Council of the European Union
General Secretariat

Brussels, 07 May 2026

WK 6054/2026 INIT

LIMITE

PROCIV
IPCR
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:	Working Party on Civil Protection – Critical Entities Resilience (PROCIV CER)
N° prev. doc.:	WK 5223 2026 INIT
Subject:	Compilation of written replies to the Presidency guiding questions on the Action Plan on Drone and Counter Drone Security

Delegates will find in annex the abovementioned document BE, DE, FR, IE, IT, NL, PL, PT, SK comments in response to the guiding questions circulated by the Presidency in WK 5223/2026.

BELGIUM

1. What is your assessment of the strategic and operational objectives proposed in the Action Plan in relation to the resilience of critical infrastructure?

While protecting critical infrastructure against drone-related threats is important, it would **not** be appropriate to focus the deployment of counter-drone systems to critical infrastructure. The evolving threat landscape indicates that the misuse of drones extends well beyond critical infrastructure, potentially targeting a wide range of locations, including public spaces, events, and other sensitive sites. A more comprehensive and risk-based approach should therefore be envisaged, rather than singling out critical infrastructure.

Regarding the objectives proposed in the Action Plan we would welcome some clarity regarding:

- Incident notification: *"The Commission will therefore explore with Member States the possibility of progressively setting up an operational, secured, user-friendly and trusted EU drone incident platform, building on regulatory reporting of incidents where relevant and an existing open-source digital platform. The platform would allow a near real-time feed of relevant incidents and be accessible to relevant national authorities."*

We have followed the disucssion in the Antici WP on the Single Entrypoint (SEP) for incident notification in the Digital Simplification Omnibus concerning the idea to develop a EU-platform for incident notification for different legislations by Enisa. We stress again that incident notification by critical entities contains sensitive information. Centralising information like this, on vulnerablities, is creating a new vulnerability. So clarification on this action is welcome. Who is envisaged to notify what kind of incidents and how?

- The proposed EU level counter-drone regulatory framework: what will this entail for critical infrastructure operators?

2. What should the role of the Council be in delivering the Action Plan's objectives and any associated actions?

The role of the Council should be the same as for other matters, when it concerns actions regarding ciritcal infrastructure and CER, discussions should be held in the Council.

3. Of the actions proposed, which would you prioritize? Do you foresee any particular hurdles to implementing them?

The development of a Drone and Counter-drone Security Toolbox proposing proportionate security mitigation measures, in particular for the deployment of counter-drone systems around sensitive sites.

4. Have you identified any synergies or potential tensions between the actions proposed in relation to the resilience of critical infrastructure and those in other areas of the Action Plan?

We see some tensions regarding the philosophy and general framework of CER, where resilience measures need to be taken on the basis of a risk analysis, and the fact that a new legal framework specifically for drones and critical infrastructure operators is going to be developped. We stress to keep the philosophy of the CER Directive in mind, the critical entities who provide essential services in the Member States take resilience measures on the basis of a risk analysis.

_____

GERMANY

Replies by the German delegation of the WP PROCIV/CER to the Presidency guiding questions on the Action Plan on Drone and Counter Drone Security (WK 5223/2026), 30th April 2026:

1. What is your assessment of the strategic and operational objectives proposed in the Action Plan in relation to the resilience of critical infrastructure?

- *The strategic and operational objectives of the Action Plan are welcomed with regard to the resilience of Critical Infrastructure (CI).*
- *In particular, the focus is explicitly welcomed and addresses the current technical fragmentation of one-off solutions towards a holistic approach.*
- *The implementation of the CER Directive in all Member States creates a systematic framework to strengthen the resilience of CI. The timely implementation in all Member States is therefore of high importance.*
- *The risk posed by drones can be taken into account in the national and operator risk analyses and risk assessments provided for by the CER Directive.*
- *A stress test for CI against the intrusion of drones is a suitable measure, on the basis of which the topic and possible needs for action can be examined and analysed in more detail.*
- *Germany is very interested in the EU Commission's proposal for a plan for stress tests of critical infrastructure resilience against drone intrusion based on the model of the previously conducted stress tests of critical infrastructure in the energy sector and submarine cables.*
- *DEU had brought the issue of drone defence to the JHA Council meeting in October 2025.*
- *In Germany, the Federal and State Joint Drone Defence Centre, which has been in place since 17.12.2025, is an ideal point of contact in the context of the exchange of information addressed in the Action Plan and the coordination of measures at EU level.*
- *In line with the requirements of the EU Action Plan, the planned Technology Centre at the German Aerospace Center (Deutsches Zentrum für Luft- und Raumfahrt; DLR) should be used as a platform for standardisation and interoperability of drone defence technology, thus enabling the emergence and widespread use of connectivity-enabled standards for drone defence across Europe.*

2. What should the role of the Council be in delivering the Action Plan's objectives and any associated actions?

3. Of the actions proposed, which would you prioritize? Do you foresee any particular hurdles to implementing them?

- *Whether and to what extent drone defence by private CI operators is legally permissible in Germany is still being examined. This involves a number of complex legal issues, such as the state monopoly on the use of force or interference with the rights of third parties. This should be taken into account when considering the creation of an EU legal framework for drone defence.*

4. Have you identified any synergies or potential tensions between the actions proposed in relation to the resilience of critical infrastructure and those in other areas of the Action Plan?

FRANCE

NOTE DE COMMENTAIRES DES AUTORITES FRANCAISES

Objet : Note de commentaires suite au groupe PROCIV REC du 23 avril 2026 relative au plan d'action pour la sécurité des drones et des contre-mesures anti-drones

Réf : **CM 2079/2026 REV 2 ; WK 5223/2026**

Les autorités françaises remercient la Présidence pour la transmission des questions relatives au plan d'action. Elles prient la Présidence de bien vouloir trouver ci-dessous leurs commentaires et réponses aux questions suite à la réunion du groupe PROCIV REC du 23 avril 2026 relative au plan d'action pour la sécurité des drones et des contre-mesures anti-drones.

1) **Que pensez-vous des objectifs stratégiques et opérationnels proposés dans le plan d'action en matière de résilience des infrastructures critiques ?**

Les autorités françaises soutiennent les objectifs opérationnels et stratégiques proposés dans le plan d'action. Elles tiennent à rappeler à cette occasion que le dispositif de la sécurité des activités d'importance vitale (SAIV) en France prend déjà en compte la menace drone dans l'analyse de la menace de chaque secteur.

Certains secteurs comme celui de l'énergie et des transports comportent déjà des mesures de lutte anti-drone (notamment dans le volet détection) et des travaux sont en cours afin d'élargir la prise en compte de la menace à d'autres secteurs à l'aune de la transposition des directives REC et NIS2.

Pour rappel, les autorités françaises sont en train d'inscrire dans le projet de loi relatif à la loi de programmation militaire, la possibilité pour les opérateurs d'importance vitale/ entités critiques de recourir à des moyens de neutralisation de drone, actuellement uniquement détenus par les forces armées et forces de sécurité intérieure.

2) **Quel devrait être le rôle du Conseil dans la réalisation des objectifs du plan d'action et des mesures associées ?**

A titre principal, les autorités françaises estiment que 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.

Le rôle du Conseil sur ce plan d'action devrait être le même que pour la directive REC : 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.

3) **Parmi les mesures proposées, lesquelles privilégieriez-vous ? Prévoyez-vous des obstacles particuliers à leur mise en œuvre ?**

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 Etat 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 et 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, 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 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, les autorités françaises considèrent que là aussi, ces projets de concaténation d'informations sensibles pourraient potentiellement augmenter l'exposition des vulnérabilités des capacités industrielles des Etats membres, et de leurs capacités industrielles face à des acteurs malveillants. Une meilleure connaissance des capacités disponibles dans le paysage européen est toutefois profitable à l'ensemble des acteurs impliqués dans la lutte anti-drones.

S'agissant du projet de centre européen de certification de solutions de lutte anti-drone, les autorités françaises considèrent que la solution d'un centre d'excellence unique peut présenter quelques lacunes. Un risque d'engorgement des demandes et une saturation sont prévisibles face à la forte demande mesurée. Il semble donc préférable de privilégier le concours de centres de confiance de l'UE et de labélisation (ou certification) afin de répondre aux nombreuses demandes. La France est prête à tenir un rôle dans ces travaux.

Elles demandent à la Commission 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 ou d'amalgame 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.

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.

4) **Avez-vous identifié des synergies ou des tensions potentielles entre les mesures proposées concernant la résilience des infrastructures critiques et celles relevant d'autres domaines du plan d'action ?**

L'élaboration d'un plan pour tester la résilience des infrastructures critiques contre les menaces d'intrusion de drones (« stress test ») semble être une initiative pertinente mais doit être explicitée par la Commission afin que les Etats membres puissent identifier des synergies ou des tensions potentielles.

Les dispositions du plan doivent pouvoir être mises en œuvre sans préjudice des dispositions de la directive REC, notamment en matière de remontée des incidents. La désignation d'une infrastructure critique est une information classifiée, et tout survol par un drone de cette infrastructure ne pourra faire état de son statut d'infrastructure critique auprès d'une éventuelle plateforme européenne de remontée des incidents. Un tel dispositif est déjà mis en œuvre en France, conformément aux dispositions de la directive REC.

Pour rappel, la désignation des entités critiques diffère d'un Etat membre à l'autre, et aucune catégorisation générique n'est envisageable au sein d'une telle plateforme : un opérateur désigné entité critique dans un Etat membre peut ne pas l'être dans un autre.

IRELAND

AHWP Resilience & PROCIV CER

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.

ITALY

Working Party on Civil Protection / Critical Entities Resilience (PROCIV CER 23 aprile 2026) — Action Plan on Drone and Counter Drone Security – Presidency guiding questions

1. What is your assessment of the strategic and operational objectives proposed in the Action Plan in relation to the resilience of critical infrastructure?

The Action Plan recognises CI as a cross-cutting element across all four pillars and rightly leverages the CER Directive as the horizontal reference framework. Operational responsibilities should remain within the MS and their civilian authorities; any evolution towards active response capabilities, including the neutralisation of drones over CI, requires a clear hierarchy of civilian-military competences which the Plan does not fully define.

1.1 Preparedness

Non-binding CER guidelines (Q2 2026) and stress tests for CI: both measures are welcomed.

Drone Security Package (Q3 2026): the traceability of operations near CI is positive. However, the extension of the regulatory framework to *counter-drone* systems highlights potential overlaps with national security competences. An in-depth technical assessment by the competent national bodies is needed, also about the effects on the civilian and military sectors.

Pilot action for maritime domain awareness (2027): the evolution of regional cable hubs into situational awareness centres for maritime CI is consistent with the Italian proposal for a regional mechanism in the Mediterranean, which Italy is developing together with other European countries. This convergence should be leveraged in the implementation of the pilot action.

Expansion of the CUASG (Q1 2026): the expansion of the counter-drone expert group to additional participants is positive: the protection of high-risk CI requires specific military expertise that must be represented. The CUASG should also include defence agencies.

1.2 Detection

5G/ISAC network-based detection (call for expression of interest Q2 2026): this is a relevant choice for CI, which are often located in areas with a high density of network infrastructure and represent the ideal contexts for the first pilot deployments. The governance of the data generated remains insufficiently defined (who has access, with what safeguards).

EU drone incidents platform: there is a foreseeable risk of duplication with the single incident platform envisaged by the omnibus directive (single entry point). Before establishing a new infrastructure, it should be clarified whether and how the two platforms can be integrated, avoiding fragmentation in the reporting of incidents affecting CI.

1.3 Response

Initiative for the deployment of counter-drone systems for CI (Q2 2026): this initiative must not interfere with national security, which is the exclusive prerogative of MS. Significant questions remain open: which authority is entitled to activate the various countermeasures in the vicinity of CI?

Counter-drone rapid response teams (Q4 2026): the logic of European solidarity and mutual assistance is understandable, although it moves towards a *total defence* approach that Italy does not fully share. It is nevertheless necessary to ensure full ownership of MS in matters of national security and CI protection.

2. What should the role of the Council be in delivering the Action Plan's objectives and any associated actions?

The Council should ensure that the development of EU initiatives guarantees full coherence with national policies and complementarity with the Euro-Atlantic framework, avoiding duplication. There are three priority levels of action for the protection of CI.

It is necessary to promote a clear *distinction between political, technical and regulatory levels, as well as between civilian and military responsibilities*, to ensure *governance* of initiatives in a transparent way while preserving the ownership of national competences.

On the regulatory level: the Council should guide work on the *drone security package* (Q3 2026), ensuring that the provisions are assessed by Member States and competent national bodies in their respective areas, and in relation to the potential effects on the civilian and military sectors.

On the coordination level: define the interface between the new strategic coordination mechanism proposed by the Commission and the existing structures (CER platform, CUASG), avoiding overlaps that fragment the governance of CI protection. Clarify which Council working groups are competent for the follow-up across the various dimensions of the Plan, so that the CI dimension is treated coherently and not dispersed across different groups.

3. Of the actions proposed, which would you prioritize? Do you foresee any particular hurdles to implementing them?

Actions to prioritise

First priority — *counter-drone CER guidelines (Q2 2026)*: they are the first operational tool for critical entities and the enabling basis for all subsequent measures.

Foreseeable implementation hurdles

Legal fragmentation: most MS do not have an integrated counter-drone regulatory framework and private CI operators lack the legal authority to neutralise threatening drones.

Overlaps with defence readiness actions: the initiative for CI (section 4 of the Plan) and the joint procurement envisaged under EDIP and SAFE (section 5) partially overlap, without the Plan clarifying the distinction between the civilian logic of CI protection and the military

logic of defence readiness. This ambiguity risks generating duplications in funding and fragmentation in implementation.

Industrial mapping: the collection of information on national production capabilities, necessary to calibrate procurement for CI protection, involves sensitive data. The Plan does not define adequate safeguards for this phase, with the risk of slowing down or distorting the process.

4. Have you identified any synergies or potential tensions between the actions proposed in relation to the resilience of critical infrastructure and those in other areas of the Action Plan?

Identifiable synergies

Implementation of the CER Directive

Maritime CI + regional cable hubs: the proposal to evolve the regional cable hubs into situational awareness centres for maritime CI (2027 pilot action) coincides with the Italian proposal for the Mediterranean. Coordination between the two initiatives can avoid duplication and maximise the coverage of maritime CI in the most exposed areas (Baltic, Black Sea, Mediterranean).

Potential tensions

Allocation of civilian-military competences over CI: the Plan overlaps political, technical, civilian and military levels without clear governance. Two concrete examples: the proposal to entrust EASA with the certification of predominantly military systems such as C-UAVs; and the establishment of pools of counter-drone experts with civilian experience only, ignoring the specific military expertise indispensable for the protection of high-risk CI.

THE NETHERLANDS

NL answers guiding questions Drone and Counter-drone Security Action Plan

1. **What is your assessment of the strategic and operational objectives proposed in the Action Plan in relation to the resilience of critical infrastructure?**
   - NL welcomes the EU Action Plan and stresses that the use of drones poses both economic opportunities, as well increasingly security risks. Considering this, NL supports the comprehensive nature of the action plan, which integrates the different pillars of the resilience cycle.
   - In relation to the resilience of critical infrastructure, NL stresses the importance of public-private cooperation. Therefore, NL looks forward with interest to the Counter-drone deployment initiative. Such initiatives can complement and support national initiatives, for instance on improving interoperability and stimulating knowledge development. Crucially important conditions for these initiatives are proportionality, subsidiarity and respect for national competences.
   - NL is curious which counter-drone capabilities will fall under the scope of the initiative, specifically related to the voluntary joint purchasing.
   - NL also supports using existing EU-mechanisms regarding the resilience of critical infrastructure, such as the non-binding guidelines for resilience enhancing measures under the CER directive.

2. **What should the role of the Council be in delivering the Action Plan's objectives and any associated actions?**
   - The implementation of the action plan depends on effective involvement of the Member states
   - Therefore, regular updates on the implementation of the action plan in council configurations is desirable – similar to the handling of for instance the EU Action Plan on Cable Security.
   - PROCIV-CER should be actively involved with delivering the actions specifically related to critical infrastructure.
   - The council should ensure coherence with other relevant action plans, e.g. European Defence and the ReArm Europe Plan- Readiness 2030

3. **Of the actions proposed, which would you prioritize? Do you foresee any particular hurdles to implementing them?**
   - We curiously await the counter-drone deployment initiative and would like to receive in due course more information on the concrete implementation of this action (such as the scope).
   - For implementation, it is crucial that national operational responsibilities, capacities and competences are respected. The Netherlands focusses on improving detection, classification and intervention capabilities.
   - This action plan is most useful as a supporting instrumenting, complementing national initiatives, while stimulating EU-wide interoperability.
   - Potential hurdles revolve around the (lack of) a European common understanding/language concerning c-uas measures, synchronized and harmonized approach on operational measures, sufficient financing, and effective coordination across departments.

4. **Have you identified any synergies or potential tensions between the actions proposed in relation to the resilience of critical infrastructure and those in other areas of the Action Plan?**

- NL is curious how critical infrastructure will be involved with other actions, such as the EU counter-drone centre of excellence and the drone detection capacity.
- Critical entities under the CER directive must implement an all-hazard risk management approach. The threat of drones is one possible risk in this all-hazards approach. Therefor we would like to have a balanced EU approach on risk management and the resulting (administrative) burden.
- Future legislation, as announced in the Drone Security Package, will have consequences for the managers and operators of critical infrastructure, for instance regarding registration, certification, information exchange and security measures. It is difficult to foresee these consequences at this stage.

POLAND

1. Assessment of strategic and operational objectives

The Action Plan sets the right strategic direction by clearly identifying critical infrastructure as a key area exposed to drone-related threats and by linking this issue to the broader EU resilience framework. At the same time, several elements remain insufficiently defined at the operational level. This applies in particular to the role of testing centres and the planned European C-UAS Centre of Excellence, where it is not yet clear whether the support will be purely technical and certification-related or will also include operational aspects, and within what timeframe full capabilities are expected. A similar gap exists with regard to stress tests of critical infrastructure, where the Plan announces such measures but does not yet provide a common methodology or sector-specific approach.

2. Role of the Council

The Council should play an important role as a forum for coordination and further clarification of implementation priorities. In particular, it can support the development of common approaches in areas that remain open in the Action Plan, such as the methodology for stress tests, the scope and functioning of the incident reporting platform, and the design of support mechanisms such as potential rapid C-UAS Counter response teams. The Council can also contribute to ensuring coherence across different elements of the Plan, including the balance between regulatory measures (e.g. registration above 100 g) and the development of the market.

3. Priorities and implementation challenges

From the perspective of critical infrastructure, key priorities include the development of stress testing, detection and early warning capabilities, and interoperable C-UAS solutions. In this context, it is important to clarify which tools will underpin the early warning system (e.g. incident platforms, 5G sensing, EUROSUR), as well as the scope of the planned incident reporting platform and its interoperability with existing mechanisms. Additional questions arise in relation to more complex threats, such as drone swarms, and the practical functioning of response mechanisms, including potential rapid response teams. Implementation challenges may include legal limitations, differences in national approaches, and the need to ensure adequate resources.

4. Synergies and potential tensions

The Action Plan highlights important synergies, particularly between the implementation of the CER Directive, the development of detection systems, and C-UAS Counter-Unmanned Aircraft Systems capabilities, as well as in the maritime domain. At the same time, some areas require further balancing. This includes the relationship between strengthened regulatory requirements (such as registration of drones above 100 g) and the planned simplification for low-risk operations, as well as the integration of new initiatives—such as the incident reporting platform or the working group on balloon threats—into existing structures and mechanisms. In the latter case, key aspects such as mandate, scope of work and expected outputs remain to be clarified.

PORTUGAL

Please find below the Portuguese replies to the questionnaire:

1) Assessment of the strategic and operational objectives of the Action Plan in relation to the resilience of critical infrastructure

PT considers that the strategic and operational objectives of the Action Plan are appropriate and timely. The Plan is well framed in treating the drone threat as a hybrid, in some cases cross-border and multi-sectoral risk, requiring an approach centred on internal security, while integrating civil protection, transport, borders, cybersecurity and defence. This approach is consistent with the logic of the CER Directive and with the need to strengthen the physical protection and continuity of essential services.

2) Role of the Council in delivering the objectives of the Action Plan and the related actions

The Council should play a role of strategic guidance, political coordination and implementation oversight. In particular, the Council may ensure a cross-cutting approach across the relevant Council formations and working parties, promote coherence between internal security, civil protection, transport, borders, the digital sector and defence and identify common priorities for critical capabilities and for the protection of infrastructure.

3) Prioritisation of the actions proposed and main implementation obstacles

Priority 1 — Priority should be given to the deployment of counter-drone capabilities for critical infrastructure, the development of guidance for operators, and coordinated procurement/deployment mechanisms. This is the area with the greatest direct impact on the continuity of essential services.
Priority 2 — Without a robust layer of detection and identification, response will remain ineffective. For that reason, the single air display, the incident platform and 5G-related testing should advance at an early stage.
Priority 3 — Annual EU exercises and resilience stress tests are essential to validate doctrine, coordination mechanisms and response times.
Priority 4 — Regulatory review, certification, the assessment of high-risk suppliers and the "EU trusted drone" label are important, but their effects are likely to be more gradual.

Main obstacles

The main obstacles are likely to be:

- fragmentation of competences between civil aviation, police, civil protection, defence, sectoral regulators and operators;
- heterogeneity of national legal frameworks regarding detection, neutralisation, digital evidence and data protection; and
- the costs of deploying and maintaining technological measures, especially for private operators.

4) Synergies and tensions between the actions related to the resilience of critical infrastructure and the other areas of the Plan

Synergies

There are clear **synergies** between the protection of critical infrastructure and:

- detection measures, since sensors and data fusion systems improve the protection of airports, ports, energy infrastructure, telecommunications and cables;
- response measures, since joint procurement, rapid teams and exercises enhance the protection of critical sites;

- industrial readiness and certification measures, since these help ensure the availability of secure and interoperable solutions;
-

Tensions / risks

The main tensions appear to be threefold:

- first, between the speed of deployment and regulatory maturity, if Member States seek rapid neutralisation capabilities without a fully harmonised legal framework;
- second, between civil and military needs in the allocation of funding, industrial capacity and access to dual-use technology.

SLOVAKIA

Position of the Slovak republic 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 in relation to the resilience of critical infrastructure? (1) ST 6262 2026 (2) Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. 2

The strategic objectives of the Action Plan are broadly aligned with the CER Directive; however, their operational impact is constrained by the lack of sector-specific implementation guidance and the absence of minimum harmonised resilience measures. While sectoral diversity justifies tailored approaches, a baseline of cross-sector requirements is necessary to avoid fragmentation. In this context, prioritising "Security by Design" for new infrastructure, particularly in response to evolving threats such as counter-drone risks, is essential. Given the high cost and complexity of legacy systems, dedicated funding mechanisms should be strengthened to support innovation, dual-use capabilities, and the deployment of advanced security solutions across both civilian and security domains.

2. What should the role of the Council be in delivering the Action Plan's objectives and any associated actions?

The Council must assume a central and proactive role in delivering the objectives of the Action Plan in line with Directive (EU) 2022/2557. It should not limit itself to general political guidance but provide a clear and binding political mandate for the development of sector-specific resilience measures, ensuring that these are translated into concrete and operational requirements at Member State level.

Furthermore, the Council should actively guide the strategic allocation of EU funding towards design-level innovation and "Security by Design" approaches, while ensuring that sufficient resources are made available to address legacy systems where retrofitting remains unavoidable.

It should also mandate the development of common methodologies, templates, and testing mechanisms, including regular cross-border exercises, to ensure a consistent and measurable level of preparedness.

Finally, the Council must strengthen monitoring and accountability by introducing regular progress reviews and peer pressure mechanisms, thereby ensuring effective and timely implementation of the Action Plan across all Member States.

3. Of the actions proposed, which would you prioritize? Do you foresee any particular hurdles to implementing them?

The Council should support the continued development of a structured "living lab" environment bringing together a dedicated community of drone and counter-drone experts, with the objective of developing sector-specific architectural standards. Such an approach is essential to ensure that resilience measures are grounded in operational realities and reflect rapidly evolving threat scenarios.

In parallel, the Council should prioritise the establishment of clear and targeted safety and security requirements for counter-drone systems, in order to provide legal certainty and predictability for market actors. This should be complemented by the development of an EU-level certification scheme for counter-drone solutions, ensuring interoperability, minimum performance standards, and trust across Member States.

Without such coordinated action, there is a significant risk of market fragmentation, inconsistent security levels, and reduced effectiveness in addressing emerging drone-related threats.

4. Have you identified any synergies or potential tensions between the actions proposed in relation to the resilience of critical infrastructure and those in other areas of the Action Plan?

The Council should recognise that the interplay between the Action Plan and other EU frameworks creates a complex and uneven implementation landscape, reflecting differing levels of maturity in national security systems. In this context, the urgent and full implementation of Directive (EU) 2022/2557 must be treated as a non-negotiable priority. While the Commission's non-binding guidelines are a useful support tool, they are not sufficient on their own. Stronger EU-level coordination, common methodologies, and structured exchanges are required to ensure consistent and effective implementation across Member States.

As a Member State we have recognised a critical legislative gap concerning the role of privately operated critical entities in the detection and mitigation of unmanned aerial system (UAS) threats. In many cases, existing national legal frameworks do not provide a clear legal basis for private operators of critical infrastructure to deploy counter-drone measures, particularly with regard to detection, tracking, and neutralisation capabilities.

In this context, we stress the urgent and full implementation of Directive (EU) 2022/2557 that should be complemented by the development of clear national legal frameworks enabling private critical entities to take proportionate and authorised action against drone-related threats, in full respect of fundamental rights and aviation safety rules.

Furthermore, the Council should call on the Commission to support Member States through targeted guidance and, where appropriate, explore the need for a more harmonised EU approach, including minimum requirements and safeguards for the deployment of counter-drone capabilities by non-state actors.