The Role and Limitations of Counter-Drone Systems in Smart Cities

Slaviša Sovilj, MSc
Banja Luka, Bosnia and Herzegovina
slavisa.sovilj@proton.me

***Abstract*—In recent years, unmanned aerial vehicles (UAVs) have experienced significant growth in use across both military and civilian sectors due to their low production costs and wide range of applications. With the increase in UAV usage in the civilian sector, concerns arise regarding the safety of citizens in urban environments, where malicious use or unintentional handling errors of UAVs can lead to serious incidents. In response to this threat, counter-drone systems are being developed to protect against potentially dangerous UAVs. Like UAVs themselves, counter-drone systems were primarily developed for military operations, but recently there has been a need for their deployment in the civilian sector, particularly in urban areas. This paper provides a review of the literature, technologies and legal frameworks related to counter-drone systems, analyzes the specificities of their use in smart cities, identifies potential challenges in their implementation in urban environments, and proposes solutions to address these challenges. The conclusions indicate that the successful implementation of C-UAS systems in smart cities requires coordinated technical integration, alignment of the legal and regulatory framework, and strengthening of institutional and operational capacities.**

Keywords—counter-drone protection, smart cities, unmanned aerial vehicles, security

I. Introduction

Unmanned Aerial Vehicles (UAVs), commonly known as drones, are aircraft that are either autonomously operated by a computer or remotely controlled by a human operator [21]. The term Unmanned Aerial System (UAS) is broader than UAV and includes associated elements, such as communication links and other components that are necessary for the pilot to safely and effectively control the UAV [36]. Drone operation refers to the control and execution of activities using a UAS within defined missions, including flight planning, takeoff, navigation, task execution, return, and landing. This may involve manual control by a remote pilot, semi-autonomous or fully autonomous flights [15]. The Unmanned Traffic Management (UTM) system is a conceptual framework for drone operations, developed to manage UAVs in low-altitude airspace without the need for conventional air traffic control [41]. UAS is used in numerous socially beneficial areas, such as traffic control, infrastructure and environmental surveillance, delivery of goods, terrain mapping, public safety improvement, and search and rescue operations [1][2]. Simultaneously with the increased use of drones in socially beneficial activities, there is a growing number of challenges related to security, privacy, and the regulation of drone usage in smart city environments [3][4]. Drones can be used for malicious activities such as espionage, unauthorized recording, air traffic disruption, causing unintentional incidents, and even for carrying out terrorist attacks or other forms of threats to public order, property, and the lives of citizens [5][6]. This leads to the need for developing counter-drone protection systems aimed at detecting, tracking and neutralizing potentially dangerous drones [8]. On the other hand, a Counter Unmanned Aircraft System (C-UAS) is a system or device capable of legally and safely detecting, tracking, identifying, disabling, jamming or taking control of an unmanned aerial vehicle or a system of unmanned aerial vehicles [36]. The concept of a smart city refers to the integration of information and communication technologies (ICT), sensor networks, the Internet of Things (IoT), and data analytics in order to improve urban resource management, optimize traffic, enhance security and improve the quality of life for citizens [5]. The security of low-altitude airspace is becoming increasingly important due to the rise in drone usage in urban areas, which creates new risks for public safety and critical infrastructure [3]. It is necessary to develop technological, legal, and organizational mechanisms that will enable timely detection and neutralization of these threats within the complex urban environment [7]. The aim of this paper is to analyze the technical, legal, and organizational challenges of implementing counter-drone systems (C-UAS) in urban environments and to offer recommendations for their integration into smart cities. Following the introduction, the paper is structured as follows. Section II outlines the research methodology, Section III reviews relevant literature, and Section IV discusses legal frameworks for the use of UAS. Section V covers the societal perception of C-UAS, Section VI examines the technical aspects of C-UAS implementation, while Section VII focuses on the operational use of C-UAS. Section VIII identifies implementation challenges, and Section IX offers recommendations for C-UAS integration. The final section, Section X, contains the concluding remarks.

II. Research Methodology

This paper uses a qualitative descriptive approach based on a systematic review of relevant scientific and professional literature. Sources were selected based on their scientific credibility, relevance to the topic of C-UAS systems, availability through reputable academic databases, and temporal relevance, with a focus on modern technologies and urban applications. It also considers reports from regulatory bodies and international initiatives involved in the standardization and evaluation of counter-drone systems. The analysis was conducted by combining comparative and analytical methods, with the aim of identifying technical, legal, and organizational challenges.

III. Literature Review

Literature on counter-drone protection in smart cities emphasizes that effective detection and neutralization of UAV threats is closely linked to the complexity of the urban environment and the technological limitations of existing systems [8][13]. Most commercially available C-UAS solutions are not optimally designed for high-density urban environments, where multiple RF signal reflections and obstructed lines of sight significantly reduce the effectiveness of radar and RF detection systems [8]. Particular attention is given to multisensory strategies, where the combination of radar sensors, acoustic detectors, electro-optical cameras, and RF scanners achieves greater reliability in detecting and identifying UAV threats within the complex electromagnetic environment of cities [9][14]. Additionally, the growing importance of machine learning and artificial intelligence is emphasized in the implementation of algorithms for UAV flight pattern detection, tracking, and recognition, as well as and threat classification based on the fusion of data from different sensors [11]. When it comes to drone neutralization, it is emphasized that although RF jamming and spoofing remain the most common methods, kinetic interception techniques – such as interceptor drones or net projectiles – are gaining increasing attention in both academic and industrial communities, especially for scenarios where electronic jamming is prohibited by regulations [9]. The classification of operational measures and technologies in defensive scenarios during incident situations is presented in [35]. Special attention is drawn to the security vulnerabilities of C-UAS systems themselves, emphasizing the need to protect them from cyberattacks, false alarms, and sensor spoofing attacks, which could threaten the entire smart city security system [7]. From a legal perspective, although the EU has clear guidelines for UAV/UAS operations, the legal framework for the implementation of C-UAS technologies in civilian urban environments remains insufficiently regulated. For this reason, many European authors emphasize the need for transnational harmonization of legal norms and ethical standards [4][10][15]. A comprehensive review of the literature shows that the development and implementation of counter-drone protection in urban environments requires an integrated approach, which, in addition to technological innovations, also implies the establishment of clear legal and ethical frameworks. This would ensure the safe and lawful use of counter-drone systems within smart cities [8][15].

IV. Legal Framework for UAS Usage

The regulation of UAV usage in the European Union is based on Regulations (EU) 2019/947 and 2019/945, adopted by the European Aviation Safety Agency (EASA) [16]. These acts provide the foundation for the development of the UTM framework, whose functionalities include: registration of drones and operators, dynamic airspace management (geofencing, no-fly zones), real-time mission planning and authorization, aircraft tracking, and information sharing. EASA regulations define three categories of flights: open, specific, and certified [16]. The open category includes flights of small UAVs, up to 25 kg, within the Visual Line of Sight (VLOS) and at a maximum altitude of 120 meters, without the need for special authorization, but with mandatory online pilot training [16]. The specific category requires operational authorizations based on a SORA (Specific Operations Risk Assessment) for more complex missions, such as Beyond Visual Line of Sight (BVLOS) flights or operations in urban environments [16]. The certified category covers high-risk operations similar to conventional aviation, such as the transport of people or hazardous materials. Croatia, as an EU member state, has fully implemented EASA regulations since 2021, including the mandatory registration of UAVs over 250 g and pilot training requirements [10][16]. Serbia regulates UAV operations through the Rulebook on Unmanned Aerial Vehicles from 2015, which allows VLOS flights for UAVs up to 0.9 kg without special authorization. However, BVLOS operations are not permitted for civilian operators, and harmonization with EASA standards is planned but has not yet been completed [17]. In Bosnia and Herzegovina, the Bosnia and Herzegovina Directorate of Civil Aviation (BHDCA) adopted the Rulebook on the Requirements for Aerial Drone Operations in 2020, which is based on the EASA framework. However, its implementation is limited due to country’s non-membership in EASA, and requires special approvals for BVLOS operations [18]. Montenegro regulates UAV operations through a national rulebook issued by the Civil Aviation Agency, with plans to harmonize with EASA regulations, while BVLOS flights are permitted only with the approval of the Ministry of Defense [19]. North Macedonia applies national regulations currently in the process of alignment with EU standards, but BVLOS operations have not yet been formally defined [20]. Although EASA regulates UAV operations [16], the use of C-UAS technologies, such as RF jamming or GPS spoofing, falls under the jurisdiction of national laws on electronic communications and security, and is generally prohibited for civilian use due to the potential interference with licensed frequencies and GPS systems [16]. In the Western Balkan countries, there is no civil legal framework for the implementation of C-UAS technologies, and their application remains limited exclusively to military and police-security structures [17][18].

V. Societal perception of C-UAS

The use of counter-drone systems in urban areas raises privacy and civil liberties concerns. Professional organizations emphasize the need for the deployment of C-UAS technologies to be clearly regulated, subject to democratic oversight, and limited to the least intrusive neutralization methods. It is recommended to establish transparent procedures, publicly accessible reports on system usage, and legal protection mechanisms for citizens [54]. Empirical research indicates that public support grows when C-UAS measures are justified by national security and approved by the relevant authorities, while it declines if there is a risk of negative impact on civilians or critical infrastructure [55]. Incorporating these principles can significantly enhance the acceptance of the technology among the population.

VI. Technical Aspects of C-UAS

Counter-drone systems represent a set of technologies divided into two components: 1) detection, tracking, and identification (DTI), and 2) drone neutralization. An effective C-UAS system should be capable of: 1) autonomously detecting drones operating in the vicinity of the system, 2) locating and identifying threats, 3) distinguishing potentially dangerous drones from friendly ones, 4) providing operators with a visual overview of detected drone locations, 5) issuing alerts and warnings to authorized personnel, and 6) taking neutralization measures, either automatically or under operator control [34]. To detect drones, C-UAS systems use both active and passive sensor solutions [8]. Active sensor solutions emit electromagnetic or laser pulses, receive the reflected signals, analyze them, and extract data on potential drones. Passive sensor solutions receive existing electromagnetic radiation or acoustic waves emitted by

UAVs, which they use for object detection and tracking. Examples of active sensor solutions include active radars and laser-based technologies, while passive solutions include RF detectors, optical and infrared cameras, and acoustic receivers [22][23]. Radar technologies can detect large and medium-sized drones at greater distances and do not depend on the drone's RF emissions. However, their limitation lies in the inability to detect small and low-flying UAVs, as well as their susceptibility to false alarms [32]. RF sensors are effective for detecting UAVs that emit RF signals and are excellent at detecting operator-controlled drones, but they cannot detect autonomous drones. They are also limited to the frequency ranges they can cover and may be disrupted by other sources or reflections of electromagnetic radiation [42]. Acoustic detectors offer practically no advantages in urban environments – their short range and reduced effectiveness in noisy conditions or weather conditions that mask UAV sound make them unusable in urban environments. Optical sensors provide good detection capabilities but only where there is a direct line of sight and favorable weather conditions. Infrared detectors are effective at night and in low-visibility conditions but are not efficient for detecting small drones, especially in high-temperature or adverse weather conditions [26][36]. Given the limitations of individual sensor types, a C-UAS solution that relies solely on one type of sensor would be significantly limited in its surveillance capabilities [36]. Sensor fusion is an approach that integrates multiple types of sensors to improve the overall accuracy of the DTI process. The main challenges in implementing sensor fusion solutions include sensor heterogeneity, synchronization of data collection timing, and handling the large amount, variety, speed, and reliability of multimodal data, which often have complex inter-correlations [32]. According to [36], which analyzed 260 C-UAS systems available on the market, the following data were obtained: Systems using a single technology in the DTI process account for 53% of all counter-drone solutions and typically rely on one detection method – most commonly frequency monitoring or radar-based detection**.** Systems integrating two technologies make up 9%, while those using three technologies account for 15%. Solutions that incorporate four or more technologies represent 23% of the solutions, combining radars, cameras, RF monitoring**,** and additional sensors. This trend toward multi-technology systems highlights the need for robust data fusion methodologies to effectively reduce the number of false positive and false negative detections [38]. The collected sensor data needs to be processed, where AI and machine learning can play a significant role. Deep learning models, such as Convolutional Neural Networks (CNNs), can automatically extract features from raw data, enabling accurate classification of drones based on their visual, thermal, acoustic, or radio frequency signatures [24][25][33]. Drone identification can also be performed through Remote ID UAV, which serves as a 'digital license plate' for drones, which enables the drone to broadcast basic information during flight, allowing identification through its registration number, the drone's location (latitude, longitude, altitude), the location of the control station (pilot), the altitude and speed of the drone, as well as time, and system status data. According to [16], this feature is mandatory for all drones operating in public airspace, except for those in controlled zones or exempt categories. Drone neutralization is accomplished by destructive and non-destructive methods [22]. Non-destructive methods include RF jamming [33], GPS spoofing [29], and drone takeover [28], while destructive methods involve the use of lasers [27], interception drone swarms [43], and counter-drone systems that use counter-UAV munitions to neutralize drones. Drones controlled via remote controllers typically operate within specific radio frequency bands, most commonly at 2.4 GHz and 5.8 GHz. RF jamming works by emitting pulsed or continuous signals on these frequencies, with enough power to disrupt or block communication between the UAV and its controller [8]. If communication is successfully interrupted, the drone's behavior afterward depends on its configuration [27]. There are three options commonly implemented in commercial drones: 1) return-to-home (RTH) – the drone automatically returns to the location where the flight began or to a pre-defined point, 2) hover - the drone remains hovering at the point where the signal was lost and, after some time, either descends or returns to the starting position (RTH scenario), 3) landing - the drone automatically initiates landing after communication with the controller is lost [52]. GPS jamming operates identically to RF jamming but targets the 1.5 GHz frequency band, which drones use to communicate with the GPS satellite network [8]. If communication with the GPS network is disrupted, the UAV enters hover mode or immediately lands [53]. Cyberattacks, as a neutralization method, aim to take control of the drone, and the target of the attack is the communication link between the drone and its controller or the drone’s control software with the goal of disrupting its functionality. Some examples of cyberattacks include malware injection, aimed at introducing and executing malicious software to take control of or disrupt the UAV operation; denial of service attacks, which overload the UAV's communication channels; and man-in-the-middle attacks, which intercept communication and alter instructions sent from the controller [43]. Destructive neutralization methods involve physically removing drones from the airspace using nets or projectiles. There are also directed weapons, such as lasers or microwave emitters, which focus electromagnetic energy to destroy drones [44]. Techniques under development include kinetic removal of drones using drone swarms. These swarms are controlled by AI algorithms that make real-time decisions on neutralization [43]. Finally, it can be said that the use of non-destructive C-UAS methods is more acceptable in urban and civilian environments due to the reduced risk to people, property and the environment. On the other hand, destructive methods, which involve physically disabling drones, are mainly reserved for military operations and the protection of critical infrastructure where higher levels of force application are considered acceptable [41].

VII. Analysis of Operational Uses of C-UAS

C-UAS systems, depending on their mode of application, can be classified as stationary and mobile. Stationary C-UAS systems are typically permanently installed near critical infrastructure (such as airports, power plants, government buildings), and consist of spatially distributed sensor modules (radars, optical sensors, RF scanners, acoustic receivers) connected to a central command and control center (C2). These systems allow for continuous monitoring, data processing, and automatic initiation of neutralization procedures [41]. Mobile C-UAS systems represent a more flexible approach and are suitable for ad-hoc deployment or protection during high-risk events (e.g., political gatherings, sports events). These systems can essentially be divided into two categories: (1) handheld, used directly by operators in the field, and (2) integrated, installed on specialized vehicles. Handheld systems include: drone jammers that disrupt the communication between the drone and its operator or the GNSS signal, forcing the UAV to land or return [35]; counter-drone networks – handheld or drone-launched net systems that physically intercept the UAV and bring it down safely [45]; portable detection devices, such as RF scanners and acoustic sensors, which allow for the rapid localization of drones within the immediate vicinity [4]. Integrated mobile C-UAS systems, mounted on specialized vehicles (e.g., police, military or civil protection vehicles), contain complete C-UAS platforms that include: radar sensors for initial detection, RF detectors for identifying the command link, electro-optical/infrared cameras for visual target confirmation, and neutralization tools such as RF jammers and kinetic network systems [6]. Due to their high degree of mobility and rapid deployment capabilities, such systems can be relocated in real time to locations with increased security risks – such as large public gatherings, transport of high-risk shipments, VIP protection, or the safeguarding of temporary critical infrastructure [47]. Their key advantage lies in the ability to integrate with the city's broader smart sensor grid through wireless communication networks or 5G infrastructure [48]. The introduction of advanced AI algorithms for real-time threat analysis further improves the effectiveness of these systems, especially in complex urban environments where multiple sources of interference and signal reflection pose significant challenges for conventional sensors [49]. C-UAS deployment timing refers to the continuity and duration of system use to protect a specific asset or area and, it can be ether constant or intermittent [22]. Constant deployment is applied for protecting critical infrastructure such as airports, military bases, etc., while intermittent deployment activates the system during certain periods of heightened risk, such as public gatherings, concerts, etc. [22]. Over a broader geographical area, C-UAS systems can be designed as multi-layered architectures with a distributed network of sensors, where: the first layer includes radars and RF detectors for initial detection; the second layer consists of EO/IR cameras and RF fingerprinting modules for classification; and the third layer comprises neutralization modules, including RF jammers, GNSS spoofing, and kinetic measures as the final line of defense [32][35].

VIII. Challenges of C-UAS Implementation in Urban Environments

The application of C-UAS systems in smart cities faces numerous obstacles and difficulties, which can be categorized into: 1) technical risks, including limitations in detection, tracking, and neutralization capabilities; 2) operational risks, referring to the challenges of deploying counter-drone systems in urban and contested environments; and 3) strategic risks, related to political, regulatory, and legal issues that impact the effectiveness of counter-drone solutions [36].

Technical interference in the electromagnetic spectrum represents a serious obstacle to the effective operation of C-UAS in urban environments. These interferences typically originate from numerous sources such as mobile networks, Wi-Fi routers, radio and TV transmitters, industrial equipment, as well as electrical systems in buildings and vehicles. In such environments, frequency overlap, signal reflection and absorption occur, which directly impacts sensor reliability. For detection, tracking and identification (DTI), this results in reduced accuracy of RF detectors and radars, an increased number of false positive detections and greater difficulty in object classification. In the neutralization phase, especially when RF or GPS jammers are used, such interference can lead to unintended effects – including interference with legal systems and failure to take control of the UAV [40]. The lack of clearly defined legal regulations for conducting C-UAS activities is an equally significant issue. Currently, C-UAS operations can mostly be carried out only by state security agencies or military structures. This significantly limits the ability of protecting critical infrastructure and urban areas from potentially dangerous drones, as private operators and local authorities do not have legal authorization to detect or neutralize unmanned aerial vehicles [2]. The selection and application of appropriate methods for detection, identification, and neutralization of UAVs in urban environments often face mutual technical and legal contradictions. Electronic neutralization methods, such as RF jamming or GPS spoofing, although effective, can interfere with legitimate communication systems without authorization, thereby potentially compromising public safety and violating electronic communications laws [35]. On the other hand, kinetic interception methods, such as projectiles, nets, or lasers, carry a significant risk of physical damage to infrastructure, vehicles, and people, especially in densely populated urban areas. Due to these challenges, the choice of neutralization strategy must be carefully aligned with the characteristics of the environment, applicable regulations, and an acceptable level of operational risk [36]. The lack of such regulations leads to legal uncertainty in cases of drone intervention and potential liability for damage caused to third parties or disruption of communication systems in the city [4]. From an organizational standpoint, the following shortcomings have been identified, the resolution of which could significantly improve protection against potentially dangerous UAVs: 1) there is no centralized system for reporting UAV-related incidents in EU member states; 2) there is no standardized format for incident reporting; 3) information about UAS operators and their intentions must be recorded in centralized systems; 4) there is a lack of information about the technical characteristics of UAS operating in the airspace [41].

IX. Recommendations for C-UAS Implementation

Considering the previously outlined limitations and risks, it can be concluded that the implementation of C-UAS systems in smart cities must be approached in a planned, systematic, and interdisciplinary manner. A structured risk assessment framework is essential for systematically evaluating the likelihood of UAS threats in a specific area. The Specific Operations Risk Assessment (SORA) methodology is frequently used to analyze these risks, offering a step-by-step approach for assessing operational safety and mitigation strategies [46]. Despite the availability of numerous counter-drone solutions on the market [46–48], there are still no widely accepted and operationalized methods for evaluating their performance. This lack of effectiveness hinders the efforts of government agencies, security services, and local authorities in the process of selection, certification and integration of appropriate C-UAS systems. The COURAGEOUS project [39] represents a significant step toward establishing common standards through the development of the pre-standard document CWA 18150 [41], which provides a methodological framework for evaluating counter-drone technologies in real-world conditions. In addition to technical aspects, regulatory harmonization is also essential. Current efforts to define drone no-fly zones in urban areas – including perimeters around critical infrastructure, roads, public gatherings, and airports –

represent an important step in improving security and enabling effective C-UAS integration [34]. In the context of smart cities, proactive airspace planning is recommended, including the establishment of UAV corridors and virtual highways, with mandatory mapping of security-sensitive zones [37]. These elements should become an integral part of urban and technological development strategies for smart infrastructure. It is particularly important to integrate C-UAS into existing security and communication architectures of smart cities, including IoT sensor networks, traffic control centers, and emergency services. To achieve this, it is necessary to develop standardized communication and data exchange protocols between C-UAS and other urban security systems [40]. Protocols must comply with national regulations and international standards, particularly concerning privacy protection, RF spectrum usage, and liability in the event of system activation. In addition to technical and regulatory aspects, attention must also be given to organizational and institutional coordination. Local governments and civil authorities must have clearly defined responsibilities and procedures for responding to UAV threats, including personnel training and cooperation with state security authorities [35]. The integration of UTM and C-UAS systems is of vital importance. Although these systems serve fundamentally different purposes – UTM enables regulated and legal operations of unmanned aerial vehicles, while C-UAS provides protection against threats posed by unauthorized or malicious flights – their complementarity is crucial for achieving safe and efficient management of low-altitude airspace in complex urban environments. UTM systems have a primarily preventive role, allowing UAS system operators to plan and register their flights via official digital platforms. This enables the pre-definition of flight corridors, operational altitudes, and mission timing. In contrast, C-UAS systems operate reactively, i.e., they act only after a potentially unauthorized flight is detected in order to identify, track and, if necessary, neutralize it [49][22]. Data exchange between UTM and C-UAS systems enables counter-drone protection systems to effectively distinguish between legally registered unmanned aerial vehicles and potentially threatening ones [50]. Integration with UTM databases can serve as a means of real-time drone identity authentication, thereby preventing errors and unnecessary interventions [50]. Both systems can be technically integrated into a unified smart city architecture, particularly through command-and-control centers and IoT infrastructure. For example, the UTM system can automatically generate an alert in case of a restricted zone violation, while the C-UAS system, in coordination with operators, can initiate appropriate countermeasures – either automatically or with human oversight and confirmation [50]. This type of integration not only increases security but also contributes to a more rational use of urban airspace, reducing conflicts and raising the level of public trust in the digital infrastructure of smart cities [51].

Ultimately, the successful implementation of C-UAS systems also depends on transparency and public awareness, in order to avoid unnecessary public concern and to ensure the social acceptance of new technologies in urban environments.

X. Conclusion

This paper examines counter-drone (C-UAS) systems in smart cities, focusing on their technical, regulatory, and organizational implementation. It analyzes key technologies for the detection and neutralization of UAV threats, legal frameworks in the EU and Western Balkans, revealing significant obstacles to civilian use. Models of stationary and mobile application are presented, as well as the need for integration with IoT and UTM systems. It is concluded that the successful deployment of C-UAS systems requires an interdisciplinary approach that combines technical interoperability, legal clarity, and local coordination. Future research should focus on standardizing C-UAS testing, examining public acceptance and privacy concerns, improving model integration with UTM systems, and gathering practitioner insights to validate theoretical findings.

References

[1] N. Abbas, Z. Abbas, X. Liu, S. S. Khan, E. D. Foster, and S. Larkin, “A Survey: Future Smart Cities Based on Advance Control of Unmanned Aerial Vehicles (UAVs)” *Appl. Sci.*, vol. 13, no. 17, Art. 9881, Aug. 2023.

[2] Outay, F., Mengash, H. A., & Adnan, M. “Applications of unmanned aerial vehicle (UAV) in road safety, traffic monitoring and highway infrastructure management: Recent advances and challenges”, *Transportation Research Part A: Policy and Practice*, 141, 116–129, 2020.

[3] S. Mekdad, H. Chaouchi, and F. Kamoun, “A survey on security and privacy issues of UAVs” *Computer Networks*, vol. 197, p. 108265, Sep. 2021.

[4] E. Bassi, “European Drones Regulation: Today’s Legal Challenges” in *Proc. Int. Conf. Unmanned Aircraft Systems (ICUAS)*, 2019. [Online]. Available: https://www.researchgate.net/publication/335196069_European_Drones_Regulation_Today’s_Legal_Challenges

[5] J. Finn and S. Wright, “Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications” *Computer Law & Security Review*, vol. 28, no. 2, pp. 184–194, Apr. 2012.

[6] Y. Zeng, R. Zhang, and T. J. Lim, “Wireless communications with unmanned aerial vehicles: Opportunities and challenges” *IEEE Communications Magazine*, vol. 54, no. 5, pp. 36–42, May 2016.

[7] Mekdad, Y., Aris, A., Babun, L., EL Fergougui, A., Conti, M., Lazzeretti, R., & Uluagac, A. S. “A survey on security and privacy issues of UAVs”, *Computer Networks*, 224, Article 109626, 2023.

[8] Park, S., Kim, H. T., Lee, S., Joo, H., & Kim, H. “*Survey on Anti-Drone Systems: Components, Designs, and Challenges*”, IEEE Access, 9, 42635–42659, 2021.

[9] Castrillo, V. U., Manco, A., Pascarella, D., & Gigante, G. “Review of Counter-UAV Technologies for Cooperative Defense against UAV Threats”, *Drones*, 6(3), 65. European Union Aviation Safety Agency, “Drone Incident Management at Aerodromes”, 2022.

[10] European Union Aviation Safety Agency, “Drone Incident Management at Aerodromes”, 2022. [Online]. Available: https://www.easa.europa.eu/en/domains/civil-drones-rpas

[11] Shakhatreh, H., Sawalmeh, A. H., Al-Fuqaha, A., Dou, Z., Almaita, E., Khalil, I., Othman, N. S., Khreishah, A., & Guizani, M. “Unmanned Aerial Vehicles (UAVs): A Survey on Civil Applications and Key Research Challenges. *IEEE Access*, 7, 48572–48634, 2019.

[12] Mohammed A. Al-Garadi, Amr Mohamed, Abdullatif Rabah, Aiman Erbad, Ala Al-Fuqaha, and Mounir Frikha,“The Role of Unmanned Aerial Vehicles (UAVs) in Smart Cities: Network Architecture, Enabling Technologies, and Applications”, IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10288–10312, Oct. 2020.

[13] C. Mulder, A. A. Bouma, J. Ligthart, and H. A. D. de Jong, “Detection and classification of small UAVs in urban environments using radar”, *IET Radar, Sonar & Navigation*, vol. 12, no. 10, pp. 1221–1227, 2018.

[14] F. Corman, M. Hürlimann, D. Reider, and M. De Martinis, “The role of multi-sensor systems for drone detection in urban environments”, *Transportation Research Procedia*, vol. 47, pp. 439–446, 2020.

[15] European Union Aviation Safety Agency (EASA), “*Easy Access Rules for Unmanned Aircraft Systems (Regulation (EU) 2019/947)* “, Issue 5, 2022. [Online]. Available: https://www.easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems-regulation-eu

[16] European Union Aviation Safety Agency, “*Easy Access Rules for Unmanned Aircraft Systems (Regulations (EU) 2019/947 and*

2019/945)“, 2023. [Online]. Available: https://www.easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems-regulations-eu

[17] Directorate of Civil Aviation of the Republic of Serbia “*Regulation on Unmanned Aerial Vehicles* (Official Gazette of the Republic of Serbia, No. 1/20), in force since Feb. 2020. [Online]. Available: https://cad.gov.rs/upload/propisi/2020/Pravilnik%20o%20bespilotnim%20vazduhoplovima.pdf

[18] Bosnia and Herzegovina Directorate of Civil Aviation, “*Rulebook on the Requirements for Aerial Drone Operations* (Official Gazette of BiH, no. 51/20), 25 Sept. 2020. [Online]. Available on the Directorate’s website: https://www.bhdca.gov.ba (search term: “drone”)

[19] Civil Aviation Agency of Montenegro, “*UAV regulations*, 2020. [Online]. Available: https://www.caa.me

[20] Civil Aviation Agency of North Macedonia, “*Regulation on Unmanned Aircraft* (Official Gazette of the Republic of North Macedonia, No. 115/2024), [Online]. Available: https://www.caa.gov.mk/wp-content/uploads/2024/08/2.9-Regulation-on-unmanned-aircraft-115.24-ENG.pdf

[21] M. R. Hassanalian and A. Abdelkefi, “Classifications, applications, and design challenges of drones: A review” Progress in Aerospace Sciences, 2017.

[22] 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, str. 42635–42659, mart 2021.

[23] B. Liu, X. Zhang, Y. Wang and Z. Han,“Micro-UAV Detection With a Low-Cost FMCW Radar”, *IEEE Sensors Journal*, vol. 16, br. 18, str. 7202–7209, 2016.

[24] M. Al-Sa’d, M. Selim, M. Abdelhakim, A. Khreishah, and B. Hamdaoui, “Radio frequency fingerprinting based on deep learning for drone identification” *IEEE Access*, vol. 7, pp. 54205–54215, 2019.

[25] A. Saeed, M. M. Hayat, H. Malik, and H. Jung, “Detection and Classification of Multirotor UAVs Using Deep Learning and Computer Vision” IEEE Access, vol. 9, pp. 24344–24356, 2021.

[26] H. Roh and S. Kim, “Drone detection and identification system using acoustic camera” Applied Sciences, vol. 10, no. 17, pp. 6079, 2020

[27] C. Gentili, R. De Rosa, M. T. Frasca and L. Puglia, “Anti-Drone Systems: A Review” *Drones*, vol. 6, br. 2, str. 1–26, 2022.

[28] M. Donatti, F. Frazatto, L. Manera, T. Teramoto, and E. Neger, “Radio frequency spoofing system to take over law-breaking drones” in IEEE MTT-S International Microwave Symposium Digest, Dec. 2016.

[29] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys,“Unmanned Aircraft Capture and Control via GPS Spoofing,” Proceedings of the 6th USENIX Workshop on Offensive Technologies (WOOT ’12), Washington, D.C., USA, pp. 1–9, Aug. 2012.

[30] P. Pratyusha and V. Naidu, “Geo-fencing for unmanned aerial vehicle,” Int. J. Comput. Appl., vol. 975, p. 8887, Jan. 2013. [112] OpenWorks Engineering. SKYWALL PATROL—OpenWorks Engineering. [Online]. Available: https://openworksengineering.com/skywall-patrol/

[31] Seidaliyeva, U., Ilipbayeva, L., Taissariyeva, K., Smailov, N., & Matson, E. T., “Advances and Challenges in Drone Detection and Classification Techniques: A State-of-the-Art Review Sensors“, 24(1), 2024.

[32] Wang, J., Liu, Y., & Song, H., “Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges, and Future Trends“, IEEE Aerospace and Electronic Systems Magazine, 36(3), 4–29, 2021.

[33] Hemant Sirohi, C.N. Khairnar, Pramod Kumar, and Abhay Kumar, "A Comprehensive Review of Modern Counter-Drone Technologies: Trends, Challenges, and Future Directions", International Journal for Research in Applied Science & Engineering Technology (IJRASET), vol. 12, no. V, pp. 4405-4418, May 2024.

[34] J. Snead, J.-M. Seibler, and D. Inserra, “Establishing a Legal Framework for Counter-Drone Technologies” *The Heritage Foundation*, Backgrounder No. 3305, 16 Apr. 2018.

[35] G. Lykou, D. Moustakas, and D. Gritzalis, “Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies” Sensors, vol. 20, no. 12, p. 3537, 2020.

[36] CEN Workshop Agreement—CWA 18150—Unmanned Aircraft Systems—Counter UAS—Testing Methodology. European Standardization Committee. 2024. Available online: https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa-18150.pdf

[37] N. S. Labib, G. Danoy, J. Musial, M. R. Brust, and P. Bouvry, “A Multilayer Low-Altitude Airspace Model for UAV Traffic Management,” in *Proc. 9th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications (DIVANet@MSWiM ’19)*, Miami Beach, FL, USA, Nov. 25–29, 2019, pp. 57–63.

[38] Brewczynski, K.D.; Zyczkowski, M.; Cichulski, K.; Kaminski, K.A.; Petsioti, P.; De Cubber, G., “Methods for Assessing the ˙Effectiveness of Modern Counter Unmanned Aircraft Systems", Remote Sens. 2024, 16, 3714.

[39] De Cubber, G.; Petsioti, P.; Roman, R.; Mohamoud, A.; Maza, I.; Church, C. The COURAGEOUS Project Efforts Towards Standardized Test Methods for Assessing the Performance of Counter-Drone Solutions. In Proceedings of the 11th Biennial Symposium on Non-Lethal Weapons, Brussels, Belgium, 22 - 25 May 2023; p. 44

[40] Kang, H.; Joung, J.; Kim, J.Y.; Kang, J.; Cho, Y.S., “Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems",IEEE Access, 8, 168671–168710, 2020.

[41] González-Jorge, H.; Aldao, E.; Fontenla-Carrera, G.; Veiga-López, F.; Balvís, E.; Ríos-Otero, E., “Counter Drone Technology: A Review", Preprints, 2024.

[42] Sirohi, H.S.; Khairnar, C.N.; Kumar, P.; Kumar, A.,“A Comprehensive Review of Modern Counter-Drone Technologies: Trends, Challenges, and Future Directions", Int. J. Sci. Technol. Eng. 2024, 12, 4405–4418.

[43] M. R. Brust, G. Danoy, D. H. Stolz, and P. Bouvry, “Swarm-based counter UAV defense system” Discover Internet of Things, vol. 1, no. 2, pp. 1–21, 2021.

[44] G. C. Birch, J. C. Griffin, and M. K. Erdman, “UAS Detection, Classification, and Neutralization: Market Survey 2015” Sandia National Laboratories, SAND2015-6365, 2015.

[45] Delft Dynamics,"DroneCatcher: A Net Gun Armed Drone to Physically Remove Illicit Drones from the Sky", URL: https://www.delftdynamics.nl

[46] European Union Aviation Safety Agency, *“Specific Operations Risk Assessment (SORA)*",EASA Acceptable Means of Compliance (AMC1) to Article 11 of Regulation (EU) 2019/947, Dec. 2020 (rev. July 2024).

[47] V. U. Castrillo, A. Manco, D. Pascarella, and G. Gigante, “A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones”, *Drones*, vol. 6, no. 3, Art. 65, Mar. 2022.

[48] Q. Wu, J. Xu, Y. Zeng, D. W. K. Ng, N. Al-Dhahir, R. Schober, and A. L. Swindlehurst,“A Comprehensive Overview on 5G-and-Beyond Networks With UAVs: From Communications to Sensing and Intelligence” , *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 10, pp. 2912–2945, Oct. 2021.

[49] DroneShield, “SensorFusionAI – Sensor Fusion for Counter-UAS,” *DroneShield Official Website*. [Online]. Available: https://www.droneshield.com/capabilities/sensor-fusion-ai

[50] M. Abdulhadi, R. Shoufan and R. Alkadi, "Integrating Counter-UAS Systems into the UTM System for Reliable Decision Making", Nov. 2021.

[51] N. Wang, N. Mutzner, K. Blanchet, “Societal Acceptance of Urban Use of Drones: A Scoping Literature Review” *Technology in Society*, vol. 75, 2023, art. 102377.

[52] DJI Technical Manual – AGRAS T10 (2021)

[53] T. Ma, X. Zhang, and Z. Miao, "Detection of UAV GPS Spoofing Attacks Using a Stacked Ensemble Method", *Drones*, vol. 9, no. 1, Art. no. 2, Dec. 2024.

[54] Electronic Privacy Information Center (EPIC), “EPIC Coalition Urge Congress to Include Privacy and Civil Liberties Protections in Any Future Counter-Drone Authority Legislation,” 2024. [Online]. Available: https://epic.org/epic-coalition-urge-congress-to-include-privacy-and-civil-liberties-protections-in-any-future-counter-drone-authority-legislation/

[55] C-UAS Hub, “Defending America’s Skies: Public Support for Homeland Counter-Drone Operations,” 2023. [Online]. Available: https://cuashub.com/en/content/defending-americas-skies-public-support-for-homeland-counter-drone-operations/