



Protecting your
airspace from
civilian drones

2019

Kaspersky Antidrone: protection from UAVs

kaspersky

BRING ON
THE FUTURE



**Kaspersky
Antidrone**

Drones have an important role in today's world. And yet, as drones become increasingly popular, unfortunately dangerous incidents involving UAVs are on the rise.

Easily available drones are not only attracting numerous amateurs with no piloting experience, but also providing new opportunities for threat actors.

Yes, drones are useful and fun. But in the hands of inexperienced owners they can pose a threat to other people and critical infrastructure. And in the hands of threat actors, drones become dangerous weapons.

Why drones are dangerous

Mass gatherings



The unexpected appearance of a UAV at an open-air festival or a stadium where tens of thousands of fans are gathered can lead to an accidental or deliberate collision with people or objects.

May 6, 2017: a drone crashed into a tree and fell on a cyclist during the final stages of a bike race in California. The cyclist was hospitalized.

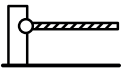
Airports and other facilities where airspace security is critical



Drones can be sucked up into airplane engines or collide with other parts of planes and cause accidents or forced landings. Today, airports include protection against UAVs into their airspace security policies.

Dec 19, 2018: 2 drones appeared over the airfield at London's Gatwick Airport. The runways were closed for 24 hours.

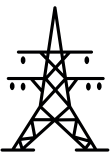
Private and commercial property



A drone with a video camera flying over private property often means that your personal information could become public. Worse still, when drones invade business spaces, the remotely controlled UAVs can easily be used for corporate espionage.

Feb 22, 2017: A drone hovered by a window in Beersheba, Israel and used a photo diode sensor to read 4 KB of data transmitted by the LED light on a computer blinking in specified patterns.

Critical infrastructure



Physical safety is a core requirement for all critical infrastructure facilities. Today, protecting airspace from accidental or malicious drone flights is part of the new normal for cities and even whole regions.

Oct 28, 2015: A drone tore through power lines and left hundreds of Los Angeles residents without electricity for 3 hours during repairs.

Industrial facilities



Collisions, even if accidental during unsanctioned UAV flights over oil refineries and other industrial facilities can cause damage with environmental, as well as economic consequences.

Safe implementation is a key requirement for any security solution. Drone flyaways should not endanger anyone or anything!

Why drones are dangerous in the hands of inexperienced amateurs or threat actors

Collisions

Drones in dangerous or uncontrolled proximity to moving or standing objects

Attacks

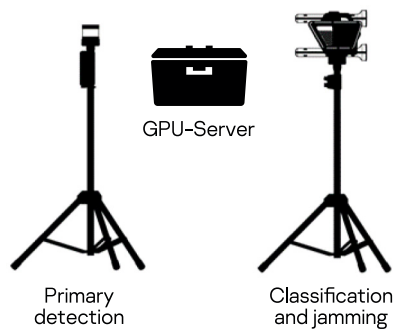
Intentional physical harm to people, mechanisms or facilities using drones

Espionage

Illegal collection of photos or video materials using drones

Smuggling

Transport of goods illegally to closed facilities and territories or to circumvent laws and established rules



Kaspersky Antidrone

The standalone Kaspersky Antidrone automatically detects and classifies civilian UAVs using a Kaspersky-trained neural network.

Sensors, chosen to secure the individual facility, work together with advanced technologies based on a neural network to warn of incoming drones to the protected area. If necessary, the solution generates permitted radio interference signals to make the incoming drone either return to base or land safely.

Detection

Kaspersky Antidrone uses a patented laser scanning technology for primary detection of consumer drones, as well as video and audio sensors, and, if applicable, radar. Scans are run in windows of 360° horizontally and 45° vertically.

Classification

The specially trained neural network identifies the drone's class and model. If more than one drone is detected the built-in algorithm prioritizes them by threat level. The neutralization scenario depends on drone's type and model.

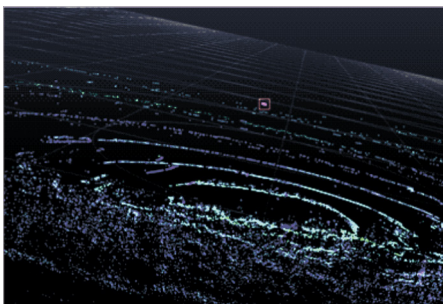
Neutralization

If required, a specially designed system generates a narrow interference beam to break the drone's connection with either a GP's satellite or the remote controller. Once the connection is broken, accidents are prevented, with the drone either returning to base or slowly descending in the area where the connection was lost.

Technology protects physical safety

Primary detection: laser scanners and lidar

Kaspersky's patented technology uses laser to create a 3D image and identify drones in the clouds of dots generated by lidar.



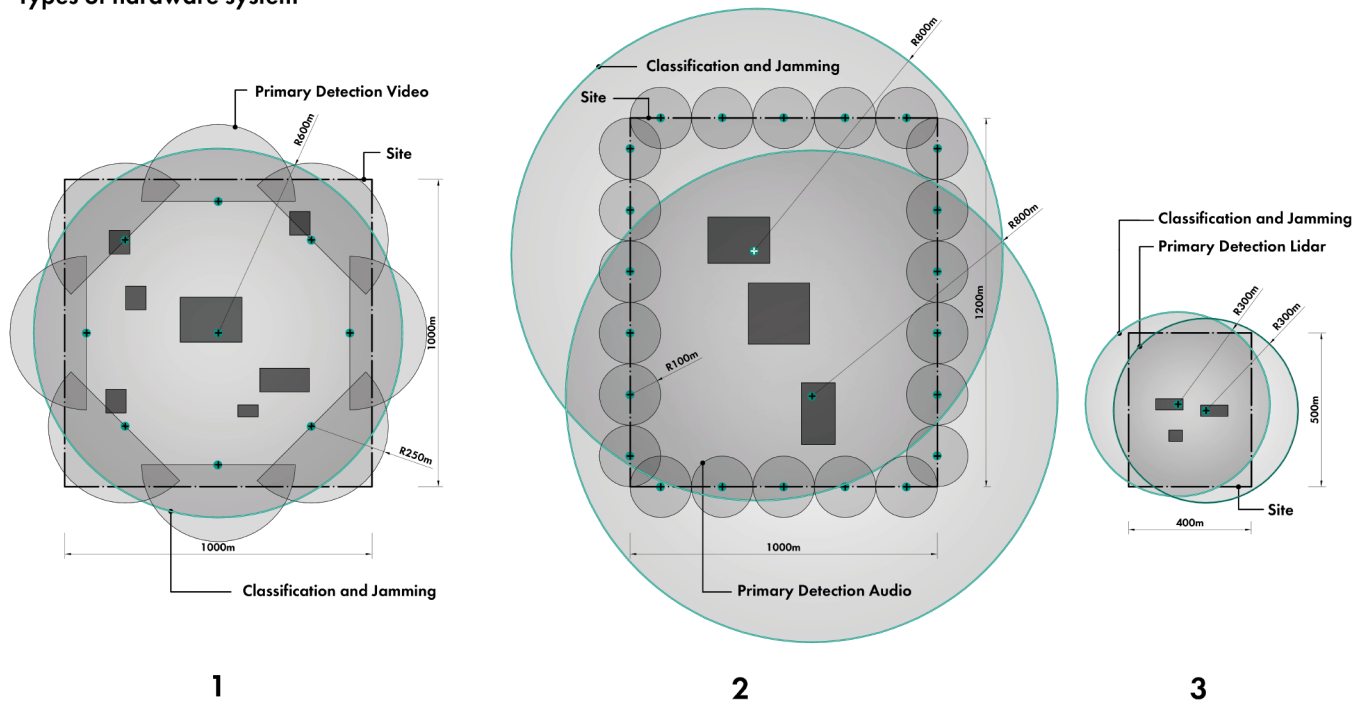
Drone classification: neural networks

UAVs are identified, excluding false positives for birds and other similarly sized objects. The proprietary neural network is trained to identify civilian drones by class and model from various vantage points, different lighting and using different types of cameras.



Installing Kaspersky Antidrone

Types of hardware system



Kaspersky Antidrone uses a variety of sensors to create different solutions to securing airspace from unsanctioned civilian UAVs. Depending on the shape of the facility and the available budget we help you choose the quantity and types of sensors, as well as the location of the primary detection module, classification module and neutralization module.

Kaspersky Antidrone modifications

Stationary system

Intended for buildings and outdoor areas

Includes a GPU server, a neutralization module and a choice of sensors: lidar, radar, video cameras or microphones

Mobile system

Intended for securing mass gatherings or remote locations

Includes a GPU server, neutralization module and a choice of sensors: lidar, video camera or microphone

Software integration into existing security systems

Designed to use existing video cameras or radars to detect and classify unsanctioned drones

Web site: kaspersky.com/antidrone

IT Security news: securelist.com

Blog: kaspersky.com/blog

kaspersky BRING ON
THE FUTURE

www.kaspersky.com

2019 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.