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

8th
Information Security conference

February 2021
Athens, Greece

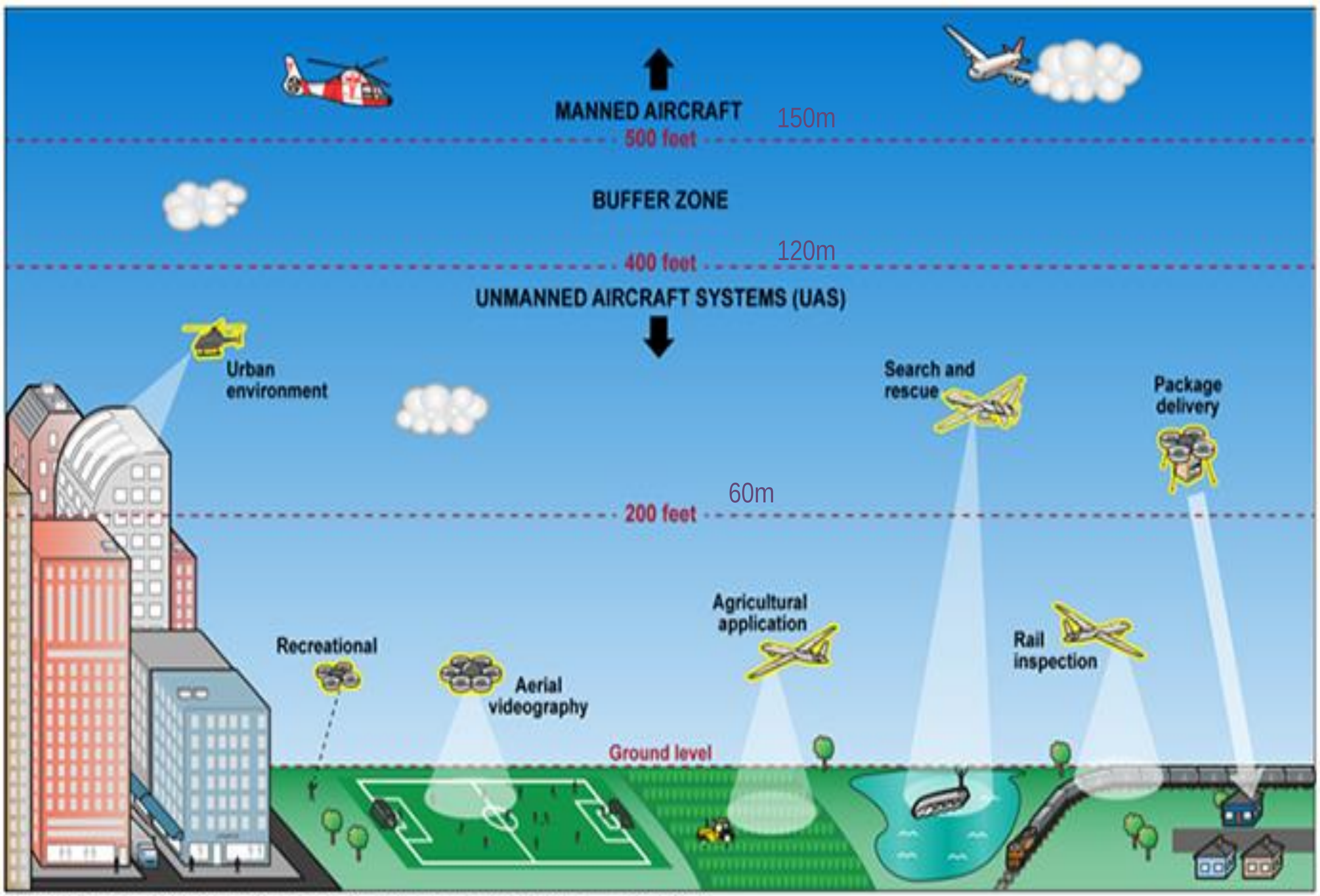
Georgia Lykou

Hellenic Civil Aviation Authority &
Athens University of Economics & Business

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

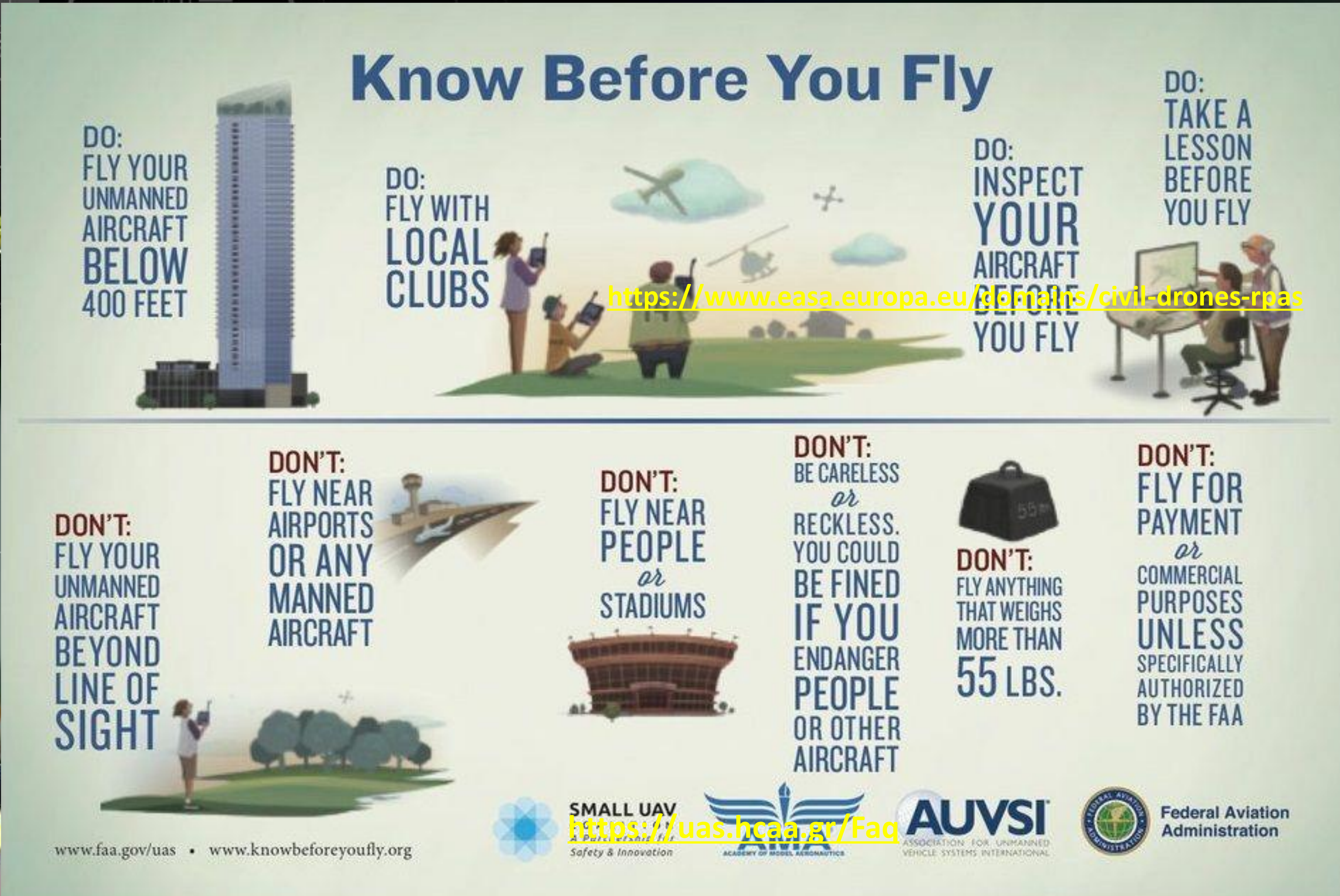
UAV: Unmanned Aircraft Vehicles

RPAS : REMOTE PILOT AIRCRAFT SYSTEMS



Source: GAO illustration of National Aeronautics and Space Administration (NASA) information. | GAO-18-110

Rules and guidance for drone operation



Know Before You Fly

DO:
FLY YOUR UNMANNED AIRCRAFT BELOW 400 FEET

DO:
FLY WITH LOCAL CLUBS

DO:
INSPECT YOUR AIRCRAFT BEFORE YOU FLY

DO:
TAKE A LESSON BEFORE YOU FLY

https://www.easa.europa.eu/domains/civil-drones-rpas

DON'T:
FLY YOUR UNMANNED AIRCRAFT BEYOND LINE OF SIGHT

DON'T:
FLY NEAR AIRPORTS OR ANY MANNED AIRCRAFT

DON'T:
FLY NEAR PEOPLE *or* STADIUMS

DON'T:
BE CARELESS *or* RECKLESS. YOU COULD BE FINED IF YOU ENDANGER PEOPLE OR OTHER AIRCRAFT

DON'T:
FLY ANYTHING THAT WEIGHS MORE THAN 55 LBS.

DON'T:
FLY FOR PAYMENT *or* COMMERCIAL PURPOSES UNLESS SPECIFICALLY AUTHORIZED BY THE FAA

www.faa.gov/uas • www.knowbeforeyoufly.org

SMALL UAV
Safety & Innovation

AMA ACADEMY OF MODEL AERONAUTICS

AUVSI ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL

Federal Aviation Administration

https://uas.hcaa.gr/Faq

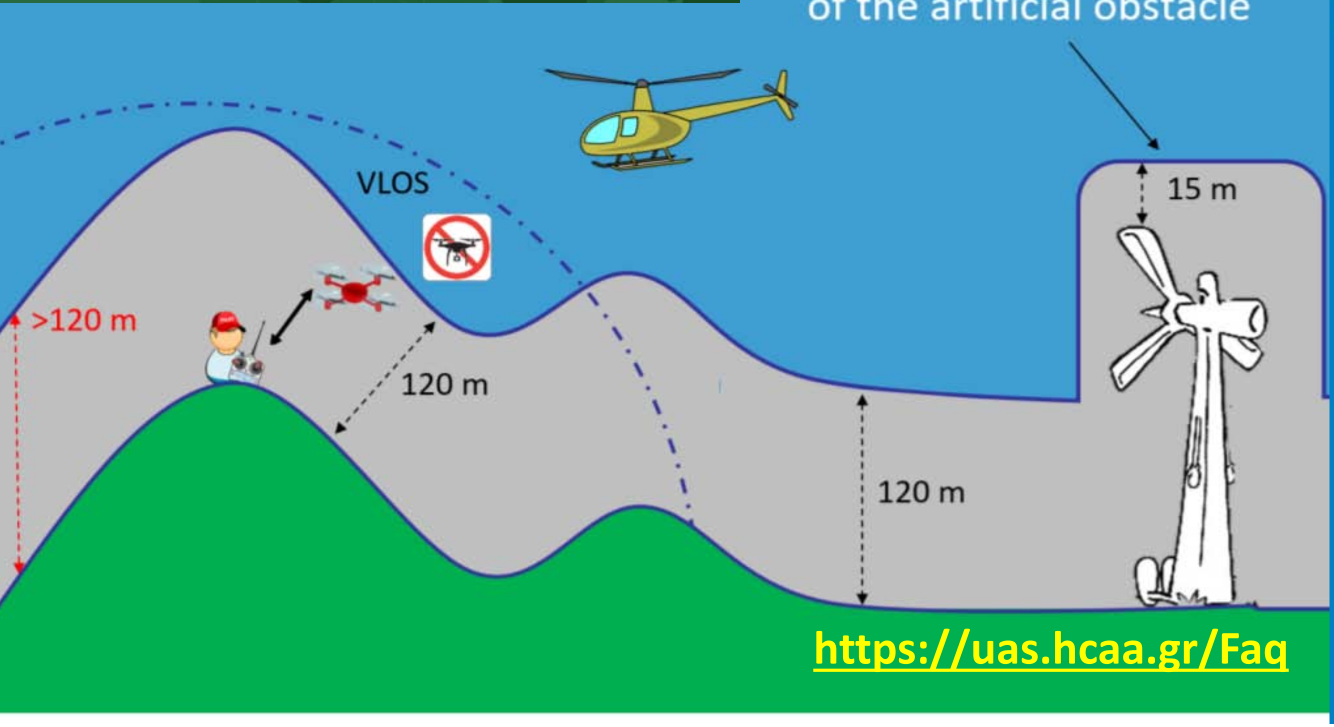
Rules and guidance for drone operation

New EU-wide rules for drones from 2021

The new EU rules ensure that the following are respected:

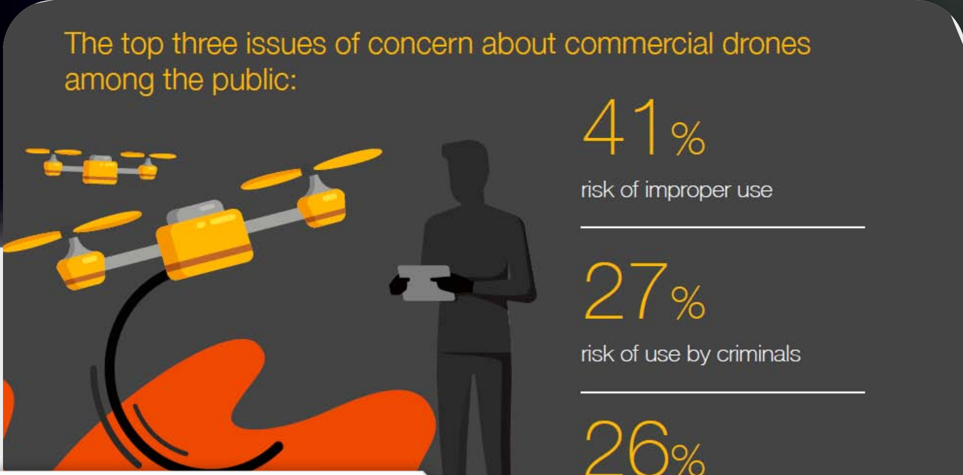
- safety
- privacy
- data protection
- environment

https://www.easa.europa.eu/domains/civil-drones-rpas



https://uas.hcaa.gr/Faq

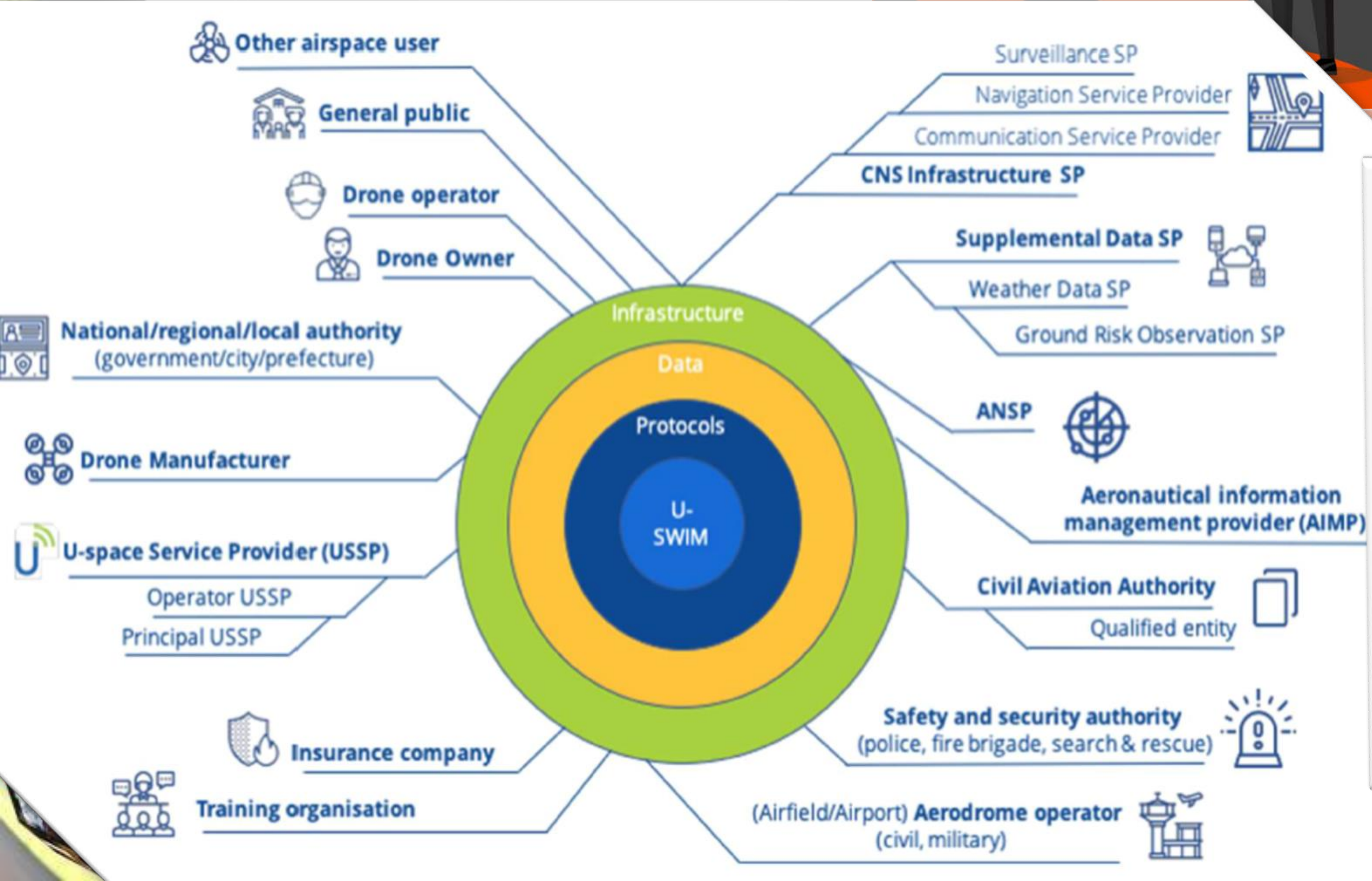
How vital is a UAS risk?

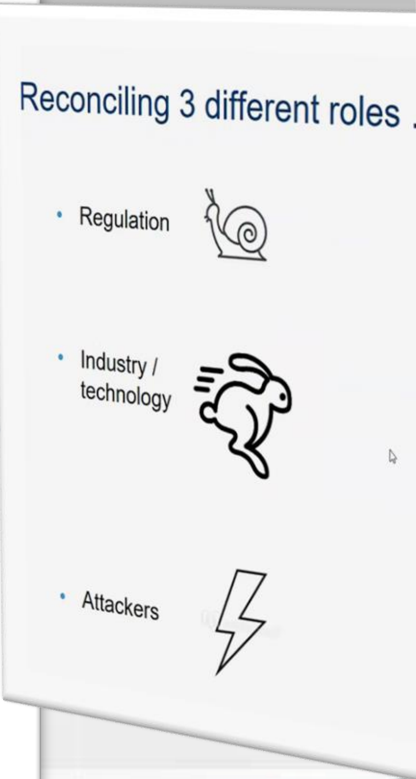


The top three issues of concern about commercial drones among the public:

41%	risk of improper use
27%	risk of use by criminals
26%	risk of accident

The U-Space Environment


Other airspace user
General public
Drone operator
Drone Owner
National/regional/local authority (government/city/prefecture)
Drone Manufacturer
U-space Service Provider (USSP)
Operator USSP
Principal USSP
Insurance company
Training organisation
Surveillance SP
Navigation Service Provider
Communication Service Provider
CNS Infrastructure SP
Supplemental Data SP
Weather Data SP
Ground Risk Observation SP
ANSP
Aeronautical information management provider (AIMP)
Civil Aviation Authority
Qualified entity
Safety and security authority (police, fire brigade, search & rescue)
(Airfield/Airport) Aerodrome operator (civil, military)
Infrastructure
Data
Protocols
U-SWIM



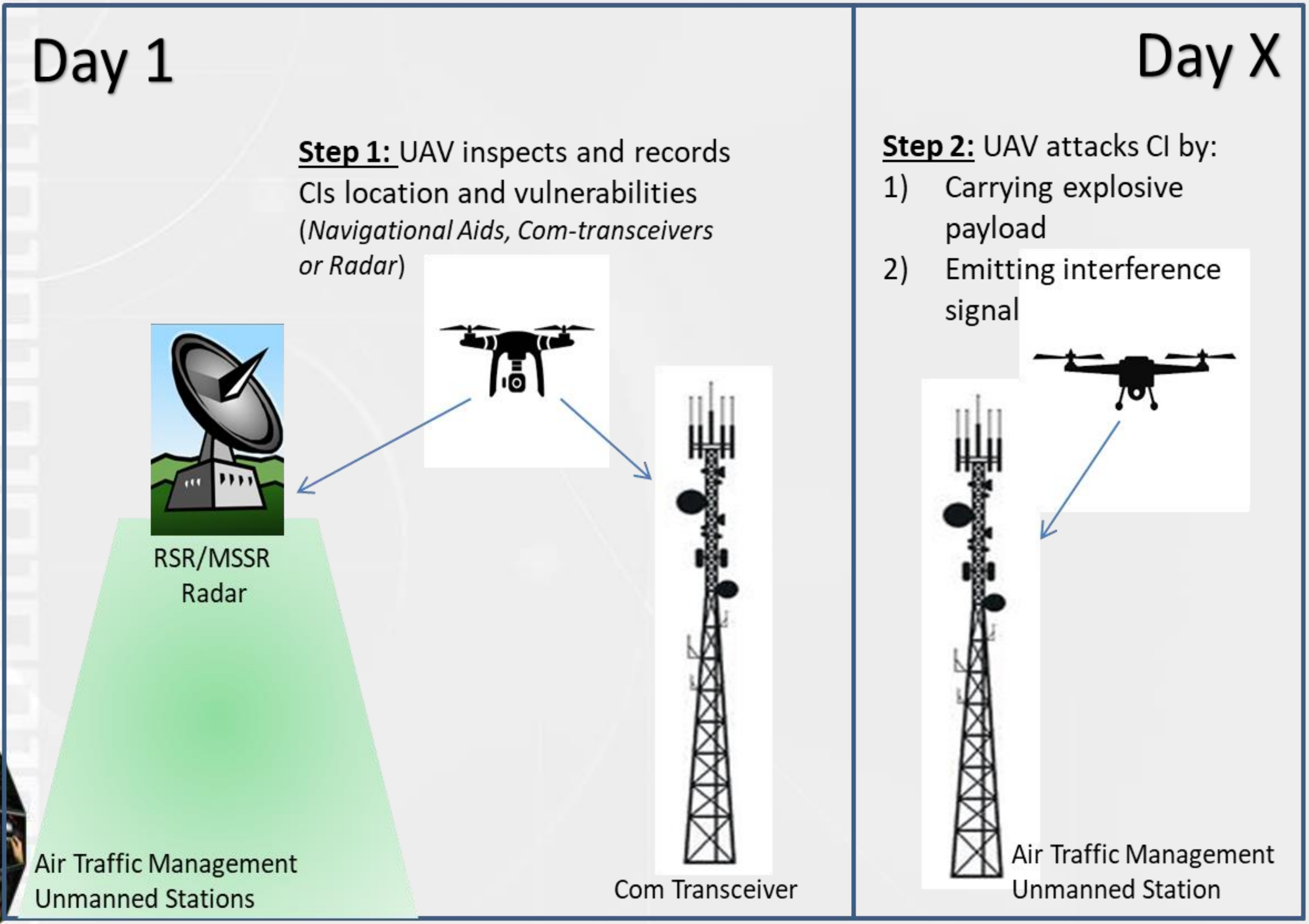
Reconciling 3 different roles

- Regulation
- Industry / technology
- Attackers

Categorizing UAS: Related Cyber-threats

	UAS as cyber weapons	UAS as cyberattack targets
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

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*)

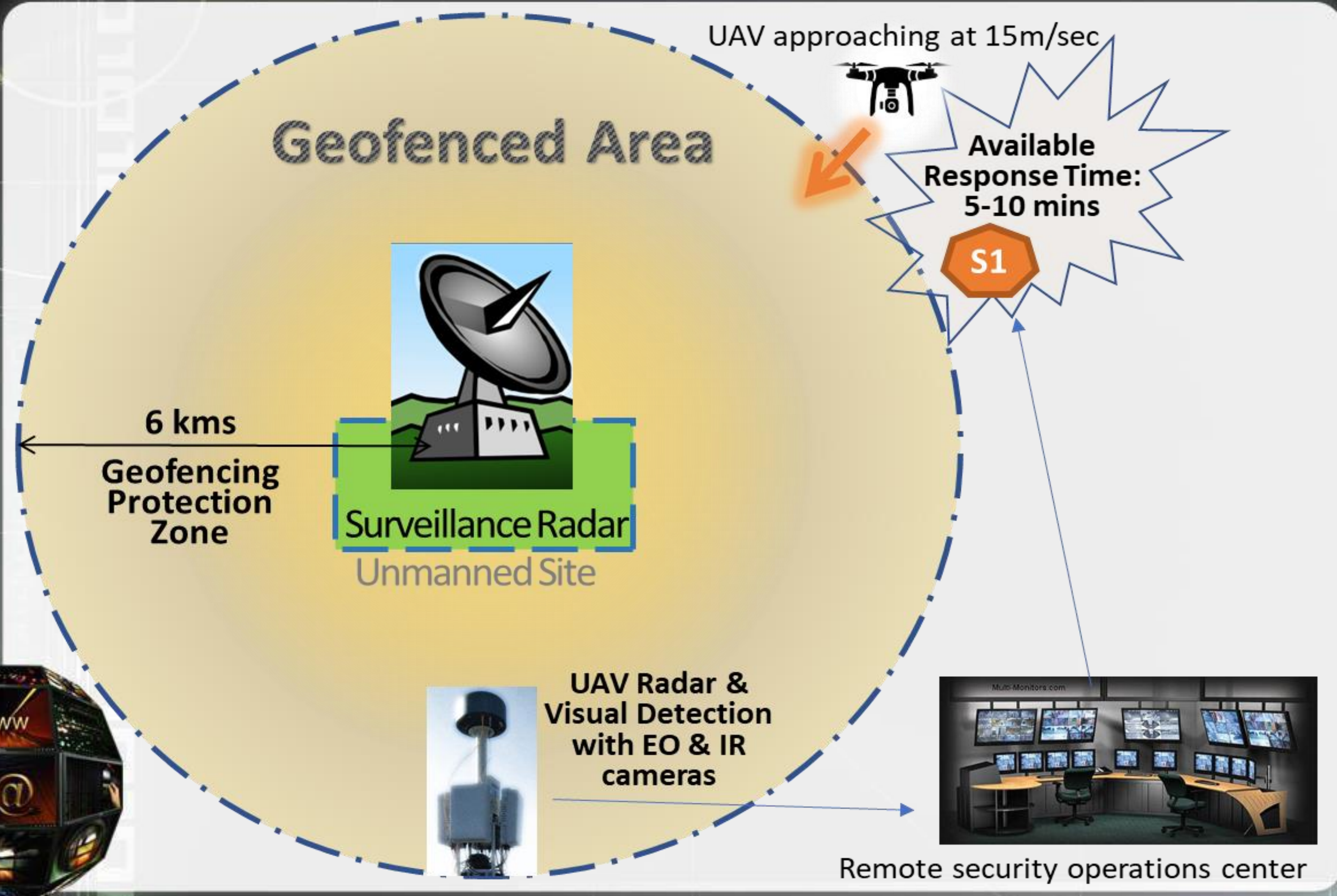
Day X

Step 2: UAV attacks CI by:

1) Carrying explosive payload
2) Emitting interference signal

RSR/MSSR Radar
Air Traffic Management Unmanned Stations
Com Transceiver
Air Traffic Management Unmanned Station

How to protect ATM & Airport facilities?



UAV approaching at 15m/sec

Available Response Time: 5-10 mins

S1

Geofenced Area

6 kms

Geofencing Protection Zone

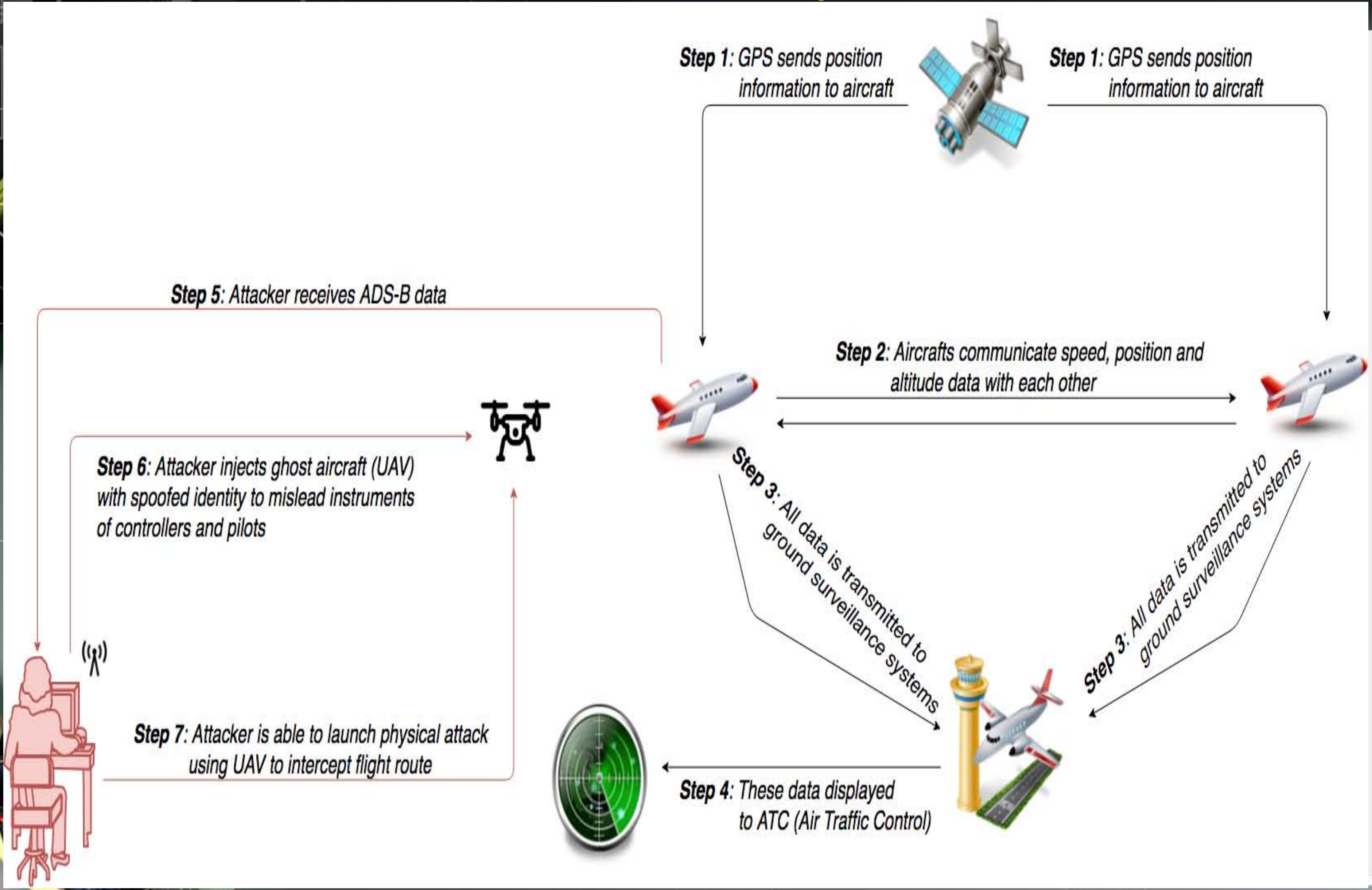
Surveillance Radar

Unmanned Site

UAV Radar & Visual Detection with EO & IR cameras

Remote security operations center

Communication attack on ATM systems
Attack Scenario to Airport facilities



Step 1: GPS sends position information to aircraft

Step 1: GPS sends position information to aircraft

Step 2: Aircrafts communicate speed, position and altitude data with each other

Step 3: All data is transmitted to ground surveillance systems

Step 3: All data is transmitted to ground surveillance systems

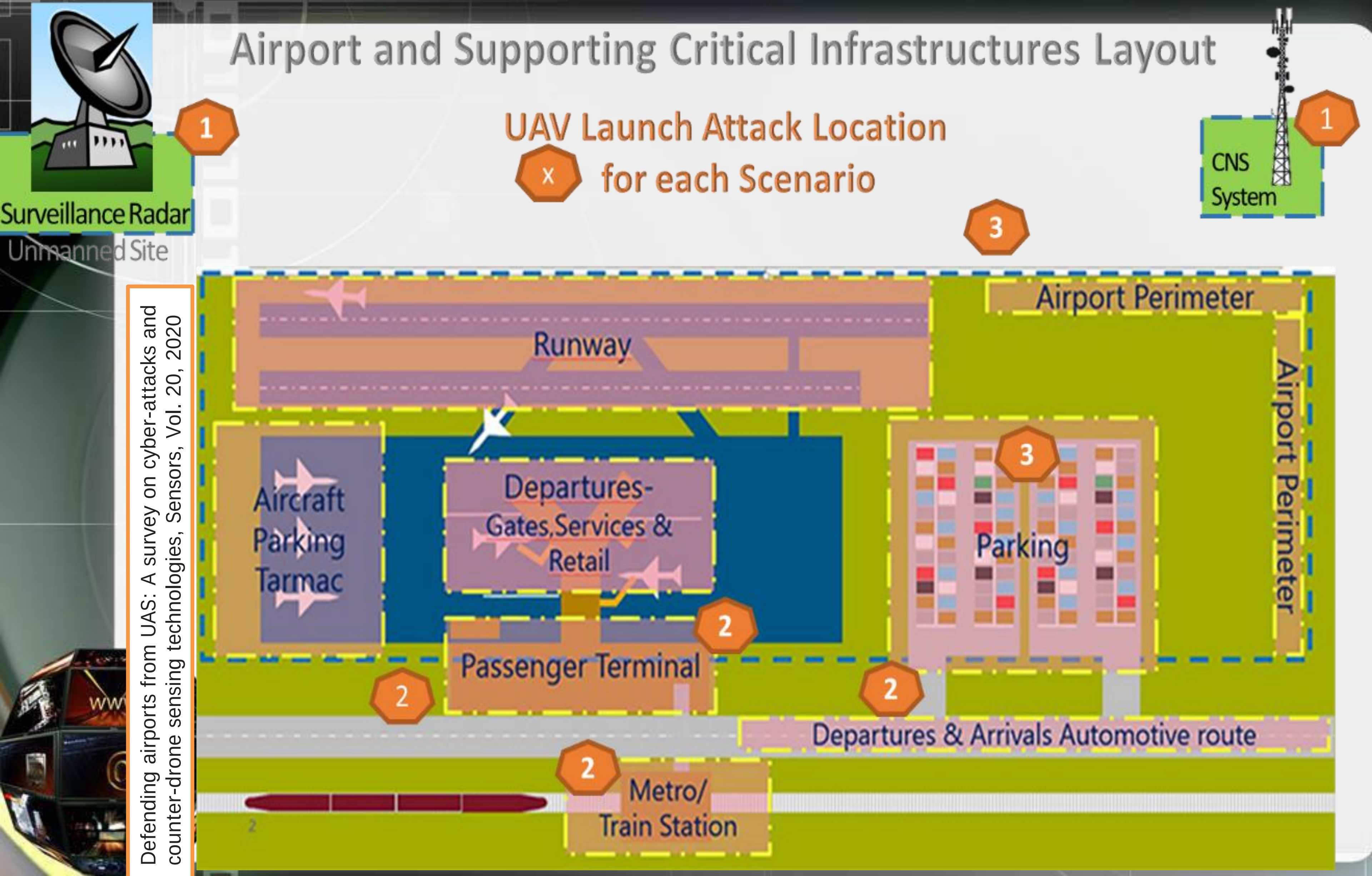
Step 4: These data displayed to ATC (Air Traffic Control)

Step 5: Attacker receives ADS-B data

Step 6: Attacker injects ghost aircraft (UAV) with spoofed identity to mislead instruments of controllers and pilots

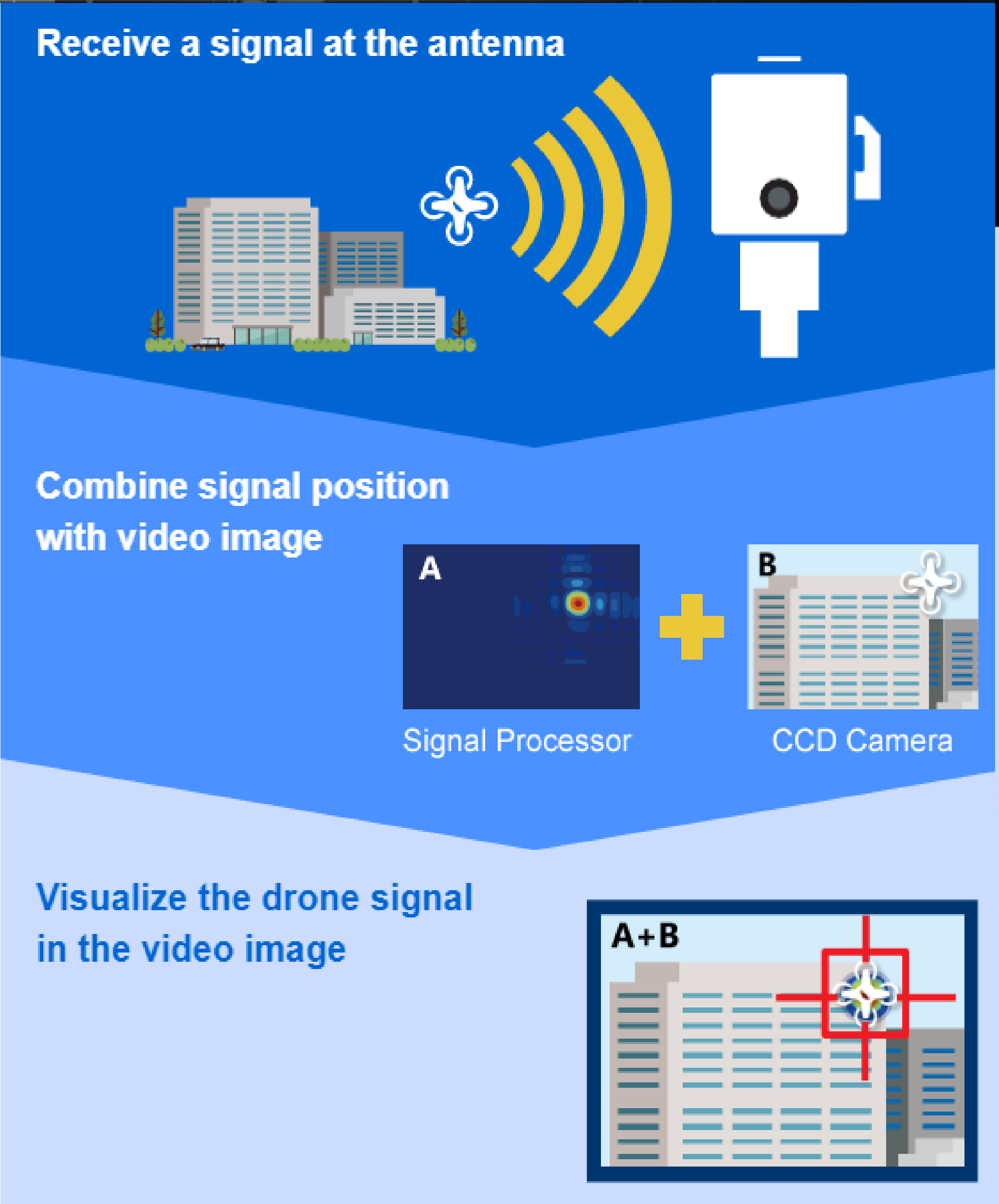
Step 7: Attacker is able to launch physical attack using UAV to intercept flight route

How to protect ATM & Airport facilities?



Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies, Sensors, Vol. 20, 2020

C-UAS Technologies



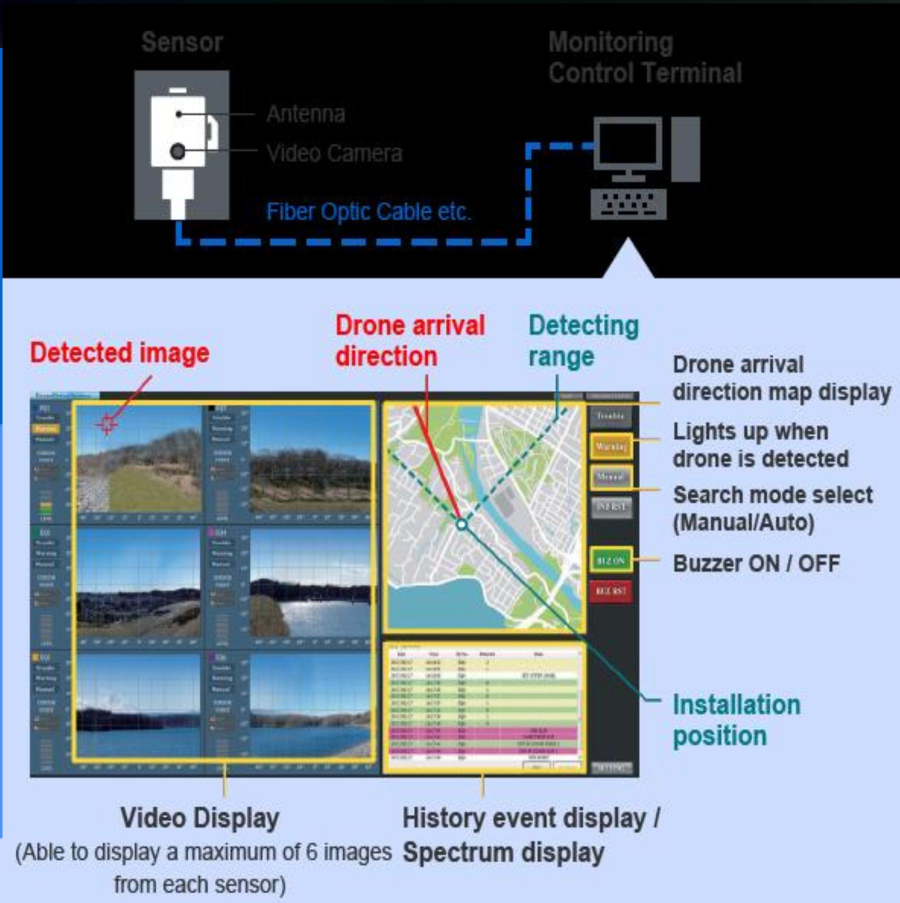
Receive a signal at the antenna

Combine signal position with video image

Signal Processor

CCD Camera

Visualize the drone signal in the video image



Detected image

Drone arrival direction

Detecting range

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

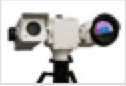
Detect, Track & Identify

React

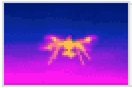
Interdict

Sensors:

Acoustic

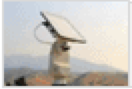


Visual/EO



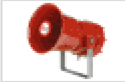
Thermal

Radio Frequency (HF, VHF, UHF)



Radar

Non-interactive[1] Response:



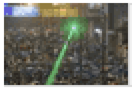
Drone Alarms

Close Window Blinds

Shut Down Wi-Fi

Evacuate an Area

Deploy a Fog Grenade

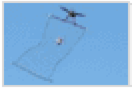


Blind the Drone Camera

Kinetic Solutions:

Laser

Projectiles



Net

Non-Kinetic Solutions:

RF/GNSS Jamming

RF/GNSS Spoofing

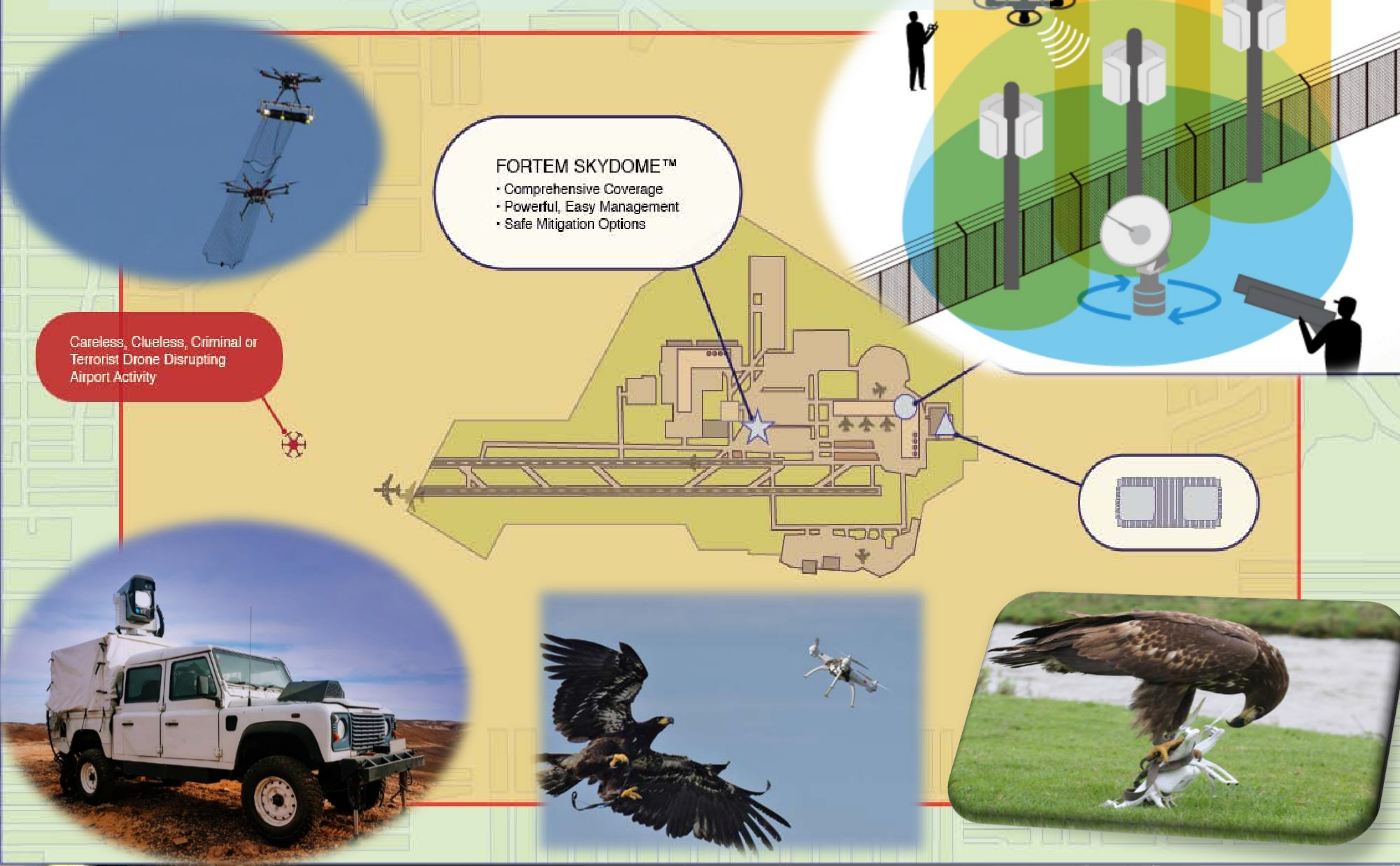
[1] Threat responses which do not interact with the drone in any way but can actively or passively mitigate the threat it poses

source: DRONEII.com

21st January 2020

Counter-Drone Systems & Airport's applicability

Is the airport operator permitted to operate detection & mitigation technologies for UAS?

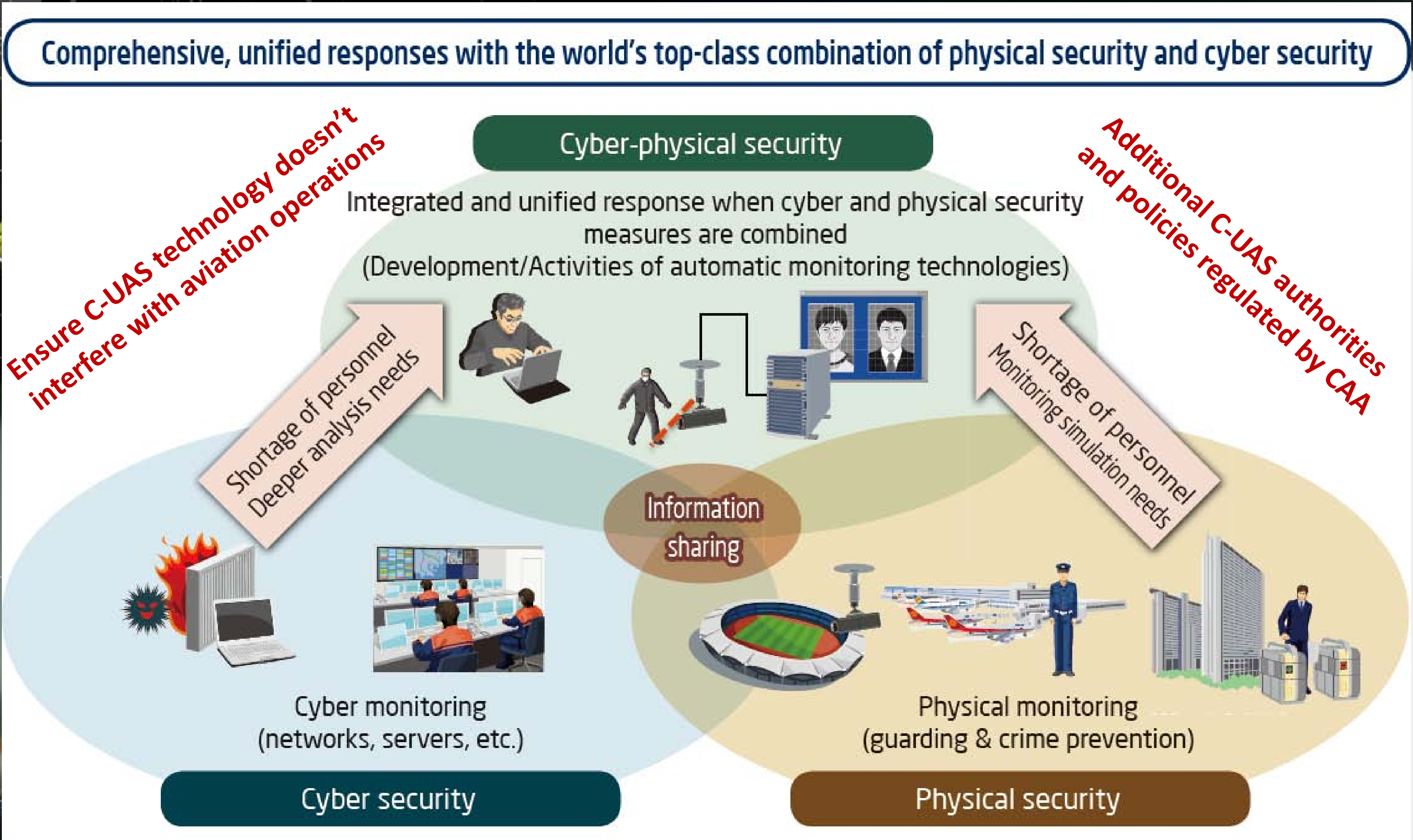


FORTEM SKYDOME™

- 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

Ensure C-UAS technology doesn't interfere with aviation operations

Additional C-UAS authorities and policies regulated by CAA

Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies
Sensors, Vol. 20, 2020. Available at: https://www.mdpi.com/1424-8220/20/12/3537

Related Scientific work @ https://www.infosec.aueb.gr/

References

1. ENISA, *Securing Smart Airports,* https://www.enisa.europa.eu/publications/securingsmart-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 EEE 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.