테러 및 전쟁용 드론에 대한 안티드론 및 보안대책 수립필요성에 대한 연구

진종구(대진대 석좌교수) · 남은미(MG 새마을금고) · 김유진(포천가족성상담센터)

국문요약

최근 드론 기술 발전으로 인해 테러 및 전쟁 목적으로 드론 활용이 증가하고 있어 심각한 안보 위협이 되고 있다. 본 논문에서는 테러 및 전쟁용 드론에 대한 안티드론 및 보안 대책 수립을 위한 필요성을 조사하고 분석하며, 효과적인 대응 방안을 제시하고자 한다. 테러 및 전쟁용 드론은 테러공격, 군사적 공격, 민간시설 공격, 사생활 침해 등을 자행할 수 있다. 이에 대한 안티드론 및 보안대책으로 탐지 및 추적, 무력화, 포획, 규제 및 법적 조치 강구가 있을 수 있겠다. 테러 및 전쟁용 드론에 대한 안티드론 및 보안대책은 지속적인 연구와 개발이 필요하다. 드론 기술 발전에 발맞춰 새로운 위협과 대응방안을 연구하고 효과적인 안티드론 시스템 구축을 위한 국제적 협력이 필요한 시점이다.

주제어: 드론, 안티드론, 드론보안대책, 무인비행기, 드론전쟁, 테러, 전쟁

I. 서론

최근 이스라엘-하마스 전쟁과 러시아-우크라이나 전쟁에서 군사용 드론을 이용한 정찰 및 공격이 빈번하게 발생하고 있다. 이에 따라 상대국 드론을 해킹하여 탈취하거나 통제 불가능한 상태로 만드는 등의 다양한 작전이 전개되고 있으며, 드론이 테러 수단으로 악용되는 사례도 증가하고 있다. 이러한 상황은 드론의 중요성을 높이는 동시에 드론 테러 및 공격에 대한 대응 필요성을 부각시키고 있다.

과거에는 조종사가 탑승한 유인 항공기가 적을 공격하는 것이 일반적이었으나, 최근에는 무인 항공 기술의 발달로 무인항공기(UAV)가 무기와 미사일을 탑재하여 적이나 적의 시설물을 타격하는 방식이 빈번히 사용되고 있다. 실제로 세계 각지에서 드론을 테러나 전쟁에 활용하는 사례가 많아지고 있으며, 북한의 위협에 직면한 우리나라 역시 북한의 드론 위협에서 자유로울 수 없는 현실이다.

2014년 백령도와 파주에서 발견된 북한의 드론에는 청와대와 해병대 6여단 시설 배치를 집중적으로 촬영한 사진이 있었으며, 2017년 강원도에서 발견된 드론에는 주한미군의 군사시설인 성주 사드 기지가 촬영되어 있었다. 2022년 12월 26일 오전 10시 25분경에는 북한 소형 무인기 5대가 경기 김포 일대 군사분계선(MDL)을 넘어 영공을 침범하였고, 이 중 1대는 서울 은평구 등 서울 북부 상공까지 침투했으며, 나머지 4대는 인천 강화도와 경기 파주, 김포 일대를 오후 3시 30분까지 비행했다.

이러한 드론의 불법 비행은 드론 테러, 즉 드론 공격의 가능성을 충분히 예측할 수 있게 한다. 국가정보원(NIS)은 2023년 3월 17일 발표한 '2022년 테러 정세와 2023년 전망' 보고서를 통해, 북한이 도발적 군사행위로 무인기와 드론을 이용해 정보 획득과 테러 위협을 계속할 것이며, 무인기를 활용한 주요 시설 파괴와 같은 다양한 공격을 실행할 가능성이 있다고 전망했다. 이는 드론을 활용한 공격 가능성이 상존하고 있음을 의미하며, 이에 대한 보안대책(안티드론)의 필요성을 지적한 것으로 볼 수 있다.

러시아-우크라이나 전쟁과 이스라엘-하마스 전쟁에서 드러나듯 현대전의 진화로 인해 전투 방식이 크게 변화하면서 무인기와 다목적 비행 물체의 공격은 기존의 군수 장비와 무기들의 상당수를 무력화시키고 있는 실정이다. 이러한 관점에서 볼 때, 앞으로 드론의 군사적 활용 가능성이 더욱 높아질 것이며, 드론을 효과적으로 활용하기 위한 보안대책 및 안티드론 기술의 발전도 극대화될 것으로 보인다.

Ⅱ. 드론에 대한 이론적 배경

1. 드론 용어 개념 및 드론의 발전

Drone은 벌 같은 곤충이 날갯짓으로 내는 웅웅거리는 소리나 악기가 배경음으로 내는 저음을 일컫는다. 그러므로 낮은 웅웅 소리를 내는 대부분의 무인기를 드론이라고 규정해도 무방할 것이다.

드론활용의 촉진 및 기반조성에 관한 법률(약칭, 드론법) 제2조(정의)에 의하면, 드론이란 조종자가 탑승하지 아니한 상태로 항행할 수 있는 비행체를 말한다. 또한 항공법 제2조 제3호 및 제6호의 초경량비행장치[1], 무인항공기[2]를 포함하며, 그 밖에 원격・자동・자율 등 국토교통부령으로 정하는 방식에 따라 항행하는 비행체를 일컫는다. 다시 말하자면, 사람이 탑승하지 않고 항공역학을 이용해 기체의 양력을 얻고 자율 비행과 원격조정이 가능한 모든 종류의 무인기(UAV, Unmaned Aerial Vehicle)를 드론이라고 할 수 있다.[3]

드론은 비행구조에 따라 고정익과 회전익으로 구분할 수 있다. 고정익 드론은 일반 항공기처럼 날개가 고정되어 있는 반면, 회전익 드론은 로터를 갖고 있다. 멀티콥터(Multi Copter)는 여러 개의 로터를 가진 회전익 비행체로, 로터의 수에 따라 바이콥터(bi copter), 트라이콥터(tri copter), 쿼드콥터(quad copter) 등으로 불린다. 현재 민간용으로 가장 많이 사용되는 형태는 쿼드콥터다.

드론의 시초는 영국 왕립해군이 방공포병 사격훈련용 가상 적기로 개발한 'DH.82B Queen Bee' 로, 이 기체에 '여왕벌' 이라는 별명을 붙인 것이 드론이라는 용어의 유래다. 실전 군사작전용 드론의 시작은 미 해군이 1944년에 폭격기 B-17 및 PB4Y-1을 개조해 만든 '아프로디테(Aphrodite)' 였다. 이 드론은 조종사가 탑승하여 목표지점까지 접근한 후 낙하산으로 탈출하고, 기체는 목표물에 충돌하도록 설계되었다. 그러나 당시 기술력의 한계로 인해 목표지점을

1) 초경량비행장치란 항공기와 경량항공기 외에 공기의 반작용으로 뜰 수 있는 장치로서 자체중량, 좌석 수 등 국토교통부령으로 정하는 기준에 해당하는 동력비행장치, 행글라이더, 패러글라이더, 기구류 및 무인비행장치 등을 말한다.(항공안전법 제2조 제3호)

2) 사람이 탑승하지 아니하고 원격조종 등의 방법으로 비행하는 무인항공기의 경우에는 …중략… (항공안전법 제2조 제6호)

3) 진종구, 러시아－우크라 전쟁 및 이스라엘－하마스 전쟁에 자폭드론 등 드론을 활용한 군사전략 성행, https://marquis-jin.tistory.com/151(검색일: 2024.01.19.)

[그림 1] 고정익(左) 및 회전익(右) 드론의 외형적 모습

정확히 타격하지 못하여 계획이 취소되었다.

1960년대에 들어서면서 베트남 전쟁 중 정글 내 적의 동향 파악이 필요했던 미 공군은 스텔스 항공기 프로젝트를 진행하던 중 무인정찰기를 개조하여 AQM-34 Ryan FireBee라는 드론을 개발했다. 이 드론은 착륙 장비가 없어 공중에 떠 있던 수송기에서 발사하여 정찰 임무를 수행한 후, 낙하산으로 회수하는 방식이었다. 이후, 지상에서 발사와 회수가 용이한 무인기로 업그레이드되어 미국뿐만 아니라 캐나다, 일본, 터키 등에서도 전력화되었으며, 2000년대 초반 대테러 전쟁에서도 활용되었다.

드론은 민간용으로도 많이 사용되지만, 전쟁을 통해 크게 발전했다. 미국 주도의 드론 개발 이후, 이스라엘은 수적 열세를 극복하고 주변 아랍 국가들에 대한 정보 수집 능력을 강화하기 위해 드론을 개발하여 24시간 영공을 정찰하는 국가로 자리잡게 된다. 특히 9.11 테러 이후 드론은 테러와의 전쟁에 투입되면서 급속도로 발전하게 되었다.

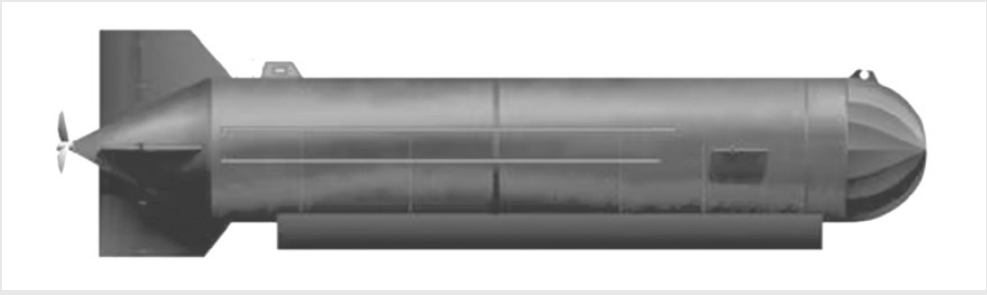
우리나라에서는 대우중공업과 대한항공이 처음 드론 개발을 시작하였으며, 이후 한국항공우주산업(KAI)이 송골매(RQ-101) 무인정찰기를 개발하여 사용하고 있다. 현재는 중고도 무인항공기(MUAV)와 고고도 무인항공기(HUAV)가 휴전선 인근에서 정찰 활동을 벌이고 있다. 우리 군은 군단, 사단, 대대급까지 전력화한 무인항공기(UAV)를 이용하여 군사분계선 인근 상공에서 작전을 수행하는 능력을 완비하기 위해 지속적으로 보완작업을 추진 중이며, 차기 UAV 사업도 활발히 진행하고 있습니다. 민간용으로는 농촌진흥청 주도의 농업용 무인헬기 개발을 시작으로 민간이 주도하는 드론 시장이 활성화되었다.

결론적으로, 드론은 훈련용 표적기에서 자폭용, 정찰용 드론을 거쳐 무기를 탑재한 공격용 드론으로 발전해 왔다. 무인항공기, 즉 드론의 기술 발전은 처음에는 군 주도로 이루어졌으나,

현재는 다양한 분야에서 서로 정보를 공유하며 발전하고 있다. 따라서 무인항공기만을 드론으로 정의하는 데는 다소 문제가 있을 수 있다. 지상, 수상, 수중에서 무인체계로 운영되는 각종 기기들도 드론의 범주에 포함시켜야 하는지에 대한 논의가 필요한 실정이다.

우크라이나는 해군 드론여단을 창설한 뒤, 2023년 8월 27일에는 해상 드론과 더불어 수중에서 활용 가능한 마리치카(Marichka, 작전 범위 1000km, 길이 6m, 폭 1m) 수중 드론을 개발하고 공개했다. 이 수중 드론은 군함, 보트, 잠수함, 해안 요새, 교량 지지대를 공격하도록 설계되었으며, 폭발물 대신 군용이나 민간용 화물을 수송하고 정찰 기능도 수행할 수 있다. 마리치카는 러시아 흑해 함대 자산뿐만 아니라 러시아의 주요 인프라와 시설을 목표로 한 작전에 활용되고 있는 실정이다. 이러한 수중 드론도 드론의 범주에 포함시켜야 할 것으로 판단된다.

[그림 2] 우크라이나의 마리치카 수중드론



2. 군사적 목적의 드론 개발

최근 인공지능(AI, Artificial Intelligence) 기술의 발달로 드론에 AI가 활용되면서 신종 무기체계인 슬로터봇(Slaughterbot, 살상로봇)이 개발되었다. 슬로터봇은 AI를 활용한 안면인식기술을 탑재하여 특정한 인물에 대해 폭탄 등을 살포하는 방법으로 살해할 수 있는 것으로 나타났다. 무게가 불과 30g인 슬로터봇은 요인들이 있는 장소에 날아가 특정 인사의 안면이나 복장을 인식해 이마에 내려앉은 뒤 곧바로 3g의 폭약을 터트려 인간의 두개골을 뚫어 치명상을 입히는 소형 자폭드론이다.[4)]

이렇듯 다양한 드론이 군사적 목적으로 개발되고 있으며, 이제 드론은 무인 항공기뿐만 아니

라 무인 작동 로봇까지 포함하는 범위로 확장되고 있다. 우리 육군은 무인 비행기와 무인 로봇에 AI 기술을 융합한 드론봇(DroneBot) 전투체계를 확립하여 미래의 전쟁 환경에 대비하고 있다.

또한, 우리 군은 500MD 헬기를 무인화 하여 KUS-VH로 재탄생시키는 등 기존의 유인 항공기를 무인화 함으로써 기존 전투 장비의 전투력을 유지하면서 인력의 안전을 보장하는 방안을 채택했다. 이러한 개발은 국방 예산을 절감하고 인력 부족 문제를 해결하는 데 효과적이었으며, 인간의 역할을 일정 부분 인공지능(AI)으로 대체하는 결과를 가져왔다. 그러나 인간의 창의성과 유연성이 요구되는 많은 영역은 AI로 대체할 수 없다는 점을 고려할 때, 드론은 향후 유·무인 복합체제인 하이브리드 전투체계에서 중요한 역할을 할 것으로 평가된다.

3. 전쟁 중 급속도로 발전한 FPV 드론

FPV(First Person View, 1인칭 시점) 드론은 원래 첨단 무선통신 및 원격제어 기술을 바탕으로 차세대 레이싱 스포츠를 목적으로 개발되었다. 그러나 전쟁 중 그 활용 방식이 급속도로 발전했다. 우크라이나는 러시아의 침공 초기, 바이락타르(Bayraktar) TB-2와 같은 군용 전술 드론을 사용하여 공대지 공격 임무를 수행했다. 그러나 러시아군의 전자전 능력 향상과 방공 무기 재배치로 인해 바이락타르 TB-2의 효용성이 감소하자, 우크라이나는 저렴한 가격과 초정밀 공격 능력을 갖춘 소형 드론인 FPV 드론을 새로운 방식으로 활용하게 되었다. FPV 드론에 수류탄과 급조폭발물(IED, Improvised Explosive Device)을 장착하여 러시아군을 공격하는 자폭 드론으로 사용한 것이다. 이로 인해 FPV 드론은 우크라이나군에 의해 최첨단 유도무기 못지않은 효과를 발휘하게 되었으며, 이제는 표준화된 운용 절차와 체계화된 교전수칙까지 마련될 정도로 발전했다.

FPV 드론의 활용은 소형 드론의 잠재력을 극대화하며, 전장에서의 전술적 유연성을 크게 향상시켰다. 이러한 드론은 실시간 영상 전송과 정밀한 원격제어를 통해 목표물을 정확하게 타격할 수 있는 능력을 제공하며, 이는 군사전략의 변화와 새로운 전술 개발에 중요한 역할을 하고 있다. 또한, FPV 드론은 민간 기술의 군사적 적용이라는 사례를 보여주며, 미래 전투에서 드

4) 김민석, 2021, 김정은 30그램짜리 초소형 자폭드론 겁낼까, 중앙일보, https://www.joongang.co.kr/article/25020839 (검색일: 2024.01.22.)

론 기술의 중요성을 더욱 부각시키고 있다. 이처럼, FPV 드론은 단순한 레이싱 도구에서 벗어나, 현대 전장에서 중요한 자산으로 자리 잡게 되었다. 전자전과 같은 고도의 군사 기술이 발달함에 따라, FPV 드론의 역할과 활용 방법도 끊임없이 진화하고 있다.

4. 테러 및 전쟁 수단으로의 드론 사용

1) 테러 및 전쟁의 정의

미국과 유럽에서는 테러의 개념과 행위가 폭넓게 규정되어 있다. 일반적으로 미국에서는 폭탄이나 독극물을 이용하여 대중을 위협하거나 대중의 공포를 유발할 의도로 타인을 위협하는 행위 등을 테러로 규정한다. 영국의 對테러법은 정치 · 종교 · 이념적 대의를 추구하는 목적을 지닌 테러 외에도 정부에 영향을 미치거나 공중 또는 공중의 일부에 대한 협박도 테러로 규정한다. 그러나 우리나라의 테러방지법은 '공중 협박의 목적'을 초과구성요건으로 규정하고 있어 목적범(目的犯)이라는 점을 입증해내지 못하면 테러에 포함되지 않는다. 또한 테러단체에 대한 정의도 '테러단체란 유엔(UN)이 지정한 테러단체를 말한다'고 규정되어 있어 테러에 대한 정의가 너무 협소하다고 할 수 있다.[5]

드론은 운용 주체에 따라 군용과 민수용으로 구분되며, 그 중 90% 이상의 드론이 군사용으로 활용되고 있다. 테러 수단으로 드론을 사용하는 경우는 전쟁 전 단계에서도 적용되며, 전쟁 중에도 군사용 드론이 테러 용도로 사용될 가능성이 높다. 전쟁은 국가 또는 정치 집단 간에 무력을 사용하는 폭력 상태 또는 행위를 의미한다. 일반적으로 두 국가 이상 간의 싸움을 의미하지만, 내전과 같은 국가 내부의 무력 충돌도 교전단체 간의 전투일 경우 전쟁에 포함될 수 있다. 전쟁의 목적은 다양하지만, 대표적으로 영토 확장, 자원 확보, 정치적 목적 달성, 자국 방어 등이 있다. 일반적으로 전쟁은 다음과 같은 특징을 지닌다.

첫째 전쟁은 개인 간의 폭력과 달리, 특정한 정치적 목적을 달성하기 위해 대규모 자원과 인원을 투입하여 국가 또는 정치 집단이 조직적으로 폭력을 행사하는 행위이다.

둘째, 전쟁은 인류 역사에 오랜 시간 동안 존재해 왔으며, 앞으로도 완전히 사라질 가능성은 없다고 보는 것이 타당할 정도의 역사적 지속성을 지녔다.

셋째 전쟁의 목적은 영토 확장, 자원 확보, 정치적 목표 달성, 자국 방어 등 다양한 목적을 가

5) 테러방지법 제2조 2호

진다.

결론적으로, 드론은 운용 주체와 목적에 따라 테러와 전쟁 모두에서 중요한 역할을 하고 있다. 드론 기술의 발전과 함께 그 사용 범위는 계속해서 확장되고 있으며, 이는 현대 전쟁과 테러의 양상을 변화시키고 있다.

2) 전쟁에 드론을 동원한 전형적 사례

최근 무인기(드론)는 군사, 산업, 민간 분야에서 다양하게 활용되고 있으며, 그 중요성이 점점 더 커지고 있다. 본 논문에서는 전쟁 시 무인기 활용의 중요성을 구체적인 사례를 통해 살펴보고자 한다. 특히, 아프가니스탄 전쟁, 리비아 내전, 시리아 내전, 나고르노-카라바흐 전쟁, 예멘 내전 등 주요 사례들을 살펴보고, 각 사례별 무인기의 역할과 영향을 평가해 본다.

(가) 아프가니스탄 전쟁(2001년)

2001년 10월, 미군은 아프가니스탄 전쟁에서 처음으로 무인기 'MQ-1 프레데터'를 도입하여 알카에다 및 탈레반 지도자들을 감시 및 추적하였다. 프레데터 무인기는 장거리 정밀 타격이 가능한 헬파이어 미사일을 탑재하고 있었으며, 실시간 영상을 미 지휘센터로 전송했다. 11월에는 카불 근처 알카에다 고위 지도자를 공격하여 테러 조직에 대한 직접적인 군사적 압박을 가하기도 하였다. 이는 특정 개인을 목표로 한 최초의 무인기 공격으로, 무인기 기술의 군사적 활용 가능성을 보여주는 중요한 사건이었다.

(나) 리비아 내전(2011년)

2011년 리비아 내전 당시, NATO는 민간인 보호 및 리비아 정부군 공격 저지를 위해 유엔 안전보장이사회 결의 1973호에 따라 미국의 MQ-1 프레데터와 MQ-9 리퍼 무인기를 출격시켰다. 이들 무인기는 리비아 정부군 탱크, 무기고, 군사 차량 등을 공격하여 카다피 정부에 압박을 가했다. 이러한 무인기 지원은 2011년 10월 카다피 사망과 내전 종결에 기여한 것으로 평가되었다. 리비아 내전은 무인기가 대규모 군사 작전에서 중요한 역할을 수행할 수 있다는 것을 보여주는 대표적인 사례다.

(다) 시리아 내전(2016년)

2016년 시리아 내전에서 러시아는 시리아 정부군을 지원하기 위해 다양한 무기를 사용했는

데, 그 중 하나가 무인기였다. 러시아는 정보 수집, 감시, 정찰뿐만 아니라 공격용 무인기까지 운용했다. 주로 정찰 임무에 사용된 오르란-10(Orlan-10) 무인기는 전자전 장비 탑재 및 소규모 폭탄 운반을 통해 경량 공격에도 활용되었다. 또한, 이스라엘 서처(Searcher) 무인기를 기반으로 한 포르포스트(Forpost) 무인기는 감시 및 정찰 외에도 무기를 탑재하여 공격 임무에도 사용되었다. 러시아는 시리아 내전에서 무인기를 활용하여 반군 위치 추적, 정밀 타격, 전쟁 양상 변화에 중요한 역할을 했다.

(라) 나고르노-카라바흐 전쟁(2020년)

2020년 나고르노-카라바흐 전쟁에서 아제르바이잔은 이스라엘製 하르오프 자폭 드론, 오르비터 1K, 헤르메스 900, 튀르키예製 TB2 바이락타르 무인기를 활용하여 아르메니아 기갑 장비와 요새에 정밀 타격을 가했다. 이를 통해 44일 만에 일부 영토를 재탈환하고 전쟁을 승리로 이끌었다. 특히, TB2 바이락타르 무인기는 저렴한 가격과 높은 성능으로 주목을 받았으며, 현대 무인기 전쟁의 새로운 가능성을 보여주었다.

(마) 예멘 내전(2019년)

2019년 9월, 예멘 내전에서 승리한 후티 반군은 인근 사우디아라비아의 국경 도시와 주요 기반 시설을 무인기(드론)를 이용하여 수차 공격했다. 이는 예멘 내전이 국제적 차원으로 확대되고 있다는 것을 보여주는 사례이며, 특히 사우디아라비아와 이란 간의 대리전 양상을 띠게 되었다. 후티 반군의 對사우디아라비아 드론 공격은 세계 석유 공급의 약 5%를 일시적으로 중단시키는 결과를 초래했다. 이는 사우디아라비아 경제와 세계 에너지 시장에 큰 충격을 주었으며, 중동 지역의 긴장을 더욱 고조시켰다. 규모 면에서 볼 때, 이 사건은 사우디아라비아와 후티 반군 간의 전쟁이라기보다는 테러의 일환으로 드론 공격을 가했다고 볼 수 있다.

후티 반군의 드론 공격은 저비용 고효율적인 비대칭 전략의 일환으로, 사우디아라비아에 군사적 · 경제적 타격을 가하려는 의도를 드러냈다. 이는 무인기가 현대 전쟁에서 새로운 위협 요소가 될 수 있다는 것을 보여주는 중요한 사례이다.

3) 러시아-우크라 전쟁 및 이스라엘-하마스 전쟁에서의 비대칭 전력으로 드론 활용

드론은 최근 수년간 군사분쟁에서 핵심적인 역할을 담당해 왔으며, 특히 러시아-우크라이나 전쟁과 이스라엘-하마스 전쟁에서 그 중요성이 더욱 부각되고 있다.

러시아와 우크라이나 간의 충돌에서 양측은 탐색, 감시, 정찰(RISR) 목적으로 드론을 널리 사용하고 있다. 드론을 통해 양국은 적의 위치를 정확히 파악하고, 고정밀 타격을 수행하는 데 크게 활용하고 있다. 우크라이나는 소형 상업용 드론을 개조하여 폭탄을 투하하는 데 사용했으며, 러시아도 유사한 방식으로 드론을 활용하고 있다. 이 같은 기술은 전선의 동향을 파악하고, 적의 기갑장비 및 요새 방어를 무력화시키는 데 중요한 역할을 수행하였다.

이스라엘도 하마스와의 충돌에서 고도의 기술을 가진 드론을 사용하여 감시, 정찰, 타격 임무를 수행하고 있다. 개전 이후 하마스는 드론을 이용한 공격을 시도했으나, 이스라엘의 철저한 방공망에 의해 대부분 차단되었지만 이스라엘에 일부 피해를 가하기도 했다. 이스라엘은 전장 감시 및 실시간 정보 수집에 드론을 활용하여 전술적 우위를 확보했으며, 하마스의 로켓 발사대와 같은 중요 목표물을 정밀 타격하는 등 드론을 다목적으로 활용하고 있다.

한편, 2023년 10월 7일 하마스의 이스라엘 기습공격으로 시작된 이스라엘-하마스 전쟁 이후, 2024년 1월 29일에는 요르단 북부에 주둔 중인 미군기지 '타워 22'가 시리아와 이라크에서 활동하는 친이란 극단주의 민병대의 드론 공격을 받아 미군 3명이 사망하고 30여 명이 부상당하는 사태가 발생했다. 이는 가자 지구(Gaza Strip) 전쟁 이후 첫 미군 사망 사건으로, 드론이 철저한 방공망을 보유한 미군에게도 피해를 입힌 비대칭 전력으로서의 위력을 보여준 하나의 사례라고 할 수 있다. 이처럼 드론은 현대 전쟁에서 탐색, 정찰, 정밀 타격 등의 다양한 목적으로 사용되며, 전술적 우위를 확보하는 중요한 무기체계로 자리잡아 가고 있다.

4) 러시아의 비대칭 전력으로 드론을 활용한 대표적 사례

2022년 2월 24일, 러시아는 우크라이나의 비무장화, 비나치화, 그리고 돈바스 지역 주민 보호를 명분으로 우크라이나를 침공함으로써 러시아-우크라이나 전쟁을 일으켰다. 이 침공에 대응하여 미국을 비롯한 NATO 회원국들은 우크라이나에 많은 무기를 제공하였고, 이러한 지원은 우크라이나가 러시아의 공격에 효과적으로 대처할 수 있도록 하였다. 러시아는 이러한 서방의 군사 지원에 대응하여 여러 가지 전략을 사용했다. 특히, 대전차 작전에서 러시아는 전통적인 대전차 미사일뿐만 아니라 값싼 드론을 대거 활용하였다. 드론은 적의 탱크와 장갑차를 겨냥한 정밀 타격을 수행하는 데 사용되었으며, 이는 비용 대비 효율이 높은 방법으로 평가할 수 있다.

미국은 대당 1,000만 달러(약 137억 원)에 이르는 세계 최강 전차로 열화우라늄 복합장갑을 채택하는 등 뛰어난 방호력을 자랑하는 M1에이브럼스 탱크 31대를 우크라이나에 제공했으나,

러시아는 불과 2개월여 만에 고작 500달러(약 70만원)에 불과한 자폭드론을 이용, 5대나 파괴하였다. 미국의 M1에이브럼스 탱크와 더불어 독일의 레오파르트 전차 등도 우크라이나 전장에서 자폭드론에 의해 30여대가 파괴된 것으로 보도되었다. 전차 킬러라고 일컫는 'FPV(First Person View, 1인칭시점)' 드론에는 실시간 이미지를 컨트롤러로 다시 스트리밍 하는 카메라가 장착돼 있어 탱크의 가장 취약한 곳을 공격하도록 조종할 수 있다. 특히 러시아 탱크의 포탑 뒤쪽에는 통상 탄약고가 부착돼 있다. FPV를 이용하여 포탑 뒤쪽을 명중시키면 탄약에서 거대한 폭발이 일어나 탱크를 파괴시킨다. 특히 주간에 궤도가 손상된 탱크는 야간에 FPV드론의 손쉬운 공격대상이 된다. 일반적으로 전차가 지뢰 또는 대전차 미사일 등에 의해 손상을 입으면 전장에서 전차를 회수하거나 수리하게 되는데, FPV를 이용한 자폭공격이 일상화되면서 이러한 수리를 불가능하게 만들고 있는 추세다.[6]

현대 전쟁을 변화시키고 있는 드론 전투는 향후 전쟁에서 드론과 안티드론의 활용방법을 고민하게 만드는 요인 중 하나이다. 현 단계에서 FPV를 격파하는 가장 효과적인 수단은 방해전파 송출 등 전자전(電子戰)을 통한 드론 무력화 및 드론 탈취가 바람직하며, 저렴한 레이저 빔을 활용한 드론 파괴도 가능하다 할 것이다.

5. 현대전에서 드론의 중요성

현대전에서 드론의 중요성은 계속해서 높아지고 있는 실정이다. 드론은 저비용 고효율적인 무기로 활용될 수 있다는 점에서 매우 매력적이며, 특히 자국군의 인명피해를 최소화하는 것이 중요한 서구 사회에서는 무인기인 드론을 활용하는 것이 국민들의 지지를 얻기에 충분하다. 드론은 적의 위치와 활동을 파악하고 방어화된 요새를 발견하여 고도로 정밀하게 타격을 가할 수 있다. 또한, 저렴하게 제작하여 사용함으로써 전비를 줄일 수 있는 장점도 지니고 있다.

드론은 용도에 따라 다양한 유형으로 개발될 수 있으며, 특정한 임무에 적합하게 사용될 수 있다. 예를 들면, 드론은 테러 공격, 마약 밀매 단속, 국경 감시 등 다양한 목적으로 사용되고 있다. 드론은 저렴하고 사용하기 쉬우며, 정밀한 공격이 가능하다는 점에서 현대 전쟁의 중요한

6) New York Times, "Do Tanks Have a Place in 21st-Century Warfare?", 2024.04.20.
서울신문, '세계 최강 전차' M1 에이브럼스, 70만원짜리 드론에 당해…드론 피하려 그물 덮기도, 2024.04.22.
https://nownews.seoul.co.kr/news/newsView.php?id=20240422601007(검색일: 2024.04.27.)

무기로 자리 잡았으며, 앞으로도 더욱 다양한 방식으로 활용될 것으로 예상된다.

전쟁 무기로서의 드론 활용은 차치하고라도, 드론은 최근 새로운 테러 위협 수단으로 등장하고 있다. 자폭 드론 등을 활용한 테러는 테러범이 외부의 안전한 장소에서 원격 조종을 통해 테러 대상 목표물에 극대화된 타격을 달성하기 위한 최상의 수단으로 급부상하고 있다. 이러한 드론 테러는 감시와 방어를 더욱 어렵게 만들며, 테러범의 생존 가능성을 높이는 동시에 피해를 극대화할 수 있는 위험한 도구로 인식되고 있다.

이러한 드론의 다양한 활용과 그로 인한 변화는 앞으로도 군사 및 비군사 분야에서 지속적으로 확장될 것으로 보이며, 이에 대한 대응과 방어 전략도 함께 발전해야 할 것이다.

Ⅲ. 드론생태계의 보안 위협

드론이 제 성능을 발휘하려면 블루투스, GPS, 5G 등의 네트워크 통신을 통해서 무인비행체에 전달된 명령을 기반으로 원격 제어 · 조종을 통해 사전에 프로그램화된 경로 및 임무를 수행해야 한다. 이처럼 드론 생태계의 인프라 자체가 무선 네트워크를 기반으로 이뤄지기 때문에 무선 네트워크 특성 상 누구나 접할 수 있는 취약한 보안체계가 문제로 대두된다. 따라서 적이나 테러집단의 해킹에 의한 탈취 및 인적 · 물적자원에 대한 공격에 활용하기 위한 목표물로 전락할 가능성도 간과할 수 없는 실정이다.

실제 운용 중인 드론에서 발생할 가능성이 높은 보안위협은 첫째 지상제어 시스템, 정보제공 장치별 자산요소, 드론 자체에서 발생할 수 있으며, 둘째 보안위협요인은 드론을 이용한 테러, 범죄실행, 이로 인한 인명피해 등과 같은 드론을 활용한 직접적인 인적 · 물적 피해 등으로 나눠볼 수 있다. 드론 시스템의 자산환경에서 발생할 수 있는 보안 위협들이 다양하기 때문에 가상의 보안위협을 구성해 이에 대한 대처방안 마련이 필요하다. 무인 항공기의 가용성과 정교함의 급격한 증가는 악의적인 소형 무인 항공기가 제기하는 위협을 평가하고 완화하는 능력보다 더 빨리 발전하기 때문에 심각한 문제가 우려된다. 그러므로 세계의 다수 국가들이 무인항공기 공격으로부터 보호하기 위해 국토 안보에 투자하고 있는 실정이다.[7)]

7) 박설민, 2022, 급증하는 드론, 보안산업 새로운 먹거리 되나, 시사위크, https://www.sisaweek.com/news/articleView.html?idxno=154904(검색일: 2024.2.8.)

1. 자산요소별 보안위협

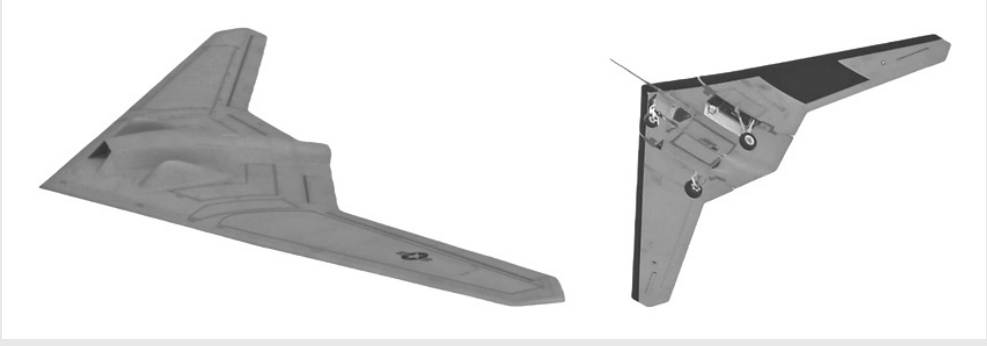
1) 드론에 대한 보안위협

드론의 자산요소별 보안위협을 살펴보자면 드론 환경에서는 GPS, 센서, 임베디드 시스템 등의 요소로 구성되어 있으며, 각 구성요소는 고유한 보안 취약성을 지니고 있다.

드론의 보안위협은 첫째로 GPS Spoofing[8]과 GPS Jamming[9]으로 나눌 수 있다. GPS 스푸핑(spoofing)은 드론에 가짜 데이터를 보내 드론이 해커가 의도한 곳으로 이동하거나 착륙하도록 만드는 것으로, 2011년 아프가니스탄 상공을 비행하며 정찰 업무를 수행하던 미군 소유 드론 'RQ-170' 이 이란에 의해 나포되는 사건이 대표적인 사례다. 미국 록히드마틴사와 이스라엘이 공동 제작한 무인 스텔스기 조종이 무작위로 이뤄져 이란 영토에추락한 것인데, 해커가 의도한 착륙지점을 의미하는 GPS 신호를 드론에 보내는 수법인 '스푸핑' 을 악용한 것으로 파악됐다.[10]

두 번째 보안 취약 요소로는 제어신호 전파방해를 통한 드론의 무력화다. 제어신호 전파방해는 드론 조종에 사용되는 무선 제어신호를 방해하여 드론을 제어할 수 없게 만드는 공격이다.

[그림 3] 이란에 나포된 것과 동종인 RQ-170 센티널



8) GPS Spoofing이란 지상에서 가짜 GPS신호를 발생시켜 드론에게 전송함으로써 기체가 자신의 위치를 착각하여 잘못된 위치나 잘못된 시간정보로 계산토록 하여 잘못된 장소로 유인하는 방법이다.

9) GPS Jamming이란 GPS신호를 방해 또는 교란하는 방법으로 드론을 무력화시키는 것이다.

10) 이정율, 2021, 드론 사이버 보안 위협과 해결방안, KOSEN, p.4.
https://kosen.kr/info/reports/REPORT_0000000002013(검색일: 2024. 5. 9)

이러한 공격은 주로 드론의 통신 주파수 범위에 대해 강력한 전파를 발생시켜 제어신호를 방해함으로써 조종자가 드론을 원하는 대로 조작하지 못하게 만들어 드론의 통신 및 제어 시스템을 마비시킨다.

세 번째 드론 시스템의 주요 보안 취약점은 센서 교란 및 센서 데이터 위·변조이다. 공격자는 드론 탑재 센서 데이터를 교란 또는 조작하여 드론의 주변 환경 인식 능력을 약화시킬 수 있다. 이는 장애물 감지 실패나 오인으로 이어져 심각한 사고를 초래할 수 있게 된다. 또한, 공격자는 위조된 센서 데이터를 제공하여 드론 운영자를 속이기도 한다. 이는 오판단과 잘못된 의사결정으로 이어져 드론의 안전 운행을 위협한다.

넷째 보안위협은 임베디드 시스템(embedded system)[11]의 펌웨어 변조를 통한 시스템 권한 탈취 등이 발생할 수 있다는 점이다. 펌웨어[12] 변조는 공격자가 드론에 탑재된 임베디드 시스템의 펌웨어를 변조하여 시스템 권한을 탈취하고 드론을 제어하는 공격이다. 공격하는 해커는 악성코드를 삽입하거나 핵심 기능을 변경하는 방식으로 드론에 탑재된 임베디드 시스템의 펌웨어를 변조하는 것이다. 또한 임베디드 시스템의 보안취약점을 악용하여 시스템에 침투, 권한을 탈취하거나 원격제어를 시도하는 등의 행위를 하기도 하며, 시스템을 손상시키는 공격을 가할 수도 있다.

2) 지상제어장치에서의 보안위협

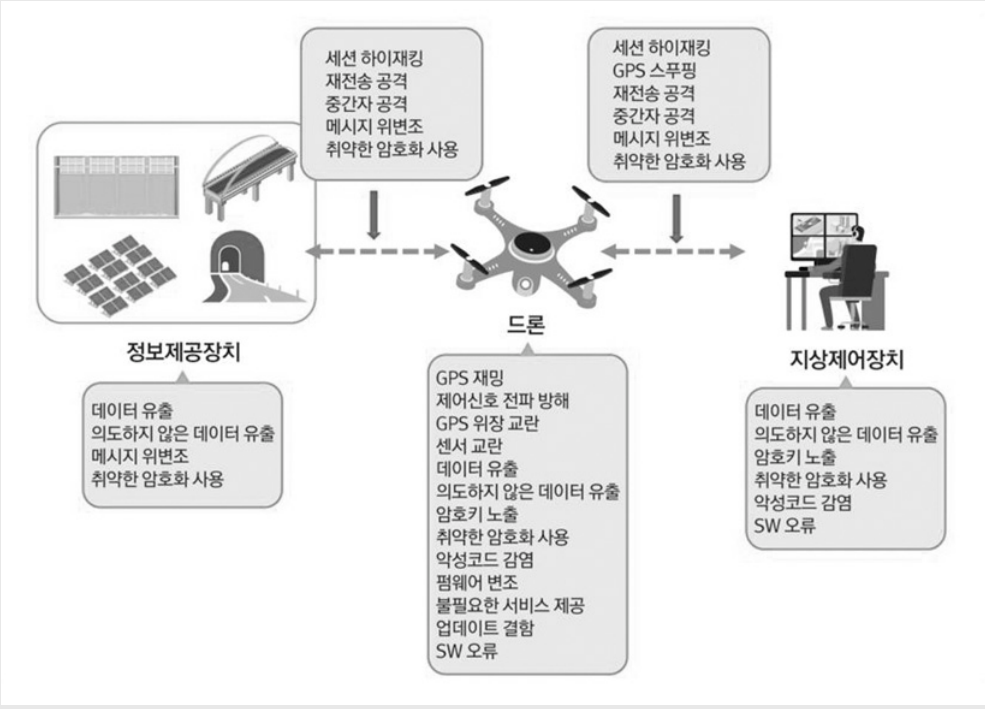
드론의 지상 제어 장치는 기밀 정보 유출의 위험에 직면해 있다. 첫째로, 공격자가 지상 제어 장치의 암호 키를 탈취하여 드론 제어 시스템에 접근하거나 기밀 정보를 유출해 갈 가능성이 존재한다. 둘째로, 취약한 암호 알고리즘을 사용하는 경우, 공격자가 암호를 쉽게 해독하여 시스템에 접근할 위험이 있다. 셋째로, 공격자가 지상 제어 장치의 데이터베이스에 침투하여 기밀 정보를 유출시키거나 삭제할 수 있는 데이터베이스 공격 역시 중요한 보안 위협이다.

이와 같은 보안 위협 외에도 잘못된 설계 및 구성으로 인해 소프트웨어 오류가 발생할 수 있다. 또한 정보 제공 장치에서는 드론과 지상 제어장치(GCS) 간의 통신 세션이 가로채여 드론을

11) 임베디드 시스템은 드론의 비행, 센서 데이터 처리, 카메라 제어, 통신 등 다양한 기능을 수행하는 컴퓨터 시스템이다. 컴퓨터 하드웨어, 소프트웨어, 센서, 통신 장치 등으로 구성된다. "Embedded"는 "내장된"이라는 뜻이며, "System"은 "시스템"이라는 뜻이다. 따라서 임베디드 시스템은 다른 시스템에 내장되어 특정 기능을 수행하는 시스템이라고 이해할 수 있다.

12) 펌웨어는 임베디드 시스템의 하드웨어에 내장되어 특정 기능을 수행하는 소프트웨어다. 컴퓨터 프로그램으로써 하드웨어와 직접 상호 작용하여 드론의 다양한 기능을 구현한다.

[그림 4] 드론 시스템의 주요 보안 위협



(출처: 한국인터넷진흥원)

제어 당할 수 있는 세션 하이재킹, 과거에 전송된 유효한 메시지를 가로채어 나중에 다시 전송하여 시스템을 속이는 재전송 공격, 그리고 통신 경로에 삽입되어 통신을 가로채고 악의적인 행위를 수행하는 중간자 공격 등 다양한 메시지 위·변조 및 데이터 위·변조 공격이 발생할 수 있다.

2. 빈번히 발생하는 보안위협

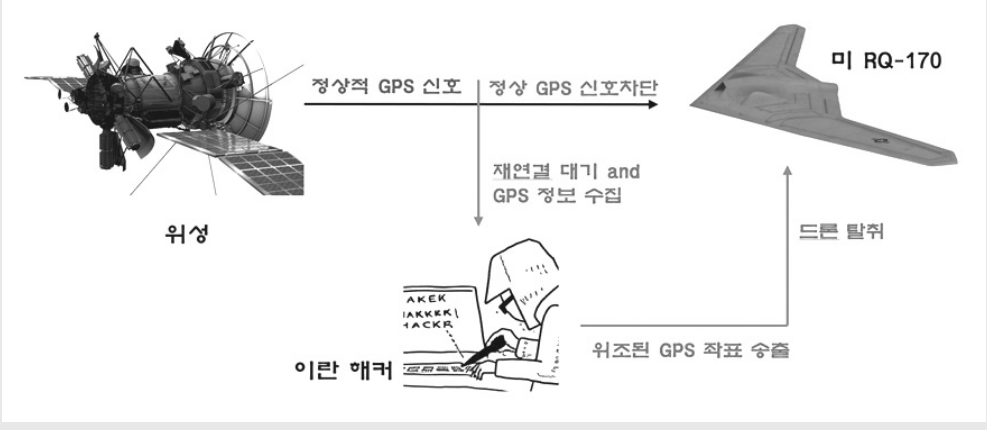
드론 시스템의 자산 환경에서 발생할 수 있는 보안 위협은 다양하며, 이에 대한 대응 방안을 제시하기 위해 3가지 보안취약요소를 활용해 보기로 한다. 공격자인 해커들은 일반적으로 1) 콘트롤러 칩에 대한 공격, 2) 잘못된 설계를 파고드는 공격, 3) 지상 통제센타, 사용자 및 드론 사이의 통신 과정에 개입하는 공격 등 3가지 방법을 주로 활용하는 것으로 전해진다.

1) 콘트롤러 칩에 대한 공격

2011년 12월, 미국과 이스라엘이 공동 개발한 스텔스 드론 RQ-170이 이란 상공에서 정찰 임무를 수행하던 중, 이란의 GPS 스푸핑 공격에 의해 탈취된 사건이 발생하였다. 이란은 드론의 GPS 신호를 차단한 후, 재연결 시 암호화되지 않은 GPS 신호를 이용하여 자신들이 원하는 좌표를 전송함으로써 드론을 이란 영토로 유도하여 착륙시켰다. 이를 통해 이란은 드론을 탈취하고 리버스 엔지니어링을 통해 드론 기술을 획득 및 복제하는 데 성공하였다. 이란은 2014년에 복제 드론의 시험비행에 성공하였으며, 2016년에는 스텔스 기능을 탑재한 장거리 공격용 드론을 공개하였다.

컨트롤러 칩은 드론 기체 내에서 GPS 수신, 자이로 센서[13], 기압 센서 등의 신호를 처리하고 모터를 제어하는 중요한 역할을 한다. 자이로 센서는 코리올리 효과를 이용하여 회전 물체의 각속도를 측정하며, 이를 통해 드론의 안정성 유지와 방향 제어, 자동 조종 기능을 수행한다. 이러한 핵심 요소들은 공격에 취약할 수 있다. 특히 GPS 수신기는 드론의 정확한 위치 정보를 처리하는 데 필수적이므로, 이를 통한 공격이 가능하다. 군용 GPS 신호는 암호화되어 있지만,

[그림 5] RQ-170에 대한 이란의 GPS Spoofing 개념도



13) 자이로 센서는 코리올리 효과라는 원리를 이용하여 작동하는데, 회전하는 물체에 힘을 가하면 회전축에 직각인 방향으로 겉보기의 힘이 발생한다. 이것을 코리올리 힘이라고 한다. 자이로 센서는 이 코리올리 힘을 측정하여 물체의 회전 속도를 계산함으로써 드론의 안정적 유지, 방향 제어. 자동 조종 등을 하도록 한다. 즉, 자이로 센서는 회전하는 물체의 각속도를 측정하는 센서다.

민간용 GPS 신호는 암호화되지 않은 경우가 많아 민간 드론은 중간자 공격에 노출되기 쉽다.

이와 같은 구조적 취약점을 이용한 대표적인 공격 기법으로는 GPS Spoofing과 GPS Jamming이 있다. GPS 스푸핑은 위성의 위치와 시간을 미리 계산하여, 정상적인 GPS 신호 대신 변조된 신호를 전송함으로써 위치와 시간을 조작하는 공격 방식이다. 최근에는 GPS 시뮬레이터나 무선 통신 연구 목적의 USRP 등을 통해 이러한 공격이 더 쉽게 구현될 수 있다. GPS 재밍은 드론이 사용하는 주파수 대역보다 높은 강도의 신호를 송출하여 정상적인 GPS 신호 수신을 방해하는 공격 방식이다.

2) 설계 결함으로 인해 발생하는 공격

드론에는 임무를 수행하기 위한 이미지처리 센서, 고해상도 카메라 등의 다양한 센서와 이를 활용하기 위한 어플리케이션 등의 다양한 하드웨어와 소프트웨어들이 존재한다. 최근 오픈소스 활용이 빈번해지고 보안이 고려되지 않은 설계 및 개발로 인해 보안위협 가능성은 높아지고 있다. 특히 잘못된 설계로 인한 펌웨어 취약점 및 접근제어 미흡 등은 악의적인 기능조작 및 프로그램 제어 등을 통한 펌웨어 변조로 인해 시스템 무력화 등에 활용 될 수 있다. 펌웨어 취약점 등으로 인한 악성코드 삽입은 드론 디바이스 자체의 보안위협 뿐만 아니라 드론을 제어하는 지상제어소까지 영향을 미칠 수 있게 된다.[14)]

2017년 5월에 발생한 사건은 이와 같은 보안 위협의 대표적인 사례로 꼽힌다. 당시, 한 익명의 해커 그룹이 네바다 공군기지의 시스템을 해킹하여 키로거 악성 코드를 설치했다. 이 키로거는 드론 조종사들이 키보드를 누를 때마다 입력 내용을 기록하도록 설계되었다. 해커들은 수개월에 걸쳐 키보드 입력 내용을 감시하였고, 이를 통해 드론의 비행경로, 무기 시스템의 작동 방법, NATO 국가들의 군사작전 계획 등의 기밀정보를 탈취했다.

3) 드론과 교신하는 무선통신에 가해지는 공격

드론의 무선 통신은 비행 중 필요한 중요한 요소로써, 다음과 같은 주요 방식으로 나눌 수 있다. 첫째는 4G와 5G를 통한 초저지연 서비스를 제공하는 셀룰러 무선 통신이다. 둘째, Wi-Fi와

14) 권구환, 2021, 드론산업의 발전과 보안강화 방안, IGLOO.
https://www.igloo.co.kr/security-information/%EB%93%9C%EB%A1%A0%EC%82%B0%EC%97%85%EC%9D%98-%EB%B0%9C%EC%A0%84%EA%B3%BC-%EB%B3%B4%EC%95%88%EA%B0%95%ED%99%94%EB%B0%A9%EC%95%88/(검색일 : 2024. 5. 10)

같은 비면허 무선 통신 방법이다. 셋째, 상용 위성 통신 기술이 있다. 드론은 상공에서 이동하기 때문에 무선 통신의 안전성이 매우 중요하다. 특히, 개방형 Wi-Fi를 사용할 경우 불법 접근 및 펌웨어 위변조 등의 위험이 높아 주의가 필요하다.

드론에서 많이 사용되는 통신 프로토콜인 MAVLink(Micro Air Vehicle Link)는 드론 환경에 최적화된 경량화 프로토콜이지만, 단순한 패킷 구조로 인해 암호화 강도가 약하다는 단점이 있다. 이러한 약점은 통신 과정에서 패킷을 가로채거나 변조할 수 있는 중간자 공격(MITM, Man In The Middle Attack)에 취약하다. 이 공격 방식은 권한이 없는 사용자가 네트워크 통신을 도청하거나 조작하여 정보를 가로채는 것이다. 스니핑[15], 세션 하이재킹, 패킷 주입 공격 등을 통해 드론과 사용자 또는 지상 제어장치 사이에서 전송되는 데이터를 도청하거나 변조하여 시스템 오류를 유발할 수 있다.

IV. 안티드론 및 보안대책

1. 안티드론과 드론 보안대책의 차이점

안티드론과 드론 보안대책은 밀접하게 연관되어 있지만 완전히 동일한 개념은 아니다. 결론부터 말하자면 안티드론은 불법 드론을 무력화하는데 초점을 맞춘 것이고, 드론 보안대책은 드론 자체의 보안을 강화하는데 초점을 맞춘 것이다. 즉 안티드론이 창(槍)이라면, 보안대책은 방패(防牌)라 할 수 있다.

안티드론은 불법 또는 악의적인 목적으로 사용되는 드론을 감지, 추적, 무력화하는 시스템을 의미한다. 여기에는 다음과 같은 기술들이 활용되고 있다. 드론의 무선신호를 감지하여 추적하는 레이더, 드론의 소리를 감지하는 음파탐지, 드론의 영상을 식별하는 광학감지, 드론의 조종신호를 방해하여 추락시키거나 무력화시키는 무선신호 방해, 드론을 포획하는 네트포획 등이 대표적이라 할 수 있다.

15) 스니핑(Sniffing)은 네트워크에서 전송되는 데이터를 가로채고 분석하는 공격 방식이다. 드론 통신에서 스니핑은 공격자가 드론과 지상 제어 장치 간의 통신을 몰래 엿보는 것을 의미한다. 이를 통해 공격자는 전송되는 기밀 정보, 비행 경로, 제어 명령 등을 수집할 수 있다. 스니핑 공격은 주로 암호화되지 않은 통신에서 발생하며, 공격자가 네트워크 트래픽을 모니터링하고 기록할 수 있는 위치에 접근할 수 있어야 한다.

현대전에서 드론의 역할이 점점 더 중요해짐에 따라 드론의 격추 · 무력화에 대한 필요성도 점점 더 커지고 있다. 이제 '드론-안티드론 대결'은 '고양이-쥐 게임'의 양상이 되었다. 독일 기업인 퀀텀 시스템스는 2023년 1월 우크라이나에 정보 · 감시 · 정찰용(ISR) 벡터 드론 100여대를 공급했다. 인공지능(AI) 기반의 소프트웨어와 전기광학 및 적외선 센서가 장착된 '트리니티'란 이름의 이 독일제 드론을 러시아군 탱크 · 병력 탐지 및 공중 습격 등의 임무에 요긴하게 활용했다. 그런데 2023년 11월 이들 드론이 임무를 마치고 복귀하던 도중에 하늘에서 갑자기 추락하기 시작했다. 이와 관련 뉴욕타임스(NYT)는 2023년 11월 '전자기파를 둘러싸고 우크라이나에서 벌어지는 그림자 전쟁'이라는 기사에서 우크라이나 전장에서 드론-안티드론 간 대결이 전자기 스펙트럼으로 확장되었다고 진단했다. 이러한 드론 추락은 러시아가 위성과 드론을 연결하는 무선신호를 중간에서 방해한 것으로 안티드론의 상징적인 사례로 볼 수 있을 것이다.[16]

한편, 드론 보안대책은 우리가 사용하는 드론 자체의 보안을 강화하고 악용을 방지하기 위한 노력을 말한다. 여기에는 다음과 같은 방법이 있을 수 있겠다. 드론 사용자를 식별하고 승인된 사용자만 드론을 조종하도록 제어하는 인증 및 권한 부여 제도, 드론 간의 통신과 데이터를 암호화하여 도청이나 위 · 변조를 방지하는 암호화, 드론 시스템 해킹을 방어하기 위한 보안패치 및 업데이트, 드론 도난이나 무단접근을 방지하기 위한 물리적 보안장치, 드론 시스템 오류나 사고 발생 시 안전하게 대처할 수 있는 절차마련 등이 대표적 보안대책이라 할 수 있을 것이다. 위에서 기술한 독일 드론 추락 사례가 발생한 뒤 독일 퀀텀 시스템스 기술자들은 일종의 보조 조종사(secondary pilot) 역할을 하는 AI 기반 소프트웨어를 개발하고 조이스틱(Xbox 컨트롤러)으로 드론을 착륙시킬 수 있도록 수동 옵션을 추가했다. 이러한 대응이 바로 드론 보안대책이라고 할 수 있다.

2. 안티드론의 필요성

안티드론이란 불법드론 등 전쟁 또는 테러 수단으로 활용되고 있는 드론을 무력화시키는 기술이다. 국민의 안전과 생명을 보호하기 위해서는 안티드론을 향상, 발전시켜야 할 것이다. 이

16) 주간조선, 우크라전에서 벌어지는 CIA의 '그림자전쟁'
https://weekly.chosun.com/news/articleView.html?idxno=34185(검색일: 2024. 5. 10)

스라엘–하마스 전쟁 및 러시아–우크라이나 전쟁에서 드론 공격의 증가는 효과적인 안티드론(anti-drone) 기술에 대한 증가하는 필요성을 강조한다. 다음과 같은 취약 요인들은 이러한 안티드론의 중요성을 여실히 보여준다.

1) 드론 공격의 증가하는 위협

드론 기술의 발전은 드론을 더 쉽게 접근할 수 있고, 저렴하며, 그리고 효율성이 풍부한 능력을 갖출 수 있게 만들어지고 있다. 이러한 기술의 발전은 드론의 도달범위, 포탄 등 무기 탑재 용량 그리고 공격적인 무기로의 사용 가능성을 향상시키는 자율 비행의 개선을 포함하여 점차 위협적인 무기로 향상되고 있다. 또한 국가 및 비국가 행위자 모두를 정찰, 감시 및 직접 공격을 단행할 수 있게 되었으며, 이러한 이유로 드론을 점점 더 많이 사용하고 있는 실정이다. 최근 각국의 분쟁은 드론 기반 전략에서 전략적 가치를 반영한 공격을 현저하게 증가시켰다.

2) 중요 인프라의 취약성

소위 테러용으로 사용되는 드론은 전력망, 통신망, 민간 지역과 같은 중요한 사회 기반 시설을 목표로 사용되어 왔다. 물론 전쟁용 드론도 마찬가지다. 이것은 필수 공공서비스를 방해할 뿐만 아니라 다중(多衆) 사이에 두려움과 불확실성을 심어줘 공포감을 유발한다. 드론의 정확성과 민첩성은 드론이 특정 고부가가치 목표물을 타격하는 데 특히 효과적이어서 전통적인 방어 메커니즘을 복잡하게 만든다.

3) 탐지 및 무력화에 대한 과제

드론은 낮은 고도에서 비행할 수 있고, 심지어는 레이더 탐지를 피할 수 있는 스텔스 기능까지 겸비할 수도 있기 때문에 전통적 방어 시스템이 복잡한 도시환경에서 드론과 다른 물체를 구별하는 데 어려움을 겪을 수 있다. 효과적인 안티드론은 드론을 탐지할 뿐만 아니라 부수적인 피해를 주지 않으면서도 적대적인 드론을 무력화해야 하는 과제를 안고 있다.

4) 안티드론 기술 개발 절대 필요

최근 각국의 분쟁과 관련하여 드론을 활용한 직접적인 전투 및 테러 가능성이 높은 것이 사실이다. 이러한 위협을 해결하기 위해 안티드론 기술 혁신, 전략적 국방 계획 및 포괄적인 규제 프레임워크가 필요한 실정이다. 아울러 테러 가능성에 대해서 폭넓게 연구하여 해외공관은 물

론 우리 내부의 보안시설물에 대한 안티드론 대책도 수립하여야 한다.

구체적인 안티드론 대책으로는 효과적으로 드론을 감지하여 무력화시킬 수 있는 시스템 개발이 절대적으로 요청된다. 레이더, 음향센서, 광학시스템, 전자전 장비 등 다양한 기술을 통합하여 다층 방어 네트워크를 구축하는 포괄적인 접근 방식이 요구된다 하겠다. 또한 드론의 확산은 드론의 사용을 통제하기 위한 강력한 규제체계를 필요로 한다. 여기에는 드론 사용에 대한 규범과 협정을 제정하기 위한 국제 협력과 국내 · 외적인 드론 대응 조치가 포함되어야 한다.

3. 드론 보안대책

드론에 대한 보안대책이라 함은 우리의 드론이 적(敵)으로부터 탐지, 포획, 파괴되지 않도록 방지하는 것이다. 그러기 위해서는 다층 보안 프레임워크를 수립하여 시행해야 할 것으로 판단된다. 구체적인 방안으로는 크게 아래와 같이 분류해 볼 수 있을 것이다.

1) 암호화 및 보안 통신

우리의 드론 보안대책으로는 우선적으로 암호화 프로토콜이 선행되어야 한다. 드론과 관제소 간의 모든 통신에 대한 고급 암호화 표준을 구현하여 감청 및 변조를 방지해야 한다. 강력한 인증 방법을 사용하여 승인된 직원만이 드론에 액세스하고 제어할 수 있도록 하는 인증 메커니즘이 필요하다.

2) 방해 방지 기술

스프레드 스펙트럼(FHSS, frequency hopping spread spectrum)을 사용하여 공격자가 통신 신호를 방해하기 어렵게 만드는 주파수 호핑(Frequency Hopping) 방법을 개발하는 한편, 하나의 채널이 손상되어도 다른 채널이 지속적으로 작동할 수 있도록 이중 통신 시스템(Redundant Communication Channels)을 개발하는 것도 좋은 방법이다.

3) 사이버 보안 조치

테러 해커들이 사이버 상의 라인을 통해 접근하는 것을 차단하기 위해 드론과 관제소 모두에 방화벽 및 침입 탐지 시스템(IDS)을 설치, 무단 접근을 탐지하고 방지한다. 또한 정기적인 소프

트웨어 업데이트를 통해 취약성을 패치하고 보안 기능을 개선해야 한다.

4) 물리적 보안

우리 드론에 대한 무단 접근이 감지되면 자멸 또는 데이터 삭제를 유발하는 변조 방지 메커니즘(Anti-Tampering Mechanisms)을 드론에 장착하는 것도 좋은 방법이다. 물리적인 포획을 방지하기 위하여 드론이 작동하지 않을 때 보안 스토리지 솔루션을 구현하는 것도 하나의 좋은 방법이다.

5) 운영 프로토콜

드론 운영자에게 보안 프로토콜 및 위협 인식에 대한 포괄적인 교육을 실시하여야 하며, 보안 위반 시 비상 대응 조치를 포함한 안전한 드론 운영을 위한 표준운용절차(SOPs, Standard Operating Procedures)를 개발하고 시행한다. 아울러 드론에 대한 보안조치가 효과적이었던 사례, 보안조치의 실패 사례를 분석하여 보안 프레임 워크를 지속적으로 보완해 나가는 것도 중요하다 할 것이다.

V. 결론

드론 기술의 급속한 발전은 다양한 분야에 걸쳐 중요한 기회와 도전을 동시에 제시했다. 드론은 농업과 인프라 점검부터 비상 대응, 배달 서비스에서테러와 전쟁에 이르기까지 확장되어 드론의 응용 분야에서 매우 효율적인 도구로 입증되었다. 그러나 이러한 광범위한 이용으로 인해 강력한 안티드론대책 수립 및 드론 보안 조치가 필요하게 되었다. 드론은 허가되지 않은 감시, 밀수, 심지어 테러 및 전쟁 행위의 도구로 사용되는 등 악의적인 목적으로 악용될 수 있기 때문이다.

따라서 이러한 위험을 효과적으로 완화할 수 있는 포괄적인 보안 프레임워크가 시급한 형편이다. 레이더 시스템, 무선 주파수 재밍 및 고급 AI 기반 탐지 및 무력화 방법과 같은 안티 드론 기술은 공격은 물론 방어 도구로도 부상하였다. 이러한 안티드론 및 보안대책은 진화하는 위협에 맞서기 위해 지속적으로 개발되어야 하고 기존 보안 프로토콜도 진화하여야 한다.

드론 기술의 발전과 활용 확대는 사회 전반에 걸쳐 긍정적 영향을 미치고 있지만, 동시에 새

로운 위협 또한 야기하고 있는 실정이다. 적의 드론 공격으로부터 중요 시설과 인명을 보호하기 위해서는 공격적인 안티드론 전술과 방어적인 드론 보안 대책이 상호 보완적으로 발전되어야 할 것이다.

국가 지원 하 기업이 참여하여 AI 첨단 기술을 동원한 안티드론을 지속적으로 개발하여 중요 시설, 국경지역, 군사작전지역 등 전략적 위치에 안티드론 시스템을 배치하여 예상되는 적 또는 테러분자의 공격에 대비하는 것이 중요하다. 또한 예방적인 방어를 강화하기 위해 강력한 인증 및 암호화, 사이버 공격방어, 비행 제한구역 설정, 조종자 교육 등 더욱 첨단화된 드론 보안대책을 수립하여 시행하는 것이 요구된다.

드론 기술은 빠르게 발전하고 있으며, 이에 따라 안티드론 및 드론 보안 대책 또한 지속적으로 연구 및 투자되어야 한다. 미래 드론 기술의 변화를 예측하고, 이에 대비할 수 있는 차세대 안티드론 시스템과 드론 보안 기술 개발이 보안을 책임지고 있는 국가정보원 등 관계부처가 참여하여 이뤄져야 할 것으로 판단된다.

드론 위협은 국경을 넘어 전 세계적으로 발생하고 있다. 따라서, 효과적인 대응을 위해서는 국가 간의 협력이 필수적이다. 정보 공유, 기술 협력, 공동 운영 등을 통해 국제적인 안티드론 및 드론 보안 대응 체계를 구축하는 것도 필요하다 할 것이다.

안티드론과 드론 보안대책은 서로 분리된 개념이 아닌, 상호 보완적인 전략이다. 안티드론 시스템만으로는 모든 위협을 차단하기 어렵고, 드론 보안 대책만으로는 예상치 못한 공격에 취약할 수 있기 때문이다. 따라서, 적극적인 공격과 예방적인 방어를 동시에 강화하여 불법적인 드론으로부터 안전한 환경을 조성해야 할 것이다. 결론적으로, 안티드론과 드론 보안 대책은 공격과 방어의 균형을 통해 상호 보완적으로 발전되어야 한다는 의미다. 지속적인 연구, 투자, 국제 협력을 통해 미래 드론 기술의 변화에 대비하고, 불법적인 드론으로부터 안전한 국가와 사회를 구축해야 할 것이다.

참고문헌

[저서]

강원구 외,『드론 바이블』(서울: 플래닛미디어, 2015).

권희춘 외,『하늘의 눈 드론학』(서울: 홍릉과학출판사, 2020).

공현철 외,『픽스호크 드론의 정석』(서울: 성안당, 2019).

박종현 외,『사물 인터넷의 미래』(서울: 전자신문사, 2014).

신정호 외,『드론학 개론』(서울: 복두출판사, 2021).

윤홍주,『드론학 개론』(서울: 더블비, 2021).

좋은정보사,『드로시장의 인공지능 융합기술 기반 주요기술개발 동향 및 사례분석』(성남시: 좋은정보사, 2018).

[논문]

가경환 외, "불법드론에 대한 공항 대응 체계에 관한 연구." 「한국항공경영학회지」 제19권 3호, 2023.

강정현 외, "드론 하드웨어 고유특성을 이용한 식별 및 인증 기술 연구 동향." 「ACK 학술발표대회 논총」 제30권 1호, 2023.

김세일 외, "드론 위협에 대한 방어체계 분석," 「한국융합과학회지 논총」 제11권 11호, 2023.

김수현 외, "정밀농업 기술의 수용의사에 미치는 영향 연구: 드론 영상 기술을 중심으로," 「협동조합경제경영연구」, 제58집, 2023.

김일곤, "재난 · 재해 지역에서의 드론 활용체계 구성에 관한 연구," 「융합과 통섭」 제4권 2호, 2023.

김재경, "카고 드론 개발 동향 및 활용 방안," 「항공우주메거진」 제17권 1호, 2023.

류병훈, "UAM의 도입 및 산업화를 위한 법 · 제도의 설계." 「홍익법학」제23권 2호, 2022.

박상현 외, "드론 임베디드 시스템 및 네트워크 프로토콜 기반 보안위협 동향." 「ACK 학술발표대회 논총」 제30권 1호, 2023년

양권 외, "해난구조용 드론 디자인 연구: 드론의 형태비교를 중심으로," 「한국기초조형학회」 9월호, 2023.

유지웅 외, "경찰의 드론 활용을 위한 법제 개선 방안 연구," 「한국경찰학회보」 제25권 3호, 2023.

장용진 외, “군사기술 네트워크가 민군겸용 기술개발에 미치는 영향.”「고려대 경영대학 연구서」8월호, 2021.
정성민 외, “드론봇 전투체계 발전을 위한 드론 설계의 이해와 군사적 활용,”「국방과 기술」제525권, 2022.

외국자료

[저서]
고바야시 아키히토 · 배성인 옮김,『드론 비즈니스』(서울: 아테나, 2021).
데이비드 맥그리퍼 · 임지순 옮김,『Make 드론』(서울: 한빛미디어, 2017).
찰스 바우텔 · 박광순 옮김,『무기의 역사』(서울: 가람기획,2002).
테리 킬비 · 베린다 킬비 · 이하영 옮김,『처음 시작하는 드론』(서울: 한빛미디어, 2016).

Abstract

A Study on the Necessity of Anti-Drones and Security Measures against Terrorism and War Drones

Jin, JongGu (Chair Professor of Daejin University)
Nam, Eunmi (MG Community Credit Cooperatives)
Kim,Yoojin (Pocheon Family Sexual Counseling Center)

Due to the recent development of drone technology, the use of drones for terrorist and war purposes is increasing, which poses a serious security threat. This paper investigates and analyzes the necessity of establishing anti-drone and security measures for terrorist and war drones, and suggests effective countermeasures. Terrorism and war drones can carry out terrorist attacks, military attacks, attacks on civilian facilities, and invasion of privacy. Anti-drone and security measures against this may include detection and tracking, neutralization, capture, regulation, and legal measures. Anti-drone and security measures for terrorist and war drones need continuous research and development. It is time for international cooperation to study new threats and countermeasures in line with the development of drone technology and to establish an effective anti-drone system.

Key Word: Drone, anti-drone, drone security measures, unmanned aerial vehicle, drone war, terrorism, war

• 투고일: 2024. 5. 26. • 심사일: 2024. 6. 10. • 심사완료일: 2024. 6. 22.