INTERPOL

PROJECT **STADIA**

Safe & Secure Major Events

STADIA PROTECTION AND MITIGATION FROM DRONE INCURSION AND THREATS

Guidelines for Testing and Evaluation of Counter Unmanned Aircraft Systems (C-UAS) Capabilities

October 2023

Forewords

«It is with great excitement and anticipation that we introduce these Guidelines building on the insights gained from the red/blue team exercise that tested the 2022 FIFA World Cup C-UAS security operations.
Capitalizing on the results of this exercise, these Guidelines strive to equip the law enforcement community and security stakeholders with actionable strategies to enhance their preparedness and lay the foundation for safe and secure major events. Embracing INTERPOL's vision to make the world a safer place, Project Stadia and the Innovation Centre stand united in our commitment to assist INTERPOL's member countries in delivering safe and secure major events through the implementation of the Guidelines introduced here».

Stephen Kavanagh, Executive Director Police Services

«This manual highlights the importance of red and blue teaming to ensure that a member country can respond to the threat of drones at mass sporting events.
This manual also illustrated the complexity of tackling this issue and we hope that member countries will benefit from the work that INTERPOL has undertaken to ensure the safety of the public and law enforcement at sporting events».

Madan Oberoi, Executive Director Technology and Innovation

«To prepare for the safety and security of the FIFA World Cup Qatar 2022™, and given the increasing threat posed by Unmanned Aerial System (UAS) to stadia infrastructures, a Red Teaming exercise with penetration testing of key World Cup locations was undertaken in October 2022. In coordination with the Qatari Police Forces, the unique combination of INTERPOL Project Stadia and Innovation Centre teams as well as their network of international experts in the Unmanned Aerial System (UAS) / Counter Unmanned Aerial System (C-UAS), was instrumental in performing efficient preparations to ensure the safety and security of FIFA World Cup Qatar 2022™. The Red Teaming exercise was the opportunity to bring together international experts along with Qatari law enforcement officers to enable the sharing of knowledge, good practices and experience so that airspace threats were assessed, risks mitigated and the best counter-measures chosen.
As a result, the Stadia Protection and Mitigation from Drone Incursion Threats – Guidelines for Testing and Evaluation of C-UAS Capabilities have been developed to provide analytical insights and recommendations for planning and executing security arrangements for countering potential threats brought by UAS in stadia. It builds on the Red Teaming exercise as a case study, providing advice on good practices to follow and pitfalls to avoid when setting up C-UAS capabilities. We hope that these Guidelines will support the law enforcement community capacity to carry out effective Red Teaming exercise and that they provide value when planning C-UAS strategy to deliver safe and secure major events».

Captain Talal A. Al-Mulla, Head of Drone Team Operations, Safety and Security Operations Committee (SSOC)

Captain Rashid Fahad Alali, Head of Counter Drone Unit, SSOC

Acknowledgements

These Guidelines are the result of a collective effort from a select group of experts and organizations. INTERPOL Project Stadia and INTERPOL Innovation Centre thank and acknowledge Brooke Tapsall, Gokul Srinivasan, Matt Service, and their team of Counter Unmanned Aerial Systems (C-UAS) experts for their invaluable contributions and support to this document. Their combined expertise, knowledge, and time have been instrumental in helping the Stadia Project team compile this guide, which aims to provide actionable guidelines and recommendations to INTERPOL member countries on the topic of developing C-UAS processes, protocols, and testing for the protection of an asset, event, or public space.

The baseline for these Guidelines was the FIFA World Cup Qatar 2022™ Red Teaming Operation, which was facilitated between INTERPOL Project Stadia, INTERPOL Innovation Centre, and the Qatar Ministry of Interior (MOI) to create a Red/Blue Team project for testing a member country's response to a drone coming in the close vicinity of a stadium. INTERPOL would like to thank the Ministry of Interior (MOI), Qatar, for supporting the operation where all parties learned and achieved their goals, all of which will benefit the INTERPOL member countries in the future.

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

Target Audience

These Guidelines are intended for the use of INTERPOL member countries. It has been developed to support the ongoing preparatory Counter Unmanned Aerial Systems (C-UAS) work of two core audiences: the security practitioners, who develop the concept of operations, operational strategies, and plans; and the first responders and police officers who need to implement those plans, train, and respond effectively to incidents in stadia or events, using C-UAS technologies and systems. These Guidelines aim to illustrate the minimum requirements a law enforcement organization needs to prepare, test, and defend an asset, event, or public space from malicious threat actors.

This document covers 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 defences and reaction to threat capabilities. Some highlights are also identified on the capacity building level, listing potential training areas. The insights and general guidelines provided are intended to be used as a reference framework during the planning and execution phases, both at operational and tactical levels.

These Guidelines should only be used as a standard supporting document that can be referenced by member countries when developing and testing their C-UAS capabilities and processes for a potential drone threat. They should be modified or adjusted in line with each member country's local legislation, policies, practices, and procedures to best suit the country's actual needs and organizational structures. The Guidelines must account for the national regulations and international civil and aviation laws and do not replace or supersede any conditions of any aviation authority.

By working with law enforcement partner agencies and organizations in its member countries, INTERPOL aims to ensure that processes and operations are thoroughly analysed to protect assets, events, and public spaces and that international, regional, and local expertise is shared.

1.Stadia Overview and Threat Summary

A decade ago, non-military Unmanned Aerial Systems (UAS) were primarily custom-built remote-piloted aircraft used for personal entertainment by model aircraft enthusiasts. Today, affordable commercial systems can be operated with minimal training and are used as powerful tools across multiple industries, improving work processes and offering new and innovative methods of operation. In addition, the rapid development of autonomous systems driven by market forces has led to new technologies, such as advanced networked and persistent communications for extended logistics and payload delivery.

However, drones have also proven to be a potential threat. These unmanned aerial vehicles, commonly referred to as «drones», are automated flying robots, computers, or cell phones that have quickly established themselves as malicious tools in various environments. The potential dangers drones pose in the wrong hands cannot be underestimated. This technology, if used maliciously, can be transformed into weapons or tools for criminal activities, and their versatility makes them attractive to innovative criminals seeking to conduct illegal acts.

The growing concern over drones entering restricted airspaces has become a significant challenge for law enforcement agencies worldwide, particularly for the 195 member countries of INTERPOL. This concern is significantly heightened when drones are detected in densely populated areas, such as stadia hosting major events. The presence of drones in these sensitive spaces can result in event disruptions, delays, cancellations, and criminal activities, such as terrorism, potentially, affecting those in attendance and television viewers worldwide.

The risk of drones being used to disrupt a crowded and public event within a stadium is growing. Multiple events have been reported in INTERPOL member countries concerning disruption caused by unauthorised drones entering protected airspace around stadia. The majority of the reported drone incidents are from nuisance drone pilots who are testing the enforcement boundaries of the airspace or ignorant pilots who just want to get footage of the event hosted in the stadium. However, there is also the possibility of criminals or terrorists who may want to disrupt, influence, or gain an advantage related to the asset or event being hosted. Additionally, the stadium may be considered a high-value target for a terrorist organization. Other scenarios may include the promotion of an ideology or belief where a drone can be used to incite violence or to gain publicity around a belief or protest using signage or flags that may incite an escalation of emotions between opposing countries, groups, playing teams, or individuals.

In this context, C-UAS technology plays a supporting role in contributing to the security of stadia and events. Commercial providers have already developed a wide range of solutions to address this challenge. C-UAS will likely become more prominent as authorities in member countries develop regulations and legislative frameworks around the legal and illegal use of drones.

Most countries rely on legislation and regulation as the primary strategy to mitigate the unauthorised use of drones, especially for the most common, non-criminal incidents. However, as drone technology becomes increasingly more accessible and advanced, drone use by malicious threat actors (i.e., criminals, terrorists) will inevitably become more prevalent.

2.Stadia Protection Phases

Best practices for asset security begin with a thorough risk assessment for each type of event and situation. Information developed in the course of conducting a risk assessment will influence each of the other workflows of the overall security operational procedures (Figure 2). While general risk assessment has been studied for a number of different industries and has extensive literature, assessment of risks around stadia has certain unique characteristics:

- **Stadia may host extremely high-profile events (raising the value of an attack in the minds of threat actors).**
- **They may include access paths that are very difficult to control.**
- **Crowds may congregate, or queues may build up at gate entrances.**
- **They are subject to conflicting goals of stakeholders ranging from ticket holders seeking entertainment to law enforcement practitioners with a deep concern for event security.**

Overall, risk is a product of three factors: threats, vulnerabilities, and consequences. Threats comprise all possible forms and weapons of attack based on specific incidents and intelligence that expand well beyond C-UAS, such as active shooters, improvised explosive devices, protest, insider threats and sabotage, cyber-attacks, etc. Vulnerabilities are identified during the threat risk analysis process (Section 8.1) and are areas or situations in which the threats would be able to breach to cause harm – i.e., the vulnerable areas such as crowd congregation, VIP areas, weaknesses in protective technology or equipment, etc. Together the threats can define the vulnerabilities; therefore, these two elements will determine the consequences of their combination.

For example, the threat of a drone attack on a stadium via aerial improvised explosive device (IED) drop or a drone that can spray a substance over the crowd (threat) in an area where crowds congregate due to a necessity to pass entrance gates (vulnerability). This can result in many people being injured from a potential explosive device, unknown corrosive substance, or crowd stampede arising from panic (consequence).

Testing an organization's response plans and supporting C-UAS technology deployed over an asset, event, or public space is vital to determining effectiveness and robustness. This is performed via Adversarial Testing, a series of war-gaming scenarios where a number of teams mimic and play out real-world threats in a large-scale, safe simulation. This adversarial testing is also commonly known or written as Red Teaming, Penetration Testing, Red vs. Blue Teaming or Red/Blue Teaming (See Section 10.2 for further details of teams and composition).

For the purpose of these Guidelines, we call this adversarial testing Red Teaming and the act of a Red Teaming Operation.In detail, Red Teaming is when several teams perform a series of war-gaming scenarios to mimic real-world threats which test the defences and operational procedures of an asset or location from the attacks of the Red Team. Within the Red Teaming Operation are war-gaming scenarios in which the Red Team behaves as a threat actor, attacking assets or locations trying to break past the defences. As the defender, the Blue Team aims is to secure the asset or location against these threats or attacks from the Red Team using the operational procedure enacted and the C-UAS technology deployed.

This Red Teaming Operation is used as a critical capacity testing tool to assess the operational procedures (Section 3), C-UAS Technology capabilities (Section 8.2), and overall coordination of security defences. The tests normally identify gaps in operational procedures, personnel training needs, technology weaknesses, and other procedural or technological requirements that would increase an asset or location's defence capabilities. See Section 10 for further details on how Red Team activities operate.

It is to be noted that within these Guidelines, we do not address drone forensics or drone incident evidence collection as these are documented in INTERPOL frameworks referenced in Annex 1 and recommended for organisations to read to complement this guide and their knowledge. Other useful readings are found in Annex 3.

2.1 Protection Phases Overview

These Guidelines provide a flexible yet comprehensive framework that can contribute to developing enhanced security over assets and public spaces.

These Guidelines are broken down into four phases contributing to a general concept of a 'C-UAS Protection Cycle' (Figure 1), which means that the concepts which are mentioned within each of the phases will support organisations in developing the minimum viable security needs which will give their asset or location an adequate level of protection. All of these phases within the C-UAS Protection Cycle contribute to the overall C-UAS Strategy that will govern an asset or location protection. For the purpose of these Guidelines, we focus on the four phases and how to build these within an organisation.

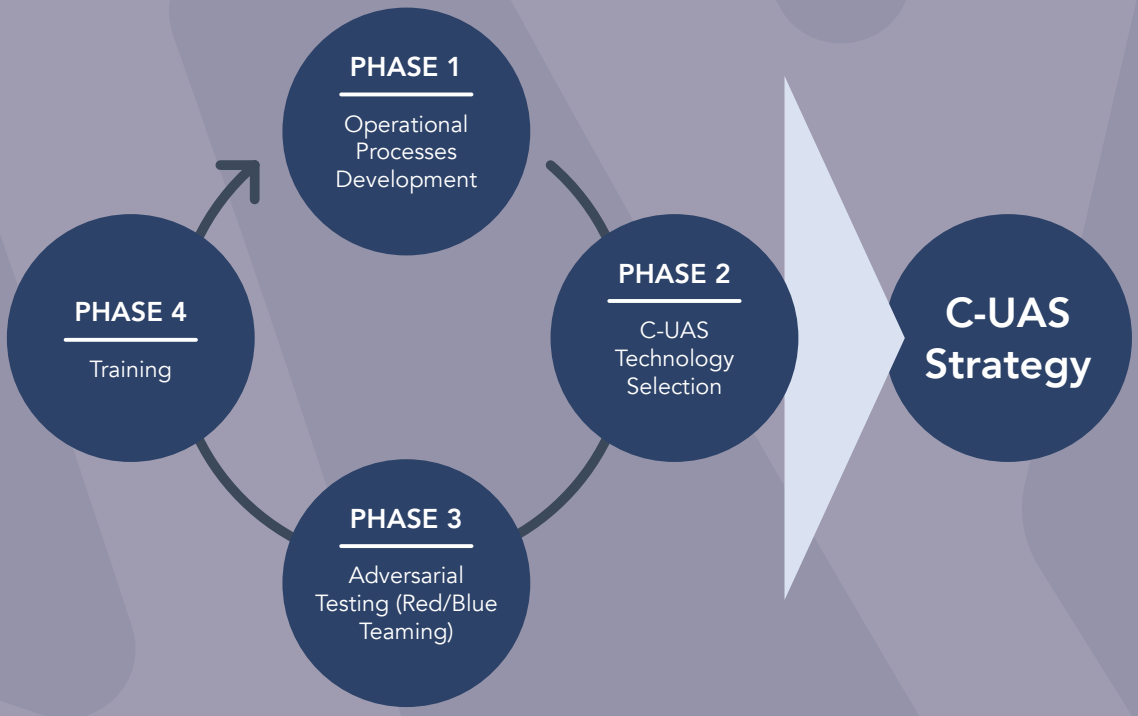

Figure 1: C-UAS Protection cycle & strategy

Each phase of the C-UAS Protection Cycle focuses on the specific requirements and operational procedures within that phase, all of which contribute towards or interlink with other phases as described below and shown in detail graphically in Figure 2.

The four protection phases are:

- **Protection Phase 1: focuses on the development of the processes that will be used to manage and respond to UAS threats.**
- **Protection Phase 2: examines the various C-UAS technologies that are available to mitigate these risks.**

- **Protection Phase 3: tests the operational procedures and deployed C-UAS technologies through Red Teaming adversarial testing to ensure all operational procedures (phase 1) and implemented C-UAS technology (phase 2) are effective as an overall defence of an asset or location.**
- **Protection Phase 4: highlights tactical responses and processes training needs identified (from Phases 1-3), ensuring that those responsible for security are fully equipped and confident to handle any UAS threat.**

These protection phases work together to provide a holistic approach to the development of C-UAS operational procedures for the protection of assets, events, and public spaces and have been graphically portrayed in Figure 2 to show the hierarchical and inter-dependencies of each phase and subsequent underlying requirements and operational procedures.

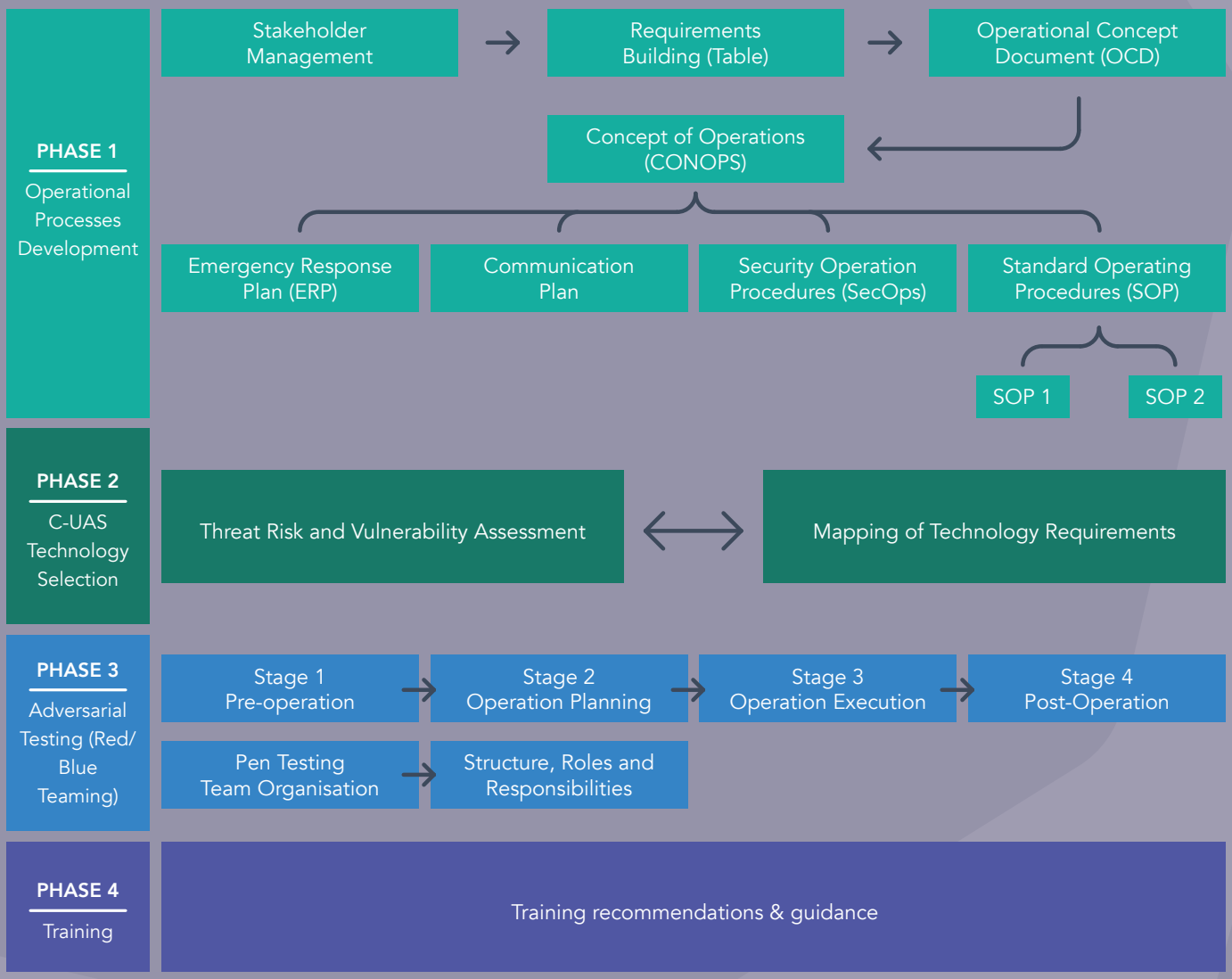

Figure 2: C-UAS processes covering four phases for protection of an asset

3.Protection Phase 1: Operational Procedure Development

Preparation is a key element when defending against a threat. During the scoping of these operational procedures, many avenues of action are developed, discussed, and enacted for execution. Operational procedures (Section 3) are documentation for processes and protocols on operations, security, emergency, and communications (Section 5) each giving relevant process flows and protocols that will enable law enforcement organizations to be better prepared for potential threats. These operational procedures, when confidently developed, should be tested by a Red Team (Section 10, Section 11) to support mitigation actions and training (Section 13).

In this section, we will highlight the key elements to be considered, at minimum, for the development of suitable operational procedures recommended under protection phase 1, as defined in Figure 3.

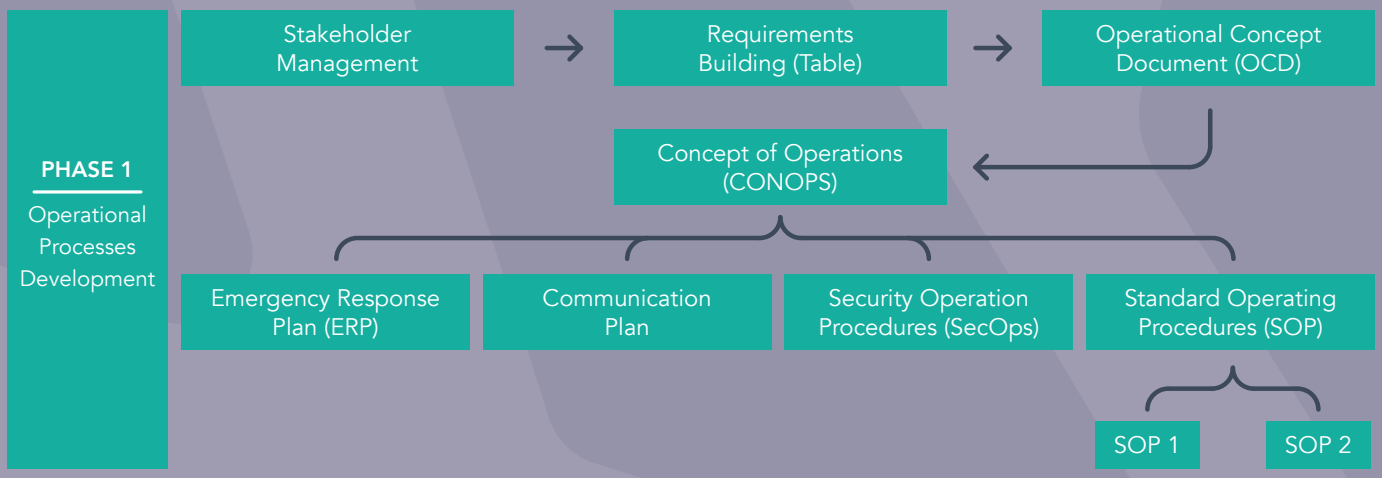

Figure 3: Protection Phase 1 – Operational Procedures Development

3.1 Stakeholder Management

Throughout the stages of developing operational procedures for the protection of assets, stakeholder engagement, and involvement are critical for ensuring clear communications and knowledge exchange. Many stakeholders can overlap across the different operational procedures addressed within these Guidelines. As such, we mention first the need for a clear identification of stakeholders across all operational procedures.

Below is a non-exhaustive list of stakeholders who may be involved across several operational procedures described in this guide:

- **Aerodrome management (airports)**
- **CAA (Civil Aviation Authority)**
- **Emergency Services (Fire & ambulance services)**
- **Law enforcement agencies (LEAs)**
- **Local government responsible for public spaces**
- **Media outlets**
- **Military Services**
- **National air regulation bodies (if differing from the CAA)**
- **National authorities responsible for security & intelligence**
- **Public health infrastructure (hospitals)**
- **Public transport services**
- **Stadia, asset, Area of Interest (AOI) management**
- **ATS (Air Traffic Services)**
- **Volunteer organization (supporting LEAs).**

Stakeholder Management is very relevant for contributing to the four protection phases and the overall C-UAS Strategy (Figure 1). These stakeholders can potentially and greatly influence the operational requirements and the subsequent operational procedures. As such, it is recommended to start the design of the Stakeholder Management Plan before or concurrently with many types of operational procedure development. Early design can ensure secure alignment and collaborations between stakeholders and establish a clear understanding of the legal and regulatory needs and the technical and operational nuances which may arise within individual organisations or INTERPOL member countries.

Stakeholder and Communication Plans are further detailed in Section 5, and stakeholder management in Section 3.1.

3.2 Operation Requirements Building

Below, Table 1 indicates several chronological elements which should be considered when planning a Red Teaming Operation to protect and mitigate assets, such as stadia, or other locations, such as a public space.

Many are recommended as mandatory in order to achieve a successful foundation towards the four phases of the C-UAS Protection Cycle and, consequently, a robust overall C-UAS Strategy (Figure 1). Other requirements are strongly suggested and listed as 'recommended' within the table; these support the mandatory requirements and would add value to planning yet are at the discretion of the organisation.

Table 1 lists the requirements with abbreviated descriptions of the process, some of which may be elaborated further in the Guidelines or within the case study and are accordingly referenced. Otherwise, this table is a guide for users to investigate and elaborate in accordance with their organisational needs.

Table 1: Operational Requirements Building Parameters

	TASK	ACTION
Mandatory	Operations Budget	Before commencing an adversarial testing Red Teaming operation, a budget should be secured for operational costs, at a minimum: equipment, personnel, logistics and administration.
	Operations Timescales	The timescales for planning, execution and post-operation must be known to plan and execute an adversarial testing Red Teaming operation successfully. Within each operation are included individual/ sub-operations, which require their own timescales.
	Learning Needs Analysis (LNA)	There may be a training element as part of the user requirements for an operation. This analysis must be carried out to determine the training gaps and the resources required to carry out the training to ensure all parties' expectations are fulfilled (Section 13).
	User Requirements	Before the Red and Blue Teams can be gathered and field events can be planned, the needs of the client for which the event is being carried out must be clearly understood and achievable. This is linked to the user requirements.
	Security Operation (SecOps)	This is an operational procedure which defines the security parameters. Security during operations is vital for the safe and secure execution of processes and the safety of personnel (Section 4.4).
	Concept of Operations (CONOPS)	This is an operational procedure to determine the objectives of a Red Teaming Operation. It is crucial to have a CONOPS in place to determine the goals and objectives of the operations as well as a clear set of guidelines (Section 4.2).

Mandatory	Rules of Engagement (RoE)	This is an operational procedure which details how the teams within the Red Team Operation (Red, Blue and other) (Section 10.2) engage during the war-gaming scenarios (Section 10.3). Before a Red Team Operation can take place, the Rules of Engagement (RoE) for when the event is being executed must be clearly outlined. As a minimum, this includes the range of scenarios that the Red Team can perform, the equipment which can be used and how the teams will interact together.
	Threat Risk Assessment	Understanding the threats (Section 8.1) associated to an asset or location for which the Red Teaming Operation is undertaken, is essential for developing the CONOPS (Section 4.2) for the operations field execution. Examining the threats from numerous media and information sources is useful in the preparation of the Red Teaming Operation. This activity is linked to Reconnaissance (ISR), which can be performed as support towards or verification of the threat analysis (Section 8.1).
	Threat Intelligence and OSINT	Open-source intelligence (OSINT) can be used to feed the Threat Risk Assessment (Section 8.1) by compiling and analysing public data and information.
	Threat Modelling	Even though Threat Modelling is a preparatory element of the Red Teaming Operation, it should also be a continuous process. It consists in pinpointing security flaws and finding solutions on how to overcome them.
	Capacity Modelling	By looking at the outcomes of previous Red Teaming Operation, capacity modelling is a useful technique to simulate future potential threats and how to address them. This leads into identifying training needs (Section 13).
	GEOINT	Geospatial Intelligence (GEOINT) is composed of imagery and geospatial information systems (GIS). It is a key component for building a complete Threat Risk Assessment (section 8.1).
	Intelligence, Surveillance & Reconnaissance (ISR)	Carrying out lawful reconnaissance missions is important for information gathering and planning of the Red Teaming Operation war-gaming scenarios. Key field, situational and geographical information is gathered to ensure the optimum use of technology, personnel, and infrastructure to meet the CONOPS (Section 4.2).
	Identification of Stakeholders and Responsibilities	These are operational procedures which need to be complied with for event security. They detail the stakeholders, their interactions and the processes and procedures to follow (Section 3.1, Section 5).
	Standard Operating Procedure (SOP)	The main guide for linking all the operational procedure of an organisation. They describe all stakeholders, their roles and responsibilities, how they interact and under what conditions. It is important to have SOPs in place before a Red Teaming Operation as the outcomes of the Red Teaming Operation can contribute to updating existing SOPs (Section 4.3).

Mandatory	Communication Plan	This is an operational procedure. Communication is a vital element of any operation. With many stakeholders and teams involved in a Red Teaming Operation, it is important to know what, how and when to communicate with whom. The communication plan supports the SOP (Section 4.3) and links to stakeholder identification and responsibilities (Section 3.1, Section 5).
	Emergency Response Procedures (ERP)	Linked to the communication strategy, the ERP details the stakeholders, rules and processes to be activated in the event of an emergency situation (Section 5.1).
	Legal & Regulatory Frameworks	It is expected that the legal and regulatory frameworks of the country where the event takes place are known and respected.
	Audit and Reports from previous operations	This is useful for first Red Teaming Operations, and essential for second Red Teaming Operations. It is useful to have any documentation, outputs or recommendations from previous Red Teaming Operations, (or similar testing if no Red Teaming has been previously carried out), to be able to mitigate past issues, learn from best practices and target the Red Teaming Operation war-gaming scenarios design for capacity building.
Recommended	Forward Operating Procedure (FOP)	A Forward Operating Procedure is a subset of a SOP.
	Drone Manufacturer GEO Fencing software functionality	Some manufactures have the ability to create zones that stop their drones from flying within specific areas. These 'geo-fences' can be automatically applied to the manufacture drones on purchase or during software updates. Having these in place over larger events can aid in deterring or reducing the ability of certain drones from entering the airspace of the event.
	No Fly Zones (NFZ)	No Fly Zones can be established by infrastructures such as airports and military grounds to prevent many breaches of airspace. These are also referred to as "Notice to Air Missions" (NOTAMs). It is useful to cross-check any existing NFZ which may impact a Red Teaming Operation or operations of friendly/police drones.
	Technology awareness and validation against requirements	Horizon scanning for new technological developments and their potential adequacy for the Red Teaming Operation should be performed well in advance in preparation of the forthcoming operation.

4.Operational Procedures and Response Plans

Figure 2 details an overview of the planning sequences recommended when coordinating a Red Team Operation. When organising a Red Teaming Operation, many may believe that flying a drone is the largest consideration; however, as Figure 2 indicates, there are many documents to develop under the four phases of the C-UAS Protection Cycle (figure 1). These are called operational procedures, and within these Guidelines, we will focus on how to develop the following operational procedures:

- **Operational Concept Description (OCD)**
- **Concept of Operations (CONOPS)**
- **Standard Operating Procedures (SoP)**
- **Security Operation Procedures (SecOps)**
- **Emergency Response Plans (ERP)**
- **Stakeholder and Communication Plans.**

Each of these operating procedures will lay the groundwork of a process and/or protocol, contributing to the security, protection, and safety of an asset or location and corresponding personnel. As Figure 2 indicates, and as previously mentioned, there are interlinkages and dependencies of process and procedural flow between these operating procedures; these interdependencies are addressed in the following sections of the Guidelines.

4.1 Operational Concept Description (OCD)

The Operational Concept Description (OCD) is a high-level executive summary for any operation, using a broad system-centric description of the intended users, use cases, the overall intention of the operation or system, and the external conditions expected during the use of the system for the specific use cases. An OCD may also identify other stakeholders and the interest in the operation of each stakeholder. Usually, the OCD becomes a reference for high-level stakeholder alignment and is a key satisfaction metric because it will define the scope of the work.

In Table 2, there are a number of steps for incorporating an OCD into your C-UAS Protection Cycle (four protection phases) and overall C-UAS Strategy (Figure 1):

Table 2: Operational concept description (OCD) parameters

OCD ELEMENTS	DESCRIPTION
Define local operational requirements	It is important to define the operational requirements to your local requirements. This includes identifying the mission objectives, the operational environment, and the operational constraints. This information will form the basis of the OCD and guide the development of the C-UAS strategy.
Linking the OCD with Stakeholder and Communication plans	The OCD should be developed in collaboration with all stakeholders, including end-users, operators, and technical experts. The OCD should outline the specific C-UAS capabilities needed to meet the operational requirements that need to be defined. It should also describe how these capabilities will be employed to achieve the mission objectives.
Integrating the OCD into the C-UAS strategy	Integration of the OCD into the C-UAS strategy is bridged by the CONOPS (Section 4.2), the system design in parallel to the operational procedures. The OCD should also be used to inform the selection of specific C-UAS technologies (Section 8) and the development of training programs. (Section 13)
Test and evaluation of multiple C-UAS systems	Test and evaluation of multiple C-UAS systems in the operational environment is of the upmost importance. This will ensure that the C-UAS strategy, as informed by the OCD, meets the operational requirements, and achieves the mission objectives. Any gaps or deficiencies identified during testing and evaluation should be addressed through updates via well documented change controls to the OCD and the C-UAS strategy.

4.2 Concept of Operations (CONOPS)

A Concept of Operations (CONOPS) is a high-level, descriptive document outlining a system or process' operational requirements, characteristics, and capabilities. It serves as a detailed conceptual communication tool, bridging the gap between stakeholders, operators, and service providers. It provides a clear and concise understanding of the intended use of the planned operations and testing. In the context of a testing and evaluation operation that employs adversarial Red Teaming to assess the effectiveness of Counter-Unmanned Aerial Systems (C-UAS), the CONOPS is a crucial element in ensuring the operation's success and alignment with the desired objectives.

From an operational level in planning, it explains how the different human and technical resources interact to achieve a particular effect or capability outcome within the expected solution. As such, CONOPS are a step below the OCD in that they provide more detailed information from the user's perspective. In conclusion, the CONOPS for this testing and evaluation operation provides a comprehensive framework for executing an adversarial Red Teaming exercise to assess the effectiveness of C-UAS systems. By clearly outlining the objectives, scope, methods, roles, and responsibilities, the CONOPS ensures that all stakeholders have a shared understanding of the operation, which is essential for its successful execution and for deriving meaningful insights to improve the C-UAS systems.

CONOPS can be diverse in content due to the different situational and environmental elements of operations and their locations. They are employed to achieve specific objectives, outlining key operational concepts, assumptions, and constraints. The CONOPS will also detail the roles and responsibilities of each participating team, including the Blue Team responsible for operating the C-UAS systems, the White Team (when applicable) overseeing the operation and ensuring a fair assessment, and the Red Team simulating the adversarial threat. It will also specify the communication protocols, performance metrics, and evaluation criteria used to gauge the effectiveness of the C-UAS systems under test.

A C-UAS Strategy can be defined as a comprehensive approach to detecting, tracking, and neutralizing potential threats posed by UAS in various operational environments. It generally encompasses the integration of technological, procedural, and tactical measures designed to safeguard critical assets, infrastructure, and personnel from the risks associated with unauthorized or malicious drone activities. The CONOPS plays a pivotal role in shaping an effective C-UAS strategy by providing a clear and coherent framework that outlines the operational requirements, capabilities, and intended use of the C-UAS systems. In addition, by bridging the gap between stakeholders, operators, and developers, the CONOPS ensures a shared understanding of the mission objectives, performance expectations, and operating conditions, fostering alignment and coordination among all parties involved. This collaborative approach ultimately contributes to developing and implementing a robust and adaptive C-UAS strategy, capable of addressing evolving UAV threats and ensuring the security and resilience of critical assets and operations.

The following steps should be considered when incorporating a CONOPS into both the OCD, the four focus areas, and the overall C-UAS strategy:

1. Defining the operational requirements of a CONOPS, which informs the OCDs for the overall C-UAS strategy, includes **identifying and aligning the mission objectives, the operational environment, and the operational constraints.** This information will form the basis of the CONOPS and assist in the parallel development of both the OCD and the C-UAS strategy.
2. **Developing the CONOPS should be done in collaboration with all stakeholders,** including end-users, operators, and technical experts who may or may not be external. The CONOPS should outline the key operational concepts, assumptions, and constraints of the C-UAS systems considered, including how the system will be employed to achieve the objectives of the mission.
3. **The CONOPS should be used to guide the development of the C-UAS system functionality,** non-functionality, layered security design, and the operational procedures within the overall C-UAS strategy. The CONOPS should also be used to inform the selection of specific C-UAS technologies and the development of training programs associated with the objectives of the mission.
4. **Testing and evaluation is the final phase** before the operational decisions on C-UAS system selection are made in the operational environment. This ensures that both the OCD and the C-UAS strategy, as informed by the CONOPS, meet the operational requirements, and achieve the objectives of the mission. Any gaps or deficiencies identified during the testing and evaluation phases should be addressed through updates to the CONOPS, OCD, and other relevant operation procedures in an iterative cycle.

To guide in the development of the operational procedure, CONOPS, Table 3 is a compilation of the main elements, at a minimum, to add to a CONOPS, the order of which can form a basic Table of Contents:

Table 3: Concept of Operations (CONOPS) Parameters

CONOPS ELEMENTS	DESCRIPTION
Objectives	What are the key objectives, priorities and activities to be carried out under this operational procedure, internal and external to the organization?
Target audience	Who is the operational procedure intended for within the organization?
Stakeholders	Who are the other stakeholders, internal and external to the organization who have a role within the procedure?

Levels of engagement	Stakeholders will require differing levels of engagement and their levels of engagement and how they are to be engaged, and with whom can be mapped to ensure clarity of roles within the processes and when these roles are needed.
Threat modelling	Threat modelling work should be done in conjunction with national/ state law enforcement and intelligence agencies or as foreseen under national law. Modelling possible threats and establishing their probability will help plan the rest of the operations.
Threat type	The main threat types from drones and risks should be assessed and compiled.
Requirement gathering	Based on the threat types and the threat models, the requirements for appropriate defensive and offensive measures should be formed.
Scenario modelling	A list of war-gaming scenarios should be prepared to be used for the security team training. Each scenario must be played out by all the stakeholders involved.
C-UAS Technology deployed	State the type of counter measures in place for protection, their role and function.
Command and control (C2)	A robust chain of command and control should be established and followed as part of the standard operating procedures.
Adversarial Testing Red Teaming	General statement of the requirement of a Red Teaming Operation, the high-level objective and the equipment to be used. This information will be more detailed in the Rules of Engagement (RoE).
Timeframes	Timeframes for the entire coordination and planning of the Red Teaming Operation should be added within your organization's plan.
Roles and responsibilities	Roles and responsibilities within the plan should be defined and mapped for relevant parties.
Emergency and contingency procedure planning	Protocols and procedures are to be established and followed by all personnel involved, across the hierarchy, in case of an emergency, or incident, or unprecedented event.
Communication plan	What tools does the organization have for communicating stated messages and to which stakeholders - i.e. public awareness campaigns, press releases, media (visual, publications), social media, internal training etc.? *Sub communications:* Communication messages: What main messages need to be conveyed and when during the execution of the plan? Communication channels: Which communication channels are to be used to convey which messages?
Evaluation and review	Select KPIs that determine success for the execution of the CONOPS during an incident and how often these should be tested or reviewed.

4.3 Standard Operating Procedure (SOP)

On a tactical level, the Standard Operating Procedure (SOP) provides an actionable, clear-cut description of a repeatable process, with detailed instructions on the steps necessary to complete a specific task or process. In short, it can be considered as an execution tool. For example, a piece of technology equipment needs to be operated at a particular temperature, only outside, and for a maximum of three hours a day to be operationally effective. This parameter will be different if the equipment is operated at another site; as such, an SOP is needed for that site to state what conditions are required.

Each SOP will differ in scope depending on varying factors, such as situational, environmental, and the type of technology solution that is being deployed (detection only, effectors, kinetic, etc.), as each deployment may require its own SOP (See Figure 3). The SOP may also vary from one venue to another, especially if the threat levels are different. Therefore, developing the SOP should be carried out in collaboration with all stakeholders, including end-users, operators, and technical experts.

It should be noted that the operational procedure called CONOPS may be distilled into more than one SOP for process standardisation purposes. For example, the SOP can be described as a more detailed step-by-step guide or checklist to process when carrying out an action(s). As shown in Figure 3, it is possible to have one SOP for the preparation of the site, another SOP for the Red Teaming Operation, and one SOP for how to operate the C-UAS technology etc.

Integration of the SOP into the OCD is also a key element for aligning operational procedures and continuity of process flow. The SOP should outline the specific procedures and processes for specific C-UAS operations. The SOP should also ensure that the OCD provides a clear picture of how the C-UAS technology system will be used and how tasks will be executed.

Integration of the SOP should be developed from the outset to be included in training programs. This will ensure that the C-UAS system is operated in a consistent and safe manner. Any gaps or deficiencies identified during training and implementation should be addressed through updates to the SOP, OCD, and other operational procedures under the four focus areas and towards the overall C-UAS Strategy.

Keeping in mind the variabilities, Table 4 highlights the main elements, at a minimum, to add to an SOP. Each organization is encouraged to add further fields as per situational requirements.

Table 4: Standard Operating Procedures (SOP) Parameters

SOP ELEMENTS	DESCRIPTION
Objectives	What are the key objectives, priorities and activities to be carried out under the SOP, internal and external, to the organization?
Target audience	Who is the SOP intended for within the organization?
Stakeholders	Who are the other stakeholders, internal and external to the organization who have a role within the SOP?
Rules of Engagement (RoE)	A clear set of rules are to be followed by all the stakeholders while engaging with each other.

Radio permissions	Permissions to use Radio Frequency (RF) detectors and effectors to be obtained ahead of time from appropriate national, and/or local authorities.
Operational handbook	A handbook to be provided as a quick reference to all operation operators and teams for highlighting processes, terminologies and communications, etc.
No Fly Zones (NFZ)	No Fly Zones to be established in relevant areas in coordination with the local Civil Aviation Authority (CAA).
Flight permissions	In order for the Red Team to fly and conduct operations as part of the Red Teaming Operation, appropriate flight permissions and NFZ waivers to be issued in advance from the relevant authorities and/or CAA.

4.4. Security Operating Procedures (SecOps)

An organization's Security Operating Procedures (SecOps) cover the security measures and procedures which will be deployed to ensure a safe and secure environment for personnel around an asset on site and during Red Teaming operations.

When developing these procedures, Table 5 lists the minimum elements to be covered in your organization's operational procedure, and it is recommended to add further fields according to specific situational requirements.

Table 5: Security Operating Procedures (SecOps) Process Elements

SECOPS ELEMENTS	DESCRIPTION
Information sharing	The sharing of information, data, files, plans or operational procedures related to the operation to be done only by, and with, authorised personnel who have been thoroughly vetted by a security clearance process.
Background check	All participating personnel to go through a screening process.
NDA and confidentiality	All stakeholders to be subject to appropriate Non-Disclosure Agreements (NDA) and confidentiality clauses to prevent leakage of information to unauthorised individuals or to social media channels.
Insurance	All infrastructure and/or assets involved to be appropriately insured.
VOC	Establish a Venue Operations Command and integrate that with the command and control and headquarters units.
Red Amber Green (RAG) threat levels	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.

5.Emergency, Stakeholder and Communication Plans

Linked to the operational procedures above are the 'people-oriented' processes regarding how all stakeholders engage during an operation or, more broadly, during a drone threat incident. These will be referred to as a 'plan' or 'plans' to aid in differentiating from the aforementioned operational procedures.

As with the operational procedures (SOP, SecOps, CONOPS, RoE (part of the Red Teaming Operation), the following plans will also be unique to an organizational asset, event, or public space as each will have environmental, legal/regulatory and situational elements only for that asset that can alter processes within the plans. The below sections provide recommendations of the main elements to add to these plans, at a minimum, to provide a suitable level of information and coordination within the documents.

Also, it should be taken into consideration when developing these plans that emergency and first responder services use a different designation of Strategic/Operational/Tactical levels and structure. If any cross-border plans are made or shared, these differences in structures should be clearly described and clear for all stakeholders. This element is recommended to be addressed early in operation coordination planning and document definition, if applicable.

5.1 Emergency Response Plan (ERP)

An Emergency Response Plan (ERP) will detail how and who will be active and in what roles during an incident over an asset, event, or public space. This document should detail the key stakeholders involved, when, and, most particularly, how each engages by clearly stating the roles and responsibilities of each key stakeholder within the process of an active emergency. The stakeholders' engagement level will depend on the severity of the incident and the consequent outcome. Taking the information gathered during the threat assessment process (Section 8.1), it can be useful to map an emergency response to your asset's most probable risks and threats.

Table 6 lists the elements to consider, at a minimum, within the Emergency Response Plan:

Table 6: Emergency Response Plan (ERP) Parameters

ERP ELEMENTS	DESCRIPTION
Objectives	What are the key objectives, priorities and activities of the ERP, internal and external, to the organization?
Target audience	Who is the ERP intended for within the organization?

Stakeholders	Who are the other stakeholders, internal and external to the organization who have a role within the ERP?
Risk and threat response	What risks, identified in the ERP, need a response? These should be mapped to the appropriate stakeholders and their roles and responsibilities.
Timeframes	Timeframes for executing actions or the overall ERP should be added within the organization plan.
Roles and responsibilities	Roles and responsibilities within the plan should be defined and mapped.
Evaluation and review	Select KPIs that determine success for the execution of the ERP during an incident and how often these should be tested or reviewed.

Each response plan can be unique. Extending Table 6, below are listed other important elements for consideration within the ERP and Communications plans according to the organizational asset protection situation.

FOR CONDSIDERATION	
Link communication and stakeholder plan	Link any outputs of the organizational plan to the communication and stakeholder plan.
Link to other organization plans	If required, link to CONOPS and other plans in place within the organization.
Cluster or mapping	Cluster or map any process flows as much as possible in tables for easy reference, i.e., mapping stakeholder versus messages versus channels.

5.2 Stakeholder and Communication Plan

Linked to the emergency response plan is the Stakeholder and Communication Plan. The actors identified within the Emergency Response Plan (ERP) will all require a process and method of communication and engagement that will need to be clearly stated to ensure a smooth operation in the event of an emergency or incident. Other stakeholders not potentially identified within the ERP, such as news outlets, will need to be mapped into the Communication plan to ensure information flow is managed. Below are the main elements to consider, at a minimum, when developing the communication plan.

Table 7: Stakeholder and Communication Parameters

ELEMENTS	DESCRIPTION
Objectives	What are the key objectives, priorities and activities of the communication plan, internal and external, to the organization?
Target audience	Who is the plan intended for within the organisation?
Stakeholders	Who are the other stakeholders, internal and external to the organization who have a role within the plan?

Levels of engagement	Stakeholders will require differing levels of engagement and can be mapped.
Timeframes	Timeframes for executing actions or the overall plan should be added within the organizations plan.
Roles and responsibilities	Define and map what are the roles within the plan and their responsibilities.
Communication plan	What tools does the organization have for communicating stated messages and to which stakeholders – i.e. public awareness campaigns, press releases, media (visual, publications), social media, internal training etc.? *Sub communications:* Communication messages: What main messages need to be conveyed and when during the execution of the plan? Communication channels: Which communication channels are to be used to convey which messages?
Evaluation and review	Select KPIs that determine success for the execution of the Communication Plan during an incident and how often these should be tested or reviewed.

6.Public Information: Deterrent Considerations

Active campaigning of deterrents supports better drone behaviour or makes certain drone operators think twice before performing potentially careless, criminal, or further actions. Public deterrents lower the potential of threat risks from certain actors; as such, they are a useful mechanism to deploy over an asset, event, or public space. Below is a selection of common deterring actions which can be deployed:

Table 8: Threat Deterrent Considerations

ACTION	DESCRIPTION
Signage	Adding clear and distinct signage around the area to be protected, gives an initial warning and a clear, physical boundary of where drones cannot be flown.
Media campaign	Incorporating TV, radio, print or social media campaigns on the expected 'drone behaviour' of persons in, or around, the assets will aid in clarity for all attending.
No Fly Zones (NFZ)	Setting up No Fly Zones (NFZ) with the local CAA or drone manufacturers to 'geo-fence' the area will support the deactivation of the incursion drone's ability to fly within these zones.
Financial penalties	The potential risk of a financial penalty to a person who has breached the requirements of good 'drone behaviour' is a strong deterrent. Stronger penalties can also include jail time, in addition to the financial ones.

Blue skies policy	If the risk has been deemed too high, then a 'Blue skies' policy can be operated over the asset. This is when there is no drone activity at all, by anyone (police, media, asset owners etc.).

7.Protection Phase 1: Recommendations

- **Design CONOPS** in such a way as to ensure that a representative from each command level is embedded and linked with representatives of a similar level from relevant stakeholders (Section 4, Section 5).
- **Allocate more time** to learning need analysis (LNA), skills and competence development, development of intelligence and investigation continuity in the C-UAS Protection Cycle, and refine policy, procedure, and interoperability across host nation departments (Table 1).
- **Develop overarching messaging and adequate platforms for the diffusion of communications** (internal and external). Accessible information beyond the operational is critical for police engagement and impact (Section 5).
- **Ensure close collaboration with local partners**, such as residents, businesses, community groups, etc. Engage them in the security process and ensure they are informed of any constraints that may impact them (Section 3.1).
- If media company drones are to be flown during major events, an SOP stating 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. Media agencies are also stakeholders, and their engagement and how they are to be dealt with can also be addressed within the Communication Plan (Section 3.1, Section 5).
- **Implement peer reviewing** (national or international) during the planning phase to ensure feedback on all operational procedures and/or other security documentation. A timely review by non-affiliated experts ensures that gaps in planning and preparation can be identified and mitigated well in advance of the event.
- **Define risk appetite** in the initial planning stages to facilitate strategic decision-making and allocation of resources. To avoid a 'one size fits all' approach to security, venue tiering and associated mitigation measures are advised to guide an appropriate and targeted security methodology (Table 1).
- **Set up a dedicated plan and teams to deal with specific crimes** related to a major international event (investigation, intervention, and prevention).

8.Protection Phase 2: C-UAS Technology

When suitable operational procedures are being developed for coordinating and protecting an asset, it is important for organizations to define what threats are posed to their organization asset and what, if any, technology is suitable to counter this potential threat (See Figure 5). This section will guide users on identifying their threat potential to determine what C-UAS technology is required for supporting defence.

Figure 4: Protection Phase 2 – C-UAS Technology Assessment Overview

8.1 Threat, Risk and Vulnerability Assessment

Understanding what, or if, C-UAS technology is required for the protection of an asset is an important decision to make for all organizations. Many elements should be considered during this process, as the technology chosen can affect an organization's operating procedures, response plans, and training requirements. We will focus on the elements from Figure 5, which are well documented within the *INTERPOL Drone Countermeasure – Exercise Report*[1].

The report is a result of testing C-UAS systems at a live airport in Oslo, Norway, in 2021. It is recommended to read the aforementioned report for further details on C-UAS Technology Assessment, as we will be defining it only to a high level within this guideline.

Figure 5: C-UAS Technology Assessment Overview

[1]*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

Many questions arise when assessing the threat level of an asset, event, or public space. This ranges from the quantity of incidents, the severity of current threats, 'worst-case' impacts, and what C-UAS technology can be used to neutralise these threats within reasonable collateral damage or impact parameters. Being responsible for the protection of an asset, event, or public space begins when preparing to mitigate threats and development of operational procedures to address these threats with technology to support neutralisation.

Table 9 below is an example of assessing and assigning a threat level for each threat type, followed by a list of the main potential threats to an asset, event, or public space. This can be used as a guide for your process of assessing the threat risk to an organizational asset or public space.

It is important to note that the threat and priority levels can vary for each organization as situational,legal/regulatory, environmental, and technological elements influence the final levels.

Table 9: Threat Assessment Requirements

Threat level	Priority level	Threat type	Threat description	Action
What is the likelihood of the drone incursion occurring (Low, Medium or High)	If the drone incursion occurs, what is the priority of action or deployment of mitigation processes/technology (Low, Medium or High)	What is the threat scenario (i.e., drone carrying an IED)	General description of the situational incident	What action has been determined within your SOP to be taken to mitigate the risk and by whom

The type of threats to an asset, event or public space can vary depending on the situation and environment. To aid in the assessment, examples of threats are listed below for consideration:

- **Drone carrying liquids or other substances**
- **Drone used for ISR (Intelligence, Surveillance and Reconnaissance)**
- **Drone used to video coverage of sporting matches or other events**
- **Drone with IED payload**
- **Drone with jammer on board**
- **Drone with targeted messages or country flags**
- **Drones carrying contraband & narcotics**
- **Drones with CBRNE payload**
- **Kamikaze or swarm drone(s)**
- **Loitering munitions**
- **Stampede (caused by drone chaos)**
- **Tourist selfie drone activity.**

8.2 Mapping technology requirements

Linked to the section above, determining what C-UAS technology is needed to support the protection of the asset depends on the type of incidents potentially to be encountered, the physical environment, and the allocated budget. As such, each assessment for the protection of a particular asset, event, or location will be unique. Table 10 is an overview of what C-UAS technology is available, with a short description of their application, to aid understanding and for organizations to take into consideration when carrying out the threat/risk assessment.

Table 10: Types of C-UAS Technology

TECHNOLOGY	APPLICATION
Radar	Radar is a radiolocation system that uses radio waves to determine the distance (range), angle (azimuth), and radial velocity of objects relative to the site.
Jamming	Jammers work by blasting electromagnetic noise at the radio frequencies that drones use to operate and emit information. Effectively, they drown out the conversation between a drone and its operator.
Kinetic	Kinetic methods employ weapons systems using guns or missiles in conjunction with a targeting system to shoot down the drone. This includes high-powered laser or microwave to destroy the target drone as well. Other possibilities are to use nets and weighted lines, which may be launched with compressed air or propellant from a handheld device or from another Unmanned Aerial Vehicle (UAV).
Radio Frequency (RF) Detector	An RF sensor works by passively listening to the Radio Frequency spectrums in which drones communicate with their controller.
Electro-Optical/ Infra-Red (EO/IR)	EO/IR systems are imaging systems used for military or law enforcement applications, which include both visible and infrared sensors. Because they span both visible and infrared wavelengths, EO/IR systems provide total situational awareness both day and night and in low light conditions.
Acoustic	Acoustic detection systems may use an array, or a distributes array of passive acoustic sensors that can listen to a drone's sound and detect and classify them based on a prior knowledge.

It is important to note that C-UAS technology may cause collateral damage or impacts (i.e., drone may fall to the ground and potentially cause injury or damage to property), which needs to be taken into consideration when selecting the technology for the environment, operational deployment and regarding Red Teaming Operations, how the Red and Blue Teams and their equipment engage to be clearly detailed in the RoE.

9.Protection Phase 2: Recommendations

- **Determine what/if C-UAS technology is needed for performing a detailed threat analysis on the asset:** Not all C-UAS technology is suitable for all situations; as such, understand the threat/risk before choosing a C-UAS system or determining if a technology is even required.
- **Diverse Operational Environments:** Consider the fact that C-UAS solutions can be effective within one environment but may be limited in another. For instance, the use of C-UAS within an urban environment could be particularly complex due to the interference from existing devices and radiofrequency landscape and infrastructure limitations, including glass-fronted buildings, skyscrapers, and frequency-absorbing materials. This could severely affect the range and capability of the C-UAS solution.
- **Testing of C-UAS in Real-Time Environments:** When evaluating a C-UAS system, it should be tested in the environment it is intended to be operating in to ensure its effectiveness and reliability in detecting, tracking, identifying or mitigating drones. If the system is tested in a different environment than its intended operation, the results, and the effectiveness of the C-UAS may be compromised.
- **Set up an independent team for integrated testing and exercising the selected C-UAS technology.**
- **Employ mobile and fixed C-UAS Technology:** Law Enforcement Agencies (LEAs) interested in using C-UAS systems should address the need for fixed and mobile solutions. This presents a challenge as most systems are intended to be fixed and require time to be calibrated, tested, and optimized for efficient use in different environments. As a result, LEAs may need to utilise a multiple solutions approach that could provide different capabilities and deployment options. Moreover, LEAs should consider that most case scenarios require a multi-layered detection system that covers long, mid, and short-range detection capabilities to secure airspace. Where a mobile capability is tested or deployed, the environment should be understood with SOP tested against the necessity of use and judgement and authorisations for the collateral impact of the use of effectors (Section 8).
- **Ensure C-UAS Technology Operator competency:** When conducting the tests of C-UAS technology, trained users from the C-UAS system suppliers are generally used to operate the systems. In a real-life environment, however, the operator would most likely be the owner or responsible parties of the facility or a member of an LEA protecting the area. Hence, these individuals would require training and extensive evaluation of the system's capability and limitations to ensure its most effective use (Protection Phase 4).

- **Maintain C-UAS Systems:** When the C-UAS is installed at a location, the system may need constant or regular adjustments to ensure that it operates at its most effective capability and ensure that any existing or new infrastructure that is constructed within the detection range of the system does not reduce its operational envelope. Each C-UAS also needs to be regularly tested to ensure it meets the operational needs of law enforcement by confirming its operability to detect, track, identify, and mitigate drones. These tests should consider the emerging drone threat and evolution of the drone market to ensure that any system's capability matches the evolving threat from the criminal use of drones.
- Read the *INTERPOL Drone Countermeasure – Exercise Report*[2] (Annex 2).

10.Protection Phase 3: Red Teaming Operations – Adversarial Testing

Evaluating and testing an organization's operational procedures and supporting C-UAS technology (if required) deployed over an asset, event, or public space is a vital element to determine their effectiveness and robustness. It also highlights the training requirements of an organization for the protection of its asset. This adversarial testing is called Red Teaming yet can also be known as 'Penetration Testing' (pen test) or 'Red/Blue Teaming' and is carried out by a number of teams in as close to a 'real world' situation as possible by emulating environmental, legal/regulatory, operational and technology considerations in which a potential threat can occur; however, it is executed in a safe and controlled environment for all teams.

This section covers the teams, stages, and minimum requirements recommended for coordination and execution of an adversarial Red Teaming Operation.

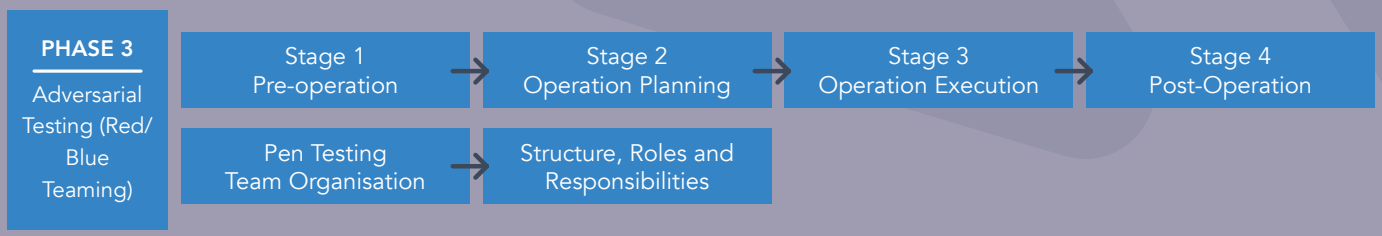

Figure 6: Protection Phase 3 – Adversarial Red Teaming Testing Overview

[2]*INTERPOL Drone Countermeasure - EINTERPOL 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*

10.1 Red Teaming coordination

A Red Teaming Operation consists of a series of teams, each executing specific tasks under roles of an attack operation, defence/mitigate, command, or observation. The use of a Red Teaming Operation to validate the operational procedures of an organization to drone threat incursions over an asset, event, or public space is a very valuable tool for all teams and stakeholders to determine capacity building.

The Red Team gains insights into the different strategies law enforcement may face when protecting a facility or event and how challenging this can be, which can then be passed to subsequent Red Teaming Operations and stakeholders as knowledge transfer. The Blue Team gains operational experience in responding to unknown drone threats. It can test their response, command and communication, and the strategic decisions required to combat unknown drone threats (i.e., their operational procedures).

Using an independent and experienced Red Team from outside the organisation ensures a fresh outlook on the drone threat dynamics and access to operational expertise and knowledge, which will sufficiently challenge the Blue Team through the strategic war-gaming scenarios and knowledge transfer for Blue Team capacity building. The internal organisation personnel who help build and train the Blue Team witness how using a neutral party, such as an external Red Team, to create controlled drone incursions based on parameters set out and understood by all helps create confidence and collaboration within the Blue Team during and post-operation.

An overview of the teams and actions is available below:

Table 11: Red Teaming Operation Teams

TEAM	ROLE
Red Team	Behave as the physical (in-field) threat actors and attack the asset(s) of interest. This team can be made up of participants external or internal to the organization. It is beneficial to have an external element to the composition of the Red Team to ensure neutrality and an unbiased appraisal of operational procedures to be tested.
Blue Team	Behave as the defenders of the asset. The Blue Team will operate the C-UAS technology if deployed over an asset.
White Team	Command team in the VOC. This team can work closely with the Blue Team as they are also a 'defending' team.
Purple Team*	Behave as the cyber threat actors. If this team is active, they can work together or independently to the Red Team as they attack an asset in a different way, however, coordination between the two attacking teams would be beneficial.
Observer Team	Observers can support all teams in providing unbiased observations and in-field support.

**The Purple Team will not be detailed further in this guide; it is represented in this table to show the wider scope of potential teams in a Red Teaming Operation*

10.2 Operation Team structures, roles & responsibilities

The structure of the individual operational teams can follow, at a minimum, a simple hierarchical format such as detailed below. For the minimum requirement of individual teams, see the following sections.

10.2.1 Red Team

The objective of the Red Team is to behave in-field, emulating physical threat actors attacking an asset or location using whatever platforms and devices in a planned deployment sequence, which will test the defence of the Blue Team as per the RoE, SecOps, CONOPS and SOP. The Red Team is normally a grouping of persons with a collection of specialised skills in war-gaming, GeoIntelligence, ISR, C-UAS Technology, drone piloting, etc., which act as a threat actor. The Red Team structure tends to follow the hierarchy below, at minimum and can be expanded as per operational requirements, such as two or three drone operators with corresponding observers being managed by the Red Team Commander.

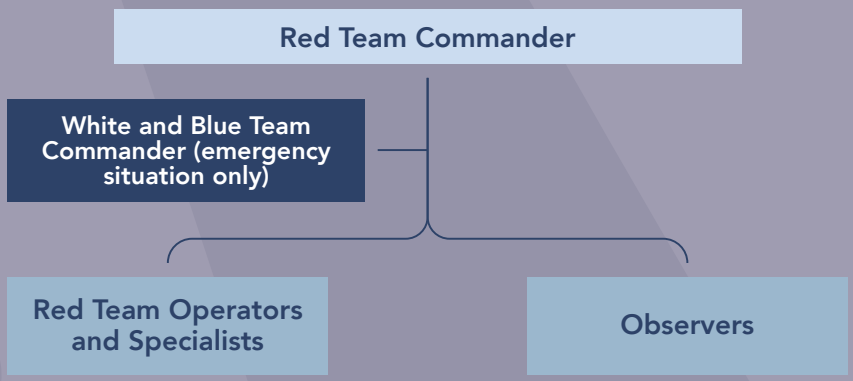

Figure 7: Red Team - Structure Overview

The roles and responsibilities of Red Team members is summarised in the below table:

Table 12: Red Team Roles And Responsibilities

TEAM	RESPONSIBILITY
Red Team Commander	The commander is responsible for the execution of the planned operations as per the RoE, SecOps, CONOPS and SOP. They are the contact point between the other teams within Red Teaming Operation and are the final decision maker within the Red Team on all procedural and safety matter.

Red Team Operators and Specialists	Red Team operators behave as attacking threat actors to attack the asset via multi-platforms and/or devices to achieve the goal of breaching Blue Team defences. These persons have specialised skills and knowledge of C-UAS technology (if applicable) over an asset, which can also allow for counting the C-UAS technology. Overall, the Red Team bring together several skills, which complement other team members to form a team that can play a 'malicious' role for a good purpose.
Observers	Observers can support team members in providing unbiased observations and in-field support by making notes and log time and date of any actions, communication and decisions that affect the exercise.

10.2.2 Blue Team

The objective of the Blue Team is to defend the asset of interest or location from Red Team attacks using all available technology, processes, and systems as stated within the RoE, SecOps, CONOPS, and SOP. During the Red Teaming Operation, the Red Team attack schedule and attack vectors should not be known to the Blue Team to ensure the test is as realistic as possible. By testing the Blue Team and other teams together, it builds confidence in the use of the C-UAS technology, increases knowledge of how a real attack can 'look and feel,' and provides valuable feedback on operational procedures, process improvement, and potential training needs. The Blue Team structure tends to follow the hierarchy below, at a minimum and can be expanded as per operational requirements. The Blue Team is generally the largest team of all Red Teaming Operation teams.

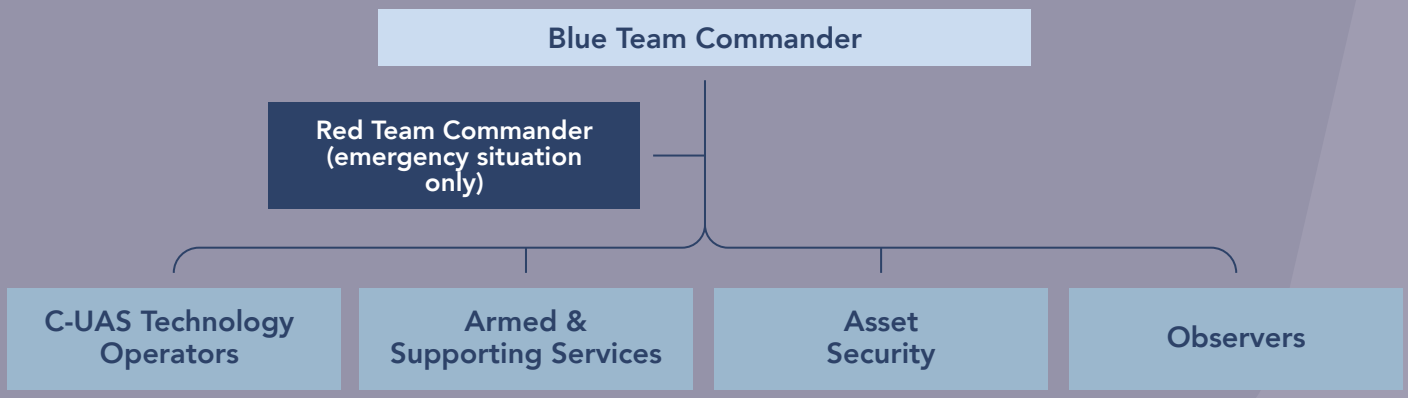

Figure 8: Blue Team - Structure Overview

The roles and responsibilities of Red Team members is summarised in the below table:

Table 13: Blue Team Roles And Responsibilities

TEAM	RESPONSIBILITY
Blue Team Commander	The commander is responsible for the execution of the planned operations as per the RoE, SecOps, CONOPS and SOP. They are the contact point between the other teams within Red Teaming Operation and are the final decision maker within the Blue Team.
C-UAS Technology Operators	The C-UAS operators use the C-UAS technology deployed over the asset to defend against the Red Team attacks using the technology as per manufacture standards.
Armed & Supporting Services	The Armed Forces may be deployed to support the protection and security of an event due to the scale and the skills required. These personnel can be a part of the Blue Team defence using specialised or C-UAS equipment.
Asset Security	The permanent security detail of the asset takes the role of defender with the Blue Team to ensure all security processes of the asset align, that they support the armed services, C-UAS technology operators and Commander.
Observers	Observers can support team members in providing unbiased observations and in-field support by making notes and log time and date of any actions, communication and decisions that affect the exercise.

10.2.3 White Team

The White Team is present in the Command Centre (VOC). The White team can act as a coordinator of the other defending teams in the field to ensure safety, and support towards the Blue Team defence execution.

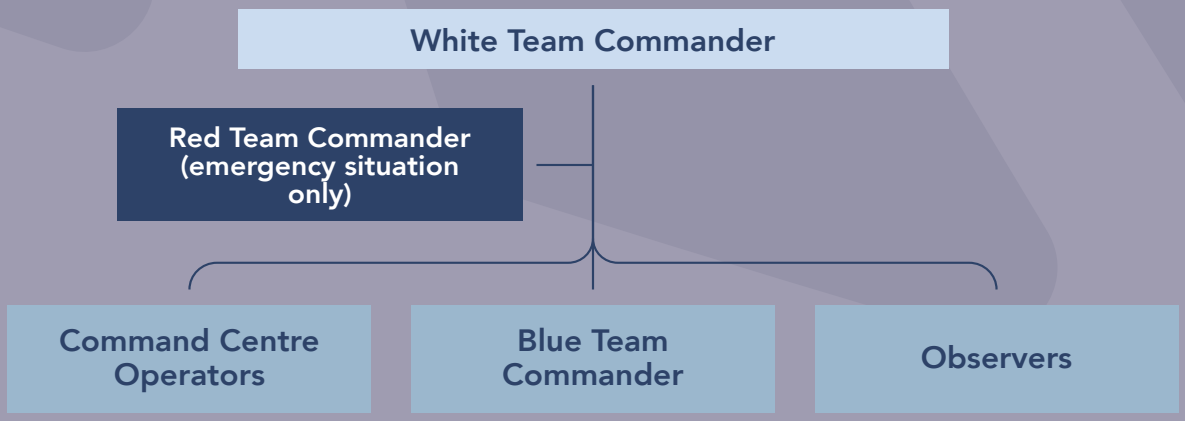

Figure 9: White Team - Structure Overview

The roles and responsibilities of White Team members is summarised in the below table:

Table 14: White Team Roles And Responsibilities

TEAM	RESPONSIBILITY
White Team Commander	Located out of the field in a control room, the commander is responsible for the coordination of the Blue, White, Purple and other Teams during the Red Teaming Operation. They are not responsible for managing the Red Team. They ensure all operations are as per the RoE, SecOps, CONOPS and SOP. They are the contact point between the other teams within the operation (Red Team in emergencies) and are the final decision maker within the White team.
Command Centre Operators	The operators man the desktops, which features IT structure, video surveillance and other avenues required to be fed into the VOC and use this information to support all teams in defending against the Red Team attacks.
Red Team Commander	Communication from the Red Team Commander to the White Team Commander only in emergency situations or breaches of RoE.
Blue Team Commander	Are in open and frequent communication with the White Team Commander to ensure team coordination.
Observers	Observers can support team members in providing unbiased observations such as decisions, communications, and interactions within the VOC noting the command-and-control chain; compare any actions against the SOPs and note any deviations or anomalies; make notes and log time and date of any actions, communication and decisions that affect the exercise.

10.3 Team interaction

Engagement can be divided into three stages: Pre-operation, Operation execution, and Post-operation. Inter-team engagement differs at each pen testing operation; for example, in the preoperative and postoperative stages all teams interact. During operation execution, the Red Team acts alone, and all other teams interact. It is important to note, for a successful pen test operation, the planned attack vectors and details of the Red Team should not be relayed to any other team. During the operation, Red Team communication should only be within the Red Team. For safety or other risk mitigation during the operations, the Red Team Commander will communicate with the Commanders of the Blue and White teams.

11.Red Teaming Operation Planning Stage

Adversarial Red Teaming testing can be broken down into four different stages: pre-operational, planning, execution and post-operational.

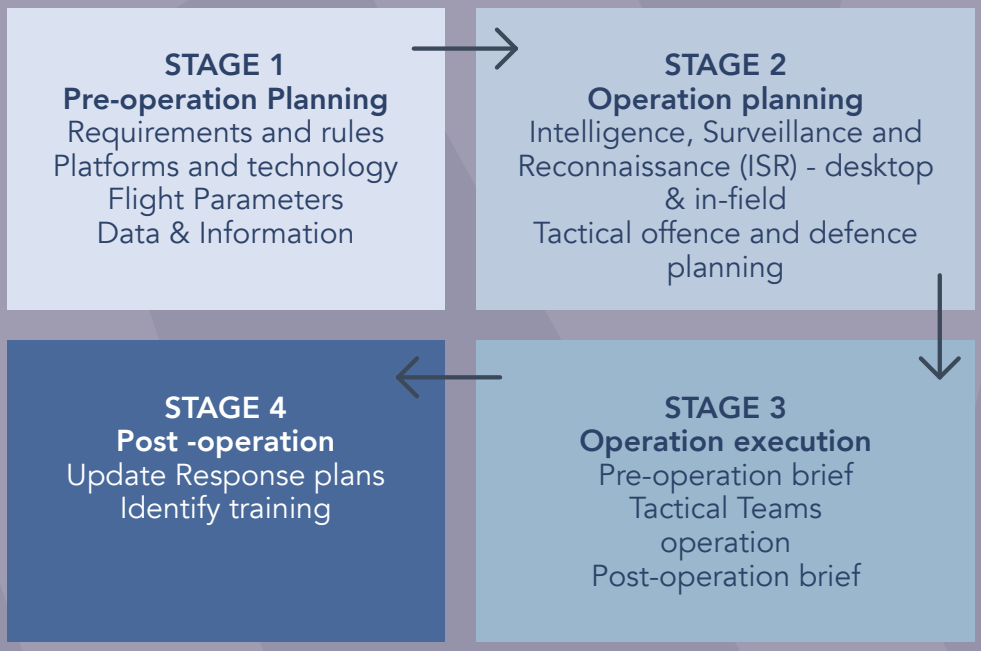

Figure 10: Red Teaming Operation Stages

11.1. Red Teaming Stage 1: Pre-Operation Planning

Throughout the planning and execution of a pen test operation, it is crucial to ensure that all operational stakeholders clearly define the planning, operation objectives and goals, operational processes, and flight parameters. Taking time for this stage will ensure a clear understanding for all stakeholders and a safer environment for execution.

To start, it is important to discuss and clearly outline the objectives of the Red Teaming Operation from the point of view of the end client, the Red Team, the Blue Team, and other supporting stakeholders. If required, any general process or operational procedures should be updated in Section 4. Additionally, exercise and operational objectives should be very clear as this can influence how the Red Team will plan their engagement and war-gaming scenarios during the Red Teaming Operation.

11.1.1 Rules of Engagement (RoE)

Once objectives are defined for all teams and stakeholders, the Rules of Engagement (RoE) operational procedure for the operation can be written. The RoE document is crucial for outlining the objectives, stakeholders, team roles, technology and equipment, and safety protocols for all teams engaging in pen test exercises.

Particular attention should be paid to the definition of engagement between the Red Team and the Blue Team (and others as required), both as individual teams and their engagement together.

In the RoE, the recommended minimum requirements to address in the operational procedure are listed below:

Table 15: Rules of Engagement (RoE) Parameters

RoE ELEMENTS	DESCRIPTION
Objectives	What are the key objectives of the Red Teaming Operation? Why is the operation being planned? What are the expected goals?
Target audience	For whom is the operation being carried out and why?
Stakeholders	Who are the other stakeholders, internal and external to the organization who have a role within the RoE?
Roles and responsibilities	The roles and responsibilities of those stakeholders who will be active in the operations should be clearly defined. Having a clear understanding of roles and responsibilities will support a safe operation execution and overall environment of the exercise.
Levels of engagement	The level and type of engagement between all stakeholders (Red, Blue, White Teams, Communications, and LEAs etc.) are clearly defined for all potential scenarios and expected goals.
Timeline of engagement	Plan when, and for how long the operation 'window' of the operation will be carried out. This is the amount of time that the Red Team Operation will be 'open'. It is important to note that the window can be from a few hours to a few weeks and the Red Team is not required to be active all the time within this window; only during the scenarios. Knowing the flight window information can be used for determining the NFZ, UAS platforms and engagement method enacted by the Red Team in Stage 2 of the Red Teaming Operation when planning war-gaming scenarios.
Flight parameters	For each operation the flight parameters, flight volumes (the altitude, length and breadth within which the drone can only fly), which will be used during the Red Teaming Operation need to be determined and approved by the relevant authorities. Throughout the operations, these parameters must not intentionally be breached and if so, a safety protocol must be in place for the safe return of the drone to home (RTH).
No-Fly-Zone (NFZ)	When the flight parameters are finalised, a clear NFZ for the operation is established. This volume can be presented to the CAA for approval to ensure the airspace of the operation is blocked to third party drones (i.e., no pen-test platforms).

Red Amber Green (RAG) threat levels	The RAG is an important element of the SecOps and aids the Red Team to determine their attack vectors to give greatest impact to the defending teams.
Platform requirements	Each platform to be used in the pen test by the Red Team will be determined in the operation planning stage and does not need to be disclosed to other teams. This ensures a good, realistic testing environment. It is recommended that each platform chosen has all safety mechanisms activated, at minimum, RTH: in case the drone is neutralised, it will safely RTH.
Confidence operation engagement	The Red Teaming Operations can have elements of education and confidence building exercises in the war-gaming scenarios enacted by the Red Team for the benefit of the Blue Team. These carefully planned elements can give the Blue Team confidence in their processes, equipment use, and operations procedures. As such, different engagement protocols in the RoE depending on the nature of the scenario being enacted. For example, an education element for the Blue Team to build confidence in their technology - if a drone is neutralised and it is released to safely RTH, compared to an educational element such as, the drone is neutralised, and the Blue Team must completely remove the threat (i.e., take the drone from the sky in all manners possible regardless of collateral).
Tactical operation engagement	This avenue of engagement between the Red and the Blue Team is very tactical and may have collateral outcomes for both teams as it will emulate the real-world neutralisation of a drone threat. Collateral outcomes can mean the loss of a platform or the Red Team breaching the Blue Team defences. As such, the risks and mitigation for potential collateral damage should be discussed, understood, and accounted for in the operation.
Operation terminology	Set up a clear use of terminology and protocol for communications between and within teams. Protocols for communicating on radios, call signs, code words and safety words should be used when needed. To aid in a standardised terminology for C-UAS, see the Glossary in Annex 1 and the tables within this guide.
Safety measures	Any operation can have unexpected outcomes. Therefore, it is important to add clear safety protocols into the RoE for aborted flights, collateral damage, danger to personnel, etc., which define a process to follow if any of the main identified risks to operations in the RoE are present. Code words or pre-determined terminology can support these actions.
Reporting protocol	During the operation, there will be many communications in action within teams and between teams. It is recommended to have a reporting protocol between team members and how the Team Commanders will report to each other during the exercise. This includes the Red Team Commander as, for safety reasons, should maintain a communications link to the White Team Commander to use if required. This reporting protocol can be linked to the recommendation on defining standardised terminology for successful operations.

11.1.2 Operations Handbook

Developing an Operations Handbook tailored to support a Red Teaming Operation is highly recommended. This valuable resource serves as a comprehensive guide, encapsulating vital operational procedures, established standards, and agreed-upon terminology for the Red Team throughout the operation, particularly during radio communications. Each participating team is advised to have a customized, concise Operations Handbook to streamline their respective roles and responsibilities.

The Operations Handbook should encompass pertinent details such as the pen testing scenarios to be executed, timeframes, equipment, team compositions, individual roles and responsibilities, and the location of team members for enacting specific scenarios, such as flying the attack vectors. Additionally, the handbook should provide a standardized terminology for efficient communication during operations and across radio channels, and essential safety procedures. Table 16 outlines the minimum elements to incorporate into an Operations Handbook. It is crucial to note that the term «Red Team» can be replaced with the appropriate team's name, and organizations are encouraged to augment the handbook with any further relevant elements based on their unique situational requirements.

Table 16: Operational Handbook Parameters

OPERATIONAL HANDBOOK ELEMENTS	DESCRIPTION
Objectives	List the key objectives of the Red Teaming Operation followed by the particular objectives of the Red Team, i.e., why is the operation being planned? What are the goals of the Red Team which is satisfying the stakeholder etc.?
Pen testing scenarios	Details of the site of operation, the scenarios to be enacted (very detailed with a timeline in minutes), the platforms or equipment to be used and by which team member.
Operation Timeline	A detailed timeline of each scenario should be developed to show which Red Team member carries out what operation, when and with what platform/ equipment. This is important for all to understand the order of operation and the order in which each scenario is being enacted.
Timeline of engagement	Indicate the 'window' of the operation. This is a timespan within which the Red Teaming Operation will be enacted, at any time chosen by the Red Team, without the knowledge of the Blue Team. The window is normally longer than the scenarios to ensure the 'surprise element' for the Blue Team and allow the scenario to be as realistic and unpredictable as possible.
Operation Parameters	This will include the flight volume of the operation (i.e., the maximum height, width and length the drone can be flown in and is normally approved by the country CAA), frequencies (2.4hz, 5.8hz), hard barriers (i.e., if the Red Team successfully penetrates the defences, the drone can only be flown a maximum of 50m from the stadium), RTH (return to home protocols), and any NFZ etc. These operational parameters are tangible.

Roles and responsibilities	The roles and responsibilities of Red Team members (Commander, Drone Operator etc.), their roles within the scenarios, who will be active in the operations must be clearly defined. All tasks and expectations are to be made clear and any milestones or deadlines to meet are all to be described to make sure all team members understand their role and objectives.
Red Team terminology	To ensure clear and neutral communication, it is important to set out the standard of terminology, call signs and other radio or communication protocols to be followed before, during and post Red Teaming Operation. This is critical as certain operations may require secure communications where team members are not identifiable and communicate under a call sign.
Safety measures	State the safety protocols (found in the RoE) that the Red Team must follow, for example, aborted flights, collateral damage, danger to personnel, etc. Code words from the terminology can support this measure for actions related to RTH, neutralisation protocol from the Blue Team etc.
Reporting protocol	During the operation, there will be many communications in action within teams and between teams. It is recommended to have a reporting protocol between team members and how the Team Commanders will report to each other during the exercise.

11.2 Red Teaming Stage 2: Operation Planning

When all 'desktop' evaluations and planning parameters for the operation have been completed in Red Teaming Stage 1 (Section 11.1), it is time to turn to the 'physical' planning of the operation by collecting relevant information from Intelligence, Surveillance, and Reconnaissance (ISR). The Red Team generally carries this out to aid their decision-making in finalising the war-gaming scenarios, which include which drone platforms to use, what attack vectors to fly and under what flight conditions (night/day/frequencies/altitudes etc.), attack timelines, and order of Red Team flying attacks. The Table below is targeted to the operational elements of the Red Team, yet similar elements can be determined for the other teams and are detailed below in 'Other Team operational elements' (See Table 18).

Table 17: Red Team Operational Elements

RED TEAM OPERATIONAL ELEMENTS	DESCRIPTION
Intelligence, Surveillance and Reconnaissance (ISR)	This element forms a desktop and physical gathering (actual site visit) of information, which will aid the Red Team in planning their attack vectors and operational requirements.
Site visits	To complement any desktop ISR, it is important to carry out in-field reconnaissance to confirm or discard any assumptions made from desktop works and to identify new information, which may not have been visible until a site visit. The site visits are vital to visually determine potential threat areas.

Gather Open-Source Intelligence (OSINT) & sensitive information	It is important to gather all lawfully available data over the area of interest, which is online, open, or sensitive data provided from the end client or even the Dark Web. The availability of data can impact the risks of particular threat actors and should be emulated as closely as possible to find gaps in information flow and fill them.
Platforms and technology	Once the ISR is completed (desktop and in-field), the Red Team can confidently determine the best platforms and supporting technology for the proposed attack vectors and operation objectives.
War-gaming scenarios (aka attack vectors)	The final stage is to plan the attack vectors, taking into consideration all elements of the RoE, ISR, and platforms and technology for the Red Team. The scenarios or attack vectors are the flights the Red Team will enact, for example, fly at 30m, full speed around the stadium with a racing drone to test close proximity detection and neutralisation capability of the Blue Team.
Review	It is important to review all elements of operational activities with regular briefings and reviews with stakeholders.

Each tactical team has varying roles and responsibilities, therefore below are elements for defensive (non-Red Team) operational teams to consider.

Table 18: Other Team Operational Elements

OTHER TEAM OPERATIONAL ELEMENTS	DESCRIPTION
Intelligence, Surveillance and Reconnaissance (ISR)	This element forms a desktop and physical gathering (actual site visit) of information, which will aid the Red Team in planning their attack vectors and operational requirements.
Site visits	To complement any desktop ISR, it is important to carry out in-field reconnaissance to confirm or discard any assumptions made from desktop works and to identify new information, which may not have been visible until a site visit. The site visits are vital to visually determine potential threat areas.
C-UAS technology	Once the ISR is completed (desktop and in-field), the other teams can confidently determine the best ways to defend potential attacks using the technology available.
Defence Strategy	All defending teams can work together to define a defence strategy taking into consideration all the ISR, C-UAS technology installed and their own assessment of potential areas of high risk from threat attacks.

11.3 Red Teaming Stage 3: Operation Execution

A Red Teaming Operation is not merely arriving at a site and flying; the planning and preparation before the actual operation is large and needs to be. When the operation is ready to be enacted, i.e., the war-gaming scenarios will be enacted, there are a number of steps to follow, which are highlighted in this section.

11.3.1 Pre-operation brief

Briefings are an important element for relaying information and keeping communications open. For events such as a Red Teaming Operation, being certain of correct information exchange and clear communications can impact the overall success of how the operation is enacted. To aid communication and clarity, it is recommended to hold briefings.

A Group Briefing: on the day of each operation, it is important for each Team to have a group briefing on expectations of the day, the operations and safety. It is also a time where members of the team can ask questions etc. This briefing can be with all teams and can cover the main element of the RoE, safety, and the time windows of the operations before each individual team breaks off for their own individual brief to focus on each Team requirements (Table 19). Suggestions of the type of briefing and what elements to cover within a briefing are below:

Table 19: Pre-Operational briefing elements - All Teams

BRIEFING ELEMENTS	DESCRIPTION
Rules of Engagement (RoE)	The RoE are clearly outlined for the operation.
Operation timeframe	The operation will take place within a predefined window where the individual teams will execute their offence or defence. The operation window should be clearly defined so that all teams are aligned on operational hours.
Safety protocol	All teams are briefed on safety measures during the operation, from site safety requirements, operation safety and other environmental safety considerations.
Debrief time	All teams return from their positions post-operation for an all-team debrief. Here, elements of the operation such as challenges, success and improvements can be discussed and addressed or implemented in the next operation.

Individual Team Brief: during the individual team brief, it is important to cover what each team member will be doing, when, where and with what equipment, safety, and terminology:

Table 20: Pre-Operational briefing elements - Individual Teams

BRIEFING ELEMENTS	DESCRIPTION
Rules of Engagement (RoE)	Clearly restate the RoE for the operation. This will entail some of the elements listed below; however, we highlight some main points.
Attack and defence positions	For each team, clearly define Red Team attack vectors, locations and goals and for the defence (Blue, White teams) strategy, positions, and scenario defences.

Platforms and C-UAS technology	All equipment to be used within the operation, be it Red or Blue Teams, need to be clearly defined: what, where, by whom and when. It is recommended to have a table of equipment, roles, and responsibilities against the location of deployment at a timeframe for execution (Red Team attacks) or defence (Blue Team) goals.
Safety protocols	Within each team there will be different exposure to risks, as such, it is important to have safety measures in place and well understood by all members. These elements will cover technical or platform issues (defaults, crashes, public harm, etc.), breaches of the RoE (operation outside of exercise parameters, etc.), personal emergencies or other elements, which are situationally relevant.

11.3.2 Red Teaming Operation

When the window for the operation is active, all teams are deployed as per their team operation plans (War-gaming scenarios), keeping within the RoE. During operations, teams need to adhere to their operation plans, timeframes, and offence/defence strategy as closely as possible. It is crucial to always keep communications clear and open within teams and between Team Commanders as required. This ensures that individuals within the teams deployed to various locations can execute their roles to the best of their ability and within all safety protocols. Regardless of plans, not everything is precise, accurate, and on time in the field; therefore, agile changes within RoE should be expected.

The operational goal is to ensure that the Red and Defence Teams (Blue, White) can enact their roles in the most realistic manner possible. By doing this, each team will have the greatest training and learning experiences, solidifying their confidence, and testing their operational procedures and overall defence precision of the asset or location. The goal is not to 'cut corners' but make it real for all teams and the end client to benefit from the experience.

11.3.3 Post-operation debrief

Once the operation has officially ceased, it is important for all teams and the end-client to hold a debriefing to gather all team feedback on their operations. As with the briefings, the debriefings can be a series of separate meetings which target particular stakeholders to be sure to address requirements. For example, a post-operation debrief can take the form of a small meeting with the operation teams (together and individually) after each day's operations.

If a multi-day operation schedule is in place, the smaller, single team debriefings should be daily, followed by an all-team and client debriefing once all operations have been executed and the operation window is closed. Feedback should include, at a minimum, all outcomes, challenges, equipment, and process elements:

Table 21: Post-Operational debrief elements

BRIEFING ELEMENTS	
Successful outcomes	Actions of success should be stated for the entire operation and for all teams. This can be successes, which contributed towards the entire operation goals, or within team success.
Challenges and improvements	It is important to gather from all teams what needs to be improved or did not work. These elements are crucial for improving the operational processes and protocols of the end-client and for the overall defence quality of the asset.
Equipment	Equipment can behave in many unknown and surprising ways when in the field. To improve and learn, all feedback from teams on their equipment, both technical and platforms (success, failures, vulnerabilities, etc.) should be gathered.
Processes	Within the operation, many processes are enacted in as many real scenarios as possible, which exposes solidity or areas for improvement of the processes and protocols. Each team can give valuable feedback on how these either work or can be improved within the debriefing. This can also highlight themes presented by the teams who may require further meetings to gain more details with the goal to update processes and protocols.
Safety	Safety during an operation is paramount yet can be unpredictable. Gather all feedback on any elements from all teams, which highlight success or improvements for safety processes or during operations.
Confidentiality	Depending on the operation and end-client requirements, it may be necessary to remind all teams who participated to the operation of any confidentiality requirements (i.e., gagging on social media, public domain, etc.) and how to deal with sensitive information from the operations.

11.4 Red Teaming Stage 4: Post-operation

This section focuses on the end client or beneficiary of the operation. Once the operation has been completed and all teams departed, the information gathered from the debriefings can be used to update any operational procedures or technology as required. There may also be clear indications for areas of improvement, which the remaining security personnel of an asset or location may benefit from as a result of the operation.

It is recommended that if operational procedure updates and/or training are carried out post-operation, these be re-tested in another Red Team Operation to clarify for the organisations and Blue Team that the updated practices of the new standards and new training have closed any gaps and are more effective. This develops a healthy cycle of testing all parameters as close to a real scenario as possible, ensuring the asset, event or public space defence is always at is strongest and the personnel at their most confident and strongest to defend.

12.Protection Phase 3: Recommendations

Operational – All teams

- Seize the opportunity of major events to **carry out national-level security exercises** that have far-reaching benefits.
- **Carry out different types of exercises** and scenarios from national to local and from generic to specific.
- **Operations handbook** – a short, concise handbook specific to each team could be distributed detailing the scenarios to be played, timeframes, equipment, teams, locations, etc. It could also contain common vocabulary to be used during operations and across radio communications.
- **Define Training and Tactical RoE as separate SOPs** – It is recommended to run both training and tactical Red Teaming scenario operations as the collateral impact will be different for both and also how they are executed.
- **Standardised vocabulary** – a set of known and pre-agreed terminology should be created and used for simple communication such as 'drone power off,' 'land drone,' 'prepare to take off'. Also, establish terminology for communication across the radio. This should be added to the aforementioned operations handbook (See Annex 1 Glossary).

    - **Collaboration:** All stakeholders involved in C-UAS operations, including aviation authorities, law enforcement agencies, and defence organizations, should collaborate to establish a common understanding of the terminology used in the field. This can be achieved through regular meetings, workshops, and training sessions, where representatives from different organizations can come together to discuss and agree on standardized terminology.
    - **Standardization Bodies:** International standardization bodies such as the International Civil Aviation Organization (ICAO) and the European Union Aviation Safety Agency (EASA) can play a crucial role in promoting the adoption of standardized terminology within the C-UAS domain. These bodies can develop guidelines and best practices for terminology usage and promote their adoption through their member states.
    - **Training and Education:** To ensure the standardization of terminology is adopted, all individuals involved in C-UAS operations must receive adequate training and education. This can include online courses,

seminars, and in-person training programs. Training programs should be tailored to the needs of different stakeholders, ensuring that each group understands the terminology specific to their area of work.

- **Ongoing Review:** Standardization of terminology is an ongoing process, and it is essential to periodically review and update the established standards to ensure they remain relevant and effective. Stakeholders should regularly review their usage of standardized terminology to identify any areas for improvement and adjust their practices accordingly.

- **Radio sets** – radio sets should be given to all persons who are controlling or observing a pilot/drone operator in the Red Team or to a person who has the ability to communicate with the Red Team drone pilot. It is important that the person with the radio set communicates clearly over the radio and with the remainder of the team wherever they are stationed.
- Consider **extending Red Teaming to areas around the asset of interest**, such as: ports, entry borders, and stadium entry ports, including the use of deployed open-source intelligence using the Red Team Persona, the authorised attempt to import a drone, and the authorised attempt to gain entry to stadia and facilities with drones.
- **Red, Amber, and Green (RAG) Grid maps** using appropriate grid squares should be developed for each venue/asset/location.
- **Friendly Drone flight logbook:** Exercises can be 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.
- **Gather all operational team feedback on the exercise from the debriefings** to highlight areas for each team of success, improvements, and non-functional elements to incorporate into subsequent operations and procedures.
- **Cross-check all operations logs from offensive and defensive teams to correlate against deployed C-UAS technology** to understand clearly what the technology did and did not neutralise and why.

Operational: Red Team

- Red Team: It is advised that a Red Team **re-test defining more focused operations objectives which target the areas, operational procedures, or technology which was updated as a result of the first Red Teaming Operation (i.e., with limitations to the RoE), with re-testing operations run two weeks (minimum) before the start of an event.**

Operational: Blue Team

- Blue Team: **Decision to Neutralis**e - It is advised that the decision to neutralise is provided via the shortened command chain as possible. A drone attacking at speed needs to be neutralised, and delays of seconds allow a threat to get closer to an asset or to complete their mission.
- Blue Team: **Weekly training and drill**s for all C-UAS Technology Operators and Technical Officers running up to the event start will enable the maintenance of skills requirements to a high level.
- Encourage all teams (Blue, White) to **think like a threat acto**r. It will help the team to understand how to defend better.

13.Protection Phase 4: Training

Keeping personnel responsible for the defence of an asset, event, or public space from potential threats in operational readiness requires regular training exercises. Regular training and frequent Red Team Operation re-testing will ensure personnel is, and remain, confident in all operating procedures, technology use, and response protocols.

PHASE 4 Training	Training recommendations & guidance

Figure 11: Protection Phase 4 - Training overview

Through regular Red Teaming Operations (i.e., adversarial testing, Red/Blue Teaming), asset or location defences will be tested, and any identified and mitigated against to ensure that if a real threat arises, all personnel, operational procedures are as honed and streamlined as possible for efficient and confident threat neutralisation.

Training needs are also identified when carrying out the Learning Needs Analysis (LNA). Through the LNA and the Red Teaming operations, organisations can identify what are the needs of their personnel to keep skilled and confident in their working capacity, with the equipment they use and the operational procedures they need to follow. Training and Red Teaming operations can also help build team morale and confidence and individual confidence in performing their professional role well.

It is highly recommended that organisations take the time to understand their personnel's training needs and to carry out regular training, in-field, and desktop, to ensure their 'team' is functioning at its highest capacity. Below are a series of recommendations for team and operational procedure optimisation. How these are to be carried out is at the discretion of the organisation or following their existing training protocols.

14.Protection Phase 4: Recommendations

- The **Red Teaming Operation (adversarial testing) will identify what training an organisation should continue** regularly to ensure all C-UAS teams have the confidence to deploy technology, enact operational procedures, and confidently neutralise drone incidents at any given time.
- During Red Teaming Operations, the **strengths and weaknesses of the CONOPS will be exposed**. As such, highlighting the areas where all personnel within a process should focus on regular training to maintain quick response times, active and accurate decision-making responses, and overall, a smooth operational process as a team is important for stronger asset protection and defence.
- **It is suggested to perform multi-operational training for all the teams within an SOP.** There is a need for training (confidence building for the Blue Team) and tactical (full kill-chain testing) Red Teaming Operations. As such it is recommended to run both training and tactical Red Teaming Operations. This will allow the Blue Team to practice tactical testing, for example, the full 'kill-chain' which can demonstrate complete removal of a drone threat (i.e. physically bringing the drone down) thus allowing the Red Team to prepare the correct, expendable equipment for such an operation (i.e. expected collateral damage) and confidence building – for example, the Red Team will select a series of war-gaming scenarios which will allow the Blue Team to neutralise a drone and learn confidence in how to use the technology for such a task.
- **Continually gather operational feedback from all teams** to identify challenging elements and appropriate actions and training to be carried out on a regular cycle.

Annex 1: 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
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference

ABBREVIATION	DEFINITION
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

Annex 2: 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 3: 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)

List of Tables

Table of Figures

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) (Annex 2). 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