`

United Nations
Department of Operational Support /
Department of Peace Operations
Ref. 2025.16

Guidelines

Counter Unmanned Aircraft Systems

Approved by:	Atul Khare, USG DOS Jean-Pierre Lacroix, USG DPO
Effective date:	*1 July 2025*
Contact:	OMA/Military Planning Service
Review date:	June 2030

Members of the Counter Unmanned Aircraft Systems Guidelines writing workshop Stans, Switzerland, February 2025

Serial	Rank	Name	Nationality / Entity
1	Captain	Rodrigo Sande Souza	Brazil
2	Lieutenant Colonel	Rodrigue Boris Foming	Cameroon
3	Lieutenant Colonel	Jérémy Gueye	France
4	Major	Karim Waheed Ali Almakhadmeh	Jordan
5	Lieutenant Colonel	Youseff Melyani	Morocco
6	Major	Muhammad Abrar	Pakistan
7	Lieutenant	Ivan Rwagasana	Rwanda
8	Captain	Majed Alzahrani	Saudi Arabia
9	Lieutenant Colonel	Pieter Bosch	South Africa
10	Wing Commander	Praneeth Sameera Kodikara	Sri Lanka
11	Lieutenant Colonel	André Comps	Switzerland
12	Staff Warrant Officer	Maximiliaan Vermaat	Switzerland

Serial	Rank	Name	Nationality / Entity
13	Ms.	Patricia Hörmann	Switzerland
14	Colonel	Jamal Alhosani	United Arab Emirates
15	Lieutenant Colonel	Tiffany Frankland	United Kingdom
16	Colonel	Patrick Allen	United Kingdom - United Nations Peacekeeping Force in Cyprus (UNFICYP)
17	Major	John Rice	Canada - United Nations Peacekeeping Force in Cyprus (UNFICYP)
18	Lieutenant Colonel	Muhammad Zubair Cheema	Pakistan - United Nations Interim Security Force for Abyei (UNISFA)
19	Lieutenant Colonel	Matthew Parsons	United States - United Nations Mission in South Sudan (UNMISS)
20	Lieutenant Colonel	André Cardoso Moura	Brazil - United Nations Multidimensional Integrated Stabilization Mission in the Central African Republic (MINUSCA)
21	Lieutenant Colonel	Andrew John McGrane	United Kingdom - United Nations Organization Stabilization Mission in the Democratic Republic of the Congo (MONUSCO)
22	Lieutenant Colonel	Ridwan Abdul	Indonesia - Office of Military Affairs (OMA)
23	Lieutenant Colonel	Dorra Chehata	Tunisia - Office of Military Affairs (OMA)
24	Colonel	Leigh Crawford	Australia - Office for the Peacekeeping Strategic Partnership (OPSP)
25	Major	Brian Cowick	United States - United Nations Mine Action Service (UNMAS)
26	Wing Commander	Nicholas Barratt	United Kingdom - Office of Military Affairs (OMA)
27	Mr.	Miguel Lens Pardo	Spain - Office of Supply Chain Management (OSCM)
28	Mr.	Arturo Ojeda Demaria	Chile - United Nations Global Support Centre (UNGSC)

DPO/DOS GUIDELINES ON COUNTER UNMANNED AIRCRAFT SYSTEM

Contents:

A. Purpose and Rationale
B. Scope
C. Guidelines
D. Roles and Responsibilities
E. References
F. Contact
G. History

ANNEXURES

A. Counter UAS Threat Analysis: Step-by-Step Process

B. C-UAS Report Template

A. PURPOSE AND RATIONALE

This document outlines United Nations guidelines for the development and use of Counter Unmanned Aircraft Systems (C-UAS) in field missions. It aims to ensure a standardized approach to managing and integrating C-UAS technology to enhance the safety, security of UN personnel and assets and effectiveness of UN operations. By providing UN-recognized terminology and key deployment considerations, the guidelines support military planners, force generation teams, and operators in implementing cohesive and mission-specific C-UAS strategies.

B. SCOPE

These guidelines apply to United Nations Headquarters (UNHQ) staff, military commanders, staff officers and United Nations personnel in Field Missions. They are intended to provide an overview of the considerations when generating C-UAS capabilities to support UN missions.

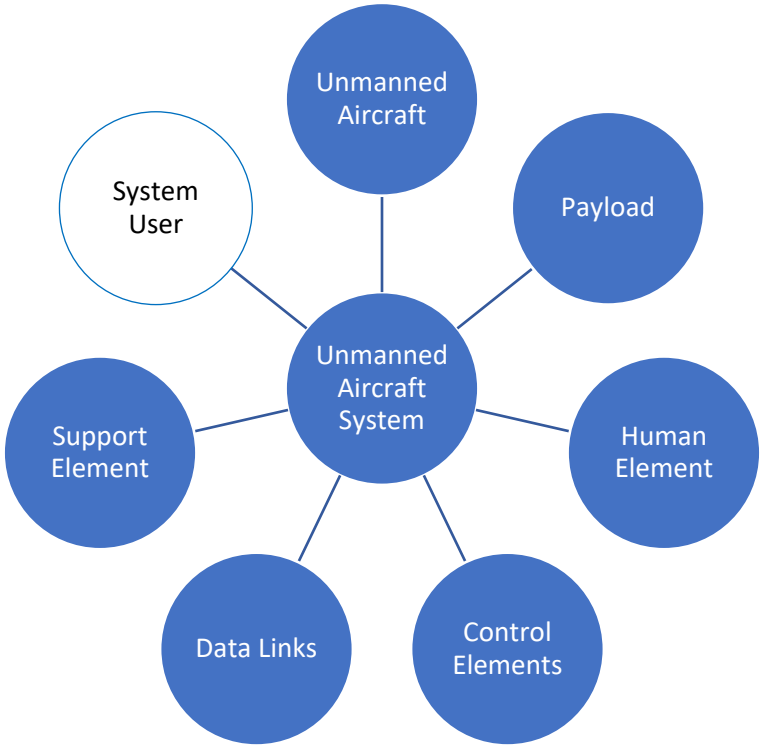
C. GUIDELINES

1. Background

The UN defines an Unmanned[1] Aircraft as “an aircraft that does not carry a human operator and is operated remotely using varying levels of automated functions, is normally recoverable and can

[1] Much of the existing UN documentation on this subject uses the term “Unmanned”, which is still the current term used by the International Civil Aviation Organization (ICAO). Increasingly, the gender-neutral term “Uncrewed” is being adopted by various entities. These terms are to be regarded as wholly interchangeable for the purposes of these Guidelines and their relation to other documents.

carry a different number and types of payloads"; an Unmanned Aircraft System (UAS), meanwhile, is "a system whose components include the unmanned aircraft, the supporting network and all equipment and personnel necessary to control the unmanned aircraft".[2]



The employment of UAS is far from being a new phenomenon, though as with all technologies the rate of evolution, capability, and reduction in cost is noteworthy. UAS have been a mainstay of many state militaries for years, and their adoption by Non-State Armed Groups (NSAGs) has also been widespread for some time. Given the environments into which the UN is required to deploy there is a high probability that UAS operated by states, NSAGs, or both will be present in a UN mission's area of operations.

State use of UAS – that is, UAS operated by or on behalf of the ruling authority within a country – can span the civilian, police, military and other sectors.[3] The size and variety of UAS may also cover a broad spectrum, ranging from short-range micro/mini systems used by military, civil authorities or police, up to large and capable systems operated by the military which carry advanced observation sensors and purpose-designed munitions. UAS can be used in a variety of roles, but as a general rule the larger the UAS the greater scope there is for load, capability and range. UAS are often considered a valuable asset for states to obtain. In the environments where the UN typically operates, it's common to encounter state-operated systems from various manufacturing countries and regions.

[2] See: DOS Aviation Manual, February 2021, Page 100.

[3] For the purposes of these Guidelines, UAS operated by Private Military Companies or other bilateral security partners of a host state are considered in the same category as state UAS.

NSAG use of UAS also exists on a broad spectrum. Relatively large and capable UAS requiring significant third-party support or advanced technical knowledge have been employed by groups such as the Houthis in Yemen, Hamas in Gaza, and Hizbullah in Lebanon to project explosive payloads accurately across long distances. At the lower end of the scale, a number of NSAGs have adopted the use of small commercial UAS either to conduct observation activities or, when subjected to relatively basic modifications, to deliver kinetic effects; terrorist groups such as Islamic State of the Iraq and the Levant (ISIL, hereafter "Da'esh") have increasingly employed UAS in numerous contexts. Use of all sizes and capabilities of UAS to conduct smuggling of narcotics and other illicit payloads has been noted by organized crime actors around the world, while concerns regarding use of UAS in dense urban environments is a particular concern in many Western countries facing domestic and international terrorist threats. In current UN operating environments, NSAG-operated UAS present an unpredictable threat due to their flexibility of employment and the variable levels of technical expertise and intent different NSAGs will have to modify and employ these systems against the UN.

Case study: UAS attack in MONUSCO

On 12 February 2024 a UN blocking position at Kimoka, approximately 22km west of Goma in the Democratic Republic of the Congo, came under attack from armed elements. In addition to various other weapons systems that were employed against the UN troops, a total of eight UAS were used to deliver explosive payloads.

The UAS were launched and operated from a location approximately 3.5km from the UN position and each were modified to carry an explosive charge. Six of the eight UAS successfully detonated against the UN position, with one of the two unsuccessful UAS being captured.

Examination of the captured UAS determined that it was a commercially available model designed to be flown using First Person View, which appears to have helped the operators launch the UAS from outside direct line of sight of the UN position and still navigate precisely to their target. The maximum range of the model of UAS used was approximately 18km and it was equipped with an external camera mount that had instead been modified to carry the explosive charge.

Within this broad global context, UN peacekeeping personnel and facilities have been relatively unaffected by the UAS threat until fairly recently. Presence and observation of unidentified UAS over or near UN positions have been observed for several years, especially in missions in Africa, but it was not until 2024 that the UN reported the first confirmed kinetic attack against its personnel from UAS.

The attack in MONUSCO highlighted factors that make use of UAS, and commercially available UAS in particular, an attractive prospect to NSAGs:

a. **Low cost.** The most readily available commercial UAS (colloquially referred to as "hobby drones") are inexpensive, with very basic models costing under $100 USD. Even more capable commercial UAS cost relatively little and are likely to be well within the financial reach of most established NSAGs.

b. **Ease of acquisition.** Unlike conventional weapons systems, commercial UAS are generally not subject to international counter-proliferation controls and are freely available for purchase in most countries. Some countries do attempt to restrict the importation of UAS, but this will be of little concern to NSAGs or other illegal actors who are likely to rely on illicit supply routes.

c. **Ease of operation.** Commercial UAS, especially those designed primarily for the civilian hobby market, are increasingly user-friendly and are generally designed to be easily operated by anyone with basic smartphone/tablet skills. The technical barrier to entry to field a basic UAS capability is therefore notably low compared to the effect they offer.

d. **Flexibility.** The simple design of most commercial UAS tends to make them relatively easy to modify for use in a variety of roles. For example, many of the more capable "hobby" UAS will feature pre-installed rails or hardpoints to allow the operator to attach better camera systems. Such features can be easily used instead to attach small explosive charges or other items, as seen in the MONUSCO incident detailed above.

e. **Operational advantage.** As a result of the above factors, hostile use of UAS represents a potent threat due primarily to the levelling of the technical playing field that they allow. A hostile actor acquiring a relatively basic UAS has the ability to conduct aerial surveillance and – potentially – precision kinetic attacks at range. These capabilities, once exclusive to state militaries, are now accessible to any hostile actor with minimal funds and basic technical skills.

2. Threat Assessment

2.1. Types of UAS Threats.

The threat posed by a UAS can be regarded as defined by three inter-related factors: the type and capability of the UAS in question; the operator of the UAS; and the nature of the activity that the UAS is conducting. Individual UN Missions are best placed to determine the combination of factors that applies in their specific environment.

2.2. UAS types and features

2.2.1. Classification

Various frameworks exist to classify UAS, usually based primarily on the weight, maximum altitude and/or range of the UAS. The UN divides UAS into four (4) classes. For coherence with the terminology used for the UN's own UAS, this is the classification system used in these Guidelines to refer to hostile/unidentified UAS. It should be noted that these classifications cannot reflect every type of UAS, and some systems may straddle a class boundary.

a. **Class I.** Small, mini and micro UAS, usually operated up to a maximum altitude of not more than 10,000ft above ground level (AGL), normally with a weight of between 1 and 25kg, and within radio line of sight (RLOS) of the operator, with a maximum range of up to 100km. Micro UAS should not exceed 2kg in weight. This class is the most likely to be encountered because commercially available civilian UAS sold for hobby use tend to fall into this category as Class I micro/mini systems, making them numerous and widespread. Their small size and low audio signature can make them difficult to detect, while still

capable of carrying cameras and being modified to deliver small explosive payloads (as seen in MONUSCO in February 2024). Class I systems can be highly portable, with Class I Micro UAS often being hand-sized and even the largest Class I (Small) systems often being capable of being transported in a large backpack when disassembled. Class I systems tend to be capable of being operated without the need for any specialized launch or recovery equipment.

b. **Class II.** Tactical UAS, usually with a maximum take-off weight (MTOW) between 150kg and 600kg. Normally operated up to 20,000ft AGL, with a maximum range of 500km in a tactical environment, with none or limited access to standard aviation infrastructure such as runways, navigation aids, etc. Due to the increase in size and weight compared to Class I systems, these UAS will normally require some form of launch and recovery equipment such as a catapult launcher and/or a recovery net. Their larger size means they can fly further and faster than Class I systems and tend to carry more capable cameras. Class II systems generally require a small team of operators and (depending on their exact method of operation) may also need some form of mobile or fixed ground control station.

c. **Class III.** Typically, Medium Altitude Long Endurance (MALE) and High-Altitude Long Endurance (HALE) UAS/RPAS, normally weighing more than 600kg and operated up to 65,000ft AGL with unlimited control range and beyond visual line of sight (BVLOS). Such systems will use satellites for flight control, allowing the UAS to be based in one location but operated from anywhere in the world provided suitable satellite communications are in place between the two. This class is sub-divided into Class III (MALE) and Class III (HALE), with the former being capped at operating altitudes of up to 45,000ft and the latter capable of operating at up to 65,000ft. These systems are inherently large and expensive, and as such will almost exclusively be the preserve of state operators, often militaries. Such UAS can carry a variety of highly capable sensors and may also be armed with advanced air-to-surface munitions.

d. **Class IV.** Autonomous aircraft systems capable of being operated with no involvement from humans whatsoever. These can be categorised as small, mini and micro, with an operating altitude of 10,000ft AGL and a maximum range of 100km. Such systems are currently not utilised by the UN and are unlikely to form the majority of the systems encountered by UN personnel in operational environments; however, the class is included here for completion and alignment with established DOS Aviation Manual terminology.

2.2.2. Sensors

All UAS will carry some type of sensor, whether simply to provide the operator with a view of what the UAS is seeing or (with more advanced sensors) to acquire detailed types of information for highly specific purposes.

a. The standard sensor carried on a UAS tends to be an Electro-Optical (EO) camera. These are digital cameras capable of capturing full-colour video and still images both for live viewing by the operator and recording onto internal memory storage (if fitted) for later download. Even the most basic Class I systems will come with some form of integrated EO camera, and as the size of the UAS vehicle increases so too will the capability of the camera, with resolution and zoom both increasing dramatically on Class II and Class III systems.

b. More advanced models of UAS may incorporate an Infra-Red (IR) camera alongside the EO camera. This configuration, known as an EO/IR sensor, provides a low-light and nighttime capability that allows the UAS to be flown in darkness as well as daylight. In addition, the IR camera can be used in both daylight and at night to help detect heat sources such as people, animals, hot vehicle engines, fires, etc., adding additional tactical flexibility and greater situational awareness.

c. Larger and more expensive UAS in the Class II and Class III categories may also carry additional sensors such as air-to-ground radars for target identification, laser range finders/designators, and/or other kinds of sensors operating across different bands of the electromagnetic spectrum (such as sensors that can detect emissions from radios or various kinds of radar, both civilian and military). Such sensors have specialised purposes and tend to be both expensive to acquire and complex to exploit, meaning that they will normally be seen being used by state operators. However, technological advances mean that sensors are generally becoming smaller and more available, necessitating flexibility and constant review when considering the potential risk a UAS may pose.

2.2.3. Control Methods

The manner in which a UAS is operated is determined by its size and the distance it is designed to fly.

a. **Line of Sight (LOS).** The most basic UAS control method is LOS, in which the operator will maintain direct visual contact with the UAS as it flies and control it via a signal from the control device; this will usually be the case for Class I (Micro) systems. UN personnel observing such a system near their location should have a good chance of being able to directly identify likely operators based on the very short range between the UAS and the person flying it.

b. **Beyond Line of Sight (BLOS).** As the range of a UAS increases, the control method will have to change since the operator will no longer be able to see the UAS with their own eyes. Many Class I (Mini) and Class I (Small) systems offer First Person View (FPV), in which a forward-facing camera mounted on the UAS provides a live video feed back to the operator that they can view on a screen or using a worn headset. The control signals from the operator will be transmitted via a signal from the control device to the UAS. If the UAS is within Radio Line of Sight (RLOS) of the operator, then this signal can be transmitted directly. For UAS with extended range, such as Class III systems operating Beyond Radio Line of Sight (BRLOS), it is necessary for this control signal to be transmitted via a satellite link between the operator and the UAS itself. UN personnel observing such systems will likely not be able to directly identify the operators due to the likely significant distance between operator and UAS, and/or the deliberate use of terrain/cover to mask the operator.

2.2.4. Actors

The UN may encounter a variety of actors operating UAS; the main categories are listed below. It is important to note that it is not necessary for an actor to have hostile intent towards the UN in order for a UAS operated by them to pose a potential threat. Negligent or reckless operation of a UAS by a non-hostile local civilian (even if conducted in innocence) may still pose a serious flight safety hazard to UN aircraft, for example.

a. **State Authorities:** This group of actors are the most likely to have access to the full range of UAS classes, up to and including Class III systems. Depending on the specific details of the operating environment in question, these actors may coordinate airspace use with the UN to minimise flight safety concerns; however, this will not necessarily be the case. Examples of State users of UAS may include the military, police, environmental/wildlife protection services, civil engineers, and bi-lateral security partners working alongside the host state.

b. **NSAGs, including United Nations-designated groups:** Likely to primarily have access to less capable UAS than state authorities, these actors may nonetheless possess a variety of systems. Operating processes are unlikely to align with any form of airspace management frameworks in place, meaning that even if the NSAG in question does not have overt hostile intent towards the UN, their UAS are likely to pose potential risk due to the unpredictable nature of their employment. NSAGs with hostile intent towards the UN will be able to present a range of threats through the use of their UAS over and above flight safety concerns, up to and including direct attack on UN personnel/facilities/assets.

c. **Local civilians:** It is possible, depending on the specific mission environment, that some members of the local civilian population may have access to basic UAS. These would likely be of the so-called “hobby drone” variety and may be operated near UN personnel/facilities for a number of reasons ranging from curiosity, desire to capture images to provide to local media outlets, or to fuel a specific narrative goal (either positive or negative towards the UN). Regardless of the intent of such actors, there is a low probability that they will operate UAS with any coordination with the UN or in line with flight safety procedures. The potential for actors in this category to operate their UAS in a clueless (completely unaware of air safety protocols) or careless (aware of protocols but too inexperienced or unconcerned to abide by them) manner is high.

d. **Other:** In addition to the above actors, UAS may be operated by numerous other entities. These could include humanitarian groups, disaster response organisations, members of international media organisations, etc. There is also the potential, if sufficient procedural controls are not in place, that UAS operated by one UN entity may not be easily identified as UN assets by other UN entities, leading to potential confusion and/or safety concerns. Criminal actors who are not part of local NSAGs may also make use of UAS in support of illicit activities such as smuggling, observation of law enforcement groups, or other purposes.

2.2.5. Activity

UAS, regardless of their classification and the actor operating them, can be used to conduct a variety of different activities. The suitability of a specific UAS for each activity will vary depending on its characteristics (range, payload capacity, the ability of its sensors, whether it has weapons fitted, etc.) and on the intent/capability of the actor operating it. UAS are by their nature a highly flexible tool and can be used for a wide range of activities; some of the less routine uses could include creating unrest/panic through use of a low-flying UAS, contaminating water or other supplies by delivering pollutants, or blocking airspace to deny aircraft the ability to safely operate. However, when considering the main threats that UAS can pose to the UN, three broad activity categories can be identified as the most prominent at time of writing.

a. **Observation.** This involves a UAS being used to conduct surveillance, reconnaissance, or other form of information-gathering activity against UN personnel/facilities. The degree and type of threat this activity may pose will be directly related to the intent of the actor operating the UAS. Observation could range from casual curiosity on the part of a local civilian, through to an individual or group with an anti-UN agenda seeking to gather images to fuel mis/dis-information efforts against the UN, all the way up to an NSAG conducting deliberate reconnaissance of a location to aid attack planning. Because it will be often nearly impossible for the UN to readily identify the operator of a UAS or their intent, any unidentified UAS in proximity to a UN location should be regarded as posing an observation threat by default.

b. **Kinetic Attack.** The most direct physical threat a UAS can pose is as a vehicle for the conduct of a kinetic attack. This might involve either a UAS designed to carry weapons deploying them against a target (as will be the case with most UAS operated by a state military) or a modified commercial UAS that a NSAG has adapted to release an Improvised Explosive Device (IED) or other munition (such as a grenade, mortar bomb, etc.). Alternatively, a UAS attack may involve the UAS itself flying into the target and detonating its payload, being destroyed in the process. This attack method is seen with purpose-designed one-way attack UAS (colloquially known as “suicide drones”) used by some militaries and well-funded/supplied NSAGs. It is also seen in relation to modified commercial UAS that have been fitted with a simple explosive charge and an initiation mechanism, as was the case in the MONUSCO attack in February 2024.

c. **Electronic Attack.** It is technologically possible for a UAS to be used as a platform to carry Electronic Warfare (EW) equipment. Airborne EW capabilities have been employed on crewed aircraft by state militaries for decades, and delivery of some form of EW effect from a UAS would only require suitable miniaturization of the necessary components to fit the airframe. Of particular concern from a threat perspective would be delivery of Electronic Attack (EA) effects from a UAS; whilst the power source that can be fitted to smaller UAS would inherently limit the strength of signal outputs that could be generated, localised effects could be achieved. This is likely to be the most niche of the three activities identified here, with the technical barrier to entry to such a capability being relatively high. However, potential interference with UN communications and position, navigation and timing systems such as Global Navigation Satellite System (GNSS) would have serious consequences.

2.3. Threat Scenarios

Based on the details above the following seven representative scenarios have been developed. These scenarios are not exhaustive, and it should be noted that both UAS technology and actor intent can evolve rapidly, changing the potential likelihood and impact of these scenarios or causing new ones to arise. However, these scenarios are presented to illustrate the spectrum of threat facing the UN and to highlight priority areas to assist UN Missions with starting to develop their own tailored threat assessments.

Note that the threat posed to UN aircraft, personnel, and facilities by negligent or reckless operation of UAS is not presented as a separate scenario, since this is regarded as an inherent underlying factor in all of the scenarios below. It should also be noted that, as was seen in the MONUSCO incident detailed above, actors will not necessarily employ UAS in isolation but may instead combine them with other forms of observation, attack, or distraction.

2.3.1. Scenario One: deliberate UAS attack by a state against the UN

This scenario would see a state – likely though the use of its military – conduct an attack on UN personnel/facilities using their UAS assets (either because they wished to target the UN or due to mistaken identification of the UN as hostile forces). The class of UAS could vary depending on the systems in the state's inventory but would likely involve Class II or Class III military systems operating at range and deploying purpose-designed munitions. Depending on the capabilities of the mission in question, detection of incoming UAS may be possible, and the significant shift in intent from a state to deliberately target the UN is likely to have been made clear in the buildup to such an attack (assuming it is not conducted on a deniable basis). Although unlikely, the impact of such a scenario would have the potential to be severe in terms of risk to life.

2.3.2. Scenario Two: accidental collateral damage from state UAS attack

Under this scenario, UN personnel/facilities would suffer unintended damage as a result of a UAS attack conducted by a state against a different target. Whilst the UN would not be the planned target in this scenario, operational experience from peacekeeping missions has highlighted the risk of the UN being caught in the effects of state strikes against NSAGs. At the same time, in a complex operating environment there is always the risk that the UN could be mis-identified as hostile forces by a state or suffer the effects of a munition that fails to strike the intended target. Although the non-deliberate nature of such an attack may (but will not necessarily) reduce the lethality of the effect, the risk to life under this scenario would remain high-to-severe.

2.3.3. Scenario Three: deliberate attack on UN by NSAG using modified commercial micro/mini UAS

This scenario is the one which was seen to manifest in MONUSCO on 12 February 2024. By performing relatively basic modifications to a commercially available micro/mini UAS a NSAG has the ability to conduct a deliberate attack against UN personnel/facilities. Given the user-friendly nature of modern commercial UAS, along with their low cost and lack of counter-proliferation controls, this option is a realistic one for many NSAGs. Access to individuals with the appropriate skillsets to modify the UAS to carry some form of lethal element is likely to be the most limiting factor, though any group with access to basic IED construction expertise is likely to be able to achieve the required result. Examples from Middle Eastern NSAGs also demonstrate that attachment of common munitions, such as grenades, to a commercial UAS can result in a crude but potentially effective capability. The confirmed instance of this scenario playing out in MONUSCO, the proven adoption of the tactic by various NSAGs worldwide, and the likely lack of warning that the UN would receive of an attack combine to make this scenario both likely to occur against the UN again and of potentially high risk to life.

2.3.4. Scenario Four: deliberate attack on UN by NSAG using military-grade UAS

This scenario represents an extension of the previous but employing more capable UAS. These could either be UAS designed and manufactured by a state for use by military or paramilitary forces or systems designed and built by a large and capable NSAG itself. In either case, the range and payload capacity of such UAS is likely to significantly exceed that of the commercial micro/mini UAS seen in Scenario Three, offering the ability to attack UN personnel/facilities from further away and with larger/more lethal munitions. Such UAS are likely to be of the one-way attack type (often colloquially referred to as "suicide drones") that directly fly into the target and destroy themselves in the resulting detonation of their payload, in contrast to the reusable UAS

that deploy munitions and return to their home base likely to be seen in Scenario One and Scenario Two. Although the increase in required technical expertise makes this scenario less likely compared to Scenario Three, the potential for increased lethality would likely result in greater risk to life.

2.3.5. Scenario Five: non-malicious observation of UN by civilian actors

Under this scenario the UAS is not used to directly or indirectly attack UN personnel/facilities; rather, it is used to conduct observation only using the inbuilt (or aftermarket) camera. The operator of the UAS in this scenario is a civilian rather than a member of a NSAG or state military/police, and there is no specific intent to use the information gained through the UAS to enable attacks against the UN. However, there is still risk to reputation in this scenario given the potential for footage to be misinterpreted, misleadingly edited, or otherwise presented in a way that casts the UN in a bad light through mis/dis-information. In addition, even if footage is acquired out of innocent curiosity but subsequently uploaded to the internet or otherwise shared, any sensitive information contained within will then be available to potentially hostile actors. For example, footage showing the interior of a UN patrol base that inadvertently captures the fact that a gate is not properly secured could give any NSAG who saw the footage a tactical advantage that may lead to increased risk to life for UN personnel.

2.3.6. Scenario Six: malicious observation of UN via UAS

In this context, malicious observation refers to the act of using a UAS to gather information with the intention of using in a manner that is disadvantageous to the UN. This scenario is an extension of the previous, with the operator of the UAS in this instance being a hostile actor (state, NSAG, or other). The same risks to reputation as detailed in Scenario Five still apply, albeit amplified due to the explicit hostile intent of the operator. The potential risk to life is significantly increased as well, since there is a much higher probability that the observation will be conducted with the intent to gain information of operational advantage such as attack planning, advance warning of UN patrol departures, or specific reconnaissance of potential weak spots in base defences. NSAGs in Africa have been noted using UAS to film their attacks in order to capture propaganda footage, as well as using UAS to help indirect fire weapons such as mortars adjust their aim onto a target.

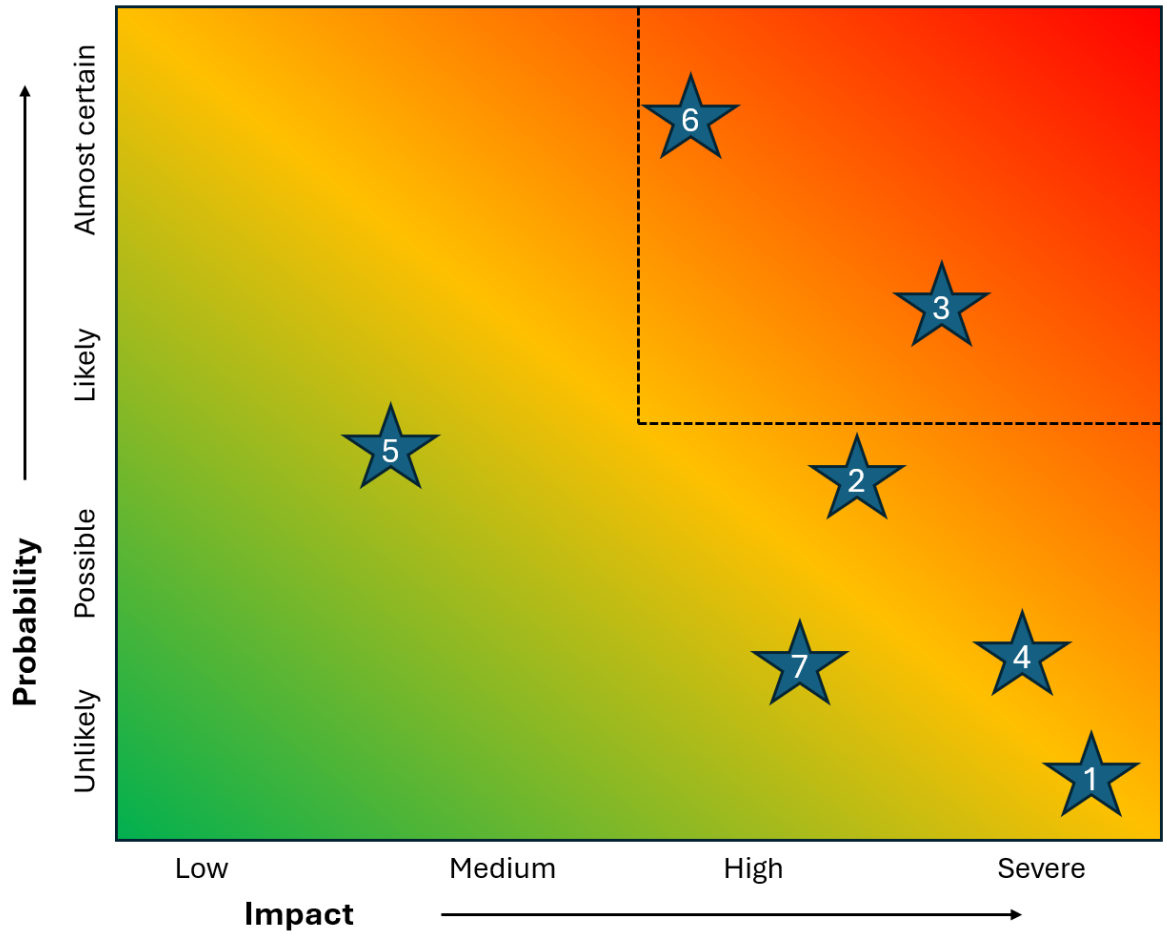
2.3.7. Scenario Seven: electronic attack via UAS by NSAG or state actor

This scenario is a broad one given the lack of evidence of such a capability being employed against the UN to date. However, the potential exists for an actor to interfere with UN electronic systems by employing an EA capability mounted on a UAS. Given the technical demands of such a capability, collateral interference from a state using one of the larger UAS classes to employ EA against a group other than the UN is likely the most credible way in which this scenario could manifest. However, a technologically advanced NSAG, or one sponsored by a state with such capabilities, could have the potential to employ such a capability on a smaller class of UAS – if not currently, then in the relatively near future. The impact of such a scenario would vary significantly depending on the nature of the electronic systems that were targeted. Effects could range from minor interference with non-essential communications systems up to potentially severe effects on safety-critical navigation systems at airfields, for example.

2.3.8 Scenario Probability / Impact graph

A representative Probability / Impact graph derived from these scenarios is at Figure 1 below. This is not mission or region specific but instead attempts to present an overview across all UN operating environments. Individual UN missions may wish to use this as a starting point to refine their own assessments based on the unique circumstances in their areas of operation and to assist in developing risk matrices based on mission leadership guidance.

In developing this graph, **probability** has been derived from a qualitative assessment of the opportunity and intent of the actor concerned, reported instances of similar events occurring in UN mission areas in the past, and developing trends in operating environments based on mission reporting. **Impact** has been derived from a qualitative assessment of the level of risk that the event would present to the UN. Broadly, this has been considered in terms of risk to life and risk to reputation. For example, a UAS attack on UN personnel would primarily represent risk to life, whereas non-malicious observation of the UN by civilians would primarily represent risk to reputation if images were captured that could then further the spread of damaging mis/dis-information. By the same logic, malicious observation of the UN by a NSAG would primarily represent risk to reputation through intent to spread dis-information; however, clear potential for risk to life also exists under this scenario if the observation is used to inform NSAG attack planning.



Scenario 1
(deliberate UAS attack by a state against UN)

Scenario 2
(accidental collateral damage from state UAS attack)

Scenario 3
(deliberate attack on UN by NSAG using modified commercial micro/mini UAS)

Scenario 4
(deliberate attack on UN by NSAG via military-grade UAS)

Scenario 5
(non-malicious observation of UN by civilian actors)

Scenario 6
(malicious observation of UN via UAS)

Scenario 7
(electronic attack via UAS)

Figure 1: Scenario Probability / Impact graph

2.3.9. Assessment of priority focus areas

Based on the scenarios and Probability / Impact graph above, the following conclusions can be made based on the overall situation across all UN mission areas:

a. **Most Likely scenario**: Scenario Six (malicious observation of UN via UAS). This scenario is assessed as being Almost Certain to occur and is likely to represent a Medium-to-High impact. Given the relative ease by which NSAGs can acquire and operate UAS, and the clear advantages they offer in facilitating observation of UN personnel/facilities, it is reasonable for the majority of UN missions to assume they are at risk of coming under such observation unless clear evidence exists to the contrary.

b. **Most Dangerous scenario**: Scenario One (deliberate UAS attack by a state against the UN). This scenario is assessed as being Unlikely to occur but would represent a Severe impact if state military assets were employed.

c. **Recommended UN focus**: Considering scenarios which are assessed to be more likely to occur than not (Likely or Almost Certain ratings), and which also have potential for significant impact (High or Severe ratings), Scenario Three (deliberate attack on UN by NSAG using modified commercial micro/mini UAS) and Scenario Six (malicious observation of UN by NSAG) present themselves as recommended priority focus areas for mitigation action.

Each mission is encouraged to conduct its own threat analysis, identify potential gaps and requirements, and explore feasible C-UAS capabilities within mission constraints. A step-by-step process for Counter UAS Threat Analysis can be found in **Annex A**.

3. C-UAS Framework

Counter-Unmanned Aircraft Systems (C-UAS) is a set of technologies, strategies, and measures designed to detect, track, identify, and mitigate threats posed by unauthorized or hostile unmanned aerial systems (UAS).

A comprehensive C-UAS system requires multiple integrated components that collectively establish a robust defence mechanism. These components function in unison to detect, track, identify, and mitigate UAS threats.

3.1. Detection

Detection is crucial for providing early warning, allowing United Nations personnel to respond promptly and mitigate risks to both personnel and property. The detection of the most probable threats can be classified into several broad categories, each presenting its own complexities, limitations, and challenges. The table below outlines the available options and key considerations for acquiring and operating each of these options.

3.2. Tracking

The ability to track a single or multiple UAS is also an indication that the capability solution is significantly complex, costly and will be justified based on cumulative risk at a given location or base. Tracking functionality is generally integrated into either Sense and Warn or Sense, Warn, and Intercept systems to enhance the effectiveness of the C-UAS mission. Moreover, robust tracking capabilities enable the collection of precise data on UAS activity, providing valuable insights into trends and incidents.

3.3. Identification

The ability to identify and classify an unknown UAS is critical to providing the required response and avoid any unnecessary collateral damage. In the context of UN missions, the reclassification of a UAS from unknown to hostile generally requires a positive visual identification confirming both its capability, such as the presence of weaponry, and a clear intent to pose a threat to UN personnel or property. The consideration of electronic transponders for all UN UAS could be beneficial in facilitating frequency-based interrogation (IFF) and ensuring effective deconfliction measures.

3.4. Mitigation

The mission will have several options to mitigate the threat posed by hostile UAS. However, the extent of mitigation and the ability to neutralize the threat will depend on the specific capabilities available at each location within the mission. Mitigation efforts will encompass both Active and Passive measures.

3.4.1. Passive Measures

Passive measures are an essential component of any C-UAS plan. They should be carefully planned and regularly exercised by all UN missions, as they can play a significant role in reducing the impact of hostile UAS threats. Passive measures include camouflage, concealment and deception, dispersing forces, hardening, and providing shelters. UN Forces should routinely conduct "red teaming" exercises at operational bases by deploying friendly UAS against the perimeter. This practice helps assess responses, identify weaknesses, and address potential gaps and vulnerabilities in security measures.

3.4.2. Active Measures

Active measures will encompass capabilities that will be integrated into the mission’s layered C-UAS strategy, specifically in areas where risk and vulnerability necessitate robust protection. Active response includes both “soft kill” and “hard kill” options, utilizing the electromagnetic spectrum alongside conventional munitions to counter hostile UAS threats. Active countermeasures encompass jamming devices aimed at disrupting UAS communications, missile interception systems designed to neutralize UAS threats, and high-power lasers capable of temporarily impairing or disabling UAS operators. The decision-making process for supporting active engagement will be inherently complex and time-sensitive, requiring careful assessment of potential collateral damage risks.

4. Operational Phases

4.1. Deployment

The deployment of C-UAS capabilities is crucial for safeguarding the security and integrity of mission operations. To effectively counter evolving threats, the C-UAS framework must be scalable, mobile, and adaptable to a wide range of operational environments.

The deployment of C-UAS system in the context of UN peacekeeping is guided by several key principles, including:

a. **Pre-Deployment Assessment**: Conduct a comprehensive risk assessment to identify high-threat areas and critical infrastructure requiring C-UAS protection.

b. **Critical Positioning**: Deploy detection and mitigation systems at key locations, including mission headquarters, troops camps, and areas of operational significance.

c. **Mobile Units**: Integrate mobile C-UAS teams to provide rapid response capability across the mission area.

d. **Integration with Existing Systems**: Where possible, C-UAS systems should be interoperable with existing surveillance, communication, and command-and-control (C2) systems.

e. **Coordination with Mission stakeholders**: Effective C-UAS operations necessitate close collaboration among Mission stakeholders, including Host Nations.

4.2. Detection and Monitoring

The detection of UAS is the first step in the C-UAS operational framework. Detection systems must be capable of detecting UAS threats in real-time, across a variety of weather and environmental conditions.

Some commonly used detection methods are:

Detection mode	Limitations	Considerations
Visual detection	Range is limited to combination of sound/optics available. Difficult in low illumination.	There will never be adequate reaction time if the reliance is on visual detection (day only).
Acoustic detection	Range is limited (500m) and accuracy sometimes questionable if there is ambient noise nearby. Cost is significant but workable.	In a layered defence system, these systems can be effectively deployed in outer operating bases or mobile patrols without requiring a direct line of sight.

Electro-optical and Infra-red	Operate within the visual or IR frequency ranges, with imaging systems effective up to approximately 1000m and non-imaging systems reaching 1500m against small UAS threats. EO systems are less effective in low-light conditions or adverse weather.	Employ advanced processing to track and identify UAS, relying solely on imaging systems for identification.
LADAR/LIDAR (Laser Detection and Ranging/Light Detection and Ranging)	These are active systems that generate location signatures, thereby making them vulnerable to targeting. Additionally, they pose potential risks to their operators. Typically, they are sensitive, costly, and challenging to acquire, as they represent cutting-edge technology. While LADAR/LIDAR systems offer an excellent passive and accurate alternative, their range is significantly limited, typically to 30 meters.	Offer high accuracy, advanced signal processing, and reliable support for the detect-track-engage aspect of C-UAS. The most effective systems integrate complementary radars to optimize detection, tracking, and engagement while accounting for UAS radar profiles, ground clutter, and atmospheric condition.
Active Radio - RADAR/Dopler	Cost of these systems is significant, however provides a higher degree of accuracy, range and warning.	These systems will likely only be fiscally available in high risk and vulnerable nodes within a UN mission. Small UAS will be extremely difficult to detect based on radar cross section and the use of ground clutter to mask signature.
Radio Frequency detection method (Radio Direction Finders)	The presence of various interfering signals in a complex electromagnetic environment can degrade the accuracy of radio detection and hinder the precise determination of physical location. Addressing this challenge requires	The technology is mature and has been widely applied.

	specialized equipment and trained personnel.	

Detecting UAS comes with several challenges, including:

a. Low-altitude, slow-moving UAS can evade traditional radar systems due to its low-level cross section.

b. UAS may operate without active RF signals, requiring multi-layered detection capabilities. For example, use of GNSS, fiber-optic cable, or other non-radio communication or operation.

4.3. Response and Engagement

The Response and Engagement phase in C-UAS involves actively addressing and neutralizing the threat posed by hostile UAS. This phase typically includes Identification, Tracking, Mitigation and Exploitation.

4.3.1. Identification

Once a potential UAS threat is detected, it must be positively identified to determine its intent and level of threat. Identification Process:

a. **Classification**: Differentiate between friendly, neutral, unknown, and hostile UAS.

b. **Behavioural Analysis**: Assess the flight pattern, altitude, and speed of the UAS to determine potential threat levels. For example, following consistent routes, predictable techniques, tactics, or procedures (TTP), or following friendly UAS.

c. **Payload Assessment**: Identify whether the UAS is carrying any suspicious payloads that could pose a risk to personnel or infrastructure.

d. **Visual Confirmation**: Where possible, utilize on-ground personnel or cameras to visually confirm the UAS type and characteristics.

4.3.2. Tracking

Tracking ensures that once a UAS is detected, it remains under continuous surveillance to prevent loss of situational awareness and to aid in identification.

Tracking can be accomplished through the following methods:

a. **Radar Tracking**: Maintain radar lock on the UAS to track its movements

b. **RF Tracking**: Follow the UAS communication signals to predict its flight path.

c. **Multi-Sensor Fusion**: Combine data from multiple sensors (radar, RF, EO/IR, human observation) to achieve a comprehensive tracking picture.

The objectives of tracking are:

a. Prevent UAS from reaching critical areas.

b. Monitor UAS movements for peacekeeping-intelligence purposes.

c. Maintain continuous situational awareness.

d. Support identification.

e. C-UAS system targeting.

4.3.3. Mitigation

Mitigation involves neutralizing the threat posed by UAS once it has been identified and tracked. The mitigation response must be proportionate to the threat level and comply with mission rules of engagement and legal frameworks.

There are various mitigation techniques for identifying and neutralizing UAS, including library-based and non-library-based approaches.

a. **Library-based techniques** rely on a pre-existing database (or "library") of known UAS signatures. When an UAS is detected, the system compares its signature against the library to determine if it matches a known threat. If a match is found, appropriate mitigation measures are selected and accordingly deployed.

b. **Non-library-based techniques** do not rely on a pre-existing database. Instead, they use real-time analysis and adaptive algorithms to identify and select best mitigation method to UAS threat. These techniques may involve machine learning, artificial intelligence, and other advanced technologies to detect and respond to UAS based on their behaviour, movement patterns, and other dynamic factors.

Key mitigation methods include:

a. **Soft Kill Methods**: Soft kill techniques aim to disrupt the UAS's systems preventing it to carry out its intended actions by using soft means (or non-kinetic means). These methods are often preferred in environments where collateral damage must be minimized.

   - **Jamming**: Disrupt UAS communication and GNSS signals.

   - **Spoofing**: Send false signals to mislead the UAS.

b. **Hard Kill Methods**: Hard kill techniques involve physically incapacitating the UAS. These methods are typically used in high-security areas or military operations where the immediate neutralization of the threat is critical.

   - **Kinetic Interceptors**: Use of Counter-UAS projectiles or net-based systems.

   - **Directed Energy Weapons**: Utilize lasers or high-powered microwaves to disable UAS.

Some factors to consider on the selection of mitigation method:

a. **Collateral Damage**: Take steps to protect civilians and civilian objects, and to mitigate potential harm to civilians and infrastructure that may result from counter-UAS operations, including before, during, and after such operations.

b. **Legal Compliance**: Follow mission-specific rules of engagement and international legal standards.

c. **Escalation Management**: Ensure mitigation responses do not escalate conflicts unnecessarily.

4.3.4. Exploitation

Exploiting neutralized UAS in C-UAS operations offers significant peacekeeping intelligence and countermeasure opportunities. By scrutinizing the UAS's electronics, one can ascertain its manufacturers, capabilities, and vulnerabilities. Analysing flight logs can uncover the UAS's origins and intended targets. Software analysis may uncover flaws, encrypted protocols, or malicious code, aiding in mitigation strategies. Additionally, reverse engineering and frequency analysis can help disrupt or spoof future threats, effectively turning enemy technology against them.

However, post-neutralization efforts must be conducted with extreme caution due to the potential for explosive hazards. Many UAS, particularly those used in hostile environments, may carry Improvised Explosive Devices (IEDs) or tamper-activated mechanisms designed to detonate upon handling. Only trained Explosive Ordnance Disposal (EOD) personnel should interact with the UAS until it is deemed safe. Additionally, operators must be aware of potential electronic fail-safes, such as self-erasure or self-destruction protocols triggered during unauthorized access. By integrating safety protocols with technical expertise, post-neutralization exploitation can yield valuable peacekeeping-intelligence while minimizing risk to personnel and infrastructure.

4.4. Post-Engagement

After each C-UAS deployment, it is essential to conduct a comprehensive review to evaluate the effectiveness of the detection, identification, tracking, and mitigation measures.

a. **Debriefing**: Conduct debriefs with C-UAS operators to gather insights.

b. **Data Analysis**: Review sensor data to identify patterns and improve future responses.

c. **Lessons Learned**: Document lessons learned to refine C-UAS tactics, techniques, and procedures. Information should be shared with the widest applicable audience, whereas this may benefit other Missions or guide policy. Examples include significant activity reports (SIGACTS), engagement reports, storyboards, or after-action reports (AAR).

5. Integration with Existing Systems

A comprehensive C-UAS strategy requires seamless integration with existing operational systems to maximize effectiveness and maintain situational awareness. This integration will ensure

efficient communication, command and control (C2), and interoperability across various units and assets.

5.1 Communication Systems

Effective communication is the backbone of any C-UAS operation. The integration of C-UAS assets into existing communication systems is essential to ensure real-time information sharing and coordination between different units.

a. **Secure Channels**: C-UAS systems should utilize encrypted communication channels to prevent interception by hostile actors.

b. **Real-Time Data Sharing**: The C-UAS should be capable of transmitting detection and tracking data to command centres, air traffic control, aviation management, and frontline operators in real-time.

c. **Redundancy**: Backup communication links should be established to ensure continuous operation in case of primary channel failure.

5.2. Command and Control (C2)

The integration of C-UAS capabilities within the existing C2 framework is critical to maintaining operational coherence and ensuring timely decision-making.[4]

a. **Centralized C2 Integration**: The C-UAS system should be integrated into the mission's existing C2 framework and staff decision making processes to provide commanders with a comprehensive operational picture.

b. **Automated Alerts**: The system should possess the capability to generate automated alerts and threat assessments, thereby alleviating the cognitive burden on operators.

c. **Adaptive Tasking**: The C-UAS C2 system should facilitate the dynamic allocation and reallocation of assets in response to real-time threat indicators and warnings, leveraging peacekeeping-intelligence.

5.3. Interoperability

Interoperability with existing systems and allied forces is essential to maximize the effectiveness of C-UAS operations. This ensures that different platforms and units can work together seamlessly.

a. **Standard Protocols**: C-UAS systems should adhere to standard protocols for data exchange to ensure compatibility with legacy systems.

b. **Joint Operations**: The C-UAS framework should facilitate joint operations among mission components, ensuring shared situational awareness and coordinated responses.

[4] Authority, Command and Control in UN Peacekeeping Operations, October 2019

c. **Modular Design**: The C-UAS system should be designed with modularity at its core, facilitating seamless upgrades and integration with emerging technologies.

6. C-UAS Capability

The C-UAS capability should be organized as an integral part of the mission's security and defence framework to ensure efficient coordination and resource utilization.

6.1. Organization

The organizational structure for C-UAS capabilities necessitates the integration of diverse personnel and units with distinct operational roles, ensuring a unified and effective response to UAS threats.

6.1.1. Personnel

A C-UAS unit should at least include the following essential components:

a. **C-UAS Planner:** Officers responsible for planning, orchestrating, and executing measures to detect, monitor, and neutralize hostile or unauthorized UAS.

b. **C-UAS Operator**: Specialized teams tasked with the real-time operation of C-UAS systems, encompassing detection, tracking, and mitigation efforts.

c. **C-UAS Analyst**: Personnel dedicated to analysing UAS threats focus on identifying patterns and providing peacekeeping-intelligence support.

d. **Maintenance Team**: Technical staff ensuring the operational readiness of C-UAS equipment.

6.1.2. Operational Roles

a. **Detection and Monitoring**: Continuous surveillance of airspace to detect unauthorized UAS activity.

b. **Threat Assessment**: Understand the threat level posed by detected UAS and determining appropriate mitigation responses.

c. **Response and Mitigation**: Implementing defensive measures to address potential threats involves techniques such as jamming, signal disruption, and physical interdiction.

6.1.3. Command structure

a. The C-UAS capability should operate in synchronization with the Mission's Force Protection Unit, integrated base defence,[5] and coordinate with the Mission Headquarters' C2 to ensure, coordinated planning timely information sharing and decision-making.

[5] UN DPO Policy on Integration of Capabilities for Defence of Bases, January 2023

b. Integration with Peacekeeping-Intelligence, Surveillance, and Reconnaissance (PKISR) units is crucial for enhancing situational awareness and improving the overall security posture. This begins with a robust C-UAS threat analysis.

6.2. Force Generation

The procurement and deployment of C-UAS systems can follow three primary contracting frameworks: Contingent-Owned Equipment (COE), United Nations-Owned Equipment (UNOE), and a system contracted capability. Each approach has distinct advantages and limitations based on operational, logistical, and financial considerations.

6.2.1. Contingent-Owned Equipment (COE)

In the COE model, the contributing country provides the C-UAS equipment and personnel to the mission. The Troop/Police Contributing Country (T/PCC) retains responsibility for maintenance, upgrades, and replacements of equipment. The UN reimburses the T/PCCs based on agreed rates outlined in the Memorandum of Understanding (MoU).

6.2.2. United Nations-Owned Equipment (UNOE)

In the UNOE model, the UN procures, owns, and maintains the C-UAS systems. The UN provides trained personnel or contracts external vendors for system operation. Equipment is standardized across missions, ensuring interoperability and compliance with UN operational requirements.

6.2.3. UN System Contracted Capability

In situations where there is a time-sensitive capability needs and the availability of member states' COE and UNOE options are limited or unavailable, contracting commercial-off-the-shelf capabilities is a viable and effective solution. System contracts provide a swift and fiscally responsible means to develop and test capability solutions to address emerging threats, such as hostile UAS.

6.2.4. Hybrid Approach

A hybrid approach could be considered, wherein critical, high-risk C-UAS capabilities are deployed as UNOE or through system contracts to ensure timely deployment, standardization, and control. Meanwhile, additional or supplementary capabilities could be provided by T/PCCs under the COE framework. This decision should take into account the mission's threat assessment, operational requirements, and deployment timeline.

7. Maintenance, Supply Chain and Training

The logistical support for C-UAS operations is crucial for ensuring the effective deployment, maintenance, and sustainability of C-UAS systems. Coordinated logistics, timely support, and efficient resource management are vital to maintaining operational readiness and addressing emerging threats.

7.1. Maintenance

Maintenance is critical to ensure that all C-UAS components remain fully functional and can deliver reliable performance in detecting, tracking, and mitigating UAS threats. Maintenance includes both preventive and corrective measures to address equipment malfunctions, software updates, and hardware replacements. Key considerations:

a. Establishment of certified Maintenance Teams within the mission, including both on-site technical personnel and remote support from vendors or T/PCCs.

b. Availability of spare parts and repair tools in the mission area to reduce downtime.

c. Maintenance contracts with original equipment manufacturers (OEMs) to ensure ongoing support and access to technical expertise.

7.2. Supply Chain

The supply chain is a critical component of logistics, ensuring the timely availability of all necessary equipment, spare parts, and consumables to maintain the C-UAS capability. A resilient supply chain minimizes delays in operations and ensures mission readiness.

7.2.1. Components of the Supply Chain

a. **Procurement**. The timely acquisition of C-UAS equipment, spare parts, and consumables should be facilitated through UN procurement channels or contributions from T/PCCs. Additionally, contracts should be established with reliable vendors to ensure a consistent supply of equipment and comprehensive maintenance support.

b. **Inventory Management**. A centralized inventory system should be established to track all C-UAS assets and spare parts within the mission. Regular stock audits should be conducted to ensure that critical components are readily available when needed. Future supply needs should be forecasted based on the operational tempo and the wear-and-tear rates of the equipment.

c. **Logistics Coordination**. Coordination between mission logistics units, the UN Global Service Centre (UNGSC), and T/PCCs should be strengthened to streamline the flow of supplies. Transportation plans should be integrated to ensure the timely delivery of equipment and parts to remote locations. Additionally, contingency plans should be established to mitigate disruptions in the supply chain, including delays caused by political or security factors.

7.2.2. Key Challenges and Solutions

a. Delays in the delivery of specialized C-UAS components can impede operations. To address this issue, maintaining a buffer stock of essential spare parts is crucial. Additionally, establishing pre-arranged contracts with multiple vendors can help avoid supply bottlenecks and ensure a steady flow of necessary components.

b. While local repair facilities in mission areas may face certain challenges, establishing forward repair hubs within or near these regions can help mitigate these issues. This approach would reduce turnaround times and enhance operational readiness.

7.3. Training

A successful C-UAS capability depends on having well-trained personnel who can effectively operate, maintain, and adapt the systems to evolving threats. Training programs must address both technical and operational aspects of C-UAS systems.

7.3.1. Types of Training

Types of training for C-UAS personnel are as follows:

a. **Initial Training**. Initial training on C-UAS systems should be provided by system manufacturers or vendors during deployment or by T/PCCs prior to deployment. This training should encompass system setup, operation, fundamental troubleshooting, and preventive maintenance. Additionally, it should include theoretical modules on UAS threats, C-UAS strategies, and the legal and ethical considerations pertinent to their utilization.

b. **Refresher Training**. Refresher courses should be instituted to ensure operators remain abreast of the latest threat profiles and system enhancements. Scenario-based exercises ought to be conducted to enable operators to practice detecting, tracking, and mitigating UAS threats under real-world conditions. Furthermore, advanced technical training should be provided to maintenance teams, empowering them to manage more intricate repairs and system configurations with proficiency.

It is essential that all UN personnel across various units receive **basic counter UAS training** as part of its pre-deployment training and in-mission induction training. This includes comprehensive C-UAS Generalist training, covering basic recognition, reporting procedures, and appropriate actions to take, aimed at enhancing the recipients' knowledge of UAS threats and basic C-UAS measures.

It is imperative to acknowledge that the responsibility for ensuring peacekeepers is adequately trained and qualified, both before their deployment and throughout their service in any UN peacekeeping mission, is a collective duty shared among T/PCC, command, and staff.[6]

7.3.2. Training Delivery Methods

a. In-Person Training:

- Delivered on-site by system manufacturers, vendors, or T/PCCs instructors.
- Hands-on practice with real equipment to build operator confidence.

b. Remote Training:

[6] See: Training for all United Nations Peacekeeping Personnel, 2010.

- Online courses and virtual simulations for ongoing skill development.
- Remote troubleshooting support from vendors or OEMs.

c. Key Considerations:

- Ensure training is comprehensive and standardized across the mission to avoid inconsistencies in operational procedures.
- Include certification programs to validate the proficiency of C-UAS operators and technicians.
- Develop a training rotation schedule to accommodate personnel turnover and ensure continuity in operations.

8. Legal and Ethical Considerations

The deployment of C-UAS within UN missions must be guided by a comprehensive framework that ensures full compliance with international law, including international humanitarian law and international human rights law, as well as established ethical standards. The Head of Mission (HOM), or a designated expert acting on their behalf, is responsible for reviewing all legal and ethical considerations associated with the planning, deployment, and operational use of C-UAS capabilities. This includes ensuring that appropriate safeguards are in place to protect civilians and civilian infrastructure. Furthermore, the HOM or their delegate must develop detailed Standard Operating Procedures (SOPs) outlining the steps to be taken in the event of collateral damage, including reporting, investigation, and remedial actions, in line with UN accountability and protection frameworks.

8.1. Legal Framework

The following frameworks help ensure that C-UAS operations are conducted responsibly and in accordance with legal standards:

a. **International Humanitarian Law (IHL)**: The deployment of C-UAS technology in conflict zones must adhere to the principles of IHL, including distinction, proportionality, and necessity. Countermeasures must clearly differentiate between legitimate military targets and civilian entities to prevent unintended harm.

b. **International Civil Aviation Organization (ICAO) Regulations**: C-UAS systems must comply with ICAO regulations regarding airspace management. This entails respecting national airspace sovereignty and ensuring that C-UAS operations do not interfere with civilian air traffic.

c. **Host Nation Agreements**: The deployment of C-UAS systems must align with the agreements between the UN and the host country, including Status of Forces Agreements (SOFA).

d. **UN Policies and Guidelines**: C-UAS operations should conform to existing UN policies on the use of force, the protection of civilians, and the safeguarding of mission personnel and assets.

8.2. Human Rights Considerations

The deployment of C-UAS systems must uphold fundamental human rights principles, particularly:

a. **Right to Privacy**: Given that C-UAS technology often involves surveillance and data collection, it is imperative that operations respect individuals' right to privacy. Data collected must be used strictly for mission-related purposes.

b. **Accountability and Oversight**: It is essential to establish robust mechanisms for accountability and oversight to ensure that C-UAS operations do not infringe upon human rights. This includes regular reporting, audits, and investigations into any alleged misuse.

8.3. Protection of Civilians

a. When carrying out counter-UAS operations, UN peacekeeping missions must take steps to protect civilians and mitigate potential harm that could arise from these operations, before, during, and after.

b. Efforts to mitigate harm to civilians must inform operational planning and the conduct of operations, and should be undertaken before, during, and after the implementation of operations.

c. Counter UAS operations should be followed by an after-action review that analyzes the impact of the operation and identifies lessons learned for future operations.

8.4. Ethical Considerations

Ethical considerations are critical to ensure that C-UAS deployments align with the UN’s core values. Each of the following considerations should follow applicable policies, guidelines, regulations and agreements:

a. **Proportional Use of Force**: Countermeasures must be proportionate to the threat posed by unauthorized or hostile UAS. Excessive use of force must be avoided.

b. **Transparency and Reporting**: C-UAS operations should be executed with utmost transparency, ensuring that all relevant stakeholders, including host nations, are duly informed of operational activities and potential risks.

c. **Data Management**: Clear policies must be established regarding the collection, storage, and utilization of data obtained through C-UAS systems. It is essential to safeguard this data from unauthorized access and misuse.

d. **Training and Awareness**: Personnel operating C-UAS systems must receive comprehensive training on the legal and ethical implications of their actions, including the rules of engagement and respect for individual rights. This training should be conducted both in pre-deployment training and in-mission training.

8.5. Risk Mitigation Measures

To mitigate potential legal and ethical risks, the following measures should be implemented:

a. **Legal Reviews**: Regularly conduct legal reviews of C-UAS policies and procedures to ensure alignment with international and UN regulations.

b. **Ethical Guidelines**: Develop and disseminate ethical guidelines tailored to the use of C-UAS technology in peacekeeping operations.

c. **Incident Reporting Mechanisms**: Establish clear procedures for reporting and investigating incidents involving C-UAS systems to ensure accountability and continuous improvement. An example of standardized reporting forms can be found in **Annex B**.

8.6. Rules of Engagement (ROE)

UN Peacekeepers must meticulously consider any special regulations or amended rules of engagement when deploying C-UAS capabilities in mission areas. The utilization of C-UAS capabilities within the context of peacekeeping operations is intended for self-defence and the protection of civilians. Such use must be in strict alignment with the Mission mandate, Host Nation regulations, and the Status of Forces Agreement (SOFA).

Article 51 of the United Nations Charter enshrines the inherent right of states to engage in self-defence, including collective self-defence, in response to an armed attack. This provision thereby authorizes UN peacekeeping forces to employ C-UAS capabilities to safeguard themselves against assaults involving hostile UAS.

However, it is strongly recommended that, prior to the testing, acquisition, installation, or use of C-UAS systems in any UN Missions, including "passive" or "detection-only" systems, Mission leadership fully understand the operational functionalities of these systems and seek the counsel of C-UAS experts.

8.7. Ethical Issues

The deployment of C-UAS capabilities necessitates careful consideration of several ethical issues. These concerns often pertain to privacy, proportionality, unintended consequences, and the potential misuse of technology. Below is an outline of key ethical considerations

a. **Surveillance Risks**: The deployment of C-UAS systems, which often utilize radar, cameras, and signal interception technologies, may inadvertently capture personal data or monitor individuals not engaged in any unlawful activities.

b. **Mass Data Collection**: The sophisticated nature of advanced C-UAS systems, particularly those incorporating artificial intelligence (AI), could result in the indiscriminate collection of information, thereby raising significant concerns regarding data protection and privacy rights.

c. **Response Escalation**: The use of active countermeasures, such as jamming or kinetic interception, may cause undue harm or damage, especially when the perceived threat is minimal or the UAS is employed for benign purposes, such as by hobbyists or researcher.

d. **Unintended Consequences/Collateral Damage**: Countermeasures like jamming have the potential to disrupt civilian communications or navigation systems, including Wi-Fi, GNSS, or aviation equipment, leading to unintended and possibly severe repercussions.

e. **Misuse of Technology**: There is a risk that C-UAS capabilities could be exploited for unauthorized surveillance, oppression, or the violation of human rights, particularly in regions with weak governance or oversight mechanisms.

f. **Legal Ambiguities**: The lack of clear international or national regulations governing the use of C-UAS presents ethical dilemmas regarding the appropriate entities to deploy them, the circumstances under which they should be used, and the limitations that should be imposed.

g. **Algorithmic Bias**: The reliance on AI for detection within C-UAS systems may introduce biases in the algorithms, potentially leading to unfair targeting or inaccuracies.

h. **Environmental Concerns**: The continuous operation of monitoring systems for C-UAS may have substantial energy requirements, thereby contributing to resource consumption and environmental impact.

i. **Gender Considerations**: It is imperative that C-UAS programs, guidelines, training, and procedures adhere to all United Nations gender-related policies and regulations, ensuring inclusivity and equity.

9. Evaluation

The evaluation prior to deployment follows the UN Policy on Operational Readiness Preparation[7], providing the framework and timelines for assessing and self-certifying UN Military units by T/PCCs. The main goals are to help T/PCCs meet national and UN performance standards and to ensure initial training levels are maintained, making necessary adjustments for future rotations. In-mission evaluations are conducted progressively, from individual to Commanders, and by activity, to build expertise and integrate capabilities for collective application. Units in the mission areas are evaluated for operational effectiveness and integration with the Force for the achievement of mission mandate. Needless to say, the tasks enumerate in the SUR of the unit forms the basis of these evaluations.

9.1. Performance Metrics.

The performance metrics of Counter-Unmanned Aircraft Systems (C-UAS) serve as essential indicators for evaluating their effectiveness, efficiency, and appropriateness in detecting, tracking, identifying, and neutralizing UAS threats. These metrics are pivotal in assessing the operational capabilities of C-UAS technologies, ensuring they fulfil mission-specific criteria. Key performance metrics encompass detection, tracking, identification, mitigation, and overall operational metrics.

The evaluation of C-UAS capabilities will also assess the proficiency of operators, the integration and interoperability with mission systems, the logistical readiness to sustain operations, and the ability to adapt to evolving threats. Additionally, the evaluation should measure the C-UAS system's effectiveness in minimizing collateral damage and unintended civilian impact, while

[7] See: United Nations Policy on Operational Readiness Preparation, 2024

ensuring adherence to international humanitarian law and human rights principles. This holistic approach to performance evaluation will help ensure the C-UAS capabilities remain effective, efficient, and aligned with the mission's operational, legal, and ethical requirements.

9.1.1. Detection Metrics

a. **Detection Range**. This refers to the maximum distance at which the system can reliably detect a UAS. A longer detection range allows for more time to assess and respond to potential threats.

b. **Detection Accuracy**. This metric measures the system's ability to correctly identify the presence of a UAS, minimizing false positives and negatives.

c. **Detection Speed**. This is the time it takes for the system to detect a UAS after it enters the monitored area. Faster detection speeds enable quicker response actions.

9.1.2. Tracking Metrics

a. **Tracking Range**. This is the distance within which the system can continuously monitor the movement of UAS.

b. **Tracking Accuracy**. This metric measures how precisely the system tracks the position, speed, and trajectory of a UAS.

c. **Target Continuity**. This refers to the system's ability to maintain uninterrupted tracking of a UAS without losing it, even in challenging environments such as dense urban areas or adverse weather conditions.

9.1.3. Identification Metrics

a. **Identification Accuracy**. This metric measures the system's ability to correctly identify a UAS, including details such as its model, size, or payload.

b. **Identification Speed**. This refers to the time required for the system to identify a UAS after it has been detected.

9.1.4. Mitigation Metrics

a. **Neutralization success rate**. This metric represents the percentage of times a C-UAS system successfully disrupts or disables a UAS threat.

b. **Mitigation method effectiveness**. This measures how well different mitigation techniques (such as jamming or kinetic disruption) perform against various types of UAS.

9.1.5. Operational Metrics

a. **Coverage Area**. This refers to the total area that the C-UAS system monitors and protects.

b. **Reliability and Availability**. This metric measures the system's ability to consistently perform its functions over time without failure.

c. **Adaptability**. This indicates the system's capability to operate effectively in diverse environments, such as urban, rural, or maritime settings, and to counter evolving threats.

9.2. Continuous Improvement

Continuous improvement in C-UAS focuses on consistently enhancing the system's capabilities, performance, and adaptability to address evolving threats and operational challenges. This approach is vital for maintaining effectiveness against the rapid advancements in UAS technologies and the increasing complexity of threats. It involves iterative development, incorporating feedback, and adapting to new use cases and environments. The approach to continuous improvement includes:

a. **Plan**: Identify gaps or opportunities based on threat analysis, operational feedback, and emerging technologies.

b. **Execute**: Implement enhancements, upgrades, or changes.

c. **Evaluate**: Test and evaluate improvements in realistic scenarios.

d. **Implement**: Integrate successful changes into standard operations and repeat the cycle.

Implementing performance monitoring in UN system contracts and hybrid approaches (including potential COE options) is essential to ensure that these contracts are executed effectively, efficiently, and in alignment with established standards and objectives. This practice fosters accountability, mitigates risks, and promotes continuous improvement, thereby enhancing outcomes and bolstering stakeholder confidence.

An effective way to evaluate and enhance security measures is through C-UAS Red Teaming. This method simulates potential threat scenarios to assess response protocols and technological capabilities, aiding in the development of robust defences and systems capable of handling various situations.

Red Teaming uses an adversarial testing approach to replicate realistic threats, evaluating the performance of security systems and procedures. It offers a structured framework to identify vulnerabilities, test standard operating procedures (SOPs), and refine responses to UAS-related threats. By mimicking real-world threats and thoroughly assessing response plans and technologies, organizations can improve their readiness to address the growing risks posed by hostile UAS. Success relies on establishing a solid foundation, continuously enhancing SOPs, and adopting a proactive stance on testing and training.

C-UAS capabilities and Command and Control (C2) are vital components of Integrated Base Defence (IBD). Each UN mission should develop layered defensive plans tailored to the specific threat level, likelihood of occurrence, and a balanced assessment of available resources and risk.[8]

[8] UN DPO Policy on Integration of Capabilities for Defence of Bases, January 2023

D. ROLES AND RESPONSIBILITIES

1. Office of Military Affairs (OMA)

a. **Develop and Update Doctrinal Manuals**: Regularly revise doctrinal manuals to include current C-UAS principles, incorporating lessons learned and emerging best practices through periodic updates.

b. **Incorporate C-UAS Capabilities in Force Generation Processes**: Ensure that force generation processes, including the planning development and updating of Statement of Unit Requirements (SURs) and Memorandums of Understanding (MOUs), integrate C-UAS capabilities.

c. **Conduct Comprehensive Assessments**: During Pre-Deployment/Rotation Visits, Military Skills Validation Exercises, and Advisory-and-Assessment Visits, perform thorough and accountable assessments of critical C-UAS skills and capacities.

2. Integrated Training Service (ITS)

a. **Develop Training Material**: Develop training materials on Basic UAS Threat Awareness to ensure all uniformed personnel are thoroughly prepared before deployment.

b. **Address Training and Capability Gaps**: Collaborate through multi-lateral partnerships to find solutions for Mission and T/PCC C-UAS related training and capability gaps.

3. United Nations Mine Action Service (UNMAS): Provide Counter Improvised Explosive Device (C-IED) expertise on C-UAS efforts to UNHQ and Missions.

4. Department of Operational Support (DOS):

a. **Serves as the secretariat for the reimbursement framework** for formed units deployed under MOUs. Manages the MOU process and collaborates with the DPO to ensure capabilities meet mandated tasks. Processes reimbursements to Member States for capabilities deployed in UN field missions.

b. **Oversees and manages the sourcing process** for commercial C-UAS, military units' Letters of Assist or pro bono agreement. Additionally, DOS facilitates outreach to potential C-UAS providers, registers vendors, and assesses both T/PCCs and commercial C-UAS providers.

c. The Aviation Safety Section, along with the UAS/RPAS and Airborne ISR Category, is responsible for **providing integration solutions** and **risk assessment tools** to implement C-UAS capabilities within shared aviation airspace.

d. The UNGSC supports the DOS UAS/RPAS and Airborne ISR Category by providing technical expertise, procurement support, operational evaluation, policy drafting, and asset management for C-UAS systems, **acting as a link** between missions, vendors, and the UAS Joint Cell.

5. Missions

a. **Perform an analysis of hostile UAS threats**, pinpoint potential gaps and requirements, and investigate viable C-UAS capabilities within the constraints of the mission.

b. **Develop a mission SOP for C-UAS** and integrate the C-UAS factor into the mission decision-making process.

c. **Maintain C-UAS military expertise** within Force staff to inform operational planning, peacekeeping-intelligence processes, and Force generation of key specialized Force enablers.

6. **Troop/Police Contributing Countries**: Responsible for training, preparing, and deploying both general and specialized contingents to effectively conduct peacekeeping operations in a UAS threat environment, ensuring they meet the agreed standards of pledged capacity as outlined in SURs and MOUs.

E. REFERENCES

Superior References

A. United Nations Peacekeeping: Principles and Guidelines, DPKO-DFS (2008) ("Capstone Doctrine")

Related Policies, Procedures or Guidelines

A. United Nations Policy on Operational Readiness Preparation, April 2024

B. United Nations Force Headquarters Handbook, November 2014

C. United Nations Peacekeeping Missions Military Aviation Unit Manual, April 2021

D. United Nations Department of Operational Support Aviation Manual, February 2021

E. United Nations Peacekeeping Intelligence Policy, 2017

F. United Nations Manual for the Generation and Deployment of Military and Formed Police Units to Peace Operations, May 2021

G. Generic Guidelines for Troop Contributing Countries Deploying Military Units to the United Nations Peacekeeping Missions, 2008

H. Manual on Policies and Procedures Concerning the Reimbursement and Control of Contingent-Owned Equipment of Troop/Police Contributors Participating in Peacekeeping Missions (COE Manual), 2023

I. Authority, Command and Control in UN Peacekeeping Operations, October 2019

J. Operational Readiness Preparation for Troop Contributing Countries in Peacekeeping Missions, December 2018

K. United Nations Use of Unmanned Aerial Systems (UAS) Capabilities Guidelines, February 2019

L. Guidelines on the Force Protection for Military Components of United Nations Peacekeeping Missions, March 2021

M. Protection of Civilian: Implementing Guidelines for the Military Component of UN PKO, September 2023

N. Training for all United Nations Peacekeeping Personnel, May 2010

O. Management of Temporary Operating Bases (TOBs) in United Nations Peacekeeping Missions, June 2024

P. United Nations Department of Peace Operations Policy on Integration of Capabilities for Defence of Bases, January 2023

F. CONTACT

The point of contact for these guidelines is the C-UAS Working Group in the UNHQ New York, through the OMA.

G. HISTORY

These guidelines are the first produced on C-UAS. The review will be in five years from the date of approval.

DATE OF APPROVAL: 3 June 2025

APPROVAL SIGNATURES:

Jean-Pierre Lacroix
Under-Secretary General
for Peace Operations

Atul Khare
Under-Secretary General
for Operational Support

Annex A

Counter UAS Threat Analysis: Step-by-Step Process

1. Define the Mission and Operational Environment

a. **Mission Objectives**: Clearly outline the mission's purpose, including the assets, infrastructure, or personnel that need protection from UAS threats. Identify critical points within the mission area and understand the potential consequences of UAS intrusions.

b. **Environment Analysis**: Conduct a thorough assessment of the operational environment, considering topography, climate, population density, and existing infrastructure. Analyse electromagnetic spectrum conditions and potential interference sources.

c. **Historical Incidents**: Research past UAS incidents in similar environments to understand threat patterns, adversary behaviour, and system vulnerabilities. This historical data provides context and helps in planning more effective countermeasures.

2. Identify Potential UAS Threats

a. **Types of UAS**: Identify various UAS platforms that could pose a threat, ranging from small commercial UAS to larger military-grade UAVs. Assess their technical specifications such as flight range, payload capacity, communication methods, and autonomy levels.

b. **Threat Actors**: Analyse potential adversaries including state and non-state actors including terrorist groups, lone-actor operators, and criminal organizations. Understand their motives, capabilities, and historical use of UAS technology.

c. **Tactics, Techniques, and Procedures (TTPs)**: Study known adversary tactics like reconnaissance, electronic warfare, payload delivery, and swarm attacks. Include analysis of historical UAS attacks globally to refine defense strategies.

3. Assess Vulnerabilities

a. **Critical Assets Identification**: Catalogue and prioritize critical assets based on their importance and the impact of potential UAS threats. Include infrastructure, key personnel, and sensitive operations.

b. **Detection Gaps**: Assess current detection systems for range limitations, blind spots, and environmental challenges. Include lessons from past UAS intrusions to identify weak points.

c. **Response Weaknesses**: Evaluate existing countermeasures, analysing historical performance data and expert evaluations. Identify the need for rapid response systems, redundancy, and integrated multi-layered defences.

4. **Conduct Risk Analysis**

    a. **Threat Likelihood**: Use intelligence reports, historical UAS attack data, and predictive models to assess the likelihood of threats. Include threat evolution trends and emerging technologies.

    b. **Potential Impact**: Quantify the consequences of UAS attacks on critical assets, including physical damage, casualties, operational disruption, and reputational harm.

    c. **Risk Matrix**: Develop a risk matrix based on historical incidents and expert insights, categorizing threats for effective prioritization.

5. **Develop C-UAS Mitigation Strategies**

    a. **Detection and Tracking Solutions**: Recommend multi-sensor fusion systems, integrating radar, RF detection, EO/IR sensors, and acoustic sensors for comprehensive coverage.

    b. **Threat Neutralization Methods**: Propose diverse countermeasures including RF jamming, GPS spoofing, interceptor UAS, and directed energy weapons.

    c. **Layered Defense**: Design a layered defense integrating physical, electronic, and cyber measures. Include expert consultations during planning and system selection.

6. **Implement Operational Procedures**

    a. **Standard Operating Procedures (SOPs)**: Develop detailed SOPs based on historical incidents, expert recommendations, and system capabilities. Include incident response timelines, escalation processes, and coordination with external agencies.

    b. **Communication Plans**: Establish clear communication channels for real-time information sharing and coordination among all stakeholders.

7. **Train Personnel and Test Systems**

    a. **Training Programs**: Implement training programs in collaboration with C-UAS experts, focusing on threat recognition, system operations, and emergency protocols.

    b. **Simulations and Drills**: Conduct regular threat simulations and drills based on historical UAS incidents, ensuring system readiness and personnel preparedness.

8. **Continuous Monitoring and Adaptation**

    a. **Real-Time Threat Monitoring**: Establish 24/7 monitoring centres with advanced technology for real-time threat detection and response.

    b. **Threat Intelligence Updates**: Regularly update threat intelligence using historical data, expert analyses, and emerging technology trends.

c. **System Upgrades**: Continuously upgrade C-UAS systems and operational procedures based on expert advice, historical incident reviews, and evolving threats.

Annex B

C-UAS Report TemplateC-UAS REPORT						
1.	UNIT	C/S, Name, Contact Number				
2.	DTG	Date, Time of Detection				
3.	METHOD OF DETECTION	See, Hear				
4.	LOCATION OF DETECTION	Grid Ref, Number/Name				
5.	DESCRIPTION a. Observation	Describe activity seen				
	b. Attitude	Aggressive, neutral, don't know				
	c. Type	Rotary	Fixed Wing			
	d. Number	Single	Multiple			
	e. Payload	Visible	Not Visible	Type		
	f. Size	Small	Medium	Large		
	g. Height	Grounded	V Low	Low	Medium	
	h. Heading	North	East	South	West	Hovering
	i. Other	Lights	Colour	Speed		
6.	ACTION TAKEN Consider ROE	e.g. observing, taking cover, engaging				
Post Incident Considerations EOD CLEARANCE EXPLOITATION INFORM LOCAL AUTHORITIES