Council of the European Union

Brussels, 18 October 2023
(OR. en)

14394/23

COSI 181
CRIMORG 139
ENFOPOL 433
CT 156
COTER 186
AVIATION 194
JAI 1334

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	18 October 2023
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2023) 659 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT on countering potential threats posed by drones

Delegations will find attached document COM(2023) 659 final.

Encl.: COM(2023) 659 final

EUROPEAN
COMMISSION

Brussels, 18.10.2023
COM(2023) 659 final

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT

on countering potential threats posed by drones

I. INTRODUCTION

This Communication sets out the EU's policy on countering the potential threats from non-cooperative unmanned aircraft systems (UAS), commonly known as 'drones'. It is part of a wider counter-drone package that also comprises two handbooks, which provide practical guidance on key technical aspects of this policy. This package was announced as a flagship action under the Commission Communication *A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe*[1]. This Communication responds to the need to: (i) provide a comprehensive and harmonised policy framework; (ii) build a common understanding of applicable procedures to face the continuously evolving threats possibly posed by drones; and (iii) take into account the rapid developments in technology.

A. Complementing the EU framework on drones

The legitimate use of drones is a key part of the path towards the twin green and digital transitions, as laid out in the EU's 'Drone Strategy 2.0'. They play an important role notably in the domains of transport, defence, commerce, and services. The number of drones in use in the EU is set to grow significantly in the coming years, and they will improve greatly in terms of speed, agility, maximum range, payload capabilities, precision of sensors, and use of artificial intelligence. These developments will lead to a wider range of legitimate and lawful uses for drones. However, in order for this potential to be achieved, it is necessary to address the potential threat that can be posed by non-cooperative drones. A non-cooperative drone is to be defined according to the nature of non-cooperation that could include criminal, illegal (intended regulatory breach) or amateur (ignorant, careless).

This Communication addresses threats posed by drones that are designed for civil use, and it seeks to tackle threats from these drones in a civil environment. Although drones designed for defence purposes are not the focus of this Communication, there remain several interlinkages with the defence domain. These connections include the potential use of smaller drones designed for defence purposes by criminals or terrorists, as well as the synergies between technologies to counter drones. Drones designed for defence purposes could occupy the same airspace as civil drones, and in these cases they need to be identifiable by competent authorities for situational awareness.

The scope of this Communication is specifically on *countering* the potential threats posed by drones. It therefore does not aim to cover the wider dimension of the role of drones in the internal security domain, namely their use for law enforcement, public security, or public safety.

Member State authorities are primarily responsible for countering the threats posed by non-cooperative drones. However, Member States also benefit from action at EU-level, making possible closer cooperation and coordination in the different means and tools used for that purpose. Therefore, this Communication promotes various actions related to community building and information sharing. It is also supporting Member States with guidance, training, funding and operational procedures.

Potentially dangerous incidents involving drones have become more frequent – both within the EU and beyond its borders. It is therefore important to facilitate the uptake of physical or digital counter-drone solutions by law enforcement and other public authorities in the EU and by operators of critical infrastructure. Drawing up an EU counter-drone policy will help to strengthen procedures for testing the

[1] A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe, COM(2022) 652 final of 29 November 2022.

efficiency of available new solutions, and to facilitate the targeted use of research and innovation in that domain. By drawing up this counter-drone policy, the Commission is helping to strengthen an EU market for counter-drone solutions. This will pave the way for increased strategic autonomy and technological sovereignty for the EU, including in areas of critical technologies. It will foster European capacities to develop cutting-edge solutions in the defence, aerospace, and civil-security domains and reduce dependence on non-European suppliers. This will build on the outcomes of the assessment of critical technology dependencies[2] and will provide further data and analysis. It will also: (i) inform the Commission's understanding of the use of critical technologies and dependencies on non-European suppliers; and (ii) provide a sound overview of the level of dependency.

Moreover, with a view of countering threats posed by non-cooperative drones from a public authority's perspective, it is also important to: (i) have clear and harmonised frameworks and procedures in place; (ii) provide clear authority for responsible public and private stakeholders to intervene against non-cooperative drones ; and (iii) facilitate collaboration between stakeholders that are not always accustomed to working together (law enforcement, civil aviation authorities, operators, manufacturers, mobile-network operators). This Communication puts forward actions to: (i) build a common understanding of applicable procedures when dealing with threats posed by drones; and (ii) identify possible needs in terms of harmonisation of regulatory measures

B. Addressing a current – and rapidly evolving – threat

Both the EU's 'Security Union' strategy[3] and the Counter-Terrorism Agenda[4] stress that the threat of non-cooperative drones is a serious concern in Europe.

The rapidly advancing capabilities of drones pose a growing security risk. In recent years, plans have been uncovered to try and make use of drones for terrorist attacks[5]. There have also been sightings of suspicious drones around critical infrastructure, such as energy facilities, airports, and ports, indicating the potential misuse of drones for hostile information gathering. Drones are used by criminals engaged in smuggling across borders, or to facilitate other illicit operations, including drug trafficking. Drones can furthermore be a source of cyber risks, for example if being used for digital reconnaissance. Threats posed by drones are not simply a technical problem. Today, most drones designed for civil purposes may be detected and identified, but it is still very challenging to engage or neutralise them (i.e. to take control of them, land them safely, or shoot them down), often due to the lack of legal authorisation to do so. This is especially true for private operators of critical infrastructure. Countering the threats posed by drones should therefore be taken into consideration in future risk assessments under the Directive on the resilience of critical entities[6].

The threat picture becomes even clearer when looking at incidents in countries near the EU and in other parts of the world. Drones proved a cost-efficient and effective dual use platform that boosted defence innovation in the Russian war against Ukraine. The use of drones designed for civil purposes for destructive

[2] A Commission-internal deep-dive assessment on autonomous systems conducted in 2022.

[3] EU Security Union Strategy, COM (2020) 605 final of 24 July 2020.

[4] A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, COM (2020) 795 final of 9 December 2020.

[5] Examples include: (i) the plan of an inspired jihadist who was sentenced by a Spanish court in October 2022 for planning to attack a stadium during a major football match using a drone packed with explosives; and (ii) a Belgian citizen, sentenced for attempting a bomb attack using drones against a prison.

[6] Directive on the resilience of critical entities (EU) 2022/2557 of 14 December 2022 (OJ 2022 L 333, p. 164).

attacks even in other armed conflicts (such as in Yemen or Syria) is a phenomenon likely to have implications for the EU's internal security. The modus operandi of terrorist groups and the enhanced skills in the use of "off the shelf drones" could reach our borders and represent a threat. The same is true for the use of drones for attempted targeted assassinations[7].

However, counter-drone solutions are not only necessary against targeted malicious use. They are also needed to prevent incidents caused by negligence or recklessness. Most drone users in the EU (notably licensed professional remote pilots or organised leisure pilots) comply with existing rules, regulations, and technical limitations. Nevertheless, ignorant, careless, and criminal drone users are responsible for the many dangerous incidents involving drones across the EU. Large-scale public events are particularly vulnerable to such disturbances, as are some critical sectors like air transport. In addition, the unlawful use of drones can also affect the personal safety and right to privacy of individual members of the public, notably when drones are operated in residential areas.

C. Keeping pace with technological developments

Protecting our societies against malicious and non-cooperative drones requires access to affordable and reliable counter-measures that enable flexible solutions. Solutions usually address the three aspects of detection, tracking and identification, while public authorities are also interested in two additional aspects: neutralisation and forensics.

In both the defence and civil-security domain, innovative counter-drone solutions are already being developed and tested. Their entry into the market and their uptake by end-users can be facilitated by an overarching EU framework on countering drones, as it is promoted in this Communication. However, it is not possible to have a standardised 'one-fits-all' approach to the implementation of counter-drone measures due to the large variety of possible operational scenarios and environments.

Counter-drone measures must therefore be adapted to different needs and different operating environments. From the perspective of authorities in charge of internal security, there may be situations where the full physical destruction of a drone is the preferred and only option, for example to prevent an imminent attack on people or infrastructure. In other cases, such as criminal use or the hostile gathering of information, there is a strong interest in securing control of the drone to land it while leaving it as intact as possible, so as to allow for optimal forensic investigation. This includes the need for sophisticated cyber solutions to take control over a drones operating system.

One of the technological trends that should be monitored and actively used is the development of sensors for the more accurate detection of drones. Existing sensor capabilities can be further developed not only to detect a drone, but also to assess the threat it poses by flight-pattern analysis, payload detection, and equipment detection. Sensors and detection systems need to be able to cope with the changing shapes and capabilities of drones (speed, agility, ability to deploy decoys, etc.). The capacity of public authorities and private operators of critical infrastructure to analyse data from those sensors will be increasingly important. Artificial intelligence will also play a role, for example by automatically generating alerts, calculating risks, predicting routes, or predicting landing sites. Thus, new trends in drone markets need to be continuously monitored and incorporated into counter-drone solutions. The monitoring of these technological developments should enable the authorities in the EU to identify priorities for investment and to support

[7] Examples include an unsuccessful attempt to assassinate the President of Venezuela, and Mexican drug cartels using drones against representatives of other criminal organisations.

the developments that are best suited to meeting the operational needs expressed by Member State law enforcement authorities and private operators.

On engagement and neutralisation, further testing is needed on technologies that are suitable in different environments and scenarios. In the defence domain, solutions have been identified to physically destroy or entirely capture a drone while it is in the air, thus reducing the generation of debris which could lead to injuries to people or damage to objects. This includes directed energy in the form of high-energy lasers, as well as the use of high-powered radio-frequency and net-capture systems as well as digital tools to gain control over non-cooperative drones.

For law enforcement and investigation, it would be particularly helpful to be able to neutralise a drone threat by taking control over its control system and safely landing it, giving authorities and investigators the best possible access to potential physical and digital evidence. Therefore, a wide range of different solutions should be available and validated for different purposes to serve the internal security domain. It is therefore necessary to foster a genuine market and innovation environment for counter-drone solutions that serve the needs of the civil-security domain. Otherwise, developments in counter-drone solutions are unlikely to keep pace with the increasing numbers and capabilities of the drones themselves. It is also essential to structure and segment this market to help relevant authorities to identify the solutions that best meet their needs.

In addition, it is important to monitor so-called counter-counter-drone systems used by criminals. Counter-counter-drone systems are devices that are either carried by the drone or deployed from the ground and are designed to obstruct specific counter-drone measures.

Finally, many counter-drone systems are also developed for defence purposes. Although different in requirements, they often share common characteristics and technologies with systems intended for civil purpose, leading to a need for close cooperation with the defence domain.

This evolving technological landscape also requires a consistent and continuously updated regulatory framework for the use of counter-drone systems.

II. FORMULATING AN EU COUNTER-DRONE POLICY

The Commission has worked with Member States and other stakeholders on the potential threat posed by drones since 2016, when the first EU counter-drone workshop took place. Since then, a wide array of initiatives has been introduced to facilitate community building, information sharing, the development of best practices, and the dedicated funding of projects. As a result of discussions with Member State experts, the Commission will continue to support these ongoing initiatives while further developing and integrating new strands of work to draw up a fully-fledged EU counter-drone policy. This work will consist of the following six key activities:

A. Community building and information sharing

A wide range of different networks and actors is now working at EU-level on counter-drone solutions. There is therefore a need to streamline and steer their future activities in policy, technical, and operational terms to: (i) build functioning stakeholder communities; (ii) ensure the effective sharing of information and best practices; and (iii) avoid the duplication of work.

The Commission will foster existing initiatives at technical level while setting up a **Commission counter-drone expert group** to provide advice at policy level. This expert group will be able to provide strategic input to various EU-level policies with relevance for counter-drone activities, such as in the domains of internal security, border management, or critical-infrastructure resilience. To this end, the expert group will cooperate with other expert groups and, where appropriate, with relevant Council working parties.

Workshops and expert meetings on counter-drone solutions and policies take place regularly. These bring together policy makers, technical experts, and researchers from the Commission, Member States, other EU institutions, EU agencies, EU-funded projects, international organisations, and partner countries. These activities have led to the continuous engagement of all stakeholders, significantly facilitating their operational and practical cooperation. To this end, the Commission has set up **the Counter-UAS Information Hub**[8] which currently has more than 300 members. This online platform is regularly updated and hosts different sources of information, such as outcomes from relevant EU-funded projects, presentations, reports, and a semi-annual newsletter.

Another important part of community building and information sharing, notably for the operational needs of law enforcement, takes place as part of the EU-funded **European Law Enforcement Networks**. For example the following networks have all started their own activities on countering the threats posed by drones: the European Network of Law Enforcement Technology Services (ENLETS); the EU Network for Police and Border Guard Units at airports (AIRPOL); the EU Network of Special Intervention Units (ATLAS); and the EU High-Risk Security Network. The newly created Law Enforcement Network Working Group, a DG HOME initiative aiming to foster cooperation among police networks and funded by the Commission[9], will streamline the ongoing strands of work in the counter-drone domain in a dedicated sub-working group.

The **European Aviation Safety Agency (EASA)** has drawn up non-binding guidelines helping authorities and airports to prepare for, respond to, and recover from drone incidents[10]. In order to promote informed support activities and policy-making at EU-level, it is essential to have reliable and detailed exchanges of information on incidents involving drones in the EU beyond the exchanges already taking place in specific critical areas such as airports. While fully respecting the confidentiality of investigations, there is significant potential to improve the sharing of information on: (i) methods used by operators of non-cooperative drones; (ii) specific threat patterns; and (iii) potential risks identified. To facilitate and harmonise the sharing of such information on incidents, the Commission shared with Member States a template for reporting on drone incidents. To further increase the quality and frequency of information sharing, the Commission will explore the possibility of setting up a **digital platform containing information on drone incidents,** for the use by relevant public authorities. It could serve to properly identify and collate major

[8] Using the EU CIRCABC platform that is supported by the European Commission's ISA² programme, which promotes interoperability solutions for European public administrations.

[9] The (informal) Law Enforcement Network Working Group (LENWG) is chaired by the Commission, and met for the first time on 20 March 2023 to foster better cooperation between the networks funded by DG HOME. After a twelve-month evaluation period, the LENWG could be turned into a proper Commission Expert Group.

[10] The European Union Aviation Safety Agency (EASA) published in March 2021 a set of guidelines for managing drone incidents at airports: Drone Incident Management at Aerodromes.

security incidents involving drones in the EU. This may include also the cyber dimension as drones are used not only to visual reconnaissance, but also digital reconnaissance. This platform would be consistent with existing reporting obligations under Regulation (EU) No 376/2014[11] and would not duplicate existing efforts.

The Commission will also organise regular classified meetings to promote the exchange of lessons learnt from incidents in an appropriate format.

Key actions for community building and information sharing

- **The Commission will set up an expert group, consisting of Member State experts and other stakeholders on counter-drone activities.**
- **The Commission will explore the possibility of developing a digital platform containing information on drone incidents.**
- **The Commission will organise regular meetings to facilitate the exchange of classified information between Member States on major security incidents involving the use of drones.**

B. Testing counter-drone systems: identifying and testing solutions

Member States and local authorities can choose from a wide array of commercial- cyber and non-cyber-counter-drone solutions that are available on the market. Making this choice is challenging, especially for local entities that do not have sufficient technical capabilities. The Commission will help Member State authorities to make the right choice for their operational needs by providing advice and guidance via the dedicated counter-drone expert group and the work of the Commission's Joint Research Centre (JRC).

EU-level activities to test counter-drone systems were launched in 2019. They aim to develop a common methodology for evaluating systems that can be used by law enforcement and other public authorities to detect, track, and identify potentially malicious drones. A central pillar of these activities is the 'Courageous'[12] project (2021-2024), which is funded by the EU Internal Security Fund - Police (ISF-Police). Courageous is led by the Belgium Royal Military Academy and has been tasked with: (i) identifying relevant standard scenarios for testing counter-drone systems; (ii) developing functional and performance requirements; and (iii) developing a testing methodology. The project is also testing the performance of sensors and integrated systems. Outcomes from the project are continuously shared with Member States as well as selected partner countries and international organisations. After completion of the project, the Commission and the Courageous consortium will present options to Member States to ensure the sustainability of the project and recommend a **methodology for counter-drone testing facilities** in Member States.

Technological developments of relevance to counter-drone systems are evolving rapidly. Therefore, testing activities must be complemented by constantly monitoring trends to identify both the most promising solutions and any potential new challenges to the development of counter-drone systems. The JRC has built up capacity to conduct this monitoring and to identify these new challenges. This benefits Member States and provides valuable input to EU-level testing initiatives. The information will be shared through appropriate channels notably the expert group.

[11] Regulation (EU) 376/2014 of the European Parliament and of the Council of 3 April 2014 on the reporting, analysis and follow-up of occurrences in civil aviation, amending Regulation (EU).

[12] https://courageous-isf.eu/.

Standardisation is one instrument to harmonise technological solutions. The Courageous project drew up specific advice on pre-standardisation, based on which the feasibility of – and need for – launching standardisation processes can be further assessed. At EU level, good progress has been made with the development of voluntary performance requirements for detection equipment outside aviation (e.g. for x-ray machines and metal detectors[13]). Together with experts from Member States and industry, the Commission will now also develop **voluntary performance requirements** for counter-drone systems, where relevant in coherence with provisions of Cybersecurity Act[14]. Setting up a certification process for counter-drone systems should remain a mid-term objective. Where appropriate, hybrid civil-defence standards will also be considered.

Standardising and certifying the cybersecurity of counter-drone systems, especially if they are provided by suppliers from non-EU countries, is another key element. At this stage, there remains uncertainty over how well protected the data are that are gathered by certain detection systems. In addition, it is important to prevent as much as possible the hacking and misuse of counter-drone systems by ensuring the cyber resilience of their components.

In September 2022, the Commission adopted a proposal for a regulation on cyber resilience[15], aiming to draw up general cybersecurity rules for products with digital components – both hardware and software – that access the single market. The proposed new regulation aims to introduce mandatory cybersecurity requirements for these products. These requirements will include cybersecurity by design and by default, as well as requirements to address vulnerability. As proposed by the Commission, drone systems that are not developed exclusively for national security or military purposes and that are not already certified in accordance with Regulation (EU) 2018/1139 would be covered as products with digital elements by these new rules, with the exception of those developed exclusively for national security or defence purposes.

Key actions for testing counter-drone systems

- **The Commission will work on implementing a harmonised testing methodology for counter-drone systems based on the outcomes of the Courageous project.**
- **The JRC will compile an annual report on technical developments in counter-drone technology.**
- **The Commission, in cooperation with relevant expert groups, such as the Law Enforcement Networks ENLETS, HRSN, AIRPOL, will develop a set of voluntary performance requirements for counter-drone systems.**

C. Practical guidance and operational support

Tackling threats posed by non-cooperative drones has already been identified as a priority in a number of publications by the JRC, such as in guidelines focusing on building perimeter protection[16] and in the

[13] Commission Recommendation on voluntary performance requirements for X-ray equipment used in public spaces, C(2022) 4179 final

[14] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification

[15] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454 final.

[16] Karlos, V. and Larcher, M., Guideline - Building Perimeter Protection, EUR 30346 EN, Publications Office of the European Union, Luxembourg, 2020,.

dedicated study on drone-transported explosive charges[17]. Moreover, the recent publication[18] on the concept of security-by-design highlights the importance of integrating proportionate, appropriate, and multifunctional protective measures in a thought-through approach from the very beginning of the planning and design phase of a project, including measures to counter any attacks that make use of drones.

Furthermore, EASA's manual on *Drone Incident Management at Aerodromes* provides guidance on how to develop appropriate arrangements and procedures which support an incident-response system at airports that is quick, effective, and proportionate. In this way, air-traffic suspensions, or the closing of air space or runways, may be avoided or kept to a minimum and airport closures would remain a last resort. EASA's work takes account of the International Civil Aviation Organization's guidance on aviation security[19].

Two new handbooks have been developed by the JRC:

- ***Protection against Unmanned Aircraft Systems:*** *Handbook on UAS protection of Critical Infrastructure and Public Space - A five Phase approach for C-UAS stakeholders*

- ***Protection against Unmanned Aircraft Systems:*** *Handbook on UAS Risk Assessment and Principles for Physical Hardening of Buildings and Sites.*

In the area of **training**, the EU-funded project DroneWISE[20] created a package of counter-drone command, control, and coordination strategies for first responders. The project also produced 10 training modules, a handbook, and an online training portal. These training modules have been integrated into the curriculum of CEPOL, the European Union Agency for Law Enforcement Training. Another ISF project that was dedicated to counter-drone training was the Skyfall project. There is a need to further extend the available training to private security providers, specifically those responsible for protecting critical infrastructure.

The Commission's **EU protective security advisers (EU PSA) programme**[21] has a section devoted to counter-drone activities, which offers: (i) a specific vulnerability assessment for high-risk facilities and infrastructure; (ii) practical advice on how to cope with the drone threat; and (iii) practical advice on how to cope with the deployment of drone-detection equipment during high-risk events. The Commission will explore the need to create an EU pool of counter-drone equipment available for Member States to support them at large-scale events.

Exercises such as those organised with the Law Enforcement Network at EU-level contribute to operational preparedness in different domains of internal security. Where relevant, the Commission will work with the relevant networks to include counter-drone elements in future exercises. This will help to further increase knowledge and the exchange of best practices, making use of different solutions. One requirement for an effective response to threats posed by drones is that there needs to be reliable secure communication between different authorities. Therefore, countering threats posed by drones will be part of the future exercise planning to be conducted as part of the EU-funded BroadEU.Net preparation project, testing the

[17] The threat of UAS using explosives was investigated by the JRC in: Larcher M, Karlos V, Valsamos G, Solomos G: Scenario study: drones carrying explosives, JRC107683, 2018

[18] European Commission, Security by Design: Protection of public spaces from terrorist attacks, JRC131172, 2022.

[19] The ICAO Aviation Security Manual (Doc 8973 – Restricted) assists Member States in implementing Annex 17 to the Chicago Convention by providing guidance on how to apply its standards and recommended practices (SARPs) Aviation Security Manual.

[20] https://dronewise-project.eu/

[21] https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en.

basis of the future EU critical communication system[22]. Furthermore, joint exercises could be conducted including cybersecurity and drone security experts address cyber risks posed by drones, as well as digital solutions to neutralise drones.

Key actions for practical guidance and operational support

- **The JRC will publish two handbooks as part of the counter-drone package.**
- **The Commission, in cooperation with relevant agencies, will support extending existing counter-drone training to the private security sector.**
- **The Commission will integrate the counter-drone components in the planning of exercises, in cooperation with the Law Enforcement Networks.**

D. Research and innovation

The EU is continuing to finance its security-research programme as part of **Horizon Europe (2021-2027)**[23]. This security-research programme represents roughly 50% of overall public funding invested in the EU and its Member States in the area of security. As a strategic contributor to various EU security-policy priorities, this security research has also already begun to address the threats posed by drones. Notable examples include ALADDIN, which provides solutions for detecting and neutralising drones in restricted areas[24] or 7SHIELD, which researched the development of counter-drone solutions for ground segments of critical space infrastructure. The ALFA project was also successful in developing a system to detect and track drones used for smuggling[25]. These research and innovation initiatives may be continued under Horizon Europe, validated, or supplemented by actions undertaken within the ISF-Police.

In the future, the Commission will facilitate the more systematic exchange of relevant project outcomes with relevant stakeholders, including via the Community for European Research and Innovation for Security[26]. This would further strengthen specific data exchange. It would also make it possible to more efficiently gather user requirements and communicate these requirements to industry in order to steer innovation. Furthermore, the systematic exchange of project outcomes will help to make possible a structured dialogue with Member States and stakeholders to identify promising technologies, tools, and solutions that could be taken up by a group of Member State authorities. In that context, the Commission will assess with Member States[27] the possibility of: (i) creating an independent research topic on counter-drone solutions in the future work programmes of Horizon Europe; and (ii) supporting specific innovative

[22] The EU critical communication system will provide a secure, broadband-based infrastructure to ensure cross-border interoperability of communication systems used by law enforcement and emergency responders in the Schengen area.

[23] Previously, until end 2020, security research and innovation were financed under Horizon 2020 and the 7th framework programme.

[24] https://cordis.europa.eu/project/id/740859.

[25] ALFA is also the basis for the ISF-project Courageous and its testing activities.

[26] The Community for European Research and Innovation for Security (CERIS) brings together security research stakeholders, ranging from policy makers, end-users, academia and industry to civil security: https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en

[27] In the Horizon Europe programme committee configuration 'Civil Security for Society'.

systems via pre-commercial procurement[28]. This is fully in line with the capability-driven approach detailed in the Commission's staff working document 'Enhancing security through research and innovation'[29].

Strengthening synergies in counter-drone solutions between Europe's civil-security, defence, and space industries is crucial. The aim of this should be to foster synergies in drone and counter-drone technologies among the three sectors[30]. In practice, strengthening these synergies means that defence projects can benefit from innovative developments in the civil domain, while civil aeronautics can benefit from developments in defence.

The **European Defence Fund (EDF)** and its precursor programmes incentivise and support collaborative, cross-border research and development in the area of defence. Complementing and amplifying Member States' efforts, the EDF promotes cooperation among companies and researcher of all sizes and from all Member States in the EU. The EDF precursor programmes have already funded counter-drone projects as part of defence research and development.

The EDF work programme for 2023 contains a counter-drone development action[31], with an indicative budget of EUR 43 million. The action aims at developing hardware or software modules for a comprehensive mobile solution to counter a wide range of drones, including swarms.

The main expected outcome of the EDF's support in the counter-drone area in 2021-2027 is a developed prototype of counter-drone solution leading up to possible future joint procurement at the EU-level. Technological challenges in the area of counter-drone systems are addressed through the EU Defence Innovation Scheme (EUDIS). Furthermore, the EUDIS includes a strand for dual-use incubators to promote better collaboration between the civil and defence domains and to spur technological maturation and adaptation.

Another key pillar for innovation – and specifically for applied research on how to counter threats posed by drones – is the work of the JRC. As part of the JRC's Drone C-UAS project, the JRC will review active and passive counter-measure technologies, and how these technologies can be used to ensure the security of public spaces and critical infrastructure.

To this end, and as a first step, the JRC will create a **living lab** to study counter-drone technologies and how these technologies can be applied in real-world settings. The lab setup will cover the planning, preparation, and implementation of a solution. It will also cover detection, tracking, identification, neutralisation and the integration of stakeholders and processes. The scope of implementation for the living lab will include integration with manned and unmanned traffic-management systems, most notably U-space[32]. The living lab will also study how machine learning and artificial intelligence can be integrated in order to improve the overall performance of a counter-drone solution.

---

[28] Pre-commercial procurement (PCP) is an approach to the public procurement of research and development (R&D) services that was outlined in the PCP Communication (C(2007) 799 final) of 14.12.2007. It is an important tool to stimulate innovation, as it enables the public sector to steer the development of new solutions towards its needs.

[29] Commission Staff Working Document 'Enhancing security through research and innovation', SWD (2021) 422 final of 15.12.2021.

[30] SWD (2022) 362 of 10.11.2022. As described in the progress report on the implementation of the action plan on synergies between civil defence and space industries under Action 9.

[31] C(2023) 2296 Commission Implementing Decision of 29.3.2023 on the financing of the Europe Defence Fund established by Regulation (EU) No 2021/697 of the European Parliament and the Council and the adoption of the work programme for 2023 - Part II.

[32] Commission Implementing Regulation (EU) 2021/664 on a regulatory framework for the U-space. The term 'U-space' has been adopted to describe the management of unmanned aircraft traffic to ensure the safe interaction with other entities using the same space in urban areas and any other location.

In the medium term, this JRC living lab will be developed into a **counter-drone centre of excellence.**

Priority actions for making the most of research and innovation

- **The Commission and Member States will decide on future needs for new counter-drone solutions to be addressed by relevant European research and innovation programmes, notably Horizon Europe.**
- **The Commission and Member States will identify a list of promising counter-drone solutions and assess the feasibility for pre-commercial procurement of some of these solutions.**
- **The Commission will identify ideas, technologies, and solutions to be integrated into the development of defence capabilities, and will support projects that seek to disseminate these ideas, technologies, and solutions to civil sectors.**
- **The JRC will establish a counter-drone Centre of Excellence as further evolution of a living lab.**

E. Funding support

The Commission will continue to provide financial support to relevant counter-drone activities, primarily through the ISF but also under the Instrument for Financial Support for Border Management and Visa Policy (BMVI) and the Horizon Europe programme (for research- and innovation- related actions).

The ISF thematic facility will support: (i) the European Law Enforcement Networks; (ii) the related work of the JRC; (iii) the new counter-drone expert group; and (iv) the creation of an information exchange platform. The Commission is already funding projects to pilot and validate systems to detect and locate drones that illegally cross the EU's external borders. Those projects are based on results from previous EU-funded research projects[33].

Under the ISF's thematic facility, the Commission will open in the first half of 2024 a **call for proposals** aiming specifically at supporting the deployment of counter-drone solutions with high potential for uptake.

Member States will be encouraged to implement this Communication and take up the results of EU- funded research into counter-drone solutions through their ISF programmes.

Key actions for funding support

- **The Commission will launch a call for proposals on counter-drone solutions under the ISF's thematic facility work programmes for 2026-2027.**
- **Member States will be encouraged to make full use of their ISF programmes for 2021-2027, in order to identify and implement efficient counter drone solutions.**

[33] Examples include projects funded under the BMVI specific actions on: (i) innovation for sea/shore, and/or land borders; and (ii) Frontex. Some projects funded under the specific action on innovation for sea/shore, and/or land borders focus on piloting innovative surveillance technologies. There is also a specific action for purchasing and making available equipment for deployment by European border authorities to detect and locate drones that cross borders in connection with illegal or criminal activities. This specific action will enable Member States to procure two counter drone systems. As an EU added value, upon a request made by Frontex as part of the annual bilateral negotiations, the technical equipment purchased under the specific actions must be put at the disposal of Frontex for a period of up to 4 months per year, for use in its joint operations.

F. Exploring regulatory measures

Although the EU has regulated the legitimate use of drones, at the EU-level there are currently no specific counter-drone regulations that set a common harmonised framework for Member State authorities, operators, and manufacturers. Although the non-binding EASA guidelines addressing drone incidents at airports (referred to earlier in this Communication) were favourably received by the sector, their advisory nature and limited scope makes them insufficient to mitigate the threat posed by non-cooperative drones. As the need to effectively prevent the unauthorised use of drones is constantly growing, the Commission, in close collaboration with experts from the Member States, will further analyse the need for legislative or non-legislative measures in the future. To that end, the Commission will initiate a dedicated **mapping study** to establish the current regulatory landscape. This mapping study should also take into account the ICAO framework and developments, as well as consider that rules to counter the potential threats posed by drones should not unduly impede legitimate operations, including the activities of organised leisure pilots.

Airports in the EU benefit from detailed and comprehensive security rules that also cover the threat from drones. To ensure that aviation authorities and airports are more resilient when faced with the risks posed by drones, and in line with an evidence-based approach, the Commission will in cooperation with Member States **identify potential additional vulnerabilities in protection against non-cooperative drones in a security-risk assessment that may mandate regulatory changes**.

A structured dialogue with industry and drone manufacturers on security-by-design measures is needed in this context (e.g. robust systems against spoofing, capability limitations, sharing of communication protocols, and updates for counter-drone databases).

Key actions for exploring regulatory measures

- **The Commission will initiate a mapping study to identify regulatory needs and the potential for harmonising Member States' laws and procedures.**
- **In line with an evidence-based approach, the Commission will undertake an aviation security-risk assessment on drones to identify potential additional vulnerabilities of airports, which could mandate regulatory changes.**
- **The Commission will engage in a structured dialogue with industry on the necessity for – and nature of – potential additional specific measures relating to the security of drones.**

III. WAY FORWARD

To ensure that rapid technological developments and the growing number of drones do not lead to an uncontrolled increase in threats posed by non-cooperative drones, it is necessary to step up cooperation at EU-level, based on the comprehensive EU counter-drone policy set out in this Communication. To this end, current EU-level activities will be continued and supplemented by the set of key actions listed in this Communication which will be implemented in the coming years.

The activities outlined in this Communication will cover the period until 2030. By 2027, a mid-term stocktaking through the expert group will take place, while a full revision of the EU's counter-drone programme is planned by 2030 at the latest.