TransNav
http://www.transnav.eu
the International Journal on Marine Navigation and Safety of Sea Transportation
Volume 17
Number 2
June 2023

DOI: 10.12716/1001.17.02.23

Anti-drone Sensors, Effectors, and Systems – A Concise Overview

D. Zmysłowski, P. Skokowski & J.M. Kelner
Military University of Technology, Warsaw, Poland

ABSTRACT: The dynamic development of microelectronics and wireless communication at the turn of the 20th and 21st centuries contributed to the increase in the availability and popularity of all kinds of unmanned platforms, air, land, surface, and underwater. In the case of unmanned aerial vehicles (UAVs), also popularly known as drones, the significant (crucial) advantages are high freedom of motion (i.e., the ability to move in three planes) and the possibility of using it practically anywhere (as opposed to water platforms). These factors influenced the dynamic development of this market sector and the high availability of various models and equipment. UAVs are being used in many sectors and services, both for civil and military purposes. Widespread availability, low cost, and ease of use also favor the possibility of using civilian UAVs for criminal, smuggling, terrorist, or military purposes. Recent armed conflicts, e.g., in Nagorno-Karabakh or Ukraine, and the situation on the eastern Polish-Belarusian border clearly show this. All countries recognize the potential and threat posed by the development of unmanned platforms. Therefore, for several years, special attention has been paid to analyses and research in sensors, effectors, and anti-drone systems. It is worth emphasizing that some effectors (e.g., jammers or spoofers) may significantly affect the navigation process of neighboring objects that use global navigation satellite systems (GNSSs). On the other hand, the use of anti-drone systems is important, especially in the context of protecting institutions and facilities of companies, state administration (i.a., embassies, consulates), army, strategic importance objects (e.g., related to energy, chemical industry), or protection of mass events. In this paper, we present an overview of solutions available on the market and development directions in the field of anti-drone technology.

1 INTRODUCTION

Drones, also known as unmanned aerial vehicles (UAVs), have become ubiquitous in recent years due to their various applications, including aerial photography, surveying, and delivery services. However, drones can also be used for nefarious purposes, including espionage, terrorism, and smuggling. The number of drones is growing very fast, and their commercial use is becoming more widespread, attracting a high level of interest from investors, industry, business, government institutions, the military, agencies, special services, and private individuals. Knowledge and practice in designing and manufacturing drones have become more accessible. A lot of institutions and individuals are designing and using their drones. The components for constructing simple micro-class drones are available in the market without legal restrictions. All of these factors prevent using commercially available drones and self-made drones for military, terrorist, or unintentional use that violates the law. The development of anti-drone systems has become the need of the hour. The increasing number of incidents or acts of security breaches or even attacks using drones has led to the emergence of increasingly sophisticated drone detection and countermeasure equipment. Therefore, it is necessary to have anti-drone systems in place to detect and neutralize these threats. Anti-drone systems called also as counter unmanned aerial systems (C-UASs), both stationary and mobile, have also started to be built and offered.

The dynamic growth of the C-UAS sector is evidenced also by the ongoing research and development in this area. Results of searching for works related to the keyword 'anti-drone' in the IEEE Xplore international technical publications database [1], the database provides 45 works (as of 10 March 2023), including one book, two journal articles, six scientific journal articles, and 36 conference papers. All these works are from the period 2017–2022.

One of the primary methods of detecting drones is using sensors. There are several types of sensors that can be used for this purpose, including acoustic sensors, radar systems, and optical sensors. Once a drone has been detected, it is necessary to neutralize the threat. There are several types of effectors that can be used for this purpose, including jamming systems, directed energy weapons, and nets.

This paper presents the general concept of C-UAS, its functionalities, and main elements. This class of systems started to be more important these days. We decided to make a high-level functional overview which can be a kind of guidance around anti-drone systems and their elements. We intended to characterize the topic as simply as possible, to be a quick start guide for people not well-oriented in this area of knowledge. We believe it will help them in further personal investigations. Section 2 presents reasons for designing, deploying, and using drone countermeasures. We considered constructing and functional aspects of existing and future drones as platforms that could be potential threats to people and states, especially for critical infrastructure. How effective could be a concrete C-UAS depends on its sensors and effectors. Section 3 describes the most often implemented cost- and target-effective sensors as acoustic radio frequency (RF), radar, and optical sensors. Section 4 shows anti-drone effectors such as jamming systems, directed energy weapons, and nets. In Section 5, both fixed and mobile systems have been described. We also presented selected vendors of anti-UAS. The paper is finished with the conclusions.

2 FUNCTIONAL CONCEPT OF ANTI-DRONE SYSTEM

Modern drones are unmanned flying objects, which are mechanical devices with:

- drive based on engines: electric, combustion (piston or turbine) or operating in hybrid systems;
- avionics providing control and flight control, which are electromechanical and electronic systems;
- navigation devices and systems, mainly gyroscopic – inertial () and electronic – satellite, i.e., based on global navigation satellite system (GNSS),
- electronic devices and radio communication systems, providing support for remote control and flight control as well as transferring of data from sensors and control of effectors;
- mainly electronic sensors:
  - for multispectral imaging (visible range, thermal range, forward looking infrared (FLIR)),
  - for radio-electronic surveillance,
  - others;
- effectors for affecting objects:
  - RF jammers and spoofers - electronic devices,
  - explosives - bombs and guided missiles,
  - others.

The principle of operation, architecture, and procedures of using anti-drone devices and systems are closely related to the functions, operational use, and technical parameters of modern drones. To effectively counteract the potentially harmful impact of drones, the anti-drone system should identify drones, classify them, assess their activity, and countermeasure them if they have been identified as a threat to the protected facility. The important role of unambiguous identification and classification of objects observed by the anti-UAS system should be considered. Practice shows that mere detection of an object is insufficient because the radar that detects drones can also recognize other flying objects as birds. In addition, own flying objects such as planes and drones can move in the protected space. It makes identification and classification of the elementary functions of modern C-UAS devices.

The role of these functions will grow in the future, mainly to protect critical infrastructure and its mobile elements (e.g., oil terminals, gas terminals, tankers, gas carriers, etc.). The technology that classifies drones will usually be able to separate them from other objects – such as planes, trains, and cars. The next step is to identify the classified objects. Some devices can assess a specific drone model and identify the radio emission signature of the UAV (i.e., digital fingerprint) or its controls or controllers.

The elementary criterion for evaluating the C-UAS system is the effectiveness of protection against drones provided to a given facility. The system must be appropriate from the viewpoint of the characteristics of the protected facility (location, size, technological processes, functions performed, and activities performed).

Anti-drone devices and systems are being constructed to eliminate threats resulting from the impact of drones on protected facilities. After detecting and identifying a drone as a potentially dangerous object, their operation should enable its disposal by eliminating it (physical destruction) or preventing its destructive impact on the protected location (turning around, changing the flight parameters so that it is impossible to reach the target). It means that C-UAS devices and systems affect the droning engine and all devices and systems, both on-board and sensors and effectors. It leads to taking into account in the design, implementation, and operational use of anti-drone systems many aspects related to drones as risk factors for the protected objects, the technology of their production, tactics of their use, but also the development trends of the information and communication technologies (ICT), aerospace, and breakthrough technologies, because they are chosen for the construction and operation support of drones.

A holistic, multi-faceted approach also requires the very selection of technically effective solutions for anti-UAS devices and systems, considering the following issues [2,3]:

- the design of broadband radio detectors and direction finders, covering the drone's communication and navigation bands,
- development and use of operationally effective hemispheric radars, operating in X and S bands and using the micro-Doppler effect to identify and distinguish drones from other objects (birds), high-resolution, multi-spectral cameras (visible range, thermal range, FLIR)
- highly effective & sensitive acoustic microphones and analyzers for audio identification of drones,
- artificial intelligence(AI) algorithms to support identification processes, classification,
- a creation of situational imagery to facilitate the handling of hazardous situations,
- customized system interface - customized human machine interface (HMI),
- highly performative effectors usage: RF jammers and spoofers, laser systems, high power energy (HPE) systems [4–6], C-UAS nets, anti-aircraft weapons capable of fighting drones, etc.

The functionality concept of the modern anti-drone system is presented in Figure 1.

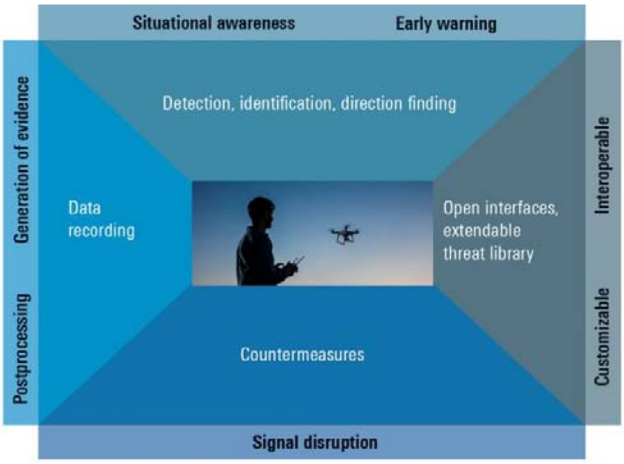

Figure 1. Functional concept of anti-drone system (source: [7,8]).

3 ANTI-DRONE SENSORS

3.1 *Acoustic sensors*

Acoustic sensors use microphones to detect the sound of drones. The sound of a drone's propellers is distinct and can be used to detect its presence. Acoustic sensors effectively detect drones at close range, but their effectiveness diminishes as the drone moves further away. Figure 2 depicts exemplary precision acoustic detection system.

3.2 *RF sensors and direction finders*

RF sensors and direction finders are critical sensors used in C-UAS to detect and locate drones. RF sensors detect the electromagnetic signals emitted by drones, while direction finders provide the direction of the drone's source. Together, these sensors enable C-UAS systems to quickly identify and locate drones, allowing operators to take necessary countermeasures to mitigate potential threats. With the increasing proliferation of drones, RF sensors, and direction finders are becoming more crucial in ensuring the safety of critical infrastructure, facilities, and events [7,8,10,11]. Concept of drone position tracking by multiple RF scanners is shown in Figure 3.

Figure 2. Discovair G2 acoustic detector (source: [9]).

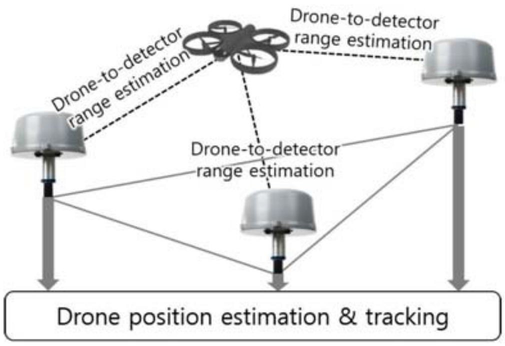

Figure 3. Drone position tracking by multiple RF scanners (source: [2]).

3.3 *Radar systems*

Radar systems use radio waves to detect drones. Radar can detect drones at a distance and can track their movements. There are several types of radar systems, including pulsed radar, continuous-wave radar, and frequency-modulated continuous-wave radar. Each type of radar has its advantages and disadvantages, and the choice of radar system depends on the specific application [7,11–18]. Samples of radar for drone detection are illustrated in Figures 4 and 5.

Figure 4. Radar R8SS-3D made by Teledyne FLIR (source: [18]).

Figure 5. Radar MESA-SSR made by Echodyne (source: [16]).

3.4 *Optical sensors*

Optical sensors use cameras to detect drones. Optical sensors can detect drones at a distance and can provide visual confirmation of the drone's presence. Optical sensors can be used during the day or at night using infrared cameras [3,19]. The optical detection system made by Aronia is presented in Figure 6.

Figure 6. The optical detection system made by Aronia (source: [19]).

4 ANTI-DRONE EFFECTORS

4.1 *Jamming systems*

Jamming systems disrupt the communication between the drone and its operator. The jamming system sends out a signal that interferes with the drone's control signal, causing it to lose control and crash. Jamming systems are effective against drones that are controlled by remote operator [7,8,10,16,20–22]. Figures 7 and 8 present the commercial jammer examples.

Figure 7. Jammer R&S®ARDN-GS GNSS made by Rohde & Schwarz (source: [8]).

Figure 8. Jammer SKY NET made by LONGBOW+ (source: [22]).

4.2 *Directed energy weapons*

Directed energy weapons use high-powered lasers to disable or destroy drones. The laser beam can damage the drone's electronics or cause it to crash. Directed energy weapons are effective against drones that are within line of sight [5,6,20,23]. Figure 9 illustrates the vision of destroying drones by a military system based on a high-energy laser.

Figure 9. High-powered laser in action (source: [6]).

4.3 *Nets*

Nets can be used to capture drones mid-flight. The net is launched from a device that can be hand-held [17,24], or mounted on a vehicle [24]. The net entangles the drone, causing it to lose control and crash. Nets are effective against drones that are flying at low altitudes.

Figure 10. Net cannon made by OpenWorks Engineering (source: [24]).

5 ANTI-DRONE SYSTEMS

Anti-drone systems are composed of sensors and effectors that work together to detect and neutralize drones. There are several types of anti-drone systems, including fixed systems and mobile systems [2,3,10–13,17,19,25–29].

5.1 *Fixed systems*

Fixed anti-drone systems (see Figure 11) are installed in a specific location and are designed to protect that location. Fixed systems are commonly used to protect critical infrastructure, such as airports, power plants, and government buildings.

Figure 11. Container version of GUARDION system (source: [10]).

5.2 *Mobile systems*

Mobile anti-drone systems (see Figure 12) are designed to be deployed quickly and can be moved to different locations as needed. Mobile systems are commonly used for events, such as concerts and sporting events, where there is a need for temporary protection.

Figure 12. Mobile version of AARTOS drone detection system (source: [19]).

5.3 *Exemplary vendors*

There are numerous vendors of anti-drone systems in the market. These vendors offer various solutions that are tailored to meet the needs of different industries, such as military, law enforcement, and private organizations. Some of the notable companies and their systems include:

- DJI Aeroscope: This system provides drone detection and tracking capabilities for law enforcement agencies, allowing them to locate drones in restricted airspace and identify the pilot's location. The system is compatible with DJI drones, making it an ideal solution for those operating DJI drones [27].
- Dedrone: Dedrone provides an airspace security platform that uses multi-sensor detection to detect and track drones, providing early warning to users. The system integrates with various other security systems and can be used to protect critical infrastructure, events, and other sensitive locations [4].
- Raytheon: Raytheon offers a range of anti-drone solutions, including the Drone Defender, a handheld device that uses radio frequency jamming to disable drones, and the Coyote drone,

which is used to intercept and destroy other drones [23].
- D-Fend Solutions: D-Fend Solutions provides a radio frequency-based system called EnforceAir that can detect and mitigate rogue drones. The system can be used in urban, rural, and indoor environments, making it suitable for various applications [28].
- Rheinmetall Defence: Rheinmetall Defence offers the Skysweep system, which uses radar to detect and track drones. The system is capable of detecting drones at a range of up to 10 km, making it an ideal solution for protecting large areas [29].

When comparing these solutions, it's essential to consider factors such as detection range, accuracy, cost, and ease of use. Some solutions, such as DJI Aeroscope and Raytheon's Drone Defender, are designed for specific applications and may not be suitable for all scenarios. Other solutions, such as Dedrone's platform, offer a more comprehensive approach that integrates various detection sensors to provide a complete airspace security solution. The choice of an anti-drone system ultimately depends on the specific needs of the user, such as the size of the area to be protected, the type of drone threat, and the budget available.

As examples of Polish vendors, we may indicate:
- Hertz Systems: This company provides a range of anti-drone systems, including the DroneBlocker, which uses radio frequency jamming to disable drones, and the DroneTracker, which uses acoustic and electromagnetic sensors to detect and track drones. The company's systems are used to protect critical infrastructure, such as airports and power plants [17].
- APS Systems: It offers a range of anti-drone solutions, including the SkyWall 100, a handheld device that uses a net to capture drones, and the SkyWall 300, a fixed installation that can capture drones at longer ranges. The company's systems are designed for use in urban environments and can be integrated with other security systems [12].

Both Hertz Systems and APS Systems provide innovative solutions to detect and mitigate drone threats. However, the choice of a system ultimately depends on the specific needs of the user, such as the size of the area to be protected, the type of drone threat, and the budget available. As the threat of drone incursions continues to grow, it's essential for organizations to invest in reliable and effective anti-drone systems to ensure the safety of critical infrastructure and personnel.

6 SUMMARY

The events of recent years, especially armed conflicts and terrorist attacks, show that the number of incidents with intentional destructive use of drones is increasing. Incidents of unintentional harmful drone activity are also frequent. This results in potential threats to human health and life and to the critical infrastructure facilities of countries. These trends are triggering the dynamic development of C-UAS systems, which are used to protect military units, airports, public facilities, or the country's critical infrastructure. The survey of anti-drone solutions is shown in this paper. We want to continue research in designing and implementing C-UASs for the protection of military units, state administration, and critical infrastructure facilities. We also plan to consider in our future works aspects of command and control of C-UAS.

ACKNOWLEDGMENT

This work was financed by the Military University of Technology under project no. UGB/22-863/2023/WAT on ‘Modern technologies of wireless communication and emitter localization in various system applications’.

REFERENCES

[1] IEEE, “Search Results ‘anti-drone,’” IEEE Xplore. https://ieeexplore.ieee.org/search/searchresult.jsp?queryText=anti-drone&highlight=true&returnType=SEARCH&matchPubs=true&returnFacets=ALL (accessed Mar. 12, 2023).
[2] S. Park, H. T. Kim, S. Lee, H. Joo, and H. Kim, “Survey on anti-drone systems: Components, designs, and challenges,” IEEE Access, vol. 9, pp. 42635–42659, 2021, doi: 10.1109/ACCESS.2021.3065926.
[3] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi, and J. Chen, “Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges,” IEEE Commun. Mag., vol. 56, no. 4, pp. 68–74, Apr. 2018, doi: 10.1109/MCOM.2018.1700430.
[4] Dedrone, “Best antidrone solution uses multilayer approach for complete solution.” https://www.dedrone.com/products/counter-drone-technology (accessed Mar. 12, 2023).
[5] Leonardo UK Ltd, “Falcon Shield.” https://uk.leonardo.com/en/innovation/falcon-shield
[6] Lockheed Martin, “Laser Weapon Systems,” Lockheed Martin, Apr. 19, 2022. https://www.lockheedmartin.com/en-us/capabilities/directed-energy/laser-weapon-systems.html
[7] Rohde & Schwarz GmbH & Co. KG, “Counter drone systems.” https://www.rohde-schwarz.com/nl/products/aerospace-defense-security/counter-drone-systems_250881.html
[8] Rohde & Schwarz, “R&S®ARDN-GS. Countering autonomously navigating drones that use GNSS based localization,” Rohde & Schwarz GmbH & Co. KG, Munich, Germany, 2.00, Apr. 2020.
[9] Squarehead Technology AS, “Precision Acoustic Detection.” https://www.sqhead.com/drone-detection/
[10] Rohde & Schwarz, “GUARDION. Countering drones system description,” Rohde & Schwarz GmbH & Co. KG, Munich, Germany, 1.04.
[11] Robin Radar Systems, “ELVIRA® Anti-Drone System.” https://www.robinradar.com/elvira-anti-drone-system
[12] APS, “Kompleksowy system antydronowy,” APS. https://apsystems.tech/produkty/sky-ctrl/
[13] Diehl Defence GmbH & Co. KG, ESG Elektroniksystem-und Logistik-GmbH, and Rohde & Schwarz GmbH & Co. KG, “GUARDION Countering Drones.” https://guardion.eu/
[14] DRS RADA Technologies, “Military Radar Solutions: Hemispheric Coverage,” DRS RADA Technologies. https://www.drsrada.com/radars (accessed Mar. 15, 2023).
[15] DRS RADA Technologies, “Multi-Mission Hemispheric Radar (MHR),” DRS RADA Technologies.

https://www.drsrada.com/products/mhr (accessed Mar. 15, 2023).
[16] Echodyne, “Counter Drone Radar,” Echodyne. https://www.echodyne.com/applications/government/counter-drone-radar/ (accessed Mar. 15, 2023).
[17] Hertz Systems, “Systemy antydronowe.” https://www.hertzsystems.com/systemy-antydronowe/
[18] Teledyne FLIR, “Ranger R8SS-3D Air and Ground Drone Surveillance Panel Radar,” Teledyne FLIR. https://www.flir.eu/products/ranger-r8ss-3d?vertical=surveillance+general&segment=surveillance (accessed Mar. 15, 2023).
[19] Aaronia AG, “Aaronia—AARTOS Drone Detection System,” 2022. [Online]. Available: https://downloads.aaronia.com/datasheets/solutions/drone_detection/Aaronia_AARTOS_Drone_Detection_System.pdf
[20] ESG Elektroniksystem- und Logistik-GmbH, “Counter-UAS Solution.” https://esg.de/en/solutions-services/air/counter-uas-system
[21] Kirintec, “Sky-Net-Longbow+. Datasheet.” [Online]. Available: https://www.kirintec.com/wp-content/uploads/2021/01/Sky-Net-Longbow-Datasheet_A4.pdf
[22] SKYLOCK, “RF Jamming System - 360° Anti Drone Jamming System,” SKYLOCK. https://www.skylock1.com/modular-components/counter-drone-mitigation-systems/rf-jamming-system/ (accessed Mar. 16, 2023).
[23] Raytheon, “High Energy Lasers.” http://www.raytheonintelligenceandspace.com/what-we-do/advanced-tech/lasers
[24] OpenWorks Engineering, “SkyWall Safer Airspace. Counter UAS and Air Defence,” openworksengineering.com, Dec. 27, 2022. https://openworksengineering.com/
[25] Rohde & Schwarz, “R&S®ARDRONIS. Countering RC drones – every second counts,” Rohde & Schwarz GmbH & Co. KG, Munich, Germany, 7.0, Nov. 2021.
[26] DroneShield, “View All Counterdrone (C-UAS) Products,” AI-enabled Multi-Mission Solutions. https://www.droneshield.com/products (accessed Mar. 12, 2023).
[27] DJI, “AeroScope,” DJI Official. https://www.dji.com/pl/aeroscope
[28] D Fend Solutions, “Counter Drone Technology,” D-Fend Solutions. https://d-fendsolutions.com/ (accessed May 02, 2023).
[29] Rheinmetall, “Air defence systems,” Rheinmetall. https://www.rheinmetall.com/en/products/air-defence/air-defence-systems (accessed May 02, 2023).