

2020 vol.3

KISA 한국인터넷진흥원  
KOREA INTERNET & SECURITY AGENCY

# KISA REPORT

# CONTENTS

## ISSUE

- 01 사회적/물리적 거리두기가 IT 산업과 사회에 미치는 영향과 주요 이슈  
[한상기/ 테크프론티어 대표]
- 02 감염병예방방법의 정보공개 규정 살펴보기 - 공공의 건강 및 안전, 그리고 프라이버시의 균형  
[이진규/ 네이버주식회사 개인정보보호책임자(이사)]
- 03 원격근무, 회사를 떠나 일한다는 것  
[최호섭/ 디지털 칼럼니스트]
- 04 코로나19 확산에 따른 비대면 원격수업에 대한 단상  
[윤대균/ 아주대학교 소프트웨어학과 교수]
- 05 비대면 협업툴의 미디어적 필수 요건에 대하여  
[최홍규/ EBS 연구위원]
- 06 코로나19가 앞당긴 원격 사회 이후 사이버 대피 공간을 위한 가상현실의 역할  
[최필식/ 기술작가]

## TREND

- 07 RSAC 2020 - 보안 트렌드 살펴보기  
[송혜인/ 한국인터넷진흥원 보안산업단 해외사업팀장]
- 08 연합학습으로 AI 빅브라더 문제 해소  
[유성민 /IT 칼럼니스트]
- 09 미국과 영국의 드론 대응(Ant-drone) 정책 및 전략 추진동향  
[이응용/ AI&security 애널리스트]
- 10 중국 “네트워크 안전등급 보호 제도” 개요 및 관련 국가표준 제정 동향  
[정연수/ 한국인터넷진흥원 연구위원]
- 11 광주의 미래 - 인공지능 기반 산업융합 집적단지 조성사업  
[나종희/ 광주대학교 컴퓨터공학과 교수]
- 12 미래인터넷 기술 성공의 핵심 포인트, 보안  
[김대엽/ 수원대학교 정보통신학부 교수]

## KISA 주요 활동 안내

- 01 민간 500대 웹사이트 플러그인 개선 실적 및 웹 표준 전환 지원사업 안내
- 02 개인정보보호 국제협력센터 안내

KISA Report의 내용은 한국인터넷진흥원의 공식 견해와 다를 수 있습니다.

주제 제안 및 정기 메일 신청 | [kisareport@kisa.or.kr](mailto:kisareport@kisa.or.kr)

인터넷 정보보호 관련 이슈, 현안 등 궁금한 내용을 보내주시면 선별 후 보고서 주제로 선정됩니다.

또한, KISA Report 온라인 서비스 제공을 원하실 경우 신청해주시면 매월 받아보실 수 있습니다.

## 미국과 영국의 드론 대응(Ant-drone) 정책 및 전략 추진동향

이응용 (david9631@gmail.com)

AI&security 애널리스트

무인 자율비행체, 즉 드론은 이전에는 국방 등 군사 목적 등에서 이용되었으나, 최근 저가의 일반용 드론의 보급 확산에 따라 일상화되고 있다. 드론은 20년 넘게 존재해 왔으며, 심지어 최초의 드론은 미국과 프랑스가 자동무인 항공기 개발에 참여한 1차 세계대전때까지 거슬러 올라갈 수 있다. 그러나 지난 몇 년간 산업 전반에서 드론 이용 확대, 일반인들의 레저용 드론 이용 확산 등으로 인식의 측면에서 드론이 매우 중요해졌다. 드론은 다양한 행태가 발전해왔으며, 최근 인공지능, IoT 등 ICT 기술과 융합하면서 지능화 및 고도화되면서 전 세계적인 관심과 활용이 급증하고 있다.



드론 유형 [출처:regimage.org]

전 세계 기업들은 드론 제품 생산에 진입하고 있으며, 기업들은 드론을 이용해서 상품을 배달하거나, 농약 살포, 경찰, 감시 등 다양한 목적에서 사용을 준비하면서 드론의 활용은 지속 증가할 전망이다.

반면, 드론의 활용은 잠재적인 산업적 기회를 제공하는 반면, 드론의 악의적 이용에 따른 위험으로 물리

적 보안 및 사이버보안 영역에 중대한 영향을 끼칠 것으로 예상하고 있다. 2019년에 이란은 미국의 드론을 공격해서 파괴함으로써 전 세계적 관심을 촉발한 바 있다. 이란은 정치적으로 민감한 호르무즈 해협에서 미국의 감시 드론을 격추하면서 이란은 미국 간의 새로운 차원의 긴장을 촉발했다.<sup>1)</sup> 올해 1월 미국은 드론을 이용해서 적대자가 탑승한 차를 공격해서 암살함으로써 전 세계를 깜짝 놀라게 하였다. 미국 국방부는 비밀정보원, 이란 정부 통신시설에 대한 도청, 비밀 감시 장비 등을 통해 솔레이마니의 움직임을 파악하여 국방용 드론일 활용한 미사일로 솔레이마니 차량에 대해 미사일 공습을 통해 암살에 성공했다. 전 세계적으로 비행장에서 드론의 비행기 충돌 사고, 드론의 악의적 이용이나, 무분별한 오남용 등 다양한 안전사고도 빈번히 발생하고 있다.

국내외에서 드론의 활용에 따른 개인의 사생활 침해도 위협받고 있다. 드론에 장착하는 카메라 기술이 발전하면서 드론의 이용하여 타인의 사생활을 노출할 수 있는 위험도 준비하고 있다. 또한 드론의 오작동으로 인해 충돌을 일으킬 수도 있고, 안전사고로 이어질 수 있다. 이러한 안보 위협, 안전위협, 사생활 침해 등 드론의 활용 증가에 따른 이슈가 광범위하게 확대되면서 드론 대응을 위한 방안으로 안티드론(Anti-Drone), 카운터 드론(Counter-Drone), 카운터 무인항공시스템(Counter Unarmed Aircraft Systems) 등 다양한 용어들이 등장하고 있다. 본고에서는 드론 대응으로 통일해서 사용하고자 한다.

최근 인공지능을 이용한 자율이동체에 대한 인기가 폭증하면서 드론의 성장 가능성에 대한 기대가 한층 고조되었다. 기존에는 주로 군사적 측면 또는 산업적 측면에서 개발되는 지상에서는 자율주행차, 수상에서는 자율선박, 상공에서는 무인비행체(드론)가 인공지능의 급속한 발전에 따라 많은 사람의 관심이 증폭하며 상용제품 시장 성장을 견인하고 있다.

드론 시장은 국방용, 산업용, 배달용 등으로 활용되고 있으며, 현재는 국방용 드론 분야가 최대 규모이지만 앞으로는 배달용 드론, 산업용 드론 등 대중의 접근이 용이한 드론 시장이 급신장하고, 드론의 대중화가 가속화될 전망이다.

글로벌 드론 시장 전망

구분	2020(E)	2025(E)	연평균성장율(CAGR)
국방용 드론	~50억	~75억	~7%
배달용 드론	<10억	~50억	~60%
산업용 드론	~15억	~150억	~50%
총계	~80억	>250억	~30%

[출처:US Equity Research<sup>2)</sup>]

드론 활용의 증가와 더불어 국가안보, 치안 등의 측면에서 드론의 위협에 대한 인식이 확산하면서 드론 대응에 대한 논의가 활발해지고 안티드론 시장도 새롭게 형성되고 있다. 시장조사기관인마켓앤마켓은 글

1) <https://time.com/5611222/rq-4-global-hawk-iran-shot-down/>  
2) US Equity Research, Aerospace and Defense, 2020.1.22.



로벌 안티 드론 시장이 2018년 약 4.99억 달러에서 2024년 22.76억 달러로 연평균 28.5%로 성장할 것으로 전망하였다.<sup>3)</sup> 최근 이란의 미국 드론 격추, 미국의 드론을 이용한 적대자의 암살 등으로 인해 주요 국과 기업들의 안티드론 시스템에 관한 관심과 투자가 더욱 촉발된 상황을 고려하며, 드론 대응 시장은 더욱 확대될 수도 있다.

주요국 중에서는 미국이 국방부를 중심으로 다양한 드론을 개발해서 운용하고 있고 안티 드론에도 적극적이다. 국내의 경우 방산 기업인 한화시스템이 드론 감시 레이더 센서 개발 작업을 추진하고 있다. 이 사업은 한국전자통신연구원(ETRI) 주관으로 2021년까지 사업비 120억 원이 투입될 예정이다.<sup>4)</sup>



한화시스템의 안티 드론 솔루션 개념도[출처: uasvision.com]

미국에서는 이전부터 드론을 전투 목적에 개발을 지속했으며, 적대자들의 드론 공격에 대응하기 위한 전략을 국방부 등을 중심으로 추진해왔다. 특히 작년 말에는 드론 대응을 위한 법률이 입안되어 추진되고 있으며, 법률의 진행 상황에 따라 미국의 사이버안보를 담당하는 국토안보부(DHS)를 중심으로 드론 대응 방안을 마련하고 있다, 또한 미국 국방부는 이전부터 전투 목적으로 드론을 개발하여 활용해왔으며, 최근 드론 위협이 증가함에 따라 드론 대응 전담 조직을 신설을 추진하고 있다.

영국에서는 드론의 악의적인 이용에 따른 우려가 커지면서 드론 위협 대응의 중요성을 인식하고, 정부 차원에서 드론 대응을 위한 연구를 진행하고, 영국 최초로 2019년 말 드론 대응 전략을 수립하였으며, 향후 드론 대응 전략에 기반을 두어 이 분야에 대한 투자를 확대할 계획이다.

이에 본고에서는 정부 차원에서 드론 대응에 적극적인 미국과 영국의 드론 공격 대응 전략을 중심으로 살펴보고 정책적 시사점을 도출하고자 한다.

3) Market and Market, Anti-Drone Market by Technology (Laser, Kinetic, and Electronics), Application (Detection, Detection & Disruption), Vertical (Military & Defense, Homeland Security, and Commercial), and Geography – Global Forecast to 2024.

<https://www.marketsandmarkets.com/Market-Reports/anti-drone-market-177013645.html>

4) [https://biz.chosun.com/site/data/html\\_dir/2019/02/25/2019022500147.html](https://biz.chosun.com/site/data/html_dir/2019/02/25/2019022500147.html)

## 미국의 드론 대응 정책 및 기술개발 추진동향

### 국토안보부(DHS) 추진동향

2019년 10월, 국토안보부 하원위원회는 드론 대응 관련 법안으로 DHS 무인항공체대응조정법(DHS Countering Unmanned Aircraft Systems Coordinator Act: H.R. 3787)을 입안했다. 이 법안은 DHS가 관리 중 한 명을 지정하여 드론의 위협에 대처하기 위한 각 부처의 활동을 조정하도록 규정한다. 이 법안의 주요 내용은 다음과 같다.<sup>5)</sup>

1. 조정관(Coordinator, 코디네이터): 국토안보부 장관은 시민권리 및 시민자유실, 개인정보보호실 및 기타 관련 연방기관 등 부처 관련 조직과 무인항공체(UAS: Unmanned Aircraft Systems, 이하 드론<sup>6)</sup>)의 위협에 대한 정책과 계획을 협력하여 개발하기 위해 조정관(Coordinator)을 지정해야 한다. 조정관은 다음의 업무를 수행한다.
  - 테러 공격에 사용될 수 있는 드론 대응
  - 드론 대응 기술 연구 및 개발 촉진
  - 드론 위협 대응과 관련된 정보 및 지침의 보급 보장
  - 연방, 주, 지방 및 부족의 법 집행기관과 민간부문의 UAS 대응과 관련된 부처의 연관 역할을 수행
  - 국토안보부 장관의 지시에 따라 관련 드론 활동 수행
2. 관련 연방법과의 조정협력: 조정관은 다른 직무 이외에도 드론을 식별, 평가 또는 물리치는데 사용되는 시스템이 관계 법령에 따라 수행하기 위해 관계 부처 및 부서 및 기타 관련 연방기관과 적절히 협력해야 한다.
3. 민간 부문과의 조정협력: 조정관은 협력계약실, 기타 관련 부처 조직, 기타 연방기관과 협력하며, 드론 대응기술을 민간부문에 정보(특히 드론 대응기술이 합법적인 민간 부문 서비스 또는 시스템에 영향을 미칠 수 있는 경우에 관한 정보 제공)를 보급하는데 있어서 부처의 주요 책임자 역할을 수행해야 한다.

드론 대응 관련 국토안보부에 임무를 부여하는 하원의 최신 법안 등에 따라, 국토안보부는 드론 대응체계 마련을 위한 연구 등 준비 작업을 진행 중이며, 드론 관련 위협요소, 간략한 대응 지침 등을 제공하고 있다.<sup>7)</sup> 국토안보부는 드론 관련 위협을 다음의 4가지 유형을 요약해서 정의하고 있다.

5) H.R. 3787, DHS Countering Unmanned Aircraft Systems Coordinator Act;  
<https://www.cbo.gov/publication/55954>

6) 미국의 법률 및 국토안보부의 보고서 등에서는 UAS 용어를 사용하고 있으나, 본고에서는 동일한 의미로 사용되는 경우에는 가능한 드론으로 용어를 통일해서 사용

7) <https://www.cisa.gov/sites/default/files/publications/uas-ci-challenges-fact-sheet-508.pdf>

- 무기화 또는 비밀 운송(Payload): 드론이 밀매품, 화학물질 또는 기타 폭발성, 무기제품 등을 운송
- 금지된 감시 및 정찰: 드론이 악의적 목적으로 하늘에서 넓은 지역을 자동으로 모니터링
- 지적재산권 도난: 드론을 사용하여 영업 비밀, 기술 또는 민감한 정보 도용과 관련된 사이버 범죄를 수행
- 의도적 중단 또는 괴롭힘: 드론이 타인의 개인정보를 침해하거나 침해하는 데 사용

국토안보부는 드론이 주요기반시설에 대한 위협요소로 작용하므로 드론 대응이 중대하다고 강조하였다. 미연방 항공국(FAA)은 미국에서 드론 사용이 비용 효율적이고 다재다능한 국가 안보 및 기업 보안 도구로 사용되고 대중적인 레크리에이션 취미활동이 기기로 사용이 확대되고 있으며, 미국에서 전체 취미 및 상업 드론 판매를 합해서 2016년 250만대에서 2020년에는 700만 대로 급증할 것으로 예상하고 있다. 이에 따라 향후 드론 관련 잠재적 위협이 지속적으로 증가할 것으로 예측하였다. 그러나 드론의 물리적 및 운영적 특성으로 인해 종종 주요기반시설 운영자들의 탐지를 벗어나 중대한 문제를 일으킬 수 있음을 동시에 지적하였다.

국토안보부는 연방, 주 및 지역 규제 요건을 충족하는 보안 모범사례를 탐색하고, 구현하는 것이 드론 관련된 잠재적인 보안 사고를 성공적으로 관리하는 데 중요하다고 강조한다. 국토안보부는 드론 관련 보안 문제를 해결하기 위해 수행할 수 있는 조치사항으로 다음사항들을 제시하였다.

- 법적으로 승인된 드론 대응기술을 연구하고 구현
- 시설 주변의 공중 영역을 파악하고, 보안 강화 조치를 취할 권한이 있는 담당자를 파악
- 고정된 현장설비의 근거리에서 드론 제한사항을 고려하기 위해 미연방항공청(FAA)에 문의
- 드론 보안 및 대응 전략을 추가하기 위해 비상 및 사고 조치 계획 개정
- 모범사례 및 정보공유를 위해 연방, 주 및 지역 파트너십 구축
- 잠재적인 드론 위협에 대해 지역 법 집행기관에 보고

국토안보부의 과학기술국(Science and Technology Directorate)에서는 드론 대응을 위한 솔루션으로 CUAS(Countering Unmanned Aircraft Systems) 프로그램을 추진하고 있다.<sup>8)</sup> 국토안보부의 이니셔티브 주도 하에 과학기술국은 정보분석국(I&A), 정책실 등과 드론 위협을 해결하기 위해 협력하고 있다. DHS의 과학기술국은 관련 부서와 협력하여 부처 수요와 요건에 의거하여 CUAS를 구매하고, 활용할 수 있도록 하기 위해 CUAS 솔루션을 평가하기 위한 방법을 개발하고 있다.

국토안보부는 CUAS 프로그램의 전략적 목표를 다음과 같이 제시하고 있다.

1. 국토안보와 관련된 기업들이 최신 기술에 대한 조언을 받고 CUSA 솔루션에 쉽게 접근할 수

8) DHS Science and Technology Directorate, Countering Unmanned Aircraft Systems; <https://www.dhs.gov/sites/default/files/publications/Counter%20UAS%20Factsheet.pdf>

있도록 지원

2. 긴급한 격차를 해결하기 위한 빠른 대응 능력을 보장
3. 미래의 위협을 해결하는 역량 보장

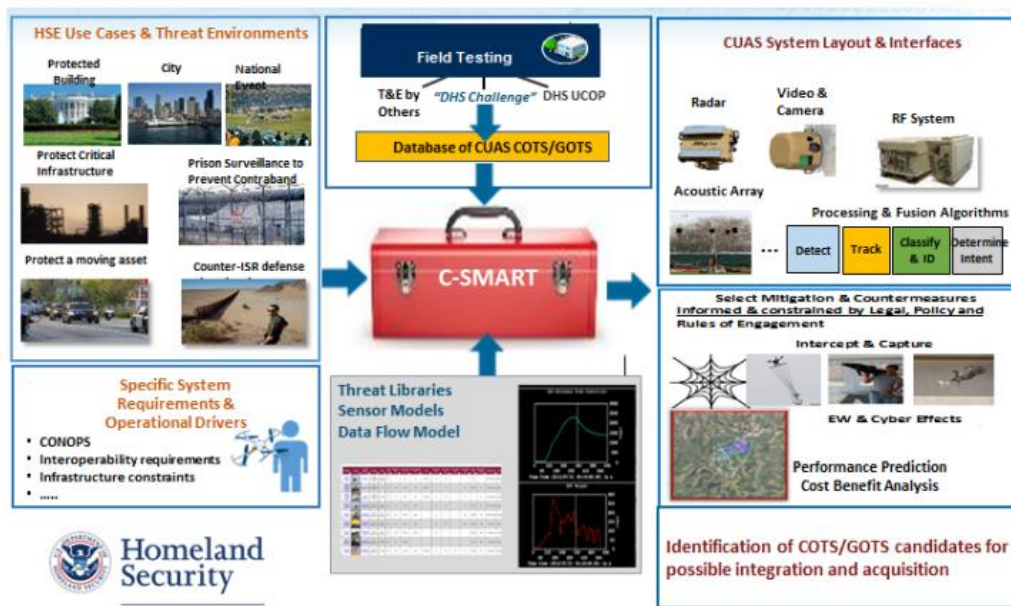
국토안보부의 과학기술국은 CUAS 프로그램의 전략적 목표를 달성하기 위해 CUAS 기능지원 및 검토 툴킷(CSMART)을 개발하여 운영사업자, 국경보호국, 미국비밀정보국(U.S. Secret Service), 국가보호계획국(National Protection and Programs Directorate), 미 연방항공청(FAA), 주 및 지역 법 집행기관들에게 기술이전 및 조달 지원을 제공할 수 계획이다.

과학기술국은 CSMART와 해당 애플리케이션을 국토안보부에 적용하여 지식자원 센터로서의 역할을 수행할 계획이다. C-SMART는 특정 작업에 대한 C-UAS 보안상태를 분석하고 계획하는 활동을 지원하는 컴퓨터 모델, 데이터베이스 및 분석 도구들의 모음이다. 이 기능을 통해 국토안보부의 협력기관들은 부처의 드론 담당 부서를 활용하여 C-UAS 위협을 이해하고 보안준비를 개선할 수 있을 것이다.

드론의 위협에 대응하기 위한 과학기술국은 다음 활동을 역점적으로 추진할 계획이다.

- CSMART 개발: C-SMART, 컴퓨터 모델, 데이터베이스 및 분석 도구를 사용하여 DHS 고객인 상용제품(COT) 및 정부제품(GOT)을 사용하여 특정 작업에 대한 CUAS 기능을 도입할 수 있도록 지원
- 시험 및 평가: DHS 데이터베이스에 포함시키기 위해 CUAS 상용 및 정부제품을 정량화함으로써 C-SMART의 모델링 및 시뮬레이션 구성요소에 대한 검증, 운영시험 시스템 선정, 시험 방법, 데이터 수집 및 형식을 표준화 등
- CUAS 운영 테스트베드 및 프로토타입 평가: 선정된 인프라에 대한 실시간 CUAS 기능 시험 (1 단계로 현재 도입된 이중 센서를 모두 통합하고, 이용자들에게 제품을 배포하며, 기관 간 아키텍처 및 표준 제정 등을 수행하고, 2 단계로 미래 위협 시나리오 대한 시뮬레이션 검증 등 수행)
- 신속한 대응 역량 확보: 긴급한 수요에 대응하기 위해 상용기술 및 미래기술을 수요에 맞추어 통합하고, 테스트 및 분석 기능과 비즈니스 프로세스를 통해 수요처의 운영 환경에서 새로운 장비를 신속하게 평가할 수 있도록 지원
- 미래의 위협: 기술 발전에 따른 미래위협을 예측, 특성화 및 평가





C-SMART 체계도 [출처: DHS]

#### 국방부(DoD) 추진동향

드론 대응 기술은 미국 국방 분야에서 최우선 과제가 작용한다. 2019년 미국 국방 및 정부 발전 연구소의 “DOD의 C-UAV 전략”에 따르면 미국은 드론 대응(UAV) 솔루션에 약 9억 달러를 지출한 것으로 알려졌다. 국방부는 2020 회계 연도에 드론 대응 솔루션을 보다 광범위한 프로그램에 통합하기 위해 5억 달러를 요청했다고 밝히고 있다. 국방부는 인공지능에 기반한 드론 대응 시스템도 개발 중이며, 완전한 자율인공지능 중심의 드론 솔루션은 아직은 계획 단계에 있는 것으로 알려졌다.<sup>9)</sup>

미국의 국방부(DoD)의 최고 무기 조달자는 2020년 1월 국방부는 곧 육군이 주도할 드론대응실을 설립할 계획이라고 밝혔다.<sup>10)</sup> 국방부 지도자들은 최근 육군을 드론 대응 기술의 집행조직으로 지정하기로 했으며, 새로운 드론대응실은 버지니아 주 알링턴에 60명의 직원으로 구성될 것이라고 밝혔다. 적대자들의 드론 공격에 대응에 대해 오랫동안 국방부의 관심목표였으나, 지난해 9월 사우디 아라 마코 시설에 대한 이란의 공격, 이란의 미국 드론 공격 등 최근의 주요 사건들로 인해서 국방부는 드론 대응에 관한 관심을 높아진 상황에서 이번의 드론 대응조직의 신설을 계기로 작용한 것으로 판단된다. 국방부의 관리자는 산업 기반 측면에서, 드론 대응은 구매 및 유지관리실의 마이크로일렉트로닉스, 5G 네트워크, 초음속기기와 함께 4가지 핵심 분야 중 하나라고 지적하였다.

9) <https://i-hls.com/archives/97191>

10) National Defense, JUST IN: Defense Department to Stand Up New Counter-Drone Office, 2020.1.14

## 영국의 드론 대응 전략 수립

2018년 크리스마스 동안 영국의 가트윅(Gatwick) 공항에서의 드론 파괴로 인해 수만 명 시민의 여행을 중단시켰고 수천만 파운드의 경제적 손해를 입은 것으로 파악되면서 영국은 악의적인 드론 이용에 대한 경각심이 고조되었다. 이에 따라 영국은 선도적으로 드론 공격에 대응하기 위해 정부의 포괄적이고 체계적인 접근 방법으로써, 기술 혁신과 법률, 규제 및 교육 등을 종합적으로 고려한 방안을 구상해왔다. 2019년 10월 영국 정부는 그동안의 연구를 기반으로 영국의 국가안보 및 주요 국가기반시설 위협 등 드론의 악의적 이용에 따른 위험을 완화하기 위한 전략으로 영국 무인항공기대응전략(UK Counter-Unmanned Aircraft Strategy<sup>11)</sup>: 이하 드론 대응전략)을 발표하였다.

동 전략에서 영국은 악의적인 드론 이용에 대비하여 드론 개발자들의 보안취약점을 고려해야 하며, 합법적으로 보안취약점을 완화하는 방법에 대한 고려가 필요하며, 바람직한 드론의 발전을 위해 역기능에 대한 기술적 대응책, 그리고 적절한 규제체계가 동시에 필요함을 강조하였다. 이 전략에서는 드론의 악의적 사용을 해결하기 위한 전략목표와 대응방법에 제시하였으며, 진화하는 보안요구 사항을 충족하기 위해 산업계와의 협력을 강조하였다.

영국의 드론 대응전략은 드론의 악의적 이용으로 인해 예측되는 고위험을 감소시키기 위한 다음의 4개 목표를 설정하였다.

1. 드론의 악의적이고 불법적 이용으로 초래하는 진화하는 위험에 대한 포괄적인 이해 제고
2. 드론의 남용을 저지하고 억제, 탐지, 분쇄하기 위해 총괄적인 접근
3. 드론 제품이 최고수준의 보안 표준을 충족하도록 산업계와 강력한 관계 구축
4. 드론 대응(Counter-drone) 기능의 이용, 효과적인 입법, 교육 및 지침을 통해 경찰 및 기타 운영 대응조직의 권한 강화

영국의 드론 대응전략은 4대 상위 목표별로 전략을 제시하였으며, 주요 내용은 다음과 같다.

영국 드론 대응 전략의 주요 목표 및 전략

전략목표	세부전략
종합적인 위험 이해	① 드론의 위협, 영향 및 취약성에 대한 이해도를 개선하여 포괄적이며 최신 위험 상황(risk picture)을 파악 ② 진화하는 위험을 예측하기 위한 수평적 검토 ③ 위험상황 정보를 수요자에게 전달
위험을 해결하기 위한 단대단(End-to-End) 접근법	① 사용가능한 모든 도구를 활용 ② 불법 드론 이용을 보다 쉽게 식별 가능하도록 조치

11) HM Government, UK Counter-Unmanned Aircraft Strategy, 2019.10

드론 대응 기술, 테스트, 산업계	① 영국의 보안 요구사항을 드론 대응(Counter-drone) 산업에 알림 ② 영국 정부의 요구사항을 충족하도록 드론대응 산업에 인센티브를 제공하고 요구사항을 충족하도록 촉진 ③ 산업계에서 개발하는 드론 대응 솔루션 평가 및 보장
효과적인 운영 대응 활성화	① 운영 대응조직이 행동 시간과 방법을 알 수 있도록 보장 ② 계층화되고, 상호보완적인 드론 대응 방어에 대한 이용 촉진 ③ 효과적인 대응을 위해 적절한 권한 부여

[출처:HM Government]

영국 정부는 악의적인 불법 드론 사용으로 인한 위험을 줄이려면 시간, 재정, 인력을 투입하고, 적극적인 투자가 긍정적인 혜택을 제공할 수 있도록 노력할 계획이다. 이를 위해 영국 정부는 드론 대응 전략 추진 기간 동안 성과를 평가하고, 이 전략의 수행을 추적하기 위해 새로운 성과측정 방법을 개발할 계획이다. 영국정부는 정기적인 검토를 통해 드론 보안에 대한 투자의 균형을 재조정할 방법을 결정함으로써 하고 영국이 드론 기술을 비즈니스와 사회에 통합함으로써 긍정적 혜택을 유도할 계획이다. 영국정보는 드론 및 안티드론 기술의 빠른 진화 특성으로 인해 3년 내 드론대응전략을 전략을 재검토하고, 필요할 때 수정해 나갈 계획이다.

## 정책시사점

드론의 사회경제적으로 다양한 편익을 제공할 수 있는 무한한 가능성을 제공할 수 있다. 그렇지만 드론으로 인한 공격은 사이버 기술의 발전과 함께 융합된 형태로 진화되고 있다. 드론 관련 물리적 위협과 사이버위협이 통합된 형태로 발전함에 따라, 융합보안 차원에서 드론 대응 방안 준비할 필요가 있다.

미국, 영국 등은 드론 개발에 투자뿐만 아니라 드론의 악의적 이용에 대한 위험을 예측하고, 선제적으로 국가 차원에서 드론 대응을 위한 전략 개발을 개발하고, 드론 대응시스템을 개발하고 있다.

우리나라에서도 안티 드론 시스템 개발 등에 일부 기업들이 참여하고 있으나, 아직은 국가적으로 드론 대응에 대한 정책과 정책을 미흡한 상황이다. 국내에서 드론의 활용이 증가하고 있고, 드론의 악의적 이용에 따른 안전사고, 사생활 침해 등의 문제가 발생하고 있고, 향후 드론을 이용한 적대적인 공격의 증가가 예상되므로 이에 대한 대책을 선제적으로 준비할 필요가 있다. 특히 다양한 기술을 융합되고 인공지능 기술이 적용된 형태로 발전할 것으로 예상되므로, 드론 대응을 위해 국방부, 과학기술정보통신부 등 다양한 산업관련 부처 및 규제 관련 부처, 산업계, 학계, 시민단체 등의 다양한 이해관계자들이 참여하는 종합적인 드론 대응 대책을 마련할 필요가 있을 것이다.

또한 안티드론 관련 산업도 급증할 것으로 예상됨에 따라 안티드론 관련 기술을 개발하고, 상용제품을 개발하여 국제적인 경쟁력을 확보할 필요가 있다. 국내 사이버보안 업체 중에 글로벌 상위 기업이 존재하지 않는 상황에서 드론 융합보안 분야에 대해 선제적인 기술개발 및 상용화를 통해 성장하는 융합보안 산업에서 경쟁력을 확보하고, 다양한 스타트업을 양성할 수 있는 기회로 작용할 수 있을 것이다.

아울러 일반인들이 드론 이용이 증가함에 따라 드론 활용에 따른 타인의 사생활 침해, 안전사고 등의 문제가 확산하지 않도록 일반 이용자에 대한 인식제조를 위한 가이드라인, 드론 개발 시 안전장치의 탑재 등에 대한 지침 등을 개발 및 보급할 필요가 있다.

#### [참고문헌]






1. US Equity Research, Aerospace and Defense, 2020.1.22.
2. Market and Market, Anti-Drone Market by Technology (Laser, Kinetic, and Electronics), Application (Detection, Detection & Disruption), Vertical (Military & Defense, Homeland Security, and Commercial), and Geography - Global Forecast to 2024.
3. H.R. 3787, DHS Countering Unmanned Aircraft Systems Coordinator Act
4. DHS Science and Technology Directorate, Countering Unmanned Aircraft Systems
5. National Defense, JUST IN: Defense Department to Stand Up New Counter-Drone Office, 2020.1.14.
6. HM Government, UK Counter-Unmanned Aircraft Strategy, 2019.10



## < KISA 주요 활동 안내 >

### 민간 500대 웹사이트 플러그인 개선 실적 및 웹 표준 전환 지원사업 안내

#### □ 플러그인이란?

- (정의) 보안, 결제, PC제어 등 웹 브라우저\*에서 지원하지 않는 기능을 사용하기 위해 PC에 설치하는 별도 프로그램(액티브X, 실행파일 등)
  - \* 이용자가 PC, 스마트폰 등에서 웹사이트를 볼 수 있게 해주는 응용프로그램으로  인터넷 익스플로러(IE),  크롬,  파이어폭스,  사파리,  오페라 등 종류 다양
- (용도) 인터넷에서 **이용자 편의 서비스**(결제, 금융이체 등)나 **보안 서비스**(공인인증서, 보안3종(키보드보안, 백신, 방화벽)) 등을 제공

#### □ 플러그인 개선 필요성

- ① (국민 불편) 웹사이트 접속 시 플러그인을 설치해야 하고, 이 과정에서 여러번 웹 브라우저가 재시작 되면서 국민 불편 초래
- ② (보안성) 다양한 웹사이트의 플러그인 강제 설치에 따라 생긴 이용자의 무의식적인 설치 습관으로 인해 악성코드 유포 등의 경로로 활용
- ③ (플랫폼 종속) 실행파일은 다양한 웹브라우저(크롬, 사파리 등)에서 동작하는 반면, 액티브X는 MS社 웹브라우저인 인터넷익스플로러(IE)에서만 동작

#### □ 민간 500대 웹사이트(국민 83% 이용) 플러그인 개선 실적

- (플러그인 수) '17년 대비 **액티브X 82.3% 감소**, **실행파일 81.8% 감소**

구 분	'17년	'18년	'19년
액티브X 개수	810개	510개 (△37.0%)	143개 (△82.3%)
실행파일 개수	1,456개	290개 (△80.1%)	265개 (△81.8%)
합 계	2,266개	800개 (△64.7%)	408개 (△82.0%)

#### < 플러그인 개선 방향 >

- ◆ (액티브X) 웹 표준 등 솔루션으로 대체하여 제거 ⇒ '19년말까지 82.3% 제거
- ◆ (실행파일) ▲웹 표준 솔루션으로 대체 가능한 것은 제거, ▲불가능한 것\*은 웹서비스 프로세스 개선(설치없는 간편결제, 앱카드 등)을 통해 설치 최소화

\* 실행파일 265개 중 98%(보안 프로그램 등 총 260개, 이 중 200개가 금융 관련) 차지('19년)



## □ 웹 표준 전환 지원사업 안내

### 2020년 민간 500대 웹사이트 액티브X 개선 관련 정부 지원사업이 종료될 예정입니다!!

#### ○ (사업분야) 민간 500대 웹사이트\* 액티브X 개선 지원사업

\* 민간 500대 웹사이트 목록은 HTML5 기술지원센터(koreahtml5.kr)에서 확인 가능

#### ○ (사업기간) 약 6개월('20. 6월~12월 예정)



※ 상기 일정은 사정상 변동 될 수 있음

#### ○ (사업예산) 총 1,000백만원(정부지원금 상한액\* 존재)

\* 기업당 정부지원금 상한액이 존재하며, 상세내용은 한국인터넷진흥원 홈페이지(www.kisa.or.kr)의 사업 공고문('20.4월 공고 예정) 참조

#### ○ (사업목적) 민간 500대 웹사이트에서 사용 중인 액티브X의 웹 표준(불가피할 경우 실행파일) 전환을 통해 국민들의 웹사이트 이용 편의 제고

#### ○ (참여대상) 민간 500대 웹사이트 운영기업 또는 국내 민간 500대 웹 사이트가 보유한 액티브X 개선(웹 표준 또는 실행파일)이 가능한 기업

#### ○ (지원방식 및 기준) 한국인터넷진흥원 및 참여기업 매칭방식으로 진행

전체사업비 중 자체부담금 기준	자체부담금 중 현금부담 기준
<ul style="list-style-type: none"> <li>■ (대기업) 최소 50% 이상</li> <li>■ (중견) 최소 40% 이상</li> <li>■ (중소) 최소 25% 이상</li> </ul> <p>※ 비영리기관 및 연구개발서비스사업자 자체부담금 없음</p>	<ul style="list-style-type: none"> <li>■ (대기업) 최소 40% 이상</li> <li>■ (중견) 최소 26% 이상</li> <li>■ (중소) 최소 20% 이상</li> </ul> <p>※ 비영리기관 및 연구개발서비스사업자 해당사항 없음</p>

#### ○ (문의처) 한국인터넷진흥원 인터넷기반조성팀 [html5@kisa.or.kr](mailto:html5@kisa.or.kr)

## 개인정보보호 국제협력센터 안내

개인정보보호 국제협력센터는 “해외 침해사고 발생 시 내국민 피해구제 및 해외 진출 기업에 글로벌 개인정보 규제 정보 제공”을 위하여 개소(‘17.10, [www.privacy.go.kr/pic](http://www.privacy.go.kr/pic))

### □ 제공 서비스

- (해외 국가 정보) 9개국(미국, 일본, 중국, 영국, 독일, 호주, 캐나다, 싱가포르, 베트남) 개인정보 보호 법률, 행정, 피해구제, 사건 사례, 동향 정보 제공
- (해외 민원 제기 절차) 12개국(그리스, 뉴질랜드, 미국, 싱가포르, 아일랜드, 영국, 일본, 중국, 캐나다, 프랑스, 호주, 홍콩) 개인정보 감독 기구에 개인정보보호 유출 등 관련 민원을 신청할 수 있도록 step-by-step 가이드 제공
- (해외 법제 자료) 유럽(EU GDPR, 영국, 독일, 체코), 아시아(중국, 일본, 싱가포르, 베트남), 북미(미국, 캐나다) 권역별로 개인정보보호 관련 법령, 가이드라인 등을 원문과 한글 번역 자료 제공



### □ 향후 계획

- (이벤트) '20년 상반기 중 “해외 개인정보보호 무엇이든 물어보세요!” 이벤트를 개최하여 해외 개인정보보호 이슈 분석, 관련 법률 번역 신청을 받고, 추첨을 통해 기프티콘 증정 예정  
※ KISA SNS 채널(Facebook, Twitter, Blog, 카톡 채널)을 이용하여 이벤트 안내

개인정보보호 국제협력센터는 이용자들의 의견을 항상 경청하고 있습니다.  
홈페이지 개선 의견은 이메일([iprivacy@kisa.or.kr](mailto:iprivacy@kisa.or.kr))로 보내주세요.

## 2020 Vol.1

### 이슈&트렌드

CES 2020 - 인공지능과 로봇의 만남: 더 많은 시간이 필요  
CES 2020 행사에서 가장 핫(hot)했던 제품  
CES 2020 서비스화 되는 모빌리티  
CES 2020 뷰티테크(Beauty Tech) 화두는 인공지능과 개인화  
CES 2020에서 PC의 변화  
CES 2020에서 살펴보는 슬립테크 동향  
온라인 데이터에서 나타난 “CES 2020” 관심도와 그 내용들  
CES 2020 스케치: 모든 것에 테크를 붙인 CES의 뒷담화  
미국의 의료분야 데이터사이언스 및 인공지능 정책 동향  
개인정보 유출 통지·신고 제도의 개선 검토

## 2020 Vol.2

### 이슈&트렌드

인공지능과 데이터 분석으로 질병 확산을 예측할 수 있는가?  
코로나 바이러스와 개인정보 활용에 대한 소고  
데이터와 헬스케어의 진화  
EU의 5G 네트워크의 위험 완화를 위한 조치 방안  
데이터 3법 개정의 주요 내용과 전망  
국내외 중소기업 정보보호 지원 정책 분석 및 개선 검토  
일본 IoT 보안정책 동향 분석 및 시사점





발 행 일	2020년 3월
발 행 처	한국인터넷진흥원 (전라남도 나주시 진흥길 9)
기 획	한국인터넷진흥원 ICT미래연구소
편 집	(주) 해리