EUROPEAN COMMISSION

DIRECTORATE-GENERAL MIGRATION AND HOME AFFAIRS
DIRECTORATE-GENERAL FOR MOBILITY AND TRANSPORT

Chair's Statement

on the outcome of the High-Level International Conference and subsequent EU-internal meeting on countering the threats posed by unmanned aircraft systems (UAS)

Brussels, 18 October 2019

On 17 October 2019, the European Commission organised a High-Level International Conference on countering the threats posed by unmanned aircraft systems (UAS), the latest in a series of meetings on this topic organised by the Commission in recent years. The aim was to bring together stakeholders from EU Member States, third countries, international organisations, industry, academia and civil society to exchange views on how best to combat the potential for disruptive, sometimes malicious use of drones. The International Conference was followed by an EU-internal meeting on 18 October involving Member States, relevant EU Institutions and EU Agencies. The participants recognised the many positive use cases for drones and their potential to make many missions safer, greener and quieter. However, there is also a potential for drones to be misused for terrorist and other criminal acts. Participants identified several areas where further European action on drone threat mitigation should be explored.

First of all, there is a clear need for authorities and other stakeholders to understand and be equipped to continually **assess the developing security threats posed by drones**. **Regular risk assessments** in vulnerable sectors, e.g. aviation, critical infrastructure, mass events, borders, prisons, etc. should inform associated counter-drone work.

Secondly, there is a need to continue to **empower competent authorities to exclude non-cooperative drones from restricted airspace.** The EU recently adopted a set of regulations aimed at ensuring the safe operation of drones in Europe that also have security relevance. For instance, they require drone operators whose operations may present a risk to safety, security, privacy, and protection of personal data or environment to register with national authorities. They in turn are given the authority to restrict drone use in specific geographical zones. Furthermore, off-the-shelf drones will be required to emit a remote identification signal. This will facilitate the identification of, among other things, the drone and its operator. While these measures will make it easier to protect vulnerable facilities like airports, prisons, and stadiums from unwanted drone incursions, they can still be circumvented by determined antagonists. The unmanned traffic management concept in Europe (U-Space) that is currently under development should enable authorities to more effectively identify cooperative drones in urban airspace. At the same time, for U-Space to be viable, it must account for the concerns of law enforcement and other security authorities operating drones in the same airspace.

Thirdly, there is a need to **facilitate the development of effective tools to counter non-cooperative drones now and in the years to come.** This work must necessarily account for the rapid pace of technological advances, how these might be leveraged by antagonists, and the anticipated impact of incidents in different sectors. Doing so will allow stakeholders to develop tools that are commensurate to the risk. For instance, the European Union Aviation Safety Agency (EASA) recently initiated a research project looking into the impact of mid-air collisions between manned aircraft and drones, the result of which should allow authorities to calibrate their responses in line with anticipated effects. It is clear that effective, workable plans and routines are central to any response regardless of sector. Actors should be encouraged to work proactively in laying out responsibilities and putting in place procedures for use in the event of a drone sighting. In the aviation sector, ongoing industry discussions on contingency planning should be encouraged and the need for a regulatory intervention at European level explored.

There is a pressing need for effective, cost-efficient drone countermeasures solutions. Member States, EU Agencies and EU-funded research initiatives in both the civilian and defence arenas are involved in the development and testing of countermeasures. However, the continued evolution of the threat means that even more testing will be needed in order to make informed procurement decisions at national level. The participants emphasised the need for authorities and other relevant stakeholders to share both the burden of testing countermeasures and outcomes, and encouraged the Commission to support and facilitate a coordinated approach that includes appropriate funding mechanisms and accounts for ongoing and future relevant initiatives. For instance, the Commission was encouraged to explore possible EU funding to support cooperation between law enforcement authorities on the testing of countermeasures. In this regard, there is a need for close dialogue between authorities and countermeasures developers working to meet end-users' performance requirements, which could be subject to harmonisation. No matter which technological solutions authorities deploy in different settings, there will always be a human dimension to their operations. For this reason, adequate training and guidance organised both at national and EU level is essential in ensuring that drone countermeasures are deployed effectively and within the bounds of applicable law.

Furthermore, **the drones that find their way onto the European market need to be safe, secure, operationally reliable, and difficult to use for malicious purposes**. Industry is now required to meet certain technical requirements described in the new EU regulations on drones. Besides these mandatory measures, there is a need to continue to explore with industry possible additional voluntary steps that can be taken to make it harder for off-the-shelf drones and drone components to be used in ways that are non-compliant with applicable law. By the same token, the drone industry should make every effort to ensure that their products are cyber-resilient, especially drones that are tasked with providing essential services, such as critical infrastructure facility inspections. In this context, issues of data integrity, confidentiality, and privacy are of relevance. Finally, a future in which drones will operate at low altitudes over urban centres is predicated on secure and reliable communications systems.

There is also a need to **cultivate a common drone culture** in Europe. A key way to reduce the number of violations of restricted airspace is through effective outreach to members of the public, e.g. by implementing the existing requirement of a mandatory information leaflet with each purchased drone. By further raising people's awareness about the risks and liabilities associated with drone operations in restricted areas (like in the vicinity of airports, for instance), we might be able to achieve a common European "drone culture", where citizens can distinguish between appropriate and dangerous and/or criminal drone use. Besides reducing the number of accidental incursions into controlled airspace, greater public awareness could encourage the public to report on incidents, including instances of misuse. The successful prosecution of rule-breakers may also contribute to a better understanding of the responsibilities of drone operators. Doing so requires that authorities have appropriate awareness of the issue and robust forensic capabilities.

Finally, **the exchange of good practice and experiences** across sectors and continents must be intensified. This pertains to areas such as legislation, the setting of standards, testing of different solutions, and operational routines/practice. It is clear that the drone issue is a cross-cutting one that affects a wide range of sectors here in Europe and around the world. It is local and global, public and private. It involves cities, regional authorities, national governments, and likeminded international partners. For these reasons, it is vital that we maintain a vibrant cross-sectoral and multi-level dialogue in the years to come.