EUROPEAN
COMMISSION

Brussels, 11.2.2026
COM(2026) 81 final

# COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

## Action Plan on Drone and Counter Drone Security

## 1. Introduction

Drones, whether used in the air, at sea or on land, have become an **integral part of modern economies and societies**. Unmanned, automated and increasingly supported by artificial intelligence, they deliver tangible economic benefits across sectors such as construction, energy, transport, agriculture, emergency response and logistics. Since 2019, the use of airborne drones is governed in the European Union by a harmonised regulatory framework. The growing role in surveillance and reconnaissance has also made drones a key component of Europe's security. From a European industrial perspective, the commercial airborne drone market segment alone is forecast to be worth around EUR 14.5 billion by 2030 and potentially exceed EUR 50 billion by 2033.

However, recent incidents involving malicious or irresponsible use of drones have exposed **significant and growing security challenges** for the Union. Drones have been used in violation of Member States' airspace, they have disrupted airport operations, and caused near-misses with civilian aircraft, highlighting vulnerabilities in our security architecture including in aviation safety. In fact, the impact of these incidents extends well beyond airspace, affecting the protection of critical infrastructure, external borders, ports, transport hubs and public spaces, including densely populated areas, as well as maritime safety and energy security. Specifically, in the energy sector, drones have been used to disrupt the operations of power plants, wind and solar installations, district heating systems and energy transport vessels, demonstrating their potential to undermine continuity of supply and economic resilience. Overflights by unidentified or non-cooperative drones increase security tension and act as a signalling tool, testing Union's preparedness, as well as its capacity to respond and take countermeasures.

Hiding behind these security threats and challenges are a wide range of actors – state and state-linked hostile actors, terrorist organisations, organised crime networks and individuals. They span different levels of intensity, from criminal or negligent behaviour to hybrid operations and military-type activities. They deliberately blur the boundaries between civilian and military domains. They also exploit the cross-border nature of the internal market and shared infrastructure making clear that **a threat against one Member State is a threat against the Union as a whole**.

In this context, while safeguarding critical infrastructure, external borders, public spaces and ensuring aviation and maritime security remain primarily the responsibility of Member States, the cross-border character and high-impact of drone-related incidents make **enhanced coordination, shared preparedness and solidarity at EU level indispensable**. An effective response requires a comprehensive, coordinated and targeted approach, bringing together the civil and military dimensions. This Action Plan is a response to the calls from Member States[1] and the European Parliament[2] to develop a **united approach** against the threats posed by malicious drone operations. It is designed to support Member States through coordinated action and to complement national measures, reinforcing a coherent and effective response.

[1] European Council conclusions of 23 October 2025. EUCO 18/25.

[2] European Parliament resolution of 9 October 2025 on a united response to recent Russian violations of the EU Member States' airspace and critical infrastructure (2025/2901(RSP)); European Parliament resolution of 22 January 2026 on drones and new systems of warfare – the EU's need to adapt to be fit for today's security challenges (2025/2088(INI)).

This Action Plan ensures a **coherent whole-of-government approach**, in full respect of relevant competences, while avoiding fragmentation. This Action plan focuses primarily on the civilian internal security side, where important gaps and loopholes remain, it addresses the full continuum of drone-related threats from the prevention of unintended or negligent incidents to threats against the EU's internal security and hybrid threats, while complementing and supporting the work carried out in the defence domain. It sets out a prioritised set of actions in the civilian field, designed to reinforce prevention, detection and response, and to strengthen civil–military synergies as needed. It also strengthens Europe's defence readiness, in line with work carried out by the EU and Member States through several work-strands linked to the Defence Readiness 2030 Roadmap.

**Enhancing the security of drone operations** and protection from malicious drone use are prerequisites for trust, public acceptance and the large-scale deployment of legitimate drones. This Action Plan therefore also supports a positive agenda on drones. By reinforcing security, it contributes to the development of a competitive European drone market, unlocking the potential for innovation, economic growth and job creation across sectors.

This Action Plan is to be read within the framework of a broader set of initiatives brought forward by the Commission to reinforce the **EU's preparedness, and its internal security and defence priorities**. Considering the imminent security challenges, the Action Plan focuses on actions that can be implemented in the short term, while also designing measures for longer-term preparedness. While most recent threats concern airborne drones, the Action Plan also covers terrestrial, maritime surface and undersea drones, and related counter-drone capacities, as well as meteorological balloons used against some Member States. This Action Plan builds on the 2023 Communication[3]on countering potential threats posed by drones and supersedes its mid-term review as well as on the EU Drone Strategy 2.0[4] which provides the overarching policy framework for the development of a competitive and safe European drone ecosystem.

## 2. Prepare: increasing the resilience of the EU

The Action Plan focuses on **strengthening resilience and preparedness**. This relies, first, on the capacity of Europe to remain at the edge of the technological evolution in drones and counter-drone systems, but also on the capacity to ramp-up industrial production. Second, this requires enhanced actions against malicious drones, with a safe and secure integration of drones into the airspace and the market, as well as increased resilience measures to protect critical infrastructures, external borders and public spaces, the maritime domain.

### 2.1. Ramping up technological development and industrial production of drones and counter-drone systems

Drones are evolving rapidly, with advances in speed, range, payload, autonomy, swarming, AI integration, advanced materials, miniaturisation and resistance to electronic warfare. Counter-drone systems must therefore also adapt fast to keep pace with these evolutions. Supporting the development of these technologies is essential for Europe's preparedness. This requires mobilising the right level of public and private investments at national and EU level, and from both a civilian and defence perspective.

[3] COM(2023) 659 final
[4] COM(2022)652 final

EU funding programmes support the technological development of drones and counter-drone capacities, notably through Horizon Europe or the European Defence Fund. Several schemes are also dedicated to supporting specifically start-ups and scale up to grow, whether it is the European Innovation Council (EIC) through its accelerator scheme, or the EU Disruptive Innovation schemes (EUDIS) for defence applications through dedicated Hackathons and Accelerators, EDA's HEDI (Hub for EU Defence Innovation) as well as BraveTech EU, allowing to build on battlefield-tested innovations from Ukraine. Private financing should also be leveraged to support innovation and the ramping up of production.

However, there is an urgent need to increase coherence and impact between the different EU instruments, including cohesion funds, as well as national investments, with a view to avoid overlaps, reduce dispersion of funds and maximise impact on clear priorities. To that end, the Commission proposes **a new and coordinated framework to boost the technological development** and the production of drones and counter-drone systems building on **five pillars**.

First, the EU must focus its **investment where it really matters**. The Commission will initiate with Member States a **civil-military industrial mapping**, designed to define the right priorities in terms of technologies and capacities. This will inform the investments into the development of technologies, their integration into drones and counter-drone systems and the necessary industrial production ramp-up. Such an endeavour will require cooperation and exchange of information between Member States, the Commission in consultation with the High Representative, within their respective responsibilities, as well as different national and EU actors across the civil and military domains.

Second, the EU must embrace a **new approach to testing innovative solutions** allowing faster movement from lab to deployment. To that end and based on the Commission's proposal for regulatory sandboxes[5], any obstacles to test innovative drone and counter-drone technologies in specifically designated areas and under a temporary and controlled framework established by a Member State or EASA should be removed. European industry needs infrastructure to test and validate counter-drone solutions. The EU will aim to **strengthen a network of multinational test and expertise centres for drones** across Member States, established to test, demonstrate, validate and qualify military or dual-use systems in their specific operational environments, such as the maritime Seabed Security Experimentation Centre (SEASEC).

The **counter-drone Living Lab of the Joint Research Centre** (JRC) will be **upgraded into a fully-fledged EU counter-drone centre of excellence.** The Centre will work in synergy with the **EU Civil-Defence Drone Testing Centre Network** which is currently in its pilot implementation phase in cooperation with the European Defence Agency. It will run – on a regular basis and whenever necessary – a **large testing and validation programme of counter-drone measures**, starting with the first edition focused on the protection of critical infrastructure. The Commission will also support the development of a harmonised testing methodology[6] for counter-drone systems and will issue **a Recommendation on voluntary performance requirements for counter-drone systems**.

[5] Proposal for a regulation of the European Parliament and of the Council on establishing a framework of measures to facilitate the transport of military equipment, goods and personnel across the Union.
[6] Through the ongoing ISF funded project Courageous2.

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.

Fourth, **interoperability** is essential for drone and counter-drone producers to be able to scale production for both the civilian and military markets, bringing flexibility, operational continuity and fostering effective cross-border cooperation. Building on ongoing work by EASA, the European Defence Agency and NATO to align civil-military standards, the Commission, with the support of the High Representative, will examine ways to promote the use of standards applicable to both civilian and military drone and counter-drone technologies.

Fifth, **producing drones and counter-drone systems at scale** is paramount. Many EU industrial actors are ramping-up capabilities in different domains, including submarine drones. The EU therefore needs to invest into massification of production capacities for deployable drones and counter-drone systems, with specific attention to the needs of emergent innovative companies. To that end, the European Commission will assess the possibility to leverage the forthcoming Industrial Accelerator Act, as well as the joint deployment initiative for critical infrastructure presented in section 4. Additionally, it will also use industry reinforcement actions under the European Defence Industry Programme to boost the production in the EU of drones and counter-drone capacities as described in section 5.

European efforts to scale-up drone and counter-drone production must be a joint public-private effort. The Commission will expand industry engagement by convening **a drone and counter-drone Industrial Forum,** building on the Drone Alliance initiative with Ukraine. This will bring together a large ecosystem of underlying and enabling technologies such as chips, AI, quantum, cloud and cyber. The Commission will furthermore consider options for public-private partnership to address key technology gaps for the development and industrialisation of EU produced drone systems.

### 2.2. Enhanced internal security and resilience against drones

The growing presence of unregistered drones in the EU increases the risks of misuse. At the same time, a wide range of state and non-state actors can exploit drones, as even basic "off the shelf" models can be deployed over strategic assets with minimal efforts. The inherent plausible deniability of such acts makes them an effective vector of hybrid threats, capable of causing disruption and exploiting vulnerabilities. It is therefore urgent to level-up resilience requirements across several areas.

#### *2.2.1. Safe and secured integration of drones into the airspace and on the market*

By the end of 2024, the EU drone ecosystem had surpassed two million registered operators, representing an increase of around 20% in just one year. At the same time, professional and higher-risk operations expanded rapidly, reflecting increasing organisational maturity among operators[7]. This rapid professionalisation confirms drones as a permanent and expanding

[7] The number of operational authorisations increased almost five-fold, from around 700 to over 3 400, while Light UAS Operator Certificates (LUCs) grew by more than 60%, Figures: EASA IAM Hub.

component of European aviation, while underscoring the urgency of reinforcing trust, security, and resilience.

The EU has already established a comprehensive aviation framework for airborne drones, providing a strong foundation for the safe development of a rapidly growing sector. However, evolving security threats and recent incidents have highlighted limitations in the current framework. The Commission, in close cooperation with EASA, will propose a **Drone Security Package** to adapt the airborne drone framework to today's security realities, while preserving the conditions for innovation and market growth. It will amend the relevant implementing and delegated acts[8] stemming from the regulation on common rules for civil aviation[9]. The objective is to strengthen the identification and accountability of drone operations, both for drone operators and drone pilots, including by extending registration and identification requirements to all drones above 100g. In this way, the link between operator registration and drone usability will be strengthened, thereby avoiding the use of drones that cannot be identified.

At the same time, the safe expansion of legitimate drone operations requires a modern traffic-management environment. The EU has already put in place a harmonised framework for **U-space[10]**, which introduces digital services to support safe, automated and scalable drone operations. While this framework is in force, its deployment across Member States remains uneven. The Commission will therefore encourage and support a more active implementation of U-space services, in line with national priorities and operational needs. It will also accelerate work with Member States to improve the definition and digital publication[11] of **geographical zones** where drone operations are restricted or subject to conditions. Building on this, the Commission, together with EASA and Member States, will assess the technical conditions for future geofencing functionalities that could help prevent compliant drones from unintentionally entering sensitive or high-risk areas.

The Commission will also present **regulatory simplification measures for drones** aimed at introducing flexibility for certain operations[12] such as removing the need of pre-approval by authorities and reducing the associated administrative burden. This will also include a possible extension of geo-awareness requirements to all drones above 100g.

The Commission will seek to mobilise relevant EU funding instruments to ensure effective and coherent implementation across the Union of the measures outlined above.

Beyond the specific legislative needs and operational measures mentioned above to enhance resilience, a central element of security is to make sure that drones placed on the EU market meet appropriate security requirements so that legitimate drones cannot become a security risk for EU citizens or be turned into threats vectors by malicious actors.

The Commission will therefore propose to initiate work with Member States on a coordinated Union wide security risk assessment of drones and counter-drone capacities, assessing risks in their ICT supply chain. This could be followed by a **Drone and Counter-drone Security**

[8] Implementing regulation (EU) 2019/947 & Delegated regulation 2019/945.
[9] Regulation (EU) 2018/1139 and the related implementing.
[10] Implementing regulations (EU) 2021/664, (EU) 2021/665 and (EU) 2021/666.
[11] Through for instance the EASA Innovative Air Mobility (IAM) Hub.
[12] For Visual Line Of Sight (VLOS), Beyond Visual Line Of Sight (-BVLOS) operations.

**Toolbox** proposing proportionate security mitigation measures, in particular for the deployment of counter-drone systems around critical infrastructures.

With the full application of the Cyber Resilience Act (CRA) in December 2027, a large majority of drones placed on the EU market will be subject to mandatory cybersecurity requirements, thereby promoting security-by-design at product level. Given the important role of semiconductors in the development and operations of autonomous systems, drone manufacturers should **embed trusted chips** in their systems. This means chips that are secure, reliable, and resistant to tampering or cyber threats.

At system level, the Commission will work also on the establishment of an **EU Trusted Drone Label** to further enhance trust in civil drones. The label would rely on independent third-party verification and define additional product-level trust and resilience criteria without duplicating existing EU cybersecurity legislation.

Finally, in view of the fast-evolving markets of drones, and following calls from the European Parliament[13] and Member States[14] to assess the continued relevance and effectiveness of the EU Drone 2.0 Strategy, the **2026 progress review** will provide a comprehensive stock-taking of the Strategy, identifying gaps and delays in implementation, and assess whether its actions remain fit for purpose or require adjustment, notably those contributing to security and competitiveness.

### *2.2.2. Enhancing preparedness at external borders, public spaces and critical infrastructures*

Enhancing EU's preparedness means significantly investing into the protection of critical infrastructures, including in the maritime domain, the external borders and public spaces.

When it comes to the physical resilience of critical infrastructures, the EU has put in place a horizontal framework: **the Critical Entities Resilience (CER) Directive**, which requires Member States to adopt a national resilience strategy, conduct risk assessments in all the eleven sectors covered by the Directive, identify their critical entities and take the necessary to prevent disruptive incidents. Urgent and full implementation of the CER directive by Member States should be an immediate priority. To support Member States and critical entities, the Commission will issue non-binding **guidelines for resilience enhancing measures**, including on countering threats posed by drones and the use of geofencing functionalities. The Commission will also propose to willing Member States a **plan to stress test the resilience of critical infrastructures against drone intrusion**, based on the model of the previously conducted stress testing of critical infrastructure in the energy sector and for submarine cables.

The maritime domain is particularly susceptible to threats and attacks by aerial, surface and underwater drones. Enhanced maritime domain awareness is essential to protect critical maritime infrastructure and serve military needs. Once established, the **Regional Cable Hubs**[15], could be expanded to ensure a broader Maritime Domain Awareness function, using drone assets, and monitoring threats from drones[16] with a view to protection especially all maritime critical infrastructure.

[13] A European Lead Market for Civilian Drones – Now or Never.
[14] COUNCIL: 16054/25 REV 2.
[15] As referred into the Action Plan on Cable Security. JOIN(2025) 9 final.
[16] As elaborated under the EU Action Plan on Cable Security and in line with the European Ocean Pact, relevant actions of the EU Maritime Security Strategy (EUMSS).

To this end, the Commission will **launch a pilot action to enhance maritime domain awareness**. It could be implemented by Member States in the context of the Regional Cable Hubs, promoting coast guard cooperation and involving European Fisheries Control Agency (EFCA), European Maritime Safety Agency (EMSA) and Frontex. The pilot action will also identify gaps and urgent operational needs for detecting and countering drones in the maritime domain. It could be supported by EU defence programmes. Close cooperation with EDA MARSUR project and NATO maritime surveillance systems will be ensured. The Commission will also support the deployment of undersea sensing capacities, contributing to underwater domain awareness capacities, useful both for the protection of critical infrastructure and for defence maritime applications, especially in areas where infrastructures are subject to threats (e.g. Baltic, Black Sea or Arctic regions).

Malicious use of drones can directly undermine control at the external borders and specifically border surveillance by enabling reconnaissance of patrol patterns and border crossing points, facilitating cross-border crime, and disrupting border management infrastructure and operations. The Schengen Borders Code allows the use of civil counter-drone measures to protect land and maritime borders, and by extension, where needed to prevent the circumvention of border controls, extends to airport security perimeters.

The protection of public spaces from threats posed by non-cooperative drones has been at the core of the current Commission counter-drone policy framework[17]. The objective is to provide law enforcement authorities with the right capacities and training to respond to drone threats and to use drones for public security objectives, such as crowd control. The Commission will **intensify its action to support law enforcement** in these efforts, especially upgrading the training to integrate the use of mitigation and neutralisation measures and extend it to operators of critical infrastructures. The already established **counter-drone expert group** will be extended to include relevant EU Agencies (e.g. Frontex, Europol, EASA, EDA). It will support the identification of promising common counter-drone solutions, including by increasing the frequency of classified information exchange. To facilitate this work, a biennial work programme will be developed for the counter-drone expert group.

### *2.2.3. Protection against hybrid threats from other unmanned threat vectors such as balloons*

Over the past year, several hundreds of meteorological balloons have been launched from outside the EU into the airspace of some Member States for different illicit purposes including smuggling. Typically fitted with SIM cards to transmit their location after landing, they allow smugglers to recover the payload. Due to their size, weight, unpredictable wind-driven trajectories, potential operating altitude, and payload capacity, these unmanned balloons pose serious safety and security risks, particularly when overflying critical infrastructure such as airports, where they can cause accidents or trigger closures. Their detection is especially challenging as connectivity modules are usually inactive during flight. As a result, heavy unmanned balloons represent a strategic and largely uncontrollable threat.

Several measures in this Action Plan could be useful to address threats from meteorological balloons. There is a need to take additional measures to disrupt the possibility for criminals to use such balloons and for state and non-state actors to exploit it as a tool of hybrid campaign. The Commission proposes to **organise a specific working group to address the multi-dimensional aspect of the threats**, looking at measures linked to connectivity, spectrum monitoring, diversion of flight path as well as other ways to remedy the threats including

[17] Stemming from the 2023 Communication on countering threats posed by drones.

cooperation between telecommunication operators and national authorities on national security and defence matters. Moreover, in view of bringing innovative, quick and operational solutions to increase the resilience against this type of threat, the Commission, together with the Member States most concerned, will swiftly organise **a mission driven call for interest to the private sector**, especially start-ups, to propose new ways to handle such threats.

**Key actions on preparedness:**

- As a matter of priority, the Commission, together with Member States, where appropriate, will:
  - **Propose a Drone Security Package** by Q3 2026 to rapidly adapt the regulatory framework to new security threats:
    - **Ensure mandatory registration** for all drone operators of smaller drones (above 100g).
    - **Extend drone direct remote identification** obligation to smaller drones (above 100g).
    - **Avoid take-off of drones** unless an operator identification number has been entered.
    - **Introduce regulatory simplification and flexibility** for certain operations.
  - **Work with willing Member States on a voluntary plan to stress test** the resilience of critical infrastructures against drone intrusion.
  - Adopt non-binding **CER guidelines** on resilience enhancing measures for critical entities with targeted guidance on countering threats posed by drones (Q2 2026).
  - Issue a **Recommendation on voluntary performance requirements** for counter-drone systems (Q4 2026)
  - Launch by Q3 2026 a **Coordinated Security risk assessment on drones and counter-drone capacities,** with a view to adopt a **Drone Security Toolbox.**
  - Launch in Q2 2026 **a drone and counter-drone industrial forum – the "D-TECT Forum" (**Drone TEch for Countering Threats).
  - Support the scaling up of drone and counter-drone start-ups and **the ramping up of production capacities**.
  - **Gather immediately a working group** with interested Member States targeting balloon threats and **launch in Q2 2026 a dedicated hackathon on balloons threats,** for the industry and start-up community to propose innovative solutions.

- The Commission, will follow up with Member States, in order to:
  - **Develop by Q4 2026 an** EU Trusted Drone Label to enhance trustworthiness of civil drones placed on the market.
  - **Improve by Q4 2026 the availability of UAS geographical zone information, and by 2027** establish the technical requirements **for geofencing function.**
  - **Establish by Q1 2027 a EU counter-drone centre of excellence** and launch testing programmes, integrating aviation safety requirements. Support the development of **full standard for a harmonised testing methodology** for countering unmanned aircraft systems.
  - **Launch by 2027 a pilot action to enhance maritime domain awareness** to counter surface and undersea drone threats
  - **Expand in Q1 2026** the composition of the Commission-chaired **Counter-drone Expert Group** (CUASG) to include relevant EU Agencies (e.g. Frontex, Europol, EDA, EASA).
  - **Upgrade by Q2 2026 the training cycle for law enforcement operators** to include mitigation and neutralisation measures.

## 3. Detection: increasing the capacity to detect threats from drones

Detection, tracking and identification are central elements in the fight against malicious drone activities. Being able to distinguish friends from foes helps to filter and classify detected drones according to their risk profiles, allowing ultimately to focus the attention and the resources of security authorities. This requires seriously enhancing situational awareness around drone operations, including through the integration of several information feeds which today are not connected. It also requires enhancing detection capacities through the deployment of a multi-sensing approach and leveraging technological evolution as well as telecommunication networks.

### 3.1. Improved situational awareness

The absence of integrated air surveillance for drone activities, combined with the inherent limitations of detection capacities, allows malicious actors to potentially evade detection, at least temporarily, and create plausible deniability. It is therefore essential to improve situational awareness of drone operations.

First, there is a need to **support the integration of relevant data into dedicated single display systems**. Based on the existing regulatory framework such as U-space, as well as a strengthened registration obligations in the future, it will be possible to establish a capacity to detect, track and identify in near real time any legitimate drones. Different information feeds will need to be fused. In this regard, Eurocontrol has developed a **single air display system – CIMACT** (Civil-Military Air Traffic Management Coordination tool), allowing the detection and identification,

in real time of potential threats from drones. The Commission will support the emergence of such tools integrating detection and identification data as well as upstream enablers to distinguish between authorised and non-cooperative drone activity. Looking ahead, enhanced situational awareness could be further strengthened through the gradual development of drone conspicuity solutions, building on U-space, registration and identification frameworks.

Second, **relevant data should be accessible by competent authorities**. The EU regulatory framework for aviation safety already provides the legal basis for it[18]. Building on this, Member States should make practical arrangements to ensure that relevant data is shared among competent authorities in civil aviation, law enforcement and the military. This would allow to monitor and assess the level of threats, ensure faster response, and enforce liability for operators of drones that do not respect security measures.

Third, it is **essential to foster more information sharing between Member States to improve lessons learnt** from previous incidents and establish a clear situational picture. 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. The platform could support the creation of a structured database of non-authorised drones and would benefit from the development of common data format for counter-drone systems. The Commission will support initiatives from willing Member States to enhance information sharing, for instance at regional level.

Fourth, **detection, tracking and identification capabilities** should also be integrated into national border surveillance systems and contribute to the European situational picture, including EUROSUR[19], to enable operational support and the coordinated handling of cross-border incidents. This should also, where appropriate, cover relevant detections in the context of Frontex operations. The Commission will support willing Member States in seeking civil-military synergies with military situational awareness systems and security systems, in full respect of EU legislation.

### 3.2. Deployment of multi-domain sensing capacities

Detection of illegitimate and potentially malicious drones necessarily relies on several sensors. Traditional radar-based detection comes with specific characteristics. Long-range radars detect larger objects at higher altitude, while short-range radars are focusing on short distance tracking. Additionally, different characteristics of drones and drone operations present challenges, such as the reflection of the terrain, the small radar cross section of drones, the low altitude at which drones can fly, and the risk of saturation in case of drone swarms. Consequently, detection of malicious drones requires a **multi-sensor approach, integrated through AI-powered command-and-control (C2) software**, allowing to establish clear situational awareness, in particular to protect critical infrastructure.

**Ongoing technological developments** will enhance detection capacities. For instance, in the domain of both passive and active radar systems, software-defined radars in the X band and

[18] Regulation (EU) 2018/1139, Article 74.
[19] European Border Surveillance system.

beyond can provide enhanced detection capacities. Other areas of interest are **acoustic sensors** such as AI-powered acoustic phased array microphones, LiDAR (Light Detection and Ranging) using pulsed laser, thermal infrared cameras allowing to detect small variations of heat, and optical sensors.

The **EU should enhance its support for home grown development of these dual use technologies**, that must be integrated into multi-domain sensing systems, supported by a modular, distributed, AI-powered C2, and encrypted communication. These systems could either be deployed to protect specific critical infrastructure on a permanent basis or be mounted on terrestrial or maritime vehicles for increased flexibility. These are civilian by design, but they could usefully complement existing military capacities to enhance the overall detection capacities. Interoperability – through the deployment of recognised standards – is key to allow modularity with legacy and future sensors as well as effectors, and smooth integration with air defence or air surveillance systems. These modular capacities could be usefully deployed through a joint procurement programme for the protection of specific critical infrastructure.[20]

### 3.3. Leveraging telecommunication networks for enhanced detection

Existing **5G telecommunication networks could be leveraged to enhance and broaden the detection of drones**. The EU and its Member States should support the deployment of a two-layered cellular based drone detection and tracking capacity.

On the first layer, existing network capacity should be used to **detect connected drones** by identifying unusual SIM card identities, types of data transmission or activities. Networks should provide behaviour-based alerts of fast-moving assets over non-traditional paths, forming AI-based automated detection and early alert systems. This method of detection would rely on a strong partnership between national authorities, and telecommunication operators. It requires also solid industrial partnerships between AI companies and telecommunication providers and operators as well as a full implementation of the 5G Cybersecurity Toolbox[21][22].

This connectivity tracking capacity could be enhanced with the deployment of the **concept of "digital airspace"** providing 5G-based connectivity to drones – and therefore allowing their detection - in higher altitudes than today. To this end, the Commission is working with Member States on an **Implementing Decision to ensure sufficient harmonised spectrum availability in the traditional harmonised terrestrial mobile frequency bands**. This will enable safe operations of drones over large distances. It would also design a mechanism to differentiate a drone from other users and establish an obligation to condition connectivity to the mobile network to a pre-identification as drone.

On the second layer, cellular sensing should be leveraged to **detect non-connected drones**. **Integrated and Sensing Communication (ISAC)** integrates sensing into the mobile communication network. It can in effect turn 5G and next-generation antennas into radar sensors, able to detect the spatial location of any flying unidentified object, including balloons. In the short term, such technology could be deployed above certain locations such as critical

[20] See section 4.
[21] See https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
[22] In line with Cyber Security Act revision COM(2026) 11 and the Digital Network Act COM(2026) 16 .

infrastructure facilities. If and when fully deployed over a territory or a large region, it could be the basis of digital twins, representing digitally the physical presence of objects in the airspace. This could have also potential military applications such as complementing existing military air surveillance systems or detecting radio frequency jamming.

ISAC is being tested by European telecommunications providers, and initial steps have been taken for its standardisation, especially in the framework of 6G. To accelerate its deployment, the Commission will propose the necessary regulatory changes, such as ensuring that spectrum allocation allows sensing, while limiting interference with aviation. To that end, the relevant provisions have been foreseen in the recently proposed Digital Networks Act. At short term, the Commission will propose a mandate to the CEPT (European Conference of Postal and Telecommunications Administrations) to develop technical and operational conditions for sensing, which would be followed by an amended harmonisation decision allowing spectrum to be used for sensing.

Additionally, the Commission will explore with Member States ways to leverage, for both civilian and military usage, 5G telecommunication networks for distributed computing capacity, looking at edge and cloud solutions.

The Commission will **support Member States willing to live test and deploy these new detection capacities** to protect critical infrastructure or scale this detection capacity across a territory serving the military, law enforcement and any other relevant authorities. The Commission will also invited Ukraine to consider its participation in these activities. The deployment of cellular sensing capacities along the borders of Member States most impacted by threats from drones or other flying objects such as balloons could be considered. An appropriate national governance framework will have to be established between civilian and military authorities, telecommunication equipment suppliers, tower owners, telecommunication operators and infrastructure manager, to make sure that national security requirements are explicitly satisfied.

***Key actions on detection:***

As a matter of priority, the Commission, together with Member States, will:

- Launch a **Call for Expressions of Interest** to Member States, Ukraine and European industrial partners to **live test and deploy cellular-based, dual-use drone detection capacity (Q2 2026)**:
    - AI-based early alert mechanism of malicious connected drones enhanced by the digital airspace concept;
    - Cellular sensing detection of non-connected drones;
    - Embedding cellular sensing into current and upcoming military applications.

- **Take the necessary regulatory steps to allow spectrum to be used for sensing** through an amended spectrum harmonisation decision.

The Commission will also follow-up with Member States in order to:

- **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.

- Strongly **encourage Member States to set up an information-sharing framework** between civil aviation authorities, law enforcement and military.

## 4. Response: Stronger EU cooperation and solidarity

Whenever an incident occurs and one or more malicious drones are detected, threats must be promptly and effectively addressed. Operational incident response is the responsibility of Member States, given the strong link with national security and defence matters. However, coordinated actions at EU level can support Member States in the deployment of counter-drone capacities and solutions. This dimension requires strong civilian-military synergies, and well defined and rehearsed rules of engagement based on the threat.

### 4.1. Operational synergies between civilian and military

When it comes to collective air defence, NATO holds a primary role to protect against conventional threats, such as high-end air and missile threats. With the emergence of drone threats, especially low-cost systems, air defence is evolving, requiring an additional layer of counter-drone network. At the same time, protecting borders, airports, seaports, energy infrastructure and sensitive sites from low-cost drones cannot rely on the military alone. This highlights the necessary civil and military coordination. Counter-drone capacities must be approached as a dynamic, adaptable and comprehensive network, for both civilian security and defence purposes.

Once a threat is detected, national protocols are activated leading to preventive measures (such as airspace closure), as well as counter-drone measures from a wide array of solutions. While these procedures are decided and operated at national level, there is a need to stress test them against a scenario of cross border or multi-vector threats but also against emerging threats such as swarmed or miniaturised drones.

Additionally, at very low altitude, counter-drone response requires seconds-long reaction times and tightly synchronised civil–military procedures, which remain uneven across borders. The cost asymmetry between low-cost threats and scarce defensive means, combined with mass and saturation, makes fragmentation difficult to sustain. Divergent data formats, classification and reporting chains prevent a shared low-altitude picture and complicate attribution in hybrid scenarios. Addressing these gaps require interoperability, governance and rapid operational delivery across ecosystems.

This is why it is important that relevant procedures and lines of communication are established between all the actors, including at EU level. To that end, it is proposed to launch, with all relevant civilian and military actors a yearly EU-level counter-drone exercise.

### 4.2. Support on the deployment of counter-drone capacities

A multi-layered and multi-effector (combining several counter-drone technical measures) approach is necessary to counter the large spectrum of threats posed by non-cooperative drones. Counter measures rely on a combination of a wide array of solutions such as jammers, lasers, high power microwaves, drone catchers, cyber takedown as well as hard kinetic solutions, for instance individual or 'in swarm' strike drones, gunnery and short ranges missiles and ammunition.

When drones are connected to a communication network, a possible counter measure includes the capacity to disrupt, slow down, jam or end the connectivity of the malicious vectors, without affecting the connectivity of friendly drones. Based on a request from relevant national authorities, telecommunication operators should be in position to take the necessary measures to ban the SIM or the connectivity module, operate a forceful detachment, or establish a geofencing approach. The Commission is currently working on an Implementing Decision harmonising operational and technical conditions for the safe operation of terminal devices such as drones.

In light of the evolving security situation, it is essential and urgent that critical infrastructures are equipped with the latest counter-drone equipment and systems. In full complementarity with ongoing activities in the defence domain, the Commission will therefore work with Member States to launch – through **a call for expression of interest** – an **EU Counter-drone Deployment Initiative** for **Critical infrastructure:**

First, based on the mapping of needs described in section 2, the Commission will continue supporting **the development of home-grown counter-drone systems** giving particular attention to the support of innovative and scalable approaches, notably from new players across defence and civilian ecosystems. In this perspective, it will work with industry, and Member States, to define priority areas of investment under EU defence and civilian programmes, with the view to scale the approach under the future European Competitiveness Fund.

Second, the Commission will propose a **voluntary EU counter-drone joint purchasing initiative** for deploying counter-drone solutions in critical infrastructures. The objective is to leverage the procurement capacity of relevant EU agencies (e.g. Frontex, EMSA, EFCA), as well as creating synergies with joint procurement (including pre-commercial or innovative procurement schemes) run by relevant national Ministries, notably defence or interior ministries, in the context of the implementation of ISF, BMVI as well as SAFE[23], EDIP[24] and the work of the Drone Capability coalition or, if the Member States choose to, the European Defence Drone Initiative, the Eastern Flank Watch and the Air Shield initiatives, as well as the implementation of the EU strategy for the Black sea and the Black Sea Maritime Security Hub.

### 4.3. Building the "software layer" of counter-drone capacities

[23] Council Regulation (EU) 2025/1106 of 27 May 2025 establishing the Security Action for Europe (SAFE).
[24] Proposal for a Regulation of the European Parliament and of the Council establishing the European Defence Industry Programme and a framework of measures to ensure the timely availability and supply of defence products. COM(2024)/150 final.

Effective counter-drone capabilities are necessarily powered by a Command and Control (C2) system, the software layer allowing to integrate the sensors and the effectors, as the experience of Ukraine has shown. To detect and counter sophisticated and coordinated threats from drones it is essential that Member States jointly develop **sovereign European Command and Control (C2) capacities**, powered by AI software, high level of cybersecurity, state-of-the-art encryption, secured cloud on the edge, and high-performance computing capacity. Interoperable by design, dual by nature, these C2 solutions, should be able to work in synergies with detection capacities and designed to engage with multiple effectors against malicious drones. They should allow integrating legacy equipment, interacting with each other and with relevant civilian and defence systems. In line with the Apply AI strategy, the AI Gigafactories currently being established with the support of the EU budget should facilitate the development of such C2 capacities.

### 4.4. Solidarity: Rapid counter-drone emergency response teams

Facing threats or to secure targeted sites in anticipation of events, Member States must be able to rely on an enhanced, rapid and scalable European solidarity. This is particularly relevant, when the nature or the scale of threats exceeds the capacities of a Member State to respond.

The Commission proposes to work with Member States to set up **Rapid Counter-drone Emergency Response Teams** that could act as rapidly deployable reserve units, equipped with the latest technologies for detection and response, at the request of a Member State authority in a mutual assistance approach. The Emergency Response Coordination Centre could provide the necessary support, as appropriate. The Commission will explore how this can build on the expansion of the pooling and sharing mechanisms of the EU-funded law enforcement networks[25], the Protective Security Advisory (PSA) Programme, and EU agencies (e.g. Frontex) to provide cross-border coverage and the deployment of mobile units in the context of high-risk and high-profile events while maintaining interoperability. It would also work in synergies with existing capabilities such as the EU Hybrid Rapid Response Teams.

### 4.5. Counter-drone capacity integrated in border management

The EU's external borders are subject to intense drone threats across land and maritime border sections and their vicinity. Frontex supports Member States in addressing these threats. It deploys drones for border surveillance in joint operations and promotes interoperability.

The **Commission will support Frontex in the organisation of drone and counter-drone pilots**, live demonstrations and prize-based innovation challenges in realistic border settings. It will enhance the integration of drones and counter-drone skills into the training of the standing corps. Frontex will also provide practical guidance on layered deployment models and cross-border incident handling.

The **Border Management and Visa Instrument (BMVI)** supports Member States in improving border surveillance and detection of threats at the EU's external borders, including on drones and counter-drone capacities. The Commission has evaluated applications received for a EUR 150 million call for equipment. The aim is to support Member States in purchasing

[25] Such as the High-Risk Security Network- HRSN or ATLAS

uncrewed equipment for aerial and maritime surveillance with the ultimate objective of deployment by Frontex in joint operations.

Additionally, a recent EUR 250 million call to better secure EU external borders, including against drones, was published in December 2025. It targets Member States experiencing increased and complex pressure on border management and it supports them in one or more of the three priority areas: the direct purchase of drones and counter-drone systems for external borders, the integration of drones and counter-drone systems into national border surveillance systems and the deployment of innovative technologies and communication systems to address hybrid threats affecting external borders and border crossing points including those in international airports. To facilitate implementation and interoperability, the Commission encourages coordinated approaches among interested Member States, including cooperation through joint/cross-border innovation procurement and joint procurement, where relevant.

### 4.6. Towards an EU level counter-drone regulatory framework

Today, the legal and operational frameworks for countering non-cooperative or unsafe drone activity remain highly fragmented across the Union, as demonstrated by a recent comprehensive mapping study of Member States' regulatory frameworks for counter-drone systems.

Most Member States rely on dispersed provisions in aviation, police, defence and telecommunications legislation, and only a few have started developing integrated national counter-drone strategies. Some Member States have no national rules at all. Civilian and critical infrastructure operators typically lack legal authority to neutralise a threatening drone. Active mitigation measures such as jamming, spoofing or kinetic intervention remain restricted to military and specialised police units due to strict spectrum-interference and aviation-safety rules. As a result, some operators can detect threats but cannot respond effectively to them, which delays neutralisation and increases security risks.

There is therefore a need to consider expanding the framework of the 2023 Communication on countering threats posed by drones towards a **set of common binding and non-binding rules for Member State authorities and private operators** to clarify roles and mandates of all actors involved, including the owners of critical infrastructure. This could include minimum performance requirements for counter-drone systems, harmonised terminology and taxonomy, integrated monitoring, support the incident reporting platform, and incentives for standardisation. It should provide a baseline level of resilience for Member States and be implemented in complementarity with the framework for legitimate use of drones. To that end, the Commission will launch a feasibility study on possible options f**or establishing an EU level counter-drone regulatory framework by 2030**. In parallel, to meet short-term needs, the Commission will issue **a Recommendation on countering threats posed by drones, detailing guidance for law enforcement operators**.

***Key actions on response:***

As a matter of urgency, the Commission, together with Member States will:

- **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).

- As part of the ongoing rollout of AI Gigafactories, support **home grown, dual use and AI-Powered C2 capacities for autonomous assets** with the view to deploy sovereign software solutions.

- **Launch a yearly EU large-scale drone security/blueprint exercise** to testcross border cooperation and civilian/military synergies (first exercise in autumn 2026).

The Commission will follow up with Member States to:

- **Launch a feasibility study for an EU level counter-drone regulatory framework** setting a common minimum baseline for Member State authorities, and private operators of critical infrastructure.

- Adopt a **Commission Recommendation on countering threats posed by drones for law enforcement operators**.

- **Support Frontex in using drones for enhanced border surveillance purposes** through joint operations, drone and counter-drone pilots and live demos.

- Explore by Q4 2026 the establishment **of Rapid Counter-drone emergency teams** to enhance the solidarity and mutual assistance against drone threats.

- Encourage Member States to **develop the right legal framework** in place to allow to take efficient remedial measures, including take downs, against drone threats and empowering private critical infrastructure owners to take the necessary measures.

## 5. Strengthening Europe's defence readiness against drone threats

Beyond enhancing EU's resilience to the wide arrays of drone threats, there is also a need to further strengthen Europe's defence readiness to counter drone threats considering that the use of drones has become an integral part of modern warfare. In this context, Europe is drawing lessons from the unprovoked war in Ukraine, as well from the innovative ecosystem that was put in place to rapidly adjust to the dynamics of the battlefield.

From a defence perspective, the increasing use of drones and counter-drone systems reflects broader evolutions in the security environment, including faster operational tempos, activities below the threshold of armed conflict and the growing interaction between civilian and military domains. These developments affect not only the conduct of military operations, but also wider

considerations related to territorial protection, securing critical assets and overall defence readiness.

Drones are employed across a wide range of military functions, including intelligence, surveillance and reconnaissance, strike, force protection and logistical support. At the same time, counter-drone capabilities have become an integral element of force survivability and freedom of manoeuvre, particularly in contested and saturated environments.

Drones and counter-drone systems are one of the capability priority areas identified and agreed by Member States. The **Defence Readiness Roadmap** has underlined the need to address this capability as a matter of priority. Lead nations and other Member States, with the support of the High Representative, notably through active coordination role of the EDA, have already started work on drones and counter-drones within a dedicated Priority Capability Area (PCA) to address very specific capability shortfalls. Other adjacent capabilities are addressed in capability areas such as Air and Missile Defence, Artillery, Electronic Warfare and Artificial Intelligence. This coordination group provides the framework within which the interdependencies as well as interoperability challenges and operational dependencies can be jointly addressed. It should serve as the main vehicle to coordinate Member States' efforts towards agreed Defence Readiness objectives, including by connecting capability priorities with relevant industrial support instruments.

Regarding financial support, the PCA on drones and counter-drones is aiming at procuring and fostering European industrial capacity in airborne drones through specific objectives and timelines and leveraging the European Defence Industry Programme (EDIP) and the SAFE Instrument. The Commission will intensify its support to this, including through EDIP's collaborative frameworks (Structure for European Armament Programme- SEAP, European Defence Project of Common Interest - EDPCI), facilitating dialogue with the Drone Alliance and performing industrial mapping in coherence with the actions described earlier. This work will feed into the European Drone Defence Initiative, as well as the Eastern Flank Watch initiative, proposed in the Defence Readiness Roadmap.

The Commission and the High Representative will take forward the **European Drone Defence Initiative**, with a view to supporting coherence across capability, operational and industrial efforts at EU level, towards achieving the Defence Readiness priorities, including across civil, dual-use and military strands, and in a cross-cutting manner with ongoing work under relevant PCA coalition efforts.

This work will draw notably on Ukraine's battlefield experience in areas of interoperable data management systems, including Command and Control (integration), detection systems (awareness) and cost-effective effector systems (response). The European Drone Defence Initiative should support a more integrated approach, taking into account key operational dependencies across the full operational response chain. It will aim at building an industrial ecosystem of end-users, innovators, and production lines able to deliver when necessary. Countering attack of swarms of drones requires a modular and interoperable systems, based on an open architecture. Such systems are also instrumental to perform countering strikes in the depth. Strong synergies with the development of dual use C2 systems for the protection of critical infrastructure should be leveraged. This will also contribute to the **Eastern Flank Watch** initiative in domains, such as building of an industrial base for drone and counter-drone capabilities, air and missile defence, early warning, C2 and data management, detection and situational awareness capabilities, kinetic and non-kinetic, as well as Electronic Warfare (EW) effectors.

Efforts at European level should lead to a **comprehensive European drone and counter-drone capability** and offer a multi-layered and multilevel overarching approach, able to link sensors and effectors across the Union, to support decision-making processes and to guarantee continuous situational awareness.

Being able to accelerate the development of increasingly advanced drone and counter-drone defence capabilities is an integral part of defence readiness of Europe. So far, a total of EUR 1 billion from the **European Defence Fund (EDF)** and its precursor programmes have been dedicated to a wide range of drone-related research and development actions. The EU plans to continue investing into drones and counter-drone technologies over the next 2 years, with **EUR 200 million foreseen under the EDF.**

Moreover, EU Member States are about to invest significantly to purchase the latest drones and counter-drone weapon systems through the **SAFE instrument.** This will enhance EU border security, military readiness, and strategic autonomy in systems that are optionally manned, while boosting the defence technological and industrial base and reducing dependence on non-EU suppliers.

The EU will also accelerate the development of innovative and disruptive players in the field of drones and counter-drones for defence. With the upcoming AGILE initiative, the Commission will propose a new instrument in support of agile and rapid innovation of cost-efficient defence products and technologies for armed forces. The BraveTechEU initiative is also expected to include actions aimed at rapid innovation of counter-drone solutions in response to real operational needs agreed with Ukraine, taken forward together with the EDA. The Commission is also facilitating access to capital (equities) for such companies, that will benefit from the EUR 1 billion fund of fund under creation with the EIB/EIF. Furthermore, as announced in the EU Defence Industry Transformation Roadmap, the Commission will launch EUDIS Tech Alliances, setting up a network of defence startup/scaleups and armed forces around priority capability areas. This will help companies to better address Member States' needs. One of these Tech Alliances will be on drones.

Member States need also to invest into massification of production capacity for drones and counter-drone systems, in the same way it is done for Ammunition, either to actively deploy them now or to stock-pile them as strategic reserve. In this vein, and upon agreement of Member States, EDIP will provide support to drone and counter-drone industrial production capacities, which will work in synergies with the civilian equivalent initiative. As part of this work, there is a need to secure access to critical raw materials for the drone industry through research into alternatives or through stockpiling where necessary. Additionally, the Commission will prioritise the implementation of EU Defence Industry Transformation Roadmap in building drone defence capabilities. Beyond 2027, the defence, resilience, security, and space window of the European Competitiveness Fund (ECF), in synergies with other windows, will offer a stable and predictable framework, and flexibility to respond to emerging priorities.

Finally, to enhance the cooperation with Ukraine, the Commission is establishing **a Drone Alliance with Ukraine** as announced in the Defence Readiness Roadmap. This Alliance will bring together system producers start-ups/scale-ups and a community of innovators to build on Ukraine's experience and industrial basis. It will interact with end-users, including from Ukraine, so that it can provide rapid solutions and leverage battle proven solutions. It will also facilitate the work on standardisation, certification and interoperability. It will contribute to establishing of joint ventures and public-private partnerships in EU and Ukraine. The Drone Alliance board will coordinate actions with the Member States and industry representatives. The Alliance will work in full synergy with the Drone Industrial Forum D-TEC. Where relevant

the Drone Alliance will build on network, knowledge, and partnerships generated by the Ukraine Investment Framework and broader EU-Ukraine Partnership.

In parallel, enhanced **EU-Ukraine cooperation on supply-chain securitisation and diversification** will be essential to overcome bottlenecks in drone production, particularly to **ensure surge capacity and availability of critical electronic components**. This will be taken forward notably in the context of the EU-Ukraine Task Force on Defence Industrial cooperation.

The European Union should also, through the full range of relevant instruments and initiatives (including exploring use of EPF and EUMAM), incentivise and support **exchanges and training programmes between Ukraine and Member States for drone pilots, engineers and maintenance specialists**.

***Key actions on defence readiness***

As a matter of priority, the Commission and the High Representative within their respective prerogatives, will:

- **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.
- Support the rapid **industrialisation of drone / counter-drone solutions for defence purposes**.
- Launch **the Drone Alliance Initiative with Ukraine** to incentivise the creation of an innovative industrial ecosystem.
- Incentivise and support **exchanges and training programmes** between Ukraine and Member States for drone pilots, engineers and maintenance specialists.

## 6. International Cooperation

Enhancing the EU's security against drone threats can only be envisaged in a broader context and through cooperation with partners. Cooperation with Ukraine is central to this Action Plan. Many of the actions envisaged will be implemented as part of an intense partnership with Ukraine and across all the strands, which would benefit both Ukraine and the EU.

The Action Plan will open dedicated cooperation with close neighbours, such as the UK, Norway, Switzerland, Iceland, as well as Moldova, the partners in the Western Balkans, in the Mediterranean , the Black Sea region and other partners with which EU's security and defence interests converge, recognising the fact that the EU's partners are subject to the same kind of drone threats. The EU has strong interest in establishing necessary cooperation mechanisms with partners, especially as there may be cross-border considerations in the protection of critical infrastructures. There is particularly a need to envisage mechanism of early alerts between partners when a threat is detected.

A strong EU-NATO cooperation on drones and counter-drone measures is essential for the rapid and efficient delivery of the Action Plan. The Commission and the High Representative will engage in regular and structured exchanges with NATO in order to identify mutual integration of potential dual-use counter-drone solutions, to avoid duplication and maximise synergies.

## 7. Conclusion

The EU must take swift and decisive action to set a powerful example of solidarity and unity. The measures laid down in this Action Plan are designed as the EU level contribution to bring immediate and short-term responses to the continuum of threats from drones the EU is facing. The Action Plan sets a holistic approach by addressing the question of the protection of critical infrastructure, external borders, as well as proposing to adapt the necessary legislation to enhance the security from drones and deploy the latest technological evolution to increase detection and improve response.

The Action Plan should be seen as a dynamic process, to be adapted according to the evolution and nature of the threats. The Actions put forward are proposals to Member States for enhanced joint action and cooperation, based on the principle of co-ownership, to address the entire scope of the issue. Following adoption of this Action Plan, the Commission intends to launch an intense and structured discussion on all the proposed actions with interested parties, including the industry, the European Parliament and the Member States to establish a clear prioritisation of the actions.

To that end, the Commission will consider setting up with Member States a strategic mechanism to coordinate the implementation of the measures proposed in this Action Plan, connecting the different dimensions, and ensuring close cooperation with the Council. In view of this, the Commission invites Member States to nominate a **National Drone Security Coordinator**, whose role will be to oversee, foster and promote the national implementation of this Action Plan. Such mechanism should be without prejudice to the existing technical cooperation platforms in this area. The Commission will publish a yearly census report based on voluntary contributions from Member States to monitor implementation of the Action Plan.