

# **REPORT: High-Level International Conference**

## **on countering the threats posed by unmanned aircraft systems**

**17 October 2019**

EUROPEAN COMMISSION DIRECTORATE-GENERAL MIGRATION AND HOME AFFAIRS – DG HOME – and DIRECTORATE-GENERAL FOR MOBILITY AND TRANSPORT – DG MOVE – organized a high-level international conference on countering the UAS threat on 17 October 2019.

“The aim is to bring together different communities with varied but complementary experiences to exchange views and ideas on countering the drone threat. Besides the Member States and the relevant EU Institutions and Agencies, ...”

### **Welcome and opening remarks**

The conference was open by the Commissioner Dimitris Avramopoulos who underlined the opportunity and the challenges offered by new technologies and drones.

The European Commission supports technological innovations and the use of drones but also recognize that drones could be used with malicious intentions. To avoid or limit the effect of this misuse the Commissioner identifies a list of priorities that need to be implemented:

- track the trend of malicious use,
- support the project of Europol in registering European drone incidents,
- support training activities and support the founding action of H2020 in research and deployment on drone countermeasures, able to identify, track and intercept drones with malicious intentions.

He recognizes that countermeasures are very expensive.

A regulatory framework for security and safety operation is needed. U-Space is identified as the system that can ensure safety operation at Very Low Level. The security will be achieved through the cooperation between U-space and law enforcement authority. The aviation security is a very high priority for the global security agenda.

The Commissioner Violeta Bulc put emphasis on potential vs threats posed by drones, on stakeholder collaboration and on sustainability. The goal is to develop an Urban Air Mobility system. Through H2020, SESAR has already funded a U-space demonstration around Europe. All these activities bring more awareness and responsibilities, demonstrating the need to integrate Urban Air Mobility in Air Traffic Management system.

Commissioner Bulc and European Investment Bank announced the launch of a “European Drone Investment Advisory Platform” to support innovation and investment in drones.

Commissioner Bulc concluded underlining the importance of cooperation at the global level to support the drone market.

[https://ec.europa.eu/transport/sites/transport/files/drone\\_investment\\_advisory\\_platform\\_hand\\_out.pdf](https://ec.europa.eu/transport/sites/transport/files/drone_investment_advisory_platform_hand_out.pdf)

## **Panel discussion: Confronting the UAS challenge today and in 2050**

Mr. Arthur Holland Michel, Co-director, Center for the Study of the Drone (keynote)

Drones are difficult to identify and stop. The use of microwave radar is not effective as its range is very low (2-4km). It is not enough time to be prepared and act as drones are becoming faster. In the future it will be more difficult to identify malicious drones and stop them because as new technology is available it will be harder to shoot down drones.

Mr. Michael Schneider, Deputy Assistant Director, Federal Bureau of Investigation (FBI) (USA)

FBI has set a group of works on malicious use of drones. They found out that, most probably, small drones could be used for illegal activities. This group has presented his work to the Congress that empowers FBI to contrast threats and to increase the efficacy of countermeasure.

FBI finds that a collaboration with the Department of Justice the Department of transportation are crucial.

The Deputy Assistant Director reports that not only flying drones are taken in account but all new technology like 5G and radio controlled submarine.

Mr. Ulrik P. Ahnfeldt-Mollerup, Chief, Countering Terrorism Section, UN Office of Counter-Terrorism (UNOCT)

Drones are not used only in malicious way but also for peace operations, surveillance and to deliver vaccines. The United Nations is a forum where all Member States can discuss and share ideas about problem. Recently, Member States report an increasing worry about possible attacks from drones that are difficult to detect.

The only efficient way to better manage these threats is to share knowledges and capabilities.

Everybody knows that the regulation lags behind technologies.

The regulatory framework should include new technologies at global level. The academic world and institutions, together with industry, should collaborate to reach the goal.

United Nations offer their support to train all Member States on these activities.

Mr. Manfred A.W. Mohr, Assistant Director, International Air Transport Association (IATA)

The “We are One in the Sky” campaign signed by ETF (European Transport Workers’ Federation) was presented by the IATA Assistant Director Manfred Mohr. He underlined how collaboration, coordination and cooperation between all the organizations, that signed the campaign, has been crucial.

Then he focused the discussion on the need of standardization of drone countermeasures; EUROCAE is working on this. He underlined the lack of funding for the integration of drones in an already secure system. He recalled one of the points of the “We are One in the Sky” paper which states that many airspace infringements could be avoided by rising users’ awareness through information campaigns.

During the “Question time” it was remarked that ‘remote identification’ or well-known e-identification is a must.

There is a strong need, at global level, to standardize countermeasures for drones.

Nowadays, there is a gap between what experts know about cybersecurity and technology and what is implemented at policy level.

An iterative approach could be effective in implementing appropriate practices.

There is no framework of legal rules in EU that provide integration, instead of separation, of drones.

## **Panel discussion: Bringing communities together**

### Mr. Jerome Morandiere, Airport Council International (ACI) Europe (keynote)

The procedures adopted by airports are not sufficient to prevent drones attack and it should be considered that the security risk cannot be eliminated.

He presented several technologies, some already in place, others only tested, that can detect and identify drones nearby airports.

### Ms. Elizabeth Neumann, Assistant Secretary for Threat Prevention and Security Policy, Department of Homeland Security (USA)

Collaboration between Border Patrol, Secret Service, Coast Guard and FBI is fundamental especially during big events, sport events or special operations.

The USA Department of Justice defined a roadmap assigning competence to each agency involved.

Also, the collaboration with UN (United Nations) was crucial and allow the Department of Homeland Security to coordinate all actions with the Coast Guard.

### Mr. Franck Desit, Deputy Director for Capability, Armament and Planning, European Defence Agency (EDA)

Detection, tracking and identification are needed in order to implement algorithm and to educate who has to use these countermeasures.

C-UAS are on roadmap, and are able to provide a minimum level of protection also against mini UAV

### Ms. Frank Piana, Director-General, CoESS

They represent 2.000.000 private guard in Europe.

The CoESS delegate underlined the necessity to have a plan B and a clear vision of which responsibility has each actor in the process putted in place to avoid drones attack.

Technological competence and person properly trained are the core of the process.

### Mr. Fredrik Wilhelmsson, Swedish Prison and Probation Service

Prisons have lot of electronic intrusion system but what has been forgotten is the threat coming from the sky, helicopters and drones.

Even if nets can be put over prisons, there is an ethical problem to solve: the prisoner has to see the sky.

Drones could bring inside prisons cigarettes, information, drugs and weapons. When drones will be able to lift a person they can be used to escape.

Radar system installed in some prisons are now able to detect drones, distinguishing drones from birds (not small drones).

He welcomes cooperation with other critical infrastructure, even because this countermeasure systems are expensive.

Mr. Javier Quesada, European Border and Coast Guard Agency

Technologies and regulation should be aligned.

Low flying object can transport goods across the border.

Industry and academia should work together.

### **Parallel panel discussion: Public-private engagement in threat mitigation**

Mr. Charles Telitsine, Groupe ADP

During the research projects followed by ADP, they asked to ATC at which distance they would like to detect a drone. The answer was 18 km. But current technology allows to detect drones only at 2-4 km from the airport. A multisensory system was deployed in different French airports.

Police was more interested to find the pilot than to find the drone.

To allow all different users coming from air force, police, and airport personnel to interact and take decisions on a malicious drone identification process it has been developed a very user friendly interface.

Drones are a good business for airports, because they would be able, in the future, to deliver goods and passenger. So, they decided to invest in "SkyPort" and a new terminal for VTOL aircraft was already deployed.

Mr. Christoph Raab, Drone Alliance Europe (DAE)

Drones are new technology like internet, 5G and AI.

How can we secure critical infrastructure?

A layered system with more human resources can be scalable when you have more information.

Mr. Victor Vuillard, Parrot

Drones are a huge opportunity, but there is a need to balance countermeasures and legitimate drones to ensure continuity of business.

Better regulation should prevent human mistakes.

Mr. Munish Khurana, Senior Manager – Business Development, Eurocontrol

Eurocontrol held a workshop on countermeasure with all the major organization in Europe (IATA, CANSO, EDA, AIC).

A campaign on using AI in aviation is open (See Term of Reference).

Mr. Vassilis Agouridas, UAM Initiative Leader, European Innovation Partnership on Smart Cities and Communities (EIP-SCC)

Implementation of Urban Air Mobility influences Smart Cities and communities. There is a need for urban plan to cope with emerging technology. Developing Smart Cities requires different sectorial knowledge. UAM required the digitalization of the traffic data and the creation of new business models, new services and new mind-set.

A collective action is needed. Human actions are effective when there is an active involvement of citizens and when there is social embracement.

Some major cities think that the sky above is an extension of the public space and they want to manage it. There is a need to work on it.

### **Parallel panel discussion: Current/future research and testing needs**

Mr. Andre Hentz, Acting Deputy Under Secretary, Department of Homeland Security (USA) (keynote)

Nowadays, we don't understand the business case. There is a need to develop standards, indeed a set of standard capabilities. To develop standards, we should share information and test results.

We should keep humans in the loop.

Mr. Denis Koehl, Senior Advisor, European Aviation Safety Agency (EASA)

First question with no answer is: who pays for this?

Manage Police helicopters and drones in the same airport is not easy. The challenge is the commitment in different situations where police helicopters and pizza delivery (for instance) are flying together in a certain volume of airspace. Which sensor do we need to use to integrate existing systems?

We need to share data from different sensors for the best decision making process.

Mr. Peter Hotham, Deputy Executive Director, SESAR JU

SESAR has already founded U-space demonstrator researches where air taxi and goods delivery were integrated and interfaced with ATM.

The lessons learned are:

1. Collaboration, cooperation and sharing information are fundamental.
2. U-space needs a clear regulation. Technology is moving faster than regulation.

3. Demonstrated technology, able to detect drones, should be deployed.

EUROCAE is setting a working group on security and industry partners are welcome.

Mr. Maurizio Gemma, Elettronica Group

Elettronica Group, 4 years ago in France, identified an urgent request of countermeasure technologies. They did a lot of reverse engineering to get and understand all command and control working stations in order to generate and jam selected frequency able to interfere with remote piloted drones.

A lot of people are ready to buy this technology even if it is not ready yet. It's a multi-domain sensor data fusion problem.

Elettronica Group develop multisensory solution where radar, direction finder and artificial intelligence are integrated.

The major aim was to understand if the object detected is a drone or not.

In the future, we need to test if GPS spoofing in airport is possible.

Mr. Jaanus Tamm, Chairman, Marduk Technologies

He thinks that GPS spoofing is not useful if the drone has an off-line map and is able to fly with visual references.

They develop a low power laser able to burn some elements of the malicious drone. Jamming doesn't work and also radar is not effective because when they detect the drone it's too late and it is too close to the critical infrastructure.

There is a need to test and to set use cases.

Criminal technologies run faster than law enforcement countermeasure.

## **Closing remarks**

*Commissioner Sir Julian King*

We need to prevent misuse of technology like drones, 5G and artificial intelligence.

Possible target should be prepared and properly protected from misuses of drones. There will be zero tolerance for transgressors. There is a need to reinforce drone forensics procedures.

International partner, public academic, industry and organization are called to work together on the following issues.

1. There is a need to work with responsible authority for setting rules and technical requirement considering that the airspace is shared with manned aircraft. Critical infrastructure should be detected. UTM services should be provided to control safely and secured all the unmanned traffic.
2. There is a need to act against no compliant use of drones. Countermeasures should be deployed. Countermeasures manufactures should share idea with police. It is well known that countermeasures are expensive, require a lot of human resources and need training.
3. New regulation oblige manufacturer to adopt technical requirements.
4. A common drone culture is needed. We should work with users to educate to be responsible and to inform that they may be sanctioned.
5. Exchange good practice, experience, technology and legal view it's fundamental.

6. The huge potential of drones is recognized.
7. There are huge challenges for law enforcement authority.
8. We need to monitor and evaluate, being proactive, thinking ahead even if we have some mandate to act but it is incomplete.

Reference:

<https://audiovisual.ec.europa.eu/en/video/l-179311?lg=OR&sublg=undefined>

Brussels, 17 October 2019

ETF Delegate  
Cristian Nativi