Confederation of European Security Services

# Position Paper

## on the EASA Notice of Proposed Amendment 2017-05 (A) and (B)

September 2017

As indicated in CoESS' previous publications[1], Unmanned Aircraft (UA) represents an interesting and useful addition to the range of technological means and equipment in use in private security services. The use of UA and are other unmanned vehicles is also consistent with the new paradigm in private security, the so-called "New Security Company"[2]. Here, security agents and technology are combined into "security solutions", in order to optimize services to clients and to provide enhanced security.

The Private Security Industry provides an increasing range of services to both private and public clients, including critical infrastructure protection.  CoESS therefore argues that private security, whilst being a commercial activity, serves a key purpose in protecting people and assets, and should therefore be treated differently from other types of commercial services using UAs.

The Private Security Industry sees opportunities in **three types of activities** with unmanned aircraft:

- **Supporting guards in their missions**, to enhance safety and efficiency, using both automatic and autonomous drones to carry out security missions either (preventive as well as for intervention/verification);
- **Tracking, tracing, monitoring and responding to alerts related to drones**, in the same way as the industry already tracks land vehicles, in coordination and cooperation with air control agencies;
- **Detecting and preventing the ill use of UA's**, whether unintentional, intentional or malicious, insofar as rules and regulations provide a legal basis for this type of response and the ensuing liability that may result of the latter.

[1] *"Position Paper on the EASA's Technical Opinion and Position Paper on EASA's Prototype Rule" and "The Use of UA in Private Security" March 2017 - pls see www.coess.eu Newsroom Section - Position Papers*

[2] *White Paper "The New Security Company" - pls see www.coess.eu - Newsroom section - White Papers*

The comments below are posted on the EASA on-line consultation website and are meant to support the creation of a safe, secure and efficient legislation for UAS in the EU.

General comments

Giving more attention to Security – NPA 2017-05 (B)

- As pointed out in previous CoESS publications, whilst EASA has a role in safety, the operation of UAs, especially in today’s context, require that more attention is given to security.
- Based on this principle, a number of comments on the proposed Commission Regulation address the need for Security Risk Assessments to be carried out, not just Safety Risk Assessments.
    - P. 55 of NPA 2017-05 (B) mentions that over 1,200 RPAS occurrences were reported for 2016 only, more than 100% increase compared to 2015). Even if they qualify as “incidents” (mid-air collisions mainly, but also loss of control and loss of data link), the likelihood of security incidents occurring needs to be taken into account. In manned aviation there have been minor security incidents reported recently, which should be considered as serious, as they can potentially be attempts in view of more significant breaches of security or attacks. There is no reason why UAS could not be used malevolently by people seeking to create damage. Attacks have already been carried out, for example by ISIS in the Middle East with explosives, and trials with chemicals (Sarin, Mustard Gas) have also been reported.
    - UAS can, have and will be used illegally for a number of purposes: transporting drugs, and other illegal products, transporting stolen goods, interfering with communication, spying and making pictures of Critical Infrastructure, carrying out reconnaissance missions, etc.
    - Critical Infrastructure, in particular, needs a high level of protection. This is also the case for high profile and official events (political, sports, and other), as well as specific human targets (politicians, etc).
    - The Oxford Research Group’s Remote Control Project has made a report on “Hostile Drones”(http://www.oxfordresearchgroup.org.uk/publications/briefing_papers_and_reports/remote_control_project_report_hostile_drones), which makes a number of recommendations, including legislative, in order for hostile drones to be prevented and detected and for active countermeasures to be developed and be made ready to use.
    - This is further corroborated by a report from CTC (Combating Terrorism Center), which indicates that at least 4 terrorist groups, mainly based in the Middle East, have programmes in place to use UAs for attacks and preparation of the latter.
    - As a preventative measure, CoESS argues that all UAs should be registered. In addition, we recommend to conduct a Security Risk Assessment in order to evaluate whether electronic identification and geofencing should be made mandatory for all categories. There is no possibility yet to know how in the future even very light UAs (or their parts) that qualify as toys could be used in a harmful way.
    - From both a hardware and software perspective, UAs should be made as safe as possible in order to reinforce preventative measures.

  - Whilst the current context points to possible terrorist attacks, other malevolent uses can and will be developed, such as surveillance, reconnaissance, filming illegal acts (e.g. for propaganda reasons), and any type of criminal operation.
  - At the very least, therefore, a full Security Risk Assessment should be carried out in the same way as it was done for Safety, so that mitigation measures can be designed.
  - Amongst the mitigation measures, commercial companies have been working on detection means, including acoustic-based alerts, blocking features through signal jamming, as well as active countermeasures when drones remain a threat after the control frequency and GPS have been blocked. These involve kinetic defence systems and laser defence.
  - The EU should support R&D for active countermeasure tools that can be used in populate and/or sensitive areas with as little as possible collateral damage.
  - Of course, terror or criminal groups may seek to provide themselves with anti-drone systems used by governments and law enforcement agencies, so that ultimately the best countermeasure is to address the root drivers of the threat in the first place.

- Certified category: the concept of complexity should be fully discussed within the Informal Drone Expert Group, so that a clear boundary can be established between the specific and certified categories, in such a way that corresponds to reality.

Comments on the Draft Commission Regulation (NPA 2017-05 (A))

Recitals 3 to 5

CoESS fully supports the proportionality and risk-based rules, and reiterates that the risk is not only a safety risk, but also a security risk. We therefore recommend that a Security Risk Assessment is performed before moving to the next decision-making step. As indicated above, publications and reports point to the current trials being made with drones as a means to transport explosive and dangerous chemicals, so that it is only a matter of time until these are used in Western countries.

3.1.1. Draft cover regulation - Article 2 – Definitions

(y) The role of Joint Authorities for Rulemaking on Unmanned Systems (JARUS) in establishing Specific Operations Risk Assessments (SORA) is unclear. Concretely, CoESS has been invited to become part of the Community of Interest (CoI) of JARUS, which involves 2 week-long meetings per year in remote places (the next one is in South Africa), and are chaired by a US-based consultant.

We do not support that SORA, by involving non-EU stakeholders, would be established outside of the EU scope. Also, we believe that the committee's work lacks transparency and impedes participation of SMEs and SMOs, because of the time and cost involved.

Furthermore, a future Security Risk Assessment should be established by authorities that have competence, knowledge and experience in Security, involving both the DG MOVE unit that has competence in Transport Security, and DG HOME.

3.1.1. Draft cover regulation - Article 3

Point 3 and 4: A Security Risk Assessment should be conducted to evaluate whether electronic identification and geofencing features should be mandatory for all UAS.

3.1.1. Draft cover regulation - Article 4: again, the word risk is only used in the context of safety and not security. A Security Risk Assessment should be conducted to confirm or not if this division and deriving obligations are still appropriate.

3.1.1. Draft cover regulation - Article 5: most security operators will be covered by this category and we assume that most of them will register for LUC.

As pointed out in previous publications (see footnotes on front page), security missions must be governed by national legislation regarding private security companies, and performed by fully licensed security staff, which have been specifically hired, vetted and trained for performing security missions in general, and with drones in particular.

3.1.1. Draft cover regulation - Article 7: where appropriate, for operations relating to sensitive elements, it should be ensured that staff performing those missions have been vetted, have a security license and are trained appropriately.

3.1.1. Draft cover regulation - Article 9: such exchange of information would also make sense for security incidents.

3.1.1. Draft cover regulation - Article 13: such exchange of information would also make sense for security measures.

3.1.1. Draft cover regulation - Article 15.4: the risk analysis should also look at possible security gaps as a result of creating a transitional period and the resulting obligations, for example e-identification and geofencing obligations.

Subpart A – OPEN CATEGORY

UAS.OPEN.20 Registration

CoESS believes that registration should be mandatory for all categories and sub-categories.

Subpart B – SPECIFIC CATEGORY

UAS.SPEC.40 Operational risk assessment

(a) CoESS published standard scenarios in the previous publication about the Prototype Rule. What is the process for these to be adopted?
As indicated above, CoESS applied to join the Community of Interest of JARUS, and found out that in order to join the meetings, the investment in time, human resources and money is quite significant. Hence the question: why are SORAs being adopted at a level that is not European, and why is the process not transparent and inclusive, and run by a US consultant?

Subpart C – LIGHT UAS OPERATOR CERTIFICATION (LUC)

UAS.LUC.30 Management System

As in other parts of the draft Regulation, reference is made to safety and not to security. A Security Risk Assessment should establish whether the provisions in the article are sufficient to anticipate and prevent security breaches.

In the same way, it needs to be examined whether the person in charge of safety management should not also be in charge of security. An increasing number of companies are integrating security to create "Safety and Security at Work" programmes, so this should be considered under the Security Risk Assessment. Security is increasingly being considered as an essential part of good governance, both to protect the company assets and also its staff against threats in general, including theft, espionage, sabotage, or other criminal acts motivated by any reason (anger, political, activism, terrorism, etc.)

Appendix I.2
Product requirement for UAS Class C1
(d) and (k) Is it practical to require electronic identification only when the UA is equipped with a camera? UAs and payloads can be bought separately, so that it may be safer and more secure to require electronic identification in all cases when the UA is purchased.

Annex II
Section 2 – Article II.5 Obligations of manufacturers

CoESS wonders where Security and Cybersecurity are addressed and how manufacturers and software developers can be encouraged to make hardware and software as robust as possible, so that it makes hacking and taking control of UAS as difficult as possible.

**Catherine PIANA**

**Director General**

*CoESS acts as the voice of the private security industry, covering 24 countries in Europe, of which 19 in the EU, representing around 2 million licensed guards, 45,000 companies and generating a turnover of €40M+.*

*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 centres, public hospitals, universities, etc.).*