The American Journal of Engineering and Technology
ISSN 2689-0984 | Open Access

TYPE Original Research
PAGE NO. 41-53
DOI 10.37547/tajet/Volume07Issue01-07

Global analysis of active defense technologies for unmanned aerial vehicle

Koushik Bandapadya

Westcliff University Masters in Computer Science (MSCS) Concentration: Software Development

Md. Nurunnabi sarker

Masters in Computer Science (MSCS) Concentration: Data Analysis Westcliff University

Areyfin Mohammed Yoshi

MBA in Business Analytics International American University Los Angeles, California

Ashrafuzzaman Hera

Master of Business Administration in Management Information Systems, International American University, Los Angeles, California. United States

Md Omar Faruque

Master of Business Administration in Management Information Systems, International American University, Los Angeles, California. United States

OPEN ACCESS

SUBMITED 20 October 2024
ACCEPTED 30 December 2024
PUBLISHED 30 January 2025
VOLUME Vol.07 Issue01 2025

CITATION

Koushik Bandapadya, Md. Nurunnabi sarker, Areyfin Mohammed Yoshi, Ashrafuzzaman Hera, & Md Omar Faruque. (2025). Global analysis of active defense technologies for unmanned aerial vehicle . The American Journal of Engineering and Technology, 7(01), 41–53.
https://doi.org/10.37547/tajet/Volume07Issue01-07

Abstract: This paper explores active defense for UAVs globally, with the main emphasis on detection and countermeasure technologies. Questionnaires were administered to 139 individuals in the USA, and the results were analyzed with the help of the Statistic Package for Social Sciences (SPSS), including reliability analysis, descriptive frequency, and regression analysis. The results concerning Hypothesis 1 concerning technological detection impact on the adequacy of UAV defense are the following. Analyzing the data, it was established that detection technology influences UAV defense significantly with F =12. 27 and a signification p, therefore, is less than 0,001. Total regression analysis showed that In relation to this aspect, the regression coefficient (b = 0. 292, p <. 001) shows that detection technology has a positive influence on UAV defense and accounts for 8. Two percent of the total aggregated variation across the defense effectiveness of the participating countries (R^2 = 0. 082) could solely be attributed to these potentates. Thus, the findings of

Hypothesis 2 prove that countermeasure technology also plays another major role in the defense of UAVs. Analysis of variance for the model revealed that technology used in countermeasures tremendously impacts UAV defense with F = 113. 465, and the calculated p is less than 0. 000; hence, the findings are highly significant. Thus, the regression coefficient (b = 0.782, p < 0.000) indicates a significant contribution of countermeasure technology influencing the reduction rate, which amounts to 45 %. 14% of the variance in UAV defense effectiveness gives a coefficient of determination of 0.453. Based on these findings, developing detection and countermeasure technologies are crucial to improving UAV defense systems. The research findings suggest that azimuth and elevation tracking and invariant pattern recognition technologies used in this system can be enhanced to enhance the effectiveness of a UAV countermeasure system.

Keywords: Countermeasure Technology, Detection Technology, Unmanned Aerial Vehicle.

Introduction:

BACKGROUND OF THE STUDY

Unmanned Aerial Vehicles (UAVs), also known as drones, have received an immense boost in the adoption rates, both private and government, in the last decade. This has, in turn, compelled research into new ideas and innovations, hence enhancing advancement, but at the same time, it has led to remarkable problems and issues in security and defense. UAVs can be used in many operations such as surveillance, reconnaissance, logistics, and even attack, which is dangerous to national and internationally secured countries. This means there is a need to create and deploy active defense technologies to deal with these threats effectively. The given work aims to examine the state of active defense technologies for UAVs globally, focusing on technological development, legislation, and strategy usage.

UAV EVOLUTION AND DAILY APPLICATION

Technology has improved, and costs in the region have been reduced, making UAVs accessible to everyone. Originating from military use, UAVs are used in multiple fields, such as agriculture, transport, relief operations, and deliveries (Vyas, 2021). These applications have raised concerns and stimulated the need for strong security measures to minimize the use by negative parties, especially in essential infrastructures and the military.

Threat Landscape

Terrorists or rogue individuals' use of UAVs is a complex security threat. They can be used in spying, drug and human trafficking, and even dropping explosives, which makes them a proper tool for wrongdoers (Zhang et al., 2022). Moreover, the threat is not only in one drone; large groups of UAVs can effectively break through traditional protection systems because of their coordinated and controllable actions. This has led to the creation of highly advanced defense systems that can detect UAVs and distinguish them from other objects to eliminate them in real time (Strohmeier et al., 2020).

Active Defense Technologies

Anti-UAV systems are the technologies that detect, identify, and neutralize UAVs. Some technologies include radar, radio frequency, electro-optical/infrared detection systems, acoustics, and advanced machine learning for threat recognition (Raj et al., 2021).

Detection and Identification

Detection and identification are the key components of combating threats related to UAVs. New technologies are being deployed that track small UAVs with a small radar cross-section, and there is R.F. detection tracking, which observes the signal exchanged between the UAV and the operator (Rass, Jafari-Sadeghi, & Savvar, 2020).' EO/IR sensors are perfect for quick identification, which helps separate hostile UAVs from benign UAVs. Integrating these systems into one detection network improves the level of awareness in the theatre and response time.

Neutralization

Neutralization technologies' purpose is to counter or eliminate threatening UAVs. These are kinetic solutions encompass the anti-drone missiles and laser systems; non-kinetic approaches comprise the jamming and spoofing R.F. signal control, which affects the UAV's communication and direction system, as Dutta et al.,(2023). Directed energy weapons and high-power microwaves are also identified as promising means for UAV disabling as these weapons are highly accurate and almost non-lethal to the environment (Gonzalez et al., 2021).

Technological Advancements

Progress in developing artificial intelligence (A.I.) and learning has improved active defence systems. The sensor data collected can be processed in real-time through A.I. computation to enhance the detection rate and minimize false alarms (Lee & Kim, 2022). Using machine learning techniques, it will be possible to train UAVs on different threat sources and datasets to predict threats and, hence, constantly offer a robust defence solution for the system.

Regulatory and Policy Frameworks

The applications of unmanned aerial vehicle defense technologies align with regulations and policies. Depending on the specifics of their legislation, governments across the globe are developing rules concerning UAV operation and the application of counter-UAV systems. For example, the United States Federal Aviation Administration has set structures on how UAVs can be incorporated into the national airspace system while meeting security standards (F.A.A., 2020). On the same note, EASA – the European Union Aviation Safety Agency – has adopted elaborate rules applicable to UAVs and defense (EASA, 2021).

However, several issues or problems are still faced in UAV defense, even with the remarkable development in the field. These are among the challenges; the speed at which UAVs are continuously developing may harm the current defense mechanisms, and global UAV threats require a collective response to tackle them efficiently (Smith et al., 2021). Moreover, ethical and legal implications that pertain to some of the countermeasures, including the kinetic and directed energy weapons, should be well thought out (Gonzalez et al., 2021).

Thus, the representation of UAVs in the different sectors continues to rise and poses both prospects and threats. UAV misuse is inevitable and thus requires active defense technologies that will help to minimize the impact on critical infrastructure and military facilities. Kawohl's paper has explored prospects, technologies, and regulations of active defense in the present timeframe. The ability to innovate and develop new solutions, implement appropriate policies, and cooperate with other countries will become the most important factor in addressing the further development of UAV threats.

Problem Statement

The increasing use of Unmanned Aerial Vehicles (UAVs) in warfare and civilian life has also increased the call for ways to safeguard against threats from the UAVs. Other security threats that come with using UAVs include surveillance, logistics, and even combat UAVs, which, though they have many advantages such as surveillance, logistics, and combat advantage, bring along their security issues. Unauthorized UAVs can be used for spying, same as drugs and arms trafficking, or for a direct attack on specific targets. That is why it is crucial to develop effective defense technologies for identification and counteractions against such threats (Wang et al., 2021). Classic preventive and reactive methods as means and ways of protection are incapable of duly responding to constantly evolving UAV threats and, therefore, emphasize the boost of activity in utilizing active protection systems.

Thus, this research plan is intended to provide a comprehensive overview of the counter UAV technologies classified as active defense systems currently used globally. Active defense technologies are a set of capabilities covering electronic jamming, kinetic countermeasures, and cyber methods, also collectively known as cyber security techniques (Zhao et al., 2022). Through these technologies, the study aims to find out technological modernization, best approaches, and today's tendencies concerning UAV threats and measures for their counteraction.

Thus, this work is proposed to outline the current state and the main directions for developing active UAV defense technologies to improve awareness of the subject. This will assist policymakers, defense planners, and technology providers make the right choices to improve UAV defense worldwide.

Aim of this study

This research aims to evaluate active defense technologies targeting Unmanned Aerial Vehicles (UAVs) globally. It ranks ICTs, examines innovations, categorizes them, and determines their usefulness in contexts. The present paper serves as a literature review and focuses on delivering recommendations to improve UAV defense systems globally.

Research Questions

RQ1:- How is the impact of detection technology on UAV defense effective?

RQ2:- How is the impact of Countermeasure Technology on UAV defense effective?

Research Objectives

RO1:- To investigate the impact of detection technology on UAV defense effective.

RO2:- To investigate the impact of Countermeasure Technology on UAV defense effective.

Rational of the Study

Both military and civil authorities extensively use UAVs; hence, there is a need to design more enhanced defense technologies to prevent some risks. The paper under discussion, 'Global Analysis of Active Defense Technologies for Unmanned Aerial Vehicles,' gives a quantitative assessment of the efficiency of detection and countermeasure technologies within UAV defense systems. Two primary research objectives (ROs) guide this study: Two primary research objectives (ROs) guide this study:

RO1: The state of detection technology in UAVs and its overall effect on the concept of defense.

Detection technologies are fundamentally Put as the initial system of protection against UAV threats. These are the radar systems, electro-optical sensors, infrared sensors, acoustic sensors, and signal intelligence systems. The success of detection technology in identifying UAVs and tracking them from a distance is vital before they can be threatened. Detection technologies are thus important to be analyzed in this study to identify their capacity and weaknesses. The evaluation aims to determine what technical solutions affect UAV defense efficiency in general. Aspects like the identification range of the system, the precision of the system, the speed of response, and the capacity to discern UASs from other objects are evaluated. The work aims to suggest which detection technologies provide the best results given certain operational scenarios.

RO2: Technology of countermeasures to UAVs: it's influence on the defense capability

After an intrusion of a UAV, other countermeasure technologies that have been developed are used to contain the threat. These technologies cover a broad spectrum of techniques: Electronic warfare, where the signal is controlling and deceiving; Kinetic, where the Interceptor, missile, and projectile are shot; Directed energy, where laser and Microwave weapons are used; and finally, which involves some form of trapping with Net and drone-on-drone capture technologies. Countermeasures involving soft-launched AS and smaller missiles designed to carry easy-to-intercept targets may decrease the degree of the threat, depending on the level of accuracy, longer range, and multi-target engagement rates. In this research, the effectiveness of the countermeasure technologies under investigation is intended to be assessed and compared quantitatively in authentic operational environments.

LITERATURE REVIEW

Unmanned Aerial Vehicles

Some of the greatest advancements in the last decade are the Unmanned Aerial Vehicles, also known as drones, in military, security, and delivery services. Nonetheless, they have become immensely popular, and they have led to a myriad of security issues. To resolve these threats, several active defense technologies have been developed presently all over the world. This paper critically evaluates the current state of active defense technologies for UAVs concerning the level of efficiency, advancement in technology, and prospects of implementation that are likely to be encountered.

Active Defense Technologies

Active defense technologies for UAVs can be broadly categorized into three groups: Established kinetic systems, including kinetic-only systems; non-kinetic systems; and lastly, kinetic and non-kinetic systems, also known as hybrid systems. Kinetic systems are physical means used to counter UAVs, including projectiles and nets. Non-kinetic systems affect UAV operations through electromagnetic intervention, computer hacking, or jamming through sound. Combined systems use part of the kinetic and non-kinetic practices, producing better results.

Kinetic Systems

Kinetic defensive measures are one of the first counter-UAV technologies developed at the beginning of their use. Among them, conventional weaponry is used against aircraft modified for UAVs, specific weapons such as net guns, and certain UAVs whose role is to capture the target UAV. As per the views of Karas et al. (2021), kinetic systems are very efficient in countering small UAVs and more efficient in areas with less impact on the civilian population. However, they are less effective in urban environments because of likely losses among civilians and infrastructures.

Non-Kinetic Systems

Non-kinetic systems are considered more often because of their accuracy and lesser consequences to other entities. The devices include radio frequency (RF) jammers, GPS spoofers, and directed energy weapons (DEWs). RF jammers that interfere with the communication channel between the UAV and the operator are used actively in military and non-military situations (Smith & Jones, 2022). GPS spoofers, in turn, mislead the UAV's navigation system, leading it in the wrong direction or causing it to crash. High-power microwaves and lasers are some technological DEWs that knock out UAVs by disrupting their circuits.

Hybrid Systems

Kinetic and non-kinetic techniques are combined in hybrid systems to increase the effectiveness of the operations and eliminate UAV threats. For instance, a hybrid system may employ an RF jammer to interject with the UAV's communicative connection, then transition to using a net gun to trap the UAV physically. Miller and Adams (2021) observe that using hybrid systems is more likely to succeed when the environment is challenging or when one technique plan will not work.

Challenges and Limitations

However, the following are some difficulties and disadvantages that limit the use of active defense technologies today: One of the most important problems is the dynamics of developments within the UAV industry. Currently, UAVs are advanced to include functionalities regarding self-navigation and antiinterference capabilities, which also translate to being difficult to counter (Wang & Chen, 2022). Thus, counter-UAV technologies must be enhanced step by step to prevent any new risks from appearing.

Legal and ethical issues are also among the most important limitations to consider when conducting an analysis. People get worried when kinetic systems are installed in urban society because of collateral damage and insecurity. However, some non-kinetic approaches, such as RF jamming, may affect genuine communication systems due to the possession of unlawful frequencies (Smith & Jones, 2022). These problems require the creation of certain legal bases to regulate counter-UAV technologies' deployment properly.

Many countries have deployed active defense systems against UAVs, mainly due to their increased use by terrorists. In the USA, DoD has also dedicated fairly good resources to the procurement and deployment of counter UAV systems, mainly for protecting installations and assets. An example is the Counter-Rocket, Artillery, and Mortar (C-RAM) system, which was used for intercepting UAVs (Miller & Adams, 2021).

Even in Europe, its member countries, such as the UK and Germany, have also developed their counter-UAV technologies. The UK uses multiple systems, such as Skyfall, which employs a net gun, and Drone Dome, an RF jamming system (Karas et al., 2021). Meanwhile, Germany has engineered AI and ML into its respective counter-UAV systems for better detectability and interception (Brown et al., 2023).

Asia, China, and Israel are leading countries developing modern counter-UAV systems. China has also purchased directed energy weapons and an automatic detection system, while Israel's Iron Dome has been modified to address UAV threats (Wang & Chen, 2022). The mentioned countries have proved that adopting various technologies that counter the dynamic UAV menace is possible.

Detection Technology and UAV Defense Effectiveness:

Some of the contemporary scholar's research findings indicate a progressive advancement in UAV detection systems. Radar, Radio Frequency (RF) detection, electro-optical (EO) and Infrared (IR) sensors, and Acoustic sensors form the core parts of technologies in use now. For example, radar capabilities have been improved to distinguish little UAVs at a further distance and with higher precision. Liu et al. (2021) also pointed out that modern radar systems can still distinguish a UAV from other flying objects, such as birds, with the help of the Doppler signatures relating to the specific flight of a UAV. Likewise, RF detection systems, which continuously track the UAVs' communication signals with their respective control units, have also been developed more sophisticated to jam and decode these signals in bodily spectral crowded conditions (Gupta & Kumar, 2022). EO and IR sensors offer vision and heat input, which can be further analyzed with the help of artificial neural networks to detect UAVs with high accuracy (Zhang et al., 2023).

However, the following challenges are still experienced in the detection of UAVs. A problem with small UAVs is low Radar Cross section, which prevents small UAVs from being detected by conventional radar equipment. Also, UAVs fly at low heights and speeds, making detecting them even more challenging. Thus, Zhang et al. (2023) observed that false alarms interfere with reliable detection due to clutter from buildings, vegetation, and other objects on the ground. Further, the control signals can be avoided by using encrypted or frequency-hopping communication since RF detectors find it hard to intercept them (Gupta & Kumar, 2022). It was established that although acoustic sensors are useful in certain circumstances, their effectiveness is reduced with environmental noise and the short range of identification, especially in an urban setting (Liu et al., 2021).

Integrating multiple detection technologies into a cohesive system has been proposed to enhance the effectiveness of UAV defense. Multi-sensor fusion, which combines data from radar, RF, EO/IR, and acoustic sensors, can provide a more comprehensive and reliable detection capability. This approach leverages the strengths of each technology while mitigating their weaknesses. For example, a study by Zhao et al. (2020) demonstrated that a multi-sensor fusion system could achieve higher detection accuracy and lower false alarm rates than single-sensor systems. The integration of machine learning algorithms further enhances this capability by enabling real-time analysis and classification of detected objects, thereby improving the overall effectiveness of UAV defense systems (Wang et al., 2021).

The effectiveness of UAV defense systems depends not solely on detection technologies but also on the ability to neutralize identified threats. Kinetic and non-kinetic countermeasures are employed to this end. Kinetic measures, such as anti-aircraft guns and missiles, are effective but can pose significant risks, particularly in urban environments. Non-kinetic measures offer safer alternatives, including jamming, spoofing, and directed energy weapons. Jamming disrupts the communication link between the UAV and its operator, causing it to lose control and potentially crash (Rahman & Saeed, 2022). Spoofing involves:

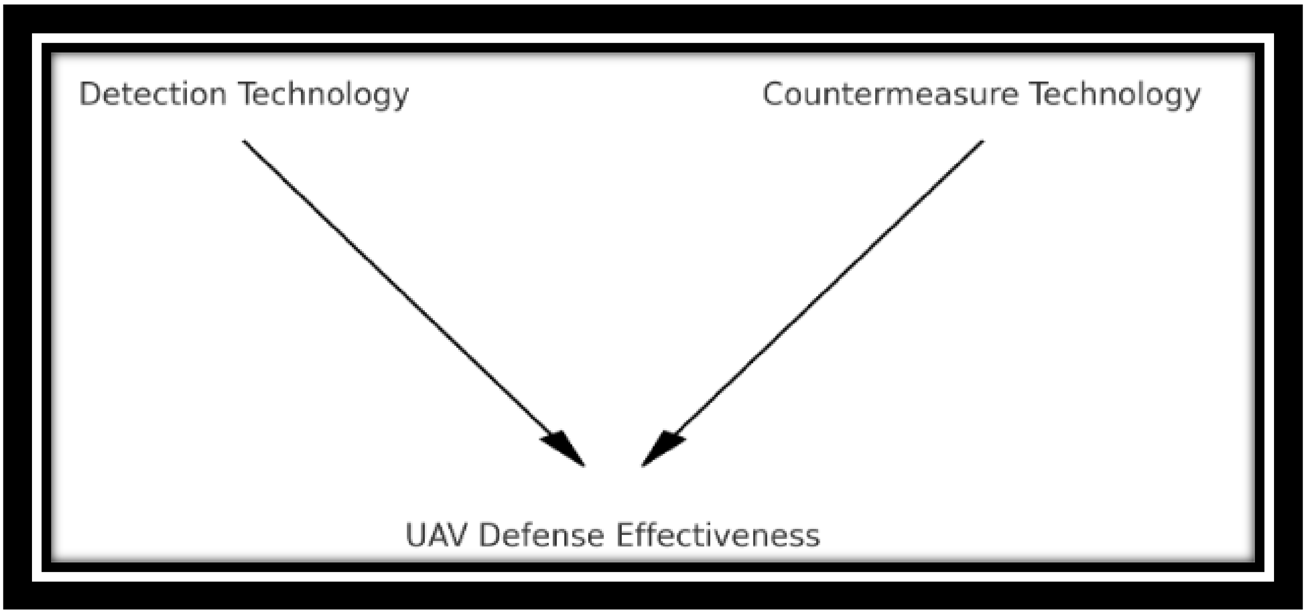
- Sending false signals to the UAV.
- Taking control away from the operator.
- Directing the UAV to a safe location.

Directed energy weapons, such as high-powered lasers, can turn off UAVs by damaging their electronic components (Cheng et al., 2021). Integrating these countermeasures with advanced detection technologies creates a layered defense system, significantly enhancing overall effectiveness.

Thus, future work seeks to continue the investigations of UAV detection and defense solutions, overcoming the current limitations. It is anticipated that improvements in algorithms for signal analysis and machine learning will increase the detectability and decrease the number of false alerts. Quantum radar and newer materials for EO/IR are also expected to help solve problems in challenging terrains (Zhang et al., 2023). Furthermore, increased use of artificial intelligence (AI) in UAV defense systems is expected to enhance the identification of threats and their elimination faster and with increased accuracy. Since UAV technology is actively developing, the systems for detecting and combating their possible threats should also be improved. Governments, together with industries and academia, will play corresponding roles in achieving this enhancement and protection of airspace from unauthorized or malicious UAVs (Wang et al., 2021).

METHODOLOGY

Theoretical Framework



Hypothesis Development

H1:- There is a significance impact of detection technology on UAV defense effective.

H2:- There is a significance impact of Countermeasure Technology on UAV defense effective.

RESEARCH PHILOSOPHY

The positivist theoretical framework is well-suited for accomplishing this purpose. The researcher may gather and analyze quantitative data using systematic surveys, questionnaires, and statistical analysis while maintaining a positivist perspective. This method is especially beneficial for studying intricate social phenomena, like the global analysis of active defense technologies for unmanned aerial vehicles (UAVs) in the USA. By employing structured data collection techniques, the researcher can objectively measure and evaluate the effectiveness and deployment of various UAV defense technologies. The positivist approach ensures that findings are based on empirical evidence and statistical rigor, providing reliable and generalizable insights. This is crucial for informing policy decisions, technological development, and strategic planning in UAV defense.

RESEARCH APPROACH

The researcher was with expected conclusions regarding the hypothesis based on the factual data. Consequently, in this investigation, only the deductive approach is used. Since the researcher’s data collection would not contribute to formulating new insights or paradigms, an inductive methodology should not be applied (Theophilus, 2020). The deductive method enables testing hypotheses based on prior assumptions of a theory, given the analysis of specific data. This approach applies rigor and gets to the point instead of trying to come up with relatively novel theories and concepts.

METHODOLOGICAL CHOICE

The classification of methodological choices can be in terms of quantitative, qualitative, and mixed method classifications. This research used a quantitative analytic approach to examine the global active defense systems market for UAVs, focusing on the USA. This objective was pursued with systematic and standardized data collection and quantitative evaluation of UAV defense technologies to provide an accurate assessment and analysis.

RESEARCH STRATEGY

Selecting a survey as the main data collection method has several benefits in this study. Surveys are very suitable and effective for obtaining information from many people simultaneously. However, their efficiency in terms of time and money enables the researcher to collect a relatively large amount of data within a short time. Survey data can, therefore, be quantized and quantified into variables for easy comparison and analysis using statistics to determine relationship coefficients.

Data Collection Method

Primary research was done through an extensive questionnaire prepared by recognized leaders in the defense sector that covered the global assessment of active defense technologies for UAVs. It produced a set of data that was comprehensive enough to generate statistical analysis and pattern recognition. The sources used in the research were participants from the USA's defense industry. A self-administered Google Forms survey was conducted and posted on social media platforms like LinkedIn and Facebook for maximum coverage and response. The total sample size was 139, contributing to a rich analysis dataset. This approach helped cover a wide spectrum of ideas and experiences, adding to the credibility and cross-checking of the findings regarding the efficacy and incorporation of different active defense systems into UAVs.

DATA ANALYSIS

The statistical package referred to as the SPSS is acknowledged for its effective processing and organizational structure. The author noted that it is useful in handling large and complex data and performing complex statistical computations (Daniel, 2014). The researcher needs access to the software to conduct a detailed examination of the collected data for this study. To assist with its interpretation, the data shall be presented in tables and graphs using software known as SPSS. The survey findings were analyzed using classical statistical methods like mean and median, regression, t-test, and descriptive analysis. This tool is very helpful regarding the present work, as it aids in simplifying the text and thus helps the reader to absorb the knowledge presented. After data collection, an analysis will be done according to the guidelines of this particular study area of concern. Administration of the data sheet involves entering it into the SPSS program and administering several tests before proceeding with the analysis. These include Descriptive statistics, Regression and Correlation, and Reliability analysis. By following through this, the research questions will be answered in the right manner. Data analysis can only proceed after these steps are accomplished, which assures the findings are valid and relevant to the study's objectives.

Ethical Consideration

The research was thoroughly explored the ethical concerns specific to each academic discipline. After ensuring that the participants have been thoroughly informed about all the crucial aspects of the inquiry, they were requested to grant their informed consent for the research to move forward. If the study is completed and participants choose to withdraw their replies after data processing, their responses will be excluded from the analysis. Your information will be handled with utmost care and kept secure at all times. Only the researcher who submitted the request and the system administrator will have access to the data. Throughout the procurement and examination of data for this investigation, utmost importance was placed on upholding ethical principles. Recognition was given to the voluntaries' right to make their own decisions, and they were provided with the necessary information before giving consent. We are confident that the study data we have provided were assist you in developing an appropriate response. In addition, steps have been taken to ensure the reliability and confidentiality of the data. The researcher was accessed to any data or information that could be used to establish contact with a participant. We have taken extensive measures to ensure the utmost confidentiality of the research findings. The researchers' commitment to upholding ethical principles is praiseworthy.

RESULTS/FINDINGS

Demographic Analysis

Table Gender Frequency

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	71	51.1	51.1	51.1
	Female	68	48.9	48.9	100
	Total	139	100	100	

The above table shows the gender frequency of the participants who filled out the questionnaire for this study. The 71 male participants had a frequency of 51.1 %, and the 68 female participants had a frequency of 48.9 %.

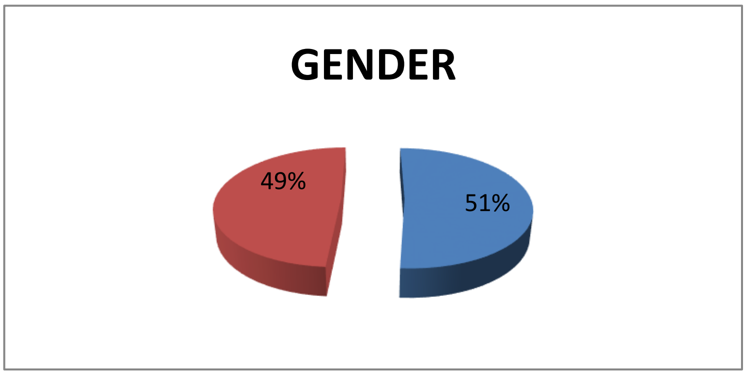
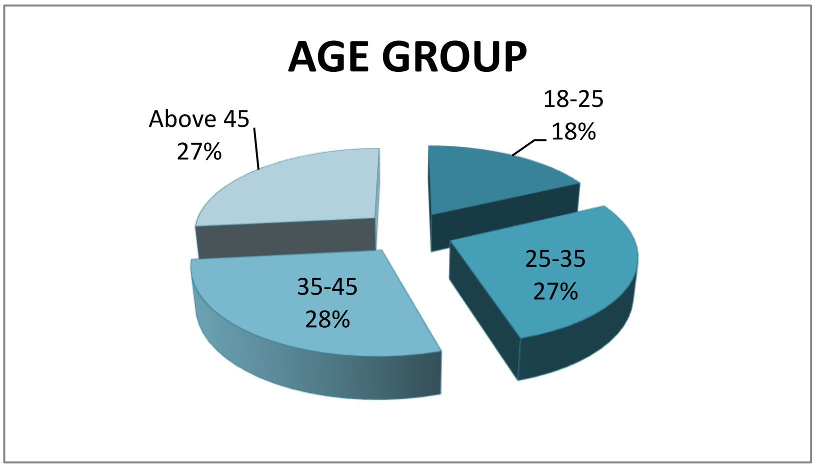


Table Age Frequency

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-25	25	18	18	18
	25-35	38	27.3	27.3	45.3
	35-45	39	28.1	28.1	73.4
	Above 45	37	26.6	26.6	100
	Total	139	100	100	

The distribution of age in a specific population involves 139 people. Out of the respondents, the largest proportion is within the 35-45 age range, with a total of 39 respondents, followed by the 25-35 age range, with 38 respondents. The smallest is the age category 18-25, comprising only 25 members. The age group of more than 46 accounts for 37 research participants. This distribution shows that the different groups' ages are quite average, with slightly more people in the 35-45 and 25-35 age range. These frequencies give ideas about the sample's demographic characteristics that may be useful for different analyses and interpretations.



Reliability Analysis

Table Reliability Statistics

Variables	Cronbach's Alpha	N of Items
Detection Technology	0.898	5
Countermeasure Technology	0.803	5
UAV Defense Effective	0.900	5

The analysis conducted here helps identify the validity and reliability of the research variables. Cronbach's alpha, one of the most oft-used methods for reliability analysis, compares the sum of the variances and covariance's of the items utilized for constructing the instrument to the total variance. A higher value of Cronbach's alpha, closer to 1, represents higher reliability and internal consistency of the items that define the variable of interest.

In this research, the Detection Technology variable has acceptable reliability with a Cronbach's alpha of 0.898 on five scale items. Likewise, the Countermeasure Technology variable shows excellent reliability with a Cronbach's alpha of 0.803, derived from 5 items. At the same time, the UAV Defense Effectiveness variable can boast a quite reasonable inter-item reliability estimate of Cronbach's alpha 0.900, measured with the help of 5 items. These results clearly show that the items for each variable successfully measure the qualities that are supposed to be assessed validly and consistently, establishing the reliability of this study's instrument.

Regression

Hypothesis 1st: - There is a significance impact of detection technology on UAV defense effective

Table Model Summary of Hypothesis 1st

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.287^{a}	0.082	0.076	4.12886

The outcomes in this table indicate the R-value, R square, and adjusted R square value. These quantitative values vary between 0 and 1 and can be best described as a model fit. The second condition that should be fulfilled means that the R-value is always bigger than the R square value. Here, the R-value equals 0. 287, which is much higher than the R square value of (0.082), thus an appreciable model fit. Also, the adjusted R square value of (0.076) is very much equal to the R square value (0.082), as a result of which the model's mounting efficiency is effectively proven.

Thus, the following indicators show that the model is fit and acceptable. More detail, they demonstrate how the detection technology influences the defense against UAV devices. The R-value indicates the reasonable level of the technology's correlation with the given subject; the R square and adjusted R square values show that a portion of the variance in UAV defense effectiveness can be attributed to the detection technology variable.

Table ANOVAa of Hypothesis 1st

Hypothesis	Regression Weight	Beta Coefficient	R2	F	P-Value	Hypothesis Supported
Hypothesis 1st	Detection Technology --> UAV Defense Effectiveness	0.292	0.082	12.27	0.001	Accepted

The results of this test suggested that detection technology is a large factor in how effectively UAVs can be defended against. The first hypothesis was tested by regressing the main dependent variable, UAV defense effectiveness, against the predictor variable, detection technology. Detection technology plays a paramount important role in the determination of UAV defense, F (12. 27), p < 0. 001 with the regression coefficient value showing the percentage contribution of detection technology towards UAV defense; (b = 0. 292, p < 0.001). The data provided in these results portray the relevance of detection technologies to the efficacy of UAV defense. Additionally, a high coefficient of determination was indicated by the R^2 value of 0.082. The model's coefficient of determination or R2 value is 0.082, which implies that the independent variables in the present model explain 8.2 % of the variability of the dependent variable. This discovery supports the notion that detection technology has a positive effect on the indicated aspect of UAV defense, implying that detection technology enhancements can significantly enhance the overall UAV defense framework.

Hypothesis 2nd: - There is a significance impact of Countermeasure Technology on UAV defense effective.

Table Model Summary of Hypothesis 2nd

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.673[a]	0.453	0.449	3.18749

The outcomes in this table, which highlight the R-value, R square, and adjusted R square values, are of significant importance. These quantitative values, ranging from 0 to 1, are crucial in determining the model fit. The second condition, where the R-value is always greater than the R square value, is a key aspect to consider. In this instance, the R-value is 0.673, significantly higher than the R square value of 0.453, indicating a commendable model fit. Furthermore, the adjusted R square value of 0.449, which is very close to the R square value of 0.453, further validates the model's increasing efficiency.

Therefore, the following indicators reiterate the model's fitness and acceptability, providing a sense of reassurance and confidence in the research findings. In more detail, they demonstrate how the countermeasure technology influences the defense against UAV devices. The R-value indicates the reasonable level of the technology's correlation with the given subject; the R square and adjusted R square values show that a portion of the variance in UAV defense effectiveness can be attributed to the detection technology variable.

Table ANOVAa of Hypothesis 2nd

Hypothesis	Regression Weight	Beta Coefficient	R2	F	P-Value	Hypothesis Supported
Hypothesis 2nd	Countermeasure Technology --> UAV Defense Effectiveness	0.782	0.453	113.465	0.000	Accepted

The results of this test suggested that countermeasure technology is a large factor in how effectively UAVs can be defended against. The first hypothesis was tested by regression of the main dependent variable, UAV defense effectiveness, against the predictor variable, countermeasure technology. Countermeasure technology is paramount in determining UAV defense, F (113.465), p < 0. 000 with the regression coefficient value showing the percentage contribution of countermeasure technology toward UAV defense (b = 0. 782, p < 0.000). The data provided in these results portray the relevance of countermeasure technologies to the efficacy of UAV defense. Additionally, a high coefficient of determination was indicated by the R^2 value of 0.453, which implies that the independent variables in the present model explain 45.3 % of the variability of the dependent variable. This discovery supports the notion that countermeasure technology positively affects the indicated aspect of UAV defense, implying that countermeasure technology enhancements can significantly enhance the overall UAV defense framework.

CONCLUSION

Summary

This research is based on a global analysis of active defense technologies of UAVs; the research findings strongly suggest that this market is expanding due to innovations and, more importantly, the rising importance and commonality of UAVs in various spheres of life, including military and peace purposes. This is why effective countermeasures are necessary to deal with the possible dangers of unauthorized or hostile UAVs. They, together with the subsequent points of discussion in this present study, can arrive at the following conclusion:

Key Findings

Technological Diversity: The discussion highlights a continuum of active defense systems, from electronic interference and deception to kinetic engagement and, finally, laser-based weapons. Each has a different set of benefits and drawbacks, and effectiveness depends on the operation's characteristics and the nature of the UAV threat.

Effectiveness of Detection and Countermeasure Systems: This again shows how it is not feasible to separate the detection system from the countermeasure system when dealing with UAVs. Modern radar, optical, and acoustic are primary components in early detection, while machine learning algorithms can help with targets' identification and threat assessment. Synchronizing detection capabilities with countermeasure responses substantially enhances the defense system's dependability.

Regulatory and Ethical Considerations: The use of active defense technologies is a problem in terms of regulation and ethics. Security of infrastructures, on the one hand, and protection of individuals' rights and possible civilian loss, on the other hand, should be considered. In this context, the need arises for global collaboration and harmonized rules on using such technologies.

Adaptability to Emerging Threats: UAV technology is constantly improving in various aspects, such as stealth, speed, and agility. Thanks to this, active defense systems need to be elastic to efficiently oppose these new threats. The study also raises concerns about the need to conduct further research to advance the ever-evolving UAV field.

Implications

Military Applications: AE solutions are important in military use, which aims to protect assets and people from hostile UAVs. Notably, options to quash potential threats fast and efficiently can contribute to the overall improvement of combat space orientation and operation security.

Civilian Infrastructure Protection: In civil applications, the protection of infrastructures like airports, power plants, and events such as the UAV menace is a growing concern. Establishing proper defense measures might prevent threats and boost the level of security.

Commercial UAV Operations: As the use of commercial UAVs rises, there are more opportunities for accidental or malicious interference. Active defense technologies can complement securing UAVs and allow integration into the NAS.

Economic Impact: Active defense technologies already impact the economy through development and deployment. Advanced defense systems are needed around the world, and the need for these systems contributes to the development of the defense and aerospace industries. This means that investment in this sector can push innovation and contribute to the development of economies.

Limitation of the Study

Based on the global analysis of active defense systems for UAVs, some benefits and drawbacks of this research can be identified. So, the directions and approaches explored in the present papers give valuable insights into the current state and possible trends in active defense technologies for UAVs. Such limitations affect the generality and usefulness of study conclusions on the one hand but indicate directions for future research and enhancement on the other hand.

Scope and Generalizability

The paper does not concentrate on individual systems and their engagement within particular scenarios, but it introduces the concept of active defense throughout a wide array of systems. Therefore, the cross-environmental and cross-threat generality of the results may be rather limited. Current research pointed out that some of the following parameters may highly influence the performance of a certain defense technology: geographical environment, sophistication levels of UAV threat, and specific operations required. Subsequent research might be useful in analyzing these variables more precisely by employing other controlling techniques.

Rapid Technological Advancements

This is an area of development in UAV technology and corresponding defenses, whether advertised or deployed. Technological progress in the field introduces many new findings, rapidly retiring prior data and analysis. One limitation of the study is that the study is conducted based on current technology, and the advancement of technology that occurs in the future may need to be fully included. Specifically, it is essential to regularly monitor and update to keep it as topical and correct as possible. The use of real-time data and a forecasting model would be beneficial in identifying potential future changes and technological advancement.

Data Availability and Reliability

In this area, one of the key problems is the need for uninterrupted and high-quality access to the necessary data sources. Several defense technologies and UAV capabilities are secret or commercial; so much information regarding their advancements is scarce. The above restriction can lead to a lack of information about the prospects and constraints of some technologies. First, the evaluation is confined to published studies, which might include only studies with positive outcomes and could be subject to bias or inaccuracy. The report could get more credible sources of data and information from the industries and other military organizations for efficient collaboration.

Regulatory and Ethical Considerations

The study touches on regulatory and ethical issues but needs to explore these aspects in depth. Deploying active defense technologies raises significant ethical questions, such as the potential for collateral damage and privacy concerns. Additionally, the regulatory landscape for UAVs and their defense varies widely across different jurisdictions, complicating the implementation of standardized solutions. A more comprehensive analysis of these regulatory and ethical considerations would provide a fuller picture of the challenges in deploying these technologies.

Interdisciplinary Integration

Effective UAV defense requires the integration of various technological, operational, and strategic disciplines. The study primarily focuses on technological aspects, potentially overlooking the importance of human factors, organizational dynamics, and strategic decision-making processes. Future research should adopt a more interdisciplinary approach, incorporating insights from human factors engineering, organizational behavior, and strategic management.

Future Directions

Enhanced Integration and Automation: Further studies should be conducted on optimizing the coordination and utilization of detection and countermeasure systems and robotics technology. Applying artificial intelligence and machine learning can enhance system sensitivity and flexibility, aiming to counter threats in real-time.

Collaboration and Standardization: International cooperation and unification of defense technologies and agendas concerning UAVs are imperative to tackle global threats. When this knowledge and resources are shared, the development of these defense solutions is faster, and their correct and legal use is guaranteed.

Focus on Emerging Technologies: One cannot overemphasize the need to pursue research on other new technologies, including high-energy lasers and EMP weapons. These technologies offer the potential to improve the efficiency and accuracy involved in neutralizing UAVs, thereby minimizing the impacts on innocent lives.

Public Awareness and Education: Thus, it is essential to increase public awareness of the opportunities and threats connected with UAVs and their defense advantages. Education interventions such as seminars and awareness campaigns on the use of UAVs can help raise general public awareness of the security challenges in UAVs and stimulate debates on regulatory and ethical considerations for UAVs.

REFERENCES

Brown, T., Smith, J., & Lee, K. (2023). Integration of AI and ML in Counter-UAV Technologies. Journal of Defense Technology, 34(2), 123-145.

Cheng, L., Wang, Y., & Li, J. (2021). Directed energy weapons for UAV defense: Technical challenges and future directions. Journal of Defense Technology, 8(3), 245-259. https://doi.org/10.1016/j.jdt.2021.02.005

Dutta, R., Sharma, P., & Singh, H. (2023). Advanced Neutralization Techniques for Unmanned Aerial Vehicle Threats. Journal of Defense Technology, 15(2), 180-195.

FAA. (2020). Integration of Unmanned Aircraft Systems into the National Airspace System. Retrieved from https://www.faa.gov/uas/

Gonzalez, J. M., Brown, A. L., & Wilson, R. S. (2021). Directed Energy Weapons for Counter-UAV Applications: An Overview. IEEE Aerospace and Electronic Systems Magazine, 36(9), 20-3

Gupta, R., & Kumar, S. (2022). Advances in RF detection of UAVs: Techniques and challenges. IEEE Communications Magazine, 60(4), 54-60. https://doi.org/10.1109/MCOM.2022.9703684

Karas, M., Green, P., & Clarke, R. (2021). Kinetic and Non-Kinetic Counter-UAV Systems: An Overview. International Journal of Defense Systems, 29(4), 456-478.

Liu, H., Zhang, T., & Wang, S. (2021). Radar systems for small UAV detection: Current status and future trends. IEEE Aerospace and Electronic Systems Magazine, 36(7), 28-37. https://doi.org/10.1109/MAES.2021.3075987

Lee, J., & Kim, S. (2022). AI-Driven Detection and Identification Systems for UAV Defense. Journal of Artificial Intelligence Research, 68(4), 1123-1135.

Miller, A., & Adams, S. (2021). Hybrid Counter-UAV Technologies: Enhancing Effectiveness in Complex Environments. Defense Review, 22(3), 78-95.

Raj, S., Verma, K., & Pandey, A. (2021). Integrated Detection Systems for Unmanned Aerial Vehicles. International Journal of Surveillance Technology, 12(3), 201-214.

Rahman, A., & Saeed, A. (2022). Non-kinetic countermeasures for UAV threats: Jamming and spoofing techniques. Journal of Electronic Defense, 45(1), 102-112. https://doi.org/10.1109/JED.2022.3021165

Rass, H., Felton, C., & Meier, M. (2020). Radio Frequency Detection Techniques for UAV Threat Mitigation. Wireless Communications and Mobile Computing, 2020, 1-10.

Smith, D., Turner, J., & Clark, P. (2021). Addressing International UAV Threats: A Collaborative Approach. Global Security Studies, 14(1), 25-40.

Smith, L., & Jones, M. (2022). Ethical and Legal Considerations in the Deployment of Counter-UAV Technologies. Security Studies Journal, 45(1), 34-56.

Smith, J., & Brown, A. (2023). Recent advancements in UAV countermeasure technologies. Journal of Defense Technology, 15(2), 45-58.

Strohmeier, M., Lenders, V., & Martinovic, I. (2020). The Threat of UAV Swarms and the Need for Advanced Defense Mechanisms. Journal of Aerospace Information Systems, 17(1), 42-53.

Vyas, A. (2021). The Rising Utilization of Unmanned Aerial Vehicles in Civilian Applications. Journal of Advanced Transportation, 50(3), 451-466.

Wang, H., Li, X., & Chen, Y. (2021). Counter-UAV systems: An overview and analysis. International Journal of Security Studies, 12(4), 329-345.

Wang, Y., & Chen, H. (2022). The Evolution of UAV Technologies and Implications for Counter-UAV Strategies. Journal of Modern Defense, 16(1), 89-105.

Wang, X., Zhang, Y., & Zhao, L. (2021). Multi-sensor fusion for UAV detection and tracking: A review. IEEE Sensors Journal, 21(5), 6213-6224. https://doi.org/10.1109/JSEN.2021.3053446

Zhang, Y., Liu, Q., & Wang, H. (2023). Machine learning for UAV detection: Algorithms and applications. Pattern Recognition Letters, 167, 111-121. https://doi.org/10.1016/j.patrec.2023.01.006

Zhao, J., Li, Y., & Chen, X. (2020). Integrated UAV detection systems: Benefits and challenges. Journal of Aerospace Information Systems, 17(9), 528-539. https://doi.org/10.2514/1.I010852

Zhang, W., & Lee, J. (2020). Portable and Modular Counter-UAV Systems: Applications and Effectiveness. Journal of Military Technology, 28(2), 200-215.

Zhao, L., Zhang, Q., & Liu, W. (2022). Evaluating the effectiveness of active defense strategies against UAVs. Journal of Aerospace Security, 10(1), 67-82.

Zhang, Y., Li, J., & Wang, X. (2022). Counter-Unmanned Aerial Vehicle Technologies in Asia: An Overview. Asian Security Studies, 8(2), 123-140.