CUAS

Drone threat and CUAS Technology - White Paper

By Haim Haviv, Elbit-Elisra

Haim Haviv
1-1-2019

Elbit Systems™
EW and SIGINT - Elisra

Drone threat and CUAS Technology

White Paper

Administrative Point of Contact

Shay Alagem

BD & Marketing Director

Elisra Marketing Division

Phone: (+972) 0549932009

E-mail: shay.alagem@elbitsystems.com

Technical Point of Contact

Haim Haviv

EW Senior Director

Elisra SIGINT Division

Phone: (+972) 0772937230

E-mail: Haim.Haviv@elbitsystems.com

Contents

Objectives

This document describes Elbit Systems`s (herein after: Elbit) understanding of the Drone threats and the roll of Regulation & Technology as part of the CUAS effort. Also in this document is Elbit concept for CUAS system and technology needed to protect against these threats.

This paper is based on Elbit's experience in design, manufacture and testing of Electronic Warfare (EW), Counter - Remote Controlled Improvised Explosive Devices (C-RCIED) and Counter Unmanned Aerial Systems (CUAS) protection systems.

1 The UAS Threat

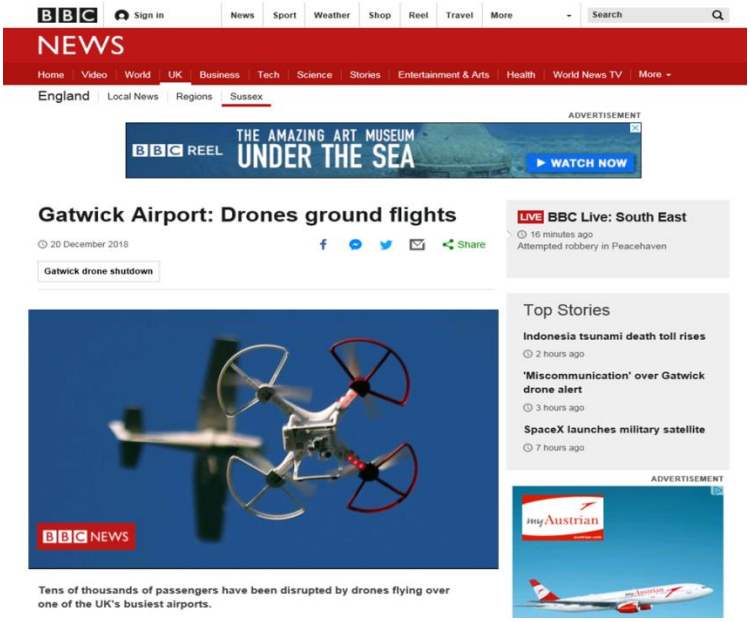
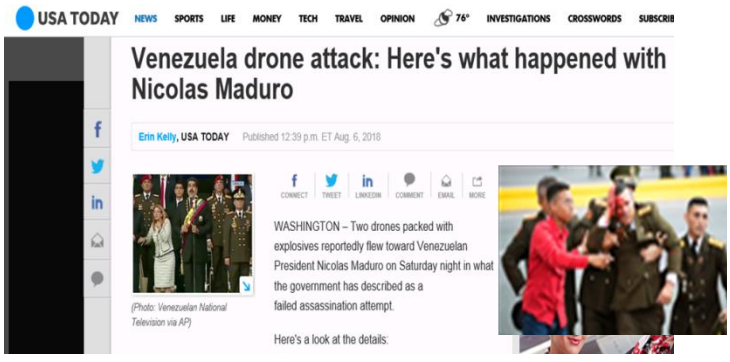
As off-the-shelf commercial UAS become less expensive, easier to fly, and more adaptable for crime, terrorism or military purposes, defense forces will increasingly be challenged by the need to quickly detect and identify such craft—especially in urban areas.

In the last two years there is a constant growth in the use of commercial UAS by amateurs and hobbyists and an alarming increase in the use of Drones by crime and terror groups.

Crime and terror groups are also modifying the commercial UAS to fit their needs.

Following are some examples of well-known UAS threats:

Treat	Example
Smuggling across borders	
Smuggling into prisons	
VIP events disruption	

Treat	Example
Commercial aviation disruption	
Flight over sensitive sites	
Terror attacks	

Treat	Example
Military\Terror use	**ISIS Drone Attack In Iraq Kills 2 Kurdish Fighters, Injures 2 French Soldiers, Reports Say** BY VISHAKHA SONAWANE ON 10/12/16 AT 4:32 AM  
Future threat- **Swarm of autonomous Armed Drones**	

1.1 Drone threat conclusions:

There is a growing use of drones for different categories: hobby, commercial, crime and terror.

Each one of these drone usages creates a different threat:

Hobby\privet – unintentional risk to public safety, aviation and personal privacy, mainly due to lack of experience and regulation unawareness.

Commercial – uncontrolled usage of low altitude air space with risk to aviation, public safety and intellectual property (IP) theft, mainly due to lack of air traffic control regulation & technology and regulation enforcement capability.

Crime – using the drone's high availability and capabilities for intentional low braking, mainly due to lack of enforcement.

Terror - using the drone's high availability and capabilities to convert it into a weapon.

2 Regulation

Governments and legislators, all over the world, are trying to close the increasing gap between the fast growing use of drone for hobby\commercial applications and the absence (or slow release) of new and effective UAS regulations.

In most cases it is also unclear who has the responsibility to enforce these new regulations (police, FAA, airport security, air force, other agency).

Most privet drone owners consider their drone as a toy or a Hi-Tech gadget and are unaware of all existing (and changing) regulations.

Despite the growing impatience from some big players in the business community's (Amazon, Google and more) to allow extensive commercial use of drones, there is a common understanding that the regulations and enforcement issues needs to be resolved to allow a safe use of drones over populated areas.

General Rules for Flying a Drone in the Netherlands:

- Commercial drone operations in the Netherlands require the drone pilot to hold a pilot's license, and the company / organization overseeing the operation to hold a permit to fly.
- Drones may not fly more than 120 meters (394 feet) above the ground or the water.
- The maximum weight for private drones is **25 kilogram**
- Drone pilots must give priority to all other aircraft, such as airplanes, helicopters, gliders, et cetera. This means that you must land immediately once you see an aircraft approaching.
- Drones must fly at a safe distance from people and buildings.
- It is not permitted to secretly film someone.
- Drones must maintain a visual line of sight with their drone during operations.
- Drones may not be flown at night.
- Drone insurance is required for commercial drone operations in the Netherlands.

2.1 Regulation conclusions:

Present regulation is more relevant to commercial use of drones,
privet drone owner are mostly untrained and unaware of all regulation.
Recommendations - A different set of regulation is needed for the commercial and private sectors, to allow for a wider and more controlled use of drones in the commercial sector (as part of low altitude commercial aviation) and to allow safe areas for private drone owners to operate (make mistakes…) and gain experience with their private drones.
Lowering the maximum weight limit for private drones should also be considered as most off-the –shelf consumer drones weight up to 5 Kg.

3 Technology

Technology can play a major role in helping to enforce and even to update UAS regulations, for example a regulation to include a “drone standard” identity & telemetry transmitter on all commercial and private UAS with weight over 5 Kg. This technology can help in creating a drone traffic control system over populated or restricted areas.

Special technology has to be applied to counter criminal and terror use of drones that do not follow the formal regulations.
Such **special technology** focus on two main capabilities of **Detection** and **Defeating**.

Detection:	**Example**
Detection by human (visual and audio)	
Active detection by RADAR	
Passive RF detection of UAS communication	

Passive IR detection of drone's heat signature	
Passive Acoustic detection of drone's acoustic signature	

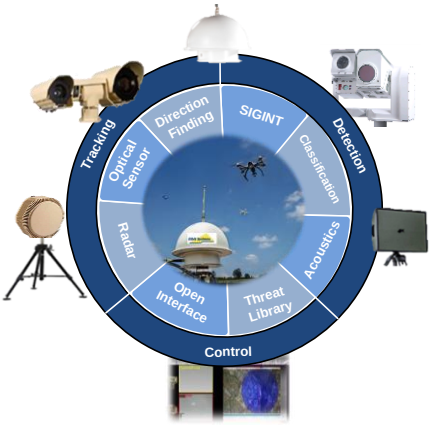
Defeating:	Example
Kinetic weapons	
Kinetic with low collateral damage	
EW –Communication and GNSS RF Jammers	 
EW – Cyber	010111011100100 
Drone vs. Drone	

Energy – High Power Microwaves	
Energy - High Power Laser	

3.1 Technology conclusions:

There is no single technology that can detect & defeat all UAS threats in all the operational scenarios. A modular and scenario-adapted solution is needed.

The combination of new regulations and technology can provide efficient tools to enforce drone safety and to counter criminal\terror use of drones.



4 Elbit approach for Counter Unmanned Aerial Systems (CUAS)

4.1 General

To counter the growing UAS threat, a variety of CUAS technologies and systems were developed.

After examining and testing the majority of the technologies we can state that there is not a single solution that fits them all and there are different solutions for different sites or threat scenarios.

This is why for CUAS we believe in a **modular and multi-layered** approach that can be customized to the needs of each site and threat scenario.

Figure 3 – SIGINT DF Antenna

4.2 UAS Detection

4.2.1 First layer - SIGINT Detection and Direction-Finding (DF)

The SIGINT passive detection capability covers all the ISM frequency bands and is utilizing a special DF antenna for both - drone and operator detection and Direction-Finding.

To achieve a high probability of detection, the SIGINT detection uses a known Drone communication library that can be frequently updated.

When two or more SIGINT systems are operated in the same vicinity the C2 system can point at the UAS location and track its route with high accuracy.
The SIGINT passive detection system complies with all safety regulations and can operate in urban or rural environments, at all weather conditions, and cover up to 1.5 Km radius of detection.

The SIGINT subsystem main advantages are:

- high PD and low false alarm rate in urban area
- classification of drone type
- direction-finding of drone and it`s operator
- detection of a hovering drone
- co-existence with other nearby communication systems
- no safety or regulation issues in populated urban area

The SIGINT subsystem main disadvantages are:

- no detection of autonomous or unknown UAS
- medium range detection (up to 1.5KM)
- medium accuracy for location measurements

Figure 4 –RADAR SYSTEM

4.2.2 Second layer - RADAR Detection

The Radar subsystem is designed to detect the presence of UAS by their radar signature. The Radar subsystem provides situational awareness, with Bearing, Range, Altitude, Location and Velocity data presented to the system operator.

The radar can detect many types of moving objects, at a wide range of velocities but it needs to transmit energy in order to do so. More energy (power) transmitted will allow higher detection range. Being active, RADAR can detect autonomous and unknown types of UAS but needs to address ground multipath effect, energy reflection in urban environment and co-existence problems with other nearby communication systems.

The Radar subsystem main advantages are:

- accurate Range and Direction measurements
- long range detection (up to 5KM)
- detection of autonomous and unknown UAS

The Radar subsystem main disadvantages are:

- high false alarm rate in urban area
- co-existence with other nearby communication systems
- detection of a hovering drone
- safety and regulation issues in populated urban area

Figure 5 –EO\IR optical SYSTEM

4.2.3 Third layer - Optical identification & classification

The optical subsystem provides visual identification & classification of UAS.
The subsystem is based on a powerful day and thermal cameras and robust pan-tilt unit. The optical subsystem has a flexible design suitable for a variety of defense applications and can be mounted on the site roof or on a mast to extend line of sight.

The optical subsystem detection capabilities are limited to the optical field of view (10-30°) and it is mainly used for visual identification & classification by the user, after a treat is detected by the SIGINT or RADAR.

The optical subsystem main advantages are:

- visual identification & classification
- visual tracking capability
- operate in day & night
- no safety and regulation issues in populated urban area

The optical subsystem main disadvantages are:

- limited detection capability
- short-medium range of up to 1KM
- range affected by weather conditions

4.3 UAS Defeat

4.3.1 EW - Communication Defeat

EW defeats the UAS by jamming all radio communication channels that are in use by the UAS (control and video).

After the system has alerted its operator of a UAS detection, the operator now decides the manner of operation and duration needed to defeat the UAS using the active part of the system. the operator is most likely to use the optical sub system to visually identify & classify the threat before engaging the defeat sub system and to assess the impact of the jamming on the UAS (BDA).

When the operator stops the active defeat operation, the system will resume passive detection automatically, maintaining awareness of the UAS.

Once the EW defeating operation is in-play, the UAS will lose communication with its operator resulting in the UAS returning home to its origin (point of takeoff) or initiate auto landing protocol.
The active defeating signal can be delivered using two main types of antennas (Omni or directional) based on site size and user requirements.

4.4 EW - GNSS Signals Defeat

Some UAS platforms can become autonomous when their control channel is jammed or by user's configuration. In this case their navigation is driven by GNSS (GPS and\or GLONASS). Since the GNSS signals are transmitted continuously, the EW-GNSS defeat sub system transmits low power defeating signals towards the drones eliminating its GNSS navigation capability and resulting in the UAS initiating its auto landing protocol.

4.5 EW – communication & GNSS Defeat

Under no communication link and no GNSS signals, most commercial Drones will go into "safe landing" protocol (slowly descent until full landing). This is the reason that in most cases EW communication and EW GNSS are combined and operated together to achieve the effect of UAS "safe landing".

4.6 EW – Cyber Defeat

New cyber capabilities include protocol manipulation to take control of the intruding drone and land it in a predefined location. In some countries this capability is considered as hijacking and it's not yet allowed for usage.

4.7 EW – Energy weapon

High power directed energy beam to disrupt the intruding drone electronic circuits and cause it to crash. Efficient for war zones and as "last line of defense".

5 Threat analysis

In order to determine the effective CUAS system configuration needed for protecting a specific site, a threat analysis is performed.

5.1 Example of threat analysis for small sensitive urban site

Site size – usually a small to medium size up to 200 by 200 meters

Site environment – urban with heavy civilian traffic nearby (cars and peoples) and dense electromagnetic environment (WiFi, cellular, radios…)

Level1 threat:
Civilian and hobbyist drone operators taking unintentional pictures\videos of the site and uploading them to the internet or social media.
Threat range- Drone 0-100 m, operator 50-300 m
Threat probability – High
Threat damage – Low
Threat relevancy – All urban sensitive sites (Embassies, government, high security)

Level2 threat:
Criminal\ espionage\ terror organization using drones for intelligence collection from the site.
Threat range- Drone 50-200 m, operator 300-1000 m
Threat probability – Medium-High
Threat damage – Medium
Threat relevancy – All urban sensitive sites (Embassies, government, high security)

Level 3 threat:
Terror organization attacking the site\site facilities\site personal with drones carrying small bombs or explosive device.
Threat range- Drone 0-50 m, operator 500-1000 m
Threat probability – Low- Medium (and rising)
Threat damage – High
Threat relevancy – well known urban sites (Embassies, Government, famous landmarks)

5.2 The CUAS solution\ main requirements for small fix site

The CUAS system main requirements:

- Operate in urban or rural environments
- Complies with civilian safety regulations
- Operate in day, night, and in most weather condition
- Detect class 1&2 commercial drones at range of 0-1000 m
- Calculate drone position (x,y) with high accuracy
- Detect and locate drone's operator position with medium accuracy
- Very simple and user friendly operation
- High PD and low FAR
- Handle a single UAS or swarm
- Provides centralized command and control functions
- Provides Audio and visual alarm

6 Conclusions

6.1 General

The use of privet and commercial drones is constantly growing, creating new threats for public safety and new challenges for law enforcement.

These threats are already here and can be seen in daily events all over the world.

The way to utilize drone's potential while protecting public safety, calls for the combination of new regulation and technology.

6.2 Regulation and Technology

There is a need to look differently at the three main drone usage segments:

Commercial – regulation and technology for air traffic control,
UAS registration and pilot training and registration.

Private – updated UAS class (with weight and performance limits),
regulation for fly\no-fly zones, UAS id-tag for high class drones,
counter UAS technology for law enforcements and public safety
(airports, sports events etc.).

Crime\Terror – Threat analysis for government and sensitive sites,
for deploying the relevant Counter UAS technology.

Military - Military grade and multi-layer CUAS technology for war zones.

All Counter UAS technology should be based on modular and multi-layer design to enable change\upgrade as the UAS threat evolves.