A study on the development directions of a smart counter-drone defense system based on the future technological environment

Jindong Kim [1], Jonggeun Choi[1], and Hyukjin Kwon[2*]
[1] Department of Safety Engineering, Seoul National University of Science and Technology
Seoul 01811, Republic of Korea
[e-mail: nolza1234@naver.com]
[2] Department of Safety Engineering, Seoul National University of Science and Technology
Seoul 01811, Republic of Korea
[e-mail: kwonhj@seoultech.ac.uk]
[*]Corresponding author: Hyukjin Kwon

Received February 12, 2024; revised May 14, 2024; accepted June 12, 2024; published July 31, 2024

Abstract

The development of drones is transforming society as a whole and playing a game-changing role in warfare. However, numerous problems pose threats to the lives and safety of people, and the counter-drone system lags behind the rapid development of drones. Most countries, including South Korea, have not established a reliable counter-drone system in response to the threat posed by numerous drones. Due to budget constraints in each country, an Analytic Hierarchy Process (AHP) analysis was conducted among a group of experts who have been involved in policymaking and research and development related to counter-drone systems. This analysis aimed to determine the priority of building a counter-drone system. Based on various research data, the counter-drone system was analyzed in three stages: detection/identification, governance, and response. The hierarchical design mapped out the existing researched counter-drone technology into a hierarchical model consisting of 31 evaluation criteria.

The conclusion provided a roadmap for establishing a counter-drone system based on the prioritization of each element and considering factors such as technological advancement, outlining directions for development in each field.

Keywords: Analytic Hierarchy Process (AHP), Drone, Counter-drone, Governance, Detection/Identification, Response

1. Introduction

1.1 Background and Objectives of the Study

The development of drones poses a threat to people's safety and raises numerous issues. Particularly, the ongoing invasion of small drones by countries is significantly impacting national security [1]. However, except for a few countries, most nations lack a proper counter-drone system in place.

The U.S. plans to spend $4.5 billion by 2026, but achieving a comprehensive response won't be easy [2]. As evidenced by the fact that Ukraine's drone interception level during the Russia-Ukraine conflict was around 30% [3], it is evident that establishing a reliable counter-drone system is not easy. Various literature reviews indicate the necessity of establishing a national-level counter-drone system, yet current research and system development efforts remain inadequate [4].

Existing studies on counter-drone systems have been limited to specific facilities or have focused on drone terrorism and the utility of certain technologies, thus presenting limitations in establishing a national-level large drone system. This study, however, utilizes the Analytic Hierarchy Process (AHP) technique to evaluate the relative importance of each aspect of the counter-drone system based on the technological level, as measured by expert groups. By doing so, the study presents directions for national-level construction, offering a comprehensive approach to establishing a complete counter-drone system [5].

1.2 Scope and Methodology of the Research

The scope of the research encompasses the necessity of national-level construction for the establishment of a complete counter-drone system. To achieve this, the research focuses on the construction of a counter-drone system considering both peacetime and wartime scenarios. If we consider the establishment of a comprehensive counter-drone system as the dependent variable, the technological level of the counter-drone system can become an independent variable, as the counter-drone system is greatly influenced by scientific and technological changes. The research model analyzed the limitations of existing studies, as shown in **Table 1**, and then utilized advanced counter-drone technology to prioritize factors through the Analytic Hierarchy Process (AHP). Subsequently, it assessed the priorities for the construction of counter-drone system and suggested directions for its development.

Table 1. The research model

Existing Research		This Study		
- Consideration only during peacetime - Emphasis on the utility of specific technologies - Analysis of only a part of the counter-drone system	→	- Consideration during both peacetime and wartime - during both peacetime and Wartime - Analysis of the entire counter-drone system	→ AHP	- Determination of technology priorities - Proposal of development directions for the counter-drone system

In the following section, we will examine the concept of counter-drone systems, including their success and failure cases, and the level of technology in detail.

2. Theoretical background

2.1 The concept of counter-drone system

Drones were developed in the United Kingdom in the 1930s for anti-aircraft artillery training purposes during World War II. Recently, they have been combined with various advanced technologies [6], the use of drones in both military and civilian sectors is also increasing exponentially [7]. This has led to many problems, such as their use in terrorism and as a means of attack [8].

Terms used in relation to drone countermeasures include Anti-Drone and C-sUAS(Counter-small unmanned aircraft systems) [9, 10]. Anti-drone is defined as a comprehensive response activity at the legal, institutional, and technical levels to prevent, detect, and block acts that infringe on public welfare and order, such as crime or terrorism caused by drones [11-13]. According to a press release from the Patent Office, an anti-drone is a drone that neutralizes ‘bad’ drones, which cause problems such as terrorism, crime, invasion of private areas, surveillance, and accidents due to inexperienced operation [14]. Meanwhile, many scholars have defined anti-drones as a defense system against illegal drones [15].

In recent years, the term "counter-drone" has begun to be used. In November 2019, the U.S. Secretary of Defense designated the Department of the Army as the agency responsible for C-sUAS, The Army established the Joint C-sUAS Office (JCO) [16]. Subsequently, in January 2021, the US Department of Defense released a report on the strategy for countering small UAV systems, which specified the term "Counter-Drone" [17].

If we consider the dictionary definition, 'Anti' means 'to oppose,' encompassing various meanings. On the other hand, 'Counter' implies being 'against ~,' indicating a clear response to drones [18]. Furthermore, given the technical, operational, and institutional aspects, this study defines the term 'Counter-Drone System,' encompassing response behavior, technology, operations, and institutional significance.

2.2 Success and failure cases of counter-drone systems

The threat of drones is steadily increasing, and establishing an effective counter-drone system is not easy. Therefore, in order to construct a more effective counter-drone system, we seek to derive lessons from both domestic and international cases of success and failure.

Depending on the situation, drones are employed for various purposes, including military applications and terrorism through the use of civilian drones [19, 20]. The Russian-Ukrainian war stands out as a conflict where counter-drone systems, alongside drones, have been actively deployed, shifting the nature of warfare from human-centric to unmanned combat systems. Russia has utilized drones such as the Zala Kyb, Eleron-3SV, Orlan-10, and Kronshtadt Orion, while employing counter-drone systems like the Borisoglebsk 2 MT-LB a jamming and spoofing electronic warfare system and the R-330Zh Zhitel. Ukraine, on the other hand, operated drones like the A1-SM Fury, Leleka-100, Switchblade, and Barilactar (TB2). The effective use of drones, coupled with various U.S. and NATO supported counter-drone systems, has been evident.

The successes and failures of both domestic and foreign counter-drone systems underscore the challenges in responding to drone threats and the human and material damage resulting from drone attacks. A notable overseas success story is the Ukrainian military's "Anti-Drone Mobile Group" during the Ukraine-Russia war. Using observation equipment carried by the fighters, they identified and targeted drones, successfully intercepting dozens of Russian Shahed-136s with conventional weapons systems. This illustrates that effective countermeasures can be implemented even without high-tech weaponry, emphasizing the importance of strategic

tactics [21, 22]. In Korea, there was an incident in the early 23rd century where a drone infiltrated the THAAD base in Seong-ju and was subsequently neutralized using a jamming gun [23].

However, an international failure occurred in September 2019 when Houthi rebels in Yemen attacked an Aramco refinery in Saudi Arabia with 10 drones, leading to a significant impact on global oil prices. This event highlights the vulnerability to drone ambushes and the potential for substantial damage, even from inexpensive drones [24]. Additionally, in Korea, there was a case in December 22 where a North Korean drone ambushed and could not be neutralized, causing security concerns among the population. This underscores the urgency of modernizing weapon systems and establishing a unified command and control system [25].

2.3 Counter-drone system and the level of counter-drone technology

The counter-drone system is presented diversely in various studies, but a common procedure can be categorized into three stages: detection, identification, and response [26, 27]. According to a press release from the Korean Intellectual Property Office, the counter-drone technology is presented as detection, identification, and neutralization. The U.S. Department of Homeland Security's Science & Technology Directorate specifies Detect, Find/Track, Classify/Identify, and Mitigate in the technical guide to counter manned Aerial Vehicle countermeasures [28]. The U.S. Journal of International Aeronautics and Space Science describes Counter-UAS as a two-fold procedure: detection and engagement [29]. The classification of counter-drone systems varies among existing research. However, what commonly takes place is command and control or decision-making for response after initial detection and identification. In other words, it can be seen as occurring in the sequence of detection/identification, decision-making, and response. This study proposes a three-stage system of detection/identification, governance, and response by adding a decision-making stage for detection/identification and response [30].

2.3.1 Detection / identification technological capabilities

The detection/identification systems can be broadly divided into passive systems and active systems. The passive system is classified as a method of establishing pre-registration, geo-fencing, a legal system, and a dedicated organization in a way that does not directly act on the drone.

(1) Pre-registration assigns an ID to the drone, owner, pilot, etc., and reports the operator's information to the public institution in advance and registers. It is a method of attaching a registered chip or PIA identification device to the drone [31]. As the use of drones has expanded, most countries have recently adopted drone real-name registration systems.

(2) Geo-fencing is a technology that installs pre-prohibited zone information in the drone's firmware or memory so that it does not automatically fly in the prohibited area [32]. It can be used for a variety of purposes, such as ensuring safety from overhead power lines or tall buildings that could threaten the flight of a drone.

(3) The legislative system is a system that allows legal measures, such as punishment for flights other than authorized drone flights.

(4) The establishment of a dedicated organization is to create an organization that can professionally respond to unauthorized drone flights. The advantages and disadvantages of this passive system are shown in **Table 2**.

Table 2. Passive detection/identification system.

Category	Merit	Disadvantages and limitations
Pre-registration (Chip, enemy and friend identification) [33, 34]	- Early identification of drones is feasible - Control and management are convenient	- Limited confirmation upon removal of attached equipment - Additional costs incurred for separate equipment attachment
Geo-fencing [35]	- Preventing illegal flights in advance	- Additional costs incurred for separate equipment attachment - Loss of original purpose upon functional incapacitation
Supplementation of the legislative System	- Legal measures against illegal drone operators	- Excessive strictness can act as an impediment to the advancement of drones
Establishment of a dedicated organization [36-38]	- Control by professional personnel - Reduction in efforts of a separate organization	- Budget necessary for organization maintenance

Active detection/identification systems include radar, RF scanners, EO/IR, and acoustic detection technologies [39-41]. (1) Drone detector radar technology scans and detects radar signals emitted from drones. It is effective for drones of medium size and above, but distinguishing small drones from birds is challenging, leading to limitations in detection [42] in recent years, stealth technology has improved to disable conventional radars, and quantum radar technology is actively being researched. (2) The RF scanner is a technology that detects the communication frequency between the drone and the drone pilot. Recently, it has been operated as part of an integrated counter-drone defense system. (3) EO/IR technology captures the movement of drones through day and night cameras. (4) Acoustic detection technology detects the sound emanating from the drone's engine or motor to calculate the direction. It is a technology that finds and identifies the same sound in a sound database [43-44]. Recently, the trend is to accumulate a database of various noises generated in urban environments and remove the accumulated noise database when detecting drones, making it easier to identify the noise generated by drones. The advantages and disadvantages of the active system are shown in **Table 3**.

Table 3. Analyze the advantages and disadvantages of active detection/identification schemes

Category	Merit	Disadvantages and limitations
Radar [45-49]	- Long-range detection/identification - Simultaneous tracking of multiple targets - Minimal susceptibility to weather conditions	- Limitations in detecting small airborne objects - Tracking constraints for Ground Control Station (GCS) - Occurrence of blind spots - High cost
RF Scanner [50-52]	- Detect of specific radio frequencies - High accuracy - More cost-effective than radar	- Limitations in detecting autonomous flying drones - Detection restrictions beyond ISM frequencies - Restricted drone detection at a time
EO/IR [53, 54]	- Relatively accurate detection/identification through visual imagery	- Operates only within the visible range - Low recognition rate and short detection distance due to camera limitations
Acoustics Detection [55-57]	- Detectable based on sound characteristics - No interference with other devices	- Affected by ambient noise - Detection limitations without a database

No detection/identification technology is perfect. Different technologies have different strengths and weaknesses, However, as shown in **Table 4**, by measuring the capabilities of radar, RF scanners, optical/infrared, acoustic, and combined sensors against seven criteria (range/capability, accuracy, tracking, discrimination, and hovering/autonomous targets), the study shows that combined sensors are the most effective technology to meet all criteria.

Table 4. The power of detection sensor technology [58]

Category	Radar	RF Scanner	EO/IR	Acoustics Detection	Composite Sensors
Detection Range	○	△	△	△	○
Detection	○	△	△	○	○
Accuracy	○	△	△	X	○
Tracking	○	○	△	△	○
Discernment	△	△	△	X	○
Hovering Targets	○	○	○	○	○
Autopilot Targets	○	X	○	○	○

2.3.2 Governance technology proficiency

There are three options for governance: decentralized, centralized, and hybrid. (1) The decentralized type involves responding to the counter-drone system based on the judgment of the person in charge of the facility or organization. (2) A centralized system is controlled by an organization established by law. (3) The hybrid type is a method that integrates the advantages of both the decentralized and centralized types. The advantages and disadvantages of each governance method are shown in **Table 5**.

Table 5. Analyze the advantages and disadvantages of governance

Category	Merit	Disadvantages and limitations
Decentralized	- High flexibility - Low interference from other agencies	- High costs involved - Possibility of duplication with other assets during response
Dictatorial	- Minimization of asset duplication - Easy sharing of the latest information	- Challenges in developing an integrated system - Legal issues such as responsibilities and authorities
Hybrid	- Applicable in various situations - Effective asset management	- Difficulty in legal actions and agreements - Agreement needed on the scope of authority establishment

2.3.3 Response technology proficiency

Hard-kill is a method of countering drones through direct physical contact, and means can include anti-aircraft guns, nets, drone killers, and high-powered lasers. (1) Anti-aircraft guns use direct fire to shoot down drones [59]. In recent years, AHEAD warheads have been developed in a form that allows flexible separation of warheads, considering the speed and distance of the drone. (2) Nets can be used to neutralize drones by firing a net from a drone countermeasure gun or drone. There have been advancements, such as hanging nets from drones to catch [60-62]. An excellent example is the "Drone Catcher" by The Netherlands, which uses a net attached to a drone to catch it, preventing secondary damage [63]. (3) A drone killer is a technology that launches a drone to directly collide with and disable an unauthorized drone. These drone killers are highly destructive because they carry explosives for their attacks [64]. (4) High-powered laser technology uses laser beams generated by op-tics to directly irradiate and neutralize drones [65, 66]. The U.S. has developed laser weapons in the 300 kW class, and Korea has developed laser weapons in the tens of kW class. The advantages and disadvantages of hard-kill means are shown in **Table 6**.

Table 6. Analyze the advantages and disadvantages of responding with hard-kill measures

Category	Merit	Disadvantages and limitations
Anti-Aircraft Guns [67]	- Economical - Capable of anti-aircraft weapon deployment by military units	- Possibility of dud rounds - Potential for civilian casualties
Nets [68-70]	- Highly accurate - Capable of semi-automatic launching	- Short range - Low effectiveness against drone swarms
Drones Killer [71, 72]	- Excellent cost-effectiveness	- Potential for civilian casualties
High Power Laser [73-75]	- Highly accurate - Quick reload and rapid response - Effective against modified drones	- High development and operational costs - Potential for collateral damage

Soft-Kill is a method of responding through non-physical contact. Common methods include jamming, high power microwave (HPM), and spoofing. (1) There are two forms of jamming: RF jamming and GNSS jamming [76, 77]. Jamming emits electromagnetic noise at high power to interfere with radio frequencies or satellite communication links, causing drones to hover in place, stall, fall to the ground, or even return to the drone pilot [78, 79]. More recently, these jammers have been miniaturized for individual combatant use. (2) HPEM (High Power Electromagnetic Wave) is a technology that fires powerful electromagnetic waves to burn out and disable the electronic circuits and components of a drone [80, 81]. Recently, it has been commercialized in various fields and is being utilized in counter-drone systems. (3) Spoofing technology involves hacking into a communication link and sending out stronger radio waves to produce false location and visual information. This is a way to take control of the drone and indirectly steer it [82]. Recently, spoofing has become more advanced and sophisticated by fusing with the electromagnetic spectrum. The advantages and disadvantages of soft-kill techniques are shown in **Table 7**.

Table 7. Analyzing the advantages and disadvantages of soft-kill countermeasures

Category	Merit	Disadvantages and limitations
Jamming [83]	- Low cost - Securely capture the drone intact	- Short range - Interference with other wireless communications
HPEM [84]	- Definitely neutralize upon hit - Damage only electronic equipment	- High cost - Potential secondary damage to nearby electronic devices
Spoofing [85, 86]	- Low cost - Safely confiscate the drone	- Impact on GNSS-equipped devices - Ineffective against autonomous drones

Combat technology is how we respond through training and doctrinal development. The art of warfare consists of two main components: doctrinal development and training. (1) Doctrine is a way of fighting based on lessons learned from various wars. It must be developed before tactical considerations can be applied to the conduct of warfare. This ensures that training aligns with the intended approach to warfare. (2) Training involves the repeated mastery of a fighting method so that conditioned reflexive behaviors emerge.

2.4 Previous Research and Its Relevance

Most of the research focuses on counter-drone systems for critical infrastructure like airports, drone terrorism, and the efficacy of specific technologies. Here's an overview:

◦ Barbora Kotkova proposed airport defense systems [87].

◦ Naveen Kumar Chaudhary reviewed relevant laws and regulatory issues, suggesting improvements [88].
◦ Yaseen N. Jurn, Sawsen A. Mahmood, Jaafar A. Aldhaibani analyzed various anti-drone technologies and key factors for selecting them, considering the diverse operational technologies of drones [89].

Analyzing prior research reveals four commonalities that help identify limitations. Firstly, most studies analyze counter-drone systems in peacetime contexts. By focusing on peacetime systems, these analyses tend to address counter-drone systems for defense against drone attacks related to crimes such as terrorism or intrusion into critical infrastructure. Secondly, the constructed counter-drone systems are facility-oriented rather than at a national level. Thirdly, while numerous counter-drone system technologies exist, many studies have proven the effectiveness of fragmented technologies. Fourthly, studies predominantly propose physical response technologies such as weapon systems. This study aims to overcome all identified limitations in prior research and propose a comprehensive approach, thereby advancing to a new perspective and level of research.

3. Research Methods

3.1 Research Framework and Hypotheses

3.1.1 Research Framework

The Analytic Hierarchy Process (AHP), proposed by Thomas L. Saaty in 1976, is a tool that provides logical support for decision-making on complex, multi-criteria problems [90, 91]. The process of AHP consists of five steps: (1) Designing for 'hierarchy', (2) Steps to determine the preference of each criterion through cross-comparison [92-94], (3) Steps to calculate relative importance [95], (4) Steps to check confidence with sensitivity analysis, (5) Synthesizing responses from multiple experts. Therefore, AHP is highly significant as it allows for the hierarchical classification of various attributes of counter-drone systems, enabling the determination of the relative importance of each attribute. This facilitates the identification of relatively more important counter-drone systems, making it easier to prioritize them. Additionally, AHP serves as a valuable analytical technique for determining how to effectively allocate limited resources across different areas, thereby confirming its utility.
To design the AHP hierarchy, various sources such as previous research and cases from advanced military nations were utilized to understand the balanced construction of detection, governance, and response for a comprehensive counter-drone system. Considering that the effectiveness of a counter-drone system heavily depends on technological advancements, technological trends were identified as independent variables and included as evaluation criteria. Furthermore, experts were surveyed during a preliminary investigation to ensure thorough validation of the evaluation criteria.

3.1.2 Research Hypotheses

To establish a comprehensive counter-drone system, balanced development of detection, governance, and response technologies is essential. However, the completeness of such a system is heavily influenced by scientific and technological advancements. Therefore, considering the analysis of counter-drone technology trends, it is necessary to prioritize the

aspects considered important by experts through a comprehensive analysis of detection, governance, and response technologies, rather than solely focusing on the application of specific technologies. Additionally, it is crucial to provide a direction for development, taking into account future environmental considerations.

3.2 Manipulative Definition of Variables and Construction of Measurement Tools

3.2.1 Dependent variable

In counter-drone systems, achieving completeness is possible when detection/identification, governance, and response are constructed in a balanced and mutually complementary manner. However, analysis of previous research and national counter-drone systems reveals inadequate balance in construction. To achieve balanced construction, it is necessary to analyze the technologies of detection/identification, governance, and response, and provide priority judgments and construction directions at the national level.

3.2.2 Independent variable

In the construction of a comprehensive counter-drone system, technological development trends exert significant influence. In this study, we have established technological factors as independent variables based on the global trends, success and failure cases of detection/identification, governance, and response technologies analyzed earlier. By considering the level of scientific and technological advancement, we have demonstrated that achieving completeness at the national level through step-by-step development based on priorities is feasible.

3.3 Data collection and analysis procedures

3.3.1 Data collection

The existing counter-drone systems demonstrate effectiveness by applying specific technologies and proposing response measures. However, due to the limitation of various budgets and resources to meet all identified counter-drone system requirements, it is crucial to provide important information for determining where to concentrate resources. Therefore, counter-drone technology should provide valuable information for establishing relative priorities in constructing counter-drone systems for more systematic resource allocation. Thus, unlike previous studies that apply fragmented counter-drone technologies, this study aims to determine the priorities of each item in the overall counter-drone system as perceived by expert groups and to draw a blueprint for early construction of the counter-drone system through concentration and savings. To achieve this, the Analytic Hierarchy Process (AHP) technique was utilized to gain a clearer understanding of priorities among expert groups.

3.3.2 Survey

The survey was conducted from May 15 to June 2, 2023, and the questionnaire was administered through in-person interviews and emails. The MS-Excel program was utilized as the analysis tool, and the Expert Choice 2000 Industrial Edition software was employed for verification purposes. The AHP analysis survey was conducted with experts who have more than 20 years of experience at three national research organizations specializing in policy studies and technology development for counter-drone systems. The participants included a

doctoral researcher currently engaged in researching and developing various countermeasure technologies, a military columnist and broadcaster with expertise in drones and counter-drone systems, five university professors who have published numerous research papers and proposed policies in the counter-drone field, and military experts with over 20 years of experience, including those involved in drone policy research and electrification in the counter-drone domain. The survey participants were interviewed in person, and for those with scheduling constraints, additional interviews were conducted via email, resulting in a response rate of 25 out of 25. With no non-responses, the reliability of the survey can be considered high.

Table 8. Who and how to survey

Category	Number of samples	Research methods
National Research Institution for Counter-Drone Systems	5	In-Person Interview Research, Email
Counter-Drone System Development Company	5	
Drone and Counter-Drone System Specialist Broadcaster	3	
University Professor Researching Counter-Drone Systems	5	
Military Personnel Involved in Counter-Drone System Operations	7	
Total	25	

3.3.3 Analysis procedure

The importance evaluation criteria for establishing counter-drone systems are structured as shown in **Fig. 1**. Firstly, detection/identification is divided into passive and active methods. Passive methods are further subdivided into pre-registration, geo-fencing, legal systems, and dedicated organizations. Active methods include radar, RF scanners, EO/IR, and acoustic detection. Secondly, in terms of governance classification, Sambamurthy and Zmud applied the IT governance structure of centralized, decentralized, and federal, which represent various decision-making forms [96]. Another term for federalism is hybridization [97]. Thirdly, countermeasures can be divided into hard-kill, soft-kill, and combat performance. Hard-kill includes anti-aircraft guns, nets, drone killers, and laser technology; soft-kill includes jamming, electromagnetic waves, and spoofing countermeasures; and combat performance includes doctrine development and training.

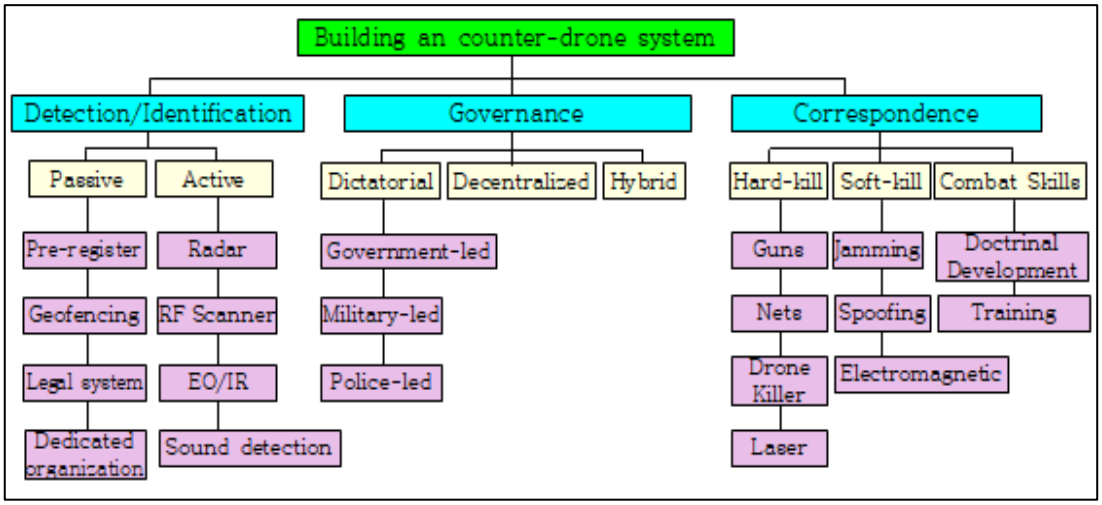

Fig. 1. Deriving AHP metrics

All evaluation criteria in AHP have a hierarchical relationship, and we aimed to ensure logical consistency through objective judgment and sensitivity analysis. To achieve this, we evaluated the importance of each field by conducting dyadic comparisons, comparing two items to each other on a 9-point scale. The relative importance was assigned on a scale from 1 to 9.

The relative importance, or weight, of n evaluation criteria can be obtained by constructing a pairwise comparison matrix A, which is an n×n square matrix.

The final score, denoted as Bn, is calculated by multiplying each element of the initial pairwise comparison matrix by its weight and then adding them together. In other words, if the column vector of weights W_1, W_2, ... , W_n is called W, it can be denoted as A·W. In this study, individual consistency in the overall assessment results was set to be less than 0.1, and respondents with consistency exceeding 0.1 underwent reevaluation to enhance reliability. Survey results with consistency ratios below 0.1 indicate high reliability.

Table 9. Consistency ratio of expert survey results

1	2	3	4	5	6	7	8	9
0.0464	0.0529	0.0597	0.0398	0.0283	0.0489	0.0309	0.0227	0.0448
10	11	12	13	14	15	16	17	18
0.0634	0.0836	0.0239	0.0307	0.0423	0.0588	0.0277	0.0642	0.0547
19	20	21	22	23	24	25		
0.0623	0.0367	0.0245	0.0425	0.0389	0.0422	0.0564	-	-

4. AHP Analysis Results and Development Directions for Counter-Drone Systems

4.1 Dependent variable (Detection/Identification, Governance, Response) AHP results

The final scores were divided into civilian, military, and overall expert groups. The scores for each of these evaluation areas were then used to identify priorities, as shown in **Table 10**.

Table 10. Relative importance and priority of evaluation factor

Classification	Private professionals		Military professionals		Total	
	Importance	Priority	Importance	Priority	Importance	Priority
Detection/Identification	0.5261	1	0.6467	1	0.5639	1
Governance	0.1819	3	0.1100	3	0.1576	3
Correspondence	0.2920	2	0.2433	2	0.2786	2

The aggregate results of the importance of the evaluation factors reveal that detection/identification, response, and governance are the key components. Notably, both civilian and military experts concurred that detection/identification holds the utmost significance. The analysis indicates that detection/identification is considered the most crucial factor, as it determines whether the subsequent steps in the drone system can be effectively implemented.

4.2 AHP results for independent variables

When prioritizing smaller items, there were instances where the perspectives of civilian and military experts differed. Some items may have more evaluation factors than others, potentially causing some errors, but the overall direction remains consistent, as demonstrated in **Table 11**.

Table 11. Small items Relative importance and priority of evaluation factor

Middle items	Small items	Private professionals		Military professionals		Total	
		Importance	Priority	Importance	Priority	Importance	Priority
Passive	Pre-register	0.0298	7	0.0190	11	0.0262	7
	Geo-fencing	0.0162	12	0.0112	15	0.0146	14
	Legal system	0.0262	8	0.0522	4	0.0324	4
	Dedicated organization	0.0123	14	0.0242	7	0.0151	13
Active	Radar	0.1046	1	0.1898	1	0.1260	1
	RF Scanner	0.0617	3	0.0529	3	0.0594	3
	EO/IR	0.0923	2	0.1016	2	0.0957	2
	Sound detection	0.0234	9	0.0225	8	0.0233	8
Dictatorial	Government-led	0.0106	17	0.0043	18	0.0081	18
	Military-led	0.0110	15	0.0076	16	0.0099	17
	Police-led	0.0049	20	0.0018	20	0.0036	20

Decentralized	-	-	-	-	-	-	-
Hybrid	-	-	-	-	-	-	-
Hard-kill	Guns	0.0101	18	0.0117	14	0.0106	16
	Nets	0.0054	19	0.0037	19	0.0049	19
	Drone Killer	0.0108	16	0.0167	12	0.0124	15
	Laser	0.0173	11	0.0407	5	0.0225	9
Soft-kill	Jamming	0.0397	4	0.0058	17	0.0225	9
	Electromagnetic	0.0364	5	0.0152	13	0.0282	5
	Spoofing	0.0304	6	0.0198	10	0.0269	6
Combat Skills	Doctrinal Development	0.0191	10	0.0204	9	0.0197	11
	Training	0.0158	13	0.0236	6	0.0179	12

The weighted importance of details in the detection/identification phase, when combining the results of both civilian and military experts, reveals that radar, EO/IR, RF scanners, legal systems, pre-registration, acoustic detection, task forces, and geo-fencing are the top five most commonly perceived threats. In the governance middle items, the prioritization is as follows: hybrid, centralized, and decentralized. Within the regime, both civilian and military experts ranked military-led, government-led, and police-led in that order. In the response phase, civilian experts emphasized that the three Soft-Kill countermeasures were of utmost importance. An analysis of patented technologies related to drones from 2009 to 2019 showed that jamming is the most common patent application in each country [104]. On the other hand, military experts highlighted the importance of effective laser technology for countering swarm drones in the future. Training and doctrinal development were also identified as crucial factors.

4.3 Establishment Roadmap and Development Direction for Counter-Drone System

It was possible to confirm the priority of AHP analysis results for each evaluation factor. However, it may not always be feasible to unconditionally apply the highest priority due to technological and budgetary limitations. Therefore, while prioritizing the results of AHP analysis, it is intended to establish a roadmap for the construction of a counter-drone system, taking into account factors such as the current level of science and technology, in order to systematically advance it.

Table 12. Roadmap for establishing counter-drone systems (considering AHP results, technology level, etc.)

Separation	Short-term (~'25 years)	Mid-term ('26-'28)	Long term ('29 years~)
Detection / Identification	4) Legal system 7) Pre-register	1) Radar 2) EO/IR 3) RF Scanner 8) Sound detection 14) Geo-fencing 13) Dedicated organization	-
Governance (Hybrid types)	21) Setting up permissions and responsibilities 22) Information sharing scope	20) Governance 23) Information Distribution System	24) AI Command and Control
Correspondence	9) Jamming 11) Training 12) Doctrinal Development 19) Nets	5) Electromagnetic 6) Spoofing 16) Guns	10) Laser 15) Drone Killer

In the detection/identification phase, the short-term challenge lies in determining the legal system and pre-registration. This is because experts prioritize these aspects, and their implementation doesn't require significant effort. Establishing a pre-registration system for civilian drones and reinforcing it with legislation can be accomplished in a short period, given sufficient parliamentary consensus. Medium-term priorities include radar, EO/IR, RF scanners, acoustic detection, a dedicated organization, and geo-fencing. This is crucial for advancing detection/identification technology promptly, elevating the technological capabilities of enemy drones, and ensuring the protection of the public.

Based on this roadmap, the following areas could be further developed or enhanced in the detection/identification phase: First, there is a need for legal and regulatory enhancements. Mitigating the threat of drones necessitates a robust legal framework for controlling hostile drones [98]. The key laws that require supplementation concerning drones include the Aviation Safety Act, the Radio Act, the Military Base Act, and the Personal Information Protection Act. There is also a need to supplement penalties for using drones to commit other crimes. Moreover, considering the limitations of incorporating everything into each existing law, it is essential to enact a separate drone law. This law can serve as a standard for the future drone system, providing a comprehensive framework to address the evolving challenges posed by drones.

Second, it is crucial to evolve into an integrated defense system utilizing complex sensors. AHP analysis highlights that detection/identification is the most critical aspect of building a counter-drone system. Without achieving effective detection/identification, subsequent steps involving command, control, and response become futile. In our interviews with experts, we discovered that the most effective approach is through a combination of the following methods [99]. Currently, numerous efforts to establish such a complex defense system have been identified in domestic private companies, even though the detection/identification distance remains limited [100].

Third, there is a need to maximize the standardization and interoperability of detection/identification technologies [101]. To integrate the best aspects of each technology, essential elements must be standardized, enabling interoperability with other systems. To achieve this, standardization criteria for each technology must be established. Operational capabilities should be presented in a manner that facilitates seamless integration with existing systems, ensuring synergistic effects through the combination and scalability of various technologies.

Fourth, the active implementation of AI systems in detection/identification technologies is essential. Recent artificial intelligence (AI) capabilities prove highly useful in identifying and categorizing drones within the airspace, offering a robust solution, particularly for illegal drones [102]. Deep learning technologies enhance the effectiveness of existing detection/identification techniques [103, 104]. The system should be designed with the concept of applying an AI system that has learned from a database and promptly integrating it into the command and control system after detection/identification. The accuracy and time savings achieved through AI in drone detection/identification are crucial for tracking and responding to drones. AI trained with state-of-the-art object detection algorithms will enhance the integrity of the counter-drone system. To achieve this, it is imperative to build various databases in advance and ensure their readiness for early implementation [105-107].

At the governance level, the AHP analysis conducted by experts suggests that a hybrid approach would be feasible for Korea. Various issues need resolution for the control system. As a short-term task, it is necessary to establish the authority and responsibility of each organization, along with determining the extent to which flight information should be shared

for civilian and military drones. As a medium-term task, it was determined that the control system and information distribution system should be addressed. In the future, with the rapid increase in the number of drones, there will be a need to integrate UTM (Unmanned Aircraft System Traffic Management), UAM (Urban Air Mobility) urban air traffic, and AAM (Advanced Air Mobility). In the long run, it is anticipated to evolve into a command and control system controlled by AI in real-time.

Based on this roadmap, the following areas could be further developed or enhanced in the governance phase: Firstly, a system should be established to share and distribute information at government, military, executive branch, and critical facility levels. Many experts also identified technical, physical, operational, and integration as the most critical issues to address [108]. The completeness of the command and control system is achieved when all systems are interconnected using software that enables seamless interoperability. Additionally, for the comprehensive functionality of this command and control system, ensuring the Internet of Drones (IoD) is crucial to ensure seamless communication and independence from cyberattacks, etc. [109, 110].

Secondly, with the ongoing urbanization, numerous national critical facilities, government offices, and densely populated areas are distributed throughout the country. In response to the escalating threat of drones, we are constructing a counter-drone system for each facility. The drone systems implemented at each of these facilities form a dense web, and with effective coordination, they can collectively establish a national drone defense network, as illustrated in **Fig. 2**.

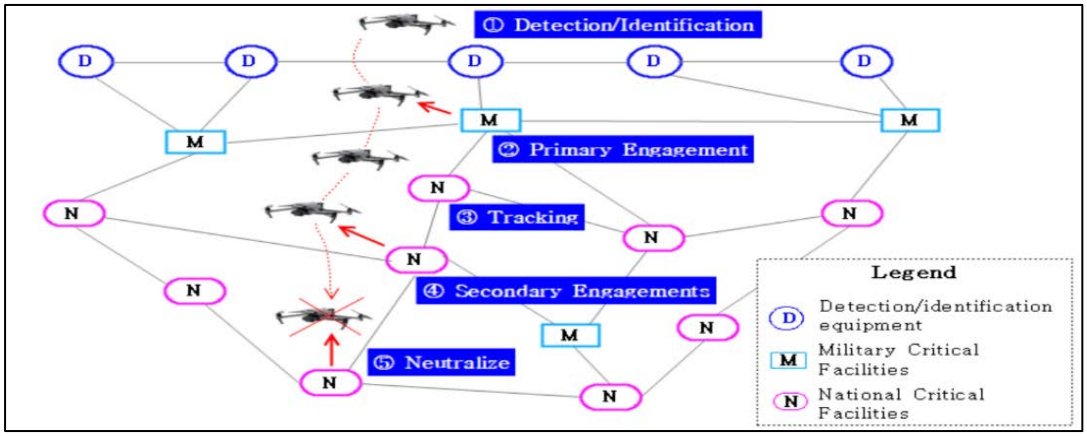

Fig. 2. National counter-drone defense network concept map

Thirdly, there is a need to establish an AI-type governance system. Given the speed of drones, time is a critical factor. The current system requires a significant amount of time to make command decisions, posing challenges in responding effectively. Hence, it is essential to develop an AI-type governance system capable of supporting real-time command decisions. AI command and control systems can play a crucial role in identifying critical nodes within a swarm of drones to prevent them from splitting into multiple unconnected clusters, thus preserving their coordinated capabilities [111]. Additionally, it is essential to establish a governance system that fully considers the legal and ethical issues related to AI.

In the response phase, short-term tasks include jamming, training, doctrinal development, and netting. Jamming is well-developed and ready for immediate use. Although education, training, and doctrine development are considered a medium priority in the experts' ranking, they are reflected as short-term tasks because they can be completed quickly. Netting technology is

currently commercialized and widely used in other countries. Medium-term challenges are categorized as electromagnetic, spoofing, and anti-aircraft. Electromagnetic waves and spoofing are based on a comprehensive consideration of the current state of technology, the development trend of enemy drones, and friendly targets. The anti-aircraft gun utilizes existing firearms, but considers the time required to develop ammunition such as dispersed ammunition that doesn't risk falling apart and can take down even clustered drones [112]. Long-term challenges encompass lasers and drone killers. Developing lasers will take some time given the current state of the art, but they are considered the most effective alternative to swarming drones [113]. Drone killers could provide a more precise countermeasure if developed to operate as swarm drones, targeting only the enemy UAVs they need to take down.

Based on this roadmap, the following areas could be further developed or enhanced in the response phase: Firstly, it is crucial to ensure various flexibilities through the standardization and modularization of different response systems. Modularity is known for its scalability and cost-effectiveness [114]. Notably, standardization becomes essential for the rapid development and upgrades of technologies in the competitive landscape between drones and counter-drone systems. Another approach to achieving standardization and modularization is the development of software that enables different hardware components to work together, even if they do not interoperate in the same way. However, even with software integration, there is a need to standardize combat loads and Lego blocks to some extent, ensuring they can be combined as robustly as Lego blocks for infinite scalability [115].

Secondly, there is a need to change the perception of counter-drone systems. The prevailing notion that counter-drone operations are solely conducted by air defense forces or specific individuals requires a shift.

Thirdly, it is essential to develop a foundational doctrine for counter-drone systems. Once the doctrine is in place, combat methods can be established by applying tactical considerations derived from the doctrine of each service. This is crucial for enabling field units to identify training challenges and incorporate them into their training programs, ensuring behavioral mastery. For instance, countering a forward area with a fence might involve using a barrier like Sky Fence [116], adopting a corridor-based response for airborne penetration in contact areas. It is necessary to develop a concept of selection and concentration, such as establishing a three-zone response framework for each protective facility in metropolitan areas and major installations.

5. Conclusion

In order to construct a rapid and effective counter-drone system within limited resources, prioritization becomes imperative. To address this, the present study employed the Analytical Hierarchy Process (AHP) technique to distinctly identify the priorities in building an anti-drone system through the expertise of a group of professionals. The hierarchical design established a layered model for evaluating existing researched counter-drone technologies across 31 assessment criteria. The analysis of the counter-drone system is categorized into detection/identification, governance, and response, with governance recognized as a distinct step not included in earlier investigations.

As a strategy to establish a counter-drone system, (1) in the detection/identification stage, the focus should be on reinforcing laws and institutions, developing an integrated defense system utilizing complex sensors, optimizing technology standardization and interoperability, and actively incorporating AI systems. (2) For the hybrid command and control phase, the proposal includes information sharing and distribution among government agencies, the military, administrative offices, and critical facilities, the establishment of a pan-national anti-drone system linkage system, and the implementation of an AI-type command and control system.

(3) In the response system phase, there is a recognition of the need to standardize and modularize the response system, transform the perception of the counter-drone system, and establish a standardized doctrine related to the counter-drone system.

The limitations of this study may not be universally applicable to all countries. This is attributed to variations in environmental conditions, social characteristics, technology levels, budgets, and decision-making processes that differ across nations and evolve over time. Consequently, the proposed counter-drone system development plan is based on expert opinions, and priorities may be subject to change with advancements in science and technology. However, given the swift evolution of drones, there is a clear understanding of the imperative need to establish a comprehensive counter-drone system. The hope is for the early development of a robust counter-drone system, moving beyond temporary attention and reactive responses when issues arise.

References

[1] Hwang. W. J, "How are drones being flown over the gray zone?," *Defense & Security Analysis*, vol.37. no.3, pp.328-345, 2021. Article (CrossRef Link)

[2] Kang. H, Joung. J, Kim. J, Kang. J, Cho. Y. S, "Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems," *IEEE Access*, vol.8, pp.168671-168710, 2020. Article (CrossRef Link)

[3] Doo. J. h, "An Analysis of Crisis in Ukraine: A Military Discourse on Strengthening Military Jointness," *Defense Policy Research*, vol.138, pp.39-66, 2022. Article (CrossRef Link)

[4] Souli. N., Makrigiorgis. R., Anastasiou. A., Zacharia. A., Petrides. P., Lazanas. A., Valianti. P., Kolios. P., Ellinas. G., "HorizonBlock: Implementation of an Autonomous Counter-Drone System," in *proc. of 2020 International Conference on Unmanned Aircraft Systems*, pp.398-404, 2020. Article (CrossRef Link)

[5] Saaty. T. L, The Analytic Hierarchy Process: Applications and Studies, pp.59-67, 1989. Article (CrossRef Link)

[6] Lee. D.K, Threats and Responses to Drones, Park Youngsa, pp.6, 2021. [Online]. Available: https://www.pybook.co.kr/mall/book/pys?goodsno=6646

[7] Çetin. E, Barrado. C, Pastor. E, "Countering a Drone in a 3D Space: Analyzing Deep Reinforcement Learning Methods," *Sensors*, vol.22, no.22, 2022. Article (CrossRef Link)

[8] Lv. H, Liu. F, Yuan. N, "Drone Presence Detection by the Drone's RF Communication," in *Proc. of Journal of Physics: Conference Series, 2020 2nd International Conference on Electronics and Communication, Network and Computer Technology (ECNCT)*, vol.1738, 2021. Article (CrossRef Link)

[9] Petar. Č, Robert. P, Sanja. M. Č, Milan. G, "Principles of Anti-Drone Defense," in *Proc. of 11th IEEE International Conference on Cognitive Infocommunications* (CoglnfoCom), pp.19-26, 2020. Article (CrossRef Link)

[10] Castrillo. V.U, Manco. A, Pascarella. D, Gigante. G, "A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones," *Drones*, vol.6, no.3, 2022. Article (CrossRef Link)

[11] Lee. D.H, Kang. W, "A Study on the Establishment of Anti-Drone Concept and Effective Response System," *Korean Security Journal*, vol.60, pp.9-32, 2019. Article (CrossRef Link)

[12] Rizk. Y, Awad. M, Tunstel. E.W., "Decision Making in Multiagent Systems: A survey," *IEEE Transactions on Cognitive and Developmental Systems*, vol.10, no.3, pp.514-529, 2018. Article (CrossRef Link)

[13] Chung. T.H., Hollinger. G. A., Isler. V, "Search and pursuit-evasion in mobile robotics," *Autonomous Robots*, vol.31, pp.299-316, 2011. Article (CrossRef Link)

[14] Patent and Trademark Office, Press Release, Anti-Drone to Catch Bad Drones, MAR 29, 2017.

[15] Ka. K.H, Yun. Y.H, Lee. Y.M, "A study on Responsing System against Illegal Drone at Airport," *Journal of the Aviation Management Society of Korea*, vol.19, no.3, pp.109-125, 2021. Article (CrossRef Link)

[16] Secretary of Defense Memorandum, Designation of the Secretary of the Army as the DoD Executive Agent for Counter-Small Unmanned Aircraft Systems for Unmanned Aircraft Groups 1, 2, and 3, November 18, 2019.
[17] Miller, C.C.; U.S. Department of Defense. "Counter-Small Unmanned Aircraft Systems Strategy," 2021. [Online]. Available: https://apps.dtic.mil/sti/citations/AD1127557
[18] [Online]. Available: https://www.wordreference.com/enko/oxford (accessed on 17 August 2023).
[19] Korea Institute of Military Affairs, "North Korean Unmanned Aerial Vehicle (UAV) intrudes air space of Republic of Korea to conduct a monitoring and suveillance of ROK's major military facilities on December 26," *KIMA Newsletter*, no.1385, DEC 30, 2022. [Online]. Available: https://www.kima.re.kr/en/publication.html?Table=ins_kima_newsletter_eng&s=20&mode=view&uid=1409
[20] Kim. H.Y, "North Korea's drone provocation is a test of South Korea's readiness - intended to stoke social unrest," *VOA News*, DEC 27, 2022.
[21] Joseph Trevithick, Ukrainian Teams Hunt Russian Drones With Laser Rifles, Gun Trucks, Apps, The War Zone, Dec. 8, 2022. [Online]. Available: https://www.thedrive.com/the-war-zone/ukrainian-teams-hunt-russian-drones-with-laser-rifles-gun-trucks-apps (accessed on 29 June 2023).
[22] Alya Shandra, Ukraine's National Guard creates mobile anti-drone groups, Euromaidan Press, Aug. 11, 2022. [Online]. Available: https://euromaidanpress.com/2022/11/08/ukraines-national-guard-creates-mobile-anti-drone-groups/ (accessed on 29 June 2023).
[23] Kim. J.W, Drone approaching Seongju THAAD base shot down by US military 'drone gun', Korea Times, Jan. 18, 2023.
[Online]. Available: https://www.hankookilbo.com/News/Read/A20230118101500041 73
[24] Kim. G.G, Drone Terrorism Becomes Reality. Key facilities hit with 3-4kg bombs per unit, Yonhap news, Sep. 16, 2019.
[Online]. Available: https://www.yna.co.kr/view/AKR20190916062100504
[25] North Korean drone: Why it reached Seoul and wasn't shot down, BBC NEWS Korea, Dec. 27, 2022.
[26] Diogo B. Ramos, Denis S. Loubach, Adilson M. da Cunha, "Developing a distributed real-time monitoring system to track UAVs," *IEEE Aerospace and Electronic Systems Magazine*, vol.25, no.9, pp.18-25, 2010. Article (CrossRef Link)
[27] Stary. V, Krivanek. V, Stefek. A, "Optical detection methods for laser guided unmanned devices," *Journal of Communications and Networks*, vol.20, no.5, pp.464-472, 2018. Article (CrossRef Link)
[28] Patel. B, and Rizer. D, "Counter-Unmanned Aircraft Systems Technology Guide," US Department of Homeland Security: Science and Technology Directorate, pp.13-14, 2019.
Article (CrossRef Link)
[29] Wallace. R.J. et al., "Exploring Commercial Counter-UAS Operations: A Case Study of the 2017 Dominican Republic Festival Presidente," *International Journal of Aviation, Aeronautics, and Aerospace*, vol.5, no.2, 2018. Article (CrossRef Link)
[30] Kang. W.K, Chae. I.T, Kye. D.H, "*The Drone Bible*," Planet Media, Seoul, p.325, 2023.
[31] Kim. W.K et al., "Study on Identification of Low-Altitude Small Drones, Frequency Operation Requirements and System Improvements," *National Radio Research Agency*, 2019. [Online]. Available: https://scienceon.kisti.re.kr
[32] Vagal. V, Markantonakis. K, Shepherd. C, "A New Approach to Complex Dynamic Geofencing for Unmanned Aerial Vehicles," in *Proc. of 2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC)*, pp.1-7, 2021. Article (CrossRef Link)
[33] Hermand. E, Nguyen. T.W, Hosseinzadeh. M, Garone. E, "Constrained Control of UAVs in Geofencing Applications," in *Proc. of 2018 26th Mediterranean Conference on Control and Automation (MED)*, pp.217-222, 2018. Article (CrossRef Link)
[34] Zhong. R.Y, Dai. Q.Y, Qu. T, Hu. G.J, Huang. G.Q, "RFID-enabled real-time manufacturing execution system for mass-customization production," *Robotics and Computer-Integrated Manufacturing*, vol.29, no.2, pp.283-292, 2013. Article (CrossRef Link)

[35] AISC, What Is Geofencing, [Online]. Available: https://www.aisc.aero/what-is-geofencing/, Aaccessed on 29 June 2023.
[36] Park. Y, NYPD Creates 'Drone Cop' Unit to Shoot Down Illegal Drones, Dong-A Newspaper, 19 Feb, 2019, [Online]. Available: https://www.donga.com/news/article/all/20190219/94182721/1
[37] Kim. Y.J, "The Air Space System and UVA's Regulation in Japanese Civil Aeronautics Act," *The Korean Journal of Air & Space Law and Policy*, vol.33, no.2, pp.115-168, 2018. Article (CrossRef Link)
[38] Cho. M.S, A police drone to make arrests has arrived, ohmynews, 16 Dec, 2015. [Online]. Available: https://www.ohmynews.com/NWS_Web/View/at_pg.aspx?CNTN_CD=A0002168767, Accessed on 20 June 2023.
[39] Akter. R, Golam. M, Lee. J. M, Kim. D.S, "Doppler Radar-based Real-Time Drone Surveillance System Using Convolution Neural Network," in *Proc. of 2021 International Conference on Information and Communication Technology Convergence (ICTC)*, pp.474-476, 2021. Article (CrossRef Link)
[40] Akter. R, Doan. V.S, Tunze. G.B, Lee. J.M, Kim. D.S, "RF-Based UAV Surveillance System: A Sequential Convolution Neural Networks Approach," in *Proc. of 2020 International Conference on Information and Communication Technology Convergence (ICTC)*, pp.555-558, 2020. Article (CrossRef Link)
[41] Bisio. I, Garibotto. C, Lavagetto. F, Sciarrone. A, Zappatore. S, "Unauthorized Amateur UAV Detection Based on WiFi Statistical Fingerprint Analysis," *IEEE Communications Magazine*, vol.56, no.4, pp.106-111, 2018. Article (CrossRef Link)
[42] Lim. J.C, "How to Counter Threats of North Korean SUAS," *Korea Institute of Military Affairs(KIMA)*, vol.61, pp.5-28, Mar. 2023. [Online]. Available: https://www.kima.re.kr/3.html?html=3-9-3.html&uid=887&s=9
[43] Salvati. D, Drioli. C, Ferrin. G, Foresti. G. L, "Acoustic Source Localization From Multirotor UAVs," *IEEE Transactions on Industrial Electronics*, vol.67, no.10, pp.8618-8628, 2020. Article (CrossRef Link)
[44] Sedunov. A, Haddad. D, Salloum. H, Sutin. A, Sedunov. N, Yakubovskiy. A, "Stevens Drone Detection Acoustic System and Experiments in Acoustics UAV Tracking," in *Proc. of 2019 IEEE International Symposium on Technologies for Homeland Security (HST)*, pp.1-7, 2019. Article (CrossRef Link)
[45] Ojdanić. D, Sinn. A, Naverschnigg. C, Schitter. G, "Feasibility Analysis of Optical UAV Detection Over Long Distances Using Robotic Telescopes," *IEEE Transactions on Aerospace and Electronic Systems*, vol.59, no.5, pp.5148-5157, 2023. Article (CrossRef Link)
[46] Lykou. G, Moustakas. D, Gritzalis. D, "Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies," *Sensors*, vol.20, no.12, 2020. Article (CrossRef Link)
[47] Musa. S.A, Abdullah. R.S.A.R, Sali. A, Ismail. A, Rashid. N.E.A, Ibrahim. I.P, Salah. A.A, "A review of copter drone detection using radar systems," *Def. S&T Tech. Bull*, vol.12, no.1, pp.16-38, 2019. [Online]. Available: https://www.researchgate.net/
[48] Rudys. S, Laučys. A, Udris. D, Pomarnacki. R, Bručas. D, "Functionality Investigation of the UAV Arranged FMCW Solid-State Marine Radar," *Journal of Marine Science and Engineering*, vol.9, no.8, 2021. Article (CrossRef Link)
[49] Merrill. I, SKOLNIK, Radar Handbook, 2nd Edition, McGraw-Hill Publishing Company, 1990. Article (CrossRef Link)
[50] Noh. D.I, Jeong. S.G, Hoang. H.T, Pham. Q.V, Huynh-The. T, Hasegawa. M, Sekiya. H, Kwon. S.Y, Chung. S.H, Hwang. W.J, "Signal Preprocessing Technique With Noise-Tolerant for RF-Based UAV Signal Classification," *IEEE Access*, vol.10, pp.134785-134798, 2022. Article (CrossRef Link)
[51] Eriksson. N, "Conceptual study of a future drone detection system - Countering a threat posed by a disruptive technology," *CHALMERS UNIVERSITY OF TECHNOLOGY*, 2018. Article (CrossRef Link)

[52] Souli. N, Kolios. P, Ellinas. G, "An Autonomous Counter-Drone System with Jamming and Relative Positioning Capabilities," in *Proc. of ICC 2022 - IEEE International Conference on Communications*, pp.5110-5115, 2022. Article (CrossRef Link)
[53] Straub. J, "Unmanned aerial systems: Consideration of the use of force for law enforcement applications," *Technology in Society*, vol.39, pp.100-109, 2014. Article (CrossRef Link)
[54] Matić. V, Kosjer. V, Lebl. A, Pavić. B, Radivojević. J, "Methods for Drone Detection and Jamming," in *Proc. of ICIST 2020 Proceedings Part I*, pp. 16-21, 2020. Article(CrossRefLink)
[55] Makarenko. S. I, MS. I, Setecentricheskaya vojna-principy, tekhnologii, primery i perspektivy. Monografiya, "Network-centric warfareprinciples, technologies, examples and perspectives. Monograph," *Saint Petersburg: Naukoemkie Tekhnologii Publ*, 2018.
[56] Benyamin. M, Goldman. G.H, "Acoustic detection and tracking of a Class I UAS with a small tetrahedral microphone array," *Army Research Laboratory*, 2014. Article(CrossRefLink)
[57] Pohasii. S, Baranova. V, Bilotserkivskyi. O, Haponenko. O, Serhiienko. O, and Vorobiov. B, "Application of Cost-Effective Acoustic Intelligence to Protect Critical Facilities from Drone Attacks," in *Proc. of 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek)*, pp.1-6, 2022. Article (CrossRef Link)
[58] Choi. J.C, and Lim. S.H, "Antidrone," *Technology Trends Brief, Korea Institute for Science and Technology Planning and Evaluation (KISTEP)*, no.10, p.6, 2021.
[59] Shaohui. X, Ji. F, Baohua. W, Fengge. W, Yong. H, Jiajia. M, and Ye. W, "Development of a shooting strategy to neutralize UAV swarms based on multi-shot cooperation," in *Proc. of International Symposium on Advanced Launch Technologies (ISALT 2022)*, vol.2460, 2023. Article (CrossRef Link)
[60] Kinetic Hard-Kill Counter-UAS technologies. [Online]. Available: https://www.airsight.com/knowledge-hub/counter-drone-technology/air-to-air, Accessed on 17 August 2023.
[61] Drone interceptor with a net gun and detachable rotors, Apr. 2022. [Online]. Available: https://www.suasnews.com/2022/04/drone-interceptor-with-a-net-gun-and-detachable-rotors/, Accessed on 17 August 2023.
[62] Nikkei staff, Nippon Toshiba to offer service to capture and destroy illegal drones, Maeil Business Newspapers, 23 March 2021, [Online]. Available: https://www.bing.com/
[63] Lyu. C, and Zhan. R, "Global Analysis of Active Defense Technologies for Unmanned Aerial Vehicle," *IEEE Aerospace and Electronic Systems Magazine*, vol.37, no.1, pp.6-31, 2022. Article (CrossRef Link)
[64] D. H. Kim, Drones Catching Drones, and it looks scary, THE FACT, Jun. 29, 2015. [Online]. Available: https://www.bing.com/, Accessed on 17 August 2023.
[65] Feickert. A, "U.S. Army Weapons-Related Directed Energy (DE) Programs: Background and Potential Issues for Congress," 2018. [Online]. Available: https://apps.dtic.mil/sti/citations/AD1170019
[66] Zohuri. B, Directed-energy beam weapons, pp.239-268, Berlin: Springer, 2019. [Online]. Available: https://link.springer.com/book/10.1007/978-3-030-20794-6
[67] Kris Osborn, Russia Has a New Anti-Drone Strategy: UAV Nets, The National Interest, Jan. 5, 2021. [Online]. Available: https://nationalinterest.org/blog/reboot/russia-has-new-anti-drone-strategy-uav-nets-175827, Accessed on 17 August 2023.
[68] Jung. B.S, "Case analysis of drone terrorism and efficient countermeasures," *Police Studies*, Korea, vol.14, no.2, pp.149-176, 2019.
[69] Park. C.J, and Kim. K.Y, "Patent Trend Analysis of Anti-Drone : Focusing on the Neutralization Means and Methods," *The Journal of Korean Institute of Next Generation Computing*, vol.16, no.2, pp.7-17, 2020. Article(CrossRefLink)
[70] Hambling. D, U.S. Navy Destroys Target With Drone Swarm — And Sends A Message To China, Forbes, 2021. [Online]. Available: https://www.forbes.com/sites/davidhambling/2021/04/30/us-navy-destroys-target-with-drone-swarm---and-sends-a-message-to-china/

[71] Tyurin. V, Martyniuk. O, Mirnenko. V, Open'ko. P, and Korenivska. I, "General Approach to Counter Unmanned Aerial Vehicles," in *Proc. of 2019 IEEE 5th International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD)*, pp.75-78, 2019. Article (CrossRef Link)
[72] Al-Aish. T. A. K, "Design and Analysis the Fiber Laser Weapon System FLWS," *Advances in Physics Theories and Applications*, vol.47, pp.59-68, 2015. Article(CrossRefLink)
[73] Pudo. D, Galuga. J, "High Energy Laser Weapon Systems: Evolution, Analysis and Perspectives," *Canadian Military Journal*, vol.17, no.3, pp.53-60, 2017. Article(CrossRefLink)
[74] Bernatskyi. A, and Sokolovskyi. M, "History of military laser technology development in military applications," *History of science and technology*, vol.12, no.1, pp.88-113, 2022. Article (CrossRef Link)
[75] Chi. Z, Chun. Z, Ruyi. K, Shiyong. X, and Jiao. Z, "An Overview of Countermeasures Against Low-altitude, Slow-speed Small UAVs," in *Proc. of International Symposium on Advanced Launch Technologies (ISALT 2022)*, 2023. Article (CrossRef Link)
[76] Noh. J, Kwon. Y, Son. Y, Shin. H, Kim. D, Choi. J, and Kim. Y, "Tractor Beam: Safe-hijacking of Consumer Drones with Adaptive GPS Spoofing," *ACM Transactions on Privacy and Security (TOPS)*, vol.22, no.2, pp.1-26, 2019. Article (CrossRef Link)
[77] Robinson. M, "Knocking my neighbor's kid's cruddy drone offline," *DEF CON 23*, 2015. [Online]. Available: https://www.bing.com/
[78] R. Joglekar, "4 strategies for stopping 'rogue' drones from flying in illegal airspace," *6ABC Action News*, Dec. 23, 2018. [Online]. Available: https://6abc.com/, Accessed on 17 August 2023.
[79] Abunada. A.H, Osman. A.Y, Khandakar. A, Chowdhury. M.E.H, Khattab. T, and Touati. F, "Design and Implementation of a RF Based Anti-Drone System," in *Proc. of 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, pp.35-42, 2020. Article (CrossRef Link)
[80] Taylor. C.D, and Giri. D.V, High Power Microwave Systems and Effects, Washington, D.C. : Francis & Taylor, 1994. [Online]. Available: https://search.lib.uts.edu.au/discovery/fulldisplay/alma991006288139705671/61UTS_INST:61UTS
[81] Kang. H, Joung. J, Kim. J, Kang. J, and Cho. Y.S, "Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems," *IEEE Access*, vol.8, pp.168671-168710, 2020. Article (CrossRef Link)
[82] Pierluigi. P, Hacking Drones … Overview of the Main Threats, Jun. 4, 2013. [Online]. Available: https://www.bing.com/, Accessed on 17 August 2023.
[83] Ulaby. F.T, and Ravaioli. U, Fundamentals of applied electromagnetics, Upper Saddle River, NJ: Pearson, 2015. [Online]. Available: https://books.google.co.kr/books/about/Fundamentals_of_Applied_Electromagnetics.html?id=U62gBwAAQBAJ&redir_esc=y
[84] Yun. Q, Song. B, and Pei. Y, "Modeling the Impact of High Energy Laser Weapon on the Mission Effectiveness of Unmanned Combat Aerial Vehicles," *IEEE Access*, vol.8, pp.32246-32257, 2020. Article (CrossRef Link)
[85] Renyu. Z, Kiat. S.C, Kai. W, and Heng. Z, "Spoofing Attack of Drone," in *Proc. of 2018 IEEE 4th International Conference on Computer and Communications (ICCC)*, pp.1239-1246, 2018. Article (CrossRef Link)
[86] Ferrão. I.G, da Silva. S.A, Pigatto. D.F, and Branco. K.R L. J. C., "GPS Spoofing: Detecting GPS Fraud in Unmanned Aerial Vehicles," in *Proc. of 2020 Latin American Robotics Symposium (LARS), 2020 Brazilian Symposium on Robotics (SBR) and 2020 Workshop on Robotics in Education (WRE)*, pp.1-6, 2020. Article (CrossRef Link)
[87] Barbora Kotkova, "Airport defense systems against drones attacks," in *Proc. of 2022 26th International Conference on Circuits, Systems, Communications and Computers (CSCC)*, pp.85-90, 2022. Article(CrossRefLink)

[88] Chaudhary, N. K, "Conceptual Model of Counter-drone System to Overcome the Current Underlying Technology Limitations," *NFSU Journal of Cyber Security and Digital Forensics*, vol.1, no.1, 2022. Article(CrossRefLink)
[89] Jurn, Y. N., Mahmood, S. A., & Aldhaibani, J. A., "Anti-Drone System Based Different Technologies: Architecture, Threats and Challenges," in *Proc. of 2021 11th IEEE International Conference on Control System, Computing and Engineering (ICCSCE)*, pp.114-119, 2021. Article(CrossRefLink)
[90] Saaty. T.L., "Group Decision Making and the AHP," *The Analytic Hierarchy Process*, pp.59-67, 1989. Article(CrossRefLink)
[91] Ho. W, and Ma. X, "The state-of-the-art integrations and applications of the analytic hierarchy process," *European Journal of Operational Research*, vol.267, no.2, pp.399-414, 2018. Article (CrossRef Link)
[92] Saaty. R.W, "The analytic hierarchy process-what it is and how it is used," *Mathematical Modelling*, vol.9, no.3-5, pp.161-176, 1987. Article (CrossRef Link)
[93] Saaty. T.L, "Rank generation, preservation, and reversal in the analytic hierarchy decision process," *Decision Sciences*, vol.18, no.2, pp.157-177, 1987. Article (CrossRef Link)
[94] Saaty. T.L, "A scaling method for priorities in hierarchical structures," *Journal of Mathematical Psychology*, vol.15, no.3, pp.234-281, 1977. Article (CrossRef Link)
[95] Saaty. T.L, "What is the Analytic Hierarchy Process*?*," in *Proc. of Mathematical Models for Decision Support, NATO ASI Series, Springer Berlin Heidelberg*, vol.48, pp.109-121, 1988. Article(CrossRefLink)
[96] Sambamurthy. V, and Zmud. R.W, "Arrangements for Information Technology Governance: A Theory of Multiple Contingencies," *MIS Quarterly*, vol.23, no.2, pp.261-290, 1999. Article (CrossRef Link)
[97] Sung. K.M, "A study on the IT governance structure of small and medium-sized enterprises: a multi-contextual perspective," *Journal of the Korean Electronic Transaction Society*, vol.12, no.3, p.57, 2006.
[98] Snead. J, Seibler. J. M, and Inserra. D, "Establishing a Legal Framework for Counter-Drone Technologies," *The Heritage Foundation*, 2018. Article(CrossRefLink)
[99] Jovanoska. S, Knoedler. B, Palanivelu. D. P, Still. L, Varela. M, Fiolka. T, Oispuu. M, Steffes. C, and Koch. W, "Passive Sensor Processing and Data Fusion for Drone Detection," in *Proc. of the NATO STO Meeting Proceedings: MSG-SET-183 Specialists' Meeting on Drone Detectability: Modelling the Relevant Signature, Prague, Czech Republic*. 2021. Article (CrossRef Link)
[100] Park. S, Kim. H.T, Lee. S, Joo. H, and Kim. H, "Survey on Anti-Drone Systems: Components, Designs, and Challenges," *IEEE Access*, vol.9, pp.42635-42659, 2021. Article (CrossRef Link)
[101] Farlík. J, and Gacho. L, "Researching UAV Threat - New Challenges," in *Proc. of 2021 International Conference on Military Technologies (ICMT)*, pp.1-6, 2021. Article (CrossRef Link)
[102] Çetin. E, Barrado. C, and Pastor. E, "Improving real-time drone detection for counter-drone systems," *The Aeronautical Journal*, vol.125, no.1292, pp.1871-1896, 2021. Article (CrossRef Link)
[103] Lee. D.Y, Lee. J.I, and Seo. D.W, "Drone movement classification based on deep learning using micro-doppler signature images," *Journal of Advanced Marine Engineering and Technology*, vol.45, no.4, pp.213-217, 2021. Article (CrossRef Link)
[104] Huizing. A, Heiligers. M, Dekker. B, de Wit. J, Cifola. L, and Harmanny. R, "Deep Learning for Classification of Mini-UAVs Using Micro-Doppler Spectrograms in Cognitive Radar," *IEEE Aerospace and Electronic Systems Magazine*, vol.34, no.11, pp.46-56, 2019. Article (CrossRef Link)
[105] Al-Sa'd. M.F, Al-Ali. A, Mohamed. A, Khattab. T, and Erbad. A, "RF-based drone detection and identification using deep learning approaches: An initiative towards a large open source drone database," *Future Generation Computer Systems*, vol.100, pp.86-97, 2019. Article (CrossRef Link)
[106] Çetin. E, Barrado. C, and Pastor. E, "Counter a Drone in a Complex Neighborhood Area by Deep Reinforcement Learning," *Sensors*, vol.20, no.8, 2020. Article (CrossRef Link)

[107] Taylor. M. E, and Stone. P, "Transfer Learning for Reinforcement Learning Domains: A Survey," *Journal of Machine Learning Research*, vol.10, pp.1633-1685, 2009. Article(CrossRefLink)
[108] Thipphavong. D.P., Apaza. R, Barmore. B, Battiste. V, Burian. B, Dao. Q, Feary. M, Go. S, Goodrich. K.H., Homola. J, Idris. H.R., Kopardekar. P.H., Lachter. J.B., Neogi. N.A., Ng. H.K, Oseguera-Lohr. R.M., Patterson. M.D., Verma. S.A., "Urban Air Mobility Airspace Integration Concepts and Considerations," in *Proc. of 2018 Aviation Technology, Integration, and Operations Conference*, 2018. Article (CrossRef Link)
[109] Abdelmaboud. A, "The Internet of Drones: Requirements, Taxonomy, Recent Advances, and Challenges of Research Trends," *Sensors*, vol.21, no.17, 2021. Article (CrossRef Link)
[110] Giray. S.M, "Anatomy of unmanned aerial vehicle hijacking with signal spoofing," in *Proc. of 2013 6th International Conference on Recent Advances in Space Technologies (RAST)*, pp.795-800, 2013. Article (CrossRef Link)
[111] Chen. W, Meng. X, Liu. J, Guo H, and Mao. B, "Countering Large-Scale Drone Swarm Attack by Efficient Splitting," *IEEE Transactions on Vehicular Technology*, vol.71, no.9, pp.9967-9979, 2022. Article (CrossRef Link)
[112] Hongbin. C, and Junfei. S, et al, "Research on Antimissile Capability of Medium Caliber Pre-fragmented Projectile," *Journal of Projectiles, Rockets, Missiles and Guidance*, no.005, pp.9-13, 2018. Article(CrossRefLink)
[113] Graswald. M, Gutser. R, Grabner. F, Meyer. B, Winter. C, and Oelerich. A, "Defeating UAVs Through Novel HPEM Effectors," in *Proc. of 31st International Symposium on Ballistics*. pp.2053-2062, 2019. Article(CrossRefLink)
[114] Müller. T, Widak. H, Kollmann. M, Buller. A, Sommer. L.W, Spraul. R, Kröker. A, Kaufmann. I, Zube. A, Segor. F, Perschke. T, Lindner. A, and Tchouchenkov. I, "Drone detection, recognition, and assistance system for counter-UAV with VIS, radar, and radio sensors," in *Proc. of Automatic Target Recognition XXXII*, vol.12096, pp.94-108, 2022. Article (CrossRef Link)
[115] Quigley. M, Gerkey. B, Conley. K, Faust. J, Foote. T, Leibs. J, Berger. E, Wheeler. R, and Ng. A.Y, "ROS: an open-source Robot Operating System," in *Proc. of ICRA Workshop on Open Source Software*, 2009. Article (CrossRef Link)
[116] D. Matthews, Drone Defence, NetGun X1-Short Range Drone Protection, Available online: https://www.dronedefence.co.uk/ skyfence/, Accessed on 7 June 2023.

Jindong Kim received the M.S. degree from Kookmin University in 2012. Currently, he is pursuing a Ph.D. degree in Department of Protection and Safety Engineering, Seoul National University of Science and Technology. His main research interests include drone and counter-drone systems, tactical nuclear and EMP protection, Behavior Based Safety (BBS), safety management systems, and safety-related legal frameworks. He has published more than five academic papers.

Jonggeun Choi received the M.S. degree from Defense Management from the Korea National Defense University in 2001 and a Ph.D. in Information Management from the Seoul Venture University in 2015. He is currently a professor in the Department of Protection and Safety Engineering, Seoul National University of Science and Technology. Additionally, he serves as the Deputy Director of the Defense AI Convergence Research Center at Seoul National University of Science and Technology and as a policy advisor for the Ministry of National Defense and the Army Headquarters of the Republic of Korea. His main research areas include defense artificial intelligence and defense informatization, fire and explosion safety policies (such as weapon systems, ammunition, and explosives), military safety policies and laws/regulations, defense AI policies and requirements planning, as well as defense and defense industry policies and planning. He has led over 11 research projects and is actively involved as a board member of the Korean Society of Safety and the Korea Intelligent Information Systems Society.

Hyukjin Kwon received his Ph.D. in Industrial Engineering from Sungkyunkwan University in 2000 with a thesis on the establishment of strategic information systems for military equipment supply and maintenance activities. He conducted research in the field of defense logistics and informatization at the Korea Institute for Defense Analyses. He also served as the Director of the Information Planning Bureau, the highest-ranking official in charge of defense informatization at the Ministry of National Defense, where he was responsible for promoting defense informatization, cyber, and smart defense. He is currently a head professor of the Department of Defense Protection & Safety, and the Department of Defense Artificial Intelligence Application at Seoul National University of Science and Technology.