Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 2 pp. 651-659, 2023

https://doi.org/10.5762/KAIS.2023.24.2.651
ISSN 1975-4701 / eISSN 2288-4688

# 드론 사고 사례와 기술 동향에 따른 안티드론 대응 방안

심준형[1], 황의천[1], 손창근[2*], 류연승[1]
[1]명지대학교 보안경영공학과, [2]명지대학교 융합보안안보학과

# Anti-Drone Countermeasures According to Drone Accident Cases and Technology Trend

Jun-Hyung Sim[1], Eu-Cheon Hwang[1], Chang-Gun Son[2*], Yeon-Seung Ryu[1]
[1]Department of Security Management Engineering, Myongji University
[2]Department of Convergence Security, Myongji University

**요 약** 기존에 군사용 목적으로 개발된 드론은 기술 발전의 영향으로 관련 산업이 성장하고 드론 시장 역시 확대되고 있다. 이에 따라 드론 위험요인 역시 증가하고, 실제 드론으로 인한 다양한 사고들이 발생하고 있는 실정이다. 드론 위험요인에 대한 대응 체계로서 등장한 안티드론은 탐지, 식별, 무력화의 과정을 통해 불법드론에 대응하고 있다. 실제로 많은 국가들이 드론 관련 사고 발생을 계기로 안티드론 시스템을 구축하고 있으며, 앞으로 드론 관련 기술 발전에 따라 드론의 활용도가 점진적으로 확대될 것으로 예상되는 만큼 우리나라에서도 드론 위험요인에 대한 실효성 있는 대응 체계의 구축이 요구된다. 또한 현재 활발하게 연구가 진행되고 있는 드론 무력화 기술의 실질적인 적용을 위해서는 드론 위험요인에 대한 정확한 파악이 전제되어야 하며, 특히 탐지와 식별 관련 기술 개발의 활성화가 요구된다. 향후 위험요인의 파악 및 고도화된 탐지 식별 기술을 토대로 보호 대상자나 시설물의 환경적 특성을 고려한 안티드론 대응 체계 방향이 설정되어야 할 것이다.

**Abstract** Drones developed for military purposes are growing related industries and expanding the drone market due to technological advances. Accordingly, drone risk factors are also increasing, and various accidents due to actual drones are occurring. Anti-drone, which has emerged as a response system to drone risk factors, is responding to illegal drones through detection, identification, and neutralization. Indeed, many countries are building anti-drone systems in the wake of drone-related accidents. The use of drones is expected to expand gradually due to the development of drone-related technologies. Hence, Korea must establish an effective response system to drone risk factors. In addition, for the practical application of drone neutralization technology, which is currently being actively researched, accurate identification of drone risk factors must be premised. In particular, the development of detection and identification-related technologies is required. In the future, based on the identification of risk factors and advanced detection and identification technology, the direction of an anti-drone response system should be set, considering the environmental characteristics of persons subject to protection or facilities.

**Keywords :** Drone, Anti-Drone, Response System, Drone Risk Factors, Neutralization Technology

*Corresponding Author : Chang-Gun Son(Myongji Univ.)
email: soncg2209@naver.com
Received November 9, 2022 Revised December 13, 2022
Accepted February 3, 2023 Published February 28, 2023

# 1. 서론

인공지능과 정보통신 기술의 발전을 통해 현대 사회는 다각적인 변화를 경험하고 있다. 군사적 목적으로 개발된 드론 역시 기술 발전에 힘입어 점진적으로 민간 영역까지 확대되어 현재 다양한 분야에서 드론의 활용 수준이 높아지고 있다.

정부 차원에서도 드론 활용도 증대를 위한 '드론 활성화 지원 로드맵'과 '드론 산업 발전 기본계획' 등의 수립 및 추진 등을 통해 드론 산업 육성을 위한 지원을 강화하고 있다[1].

드론은 비행을 가능하게 만드는 엔진과 프로펠러, 교신용 센서와 통신시스템, 이미지와 동영상을 촬영하는 카메라 등을 장착하고 있으며, 무선조종기로 조작하는 소형 헬리콥터 운용 방식과 크게 차이가 나지 않는다[2].

드론의 기본적인 운용 방식은 GPS 도입, 자율비행 컨트롤러, 다양한 센서 기술의 탑재, Motion Planning 경로계획 기술 활용 등과 같이 첨단 기술 발전의 영향으로 첨단화, 세밀화 등의 변화를 가져오고 있다. 특히 코로나19 팬데믹 상황에서도 민간 드론 시장은 2020년 56억 달러로 성장하였고, 향후 2029년에는 140억 달러로 연평균 15.6%의 성장세를 기록할 것으로 예상되고 있다[3].

이처럼 기술 발전의 영향으로 드론 산업이 성장하고 시장 규모가 확대됨에 따라 그에 따른 다양한 위험과 문제 발생에 대한 우려도 높아지고 있다. 드론을 이용한 범죄나 사생활 침해 논란, 국가 주요 시설물에 대한 테러 위협, 드론 추락에 따른 인적, 물적 피해 발생, 안전 및 보안의 취약성 등이 그것이다. 이는 드론 기술의 발달로 드론이 대중적 기술 플랫폼으로 확장됨에 따라 드론이 범죄나 테러 등에 악용되어 사회문제화되는 '비열한 드론(dirty drone)'에 대한 대응책의 마련을 요구하는 것이다[4].

따라서, 본 연구는 드론 기술 발전에 따른 위험요인과 최근 동향을 검토하고, 드론 발전과 안전의 조화를 위한 대안으로서 효과적인 안티드론 대응 방안 구축의 필요성을 제시해 보고자 한다.

# 2. 본론

## 2.1 드론 기술 현황

### 2.1.1 드론의 개념

현재 '드론(drone)'이라는 별칭으로 널리 사용되는 무인항공기(UAV: Unmanned Aerial Vehicle)는 꿀벌의 수벌이 날아다닐 때 내는 윙윙 소리가 무인항공기의 소리와 유사하다는 의미에서 드론으로 명명되었으며, 1930년대 영미에서 대공포 훈련용으로 개발된 무인항공기가 타겟 드론(target drone)이라 불리면서 드론이라는 용어의 사용이 시작되었다[5].

이러한 드론은 통상적으로 조종사가 없는 항공기를 의미하며, 미국 연방 항공청(FAA: Federal Aviation Administration)에서는 드론을 "조종사가 탑승하지 않고 공중 비행을 목적으로 사용되는 장치"로 정의하고 있고, 국제민간항공기구(ICAO: International Civil Aviation Organization)에서는 "조종사가 탑승하지 아니하고 비행하는 항공기 및 그와 결합된 요소를 포함한 시스템인 UAS(Unmanned Aerial System)"로 드론을 정의하고 있다.

이처럼 드론 개념의 정의는 조금씩 차이가 있지만, 공통적으로 '무인' 형태로 운용된다는 의미를 갖는다.

### 2.1.2 드론 기술의 활용

니콜라 테슬라에 의해 시작된 드론 초기 연구는 제2차 세계대전 당시 주로 대공포 훈련 목적으로 사용된 영국의 'Queen Bee'를 거쳐 베트남전에서 사용된 'Firebee', 1991년의 걸프전(Gulf War)에 사용된 드론 등 주로 군사 목적의 드론 연구 및 활용이 주를 이루었다.

이후 2000년대에 들어서면서 첨단 기술의 드론 적용이 이루어졌고, 군사적 용도 외에도 상업용 드론의 확장이 두드러지기 시작하였다.

무인항공기 드론의 구조는 하드웨어(프레임, 컴퓨팅 보드 등)와 컴퓨팅 보드에 내장된 소프트웨어, 펌웨어라는 세 가지 구성 요소로 이루어져 있다.

먼저 하드웨어(Hardware)의 경우, 신호를 발생하는 컴퓨팅 보드와 드론의 뼈대를 구성하는 프레임, 무인항공기 드론의 날개를 회전하도록 만드는 로터, GPS 등과 같이 주변의 환경이나 필요한 정보를 수집하는 센서(sensor) 등을 포함한다.

컴퓨팅 보드는 플라이트 컨트롤러(Flight Controller)라는 이름을 가지고 있는데, 이 플라이트 컨트롤러는 드론에 장착된 다양한 센서(sensor)에서 수신된 정보들을 수집하고 취합하여 현재 드론의 위치와 드론이 위치한 곳의 주변 환경 특성, 드론이 어떤 자세로 비행하고 있는지 등의 데이터를 파악하는 역할을 수행한다[6].

## 2.2 드론 기술 발전에 따른 위험요인

첨단기술과 드론의 결합은 드론 산업의 확장을 가져왔지만, 이에 따른 위험요인 역시 늘어난 것이 사실이다. 드론 사고를 유발하는 위험요인으로는 첫째, 드론 구조상의 결함이나 조종사의 운영상 과실을 들 수 있으며, 둘째, 해킹 및 시스템바이러스, 셋째, 추락피해 등이 있다.

먼저 드론 구조의 결함으로는 GPS 결함, 배터리 결함에 따른 폭발, 과방전, 하자 부품의 사용, 정비 불량 등을 들 수 있으며, 2009년에 발생했던 농약 살포 드론에 의한 사망사고의 경우, 조종사가 드론 트림 설정을 확인하지 않은 과실이 확인된 바 있다.

특히 조종사의 과실에는 고의과실도 포함되는데, 사생활 침해를 목적으로 드론에 대한 고의적 악용 및 드론 간 충돌사고 등의 위험이 존재한다.

Fig. 1. '09 Pesticide-spraying drone deaths

해킹 및 시스템바이러스에 따른 사고 역시 기술 발전에 따른 드론의 위험요인으로 제시할 수 있다. 2012년도 인천 송도에서 발생한 캠콥터 S-100의 추락으로 인한 사망사고의 경우, 전파 교란에 의한 GPS 수신 불가능이 원인이었다.

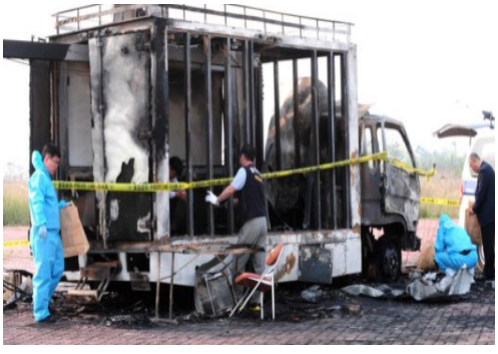

Fig. 2. '12 Songdo Unmanned Helicopter Accident Due to Hacking

드론의 경우 무선 통신망을 이용한 원격 조종으로 운용되기 때문에, 스푸핑(spoofing), 재밍(jamming), 하이재킹(hijacking) 등의 해킹에 취약할 수밖에 없다.

드론의 추락 사고는 드론 기체가 지상 혹은 지상의 사람이나 물체 등에 충격을 가해 인적, 물적 피해를 유발한다.

2012년, 인천 송도의 해군 드론 추락 사고는 사망자 1명, 부상자 2명의 인적 피해를 발생시켰고, 2015년 경남 합천의 방재용 드론의 차량 충돌 및 전소 사고 등은 물적 피해를 가져왔다.

Fig. 3. '12 Naval Unmanned Helicopter Crash

이외에도 드론 비행 중 다른 드론이나 유인항공기 등과 같은 외부 물체와의 직·간접적 접촉에 의한 공중 충돌사고, 고화질 카메라를 장착한 드론을 이용한 사생활 침해 및 범죄행위, 드론을 이용한 마약, 무기 등의 밀반입 등 드론의 사용 범위 확대에 따른 위험요인이 존재한다.

그중에서 드론 공중 충돌사고는 빈번하게 발생하는 사고 중의 하나로, 지난 21년도에 칠레의 해군 헬리콥터가 비행 중 드론과 충돌하여 비상 착륙한 사건이 발생하기도 했다. 만일 비상 착륙에 성공하지 못했다면 헬리콥터 조종사는 물론, 추락한 헬리콥터에 의한 인명피해가 발생했을 가능성이 매우 높다.

Fig. 4. '21 Chilean Navy helicopter and drone crash

이러한 사고들은 드론의 위험요인을 보여주는 것으로, 군사용 목적에서 출발한 드론이 민간 영역에서 취미 활동, 상업용 드론 활성화를 통해 생활 편의라는 장점을 가져왔지만, 그 이면에 테러나 범죄 등의 불법행위에 악용되며 사회 안전을 위협할 수 있다는 우려가 현실화되고 있음을 시사한다.

실제로 드론을 이용한 테러 위협에 대한 우려는 이미 오래전부터 현실화되고 있는 실정이다. 2011년 9월 미국에서는 C-4 폭탄을 장착한 드론을 이용한 미국 국방부와 의사당 공격 계획이 FBI에 발각되어 미수에 그치면서 드론을 이용한 최초의 테러 시도가 발생한 바 있다. 이후 일본에서는 15년 4월에 방사성 물질을 탑재한 소형 드론이 투하되는 사건의 발생으로 소형 드론에 대한 보안 취약성 문제가 이슈화되기도 했다.

전쟁에서의 드론 테러 사례도 증가하고 있는데, 16년 10월 이라크에서는 IS가 자폭용 드론 공격을 감행하였고, 당시 공격에 사용된 드론은 시중에서 쉽게 구할 수 있는 상업용 초소형 드론으로, 민간용 드론으로 인한 위험요인의 발생 가능성을 확인하는 계기가 되었다.

베네수엘라에서는 18년 8월에 드론을 이용하여 국가 원수를 암살하려는 시도를 통해 다수의 드론이 테러에 활용될 수 있다는 인식을 가져왔고, 19년 9월에는 예멘의 후티 반군이 사우디아라비아의 석유시설 2곳에 대한 드론 폭격을 감행하여 전 세계 산유량의 5%에 달하는 정유시설이 파괴되는 사례도 발생하였다.

특히 세계적으로 충격을 가져온 것은 누구나 구입이 용이한 저가의 상업용 드론이 테러의 도구로 사용되었다는 점이다. 여타의 재래식 무기에 비해 저렴한 가격과 조종사의 신변을 밝히기가 어려운 비노출 조종이라는 장점 때문에 앞으로의 드론 테러 시도에 있어서 상업용 초소형 드론을 활용하는 것에 대한 대비책 마련이 시급하다고 할 수 있다.

이처럼 드론과 같은 새로운 형태의 위협 요인으로 인한 위험의 예방을 위해서는 기술 생산 주체는 물론, 법집행을 통한 제도적 관리가 상호 유기적으로 통합적으로 대응할 수 있어야 할 것이다[7].

## 2.3 안티드론의 개념과 기술

### 2.3.1 안티드론의 개념

'안티드론(anti-drones)'은 범죄, 테러 등 여러 분야에서 사회 안전을 저해할 수 있는 드론의 위험요인에 대응하는 공중 방어 플랫폼의 개념으로 등장하였다[7].

안티드론은 주로 산업 기술 분야에서 발생하는 드론 범죄 및 사고 예방을 위한 감시와 무력화 기술이며, 드론의 공격에 대하여 '탐지-식별-무력화'라는 3단계 매커니즘을 적용한 기술, 범죄 및 사고 예방을 위해 다각도로 드론을 무력화하는 기술 등으로 정의되고 있다[8].

즉, 안티드론은 드론의 접근을 탐지하는 탐지 기술과 드론 비행 자체를 무력화할 수 있는 무력화 기술이 복합적으로 적용된 체계라 할 수 있다.

### 2.3.2 안티드론 기술 현황

일반적으로 안티드론은 상대 드론에 대한 탐지를 시작으로 해당 드론에 대한 식별, 무력화의 과정을 거쳐 드론 위험요인을 제거하게 되는데, 탐지는 불법 드론에 대한 대응 초기 단계에 해당하며 특정 구역에 침입한 물체가 드론인지의 여부를 판단하는 과정이다. 식별은 탐지된 드론이 불법 드론인지를 파악하는 과정으로, 무선 통신을 통해 드론의 ID를 송수신하여 조종자의 신원을 파악하는 것이며, 무력화는 불법 드론으로 식별된 드론의 침입과 위협에 대한 제거 과정을 의미한다.

Table 1. Anti-drone technology classification[8]

| Sortation | Content | | |
|---|---|---|---|
| Standardize regulatory and manufacturing functions | Pre-management (drone registration number, pilot license) scheme<br>Geo fencing | | |
| A passive means | Move people to safety<br>Block the view by covering the building with trees or curtains<br>Locking doors or windows | | |
| An active means | Physical incapacitation | • Drone capture<br>• Direct damage | • Use a net<br>• Using the Eagle<br>• Using the Laser<br>• Using Firearms |
| | Electronic incapacitation | • Radio jamming technology | • An interference device<br>• Drone gun |

안티드론 시스템에는 위협이 될 수 있는 드론의 접근을 효과적으로 탐지할 수 있도록 광학, 음파, 방탐, 레이더 등 다양한 센서 기술과 물리력에 따라 드론의 비행을 무력화하는 기술이 포함되어 있다[9].

센서 기술인 음향 탐지 센서는 드론이 작동할 때 일어나는 프로펠러 회전에 따른 소음을 탐지하는 것으로, 최대 탐지 거리가 짧고 소음이 많은 환경에서는 탐지가 어렵다는 한계가 있다. 방향 탐지 센서는 제어신호 및 영상 데이터 송수신용 대역의 RF(Radio Frequency) 신호의 방향과 위치를 감지하는 것으로, WiFi 주파수와 동일한

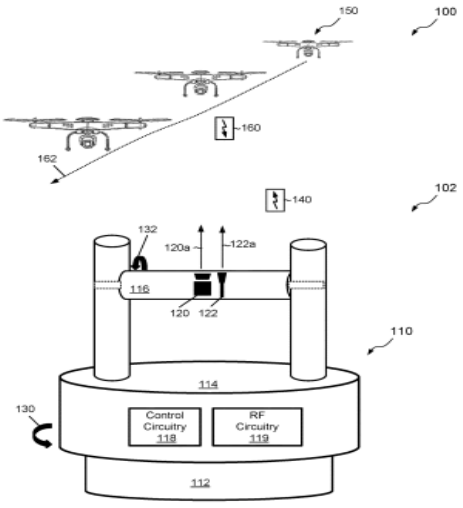


Fig. 5. U.S. Registered patent 10,044,465(Adaptively disrupting unmanned aerial vehicles)

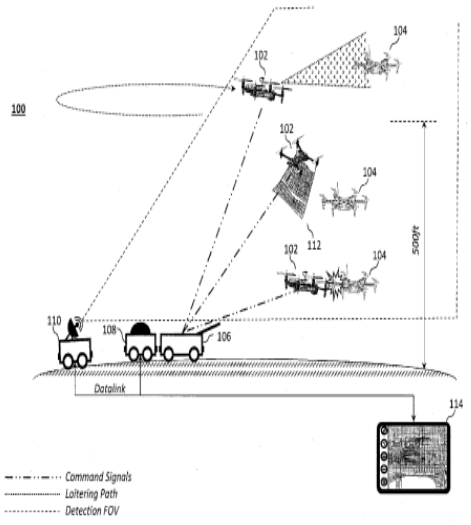


Fig. 6. U.S. Registered patent 10,495,421(Aerial vehicle interception system)

까닭에 WiFi 설치량이 비교적 많은 도심에서의 활용도가 떨어지나 조종사의 위치 추정이 가능하다는 이점을 갖는다. 이외에 가시광선 영역과 적외선 열화상 영역의 영상정보를 통해 드론을 팀지하는 영상 센서, 특정 대역의 RF 신호 송출 및 반사 신호의 수신을 통해 표적이 되는 드론을 탐지하는 레이더 센서 등의 기술이 있다.

드론을 식별하는 방식은 육안으로 드론의 조종자를 파악하는 육안식별과 전자식별이 있는데, 전자식별에는 수동식별과 능동식별이 포함된다. 육안식별은 드론 본체에 부착된 드론 식별 번호(DIN, Drone Identification Number)의 위변조와 분리를 금지하고 해당 식별 번호를 통해 사고 발생 시 드론의 소유자와 조종자를 판단하게 된다.

전자식별은 통신거리의 범위 내에서 비행 중인 드론에 대해 DIN이나 조종자 식별 번호(PIN, Personal Identification Number)를 파악하는 방식으로, 수동식별은 비행 중인 드론이 주기적으로 발송하는 DIN, PIN과 좌표와 시간, 속도 및 방향, 이륙지 좌표 등을 수동으로 파악하는 것이고, 능동식별은 식별기를 이용해 파악한 DIN과 PIN을 통해 비행 목적 등을 통신을 통해 질의응답하는 과정으로 드론에 대한 식별이 진행된다는 차이가 있다.

드론 비행 무력화 기술에는 드론 조종 신호의 대역에 방해 전파를 방사하여 제어를 무력화시키는 전파 교란 기술, 드론 자체에 산탄총이나 레이저 빔 조사 등과 같은 직접적인 물리력을 행사하여 파괴하는 파괴 기술, 드론의 추락으로 인한 피해를 방지할 수 있게끔 독수리나 그물망 등을 이용한 포획 기술 등이 있다.

전파 교란 기술의 경우, 지상의 카메라를 통해 침입드론을 식별한 후 지향성 안테나로 표적 드론의 통신 상황에 대한 모니터링이 이루어지며, 분석된 다운 링크 신호를 방해하는 신호를 생성하는 과정으로 전파를 교란시키는 것으로, 미국특허 10,044,465(Adaptively disrupting unmanned aerial vehicles)가 대표적이다.

Adaptively disrupting unmanned aerial vehicles는 카메라를 이용하여 침입 또는 위협이 되는 드론을 감지하고, 카메라와 정렬된 지향성 안테나를 통해 대상 드론의 통신에 대한 모니터링을 통해 착륙, 비행, 발사, 복귀 등을 지시할 수 있다. 이때 제어 회로는 드론의 다운 링크 신호를 감지, 분석하여 방해 신호를 생성함으로써 전파를 교란시키게 된다.

그물망을 이용해 드론을 포획하는 무력화 기술의 대표적인 사례로는 미국등록특허 10,495,421(Aurora Flight Sciences coporation)을 들 수 있다. 해당 특허 기술은 침입 드론에 대한 탐지를 통해 위험요인이 인지되면 단일 또는 다수의 방어용 드론이 네트를 전개해 침입 드론을 포획하는 기술로 지상의 단말기를 통해 인터셉트 드론에 대한 제어가 이루어진다.

Aurora Flight Sciences coporation은 공중 방어 시스템에 관한 것으로, 복수의 방어 드론과 드론 운용 시

스템, 타겟팅 시스템 및 복수의 방어 드론과 개별적으로 통신하는 컨트롤러, 휴먼 머신 인터페이스(HMI) 등을 포함하며, 탐지된 위협에 대한 타격 및 교전을 위한 표적 무력화 장치로 활용될 수 있다. 해당 무력화 기술은 지상에서 투사체를 발사한 후 침입 드론 근방에서 투사체가 그물을 전개하여 포획하는 것으로, 낙하산을 이용해 손상 없이 포획 드론의 획득이 가능하다는 이점이 있다.

현재 운용되고 있는 안티드론 시스템에서 무력화 수단으로 주로 활용되는 장비로는 RC(Radio Control) 대역과 GNSS(Global Navigation Satellite System) 대역의 재머가 있다. 드론 기술 발전에 따라 조종자가 드론 조종에 개입하지 않거나 GNSS 신호를 수신하지 않고도 목적지까지 드론을 운행하는 기술이 등장하고 있다. 이는 재머를 활용해 드론을 무력화하는 것이 드론 위험요인에 대한 확고한 대응 방식이 될 수 없음을 시사한다. 드론 포획 기술의 경우, 그물망의 사용 가능 거리가 비교적 짧은 데다가 군집비행하는 드론에 대한 대응이 어렵기 때문에 그 대안으로 요격기술이 고려되고 있는 실정이다.

현재의 안티드론 체계는 주로 전천후 활용이 가능한 레이더를 기반으로 하는 영상 센서나 RF 탐지 센서 등의 보조 수단을 적용하고 있다. 그러나 레이더 장비나 야간 탐지에서 효과적으로 탐지 영상을 얻을 수 있는 열상 장비의 경우 민간 영역에서 접근하기 어려운 높은 가격대를 형성하고 있기 때문에 장비 가격을 낮추고 탐지 성능 요건을 완화하는 방향으로 기술 개발이 진행될 필요가 있다.

다만, 현재 연구되고 있는 다양한 드론 무력화 기술과 관련 기술에 대해 출원된 특허의 경우, 각 기술별로 장점과 단점을 가지고 있음을 고려하여 안티드론 대응 체계를 구축할 때 보호 대상물의 환경적 특성을 반영하여 가장 최적화된 드론 무력화 기술을 적용해야 할 것이다.

포획 관련 안티드론 기술의 경우, 침입 드론 발견 시 파괴의 최소화를 통해 직접적인 포획이 가능하다는 장점이 있지만, 날씨 등의 환경적 요인의 영향에 따라 정확도가 감소할 수 있고 다수의 군집드론 침입 시 대응능력이 떨어진다는 단점이 있다.

전파 교란을 통한 안티드론 기술의 경우에는 침입 드론에 대한 신속한 제압과 군집드론 침입 시의 대응에 용이하다는 장점이 있지만, 재밍 신호가 상대적으로 강력하게 작용할 때 주변 전자통신기기에 영향을 미칠 수 있고, GPS 신호를 사용하지 않는 드론이나 조종신호 없이 미리 입력된 경로에 따라 비행하는 드론에 대한 무력화가 어렵다는 단점이 있다.

침입 드론 식별 후 이를 직접적으로 파괴하는 안티드론 기술의 경우에는 위험요인의 정확한 제거는 가능하지만, 주변에 2차 피해를 유발할 수 있다는 점에서 사용 환경의 제약성이 단점으로 작용한다.

## 2.4 드론 위험 대응 방안

### 2.4.1 각국의 안티드론 활용 사례

안티드론 기술의 효율적인 활용을 위해서는 별도의 주파수 할당이 요구되며, 드론 무력화 시 발생할 수 있는 추락에 의한 2차 피해에 대한 보상체계의 마련, 비행금지구역에서의 드론 비행 시 처벌 조항 등의 제도적 장치의 구축이 필요하다. 특히 안티드론을 통한 드론 위험 대응 방안을 적용하려면 사적 활용도보다 공적 활용도가 높은 드론의 특성상, 주파수 할당, 드론 전자파에 대한 인체 보호 기준, 드론 요격 기준 등의 체계가 수립되어야 한다. 따라서 안티드론 대응 체계 구축에 있어서 드론 사건 및 사고 처리에 관한 법률, 드론 위험요인이 발생할 때 즉각적인 대응이 가능하도록 제도적 차원의 체계를 마련해야 한다.

그러나 우리나라는 드론 기술과 관련하여 세계적인 기술력을 보유 중이지만, 핵심적인 기술이 되는 항법이나 엔진 기술, 통신 등의 영역에서는 선진국에 비해 취약한 것이 사실이며, 드론 위험요인에 충분히 대응할 수 있는 제도적 장치가 취약하다. 특히 앞으로 상업용 드론이 더욱 활성화된다는 전망이 나오는 가운데, 하드웨어 및 소프트웨어 관련 기술 개발을 위한 인적 자원이나 투자금 등의 지원이 요구되지만, 개발 기반이 취약하다는 지적도 나오고 있다[10].

이러한 측면에서 외국의 안티드론 활용 사례를 살펴보는 것은 향후 우리나라의 안티드론 체계 도입을 위한 기반 마련을 위한 실마리가 될 수 있을 것이다.

미국은 2019년도에 국방성이 약 1조 원대 규모의 안티드론 시스템을 구입한 바 있으며, 기존의 레이더 기반 방공시스템이 소형화되는 드론에 충분히 대응하지 못한다는 한계를 극복하기 위해 전자추적시스템과 카메라 등으로 소형 드론에 대한 추적 및 제압이 이루어지고 있다. 또한, 미국은 안티드론 관련 특허기술이 가장 많이 출원되어 있는 국가로, 3D 레이더 기술과 AI 기술을 활용해 3km 반경의 사각지대까지 탐지가 가능한 pyglass, 질화갈륨 증폭기로 향상된 성능의 High Power Microwave (HPM)를 발사해 군집 드론을 무력화하는 Leonidas 등의 안티드론 시스템이 활용되고 있다[11].

영국의 경우 18년 12월에 발생한 개트윅 공항 드론 출몰 사건과 19년 1월에 발생한 히드로 공항의 드론 출몰 등 드론에 의한 항공기 운항 마비 사태를 겪으면서 안티드론 시스템 구축이 활발해졌다. 영국은 군사적 목적으로 이스라엘 기업 라페일이 개발한 드론 돔(Drone Dome)의 탐지 기술을 운용하는 한편, 영국 기업인 오픈 웍스가 개발한 드론 포획 장치 SkyWall 100 그물건(Gun)을 도입한 바 있다.

프랑스에서는 ISIS와의 전쟁에 대비하기 위한 목적으로 별도의 지대공 방어대대를 통한 안티드론 훈련이 실시되었고, 소총형 재머 등을 이용해 드론에 대한 직접적인 물리적 타격 체제를 구축하였으며, 드론 추락 피해 방지 효과가 있는 독수리를 활용한 안티드론 시스템이 구비되어 있다.

일본은 2015년도에 발생한 총리 관저 드론 테러 사건을 계기로 드론전문부대인 무인항공기대처부대(IDT)를 창설하였으며, IDT를 통해 국가중요시설 및 비행금지구역 등에 대한 드론 위험 요인 대응 체계를 구축하고 있다. 특히, 해당 구역 내에 불법 드론 접근이 탐지되면 헬기 긴급 출동을 통한 경고 방송, 경고에 응하지 않을 시 요격 드론이 출동하여 그물을 통한 드론 무력화 방식을 운용 중이다[12]. 당시 발생했던 총리 관저 테러는 이듬해인 2016년 4월에 「소형 무인기 등 비행 금지법」의 시행으로 이어졌고, 일본 내각은 2019년 3월에 방위관계 시설의 추가 및 대상 시설 추가 지정을 위해 「중요시설 주변지역 상공에서 소형무인기 등의 비행 금지에 관한 법률」 개정안을 통과시키며 날로 늘어나는 드론 위험 요인에 대한 대응 체계를 구축하였다.

이처럼 드론 관련 사고 발생을 계기로 안티드론 시스템을 구축하는 해외 국가의 사례들은, 사고 발생 후 대응 체계 구축이라는 유사성을 가지고 있다. 향후 드론 관련 기술 발전에 따라 드론의 활용도가 확대되고, 드론 시장의 확장에 따라 증가할 것으로 예상되는 드론 위험 요인에 의한 사고 발생 가능성을 원천 봉쇄하고, 드론 위험요인에 따른 문제 발생 시 피해를 최소화할 수 있는 대응 체계의 선제적 마련의 필요성을 보여준다.

### 2.4.2 안티드론 대응 체계 개선 방안

앞서 살펴본 바와 같이 첨단기술 발전에 힘입어 드론 기술 역시 발전하면서 드론 산업이 활성화됨에 따른 위험요인에 대비하기 위한 기술 개발 연구가 활발하게 진행되고, 이를 실제 안티드론 대응 체계 구축에 적용하는 국가들도 늘어나고 있다.

이러한 기술의 실질적인 적용을 위해서는 먼저 드론 위험요인에 대한 정확한 파악이 요구되며 보호 대상물의 환경적 특성을 고려한 안티드론 체제의 방향을 설정할 수 있어야 할 것이다. 또한 안티드론 체제의 실질적 적용을 위한 제도적 정비 역시 수반되어야 한다.

안티드론은 탐지->식별->무력화의 3단계를 통해 대응 체계가 적용된다. 이러한 대응 체계가 제대로 작동될 수 있으려면 탐지 및 식별 단계에서 드론 위치정보 오차에 따른 재밍 성공률을 높일 필요가 있다. 드론을 통해 수신된 항적정보 예측 수치와 항적정보 실제 수치 간 오차를 감소시킬 수 있는 광학장비의 기술적 향상이 요구되는 것이다. 더불어 드론이 피아식별장치를 포함하지 않는다는 점에서 레이더 탐지 정보의 정밀도를 보장할 수 있도록 협역, 중역, 광역의 방호망을 설정한 후, 근거리 및 원거리에서의 직·간접적 위협에 대한 효과적인 대응 체계를 설정해야 할 것이다.

다음으로 무력화 단계에서는 물리적 파괴가 유발할 수 있는 2차 피해를 대비할 수 있도록 보호 대상 시설물 또는 대상자의 위치와 안티드론의 설치 위치, 안티드론의 탐지 가능 거리, 이동성, 대응 거리 등을 기준으로 삼을 때 면밀한 검토가 요구된다. 전파교란을 통해 드론 무력화를 시도할 때, 잡음 재밍 시의 계획경로 복귀 가능성을 고려하여 기만 재밍을 통해 침투 드론의 경로 이탈을 유도하여 안전한 지형지물에 충돌 또는 추락시킬 수 있도록 대응책을 구축해야 한다는 것이다.

마지막으로 안티드론 대응 체계가 제대로 작동할 수 있는지를 검토하고, 검토 결과를 토대로 실질적인 방어 체계를 구축할 수 있어야 한다. 이를 위해 안티드론 대응 체계와 관련한 법제의 정비가 수반되어야 할 것이다. 무엇보다 안티드론 대응 체계 구축에 있어서 우리나라의 경우 드론에 대한 광범위한 규제 속에서 드론으로 인한 피해 발생 시 실질적으로 형사 처벌까지 이어지지 못하고 있는 까닭에 드론을 통한 범죄 및 테러 발생 시 효과적인 대응이 어려운 실정이다. 특히, 드론의 다양한 위험요인에 대한 물리적 대응은 한계를 갖기 때문에 기술적인 부분에 대한 고려와 함께 법적, 제도적 차원에서의 대응도 고려될 필요가 있다.

드론과 안티드론 시스템 전반에 대한 실증분석과 함께 운영규칙을 보완하고, 안티드론 대응 체계를 운용할 수 있는 전문 운영 인력의 확보를 위한 교육과 양성 전략이 실행될 수 있어야 할 것이다.

## 3. 결론

본 연구는 최근 드론의 지능화 및 군집화 기술 활성화에 따라 새롭게 제기되고 있는 드론의 위협요인을 해소하기 위해 등장한 안티드론 대응 방안의 구축을 목적으로 드론 기술 현황과 이에 따른 위험 요인을 살펴보았다.

첨단기술과 드론의 결합은 드론 산업의 확장을 가져온 반면, 드론을 이용한 불법행위가 증가하고, 불법행위의 강도가 강해지면서 물리적 영역에서의 드론 위협이 확대되는 결과로 이어졌다. 드론의 위험요인에는 드론 구조상의 결함이나 조종사의 운영상 과실로 인한 사고, 해킹 및 시스템바이러스를 이용한 위협, 추락피해, 테러 등이 있다. 무엇보다 고성능 드론의 등장과 초소형 드론의 상용화 등은 다양한 영역에서 드론이 악용될 수 있다는 우려를 낳고 있다.

실제로 많은 국가들이 드론 관련 사고 발생을 계기로 안티드론 시스템을 구축하고 있으며, 앞으로 드론 관련 기술 발전에 따라 드론의 활용도가 점진적으로 확대될 것으로 예상되는 만큼 우리나라에서도 드론 위험요인에 대한 실효성 있는 대응 체계의 구축이 요구된다.

효과적인 안티드론 대응 체계의 구축을 위해서는 기존 안티드론 기술의 단점을 개선할 수 있는 기술적 요인과 물리적 대응의 한계를 극복할 수 있는 제도적 요인의 정비가 필요하다. 탐지 효과를 높일 수 있는 광학장비, 레이더 탐지 장비의 기술적 성능 개선이 필요하며, 전파교란 및 무력화 과정에서 발생할 수 있는 2차 피해 예방을 위한 지침 마련, 드론의 다양한 위험 요인에 대처할 수 있는 제도적 장치 구축 등이 필요하다고 할 수 있다.

현재 활발하게 연구가 진행되고 있는 드론 무력화 기술의 실질적인 적용을 위해서는 드론 위험요인에 대한 정확한 파악이 전제되어야 하며, 보호 대상자나 시설물의 환경적 특성을 고려한 안티드론 대응 체계의 방향 설정이 필요하다. 또한, 안티드론 기술이 가지고 있는 각각의 단점을 보완하면서, 불법드론 및 침입드론에 대한 신속한 탐지와 식별을 통한 선제적 대응이 이루어질 수 있도록 탐지와 식별 관련 기술 개발이 활성화될 필요가 있다.

## References


[1] Q. Kang, A Study on the Social Cost-benefit Analysis of Public Drones- Focused on the Search and Rescue Drones. Korean terrorism studies Review, 11(4), 90-107, 2018.

[2] B. D. Jin & Y. T. Jeon, A Study on the Practical Use of Civil Drones in the World. Korea Drone Studies, 1(1), 83-113, 2018.

[3] Teal-group, "Teal Group Predicts Worldwide Civil Drone Production Will More than Triple Overthe Next Decade Despite Pandemic.". 2020.10.06.

[4] Y. H. Kim, Y. S. Song & H. S. Shim, A counterattack by a drone. Defense & Technology, 470, 142-151, 2018.

[5] G. J. Yun, Current Status and Revitalization of Domestic and Foreign Drone Industries. REAL ESTATE FOCUS, 95, 4-14, 2016.

[6] C. H. Joe, S. J. Park, I. S. Um & H. N. Kim, Exploring Trends and Technologies in Drone Development. Communications of the Korean Institute of Information Scientists and Engineer, 37(1), 10-19, 2019.

[7] D. H. Lee & W. Kang, A Study on the Establishment of Anti-Drone Concept and Effective Response System. Korean security journal, 60, 9-31, 2019.

[8] J. Y. Jung & Y. T. Jeon, A study on the trend of anti-drone technologies and their applications. Special issue of drones, 35-55, 2017.

[9] S. H. Choi, J. S. Chae, J. H. Cha & J. Y. Ahn, Recent R&D Trends of Anti-Drone Technologies. ETRT, 33(3), 78-88, 2018.

[10] Y. C. Choi & H. S. Ahn, Current technology development trends and prospects for drones. The Korean Institute of Electrical Engineers, 64(12), 20-25, 2015.

[11] J. C. Choi & S. H. Lim, Anti-drone. KISTP, 2021-10, 1-36, 2021.

[12] O. H. Choi, A Study on the Application of Drone and the Anti-drone System in the National Assembly. A Ph.D. thesis at Kyunggi University Graduate School, 2020.



심 준 형(Jun-Hyung Sim) [정회원]

• 2019년 9월 ~ 현재 : 명지대학교 명지대학원 보안경영공학과 (석·박사통합과정)

〈관심분야〉
드론, 드론방어체계, 드론보안

황 의 천(Eu-Cheon Hwang) [정회원]

• 2020년 3월 ~ 현재 : 명지대학교 명지대학원 보안경영공학과 (석·박사통합과정)

〈관심분야〉
드론, 드론방어체계, 드론보안, UAM, CCTV

손 창 근(Chang-Gun Son) [정회원]

• 1999년 8월 : 건국대학교 기업경영학과 (국제통상석사)
• 2020년 8월 : 명지대학교 보안경영공학과 (공학박사)
• 2022년 3월 ~ 현재 : 명지대학교 산업대학원 객원교수

〈관심분야〉
정보보호, 정보통신, 보안암호

류 연 승(Yeon-Seung Ryu) [정회원]

• 1990년 2월 : 서울대학교 계산통계학과 (학사)
• 1992년 2월 : 서울대학교 전산과학과 (석사)
• 1996년 8월 : 서울대학교 전산과학과 (박사)
• 2015년 3월 ~ 현재 : 명지대학교 보안경영공학과 주임교수
• 2017년 1월 ~ 현재 : 방산기술보호 연구회 위원장

〈관심분야〉
시스템 보안, 무기체계 보안, 방산기술 보호