

Critical Airport Infrastructures: Cyber-attacks & Counter-Drone Technologies

8th
Information Security
conference

February 2021
Athens, Greece

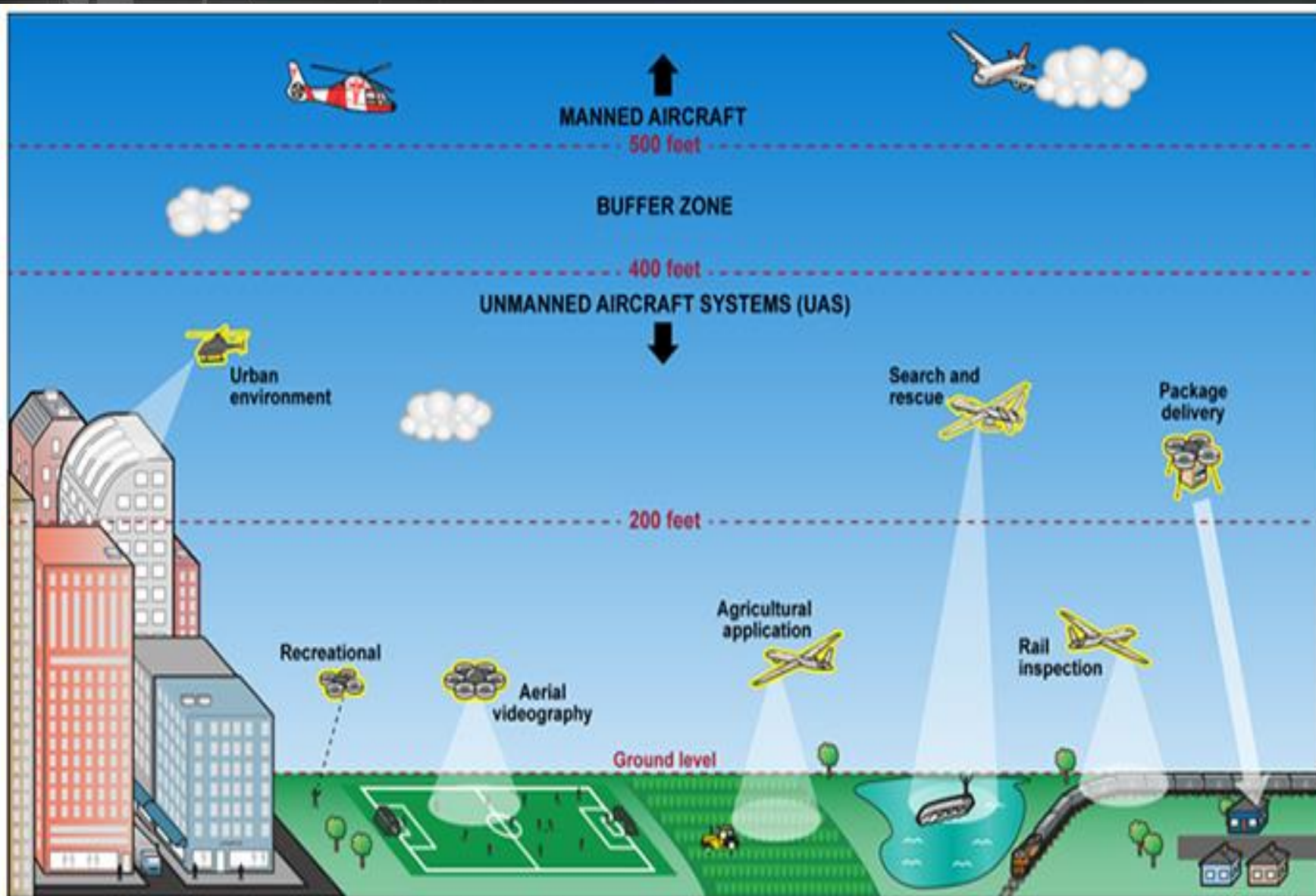


Georgia Lykou

**Hellenic Civil Aviation Authority &
Athens University of Economics & Business**



Unmanned Aircraft Systems and their intrusion into our daily activities (UAS/UAV/RPAS/Drones)



Rules and guidance for drone operation

New EU-wide rules for drones from 2021

The new EU rules ensure that the following are respected:



safety



privacy

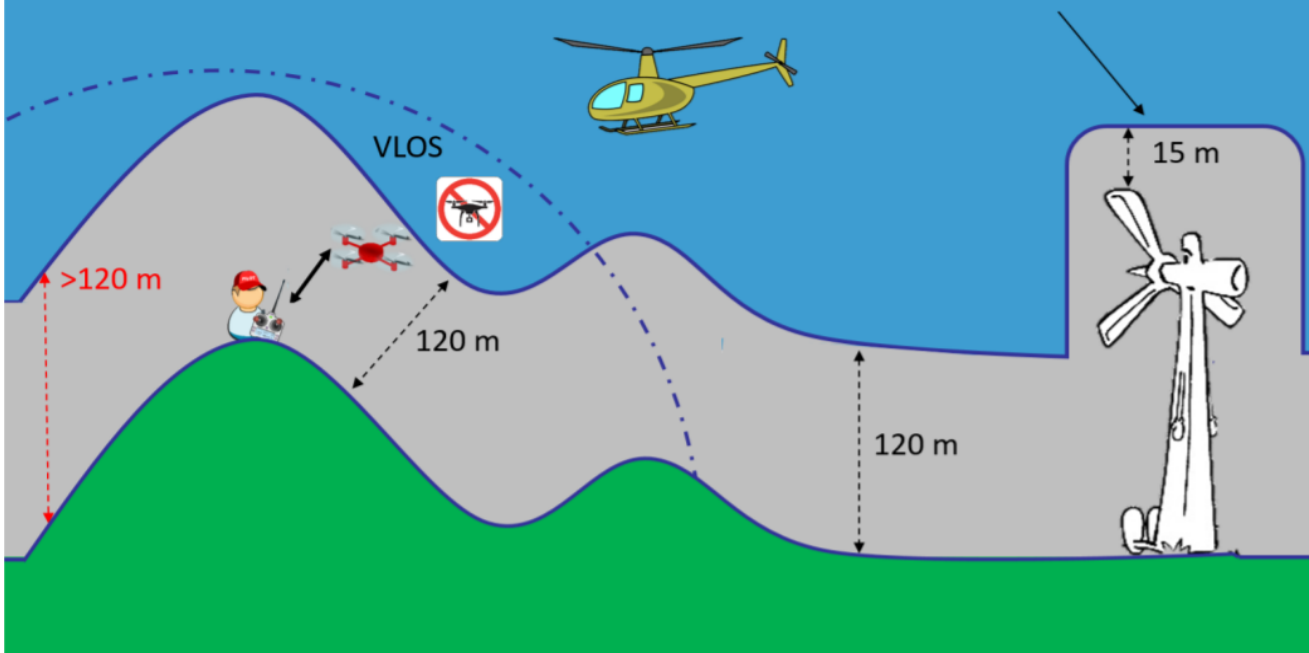


data protection



environment

Upon request of the owner of the artificial obstacle



EASA
European Union Aviation Safety Agency



How vital is a UAS risk?

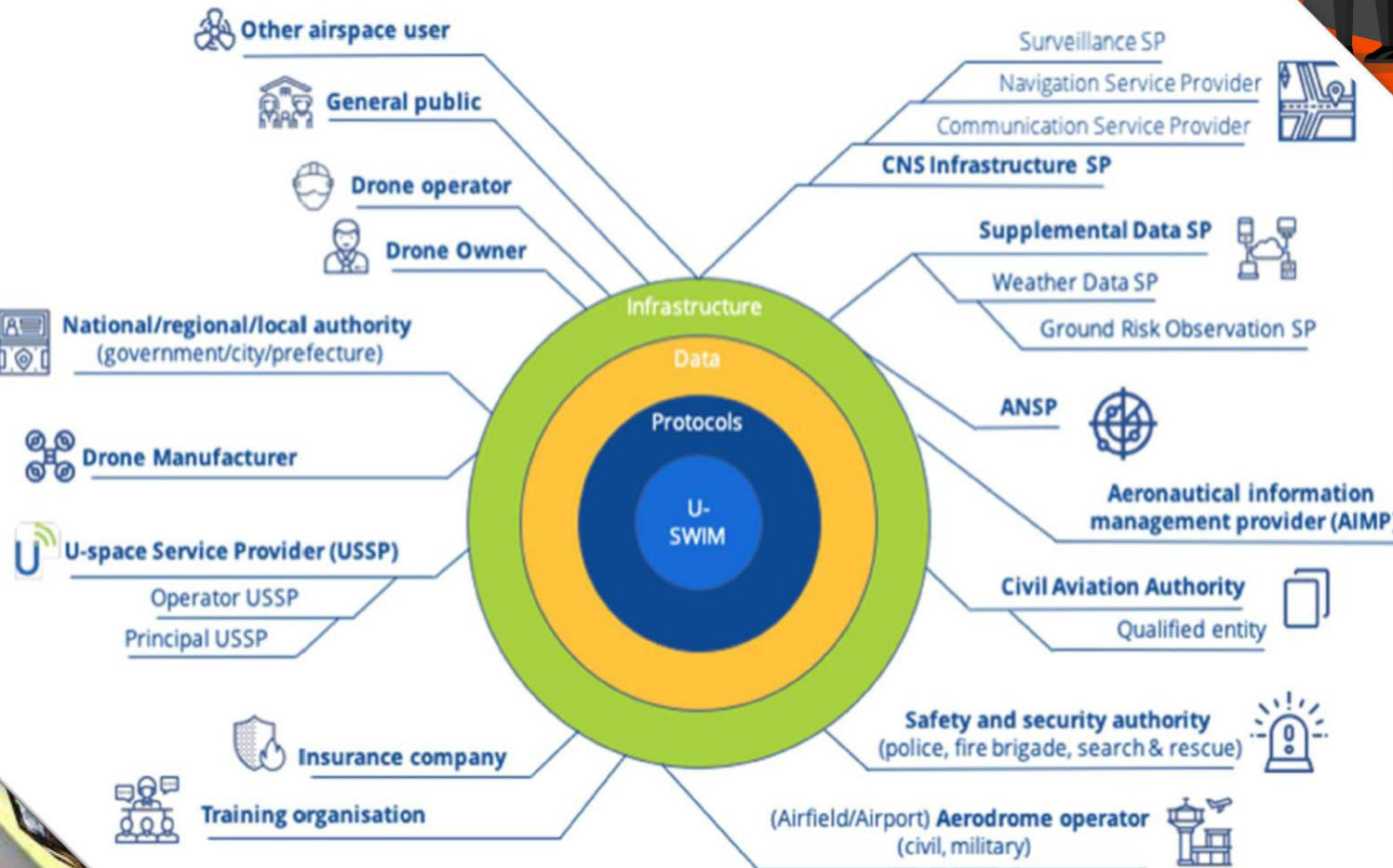
The U-Space Environment

The top three issues of concern about commercial drones among the public:




41%
risk of improper use

27%
risk of use by criminals

26%
risk of accident



Reconciling 3 different roles

- Regulation 
- Industry / technology 
- Attackers 

Categorizing UAS: Related Cyber-threats

DHS/ally UAS

- Disabling adversary networks through local interference
- Harvesting adversary credentialing information
- Data collection and probing

- Spoofing of law enforcement UAS to misrepresent location information or collected probe data
- Take-down, lock-out, or takeover of law enforcement UAS
- Theft of UAS identity, network, or collected probe data

Adversarial and other UAS

- Botnet-style stealth network infection enabled by mobile UAS and poorly protected personal WiFi networks
- Cascading infection of Internet of Things (e.g., home appliances, lightbulbs, car-charging stations) spread through mobile UAS

- Distorting or destroying collected probe data
- Take-down, lock-out, or takeover of adversarial UAS

UAS as cyber weapons

UAS as cyberattack targets

Communication attack on ATM systems

Attack Scenario to Airport facilities

Day 1

Step 1: UAV inspects and records CIs location and vulnerabilities (*Navigational Aids, Com-transceivers or Radar*)



RSR/MSSR
Radar



Com Transceiver

Air Traffic Management
Unmanned Stations

Day X

Step 2: UAV attacks CI by:

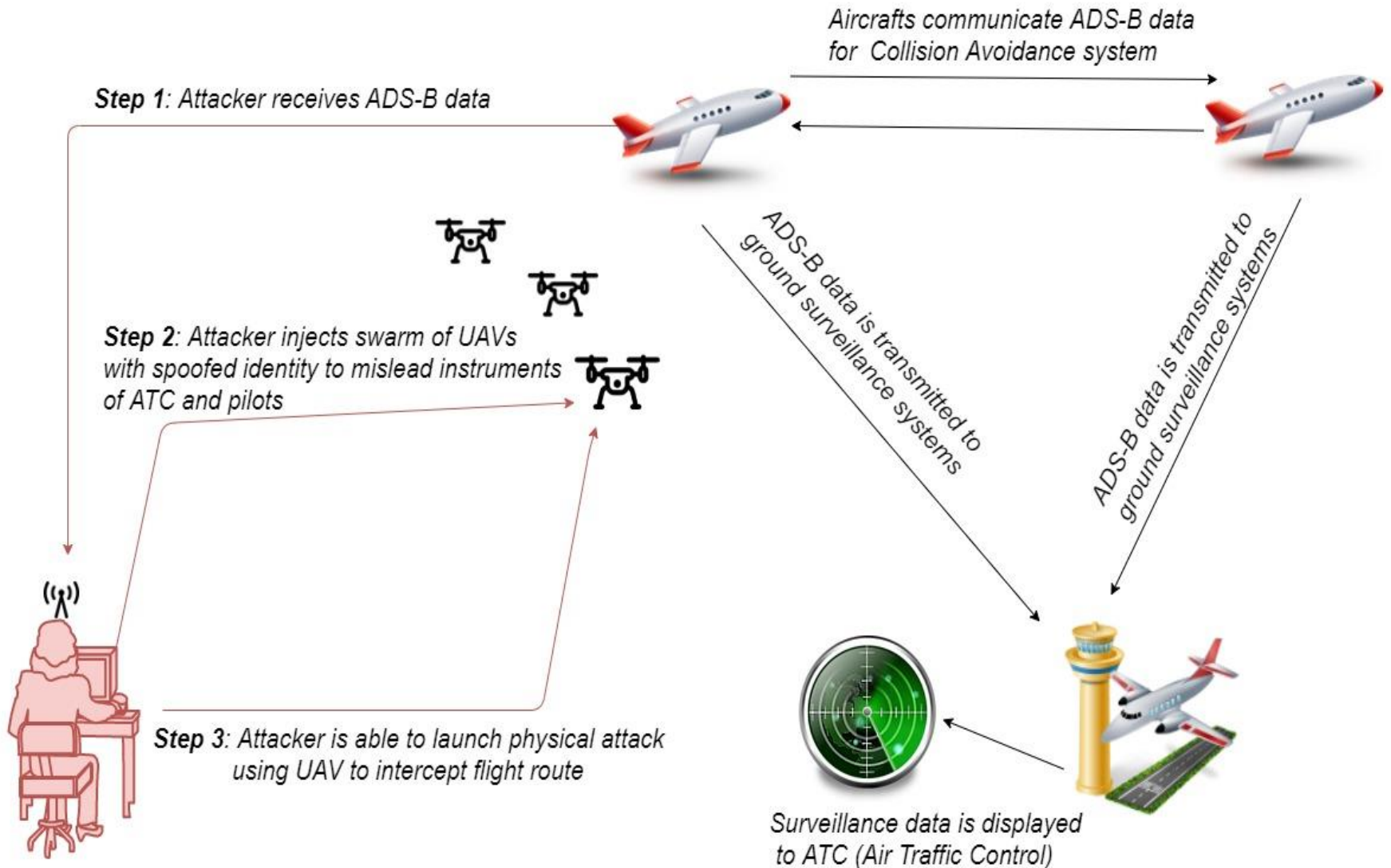
- 1) Carrying explosive payload
- 2) Emitting interference signal



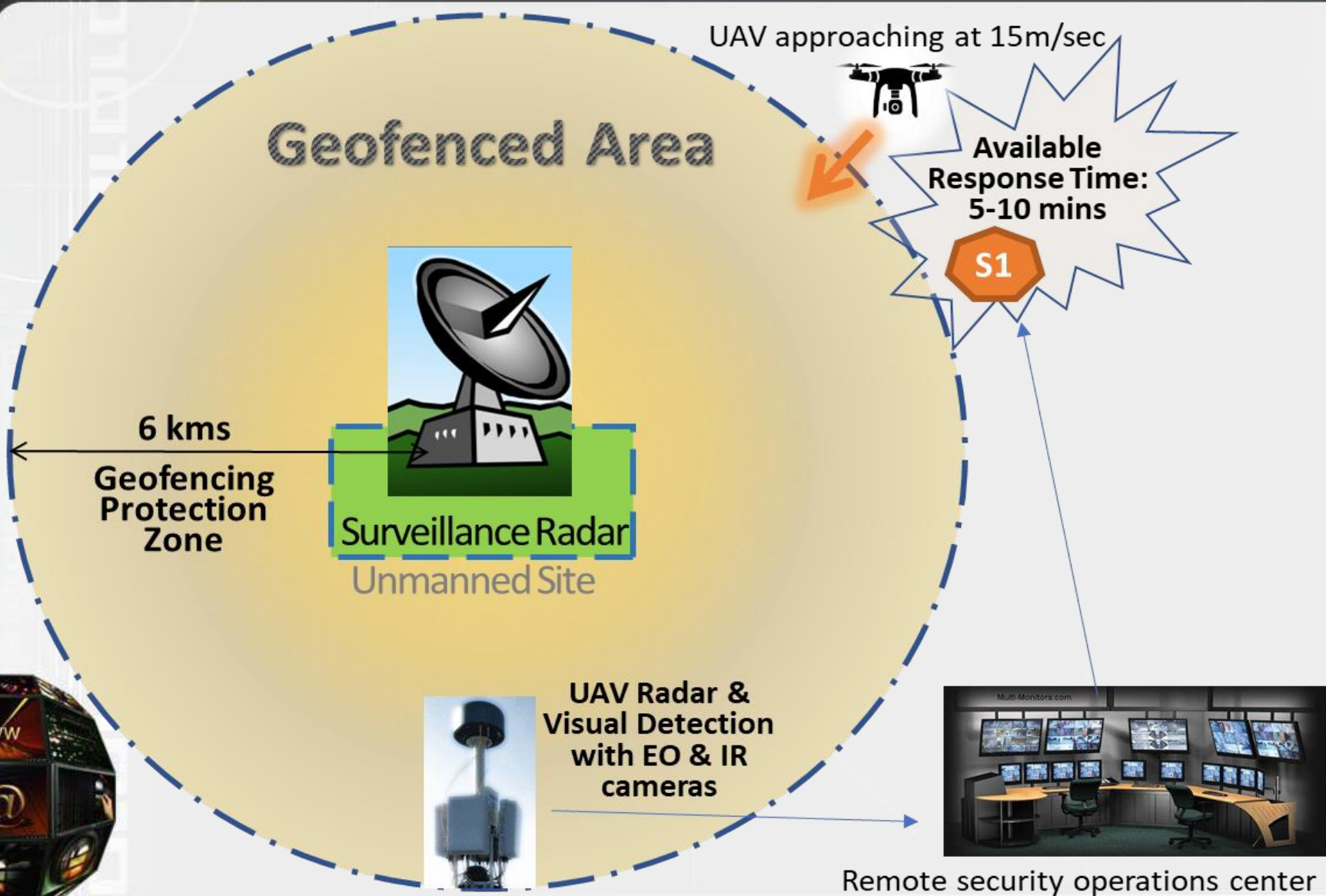
Air Traffic Management
Unmanned Station

Communication attack on ATM systems

Attack Scenario to Airport facilities

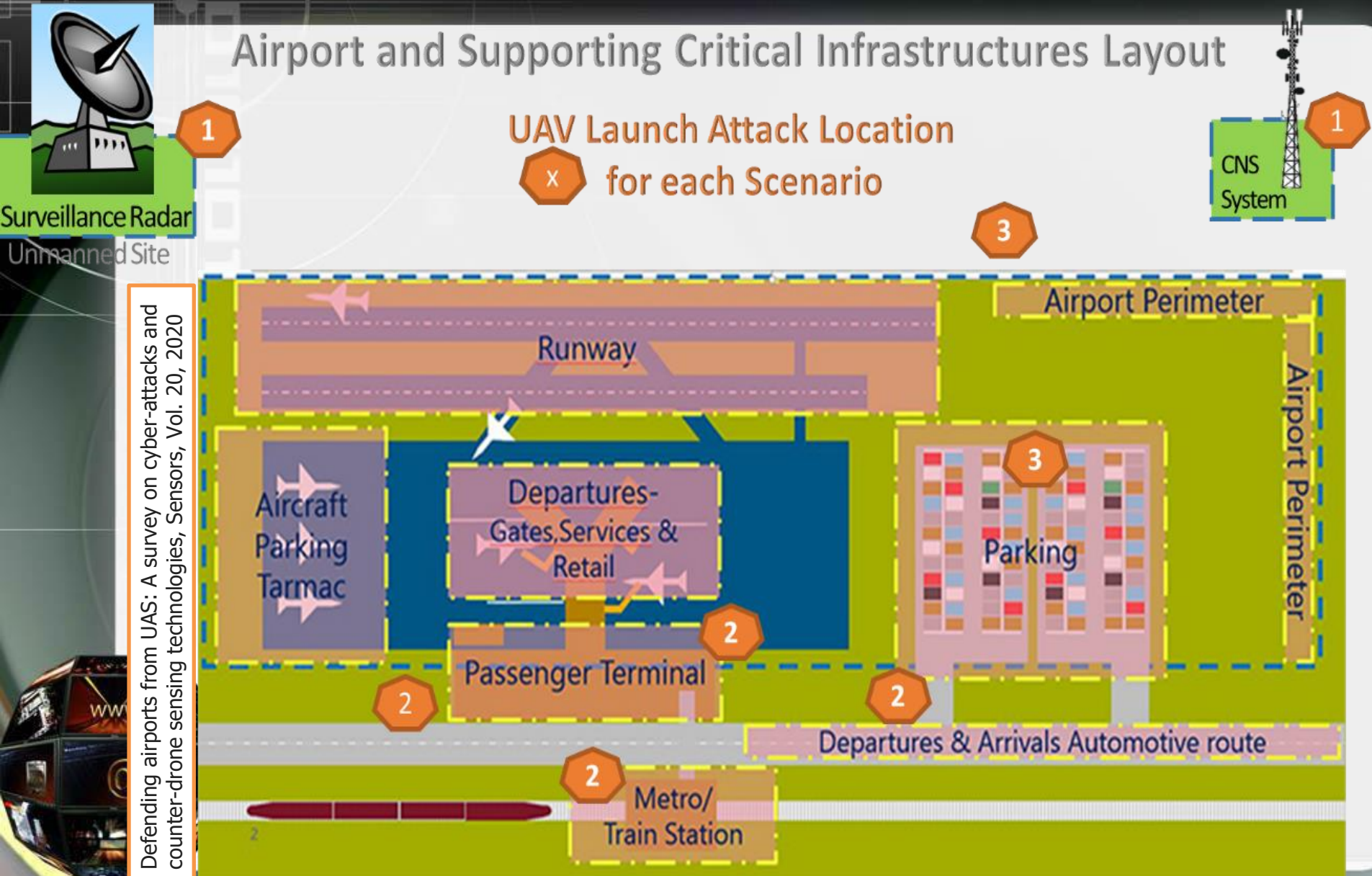


How to protect ATM & Airport facilities?



How to protect ATM & Airport facilities?

Airport and Supporting Critical Infrastructures Layout

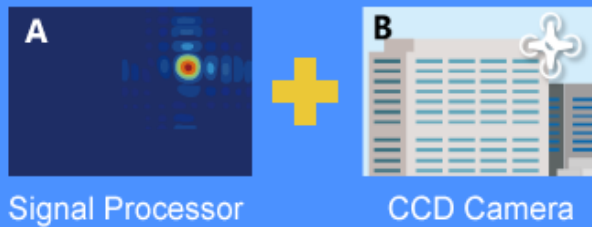


C-UAS Technologies

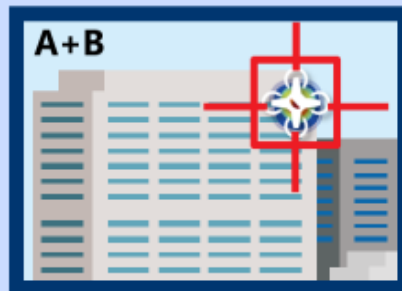
Receive a signal at the antenna



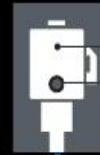
Combine signal position with video image



Visualize the drone signal in the video image



Sensor



Antenna
Video Camera
Fiber Optic Cable etc.

Monitoring Control Terminal



Detected image

Drone arrival direction

Detecting range

A screenshot of the monitoring control terminal interface. It features a grid of video feeds on the left, a map on the right showing a red line for 'Drone arrival direction' and a green dashed circle for 'Detecting range'. Below the map is a data table with columns for 'Time', 'Altitude', 'Speed', 'Direction', and 'Status'. On the far right, there are control buttons for 'Trunkle', 'Work', 'Merge', 'SEARCH', 'BUZZ ON', and 'BUZZ OFF'. A red crosshair on the top-left video feed is labeled 'Detected image'. A blue dot on the map is labeled 'Installation position'.

Drone arrival direction map display

Lights up when drone is detected

Search mode select (Manual/Auto)

Buzzer ON / OFF

Installation position

Video Display

(Able to display a maximum of 6 images from each sensor)

History event display / Spectrum display

Countering rogue drones



COUNTER-DRONE WORKFLOW AND SOLUTIONS

Detect, Track & Identify



React



Interdict



Sensors:



Acoustic



Visual/EO



Thermal



Radio Frequency (HF, VHF, UHF)



Radar

Non-interactive¹ Response:



Drone Alarms



Close Window Blinds



Shut Down Wi-Fi



Evacuate an Area



Deploy a Fog Grenade



Blind the Drone Camera

Kinetic Solutions:



Laser



Projectiles



Net

Non-Kinetic Solutions:



RF/GNSS Jamming



RF/GNSS Spoofing

¹ Threat responses which do not interact with the drone in any way but can actively or passively mitigate the threat it poses
source: DRONEII.com

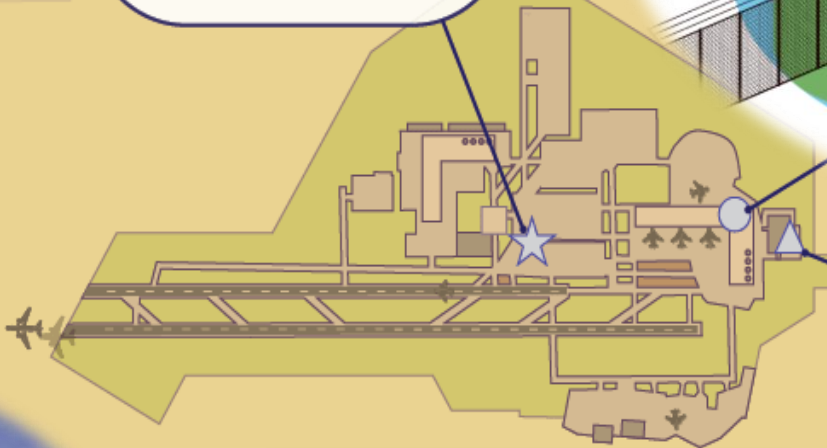
Counter-Drone Systems & Airport's applicability



FORTEM SKYDOME™

- Comprehensive Coverage
- Powerful, Easy Management
- Safe Mitigation Options

Careless, Clueless, Criminal or Terrorist Drone Disrupting Airport Activity



Epilogue: Aiming to Cyber-Resilient Aviation

Comprehensive, unified responses with the world's top-class combination of physical security and cyber security

Cyber-physical security

Integrated and unified response when cyber and physical security measures are combined
(Development/Activities of automatic monitoring technologies)

Shortage of personnel
Deeper analysis needs

Shortage of personnel
Monitoring simulation needs

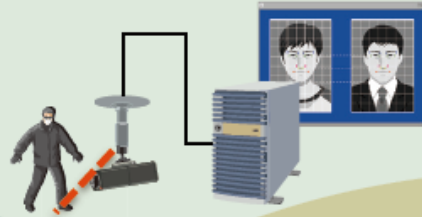
Information sharing

Cyber monitoring
(networks, servers, etc.)

Physical monitoring
(guarding & crime prevention)

Cyber security

Physical security



References

1. ENISA, *Securing Smart Airports*, <https://www.enisa.europa.eu/publications/securing-smart-airports>
2. FAA Aerospace Forecasts. Unmanned Aircraft Systems, https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/unmanned_aircraft_systems.pdf
3. Faily, S., Lykou, G., Partridge, A., Gritzalis, D., Mylonas, A., Katos, V., "Human-Centered Specification Exemplars for Critical Infrastructure Environments", in *30th British Human-Computer Interaction Conference*, UK, 2016.
4. Iliadis, J., Gritzalis, D., Spinellis, D., Preneel, B., Katsikas, S., "Evaluating certificate status information mechanisms", *Proc. of the 7th ACM Computer and Communications Security Conference*, pp. 1-9, ACM Press, 2000.
5. Lykou, G., Moustakas, D., Gritzalis, D., "Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies", *Sensors*, Vol. 20, No. 12, 2020.
6. Lykou, G., Iakovakis, G., Gritzalis, D., "Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management", in *Critical Infrastructure Security and Resilience*, Gritzalis, D., et al. (Eds.), pp. 245-260, Springer, 2019.
7. Lykou, G., Anagnostopoulou, A., Gritzalis, D., "Smart Airports Cybersecurity: Threat Mitigation and Cyber Resilience", *Sensors*, 2019 .
8. Lykou, G., Anagnostopoulou, A., Gritzalis, D., "Implementing Cyber-Security Measures in Airports to Improve Cyber-Resilience", *Proc. of the IEEE Global Internet of Things Summit*, pp. 305-310, Spain, 2018.
9. Lykou, G., Dedousis, P., Stergiopoulos, G., Gritzalis, D., "Assessing Interdependencies and Congestion Delays in the Aviation Network", *IEEE Access*, Vol. 8, pp. 223234-54, 2020.
10. Lykou, G., Anagnostopoulou, A., Stergiopoulos, G., Gritzalis, D., "Cybersecurity self-assessment tools: Evaluating the importance of securing industrial control systems in Critical Infrastructures", in *Proc. of the 13th International Conference on Critical Information Infrastructures Security*, pp. 129-142, Springer, 2018.
11. Stergiopoulos, G., Vasilellis, E., Lykou, G., Kotzanikolaou, P., Gritzalis, D., "Critical Infrastructure Protection tools: Classification and comparison", *Proc. of the International Conference on Critical Infrastructure Protection*, Springer, USA, 2016.
12. Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M., Lykou, G., Gritzalis, D., "Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures", *International J. of Critical Infrastructure Protection*, Vol. 12, pp. 46-60, 2016.
13. Theoharidou, M., Kandias, M., Gritzalis, D., "Securing transportation-critical infrastructures: Trends and perspectives", *Proc. of the 7th IEEE Conference on Global Security, Safety and Sustainability*, pp. 171-178, Springer, 2012.