International Journal of Advanced Culture Technology Vol.12 No.4 275-284 (2024)
DOI https://doi.org/10.17703/IJACT.2024.12.4.275

IJACT 24-12-34

A Study on How to Establish the Counter-Drone System for National Crucial Infrastructures

[1] Sang Keun Cho, [2] Sejin Jang, [3]Semi Kim[*]

[1] Research Professor, The Future Institute for National Strategic Technology and Policy, KAIST, South Korea
[2] Research Professor, The Future Institute for National Strategic Technology and Policy, KAIST, South Korea
[3] Research Professor, The Future Institute for National Strategic Technology and Policy, KAIST, South Korea
sm.kim@kaist.ac.kr

Abstract

In the Ukraine-Russia war and the Israel-Hamas conflict, drones have become symbols of "overwhelming military superiority," utilized across tactical and strategic levels for front-line attacks and assaults on critical national facilities. As drone threats intensify, various countries around the world are swiftly establishing "Counter-Drone Systems" to protect critical infrastructure, while North Korea has also unveiled kamikaze drones. The Repulic of Korea is similarly building counter-drone systems focused on protecting national critical infrastructure, yet issues with time synchronization and interoperability have emerged.

This study conducted Focus Group Interviews (FGI) with experts from the public, private, and military sectors to identify current issues in the areas of counter-drone system deployment protocols, diversification of counter-drone components, and mobile-based information-sharing systems. Based on these findings, this research aims to organize and optimize a framework for establishing counter-drone systems for critical national infrastructure. Furthermore, we propose this as a methodology for deploying counter-drone systems for essential infrastructure, establishing procedures to effectively respond to evolving drone threats. The procedures outlined in this study require continuous innovation through integrated R&D and training, ensuring real-time responses to increasingly sophisticated drone threats.

Keywords: *Escalation of Drone Threats, Counter-Drone Systems, Protection of Critical National Facilities, Issues of Time Synchronization and Interoperability*

1. INTRODUCTION

The ongoing Ukraine-Russia war and the Israeli-Hamas conflict have made drones a key tool of warfare. These drones are being used at a variety of levels from the tactical to the strategic, from destroying opposing forces on the front lines to neutralizing major cities or critical facilities deep in the heart of an opponent's territory. In short, drones have become an overmatch, or "overwhelming power advantage," that can drive

Manuscript received: October 12, 2024 / revised: November 16, 2024 / accepted: December 3, 2024
Corresponding Author : sm.kim@kaist.ac.kr
Tel: +82-42-350-7031, Fax: +82-42-350-1140
Research Professor The Future Institute for National Strategic Technology and Policy, KAIST

victory in a war or conflict.

As the threat of drones has escalated, not only the aforementioned warring parties, but also other countries around the world that have their eyes on both wars are building 'counter-drone systems'. This drone and counter-drone race has begun as part of an arms race full of contradictions. The Korean Peninsula is no exception, with North Korea recently unveiling a self-destructing drone similar to Israel's Hero and Harop series.

Korea is also building an anti-drone system centered on nationally important facilities for the reasons described above. However, it has shown significant problems in terms of time synchronization and interoperability. As will be described later, one of the main reasons for the above problems is the lack of clear awareness of the types of modules that comprise the anti-drone system, the required operational capabilities of each module, and the interconnection system between modules.

This study will first clarify the aforementioned problems by conducting focus group interviews with experts from the private, public, and military sectors. Next, we will derive measures to solve these problems from the wisdom of experts and organize a methodology for building a drone system for national critical facilities based on the previous research, which is the ultimate goal of this research. Finally, the researchers will optimize the previously organized methodology.

2. FGI-based problem elicitation

1) Configure the Public-Private-Military Expert Platform

Focused group interviews (FGIs) were conducted with experts from the private, public, and military sectors to identify problems with the current drone systems being deployed at critical facilities. To this end, we selected 50 experts from the private, public, and military sectors who have been working in positions related to drone systems such as drones, drones, artificial intelligence (AI), and hyperconnected networks for at least five years, or who are engaged in the defense of national critical facilities or drone systems, as shown in the following <Tagle 1>. In particular, in order to balance and harmonize the research field and the actual field, the experts were mainly organized by defense officials who are currently building actual anti-drone systems at national critical facilities.

Table 1. Expert Groups for Focus Group Interviews (FGI)

Separation		Job title	The Number of persons
Total		-	**50**
Civil (18 명)	Kyungwoon University Anti-Drone Defense Institute	Professors	4
	Asan Military Defense Research Institute	Research Professor	2
	The Asan Institute for Policy Studies	Research Fellows	1
	Korea Institue for Defense Industrial	Research Fellows	1
	Small Warfare Society	Research Fellows	5
	Korea Research Institute for	Research Fellows	2

	Strategy		
	KAIST The Future Institute for National Strategic Technology and Policy	Research Professor	3
	Science and Technology Policy Institute (STEPI)	Research Fellows	2
Public (17 명)	Institute for National Security Strategy	Research Fellows	2
	Ministry of Trade, Industry and Energy	Protection Officer	10
	Local governments (Seoul, Gumi, etc.)	Civil defense officials	3
	Ministry of National Defense Department of Defense Office of the Defense Innovation Agency	Innovation Center	2
	Army Headquarters Policy Office	Planning Officer	3
Military (15 명)	Army Future Innovation Research Center	Research Officer	3
	Army University	Professor / Combat Engineer	2
	Army Air Defense Forces	Executive Officer	5

2) FGI Results

To understand the problems of the current drone system being deployed in national critical facilities, we conducted in-depth interviews with the experts in <Table 1> from September 2, 2024 to October 31, 2024. As a result of the interviews, we found that most of them have participated in recent discussions, seminars, and evaluations of major drone systems. As a result, the researchers were able to discuss in-depth the problems of the drone system being added to nationally important facilities with them, and came up with meaningful results as shown in <Figure 1>.

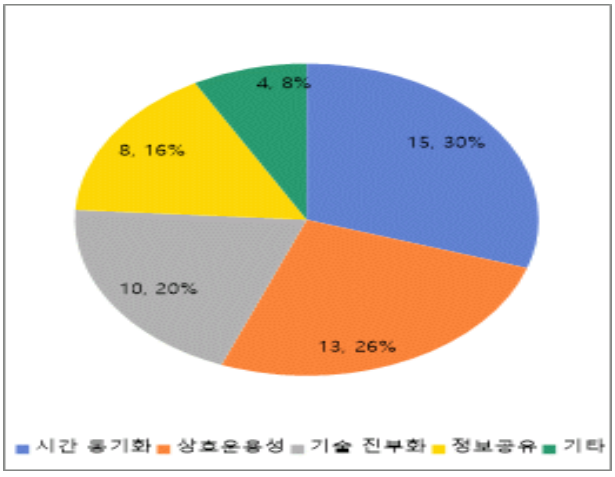


Figure 2. Identification of Issues through Focus Group Interviews (FGI)

The details of the keywords presented in [Figure 1] are as follows. First, "time synchronization" means that real-time data transmission and reception is limited between detection, identification, tracking, and neutralization equipment deployed at national critical facilities, making it difficult to offset the actual drone threat. In the field, even if the radar detects an illegal drone, the data is not transmitted in real time to the high-performance camera (EO/IR) for identification and tracking, limiting the actual tracking of the illegal drone. This delay in data transmission was the biggest problem that limited the actual neutralization of illegal drones.

Next, "interoperability" means that if any of the initially installed detection, identification, tracking, and neutralization equipment is replaced, interworking is limited. This also means that the scalability of the interworking system added to a critical facility is limited. This weak interoperability of critical facilities is a major problem because even if some equipment is replaced, the entire initial interworking system must be replaced, leading to significant budgetary expenditures.

Additionally, "technology obsolescence" means that the capabilities of the anti-drone equipment deployed at critical sites due to rapid technological advancements have not kept pace with the sophistication of the drone threat. In fact, the current anti-drone systems deployed at critical facilities can offset the threat of reconnaissance drones approaching at the right altitude. However, they are limited in their ability to neutralize FPV suicide drones, which fly low to the ground and swoop in for precision strikes near their targets, as seen in the recent Ukraine-Russia war and the Israeli-Hamas conflict.

Finally, "information sharing" means that there is no real-time information sharing system with the military and police that actually takes action in the event of a drone threat. This is because critical facilities and the military and police are under different government ministries. As a result, real-time first response is limited in the field, and the possibility of damage to critical facilities is bound to increase.

Elsewhere, some experts noted that the continued southward migration of detonator laden filth balloons and the lack of national awareness of the drone threat, despite North Korea's unveiling of a self-destructing drone, may be the biggest problem, which could lead to unexpected provocations.

3. Exploring FGI-based resolution directions

1) Civil, Public and Military experts recognize the problem

We conducted another FGI to explore solutions to the various issues mentioned above. The same experts who identified the problems were selected for the FGI. This is because they have a clear understanding of the purpose of this study, which can strengthen the logical connection of the data applied to this study. Currently, the anti-drone system for nationally important facilities is in the process of being established, but at the same time, it is continuously complemented and developed to efficiently respond to the escalation of drone threats. Currently, experts' suggestions for the development of the anti-drone system can be summarized as integration of regions, integration of means, and integration of efforts.

Prior to the FGI, the researchers explained to the experts the clear meaning of the terms "time synchronization," "interoperability," "technology obsolescence," and "information sharing" mentioned in Chapter 2 and the key examples related to them. This gave the experts a clear understanding of the issues they had not presented and allowed them to participate in the FGI with a logical connection.

2) FGI Results

After clearly recognizing the current problems identified through the first round of FGIs, experts from the private, public, and military sectors were interviewed in-depth by the researchers and offered various solutions. The researchers extracted the main keywords from their suggestions and grouped them to select the core keywords. As a result, the researchers derived solution directions such as 'stipulating the procedure for building a drone system', 'diversifying drone components', and 'establishing a mobile-based information sharing system', as shown in <Figure 2>.

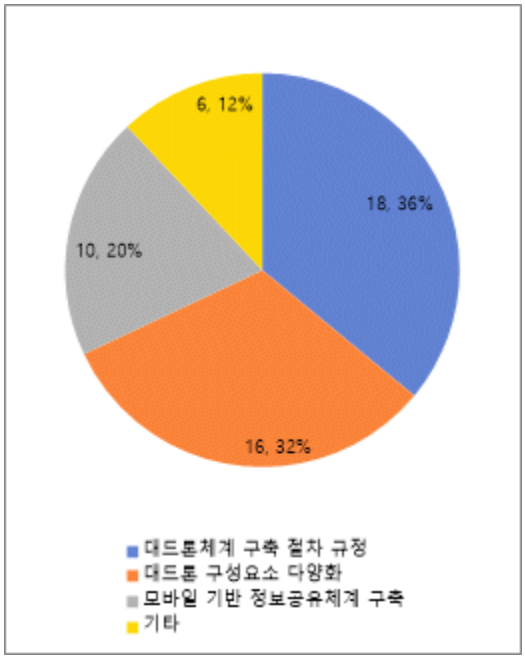


Figure 2. Analysis through Focus Group Interviews (FGI)

Each of the meanings presented in <Figure 2> are as follows. First of all, the 'Regulation on Procedures for Building a Drone System' can be seen as a solution to the problems of 'time synchronization' and 'interoperability' mentioned in Chapter 2. It means that in order to build a sustainable drone system for national critical facilities, it is necessary to first add an interlocking system, and then connect the interlocking system with detection, identification, tracking, and neutralization equipment that can transmit and receive real time data. This is in line with experts' opinions that the core of the drone system is a highly scalable interconnection system.

Next, "drone component diversification" can be viewed as a solution to the "technology obsolescence" identified in Chapter 2. In our in-depth interviews, experts expressed the view that real-time replacement of anti-drone equipment, including detection, identification, pursuit, and neutralization, is effectively limited due to budget and time to field. Therefore, it was emphasized that it is necessary to offset the escalating threat of drones by building an anti-drone system by converging not only equipment but also manpower that can form an anti-aircraft network and materials that can protect key nodes of major facilities, as shown in <Figure 3-4>.

Figure 3. Counter-Drone Team of the Ukrainian Territorial Defense Forces Neutralizing Russian Long-Range Drones

Figure 4. A Facility Designed to Protect the Critical Nodes of Major Crucial Infrastructures

Finally, "building a mobile-based information sharing system" can be seen as a solution to the "information sharing" problem presented in Chapter 2. Experts opined that integrating the command and control systems of different government departments is effectively limited by current technology, security, and budgetary issues. Instead, they noted that it is most realistic to build a cloud-based information sharing system that allows stakeholders such as local governments, the military, police, and senior, neighboring, and subordinate NOC defense officials to access each NOC in real time using portable mobile devices and share information through multiple authentication.

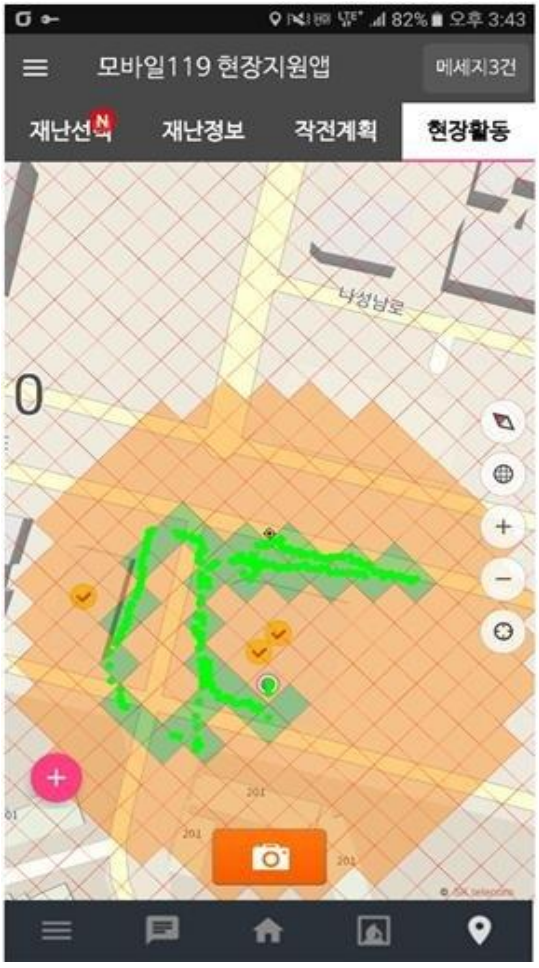


Figure 5. Graph 5. A mobile-based 119 Field Support System for Visualizing the Activity Routes [3].

In other matters, experts emphasized that the establishment of an anti-drone system for national critical facilities is not an option but a necessity given the recent war and conflict situation and the speed of North Korea's droneization, and noted that it is necessary to activate integrated civil-military anti-drone drills during periods such as Eulji drills and civil defense drills to focus national attention and efforts on this issue.

4. Establishment of a methodology for building a drone system

A methodology describes the path to the final conclusion of a study [4]. Applying this to the purpose of this study, it can be operationally defined as the process of deploying a drone system at a national critical facility. This requires a clear and common understanding of the components that are operationalized in the drone system deployment process.

1) Scoping the components of the drone system

As mentioned earlier, an anti-drone system consists of detection, identification, tracking, and neutralization equipment. This is from a mechanical perspective. However, as mentioned earlier, the Ukrainian military is

using drone teams (personnel) to offset the threat of Russian long-range self-destructive drones (Shahed-136), and U.S. forces deployed in the Middle East are protecting key nodes of key facilities by undergrounding, hardening, and installing blast panels.

As such, an anti-drone system can be built not only with equipment but also with manpower and facilities, and the defense capability of the system can be further strengthened by converging various means. From this perspective, it would be preferable to express the components of an anti-drone system as "detection, identification, tracking, and neutralization modules" rather than "detection, identification, tracking, and neutralization equipment." In other words, an anti-drone system is built with various modules such as equipment, personnel, and facilities.

It's worth clarifying the scope of "equipment" here. Most people tend to think of drone equipment deployed in national critical facilities as fixed. However, with the advancement of science and technology, the scope of drone equipment is expanding to include not only fixed types, but also mobile types, mobile platforms, and modular types that can be attached and detached in real time to personnel, facilities, etc.

The range of components of such a drone system can be selected as shown in <Table 2>, and an optimized drone system can be built by converging the detailed items in <Table 2> according to the geographical characteristics of national critical facilities.

Table 2. Elements of Counter-drone System

Separation	Detection	Identification	Tracking	Neutralize
Equipment	Fixed	Fixed	Fixed	Fixed
	Mobile	-	-	Mobile
	Modular	-	-	Modular
Workforce	Portable day/night surveillance			Great Public Network
Facilities	-	-	-	Undergrounding, concealment, and blast panels

2) Organize the drone system deployment process

The drone system can be viewed as a system of systems in which various detection, identification, tracking, and neutralization modules interact simultaneously. That is why, as mentioned by experts from the private, public, and military sectors, 'time synchronization' and 'interoperability' have emerged as the biggest problems of the current drone system being deployed in national critical facilities. Accordingly, it will be necessary to establish an interlocking system so that various modules comprising the drone system can transmit and receive data in real time.

After this interlocking system is added, various modules presented in <Table 2> should be connected to national critical facilities according to geographical characteristics. At this time, each of the detection, identification, tracking, and neutralization modules needs to create synergy by complementary convergence of equipment and manpower. In other words, the components of the anti-drone system need to apply the concept of manned and unmanned teaming.

Although the interlocking system is added to the anti-drone system, and various modules are connected to it, both manned and unmanned, the drone threat is directed from the outside to the inside of the critical facilities. In the end, drone threats are offset by coordinated measures with the military and police, as mentioned earlier, rather than by the critical facilities themselves, so a real-time information sharing system between critical facilities and the military and police is very important. This logical flow is organized as shown in <Figure 6>.

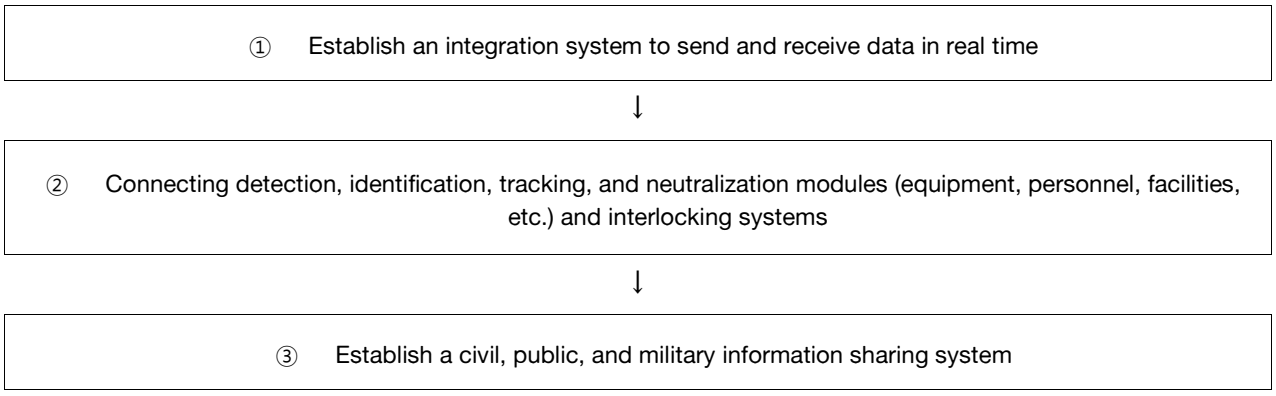


Figure 6. Procedures for Establishing an Organized Counter-drone System

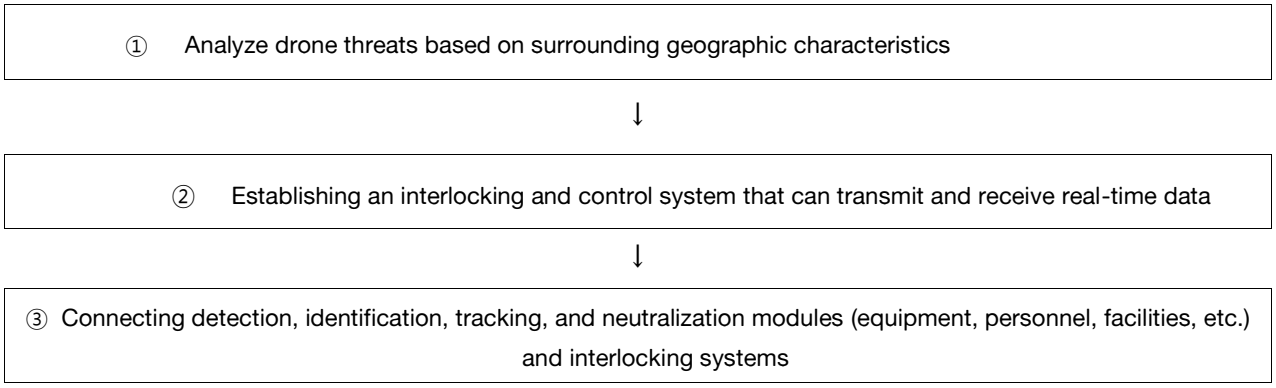
3) Optimize the drone system deployment process

The researchers went the extra mile to establish the previously organized process as a methodology for deploying a drone system at a national critical facility. The biggest consideration in this process was budget. Neither the private, public, nor military sectors have sufficient funding to respond to the rapidly evolving drone threat in real time.

Due to these budget limitations, the drone system cannot be densely deployed around critical facilities. This means that the drone system can only be built according to the principle of selection and concentration in consideration of the geographical characteristics around national critical facilities. Therefore, the first step in the drone system construction process organized in <Figure 6> should include a drone threat analysis based on the geographical characteristics around national critical facilities.

In addition, the private, public, and military experts who presented the problems and solutions earlier expressed the opinion that not only the interlocking system but also the visualization system should be added to the first step in <Figure 6>. This is because only when the anti-drone system detects, identifies, tracks, and neutralizes drones that threaten national critical facilities, it can be integrated and visualized, and real-time situational measures can be taken by defense personnel. As such, such a visualization system implies command and control, so it can be named as a control system.

As shown in <Figure 6> the above, optimizing by reflecting the opinions of researchers and public, private, and military experts, it looks like <Figure 7> .



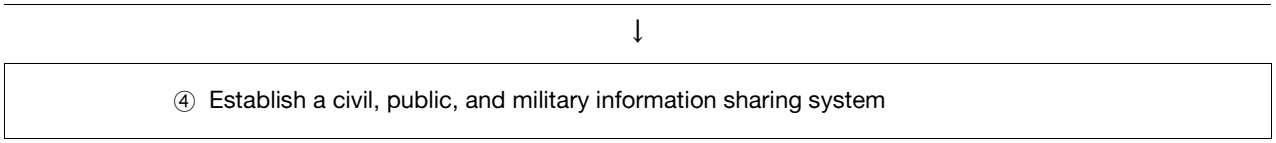


Figure 7. Optimized Counter-Drone System Deployment Procedure

5. Conclusions

The ongoing Ukraine-Russia war and the Israeli-Hamas conflict have made drones a key tool of warfare. North Korea has also recently been sending filth balloons equipped with GPS and detonators to the South, and has unveiled self-destructive drones similar to Israeli ones. As such, the drone threat has become a reality on the Korean Peninsula, and the construction of an anti-drone system for Korea's national critical facilities has become a necessity, not an option.

As the drone threat has escalated, Korea is rushing to build an anti-drone system centered on nationally important facilities under the private, public, and military sectors. However, as mentioned by experts from the private, public, and military sectors, there are various problems such as time synchronization and interoperability. As a result, it is causing a waste of effort, including budget, manpower, and time, and delaying the construction time of the drone system for Korea's national critical facilities.

To solve these problems, this study conducted FGIs with experts from the private, public, and military sectors and optimized the process of building a drone system as shown in . The researchers presented this as a methodology for building a drone system for national critical facilities. Of course, the optimized deployment procedure needs further optimization in terms of operation method, coordination system, and organization and deployment, but it can be evaluated as significant in that it is the first to present a drone system deployment procedure for national critical facilities.

In the future, the deployment process outlined by the researchers will need to be innovated upon through various public-private-military integration efforts. Longitudinal studies such as this will allow for real-time offsetting of the escalating drone threat globally. To do so, it will be necessary to build an integrated anti-drone system in areas where national critical facilities are concentrated, utilize it as a test-bed, and periodically conduct integrated public-private-military R&D and training.

REFERENCES

[1] https://essanews.com/ukraine-employs-innovative-network-acoustic-sensors-for-dronedefense, 6997073851062401a
[2] https://maritime-executive.com/corporate/interdam-fire-and-blast-resistant-panels-for-offshore
[3] https://www.fnnews.com/news/202108301202209717
[4] https://link.springer.com/chapter/10.1007/978-981-99-8925-6_1#citeas