Journal of Digital Convergence
Vol. 16. No. 10, pp. 223-233, 2018

ISSN 1738-1916
https://doi.org/10.14400/JDC.2018.16.10.223

군보안상 드론위협과 대응방안

김두환[1], 이윤환[2*]
[1]건양대학교 대학원 박사과정, [2]건양대학교 국방경찰행정학부 교수

A Study on the countermeasures and drones's threats in Military security

Doo-hwan Kim[1], Youn-hwan Lee[2*]
[1]Doctor course, Dept of Public Administration, Kon Yang University
[2]Professor, Dept of Miliary Defense & Police Administration, Kon Yang University

요 약 군은 적으로부터 국민의 생명과 재산을 보호하기 위해 헌법에서 규정한 조직으로서 조직의 특성상 군사보안은 전쟁에서의 성패를 결정지을 중요한 요소이다. 그런데 최근 제4차 산업혁명으로 대변되는 급격한 문명과 기술의 진보는 군내부 군사보안 환경에도 영향을 끼쳐 다양한 변화들을 일으키고 있다. 이런 환경의 변화에 자칫 적절한 대응을 하지 못할 경우, 군조직과 내부 보안에 치명적인 위해를 끼칠 수도 있는 상황이다. 이런 측면에서 군에 새로운 위협으로 대두되고 있는 군사보안위협 요소들을 살펴보고, 그중에서도 최근 가장 기술 진보적이면서도 광범위하게 유입되어질 수 있는 드론에 대해서 보다 중점적인 논의를 진행할 예정이다. 이를 위해 군의 지휘통제·정보작전·기동·화력·작전지속 지원에 이르기까지 그 범위를 광범위하게 확장시켜 나가는 드론이 가지고 있는 취약점과 문제점을 분석하고, 군사보안적인 측면에서 이러한 보안위협 요소에 대한 발전적 보안 대응방안 수립을 목표로 하고자 한다.

주제어 : 드론, 군사보안, 군, 보안위협, 해킹, 스푸핑

Abstract The forces to protect people's life and property against the enemy attack is an organization which is regulated by the constitutional law. In terms of nature, its security is a significant factor to determine success or failure for the war. However, recently the 4th industrial revolution represents the rapid change in the advancement of civilization and technology. It can influence on the environment of military security which can make various changes. Unless taking proper action againsty these changes, it can inflict a vital harm for the organization of forces and its internal security. In this aspect, this study discuss new threats of the military security, above all, the most technical improvements and harms for the drones in terms of security. In addition, the advantages and disadvantages of drones which can influence on the ragions of military command and control, information operations, maneuvers, firepower, operation sustainment supports are analyzed. Moreover, this study set the purpose of developmental security measure for security threats in the aspects of military security.

Key Words : Drone, Military security, Forces, Security threats, Hacking. Spoofing

1. 서론

군은 나라를 수호하기 위해 헌법적으로 무력 행사가 보장된 전투조직으로서 한 나라의 국토와 국민을 수호하기 위한 근간조직이다. 군의 힘은 그 나라의 힘과 국력으로 상징되기도 하는데, 이런 군에서 이루어지는 작전과 무기체계 등과 관련한 사항들은 외부에 대해 항상 보안과 비밀이 보장되어야 한다. 현대사회에 있어 이러한 군

* Corresponding Author : Youn hwan Lee(lyh@konyangr.ac.kr)
Received August 31, 2018 Revised October 1, 2018
Accepted October 20, 2018 Published October 28, 2018

과 군사보안에 대한 중요성은 국가간 정보전쟁으로까지 비화될 수 있을 만큼 첩보전을 방불케 해 왔으며, 군을 유지하는 예산중에도 이러한 군내 보안·정보보호 및 비밀유지에 쓰이는 예산의 비중이 날로 증가하는 추세에 있음을 누구도 부인할 수 없다.

이러한 이유로 군을 공격하는 내·외부의 보안위협들은 군의 존립을 위협하는 위해요소로서 항상 대응에 만전을 기울여야 하는 핵심과제이며, 이러한 보안적 대응에 실패할 경우 군 전투역량의 감소와 군 전체 작전의 실패에 까지 이를 수 있을 만큼 중요도가 절대적인 것이다. 이러한 상황속에서 최근 문명의 지속적인 발달과 기술의 혁신으로 인해 파생된, 과거와는 비교할 수 없는 내·외부 보안환경의 변화는 군에 있어 새로운 도전들이 되어지고 있으며, 군 내·외부적으로 급격하게 유입되는 새로운 보안위협들은 실로 군을 위협하는 수준에 까지 이르렀다고 해도 과언이 아닐 것이다. 이에 따라 본 논문에서는 이렇듯 군을 위협하는 새로운 보안위협들에 대해 간략히 살펴보고, 그중 “드론”과 관련한 보안위협에 중점을 두고 논의를 진행해 나가고자 한다.

드론에 관심을 갖는 것은 두가지 이유에서다. 첫째, 드론은 현재 육군이 역점을 기하고 있는 5대 전장의 게임체인저중 핵심적 요소로서, 그것을 통한 새로운 작전체계를 구축하고 드론봇 전투단을 창설하는 등 과거에 없던 혁신적인 조치들이 현재 진행형으로 이루어지고 있는 뜨거운 이슈이기 때문이다[1]. 둘째, ’14년도에 두 대의 북한제 소형무인기가 우리나라의 주요시설과 군 작전시설들을 무단으로 촬영하고, 그동안 정찰활동을 은밀히 지속해 왔다는 사실이 드러남과 동시에 드론(무인비행장치)이라는 장치가 군에 얼마나 위협으로 다가올 수 있는지에 대한 충격적인 사건이 있었기 때문이다.

이렇듯 군내부에 새로운 위협으로 작용할 수 있는 드론에 대한 이해와 함께 과연 그것이 군과 군내부 보안에 미치는 다각적인 영향과 보안위협들을 살펴보고, 그에 대한 발전적인 방지대책에 대해 연구하는 것은 현시점에서 가장 적시적으로 진행되어져야 할 주제라 할 수 있다.

이를 위해 2장에서는 군과 군사보안에 대한 사전이해를 위해 군조직 내부의 보안의 개념과 새롭게 군에 대두되는 보안위협요소에 대해 논의를 진행하며, 3장에서는 이러한 보안위협요소중 드론에 집중하여 드론의 기술적 요소들과 비행관련 요소들을 살펴보고, 4장에서는 그러한 드론관련 위협요소에 대한 군내부 보안관리 대응방안에 대하여 다각적인 논의를 진행할 예정이다.

2. 군조직내 보안과 새로운 위협

2.1 군내 군사보안의 의미와 새로운 환경변화

앞서도 말했듯, 군의 생명은 첨단의 무기체계와 이를 바탕으로 한 비밀스러운 군사작전이다. 그리고, 이러한 군의 생명을 적으로부터 방어하고, 수성하는 제반 방어체계가 바로 보안이다. 여기에는 소극적인 보안과 타의 침해와 위해로부터 군에 대한 자산과 체계 등을 능동적으로 방어하는 적극적인 보안이 있다. 좀더 보편적으로 얘기하면, 보안이란 개인, 조직 또는 국가가 그 존립을 확보하거나 경쟁에서 승리하기 위해 필요한 조직내 핵심요소를 보호하는 것을 말한다.

따라서 보안이란 국가만이 아니고 기업체나 단체, 개인에게도 반드시 필요하며, 실제로 그러한 대책들은 누구의 지시에 의해서가 아니라 자기 방어를 위해 본능적으로 강구하면서 행하는 것이다[2]. 이런 보안이 군에 적용된다면 그야말로 한나라의 존망과 성패와 직결된 문제이기 때문에 군사보안이야 말로 한 국가를 지키기 위한 핵심 필수요소라고 할 수 있다.

군내 군사보안에 대해 좀더 세부적으로 얘기하면, 군사적으로 적의 간첩(스파이) 행위, 관측, 파괴, 요란 및 기습으로부터 부대를 보호하기 위하여 취하는 제반 활동으로서 적의 아군에 대한 정보 수집을 거부하는 대정보(방첩)적 방어 수단의 하나라고 설명할 수 있다[3]. 여기서 말하는 ‘보호하기 위해 취하는 제반 활동’이란 군사상의 각종 행위에 대하여 보안상 유해롭고 위협이 되는 사항을 미리 예방·통제하는 제반적 보안 방지대책들을 말한다. 본 논문에서는 군내 군사보안에 대한 이러한 기초적 인식하에 기존의 고전적인 군사보안의 개념을 넘어 기술의 혁신과 문명의 발달과 궤를 같이하여 무섭게 변화되는 환경들은 어떤 것이 있는지 살펴보고, 그러한 새로운 환경변화가 군사 보안에 미치는 영향요소와 위해요소들을 면밀히 살펴보며, 이에 대해 어떠한 방향성을 가지고 군이 발전적으로 대응해야 할 것인지에 대해 검토를 할 것이다. 무엇보다 이러한 검토의 중심에 최근 전면적으로 군에 확산되고 있는 드론과 관련하여 ‘드론과 군 조직내 군사보안’에 대한 주제를 가지고 논의를 진행할 예정이다.

2.2 군조직내 새로운 위협요소

군내 새로운 환경변화에 따라 대두되고 있는 위협요소로는 첫째, 인원보안(민간외부인원들의 지속적 유입) 위협, 둘째, 군내 사이버 해킹 위협, 셋째, 군내 운용될 예정인 드론의 보안위협 등이다. 순서대로 간략하게 살펴보고자 한다.

첫째, 민간 외부인원들의 지속적인 유입이 인원보안측면에서 새로운 위협으로 등장하게 된 것은 군에 출입하는 인원들이 다양화되고, 첨단화되어 그만큼 외부로 부터의 불승인 인원들에 대한 통제에 어려움이 있을 수 있다는 것을 의미한다. 인원에 대한 보안은 전통적으로 군에 있어 피아를 식별하는 것과 같으며, 이는 언제나 군에서는 가장 중요한 보안요소이다. 인원보안은 과거 수기출입증과 비밀번호 시건장치에서 시작되어 현재 과학화된 출입증과 지문등으로 발전하였다가 앞으로는 안면인식에서 생체(홍채)인식, 맥박에 대한 체크를 하는 수준에까지 기술적으로 진보되어질 예정이다.

이러한 요인들이 중요해 지는 것은 앞서도 말했듯 군에 출입하는 외부인원들이 너무 많아졌고, 그들에 대한 출입조치와 보안소요들이 점점더 군내 보안업무에 상당한 비중을 차지할 것이기 때문이다. 무엇보다 군과 다양한 접촉 연계점으로 사업을 하는 민간 용역업체 외부인원의 출입이 그야말로 점점 더 증대되어질 예정인데, 이는 근본적으로 군내부 기술력이 군외부의 사회기술을 따라가지 못함에 따라 기인한 것으로, 군을 유지하고 운용하기 위해 필연적으로 군외부 기술자들의 군내유입이 불가피해진다는 것을 의미한다. 군내부 인원만으로 군이 운용되던 시대는 이제 지난 것이다. 그러나, 이런 추세를 받아들인다 해도 군내 기술자보다 월등한 민간 전산기술자들이 군내부로 지속적으로 유입되는 상황이 군으로 보면 하나의 외부 인원보안적 위협요소가 될 수 있으며, 이들에 대한 인원보안적인 통제 대책은 군조직 외부로부터의 위해요소에 대한 가장 기본적인 보안 방어대책일 것이다.

둘째, 지난 '16. 8월, 군의 내부망이 북한 해커에 의해 해킹되어지는 초유의 사건이 발생했다. '북한 해커로 추정되는 세력이 국방부 백신 납품업체의 자료를 다수 해킹한 뒤 이번 해킹의 수단으로 백신의 취약점을 이용, 국방통합데이터센터(DIDC) 2센터에서 국방망과 군 인터넷망의 접점을 발견한 뒤 국방망에 침투, 악성코드를 유포' 한 사건인 것이다[4]. 군의 국방망이 해킹을 당해 '군 외부 인터넷망과 내부 인트라넷(국방망)에서 유출된 기밀은 2급 226건, 3급 42건, 대외비 27건 등 총 295건으로 크기만 235GB에 달하며, 유출된 기밀에는 작전계획 5015와 침투 및 국지도발 대응계획인 작전계획 3100등'이 포함되었다[5].

사건의 시작은 군내부로 과도하게 유입되고 있는 민간용역 전산기술자(국방부 백신업체 직원)들로부터 시작되었으며, 보안의식이 결여된 이런 외부인원들이 군내부 국방망(폐쇄망)에 기술적으로 연결·연동되는 순간이 보안적인 측면에서 가장 위협적인 순간이다. 이렇듯 기술적으로 민간기술자 및 민간체계들이 군내부망 및 내부통신기반체계와 접속되어 있는 수천의 연동접점들이 문제가 될 수 있다. 무엇보다 기술개발과 IT기술의 진보는 군이라는 조직에도 그대로 전파되어 군 내부 조직의 통신환경과 사이버 공간의 발달을 심화시키고 있으며, 그에 따라 군 조직내에 끊임없이 유입되는 선진기술의 민간기술자와 용역업체 직원들을 통한 국방내부망의 약한 고리 접점들이 발생할 수 밖에 없게 되었다.

바로 이러한 약한 고리접점들이 외부 해킹세력에게 그대로 노출, 노림수가 되어 군내 보안의 위협적인 보안위해 요소가 되어질 수 있는 실정이다. 지난 해킹사고의 피해는 실로 막대한 것이어서 군의 거의 모든 주요작전문서와 작계가 해킹을 당하는 지경에 이르렀던 것이다. 물론 사건이후 군내 조직적인 후속 대책으로 재발방지에 대한 강력한 조치들이 완료되었지만, 4차 산업혁명이라고 일컬어지는 기술의 혁신속에서 이런 사이버 해킹과 사이버 보안의 문제는 언제든지 우리 군을 위협할 수 있는 강력한 보안위협이 될 수 있음을 인식하고, 경각심과 함께 세심한 주의를 게을리 하지 않으면 안될 것이다.

셋째, 드론은 4차 산업혁명을 상징하는 핵심적이면서도, 활용도 측면에서 광범위하게 확산되고 있는 분야이다. 이는 축적된 기술력을 통해 적은 노력과 비용을 가지고도 다양한 목적을 달성할 수 있다는 편의성에서 촉발된 것이다. 이런 흐름에 맞추어 육군은 지상군의 전투력 창출이라는 취지하에 드론봇 전투단 창설을 준비하고 있으며, 드론을 활용한 군 무기체계화가 점진적으로 진행되고 있는 상황이다[6].

드론을 활용한 작전체계를 구축하고, 전장의 상황을 단번에 역전시킬 수 있을 게임체인저로서의 역할을 집중조명하며, 드론봇 전투체계 비전 2030을 발표하기에 이르렀다. 그야말로 군내 드론의 활용범위가 지휘통제로

부터 시작하여 정보작전, 기동, 화력, 작전지속지원에 이르기까지 실로 전방위 全영역이라 해도 과언이 아닐 정도로 군에 적용되는 드론의 비중은 급격하게 증대되고 있는 것이다[7].

이렇게 확대되는 군사용 드론의 활용범위가 군조직내 새로운 보안위협이 될 수 있는 것은 드론이 물론 강력한 강점을 가지고 있지만 다양한 취약점 또한 노출되고 있기 때문이다. 누구나 접근하기 쉽고, 활용도가 넓다는 것은 반대로 누구나 해킹하기 쉽다는 것을 의미하며, 조정기를 공략하여 통제권을 불법으로 조정하고, GPS 위장신호를 통해 혼선을 주기도 하며, 센서를 위장하여 정보를 유출하고, 악성코드 감염 등을 통해 드론 자체를 해킹의 도구로 활용할 수 있다는 면에서 군내 드론으로 인한 보안의 취약점은 사전에 면밀하게 그 영향관계가 분석되어져야 할 것이다. 무엇보다도 드론을 활용한 군사주요시설 및 기지에 대한 불법 촬영의 가능성까지 고려한다면 그 위협의 수준은 기존에 군에 미쳤던 그 어떤 분야보다도 강력할 것이라 예측할 수 있다. 본지에서는 앞서 살펴보았던 보안의 위협보다도 금번 드론과 관련하여 발생될 개연성이 높은 보안위협을 중심으로 향후 군내 보안관리에 대해 그 대응방안을 논의하고자 한다.

3. 드론의 보안위협과 보안관리

3.1 드론의 정의와 보안 위협요소

드론은 조종사가 탑승하지 않고 무선으로 전파유도되는 비행 및 컨트롤이 가능한 회전익 모양의 항공기를 총칭하며, 세부적으로 국내 항공법에서는 연료를 제외한 자체 중량이 150kg이하인 것은 무인비행장치로, 150kg을 초과하는 것은 무인항공기로 규정하고 있다. 상용으로 판매되는 대부분의 드론은 150kg 이하의 무인비행장치이며, 특히 무인 비행장치중 자체중량이 12kg이하이면서 엔진배기량이 50cc는 스포츠용 무선조정 모형항공기로 간주하여 신고없이 비행이 가능한 상황이다. 사실 이러한 드론은 과거 우리에게 익숙한 용어인 무인항공기 UAV(Unmanned Aerial Vehicle)라고 불러왔으나, 최근 드론(Drone)이란 명칭이 일반화되어 사용되고 있다.

이러한 드론은 항공과 전자공학, IT기술의 융합체로서 일반적 구조로는 조정기, 수신기, 비행체, 비행콘트롤러, GIS모듈, 배터리, 지상통제 SW 등으로 구성되어 있으며, 무인비행장치와 비행제어시스템과의 통신적인 측면에서 바라보면, 제어부, 센서부, 엑츄에이터, 통신부, 전원부 등으로 구성되어 있다고 할 수 있다. 또한, 드론은 기술적으로 기계역학기술, 소프트웨어 컴퓨팅, 컨트롤러 통신기술로 융합되어 있는데, 기술적으로는 이러한 각각의 분야와 단계마다 기술적인 해킹과 변조, 위조 및 절취 등이 가능하여, 단계적 위협들 자체가 드론의 부작용으로서 보안의 위협요소들로 작용할 수 있다 하겠다.

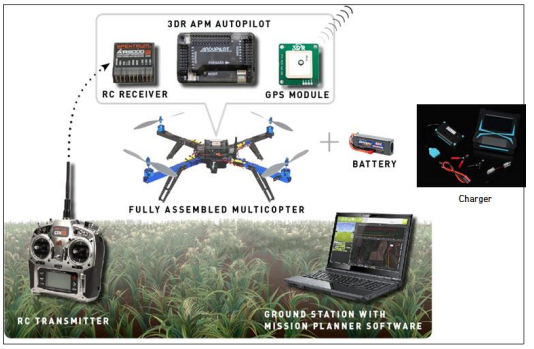

Fig. 1. Introducing Copter(The general structure of the Drones) [8]

환기하자면, 사실 무인비행장치가 군에 위협적인 존재로 느껴지기 시작했던 시점은 '14년 3월, 두 대의 북한제 소형무인기의 침범에서부터 시작되었을 것이다. 북한은 소형무인기에 조악한 촬영장치를 장착하여 우리 군 주요시설 등을 촬영하고 자동 복귀하는 시스템으로 그동안 남한내 비행정찰 활동을 은밀히 지속해 왔으며, 무인기의 추락과 함께 이런 사실이 드러나면서 크게 언론에 이슈화 된 바 있다[9].

아마도 이것이 소형 무인기가 군작전과 보안에 치명적인 위협요소가 되어질 수 있다고 경각심을 갖게 한 첫 번째 사례가 되어졌다고 볼 수 있다. 이에 더해 북한은 이미 드론을 활용한 감시·정찰활동 뿐만 아니라 주요 근접전에 대량으로 드론을 활용하는 방안까지 진전됨에 따라 소형무인기에서 드론으로의 기술적 진보를 보여주고 있는 실정이다.

군의 공중과 하늘이 지극히 작은 소형 무인비행기나 드론에 의해서도 무방비로 노출될 수도 있다는 개연성은 그것만으로 군사적 위협이며, 이러한 북의 드론과 관련한 기술적 진전이야말로, 군내 드론에 대한 물리적 위협과 함께 보안상의 위협에 대해서도 새롭게 주목하는 계기가 되었다고 생각되어 진다.(인제추락 '17. 6. 8, 백령도 추락 '14. 4. 1, 파주추락 '14. 3. 24.)

그러나, 이러한 드론의 위협이 비단 군에 국한된 것은 아니다. '14. 10월, 프랑스 원자력발전소 7곳 드론 출몰, '15. 7월, 미국 센트럴 코너티켓주립대 총쏘는 드론 제작, '16. 4월, A320 영국 항공기와 드론과의 충돌사건 등 드론과 관련한 다양한 사고사례와 위협들이 끊이지 않고 발생하고 있다[10].

좀더 구체적으로 이중 몇가지의 사례들을 살펴보자면, 무엇보다도 미국의 맨즈필드 교도소 상공에 헤로인 7g, 마리화나 57g 등을 탑재한 마약 적재 드론이 출몰('15. 7월)하여, 드론에 폭발물 탑재의 위험성을 환기한 사건과, 중국 DJI社의 직경 약 61cm크기의 상업용 드론이 조종사 실수로 백악관 건물에 충돌하는 사건은 드론의 위험성을 대내외적으로 각인시키는 사건이 아닐 수 없었다.('15. 1월) 이를 통해 얼마든지 드론이 탈취되고, 악성코드 감염 등을 통해 테러목적으로 악용될 수 있음을 경고하면서 군 주요시설에 대한 집중타격 및 스파이 정찰활동까지도 가능한 비행체로 드론이 인식되게 된 것이다[11].

이러한 드론의 위험성이 극적으로 부각된 또 하나의 사례는 일본총리 관저에 방사능 드론이 발견된 사건이라 할 수 있다. 드론에 설치된 갈색통에 방사성 세슘을 포함하여 총리관저로 날려 보냈던 일본인 40대 남성의 주장대로 '드론 비행중 조종불능 및 조종탈취 등의 상황'때문이라는 주장을 그대로 받아들이지 않더라도, 이런 류의 악의적인 드론 악용상황은 앞으로 얼마든지 발생할 수 있다고 볼 수 있는 것이다.

군사적으로도 '11. 2월에는 이란 핵시설을 정찰중이던 미 드론을 GPS 교란공격을 통해 무단으로 탈취하는 사건이 발생하여 드론 내부 보안 시스템 해킹 후, 촬영 동영상 복원 및 드론을 복제하는데 성공('14년 11월)하는 사건이 발생하기도 한 것 같이, 끊임없이 이어지는 드론과 관련한 위협적인 사례들로부터 드론이 얼마나 위험할 수 있고, 군 조직내 보안을 얼마나 일거에 위협할 수 있는지에 대해 세심한 준비와 대책을 고민하지 않으면 안되는 시점에 이르게 된 것이다.

이러한 국내외 군 및 민간영역에서 드론으로 야기되는 보안위협은 실로 심각할 수 있으며, 무엇보다도 수많은 상업용 드론이 상용주파수 범위내에서 군사시설 상공을 무단으로 점령하고, 이에 대한 적절한 통제와 규제가 확실하지 않을 경우, 기존 군사보안의 개념과 범위로는 대응하기 어려운 새로운 보안위협에 군이 얼마든지 노출될 수 있는 것이다. 드론에 대한 기술적인 해킹시도와 불법비행, 불법적인 군내 핵심시설에 대한 항공촬영 등 드론과 관련한 다양한 가능성들은 군조직내 변화된 보안환경중에서 가장 심대한 변화이며, 대응방안을 고민해야할 가장 핵심적인 분야라고 할 수 있다.

3.2 드론 보안위협의 기술적인 요소

앞서 드론의 구성에서도 잠시 살펴보았으나, 기술집약체인 드론의 시스템은 그 자체로 사이버 취약점을 가질 수 밖에 없는 구조이다[12]. 드론은 운용시스템상 거의 모든 단계에서 기술적으로 해킹이 가능하다고 해도 과언이 아니다. 드론에 대한 기술적인 사이버공격의 형태는 다양한 방법과 루트로 진행될 수 있다.

1)통신채널 통제기(Communication Channel Controller) 공격, 2)원격 통신채널 공략(Communication Channel Telematics), 3)GPS 신호 전파교란 공격(GPS Jamming, Spoofing(스마트 재밍, 기만 재밍)[13], 4)위치기반서비스 취약점(Positioning Channel)[14], 5)채널 센싱(Sensing Channel) 취약점, 6)자이로스코프 주파수 공진을 통한 드론 추락(KAIST, 2015년 8월), 7)소프트웨어 해킹(Software Hacking), 8)드론의 조종권을 빼앗는 '하이재킹' (Hijacking)[15] 등이 그것이다.

이렇듯 드론에 대한 기술적이고도 변화무쌍한 공격들은 예측가능한 Hopping 주기(재밍,통신채널 통제기 공격), 접근가능한 개방형 서비스, 인증이나 암호화 대책 부재(조정기 공략(Controller hijacking), 원격 통신채널 공격, GPS위장, 통신정보 위장, 위치기반 서비스 취약요소 공격), 필터나 증명절차 부재(센서위장(Sensor spoofing), 채널 센싱 취약요소 공격), 기타 정보유출, 악성코드 유입 가능성 상존(소프트웨어 해킹 공격)등이 원인이 되어 가능해진다. 문제는 이러한 드론의 기술적 보안 취약요소들이 한꺼번에 해결될 수 있기 위해선 다양한 기술적인 극복방안과 해결방안이 도출되어야 한다는 것이다. 단순 대응만으로는 이러한 기술적인 위협공격에 온전히 대처할 수 없으며, 기술적인 대응을 기본으로 하고, 더하여 다음에서 논의하는 드론의 불법비행 통제, 드론에 대한 간접적인 통제방법으로서의 드론관련 법규 정비 등과 같은 다각적인 공동대응을 병행해서 고민해야 하는 것이다.

3.3 드론 보안위협의 비행관련 요소(불법비행)

민간 드론의 불법비행실태는 심각한 수준이다[16]. 드

론 비행금지구역에 대한 비행 및 미인가 드론 불법비행이 급증하는 추세이며, 이러한 현상은 군과 군사시설에 대한 민간인의 불법비행 위협과 얼마든지 연계될 수 있다.

또한, 드론의 상용화, 보편화로 민간의 드론 비행신청은 매년 두배 이상으로 급증하는 상태이나 비행승인과 보안조치 인력의 부족으로 인해 적절한 통제없는 비행승인이 이루어질 개연성이 높으며, 비행현장 통제 부실과 적절한 보안조치의 전문화가 미흡한 실정에서 드론의 비행이 무방비로 진행될 가능성 또한 있다. 민간에 대해선 불법 비행의 적발 및 처벌실태 역시 적발자에 대한 미온적 처벌 등으로 처벌율이 상당히 저조한 상태이며, 이는 드론의 불법비행 통제의 어려움과 그 맥을 같이 하고 있다. 문제는 이러한 민간 드론비행의 어려운 난맥상이 군에도 그대로 적용될 수 있다는 것이고, 이에 대한 올바른 대처방안을 고민해야 하는 문제가 가까운 현실속에 자리할 것이라는 데에 있다.

사실 무엇보다 실질적으로 드론의 불법 비행이 증가되고 있는 원인중 하나는 드론에 대한 탐지와 차단이 그만큼 현실적으로 어렵다는 점 때문에 기인한 것일 수 있다. 광활한 하늘에서 점과 같은 드론을 과연 어떻게 탐지할 것인가?의 문제는 분명 쉽지 않은 이슈이며, 그 어떤 선진국도 이에 대해 확실한 솔루션을 가지고 있다고 볼 수 없다. 만일의 경우, 군 역시 이러한 악용 드론 등에 대한 대처방안으로서 군에서 운용하는 감시장비들을 활용하여 드론을 탐지해야 할 수 있는데 음향 탐지, GPS 탐지, 영상 탐지, 열 탐지, 레이다 탐지, 주파수 탐지 등의 방법으로 최대한 대안을 마련하고 있는 상황이지만, 무엇보다도 드론을 차단(예방)하는 진보된 기술인 드론 제어권 탈취(전자파, GPS 재밍 등), 드론 파괴(레이저 총 등)등의 기술적 적용에 보다 관심을 갖고 준비를 해야 할 것으로 판단되어 진다.

3.4 드론 보안위협의 비행관련 요소(항공법 등 제반 법규관계)

드론이 군내부의 새로운 보안위협으로서 정당한 대응방안을 마련할 수 있기 위해 가장 밑바탕에서 지원할 수 있는 조치사항이 바로 드론 비행과 관련한 제반 법체계들을 정비하는 것이다[17]. 드론의 불법비행이든 악성비행이든 제반의 법규정과 지침을 가지고 예방적으로 통제한다면, 지금 현재처럼 난무하는 상업용 소형 드론에 대한 통제와 기타 악성의도를 가진 불법 드론의 비행에 대한 통제에 문제가 없을 것이다. 특히, 항공안전법과 관련한 세부 법적 기반마련은 시급하게 확충되어져야 할 선결과제라 할 수 있다. 물론 드론에 대해 그 운용에 관한 개별적인 규정을 완화하여 기술발전을 도모하는 것이 원칙이겠으나, 사법적인 측면에서의 규정은 그 책임관계를 엄하게 강화하여 균형있는 발전을 이뤄야 함과 동시에 관련 법률을 현실에 부합하도록 법률개정하는 것이 전제가 되어야 함은 명확한 사실인 것이다[18].

또한, 드론과 관련한 법적 기반체계중 드론의 항공촬영과 관련한 부분도 매우 중요한 사안이다. 드론은 사실 비행을 하는 목적자체가 거의 90%이상 촬영을 목표로 하는 것이다. 드론 비행만을 위한 취미비행은 거의 없으며, 통상적으로 드론비행과 더불어 항공촬영이 이루어지게 되는데, 바로 이런 드론의 항공촬영과 관련한 법적 장치가 명확하지 않다는데 보완의 여지가 있다. 항공법이든 군사시설 및 군사기지보호법이든 현재 드론의 항공촬영을 명확하게 적시하여 통제할 수 있는 조항을 보완하여야 한다. 이에 대한 통제의 누수는 바로 군내부 보안의 위해요소로 작용할 수 있으며, 언제든지 군사시설 및 주요 핵심기지에 대한 불법비행과 촬영으로 이어질 수 있는 것이다. 차제에 드론 항공촬영에 대한 제반 법규에 대한 제·개정은 반드시 조치되어져야할 사안으로 판단된다.

4. 드론의 보안관리 대응방안

드론에 대한 보안관리 대응방안은 3가지 측면에서 검토되어져야 한다. 첫째, 불법적인 드론에 대한 물리적 무력화 방안, 둘째, 드론의 사이버 위협에 대한 기술적 극복방안, 셋째, 드론 비행과 관련한 법적·제도적 개선방안 등이다.

4.1 불법 드론에 대한 물리적 무력화 방안

무단 정찰, 감시, 테러 등의 목적으로 악용되는 불법 드론은 공격기술, 보안취약점등을 활용해 격추 또는 무력화시킬 수 있어야 한다. 통상적으로 1)그물을 장착한 드론을 이용하여 불법운용 드론을 포획하는 방안[프랑스 원자력발전소 그물드론 운용('15년), 일본 총리관저 드론 발견이후 그물 이용 불법드론 포획('16년)], 2)독수리를 이용한 드론 단속(네덜란드 '16. 2월), 3)드론킬러를 통한 물리적 충돌후 드론 격추(한국 '15. 10월), 4)미국 보잉社의 레이져 광선을 통한 드론 격추(미국, '15년), 5)미국 바

텔연구소, 드론 GPS기능 전파교란을 통한 드론 무력화(미국, '15년), 6)미국, 프랑스 등 주요 선진국, 군당국과 항공기기술 업체들이 협력해 드론 통합 방어시스템을 구축하는 방안 등이 있다. 이는 고성능 레이더, 카메라 등을 이용해 악용 드론을 신속히 탐지·식별하고, 전파방지장치를 가동해 추락시킬 수 있는 방어 시스템 구축 및 불법 드론에 대한 공격대응 훈련을 진행하는 체계이다.

우리 군역시 적극적인 불법드론에 대한 대응방안으로서 직접 타격 및 전파공격에 의한 물리적 무력화 방안에 대해 논의를 진행해야 할 것이다. 드론에 대한 보안관리 측면에서 가장 직접적인 조치로서 물리적인 무력화 방안은 군에 대한 보안위협에 대한 상징적 조치로서의 역할을 할 수 있는 분야이다.

4.2 드론 사이버 위협에 대한 기술적 극복방안

앞서 검토된 드론의 보안취약점에 대한 기술적인 방어능력이 확보되어져야 한다. 드론의 보안을 취약하게 하는 기술적인 드론운영체계와 S/W상의 보안 위해요소에 대해 기술적 대응이 가능해야 한다. 이와 관련하여 다양한 기술들이 최근 지속적으로 개발되고, 제시되고 있음은 고무적이며, 우리나라도 이러한 기술개발의 흐름과 연계하여 군내 드론 보안관리에 대한 강화된 대응을 수립하여야 한다. 다음은 드론 사이버 위협에 대한 기술적 극복 방안에 대한 것이며, 필수적으로 확보해야할 다섯 가지 선진기술에 대한 것이다.

첫째, 관성항법장치 활용기술은 GPS전파공격에 대한 대응이 될 수 있다. 관성항법장치는 잠수함, 항공기, 미사일 등 자기의 위치를 감지하여 목적지까지 유도하기 위한 장치로서 자이로스코프와 가속도계를 이용하여 이동변위를 구한 다음 처음 위치를 입력하면 현재위치와 속도를 항상 계산해 파악할 수 있는 방법이며, 악천후나 GPS 전파 방해에 현재로선 가장 효과적인 방안이다. 물론 드론에 고가의 관성항법장치를 사용하기 어렵다는 점과 긴 거리를 이동하면 오차가 지속적으로 누적되는 단점이 있지만 드론에 대한 GPS 전파공격발생시 강력한 대응수단임에는 틀림없다.

둘째, GPS 전파방해 공격에 대한 두 번째 대응방안으로서 재밍(Jamming)과 스푸핑(Spoofing)과 관련한 대응기술이다. 이와 관련하여 이스라엘 기업 라드社는 미 국방부 요청으로 정상적 GPS 신호 외에 다른 신호가 유입되면 이를 즉각 걸러내는 드론용 초소형 GPS 공격 대응장치를 개발한 바 있다. 이는 기존 GPS 공격 대응 솔루션이 고가의 가격과 그 크기 때문에 드론 분야 적용에 어려움을 겪고 있는 것에 비해 상당한 가성비와 장착의 용이성을 보장하고 있는 제품이다. 이러한 장치는 정상 GPS 신호 수신이 어렵거나 Spoofing으로 조작되었을 경우 이를 차단하고 자체 신호를 사용하는 홀드오버(Holdover) 기능까지 구비하고 있어, 드론과 관련한 대응기술로서는 기대해 볼 만한 것이라 평가받고 있다.

이에 더한 대응방안으로서 GPS 신호위조(Spoofing)라는 것이 결국 드론에게 신호위조기(spoofer)를 통해 위조된 (위치 및 시각)정보를 제공하여, 정해진 경로를 이탈하게 하거나 정해진 시간에 도달하지 못하도록 하는 행위이므로 이에 대한 대응으로서 GPS 신호에 사용자 인증을 중복으로 추가하고, 인증 불일치시 자동적으로 신호를 제거(독자적 항법체계 보유)하며, 드론의 GPS수신기에서 정상 GPS신호와 기만신호를 비교하여 기만 신호를 제거하는 항재밍 배열안테나의 사용 등도 같은 류의 대응기술로서 그 적용을 고민해 볼 필요가 있다.

셋째, 불법 악성드론에 대한 원격 드론 추적·제어 기술을 확보하여 드론에 대한 자체 통제권을 법적으로 압수하는 기술이다. 이를 위해 드론용 RPS(Radio Positioning System)시스템의 경우, 드론이 비행금지구역에 접근했을 때 자동 착륙시키거나 운영자에게 돌아가게 하는 보호형 지오펜싱(Geofencing) 기능을 사용한다. 4G 모바일 네트워크는 SIM과 기지국을 아우르는 강력한 엔드-투-엔드 암호화 운용네트워크로서, 이를 활용한 RPS 위치 데이터는 GPS 위치 데이터에 비해 해킹과 위조가 어려운 특성이 있다. 무엇보다 드론 제어에 사용하는 데이터 커넥션은 뛰어난 탄력성과 장거리 실시간 피드백 등을 제공함으로써 현존하는 드론 무선 제어 프로토콜보다도 훨씬 더 많은 장점을 자랑하고 있는 것이다[19]. 이런 RPS 시스템은 군내 불법 악성드론에 대한 강제 통제권 인수(압수)방안의 하나로서 적용되어져야 하며, 기술적으로 가장 스마트하고도 가장 효과적인 드론 보안위협관리 기술방안이라 할 수 있다.

넷째, 드론장비의 개발간에 SW 취약점을 이용하여 진행될 수 있는 해킹 등 비인가 접속, 정보유출 등을 유발하는 악성코드 감염 등에 대한 대응기술 확보이다. SW 개발단계에서 보안취약점을 제거하기 위해 시큐어 코딩(Secure cording)[20]과 화이트리스트 기반의 백신을 적용하고 주기적인 보안업데이트를 통한 대응은 사실 드론

으로 기인한 보안의 위협에 대한 가장 기초적인 기술적 대응이 아닐 수 없다.

다섯째, 기존 항공운항 및 방공 관제체계로 운용중인 피아식별시스템(IFF, Identification Friend or Foe)과 육군항공에서 운용중인 헬기위치추적체계 HAPS(Helicopter Auto Positioning System)를 보완하여 민간 드론이나 소형 무인기에 대한 피아식별 및 운용통제가 가능한 통합적인 체계관리 기술의 확보 문제이다. 현재 항공 및 방공 관제체계로는 드론을 포함한 초경량 비행체에 대한 식별 및 통제가 불가능하다고 할 수 있다.

이를 위해 초량비행장치에 대해 사전에 비행을 신고하고, 비행신청과정에서 승인까지 절차적 준수를 강조하도록 항공안전법(시행규칙)에 적시되어 있으나 실제로는 드론 및 초경량 비행장치에 대한 실시간 식별 및 추적이 기술적으로 제한되는 실정이다. 따라서 '드론 식별 및 통제용 모듈(Drone Identification Module)' 도입이 반드시 요구되며, 군 드론의 경우 민간드론이 지방항공청에서 추적 및 관제하도록 하는 것과 달리 중앙방공통제소(MCRC)에서 중앙 추적 및 관제가 가능하도록 통합적인 체계 구축이 시급하고, 더 나아가서는 군내 주요 핵심시설에 대한 민간 상용드론 보안위협에 대한 대응으로서 군 중앙방공통제소에서 민간 드론의 비행과 궤적까지도 실시간으로 추적하고 변화상황을 관제할 수 있도록 군·민 통합 드론통제체계 구축이 결국 군내 드론의 보안위협에 대한 넓은 의미의 국가적 대처방안이 될 수 있을 것이다.

4.3 드론비행과 관련한 법적/제도적 개선방안

드론을 법과 제도적으로 강력하게 통제하는 것은 드론과 관련한 보안관리의 핵심이라 할 수 있다. 따라서, 군내 드론의 통제방안 관련 제반 법률에 대한 제·개정과 제도적 개선은 정책적으로 추진되어져야 하며, 군내 드론에 대한 보안관리에 있어 가장 밑바탕에서 선결되어야 할 과제라 할 수 있다. 이와 관련하여 발전적인 방안을 연구해야 할 부분은 통상 다섯 가지다[21].

첫째, 드론 관련 개인정보 보호에 대한 법률을 신설해야 한다[22]. 드론을 사용한 개인정보 수집 및 무단 촬영 영상의 상업적·악용에 대한 처벌규정이 미비한 상황이며, 향후 드론과 관련한 개인정보위반과 군내 군사보안 위협이 병행해서 진행될 개연성이 높기 때문이다. 이는 드론에 대한 비행통제 법률과도 관련한 문제이나 아무튼 드론을 활용한 불법적인 개인정보 수집에 대한 법률 정비부터 우선하여 추진해야 할 것이다[23].

둘째, 드론비행과 관련한 항공안전법(제23조 등)을 세부적으로 제·개정해야 한다. 우선, 현재 운용되고 있는 드론의 종류와 수준, 성능 등을 무시한 채 단순히 무게 12kg를 기준으로한 규제는 현실적으로 다양한 형태의 드론과 비행상황에 대한 대응에 제한사항이 발생할 수 있다.

비근한 예로 탑재중량이 폭약이나 생화학 탄저균일 경우, 단 1kg의 중량으로도 수만 명을 살상할 수 있다고 한다면, 이정도 무게를 탑재하고 비행할 수 있는 드론의 무게는 10kg 내외만으로도 충분하기에 항공법상의 12kg 기준은 그야말로 현실성이 떨어지는 것이다.

또한 조종사 준수사항만 준수한다면 추가적인 승인 없이도 쉽게 비행이 가능한 상황은 소형드론 통제를 위한 엄격한 기준을 적용하여 개선되어져야 한다. 처벌기준 역시도 모든 불법적 드론 조종사들에게 심대한 경각심을 줄 정도의 수준으로 강화되어야 한다. 조종사 준수사항 위반시 1차:20만원, 2차:100만원, 3차:200만원이라는 미약한 처벌조항은 얼마든지 규제의 사각속에서 드론의 불법비행과 미승인 비행의 양산을 초래할 개연성이 다분하다.

셋째, 항공안전법 제129조, 시행규칙 제310조 속에 드론 비행과 관련한 세부적인 규칙들이 명기되어 있어야 한다. 현재는 표현이나 조항에 구체성이 결여되어 있는 실정으로, 가령 「비행금지시간」은 '일몰후부터 일몰전까지'로 표현되어 명확한 시간이 없고, 「비행금지행위」도 보다 구체적으로 규제사항을 적시해야 하나 다양한 편의해석이 가능할 만큼 모호한 편이다. 각종 통제도 법적규제라기 보다 권고수준의 통제에 불과하며, 비행금지구역이나 관제권 설정 역시 너무 관대하고 악용의 소지가 있는 규정이다. 드론 비행과 관련한 규제수준을 선진국의 그것과 비교해 본다면 드론 관련 세부 규제안 마련이 얼마나 급하고 절실한 일인지 알 수 있을 것이다.

미국은 드론속도에 있어 16km/h 이하 속도로 제한하고, 17세 이상은 연방항공청의 항공기초지식 시험을 통과해야 하며(2년 주기), 연방항공청에서 검사, 시험을 위한 자료 요청이 가능하도록 강력하게 통제하고 있다. 또한 기체신고·등록과 관련하여 우리나라가 자중 12kg초과에 한하는데 반해 미국은 250g 이상 25kg미만의 기체에 대해 미국 연방항공청(FAA)의 드론 등록을 의무화하고 있으며, 이마저 3년마다 갱신하여야 한다. 이를 등록하지

않았을 경우 3,200만원의 벌금형을 부과하는 등 우리나라와 비교하여 강력한 규제와 드론통제를 하고 있다. 미국은 이것도 불충분하다고 생각하여 이것보다 강력한 규제안을 담은 「미국(FAA) 제안 공고(CFR Part 107)」를 통해 입법 진행하고 있는 실정이다.

우리나라도 이제 소형 드론에 대한 통제의 시급성을 인식하여 국내 환경에 적합한 세부 드론법의 제정을 국회차원에서 논의해야 할 시점이 되었으며, 군역시 우선적으로 국가안보와 군 주요시설에 대한 군사보안적인 측면에서 강력한 자체 규정과 세부지침 수립을 서둘러야 할 때라 판단된다.

넷째, 드론과 관련한 또다른 법적 장치로서 드론을 활용한 항공영상 촬영관련 법적 조항의 보완이다. 현재 우리나라는 드론 촬영과 관련한 위반시 제재 방안이 상당히 미흡한 수준이라고 할 수 있다. 일단 드론의 비행자체를 법적으로 통제하는 것은 항공안전법 제129조, 시행규칙 제310조상의 '조종사 준수사항'이다. 여기에 '휴전선, 서울도심 상공 일부 등 국방, 보안상의 이유로 비행이 금지된 곳 비행금지'라는 조항이 있는 것이다. 여기에 더해 드론 항공촬영과 관련한 통제 근거는 국가정보원법 제3조 및 보안업무규정 제37조의 규정에 의한 국가보안시설 및 보호장비 관리지침 제32조, 제33조의 항공사진촬영 보안조치가 주된 것이다.

군내부적으로 보아도 군사보안업무훈령 제97조 (정사진·동사진 촬영 및 레이져 측량)상에 항공촬영에 대한 장성급 지휘관의 승인(허가) 및 보안조치를 하도록 되어 있고, 군 관할공역 내 민간 초경량비행장치 비행승인 업무지침서상의 부록 #1인 항공사진 촬영 지침서가 관련한 세부적인 지침이라고 할 수 있다[24].

우선 드론촬영과 관련한 통제 법적 기반이 국가 보안책임기관인 국정원의 국가정보원법이므로 민간인의 항공 촬영 위반 행위 적발시 강력한 제재에 제한이 있다고 볼 수 있다. 더불어 국정원 지침상 국방부 및 작전부대에 국가보안시설 및 군사보안시설에 대한 항공촬영 승인 및 보안조치를 위임토록 함에 따라 군내부의 제한된 인력과 자산만을 가지고 민간인의 불법적인 드론비행과 항공촬영 전체를 통제하는데 어려움이 있을 수 있다. 항공사진촬영지침서상에 법적인 제재 근거 강화와 통제책임의 명확화, 국가보안시설 및 군사보안시설, 비행장, 군항, 유도탄 기지 등의 국가안보상 핵심적인 군사시설에 대한 촬영금지 조항을 보다 더 강력하게 명기할 필요가 있다. 보다 세부적인 드론과 항공촬영 통제방안이 포함되어 개정되어진다면, 훨씬 더 대응이 원만하게 이루어 질 수 있을 것이다.

더 나아가 군사기지 및 군사시설 보호법, 통합 방위법 내 민간인 군사시설 촬영 제재 방안과 함께 처벌조항이 포함된 법제마련이 필요하며, 초범시 재발방지를 위한 군사 보안위협 가중처벌 등에 대한 조항이 추가된다면 보다 더 경각심을 환기시킬 수 있을 것이다. 민간에서도 드론과 관련한 적지 않은 법익침해(무인항공기의 소유권 침해 또는 불법행위의 문제, 무인항공기 촬영으로 인한 사생활 침해, 개인정보보호법 위반여부, 위치정보법 위반여부 등) 가능성에 대한 형사법적 제제의 성립여부와 그에 대한 입법적 보완 움직임이 있는 가운데 군 역시 보다 강력한 드론 항공촬영과 그와 관련한 군내부 법률 개정을 서둘러야 할 것이다[25].

다섯째, 드론을 통제하고 비행을 승인하는 업무 프로세스 개선과 기타 인력의 보강이 제도적으로 보장되어야 하며, 드론비행과 관련한 보안암호제도의 보강 또한 같이 이루어져야 할 것이다.

특히, 수도권내 수방사의 민간 드론 비행승인관련 인력의 보강 및 수도권 외로 이동하는 악성드론에 대한 지역자체 드론 통제방안은 향후 제한사항이 발생하기 이전에 시급히 우선 조치되어져야 할 사안인 것이다.

제도개선적인 측면에서도 정상적으로 신청하는 드론 비행신청에 대해서는 과감한 업무간소화로 원활한 비행승인을 진행하되, 불법 악용 드론을 통한 불합리한 드론 비행에 대해선 강력한 처벌수단을 통해 제지할 수 있어야 한다.

나아가 드론 제품의 보안적합성검증 제도(안정성 인증제도)를 통해 암호 SW방식 적용 및 평가인증제도(CC 인증), 한국형 암호모듈검증제도(KCMVP)에 대한 강화된 채택이 병행하여 이루어져야 할 것이다.

5. 결론

군이라는 조직의 특성상 군내부 군사보안은 아마도 가장 중요한 우선순위를 가지고 관리되어져야 하는 과제일 것이다. 이런 측면에서 최근 급격한 민간 기술의 혁신과 제4차 산업혁명에 따라 지속적인 군내 보안환경의 변화와 그에 따른 대응방안들이 논의되기 시작하였으며,

대표적으로 1)인원보안적인 측면에서 대거로 유입되고 있는 민간인들에 대한 보안통제 방안, 2)군내부 폐쇄망(국방망)에 대한 외부 선진기술과의 연동접점과 그로인한 사이버 해킹 위협에 대한 극복방안, 3)드론의 군사주요시설 촬영 및 불법정보 수집과 관련한 보안위협 극복방안 등이라 할 수 있다. 특히 무엇보다도 군내부 모든 영역에서 그 활동범위를 넓혀가고, 더욱이 군의 군사작전 영역까지 무기체계화를 진행해 나가는 드론에 대한 보안관리 대책은 그 무엇보다도 중요한 이슈가 되어졌다.

이렇게 광범위한 군내 유입이 이루어지는 드론이 군내 군사보안적인 측면에서는 상당한 위협의 수준까지 내재된 보안 위해요소들을 가지고 있는 것이며, 적절한 대응을 하지 못했을 경우, 심각한 군내 보안사고로 이어질 개연성이 매우 높다고 판단된다. 따라서 드론이 가지고 있는 태생적인 보안의 취약요소들을 검토하고, 해당 분야마다 다각적인 대응방안을 철저히 모색할 때 군내 군사보안에 대한 위협관리가 안정적으로 유지될 것이다. 이를 위해 불법적인 악성드론에 대한 물리적 무력화 방안, 불법적인 해킹과 스푸핑 등과 관련한 기술적 극복방안, 불법적으로 행해질 수 있는 비행과 항공촬영 등에 대한 법적·제도적 개선방안까지 살펴보았다.

이러한 노력들이 중요한 것은 군에서의 보안과 관련하여 사이버해킹 및 드론의 보안위협에 대한 대응은 한 국가의 운명을 좌우할 만큼 중요한 사안이기 때문이다. 무엇보다, 정보통신기술의 급격한 발전과 IT기술의 진보와 함께 제4차 산업혁명의 격동적인 과도기에 있는 우리 군은 무엇보다도 그러한 발전적인 기술의 통합체인 드론과 관련한 보안통제 대책과 보안관리 대응방안을 반드시 수립해야 하는 것이다.

모쪼록 국가와 국민을 보위하고, 국가의 영토와 주권을 수호하는 조직으로서의 군은 그 존립을 담보하는 군사보안과 관련하여, 군에 도전하는 새로운 위협중 가장 강력한 보안위해 요소인 드론에 대한 대응방안들을 수립하여야 하며, 기술의 총아인 드론이 군에 순기능으로 혁신적인 기여를 할 수 있도록 지원해야 할 것이다. 언제나 첨단기술은 활용하되 고삐를 죌 수 있어야 하며, 고삐를 죌 수 없는 기술은 위험한 것이기 때문에 군도 이러한 기술적인 변화의 흐름에 기민하고 역동적으로 운신하여 군내 확고한 보안통제 여건도 확립하고, 군 작전환경의 혁신에도 기여할 수 있는 보안 대응방안을 고민해야 할 때이다.

REFERENCES

[1] S. H. Kim. (2018). *A study on the prevention of terrorism and terrorism by using the drones.* The Master's thesis of The Chung Nam University.

[2] J. M. An. (2006). *The national Informatics*, Seoul : Pakyoun Publishing, p. 194.

[3] S. Pine. (1995). Deficiencies in military counterintelligence: A view from the filed, *International journal of Intelligence and CounterIntelligence, 8(2),* 221-227.

[4] S. Y. Maeng. (May 3, 2017). The hacking of the Military's internal networks. *The Korea defense Daily, p.12* http://kookbang.dema.mil.kr/kookbangWeb/view.do?ntt_writ_date=20170504&parent_no=2&bbs_id=BBSMSTR_000000000003

[5] H. J. Yun. (October 10, 2017). The hacking of the Military's internal networks. *The Sympathy Newspaper. p.8* http://www.gokorea.kr/news/articleView.html?idxno=28 692

[6] S. O. Lee. (2018). A study on the improvement of military drone for defense industry development as a new growth engine. *The Korean Military Academy, 37,* 32. ISSN : 1229-1609

[7] H. C. Mun. (April 3, 2018). The Drone-Bot Combat system for the game changer. *The Financial Nesw. p.22* http://www.fnnews.com/news/201804031217484406

[8] GitHub Introducing Copter. *ArduPilot(Website).* http://ardupilot.org/copter/docs/introduction.html

[9] J. H. Lee. (June 21, 2017). North Korean drones of the Reconnaissance General Bureau, *The Yeonhap News. p.11* http://www.yonhapnews.co.kr/bulletin/2017/06/21/0200000000AKR20170621092451014.HTML?input=1195m

[10] J. Y. An. (January 10, 2018). Annual increase in drone use cases., *The Global Economy Times. p54* http://www.getnews.co.kr/news/articleView.html?ud=2018011015455837514b51928797_16

[11] Y. S. Lim. (2018). *Exploring response of sports safety paradigm change and drone terror threat.* The Master's thesis of The Seong Guen Guan University.

[12] W. H. Kim. (2017). A study on application of drone thchnology. *The Journal of Korea Institute Of Information, electronics, and communication technology.* (2017) 601-608. ISSN : 2005-081X

[13] K. Kim. (2013). Analysis of Anti-Jamming Techniques for Satellite Naviation Systems. *The Journal of Korean Institute of Communications and Information Sciences 38(12),* 1216-1227.

[14] Radionavlab.ae.utexas.edu.(2018)[onilne] Available at:https://radionavlab.ae.utexas.edu/images/stories/files/

papers/drone_hack_shepared.pdf [Accessed 28 Aug. 2018]
[15] J. Reagan. (2018). New Security Hack Seizes Control of Drones. [online] Dronelife. Available at: https://dronelife.com/2016/10/31/new-security-hack-seizes-control-drones/ [Accessed 28. Aug. 2018]
[16] H. Kim. (September 11, 2015). The Urgent measures to deal with the surge of Drone's illegal flights. *The News 1. p.20* http://news1.kr/articles/?2417442
[17] H. S. Um. (August 28, 2018). We nees to fix the law to revitalize the drone industry. *The Security News. p17* https://www.boannews.com/media/view.asp?idx=72469&utm_source=dable
[18] S. M. Kim. (2018). The problems with current legal definitions and commercial operations of drones. *The Korean Journal of Air & Space Law and Policy, 33(1),* 41. KiS3618182, ISSN : 1598-8988
[19] Vodafone.com. (2018). Vodafone to protect the skies with trials of the world's first iot drone tracking and safety technology. [online] Available at: https://www.vodafone.com/content/index/media/vodafone-group-releases/2018/iot-drone-tracking.html [Accessed 28. Aug. 2018].
[20] En.wikipedia.org. (2018). Secure coding. [online] Available at: https://en.wikipedia.org/wiki/secure_coding [Accessed 28 Aug. 2018]
[21] H. S. Lee. (2018). A study on Revision of Korean Aviation Act concerning drones. *The Korean Air Management Association,* 225-230. KiS3618182, ISSN : 1598-8988
[22] C. S. Kim. (2016). A drones and criminal law. *The Chung-Ang Law Association.* ISSN : 1598-558X
[23] Y. H. Kim & K. H. Lee. (2017). A legislative proposal to prevent the infringement of privacy and to solve operational preblems by drones. *The Journal Korea Institute Of Information Security And Cryptology,* 1141-1147. ISSN : 1598-3986
[24] J. H. Lee. (February 21, 2009). The Department of Defense, The state department with a aerial photography, *The Yeonhap News. p.3* https://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=100&oid=001&aid=0002514587
[25] K. H. Jung. (2017). The criminal issue of filming using unmanned aerial vehicles(drone)-focusing on personal information protection act violation or positional information violation. *The KHU Global Corporate Law Review(10-2),* 101-127.

김 두 환(Kim, Doo Hwan) [정회원]

- 1998년 2월 : 금오공대 기계공학과(공학사)
- 2013년 2월 : 건양대학교(행정학석사)
- 2016년 3월 ~ 현재 : 건양대학교 대학원 박사과정 재학
- 관심분야 : 군사보안, 군조직보안, 정보보안, 보안위협, 군보안
- E-Mail : highmt2015@daum.net

이 윤 환(Lee, Youn Hwan) [정회원]

- 1982년 2월 : 충남대학교 법학과(법학사)
- 1985년 2월 : 충남대학교 법학과(법학석사)
- 1993년 3월 : 충남대학교 법학과(법학박사)
- 1993년 3월 ~ 현재 : 건양대학교 국방경찰행정학부 교수
- 관심분야 : 인권, 정주 외국인 참정권
- E-Mail : lyh@konyangr.ac.kr