AI 폴리싱(Policing)과 AI 범죄 동향

정수미*·박두이**

1. 개요

AI는 오늘날 우리 일상의 다방면에서 활용되고 있다. 각국 정부는 AI를 활용한 공공서비스 혁신 전략을 수립하고 사회 일반에 적용하고 있고, 우리 정부 역시 한국의 인공지능 국가전략(2019)을 세워 AI의 선제적 도입을 장려하고 있다. 특히 국민 생활 안정 측면에서 치안 서비스의 지능화를 꾀하고 있다.

AI를 활용하여 범죄를 예측, 예방, 대응, 수사하는 시스템은 이미 세계 곳곳에서 사용되고 있다. 하지만 양날의 검과 같이 AI 기술의 발전에 따라 AI를 활용한 범죄의 발생도 증가하는 추세이다. 본 고에서는 AI를 사용해 제공되고 있는 다양한 치안 서비스를 살펴보고 반대로 AI를 기반으로 하여 발생하고 있는 범죄의 동향도 살펴보고자 한다.

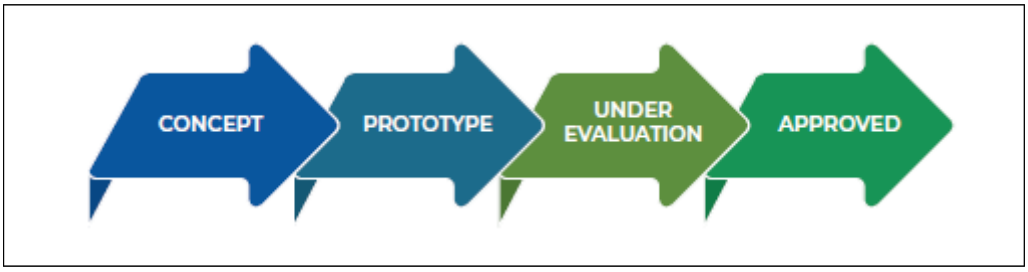
2. 인공지능 치안 서비스

아직 많은 AI 어플리케이션들이 실험 단계에 있지만, 이미 인공지능은 사법행정이나 법집행(경찰)의 과정에서 다양하게 사용되고 있다. UNICRI(2019)에 의하면 아직까지 각국

* 정보통신정책연구원 국제협력연구본부 연구원, 043)531-4217, smjeong@kisdi.re.kr
** 정보통신정책연구원 국제협력연구본부 연구원, 043)531-4125, dewy@kisdi.re.kr

의 경찰이 AI와 로보틱스를 법 집행에 활용하고 있는 수준은 국가별로 매우 상이하지만 범죄 관련 각 단계에 다양하게 사용되고 있는 것을 알 수 있다. 현재 각국에서 AI가 실무적으로 어느 정도 활용되고 있는지 그 유즈케이스는 단계별(컨셉, 프로토타입, 평가단계, 승인 단계([그림 1])로 나뉜다.

[그림 1] 지능형 치안 서비스 개발 단계



자료: UNICRI(2019)

각 단계별로 다음 〈표 1〉과 같은 AI 서비스들이 있다.

〈표 1〉 개발 단계별 지능형 치안 서비스

단계	내용
컨셉 단계	- 의심스러운 차량이나 절도차량을 판별하는 AI 알고리즘 - 영상 및 음성 분석 애널리틱스 툴 - 텍스트 기반 미디어 분석을 위한 머신러닝 - 더 나은, 공평한 범죄 수사를 위한 AI 툴
프로토 타입 단계	- 의사결정 및 작업 지원을 위한 에이전트 기반 시뮬레이션(agent based modeling) - 온라인 범죄 보고서의 처리와 수집을 지원하기 위한 정보 추출 - 얼굴이나 생체인증을 활용해 의심스러운 행동을 감지하거나 범죄자 확인, POI(Person of Interest) 찾기 등에 활용 - 수집된 정보에 대한 컨텍스트 분석 - 정치적 시위나 위법적 행위 등에 대한 예측 - 음성 머신 번역 - 문서의 컨텍스트 분석을 위한 머신러닝 활용 - 순찰 로봇 - 아동 포르노 확인을 위한 스마트 툴 사용

단계	내용
평가 단계	- 의사결정자들의 자원배분을 도울 수 있도록 지원해주는 예측적 폴리싱 시스템 - 교소도나 국경 지역의 순찰 드론 - 고위험 수감자들을 모니터링 할 수 있는 오디오 및 비디오 툴 - 범죄수사 지원을 위한 진술 기록 기계 - 오픈 디지털 포렌식 시스템 - 감시 드론 - 의심스러운 사람이나 행동을 감지할 수 있고, 태그, 추적, 대응할 수 있는 시스템 - 커뮤니케이션 로봇 - 음성 및 전화를 분석할 수 있는 머신러닝 - 범죄 행위를 모니터하고 감지할 수 있는 감시 시스템 - AI가 생성한 순찰 라이브 스트리밍
승인됨	- 기밀정보를 식별할 수 있는 AI 봇 - 범죄의 시간적/공간적 특성을 예측하여 법 집행의 자원을 최적화하고 효과적인 경찰 대응을 가능하게 하는 시스템

자료: UNICRI(2019)

아래에서는 좀 더 구체적으로 범죄예측, 범죄 수사/대응 그리고 범죄의 종류별로 AI의 쓰임을 살펴보도록 한다.

(1) 범죄 및 위험상황 예측

경찰은 AI를 사용하여 패턴을 식별해 잠재적 범죄 행위에 대한 통계적 예측을 한다. 예측적 방법은 AI가 도입되기 이전부터 사용되어 왔는데 AI는 여러 개의 데이터세트를 연결하여 좀 더 복합적이고 세밀한 분석을 할 수 있고 이에 따라 더욱 정확한 예측을 제공할 수 있다. 예를 들어 자동 자동차 번호판 인식, 유비쿼터스 카메라, 데이터 저장소와 컴퓨팅 등이 결합된 풍부한 데이터를 사용해 범죄 행위를 비롯한 패턴을 식별할 수 있게 된다.

예측 치안에는 두 가지 종류가 있다. 위치 예측은 후향적 데이터(retrospective data)를 사용하여 언제, 어디서 범죄가 나타날 가능성이 높은지 예측하는 데 사용된다. 위치는 주류 판매점, 술집, 공원 등 과거에 특정 범죄가 발생했던 위치를 포함할 수 있다. 데이터

의 분석을 통해 이 지역의 특정 요일이나 시간대에 경찰이 순찰하도록 경찰력을 배치해 범죄를 예방할 수 있다.

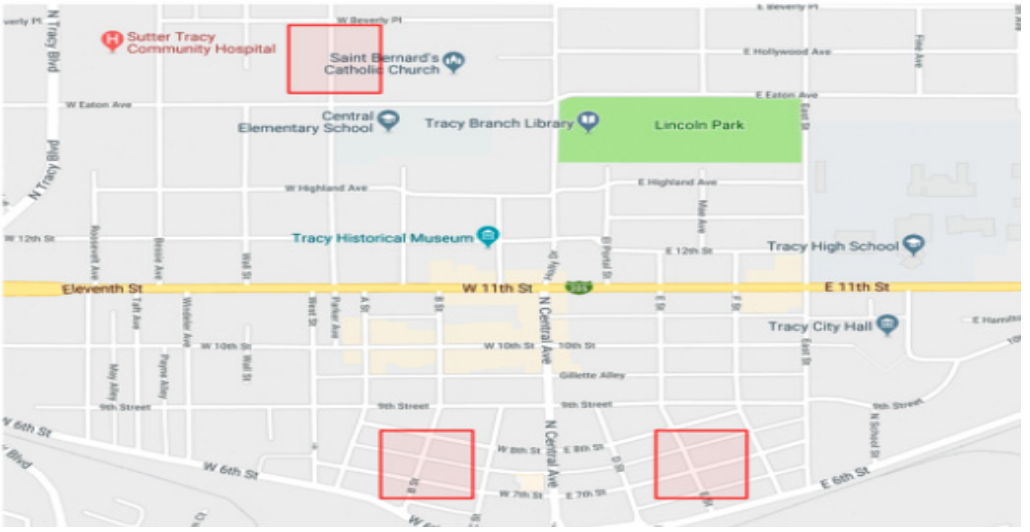
사람 기반 예측에서는 범죄 통계를 사용하여 어떤 인물이나 집단이 피해자로든 가해자로든 범죄 연루 여부를 예측한다. AI 기반의 강화된 예측 치안 이니셔티브는 맨체스터, 더럼, 보고타, 런던, 마드리드, 코펜하겐, 싱가포르 등을 포함해 전 세계적으로 트라이얼을 거치고 있다.[1)]

위치 예측

영국에서 Greater Manchester 경찰은 2012년부터 예측적 범죄 맵핑 시스템을 개발하여 사용 중이다. 영국의 켄트 경찰과 미국 LA, 워싱턴, 아리조나, 테네시, 일리노이 등 여러 도시에서는 Predpol이라는 시스템이 이미 작동 중이다.[2)] 이 시스템은 과거 범죄에 대한 기존 빅데이터와 머신러닝을 통해 새로운 범죄가 어디서 발생할 확률이 가장 높은지 분석한다. 이 알고리즘은 특정 범죄 종류가 특정 시간이나 장소에 집합된다는 관측에 기반한다. 예를 들어 특정 지역에서의 강도 사건이 나타나면 근방에서 가까운 미래에 또 나타날 수 있다. 이 기술을 실시간 epidemic-type aftershock sequence(ETAS) 범죄예측이라고 하며 원래 지진을 예측하기 위해 개발된 알고리즘을 활용한 것이다. 이 시스템은 지도에 범죄 발생 가능성이 있는 핫스팟을 제시해주어서([그림 2]) 경찰이 순찰을 강화해야 할 지역을 알 수 있게 해준다. 워싱턴 타코마 지역에서는 2013년에 본 시스템 도입 후 2015년 도난사건이 22% 감소했다. 시카고 7블록에 적용된 결과 살인, 총기사건 등 강력사건이 30% 이상 감소(2017년)하여 사회 안전이 현실화되고 있다고 한다.[3)]

1) OECD(2019)
2) ETRI(2019.02)
3) Emerj(2019.02.02.)

[그림 2] Predpol이 제시해준 범죄 핫스팟



자료: Predpol 웹사이트

범인/범죄 예측

Predpol이 위치예측의 대표적인 사례라면, 누가 범죄를 저지를지 예측해 주는 AI 시스템도 있다. Cloud Walk는 중국의 AI 기반 안면 인식 기술 회사로 출입구 안면 스캐닝이나 적외선 스캐닝에서 사용하던 기술을 확장하여 카메라 영상에서 비이상적인 행동이나 갑작스런 행동의 변화를 탐지하는 시스템을 출시했다.[4] 예를 들어 특정인이 특정 장소에서 앞뒤로 왔다 갔다 하면서 걷게 되면 이들은 소매치기이거나 미래 벌일 범죄를 위해 해당 장소를 탐색해 보는 것일 수 있다. 이 시스템은 대상을 기간을 두고 추적할 수도 있다. 예를 들어 누군가가 주방용 칼을 구매하고 나중에 여러 다른 종류의 범죄에 사용될 수 있을 법한 도구들을 추가로 구입할 경우 의심스러운 부분의 추적을 통해 미래 범죄를 예측할 수 있다.[5]

Hikvision이라는 중국 기업도 딥 뉴럴 네트워크를 구동할 수 있는 카메라를 만들고 있

4) ETRI(2019.02.)
5) Emerj(2019.2.19.)

다. 이 카메라는 자동차의 번호판을 더 정확히 스캐닝할 수 있고, 잠재적 범죄자/용의자나 실종된 사람을 찾는 안면 인식 기능을 수행할 수 있다. 또한, 군중이 많은 장소에 버려져 방치되어 있는 가방과 같은 비정상적인 상황도 포착해 낼 수 있다. Hikivision에 의하면 현재의 시각 애널리틱스는 99%의 정확도를 자랑한다고 한다. Hikivision 카메라를 장착한 도시 중 남아공의 Sea Point에서는 범죄율이 65% 나 감소했다고 한다.[6]

공판 전 석방(재범 예측)

범죄로 혐의를 받고 나서 실제로 재판을 받기까지 공판 전 석방(보석)이 된다. 과거에는 누가 재판 전에 석방이 되고 이들의 보석금은 얼마가 적정한지 판사들의 개별적인 판단이 내려졌다. 누가 도주 가능성이 있는지, 사회에 위험인물이 될지, 목격자나 증인을 해할 위험이 있는지를 판단하기에는 완벽하지 못한 시스템이었다. 영국의 더럼(Durham)에서는 AI를 사용하여 이러한 시스템을 개선하고자 하고 있다. Harm Assessment Risk Tool (Hart)이라는 리스크 평가 툴을 사용하여 AI에 5년 치 범죄 데이터를 학습시켜 특정인의 리스크(저/중/고)를 판단한다. Durham은 2013년부터 이 시스템으로 도출한 결과를 실제 결과와 비교해 보았는데 저위험으로 판단할 경우의 정확도는 98%, 고위험으로 판단한 정확도는 88%로 나타났다. Hart의 최종 목적은 어떤 범죄자가 재범이 저지를지 판단하는데 도움을 주는 것이다.[7]

국내에서도 이와 같은 위험 상황 예측 인공지능 기술을 개발 중에 있다. 한국전자통신연구원(ETRI)는 CCTV 상황을 분석하여 어떤 유형의 범죄가 발생할지를 확률적으로 보여주는 '예측적 영상 보안 원천기술'을 개발 중이다. 이는 현재의 통계적 범죄예측 방식에 지능형 CCTV 영상 분석 기술을 결합한 것으로, 기존의 범죄예측 시스템이 단순 과거 범죄 통계를 분석하여 예측하였다면, 본 기술은 CCTV를 통해 실시간 상황에 대한 정보를 반영하여 몇 분/시간 후 범죄 발생 위험도를 밝힌다. 즉, 현재 CCTV 상황을 과거 범죄 패턴에 비추어 얼마나 위험한지를 분석하는 것이다.

6) Emerj(2019.2.19.)
7) Emerj(2019.2.19.)

[그림 3] CCTV와 과거 범죄 통계 분석을 통한 범죄예측 시스템

자료: TheSciencemonitor(2020.01.02.)

예를 들어, 먼저 구두 발자국의 소리 요소를 영상으로 전환하는 시뮬레이션을 통해 긴박한 뜀박질인지 지속적 미행과 같은 상황인지를 파악한다. 화면 속 인물이 착용하고 있는 모자, 마스크, 안경, 배낭 등의 속성도 파악할 예정이다. 다음으로 현재 인식된 상황을 과거 범죄 통계 정도와 비교해 위험도를 측정한다. 이 AI 기술에는 법원 판결문 2만 건을 분석하여 범죄 발생 시 함께 나타나는 요소를 파악하고 미국 플로리다 주립대의 범죄 영상 데이터와 범죄 상황을 가정한 영상도 추가 확보하여 학습할 예정이다. 경찰 관제 시스템 등에 본 기술이 적용되면 CCTV 영상으로도 범죄 발생 위험도를 확인하여 대응 체계를 구축할 수 있을 것으로 보인다.[8)]

8) TheScienceMonitor(2020.01.02.)

(2) 범죄 수사 및 대응

범죄 수사

AI를 도입하는 수사기법은 데이터를 분석해 정보들이 어떻게 연결됐는지를 살펴본다. 사람들의 문자나 소셜네트워크서비스(SNS)를 분석할 땐 이들 사이에 연결된 말단(엣지)이 얼마나 많은가를 살펴보게 되는데 엣지로부터 전화를 많이 받으면 인기가 많고, 반대로 많이 걸면 영향력이 높다는 뜻이다. 연결된 엣지가 많으면 중심인물이라는 것을 추론해 볼 수 있다. 국내에는 대포폰을 쓰는 수배자를 이 기법을 이용해 검거한 사례가 있다. 수배자 가족들의 연락 사이 연결성을 살펴본 후 전화가 많이 걸려온 이를 찾아낸 이후 이 사용자가 대포폰을 쓴다는 것을 인지하고 수배자로 특정해 검거한 것이다.

'매개 중심'을 찾아내는 방법도 활용된다. 사건에 있어 중요한 인물과 다른 중요한 인물을 연결하는 최단 경로를 찾아내는 방법이다. 이 기법은 보이스피싱 조직을 검거하는 데 활용됐다. 보이스피싱 상담원과 콜센터 사이 연결 경로가 짧은 사람을 찾아내 뽑아냈더니 총책이었던 사례가 있다.[9)]

AI 기반 임장일지 빅데이터 분석 및 여죄 추적

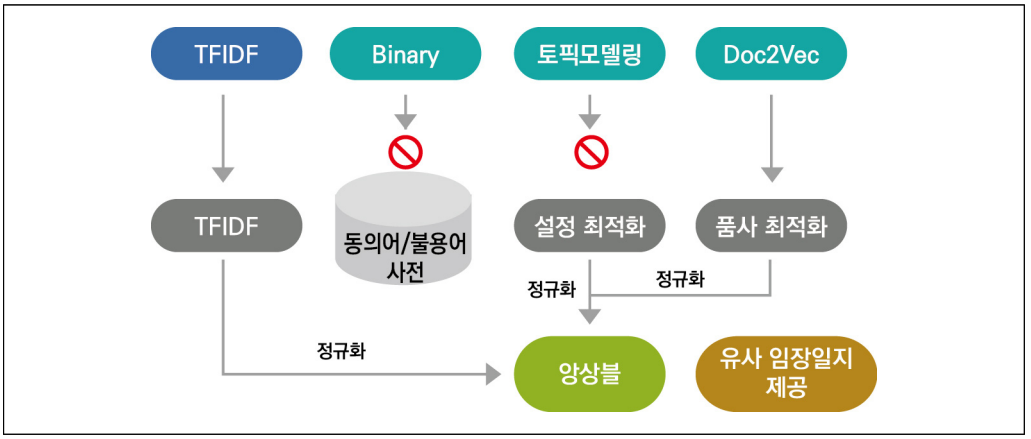
지금까지는 어떤 사건이 발생하면 경찰청 관계자는 전국에 흩어져있는 사건 기록, 즉 임장일지를 모두 뒤져서 유사 사건을 확인한 후 용의자를 추적해왔다. 방대한 자료를 수작업으로 확인하고, 경찰서 간 공조 절차를 거치다 보니 신속한 추적이 불가능했다.

국내에서는 임장일지 빅데이터 검색에 AI 기술을 적용하고 있어, AI가 사건을 분석하고 범죄 유사도가 높은 순서대로 과거의 다른 사건의 임장일지를 도출해낸다. 검거된 피의자의 임장일지와 상황·수법이 유사한 미제 사건의 임장일지를 찾아내기 위한 기존 알고리즘(TFIDF, 바이너리 벡터, 토픽 모델링)과 최신 알고리즘(Doc2Vec)의 문서 유사도 측정 알고리즘([그림 4])을 활용한다. 또한, 임장일지 분석에 적합하도록 동의어(약 1만 건) 및 불용어(약 7백 건) 사전을 자체 개발하고, 적중률 높은 품사와 설정값(알고리즘 최적화)을

9) 동아사이언스(2020.07.03.)

찾아내는 등 최적화를 위해 노력했다.[10][11]

[그림 4] 임장일지 분석 개요



자료: ZDNet Korea(2018.01.17.)

이렇게 되면 범죄 피의자의 추가 여죄도 밝혀낼 수 있다. 실제 미제 사건이 70%에 달하는 절도사건의 경우 발생 빈도가 높고 범행 수법도 다양하여 피의자의 여죄를 찾아내는데 현실적인 어려움이 있는데, 이 분석 모델 구현으로 인해 범죄 피의자 여죄 추적도 활발하게 진행 중이다.[12] 이러한 시스템을 통해 이전 사건이 현재 범죄와 직접적인 연결고리가 없다고 하더라고 범죄 해결을 위한 새로운 연결고리나 아이디어를 제시할 수 있게 될 것이다.

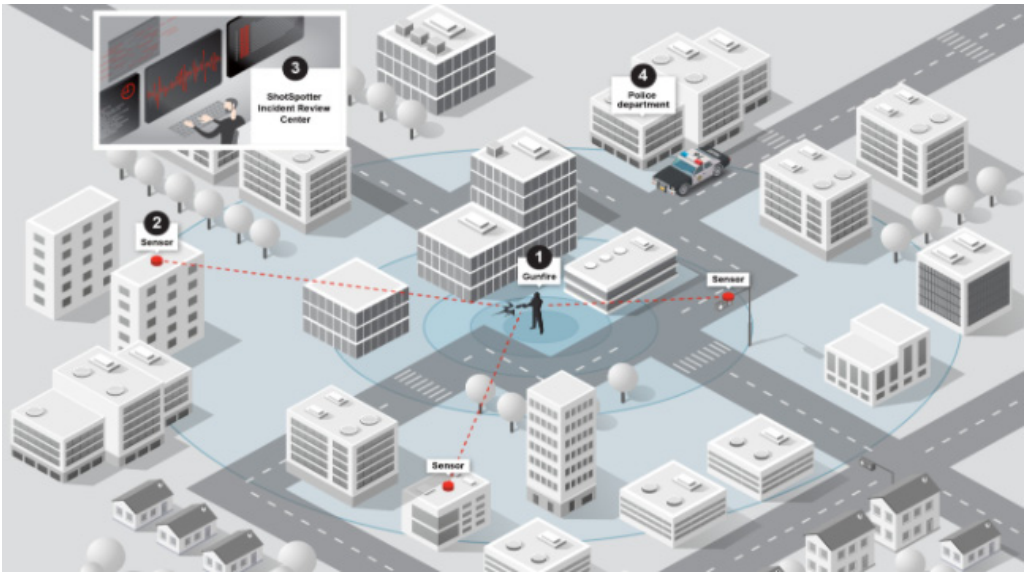
총기 사고 탐지

AI를 활용하면 총기가 어디서 발사됐는지 아무도 신고하거나 목격하지 않아도 경찰이 사건 발생 장소를 알 수도 있다. 도시 인프라에 센서가 장착되고, 클라우드 기반의 어플리케이션과 센서가 연결된다. 각 센서는 시간과 소리를 포착하고 머신러닝 알고리즘을 통해 센서가 언제 소리를 감지했는지, 소리의 레벨, 건물들 사이로의 에코잉 등을 분석하여 총

10) ZDNet Korea(2018.01.17.)
11) IT조선(2018.12.28.)
12) ZDNet Korea(2018.01.17.)

기사건의 위치 및 총기 사용자가 발사한 위치도 알 수 있게 해준다. 이 정보가 경찰본부로 보내지고 컴퓨터나 스마트폰의 스크린에 알림으로 뜬다. 보통 총기사건의 12%만이 경찰에게 보고가 된다고 하는데 AI 기술을 활용하면 총기사건이 발생했을 때 효과적으로 대응할 수 있게 될 것이다. 현재 Shotspotter라는 기업은 해당 인프라를 제공하고 있는데, 뉴욕, 시카고, 샌디에이고 등 90개가 넘는 도시에서 사용되고 있다고 한다.[13)]

[그림 5] 총기 사고 감지



자료: Shotspotter 홈페이지

Shotspotter가 작동하는 방식은 1) 총이 발사되면 2) 소프트웨어가 배경 잡음 등을 필터링하고 총소리의 특징들만 포착 한다(이를 펄스(pulse)라고 지칭). 센서들이 소리의 파형(소리의 날카로운 정도, 강도, 지속시간, 디케이(decay)까지의 시간)에 대한 정보를 추출한다. 그리고 적어도 3개의 센서가 해당 소리를 총기 소리라고 판단하면, 데이터 패킷을 클라우드 서버에 보내게 되고, 분류 소프트웨어(classifier)가 소리의 도착 시간 차이, 도

13) Emerj(2019.2.2.)

착 각도 등의 분석을 하여 총기 발사 여부를 판단하게 된다. 총 쏘는 소리로 판단이 되면 이는 3) 사건 리뷰 센터로 보내지고 4) 경찰이나 응급 대응팀의 핸드폰 앱이나 브라우저 앱에 알림이 가게 된다. 초기 총의 발사에서 알람까지는 60초 정도의 시간이 걸린다.[14]

폭발물 감지

폭발물은 범죄자나 테러리스트들이 사용하는 가장 위험한 무기인데, 폭발물을 만드는데 사용되는 니트로글리세린, 알루미늄 파우더, 테트라니트레이트, 피동형 적외선 센서 등 여러 요소들을 로봇이 파악할 수 있다. 이러한 요소를 파악할 수 있게 되면 AI 기반으로 작동하는 로봇은 보안 요원 등 인명 피해 없이 폭발물을 감지하는 것이 가능하게 된다.[15]

AI가 베트남 전쟁 때 캄보디아에 투하된 불발탄을 측정해 낸 연구 사례도 최근에 발표되었다. 현재까지는 캄보디아에서 불발한 폭탄이나 지뢰들을 찾아내서 제거하는 작업이 효과적이지 못했는데 AI를 활용한 모델을 사용하여 폭탄 크레이터(분화구)를 파악해 낼 수 있다. 우선 캄보디아 Kampong Trabaek 지역의 100km^2 내 위성 이미지로 폭발물 크레이터 존재 유무를 머신러닝으로 분석하였다. 해당 지역에 몇 개의 폭탄이 투하되었는지에 대한 정보가 있기 때문에 실제로 몇 개의 폭탄이 폭발하였는지, 미폭발 폭탄의 개수는 몇 개인지 알 수 있게 된다.

위 연구에서 첫 번째로는 유성과 달의 분화구를 탐지하게 만들어진 알고리즘을 사용했으나, 수십 년이 지나 분화구 위에 풀이라든가 관목이 자라기 때문에 분화구의 모양이 변해 분석이 정확하지 않았다. 따라서 두 번째 단계에서는 폭탄 크레이터와 유성/달의 크레이터가 어떻게 다른지에 대해 모양, 색, 재질, 크기 등의 특성을 학습 시켰다. 두 번째 단계의 테스트 결과로 177개의 실제 폭탄 크레이터 중에 152개를 찾아냈고, 1차에 비해 거짓 양성 비율을 96%나 감소시켰다. 지뢰 제거 과정은 시간이 오래 걸리고 비용이 많이 드는 작업인데, 이와 같은 모델을 통해 어떤 지역이 제거작업의 우선순위가 되어야 하는지 판단하는데 도움이 될 수 있다.[16]

14) Shotspotter 홈페이지
15) Naveen Joshi(2019.11.30.)

(3) 금융 범죄 대응

금융 기관은 안팎으로 금융 범죄의 위협에 직면하고 있으며 특히나 AI와 같은 신기술의 발달로 더욱 더 조직적이고 기계화된 금융 범죄에 노출되고 있다. 특히 AI를 활용한 AI 금융 범죄는 유기체와 같은 속성 때문에 규제와 예방이 쉽지 않다. 이러한 상황에서, 미국의 Financial Crimes Enforcement Network (FinCEN)을 포함한 다양한 기관들과, 호주의 Australian Transaction Reports and Analysis Centre (AUSTRAC), 영국의 Financial Conduct Authority (FCA) 금융 기관들이 범죄를 예방 및 추적에 AI를 사용할 것을 권장하고 있다.[17)]

은행에는 과거 고객의 금융 거래 내역(수십 만개의 유효/적법하거나 사기성의 거래들에 대한 예시)이 기록되어 있기 때문에, 이를 쉽게 정량화할 수 있다. 이 데이터를 머신러닝으로 학습해 활용하면 경찰은 아주 쉽게 잠재적 자금세탁 활동에 연결되어있는 공통적인 요인(위치, 액수, 고객 타입)을 포착할 수 있다. 과거의 거래 기록을 자금세탁 여부로 라벨링을 하면 머신이 어떤 케이스가 의심스러운 거래인지 연계된 특성에 따라 판단할 수 있게 된다.[18)]

금융 기관이 자체적으로 가지고 있는 현존하는 자금 세탁방지 시스템은 신기술의 부족, 정보의 부족과 오류로 통상적으로 90%로 높은 거짓양성 비율(false-positive rates)을 보이기 때문에 실 자금세탁 방지 케이스를 가려내고 조사를 착수하기까지 많은 시간과 자본이 소요된다. 따라서 자금세탁방지 감지 시스템에 AI를 적용하여 축적된 데이터를 습득하고 패턴을 활용, 효율적인 조사 체계와 결과를 제공할 수 있다.

자금세탁 방지뿐만 아니라 금융사기의 양대 축인 음성 및 문자 금융사기(보이스피싱)를 판별할 수 있는 AI도 개발됐다. 기업은행은 'IBK 피싱스톱' 서비스를 시작했는데 AI를 활용해 금융사기 전화를 실시간으로 차단하는 앱으로 피싱 사기일 확률이 일정 수준에 달하

16) Lin Erin, Rongjun Qin, Jared Edgerton, Deren Kong(2020)
17) IBM(2019)
18) OECD(2019)

면 경고 음성과 진동으로 위험 여부를 알려준다. 국민은행도 금감원, 아마존과 함께 개발한 스미싱 탐지 시스템인 '리브똑똑 안티스미싱'서비스를 개시해 AI를 활용한 문자메시지 사기 여부를 판별하고 있다.[19]

AI로 기업 부정 대출도 탐지할 수 있다. 우리은행은 AI와 빅데이터 기반의 탐지시스템을 운영 중인데, 여신 심사 과정에서 기업의 행동 패턴을 분석해 부정 대출 여부를 분석한다. 은행에서 보유한 기업 정보와 신용평가사 등이 제공하는 정보 등을 은행 기업진단시스템과 연동하여 기업통합 DB를 구축하고, 여·수신, 신용공여, 외환 등 6개 분야 15개 기업 행동 패턴을 분석해 부정 대출 위험도를 상·중·하 3단계로 분석해 이를 여신심사에 활용하고 있다.[20]

(4) 디지털 성범죄 대응

국내에서는 여가부와 과기정통부가 2019년 공동 개발하여 불법 촬영 피해 여성들을 도와줄 수 있는 인공지능이 디지털 성범죄 대응에 활용되고 있다. 그동안 디지털 성범죄 피해자가 신고한 불법 촬영물이 웹하드 사이트에 게시되어 있는지 확인하기 위해서는, '디지털 성범죄 피해자 지원센터'의 삭제지원 인력이 수작업으로 피해 촬영물에서 검색용 이미지를 추출하고 각 사이트를 검색해야 했다. 이를 개선하기 위해 ETRI가 AI 기술을 활용해 불법 촬영물에서 추출한 이미지를 웹하드 사이트에서 피해 촬영물과 유사한 영상물을 자동 선별/수집 가능한 시스템을 개발했다. 이를 통해 삭제지원 인력은 영상물의 이미지, 유사도, 제목, 주소 등 수집된 정보를 검토해 영상물을 확인하고 해당 웹하드 사이트에 삭제 요청을 하게 된다.[21] 페이스북도 작년 AI를 이용해 디지털 성범죄물을 선제적으로 차단하겠다고 밝혔다. 페이스북이 도입한 AI 기술은 누군가가 불법 촬영물을 신고하지 않아도 알몸 노출 상태인 사진이나 영상을 미리 검열한다.[22]

19) 뉴스토마토(2019.08.08.)
20) 시사저널e(2020.05.23.)
21) 사이언스모니터(2019.07.22.)
22) 동아사이언스(2020.04.06.)

몰카를 찾아내는 AI도 개발되었다. 최근 들어, 몰카 기술은 갈수록 발전하고 있다. 최근에는 렌즈처럼 생기지 않은 코팅 방식 몰카도 나오는 등 현재 몰카 종류만 3,000가지가 넘는 것으로 알려져 적발이 어려워지고 있다. 지금까지의 몰카 탐지 어플은 대부분 자기장 탐지 기능을 이용하는데 소형카메라는 자기장 크기가 낮고 자기장을 발산하는 전자기기가 많기 때문에 몰카 탐지에 한계가 있었다. '릴리의 지도'는 딥러닝 기술과 증강현실(AR)을 활용해 몰카를 찾는다는 점에서 차별화된다. 숙박업소, 화장실 등의 몰카 형태를 딥러닝을 통해 학습하고 휴대폰 카메라로 해당 공간을 스캔해 불법 카메라로 의심되는 이미지를 식별한다. 40cm 거리 범위에서 각도 30도 안으로 피사체가 들어오면 탐지가 가능하다. 찾아낸 몰래카메라를 지도에 표시하고 후기를 남기는 SNS 기능도 있다. 몰카 이미지가 더 많이 축적될수록 탐지 확률은 더 높아진다.[23][24]

최근 발생한 N번방과 같은 사례에 대해서도 AI 기법이 사용될 수 있다. N번방 사태는 미성년자 그루밍에서 시작한 성범죄로 한국정보화진흥원은 미성년자 대상 디지털 성범죄 위험 감지 및 신고 애플리케이션의 개발을 제안했다. 디지털 그루밍 성범죄에 사용되는 언어의 패턴을 AI가 학습하여 유사 사례를 범죄 발생 전에 찾아내는 것이다.[25]

(5) 아동범죄/실종아동

영국의 경찰은 2014년부터 국내 아동학대 이미지 DB를 구축해 왔으며, 2019년 7월 기준으로 1,300만 개의 영상이 수집되었고 6개월마다 50만 개 이상의 새로운 영상이 추가되고 있다. 런던의 AI 회사 Qumodo는 새로운 디지털 미디어 탐지시스템을 개발하여 경찰을 지원하고 있다. 일반적으로 아동 대상 성 착취물을 검열하기 위해서 경찰은 매우 긴 시간 동안 불쾌한 이미지를 봐야 하는데, 이를 조사하는 경찰도 2차 피해자로 매우 큰 심리적 트라우마를 받을 수 있다. Qumodo의 시스템은 다음이 가능하다. 1) Q-Classify:

23) 서울경제(2020.06.03.)
24) 위키트리(2020.05.08.)
25) IT조선(2020.06.07.)

CAID Vigil AI classifier를 사용하여 용의자의 기기를 스캔해 아동 성 착취물 유무를 확인한다. 이를 통해 경찰이 직접 콘텐츠 검열을 하는데 소요되는 시간을 아낄 수 있으며 가해자를 빠르게 찾아낼 수 있다. 2) Q-Discover: 대량의 디지털 데이터 중에 단서나 연결고리를 찾을 수 있도록 도와주는 검색엔진으로 복잡한 수사에 있어 필요한 증거가 경찰에게 제시될 수 있도록 한다. 3) Q-Insight: 여러 다른 종류의 범죄 트렌드를 추적하게 해주는 툴이다. 이 시스템의 시범운영 결과, 수사관들이 24시간에 걸쳐 조사할 양의 이미지가 30분 내 조사가 가능해졌고 또한 총이나 칼을 탐지하는 데에도 사용될 수도 있었다. 이 시스템은 케냐의 신설된 DIC Anti-Human Trafficking & Child Protection Unit 과도 시범운영을 거쳤고 운영 수분 만에 아동학대의 증거를 제시하였다.[26]

일본의 AI 기반 데이터 분석 기업인 프론테오(FRONTEO)는 AI를 활용해 아동학대 징후를 감지하는 솔루션을 상품화했다. 프론테오가 자체 개발한 AI 엔진 'KIBIT(키비트)'를 기반으로 하고 있으며 과거에 아동학대로 인정됐을 때의 기록이나 아동상담소의 학대 업무 담당자들의 판단 근거를 AI에 학습시켰다.[27] 상담기록이나 면담기록 등의 텍스트 데이터를 AI가 분석해 조기에 조치가 필요가 안건의 우선순위를 정할 수 있다.

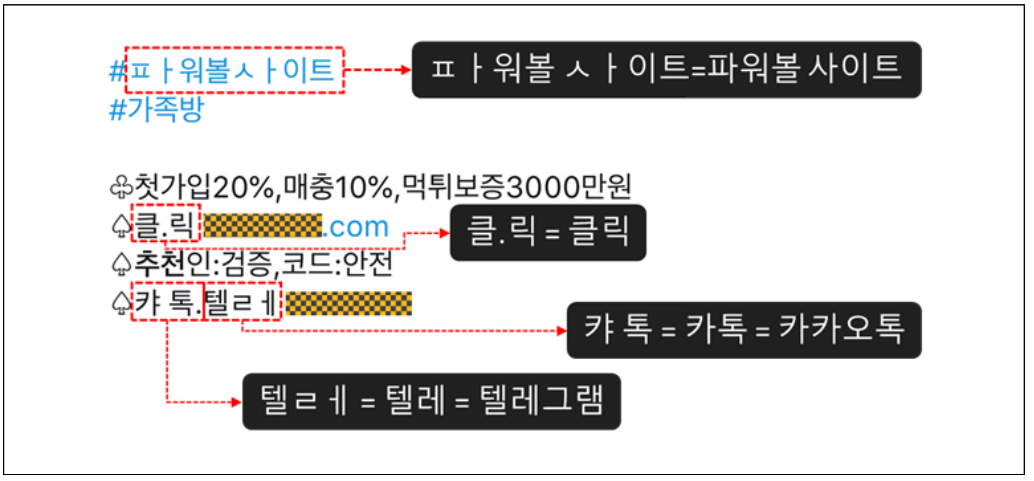
AI는 실종아동 수색도 도와주고 있다. 중국의 경찰은 실제로 AI 기술을 통해 미아를 찾고 있다. 텐센트의 머신러닝 연구실 텐센트 유투는 안면 인식 기술을 사용해 3살 때 유괴되어 10년이나 지나 시점의 실종아동 수색에 성공했다. 안면 식별 정확도는 99.99%로 알려져 있고 수초면 수천만 명의 얼굴을 대조할 수 있다. 특히, 세월이 지난 후에 사람의 눈, 코, 귀 등의 위치와 모양이 어떻게 변화할지도 정확히 예측하여 'Tuanyuan'이라는 AI 프로그램으로 800여 명이 넘는 실종아동을 찾아내기도 했다. Tuanyuan은 25개의 뉴미디어 플랫폼과 모바일 앱(디디택시, 바이두, 타오바오, QQ 등을 포함)과 연결되어 있어, 실종 아동에 대한 실시간 알림을 보내기도 한다.[28]

26) Qumodo(2019.7.12.)
27) Techdaily(2020.06.15.)
28) Chinadaily(2019.06.04.)

⑹ 불법 온라인 콘텐츠

민생범죄에서 대부 사기나 다단계 사기 등의 범죄들은 온라인을 통해 홍보해 거미줄 형태로 확대해 나가는 특징이 있어 수사관들이 직접 온라인 사이트를 찾아 방문, 검증하는 것이 불가능에 가깝다.

[그림 6] 한글파괴를 이용한 불법 콘텐츠 사례

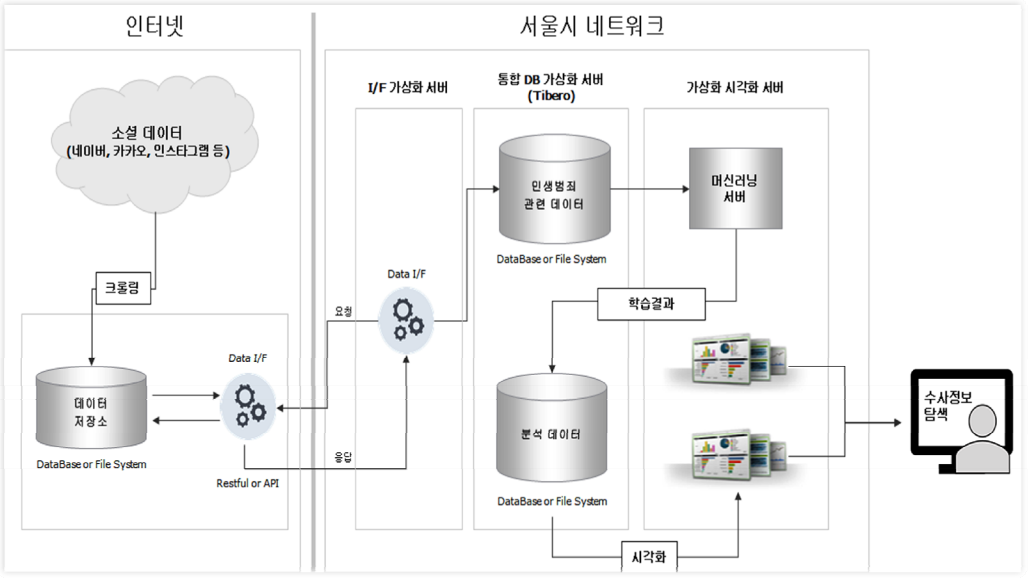


출처: 서울시 보도자료(2018.08.22.)

서울시는 민생범죄 수사에 인공지능 기술을 도입했다([그림 7]). 불법 대부업, 다단계판매 등을 유인하는 광고는 키워드 단속을 피하기 위해 한글 파괴, 은어, 신조, 기호 사용하는 경우가 많은데([그림 6]), 이러한 검색을 회피하는 AI 알고리즘을 개발했다.

뿐만 아니라 텍스트 형태가 아닌 이미지 삽입으로 검색을 피하는 수법이 증가해 이미지 정보를 추출하는 기술도 추가적으로 도입 계획이다. 2018년 실시됐던 시범사업에서는 실제 정답 대비 82%의 정확도로 불법 콘텐츠를 분류해 냈다. 범죄수사라는 특수성을 고려해 베테랑 수사관들의 노하우를 기계에 학습시키는 '지도학습'기법을 사용했다. 특히, '대출'→'머출', '명작'→'띵작' 같이 자모음의 유사성을 이용해 비슷한 글자로 바꿔쓰는 '야민정음'등 기존에 인지하지 못한 새로운 키워드를 발견하기도 했다.[29)]

[그림 7] 서울시 인공지능 민생범죄 수사 빅데이터 플랫폼 체계도



출처: 서울시 보도자료(2018.08.22.),

3. AI를 활용한 신종 범죄

살펴본 바와 같이 AI를 활용하여 범죄를 예방하고 범죄에 효과적으로 대응할 수 있기도 하지만 역으로 AI를 활용한 신종 범죄도 발생하고 있다.

(1) AI 기반 범죄

Crime science 저널에 발표된 한 연구에서는 University College London의 전문가들이 AI와 관련된 범죄들 가능성을 논의하기 위해 학계, 공공정책, 민간 분야의 전문가들과 워크숍을 통해 위험도를 분석하였다. 이 중 AI 기반 범죄 중 위험도가 높거나 중간 정도인 범죄는 다음과 같은 것들이 있을 수 있다.

29) 서울시 보도자료(2018.08.22.)

AI를 활용한 범죄 중 가장 우려되는 것은 **음성/영상의 위·변조(딥페이크)**이다. AI는 딥러닝이나 GANs(Generative Adversarial Networks)[30]를 통해 페이크 콘텐츠를 제작할 수 있게 되었다. 정해진 스크립트를 따라하는 모사는 물론 인터렉티브 모사도 곧 가능해질 것으로 보인다. 딥페이크 기술은 대중의 미디어에 대한 신뢰를 착취하는 방향으로 범죄에 사용될 수 있다. 예를 들어 영상통화를 통해 아이들을 모사하여 부모로부터 돈을 갈취하거나, 음성 통화를 통해 보안 시스템에 대한 접근 권한을 요구하거나, 대중성 있는 인물의 연설이나 행동 등을 모사하여 대중의 지지를 조작할 수도 있다. 딥페이크를 검출하는 알고리즘에 대한 성공 사례들이 있긴 하나, 장기적으로 통제할 수 없는 다양한 루트를 통해 가짜 영상들이 퍼트려질 수 있기 때문에 시민들의 행동 양식 변화만이 유일하고 효율적인 방어 수단일 수 있다. 이러한 영상을 통한 직접적인 피해는 명예훼손이나 사기가 있을 수 있고 간접적으로는 시각 증거가 조금이라도 가짜일 가능성이 있게 되는 순간 실제 증거에 대한 신뢰와 가치가 아주 쉽게 상실될 수 있다. 이렇게 되면 범죄 수사나 신뢰와 소통을 근간으로 하는 정치·사회기관에 대한 신뢰 저하로 이어질 수 있다.

다음으로는 **무인 자동차가 무기화**될 수 있다. 모터 자동차는 폭발물이나 카이네틱 무기(kinetic weapons)의 운송 수단으로 사용되어 왔다. 현재로서는 완전히 무인화된 AI 차량은 없지만, 여러 자동차 제조업체와 기술 기업들이 무인 자동차를 만들기 위한 경쟁을 벌이고 있고 이미 시범운행이 이뤄지고 있다. 무인 자동차의 경우 잠재적으로 운송체를 동반한 테러리즘의 확대로 이어질 수 있다. 운전자가 필요하지 않기 때문에 특히나 개인으로 활동하는 범죄자들도 여러 건의 공격을 시도할 수 있고 많은 자동차를 한 번에 사용하는 계획된 공격 시도도 가능할 수 있다. 비슷한 맥락에서 전투나 방어선 구축 등에 활용될 목적이었던 **무인 군사 로봇**이 범죄에 사용되면 위험성이 현저하게 높아질 수 있다.

30) GANs(생성적 적대 신경망)는 두 신경망 모델의 경쟁을 통해 학습하고 결과물을 만들어낸다. 두 모델은 '생성자(Generator)'와 '감별자(Discriminator)'로 불리는데 생성자는 실제 데이터를 학습하고 이를 바탕으로 거짓 데이터를 생성한다. 실제에 가까운 거짓 데이터를 생성하는 게 목적이다. 감별자는 생성자가 내놓은 데이터가 실제인지 거짓인지 판별하도록 학습한다. GAN은 주로 이미지 생성, 영상 합성, 텍스트 생성 분야에 활용된다(Bloter, 2018.06.08.).

피싱은 정보를 수집하거나 신뢰할 수 있는 기관(예를 들어 사용자의 은행)에서 보낸 메시지로 가장하여 말웨어(malware)를 설치하게 하는 공격이다. 일부 피싱은 스피어피싱(spear-phising)처럼 특정인을 대상으로 할 수 있지만, 규모를 키우기 어렵다. 즉, 현재의 피싱 공격은 대부분 차별화되어있진 않고 우연히 사용자의 일부에게 관심 사항이 될 만한 내용을 가장한 일반적인 메시지 형태를 보인다. 하지만 AI를 활용하면 **맞춤형 피싱**이 가능해질 수 있어 위험성이 증가한다.

AI로 제어되는 시스템에 대한 붕괴 공격이 발생할 수도 있다. 정부 기관, 기업, 그리고 가정에서 사용하는 AI가 늘면서 AI가 수행하는 역할이 늘어나고 있다. 학습 기반으로 된 시스템들의 경우 대부분 안전성보다는 편리성이나 효율성 기반으로 구축되기 때문에 이러한 시스템들의 파괴를 동반하는 테러 시나리오가 있을 수 있다. 예를 들면 전기 공급 중단이나, 교통 신호 그리드락(gridlock) 혹은 식품 수급 로지스틱에 대한 방해 등이 있다. 공공 안전 및 보안과 관련된 일련의 시스템들이 모두 공격의 대상이 될 수 있고, 특히 금융 거래를 담당 기관 등도 포함된다.

전통적인 방식의 협박은 범죄나 잘못된 행동에 대한 특정 증거의 공개, 혹은 공개하기 꺼려지는 개인정보 등을 바탕으로 행해졌는데, 그러한 정보의 획득이 쉽지는 않았다. 이런 형태의 범죄는 범죄자가 정보를 획득하는 비용보다 피해자로부터 더 큰 돈을 얻어낼 수 있을 때만 실행 가치가 있는 행위이다. 그러나 AI는 소셜 미디어나 대규모의 개인 데이터 셋(이메일 로그, 브라우저 기록, 하드 드라이브, 핸드폰 컨텐츠)을 분석하여 **대규모 개별 맞춤형 협박**을 가공해 낼 수 있어 위험성이 높다. 또한 가짜 정보를 생산해 내 협박에 사용할 수도 있다.

가짜 뉴스는 신뢰할 수 있는 기관에서 발행된 것임을 가장한 '프로파간다'이다. **AI 가짜 뉴스**는 잘못된 정보를 전달함과 동시에 진실된 정보로부터 대중을 교란시킬 수 있을 만큼 충분한 양의 거짓 정보를 제작할 수 있다. AI가 제작하는 가짜 콘텐츠는 효율성이나 구체성 면에서 훨씬 뛰어날 수 있다. 특정 콘텐츠에 대해 여러 개 버전을 생성할 수 있고, 가시성과 신뢰성을 높이기 위해 여러 출처를 활용할 수도 있다. 또한 영향력을 높이기 위해서

콘텐츠나 프레젠테이션을 개인화할 수도 있다.

의도적으로 특정한 편견을 갖게하기 위해(상업적 라이벌 제거, 정치 폭로, 대중 신뢰 왜곡 등 다양한 목적) 악의적인 학습 데이터를 주입해 머신러닝 모델을 망가뜨리는 **데이터 포이즈닝(data poisoning)**도 발생할 수 있다. 예를 들어 AI 자동화된 엑스레이 감지 기기가 있지만, 해외로 밀수하고 싶거나 비행기에 소지하고 싶은 무기에 대해서는 반응하지 않도록 만들거나, 혹은 투자 자문이 예상외의 조언을 하게 하여 시장 가치를 조작하고, 범죄자는 사전에 시장을 착취할 수 있는 정보를 이용하는 등이다. 실제로 의료기계를 대상으로 한 연구 결과에서 대상 장비의 오작동을 발생시키기도 했다.[31] 데이터 출처가 신뢰할 수 있는 기관이고 자주 사용되는 데이터일수록 이런 공격의 영향력은 커질 수 있다.

학습 기반의 사이버 공격도 증가할 수 있다. 현재의 사이버 공격은 매우 정교해서 특정 목표물이 대상이거나, 조잡하지만 자동화된 대규모 공격(DDoS, 포트 스캔)을 시전하는 방법인데, AI의 경우 정밀하면서도 대규모로 동시다발적인 사이버 공격을 개시할 수 있다.

자동화되지 않고 사람이 조정하는 드론들도 이미 마약 밀수 등에 사용되고 있으며 교통 방해의 원인이 되고 있다. **자동화된 무인 드론**의 경우 코디네이션과 복잡성을 증가시키고 범죄자가 드론의 신호 범위 내에 물리적으로 존재하지 않아도 되기 때문에 드론의 무력화나 체포를 어렵게 만들 수 있다. 현재 드론은 폭력 범죄에는 사용되고 있지 않지만, 정확한 목표물을 설정하면(비행기 엔진 등), 드론의 질량에너지나 운동 에너지가 잠재적으로 위험이 될 수 있으며 무기를 탑재할 가능성도 있다. 특히 이러한 드론이 집단적으로 사용될 경우 위협이 증가한다.

또한, 오히려 **AI 안면 인식을 속이는 현상**이 발생할 수도 있다. 경찰이나 안보 서비스 제공 업체 등은 공공장소에서 용의자 추적을 위해 이미 자동화된 안면 인식 AI 시스템을 쓰고 있다. 국경 지역에서 여객 신원 확인 절차의 신속화를 위해 쓰이기도 하는데, 이런 신원 확인에 있어 모핑(morphing)[32] 공격 등과 같이, 한 개의 사진이나 ID를 통해(예를

31) LG CNS(2020.2.13.)
32) 하나의 형체가 전혀 다른 이미지로 변화하는 기법

들어 여권) 여러 명의 개인이 통과하는 등 악용을 할 수도 있다.

마지막으로 AI가 주가조작을 잡아내기도 하지만 역으로 **AI가 시장 교란을 야기**하는데 쓰일 수도 있다. 높은 빈도나 패턴화의 거래를 통해 경쟁사에게 피해 주거나, 환율이나 경제 시스템에 피해를 줄 수도 있다.[33]

(2) AI 기반 범죄에 대한 대응

신기술에 따른 필연적인 관련 범죄의 출현과 이에 대한 대응은 점차적으로 증가할 것이다. AI를 기반으로 한 범죄에 대해서는 그 처벌에 대한 논란이 크다. 법률적인 측면에서 기존의 법으로는 인공지능 자체에 형사책임을 물을 수는 없다. 인공지능 기술을 개발하고 관련 서비스를 제공한 회사가 형사 처벌 대상이 된다. 인공지능 범죄는 고의범과 과실범으로 나뉠 수 있는데 고의범의 경우 현행 법체계 하에서 처벌하는데 문제가 없지만, 과실범은 인공지능의 역량(강 인공지능, 약 인공지능)에 따라 프로그래머의 개입 정도가 다르기 때문에 누구에게 책임을 물을지도 달라진다.[34]

AI의 법적 지위를 명확히 하여 범죄의 책임을 규명하는 것이 방법이 될 수 있지만 현재 AI는 법인격이 없으며 범죄의 책임 또한 명확한 논리 구조가 부족한 상황이다. 처벌은 흔히 금전적 배상이나, 신체활동 자유의 억압 형태로 이뤄지나 둘 다 인공지능에는 적용할 수 없다. 설령 인공지능 자체를 삭제시키는 등의 처벌이 존재한다고 하여도 인공지능이 처벌을 두려워하지는 않을 것이다.[35] 설계자와 제작자, 사용자가 책임을 분배해야 한다는 주장이 존재하나 기술의 발전에 따라 맹점이 발생하고 있다. 또한 개발자, 사용자가 의도하지 않았고 사전 지식도 없었던 케이스도 존재할 수 있다.[36]

법적인 대응뿐만 아니라 기술적인 대응도 필요하다. 크게 논란이 되고 있는 딥페이크의 경우, 페이스북은 최근 1,000만 달러(약 120억 원)를 투자해 딥페이크 영상 탐지 기술

33) M. Caldwell, J. T. A. Andrews, T. Tanay and L. D. Grifn(2020)
34) IT Times(2019.11.12.)
35) 차미영(2020.05.11.)
36) King, Thomas C., Nikita Aggarwal, Mariarosaria Taddeo, Luciano Floridi(2019)

개발을 시작했다. 구글은 문자를 음성으로 바꾸는 자사 기술을 거꾸로 활용해 영상 속 발언자가 직접 자신이 한 말인지 인증하는 기술을 개발하고 있고, 어도비는 유포된 콘텐츠에 대해 자신이 직접 제작에 참여했는지 인증하는 기술을 개발하고 있다. 누가, 어디서, 어떻게 만들었는지 정보를 사진과 영상에 미리 입력해 진위를 구분하자는 것이다. 세계적 비영리 AI 연구 단체인 'AI 파운데이션'은 AI의 안전한 사용을 위해 올해 대선 기간 언론·정당 등에 문제 소지가 있는 영상, 이미지 등을 분석해 딥페이크 여부를 파악해 주는 서비스를 제공하기로 했다.

작년만 해도 온라인에 유통되던 딥페이크 영상들은 AI가 정지화면을 학습해 만든것이기 때문에 눈을 깜빡이는 장면이 거의 없어 미 국방부 산하 방위고등연구계획국(DARPA)는 이 허점을 토대로 딥페이크 영상을 잡아내는 AI 프로그램을 개발했지만 최근에는 눈동자를 깜박이는 장면이 담긴 딥페이크도 등장했다. 컴퓨터와 바이러스를 잡기 위한 백신처럼 AI 범죄를 AI 기술로 대응하고 있지만, 끊임없이 진화하여 쉽게 끝나지 않는 전쟁이 될 것으로 보인다.[37]

4. 결론

본 고에서 살펴본 바와 같이 AI는 범죄예방과 범죄 수사 및 대응 등에서 전통적인 방식으로는 불가능했던 부분을 가능케 해주며 다양한 종류의 범죄 대응에서 크게 활약하고 있다. 특히 최근 발생하는 범죄들의 수법이 교묘해지고 디지털 범죄, 지능 범죄가 늘어나 새로운 범죄 양상은 온라인에서 비선형화 되거나 숨겨져 있는 경우가 많아 AI의 활용성이 더 커졌다고도 볼 수 있다. 하지만, AI의 법적 지위와 책임성의 문제, 가상공간에서의 수사 한계와 데이터 사용이라는 개인정보 침해 우려 등 AI의 적극적이고 대중적인 사용을 위해서는 아직 장애물이 많이 남아있다.

37) 조선비즈(2019.12.02.)

또한, 양날의 검과 같이 AI 기술의 발달로 인해 AI를 악용한 범죄들도 발전하고 있는 것을 살펴볼 수 있었다. 따라서 AI 기술 발달과 동시에 이에 수반되는 다양한 부작용에 대응하여 발 빠른 제도적 대응 및 과학수사 기술의 개발도 어느 때보다 더 필요할 것이다.

〈참고문헌〉

구태언(2019.11.12.), “[연재] 인공지능이 범인이라면 처벌은 어떻게 할까? (2)”. IT Times.

뉴스토마토(2019.08.08.), “시중은행, AI로 금융사기 잡는다…보이스피싱 피해 예방 체계 구축 분주”.

동아사이언스(2020.04.06.), “불법 영상 콕 집어 삭제... AI가 ...AI가 'n번방'의 눈물 닦아줄까”.

동아사이언스(2020.07.03.), “AI가 범죄 연결성 찾아내 꽁꽁 숨은 익명 범죄자까지 찾아낸다”.

사이언스모니터(2019.07.22.), “디지털 성범죄 피해영상 유포 방지에 AI활용”.

서울경제(2020.06.03.), “KBS몰카 사태에…몰카 탐지 벤처·중기 "반드시 찾는다".

서울시 보도자료(2018.08.22.), “서울시,'인공지능(AI) 수사관' 국내 최초 도입… 민생범죄 잡는다”.

위키트리(2020.05.08.), “지금까지와는 완전히 차원이 다른 ‘몰래카메라 탐지 어플’이 나왔다”.

시사저널e(2020.05.23.), “은행권, AI로 부정대출·금융사기 등 금융보안 강화”.

조선비즈(2019.12.02.), “AI가 만드는 가짜 동영상… 이젠 AI가 속속 걸러낸다”.

차미영(2020.05.11.), “[차미영의 미래를 묻다] 잘못 저지른 인공지능, 처벌할 수 있을까”, 중앙일보.

Bloter(2018.06.08.), “[IT열쇳말] GAN(생성적 적대 신경망)”.

ETRI(2019.2). “지능형 치안 기술 동향”. 한국전자통신연구원.

IT Times(2019.11.12.), "[연재] 인공지능이 범인이라면 처벌은 어떻게 할까? (2)".
IT조선(2018.12.28.), "[대학생 이슈 리포트] 범죄 수사에 AI기술의 적용".
IT조선(2020.06.07.), "n번방 사태 AI로 막는다".
LG CNS(2020.2.13.), "머신러닝 보안 취약점! 적대적 공격의 4가지 유형".
Techdaily(2020.06.15.), "[Tech Trend] "AI가 아동학대 징후 감지한다"…日에 솔루션 등장",
TheScienceMonitor(2020.01.02.), "AI 예측적 영상보안, 성범죄 및 4대범죄 선제 대응".
ZDNetKorea(2018.1.17.), "AI탐정, 범죄현장에 투입된다".

Chinadaily(2019.06.04.), "Police using AI to trace long-missing children".
Emerj(2019.02.02.), "AI for Crime Prevention and Detection – 5 Current Applications".
IBM(2019). "Fighting financial crime with AI".
King, Thomas C., Nikita Aggarwal, Mariarosaria Taddeo, Luciano Floridi (2019). "Artificial Intelligence Crime: An Interdisciplinary Analysis of Forseeable Threats and Solutions". Science and Engineering Ethis(2020), 26:89-120.
Lin Erin, Rongjun Qin, Jared Edgerton, Deren Kong(2020). "Crater detection from commercial satellite imagery to estimate unexploded ordnance in Cambodian agricultural land." PLOS ONE.
M. Caldwell, J. T. A. Andrews, T. Tanay and L. D. Grifn(2020). "AI enabled future crime." Crime Science, (2020)9:14.
Naveen Joshi(2019.11.30.), "The rise of AI in crime prevention and detection", 2020.07.06., https://www.allerin.com/blog/the-rise-of-ai-in-crime-prevention-and-detection.
OECD(2019). "AI in Society".
Qumodo (2019.7.12.), "Ground-breaking AI to combat Child Exploitation".

UNICRI(2019). “Artificial Intelligence and Robotics for Law Enforcement.”

웹사이트

Predpol 웹사이트: https://predpol.com/

Shotspotter 홈페이지: https://www.shotspotter.com/