ETRI Insight
Insight Report 2019-25

국가지능화 특집

사이버범죄 대응을 위한 국가지능화 적용 방향

하영욱 ● hahaa@etri.re.kr
기술정책연구본부

사이버범죄는 모든 사람과 접촉 가능하다는 측면에서 영향력이 매우 크다고 할 수 있는데, McAfee & CSIS(2018)의 추정에 의하면, 사이버범죄에 따른 피해금액은 2014년 $500 bil 혹은 전세계 소득의 0.7%에서 2018년에는 $600 bil 혹은 전세계 소득의 0.8%로 증가하였다. 또한 AI와 IoT의 확산에 따라 사이버범죄는 보다 고도화되고 범죄 대상 범위가 방대해지며, AI의 무력화를 기반으로 한 새로운 공격의 등장이 예상된다. 이에 따라 사이버범죄에 대한 대응은, 알려진 위협에 대한 대응이라는 기존의 대응 체계에서 새로운 위협에 대한 대응이 가능한 체계로 패러다임이 수정되어야 할 것이다. 국가지능화는 알려지지 않은 바이러스 및 악성 코드 대응, 콘텐츠 실시간/자동 검열 등으로 현재 및 미래의 사이버범죄에 대한 대응에 기여할 것으로 예상된다. 국가지능화가 사이버범죄 대응에 원활히 작동하기 위해서는, 행정적인 실행력 강화뿐만 아니라 기반 산업 및 기초 기술의 지원이 동시에 요구되는데, 본고에서는 이에 대한 세부적인 대안이나 예시도 다루었다.

1 사이버범죄의 개념

사이버범죄는 '00년 오키나와에서 있었던 선진국 수뇌회의에서 처음으로 사용된 용어로, 개념이나 분류에 대해서는 다양한 의견이 존재한다.[1] 그러나 대체로 ICT기술을 악용한 사이버공간에서의 범죄 행위를 의미한다고 할 수 있다. 사이버범죄는 해킹이나 바이러스와 같이 기술 발달에 따라 새롭게 등장한 범죄유형과 전자상거래 사기나 사이버 명예훼손 등 기존의 범죄행위에 ICT기술이 사용되는 유형으로 크게 구분이 가능하다.[2]

경찰청에서는 사이버범죄를 '고도정보통신 네트워크를 이용한 범죄나 컴퓨터 또는 전자적 기록을 대상으로 한 범죄 등 정보기술을 이용한 범죄'로 정의하고 있으며, 유형에 대해서는 2013년 이전에는 사이버범죄를 테러형 범죄와 일반 사이버범죄로 구분하였으나, 새로운 유형의 사이버범죄의 등장에 따라 2014년부터는 사이버범죄의 유형을 정보통신망 침해범죄, 정보통신망 이용범죄, 그리고 불법 콘텐츠 범죄로 구분하고 있다(법무법인 수호, 2017).

표 1 사이버범죄의 유형 구분

舊 사이버범죄	新 사이버범죄	범죄 행위
테러형 범죄	정보통신망 침해범죄	해킹, 계정도용, 단순침입, 자료유출 및 훼손, 디도스, 악성프로그램 등
일반 사이버범죄	정보통신망 이용범죄	온라인 사기, 게임 사기, 피싱, 파밍, 몸캠피싱, 스팸메일, 개인위치정보 침해 등
	불법 콘텐츠 범죄	사이버 음란물 배포/판매/전시, 사이버 도박, 사이버 모욕, 청소년유해매체물 등

※ 출처: 법무법인 수호(2017) 자료 재구성

사이버범죄와 연관된 개념으로 컴퓨터범죄, 사이버보안, 그리고 사이버안보 등이 있다. 컴퓨터범죄는 인터넷이 발달하기 전에 컴퓨터·프로그램·데이터에 국한되어 사용된 개념인데, 현재와 같은 신종 범죄들이 등장함에 따라 사이버범죄라는 용어로 바뀌게 되었다. 사이버보안이라는 개념은 사이버공간에서의 범죄 방지·예방을 위한 사전적인 의미인 반면, 사이버범죄는 범죄행위 및 처벌 등의 사후적인 의미로 해석될 수 있다.[3] 한편 사이버안보는 산업, 행정, 국방 등 국가 전반과 개인·기업·정부 등 모든 주체들을 포괄하는 범위로 볼 수 있으며, 이때 사이버범죄라는 것은 사이버안보를 위협하는 공격 중의 일부분으로 이해될 수 있다.[4]

1) 법무법인 수호(2017), 사이버범죄 예방 기본법 제정에 관한 연구.
2) Yar(2005), "The novelty of 'cybercrime' - An assessment in light of routine activity theory" 에서는 사이버범죄를 컴퓨터가 지원된 범죄와 컴퓨터가 중심이 된 범죄로 크게 구분
3) 법제처(2014), 2014 세계법제 연구보고서.

2 사이버범죄의 심각화

사이버범죄는 온라인을 이용하는 모든 사람과 접촉 가능하다는 측면에서 영향력이 매우 크다. 사이버범죄는 법 집행의 사각 지대에서 성행하며, 기밀 정보손실, 생산 및 서비스 중단, 온라인 사기, 복구비용, 기업 이미지 손실 등을 포함한 사이버범죄 비용은 국가 경제의 상당 부분을 잠식하고 있고 시간이 갈수록 늘어나고 있다. McAfee & CSIS(2018)의 추정에 의하면, 사이버범죄에 따른 피해금액은 2014년 $500 bil 혹은 전세계 소득의 0.7%에서 2018년에는 $600 bil 혹은 전세계 소득의 0.8%로 증가한 것으로 추정되었다.[5)]

이와 같이 사이버범죄가 증가하는 원인은 여러 가지가 있다. 먼저 사이버 범죄자들이 신기술을 발 빠르게 도입하고 있다는 점이다. 신기술은 맬웨어 생성을 자동화 시키고, Cybercrime-as-a-Service는 사이버범죄를 저비용으로 손쉽게 수행할 수 있도록 도와준다.[6)] 다음으로 암시장의 발달과 가상화폐 시장 활성화는 사이버범죄로 취득한 데이터의 현금화를 용이하게 만든다. 즉, 도난당한 개인정보는 암시장에서 중개인 및 기타 중개인과 관련된 복잡한 거래를 사용하여 “Dark Web”에서 대량으로 판매되며, 가상화폐는 랜섬웨어 결제를 보다 쉽게 하고 추적하기 어렵게 만든다. 마지막으로 사이버보안이 취약한 저소득 국가 중심으로 온라인 신규 가입자가 폭발적으로 증가하는 것이 주요한 원인 중의 하나인데, 실제 아프리카에서 사이버범죄 비용이 국가 소득에서 차지하는 비중은 크게 높아지고 있는 추세이다.[7)]

한편 사이버범죄는 AI와 IoT의 확산에 따라 더욱 기승을 부릴 것으로 예상된다. 우선 AI의 경우, NIA(2018)[8)]은 AI로 변화되는 두 가지 위협을 예상하고 있다. 첫째 기존의 위협이 확대될 수 있다. 즉, 효율적인 AI 기술의 확산으로 사이버 공격이 용이해 짐에 따라 결과적으로 공격자 수와 공격 속도가 증가하게 되고 공격 대상도 확대된다. 또한 공격 대상의 정밀 표적이 가능하게 됨에 따라, 특정인과 단체를 대상으로 한 스피어피싱(spear phishing)이 활성화 될 가능성이 높다. 둘째, AI가 자동 로봇 및 악성코드 동작을 제어한다든지, 혹은 AI가 적용된 사회 인프라의 취약점을 역으로 공격하는 등으로 새로운 위협의 출현이 예상된다. 구글은 AI 인식 교란 스티커에 의해 AI가 비정상적으로 인지되는 실험을 수행한 적이 있는데, 예를 들어 자율주행자동차의 인지적 약점을 노린 사고 유도가 충분히 발생 가능하다. 또한 음성 모방을 통한 사칭이나, 합성 기술을 이용한 가짜 뉴스 전파가 성행할 수도 있다.

---

4) 관계부처 합동(2019), 국가 사이버안보 기본계획.
5) McAfee & CSIS(2018), Economic impact of cybercrime – No slowing down.
6) 디도스 공격을 실시하기 위해 일주일 동안 봇넷을 빌리는 비용이 150달러 정도에 불과
7) McAfee & CSIS(2018)에 의하면, 아프리카는 GDP 대비 사이버범죄 비용이 2014년 0.07%에서 2018년 0.20%로 약 세 배 증가
8) NIA(2018), 향후 5년 후 개발 가능한 기술을 바탕으로 예상되는 악용 사례와 대응 방안.

다음으로 IoT의 도입 확산 및 커넥티드 디바이스 수 증가에 따른 위협 증가가 예상된다. IoT는 가치가 없지만 개인 정보를 도용하거나 중요한 데이터 또는 네트워크에 접근할 수 있는 새롭고 쉬운 방법을 제공해 줄 수 있다. PC와 네트워크로 연결된 수백만 대의 프린터나 IoT 장치들은 최신 보안 패치가 설치되어 있지 않아, 민감한 데이터로의 접근이 무방비 상태로 노출되어 있어 전체 인프라가 위험에 빠질 수 있다.[9)]

3 주요국들의 사이버범죄 대응 동향

주요 국가들은 국내보다 앞서 사이버안보 국가전략을 수립하였는데, 사이버범죄를 사이버안보의 주요 하부 전략에 포함하고 있다. 또한 신기술로 사이버범죄가 고도화됨에 따라 사이버범죄에 대응하기 위한 국가 전략이 마련되고 법 정비가 이행되고 있다.

최근에는 AI를 이용하여 사이버범죄를 해결하거나 잠재적인 AI의 부작용을 방지하기 위한 계획들이 발표되고 있다. 미국은 '미국 AI 이니셔티브 (2019.2.)'를 통해 AI의 안전하고 윤리적인 사용을 보장하는 AI 관리를 미국 AI 국가전략의 5대 핵심영역 중 하나로 설정하는 등[10)], AI의 부작용을 방지하기 위한 전략 마련에도 관심을 가지고 있다. 사이버 안전 규제 관련 가장 선도적인 위치에 있는 영국은, '영국의 AI: 준비, 의지, 가능성 (2018.4.)'에서 AI의 범죄 활용 위험을 완화하기 위하여 펀딩 시 AI 관련 기술 개발의 오용을 방지할 수 있는 세부 절차를 마련하도록 하고, 데이터 방해 행위에 대한 공공/민간 데이터셋 보호와 관련한 추가 연구를 권고하였다. 일본은 2020년 도쿄 올림픽을 앞두고 특별히 사이버보안의 중요성을 인식하고 있는데, 'AI 전략 2019'에서 사이버 공격을 AI로 해결하기 위한 R&D 전략 프로그램을 마련하였다. 구체적으로는 AI를 이용하여 하드웨어 동작의 부정 기능을 검출하는 예방, 대량 패킷 정보 분석을 통한 감지, 그리고 알람 자동 추출로 대응하는 프로그램이다.[11)]

우리나라도 AI를 활용한 사이버범죄 대응에 적극적이다. 행정안전부는 '지능형 정부 기본계획(2017)'에서 AI를 기반으로 최신 보안위협을 스스로 학습하고 체계적으로 대응 및 방어하는 자가진화형 사이버 안전 기반 구축 계획을 포함하였는데, 여기에는 AI 오작동, IoT 인프라 보안, 개인정보 유출 등의 위협에 대한 자가진화형 대응 방향이 간략히 제시되었다.[12)] 과학기술정보통신부의 'AI R&D 전략(2018)'에서는 AI가 통제 가능한 상태를 유지하도록 모니터링하는 기술 등 AI의 부작용을 방지하기 위한 R&D 과제를 선정하였다.[13)] 관계부처합동의 '제6차 국가정보화 기본계획(2018)'은 국가 지능화 계획으로 사

9) HP(2018), 2018 사이버보안 지침.
10) 백악관 홈페이지, https://www.whitehouse.gov.
11) SPRI(2019), 일본의 인공지능 전략 동향: AI 전략 2019.
12) 행정안전부(2017), 지능형 정부 기본계획.

이버범죄 관련, 정보보호 예방/대응 능력 강화, 정보보호 산업 육성, 그리고 통신망 재난 안전성 강화 등의 실행 아이템들을 포함하고 있고, 특히 AI를 기반으로 신규 보안 위협에 대응하고 IoT 기기 보안을 강화하는 등 신기술 발전에 대응하는 계획이 담겨져 있다.[14]

4 국가지능화의 적용 방안

앞서 살펴본 사이버범죄의 발전 방향에 대한 내용을 재구성해보면, ①사이버범죄는 기술의 진화와 신기술의 도입에 따라 보다 고도화되고, ②범죄 대상 범위는 방대해지며, ③AI를 무력화 혹은 역이용하는 새로운 공격이 등장할 전망이다.

이를 보다 구체적으로 살펴보면 다음과 같다. 먼저 사실과 사실이 아닌 것의 구분이 모호해 짐에 따라 온라인 사기와 사이버 명예훼손 등이 더욱 고도화될 것이다. 온라인 사기의 경우 기존에는 특정 정보에 익숙하지 않은 사람들이 주로 범죄의 피해자가 되었다면, 미래에는 웹페이지 등이 진짜와 가짜를 구분하기 어려울 정도로 정교해짐에 따라 온라인 쇼핑을 이용하는 사람들 대부분이 범죄에 노출될 것이며, 이는 온라인 쇼핑과 기업에 대한 신뢰감 하락으로 연결될 것이다. 사이버 명예훼손 또한 고도화 것으로 예상되는데, 현재는 소수의 인원이 정략적으로 여론을 호도하고 비방하는 악의적인 댓글로 인식공격을 수행했다면, 향후에는 특정인의 가짜 사진/동영상을 제작 및 배포하여 명예를 훼손하는 것도 훨씬 손쉽게 이루어질 것이다. 또한 AI의 고도화에 개인 또는 집단의 방대한 정보 수집을 결합한 스피어피싱의 범람도 주요 우려사항 중 하나가 될 것이다.

다음으로 범죄 대상과 불법 콘텐츠의 방대화가 예상된다. 지금도 수천 개의 하부 프로그램 조각들이 자동으로 조합되면서 하루 수십만 개의 새로운 맬웨어가 추적되고 있는데, AI가 하루 24시간 일하는 시점에는 새로운 맬웨어가 더욱 폭증할 것이다. 기관이나 개인의 주요 컴퓨팅 시스템을 중심으로 행해지던 해킹은 IoT의 확산에 따라 네트워크에 연결된 프린터나 CCTV 등 다양한 주변기기들을 목표로 한 해킹으로 발전할 전망이다. 또한 불법 콘텐츠 유통이 기존에는 공공의 감시망을 피해 은밀하게 진행되어 왔다면 향후에는 보다 지능적으로 유통 경로가 재설정되어 일반인에게 전달될 것으로 예상된다.

마지막으로 AI가 가지고 있는 치명적인 약점을 뚫고 행해지는 범죄가 우려된다. 앞에서도 언급한 것과 같이 드론이나 자율주행자동차를 해킹하여 사고를 유도하게 할 수도 있으며, 혹은 잘못된 학습 데이터를 주입함에 따라 제품의 치명적인 오류를 발생하게 만들어 AI 서비스 업체에게 큰 타격을 미치게 할 수도 있다.

13) 과학기술정보통신부(2018), I-Korea 4.0 실현을 위한 인공지능(AI) R&D 전략.
14) 관계부처합동(2018), 제6차 국가정보화 기본계획.

표 2 사이버범죄의 진화와 국가지능화의 기여

	As is	To be
사이버범죄	- 사람의 인지력을 흐려 사기 - 불특정 다수를 타깃으로 범행 - 불법 콘텐츠의 은밀한 유통 - 맬웨어, 악성코드 - 컴퓨터 메인 시스템 해킹 - 랜섬웨어, 디도스 등	- (고도화) 진짜와 가짜의 구분 모호로 사기 폭증 및 명예 훼손 고도화, 특정 사람과 특정 그룹 타깃의 범행 - (방대화) 불법 콘텐츠 감시망의 무용화, 신종 맬웨어의 폭증, IoT 해킹 - (무력화) 드론/자율차 사고 유도 등
예방 및 대응	[알려진 위협에 대한 대응] - 위험 고지 및 관련 정보 제공 - 알려진 맬웨어에 대한 패치 배포 - 시민의 자발적 신고 - 수동 검열 (사이트 접속 차단)	[알려진 + 새로운 위협에의 대응: 지능화 기여] - 알려지지 않은 바이러스 및 악성 코드 대응 - 콘텐츠 실시간/자동 검열 - 자동 증거 수집 및 빠른 검거 - 안전한 드론/자율차 및 강건한 IoT 보안

사이버범죄에 대응하기 위해, 현재는 경찰청 등 정부기관에서 시민의 자발적 신고 등 여러 경로를 통해 수집된 사이버범죄와 관련된 정보를 토대로 금융거래 시 위험을 고지해주고, 불법 콘텐츠 유통이 예상되는 웹페이지 접속을 차단하고 있으며, 앱을 통해 사이트의 사기이력을 조회해 주거나 맬웨어를 검사할 수 있도록 지원해 주고 있다. 이와 같이 현재의 사이버범죄의 예방 및 대응 체계는 알려진 위협에 대한 대응 수준에 그치고 있는 실정으로, 시간이 지날수록 사이버범죄의 진화에 적절히 대응하기 어려운 상황에 내몰리게 될 것으로 예상된다.

따라서 사이버범죄의 진화에 따라 알려진 위협에 대한 대응뿐만 아니라 새로운 사이버범죄에 대한 대응이라는 패러다임의 전환이 요구된다. 이러한 사이버범죄 대응 패러다임 변화에 국가지능화가 적용될 수 있는데, 여기서는 국가지능화의 사이버범죄 예방과 대응에 대한 네 가지 기여부분을 제시하고자 한다. 첫째, 알려지지 않은 바이러스 및 악성 코드에도 대응하도록 패치 프로그램을 지능화 하는 것이다. 패치 프로그램은 공공기관이나 신뢰성 있는 기업체에서 지속적인 학습을 수행하고, 수요자에게 제공 시에는 손쉬운 방법의 업그레이드 방법이 고안되어야 할 것이다. 둘째, 불법 콘텐츠의 실시간 및 자동 검열이다. 인터넷/통신 서비스를 제공하고 있는 사업자가 자체 네트워크에서 유통되는 불법 콘텐츠를 검열하거나, 콘텐츠 플랫폼을 제공하는 서비스 사업자의 자체 서버 검열, 혹은 최종 수요자의 단말에서 불법 콘텐츠를 지능적으로 차단하는 등의 방법이 있을 수 있다. 어떠한 경우라도 매우 빠른 처리 속도가 요구될 것으로 예상되는데, 이 경우 AI 반도체의 활용이 필수적으로 요구될 것으로 판단된다. 셋째, 고도화된 사이버범죄에 대한 대응으로써 자동 증거 수집 및 빠른 검거 지원이다. 물론 이를 위한 관련법 정비가 선행되어야 하겠지만, 현재의 사이버범죄는 복합적인 특성으로 명확한 법 적용이 모호하고 익명 등의 방법으로 범죄자의 식별이 어려우므로, 이의 해결을 위한 자동적인 증거 수집과 빠른 범

죄행위 규정 및 범죄인 식별에 대한 의사결정 지원이 필요할 것이다. 넷째, 안전한 드론/자율차 및 강건한 IoT 보안을 국가정보화가 지원해 줄 것으로 판단된다. 블록체인 기술을 결합하여 신뢰할 만한 학습 데이터를 제공할 수 있으며, 화이트 해커에 의한 침투 프로그램과 방어 기술 개발로 강건한 보안 시스템을 구축할 수 있을 것이다.

5 지능화 추진을 위한 주요 과제

사이버범죄에 국가지능화를 효율적으로 적용하기 위해 규제 실행력의 제고, 산업 육성, 그리고 R&D 투자라는 세 가지 과제 유형을 제시하고자 한다.

먼저 사이버범죄는 법/규제의 실행에 직접적으로 영향을 받게 된다. 현재는 근거 법령이 20개 이상으로 산재해 있는 상황이라 복합적 성격의 사이버범죄를 규정하는 데 어려움이 있다. 정보통신망법은 사이버범죄에 대해 종합적인 처벌 규정을 담고 있으나 적극적인 사이버범죄 예방에 대한 근거는 충분하지 않으므로 신속하고 종합적인 예방과 대응을 위해 단일법 제정과 같은 법/규제 정비가 요구된다(법무법인 수호, 2017). 정비되는 법/규제는 AI가 저지르는 범죄와 같은 새로운 유형의 범죄에 대한 내용을 포괄할 수 있어야 할 것이다. 또한 사이버범죄는 다양한 부처에서 다루고 있고 정보의 수집 및 분석 능력 또한 부처별로 차이가 존재한다. 이에 따라 정보의 중복수집이나 필요한 정보를 필요한 곳에서 확보하지 못하는 등의 비효율이 발생하고 있다. 따라서 현행 '정보통신망법'에 규정되어 있는 '정보의 공동활용체제'에 대한 실효성을 확보할 수 있도록 '사이버범죄 빅데이터 센터'와 같은 조직을 신설하거나 기존의 조직 역할을 확대할 필요성이 있다. 센터는 실시간 정보 및 증거를 자동으로 수집하고 1차적인 분석을 수행한 후 담당 부처에 분배하여 업무의 효율성과 신속성을 향상할 수 있는 시스템을 갖추어야 한다. 한편 범죄와 관련된 정보 수집을 위해서는 네트워크 및 통신 서비스, 그리고 콘텐츠 서비스를 제공하는 민간 사업자와 협력에 대한 논의가 필요하며, 사이버범죄 상당 부분이 국제적으로 이루어지고 있으므로 국제 협력에도 적극 참여가 필요하다.

다음으로 사이버범죄 관련된 법/규제를 실행하기 위해서는 상용화된 보안 기술 지원이 필요하므로, 이를 위한 산업 활성화가 요구된다. 2/3 이상의 조직들이 숙련된 사이버보안 전문가가 부족하다고 느끼고 있는데[15], AI 기술을 함께 다룰 수 있는 사이버보안 전문가는 이보다 훨씬 더 부족할 것이다. 따라서 사이버보안과 AI를 포괄적으로 다룰 수 있는 인력의 양성이 요구된다. 또한 사이버보안 제품/서비스는 다양함이라는 특성이 있어 중소기업에게 적합한 사업 영역 중 하나이므로, 관련 중소기업의 육성이 필요하다. 이와 더불어 보안 제품/서비스의 외산 의존을 탈피하고 관련 기술력을 축적하기 위해서는, 공공 부

15) Marketsandmarkets(2019), AI in cybersecurity market; Cybrary(2016), Cybersecurity job trends report 재인용

분에서의 수요를 늘여나가는 정책이 유효해 보인다. 공공 조달 이외에, 활용 가능한 양질의 데이터 제공과 컴퓨팅 역량의 지원이 필요한데, 이러한 부분은 공공 기관에서 역할을 할 수 있는 부분이라 판단된다. 한편 올해 하반기 시작되는 AI 활용 사이버보안 국제 표준화 논의에 주도적인 참여가 요구되며, 표준화의 과정 단계에서 민간이 함께 참가하는 방안도 적극 고려해볼만 할 것이다.[16)]

마지막은 사이버범죄 예방 및 대응을 위한 밑바탕이 되는 단계로서 R&D에의 적극적인 투자이다. 빅데이터를 실시간 모니터링하기 위해서는 기반 기술로서 AI 반도체가 필수적인데, 범용의 AI 반도체 개발과는 별개로 사이버보안 기능에 최적화 된 AI 반도체 개발에의 투자가 필요하다. 또한 현실과 구분이 어려운 가짜를 구별하여 걸러내기 위한 기술적 요구가 높은데, 블록체인 기술과 AI를 융합하여 어느 정도 기여가 가능할 것으로 예상된다. 이외에도 사이버범죄의 원인 진단과 조치 방안 마련을 위해 AI 학습이 필요하다. 이를 위해 사이버범죄 빅데이터 분석 기술의 개발이 필요하며, 데이터의 신뢰성을 확보하기 위해 블록체인 기술을 접목하거나 화이트 해커에 의한 침투 테스트 방식을 활용할 수 있다. 다만 화이트 해커의 경우 기업들의 보안 취약점을 잘 알고 있어 범죄 단체의 영입 대상이 될 수 있으므로 이에 대한 방지책도 염두에 두어야 할 것이다.

표 3 사이버범죄 해결을 위한 국가지능화 과제

유형	주요 과제	예제
규제 실행력 제고	- 법/규제 정비 - 지속 모니터링/분석, 정보 공유/재분배 위한 조직 역량 강화 - 협력 강화 (민간협력 및 국제협력)	- 사이버범죄 단일법 제정, AI가 저지르는 범죄/사고에 대한 규정 - 사이버범죄 빅데이터 센터 - 사이버범죄 정보 공유 (민간 및 국제)
산업 육성	- 사이버보안 전문 인력 양성 - 중소 업체 지원 - AI + 사이버보안 표준 정립	- 사이버보안 + AI 전공 과정 개설 - 국산 사이버보안 SW 공공조달, 공공기관의 컴퓨팅 자원 지원, 빅데이터 지원 - AI + 사이버보안 국제 표준 주도
R&D 투자	- AI 반도체 개발 - Real vs. fake 구분 기술 - AI 학습: 사이버범죄 빅데이터 분석, 블록체인/침투프로그램, AI 부작용 방지	- 서버용 AI 반도체, 네트워크 감시용 AI 반도체, Edge용 AI 반도체 - 블록체인 기술 기반 Real vs. fake 구분 - 지속 학습 가능 사이버보안 AI SW

16) 아이뉴스(2019.2.11.), AI 사이버보안, 국제표준 주도권 누구 손에? (http://www.inews24.com/view/1156488)

www.etri.re.kr

본 보고서는 ETRI 기술정책연구본부 주요사업인 "ICT R&D 경쟁력 제고를 위한 기술경제 및 표준화 연구"를 통해 작성된 결과물입니다.

ETRI Electronics and Telecommunications Research Institute

34129 대전광역시 유성구 가정로 218
TEL. (042) 860-6114 FAX. (042) 860-6504