Feedback on
EC Call for Evidence for an Initiative on
Drones – countering the potential threats from unmanned aircraft systems

The European Organisation for Security (EOS), as the representative of the European Industrial and Research Security Community, welcomes the European Commission's initiative to collect evidence on countering the potential threats from unmanned aircraft systems (UAS). EOS believes that UAS deployment and development should go hand-in-hand with the implementation of security standards, procedures and guidelines to avoid misuse and strengthen European civil security.

UAS applications offer great potential for the resilience and growth of the European economy and society through the automation of urban mobility and logistic-related services. At the same time, their surveillance and monitoring capabilities can contribute to and strengthen the security of public spaces, critical infrastructures and border management. UAS are already being deployed for defence purposes and are used by law enforcement across Europe to monitor large scale public events, as well as manage Europe's external borders among others. Undoubtedly, the development and deployment of UAS should be further encouraged by the Commission in all sectors and specifically in civil security applications (e.g., for the protection of ports, offshore facilities, airports, critical entities, in major events, for disaster relief etc) through a forward-looking approach based on European research and innovation.

At the same time, however, as the technology matures and its uses increase, so do the opportunities for misuse. For example, UAS in themselves can be tampered with or have their course diverted to cause harm. On the other hand, commercial drones – including recreational drones and larger unmanned aerial vehicles – can be used directly by malicious actors for espionage, to carry explosives, illicit substances, smuggling of illegal goods, in other contraband activities, to hijack telecommunications systems or simply to cause mass panic and disrupt the provision of services in a hybrid attack. UAS could also be used together with other physical or cyber means to monitor for vulnerabilities or hijack signals in a way that would facilitate an attack. These examples showcase how UAS misuse is a particularly wide topic, referring not only to terrorist but also criminal activities. As such, strong pan-European standards and guidelines are needed to support European resilience and security, while allowing UAS technologies to further develop.

In terms of solutions, raising awareness of potential threats among public authorities and private actors that could be targeted is a key step, followed by the implementation of countering UAS (C-UAS) technological and non-technological solutions. These solutions could be sensors, spectrum analysis equipment, data analysis software, radars able to detect UAS of any size and other detection services including cameras or AI-based solutions. EOS recommends that the Commission scales up the deployment of C-UAS for civil security purposes both for critical infrastructure and public spaces protection. These technologies include soft kill solutions such as jamming and cyber-enabled take-over. Directed Energy Weapons (DEW) such as High Power Microwave (HPM) systems and (dazzling) laser systems could be very effective against malicious drones. Kinetic means such as semi-automatic interceptor drones and net capturing devices should also be considered to physically take down drones safely.

EOS also wants to stress the point of critical infrastructure protection from UAS misuse. As Member States begin the transposition of the recently adopted Directive (EU) 2022/2557 on the resilience of critical entities, operators will also begin to assess existing risks and gaps in their systems. EOS maintains that the potential threat posed by UAS should be included in this assessment and operators should be encouraged by Member States and the Commission to implement technological solutions and non-technological procedures that could also counter such threats. EOS recommends opting for integrated security solutions for critical infrastructure that address the ecosystem's concrete needs. Member State authorities should also continue to investigate to which extent they could implement detection solutions as part of national civil security programmes and offer services to operators or be used by law enforcement, especially taking into consideration that UAS may fly in lower zones of airspace not covered by radars or overseen by the airforce. The new challenges in airspace brought by the wide use and misuse of UAS would require new powers and tools for national authorities, as well as a cooperation framework in case multiple authorities are involved in dealing with a potential incident (LEAs, air traffic controllers, air force, private operators). A European approach to how and when C-UAS can be used is also necessary to facilitate their use.

To conclude, EOS calls for the Commission's support to studies, assessments, guidance documents and research programmes. For example, programmes like the JRC DRONE looking into a proof of concept for countering UAS for critical infrastructure should be expanded and all actors should be consulted for the development of C-UAS handbooks. R&I programmes bringing together industry, critical entities and law enforcement to define and share requirements and standards to ensure that C-UAS equipment is operational and fit for purpose will also be extremely beneficial. Finally, scenarios and guidelines for all relevant actors to train and prepare their staff for incidents would be beneficial.

EOS members remain open to further contributing to the Commission's ongoing work in this field.

3 April 2023