Position Paper on the European Aviation Safety Agency Technical Opinion

Introduction of a regulatory framework for the operation of unmanned aircraft (dated 18.12.2015)

The Confederation of European Security Services (CoESS) welcomes the EASA's Technical Opinion, published on 12 December 2015.

CoESS acts as the voice of the private security industry, covering 23 countries in Europe and representing 2.2 million guards, over 60,000 companies and generating a turnover of over €34 billion.

The private security services provide a wide range of services, both for private and public clients, ranging from Ministry/EU Institutions buildings to nuclear plants, airports, critical infrastructure facilities, inter-modal transport hubs, public transport stations and areas, national governmental agencies and institutions (such as asylum seekers centers, public hospitals, universities, etc). The role of security in protecting people, assets, and society at large is increasing and public-private partnerships in security are becoming the norm in Europe.

In performing its mission, the private security industry abides by codes of ethics and codes of conduct and is sensitive to citizens' concerns regarding data protection and privacy. Whilst this aspect is not covered in this document, as it does not fall under EASA's scope to address this, we feel that concerns must be discussed in an open and transparent way, as well as the technological means that can be used to address them. It is crucial that citizens have a full understanding of how private and public players abide by legislation on data protection and privacy.

As indicated in the EASA document, and highlighted in the Riga Declaration, drones represent a huge opportunity for Europe, creating jobs and economic opportunities. Likewise, for the private security services, drones represent an interesting and useful addition to the range of technological means and equipment it already uses. It is also in line with the industry's new paradigm, the so-called "new security company", which responds both to demographic trends and customers needs and whereby people and technology are combined in such a way as to optimize the service to clients.

General comments on the EASA Proposals:

This position paper comes in addition to the earlier opinion expressed during the online consultation of EASA on drones in September 2015.

The first observation on the Technical Opinion is that it is written from the perspective of safety, rather than security. In this sense there are risks, weaknesses and threats arising from the use of UA's, which

will, as time goes by, require adaptation and adjustments. This is similar to the fears and risks identified when automobiles were first introduced.

However we live in a very different time compared to those that saw the introduction of cars, and the combination of the threat level, the development of Information and Communication Technologies, "Big Data" and the "Internet of Things" create a situation where the highest care must be taken.

As it is outlined in our detailed comments, CoESS:

- ***Supports the spirit*** of the regulatory framework along the following principles:
  - Risk- and performance based approach
  - Progressive and operation-centric
- Supports ***more stringent rules for the open category*** than those foreseen in the Technical Opinion, for reasons of both ***safety*** and ***security***;
- Supports ***rules that are harmonized as much as possible across the EU***, even where they cover areas of national competence. This cannot be achieved through legislation, unfortunately, so CoESS can only encourage Member States to cooperate in order to achieve as much consistency as possible;
- Takes the view that ***Public Private Partnerships should be concluded*** to carry out ***new tasks of security-related inspection, detection and prevention***, and that these can only be done with ***duly registered and licensed companies***, which employ duly licensed, carefully screened and vetted staff. Private security companies meet these conditions, which are key to ensure the right security measures in those missions.
- Highlights that there is currently ***no legal basis to act against drones that are threatening*** the assets of private security companies' customers. This should be discussed and clarified, and a consistent response should be found across the EU. As highlighted above, one of the missions that private security companies could cover is to detect and prevent against the bad use of UA's, whether it be unintentional, intentional or malicious.
- Suggests that ***a different regime than that foreseen for commercial activities should be provided for private security companies***, in view of the fact that, together with law-enforcement agencies or rescue services, they perform ***specific security and safety operations***. The employees who work for the private security industry are all ***licensed and specifically trained*** to perform missions that can be ***technically complex and sensitive***, and are ***used to cooperating with the police*** and other law enforcement agencies. Furthermore, private security companies protect ***sensitive assets and infrastructure*** and, therefore, cannot be treated in the same way as companies performing purely commercial services. To this end, ***CoESS proposes***

that it contributes actively in providing "standard solutions" (cfr Proposal 20) and that ***operation authorizations are given by type of operation***, rather than for each specific occurrence of such operations.

Specific comments

2.3.4. Use of product legislation

Whilst these provisions are sufficient for the "harmless" category, they are insufficient for the "open category", which needs to have tracking devices and backup systems. For the specified category, these devices and systems must also be provided.

2.3.6. Oversight and Enforcement

Whilst it is clear that there is no competence for harmonization through legislation, it is important that there be consistency across the EU.

Penalties should also be defined for bad use of UA's in a consistent way throughout the EU.

Public-private partnerships should be defined to carry out tasks of security-related inspection, detection and prevention. The rules that oversee the activities of private security companies create the right environment for such missions. In fact both the company and its staff must be specifically licensed – and the staff must abide with specific criteria, is selected and vetted carefully.

With regard to the bad use of UA's, where this threatens the assets of private security companies' clients, there is no legal basis to act against these UA's, in particular what can and can't be done, and what the liability is.

2.3.7. Environmental Protection

UA's are a useful tool to detect potential environmental damage, such as leaks, fires, or pollutions, and should not only be seen as potential threats to the environment.

Regarding the noise-reducing devices mentioned in this paragraph, CoESS suggests that the noise should not be fully reduced to the point that the UA cannot be detected by the sound it makes, as sound is often used by drone detection equipment.

2.3.8 Occurrence Reporting

CoESS would like to understand how this extension is operated concretely, and in particular if a rule of proportionality would apply.

Furthermore, as some of the incidents might affect critical infrastructure, a rule of confidentiality should be considered, in that some information could be too sensitive to be communicated to the general public.

3.1. Safety risks

The second indent at the beginning of this section reads “mid-air collision with manned aircraft”. CoESS suggests that this should be made more general and read “collision”, as not only mid-air collision with manned aircraft can occur, but also ground collision with any other equipment or mid-air collision with unmanned aircraft.

Furthermore, the risk linked with launching and landing of UA’s should be considered. The type of launch and land should also be listed in the safety risks (vertical or other type of launch/land).

Further risks could also be listed, including, but not limited to:

- Radio interference
- Noise on the spectrum
- Chips being cloned
- Cyber security and hacking
- Insider threat in organisations using drones

3.2. Security and privacy risks

The power and power source of UA’s can also generate security risks, for example fuel-operated drones.

What happens when the UA’s battery is low should also be addressed, and in this case the “back to base” mode should govern and could not be overthrown.

3.3. Benefits

CoESS would welcome a specific mention in this paragraph of private security operations as a benefit to individuals, companies and authorities alike. It protects individual, commercial and public assets, which are critical to society in general, and the use of drones in this mission will be an opportunity. In addition, search and rescue, fire detection and assistance in disaster areas can also be improved thanks to the use of UA’s.

As indicated in the general comments, the private security industry sees benefits in two types of activities with drones:

- Supporting guards in their missions, making their work less dangerous and more efficient, as well as replacing guards in certain cases, allowing more focused action where human intervention is needed;

- Detecting and preventing from the ill use of UA’s – subject to rules and regulations creating a legal basis for the type of response and the ensuing liability as a result of the latter.

3.4. Risk mitigations

As indicated in the general comments, it would be desirable to optimize harmonization in the way that risk is addressed, limitations and other provisions aimed to mitigate risks. As it is well understood that this cannot be achieved by EU legislation, it would be essential that Member States cooperate and seek to establish common rules as much as possible.

3.4.1. Operational limitations

As highlighted in the general comments, private security companies perform missions that aim to protect critical infrastructure, such as ports, airports, energy plants, etc. As a result they should have exemptions to no fly zones for specific categories of operations through Operation Authorizations.

For example, they should be able to fly over ports, airports during closing of the airspace, industrial areas, etc., or more zone types and situations should be created and described.

3.4.2. Technology and airworthiness

The speed of technological improvement and the difficulty to follow it make it difficult to design hack-proof solutions. CoESS would just like to mention that whilst the limitation of performance is a useful feature for the general well-intentioned public, it will not be sufficient for ill-intentioned people who can alter the systems and boost the UA's performance.

3.4.4 Identification, registration and enforceability

CoESS highlights the difficulty for the registration system to be enforced within the EU, let alone the rest of the world. For example, mobile phones can be bought in certain countries with no (CC)ID. It is expected that this will also be possible for UAs. Furthermore, identifying the UA is not sufficient; it should also be possible to identify the operator. UAs may cause the same issues as connected object within the so-called "Internet of Things" environment.

Finally, for specific operations in security, it should be mandatory to be registered / licensed in accordance with the security regulations of the various EU Member States. This gives the guarantee that the UA is operated by legitimate companies and people, who have a license and abide by criteria defined by the Member States' authorities in charge of supervising private security operations. Also when the UAs operate in a swerm/group, it should be possible to identify the "friendly" and "unfriendly" UAs.

3.4.5. Authorization and oversight

CoESS would require clarification of this paragraph: do the limitations (visual line of sight, maximum altitude, distance from airport and sensitive zones) apply only to the open category? (cfr the text in the 3 coloured boxes)

3.5.4. Distance from uninvolved persons on the ground

CoESS would require clarification about the concept of "uninvolved". For example, would this include a person engaged in a criminal activity?

3.5.5. Separation from other airspace users

In proposal 14, last indent: who defines if the pilot has the adequate pilot competence?

3.5.6. Pilot competence

CoESS would require clarification about the "fit to fly" concept and who/what authority decides what it covers?

CoESS believes that the weather conditions should be mentioned: UAs cannot be operated in any type of weather and the risks are different according to weather conditions.

Finally CoESS highlights that the automatic limitations of performance can be changed/removed.

3.6. Specific Category

CoESS assumes that private security operations with drones will fall under this category. Below are a few examples of operations where drones could be used in support or instead of guards:

- Crowd management (also referred to as crowd control)
    - Event security
- Guarding in a variety of environments: general and Critical Infrastructure (ports, power plants, etc)
    - Drone support in static and mobile guarding as well as drone being used for more regular mobile guarding (e.g. around buildings)
    - Alarm response: drones could be sent instead of a patrol to make a first check
- Public order services
    - Traffic control could be done by drones
- Inspection of infrastructure (e.g. pipelines)
- Search and rescue, and assistance

3.6.1. Specific operation risk assessment (SORA)

Private security companies have acquired a long experience and high expertise in risk assessment and would therefore offer assistance in performing standard solutions, as a response to the call made in Proposal 20.

3.6.2. Standard scenarios and mitigation

CoESS draws EASA's attention to the fact that contrary to other users, private security companies have much experience in performing risk assessments, as highlighted in 3.6.1. above. Incidentally, it highlights the fact that "industrial inspections" (2nd indent) and "infrastructure inspections (power lines, railways, etc)" are not standard solutions. In view of the risks associated with inspection and infrastructure, and of the fact that private security companies have specific tasks in providing security, and for this reason require a license both for the company and the staff (which in addition go through a regulated and supervised selection and vetting process), this industry is particularly prepared and willing to give support and provide the "standard scenarios and mitigations". At any rate, the standard scenarios should not be carried out by companies or organisations, which are not duly licensed. Otherwise this would create a new threat.

3.6.4. OA – Operation Authorization

Given the specific type of activities performed by the private security companies, CoESS calls for a separate set of provisions:

- Which accelerate the process to get an OA, in view of the fact that private security performs missions of security on behalf of private and public customers who are in charge of critical infrastructure (finance, power, water supply, ports, airports, health, etc.)

- Whereby the same operation in 2 different locations and/or for 2 different clients are subject to a single OA, so that the in-depth analysis is performed only once. For example, in the case where a drone performs mobile guarding on a client property at regular intervals during office closing time, this should be subject to one OA, which would also cover the same operation at another building and/or for another client in similar condition.

Closing remarks

CoESS has put in place a UA Project Team in order to prepare the above comments. The Project Team brings together experts from different European countries, with a wide variety of skills and expertise, knowledge area and a high level of experience.

CoESS offers its assistance in the next few months/years, all along the decision-making process and beyond, with the objective to obtain the best possible, safest, most secure and cost-beneficial solutions for the development of drones, with the best interest of society in mind.

Brussels, April 2016

Catherine Piana
Director General