Journal of Digital Convergence
Vol. 18. No. 11, pp. 247-257, 2020

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2020.18.11.247

국가중요시설 방호를 위한 안티드론 시스템 구축 방안 연구

황순필[1], 김두환[2*]
[1]대전대학교 대학원 박사과정, [2]육군본부 정보작전참모부 서기관

A Study on the Establishment of Anti-Drone system for the Protection of National Important Facilities

Soon-phil Hwang[1], Doo-hwan Kim[2*]
[1]Doctor course, Dept of Public Administration, Dae Jeon University
[2]Secretary, G2/3, ROKA HQ

요 약 본 연구는 범죄 집단이나 테러리스트 등 악의적 의도로 사용되는 드론으로부터 국가중요시설 방호를 위한 효과적인 안티드론 시스템 구축 방안을 제시하는 데 목적이 있다. 연구목적 달성을 위해 안티드론 시스템에 관한 기술 및 정책 보고서, 제조업체의 공개 자료, 학술 연구논문을 검토하고, 드론 관련 분야의 전문가를 대상으로 안티드론의 복합적인 대응체계 구축과 관련한 인터뷰를 실시하였다. 연구결과, 탐지체계는 다양한 센서의 장단점을 보완하여 탐지율을 향상시킬 수 있도록 중첩·혼합운용하는 것이 효과적이며, 무력화 수단은 소프트킬 방식과 하드킬 방식을 배비하여 작전환경에 맞게 선택적으로 사용할 수 있도록 융통성을 확보하는 것이 효과적인 것으로 나타났다. 다시말해 불법드론 사전관리체계 정립, 탐지자산 혼합 및 중첩운용, 적합한 대응방안 결정, 무력화 수단 다중배비 등이다. 이러한 중첩·복합적 안티드론체계 운용을 통한 국가중요시설에 대한 방호체계 구축이 무엇보다 시급한 과제라 할 수 있다.

주제어 : 드론, 안티드론, 탐지 기술, 전파방해, 스푸핑

Abstract The Purpose of this study is to present effective Anti-Drone systems to protect national important facilities against drones that are illegally used by crime groups and terrorists with malicious intents. In order to accomplish the purpose of the study, technical and policy reports regarding Anti-Drone systems, open documents from manufacturers and various research papers are reviewed, and in-depth interviews with experts were conducted. Studies have shown that it is effective to overlay and mix different detection systems so that they can improve detection rates by supplementing each other's advantages and disadvantages, and that the means of incapacitation need to acquire flexibility by using both soft-kill and hard-kill methods in accordance with operational environment for the effective usage. In other words, the establishment of an illegal drone pre-management system, mixed and overlapping detection assets, determining appropriate countermeasures, and multiple distribution of means of incapacitation. The establishment of a protection system for important national facilities through the operation of overlapping and complex anti-drone systems is the most urgent task.

Key Words : Drone, Anti-Drone, Detection technology, Jamming, Spoofing

*Corresponding Author : Doo hwan Kim(highmt2015@naver.com)
Received October 15, 2020 Revised November 4, 2020
Accepted November 20, 2020 Published November 28, 2020

1. 서론

4차 산업혁명 시대의 핵심 산업인 드론은 저렴한 가격, 사용의 편의성 등으로 레저, 촬영, 농업, 재난 구호 등 많은 분야에서 널리 활용되고 있다. 드론은 인간의 삶의 질을 향상시키기 위해 긍정적 목적으로 개발되고 영역을 확장하고 있으며 성장 잠재력이 무궁하여 확산 속도는 더욱 가속화될 전망이다. 그러나 드론 시장의 성장과 급속한 확산은 공공 안전과 개인의 사생활 영역에 많은 부작용을 야기하고 있다. 특히, 저렴한 가격으로 무기를 장착할 수 있고 운용 주체를 숨길 수 있으며 감시 장비를 회피할 수 있다는 점에서 범죄 집단이나 테러리스트의 매력적인 도구가 되고 있어 드론을 이용한 테러 가능성이 증가하고 있다. 실제로 세계 각지에서 발생하고 있는 여러 사건들은 드론이 제기하는 위협을 무시할 수 없고 무시해서도 안된다는 것을 보여주고 있다. 2018년 12월 영국 관문공항인 캐트윅 공항에 미확인 드론이 발견되어 항공기 운항이 중단되었고[1], 2019년 9월 사우디아라비아 아브카이크와 쿠라이스 정유시설이 10여대의 드론 공격을 받아 가동을 중단해야 했다[2].

이러한 불법 드론에 대한 우려가 커지면서 드론으로 인해 야기되는 범죄나 테러 등 공공의 안녕과 질서를 침해하는 행위를 예방, 탐지, 차단하기 위한 법적, 제도적 기술적 차원의 종합적 대응 활동인 안티드론 시스템이 주목받고 있다[3]. 그러나 드론은 작고 소음도 작아서 현재의 감시 시스템으로 탐지 및 식별이 어렵고 나날이 발전하는 드론의 제작 기술은 안티드론 시스템 개발에 새로운 도전 과제가 되고 있다.

따라서 본 연구는 범죄 집단이나 테러리스트 등 악의적 의도로 불법 사용되는 드론으로부터 국가중요시설을 방호하기 위한 효과적인 안티드론 시스템 구축 방안을 제시하고자 하였다[4]. 이러한 연구목적 달성을 위해 안티드론 시스템에 관한 기술 및 정책 보고서, 제조업체의 공개 자료, 학술 연구논문 등 문헌연구를 통하여 어떤 기술이 이용 가능하고 어떤 기술이 개발되고 있는지 중점적으로 검토하였으며, 이를 통해 안티드론 시스템 구축과 관련한 효과적인 방안을 도출하기 위하여 군내부 드론과 관련한 실무경험자와 운용전문가 위주로 복합적인 안티드론체계 구축과 관련한 인터뷰를 실시하였다.

본 논문의 구성은 2장에서 먼저 드론의 역기능과 국가중요시설에 미치는 위협과 기술발전추세를 살펴보고, 3장에서는 드론탐지와 위협적인 드론에 대한 무력화기술에 대해 규명하며, 마지막 4장에서 국가중요시설 방호를 위한 효과적인 안티드론 시스템 구축 방안을 제시하고자 한다.

2. 드론의 위협과 기술발전 추제

2.1 드론의 위협

국가중요시설에 대한 드론을 이용한 테러 위협은 치명적이며 기술 발달에 따라 그 위협은 더욱 증가하고 있다. 드론을 이용한 해외의 주요 테러 사례는 Table 1.과 같다.

공항 인근에서 비행하는 새와 같은 작은 드론도 수많은 항공기의 운항을 중단시킬 수 있고, 원전 같은 핵심시설에 대한 공격은 상상할 수 없는 참담한 결과를 초래할 수도 있다. 영국 정부가 실시한 실험에서 400g의 드론은 헬리콥터의 앞유리를 부수고, 2kg 중량의 드론은 여객기 앞유리에 심각한 손상을 줄 수 있다는 것이 밝혀졌다[7]. 따라서 공항 주변 불법 드론이 탐지되면 안전상의 이유

Table 1. World Cases of Drone Terrorism[5, 6]

DATE	COUNTRY	EVENT DETAILS
January, 2015.	USA	In Washington D.C., a civilian UAV flew over the White House fence and crash-landed on the lawn.
April, 2015.	JAPAN	Phantom 2 drone carrying traces of radiation was found on the roof of the Japanese Prime Minister's Official Residence
October, 2016.	Iraq	ISIS may have used a commercial drone rigged with explosives to kill two Kurdish Peshmerga soldiers and wound two French soldiers in Iraq
August, 2016.	South Africa	A Small UAV crashed into a nuclear powerplant in Koberg.
August, 2018.	Venezuela	Two drone bombs used in an attempt to assassinate President Nicolas Maduro
December, 2018.	United Kingdom	Two drones found at Gatwick airport. The airport's closure led to more than 100,000 people being stranded or delayed.
September, 2019.	Saudi Arabia	Two Major Saudi Oil Installations Hit by Drone Strike. Production of 5.7 million barrels a day was suspended.

로 공항 전체가 폐쇄되고 항공기 운항이 중단될 수 있다.

우리나라도 2014년부터 백령도, 삼척, 파주 등지에서 청와대 전경과 군 시설을 촬영하고 복귀하다 추락한 북한 무인기로 추정되는 드론이 발견되었고, 2017년 6월에는 성주의 사드 기지를 촬영하고 복귀하던 북한발로 추정되는 드론이 발견되었으며, 또한 원전 인근에서 불법 드론이 출몰하는 사례가 증가하고 있다.

북한 드론 발견이후 드론 탐지용 레이더를 수입하여 배치하고 지상감시장비를 대공 감시로 전환하여 드론 접근로에 대한 감시체계를 구축하여 대응책 마련에 부심하고 있으나, 드론은 RCS (Radar Cross Section ; 레이더 반사 면적)가 작고 소형으로 탐지 및 식별이 어려우며 설사 탐지가 되더라도 요격하거나 무력화 할 수 있는 특별한 수단이 없어서 대응이 어려운 실정이다. 따라서 원전 주변에 드론 등 미확인 비행체가 나타나면 군과 경찰 병력에 의존하여 운용자를 수색하여 색출하는 것이 현실이다.

2.2 드론의 기술발전 추세

드론 시장이 확대되고 쉽게 구할 수 있는 드론의 유형이 다양해 지면서 안티드론 시스템은 다양한 형태와 크기의 드론을 탐지하고 무력화할 수 있도록 개발해야 한다. 그러나 나날이 발전하는 제작 기술은 안티드론 시스템 개발이 따라잡아야 할 새로운 도전 과제가 되고 있다. 이에 따라 드론의 기술개발과 함께 안티드론과 관련한 연구들도 활발하게 이루어지고 있는 것이 사실이다.

Table 2. A Proactive Study on Drone

Researcher	Details	Year
Lee,S.Y.,Kang,Uk. [8]	Post 2000, the third period of the drone, which is also called the expansion period and in connection with anti-terrorism warfares	2019
O.H.Choi[9]	The roles of the drone expanded into other fields outside the military	2020
Lee.I.G [10]	Specialized search team consisting of the Kyeongnam Provincial Police Agency's police officers and experts certified to control drones	2019
Shin.H.J [11]	SWOT analysis of applying drones for policing	2016
Jang.E.T [12]	Study on countermeasures of the police against drone terrorism	2019
Kim.D.H [13]	Study on threats against drone security inside the military	2018
Jo.H.J.,Yun.M.W [14]	Drones can be the target of a cyber attack since they can freely move and are hard to track down	2016
Kim.S.T,Lee.S.W [15]	Study on ways to improve civil security for national key infrastructures in response to drone terrorism	2015

Table 3. A Proactive Study on Anti-Drone

Researcher	Details	Year
Wallace & Loffi [16]	Anti-drone in-depth model, Prevention,Deterrence,Denial,Detection,Interruption,Destruction	2015
Lee.D.H.,Kang.U [17]	Legal, institutional and technical responses organically conducted by industries and technologies regarding law enforcement agencies	2019
Choi.S.H.,etc[18]	Comparative study of radar sensors and direction detection sensors	2018
Jeong.J.Y., Jeon.Y.T[19]	Jammer, launch techniques of radio waves that interfere with ISM (Industrial Scientific Medical) 2.4GHz band and GNSS (Global Navigation Satellite System) band with which UAVs obtain information on location and altitude	2017
Kim.H.H,Lee.S.W.Kim.B.M [20]	Research and development system of anti-drone technologies such as sound wave detection, GPS, frequency signal jamming and drone shoot-down system in its infancy	2018
Jang.E.T	Active menas such as prevention of drone terrorism in advance and evacuation in case of such attacks as well as passive means of using drone frequencies or physical force in response	2019

드론기술의 발전은 안티드론의 기술 역시도 복합적인 대응방안이 요구된다는 것을 의미한다. 최근 일부 드론은 무선 주파수 방해에 대응하기 위해 무선 주파수의 제어 없이 작동하거나 모바일 LTE 네트워크를 통하여 조종할 수도 있으며, 주파수 호핑 시스템을 이용한 드론도 개발되고 있다. 또한 GNSS(Global Navigation Satellite System) 신호에 의존하지 않는 드론은 GNSS가 단절된 상황이나 스푸핑 공격에서 자유롭게 운용될 수 있으며[21], GNSS 재머의 신호를 회피하기 위해 지상 신호의 간섭을 받지 않도록 설계하거나 조종사의 개입없이 자율비행 모드를 이용하여 운용 할 수 있는 드론이 개발되고 있다. 음향 탐지 센서를 회피하기 위해 엔진과 프로펠러의 소음을 최소화하는 기술이 개발되고 있으며, 빠른 속도로 움직이는 물체를 가까운 거리에서 회피하는 기술은 충돌하는 방식의 무력화 시스템을 회피할 수 있고, 스텔스 기능을 이용한 드론은 레이더의 탐지를 어렵게 한다. 또한 최근 개발되고 있는 군집 드론은 안티드론 관점에서 대응을 위해 많은 기술적 난제를 야기한다. 전파 방해는 넓은 지역에 확산된 드론에는 효과적이지 못하고, 탐지 및 식별도 어려워 일부 소수의 드론만 가능할 뿐이다.

드론 및 안티드론과 관련한 기술개발과 함께 그와 관련된 선행연구들을 살펴보자면, 현재의 대응방식에 대한 한계점과 개선방안에 대한 인식이 가능하며, 보다 핵심적인 국가중요시설에 대한 안티드론 대응방안 수립이 절실

하다는 필요에 직면하게 된다. 여러 가지 연구들은 일부 국가중요시설에 대한 안티드론 대응체계 구축과 관련한 대응방안들이 연계성있게 구축되어 있지 않고, 특히, 국가중요시설중 하나인 군시설에 대한 드론의 영역확장과 그로 인해 고민하여야 하는 안티드론의 실질적인 대응방안들이 확정적으로 수립되어 있지 못한 실정이다. 본 연구에서는 군부대와 군시설운용의 경험을 비추어 국가중요시설에 대한 드론테러 및 그에 대한 예방과 무력화를 위한 안티드론 대응방안을 수립하고 해결방안을 제언할 수 있도록 우선적으로 드론탐지 및 무력화기술과 관련한 선행연구결과를 종합하며, 4장에서 이에 대한 군내부 드론분야 운용 전문가, 안티드론 체계구축과 관련한 차별화된 의견들을 제시할 수 있는 해당분야 전문가들의 의견들을 반영하여 차별화된 대응방안 수립을 고민해 보고자 한다.

3. 드론 탐지 및 무력화 기술

3.1 탐지 및 식별

드론을 탐지하는 방법에는 레이더, 주파수 탐지(RF SCANNING), 전자공학 및 적외선(EO/IR), 음향탐지 등으로 분류할 수 있으며, 각 기술의 장점 및 제한사항은 Table 4.와 같다.

3.1.1 레이더(Radar)

레이더는 전자파를 방사하여 표적으로부터 반사되는 전자파를 수신하여 표적을 탐지하고, 전파의 도달 시간 차이를 측정하여 거리를 측정하는 것으로 대형 항공기의 탐지 및 추적에 유용한 도구이다. 그러나 드론은 레이더 반사 면적(RCS)이 적고, 주로 저고도에서 저속으로 비행하기 때문에 기존 대공방어를 위한 레이더는 탐지 및 추적이 곤란하다[22]. 그렇다 하더라도 레이더는 드론을 탐지하고 추적하는 데 유력한 수단으로 사각지대가 발생하고 초소형 물체를 잘못 식별할 수 있으나, 탐지거리가 비교적 길고 탐지 가능성이 높으며 기상의 영향을 받지 않고 전천후 운용이 가능한 장점으로 드론탐지와 관련하여 배제할 수 없는 유력한 장치이다. 특히, 3D 레이더는 거리와 방향, 고도 정보를 제공하여 위치식별이 가능한 강력한 장점이 있다. 다만, 레이더 자체가 높은 전자기 에너지로 밤낮을 가리지 않고 방출하는 특성이 있기 때문에, 혼잡한 도시 지역에 고출력 레이더를 배치하는 것이 적절한 지 여부는 판단해 보아야 할 사항이 아닐 수 없다.

3.1.2 주파수 탐지(RF Scanning)

드론이 방사하는 무선주파수(RF) 신호를 측정하여 탐지하는 기술이다. 대부분의 상용 드론은 일반적으로 특정 주파수 대역에서 운용된다. 따라서 드론에서 방출하는 무선 신호를 포착하여 방향을 탐지하고 교차 및 삼각점 원

Table 4. Comparing Anti-Drone Detection Technologies[1]

Method	Benefits	Limitations
Radar	Long-range primary surveillance detection system, depending on RCS and altitude Can track most drone types, regardless of autonomous flight Able to track multiple targets simultaneously Independent of visual conditions (day, night, overcast weather, etc.)	Detection range dependent on drone size and radar cross-section (RCS) High acquisition and installation cost Hard to detect low-altitude-flying, slow-moving or hovering UAVs False positives with similarly shaped objects (birds, clouds, etc.)
RF detection	Detects certain radio frequency bands where UAVs and GCS communicate for command and control (C2). High-accurancy detection Early warning capability even before UAV takes-off (when turned on) Triangulation is possible with multiple RF sensors Machine learning algorithms can classify drone transmissions	RF signal required, cannot detect autonomous flying drones Variable detection accuracy depending on drone type and frequency band Can detect only a few UAVs at a time Detection limitations for swarm of drones Some passive systems may emit RF signals, despite being characterized as passive systems
Visual (EO/IR)	Can distinguish drones from birds, especially with IR sensors IR cameras visualize surrounding environments, regardless of the external lighting or weather conditions and even in total darkness	Need for human interference or artificial intelligence to efficiently detect UAVs IR and EO cameras need a direct line of sight May confuse UAV with a bird or shaped small airplan Range limitations depending on weather conditions (clouds, rain, fog, mist, etc.)
Acoustic	Can differentiate between authorized and unauthorized UAS Can detect autonomous flying UAVs UAV detection can extend beyond line of sight Can provide drone direction or rough estimation	Depends on an available library of sound signatures Higher false positives due to the increasing number of drone models Does not work as well in noisy environments Detection limitations for swarms of drones

리를 이용하여 드론의 위치와 조종사의 위치 추정이 가능하다. 그러나 드론과 동일한 주파수 대역을 공유하는 통신 장비는 드론 탐지를 방해한다. 따라서 광범위한 주파수 대역을 탐색하고 상용 드론에 대한 주파수 특성을 데이터로 구축하여 미확인 주파수 출현시 불법 드론으로 추정하는 방법을 사용하기도 하지만 미확인 주파수가 반드시 불법 드론으로 확신할 수 없기 때문에 정확성이 떨어지는 단점이 있다.

3.1.3 전자광학 및 열영상(EO / IR)

가시광선 및 적외선 영역의 영상을 획득하고 처리하여 영상을 전시함으로써 표적을 탐지 및 식별할 수 있는 기술이다. 드론의 색상과 외관 형태, 비행 자세의 특징에 기초하여 다른 물체와 구분하며, 특히 적외선 영상 센서는 드론에서 발생하는 열을 감지하여 새와 구별할 수 있다. 광학적 특성과 해상도 때문에 탐지 거리에 한계가 있으며 위치파악을 위해서는 중복 운용되는 인접 자산과 연계하여 삼각법으로 위치를 추정하거나 레이저 거리 측정기를 활용해야 하나, 저고도로 상시 움직이는 드론을 조준하기가 쉽지 않은 단점이 있다.

3.1.4 음향탐지

드론 비행 중 모터와 프로펠러에서 발생하는 소리를 인식하여 탐지한다. 탐지된 음향이 드론이 방출하는 음향인지 여부를 식별하기 위해서는 모든 드론에 대한 음향 데이터베이스를 사전에 구축해 놓아야 한다. 음향 탐지 시스템 구축은 비용이 저렴하지만, 주변 소음에 민감해 주위 환경에 따라 탐지 범위가 제한된다. 독립적으로 운용할 때에는 효과적인 시스템은 아니지만 다른 탐지방법과 혼합하여 사용할 때에는 보다 강력한 탐지해법을 제공할 수 있다.

3.2 무력화 기술

탐지시스템과 마찬가지로 탐지된 드론을 무력화시키는 기술이 안티드론 시스템의 주요 비중을 차지하게 되는데, 이에는 전파방해, 스푸핑 등의 기술로 드론의 임무를 방해하는 소프트킬(Soft Kill) 방식과 레이저나 고출력 전자파, 대공화기를 이용하여 드론 비행체를 파괴하는 하드킬(Hard Kill)방식이 있다. 박찬정·김기용(2020)은 2000년부터 출원된 안티드론에 관한 151건의 특허를 분석한 결과, 드론 무력화 수단으로 그물이 66건, 전파교란 62건, 스푸핑 8건, 물리적 파괴 11건, 기타 4건으로 그물을 이용한 방식과 전파교란 기술이 가장 많음을 보여주었다[23]. 각각의 무력화 기술은 Table 5.와 같이 장단점을 내포하고 있어 국가중요시설의 특성과 특수한 안티드론 작전환경에 따라 선택적으로 사용해야 한다.

3.2.1 전파방해(JAMMING)

Table 5. Comparing C-UAS mitigation measures[1]

Method	Benefits	Limitations
RF Jamming	Use RF transmission to block signals and disrupt C2 between the GSC operator and UAV Disrupts radio-frequency (RF) communication link sCan include WiFi links Use of directional jamming to minimize interfering	May also jam and interrupt other communication signals Cannot affect autonomous driven drones (without an active RF link) May cause uncontrolled UAV flights and crashes A jammer's ability relies on the strength of its radio transmitter
GPS Jamming	Replaces GPS communication, increases difficulty to control the drone Disrupts Global Positioning Satellite communication link Prevents the return-to-home functionality	Cannot work if UAVs disable GPS or use encrypted GPS (military mission) Dangerous when used near airports, because airplanes also use satellite navigation May cause uncontrolled UAV flights and crashes
Spoofing	Replaces the communication link and takes control of drone operation Employs algorithms enhanced with artificial intelligence Can drive a malicious UAV to a designated area	Illegal procedure for civilian use, acts against computer fraud and abuse Not always successful, especially when encryption is used for C2 links Complicated method, not always successful Cannot affect autonomous driven UAVs not using GPS
Net or Birds	Active and aggressive countermeasures Net capturing: enforced and hardened UAVs physically capture a drone Birds of prey are used to attack and grab UAS Captures and drives UAVs in a specific area.	May cause collateral fatalities to other aircrafts. Not appropriate for airports Net capturing efficiency depends on UAVs' flight behavior, reaction time etc. Birds also pose hazards when flying around airports Depends on speed or maneuvering capabilities of rogue UAVs
EMP or Laser Guns	Aggressive and long-range countermeasures Destroys electronic systems of UAVs Disables drone flight	Can have negative effects on other passing aircrafts with fatal consequences May cause uncontrolled UAV flights and crashes Illegal in civil aviation contexts. Violates aviation security laws

전파방해는 조종자의 무선 조작이나 드론의 GNSS 수신기를 교란하여 드론이 원하는 목표로 이동할 수 없도록 한다. 무선 연결이 끊어지면 드론은 보통 지상으로 착륙하거나 이륙지점으로 복귀하기 시작한다[24]. 전파방해 장비는 제한된 범위에 영향을 미치므로 침입한 드론에 근접해야 하고, 가시선이 확보되어야 한다. 자동경로비행(Waypoint) 기능을 이용한 자율비행 드론에는 영향을 미치지 못한다. 광정면의 넓은 구역을 통제할 수 있으나 다른 통신장비에 간섭을 발생시키거나 목표 드론이 추락할 시에는 부수적 피해를 야기할 위험이 있다.

3.2.2 스푸핑(Spoofing)

통신 프로토콜을 조작하여 드론의 무선 주파수를 탐지하고 이보다 강한 전파를 송출하여 통제권을 탈취해 강제로 착륙시키는 방법이다. 통신 데이터 링크를 가로채 대상 드론을 제어하거나 GNSS 수신기에 가짜 신호나 악성 코드를 주입하여 위치 식별을 교란하여 강제로 착륙시키기도 한다[25]. 실제로 2011년 이란이 미국의 RQ-170 무인기를 GPS(Global Positioning System) 스푸핑 기술로 추락시켜 나포한 사례가 있다[26]. 그러나 스푸핑 시스템은 기술적으로 구현이 매우 어렵고, 목표 드론이 사용하고 있는 통신 및 신호 기술에 대한 세밀한 정보가 필요하다. 암호 통신이나 GNSS를 사용하지 않는 자율비행 드론에는 영향을 미칠 수 없다는 단점도 있다.

3.2.3 그물 또는 맹금류 이용 포획

드론이나 지상 발사체에 장착된 그물을 이용하거나 독수리나 매 등 맹금류를 이용하여 드론을 포획하는 기술이다. 그러나 고속으로 이동하는 드론을 포획하는 것은 쉽지 않고, 지상 발사체는 매우 근접해야 사용이 가능하다. 따라서, 맹금류는 숙련된 운용자가 필요하고, 소형 드론에 한해 포획 가능성이 있는 방식이며, 한편 공항 주변에서 운용시에는 항공기 운항에 방해 요인이 되어 위험한 점도 고려되어야 한다.

3.2.4 레이저(LASER)

고강도의 광선이나 레이저를 사용하여 드론의 카메라를 마비시키고 레이저 에너지로 드론 기체의 핵심 부분을 파괴하여 지상으로 추락시킨다. 개발 비용이 많이 들지만 운용 비용이 저렴하다. 한 번에 한 대의 목표에 제한되며 구름, 비, 안개와 같은 악천후에 영향을 받고 주변 인프라에 위험을 줄 수 있으며, 표적 드론만을 조준하여 맞추기 위한 정밀 기술 개발이 요구된다.

3.2.5 전자기파(EMP, Electromagnetic Pulse)

드론에 고출력의 강력한 전자기파를 방출하여 전자 회로를 태우거나 전자부품의 작동을 정지시켜 드론을 추락시킬 수 있는 기술로, 장기적이고 근본적인 대응책이 될 수 있다. 고출력 전자기파는 다른 항공기에도 영향을 미칠 수 있으며, 표적 드론이 추락 시 민간 피해 등 부수적인 2차 피해를 고려하여 사용에 주의를 해야 한다.

3.2.6 대공화기

비행중인 드론을 화기로 명중하는 것은 매우 어렵다. 드론은 소형으로 눈에 잘 보이지 않아 드론을 조준하여 사격하기 어렵고 빠르게 이동하는 드론을 명중시키는 것은 거의 불가능하다. 따라서 접근하는 드론의 움직임이 적거나 선회하는 등 제한된 조건 등이 충족될 경우에 유효한 방법이다. 특히, 드론이 격추되면 수직 낙하하여 지역에 따라 2차 피해를 야기시킬 수 있다는 점을 명심해야 한다. 폭탄을 장착하거나 유해한 물질을 탑재한 드론이라면 도시지역 인구밀집 등 작전지역의 특성을 고려하여 사용해야 한다.

4. 효과적인 안티드론 시스템 구축 방안

소형 드론의 확산으로 안티드론 시스템은 향후 분쟁에서 필수적인 시스템이 될 것이다. 사전 관리체계를 정립하여 합법적인 드론이 정상적으로 운용할 수 있도록 법과 제도적 정비가 선행되어야 하지만 불법 드론의 치명적인 공격으로부터 국가중요시설을 방호하기 위한 탐지 → 식별 → 결정 → 타격의 절차를 적용한 대응 시스템 구축이 필요하다.

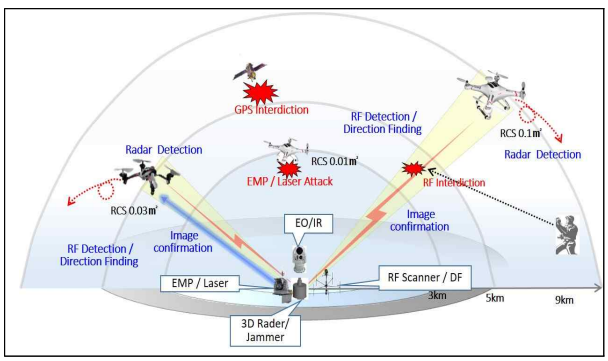

Fig. 1. Anti-Drone System (Author-Directed Creation)

Fig. 1.은 문헌 연구를 바탕으로 드론 관련 분야의 전문가를 대상으로 인터뷰를 실시한 결과, 효과적인 안티드론 시스템 구축 방안을 정리하여 그림으로 표현한 내용이다.

앞에서 살펴본 바와 같이 어떠한 시스템도 소형 드론에 대한 완벽한 대응 기술을 보유하지 못하기 때문에 장단점을 보완할 수 있는 시스템 구축이 효율적인 것으로 나타났다.

본 연구에서는 보다 효과적인 안티드론 시스템 구축방안에 대한 개선된 방안 수립을 위해, 앞서도 언급했듯 각종 문헌연구와 함께 간략한 델파이 조사법을 준용하였다. 기존 많은 연구가 개별적으로 단편적인 안티드론 기술 연구이거나 일반적인 해외 드론과 관련한 무력화 기술들을 소개하는 경향들이 있고, 무엇보다 국가중요시설의 큰 축에 해당하는 군시설과 관련한 대응방안은 아쉬운 측면이 있었다. 따라서 군조직내 드론의 군사적 활용방안과 그로 인한 안티드론에 대한 대응방안에 대한 실질적인 경험요소가 있는 군부대 현장 중심의 실효성 있는 대응방안을 마련하고자 델파이 조사를 병행한 것이다. 이종성(2006)[27]과 최규리(2012)[28]의 델파이 방법대로 군내부의 일반적인 여론조사방법과 전문가협의회의 장점 모두를 결합하여 적용할 수는 없었지만, 군내부 중요시설에 대한 현장의 특수한 상황을 충분히 반영하고 실효성 있으면서 신뢰할 만한 안티드론 대응방안 연구결과를 도출하기 위해 군내 근무경력 20년 이상의 영관급 군전문가들로 패널을 구성하였다. 무엇보다 드론과 관련한 운용 및 안티드론 대응방안에 대한 실질적인 의견을 제시할 수 있는 7명으로 국한하여 패널을 구성하였으며, 이중에는 육군에서 운용중인 드론관련 사업담당자와 드론봇전투체계 정책관여자 등까지 포함되어 있으므로 그 신뢰성은 높다 할 수 있다. 원래 델파이 방법(Delphimethod)이 美 랜드 연구소에서 개발되었을 당시부터도 시급하고 보안유지가 필요한 국방문제(소련 원자탄 보유량 추정)에 관한 전문가들의 숙의와 합의 도출이 목적이었듯이, 군시설을 포함한 국가중요시설에 대한 안티드론 대응방안에 대한 합리적인 수립에도 충분히 기여할 수 있는 방법으로 판단된다. 특히, 군의 특성상 계급고저에 따른 상호간 의견영향을 최소화하고, '두 사람의 의견은 한 사람의 의견보다 존중되어야 한다.'는 보편타당한 객관의 원리와 '다수 전문가의 판단은 소수 전문가의 판단보다 정확하다.'는 민주적 의사결정 원리에 가장 충실하게 대입할 수 있는 방식이라 할 수 있다. 무엇보다 델파이 패널(Delphipanel, 델파이 토론 참여자)들이 반복되는 델파이 절차속에 前단계의 의견들을 수정하고 피드백하는 과정에서 서로 공개되지 않고 상호간 직접적인 접촉없이 이루어진다는 점이 군조직과 가장 부합한 절차인 것이다. 본 연구에서는 델파이 방법을 3회에 걸쳐 질문을 하면서 각 단계에서의 대응방안 수렴을 위한 절차들을 진행하였고, 1차 개방형 질문(open-endedquestion)으로부터 2차 구조화된 폐쇄형 질문들을 만드는 과정을 통해, 안티드론 체계 구축과 관련하여 정리되고 개념화된 복합적인 안티드론 대응체계 구축방안을 제시하고자 하였다.

4.1 사전 관리체계 정립

불법 드론의 사용을 방지하기 위한 사전 관리체계는 드론 소유자와 드론에 등록번호와 식별번호를 부여하는 방법[29]과 드론의 항법 소프트웨어에 비행금지구역을 설정하여 GNSS를 기반으로 금지구역에 들어가면, 조종사에게 경보하거나 드론의 작동을 중지시키는 지오 펜싱(Geo Fencing) 기술이 있다. 운행 금지구역의 위도와 경도를 GPS상에 입력하여 일종의 가상 펜스(Virtual Fences)를 치게 된다[24]. 그러나 사전 관리체계는 위법행위를 식별하고 면허를 취소하거나 제한할 수 있어 무분별한 드론 운용을 통제할 수 있으나, 비행승인 없이 사용할 수 있는 모든 소형 드론을 사전에 등록하는 것이 불가능하고, 또한 지오 펜싱(Geo Fencing) 기술은 그 기능을 작동하지 못하도록 개조하거나 작동이 안되도록 조치한다면 억제효과를 기대하기 어렵다.

4.2 탐지자산의 혼합 및 중첩 운용

기존의 방공 시스템은 대부분 항공기를 염두에 두고 설계되었기 때문에 빠르게 비행하는 대형 물체를 탐지 및 추적하고 격추하는데 최적화되어 있다. 따라서, 작고 느리게 저공 비행하는 드론을 탐지하는데 한계를 드러내고 있다. 실례로 2016년 7월 이스라엘은 시리아에서 영공으로 날아온 러시아제 고정익 무인기를 전투기의 공대공 공격과 두 차례의 패트리엇 미사일 공격을 가했지만 결국 요격에 실패하였다[30]. 즉, 첨단 대공 방어망의 사각지대에서 운용되는 무인기의 확산에 맞추어 탐지 및 식별을 위한 안티드론 시스템 구축이 필수적이다.

상용드론이 초소형화되고 기동 및 적재 능력이 향상됨에 따라 레이더 및 센서와 같은 시스템을 통해 Radar Cross Section (RCS) 0.01 m2 이하의 작은 드론을 탐지할 수 있어야 한다. 그리고 수직 탐지범위(Elevation Coverage)가 50° 이상이어야 하고, 조류와 드론이 구분

되어 탐지될 수 있어야 한다. 또한 드론 운용에 사용되는 무선 통신채널의 주파수 제원을 확인할 수 있는 능력이 요구된다[31].

Fig. 2.는 탐지 자산의 능력과 효율적인 탐지자산의 운용을 개념적으로 제시한 그림이다. 기본적으로 전천후 활용이 가능한 레이더를 기반으로 영상센서, RF 탐지 센서를 보조 수단으로 다중 통합감시체계를 구축해야 효과적이다[32].

우선 1차 시스템은 레이더와 무선 주파수 센서를 이용하여 원거리 미확인 비행체의 접근을 탐지하고, 조기경보할 수 있도록 구축되어야 하며, 또한 사각 지역에서 접근하는 미확인 물체에 대한 탐지를 위해 음향 탐지장비가 보조로 구축되어야 한다. 2차 시스템은 레이더가 미확인 비행체를 탐지하면, 고성능 영상 카메라를 이용하여 확대 사진을 찍어 영상정보를 제공하고 불법 드론인지 또한 접근 목적이 무엇인지를 영상 이미지 신호를 프로세싱하여 분석할 수 있도록 구축해야 한다.

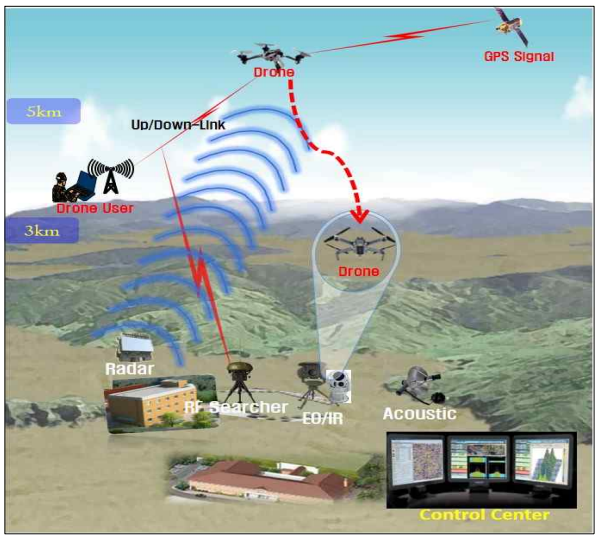

Fig. 2. Detection System (Author-Directed Creation)

줌 기능을 이용하여 고배율로 탐지하면 원거리 탐지 및 식별이 용이하나, 탐지 범위가 좁아져 감시 공백이 발생할 수 있다. 따라서 한번에 감시할 수 있는 공간 면적을 분할하고, 드론의 접근 속도를 고려하여, 순차적으로 탐색한다면 효과적이다. 물체 포착시 자동으로 경보하고 추적하는 기능을 보강한다면 탐지 거리를 확장할 수 있다. 또한 식별능력 제고를 위해 네트워크를 활용하여 모든 드론에 대한 외형 및 비행자세, 주파수 특성, 음향 특성 등 데이터베이스를 사전에 구축해야 한다.

4.3 적합한 대응방안 결정

탐지된 드론에 대한 적합한 대응방안 결정은 드론의 목적과 위협을 식별하고 주변 환경을 고려하여 적합한 무력화 수단을 선택해야 하는데 가용시간이 매우 제한된다. 예를 들어 3Km 거리에서 시속 60km로 접근하는 드론에 대한 탐지 및 식별 가용시간은 무력화를 위한 대응시간을 고려하면 대략 1분 이내로 제한된다. 기술의 발달로 드론은 훨씬 더 빠른 속도로 접근할 것이고, 가용 시간은 점점 줄어들 것이다. 따라서 탐지자산과 무력화 수단을 네트워크 연결하여 작전 통제소에서 실시간 제어할 수 있도록 구축해야 한다. 가용시간을 고려하여 적절한 대응 수단이 적시적으로 결정될 수 있도록 탐지 자산을 네트워크로 연결하고, 작전 환경에 따라 적합한 수단에 무력화 명령을 할 수 있도록 지휘통제 시스템을 구축해야 한다.

4.4 무력화 수단 다중 배비

드론의 무력화 및 파괴 능력 요소에서는 혹한과 혹서기와 같은 악조건에서 사용할 수 있는 능력과 함께 탐지 및 식별된 드론을 전파 교란을 통해 무력화할 수 있는 능력이 요구되었다[31].

세계 시장에 공개된 안티드론 시스템은 다양한 탐지 및 무력화 기술을 사용하고 있는데, Table 6은 Michel(2018)이 세계의 안티드론 시스템을 조사한 결과로, 무력화 시스템 147개 중에서 96개 시스템이 전파방해 기술을 사용하고 있고, 약 30개의 시스템이 포획 및 파괴 등 물리적 타격 기술을 사용하고 있는 것으로 나타났다. 그러나 어떠한 시스템도 100% 무력화는 불가능하여 작전환경을 고려하여 2개 이상의 시스템을 복합 운용하는 것이 효과적인 것으로 드러났다.

Table 6. C-UAS INTERDICTION METHODS[33]

Methods	Amount
Jamming (RF, GNSS, or Both)	96
Net	18
Spoofing	12
Laser	12
Machine Gun	3
Electromagnetic Pulse	2
Water Projector	1
Sacrificial Collision Drone	1
Other	6

드론을 무력화 하는 방법은 드론의 임무를 저지하는 소프트킬 방식과 드론 자체를 파괴하는 하드킬 방식으로 구분하여 대응 가용시간과 드론에 탑재된 무기체계 및 2차 부수적 피해를 고려하여 적절한 대응 방법을 선택해서 사용해야 한다. 드론의 기술 발전을 고려할 때 재머를 활용한 무력화는 확실한 대응수단이 될 수 없다. 또한 전파방해는 주변 통신장비에 간섭을 야기시켜 공항에서 운용시 항공 통제를 방해하고 GNSS교란은 항법장치에 의존하는 지역에서 사용시 위험한 방식이다. 포획 그물망은 사용할 수 있는 거리가 매우 짧고 다수의 무인 비행체를 활용하는 군집비행에 대응하기 어려운 방식이다[32]. 따라서 드론이 접근하는 원거리에서부터 소프트킬 방식으로 드론을 차단하고, 이를 극복하고 가까이 접근하는 드론에 대해서는 근거리에서 하드킬 방식으로 파괴하여 무력화 할 수 있도록 대응 수단을 다중 배비하는 것이 효과적이다. Fig. 3.은 다양한 무력화 기술의 능력을 도식화하고 이를 적용한 효율적 대응방안을 제시한 그림이다.

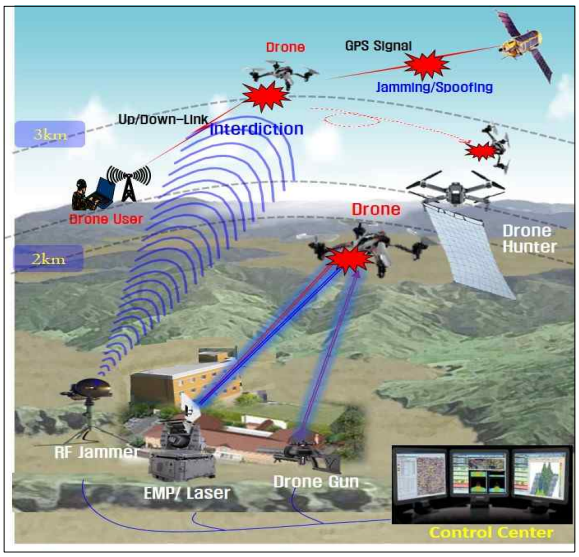

Fig. 3. Interdiction System (Author-Directed Creation)

안티드론 시스템이 작동되면 드론이 요격된다. 이는 사용된 무력화 수단에 따라 드론이 지상에 착륙하거나 이륙지점으로 복귀, 드론 포획(그물), 드론의 부분 또는 완전파괴 등 다양한 결과를 초래한다. 가급적 분석 및 처리를 위해 파괴보다는 회수하여 분석에 활용하는 것이 바람직하다. 만약 드론이 잠재적으로 무장한 경우 폭발물 처리반을 불러 평가한 후 장치를 해제할 수 있다. 비무장 드론도 마찬가지로 주의해서 다루어야 한다. 장치가 손상되면 리품 이온 배터리가 연소할 위험이 있다. 기기가 계속 작동하면 로터가 손상될 수 있다. 드론의 장치에 대한 범죄수사 및 과학적인 정밀 분석을 위해서 시스템의 완전성과 시스템이 운반하는 잠재적으로 귀중한 데이터가 손상되지 않도록 일련의 조치 단계를 따라야 한다.

5. 결론

국가중요시설에 대한 드론방어체계 구축방안들은 기존 연구에서도 탐지·식별과 무력화의 공식으로 제시되고 있는 것들은 있으나, 사실상 구현되기 어려운 원론적 논의에 그치고 있는 실정이다. 실질적으로 국가중요시설에 대한 안티드론 시스템 구축은 매우 미흡한 실정이다. 그럼에도 최오호(2019)가 국회 보안분야를 담당하는 공무원을 대상으로 실시한 설문조사 결과, 드론을 이용한 국회 테러 공격 가능성에 대해 55.7%가 가능성이 높다고 인식하고, 안티드론 시스템 도입에 61.8%가 필요한 것으로 인식하고 있는 것으로 나타났다[34].

따라서 본 연구는 최근 안티드론 기술이 국가중요시설 방호에 사용될 수 있는 여러 가지 기술을 검토하여 드론의 위협으로부터 국가중요시설을 방호하기 위한 효과적인 안티드론 시스템 구축 방안을 제시하고자 하였다. 연구결과, 탐지체계는 다양한 센서의 장단점을 보완하여 탐지율을 향상시킬 수 있도록 중첩·혼합운용하는 것이 효과적이며, 무력화 수단은 소프트킬 방식과 하드킬 방식을 배비하여 작전환경에 맞게 선택적으로 사용할 수 있도록 융통성을 확보하는 것이 효과적인 것으로 드러났다. 다시 말해 불법드론에 대한 사전관리체계(DB) 정립, 탐지자산 혼합 및 중첩운용, 적합한 대응방안 결정, 무력화 수단 다중배비 등이 그것이다. 이러한 중첩·복합적 안티드론체계 운용은 국가중요시설의 특성과 운용환경 등을 고려하여, 최적의 방호체계를 복합적으로 구축하는 것이 무엇보다 시급한 과제임을 설명해 주고 있다. 물론 그럼에도 드론의 특성을 고려할 때 이를 완벽히 방호할 수 있는 체계를 구축한다는 것은 불가능하다는 한계는 엄연히 존재할 수 있다. 현존 기술을 가장 효율적으로 활용할 수 있는 대응방안 모색과 드론 제작기술에 걸맞는 안티드론 솔루션을 지속적으로 모색함과 아울러 안티드론 기술 개발을 위한 차후 연구 과제를 꾸준히 도출하는 노력이 필요할 것으로 사료된다.

이는 창과 방패의 모순처럼 안티드론 기술이 발달하면 드론 기술 또한 안티드론 시스템을 회피하기 위해 부단한 업그레이드를 시도하며 진화되어 가고 있기 때문이다.

드론의 창이 날카로워지면 안티드론 방어 시스템도 더 견고하게 구축되어야 하는데, 한 번에 해결할 수 있는 시스템을 찾는 것은 어려운 일이 아닐 수 없다. 각 기술의 장점을 활용한 복합·융합적인 방호시스템을 구축하여 방어망을 이중삼중으로 견고하게 중복 구비해야 비로소 안전한 환경 조성이 가능할 것이다.

REFERENCES

[1] G. Lykou, D. Moustakas & D. Gritzalis. (2020). Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies. Sensors (Basel, Switzerland), 20(12), 3537. https://doi.org/10.3390/s20123537

[2] B. Hubbard, P. Karasz & S. Reed. Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran. The New York Times. https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html

[3] D. H. Lee & W. Kang. (2019). A Study on the Establishment of Anti-Drone Concept and Effective Response System. *KOREAN SECURITY JOURNAL, 60,* 9-31.
DOI : 10.36623/kssa.2019.60.1

[4] O. H. Choi (2019). *A Study on the Application of Drone and the Anti-drone System in the National Assembly*. Doctoral dissertation. Kyonggi University, Seoul.

[5] T. Jang & H. H. Yang. (2020). A Study on the Response of Police against Terrorism Using Drone. *Korea Drone Studies, 2(1)*, 24-47.

[6] J. S. Kim. (2019). A Study on the Possibility of Unmanned Aerial Vehicles(UAV) Threat in Nuclear Facilities. *Transations of the Korean Nuclear Society Autumn Meeting*.

[7] Park. H. K. (2018.12.21. 14:45). *Gatwick Airport Closed, How dangerous is a drone in a plane?* https://news.mt.co.kr/mtview.php?no=2018122114438222633.

[8] Lee S. Y. Kang Uk. (2019). *A study on the reestablishment of the drone's concept,* Korena security journal. Vol. 58.
DOI : 10.36623/kssa.2019.58.2

[9] O. H. Choi (2019). *A Study on the Application of Drone and the Anti-drone System in the National Assembly*. Doctoral dissertation. Kyonggi University, Seoul.

[10] Lee Im Gul. (2019). *A study on the Police Use of Drones,* Doctoral dissertation. Hansei University, Gyeonggi.

[11] Shin H. J. (2016). *A study on application strategies and tasks of the police drones*, Journal of Korean Public Police and Security Studies. Vol 13(1) pp. 211~232
DOI : 10.25023/kapsa.13.1.201605.211

[12] Jang E T. (2019). *A Study on the Response of Police against Terrorism Using Drone.* Master's thesis. Hansei University, Gyeonggi.

[13] Kim D. H. (2018). *A Study on the countermeasures and drone's threats in Military security*. Journal of digital convergence. Vol.16(10)
DOI : 10.14400/JDC.2018.16.10.223

[14] Jo H. J., Yun M. W. (2016). *The probable use of UAV(Unmanned Aerial Vehicle) in crime, cybercrime, and terrorism and responses*, Korean Security review. Vol 46. pp. 189-216.
UCI : G704-001904.2016..46.001

[15] Kim S. T., Lee. S. W. (2015). *A Study on Improving Private Guard for National Critical Facility Against 'Drone Terror'*, Journal of The Korean Society of Private Security. Vol.14(5), pp.1~28.
UCI : G704-SER000010424.2015.14.5.013

[16] Wallace, R. J. & Loffi, J. M. (2015). Examining Unmanned Aerial System Threats & Defenses: A Conceptual Analysis. International Journal of Aviation, Aeronautics, and Aerospace, 2(4): 1-32.
DOI:10.15394/ijaaa.2015.1084

[17] Lee Dong Hyuk. Kang Uk. (2019). *A study on the establishment of anti-drone concept and effective response system,* Korena security journal. Vol. 60.
DOI : 10.36623/kssa.2019.60.1

[18] Choi,S.H., Chae, S.H., Cha, J.S., Cha, J.H., Ahn,J.Y., (2018), *Recent R&D Trends of Anti-Drone Technologies*, Electronics and telecommunications trends, Vol. 33(3): 78-88.
DOI:KINX2019065693

[19] Jeong J. Y., Jeon Y. T. (2017), A study on the trend of anti-drone technologies and their applications, Korean Security Journal, Drone Special Issue. Vol-No.S. 33-56.
DOI : 10.36623/KSSA.2017.51.1.2

[20] Kim H.J., Lee,S.W., Kim, B.M., (2018). An Empirical Study of Anti-Drone for the Police Use , 『Police Science Institute. Vol. 32(2): 69-94. DOI : 10.35147/knpsi.2018.32.2.69

[21] Kim Hyung Zu. Sangwon Lee & Kim Beom Mo (2018). An Empirical Study of Anti-Drone for the Police Use : The Police Science InstituteFocusing on the Neutralization Means and Methods. *THE JOURNAL OF POLICE SCIENCE INSTITUTE, 32(2)*, p. 79.
DOI : 10.35147/knpsi.2018.32.2.69

[22] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi & J. Chen. (2018). Anti_Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges. *IEEE Communications Magazine*. vol. 56, No. 4, pp. 68-74.
DOI: 10.1109/MCOM.2018.1700430

[23] C. J. Park & K. Y. Kim. (2020). Patent Trend Analysis of Anti-Drone : Focusing on the Neutralization Means and Methods. *THE JOURNAL OF KOREAN INSTITUTE OF NEXT GENERATION COMPUTING, 16(2)*, 7-17.

[24] J. Y. Jung & Y. T. Chun (2017). A study on the trend of anti-drone technologies and their applications. *KOREAN SECURITY JOURNAL, 51(1)*, 33-55.
DOI : KINX2017210883

[25] J. Y. Park. (2020). Anti-Drone Technology for Protecting Electric Power Facilities from Bad Drones, *The Korean Institute of Electrical Engineers, 69(4),* 15-20.
DOI : KINX2020156300

[26] N. Owano. (2011). *RQ-170 drone's ambush facts spilled by Iranian engineer.*
https://phys.org/news/2011-12-rq-drone-ambush-facts-iranian.html

[27] Lee. J. S. (2006). Delphi method. KYOYOOKBOOK. Seoul.

[28] Choi. G. L (2012). A Study on Delphi for the Development of the Creative Personality-Oriented Scientific Talent Education Plan. The Journal of Global Institute For Talented Education Vol. 22(2). pp. 387-410.

[29] S. B. Jung. (2019). Case Analysis of Drone Terrorism and Its Efficient Countermeasures. *The Police Science Journal (PSJ), 14(2),* 149-176.
DOI : 10.16961/polips.2019.14.2.149

[30] H. Michel. (2019). *COUNTER - DRONE SYSTEMS, 2nd Edition,* Center for the Study of the Drone at Bard College.

[31] H. C. Ahn, K. J. Kim, H. S. Yang, K. D. Hong & Y. J. Park.(2020). A Study on the Consideration of the Required Operational Capabilities for the Smart Defense Drone System against Hostile Drones in National Important facilities. *J. Korean Soc. Hazard Mitig.* Vol. 20, No. 3, pp. 187~195.
DOI : KINX2020128582:SERL1000017932

[32] S. I. Kim. (2019). A Study on Regulatory Regulation and Improvement Plan of RPA. *The Korean Journal of Air & Space Law and Polity, 34(2)*, 3-32.
DOI : dx.doi.org/10.31691/KASL34.2.1.

[33] H. Michel. (2018). *COUNTER - DRONE SYSTEMS,* Center for the Study of the Drone at Bard College.

[34] O. H. Choi. (2019). *A Study on the Application of Drone and the Anti-drone System in the National Assembly.* Ph.D. Dissertation. .Kyonggi University, Seoul.

황 순 필(Soon-Phil Hwang) [정회원]

·1987년 2월 : 육군사관학교 중국어학과(학사)
·1998년 2월 : 연세대학교 교육학과(교육학 석사)
·2019년 2월 : 대전대학교 국방정책/전략학과(박사) 수료
·2019년 5월 ~ 현재 : 육군부대 근무
· 관심분야 : 드론, 안티드론(대드론), 드론보안
· E-Mail : hspsalam@hanmail.net

김 두 환(Doo-Hwan Kim) [정회원]

· 1998년 2월 : 금오공대 기계공학과(공학사)
· 2013년 2월 : 건양대학교(행정학석사)
· 2020년 3월 : 건양대학교 대학원 행정학 박사
· 현재 : 육군본부 정보작전참모부 서기관 근무
· 관심분야 : 드론, 안티드론, 군사보안, 정보보안, 해킹, 양자보안, 블록체인, 빅데이터(텍스트마이닝)
· E-Mail : highmt2015@naver.com