항공보안 공모전

디지털 침투와 공중 위협
(사이버 · 드론 위협의 미래를 막다)

한서대학교 | 허장민 국새론 윤주연

목차

항공테러의 주요 유형

1. 드론 테러

- 상대적으로 적은 자본으로도 큰 피해 유발 가능
- 지상·출입 통제와 무관하게 공중을 통해 우회 침투 가능
- 원격 무선 조종 (사전에 드론을 좌표에 따라 자동 비행 설정)
- 대표 사례: 베네수엘라 드론 테러 시도

2. 사이버 테러

- 항공 운항 시스템 해킹
- 공항 정보 시스템 공격
- 항공 안전에 직접적 위협
- 대표 사례: 2015년 LOT 항공 해킹

드론 테러 사례

2018년 베네수엘라 마두로 대통령 암살시도 사건

국제 | 국제종합

"베네수엘라 마두로 대통령 암살 시도 드론에 C4 폭탄 1kg 실려"… 반경 50m

입력 2018-08-06 10

베네수엘라 정부, '마두로 대통령 드론 암살 시도' 용의자 6명 체포

김정우 기자 입력 2018.08.06 09:05

내무장관 "드론 2대에 1kg씩 폭발물 탑재
1대는 격추, 다른 1대는 건물 충돌해 폭발"
군부 '충성' 재확인… 반대파 탄압 구실 우려도

4일 베네수엘라 수도 카라카스에서 열린 방위군 창설 81주년 기념식 도중, 니콜라스 마두로 대통령을 겨냥한 드론 폭발물 공격으로 부상을 입은 한 군인이 피를 흘리며 몸을 피하고 있다. 카라카스=신화 AP 연합뉴스

베네수엘라 정부가 니콜라스 마두로 대통령을 겨냥한 드론(무인기) 암살 공격의 용의자 6명을 체포했다.

피해 규모

- 군인 7명 부상
- 드론 규제 정책 재검토 계기

테러 수법

- 상업용 드론에 폭약을 장착한 드론 2대 사용
- 하나는 공중에서 폭발, 다른 하나는 인근 건물에 충돌 후 폭발

의의

- 상업용 드론의 무기화 가능성 현실화
- 국가 수반을 향한 '공중 암살'의 실현

베네수엘라 드론 테러 시도

사건 개요	- 2018년 8월 마두로 대통령 암살 시도 - 군 행사 중 폭발물 탑재 드론 2대 공격
대응 방안	- 드론 비행 제한 법령 긴급 통과 - 행사장 경호 강화 조치 시행
문제점	- 드론 탐지 레이더 부재 - 전파 방해 장치 등 대응 장비 미비
필요성	- 드론 테러의 현실적 위협 인식 - 대(對)드론 방어 체계 구축
개선 과제	- 드론 탐지·요격 시스템 도입 - 관련 법규 정비 및 대응 매뉴얼 수립

사이버 테러 사례

2015년 폴란드 항공 LOT 해킹 사건

폴란드 공항 항공시스템 해킹당해.. 비행기 해킹 우려 고조

입력 2015.06.22 18:50

김서영 기자 westzero@kyunghyang.com

비행기를 관리
드 국적기 LOT
생하면 수백명
항공사측은 21
혔다. 항공사 다
황은 아니었다
피해는 없었다

해킹에 뚫린 항공 시스템... 사이버 테러 위협 현실로

오상도 기자

입력 2015-06-24 00:22 | 수정 2015-06-24 03:15

폴란드 국적기 30편 운항 취소·지연 '사상 초유'

폴란드 국적 항공사인 LOT의 운항시스템이 해킹당하며 30편 넘는 항공기 운항이 취소되거나 지연되는 사고가 일어났다. 5시간 가까이 지속된 사상 초유의 해킹으로, 이 회사의 비행 스케줄이 뒤엉켜 버렸지만 폴란드 당국은 해커의 정체조차 파악하지 못하고 있다. 지난 4월 독일 저먼윙스 여객기 사고 직후 미국 의회 보고서가 경고한 항공시스템에 대한 사이버 테러의 위협이 현실화됐다는 지적이다.

피해 규모

- 수천 명의 승객 일정 차질, 경제적 손실 및 항공사 신뢰도 하락
- 항공사 운영 시스템의 보안 취약성 드러나 안전에 심각한 위협 제기

테러 수법

- 해커들이 항공사의 내부 시스템 취약점 공격
- 지상 운영 시스템을 대상으로 사이버 공격 감행

의의

- 사이버 보안이 항공 안전의 핵심 이슈로 부각
- 유럽 항공청(EASA)과 ICAO의 사이버보안 지침 강화

LOT 항공 사이버 테러

사건 개요	- 항공사 내부 시스템 공격, 지상 운영 시스템 마비 - 비행 계획 수립 시스템 작동 오류로 항공편 출발 절차 차질 발생
대응 방안	- 시스템 복구 작업 실시 - 백업 시스템 가동 - 수동운영으로 전환
문제점	- 사이버 보안 투자 미흡 - 전담 인력 부족 - 대응 지연
필요성	- 항공 사이버 보안 중요성 - 실시간 모니터링 필요 - 백업 시스템 구축 중요
개선 과제	- 사이버 보안 예산 확대 - 정기적 취약점 점검 - 국제 협력 강화

테러사례 SWOT 분석

강점 (Strengths)

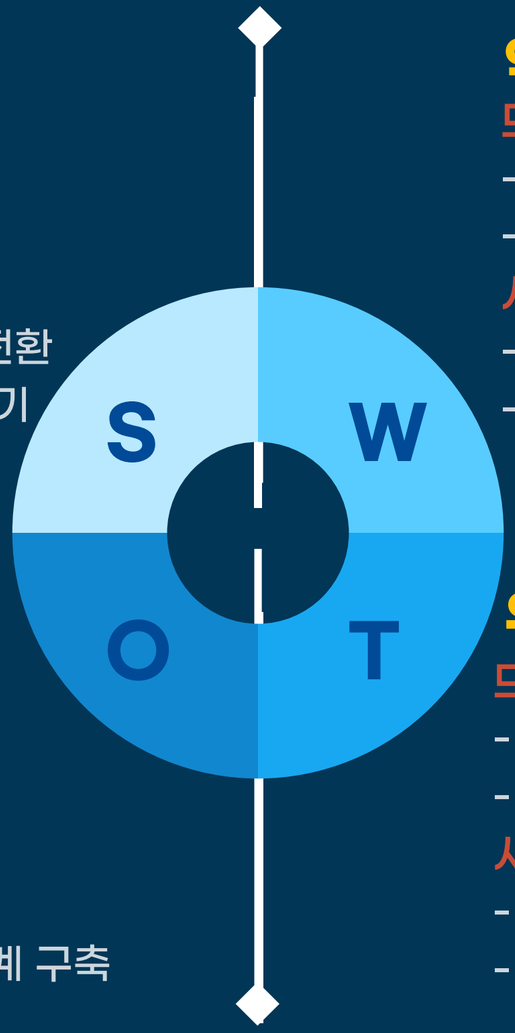
드론
- 사건 직후 빠른 대응 (비행 금지 조치)
- 드론 테러 위험성 국제적으로 알려짐

사이버
- 사건 직후 백업 시스템 가동 및 수동 운영으로 신속 전환
- 항공 사이버 보안의 필요성에 대한 국제적 경각심 환기

약점 (Weaknesses)

드론
- 드론 탐지 장비 없음
- 대드론 방어 시스템 부족

사이버
- 보안 투자 부족, 사이버 인력과 시스템 미비
- 초기 대응 지연으로 운항 마비 및 신뢰도 하락



기회(Opportunity)

드론
- 드론 대응 법·제도 정비 필요성 부각
- 대드론 기술 개발 기회

사이버
- 실시간 모니터링 시스템 구축 필요성 부각
- EASA, ICAO 등 국제기구 협력 통한 공동 대응 체계 구축

위협(Threat)

드론
- 드론 무기화 현실화
- 유사한 방식의 테러 재발 우려

사이버
- 해커들의 항공 시스템 직접 공격 현실화
- 경제적 손실, 승객 안전 위협, 항공사 이미지 타격 가능성

드론 테러 대응방안

OOAD LOOP

- 미국 공군 전략가 John Boyd가 만든 의사결정 사이클
- 더 **빠르고 유연하게 대처**하기 위한 사고 과정

관찰(Observe)

주변 환경과 상호작용,
정보 수집

방향 설정(Orient)

수집된 정보 분석,
상황 해석

순환 과정

지속적 반복으로
대응력 향상

결심(Decide)

최적의 대응 방안 선택

행동(Act)

선택한 방안 실행

드론 테러 대응방안

관찰(Observe)

- 전파 감지 센서 활용
- 실시간 데이터 수집
- GPS 신호 이상 탐지

방향 설정(Orient)

- 수집 데이터 분석
- 위협 수준 평가
- 영향 범위 예측

OODA LOOP의 첫 두 단계 심층 분석

- GPS 전파교란 대응에 있어 핵심적인 역할
- 상황을 정확히 파악하고 대응 방향 설정 가능

결심(Decide)

- 방향 설정 단계에서 적절한 대응방안 결정
- 상황에 영향을 범위를 고려 최적의 대응 선택
- 다양한 사전 대응 계획 수립
- 위기 경보 단계 적용
  1. 관심 2. 주의 3. 경계 4. 심각

행동(Act)

- 결정 사항을 실행에 옮기는 단계
- 신속하고 효과적인 행동
- 지속적 모니터링
- 구체적 행동 예시
  1. 백업 시스템 활성화
  2. 관련 기관에 상황 전파
  3. 대국민 안내 메세지 발송

드론 테러 대응방안

AI 기반 저고도 통합 감시시스템 U-LowRadar 시스템

- U-LowRadar 란?
  - 초저고도(ULow, Ultra-Low)에서 날아오는 물체를 탐지하고 추적하는 감시 레이더 시스템

초저고도 비행체 감시

일반 레이더가 놓치는
저고도 드론,
소형 항공기 탐지

24시간 실시간 모니터링

날씨·시간과 관계없이
지속적인 감시 가능

보안 시스템 연동

감지 즉시 경보 발령
→ 방어 체계와 자동 연동 가능

초기에 포착하고 대응할 수 있게 도와주는 '조기 경보 시스템'

사이버 테러 대응방안

실시간 훈련	통합 대응	자동화 시스템	지속적 개선
- 실제 공격 시나리오 - 즉각적인 대응 연습 - 다양한 상황 시뮬레이션	- 정보 공유 시스템 구축 - 의사결정 과정 최적화 - 전사적 보안 의식 고취	- AI 기반 위협 탐지 - 24/7 모니터링 체계 - 자동 복구 프로세스	- 사후 분석 시스템 도입 - 정기적인 보안 감사 - 국제 보안 동향 반영

- ☑ 실시간 대응 능력 강화
- ☑ 통합 보안 체계 구축 및 자동화로 효율성 향상
- ☑ 지속적 개선을 통해 최신 보안 상태 유지
- ☑ 사이버 테러에 대한 강력한 방어 체계 확보

사이버 테러 대응방안

디지털 면역 시스템
: DIS(Digital Immune System)

자가 진단, 자가 회복, 자가 적응 기능을 부여하는
자율형 사이버 방어 생태계를 구축

디지털 백혈구

실시간 감시 모듈을 심어 놓고
실시간으로 데이터 흐름을 감시

자가 학습 항체 모듈

스스로 공격 패턴을 학습
그에 맞는 알고리즘 생성

구성 요소

위장 / 변이 기술

핵심 시스템의 코드와 구조를
주기적으로 변경

면역 메모리 저장소

한 번 감지된 공격유형, 탐지방식,
대응결과를 자동으로 기록

디지털 림프절

감염 징후 발생 시 네트워크의
다른 노드로 즉시 경보를 전파

드론 테러 대응방안의 기대효과

U-LowRadar 시스템으로
저고도 드론 및 이상 징후 조기 감지 가능

실시간 모니터링, 전파센서, GPS 이상 감지
등으로 공격 전 사전 인지와 조치 가능

공격 발생 전, '탐지 → 분석 → 판단 → 대응'이
빠르게 이뤄져 실질적인 피해 최소화

OODA LOOP 기반 사고체계를 적용 시
관찰→방향 설정→결심→행동의 과정이 명확

위협 발생 시 혼란 없이 체계적이고
신속한 대응 흐름을 제공

초기 1~3분 대응의 골든타임 확보,
현장대응자와 연계기관 간 협력 속도 상승

사이버 테러 대응방안의 기대효과

AI 기반 위협 탐지 및 자동 복구 시스템은
흔들리지 않는 보안체계 제공

공격 시 자동 경보 및 백업 시스템,
네트워크 격리 조치까지 무중단 대응 가능

기존 '정적 보안 체계'에서 벗어나, 지능형
위협에도 실시간 적응하는 '동적 방어' 실현

위기 발생 시 자동으로 관련 기관에 정보 전파,
백업 시스템 활성화, 국민 안내 메시지 발송 가능

통합된 정보 공유 플랫폼은 기관 간 협업의
질을 높이고 중복 대응 및 혼선 최소화

단순 지식 습득을 넘어 현장 상황에서의
판단력·적응력 극대화

감사합니다.

참고문헌

[사진]
- https://timeslife.com/life-hacks/the-ai-scam-playbook-everyone-needs-to-know/articleshow/120428047.html
- https://www.news2day.co.kr/article/20240708500029?site_preference=normal

[드론·사이버테러]
- https://www.seoul.co.kr/news/newsView.php?id=20150624018026
- https://www.khan.co.kr/article/201506221850441
- https://www.joongang.co.kr/article/25042729
- https://www.ytn.co.kr/_ln/0104_202409150951365743
- https://www.kyeongin.com/article/1294676

[OODA LOOP]
- https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE10105382

[디지털면역시스템]
- https://scienceon.kisti.re.kr/srch/selectPORSrchArticle.do?cn=NPAP08067000
- https://m.boannews.com/html/detail.html?idx=120915

한서대학교 | 허장민 국새론 윤주연