Council of the European Union
General Secretariat

**Brussels, 18 May 2026**

**WK 6526/2026 REV 2**

**LIMITE**

**IPCR**
**PROCIV**
**COSI**
**JAI**
**CYBER**

*This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.*

**WORKING DOCUMENT**

| | |
|---|---|
| From: | General Secretariat of the Council |
| To: | Ad hoc Working Party on preparedness, response capability and resilience to future crises |
| Subject: | Revised compilation of Member States' written replies to the Presidency guiding questions on the Action Plan on Drone and Counter Drone Security |

Delegations will find in annex written replies from 13 MS (CZ, DE, EL, FI, FR, HR, HU, IE, IT, PT, RO, SE, SK) to the guiding questions on the Action Plan on Drone and Counter Drone Security, following the AHWP RESILIENCE meeting on 30 April 2026.

## The Czech Republic's position on questions discussed at the AHWP Resilience meeting on April 30, 2026

1) What is your assessment of the strategic and operational objectives proposed in the Action Plan?

- *CZ generally supports the objectives and considers them relevant, timely and well aligned with the current security environment.*
- ***CZ welcomes that the Action Plan fully respects responsibility of MS for internal security** and defense, and that it **clearly declares complementary with NATO**.*
- *The Action Plan appropriately reflects current risks and combines short-term measures with a longer-term ambition to develop robust and gradually integrated European solutions. CZ welcomes the comprehensive civil-military approach, the emphasis on resilience, situational awareness and response capacity, as well as the focus on strengthening detection capabilities, protecting critical infrastructure and enhancing interoperability among Member States.*
- *CZ **supports** the proposed **coordinated framework for technological development** based on five pillars, as well as tightening of **regulatory requirements**.*
- *On the other hand, **the AP insufficiently addresses strategic dependencies on non-EU drone manufacturers** and their associated digital ecosystems, including cloud-based data processing and third-country access risks.*
- *From a **cyber perspective**, we believe that the envisaged coordinated risk assessment should have been a preceding step to the Action Plan.*

2) Which actions would you prioritize?

- ***Legislative amendment package**, including: remote identification (ID), geographical zones, mandatory registration and identification of unmanned systems weighing over 100 g, or counter-drone -related provisions (i. e. geofencing/geozoning);*
- ***Coordinated risk assessment of drones and counter-drone capacities**, provided that its scope, governance and expert composition are revised in line with defence and security needs;*

- ***Creation of a unified European database and a common drone traffic data-sharing system**, including information on drone operators and serial numbers, and the exchange of positive and negative experiences among Member States**; the system settings must also respect specific needs, especially of law enforcement authorities and secret services;***

- ***Measures to improve situational awareness of Member State authorities**, in particular through data-integration solution;*

- ***Support of voluntary practical cooperation among Member States**, especially in training, testing and exercises, including the sharing of operational know-how;*

- ***Strengthening civil-military interoperability in the C-UAS domain**, including systematic exchange of experience and best practices;*

- ***Development of a sovereign European command-and-control (C2) capability**, based on AI-enabled software, high cybersecurity standards, up-to-date encryption and high-performance computing;*

- ***Development of detection, identification and neutralisation capabilities against drones, aimed at protecting critical infrastructure, military facilities and the civil population**, based on a multi-sensor approach and advanced command-and-control (C2) system;*

- ***Civil-industrial mapping** to provide Member States with comprehensive data on the state of technological development and production;*

- ***Support for technological development and industrial production of drone and counter-drone systems within the EU**, making effective use of existing EU instruments (EDF, EDIP, SAFE);*

- ***Development of UAV mass-production capabilities**, together with maximisation of supply-chain security and diversification;*

- ***Facilitation of acquisition and joint procurement of C-UAS solutions, capabilities and equipment by Member States**, including through EU funding, with a focus on critical infrastructure resilience;*

- ***Upgrade of law-enforcement operators' training cycles**, ensuring that curricula are relevant, up to date and with sufficient capacity for Member State participants;*

- ***Integration of relevant expertise from other domains**, notably civil aviation (EASA), into the C-UAS Expert Group;*

- ***Establishment of a Common EU Counter-Drone Centre of Excellence (CoE)*** *for development, training and testing, serving as a coordinating and educational platform;*

- ***Establishment of rapid response teams for drone-related emergencies****, equipped with modern detection and response technologies;*

- ***CZ supports the idea of developing 'EU-trustworthy' unmanned and counter-drone systems****, understood as co-developed, certified and interoperable solutions for security authorities. On the other hand, we do not see the added value of the* ***proposed EU Trusted Drone Label at this stage****, compared to more urgent cybersecurity priorities under the Cyber Resilience Act ecosystem.*

3) What should be the role of the Council in the implementation of the actions?

- ***Provide overall political, strategic and coordinating leadership*** *including regular monitoring of implementation;*

- ***Ensure coherence and harmonisation*** *across EU policies (e.g. NIS2 and the Cyber Resilience Act) or* ***between EU and NATO efforts****, avoiding fragmentation, duplication, and parallel decision-making;*

- ***Safeguard institutional balance and national competences****, preserving space for voluntary cooperation.*

4) Do you foresee any particular challenges to implementing the actions?

- ***First and foremost, CZ views the need to respect national interests and exclusive competences in the area of internal security,*** *particularly special regimes or safeguards for public or private security actors while protecting critical infrastructure, and* ***the need for clearly defined internal security and military (national security) exemptions.***

- ***Fragmentation of national solutions and lack of interoperable technologies****, with many Member States investing in isolated national anti-drone systems, leading to risk of* ***duplication of effort and inefficient use of resources****, in the absence of a joint coordination or competence centre;*

- *Risk of duplication between EU and NATO activities;*
- ***High budgetary demands, limited national expert and human capacities, rapid technological change and potentially unrealistic implementation timelines**;*
- ***Unclear interaction with existing cyber-risk governance and product security frameworks**, in particular with NIS2 and the Cyber Resilience Act;*
- ***Supply-chain security and diversification challenges**, including difficulties in diversifying certain critical inputs such as rare earth elements used in UAV components (e.g. IR detectors), or dependence on non-EU suppliers and their data ecosystems.*

5) Would MS contribute to the establishment of a CoE, and if so, how? Specifically, is there a willingness to contribute to this new strand of work by offering specialised human resources?

- *CZ could consider occasional expert contributions on an ad-hoc basis, if the CoE is established.*
- *In any case, CZ remains open to sharing expertise and providing targeted expert input.*
- *Particularly The Fire and Rescue Service of the Czech Republic is open to contribute. Regarding its specialization, The Fire and Rescue Service of the Czech Republic is primarily capable of providing a robust transmission system along with the necessary infrastructure for receiving video signals. They are thus able to provide a complete digital replica of an emergency or destination.*

6) One of the pillars of the CoE involves establishing satellite Training & Testing centres (with the next session scheduled in early June). Is there an appetite for Member States (other than those already involved) to offer their facilities for future training sessions funded by the Commission?

- ***CZ participation must be firstly subject to prior discussion at national** level and decision based on more details.*

**GERMANY**

**AHWP Resilience 30. April 2026 – Drone Action Plan**

**German Comments**

1. What is your assessment of the strategic and operational objectives proposed in the Action Plan?

Germany approves of the priorization by the action plan, especially in addressing the current technical fragmentation and developing a wholistic approach.

NATO-Structures should not be duplicated. It is necessary to consider existing NATO initiatives and long term NATO experiences, which may also be applicable in the civilian sector.

Germany favors the continued support of the whole of government approach including military and security agencies.

The action plan for autonomous systems, which EDA has been tasked with, was not considered in the drone action plan. From GER's point of view this would have been necessary, especially regarding thematic and policy reports.

2. Which actions would you prioritize?

- Regulation for a drone air space as a European solution
- Comparison and standardization of testing- and selection programs
- regulatory simplification measures for drones aimed at introducing flexibility for certain operations such as removing the need of pre-approval by authorities and reducing the associated administrative burden, including a possible extension of geo-awareness requirements to all drones above 100g
- Outside of the technical scope, the topic of data protection and any potentially improved capabilities for location and tracking of drones should be taken into account.

3. What should be the role of the Council in the implementation of the actions?

Member States need to be fully and proactively engaged in the action plan's implementation, with adequate time for preparation.

4. Do you foresee any particular challenges in implementing the actions?

The proposed measures affect various areas. To ensure effectiveness, duplicate structures and parallel discussions must be avoided. The existing structures of the Member States must also be adequately taken into account.

According to point 2.1, the Commission is planning to initiate with Member States a civil-military industrial mapping. Germany highlights, that any industrial mapping has to comply with the applicable regulations, such as EDIP. In addition, it remains unclear as to why the Commission has to initiate a mapping to identify projects for industrial acceleration. In general, these are identified by request for proposals in the different thematic areas. This approach respects the rules of competition.

Since work at the PCA is advanced by the member states, topics and initiatives are also defined by the member states. The Commission and the High Representative should develop instruments to support the work of the member states on common initiatives. They should not – as suggested in section 5 – support individual initiatives.

The suggestion to support a European C2-build up of AI-Gigafactories (4.3) as special support carries the risk of fragmentation.

5. Would MS contribute to the establishment of a CoE, and if so, how? Specifically, is there a willingness to contribute by offering specialized human resources?

Germany supports in general the establishment of a EU counter-drone Centre of Excellence (CoE). This should be integrated with other initiatives, for example with the works by the PCA on drones and counter drone systems. Duplication of structures and the connected commitment of national resources have to be avoided.

6. Regarding the pillar of the CoE establishing satellite Training & Testing centers: Is there an interest from Member States (beyond those already involved) to offer their facilities for future Commission-funded training sessions?

This still has to evaluated.

**GREECE**

**1. What is your assessment of the strategic and operational objectives proposed in the Action Plan?**

Greece assesses positively the EU Action Plan on drone security and counter-drone measures, as it responds to a rapidly evolving threat with a clear cross-border, hybrid, and dual-use dimension. The need for a common European approach is particularly critical, given the increasing use of unmanned aerial systems (UAS) both for legitimate applications and for malicious activities targeting critical infrastructure, borders, public spaces, energy facilities, maritime infrastructure, and transport networks.

The strategic and operational objectives of the Action Plan are considered appropriate, particularly with regard to:

- the recognition of unauthorized drones as a horizontal hybrid threat,
- the emphasis on prevention, early detection, and resilience of critical infrastructure,
- the cross-sectoral approach linking security, digital infrastructure, and civil protection,
- the cellular-based / dual-use drone detection approach and 5G-based detection capabilities, which enable proportional, passive, and technically targeted detection.

Please also note that Greece has already developed a National Strategy for Unmanned Vehicles (UVs), aiming to establish a unified, coherent, and long-term policy framework for the structured, safe, and sustainable development, use, and integration of unmanned systems into the national regulatory, operational, and technological environment. Our national strategy is expected to be published by the end of May (TBC).

The national strategy is fully aligned with the principles and directions of the EU Action Plan, while actions already being implemented at national level reflect and support the corresponding European priorities, contributing to strengthening both national and European security and resilience. The national strategy also provides for two actions to counter malicious drones: first, the development of a regulatory framework, and second, the development of national technological and operational capabilities.

**2. Which actions would you prioritise?**

Priority should be given to actions that create immediate operational value for Member States.

First, we would prioritize the development of common capabilities for the detection, identification, and monitoring of drones, leveraging 5G, sensors, geospatial data, C2 systems, and a unified airspace picture.
Second, the protection of critical infrastructure and borders, including ports, airports, energy facilities, subsea infrastructure, and telecommunications hubs, as well as the implementation of pilot projects (pilots & sandboxes) in high-risk critical infrastructure.
Third, the development of common European standards, procedures, testing scenarios, and certification of counter-drone systems.
Fourth, the strengthening of the European industrial base and supply chain security, through trusted technologies, supplier screening, and the introduction of an “EU Trusted Drone” label.

**3. What should be the role of the Council in the implementation of the actions?**

The Council should play a coordinating, political, and supervisory role.

More specifically, the Council should:

- ensure coherence between different working groups and sectors (telecommunications, internal security, civil protection, cybersecurity, defence, borders, and critical infrastructure),
- monitor compliance with EU law (GDPR, AI Act, CER, NIS2, etc.),
- encourage voluntary contributions and pilot cooperation rather than binding obligations.

**4. Do you foresee any specific challenges in the implementation of the actions?**

With regard to implementation challenges, we have identified the following challenges:

- the need to clarify responsibilities among civil, law enforcement, military, regulatory, and civil protection authorities,
- system interoperability,
- protection of personal data,
- cybersecurity of drones and counter-drone solutions,
- dependence on non-European suppliers, and the need for common testing and certification standards.

**5. Would MS contribute to the establishment of a CoE, and if so, how? Specifically, is there a willingness to contribute to this new strand of work by offering specialised human resources?**

Regarding the establishment of a European Counter-drone Centre of Excellence, Greece could support the initiative, provided that the Centre operates as a practical mechanism for the exchange of know-how, testing, training, certification, and operational support to Member States. Such a Centre should not replace national security or defence responsibilities and should function in a complementary manner to existing European frameworks.

The contribution of Member States could include the provision of specialized human resources (operational personnel and experts), participation in working groups, exchange of best practices, development of common exercise scenarios, and interconnection with national operations centres, civil protection bodies, security authorities, telecommunications entities, and defence authorities.

Greece is positively considering participation in such a network, including making facilities available for future training and testing activities. The country's geographical diversity - urban environments, insularity, maritime borders, critical infrastructure, ports, airports, and mountainous areas - provides suitable environments for realistic testing and exercises. Such participation should be assessed in coordination with the competent Ministries and authorities, in order to ensure security, legality, protection of classified information, and consistency with the national drone strategy.

**6. One of the pillars of the CoE involves establishing satellite Training & Testing centres (with the next session scheduled in early June). Is there an appetite for Member States (other than those already involved) to offer their facilities for future training sessions funded by the Commission?**

Greece expresses, in principle, its interest in examining:

- the possibility of hosting specific training activities and testing centres in the future,
- subject to a clear framework:
    - voluntary participation,
    - funding by the European Commission,
    - and alignment with the National Strategy for Unmanned Vehicles.

Ministry of the Interior
Finland

**Working Party on Civil Protection – Critical Entities Resilience (PROCIV CER)**

**Action Plan on Drone and Counter Drone Security – Presidency guiding questions**

11.5.2026

**Additional information (AHWP Resilience):**

1. **What is your assessment of the strategic and operational objectives proposed in the Action Plan?**

- We support the objectives of the Communication.
- The operating conditions of the authorities must be continuously reviewed and developed proactively so that the authorities can react to and respond to changing security threats.
- We welcome the fact that the Commission extensively examines the development of practices by both aviation and security authorities in the fight against drones in the Action Plan.
- An effective response to the threat posed by drones requires a comprehensive, coordinated, and targeted approach combining civilian, law enforcement and military dimensions.
- We support the Commission's objective of implementing many of the actions of the Action Plan as part of its close partnership with Ukraine.
- We emphasise the use of existing EU instruments, such as the EDIP, to promote and fund drone defence initiatives.

2. **Which actions would you prioritise?**

- EU initiatives related to the capability development should be a priority.
- Improving border surveillance and detection of threats at the EU's external borders is an important goal.
- We should continue the fruitful work that has started in EU defence initiatives regarding development of drone and anti-drone capabilities. We recognise the importance of international partnerships in the development of European defence capabilities in the field of drone defence.
- In this context, it is particularly important to utilise Ukrainian lessons in drone defence.
- We support the Commission's Proposal for a Drone Security Package to rapidly adapt the regulatory framework to new security threats.
- We are in favour that Commission will propose a mandate to the CEPT (European Conference of Postal and Telecommunications Administrations) to develop technical and operational conditions for sensing.

Ministry of the Interior
Finland

- We are positive to the initiative to take the necessary regulatory steps to allow spectrum to be used for sensing through an amended spectrum harmonisation decision.
- Unnecessary administrative burden to different actors needs to be avoided.
- Coordinated Union wide security risk assessment of drones and counter-drone capacities, as well as the following development of the Drone and Counter-drone security toolbox, can strengthen supply chain and cyber security in this domain across the Union.
- Through security-related measures the action plan can also enhance competitive European drone market and European innovation and industrial growth.
- For example, development of drones above the sea, on the surface of the sea and underwater is a remarkable initiative for the development of the technology and operations. This can build on the existing work and the current initiatives to support the protection of the critical underwater infrastructure. There will be synergies.
- On top of EU initiatives, it is very important that Member States review the national setup to counter drones. There must be appropriate national coordination in place and the national legislation must define competent bodies to respond to the threat of the drones, including interception. We are not there yet in a number of Member States. This has a negative impact to the whole EU as the threats do not respect our internal borders.

**3. What should be the role of the Council in the implementation of the actions?**

- The Council should monitor and follow up the implementation of the action plan. We expect full and efficient implementation.
- The Council is waiting legislative initiatives and more detailed policy initiatives from the Commission to implement the action plan. The Council has an important role as a co-legislator to implement all the ambitions in this regard.
- The Council should also look into actions in Member States. As a large part of the actions are about national competence, including national security, law enforcement and military defence, it is important that Member States do their part. Member States should be encouraged to participate the pilot projects and to make use of the possibilities of the European cooperation around drones and countering drones.
- The Council should also follow up the actions which are about implementing the EU law. For example, in the border management there are several issues that Member States should ensure. A proper situational picture, contributions to the Standing Corps and having proper operational plans are ultimately Member States' responsibility. Schengen evaluations of the Member States should reveal the possible shortcomings, and this should be discussed in the Council openly.

Ministry of the Interior
Finland

Member States should also steer the Agencies, such as Frontex, to ensure proper implementation of the actions.
- The Working Parties of the council should continue the discussions based on the competences and the roles of the Working Parties. As this is extremely horizontal issue, it is impossible to cover all aspects in one Working Party.

**4. Do you foresee any particular challenges to implementing the actions?**

- The implementation and follow-up of Commission's Action Plan is essential due to its' horizontal nature.
- The Member States have the main responsibility, but the EU has an important supporting role in each policy area.
- Only once we have the common understanding that drone threat is a cross cutting topic, we can ensure efficient implementation of Commission's Action Plan.
- We should not drop the focus. As the EU agenda changes quickly, there is a danger that we pivot something else soon. This should not happen.

**FRANCE**

**NOTE DE COMMENTAIRES DES AUTORITES FRANCAISES**

**Objet** : Note de commentaires suite à la réunion du groupe AHWP Résilience du 30 avril 2026 relative au plan d'action pour la sécurité des drones et des contre-mesures anti-drones

**Réf** : **CM 02434/2026 REV 2 ; WK 05645/26**

Les autorités françaises prient la Présidence chypriote de bien vouloir trouver ci-dessous leurs commentaires et réponses aux questions transmises dans le cadre de la réunion du groupe AHWP Résilience du 30 avril 2026 relative au plan d'action pour la sécurité des drones et de la lutte anti-drones.

1) **Quelle est votre évaluation des objectifs stratégiques et opérationnels proposés dans le plan d'action ?**

Les autorités françaises saluent une nouvelle fois l'ambition du plan d'action, qui dans un souci d'autonomie stratégique et de résilience, ambitionne de bâtir une industrie européenne en matière de solutions souveraines de drones, anti-drones et logicielles, à travers des financements fléchés vers les entreprises européennes.

Sur le plan de la méthode, il conviendra de distinguer les différents types de drones et ce qui relève de la compétence des Etats membres, de la compétence de l'UE, et de la coopération avec l'OTAN. Les propositions qui déclineront ce plan d'action ne devront pas porter atteinte à la responsabilité des États membres en matière de sécurité nationale. Les actions des agences comme Frontex doivent être conduites dans les strictes limites de leurs compétences respectives.

Dans le fond, la déclinaison concrète de certaines actions mériterait d'être précisée :

- Les exigences techniques applicables à la fonction de géo repérage (volet Préparation) ;
- Le cycle de formation des agents des services répressifs afin d'y inclure des mesures d'atténuation et de neutralisation (volet Préparation) ;
- Les mesures réglementaires nécessaires pour permettre l'utilisation du spectre à des fins de détection au moyen d'une décision modifiée d'harmonisation du spectre (volet Détection) ;
- La recommandation de la Commission relative à la lutte contre les menaces posées par les drones pour les agents des services répressifs (volet Réaction).

2) **À quelles actions donneriez-vous la priorité ?**

Les autorités françaises sont favorables à l'organisation **d'un exercice annuel européen de lutte anti-drones** engageant les acteurs civils et militaires. La tenue régulière d'un tel exercice semble nécessaire compte-tenu du rapide progrès technologique de cette capacité.

De manière transversale, il importe que les projets envisageant l'enregistrement et le suivi des drones puissent **préserver la confidentialité nécessaire aux opérations impliquant des drones et menées par les services des Etats Membres dans leur état d'implantation,** notamment des procédures d'enregistrement et d'identification des vols de drones.

Si le recensement des incidents relatifs aux drones apparaît comme une mesure utile, cette action doit :

- 1° **préserver la confidentialité liée à la localisation des entités critiques qui relèvent de la sécurité nationale**
- **2° être organisée dans le respect des compétences de chacun** (Etat membres/ Conseil/ Commission mais également en interne Commission, la DG HOME étant responsable du volet sécurité/ entité critique).

S'agissant du **projet pilote pour améliorer la connaissance du domaine maritime**, la surveillance des fonds marins est un domaine éminemment sensible et dont les enjeux, notamment en matière de renseignement, nécessitent que toute action dans ce domaine tienne compte de cette sensibilité et des prérogatives souveraines de sécurité et de défense des Etats membres.

En ce sens, le déploiement de capteurs sous-marins dans les bassins maritimes européens, tel qu'indiqué dans le projet pilote du Plan d'action, doit faire l'objet d'une **discussion approfondie au Conseil et de l'accord préalable des Etats membres**, tant sur ses objectifs, que sur sa mise en œuvre concrète et sa gouvernance.

S'agissant du projet de **création d'un centre européen de référence concernant le test des drones,** les autorités françaises soulignent la nécessité additionnelle de développer une communauté de centres de test européens afin de valoriser, de manière efficiente, l'expertise et les infrastructures existantes au sein des Etats membres.

S'agissant du projet de **cartographie des industries civilo-militaires pour orienter les investissements, et du projet d'évaluation des risques pesant sur les chaines d'approvisionnement et de production de drones et de systèmes anti-drones**, là aussi, ces projets de concaténation d'informations sensibles pourraient potentiellement augmenter l'exposition des vulnérabilités des Etats membres, et de leurs capacités industrielles face à des acteurs malveillants. Par ailleurs, un cadre règlementaire existe au travers du règlement EDIP concernant le suivi des chaines d'approvisionnement de la BITDE.

Les autorités françaises souhaitent demander à la Commission européenne d'apporter davantage de détails sur la forme finale que prendront ces deux projets et les objectifs recherchés par ces derniers.

Enfin, s'agissant de l'implication des **agences européennes** et notamment de Frontex, les autorités françaises rappellent que leurs actions doivent demeurer strictement dans leur domaine de compétence et ne pas empiéter dans des domaines relatifs au renseignement ou à la sécurité nationale. En particulier, elles tiennent à ce qu'il n'y ait **pas de confusion entre, d'une part, ce qui relève de la surveillance des frontières et/ou de la lutte contre la criminalité, et, d'autre part, ce qui rentre dans le champ de la sûreté de l'espace aérien, qui est un sujet de Défense nationale. Cette remarque vaut également pour des agences européennes comme Europol, qui intègre de plus en plus cette thématique dans la lutte contre le terrorisme et les extrémismes violents**

Par ailleurs leur intégration dans les groupes d'experts **ne doit pas avoir pour effet de leur donner une capacité à élaborer des analyses et états de la menace en dehors du champ d'action prévu par leur mandat.** La réalisation d'analyses d'état de la menace au niveau européen reste la prérogative de la SIAC.

S'agissant des priorités, les autorités françaises souhaitent que l'accent soit particulièrement porté sur la révision de la réglementation d'usages drones (2019/945 et 2019/947) et le centre d'expertise et de labellisation de solutions de lutte anti-drones (LADA).

3) **Quel devrait être le rôle du Conseil dans la mise en œuvre des actions ?**

À titre principal, le Conseil doit **veiller à ce que la réalisation des objectifs de ce plan et des mesures associées ne vienne pas empiéter sur les compétences des Etats Membres en matière de sécurité nationale** ou perturber les actions opérationnelles engagées dans ces Etats à l'aide de drones.

Les actions de ce plan ne doivent pas provoquer de charge administrative supplémentaire pour les entreprises de la filière.

Le rôle du Conseil sur ce plan d'action devrait être d'accompagner les Etats membres tout en leur laissant la latitude nécessaire à la mise en œuvre et ce, sans traiter directement avec les opérateurs impliqués.

4) **Prévoyez-vous des défis particuliers dans la mise en œuvre des actions ?**

Pour les Etats Membres, la difficulté résidera dans la capacité à agréger les données et experts d'un sujet éminemment interministériel par sa nature. Du point de vue européen, l'intégration des agences aux actions doit également répondre de la même logique et veiller à ce chacune d'entre elles reste dans son domaine de compétence et prennent bien en compte celles des Etats Membres.

Pour les autorités françaises, une difficulté apparaitrait si l'UE décidait d'un format d'échange de données entre les systèmes de lutte anti-drones différent de celui retenu par la France. Elles souhaitent que le modèle retenu soit compatible avec celui en place depuis les Jeux olympiques de Paris et qui a été communiqué aux experts du JRC en charge de cette nouvelle norme, ceci dans un but de préserver une interopérabilité essentielle.

Concernant la mise en place du Label UE Trusted drone, le défi résidera dans la capacité à intégrer les drones « Legacy » actuellement en circulation (6 millions estimés en 2025) et qui n'auront pas le label Trusted drone.

Par ailleurs, il conviendra d'orienter les travaux préalables aux initiatives législatives pour bien intégrer la nécessaire confidentialité des actions des services opérationnels et veiller à ce que les drones utilisés par ces derniers puissent être traités de manière particulière dans le cadre des projets relatifs à l'enregistrement et l'immatriculation.

5) **Les États membres contribueraient-ils à la mise en place d'un Centre d'excellence et, dans l'affirmative, comment ? Plus précisément, y a-t-il une volonté de contribuer en offrant des ressources humaines spécialisées ?**

Les autorités françaises soulignent la **complémentarité** que pourrait représenter la création d'un **centre d'excellence européen** avec les différents centres de test nationaux pour les drones à double usage, qui permettrait de valoriser les expertises nationales existantes. L'objectif pourrait être de bâtir une communauté d'excellence de ces centres nationaux avec une capacité de test et d'évaluation suffisante qui tiendra compte des spécificités et des prérogatives des Etats membres en matière de protection et de résilience de leurs infrastructures critiques.

Le développement d'un tel centre doit aussi prendre en compte les actions menées dans le cadre du « Priority Capability Area (PCA) Drones », notamment celle de mettre sur pied des « Drones Technology Hubs », afin d'éviter la duplication des efforts.

Les autorités françaises demandent à la Commission européenne de bien vouloir apporter davantage de détails sur la **forme finale du centre**. Il serait notamment utile de préciser si ce dernier sera consulté s'agissant de **l'élaboration de nouvelles normes** liées aux enjeux de sécurité aérienne pour les drones, amenées à figurer dans le futur paquet législatif sur la sécurité des drones (*Drone Security Package*).

6) **En ce qui concerne le pilier du Centre relatif à la création d'une communauté de centres de formation et d'essai : Les États membres (au-delà de ceux déjà impliqués) sont-ils intéressés à proposer leurs installations pour les futures sessions de formation financées par la Commission ?**

Les autorités françaises sont intéressées pour fournir un centre au sein d'une communauté de centres d'essai et de labellisation.

Lors de la présentation de l'ébauche du dispositif au groupe d'experts C-UAS le 29 avril 2026, il a été annoncé la volonté de cantonner chaque centre de cette communauté à une expertise spécifique particulière (détection, ou brouillage, ou C2, etc…).

Il serait préjudiciable que les centres de cette communauté soient cantonnés à l'expertise et aux tests d'une discipline capacitaire particulière (détection, ou brouillage, ou C2, etc…) et **les Etats Membres doivent disposer d'une vue large des technologies qui composent tout le spectre des systèmes.**

Les autorités françaises souhaitent que les systèmes de lutte anti drones puissent être testés sans autres limitations que celles imposées par la sécurité et les risques lié à leur environnement.

# CROATIA

1. ***What is your assessment of the strategic and operational objectives proposed in the Action Plan?***

From the military perspective, we evaluate positively the strategic objectives of the Action Plan, with special emphasis on strengthening civil-military cooperation (CIMIC). We believe that the integration of defence resources into a broader preparedness framework is necessary to be able to respond to large-scale crises. Operational objectives are clearly defined, but it is crucial to ensure their complementarity with existing NATO standards and capability objectives to avoid duplication of efforts.

From civil perspective we generally support the strengthening of resilience and preparedness, where technological evolution of measures to protect critical infrastructure is very important. In this sense, we also support the *whole of government* approach, highlighted in the Action Plan, regarding relevant competencies, especially related to defence and security. We also stand for effective civil-military coordination.

From technical perspective, we consider that the Action Plan is significantly more comprehensive in relation to previous documents (i.e. A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe, from 2022) especially in the part related to the recognition and encompass of all robotic threats, regardless of their mode of motion or the medium in which they are found. This is something that was advocated by Croatia at the HOME-D2-CUAS working group.

This Action Plan recognizes that the "drone" is a segment of aerial robotics and as such is only one dimension of the threat. Although it is currently the most prevalent, the creation of a systematic response to other forms of robotic threats must not be neglected, because the creation of any systematic response to threats requires a lot of preparation. Although threats such as autonomous vessels or vehicles and other devices are less represented, their presence and rapid development must not be neglected, and this Action Plan aims to emphasize these additional dimensions of threats.

In relation to previous documents, this Action Plan for the first time includes the military component, which is a recognition of the fact that the response cannot be separated through various state structures, but rather the most effective response is one in which all stakeholders are involved and where there is a clear regulatory framework (coherent *whole of government* approach).

The inclusion and expansion of the HOME-D2-C-UAS working group, with the participation of Frontex, DG Connect, EASA, etc., is a recognition of the aforementioned complexity, and the result is a provision of individual recommendations such as:
a) Software locking of commercial drones placed on the market (allows for a reduction in the number of uninformed and careless pilots who unknowingly endanger air navigation safety);
b) Direct Remote ID for drones larger than 100 g, which closes the gap compared to the previous provision of 250 g (namely, the vast majority of drones sold in the EU are smaller than 250 g and such drones often unknowingly create a problem for aviation safety, but also at public gatherings. Due to the previous limit of 250 g, after which the drones should have had a Direct Remote ID, there was a large number of drones that could not be identified);
c) The inclusion of telecoms in detection and prevention of occurrences is a major step, where the existing infrastructure is used to strengthen detection and the possibility of limiting service in a particular area for 5G service users on drones, thus reducing the possibility of interfering with 5G signals;

d) EU counter-drone centre of excellence – is necessary as a place of accumulation and transfer of advanced knowledge on topics such as radio frequency detection, electronic action (EW in military terminology), the use of various detection methods (radar, acoustic, optical and others) with the use of the latest AI components, and other unique detection methods and active countermeasures.

***2. Which actions would you prioritise?***

From military perspective we emphasize:

- Military Mobility - to ensure the unhindered movement of allied forces and equipment as a prerequisite for a rapid response to a crisis;
- Protection of critical infrastructure - given the geopolitical position of the Republic of Croatia, is considered crucial for national and collective security;
- Strengthening cyber defence - increasing the resilience of command and communication systems to hybrid attacks;

From civil perspective - activities related to the protection of the population, i.e. people and goods, and also the protection of critical infrastructure.

From technical perspective our priorities are:

1. Upgrade by Q2 2026 the training cycle for law enforcement operators to include mitigation and neutralisation measures.
2. Improve situational awareness through
    - The integration of relevant data into dedicated single display systems;
    - Exploring the progressive establishment an EU drone incident platform;
    - Integrating detection, tracking and identification capabilities into national border surveillance systems;
    - Common data formats for counter-drone capabilities.
3. Strongly encourage Member States to set up an information-sharing framework between civil aviation authorities, law enforcement and military.
4. Intensify its support to Member States in the Priority Capability Area Drone and Counter-Drone, including through fostering convergence and synergies across PCA's coalition work and related ongoing capability efforts as well as through tools such as the EDPCI and SEAP. Such efforts will frame the European Defence Drone Initiative, and the Eastern Flank Watch initiative.
5. Launch by Q2 2026 a call for Expression of Interest to establish a voluntary EU counter-drone deployment initiative for critical infrastructure based on:
    - An overview of EU dual use counter-drone capability needs.
    - A joint development pilot programme for counter-drone capacities.
    - Voluntary joint purchasing for the protection of critical infrastructure.
    - Deploying Counter-drone capacities in maritime and land border (through the€250m call on expression of interest under the BMVI).

***3. What should be the role of the Council in the implementation of the actions?***

The Council should maintain its role as the main body for political oversight and strategic guidance. We particularly emphasize the importance of the Council in ensuring coherence between different EU instruments (such as EDF and PESCO) and in encouraging Member States to plan coordinated strategic

equipment stocks. We also see the Council's role, preferably, in effective coordination synergy with the IPCR.

4. ***Do you foresee any particular challenges to implementing the actions?***

We identify the following main challenges:

- Resource constraints: the need for significant financial investments in the short term.
- Interoperability: different technical standards and levels of digitalization among Member States.
- Legal frameworks: harmonization of national regulations on the engagement of armed forces in civilian crises with EU recommendations.

Civil-military cooperation requires coordination of activities and collaboration of all involved stakeholders.

Regarding point 2.1. Ramping up technological development and industrial production of drones and counter-drone systems, we would like to ask for a clarification of the statement:

"Third, there is a need to bring clarity and security into the market through targeted safety requirements and a certification scheme for counter-drone systems. Embedding safety requirements into counter-drone testing and validation ensures that counter-drone measures do not compromise aviation safety. EASA, as the competent authority for aviation safety, should therefore develop criteria to be respected by counter-drone systems."

Depending on the interpretation, the above may be misapplied. Namely, the purchase and development of C-UAS systems must necessarily be carried out through three phases (peace, crisis, war) and it is necessary to purchase equipment that covers as many of these three scenarios as possible. For this reason (coherent *whole of government* approach), we must keep in mind that EASA is an agency whose primary goal is civil aviation safety, but has no role in defence or security of the Member States.

Its role may be important in developing procedures for the implementation of individual systems in peacetime, but it must not limit the development of these systems for defence or security purposes, because in the case of crisis and war this directly affects the ability of the Member State to respond from a defence or security perspective.

In short, EASA should be a partner in the development of procedures for the use of C-UAS systems in peacetime, but the systems must not be restrained in their capabilities, because this may lead to a reduction in the ability of the Member State to respond to a crisis or war threat.

*We would also welcome Member States' views on the specific proposal in the Action Plan to establish a Counter Drone Centre of Excellence (CoE), namely:*

5. ***Would MS contribute to the establishment of a CoE, and if so, how? Specifically, is there a willingness to contribute to this new strand of work by offering specialised human resources?***

We see advantages of such proposal and we believe that it would be desirable to participate in the work of the CoE by offering advice based on practice and operational experience. Considering the past experience, JRC has clear benefits from collaborating with experts with operational experience. The

inclusion of experts for the purposes of directing work and raising the quality of training would be desirable.

6. ***One of the pillars of the CoE involves establishing satellite Training & Testing centres (with the next session scheduled in early June). Is there an appetite for Member States (other than those already involved) to offer their facilities for future training sessions funded by the Commission?***

The Republic of Croatia is ready to consider the possibility of ceding its military training grounds and facilities for the purposes of conducting training and testing under the auspices of the Commission. We believe that our training grounds meet the requirements for testing anti-drone systems in different terrain configurations. We emphasize that such an engagement would require a detailed prior analysis of costs and the provision of full funding by the European Commission.

**HUNGARY**

# Written comments of Hungary on the Action Plan on Drone and Counter Drone Security

## 1. What is your assessment of the strategic and operational objectives proposed in the Action Plan?

We generally support the strategic and operational objectives of the Action Plan and welcome its publication. We agree that strengthening Member States' capabilities and fostering innovation requires a coordinated approach. We positively assess the four-pillar structure – prevention, preparedness, detection, and response – which provides a comprehensive framework to address the full spectrum of drone threats, and its alignment with the EU Internal Security Strategy and the critical infrastructure protection framework.

From an operational perspective, we highlight the deployment of multi-sensor detection systems and the establishment of an EU drone incident platform as important steps towards enabling near real-time information sharing among Member States' competent authorities. At the same time, we underline that the successful implementation of these objectives requires taking into account capacity disparities among Member States and ensuring a phased and differentiated approach.

We strongly support efforts to enhance the cybersecurity of drones and counter-drone systems. In this context, we recommend clearly defining the relationship between the ICT Toolbox developed by the NIS Cooperation Group and the planned Drone and Counter-drone Security Toolbox. Furthermore, we consider it necessary to clarify the relationship between the EU drone incident platform and the single entry point to be established under the Digital Omnibus, in particular regarding which types of incidents – including cybersecurity incidents under the NIS2 Directive or other incidents – should be reported through each system.

## 2. Which actions would you prioritise?

Taking into account available resources and the current threat environment, we consider as top priorities the early operationalisation of the EU drone incident platform to enable near real-time information sharing, as well as strengthening the protection of critical infrastructure, in particular airports and energy facilities. We also underline the importance of harmonising multi-sensor detection systems and ensuring their interoperability, as well as accelerating the implementation of U-space.

To increase resilience, we support the establishment of an EU-level unified registry system covering drone operators, certified drones, permits and declarations, as well as remote pilot competencies, accessible to all Member States. In this context, we also see added value in developing a common application similar to MyDroneSpace, providing up-to-date airspace information and enabling the notification of drone operations. At the same time, we do not consider full harmonisation of national authorisation procedures realistic due to Member State specificities, while harmonisation of registries would be beneficial.

We have reservations regarding proposals to extend mandatory registration and direct remote identification to smaller drones above 100g. The current framework based on classes and operational categories already appropriately addresses risk. Any extension should only be considered in close cooperation with manufacturers, with a sufficient transition period, and without retroactive requirements for already marketed devices. We also note that technical constraints, such as additional weight and energy requirements, may negatively affect smaller drones and impose disproportionate burdens, particularly on custom-built devices. Furthermore, their effectiveness is questionable, as non-compliant users are likely to circumvent such systems.

In the field of cybersecurity, we note that several relevant EU instruments already exist, including the Cyber Resilience Act, and that a legal basis is available for developing a European cybersecurity certification scheme. Therefore, the added value of the proposed EU Trusted Drone Label is not clear, and we recommend clarifying its legal basis and relation to existing certification frameworks.

3. **What should be the role of the Council in the implementation of the actions?**

We consider the role of the Council to be key in the implementation of the Action Plan, in particular in providing political guidance and oversight, strengthening coordination and solidarity among Member States, and contributing to the development of the necessary legislative framework. The Council should regularly, for instance on an annual basis, review implementation progress and, where necessary, adjust priorities in response to the evolving threat landscape. It should also facilitate the exchange of experience among Member States and support those with more limited capacities.

At the same time, we consider it necessary to further clarify the Commission's planned "strategic mechanism" for coordinating the implementation of the Action Plan, in particular the respective roles of drone security coordinators, the Council, and this new mechanism, as well as how effective coordination and the Council's role will be ensured.

4. **Do you foresee any particular challenges to implementing the actions?**

We foresee several challenges in implementing the actions, partly in line with our previous remarks. Legal and regulatory heterogeneity among Member States, particularly regarding the authorisation of counter-drone measures, may hinder a unified EU response. Significant capacity disparities also exist in terms of technical equipment, trained personnel, and financial resources. In addition, the dual-use nature of most detection and counter-drone technologies raises complex legal issues related to their export and sharing.

We also underline the importance of maintaining a certain level of Member State autonomy in the field of counter-drone measures, given the relevance of local conditions. Measures related to detection and incident reporting – in particular under Chapter 3 – are still under examination,

especially in light of their sensitivity and national security implications. Ensuring consistency between real-time data sharing and EU data protection requirements will also require careful legal preparation.

Furthermore, current detection and counter-drone systems are costly and subject to rapid technological obsolescence, making their maintenance resource-intensive; therefore, increased targeted EU financial and technical support would be justified. We also note a regulatory gap regarding unmanned balloons, which are not fully covered by existing drone legislation.

Finally, if the EU Trusted Drone Label is not introduced as part of a European cybersecurity certification scheme, it may create legal uncertainty in its application.

5. **Would MS contribute to the establishment of a CoE, and if so, how? Specifically, is there a willingness to contribute to this new strand of work by offering specialised human resources?**

We are currently examining the proposal to establish a Counter Drone Centre of Excellence. In order to form our position, we would require further information on the planned organisational structure, governance model, and funding arrangements of the Centre. Based on this, we will be able to assess the possibilities and modalities of Member State contributions, including the provision of specialised human resources.

6. **One of the pillars of the CoE involves establishing satellite Training & Testing centres (with the next session scheduled in early June). Is there an appetite for Member States (other than those already involved) to offer their facilities for future training sessions funded by the Commission?**

We are currently examining this proposal and are therefore not in a position at this stage to express a view on offering national facilities for future training sessions.

**IRELAND**

**AHWP Resilience**

**30 April 2026**

**Drone and Counter Drone Action Plan**

The meeting will include a Commission presentation of the Action Plan on Drone and Counter Drone Security. The following guiding questions were submitted to lead the discussion.

1. *What is your assessment of the strategic and operational objectives proposed in the Action Plan?*

   Ireland welcomes the plan, noting a good balance between developing/sharing expertise and investment in long term capability. The Commission Action Plan underlines the need for coordinated approach bringing together civil and military dimensions. This is an approach we fully endorse.

   IE are already engaging in the Defence Capability Development proposed project (Capability Coalition on Drones and Counter-Drones) led by the NL, HR and LV to identify potential opportunities to address our capability requirements.

   Ireland is concerned that the funding is through the Border Management and Visa Instrument BMVI, which Ireland cannot access, as it does not participate in that element of the Schengen acquis. Any alternative funding available through ISF?

   The U-space regulatory framework may assist in dealing with uncooperative drones (with the introduction of enhanced conspicuity and registration obligations) but its original purpose was to introduce digital services to support safe, automated and scalable drone operations.

2. *Which actions would you prioritise?*

   IE welcome alignment with the Critical Entities Resilience (CER) Directive and required outputs by Member States across the eleven sectors. IE welcome that voluntary stress testing against drone intrusion is incorporated into current plans for stress testing under CER, and would that stress testing remains part of a risk based approach. IE also

welcome full standard harmonised testing methodology for Countering Unmanned Aircraft Systems, but that any recommendations should be also included in CER Article 13 guidelines on security, technical and organisations measures for Critical Entities from the commission to be published in Q2 2026.

The Action Plan suggests a voluntary procurement initiative related to the protection of critical infrastructure. IE will explore fully any proposals from the Action Plan which could help us meet our capability needs whether for military or civilian purposes.
We would stress test critical infrastructure against drone intrusion; establish rapid counter drone emergency team to enhance mutual assistance; and develop EU drone incident monitoring platform.

The Action Plan also proposes enhanced efforts to improve situational awareness through an information-sharing framework between civil aviation authorities, police and military. IE are open to hearing proposals for concrete ways to work with other MS to enhanced our shared situational awareness to counter threats from drones

The embedding of safety requirements into counter-drone testing and validation testing to safeguard manned aviation is essential.

The involvement of the European Union Aviation Safety Authority (EASA) is critical in the developing of criteria for counter-drone systems.

It is important that counter-drone systems and the processes and procedures for their use do not compromise manned aviation. Civil aviation safety competent authorities should be involved in ensuring that the systems are compatible with broader aviation safety objectives. This is of particular importance in the use of counter-drone systems in the vicinity of airports.

Airports have been the target of malicious use of drones resulting in safety risks, cost and reputational impacts. The strengthening of the EU's ability to counter-drone activity at airports is particularly welcomed given Ireland's location.

3. *What should be the role of the Council in the implementation of the actions?*

   The Council should review progress and provide guidance – we see the potential to update the council twice yearly.

4. *Do you foresee any particular challenges to implementing the actions?*

   Regulatory Harmonisation will be difficult – we need to fully understand current approaches, what is working well, and what can be improved.

   The main objectives of the U-space framework are to enable a fair and efficient sharing and use of the airspace, allowing a safe separation between manned and unmanned aircraft implementation. Implementation of U-space is a key action in the National Policy Framework for Unmanned Aircraft System. However, the complexity and cost of implementation are challenging. Greater support from the Commission and EASA on the would be welcomed.

**1. What is your assessment of the strategic and operational objectives proposed in the Action Plan?**

- In our view, the Plan correctly captures the **cross-cutting nature** of the challenges and opportunities posed by drones. In the next phase, it will be essential to ensure that overlaps generate synergies rather than duplications or conflicts with existing or forthcoming initiatives, as well as with existing strategic and operational frameworks.
- We welcome the **integrated approach to low-altitude airspace management**, which combines multi-source data with mobile telecommunications networks.
- We appreciate that the Action Plan recognises **Critical Infrastructure as a cross-cutting element** across all pillars and identifies the CER Directive as a key horizontal reference framework.
- We also acknowledge the **importance of the territorial and regional dimension** in addressing drone-related threats, which aligns with our proposal on the setting up of a regional mechanism for the surveillance of critical infrastructure in the Mediterranean basin.
- From an **internal security** perspective, we welcome efforts to align regulatory frameworks (e.g. civil aviation and spectrum) with the need to respond to drone threats. We also appreciate that the Plan highlights the challenges faced by Member States in securing adequate investment in advanced technologies and underlines the importance of specialised training.
- At the same time, we are convinced that **operational responsibilities** should remain with Member States and their civilian authorities.
- Despite its ambitious vision, several issues remain: **limited interoperability** among Member States; **insufficiently defined data governance** and information-sharing; **dependence on non-EU suppliers**; challenges in **integrating cyber and physical systems**; and **disparities** in resources, expertise and coordination.
- Finally, while the initiative has a predominantly internal security and civilian focus, it is essential in this dual-use domain to ensure that **military requirements guide capability development**, guaranteeing coherent European-level harmonisation.

**2. Which actions would you prioritize?**

- Priorities should focus on the **harmonisation of requirements** at European level in order to avoid fragmentation of the market and of technological development. It is also considered important to further strengthen the maritime and underwater dimension, with particular reference to the protection of Critical Underwater Infrastructure (CUI) as well as to the strategic relevance of the Mediterranean, aspects which are currently not sufficiently reflected in the Plan. In this context, it is also essential to fully leverage the European innovation ecosystem, including national centres of excellence.
- In addition, priority should be given to **defining procedures for joint procurement** and to clarifying the framework in which **specialised training** will be delivered.
- Another priority is the **simplification of the regulatory framework**, including the possible introduction of controlled derogations for emergency or high-risk situations. This should enable law enforcement authorities to respond effectively to threats posed by malicious drones, including through the use of electronic countermeasures.

- Due regard should also be given to the **respective competences of the civilian and military domains**, taking into account the differing national regulatory frameworks in place across Member States.
- Finally, further clarification would be useful regarding the **strategic framework** (including 2030 readiness, NATO capability targets and national defence strategies), as well as the analytical basis underpinning the conclusions of the Plan.

**3. What should be the role of the Council in the implementation of the actions?**

- We consider it essential to ensure a **stronger role for the Council** in defining shared common requirements and safeguarding interoperability.
- In ensuring the **full involvement of Member States**, the Council should contribute to coherence with national policies and complementarity with the broader Euro-Atlantic security framework, while avoiding duplication with NATO structures. It should also promote a clear distinction between political, technical and regulatory levels, while preserving national competences and inter-ministerial coordination.

**4. Do you foresee any particular challenges in implementing the actions?**

- The main challenges of the Plan relate to the need to ensure **strategic coherence and secure synergies with EU, NATO and national initiatives**. Concerns remain regarding the **complexity of multi-level governance**, which may risk slowing down decision-making processes and the implementation of measures.
- Another challenge concerns the **mapping of industrial capabilities**, which will require robust safeguards for the handling of sensitive information. In addition, regulatory measures may have unintended impacts on industrial value chains and national strategic autonomy if not closely coordinated with the defence sector.

**5. Would MS contribute to the establishment of a CoE, and if so, how? Specifically, is there a willingness to contribute by offering specialized human resources?**

- The Italian Ministry of Defence stands ready to contribute as a **complementary actor**, by making available the **technical and operational expertise** of the Armed Forces and Defence entities (EdO). Such a contribution should, however, be subject to a thorough technical assessment ensuring clear governance arrangements and avoiding any interference with national security competences.

**6. Regarding the pillar of the CoE establishing satellite Training & Testing centers: Is there an interest from Member States (beyond those already involved) to offer their facilities for future Commission-funded training sessions?**

- There is a strong interest in **enhancing the role of national testing infrastructures**, which currently appear underrepresented in the Plan compared to centres such as SEASEC in the North Sea. Italy seeks to ensure the recognition and involvement of its centres of excellence within the European network in order to provide a comprehensive and balanced representation of the Union's testing capabilities.

PORTUGAL

S. R.

**MINISTÉRIO DOS NEGÓCIOS ESTRANGEIROS**
**Direção-Geral dos Assuntos Europeus**

**Ad hoc Working Party on preparedness, response capability and resilience to future crises – Brussels, 30th April 2026**

Action Plan on Drone and Counter Drone Security

Guideline Questions

1. *What is your assessment of the strategic and operational objectives proposed in the Action Plan?*

Overall, Portugal's assessment of the Action Plan is positive. The document is timely, well-structured, and appears more concrete than previous initiatives (notably the Commission's 2023 communication), translating the lines of work that have been developed—particularly within the C-UAS Expert Group - into operational measures.

The strategic objectives are relevant, reflecting the growing concern over the malicious use of drones in a civilian context and the need for a coordinated response at the Union level. The focus on prevention and preparedness, complementing the defense dimension with a civilian approach, is particularly positive.

The conceptual expansion to "drones" in the broad sense - not limited to unmanned aircraft—is also highly positive, keeping pace with the evolution of threats, which also include land- and sea-based platforms, even though the legal and operational framework for these remains less developed.

From a strategic perspective, the focus on preparedness, European coherence, interoperability, and coordination across sectors is also welcome. At the operational level, the recognition that the response is not limited to the acquisition of technology is valued, as it is necessary to ensure that the legal framework, information sharing (at the national level and among Member States), training, exercises, doctrine, and coordination mechanisms are clearer.

Nevertheless, it should also be emphasized that the objectives are ambitious, particularly given the proposed timelines, and that there is a significant disparity among Member States in terms of development in this area, which could hinder the uniform implementation of the plan.

Finally, it is important to emphasize the importance of ensuring that the proposed solutions are proportionate and adaptable to different national contexts, as well as to various types of critical infrastructure, including specific contexts such as, for example, correctional facilities.

2. *Which actions would you prioritise?*

Without prejudice to the gradual implementation of the set of measures, the following priorities are identified:


**MINISTÉRIO DOS NEGÓCIOS ESTRANGEIROS**
**Direção-Geral dos Assuntos Europeus**

a) Legislative and regulatory framework:

- Reduce fragmentation among Member States;
- Clarify competences, responsibilities, limits of action, and coordination mechanisms;
- (Rapid) adaptation of the regulatory framework to new threats, including:
- Mandatory registration of operators of smaller drones (>100g);
- Direct remote identification;
- Mechanisms preventing operation without operator identification;
- Regulatory simplification and flexibility for certain operations.

b) Conceptual clarification and terminological harmonization:

- Consolidate concepts and terminology (C-UAS, anti-drone, counter-drone, etc.);
- Establish a common language at the European level, with implications at the national level;
- Develop practical, non-binding guidelines, especially for sensitive civilian contexts.

c) Distinction between cooperative and non-cooperative drones:

- This is a critical operational priority;
- Again, strengthening mechanisms such as remote identification, registration, traceability, and technical interoperability.

d) Strengthening cooperation and information sharing:

- Among civil aviation authorities, law enforcement agencies, and military entities;
- Establishment of structured frameworks for information sharing.

e) Protection of critical infrastructure and resilience testing:

- Voluntary plans to test the resilience of critical infrastructure;
- Ensuring situational awareness, including in the maritime domain (surface and underwater drones), which is very important for Portugal.

f) Technological development and pilot initiatives:

- Real-time capability testing (e.g., cellular detection of dual-use drones).
- Creation of a European "trusted drone" label.

Across the board, the idea is that certain foundational actions (guidelines, concepts, cooperation) can have a more immediate impact than purely technological investments.

3. *What should be the role of the Council in the implementation of the actions?*

The Council plays an important role in ensuring consistency and helping to define the strategic direction. In addition, it must continuously monitor the implementation of the Plan to ensure that all steps are consistent with the European framework, while fully respecting the national competences of Member States, particularly in sensitive areas such as internal security.

It must also promote effective coordination among different EU policies (civil aviation, critical infrastructure protection, data protection, etc.), serving as the forum for coordination and the identification of gaps or needs for adjustment. Finally, it plays a very important role in encouraging Member States to develop national policies that enable them to meet the Plan's objectives.

4. *Do you foresee any particular challenges to implementing the actions?*

Yes. Several challenges have been identified, primarily because the objectives are very ambitious (given the timeline), but also because Member States are at very different stages in terms of the work they have carried out on C-UAS. That said, the following stand out:

a) Fragmentation among Member States:

- Differences in legal, institutional, technical, and maturity aspects;
- Geostrategic circumstances.

b) Balance between ambition and deadlines:

- The objectives seem very ambitious given the proposed timelines.

c) Differences among various operational contexts:

- Given the risk of overly uniform approaches, it is important to have flexibility and the ability to adapt to distinct realities (particularly regarding critical infrastructure, recurring events, what is specific to each urban environment, correctional facilities, etc.)

d) Transforming technology into actual operational capability:

- Detection is an important part of the problem, but it is equally important to be able to interpret each situation quickly, distinguish between legitimate use and threats, and decide/act within short time frames;
- In this regard, it is important to ensure effective real-time information sharing; therefore, it would be appropriate to conduct joint training exercises and seek to develop common doctrines that facilitate coordination.

e) Legal constraints:

- A delicate balance between security and fundamental rights;
- The need to ensure compliance with legislation on privacy, communications, spectrum interference, and aviation security, for example.

f) Resources:

- Limitations on human and financial resources.

Furthermore, regarding cybersecurity, the Action Plan outlines a very limited set of considerations and concrete actions; of particular note is the coordinated assessment of security risks associated with drones and anti-drone capabilities, with risks being assessed within the respective ICT supply chains, and the implementation of the Cyber Resilience Regulation, which will ensure compliance with mandatory requirements for such equipment and systems. In this regard, the implementation of the actions defined by this plan should, where applicable, take into account the structures established for the set of assessments and definition of requirements that may be considered in the field of cybersecurity, while recognizing as the main challenge the requirement for close alignment with the current cybersecurity framework at the European level and respect for the Member States' competences in these matters.

5. *Would MS contribute to the establishment of a CoE, and if so, how? Specifically, is there a willingness to contribute to this new strand of work by offering specialised human resources?*

We recognize the potential of this initiative to strengthen capabilities at the European and national levels. Portugal will closely monitor this initiative. The creation of a CoE, especially if linked to a network of testing, validation, and training sites, represents a very interesting opportunity, provided it is structured with a focus on practical and operational needs.

In addition to the training component, the potential to strengthen coordination between public authorities, end users, academia, and the private sector is also valued, particularly in the areas of testing, validation, and the development of effective solutions.

More broadly, it is understood that the contribution of the Member States to the CoE should be based on a logic of providing "raw material," including incentives and support for academia, support for startups and companies already working in the field of C-UAS technologies, and the promotion of synergies among the following three fundamental pillars: academia, the civilian business sector, and the military sector, specifically in terms of research and operational experience.

Regarding the potential provision of specialized human resources, our position is more cautious, suggesting that this contribution should be evaluated at a later stage, depending on the CoE's operational model.

6. *One of the pillars of the CoE involves establishing satellite Training & Testing centres (with the next session scheduled in early June). Is there an appetite for*


**MINISTÉRIO DOS NEGÓCIOS ESTRANGEIROS**
**Direção-Geral dos Assuntos Europeus**

*Member States (other than those already involved) to offer their facilities for future training sessions funded by the Commission?*

The establishment of satellite training and testing centers is seen as a positive opportunity to build capabilities, test solutions in a realistic environment, and promote knowledge sharing among Member States.

In our case, Portugal's geographical location stands out, as it allows for the simultaneous integration of land and maritime scenarios of strategic interest. Furthermore, favourable weather conditions throughout most of the year facilitate the continuous conduct of exercises and tests. Additionally, there is the potential of the national academic community and the work already carried out by various public entities, including in the maritime sector.

However, before any commitment is made, it is important to clearly define the mandate, the operational model, and the specific objectives of the training programs to ensure they are practical and aligned with national needs. It is equally important to ensure sufficient flexibility to adapt the exercises to different types of critical infrastructure, including specific contexts (such as correctional facilities).

Furthermore, the activities should be funded and organized by the Commission, so it is essential to clarify the conditions for Member States' participation. The potential provision of facilities should be assessed on a case-by-case basis, taking into account operational constraints, security requirements, and limitations on human and material resources.

In short, Portugal is open to and interested in participating, but this depends on a clear definition of the framework, a guarantee of practical utility, and the safeguarding of national capabilities.

**ROMANIA**

**1. What is your assessment of the strategic and operational objectives proposed in the Action Plan?**

Full support for the proposed objectives of the Action Plan. The current challenges posed by drones cannot be dealt with individually by MS. The cross-sector and cross-border nature of the impact that the evolution of drones generates can only be addressed mobilizing a whole of government approach and coordination at EU level. The proposed objectives cover well the most important areas of work and orient in a coherent way the required actions. Where we see space for more clarity is the interlink between internal security and defence and how this coordination will be performed at EU level.

**2. Which actions would you prioritise?**

Given the current challenges and threats, protecting the eastern flank against targeted or accidental drone incursions should be our main priority. This should include development, testing and deployment of counter-drone systems, both in the air domain and maritime domain, for defence and protection of critical infrastructure purposes. Eastern Flank Watch and Drone Defence initiatives should be seen as priorities at EU level and translated into pan-european projects of common interest.
The proposed priorities and milestones in the Action Plan are coherent and can be supported by RO. However, a number of actions are already ongoing (ex. mapping of drone industries in support of UA as part of UA support loan implementation). COM should have as a priority the coordination of various strands of work and ensuring synergies with this action plan.
We can be more ambitious on launching a coordinated security risk assessment on drone capacities with a view to developing a Drone Security Toolbox. The efforts should start immediately.
We see merit in advancing fast on COM pilot action to enhance maritime domain awareness and we will support such an action in the Black Sea. This should include the deployment of undersea sensing capacities contributing to underwater domain awareness.

**3. What should be the role of the Council in the implementation of the actions?**

The Council should use the full set of instruments at its disposal for preparedness and crisis management, to facilitate the implementation of the Action Plan, in particular with a view to ensure the interlink between industry, resilience, security and defence. Similar to military mobility, this action plan should be endorsed by the Council in order to mobilize the full weight of national administrations. It should also include the topic in its structured dialogue with NATO. Annual progress reports should be also presented to the Council.

**4. Do you foresee any particular challenges in implementing the actions?**

The main challenge we foresee is ensuring coherence between defence and non-defence related actions therefore we see merit in involving the EDA from the outset in the implementation of the plan. This Agency provides the interlink between defence efforts of MS and wider EU policies. A second challenge is linked to resources and the need to prioritize EU support to overcome the most

pressing needs. And the most pressing needs are about the lives of EU citizens exposed to constant threat generated by RU drones incidents.

**5. Would MS contribute to the establishment of the CoE and, if so, how? Specifically, is there a willingness to contribute by offering specialized human resources?**

We support the proposal to establish a CoE for drone and counter-drone security and stand ready to support this process including with specialized human resources. We need more clarity on how this CoE will operate, how it will be financed and what will be the human resources required.

**6. Regarding the pillar of CoE establishing satellite Training&Testing centres: Is there an interest from MS to offer their facilities for future COM-funded training sessions?**

We stand ready to contribute to this process but we need clarity on what exactly is required from MS.

**SWEDEN**

1. **What is your assessment of the strategic and operational objectives proposed in the Action Plan?**

Sweden considers that the very rapid developments in the drone domain – and the far-reaching consequences it entails for security and defence policy – justify the broad approach of the action plan and the large number of measures proposed. EU should strictly focus on the measures that deliver the greatest benefits and provide clear added value compared with national actions.

Furthermore, it is essential that the measures should not create duplication of ongoing efforts to counter threats to critical infrastructure. Sweden welcomes that the work and cooperation of relevant EU agencies, within the framework of their respective mandates, are highlighted in the action plan.

Sweden also emphasizes that efforts to strengthen European defence preparedness in the drone domain need to be Member State-driven and based on a clear division of responsibilities between the EU and NATO. To the extent that additional funding is required to cover the increased level of ambition implied by the measures, this should be achieved through reprioritisation within the EU budget.

2. **Which actions would you prioritise?**

The current serious security situation means that society must be able to address multiple threats simultaneously across the entire threat spectrum, that is, both in peacetime and during heightened alert and, ultimately, in war, in order to maintain essential societal functions.

Sweden therefore considers that the most urgent measures are those that contribute to strengthening protection against drones operated by capable hostile state actors. Particularly important are measures to increase capability to detect, hinder and if necessary, take down malicious drones. In this context, improved methods for protecting critical infrastructure against hostile drones are of utmost importance.

In addition, Sweden welcomes the Commission's approach in the action plan to strengthen the capability to detect drones and is positive to further exploring the proposals, for example regarding making use of 5G networks for this purpose.

3. **What should be the role of the Council in the implementation of the actions?**

The Council should have an important role in

- prioritising among measures to be taken, and

- coordinating the Member States in order to increase focus on the various measures.

4. **Do you foresee any particular challenges to implementing the actions?**

Sweden highlights the following challenges:

- fragmentation and overlap of regulatory frameworks with existing frameworks
- risks of overregulation that negatively affect innovation

5. **Would MS contribute to the establishment of a CoE, and if so, how? Specifically, is there a willingness to contribute to this new strand of work by offering specialised human resources?**

Sweden is positive to the establishment of a CoE and prepared to consider contributing to the establishment of a CoE by providing expertise.

6. **One of the pillars of the CoE involves establishing satellite Training & Testing centres (with the next session scheduled in early June). Is there an appetite for Member States (other than those already involved) to offer their facilities for future training sessions funded by the Commission?**

Sweden is analysing the issue and is therefore not in a position at this stage to commit to providing premises and resources.

**SLOVAKIA**

**Written comments of the Slovak Republic on the guiding questions on Action Plan on Drone and Counter Drone security**

**Ad hoc Working Party on preparedness, response capability and resilience to future crises**

**4.5.2026**

Following the last meeting of the Ad hoc Working Party on preparedness, response capability and resilience to future crises please find bellow the written answers of the Slovak Republic to the CY PRES guiding questions on the Action Plan on Drone and Counter Drone security.

Strategic and operational objectives of the action plan are complex and comprehensive and from our point of view they adequately reflect the current security environment, especially the increase in the number of incidents and their hybrid nature. We view positively the interconnections between measures in the area of prevention, detection and response as well as the focus on civ-mil synergies and technological development.

We consider as a priority mainly the measures focused on strengthening the identification, registration of UAS, introduction of obligation for remote identification, development of detection capacities and capabilities (including the use of 5G networks and AI), stress tests of the resilience of critical infrastructure and improving the situational awareness by strengthening the exchange of information.

We see the role of the Council in strategic coordination, support of harmonization and ensuring the political and financial support for the implementation of measures while respecting the competences of the Member States in the area of operational response.

Possible challenges can be foreseen in the area of financing, interoperability of systems, and legislative constrains as well as the need to ensure availability of qualified professional capacities and effective exchange of information.

As for the EU counter-drone Centre of Excellence (CoE) we are ready to contribute with professional capacities, taking part in testing and validation of technologies and sharing practical experiences from the operational environment. We are also open to participate in the activities related to the establishment of training and testing centres if there will be financing available and if there will be clear rules set out on their use and if there will be an alignment with national needs.