NATO STABILITY POLICING
CENTRE OF EXCELLENCE

NATO
OTAN

STABILITY POLICING AND THE DRONES' WAR: NEW CHALLENGES FOR NATO COUNTRIES' LAW ENFORCEMENT AGENCIES AND INTERNAL SECURITY ARCHITECTURES

FINAL REPORT

AA.VV.

Stability Policing and the Drones' War:

New Challenges for NATO Countries' Law Enforcement Agencies and Internal Security Architectures

Stability Policing and the Drones' War:
New Challenges for NATO Countries' Law Enforcement Agencies and Internal Security Architectures.
AA.VV.

ISBN 979-12-5539-044-2

Tecnografica di Rossi Franco & C. Sas
Via 1° Maggio, 6
36066 Sandrigo (Vicenza)

In September 2023, aside a meeting to which I had participated in Bucharest (RO), as Director of the NATO Stability Policing Centre of Excellence, I was admitted to an office call with the Romanian Jandarmeria Leadership. That was the ideal occasion, as newly appointed Director (I had been on the job only for a couple of months), to introduce myself to one of the most active and robust contributor to the Centre's activities, and to present my "Lines of Effort" (LoEs) for the upcoming triennium. Included in my LoEs, there was the list of the potential research areas for the year 2025, that included the general theme "**drones**".

I clearly recall that my formal presentation – which until then had flown without any particular incident – had suffered an abrupt stop when I presented the slide mentioning the focus of our research for 2025: the high-ranked Official to whom I was presenting, without even waiting for me to start reading the list of activities, stopped my presentation and abruptly asked

"**Drones: why 2025? We need them now**".

For me – apart from an initial embarrassment for having underestimated a topic that would have revealed itself to be so

relevant and challenging – that episode was an epiphany of the diversity of perspectives existing not just across the Alliance, but even within the small community of the NATO SP COE.

Thanks to that episode, I was able to perceive how extended and different might be the relevance assigned to a topic – or a threat, like in this case – based on the geographical area of provenance of the interlocutor, and how much strength and richness might come precisely from this diversity of perspectives, if adequately and timely intercepted.

So, as Director of a NATO-accredited "think-tank", I accepted the challenge posed by the "observation" of my Romanian counterpart, that day in Bucharest, and took the responsibility to deep-dive into the issue of the **drones' proliferation and spill-over from conflict zones** (and particularly, in the specific case, from the **Ukraine-Russia warzone**).

I reckon now, after almost a year of research and commitment of my excellent personnel – and particularly of the NSPCOE *Lessons Learned Branch* – that the choice made was the correct one, that the topic deserved – and still deserves – a thorough study, for its urgency, considering the dynamics of the Eastern Flank of the Alliance, for its complexity, because of its interactions with different traditionally non-contiguous cognitive domains (such as the Collective Defense and Internal Security ones), and for its relevance for the Alliance as a whole.

This is certainly a first step towards the full understanding of a very complex and multifaceted problem.

Certainly, it represents a step that **had to be made**.

The results of this research outline, first of all, the strong (and yet undisclosed) potential of an active integration of the Internal

Security remit of the Alliance – that, as it is commonly known, pertains to the competence of each member-State – with the Collective Defense architecture, through an **innovative** (though allowed by the current set of relevant doctrinal publications), **understanding of Stability Policing** as the tool through which channeling that potential into the full availability and utility for the Alliance.

Under a specific thematic perspective, this paper reveals the existence of a huge "grey zone", well below the surface and the evident "tip of the iceberg" of the drones' subject, where the blurred borders between the Collective Defense and the Internal Security remit of the Alliance constitute the ideal "hunting zone" for Hybrid and Irregular Warfare maneuvers. The drones' proliferation and use, in this grey zone, for malicious gains, loudly calls the full involvement of the Law Enforcement Agencies, aside of the conventional defense tools of the Alliance, through the fostering of their awareness, readiness and resilience against this specific, unconventional threat. Through the words of brilliant and exceptionally dedicated Subject Matter Experts coming from many institutions and entities across NATO and Europe, wisely coordinated by the NATO SP COE Lessons Learned Branch personnel, this paper will try to define the exact perimeter of a potential "policing gap" existing in the Alliance, and will try to establish a road-map to fill this gap, for the better performance of the Collective Defense against these unconventional threats, and for the full understanding of the possible, full integration of systems and architectures belonging to so different – and so close – *cognitive domains*.

Luigi BRAMATI
Colonel, ITA Carabinieri
NATO Stability Policing CoE Director

EXECUTIVE SUMMARY

In today's dynamic security environment, affected by a large variety of threats, the Alliance faces more challenges than ever before. In this regard, to support its qualified and specialized contribution to the Alliance and to its Sponsoring Nations, NATO Stability Policing Centre of Excellence (NSPCoE) is constantly committed to evolve and to adapt the Stability Policing (SP) capability to the wider NATO threat awareness and landscape readiness.

Considering the challenges illustrated in the NATO 2022 Strategic Concept, in order to support the Alliance's "*360º approach*"; NSPCoE organized a dedicated unclassified workshop (WS) from 6 to 8 March 2024, to support the Alliance with its specific expertise, in the remit of the civil-military integration of systems, facing new challenges such as non-cooperative, malign and potentially armed drones.

In the light of the ongoing Russo-Ukrainian conflict, the crisis in the Middle East, Africa and Central America and with reference to the observed uncontrolled UAVs proliferation, the aim of this event was to gather stakeholders, subject matter experts and practitioners from NATO, NATO Countries, EU and other IOs along with the SP Community, in order to identify how Law Enforcement Agencies (LEAs) play – or should play – their role in an harmonized "system of systems" landscape.

In other words, the idea at the base of the workshop was to analyze, how the "collective defense", engaged in its endeavor of facing the dynamically growing threat posed by the proliferation of weaponized drones, is missing a substantial contributor, that happens to be a primary actor in the mitigation of the threat itself under the perspectives of the situation awareness and protection of civilians.

As a natural subsequent speculation, in the light of the discussions originated within the workshop, NSPCoE and the stakeholders regrouped together in the event, analyzed the

adequacy of the existing Stability Policing doctrine as an effective tool to support the awareness, readiness and resilience of the Alliance towards the specific threat.

NATO defines Stability Policing (SP) as *"police-related activities intended to reinforce or temporarily replace the indigenous police in order to contribute to the restoration and/or upholding of the public order and security, rule of law, and the protection of human rights"*[1].

To talk about Stability Policing and its range of application in NATO operations, the current doctrine requires two fundamental requirements: a crisis (originated by destabilizing factors such as a war, a major natural disaster, civil unrest, famine, etc.) that affects governance and, therefore, stability; and a "policing gap", that is the gap between local police capabilities and a level of effectiveness considered functional to establish/maintain a Safe and Secure Environment and the Rule of Law, whose filling is intended to contribute to foster governance and subsequently stability.

Translated into practical terms in the current scenario, the Ukrainian crisis represents an example of crisis that needs to be addressed for its spill-over effects also in the Alliance territories.

In fact, direct or indirect actions, hybrid or irregular warfare maneuvers, or chain-effects over civil population (such as internal mass displacement) from the warzone, represent potential threats that might be mitigated also through the enhancement of the capabilities of the local LEAs.

In this sense, LEAs are (or might be) primary players in the collective defense endeavor, contributing to awareness, readiness and resilience of NATO Countries and the Alliance as

[1] NATO Allied Joint Doctrine for Stability Policing (AJP 3.22)

a whole (SP is part of NATO ACT-led Layered Resilience Working Group).

It is for this reason that NSPCoE has started investigating the drones/UAVs subject **under a policing perspective**.

In the current hybrid scenario, characterized by several multifaceted challenges and threats to security, SP represents the ideal "tool" to provide the Alliance with a broader analysis capability. In particular, SP might represent the key to better understand the threat posed by the drones' proliferation and spill-over from the warzones of the globe, considering that the area of major effectiveness of these relatively new threats lays where the boundaries between the collective defense and internal security realms are thin and often blurred.

Under these circumstances, SP should be regarded as a military tool – capable of being used by the military-strategic leadership, fully integrated in the military decision-making processes – carrying a 360 degrees policing mind-set and expertise: a "*bridging factor*" between traditionally non-contiguous cognitive worlds, such as the collective defense and the internal security.

In this sense, Stability Policing can be a booster, also from an intelligence perspective, of the ability of "*connecting the dots*" emerging from the two cognitive worlds, ensuring a cognitive edge also in the described complex security environment. In fact, the capability that might be considered typical of a SP practitioner, is that to bear the lenses (both green and blue) of those two different cognitive worlds, providing the Planner and the Commander a wider understanding of reality, observed from different perspectives and with different sensitiveness, breaking – or, better, "bridging" – the boundaries of the military and civilian worlds.

Starting from a 'Lessons Learned' (LL) perspective, the intent of the WS was to explore the subject matter across the

entire DOTMLPF-I[2] spectrum, and to provide the Alliance – once defined the SP role and competence, accordingly with the current NATO doctrinal framework – of that **wider perspective** deemed useful to **better understand and then to counter** the threat posed by the drones' proliferation and spill-over from the war zone.

[2] Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities, Interoperability

INTRODUCTION: THE KEY POINTS

During the preparatory phases of the workshop, the first observation that clearly emerged was the need to define the role that Law Enforcement plays when engaging with non-cooperative drones' threat. The absence, within the Alliance, of a common response pattern from an Internal Security Architecture perspective – including a shared legal framework and shared capabilities – has been identified as a key factor to be analyzed.

Moreover, as already observed in the case of the operations within the cyber domain, there is not a clear distinction between what is the "military" part of the threat and the "civilian" portion of it, particularly if we look at it from a competence/legal authority perspective.

These characteristics of being nested in the "grey zone" among security systems, elevates the resorting to drones' operations to a relevant factor – and a major threat – particularly in a context of hybrid warfare, where state actors and non-state actors are both aligned in terms of offensive capabilities.

Another emerging point is that the concept of drones' use is closely linked to the development of Artificial Intelligence (AI) applied to the automation of systems. This consideration leads to the need of starting an ethical discussion about drones' use by legitimate law enforcement/military agencies, not unlikely as an anti-drones' capability.

In general, for the purposes of the workshop, the discussion was structured in two main **cognitive areas**:

1) **legal framework**,

2) **capabilities** (both from a training/skills and equipment perspectives), for the Alliance's LEAs to face the drones' threat.

From an "operational" perspective, the observations of the workshop were structured in a way to embrace two main aspects: 1) **interception of active non-cooperative drones**, 2) **management of landed/crashed drones**.

Interception includes the possibility for Law Enforcement (particularly in proximity of areas bordering with a conflict area, such as the Ukraine-Russia war Theatre of Operations) 1) to be equipped with and trained to use counter-UAV (CUAV) systems (radiofrequencies, direct energy or kinetic weapons) in order to intercept/disable small drones (typically class I, or in some cases class II drones, in or out of control); 2) to be provided with procedures/communication tools to ensure a timely information flow towards the national air-defense Authorities; 3) to be provided of educational/training products, aimed to raise awareness on the risks posed by rogue drones' activities among local population, including interception activities; 4) to be supported by a factual analysis of the legal aspects connected to the conduction of interception activities (e.g. the balance of risks for the local civilian population, that is paramount for Law Enforcement).

The *management of the landed/crashed drones* (all classes) includes: 1) the dissemination/retention, by LEAs to the minimum level, of all needed safety/security measure (EOD/IED) for first responders approaching landed/crashed drones such as Law Enforcement, especially in the case of civilian drones equipped with explosives ordonnances); 2) aspects of technical exploitation of landed/crashed drones remnants, including the defense/intelligence perspective: under this category comes to relevance the Crime Scene Management (CSM – which should include highly technological forensic techniques), some legal aspects concerning the information/intelligence flow, the competences of the local Public Prosecutor/Justice and, most of all, the relationships between the technical exploitation for intelligence purposes and the secrecy of criminal investigations (particularly, the possibility of the timely exploitation, by the intelligence community, of the information extracted from the recovered materials, in presence of an ongoing criminal investigation).

Each of the two cognitive areas of the research (*Legal Framework* and *Capabilities*), applied to the two aspects of the problem (*interception* and *management*), define **the perimeter**

of the potential "policing gap" of the Alliance's Law Enforcement Agencies facing the drones' threat.

THE ORGANISATION AND THE CONDUCT OF THE WORKSHOP

In preparation for the WS, a preliminary stakeholder analysis has been conducted by the NSPCoE, in order to identify a set of contributors who could design an initial framework of the investigation, that would cover both strategies : operational and tactical level.

A full list of the participating organizations is provided in Annex A.

The working level session was introduced by seven presentations, with the aim of providing a common initial background to all participants and to offer additional information, useful to sustaining the following conversations within the panel discussion (CV of the ESMEs involved in Annex B):

- Dr. Joanna SIEKIERA, *International lawyer, legal Advisor*;
- Mr. Sean BITTICK, *Office C-UAS and Capability Development, NATO HQ Innovation Hybrid Division*;
- Dr. Michele PAVAN, *Intelligence & Geopolitical Advisor – CEO CUAS GROUP Srl;*
- Dr. Chris JENKS, *Senior Law of War Advisor National Security Law Division Army –U.S Department of Defense*;
- Prof. Christian ENEMARK, *University of Southampton;*
- Mr. Antonio FARELO, *Innovation and Technology Officer Innovation Centre Directorate, INTERPOL;*
- Lt. Col. Laszlo SZUCS, *NATO Counterintelligence Centre of Excellence;*

After the presentations, each of them describing, from different perspectives, the actual and potential role of LEAs (and SP) within the drones' war, the 27 participants were

regrouped in two different panels of discussion, dedicated respectively to the ***Legal Framework*** (moderator Dr. SIEKIERA) and to the LEAs ***Capabilities*** (moderator Mr. BITTICK).

During the discussion, among participants, (purposely coming from very diverse backgrounds), several issues and relevant considerations emerged.

PRESENTATIONS

1. Mr. Sean BITTICK – Current NATO HQ efforts and where SP could be used as an added value

There are critical gaps and challenges in addressing drone warfare. Firstly, there are procedural and content-related gaps in approaching drone technology, including the slow adaptation of doctrine to match the rapidly evolving field. The rise of *Class 1* drone warfare has necessitated a response from NATO HQ, which evolved from counter-terroristic measures, to dealing with drones as conventional warfare tools. The different stakeholders involved view CUA's efforts differently. Some see it as air defense, force protection, or border patrol, these differences underscoring the complexity of the issue. This complexity is aggravated by the easy availability of drones and rapid innovation in both UAS and CUAS solutions.

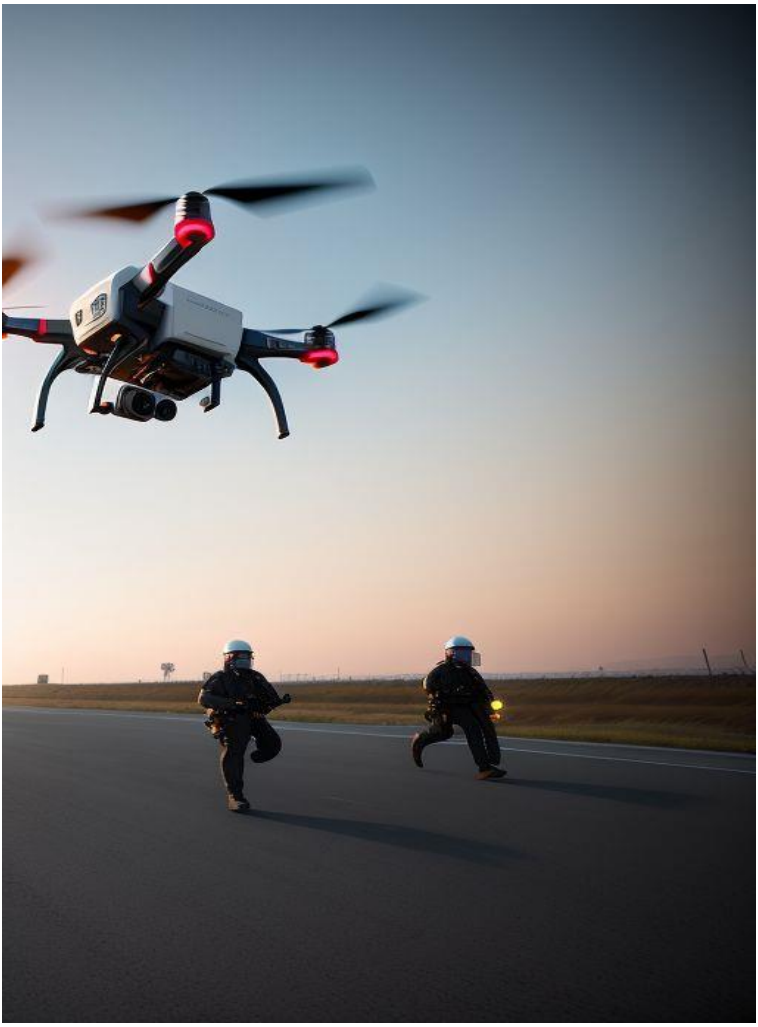
To tackle these challenges, there is a need for improved communication and urgency in addressing malign UAS use, extending beyond the military and including politicians and civilians. The focus should be on future-proofing technology and policies, looking beyond the present to create proactive systems.

Training in counter-UAS is currently varied across countries, these differences highlight the need for standardized, innovative, and future-proofed training practices. Some suggestions could be leveraging existing models to develop a NATO-wide training course and improving curriculum development and instruction processes.

There are also gaps between military and LEAs in dealing with non-cooperative UAS systems, particularly regarding the decision on when drones become a Law Enforcement or military matter and, on the collaboration, needed between military and LEAs during peace and war time. The ideal operational cycle for CUAS involves the seamless integration

of technical operations and ensuring optimal communication between various entities involved.

There is a huge need for collaboration and communication among all stakeholders, military, Law Enforcement, and others, and there are big gaps which need to be filled in doctrine, training and operational strategies necessary to efficiently face the complexity and rapid evolution of the UAS and CUAS fields.



2. Mr. Chris JENKS – US ARMY, law and policy counter UAS systems.

As the NSPCoE considers its potential role in response to the escalating concerns surrounding counter-UAS, the US Army's experience with these systems may potentially be relevant. The US Army has encountered challenges in the acquisition, training, targeting, and exploitation following the downing of a UAS. The Russo-Ukrainian conflict served as a pivotal event, signaling a profound shift in the nature of warfare, due to the extensive deployment and utilization of UAS on the battlefield. Notably, Ukraine expending approximately 10,000 small/*Class 1* UAS/month catalyzed fundamental changes within the US Army force structures.

The US recently experienced the threat posed by UAS, when a one-way UAS killed three US Army soldiers in Jordan. This event underscored critical gaps in air defense capabilities and UAS reconnaissance. The ability to detect incoming enemy UAS, which are now utilized by both state militaries and non-state actors including organized armed groups and terrorists, has emerged as a pressing concern.

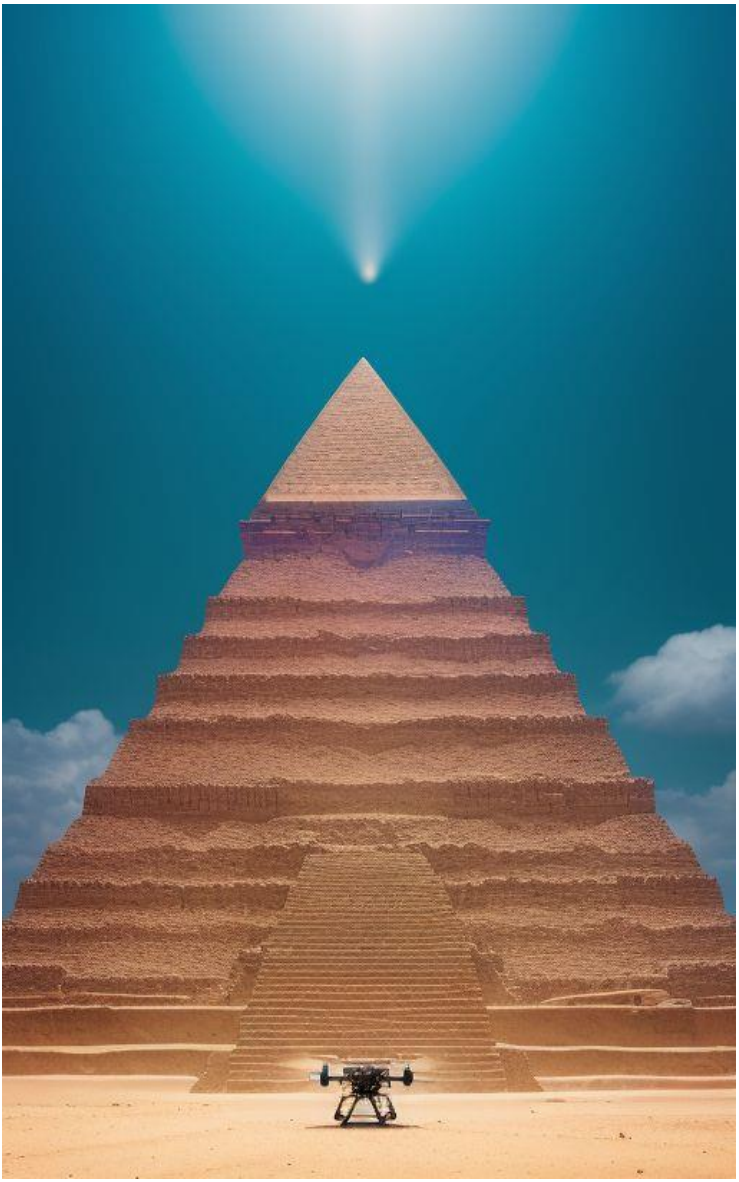
In response to these challenges, the US Army has initiated significant organizational changes within its force structure. These changes include heightened emphasis on training, equipment upgrades for units, modifications to force structures, and increased attention towards air defense capabilities. Notably, artillery upgrades, particularly in air defense artillery (which had previously been overlooked and underused), have received renewed focus and investment.

There are various types of CUAS systems and technologies, ranging from kinetic methods (involving soldiers actively engaging UAS) to net capture systems, directed energy systems (such as lasers), jamming techniques, spoofing, and electromagnetic pulse (EMP) devices. There is a strategic prioritization of CUAS capabilities within military and Law

Enforcement tasks, as well as the subsequent handling of downed UAS systems following interception (including scenarios where drones crash, return to their starting points, or are retrieved by CUAS operators).

Legal complexities surrounding CUAS operations are extensive, both domestic and international legal frameworks. In terms of domestic legal challenges, there are not many areas where militaries or Law Enforcement can train on how to down a UAS. Additionally, there are barriers within US law that restrict the sale or acquisition of Chinese UAS and there is the need for coordination and compliance with regulations to mitigate unintended consequences such as interference with civilian communications. In terms of international legal challenges concerning CUAS, these systems constitute weapons and there is a requirement that they receive a legal review under the law of war. There are many differences in weapon review processes across nations, the countries which are party to Additional Protocol I of the 1949 Geneva Conventions conduct reviews as a legal obligation, while the US conducts reviews as a best practice policy.

Lastly, frustrations with traditional CUAS acquisition procedures are demonstrating the need for innovative procurement methods to keep pace with rapid technological advancements observed during conflicts such as the Russo-Ukrainian war. Along with that is the need to improve technology sharing between military entities and fostering soldier innovation within legal boundaries.



3. Dr. Michele PAVAN – Threats, systems and solutions to Unmanned Aerial Systems and Counter Unmanned Aerial Systems

It is important to analyze the international context of drone use, particularly in regions such as Ukraine and the Red Sea, where asymmetric warfare is prevalent. It is, therefore, useful to start with basic information: the scenario. Over time there has been a clear division between national and international scenarios. Today this difference has almost disappeared. However, to facilitate the understanding of threats, we can imagine a division between the domestic and the international/foreign context. Perhaps it is easier to call it "operational." At the national level we identify scenarios that we see today in the Middle East, Africa, and certainly in "peace" contexts in Europe as well:

1. Asymmetric - unconventional - multi-domain conflict scenarios.
2. Scenarios of illicit activities and/or attacks in contexts of peace.

At the foreign/international level in addition to the classic domestic scenarios we add the scenarios that were thought not to occur anymore such as the case of Ukraine or between Israel and Iran:

1. Symmetrical conflict scenarios
2. Asymmetrical conflict scenarios - unconventional - multi-domain
3. Scenarios of illicit activities and/or attacks in peaceful settings.

A number of everyday threats, often underestimated or underreported, are identified at the national level, including maritime threats, organized crime, terrorism, border security issues, communication threats, espionage and counter-espionage (carried out with drones), and threats to public events.

Starting from the very basic information, it is necessary to start with a proper classification of drones: *Class 1, Class 2* and *Class 3* that are equal at the Italian, NATO, and EU levels. Such a classification would make it possible to coordinate the response to threats at the police (Law Enforcement) or air defense (military) level. The challenges in combating CUAS threats are many; there is a great need for integrated defense and Law Enforcement efforts, predictive policy development, and interoperability among stakeholders in both response and management of drone airspace.

A variety of military and Law Enforcement measures are and must be deployed to address threats from unmanned aerial systems, with a focus on surveillance, monitoring and control missions.

Electronic espionage and communication spying itself with the so-called "drone in the middle" is a Cold War methodology, in which the cell phone connects to the nearest phone cell,

which in this case may be installed on a drone, here the data goes through this repeater and not to the farthest antenna. In addition, the drone can pierce a building's Wi-Fi by downloading network data.

Among the threats, it is important to remember, and it is easily demonstrated, that the international context is increasingly complex in regard to relationships among NARCOS, Terrorism and Organized Crime making not only economical but also technological deals, including drones and anti-drone systems. Threats should not be understood as single, but as a cross-correlation of multiple threats.

To summarize, threats are :

- illegal maritime and border activities
- maritime attacks (container ships, etc.)
- electronic and communication espionage
- terrorism and organized crime
- prison smuggling (drugs, telephones, etc.)
- pedophilia
- attacks on events and demonstrations
- attacks on critical infrastructure: gasifiers, critical infrastructure, transportation networks, distribution networks
- violations of privacy

According to various studies carried out in the "civilian" context, there are many types of drones in addition to commercial ones: self-built, modified, automatic/autonomous, etc. (Class I) + military and others (Class II and Class III) with which it is possible to carry out the above-mentioned illicit activities.

An effective and efficient response to the indicated threats involves:

- The use of constantly updated systems;
- Integrated systems with all involved (military, security and law enforcement). This reduces expenses and fully meets the concept of inter-operability, especially for law enforcement activities;
- Predictive policing analysis for determining precursors;
- Identification of drones and pilots (legislation and specific UTM platform). In legislation, for example, mandatory identification in conjunction with the purchase of a drone. At the same time, a UTM air traffic management system to complement the classical ones for aircraft and helicopters shared with the police forces of a territory;
- Classified acquisition of C-UAS systems;
- UTM platforms that also include C-UAS "feeds."

C-UAS solutions must be adaptive, scalable, reprogrammable, and interoperable. Single, multiple, hyperspectral, and multi-domain solutions are needed to detect, mitigate, and ultimately neutralize hostile or "uncooperative" drones. There are different types of systems: cyber warfare and related electronic countermeasures (Wi-Fi - UMTS - GNSS - VHF - UHF - ISM - GSM - LTE). But it is also useful to evaluate directed energy systems. The type of response should be coordinated and adopted depending on the drone classification and deployment scenario. It is crucial to keep in mind that such systems are not sufficient to "eliminate" the threat.

The real challenge is the countering of drones traveling on LTE networks (4G and 5G) because in this case it is important to authorize a preemptive action that allows preemptive eavesdropping activity on phone cells to intercept a drone's data stream and thus monitor the area of interest. In addition, it is important to use active and passive C-UAS systems, along with UTM management systems that can talk to each other. Such arrangements, coupled with the cross-correlation of data/information at the inter-ministerial and inter-agency levels allow for an adequate response to the problem.

The phenomenon regarding the number of Italian companies on the market that are characterized by "foreign" participation often including Chinese, or that use Chinese technology resold as if it were Italian, in the UAS and C-UAS sector should be noted. Using such systems or making use of such companies can seriously compromise the security of the country.

In addition, it is also useful to consider UAS as solutions that benefit the military and police forces. Not only as possible threats. In this case, UAS solutions must necessarily include:

- Ability to realize IPB (Intelligence Preparation of the Battlefield) and territory and threat monitoring in daytime, twilight and nighttime contexts.
- EO payloads (electro-optical camera systems) must return certified images that constitute admissible evidence in court (Law Enforcement sector).
- Real-time images can be securely shared enabling integration/convolution and C2 (command and control) in an interoperable manner (e.g., State Police, Carabinieri). Including solutions with safety, resilience and low-noise features essential for the sensitive operational environment.
- UAS control can be relocated to operate with the lowest possible operational profile, diversifying takeoff and landing points. System architectures and platforms must ensure maximum risk reduction for operators while maximizing mission efficiency, effectiveness, and interoperability.

- Solutions that reflect EASA and C-Class markings and have FTS where applicable.

But at the same time, they must meet these requirements:

- Secure (full encryption), integrable into U-Space, certified, equipped with artificial intelligence.
- Have sustained autonomy to ensure uninterrupted mission execution.

- Resist jamming from saturation.
- Quietness.

To complement UAS and C-UAS systems, it is critical to use UTM or dedicated drone airspace management systems. There are systems that enable a multitude of services in a single platform:

- Tracking of drones in flight equipped with an identification system.
- Identification of drones in flight without an identification system (if the platform is connected to anti-drone systems).
- Use of the platform, unified, to fly drones.

Such a platform would solve the problems of "safety" for flight and "security" for national airspace or on a mission. It is important to keep in mind that when it comes to security with C-UAS systems for military and Law Enforcement activities, it is possible to have a fixed system to protect places and infrastructures, but also mobile and portable systems that also fit in a backpack and perform multiple functions. For example, even disabling Wi-Fi from housing units and the ability to integrate with other systems. There are also 100% passive systems. In civilian areas, these detection-only systems are useful to install in sensitive areas or as an extension of active systems so as to have specific control of an area. Finally, there are more complex systems such as laser weapons. In this case, these are systems that can be installed aboard ships or deployed in military areas abroad. The protection of bases within one's own state is already complex because one has to assess where the drone will fall, collateral damage, and, most importantly, to the continuation of the laser beam, which also risks touching aircrafts flying on the same trajectory higher up.

Finally, the use of complementary systems such as stabilized platforms for use of UAS and C-UAS systems, for takeoff and landing from boats, even small ones, or on pickup trucks for mountain operations. The possibility of data collection and information analysis supported by artificial intelligence

(OSINT/GEOINT) is of paramount importance. The potential of AI in improving intelligence collection and integrating drone Law Enforcement systems is a positive development in addressing evolving threats by reducing the possibility of error and supporting the analyst in different activities. This way three goals would be achieved :

- Collect and classify as much information as possible, according to the specifications required by the analyst.
- Having special alerts of some information that would otherwise be lost with regular alerts.
- Tracking the information. For example, if one enters a photo of an area, one can recognize with some degree of certainty whether that photo was taken in India, Pakistan, or Bangladesh, and perhaps in which city, if not even on which street.

4. Mr. Antonio FARELO – Project Courageous, a Coordinated Approach to Counter Unmanned Aerial Systems

The Project Courageous: a coordinated approach to Counter-Unmanned Aerial Systems in Law Enforcement addresses the increasing challenges posed by illegal drone activities and the need for a comprehensive strategy to counteract such threats. The initiative is a collaborative effort led by the European Commission and involves various stakeholders, including Law Enforcement Agencies, research and technology organizations, and standardization bodies.

On the current landscape, over 500 commercial C-UAS are available, each with distinct features and capabilities. However, the effectiveness of these systems varies significantly depending on the operational environment, and there is a lack of robust evidence to support performance claims. The absence of uniform testing methodologies makes it difficult to compare systems and establish reliable benchmarks for performance.

Project Courageous aims to address these challenges by developing a standardized methodology for detecting, tracking, and identifying C-UAS systems. The project has a focus on performance requirement collection, test methodology development, and validation through trials in real-world environments. The trials, scheduled for completion by September 2024, are taking place in Greece, Belgium, and Spain, providing valuable data on the performance of various C-UAS solutions.

The initiative also emphasizes the importance of standard scenario development, which involves analyzing past drone-related incidents, reviewing current C-UAS frameworks, and defining high-level threat scenarios. This process will communicate the creation of Key Risk Indicators (KRIs) and the development of comparative metrics for C-UAS solutions.

In conclusion, Project *Courageous* represents a significant step towards establishing a unified, standardized approach to C-UAS testing and assessment. The project's structured timetable of activities, including the development of standard scenarios and performance requirements, will ultimately lead to the formalization of testing methodologies. This standardization will serve as the foundation for global efforts in C-UAS assessment and implementation, ensuring the safety and reliability of systems deployed to protect aerial spaces.

5. Prof. Christian ENEMARK – Drones, policing and ethical force

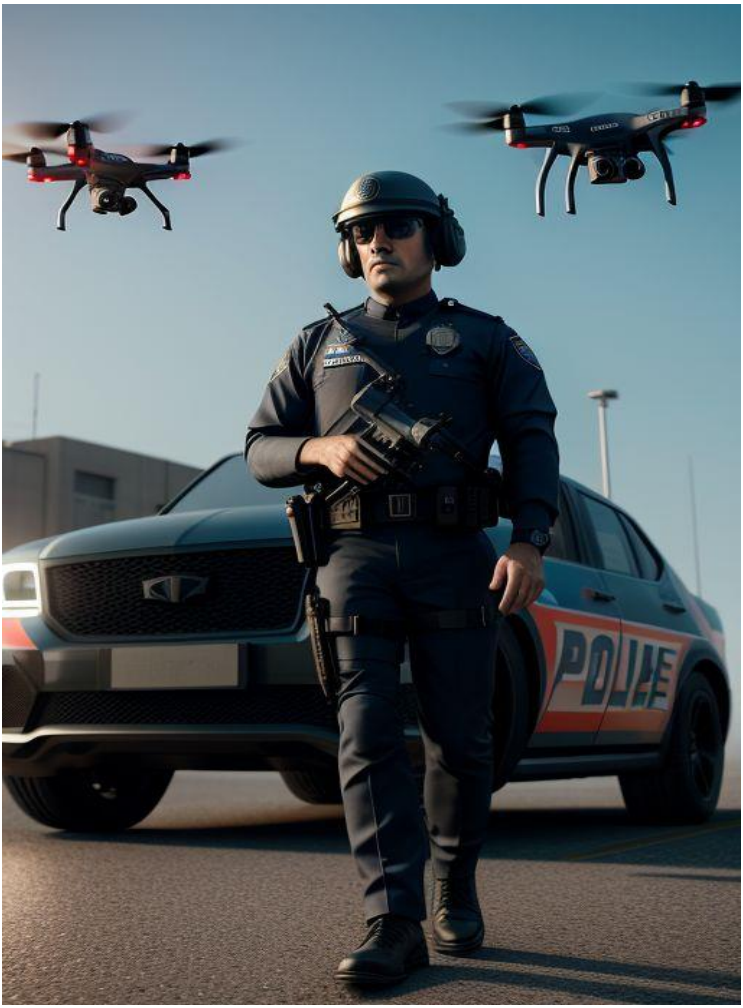
There is an important ethical dimension inherent in the use of drones within policing and security contexts, particularly considering their increasing weaponization and the resultant moral complexities. Drone violence continues to occur in "grey zone" scenarios, and this can complicate ethical dilemmas surrounding state-sanctioned use of force.

Central to the discussion is the distinction between stability operations and traditional warfare, and how this distinction impacts the ethical considerations surrounding drone deployments. There should be more reflection on what constitutes effective Stability Policing, and there is a critical need for clear ethical guidelines to govern the responsible use of drone technology in Law Enforcement settings.

A key concern is the relationship between effective policing practices and the potential integration of drones into Law Enforcement operations. There are important questions to be answered about which entities within LEAs should have access to drone technologies, and about what regulatory constraints are required to ensure accountability and prevent potential misuse of drone systems. The expanding and uncertain definition of "drone" (which often refers to a broad spectrum of technologies beyond mere weapon platforms) also complicates the tasks of making ethical assessments and designing regulations.

There are also many ethical challenges associated with one-way-use drones designed for lethal purposes, such as suicide drones or loitering munitions. These drones are well-suited to warfare, but they have limited capacity for de-escalation or non-lethal engagement in a Law Enforcement context. Due to this, there is a need for state stewardship over drone technologies and explicit political commitments to define and uphold ethical standards in drone deployment. Particular attention must be devoted to the potential problem of extrajudicial drone strikes,

especially when drone technology facilitates a blurring of the boundaries between conventional warfare and Law Enforcement activities.



The increasing militarization of some domestic police agencies is already a cause for some concern, therefore, there should be a robust ethical framework to govern militarized police forces and particularly to restrain their deployment of drones in civilian settings. Ethical principles for drone use (contained within a code of ethics) could include necessity, proportionality, and precaution in policing actions. A comprehensive drone code of ethics could also be designed to address any ethical concerns associated with using C-UAS technologies in different kind of circumstances.

A drone code of ethics could facilitate collaborative efforts among decision-makers, lawmakers, researchers, and other international actors to address the illicit miss-application of drone violence and to promote the responsible use of drone technologies.

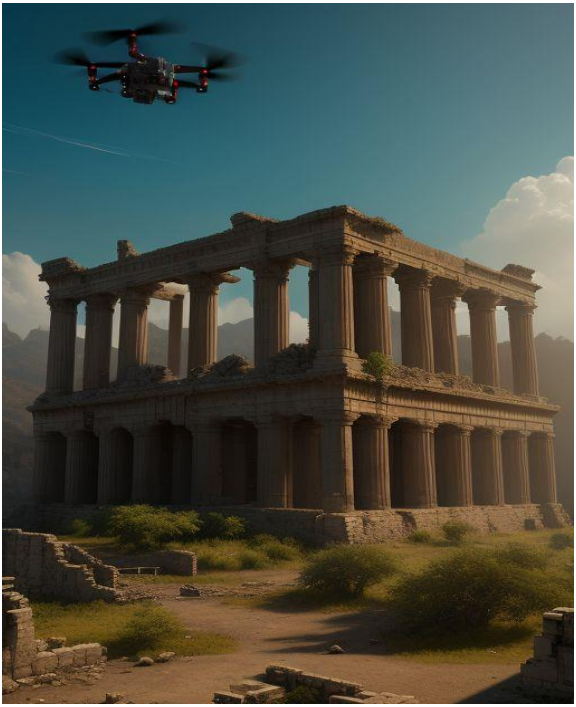
It is useful to draw attention to similar incidents, such as the lethal use of a remote-controlled police robot in Dallas in 2016, which highlight the legal and ethical complexities inherent in drone-assisted operations, particularly when the applicability of Law Enforcement ethics or military ethics is unclear. It is important to delineate clear boundaries between Law Enforcement and military activities to mitigate public confusion and to ensure that drone deployment practices adhere to the right kind of ethical standards.

6. Dr. Joanna SIEKIERA – Legal Panel Moderator

International law does not codify the usage of drones at universal level. Also, not every state has decided to pass adequate laws in this emerging domain. What is even more significant is that various states might indeed understand and interpret usage of drones, their description, categorization, and possible criminalization of misusing of unmanned aircrafts in contradictory manner. Just like with the term “cyber”, “cyber security”, “cyber threat” or “cyber-attack”, we are still missing the agreed and unified definitions. This, however, can be easily explained by the fear of states to give the firm, final and legal-binding norms, which on one hand would facilitate work of internal services, yet, on the other hand, it would enable cyber criminals to act under the threshold of the given definition and therefore escape responsibility. This state of fact (and laws) cannot be surprising when we acknowledge the true core of international law.

The most critical principle here is the sovereignty of states. Only sovereign states, as the primal actors of international relations, possess full autonomy to act however they wish, within the boundaries of international law, without explaining their deeds to anyone. NATO, as a political-military alliance, while not only military (as it is falsely believed), is an intergovernmental organization composed of 32 sovereign states. The Alliance itself does not have armed forces, but its forces are composed of those of 32 sovereign states. Only the European Union possesses legal personality, and its norms are binding on both member-states and their citizens. The examples here are indeed the "drone law": *Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency and Commission* implementing *Regulation (EU) 2019/947 of 24 May 2019 on the rules, and procedures for the operation of unmanned aircrafts* are two documents which are legally binding to those of NATO member-states which are EU members, too. They require the implementation to national legislations, which will take time and most likely will run in a slightly different manner due to assets, needs, and technological advancement of each member. When it comes to NATO, a doctrine on the usage of unmanned aircrafts can be established, yet it is in the sole states' will to acknowledge, obey and implement it. That forms a political-legal challenge which

will definitely affect security. Due to this normative reason, combating totalitarian regimes breaching international law and order, as well as gaining in relevance and power non-state actors (NSA), becomes more and more intertwined. Political and defense arrangements are easier to form than legal engagements.



However, any international treaty on drones or, for instance, Artificial Intelligence, will not guarantee peace and stability without enforcement measures and mechanisms.

Maneuvering between legal loopholes has been, unfortunately, mastered by both Russia and China, who use legal warfare (law fare) to exploit ambiguities in international law and thus leverage their position and malicious, inhuman, and illegal actions. Using drones by Russian Federation against Ukraine, NSA, like Houthis, a terrorist group in Yemen against American soldiers and sailors, or the People's Republic of China in the South China Sea against the Philippines and perhaps soon against Taiwan, proves NATO cannot wait for any international regulation on drones (like a United Nation treaty or other multilateral agreement).

Preparing a political declaration, formed as close as possible to an international declaration, could help NATO member states to look through their own constrains (national caveats), legislative limitation, and technical incapability. Interestingly, the concept of a "drone attack", within the framework of EU, highlights the legal responsibility assigned to a pilot. It is a human who takes the whole responsibility, just like within the concept of a "robot-soldier". It is the operator of such a vehicle, or machine who will be deemed responsible under disciplinary and criminal measures if they miss the regulations in this domain. As it was mentioned, there is no universal "drone law", which leaves a lot of vicious possibilities for criminals or hostile actors. Yet, any regulation must not be an enumerated and close list of definitions of a drone, a drone attack and drone

threat. Just like with cyber, it is safer for us to leave any definition open and general in order to keep any possible criminal activity accountable within the newly established norm. Again, establishing a final definition opens a door to act below its threshold.

7. Lt. Col. Laszlo SZUCS, NATO Counterintelligence Centre of Excellence - The role of counterintelligence within NATO in addressing drone threats

Project *PHONEIX* aims to provide comprehensive guidelines for counterintelligence operations focused on handling drones that have been downed over NATO bases. The core objective is to analyze and understand the tactical intent, usage patterns, and potential human networks associated with drones to gather essential intelligence.

There must be an emphasis on threat identification, where counterintelligence efforts focus on unraveling how drones can pose security risks. This involves delving into the origins of drones, their patterns of use, and the networks behind their operations to collect crucial intelligence. Great importance must be also given to differentiating between various UAS systems and tailoring counterintelligence approaches accordingly.

The counterintelligence handbook addresses *Class 1* drones (under 25 kg), while specialized operators should be designated for handling more advanced *Class 2 and 3* drones. The integration of counterintelligence strategies into NATO's UAS threat protection is of huge importance. These strategies can contribute to internal standard operating procedures (SOPs), force protection, intelligence gathering, and operational planning.

In terms of response protocols, there must be a structured approach post-drone incident, covering initial response at the scene, custodianship of the drone, and forensic exploitation of collected data to extract valuable intelligence. Clear procedures are deemed essential to prevent operational overlaps and ensure effective handling of drone-related incidents within NATO bases.

The content of the counterintelligence handbook includes comprehensive sections covering international drone laws, management strategies from a counterintelligence perspective, and specific scenarios for drone recovery and reporting within NATO operations. Tools like the Annex E incident report form and C-UAS flowchart, developed under Project *PHOENIX*, aim to facilitate drone recovery and reporting procedures.

The collaborative nature of counterintelligence operations within NATO is essential and therefore the outcomes and information from the form will be shared within NATO intelligence systems. The counterintelligence handbook is designed for adaptation beyond NATO to support national security systems and bridge Stability Policing with military operations, underscoring its versatility and applicability in diverse operational contexts. Counterintelligence has a critical role in effectively responding to evolving security challenges posed by drones within NATO and beyond.

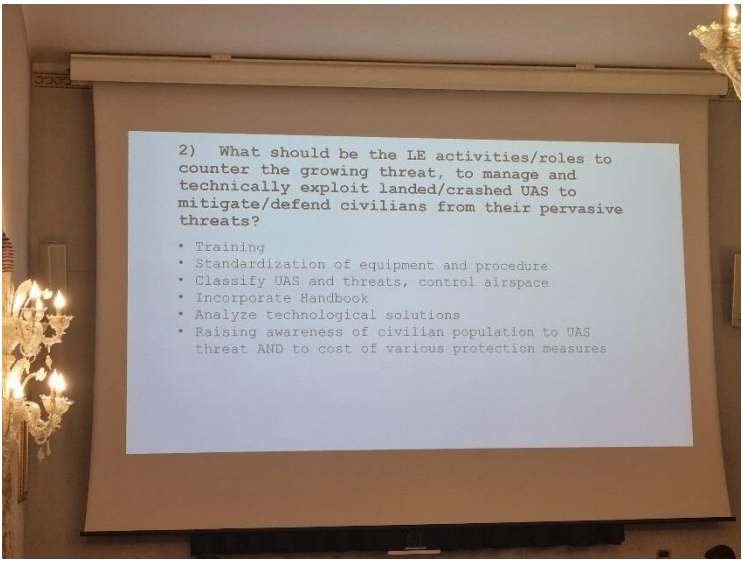
PANELS

During the event, ESMEs' inputs have been gathered and analyzed across the entire DOTMLPF-I spectrum, to assess the operational framework and to identify the initiatives of/for the Alliance's LEAs in such a hybrid warfare scenario.

The analysis was also fruitful in order to identify shortcomings of the current Stability Policing doctrine, assessed also in the light of the multiple challenges acknowledged by previous experiences and from the collected experience.

To get a more "straight to the point" response, attendees were asked to perform their analysis guided by a set of pre-determined questions (prepared by the COE Lessons Learned Branch – Analysis Section team before the event).

The questions were then divided according to the topic discussed in each of the two panels as follows.



QUESTIONS

PANEL 1 – The role of the LEAs in the Drone's War. *Legal Framework*

1.1. Which of the already existing doctrinal publications better match with SP role in contrast to the growing threat posed by non-cooperative drones? (non-cooperative Unmanned Aircraft Systems-UAS, commonly known as "drones" are to be defined according to the nature of non-cooperation, that includes criminal, illegal – intended regulatory breach – or amateur conduct).

The first topic that the Panel was tasked to explore, was the applicability of the Stability Policing doctrine to the drone-related topic, and particularly to analyze the adequacy of the documental architecture that constitutes the NATO doctrinal constructed around Stability Policing.

In fact, to adequately address the contribution of SP to counter the emerging challenges posed by non-cooperative unmanned aircraft systems, we recognized as crucial the analysis of the existing doctrinal publications, according to their applicability (and adaptability) to the current evolving threats landscape.

Within the current SP doctrinal corpus, the panel was able to detect a potential gap in the alignment between the drone threat and the traditional SP mandates.

As a first point, no doctrinal publication singularly and comprehensively addresses the intersection between the threat posed by the proliferation of drones and the Law Enforcement contribution to Collective Defense.

Moreover, the existent SP doctrine itself reveals certain ambiguities regarding its geographical scope and operational parameters.

Presently, SP doctrine mainly focuses – although not in a binding fashion – its applicability within contexts of fragile/failing/failed states, thus permitting the application of its

potential within the NATO territory only after a considerable conceptual stretch.

This might well be considered as a limit that underscores the need to overrule conventional conceptual boundaries rooted in the historical origin of Stability Policing.

As a paramount action to release the full Stability Policing potential it is necessary to remove the cognitive perimeter of its application to "outer" Countries, considering its range of operations in diverse operational theatres, including those characterized by structural stability – but that might be subject to an attempt of de-stabilization, as, for example through hybrid/irregular warfare maneuvers – such as the Allied Countries.

In this framework, SP would come on hand **not only as a factor for stabilization of a de-stabilized context**, but also – and even more relevantly – as a powerful **contributor to awareness/readiness/resilience against those attempts to de-stabilize a structurally stable context**.

Fundamentally, SP doctrine applicability is defined by three pivotal parameters: 1) a crisis that affects (or might affect) governance, and therefore is cause (or might be cause) of instability); 2) a "policing gap", considered as a gap in the performance of that function of governance that is policing; 3) a mission intended to fill the "policing gap", typically defined as "temporary replacement" od "reinforcement" mission.

Considering the "extended" understanding of the SP range of application, the evolving threat landscape caused (also, but not only) by non-cooperative drones manifests a quintessential example of a "policing gap", allowing the triggering SP engagement.

Still, according to the current formulation of the relevant NATO publications, they can provide foundational principles relevant to SP operations, but their applicability to the contemporary challenge of non-cooperative drones remains blurred and in general left to the interpretation of the reader.

A concerted effort to revise and update SP-related publications therefore deemed needed, and is actually ongoing, through the ordinary process of revision of NATO's doctrine.

It will be essential for NATO stakeholders to develop the revision of the SP doctrine also tailored to the new set of threat facing the Alliance, including the one posed by non-cooperative drone incidents.

As a secondary effort, it will be beneficial for the whole SP/LEAs community to plan a dedicated secondary level doctrinal production concerning the specific threat: a guide/handbook aiming at the harmonization of procedures and minimum skill requirements would be the effective tool in order to foster successful SP operations – and LEAs increased efficiency – also in the drone domain.

This emergent threat will challenge our capability to fully embrace interoperability and the multidisciplinary approach to operations. It eventually will result in a strengthened SP set of capabilities, that will play the role of a crucial factor in promoting awareness/readiness/resilience against the constantly evolving security threats to the Alliance.

1.2. Assuming the drone's topic as belonging to the SP Doctrine remit, what should be the LE activities/roles to counter the growing threat, to manage and technically exploit landed/crashed drones and to mitigate/defend civilians from their pervasive threats?

Considering the threat of the drones' proliferation and spillover from conflict zones, a multifaceted LE approach is indispensable. This approach must necessarily originate from robust training and educational initiatives, aimed at enhancing LE personnel's awareness and ability in the joint mitigation effort against any drones' threats.

Such training and education programs should include the analysis and awareness on various drones types and – most of all – offensive capabilities, with a connected analysis of the tactical best practices for their detection, interception, and safe neutralization.

Standardization also emerges as a decisive factor.

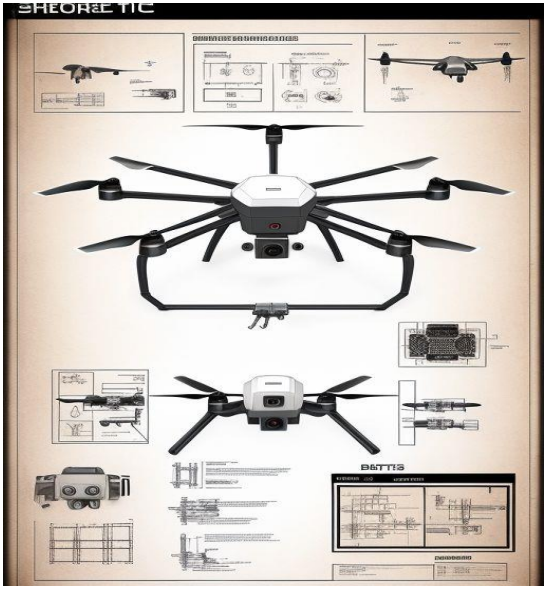
There's a critical need for the harmonization of equipment and operational protocols across LE agencies, in order to ensure seamless interoperability in responding to drone-related incidents. This standardization should also extend to the classification of drones, that according to the experiences gathered in many incidents, should be based on their operational characteristics and threat profiles. This type of classification would be best suitable to tailor response strategies based on the different capabilities expressed.

Vital to this effort would be the development and dissemination of a comprehensive **handbook**, encapsulating relevant knowledge on drones, serving as a repository of best practices and procedural guidelines for both LE personnel and military alike. Through this handbook, structured and based on the similar educational tool already available within NATO, upgraded and completed with the necessary Policing integrations and procedural observations, stakeholders could foster their LEAs readiness to drones' operations, understanding capabilities, vulnerabilities, and the relevant legal frameworks governing their remit.

Leveraging their unique position as a bridging factor between Law Enforcement and military, SP Units – in any of the formation that they may assume, based on the nature of the mission – can in general facilitate the integration and dissemination of drone-related strategies and tactics into the broader LE framework, bolstering collective awareness/readiness/resilience against this constantly evolving – also in terms of intensity – threat.

In synthesis, the implementation of drones-management capabilities within the Alliance's LEAs needs a multifaceted approach encompassing training, standardization, classification, and educational initiatives.

By fortifying LEAs capabilities and promoting cross-sector collaboration, SP Units – but also the SP expertise in general, whose spreading throughout the whole Alliance components is one of the objectives of NATO SP COE – can contribute to the mitigation of the threats posed by the drones' proliferation and spill-over from conflict zones, always considering a "*people-centric*" approach, primarily focused on safeguarding civilian populations from any harm.



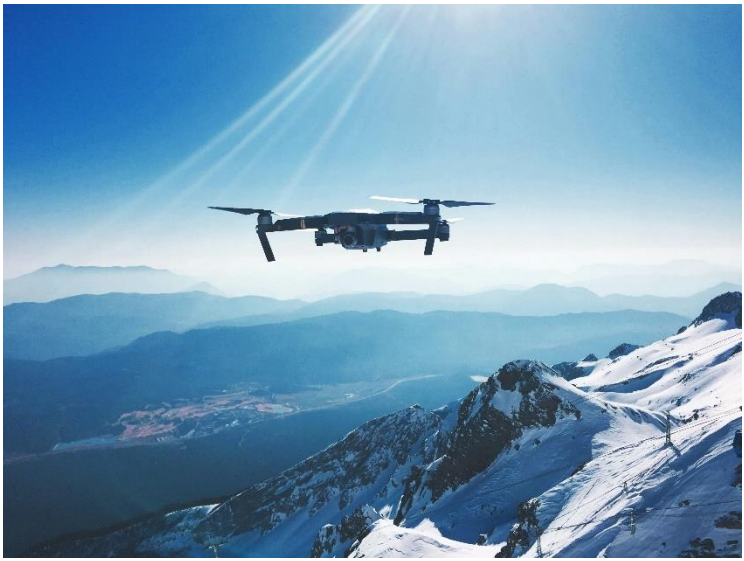
1.3. To which domain should drones be considered a part of (air, sea, land exclusively or multi-domain)?

The range of drones' operational domains transcends traditional boundaries, rendering them typical multi-domain assets.

In fact, drones manifest their influence not only in the airspace, but also into maritime and terrestrial domains, thereby challenging conventional categorizations.

Moreover, drones intersect with advancements in cyber and space domains, further complicating their classification.

Drones, often improved by artificial intelligence (AI), demonstrate an unprecedented capability for **data-centric operations**. This inbuilt data-centricity empowers drones to serve for efficient and time-effective collection, transmission, and dissemination of information, elevating their relevance within the broader intelligence and information-sharing environment.



1.4. How Allied Nations' Internal Security Architectures should be structured and how could they be efficiently harmonized (in terms of C2 capabilities) between themselves and NATO, to confront the new threat with a systematic approach, avoiding potential constraints/limits/caveats affecting the LE activities in countering drones?

At its core, the responsibility for safeguarding civilian populations resides within each sovereign Nation, thereby forming the foundational premise upon which collaborative efforts and harmonization trends can be built.

Within the framework of the international cooperation, particularly within NATO, avenues for information sharing and procedural standardization are crucial pillars for increasing collective resilience against drone-related threats.

Crucial to this effort is the need to harmonize rules and procedures governing military and Law Enforcement activities, thereby promoting interoperability and synergy in confronting shared challenges. This also requires aligning operational protocols and ensuring coherence in resource allocation and capabilities between conventional forces and LEAs.

In practical terms, several initiatives can be taken into account to mitigate the constraints delaying effective counter-drone activities carried-out by LEAs. Among them: 1) refining communication protocols to expedite information sharing among LEA agencies; 2) simplifying response mechanisms and investigative procedures; 3) enhancing training programs on drone-related threats.

However, it is important to acknowledge the complexities in achieving **legislative harmonization** at a pan-NATO level, given the divergent legal frameworks and interests of all member states. While aspirational, the pursuit of legislative harmonization may prove unrealistic in the short term.

Emphasis should be placed on providing **pragmatic solutions** and **facilitating communication between stakeholders, in order to bridge the gap between the existing legal bounds** (e.g. in the sharing of information in parallel with a criminal investigation) **and what the intelligence community needs**. By harmonizing terminology and practical tools for interagency collaboration, NATO can adopt a more cohesive and coordinated approach to countering drone, thereby enhancing the collective security of its member states.

1.5. What is the contribution of the private sector in training LEAs across the Alliance? Is there a possibility of a contribution also at operational level?

It's clear that private entities play and can play a key role in using their expertise in various areas of contribution with LEAs empowerment, through training programs, acquisitions processes, legal frameworks development, and sharing of cutting-edge technological advancements, beyond the mere theoretical knowledge.

Private sector can facilitate the assessment and use of intelligence products, enhancing situational awareness and operational effectiveness.

However, it is essential to tread cautiously regarding the extent of private sector involvement in military/LEAs capacity building: in fact, while the collaboration with the private sector is sometimes indispensable, the need for robust oversight and regulatory frameworks to safeguard against potential conflicts of interest or compromises in operational integrity, must be always fulfilled.

It’s therefore essential to maintain a balance between leveraging the expertise of third party-entities and preserving the autonomy of LEAs.

It's crucial to recognize that, while the private sector can offer valuable insights and support, the **decision-making and management process must remain within the public sector**.

Entrusting the private sector with leadership roles risks influencing the public agenda with private companies’ interests, potentially undermining the efficacy of LEAs operations.

While the private sector can serve as a valuable ally in the pursuit of collective security objectives, it’s imperative to maintain a clear distinction of roles and responsibilities, to ensure alignment with public sector priorities.

Collaboration must be guided by a shared commitment to enhance security rather than by conflicting interests.

1.6. When does a drone become a weapon for military purposes?

The transformation of an Unmanned Aircraft System (UAS) into a weapon for military purposes depends on defining the distinction between a mere platform and an instrument of destruction. While an UAS is not inherently a weapon, its utilization in a one-way destructive manner, such as for a suicide explosive drone, classifies it as a weapon. The distinction between a UAS functioning as a platform versus a component of a weapon system underscores the complexity of its classification. If employed in a manner that entails a one-way flight trajectory aimed at causing damage upon impact, the UAS assumes the status of a weapon, irrespective of whether it is explicitly armed or not.

The legal nuances regarding the classification of a UAS as a weapon or weapon system require detailed examination. In fact, the pivotal transition moment of a UAS turning into a weapon occurs when it is employed for destructive purposes, even if it was not originally conceived for such ends.

It is important to delineate clear boundaries between Law Enforcement and military activities to mitigate public confusion and to ensure that drone deployment practices adhere to the right kind of ethical standards. This distinction holds great implications for LE efforts in addressing the proliferation of malicious drone activities, necessitating differentiated responses based on the contextual demands of war zones or peacetime scenarios. Heightened awareness and effective response strategies are therefore essential for mitigating the threats posed by drones to public security.

The rise of complex scenarios of drone-related threats, makes the need for robust regulatory frameworks and technological solutions even greater to discern friends from foes. It is possible to retrieve some positive examples of this regulatory systems in the geo-zoning limitations of drones' flight, the issuing of standardized *Unmanned Traffic*

Management (UTM) platforms, and the availability of pragmatic mechanisms conceived for the mitigation of the threats to public security posed by non-compliant and malign drones' activities.

1.7. How aware are we of the risk of uncontrolled sales of drones or part of them on markets?

The unregulated proliferation of drones' sales within legitimate or black markets is a significant threat. This risk can be faced by leveraging intelligence capabilities and applying specific regulations on transactions, while also monitoring trends in drone sales and usage, identifying any indications of illicit or unauthorized transactions, and assessing the implications that these phenomena may have for the common and national security.

Regulatory interventions play a crucial role in mitigating this risk: the obligation of licensing requirements is just an example of binding regulation that might serve as an effective mechanism to limit the sale and usage of drones.

By mandating licenses for drone ownership and operation, authorities can establish a framework for accountability and oversight, reducing potential misuse and unauthorized proliferation.

The black market 's role in expanding the illicit trade of drones further worsens the foreseeable landscape. **Bridging the gap between LEAs intelligence and regulatory agencies** is an essential step – and another way on how policing activities can influence the overall security scenario – for effectively combating this phenomenon.

Dialogue, collaboration and sharing of actionable intelligence between LE agencies and regulatory bodies can facilitate targeted interventions to dismantle or at least contain illicit supply chains.

Collective defense intelligence is also essential to face the transnational nature of the illegal drones' market. By promoting cooperation and information-sharing among Allied Nations, collective defense intelligence mechanisms can improve situational awareness and allow coordinated responses to emerging threats posed by the uncontrolled sale of drones.

1.8. To what extent operating in a comprehensive approach within drone's environment may require liaising:

- *at national level, within the LE (Courts, GOs, Authorities, Private sector, Research Institutes)*
- *within the Alliance*
- *externally, with Law Enforcement Agencies/services, IOs such as IPF, EUROPOL, Interpol, UN police units?*

Operating within the intricate landscape of drone-related challenges requires an all-inclusive approach that extends various levels and involves collaboration across multiple entities.

At the national level, coordination within LEAs is essential.

This coordination implies developing partnerships between courts, authorities, GOs, private sector stakeholders, research institutes. Also pooling resources, expertise, and intelligence can enhance situational awareness and response capabilities.

Within NATO, collaboration is crucial for ensuring a cohesive approach to address drone-related threats: these could be by sharing of best practices, conducting joint exercises with "*blue force elements*", and promoting interoperability among member states, also in the police sector.

Externally, engaging with LEAS and International Organizations is essential as it can ease information sharing, joint operations, and promote efficient capacity-building

initiatives to combat transnational drone-related security challenges.

While successful information chains may exist at a tactical level and yield valuable outcomes, broader coordination faces challenges such as information-sharing hesitancy among stakeholders ("**data-jealousy**" was the term utilized by Gen. Philippe Lavigne, NATO SACT, in occasion of the "*Multi-Domain Operations*" conference, in September 2023).

It is significant to note that while LE primarily focuses on civilian operations, collaboration with military entities is essential in addressing many aspects of drone-related challenges, particularly those with security implications.

Navigating the complexities of the drones' proliferation and spill-over from conflict zones threats, requires effective liaison and collaboration across National, Alliance, and international levels.

Promoting cooperation between all the relevant stakeholders, will be increasingly mandatory to develop an effective comprehensive approach, and to mitigate the risks emerging from this new set of threats.

PANEL 2 - LEAs Capabilities

2.1. What are the most relevant and effective tools that LEAs need to contrast malign actions by drones?

To effectively counter malign drone usage, LEAs need a multifaceted toolkit including various elements. Firstly, education and training are paramount: LE personnel at all levels must possess a general understanding of drones' operations and offensive potential. This includes training on Standard Rules of Engagement (SRoE) and Standard Rules for the Use of Force (SRUoF) for C-UAS responses.

Additionally, specialized training blocks dedicated to recognizing malicious intent during drone incidents are necessary as well as upholding scene integrity and evidence preservation.

Situational awareness is another critical component: LEAs must have access to real-time intelligence, through an efficient reporting mechanism, to keep the units deployed on the ground informed about the current drones' threats. Establishing a secure reporting database (where a brief paragraph on location, material, serial number of drones collected from an incident is inserted) accessible to authorized personnel can facilitate efficient data collection and analysis, supporting management resources, as well as criminal investigations, intelligence-led operations and threat assessments.

Deploying blue UAS for Law Enforcement purposes can improve aerial surveillance and response capabilities.

Additionally, identifying the importance of cybersecurity is essential in safeguarding against potential cyber threats posed by drones.

A flexible threat assessment framework is crucial for effectively evaluating and responding to evolving drone-related threats. This framework should adapt to changing circumstances and incorporate inputs from various stakeholders, including intelligence agencies and judicial/administrative authorities.

Moreover, building societal resilience is crucial in mitigating the effects of drone-related incidents. This involves not only bolstering physical infrastructure, but also promoting community engagement and resilience-building initiatives.

Improving the legal framework in which to bind drone usage is imperative. Measures such as mandatory registration and regulating supply chains, as well as the incorporation of non-removable software for location tracking, can help effectively to limit the drones' offensive potential.

Additionally, establishing clear reporting procedures and collaboration protocols with relevant authorities**,** including Judicial and the Intelligence Community, is essential as intelligence gathered through collaborative efforts can significantly contribute to improve investigations and threat mitigation.

Addressing malign use of drones requires a comprehensive approach, that includes education, training, situational awareness, technological solutions, legal framework, and collaboration among stakeholders.

By equipping LEAs with the necessary tools and resources, they can effectively mitigate the relevant threat and safeguard public safety and security.

2.2 If drones can be considered belonging to the remit of SP Doctrine, what should be the LEAs activities/roles to counter the growing threat, to manage and technically exploit landed/crashed drones and to mitigate/defend civilians from their pervasive threats?

The incorporation of drones as a topic pertaining to the SP doctrine should be assumed. Given in fact the centrality of the collaboration between agencies belonging to **traditionally non-contiguous cognitive worlds** (such as the Collective Defense and the Internal Security framework), in presence of a potential malign structural action that **nests and thrives in the gap/grey zone between these systems**, a "Policing Gap" might certainly be detected in the flaws and imperfections of the connections between these two frameworks.

Overall, malign use of UAS might certainly be intended as a **warfighting method intended to destabilize an opponent's institutional architecture** (***governance***), through threatening the safety and security of civilians.

LEAs should prioritize the establishment of **effective coordinated intelligence-sharing and reporting mechanisms** to disseminate all available information to all levels of the internal security architecture (national dimension), and subsequently to the collective defense relevant networks (intelligence, legal, air-defense, etc.).

A specific focus such as the peculiar added value of the police expertise, must be ensured for the safeguarding of the chain of evidence preservation originated on the scenes of drones' incidents.

Training on UAS and C-UAS should be promoted from the beginning to the end of LE and military careers, at different levels of specializations based on the units' requested level of capability.

A good example of leveraging databases is the case of the Afghan HUMINT database, which should serve as a model for sharing vital intelligence across borders, particularly in countering organized crime activities.

LEAs must prioritize the development of aerial denial and drone capture strategies over mere destruction, as captured drones can provide valuable data for investigations and intelligence.

Engaging the public through social media platforms is also essential to raise awareness about the threats posed by drones. Social media can be a powerful tool, especially to inform young people about the risks connected with drones' misuse.

Moreover, LEAs should advocate for legislative reforms to address regulatory gaps and enhance operational capabilities. Initiatives such as creating competitions to design effective social media campaigns could help build public support for legislative reforms.

However, the dissemination of data on various databases poses risks to information security. To address this risk, LEAs should work to consolidate information dispersed on various databases and determine protocols for legal access to safeguard efficient data analysis.

Furthermore, creating a new methodology for collaboration among stakeholders and intelligence sharing is essential. Utilizing UTM platforms for proper drone identification can improve LEAs' capabilities in identifying and mitigating drone-related threats.

SP can play a role in this process, according to the consolidated paradigm of the threat to governance/stability (as a malign act that can be designed throughout the full spectrum of the hybrid paraphernalia), the "policing gap analysis" and the tailored mission intended to support the Nations' effort to fill the detected gap.

LEAs can really develop a cohesive and effective response pattern to the threats posed by the drones' proliferation and spill-over from conflict zones, in so doing integrating substantially the overall readiness of the alliance security architecture.

2.3 Do you think LEAs need to create special dedicated teams to counter drones' threats?

Creating dedicated teams within LEAs to counter the threats posed by drones particularly in crisis or conflict zones is essential. These specialized teams are needed as LE currently lacks the requisite capabilities to effectively counter the emerging drone threats at a more sophisticated level.

In parallel, the SP knowledge remit also lacks this capability, that should be developed both as a support to the training and education effort (towards the LEAs capacitation) and as a SPU niche capability.

In general, reporting mechanisms have also a critical role in any counter-UAS effort.

The establishment of a dedicated distribution list – among the major/willing LAEs across the Alliance – for short-term information dissemination, paired with quarterly updates (over a longer horizon of 2-5 years) and the integration/connection of the existing LEAs databases would ease and promote access to critical intelligence about this type of threat. Also counterintelligence units/actors could have a substantial role in this process, in providing support to investigations and by establishing parallel in-depth intelligence analysis to ensure operational efficiency.

In these regards, while the NSPCoE serves as a focal point for knowledge distribution, it operates outside the NATO chain of command, therefore limiting its authority to sharing intelligence and information relevant to NATO/National Decision-making process.

As such, a self-standing collaboration pattern and a coordination network that involves LEAs and all relevant NATO communities of interest are essential for a comprehensive and effective response to the drone threat.

2.4. To what extent should the NATO Commanders assess drone-related issues during the planning phase?

NATO Commanders must thoroughly assess drone-related issues during the planning phases of the military operation, especially during Phase II, while analyzing the strategic/operational environment.

Moreover, the long-range/long-term influence of social media and public opinion on Law Enforcement underscores the critical importance of including these factors into the strategic planning considerations, particularly in the context of hybrid warfare.

Coordination between the military and civilian spheres is absolutely crucial in addressing drone-related challenges. While C-UAS efforts may align with broader goals, it is crucial to ensure political buy-in for effective operations and vice-versa. Without adequate support from higher headquarters, including on de-confliction and appropriate allocation of resources, operational effectiveness may be compromised.

It's important to note that, **within military operations (and with respect to the air/space collective/national defense)**, while drone threats **primarily fall under the competences of the military**, attention to these issues shouldn't be diminished even when they fall in the civilian realms of issues (e.g. in case of class I/II incidents, virtually invisible to the air defense infrastructure).

Recognizing the multifaceted nature of threats that drones create, implies the need to comprehensively tackle the threat itself, using all tools and instrument made available by the connection of defense/security systems, with the subsequent non-denominational allocation of resources, regardless of whether the threat falls within the military or civilian domain.

2.5. Once the SP role in countering drones' activities has been defined, do you think that drones-savvy personnel are available, properly trained and equipped, within LE units/assets?

As the SP role in contributing to the comprehensive understanding of drones-related threats has been outlined, as a next step it is crucial to assess the availability, training, and equipment of drones-savvy personnel within LEAs units/assets.

While subject matter experts (SMEs) in the drones' remit are undeniably valuable, considering the extent of the needs of the Alliance's LEAs, the most effective approach to disseminate such knowledge appears to be the promotion of information sharing, from tactical to strategical level.

Establishing liaison positions dedicated to sharing information within LEAs on both national and international levels is essential. Moreover, fostering the creation of small-scale collaborative cells within each NATO nation could enhance intra-nation collaboration and disseminate knowledge across various levels of command.

LEAs can result in being invaluable assets if allowed to share the set of information made available through investigations on the ground, in so doing leveraging their expertise even in military contexts. Placing LE liaisons outside their contexts could further strengthen collaboration and knowledge sharing.

In a pure-police investigative approach, prioritizing the disabling/capture of rogue drones rather than seeking their destruction, given the protection of the local communities, is paramount.

The data gathered from such "captures" can provide invaluable intelligence, which could materialize as a strategic advantage to further counter drone activities effectively.

2.6. Should NATO's Countries LE assets include personnel specialized in preserving Drones' incidents "Crime Scenes" (computer forensics and anti-forensics techniques and/or the deployment of mobile forensics laboratories?)

Currently, specialized digital forensic personnel already exist within LEAs, but there is a pressing need for a substantial expansion of their involvement in operations down to the tactical level.

Training initiatives aimed at providing basic level forensic exploitation skills can serve as a force multiplier, while enhancing the capacity of LEAs to effectively handle drone-related incidents. Training can also help lower-level first responders to become the first "filters" to swiftly assess potentially critical situations and pass non-commercial drone incidents to more specialized and better-trained personnel for further investigation.

To preserve drones' crime scenes, rapid exploitation is essential, especially in situations where there are imminent threats to life or critical infrastructure.

However, exercising caution is also crucially important, as rapid exploitation from non-trained personnel or first responders may risk compromising evidence, if not the very safety of the intervening personnel.

Therefore, an approach to exploitation which includes various tiers of trained response and analysis is imperative for security, evidence integrity, and bottom line to facilitate effective investigations and information sharing.

2.7. Which kind of facilities are required to properly support LE for an effective protection of infrastructure from drones' attacks?

To ensure the effective protection of infrastructure from drones' attacks, LEAs require specialized facilities tailored to their operational needs.

Firstly, comprehensive training facilities are essential to providing LEAs with opportunities to develop C-UAS skills.

Secondly, hands-on training in drone detection, tracking, and neutralization techniques is critical for preparing personnel to respond in real-world scenarios. State-of-the-art analytical forensic laboratories are also necessary to enable LEAs to gather evidence on the spot and to run efficient investigations on drone-related incidents based on a time-efficient data analysis.

Specially designed ranges for kinetic and non-kinetic engagements against drones are also vital in providing LEAs with the opportunity to test and evaluate different C-UAS tactics and technologies.

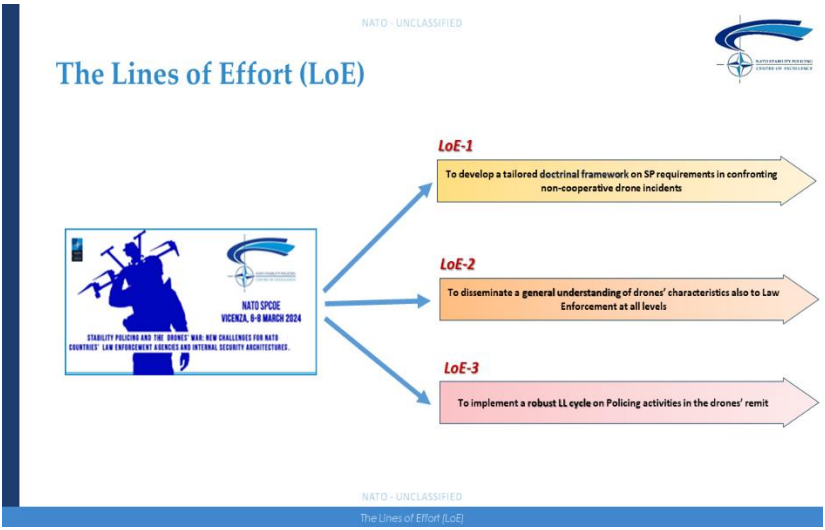
In general, strengthening relationships among allies – and military allies – is essential. Collaboration between and within allied militaries and LEAs to leverage existing resources, expertise, and support in countering drones' threats is fundamental. By working together, allied LEAs and militaries can enhance their collective capabilities and improve the overall security of critical allied infrastructure.

By investing in specialized facilities, training, and equipment, and by fostering collaboration between military and LE partners, LEAs and militaries could provide more effective responses to the evolving threats posed by drones and also improve the safeguarding of critical infrastructure and public safety.

LINES OF EFFORTS

To achieve concrete improvements in terms of updating the existing relevant doctrine and consequently to integrate the LEAs drones' threat management capability, several lines of effort (LoEs), each of them thematically attributed to one of the Branches of the NSPCoE, has been proposed.

These LoEs aim at assisting the development of a concept on SP and the Drones' war (defining and describing the LEAs involvement in this peculiar sector of the collective defense), and providing a roadmap to be followed for this purpose.



LoE 1: DOCTRINE AND STANDARDIZATION: Stakeholders should develop a tailored **doctrinal framework** expressly for SP demands confronting non-cooperative drone incidents (a publication), even though not legally binding (e.g. a *handbook*), but effective as a guide to harmonize procedures and promote successful joint operations in the drones' proliferation/spill-over from warzones remit.

LoE 2: EDUCATION, TRAINING AND EXERCISES: education and training are paramount. LE personnel at all levels must possess a general understanding of drones' characteristics and offensive potential, with a specific focus on **Standard Law Enforcement Rules of Engagement**. Law Enforcement's engagement in counter drones must participate in relevant courses and trainings, identify training gaps, develop relevant courses and, finally, participate in relevant exercises (NATO, COEs, etc.)

LoE 3: LESSONS LEARNED: to acknowledge that NATO/LEAs should develop and implement a strong LL cycle on Policing activities in the drones' remit and, mostly, have access to real-time intelligence through efficient reporting mechanisms. Establishing a secure reporting database serving as a repository of best practices and procedural guidelines for both LE personnel and military alike.

CONCLUSIONS

Our further examination of the workshop's main outcomes has generated several **conclusions and recommendations**.

Gap in doctrine

Conclusion. A gap emerges in a direct alignment with the NATO relevant doctrine with the multifaceted drones' threat, with particular reference to the SP remit. In fact, the existent SP doctrine reveals certain ambiguities regarding its geographical range and operational parameters. In this sense, SP applicability in the face of the contemporary hybrid challenges – including the one of the drones' proliferation and spillover from war zones – remains stretched with respect to an old-fashion vision of the doctrine itself and its genesis.

Recommendations. Stakeholders should encourage the development of a tailored doctrinal framework expressly for LEAs/SP demands in confronting the drones' threat. A publication, even though not legally binding (as example a handbook), might be crucial as an effective guide to harmonize procedures and promote successful LEAs/SP operations in the drone remit, including the definition and uphold ethical standards in drone deployment. Particular attention should be devoted to the potential problem of extrajudicial drone strikes, especially when drone technology facilitates a blurring of the boundaries between conventional warfare and law enforcement activities.

Extending the application of SP principles in diverse operational theatres

Conclusion. SP doctrine delineates – even if not in a binding manner – its applicability within contexts of fragile/failing/failed states, thus limiting its potential utility in NATO territories, including with respect to the drones' threat. This limitation underscores the need to overrule these conventional conceptual boundaries, and extend the application of SP

principles in diverse operational theatres. Standardization emerges as a decisive factor: there's a critical need for an extensive harmonization of equipment and operational protocols across LEAs, as well as in achieving a legislative/procedural harmonization at a pan-NATO level, this being a much more complex endeavor considering the divergent legal frameworks in each member state. The legal nuances regarding the classification of a UAS as a weapon or weapon system require, as example, detailed examination, in order to thoroughly define the pivotal moment when a UAS transitions into a weapon occurs.

Recommendations. In developing/capacitating the relevant Internal Security Architectures, LEAs should consider the need to harmonize rules and procedures governing military and Law Enforcement activities, thereby promoting interoperability and synergy in confronting shared challenges. This also requires aligning operational protocols.

Need for a multifaceted LE approach

Conclusion. A comprehensive approach to the drones' threats requires a multifaceted LE approach, originating from robust training and educational formation. All initiatives should aim at enhancing LE personnel's awareness/readiness towards the specific threat through programs including comprehensive training on drones characteristics and offensive potentials, including the best tactical practices for their detection, interception, and safe neutralization. Comprehensive training facilities are essential to providing LEAs with opportunities to develop C-UAS skills. Secondly hands-on training in drone detection, tracking, and neutralization techniques is critical for preparing personnel to respond in real-world scenarios.

Recommendation. Within NATO, collaboration is crucial for ensuring a cohesive approach to address drone-related threats, like conducting joint exercises with blue force elements, and

promoting interoperability among member states and institutions. Training on UAS and C-UAS should be promoted from the beginning to the end of LE and military careers.

Comprehensive approach

Conclusion. Addressing the threat posed by drones' proliferation and drones' spill-over from war zones requires a comprehensive approach that includes education, training, situational awareness, technological solutions, setting the appropriate legal framework, and collaboration among stakeholders. Coordination within Law Enforcement Agencies is an essential all-inclusive approach, intended to involve all levels within multiple entities. Within NATO, collaboration is crucial for ensuring a coherent approach to address drone-related issues.

This collaboration may assume the form of a process for sharing the best practices, or conducting joint exercises with blue force elements and promoting interoperability among member states.

Recommendation. Foster collaboration between and within Allied Commands and LEAs to leverage existing resources, expertise, and support in countering drone threats.

Multi-domain environment

Conclusion. Drones manifest their influence not only in the airspace but also in the maritime and terrestrial domains. Besides maritime, airspace and land domains, drones intersect also with advancements in cyber and space domains, further complicating their classification. Moreover, drones, often improved by artificial intelligence (AI), demonstrate an unprecedented capability for data-centric operations. The range of drones' operational effectiveness transcends traditional boundaries, rendering them typical multi-domain assets, thereby challenging conventional categorizations.

Recommendation. In categorizing drones' activities, LEAs should consider this unprecedented capability of being part of a multi-domain environment, and take into account all the potential consequences and the available actions to mitigate their threat towards civilians and civil infrastructure.

Private sector

Conclusion. The unregulated proliferation of drones' sales within markets is a significant threat. The black market 's role in expanding the illicit trade of drones further worsens the situation. Bridging the gap between LE intelligence and regulatory agencies is essential for effectively combating this phenomenon. Collective defense intelligence is also essential to face the transnational nature of the drone market. Private sector can facilitate the assessment and use of intelligence data, enhancing situational awareness and operational effectiveness.

Recommendation. It's crucial to recognize that while the private sector can offer valuable insight and support, the decision-making and management processes must remain within the public sector.

Robust regulatory frameworks

Conclusion. The rise of complex scenarios of drone-related threats, makes the need for robust regulatory frameworks and technological solutions to inhibit their weaponization or misuse (including secured identification tools). Geo-zoning limitations on drone flights, standardized Unmanned Traffic Management (UTM) platforms, and offering pragmatic mechanisms for mitigating non-compliant and malign drone activities are some of the tools that will have to be deployed to mitigate the drones' offensive potential.

Recommendation. LEAs should encourage the adoption of legal and technological solutions, through their respective framework, in order to mitigate the drones' proliferation risks connected to their weaponization or misconduct in general.

Info sharing& training programs

Conclusion. Liaising with entities such as the IPF, EUROPOL, INTERPOL and UN police units can ease information sharing, joint operations, and promote efficient capacity-building initiatives to combat transnational drone-related security challenges. Firstly, education and training are paramount: LE personnel at all levels must possess an initial, general understanding of drone operation and offensive potentials, including specific training on Standard Rules of Engagement. A flexible threat assessment framework is crucial for effectively evaluating and responding to evolving drone-related threats. Clear reporting procedures and collaboration protocols with relevant authorities, including judicial and intelligence agencies, are essential. State-of-the-art analytical forensic laboratories are also necessary to enable LEAs to gather evidence to run efficient investigations on drone-related incidents, feeding at the same time the internal/collective defense intelligence chains.

Recommendation. LEAs should prioritize the establishment of effective intelligence-sharing and reporting mechanisms to disseminate information. LEAs should have access to real-time intelligence through efficient reporting mechanisms to stay informed about drone threats.

Investigation and intelligence

Conclusion. LEAs must prioritize the development of aerial denial and drone capture strategies over mere destruction, as captured drones can provide valuable data for investigations and intelligence.

Recommendation. Specific procedures/tactics must be developed, also through the creation of a higher specialized tier of professionals in the drones' countering. Engaging the public through social media platforms is also beneficial to raise awareness about the threats posed by drones, enhancing the possibilities of a timely intervention in case of drones-connected incidents, with the aim of extracting the maximum intelligence possible.

WAY AHEAD

As observed since the initial phases of the workshop, the complexity of the design of a structured, comprehensive strategy to counter the drones' proliferation threat is hampered by the – legitimate – diversification of the internal legislations and security architecture, that as it is commonly known, pertain to the remit of the Nations' responsibility.

This fragmentation is opposed by the structural and tendentially harmonized reading of the challenge and mitigation factors of the "collective defense", where NATO plays a role not only as military commander for defense contingencies management, whether at strategic, operational or tactical level, but also set the level of ambition in terms of individual (referred to the Nations) growth in terms of capability. In other terms, NATO fosters the individual national growth in order to foster and increase the collective weight of the Alliance, well beyond an arithmetical summatory of the single capabilities.

That is the case, as example, of the Layered Resilience, where Resilience itself falls under the responsibility of each NATO Nation, and yet a dedicated Working Group has been tasked to study the topic and to set the threshold of the ideal, systemic resilience of the Alliance as a whole.

In the case of the drones' proliferation and spill-over from conflict zones, while a general policy and set of regulations and doctrinal supports has been issued with reference to the "collective defense" portion of the problem, the tip of the iceberg, that vast majority of the multifaceted aspects of the threat (considered as a whole) lays below the surface, under the competence of the national authorities, and in the remit of the LEAs.

This part, invisible to the collective defense, might well be considered the most relevant in a hybrid/irregular warfare scenario: whether in fact an armed drone is intercepted by the conventional air defense umbrella, that drone actions fall in the remit of conventional warfighting (above the threshold of art.5). A series of small drones, possibly weaponized by design or used as a tool for achieving military objectives (e.g.

reconnaissance and/or intelligence), might well be ignored by the collective defense, and underestimated, or worse not detected as a direct threat to security, by the local internal security agents, that are the Law Enforcement.

By definition, as said before in the present study, this "gray zone" between systems (collective defense and internal security), that by chance happens to be closer to the civilian population and its vulnerability (also from a messaging perspective), is the ideal hunting field for hybrid and irregular warfare maneuvers.

And here comes at hand the role of Stability Policing.

The Alliance LEAs, as per their common, shared standards, might well be considered the best Law Enforcement/Policing agencies in the world. And certainly their professionalism, expertise, best practices, technological advance, resilience, etc. **are assets precious to the Alliance**.

LEAs can play a significant role in the asymmetrical game of the Hybrid and Irregular Warfare.

Stability Policing, with its ability to connect – through the analysis of the "Policing Gap" – the expected level of performance of an internal security actor with its observed capabilities, is the key to parameter the **expected level of ambition** of each single system with the **requirements of an enhanced (with reference to the modern set of threats) collective defense**.

The limit, as said at the beginning of this final paragraph, is the fragmentation of the single legislations and internal security architectures.

But this is not a limit that can frustrate the constant research of the Alliance for a better and more integrated defense.

In fact, through the cooperation – **under the auspices of the Stability Policing doctrine** – of each Nation's LEA, with **a bottom-up process**, the desired harmonization of systems might be achieved.

Initially, through a thorough and detailed process of sharing of the best practices, through the study of the recurring incidents and their lessons identified/lesson learned.

This approach will bring back to the cooperating agencies, overall, a **level of ambition**, and examples of factual, practical resolution of *operational* (intended in the law enforcement jargon) problems.

As an example, the connection between the investigation process – under the control of the judiciary – and the timely alimentation of the intelligence flow might be established through the proposal of "legal shortcuts", to be studied and developed in each single Country/legal system: we saw it happening during the mission in Afghanistan, where the need to ensure the secrecy of the criminal investigations (e.g. started after an attack against the Coalition Forces) was bypassed – with the preemptive approval of the relevant judicial authorities, after a dedicated negotiation – with the urgent need to gather intelligence, critical to enhance the level of the force-protection of the international contingents.

At this point this "legal shortcutting" might well be the first step before a reform or amendment of the relevant legal system, as expected – once experimented on the field – by the law enforcement, and also by the judiciary and the intelligence community as a solution to an otherwise insolvable loophole.

More time-efficient and overall easier to achieve is the capability building effort.

The dissemination of the LI/LL, and the connected expertise aside of the conventional NATO/Military channel, involving instead/moreover the LEAs, will "naturally" enhance the tendency to develop the described capability, as always happens in the world of the internal security.

In fact, apart from primary/secondary, exclusive/shared competence issues, typical of multi-agency internal security architectures (as all the western systems are), LEAs live their capacity development as an existential challenge, used to the rapid and often unpredictable evolution of criminal patterns and modus operandi. The major role, in this case, might well be played by NATO educational and training institutions, Centers of Excellence, Research Centers, etc., that will only have to extend the accessibility to their products not only to the Military

side of the Alliance, but also to the Internal Security portion of the collective defense summatory.

Under this perspective, NSPCoE will play its role with determination, sharing the knowledge of the enormous potential of the LEAs involvement in the collective defense endeavor, there where the gray zone between the systems better hides insidious maneuvers pertaining to the hybrid and irregular warfare paraphernalia.

This workshop is therefore – and as such should be considered – just a starting point, a first, foundation brick of a wider construction, where ideally both the Military and the LEAs will contribute to "fill the gaps" in the collective defense, to achieve a better effectiveness against unconventional threats such as the drones' proliferation and spill-over from conflict zones.

NSPCoE – along with the LEAs that will positively answer to the challenge, add the "blue lenses" vision to the set of doctrinal and educational tools available to the alliance to face the drones-related threats.

Maybe a new, more comprehensive definition/classification of the drones' threat – for the use/operational viability of the LEAs – will ease the LE understanding of the complexity (if observed from a strategic, multi-domain perspective) of the problem, improving the collective responses to this new danger and help furthering the development of a more connected and harmonized Internal Security Architecture.

As said, this is only the first step of this ambitious process, that will also include a deep rethinking of the Stability Policing doctrine itself.

NSPCoE will explore – and plan – further initiatives to foster interagency cooperation around the drones' threat, starting with these first consideration towards a better understanding of the problem and, subsequently, of its possible (and sustainable) solutions.

ANNEX A

PARTICIPATING ORGANISATIONS:

- NATO HQ
- EUROPEAN COMMISSION
- INTERPOL
- SOUTHAMPTON UNIVERSITY, Southampton (United Kingdom)
- CUAS GROUP Srl (ITA)
- US DoD, Washington DC (USA)
- NATO STABILITY POLICING COE, Vicenza (Italy)
- NATO COUNTERINTELLIGENCE COE, Krakow (Poland)
- EURO-ATLANTIC RESILIENCE CENTRE, Bucharest (Romania)
- POLISH MILITARY GENDARMERIE
- ROMANIAN JANDARMERIA
- ITALIAN CARABINIERI
- TURKISH NATIONAL POLICE and GENDARMERIE
- CoESPU, Vicenza (Italy)
- ITALIAN AIR FORCE, CENTRO DI ECCELLENZA PER AEROMOBILI A PILOTAGGIO REMOTO

ANNEX B

CONTRIBUTORS' CVs.

Col. t.ISSMI Luigi BRAMATI

Luigi Bramati is a Colonel of the Italian Carabinieri Corps.
In 1994, Col. Luigi Bramati completed his high school classical three-year curriculum at the Military High School "*Nunziatella*", in Naples, and then joined the Italian Military Academy. He subsequently attended a three-year course at the Carabinieri Officers Academy of Rome, from which he graduated in 1999. That same year, he graduated in Law from the "Sapienza" University of Studies in Rome. In 2003, he graduated in Political Sciences from the University of Studies "San Pio V" of Rome, and in 2004 in "Internal and External Security Science" from the "Tor Vergata" University of Studies of Rome. During the academic year 2014/2015, he attended the Italian Joint Defense Staff College Course (ISSMI Course) at the Center for

Advances Studies of the Italian Defense (CASD), and was awarded a master's degree in international and strategic-Military Studies from the "Roma-tre" University.
He was also awarded the title of Defense Legal Advisor in 2015.
He was appointed to various duties in Italy and abroad, including in Iraq in 2003 as Deputy Provost Marshal of the Multinational Division South-East in Basra, and in 2006 as International Police Advisor and Staff Officer within the Civilian Police Assistance and Training Team in Baghdad. From 2009 to 2015, he served within the Carabinieri HQ National Operations Room, where he was appointed as Chief of the "Situation Awareness" Section. From 2016 to 2019, he served as Assistant Defense and Defense Cooperation Attaché of the Italian Embassy to the United States, in Washington, DC. Following his three-year tenure as the Carabinieri Provincial Headquarters' Commanding Officer in Avellino (Southern Italy), as of June 29th, 2023, he is Director of the Stability Policing Centre of Excellence (NATO SP COE), in Vicenza (North-Eastern Italy).
He is author, among other articles and essays, of a research paper published in 2021 by the Center of Military Strategic Studies (Ce.Mi.S.S.) of the Italian Defense, titled "*Iraq, 2003-2009: Lessons Learned from the Chilcot Commission, Where Stability Policing Could Have Made a Difference. Ten Considerations for Planners and Commanders*".
Born in 1975, he shares with his wife Stephanie and their three children the love for travelling and outdoor sport activities.

Lt Col Marti GRASHOF

Lieutenant-Colonel Marti Grashof was born in 1967 in the Netherlands. He is a Dutch Army officer within the Royal Netherlands Marechaussee. Marti served most of his professional career in multinational operations, mutual international police assistance and in police work in an international context.

In 1989, Marti's first steps in the military were as a conscript and petty officer in the Royal Marechaussee, where he served as MP.

He attended the Royal Military Academy in Breda in 1998, from which he graduated with the rank of Second Lieutenant. He held positions as MP platoon commander, and within the aviation security branch, as Commanding Officer for High Risk Flights at Amsterdam Schiphol Airport.

As a major, Marti was head of the Expertise Centre for Crowd & Riot Control at the Marechaussee Training Center in Apeldoorn, Netherlands. In 2009 Marti was deployed in Afghanistan to the ISAF mission. He served in the province of Uruzgan in the G7 cell of the Task Force Uruzgan. Within the Sector Security Reform branch, he was responsible for the training of the Afghan National Police. After this mission he worked at the General Headquarters of the Royal Marechaussee as Chief Officer for the Director of Operations. From 2012 until 2015 Marti assumed the position of Commanding Officer in the province of Utrecht and Noord-Holland for Marechaussee operations. In 2015 he joined the EULEX mission in Kosovo where he worked as shift leader in the Joint Operation Room of the EULEX HQ in Pristina.
In April 2017 he was, as Lieutenant-Colonel, detached from the Royal Marechaussee to the National Police, to work as Head of the Unit Foreign Affairs, of the National Police Information Service Organization in Zoetermeer, Netherlands.
As of September 2020, he is posted as Chief of Staff at the NATO Stability Policing Centre of Excellence, Vicenza, Italy

Col. Dorin Luta

Colonel Dorin Luta is a Romanian Gendarmerie officer, serving since 2021 as Lessons Learned Branch Head at the NATO Stability Policing Centre of Excellence, Vicenza, Italy.
He holds a bachelor's degree in "*Law*" (2005), a master's degree in "*Management of operational training of gendarmerie units*" (2011) and a post-graduate degree in "*Weapons, explosives and hazardous substances*" (2006).
Furthermore, he is a qualified NATO Lessons Learned Manager (2022) and Staff Officer (2022), a NATO Alternative Analyst (2021), a UN Senior Planner for Peacekeeping Missions (2018) and a EU Common Security and Defense Policy Planner (2017).

His career started in 2001, when he joined the Police Academy of the Romanian Ministry of Interior, to become a Gendarmerie officer. After graduating in 2005, he served as mobile gendarmerie platoon commander (2005-2007), junior staff officer at regional HQ level (2007-2008) and senior specialist at national HQ level (2008-2016).

Before holding the current position, he was head of the International Cooperation and Missions Department within the General Inspectorate of Romanian Gendarmerie in Bucharest (2016-2021). During this position, he was responsible, among others, of all Romanian Gendarmerie's engagements in crisis management operations, under the aegis of NATO (Afghanistan), EU (Kosovo, Georgia, Ukraine, Niger, Mali, Somalia), UN (Kosovo, Mali, Central African Republic, South Sudan, East Timor, Haiti) and ad-hoc coalitions (Iraq).

He attended an EU crisis management international exercise (Saint Astier, 2006), graduated in UN Middle Management Level Course (CoESPU, Vicenza, 2007) and was deployed for short term missions in Iraq (anti-DAESH coalition, 2018) and Afghanistan (NATO RSM, 2019).

He is fluent in English and French and an independent user of Italian.

Cap. Marco Codispoti

Cap. CODISPOTI enlisted in the Carabinieri in 1984 and he was deployed as warrant officer with different operational national assignments: Carabinieri Operational Department Investigative team in Vicenza; R.O.S. Carabinieri Special Operational Group; and overseas: Security Officer-Temporary International Presence in Hebron 2 TIPH2 Palestine; Security officer at the Italian Embassy in Cairo–Egypt; Jordanian Armed Forces Foreign languages school in Zarqa Jordan – Arabic language course; “Qalam wa Lawh” Arabic school in Rabat (Morocco); Bi-lateral cooperation mission at the Emiri Guards HQ– Doha Qatar. He also served four years at Eurogendfor HQ as Intel Assistant.

In 2018 he graduated with the rank of Second Lieutenant at the Carabinieri Officers School in Rome and held the position of Lessons Learned Staff Officer at the NATO SP COE in Vicenza. He was also: a member of the writing team in the development of Special Inspector General Afghan Reconstruction (SIGAR) Report “Police in conflict. Lessons Learned from the U.S. Experience in Afghanistan”; Organizer and developer of "Spoiler threats assessment a shared requirement Conference and workshop"; facilitator of “Battlefield evidence collection" in

favor of Iraqi MoI and MoD project led by Interpol and European Union; SME from ROS Carabinieri, in Combating human trafficking OSCE LIVEX.
He earned a membership from GI-TOC Global international Transnational Organized Crime and the Royal United Services Institute – Strategic Hub for Organized Crime.
He is posted as Analysis Section Staff Officer at the NATO Stability Policing Centre of Excellence, Vicenza, Italy

Dr. Joanna SIEKIERA

Doctor Joanna Siekiera is an international lawyer, legal advisor and academic from Poland. She has been cooperating with the NATO Stability Policing Centre of Excellence since 2021. Dr. Siekiera works as a consultant, lecturer, and Subject Matter Expert in various military institutions (i.a. Finland, New Zealand, Poland, Türkiye, USA), as well as a fellow at the United States Marine Corps University Brute Krulak Center for Innovation & Future Warfare. She did her postdoctoral research at the Faculty of Law, University of Bergen, Norway, and Ph.D. studies in New Zealand, at the Faculty of Law, Victoria University of Wellington. She is the author of over 100 scientific publications in several languages, 40 legal opinions for the Polish Ministry of Justice, the book “Regional Policy in the South Pacific”, and the editor of 7 monographs on international law, international relations, and security. Her areas of expertise are the Law of Armed Conflict (law-fare, legal culture in armed conflict, NATO legal framework) and the Indo-Pacific region, Pacific law, Maritime Security.

Mr. Sean BITTICK

Sean Bittick is the C-UAS and Capability Development officer for the Innovation, Hybrid, & Cyber (IHC) Division at NATO Headquarters in Brussels. He contributes to the evolution of the Defense Against Terrorism and Asymmetric Threats Program of Work (DAT POW) and its role within the IHC Division. He serves as Secretary for the C-UAS Working Group (to include

updating the Terms of Reference, Doctrine development, and the Program of Work), and liaises with internal and external C-UAS stakeholders. His formational experiences derived from service in the United States Armed Forces at the Tactical, Operational, and Strategical levels within the Air Force's Security Forces career field as well as service out of uniform with the United States' Joint Counter-Small Unmanned Aircraft Systems Office (JCO). Sean holds a Master of Arts Degree in European and Eurasian Studies from the George Washington University.

Dr. Michele PAVAN

Michele Pavan is Founder and CEO of MInter Group S.r.l., Founder and President of Mondo Internazionale APS ETS, CEO of CUAS GROUP S.r.l. and Member of the Technical and Scientifical Committee of CESMA - "Giulio Douhet" Center for Military Aeronautical Studies with focus on Military Policy, in particular with the use of satellite technologies and drones. In addition, he is involved in geostrategic and intelligence analysis for International Institutions and Organizations, in Italy and abroad, as Intelligence & Security Advisor for Travel Security and Crisis Prevention particularly for Africa and the Middle East. He is a Lecturer at several University Masters and Postgraduate Courses. He has been Lecturer and Scientific Coordinator at LUM School of Management in Milan for a number of Masters on Diplomacy, European Careers and Geopolitics.

He graduated in International Relations - Diplomacy and International Organizations at the University of Milan, specializing in crisis prevention and foreign policy analysis, particularly of Sub-Saharan Africa and the MENA area - Middle East and North Africa. He focused on the experimental study of prevention factors, distinguished himself in static and dynamic studies, which indicate the evolution of a crisis context, determining its risk and the different variables. Subsequently, he obtained an executive master's degree from SIOI - Italian

Society for International Organization in Economic, Geopolitical and Intelligence Security.
He studied for six months at the European Association of International Studies - AESI in Rome where he subsequently held the position of Director for International Relations and National Activities. He has organized and participated in a number of meetings on crisis prevention at the United Nations headquarters in New York and Geneva, the Pentagon, the United States Department of State, the Permanent Representation of Italy to the United Nations and the European Union, the Embassy of the United States of America in Italy, the Embassy of Italy to the Holy See, the Embassy of Italy to the United States of America, the Italian Consulate in St. Petersburg, the Nunciature in St. Petersburg, the Apostolic Nunciature in the United States, at the European Union, at the CASD, at the Diplomatic Institute Villa Madama, at the Holy See, at Palazzo San Macuto, at the European Commission, at the European Parliament, at the NATO JFC Command, at MGIMO University, at Saint Petersburg State University of Economics, at the American University and at George Washington University.

Dr. Chris JENKS

Chris Jenks is the Senior Law of War Advisor for the U.S Army Judge Advocate General's Corps at the Pentagon in Washington D.C. He also holds an academic appointment as a Research Professor of Law at the SMU Dedman School of Law in Dallas, Texas, where he taught and co-authored textbooks on the law of armed conflict and on criminal law.
As the Senior Law of War Advisor, his duties and responsibilities include serving as the principal law of war advisor to The Judge Advocate General, the Deputy Judge Advocate General, and the Assistant Judge Advocate General for Military Law and Operations. He also serves as a subject matter expert for Judge Advocates around the world, the Army Staff, the Army Secretariat, and for acquisition officials responsible for developing weapons systems. His research

considers the impact of emerging technology on accountability norms across the armed conflict spectrum. A Fulbright Scholars grant recipient, he researched autonomous weapons as part of an interdisciplinary group at Melbourne Law School in Australia. He has presented at a United Nations Convention on Certain Conventional Weapons meeting on autonomous weapons and twice served as a member of the United States delegation to subsequent UN meetings. He has also testified on autonomous weapons before the US Congress' Helsinki Commission and worked with both the U.S. Defense Innovation Board and the National Security Commission on Artificial Intelligence.

Professor Jenks has authored numerous book chapters and articles, including a definition of "autonomous weapons" for the Brill Companion to International Humanitarian Law, on autonomous weapons impact on the international legal order and on animals as autonomous weapons for a book which was awarded the European Society of International Law Collaborative Book Award Prize. He also served as a Research Fellow at the Center for Autonomy and Artificial Intelligence in Washington D.C. and was the lead author of a report Optimizing Classification of Intelligent Autonomous Systems for the US Navy. Prior to assuming duties as the Senior Law of War Advisor for the U.S. Army, Professor Jenks served as the Senior Law of War Advisor to the Ambassador-at-Large for Global Criminal Justice at the Department of State and previously as the Special Counsel to the Department of Defense General Counsel. He served for twenty-years as an officer in the U.S. Army, initially in the Infantry and later as a Judge Advocate. As an Infantry officer he was deployed to Kuwait and Bosnia. As a Judge Advocate, he was deployed to Iraq and in his final uniformed assignment served as the Chief of the US Army's International Law Branch.

He holds a Masters of Law from Georgetown Law in Human Rights, a Masters of Law from the Army JAG School in Military Law, a Juris Doctorate from the University of Arizona College of Law and a Bachelor of Science from the United States Military Academy.

Prof. Christian ENEMARK

Christian Enemark is Professor of International Relations at the Faculty of Social Sciences at the University of Southampton, UK. During 2018 to 2023, he was the Principal Investigator of a major project on ethics and armed drones (DRONETHICS), funded by the European Research Council under the European Union's Horizon 2020 research and innovation program (grant no. 771082). Christian's areas of research interest include military ethics, police ethics, international security, arms control, and global health politics. His latest book, *Moralities of Drone Violence* (2023), is an Open Access publication by Edinburgh University Press.

Mr. Antonio FARELO

Antonio Farelo is an Innovation and Technology Officer of the INTERPOL Innovation Centre. He joined INTERPOL 17 years ago and works at its headquarters in Lyon, France. He previously spent a decade with the Portuguese Judiciary Police, where he got experience in law enforcement and criminal investigation. He is currently involved in Project Courageous, a coordinated approach to CUAS in law enforcement, as well as other projects, particularly the implementation of smart city technologies for law enforcement applications and the Toolkit for Responsible Artificial Intelligence.

ANNEX C

GLOSSARY OF ACRONYMS:

CCDCoE: The NATO Cooperative Cyber Defence Centre of Excellence
CICoE: The NATO Counterintelligence Centre of Excellence
CO: Cyberspace Operation
COEs: Centres of Excellence
DOTMLPF-I: Doctrine, Organisation, Training, Materiel, Leadership Personnel, Facilities, Interoperability
FOM: Freedom of movement
HN: Host Nation
HQ: Headquarters
JISD: Joint Intelligence and Security Division
LEA: Law Enforcement Agency
LL: Lessons Learned
LLB: Lesson Learned Branch
LoE: Lines of effort
MDO: Multi-Domain Operation
NSPCoE: the NATO Stability Policing Centre of Excellence
RfS: Request for Support
SASE: Safe and Secure Environment
SHAPE: Supreme Headquarters Allied Powers Europe
SP: Stability Policing
TTPs: Techniques, tactics and procedures
UTM: Unmanned Traffic Management

ANNEX D

DOCTRINAL REFERENCES

List of doctrinal references (limited to Unclassified doctrine) in support of the Workshop:

NATO 2022 Strategic Concept

NATO AJP- 01 Allied Joint Doctrine

NATO AJP- 3 Allied Joint Doctrine for the Conduct of Operations

NATO AJP- 3.22 Allied Joint Doctrine for Stability Policing

NATO AJP- 5 Allied Joint Doctrine for the Planning of Operations

AC/343-D(2023)0005 (INV) NATO TECHNICAL EXPLOITATION GROUP (NTEG)
Technical Exploitation of Unmanned Aircraft Systems (UAS) Best Practice Guide

DISCLAIMER

This document has been issued by NATO Stability Policing Centre of Excellence and its contents do not reflect NATO policies or positions, nor represent NATO in any way, but only the NATO SP COE or author(s), depending on the circumstances.

Finito di stampare
nel mese di settembre 2024
presso
Tecnografica di Sandrigo (VI)

ISBN 979-12-5539-044-2