the tests, i.e., a stadium's location in or near a no-fly zone (NFZ) or critical infrastructure. • Any mechanisms in place for protection from drone incursions, such as NFZs, existing detection, mitigation sensors, or techniques that may jeopardise the tests, should be clarified at the earliest opportunity.

1.6 Intelligence, Surveillance and Reconnaissance (ISR)

The INTERPOL Red Team experts performed Intelligence, Surveillance and Reconnaissance (ISR) over two days at three stadium locations and one non-stadium location. Each site was assessed for potential threats, likelihood of the threat occurring, determining if/what C-UAS systems can be used, potential hiding or escape routes for offenders, drone platforms, which would suit the threat and determine the most appropriate threat scenarios for the environment.

Based on the reconnaissance performed, recommendations were made to complete the flight planning, scenario planning, and deciding the volume of flight operations for each location. This enabled the Red Team to brief all relevant participants from the SSOC, request the correct flight permissions from the Qatar Civil Aviation body, and prepare the right equipment for the Red Team testing operation.

1.7 Scenario Development

To ensure that the drone response teams, and the Blue Team command and control capabilities are tested according to their Standard Operating Procedures (SOPs), the Red Team devised scenarios that could be deployed during the Red/Blue Teaming. These scenarios were created from incidents of drones entering the vicinity of the facility or protected area that have recently occurred across the globe. The Red Team consulted local drone pilots and others from incidents that had occurred at other major events worldwide. These scenarios were created to reflect the different drone threats they may face and the different types of drones and flight patterns they may encounter. The scenarios were presented to the MOI and discussed, some scenarios de-scoped and the final scenarios for operation chosen.

1.7.1 Scenario Template

A scenario template is available below as an example:

Scenario 1: Summary	
User Story	Summary description of the drone actor's intention, role and aim. Contextual information surrounding the drone action: time, place of events, starting place of the launch and flying zone of the drone. Description of the drone action: filming, dropping payload, circling in the air etc.
Value Use of Drone	Describes in more details the reasons why the drone is being flown, what the pilot will gain from it: terrorist intent, curiosity, financial gain, leisure etc.
Parameters of Exercise	The drone used has a flight time of 25 minutes due to being an off-the-shelf drone. The pilot is experienced/not experienced at flying the drone.
Scenario Parameters	• Location: harbour, concert hall, stadium, fan zones. • Time of Day: day time / night time / good lighting conditions / bad lighting conditions • Drone Type • Threat Actor: careless / nuisance / espionage / protester / terrorist / ignorant to risk posed • Drone Flight Type: erratic/ point of interest
Key Points of Scenario	Drone detection, location, neutralisation, capture. Type of neutralisation: inside or outside location. Neutralisation inside location with minimal collateral intrusion and risk to people or infrastructure due to secondary incendiary ignitions.
Success Criteria	Drone Detected: Y or N Drone Observed: Y or N If Y at what distance and the time detected from drone switch on (threat lifetime) Drone Disrupted: Y or N (loss of link) Pilot Located: Y or N Drone Tracked and/or Recovered: Y or N

1.8 Red Team Attack Vector Planning

After performing reconnaissance and providing varied and different threat scenarios, the Red Team must start planning the scenarios (attack vectors) that would be flown during the operation so that all required authorisations and permissions to fly are approved.

1.8.1 Flight plan template

Pilot No.	Call sign	UAV Equipment	Location
1	Mars	Drone Model and Name	Military base (near)
2	Jupiter	Drone Model and Name	Border (1 km)
3	Saturn	Drone Model and Name	Harbour
4	Mercury	Drone Model and Name	Beach
5	Venus	Drone Model and Name	Civilian Complex 1
6	Pluto	Drone Model and Name	Civilian Complex 2

1.8.2 Flight timestamp and actions template

Timestamp	Pilot 1 Action	Pilot 2 Action	Pilot 3 Action	Pilot 4 Action	Pilot 5 Action
14:30	0ft Drone 1 leaves in Starting Point to Place 1				
15:30 (TO)	(TO) Pop Up to 100 Ft with Drone 2 for two minutes				
15:33 T+3		(TO) Pop Up to 100 Ft with Drone 3 for two minutes			
15:36 T+6			(TO) Pop Up to 100 Ft with Drone 4 for two minutes	(TO) Pop Up to 100 Ft with Drone 5 for two minutes	
	LAND T+2	LAND T+5	LAND T+8	LAND T+8	N/A

1.8.3 Detailed Pilot actions template

Timestamp	Pilot 1 Action
16:30 (TO)	(TO) Take Off from Starting Point with Drone 1
16.33 T+3	Wide 1km rotation of Location 3
16:36 T+6	Wide 0.5km rotation of Location 3
16:39 T+9	Fly over of Location 3 from West to East
16:42 T+12	Low level flyby of 40 ft: all units' eyes on
16:45 T+15	LAND - Landing in End Point for recovery

1.9 Exercise Overview

After reconnaissance, flight planning, internal briefings to the Blue Team and external briefings to the hosts, locations that are going to be used for the exercise are decided upon.

Locations are selected according to various factors, such as: risk assessment, scale of potential damage, size of threat, and diversity of geography. For example, seating capacity, whether the location is enclosed or in the open air, whether the location is strategic, density of the area and how many people would be affected by a drone accident, are factors to be considered in the choice of locations to be tested.

1.9.1 Exercise 1

1.9.1.1 SOP Testing

More targeted parameters were defined by the Red Team and approved by the Qatar Civil Aviation Authority.

(i) Administrative
(ii) Equipment
(iii) Active Operation
(iv) Supplementary
(v) Assurance

The Red Team will test SOPs. Tests will be conducted to ensure compliance of the required actions within each role of the C-UAS chain of command.

1.9.1.2 Testing Health and Safety & Collateral damage

Personnel using radars and Radio Frequency (RF) signals from transmitters (RF Effectors) must exercise caution when operating this equipment as it projects high output power, potentially resulting in RF burns if exposed directly. It is strictly prohibited for the equipment to be pointed in the direction of anyone.

In addition, all operators **MUST** be aware of the possibility of disruption and collateral damage, as defined in the RoE.

1.9.1.3 Testing Whitelisting and Blacklisting of Unmanned Aerial Systems

Depending on the location of the pen test, all UAS being operated will be required to have a form of identification, which can be gained from one or a combination of:

a) Serial Number
b) Media Access Control (MAC) Address
c) Remote ID Number

These are pre-requisites for the import of UAS into the country and will ensure that the UAS will not be considered rogue. UAS can be registered with the Anti-Drone System(s) in three ways. These are:

a) UAS manufactured by Da-Jiang Innovations (DJI)
b) UAS manufactured by DJI and certain other manufacturers
c) All other categories of UAS – Transponder

1.9.1.4 Testing of Command Structure of Counter UAS System

The chain of command for the Anti-Drone System will vary between Type A venues and Type B venues and will also vary during working and non-working hours.

Level 1 resource model for type A:

- Venue Operations Centre Commander,
- National Command Centre (NCC)/Tournament Command Centre (TCC) Operator within VOC – NCC,
- (Info only) National Command and Control Operations Centre (standard model).

1.9.1.5 Testing of Alert State

There are different alert states pertaining to the readiness of an Anti-Drone System, which is in effect during a major event: Monitor State, Enhanced State and Detect & Respond State.

One of the states that can be tested is the "Detect and Respond State", which refers to an event or situation whereby an unidentified or unauthorized UAS is detected and threatens significant disruption to the major event operations and/or which could have a major negative impact on the reputation of the organisers of the major event.

1.9.1.6 Testing of Threat Levels

In addition to the three mentioned states, the threat levels will determine which Alert State posture will be adopted and the factors determining the different categorizations.

RAGs are a set of 'traffic light' security protocols on how to engage a threat and when it is deemed a threat. RAGs are also important for planning the Red Team Operation. RAG levels example:

- **Green** (no impact - monitor) – An issue that occurs outside routine activity yet does not disrupt operations.
- **Amber** (enhanced state) – An issue that causes or could cause disruption. Neutralisation by C-UAS technology or other methods is probable.
- **Red** (detect and respond) – A major issue or incident causing an emergency or major disruption. Neutralisation by C-UAS technology or other methods have failed and evacuations or other public safety measures are to be activated.

1.9.1.7 Testing of Standard Operating Procedures – Actions Required

The following is the response for Type A venue, which is predominantly based on the venue criticality and the type of Anti-Drone System deployed.

Type A Venue:

The National Counter Drone Operator:

- Detect, Track, and Identify (DTI) any UAS that activate on the display.
- Immediately report detection to Technical Officer.
- Determine if UAV is carrying a payload.
- Provide constant updates on the speed, trajectory, and distance of UAV.
- Report the location of GCS (Ground Control Station), (if identified) to the Technical Officer.
- Follow instructions of Technical Officer for Effector instructions.
- Provide regular situation reports (SitRep) and communication with Technical Officer.

The National Mobile Effector Personnel:

- Respond to any unidentified/unauthorized UAS as instructed by the Counter Drone Operator.
- Track UAV with handheld effector(s).
- Activate when instructed.

The Technical Officer:

- Regularly update C-UAS Mobile Effector Personnel of any circumstances that may affect decisions of response.
- Responsible for all decisions when Drone in Detect zone and authorize the use of effector in accordance with the Rules of Engagement.
- Authorize the deployment of a Drone Hunter if necessary.
- Request the deployment of security forces to respond to any notification of a GCS and deployment of the Response/Recovery Team if a UAV is downed from the VOC Commander.
- Liaise between Counter Drone Operator and VOC Commander.

The NCC/TCC Operator (within VOC):

- Provide communications between VOC Commander and NCC/TCC.
- Provide communications between Technical Officer and NCC/TCC.

The VOC Commander:

- Authorize the use of an effector in accordance with the Rules of Engagement.
- Inform NCC/TCC through the NCC/TCC Operator of the situation.
- Authorize deployment of any services needed (ISR, Response Team).
- Respond to any briefing requests from NCC/TCC.

The NCC/TCC National Commander :

- Provide advice and guidance to Tournament Silver Commander (if appropriate).
- If the scale and complexity of the incident are such that some degree of central coordination is required, the Tournament Silver Commander will initiate.
- Compile SitRep.

1.9.2 Exercise 2

1.9.2.1 Testing of SOP Command Structure of Anti-Drone System

The chain of command for the Anti-Drone System will vary between Type A venues and Type B venues and in addition, will also vary during working and non-working hours.

Red Team Test State will be:

a) Green – Pop-ups that do NOT disrupt operations,
b) Amber – Pop-ups that COULD CAUSE disruption or impact service levels,
c) Red - Incursion into restricted areas that poses a threat to service levels.

RAG Threat Levels

GREEN (no impact) Monitor State	An issue that occurs outside of routine activity, but that does NOT disrupt the operations of the Championships/event delivery at the venue or FA level. Eg. Intelligence repots unidentified/unauthorised UAS activity.
AMBER Enhanced State	An issue that causes (or could cause) disruption to Championships operations and/or event delivery at the venue or FA level. Includes issues which have an impact on service levels to Client Groups or affects operations of other FAs and/or Partners Eg. Unidentified/Unauthorised UAS entering restricted airspace around venue and is detected and neutralised.
RED Detect & Respond State	Major issue or incident including an emergency causing (or could cause) disruption to wider Championships operations and/or event delivery (ie. multiple FAs or venues affected) and/or major impact on delivery of partners' operations and/or client group service provision. Eg. Cancellation of a session/training session; Partial evacuation of stadium; Failure of a supplier due to unidentified/unauthorised UAS activity.

Example of results of Response Teams to Drone Sorties

- UAS were affected within / outside of engagement zones
- UAS were engaged by one team / multiple teams
- UAS were not affected while in RTH / UAS were continually affected while in RTH and the possible negative impact this could lead to:
    - proximity alerts to critical national infrastructure, vehicles, and ground operations
    - collateral infringement of private spectrum use (WiFi, IoT, Connected Homes)
    - risk to property and life and risk to connected infrastructure

1.10 Conclusions and High-Level Recommendations

1.10.1 Conclusions

The use of Red/Blue Teaming to validate the response plans of a member country to drone incursions at stadiums is a very valuable tool for all teams and stakeholders.

The Red Team gains insights into the different strategies law enforcement may face when protecting a facility and how challenging this can be. The Blue Team gains operational experience in responding to unknown drone threats and can test their response, command and communication, and the strategic decisions required to combat unknown drone threats.

The teams that help build and train the response teams witness how using a neutral party to create controlled drone incursions based on parameters set out and understood by all, helps create confidence and collaboration within the drone response teams. Using an outside Red Team also ensures a fresh outlook on the drone threat dynamics and that the Blue Team is challenged by the different attack vectors employed during the sorties.

1.10.2 High level recommendations

(COULD/SHOULD) - Operations handbook – a short, concise handbook that could be distributed to the Red Team detailing the scenarios to be played, timeframes, equipment, teams, locations, etc., and a common vocabulary to use during operations and across the radio communications.

(COULD/SHOULD) Extend Red Teaming to Ports, Entry borders & Stadium entry ports, including the use of deployed Open-Source Intelligence using the Red Team Persona, the authorised attempt to import a drone, the authorised attempt to gain entry to stadiums and facilities with drones, and the testing of tip lines using Pop-Ups at Type B locations.

(WOULD) Allocate more time to learning needs analysis, skills and competence development, development of intelligence and investigation continuity in the C-UAS workflow, and refine policy, procedure, and interoperability across host nation departments.

1.10.3 Additional Recommendations

By monitoring the command and coordination process within the VOC, the Red Team is able to observe and make some recommendations on how the response protocols could be improved and streamlined to better react to a drone threat.

Some of these recommendations are listed below:

- An SOP update would be useful to reflect changes to sensors and tactics.
- Forward Operating Procedure (FOP) devolvement should be pushed out to 50 meters.
- Red, Amber Green (RAG) Grid maps using 50 meters grid squares should be developed for each venue.
- Command and Control venue location can be better optimised.
- Training for all Technical Officers and drills for Effector Operators.
- It is advised that a Red Team retest with limitations on the RoE.

1.11 Key Take-Aways

1.11.1 Encourage Blue Teams to think as a threat actor

Many lessons and takeaways are only made possible to the Red Team due to the utilisation of scenarios based on actual case examples and the use of local knowledge. For instance, the Red Team can use drone pilots from the national police forces, which allows for a different approach to using drones. This can give them confidence in their drones and demonstrates that by allowing them to think like a red pilot, they understand the challenges and issues they would face in keeping the airspace safe.

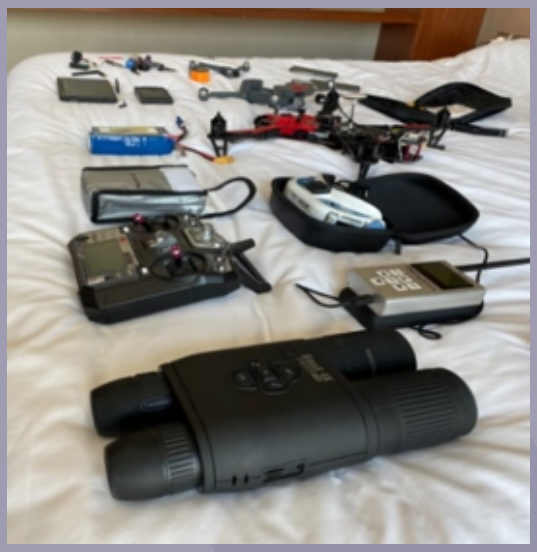
1.11.2 Allowing the use of drones by third parties during a major event

Discussions can arise regarding allowing non-law enforcement drones to be used during major events, for media purposes for instance. Even though measures are in place to identify good drones that are airborne, this may prove problematic in practice: once a drone is airborne, it is difficult to identify a good drone from a bad one.

If drones are to be flown during major events, then the rules of use for drones should be established and communicated with the media companies' drone pilots to ensure that they are not brought down or targeted by the drone response teams.

During pen tests, it can happen that some exercises are interrupted by unscheduled drone flights being undertaken by media companies or other actors involved in the preparatory phase of the major event. This can create confusion within the VOC and amongst the teams. All drone flights that are to be flown by non-law enforcement entities should be logged and recorded similar to the role of air traffic control to ensure that the airspace in and around the major event facility is managed effectively and efficiently. Otherwise, this could create false positives/negatives for the drone response team and the VOC.

1.11.3 Locate the Pilot



One element from the drone response is the pilot's location during a drone incursion. Locating the pilot responsible for flying the drone in the area is a vital action to undertake.

Some Digital Forensic devices that allow for rapid data recovery from drones can be used to identify the country of origin, initial calibration tests out of the box, and all previous flights with take-off locations.

Example of a Red Team member's equipment in a hotel room

1.11.4 Adaptability to Drone Threats

During a pen test exercise, the Blue Team might have to improvise and streamline the teams' response to drone threats and their command and coordination processes.

1.11.5 Utilisation of External Expertise and Knowledge

Using expertise outside of the law enforcement domain is invaluable, especially in reconnaissance, planning, and execution of the drone flights. Within a proper legal arrangement to ensure for the engagement's legality and confidentiality, this approach should be encouraged as it allows for fresh ideas, engagement, and trust building with the drone community.

1.11.6 No Drone Zones – No Fly Zones

In keeping a stadium and its vicinity safe from drone threats, the establishment of 'No-Drone Zones' or 'No-Fly Zones' should be considered. Member countries should utilise this capability as a first line of defense to prevent drone incursions at protected airspaces, such as stadiums and airports. If no drone zones are implemented then law enforcement should ensure that their drones are able to operate within these areas by working with the manufacturer to ensure that they are not effected.

Restricted Zone	No flight whatsoever is permitted inside a Restricted Zone. These zones cover airport runways in a rectangular shape that is 1.2 km wide and the length of the runway with 3 km added to each end.
Altitude Zones	An Altitude Zone is an area of restricted flight altitude. Each of these zones consists of two parts. Part one is a 60-meter height-restricted area, which extends 3.6 km outwards from the four corners of a Restricted Zone at an angle of 8.5°. Part two is a 150-meter height-restricted area, which extends 8.4 km outwards from the corners of part one.
Authorization Zones	In an Authorization Zone, all flight is restricted by default, but users can self-unlock with a DJI-verified account. These oval-shaped areas consist of two 4 km semicircles on each end of the runway that connect in the middle.
Enhanced Warning Zones	An Enhanced Warning Zone is a circular area that extends 2 km outwards from the perimeter of an Authorization Zone. When a drone is approaching this area from the outside, the DJI GO app will issue a warning. Users must then confirm that they wish to continue flying.
Compatible Products	Spark, M200 series, Mavic series, Inspire 2, Phantom 4 Series

Figure 1: DJI Airport GEO Zones[3]

1.11.7 Public Engagement

The value of public engagement to encourage no drones brought to a major event cannot be underestimated. Raising awareness around the use of drones during the event is key to the creation of a clear communication strategy, the deployment of signs and information around 'No Drone Allowed' should be continued. Suitable response should be used as a deterrent for anyone thinking of flying their drone during the event.

1.11.8 Private-Public Collaboration

The use of C-UAS is relatively new in many member countries, and the selection and deployment of such systems can prove challenging. Furthermore, there are many stakeholders involved in protecting the airspace, so the key players need to be identified and engaged with to ensure that they are aware of their responsibilities and reporting mechanisms during a mass public event or drone incursion.

INTERPOL has demonstrated that hosting C-UAS testing events with a neutral standpoint benefits the industry and law enforcement. Cooperation between INTERPOL, external experts, and commercial companies is key to successful pen test exercises thanks to the sharing of good practices and knowledge aggregating from many areas.

Without this collaboration, INTERPOL would not have been able to provide enhanced capacity building to its 195 member countries on safe events within the Project Stadia commitment, ensuring the successful security and delivery of these events for host nations worldwide.

[3] *DJI website, https://www.dji.com/fr/flysafe/introduction*

Annex 1: Supporting Materials

Stadia Knowledge Management System (SKMS)

A core component of Project Stadia is to develop good practices and international standards. As such, the Stadia team conducts expert groups, observation and debriefing programs with designated security officials from both the public and private sectors who have direct responsibilities for policing and security operations of major events. Lessons learned are shared with INTERPOL's 195 member countries, through the Stadia Knowledge Management System (SKMS).

Experts in the field of major event policing and security can share, discuss, analyze and publish information on the evolving aspects of major events and mass gathering security in the SKMS.

Users from law enforcement, academia, international cooperation organizations and private security companies involved in the policing and security of major events can request access to the SKMS by emailing: **StadiaKMS@interpol.int**

Framework for Responding to a Drone Incident

The global reference for drone incident management. Published by INTERPOL in 2020.

https://www.interpol.int/content/download/15298/file/DFL_DroneIncident_Final_EN.pdf

(January 2020)

INTERPOL Drone Countermeasure - Exercise Report

Results of live testing C-UAS systems in an active airport environment. Published by INTERPOL and the Norwegian Police in 2022.

https://www.interpol.int/content/download/17737/file/C-UAS_Interpol_Low_Final.pdf

INTERPOL Drone Forensics

Several INTERPOL publications are available which cover the topic of digital forensics and how they are applied with the drone domain. The publications are listed below and can be sourced from the Interpol innovation Centre website.

https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics

- **Global Guidelines for Digital Forensics Laboratories:** outlines the procedures for establishing and managing a Digital Forensics Laboratory and provides technical guidelines for managing and processing electronic evidence.
- **Framework for Responding to a Drone Incident:** provides technical guidance in managing and processing a drone incident for first responders and digital forensics practitioners. (See Section 12.3 above).
- **Guidelines for Digital Forensics First Responders:** offers advice related to search and seizure, for identifying and handling electronic evidence through methods that guarantee their integrity so that they are admissible in the judicial process.

Annex 2: Further Readings

- Countering Threats from UAS – Making Your Site Ready, Centre for the Protection of National Infrastructure (CPNI), (https://www.cpni.gov.uk/system/files/documents/40/14/c-uas-branded-doc-public-V4.1.pdf) (15 October 2021)
- Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges and Future Trends, Jian Wang, Yongxin Liu, and Houbing Song, Senior Member, IEEE, Researchgate,
- (https://www.researchgate.net/publication/343986630_Counter-Unmanned_Aircraft_Systems_C-UAS_State_of_the_Art_Challenges_and_Future_Trends). (August 2020)
- Counter-Unmanned Aircraft Systems Technology Guide, U.S. Department of Homeland Security, (https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf) (28 February 2020)
- Drones, Federal Aviation Administration (FAA), (https://www.faa.gov/uas), (Accessed on 23 February 2023)
- Protecting Against the Threat of Unmanned Aircraft Systems: An Interagency Security Committee Best Practice, Cybersecurity and Infrastructure Security Agency (CISA), Cybersecurity and Infrastructure Security Agency, Interagency Security Committee, (https://www.cisa.gov/sites/default/files/publications/Protecting%20Against%20the%20Threat%20of%20Unmanned%20Aircraft%20Systems%20November%202020_508c.pdf) (November 2020)
- Protecting vulnerable targets from terrorist attacks involving unmanned aircraft systems (UAS), United Nations Office of Counter-Terrorism, (https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2118451e-vt-mod5-unmanned_aircraft_systems_final-web.pdf) (2022)

Project Stadia

In line with INTERPOL's vision of «Connecting Police for a Safer World», Project Stadia set out to draw on expertise from across the globe to contribute to the planning and execution of policing and security arrangements for major events.

To further its objective, Project Stadia hosts expert group meetings with the key themes of physical security, crowd management, cyber security, and many more. These meetings bring together experts from law enforcement, event organizers, governments, the private sector, academia, and civil societies to explore state-of-the-art research and develop independent recommendations for planning and executing security arrangements for major international events.

To capture good practice and lessons learned before, during, and after international events, Project Stadia also conducts observation and debriefing missions with designated security officials from both the public and private sectors responsible for policing and security operations.

In addition, Project Stadia developed and delivered an accredited Safety and Security Training Programme for Major International Events. This training programme consists of six training courses covering a number of crucial topics for police commanders and incident management leaders involved in policing and securing major international events. Each course is designed to enhance the knowledge, skills, and capabilities of police commanders and incident management leaders who are responsible for policing and managing safety and security at major international events.

Established by INTERPOL in 2012 and funded by the Government of Qatar, Project Stadia has created a Centre of Excellence to help INTERPOL member countries plan and execute policing operations for major events. Project Stadia centralizes the wealth of knowledge generated through nearly 60 expert group meetings, observation programs, and debriefing activities into its online Stadia Knowledge Management System (SKMS) (Appendix 1). The SKMS provides a lasting legacy for the world's law enforcement community when securing major events.

Innovation Centre

The INTERPOL Innovation Centre (IC) supports promoting creative and innovative solutions to fight technology-enabled threats. The IC achieves this goal by bringing together experts from a wide range of backgrounds to develop contemporary, creative solutions to challenges in policing.

The IC facilitates thought leadership and connects law enforcement, academia, and private sector partners to exchange knowledge and explore new technologies and emerging cyber threats.

The work of the IC is split into four thematic labs:

- **Adaptive Policing Lab - identifies and assesses technical innovations that are relevant for law enforcement agencies;**
- **Cyberspace and New Technologies Lab - assesses key ways to disrupt, predict and investigate emerging threats in the cyberspace;**
- **Digital Forensics Lab - provides operational assistance in digital forensic investigations including, mobile devices, unmanned aerial systems, and shipborne equipment on seized vessels;**
- **Futures and Foresight Lab - identifies and analyzes global technology, strategy, and policy developments.**

Through these labs, the IC supports police in addressing emerging technology-enabled threats and challenges. By promoting close analysis and research, the Centre also highlights potential trends and phenomena affecting law enforcement work.

The IC is based in the INTERPOL Global Complex for Innovation in Singapore. Its activities are grouped into four main clusters:

- **Networking and knowledge exchange on best practices, latest technologies, tools, methodologies, and developments in law enforcement;**
- **Standard setting, guidance, and publications - assists member countries in assessing emerging trends and maintaining state-of-the-art laboratories;**
- **Support in building capabilities - delivering relevant training material and harmonizing content;**
- **Operational support – equipping law enforcement agencies with the tools and knowledge to fight against transnational crime.**

PROJECT **STADIA**

Safe & Secure Major Events

For more information, contact us at stadia@interpol.int
and visit our social media accounts:

INTERPOL-STADIA @INTERPOL_STADIA

WWW.INTERPOL.INT