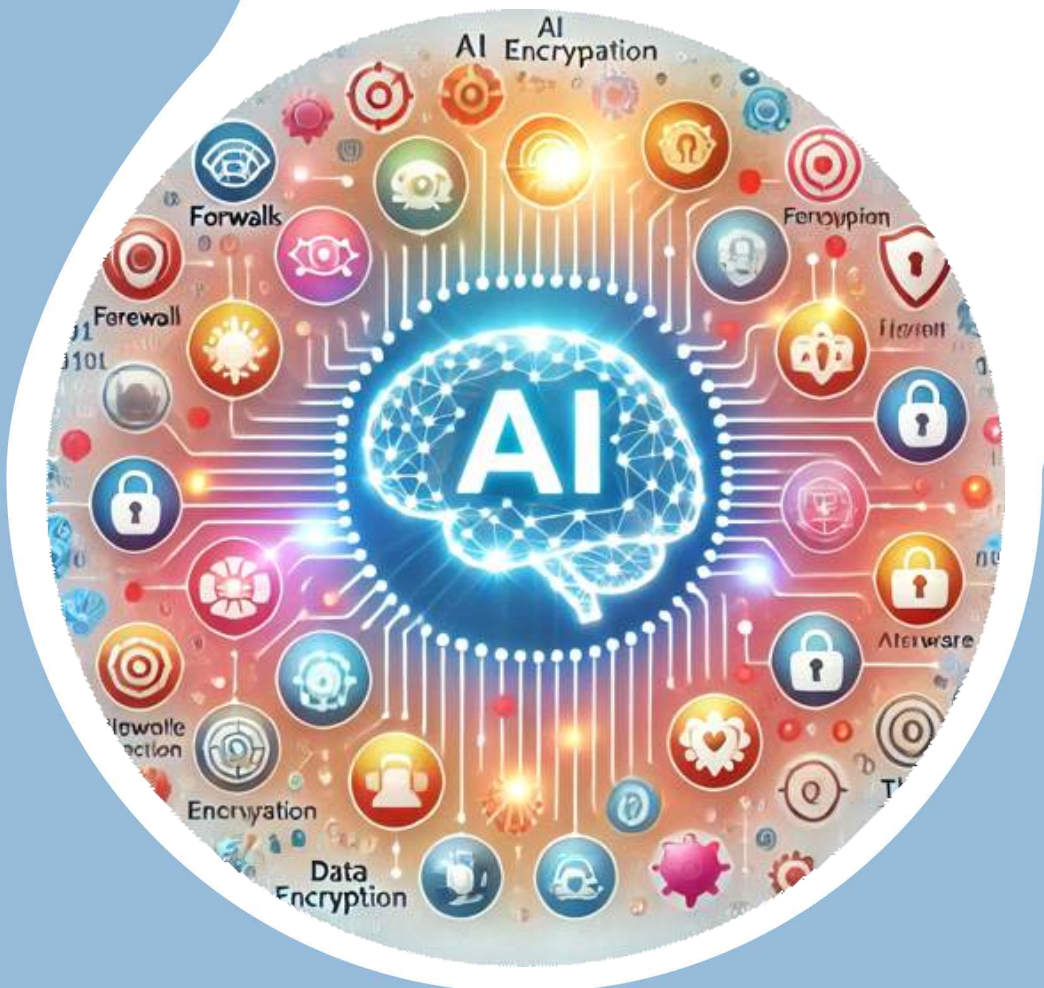
AI 분야 규제 동향보고서

EU 인공지능 법(AI Act)

2024. 12



산업통상자원부
국가기술표준원

가천대학교
Gachon University

TBT 종합지원센터
R&I Center

요약문

보고서 작성 목적

- 본 보고서는 디지털 전환의 과정에서 나타나고 있는 문제점 중에서 AI 사이버 보안 문제를 위험 요소와 함께 기회적인 부분을 살펴보고, 이를 둘러싼 국내외 동향과 대응 방향을 파악하고자 함

디지털 전환 과정에서 AI 사이버 보안 문제의 등장

- 사이버 보안은 악의적인 의도를 가지고 시스템, 네트워크 등에 접근하는 시도를 사전에 차단하는 다양한 활동을 의미하는데, 개인이 사용하는 로그인 암호, 금융기관 인증서, 개인 통신 메시지, 개인 간 금융 거래 장부부터, 국가 기간망, 전력망, 무기체계, 금융정보까지 다양한 사이버 보안 분야가 망라되어 있음

글로벌 AI 사이버 보안 동향

- 글로벌 AI 사이버 보안 규제 동향으로는 2024년 8월부터 발효된 세계 최초의 인공지능 규제법안인 EU AI Act가 대표적임
  - 이 법안은 인공지능의 활용으로 인한 위험을 최소화하고 신뢰할 수 있는 AI 개발을 장려하는 규제로 가장 최근에 발효되었고, 증가하는 사이버 보안에 대한 위험에 대응하기 위해 AI 개발과 배포의 책임성, 투명성을 요구한다는 점을 강조함
- EU AI Act는 AI 시스템을 위험 관점에서 금지된 위험, 고위험, 제한된 위험, 저위험 등으로 분류하여 규제하고 있음
  - 만약 기업이나 정부가 고위험 AI 시스템 중 하나인 사이버 공격 탐지 AI 시스템을 개발하거나 활용하고자 할 때, EU AI Act를 준수함으로써 해외 수출은 물론 사이버 보안을 더욱 강화할 수 있을 것임

결론

- 시사점
  - 최근 인공지능의 영향으로 과거 사이버 보안에서 AI 사이버 보안으로 영역이 확장되고 있음. 사이버 보안은 AI가 새로운 방식의 사이버 공격 도구가 되기도 하지만 역으로 예방하고 감시하는 기술로도 발전할 가능성이 있으므로, 비즈니스 차원에서만이 아니라 국가 차원에서 이를 적극 개발할 필요가 있음
- 대응 방안
  - 따라서 글로벌 규제법안 검토 및 사이버 공격에 대응하는 국제 사이버 협력 네트워크에 참여하여 국제간 협력을 통한 사이버 보안 능력 제고에 적극 대응해야 할 것임

CONTENTS

Chapter 01

서론

1. 개요

2. 구성 및 주요 내용

PART 01

개요

디지털 전환, 인공지능(AI, artificial intelligence) 기술의 시대

디지털 전환

- 아날로그 형태를 디지털 형태로 변환하는 '전산화(digitization)' 단계를 넘어 사회 전반에 정보통신기술을 활용하는 '디지털화(digitalization)'를 가속하는 것으로 디지털 기술을 사회 전반에 적용하여 전통적인 사회 구조를 혁신시키는 것을 지칭함
- 일반적으로 기업에서 사물인터넷(IoT), 클라우드 컴퓨팅, 인공지능, 빅데이터 솔루션 등 정보통신기술을 플랫폼으로 구축·활용하여 기존 전통적 운영방식과 서비스 등을 혁신하고 새로운 디지털 사회로 전환하는 것을 의미
- IBM 기업가치연구소의 보고서(2011)는 디지털 전환을 '기업이 디지털과 물리적인 요소들을 통합하여 비즈니스 모델을 변화시키고, 산업에 새로운 방향을 정립하는 전략'이라고 정의함

정보통신기술의 발전과 정보사회

- 21세기 정보통신기술(ICT)의 발전으로 우리 사회는 새로운 변화의 시기를 맞이하고 있음
- 20세기 물질 재화 중심의 대량생산 시스템이 퇴조하고, 21세기 비물질적이고 만질 수 없는 유연한 정보 재화 중심의 맞춤형 지식기반 정보사회로 진화하고 있음
- 정보사회로의 이행 배경에는 1969년 개발된 인터넷의 모체 아르파넷(ARPANET)의 등장에서 그 기원을 찾을 수 있음
- 네트워크의 네트워크인 인터넷은 등장 이후 이를 기반으로 하는 ICT가 비약적으로 발전하며 정보사회(information society)로 이행했고, 인터넷, 스마트폰, 태블릿 PC를 넘어 4차산업혁명 기술인 인공지능, 빅데이터, IoT, 클라우드, 메타버스, 로봇공학, 블록체인, 웨어러블 컴퓨터(wearable computer)까지 등장하는 이른바 '디지털 전환' 단계로 진입함
- 이에 우리 사회는 전통적인 산업사회의 패러다임과 다른 새로운 디지털 정보사회가 등장했다는 평가를 받고 있음

- ICT 발전의 명암
  - 디지털 기반의 ICT 발전은 장점도 있으나, 단점도 존재한다는 것에 주목해야 함

ICT의 긍정적 효과 (낙관론)	▪ 초기 미래학자들(토플러, 나이스비트, 다니엘 벨 등)은 ICT 발전은 이전과 다른 새로운 디지털 기반 시민참여 사회를 만들 것이라 예견 ▪ 디지털 기술을 활용하여 인류의 삶이 편리해지고 만족도가 향상되는 유토피아적인 세계가 가능하다고 예측
ICT의 부정적 효과 (비관론)	▪ 최근 사회과학자들은 ICT의 부정적인 사회현상에 주목하여 부정적인 영향의 가능성을 크게 보고 있음 ▪ 개인정보 유출, 보이스피싱, 악의적 해킹, 민의의 왜곡, 악성댓글, 허위 조작정보(가짜뉴스) 등 ▪ 특히 최근 국내외적으로 사이버 보안 문제가 심각하게 등장

보고서 작성 목적

- 디지털 전환(digital transformation)에 따라 인류는 새로운 위험과 기회의 갈림길에 서게 되었음
  - 기술의 양면성으로 인해 디지털 전환은 인류에서 희망찬 미래와 새로운 기회만을 제공하는 것이 아니라, 디지털 전환 과정에서 새롭게 등장하는 기술적인 문제, 특히 기술의 급격한 발전에 따른 사이버공간(cyberspace) 확대와 부작용의 발생은 필연적이라 할 수 있음
  - 본 보고서는 디지털 기술의 발전에 따라 새롭게 부각되는 사이버 보안(cybersecurity), 특히 AI 사이버 보안(AI cybersecurity) 문제를 살펴보고자 함

- 그 중, 생성형 AI(Generative AI) 등장에 따른 문제점에서 사이버 보안 문제를 중심으로 이를 둘러싼 국내외 동향을 파악하고자 함
  - 사이버 보안(사이버 시큐리티)[1]은 사전적으로 악의적인 의도를 가지고 시스템, 네트워크 등에 접근하는 시도를 사전에 차단하는 다양한 활동을 의미
  - 미시적으로는 개인이 일상적으로 사용하는 로그인 암호부터 금융기관 인증서, 개인 통신 메시지부터 거시적으로는 국가 기간망, 전력망, 무기체계, 금융정보까지 다양한 분야가 망라되어 있음

1) 본 보고서는 보안과 시큐리티(security)가 다소 혼용되어 사용되고 있음

- 현실에서 사이버 보안 문제는 개인의 문제를 넘어 국가 안보를 위협하는 문제로까지 확산하고 있음(김홍선 2023)

  - 2010년대 이후 개인정보 유출 또는 금융정보 유출, 랜섬웨어 등의 개인의 사이버 보안을 넘어 국가 간 사이버 공격 문제는 자주 일어나고 있어 더 이상 놀라운 현상이 아님

  - 최근 나타난 국가 간 사이버 공격 사례

    ① 이란의 핵 개발을 지연시킨 사이버 공격
    ② 이에 대한 복수의 일환으로 보이는 사우디아라비아 국영 석유 회사 아람코(ARAMCO)의 컴퓨터 파괴
    ③ 2016년, 2020년 미국 대통령 선거에서 해킹과 허위 조작정보(가짜뉴스) 유포
    ④ 북한을 영화 소재로 만든 소니 픽처스에 대한 사이버 보복
    ⑤ 우크라이나 국민을 추위와 공포에 떨게 한 난방과 전력 차단 등

  - 이처럼 정치 안보적 요인과 밀접한 관련이 있는 굵직한 사이버 공격 및 보안 사고가 세계 곳곳에서 일어났고 전 세계인의 안전과 인권을 위협하고 있음

- 글로벌 사이버 보안 규제 동향을 미국, 유럽, 중국 등을 중심으로 검토하여, 법·제도적 대응 방안을 체계적으로 살펴보고자 함

  - 국내외적으로 관심이 높아지고 있는 사이버 보안, AI 사이버 보안 문제를 살펴보고 국내외 동향과 산업계에 미칠 영향을 심층적으로 제시하여 글로벌 사이버 보안 규제 관련 EU AI Act, 미국, 중국 등의 법안에서 강조하는 주요 규제, 국내 기업들이 AI 관련 규제에 대응 방안 등 정보를 제공하고자 함

PART 02

구성 및 주요 내용

- 1장 서론
  - 사이버 보안 문제가 가지고 있는 특성을 제시하고 본 보고서 작성의 목적과 보고서 각 장의 내용을 요약 제시함
- 2장 정책 개요
  - 사이버 보안 위험성과 왜 중요한 이유를 살펴보고, 특히 최근 2년 동안 국제관계 속에서 나타난 사례와 공격 유형 및 위험성을 제시함
  - 사이버 보안 비즈니스 영역과 국가 안보 영역에서 다루어지고 있으며, 국가 안보 차원에서 사이버 보안 대응 기술과 정책적 준비 상황에 대해 제시함
- 3장 규제 동향 및 현안
  - 디지털 전환과 4차산업혁명 기술의 발전으로 인공지능 AI를 활용한 새로운 안보 환경이 조성되고 있으며 이에 따른 국내외적인 혼란이 가중되고 있음을 제시함
  - 글로벌 사이버 보안 규제 동향과 AI 규제 동향 및 주요 내용을 제시함
- 4장 향후 일정 및 산업계 대응 방안
  - 글로벌 사이버 보안 규제 관련 향후 일정을 소개함
  - AI 사이버 보안의 위협에 대응하는 움직임으로 기업의 기술적 대응과 국가의 법·제도적 대응을 중심으로 살펴보고, 주요 국가의 AI 사이버 보안 분야에서의 대응 태세에 대해 살펴보고 예측할 수 있는 대응 태세에 대한 논의와 정책 방향을 제시함
- 5장 결론
  - 앞서 제시한 사이버 보안, AI 사이버 보안의 핵심적인 내용을 요약하여 제시하고 우리나라 정부와 기업에 필요한 주요 내용을 요약함

Chapter 02

정책 개요

1. 도입 배경 및 목적

1.1 사이버 보안

1.2 사이버 공격의 유형 및 사례

2. 주요 내용

2.1 AI 사이버 보안

2.2 AI 사이버 보안 이슈사항

PART 01

도입 배경 및 목적

1.1 사이버 보안

기술적인 차원에서의 사이버 보안

- 사이버 보안에 관한 일반적 개념 논의[2)]
  - 사이버 보안은 컴퓨터, 네트워크, 소프트웨어 애플리케이션, 중요 시스템 및 데이터를 잠재적 디지털 위협으로부터 보호하는 행위 또는 노력을 지칭함
  - 기업이나 국가는 데이터에 보안을 적용하여 고객과 국민의 신뢰를 유지하고 규제를 준수할 책임이 있으며, 이에 적극적으로 사이버 보안 조치 및 도구를 사용하여 민감한 데이터를 무단 액세스로부터 보호하고 원치 않는 네트워크 활동으로 인한 운영 중단을 방지해야 할 것임
  - 기업이나 국가가 보유하고 있는 민감한 정보와 국가 기밀은 인력, 프로세스 및 기술 사이에서 디지털 방어를 간소화하여 사이버 보안을 구현해야 할 것임

- 사이버 보안이 중요한 이유
  - 기업 차원에서 에너지, 운송, 소매 및 제조와 같은 다양한 부문에서 디지털 시스템 및 고속 연결을 사용하여 효율적인 고객 서비스를 제공하고 비용 효율적으로 비즈니스를 운영하는 데 있어 물리적 자산을 보호할 때와 마찬가지로 디지털 자산에 보안을 적용하고 의도하지 않은 액세스로부터 시스템을 보호하는 것
  - 이러한 과정은 단지 기업 비즈니스 영역에만 한정되는 것이 아니라 국가 역시 다양한 차원에서 국제관계 그리고 적대적 국가로부터의 디지털 기술을 악용한 침략과 위협에 대응하기 위한 대응책을 준비해야 함
  - 국가 기강 컴퓨터 시스템, 네트워크 또는 연결된 설비를 침해하고 무단으로 액세스하려는 외부로부터의 사이버 공격을 막을 필요가 있기 때문임

2) 기술적인 차원에서의 사이버 보안의 주요 내용은 아마존의 사이버 보안 자료를 참조로 작성 (https://aws.amazon.com/ko/what-is/cybersecurity/)

- 사이버 보안 문제의 복잡성(벤 뷰캐넌 2023)
  - 일반적으로 사이버 보안을 단지 기술로만 한정하여 이해하는 것은 잘못된 접근이라 할 수 있음
  - 이미 디지털 기술은 새로운 전환을 맞이하며 인공지능, 빅데이터, 블록체인, 유비쿼터스 등으로 발전하면서 인간과 한 몸처럼 움직이는 수준에 이르렀기에 사이버 보안 문제를 기술만의 문제로 치부해서는 안 될 것임
  - 사이버 위협은 기계와 연관된 인간의 일거수일투족에 관여되어 있는데, 가장 맨 밑단에 있는 하드웨어부터 기계를 살아 움직이게 하는 소프트웨어, 그로부터 창출되는 비즈니스, 역동적으로 생성되는 데이터, 극히 사적 영역에 이르기까지 인간과 밀접하게 관련이 있음
  - 해킹과 결합하여 유포되는 허위 조작정보(가짜뉴스)와 댓글 조작은 민주주의 체제를 흔들기도 하고 사이버 범죄에 의한 피해자가 속출하고 사이버 문제가 기업 간 공정한 경쟁을 방해하며 국가 안보를 위협하는 등 현실과 사이버공간을 누비며 자행한 행위가 사회에 큰 피해를 주며 안전과 신뢰를 뒤흔드는 복잡한 문제가 됨

- 진화하는 사이버 보안 위협
  - 디지털 기술사를 보면 컴퓨터 바이러스의 확산과 백신 개발의 과정과 같이 사이버 위협이나 공격은 보안이나 수비 기술보다 빨리 발전하는 경향이 있음
  - 사이버 공격은 기술의 변화를 따라 더욱 진화하고 범죄자들은 무단 시스템 액세스를 위해 새로운 도구를 사용하고 새로운 전략을 고안하는데 몰두하고 있음
  - 이에 국가나 기업 차원에서 새롭게 진화하는 디지털 공격 기술과 도구를 따라잡기 위한 사이버 보안 조치를 끊임없이 개선하고 보안 환경을 최신식으로 구성해야 할 것임

- 사이버 위협의 3가지 층위(임종인 2008)
  - 사이버 위협의 피해는 다양할 것이지만, 크게 국가와 기업, 개인 등의 3가지 차원에서 사이버 위협이 제기되고 있으며 이에 따른 사이버 보안 이슈가 부각되고 있음
  - 임종인(2008)은 이를 국가·기업·개인 3가지 층위의 사이버 위협으로 구분하였으며 현재까지 가장 명확한 층위로 평가됨

〈표 1〉 국가·기업·개인 차원의 사이버 위협

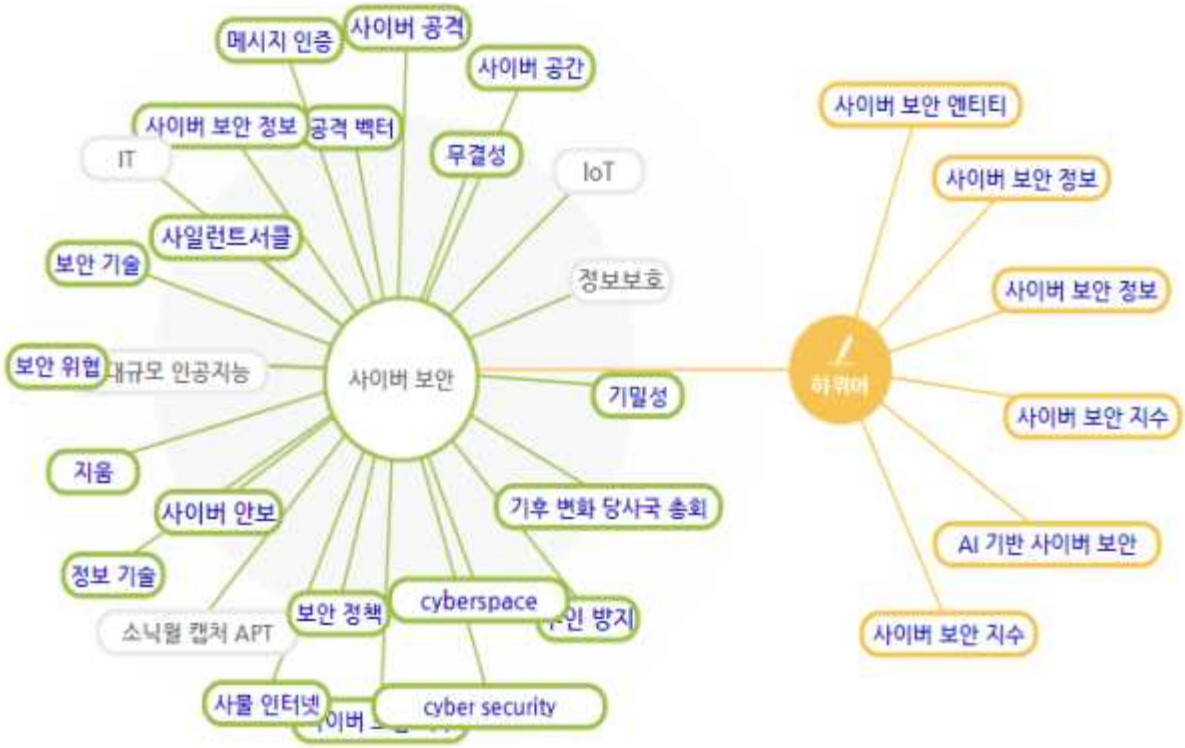
층위	주요 내용
국가	▪ 사이버공간에서 국가 기반 시설에 대한 사이버 테러와 해킹 공격 등으로 인해 정부의 기능이 마비되고 사회적 혼란이 야기될 위험 ▪ 실존하는 테러나 적국과의 사이버 전쟁으로 인해 국가 정체성을 유지하기 어려울 정도의 심각한 위기 상황 가능성 ▪ 국가의 기밀과 국가의 핵심 산업기술을 가져가려는 각국 정부 및 기업의 첩보 행위 ▪ 국가적으로는 해킹의 주요 경유지로서의 국제적 오명과 보안 무법천지라는 불명예를 안게 될 수도 있으며, 국가의 이미지 하락의 위험에 처할 수 있음
기업	▪ 비즈니스 영역이 사이버공간으로 이전되면서 산업기술을 포함한 기업의 영업 비밀이 사이버 공격에 노출되어 기업 경쟁력에 심각한 타격 ▪ 기업이 수집한 고객의 정보를 사이버 공격으로부터 제대로 보호하지 못하면, 해당 기업 경쟁력은 물론 개인정보 보호법 위반 등으로 법적 책임을 지게 되는 위험
개인	▪ 개인들은 사이버 공간상의 사회적 약자로서 더욱 많은 위험에 노출되어 있음 ▪ 공공기관이나 기업들이 더 많은 개인정보를 요구하는 반면 그에 대한 충분한 보호를 제공하지 못해 개인들은 자신의 개인정보가 유출될 위험에 일상적으로 노출 ▪ 개인정보 유출로 인한 명예훼손 및 신체적 위협, 금융 피해와 같은 2차 범죄 위험에도 노출되어 있는 상황

● 한국에서의 사이버 보안 등장

- 2003년 1·25 인터넷 대란, 2009년 7·7 사이버 테러, 2013년 6·25 사이버 공격 등 위협이 늘자 정부는 국가 차원의 안보 체계를 고민했고, 국가 사이버 안전 전략 회의를 열어 종합 대책을 마련하는 등 단순히 기업이나 비즈니스 영역에 한정된 개념이 확장되기 시작함
- 특히 코로나19(COVID-19) 이후 사이버 경제활동이 증가하면서 언론은 물론 정부기관, 사회 각계에서 사이버 보안이란 용어가 통용되기 시작함
- 사이버 보안은 초기 사이버공간에서의 보안으로 협소하게 인식하였지만, 이후 정보

통신기술이 발전하면서 사이버공간을 넘어서 오프라인까지 확장된 각종 위협이 증대되는 것으로 인식

- 사이버 보안은 국가와 기업, 개인을 공격하는 모든 행위와 이를 막기 위한 대응 개념으로까지 확장
- 이런 이유로 사이버 보안을 단순한 정보보호의 상위개념으로 보며 사이버 보안은 디지털 기술 환경의 변화에 따라 기존의 정보보호에 사이버공간이 결합하여 강조되고 있음(TTA 정보통신용어사전 2024)[3)]



〈그림 1〉 사이버 보안과 관련된 연관어 Map

3) 〈그림 1〉은 TTA 정보통신용어사전을 인용함
http://word.tta.or.kr/dictionary/dictionaryView.do?subject=%EC%82%AC%EC%9D%B4%EB%B2%84+%EB%B3%B4%EC%95%88

1.2 사이버 공격의 유형 및 사례

사이버 공격

- 인터넷은 네트워크 연계성(network connectivity)으로 서로 원격으로 연결할 수 있는 장점도 있지만 이 연계성으로 인해 사이버 공격의 대상이 될 수 있음
  - 임종인(2008)이 오래전에 제기한 바와 같이, 네트워크와 정보통신기술로 인해 사이버 공간에서 발생할 수 있는 손실 가능성이 증가하고 있으며, 사이버 공격은 위험을 발생시킬 수 있는 여러 위험 요인으로 인해 이미 현실화되고 있음

- 사이버 보안은 다양한 차원에서 논의되고 있음
  - 미시적인 차원에서 사이버 범죄자가 개인 사용자의 프라이버시를 침해하거나, 패스워드를 훔치거나, 명의를 도용하는 경우가 가장 일반적임
  - 공격자가 라우터, 태블릿, PC같이 개인이 사용하는 커넥티드 디바이스를 장악하고 좀비화하여 다른 컴퓨터 네트워크에 접근할 수 있고 별도의 프로그램을 통해 DoS(서비스 거부) 공격을 실행해서 통신 중단 같은 피해를 일으킬 수 있음
  - 공격자가 사이버 첩보나 공격을 통해서 기업 비밀을 훔칠 수 있는데 독일 연방 헌법 수호청에 따르면, 독일에서만 사이버 공격으로 인한 피해가 연간 500억 유로에 달하는 것으로 발표
  - 한편 최근에는 기업이나 개인적이고 미시적인 차원의 사이버 공격 이외에 국가 차원의 인터넷 네트워크를 공격하는 테러 형태의 사이버 공격도 증가하고 있으며, 이는 국가 전력망이나 인터넷을 전국적으로 중단시킬 수 있을 정도로 위협적임
  - 이와 같은 국가 단위의 전략적인 사이버 공격은 개인이 시도할 수 있는 규모가 아니기 때문에 체계를 갖춘 악의적 해커 조직이 필요한데, 대규모의 해커 조직 양성을 위해서는 정부와 같이 체계화된 조직의 지원이 필요
  - 양성된 악의적 해커 조직은 상대국의 시스템이나 네트워크를 마비시키거나 사이버 첩보전을 벌이는 등 광범위한 사이버 전쟁 및 테러에 활용됨(김미희 2017)

〈표 2〉 사이버 공격 신고[4)]

[단위 : 건수]

구분	연도	2022 (상반기)	비율	2022 (하반기)	비율	2023 (상반기)	비율	2023 (하반기)	비율
침해 사고 신고	DDoS 공격	48	10.1%	74	11.1%	124	18.7%	89	14.5%
	악성코드	125	26.4%	222	33.2%	156	23.5%	144	23.5%
	(랜섬웨어)	(118)	(24.9%)	(207)	(30.9%)	(134)	(20.2%)	(124)	(20.2%)
	서버 해킹	275	58.1%	310	46.3%	320	48.2%	263	42.9%
	기타	25	5.3%	63	9.4%	64	9.6%	117	19.1%
합 계		473		669		664		613	

- 사이버 공격의 유형[5)]

① 멀웨어(Malware)

- 멀웨어는 악성 소프트웨어로 제3자가 민감한 정보에 무단으로 액세스하는 것을 허용하거나 중요한 인프라의 정상적인 작동을 방해하도록 설계된 다양한 소프트웨어 프로그램으로 그 예로는 트로이 목마, 스파이웨어, 바이러스 등이 있음
- 멀웨어의 일반적인 목표는 장치의 정상적인 작동을 방해하는 것으로, 이러한 방해는 동의 없이 장치에 광고를 표시하는 것부터 컴퓨터의 루트 액세스 권한을 얻는 것까지 다양함

〈표 3〉 멀웨어의 유형

No	유형	설명
1	스파이웨어	▪ 사용자의 행동을 감시하는 데 사용되고 스파이웨어는 사용자의 웹 브라우징 활동을 모니터링 ▪ 원치 않는 광고를 사용자에게 표시하며, 제휴 마케팅 스트림을 수정하는 데 사용됨
2	바이러스	▪ 바이러스는 운영 체제 또는 소프트웨어에 포함될 수 있는 악의적 프로그램 ▪ 피해자가 운영 체제를 실행하거나 감염된 파일을 열면 피해 발생
3	웜	▪ 바이러스와 달리 웜은 자체 복제되어 네트워크를 통해 전송하는 형태 ▪ 사용자는 소프트웨어를 실행하거나 감염된 네트워크에 연결하는 것만으로도 피해를 볼 수 있음

4) 한국인터넷진흥원(이하 KISA) 통계 자료를 김영명(2024)에서 재인용
5) 사이버 공격의 유형은 IBM(2024)와 Amazon(2024), Cloudflare(2024)에서 제시하고 있는 사이버 공격과 위협의 사례를 바탕으로 재구성

No	유형	설명
4	트로이목마	▪ 다른 유용한 소프트웨어 내부에 숨겨진 멀웨어 조각으로, 사용자가 설치하도록 유도하는 형태
5	루트킷	▪ 운영 체제를 수정하여 원치 않는 설치를 사용자가 알지 못하도록 설계 ▪ 루트킷의 유명한 예는 2005년 소니 루트킷 스캔들로, 당시 소니는 구매자의 컴퓨터에서 CD 복사를 방해하기 위한 소프트웨어를 비밀리에 설치하는 루트킷에 감염된 음악 CD를 2,200만 개 판매 ▪ 이 루트킷 때문에 다른 공격자가 추가 멀웨어로 감염된 컴퓨터를 겨냥할 수 있는 기회가 생겼음
6	랜섬웨어	▪ 랜섬웨어는 범법자가 개인이나 법인으로부터 돈을 갈취하기 위해 사용하는 비즈니스 모델 및 다양한 관련 기술 ▪ 컴퓨터 또는 네트워크 파일이나 전체 운영 체제를 암호화하고 공격자에게 몸값을 지불할 때까지 암호화된 상태로 유지 ▪ 최근에는 비트코인 및 기타 암호화폐가 출현하면서 공격자가 익명으로 몸값을 받고 붙잡힐 위험이 최소화하고 있음 ▪ IBM Security X-Force Threat Intelligence Index 2023에 따르면 랜섬웨어 공격은 2022년 전체 사이버 공격의 17%를 차지

② 소셜 엔지니어링

- 흔히 '인간 해킹'이라고 하는 소셜 엔지니어링은 표적이 기밀 정보를 노출하거나, 자신이나 조직의 재정적 안녕을 위협하거나, 개인 또는 조직의 보안을 손상시키는 행동을 취하도록 조작하는 형태

③ 피싱

- 가장 잘 알려져 있고 가장 널리 퍼져 있는 소셜 엔지니어링 유형으로 피싱은 사기성 이메일, 이메일에 첨부된 파일, 문자 메시지 또는 전화를 사용하여 사람들을 속여 개인 데이터 또는 로그인 자격 증명을 공유하거나, 멀웨어를 다운로드하거나, 사이버 범죄자에게 돈을 송금하거나, 기타 사이버 범죄에 노출될 수 있는 행동을 취하도록 유도하는 형태

〈표 4〉 피싱(Phishing)의 유형

No	유형	설명
1	스피어 피싱	▪ 특정 개인을 조종하는 고도로 표적화된 피싱 공격으로, 피해자의 공개 소셜 미디어 프로필의 세부 정보를 사용하여 계략을 더욱 설득력 있게 만들어 개인정보 탈취
2	웨일 피싱 (Whale Phishing)	▪ 기업 임원이나 부유한 개인을 대상으로 하는 스피어 피싱
3	비즈니스 이메일 보안 침해(BEC)	▪ 사이버 범죄자가 경영진, 제공업체 또는 신뢰할 수 있는 비즈니스 동료로 가장하여 피해자를 속여 돈을 송금하거나 민감한 데이터를 공유하도록 유도하는 사기
4	도메인 이름 스푸핑 (DNS 스푸핑)	▪ 사이버 범죄자가 실제 웹 사이트나 도메인 이름과 유사한 가짜 웹 사이트나 도메인 이름을 사용해 사람들을 속이고 민감한 정보를 입력하도록 유도 (예: support.apple.com을 'applesupport.com'으로) ▪ 피싱 이메일은 더 믿을 수 있고 합법적인 이메일로 보이기 위해서 스푸핑 된 발신자 도메인 이름을 사용하는 경우가 많음

④ 중간자 공격(Man-in-the Middle)

- 중간자 공격이란 네트워크 연결을 도청하여 두 당사자 간의 메시지를 가로채고 전달해 데이터를 탈취하는 형태를 말함
- 보안되지 않은 Wi-Fi 네트워크는 종종 중간자 공격을 시작하는 경우가 가장 많음

⑤ 서비스 거부 공격

- 서비스 거부 공격은 대량의 부정 트래픽으로 웹 사이트, 애플리케이션 또는 시스템을 압도하여 정상적인 사용자가 사용하기에 너무 느리게 만들거나 아예 사용할 수 없게 하는 사이버 공격
- 분산 서비스 거부 공격(DDoS 공격)은 인터넷에 연결되고 멀웨어에 감염된 장치 또는 봇 네트워크(봇넷이라고 함)를 사용하여, 대상 시스템을 무력화시키거나 충돌시킨다는 점을 제외하고는 대부분 DDoS 공격과 유사

⑥ 제로데이 공격

- 제로데이 익스플로잇은 컴퓨터 소프트웨어, 하드웨어 또는 펌웨어에서 알려지지 않았거나 아직 해결되지 않았거나 패치되지 않은 보안 결함인 제로데이 취약점을 이용하는 사이버 공격의 한 유형

- 제로데이는 소프트웨어 또는 장치 제공업체가 취약점을 수정할 시간이 제로, 즉 전혀 없다는 사실을 의미하는데 이는 악의적인 공격자가 이미 취약한 시스템에 액세스하는 데 이 취약점을 이용했을 수 있기 때문
- 가장 잘 알려진 제로데이 취약점 중 하나인 Log4Shell 취약점은 악의적인 공격자가 서버를 제어하는 임의의 Java 코드를 실행할 수 있도록 하는 원격 코드 실행 취약점임
- 2021년 11월 발견 당시 이미 많은 웹 애플리케이션, 클라우드 서비스 및 서버와 같은 물리적 엔드 포인트를 포함하여 전 세계 디지털 자산의 10%에 존재하고 있는 것으로 파악

⑦ 비밀번호 공격

- 이름에서 알 수 있듯이 이러한 공격에는 사용자 계정의 비밀번호 또는 로그인 자격 증명을 추측하거나 훔치려는 사이버 범죄
- 많은 비밀번호 공격은 소셜 엔지니어링을 사용하여 피해자가 자신도 모르게 민감한 데이터를 공유하도록 속이며 악의적 해커는 무차별 비밀번호 대입 공격을 사용하여 비밀번호를 훔칠 수도 있으며, 성공할 때까지 다른 암호 조합을 반복적으로 시도하여 탈취하는 방식
- 최근에는 생성형 AI를 이용한 무한반복 암호 조합을 반복적으로 시도하여 비밀번호를 탈취하는 경우도 발생

⑧ 사물인터넷 공격

- 사물인터넷(IoT) 공격에서 사이버 범죄자는 스마트 홈 장치 및 산업 제어 시스템과 같은 IoT 장치의 취약점을 악용하여 장치를 장악하거나, 데이터를 훔치거나, 다른 악의적인 목적을 달성하기 위해 해당 장치를 봇넷*의 일부로 사용

* 봇넷이란, 악성 소프트웨어에 감염되어 공격자에게 제어권이 넘어가, 함께 작동하는 컴퓨터 네트워크를 뜻함

⑨ 인젝션 공격

- 공격에서 해커는 프로그램에 악성 코드를 삽입하거나 멀웨어를 다운로드하여 원격 명령으로 데이터베이스를 읽거나 수정하고 웹 사이트 데이터를 변경

〈표 5〉 인젝션 공격의 유형

No	유형	설명
1	QL 인젝션 공격	▪ 해커가 SQL 구문을 악용하여 신원을 스푸핑 하거나, 기존 데이터를 노출, 변조, 파괴 또는 사용할 수 없게 만들거나, 데이터베이스 서버 관리자가 되는 경우
2	교차 사이트	▪ 데이터베이스에서 데이터를 추출하는 대신 일반적으로

No	유형	설명
	스크립팅(XSS)	웹 사이트를 방문하는 사용자를 감염시킨다는 점을 제외하고는 SQL 삽입 공격과 유사

개인 간 보안 문제에서 국가 간 보안 문제로 확산

- 2010년대 이후 개인에 대한 사이버 공격도 급증하였지만, 국가와 기업을 대상으로 사이버 공격이 그 피해를 더하고 있음
  - 국제적으로 매일매일 수십 건의 사이버 공격 사례가 보고되고 있으므로 이를 모두 살펴보기는 현실적으로 어려울 것이지만, 주요 사건을 중심으로 살펴볼 필요가 있음
  - 이를 통해 사이버 보안의 심각성과 현재 진행 중인 사이버 공격의 실태 파악을 통한 경각심 제고에 도움이 될 것임

- 최근 세계적인 주목을 받았던 사이버 공격(Fortinet 2024에서 재인용)[6)]
  - 정상적인 비즈니스 상황에서 사이버 공격은 수조 달러의 손실을 야기할 정도로 규모가 커짐
  - 러시아와 우크라이나 간의 전쟁은 정치적 목적의 사이버 공격이 급증하면서 이러한 문제를 악화

〈표 6〉 최근 발생한 주요 사이버 공격 사례 요약

사례	시점	주요 내용
핫 토픽 (Hot Topic) 공격	2023년 8월	▪ 미국 소매업체인 핫 토픽(Hot Topic)이 웹 사이트와 모바일 앱에서 고객 계정에 로그인하려는 승인되지 않은 제3자의 자동 시도를 감지 ▪ "알 수 없는 제3자 출처에서 얻은 유효한 계정 인증 정보(예: 이메일 주소 및 암호)" 관련된 보안 공격 공지
프로스펙트 메디컬 홀딩스(Prospect Medical Holdings) 랜섬웨어 공격	2023년 8월	▪ 랜섬웨어 공격으로 인해 2개 이상의 진료실, 시설 및 병원이 오프라인 상태로 강제로 전환 ▪ 회사는 외래환자 시설 몇 곳을 폐쇄했으며, 페이스북 페이지와 웹 사이트를 통해 환자와 가족에게 이 공격에 대해 공지 ▪ 언론사 보도에 따르면, 네트워크가 오프라인 상태인

6) 2020년대의 주요한 사이버 공격과 그 피해 사례는 Fortinet 참조
https://www.fortinet.com/kr/resources/cyberglossary/recent-cyber-attacks (검색일: 2024년 11월 20일)

사례	시점	주요 내용
		동안 의료진이 수동 정보 절차로 전환한 것을 확인
핀란드 의회 공격	2022년 8월	▪ 핀란드 의회 웹 사이트는 의회 개회 중에 DDoS 공격을 경험 ▪ 이러한 DDoS 공격은 NATO 가입 신청에 대한 보복으로 핀란드 정부의 웹 사이트를 마비시키기 위한 러시아 정부 지원 해커의 연계 캠페인 중 일부일 것으로 파악 ▪ DDoS 공격은 일시적으로 웹 사이트 액세스를 차단하였으나 영구적 파괴는 하지 못한 것으로 파악
우크라이나 주 원자력 회사 공격	2022년 8월	▪ 인민 사이버군(People's Cyber Army)이라고 불리는 러시아의 "핵티비스트" 그룹은 2022년 8월 725만 대의 AI 봇을 동원해 Energoatom 웹 사이트를 다운시키기 위해 봇 공격 ▪ 가비지 웹 트래픽과 웹 페이지 요청이 폭주 ▪ 온라인 서비스의 중단은 몇 시간 동안 지속 ▪ 이 공격은 핵 재앙에 대한 두려움을 조성하고 유럽인들을 공포에 떨게 하려는 러시아의 심리전 캠페인의 일환인 것으로 파악
그리스 가스유통사 공격	2022년 8월	▪ 그리스 가스 유통사인 DESFA는 2022년 8월에 사이버 공격이 발생했음을 보고 ▪ 이 보안 공격은 회사 IT 인프라의 일부에 영향을 미쳐 데이터 유출을 야기 ▪ 라그나 로커(Ragnar Locker)라는 사이버 범죄자의 랜섬웨어 작전은 도난당한 데이터를 인질로 잡고 있었음 ▪ 그들은 민감한 데이터를 노출시키지 않도록 몸값을 요구했으나 회사는 지급을 거부
사우스 스태퍼드셔 워터 컴퍼니(South Staffordshire Water Company) 공격	2022년 8월	▪ South Staffordshire Water Company는 내부 기업 네트워크에서 네트워크 중단과 데이터 손실을 야기한 기업 해킹 사례를 보고 ▪ 한 사이버 범죄 랜섬웨어 그룹이 회사가 공급한 물을 조작하겠다고 위협 ▪ 범죄자들은 민감한 파일을 공개하지 않고 네트워크

사례	시점	주요 내용
		침해가 어떻게 발생했는가를 설명하는 조건으로 대가를 요구
몬테네그로 정부 공격	2022년 8월	▪ 몬테네그로 정부의 디지털 IT 인프라는 2022년 8월 전례 없는 사이버 공격을 보고 ▪ 데이터 유출이 발생하지는 않았으나 국경 통과 및 공항 운영을 포함한 특정 정부 서비스 및 통신 중단 ▪ 국영 유틸리티 회사인 EPCG는 예방 조치로 수동 운영으로 전환
에스토니아 정부 보안 공격	2022년 4월	▪ 2022년 4월, DDoS 공격으로 인해 몇 시간 동안 많은 에스토니아 정부 웹 사이트 마비 ▪ 이 공격은 대통령, 외교부, 경찰 및 국경경비대, 신분증 웹 페이지 및 주 서비스 디지털 포털을 대상으로 진행 ▪ 당시 에스토니아는 우크라이나에 대한 러시아 전쟁을 비난하여 러시아 해커의 표적이 되었음
이슬람 문화 및 커뮤니케이션 조직 사이버 공격	2022년 7월	▪ 2022년 7월에 이란 이슬람 문화 및 커뮤니케이션 조직 (ICCO)이 심각한 공격을 경험 ▪ 6개의 ICCO 웹 사이트가 다운되었고, 다른 15개 웹 사이트는 이란 저항군 지도자인 마수드 라자비 (Massoud Rajaivi)의 사진으로 변경 ▪ 또한, 44대의 서버와 수백 대의 컴퓨터에서 데이터가 파괴 ▪ ICCO는 또한 해외에 거주하는 자금 세탁, 스파이 및 테러리스트에 대한 기밀 정보가 담긴 35개의 데이터베이스를 손실
벨기에 정부 및 군사 공격	2022년 7월	▪ 벨기에 정부는 중국의 지능형 타깃 지속 공격 (APT) 범죄자의 일부로 알려진 세 개의 중국 해커 그룹이 벨기에 공공 서비스와 군사 방위군을 공격했다고 발표 ▪ 중국 정부가 후원하는 공격자들은 영업 비밀과 인텔리전스 정보를 훔쳤다고 함 ▪ 한편 Soft Cell Chinese 그룹은 최근 2022년 6월 새로운 원격 액세스 트로이 목마(RAT) 멀웨어

사례	시점	주요 내용
		(Malware)를 출시
영국 군사 소셜 미디어 침해	2022년 7월	▪ 해커는 영국 육군의 트위터 계정을 장악하여 이를 악용한 것으로 파악 ▪ 소셜 미디어 계정에서 여러 개의 이름과 사진 변경 ▪ 이 콘텐츠는 블록체인에 저장된 디지털 아트인 Angry Apes 대체 불가능 토큰(NFT)을 얻기 위한 콘테스트를 홍보 ▪ 군대의 유튜브 페이지도 사이버 공격을 받아 이름이 'Ark Invest'로 바뀌었고, 이 계정은 암호화폐에 대해 이야기하는 일론 머스크(Elon Musk)의 인터뷰 홍보에 사용되었음
리투아니아 에너지 회사 공격	2022년 7월	▪ 2022년 7월에 DDoS 공격으로 인해 리투아니아 에너지 회사인 Ignitis Group의 웹 사이트에 대한 액세스 차단 ▪ 회사는 DDoS 방어를 사용하여 공격을 관리하고 피해를 제한 ▪ 데이터 유출은 발생하지 않았지만, 공격은 끊임없이 지속적이었음 ▪ 친러시아 그룹 Killnet은 자신들의 소행이라고 주장 ▪ 이 공격은 러-우 전쟁에서 리투아니아가 우크라이나를 지원하는 것에 대한 보복
ProxyLogon 사이버 공격	2021년 1월	▪ 최근 가장 큰 피해를 입힌 사이버 공격 중 하나는 Microsoft Exchange 서버 침해로 인해 몇 가지 제로 데이 취약성이 발생한 것 ▪ 프록시로그온(ProxyLogon)으로 알려진 취약성은 처음에 Hafnium 해킹 그룹에서 시작되었으며 1월 Microsoft에 의해 처음 발견되었고 3월에 패치됨 ▪ 그러나 패치되지 않은 시스템을 공격하기 위해 더 많은 그룹이 하프늄에 합류하여 수천 개의 조직이 침해당했다고 함
MeetMindful 사이버 보안 침해	2021년 1월	▪ 2021년 1월에 데이트 앱 MeetMindful이 사이버 보안 공격을 받아 2백만 명 이상의 사용자 데이터가 도난당하고 유출되는 기업 해킹 사례가 발생

사례	시점	주요 내용
		▪ 이 사건의 배후 해킹 그룹은 사용자의 전체 이름 및 페이스북 계정 토큰과 같은 정보를 훔쳤다고 함
Tether 공격	2021년 3월	▪ 사이버 범죄자들은 Tether 암호화폐에서 문서를 유출하겠다고 위협. 공격자들은 데이터가 비트코인 생태계를 파괴할 것이라고 주장하며 약 500비트코인(2,400만 달러)의 합의금을 요구
페이스북 사이버 공격	2021년 4월	▪ 2021년 4월에 5억 3천만 명 이상의 페이스북 사용자의 이름, 페이스북 ID, 생년월일 및 관계 상태를 포함한 데이터가 온라인에 공개
아우디와 폭스바겐 사이버 보안 공격 침해	2021년 6월	▪ 2021년 6월, 아우디와 폭스바겐은 데이터 유출이 주로 미국에 기반을 둔 330만 명 이상의 고객과 잠재 구매자에게 영향을 미쳤음을 공개 ▪ 이 침해에 대한 비난의 화살은 관련 벤더로 향했으며, 2019년 8월과 2021년 5월 사이에 데이터를 노출시킨 책임이 있는 것으로 추정하고 있음

PART 02

주요 내용

2.1 AI 사이버 보안

AI 사이버 보안 문제 등장

- AI 기술이 발전하고 4차산업혁명의 중심으로 부각됨에 따라 사이버 보안은 더욱 중요한 문제로 인식되고 있음
  - AI는 효율성과 혁신을 제공하는 동시에 고유한 취약점과 보안 위협을 동반하며, 이를 관리하지 못하면 심각한 결과를 초래할 수 있음
  - AI 사이버 보안은 전통적인 보안 이슈를 넘어 새로운 차원의 도전과제를 제시하는데, 데이터 보안, 적대적 공격, 모델 도난과 같은 문제는 AI 시스템의 안전성과 신뢰성을 위협하며, 규제와 표준화의 부재는 이를 더욱 복잡하게 만들고 있음

- 일상화된 사이버 보안 대응
  - 기업 단위에서는 조직에서 사이버 보안 전략 구현 시, 사이버 보안 전문가 참여
  - 전문가들은 기존 컴퓨팅 시스템, 네트워크, 데이터 스토리지, 애플리케이션 및 기타 연결된 디바이스의 보안 위험을 평가하고 포괄적인 사이버 보안 프레임워크를 만들고 사전 예방적 수단을 조직 내에 구현의 필요성을 강조
  - 광범위한 사이버공간의 위협과 전 세계적으로 사이버 공격의 빈도와 심각성이 증가
  - 디지털 전환에 따라 새로운 기술들의 등장과 방통융합 등 디지털 컨버전스(digital convergence)로 인해 예측 불가능한 위험 발생 가능성은 기하급수적으로 증가하고 있음
  - 빅데이터, 인공지능, IoT 등 디지털 사회로의 급속한 진입은 온라인-오프라인의 유기적 결합을 통한 일상생활의 사이버 공간화를 촉진하면서 전 사회적인 차원에서 사이버공간의 위험을 확대 재생산하고 있다는 평가(임종인 2008)

- 최근에는 미국 생성형 인공지능(AI) 기술을 활용한 신종 사이버 범죄 예방과 AI 사이버 보안 문제가 등장(김희정 2024, 51)

- 21세기 인공지능(AI) 기술의 비약적인 발전과 정보화 사회로의 급속한 전환이 특징으로 의료, 금융, 제조업, 교육 등 다양한 분야에서 혁신을 주도하며 인간의 삶을 편리하고 풍요롭게 만들고 있음
- 이러한 기술 발전이 가져오는 영향은 긍정적인 측면만으로 한정되지 않고 인공지능의 급속한 발전은 사회, 경제, 국가 안보 전반에 광범위한 영향을 미치고 있으며, 특히 사이버 범죄와 같은 새로운 위협을 초래하고 있음
- 2023년 마이크로소프트의 클라우드 서비스 장애로 인해 영국의 금융기관, 언론사, 항공사 등 여러 주요 서비스가 중단되면서 전 세계적으로 큰 혼란이 발생한 것이 대표적인 사례임

- 여기에 더해 디지털 기술 특히 인공지능(AI)의 급속한 발전과 정보화 사회로의 전환이 가속화됨에 따라, 사이버 범죄의 양상은 AI를 이용한 형태로 발전
  - AI는 데이터 오염에서부터 딥 페이크(deep fake)에 이르기까지 다양하고 정교하게 발전하고 있으며 AI는 의료, 금융, 제조업, 교육 등 여러 분야에서 혁신을 이끌며 인간의 삶을 편리하고 풍요롭게 만들고 있으나, 이러한 기술 발전이 항상 유토피아적인 긍정 영향만을 미치는 것은 아님
  - AI의 급속한 발전은 사회, 경제, 국가 안보에 이르기까지 광범위한 영향을 미치며, 특히 AI 사이버 보안 범죄와 같은 새로운 위협이 부각되고 있음(김희정 2024, 49)

AI 사이버 보안의 중요성

- 사이버 공격의 고도화
  - 사이버 공격의 다양한 위험은 의도적(사이버 공격), 비의도적(내부 취약점)에 따라 다르게 나타날 수 있음
  - 그러나 최근 디지털 기술 발전에 따라 AI를 활용한 악성 코드를 공격, 불법 복제, 오픈소스나 소프트웨어에 백도어 삽입 등은 사이버공간의 네트워크 연계성으로 국가와 기업 그리고 개인에게도 무차별적으로 피해를 줄 수 있는 상황이 전개(임산호 2023)

- AI는 사이버 공격의 고도화를 끌어낼 수 있는 강력한 도구
  - 악의적인 목적으로 활용될 경우, AI는 기존의 사이버 공격 방식을 훨씬 더 정교하고 효과적으로 피해를 발생시키거나 악용될 수도 있음

- 생성형 AI는 사이버 공격의 목표를 정확히 선정하고, 공격 방식을 최적화하며, 탐지 회피 전략을 개발하는 데 사용
- AI는 자율적으로 작동하여 목표 시스템에 대한 지속적인 공격을 수행하거나, 다른 컴퓨터 시스템을 감염시켜 악성 코드를 확산시키는 데 활용
- AI를 악용하면 사이버 보안 문제가 과거 사람과 프로그램이 주도하던 시기와는 근본적으로 다른 새로운 위험 환경에 도달할 가능성이 증가함

AI 사이버 공격 무기(AWS, Autonomous Weapons Systems)

AI 자율무기 시스템(Autonomous Weapons Systems) 개발

- AWS는 인간의 개입 없이 스스로 판단하고 목표를 공격하는 무기로, 전쟁의 양상을 근본적으로 바꿀 수 있으며, 예측 불가능한 결과를 초래할 수 있음
- 예를 들어, AWS는 전투 중 인간의 개입 없이 자율적으로 작동하며 전투 상황을 판단하고 공격 목표를 정하도록 설계
- 현재 개발 중인 다양한 자율적인 무기 시스템은 인간의 통제에서 벗어나 예측 불가능한 행동을 보이는 위험성이 있어 국제 규제와 윤리적 논쟁을 야기하고 있음

AI 사이버 공격의 유형

① AI 기반 데이터 및 프라이버시 침해

- AI는 방대한 데이터를 활용하여 작동하기 때문에 데이터 보안 및 프라이버시 침해의 위험을 증가시킴
- AI는 개인정보를 수집하고 분석하여 개인의 행동을 예측하고, 나아가 개인의 의사 결정에 영향을 미칠 수 있음
- AI 기반의 감시 시스템은 개인의 프라이버시를 침해할 우려가 있으며, 이는 개인의 자유와 인권을 제한하는 심각한 문제 야기
- AI는 민감한 정보를 유출하거나 해킹 공격에 악용될 수 있는 위험을 안고 있으며, 이는 국가 안보나 개인정보(프라이버시) 등에 대한 심각한 위협을 초래할 것임

② 국가 사이버 보안 변화

- 전통적인 안보협력 부문을 넘어 사이버안보 영역으로 국가 간 협력 의제가 확대되고

있는 상황에서, AI 사이버 보안 강화 및 관련 규정 마련을 위한 논의 또한 확대되고 있음

- 특히, 소프트웨어 공급망에 대한 사이버 공격 사례가 가장 빈번하고 피해 확산 우려도 크다는 상황을 반영하여, 소프트웨어 공급망 보안을 강화하기 위한 다양한 협력 논의가 진행되고 있음

③ 생성형 AI 활용 범죄의 확산

- 악의적 해커들은 생성형 AI를 이용해 편리하게 데이터에서 단서를 찾아내 랜섬웨어 대상을 물색하고 특히 관리자(admin) 계정이 발견될 경우, 이들을 집중적으로 공략하여 목적을 달성하기 용이함(이상덕 2024)
- 악의적인 사이버 해커들은 2022년 11월 챗 GPT 등장 이후 웜 GPT, XXXGPT, XXX울프(Wolf) GPT와 같은 기성 대규모 언어 모델(LLM, Large Language Models) 텍스트를 인식하고 생성하는 등의 작업을 수행할 수 있는 일종의 인공지능 프로그램 기반 악성 AI를 개발하여 사용
- 범죄용 프로그램을 활용해 악성 코드와 자연스러운 피싱 메시지를 생성하였는데 그 실험 차원에서 사이버 보안 업체 슬래시넥스트(SlashNext)는 웜 GPT를 이용해 비즈니스 이메일을 공격하는 피싱 이메일을 생성하는 실험을 진행하기도 함
- 그 결과 웜 GPT는 가짜 송장을 지급하도록 유도하는 정교한 이메일을 생성했으며, 이는 외국어를 어눌하게 사용하지 않고 현지인처럼 접근할 방법으로 활용 가능

④ AI 활용한 딥 페이크(이상덕 2024)

- 전 세계적으로 AI로 만든 딥 페이크로 인한 사이버 보안 문제가 심각한 상황

실제로 홍콩의 한 금융사 직원은 딥 페이크로 만들어진 가짜 최고재무책임자(CFO)의 지시에 속아 2억 홍콩달러(한화 약 340억 원)를 탈취당해 논란이 됐습니다. 해당 직원은 처음에 딥 페이크 CFO에게서 “송금을 하라”는 가짜 이메일 받았을 때만 하더라도 속지 않았습니다. 하지만 주변 동료들이 참여하는 영상회의에서 딥 페이크 CFO가 동일한 지시를 내리자 의심을 거두고 송금을 진행했습니다. 알고 보니 그 모든 것이 AI로 생성된 실시간 딥 페이크 영상이었습니다.

- 마이크로소프트는 AI를 활용해 해킹을 시도하는 집단으로 러시아의 팬시베어(Fancy Bear)를 지목했는데 이들은 오픈 AI의 대형 언어 모델을 사용해 기본적인 스크립팅 작업을 처리하여 파일 조작, 데이터 선택, 멀티프로세싱, 정보수집, 위성 통신 연구 등을 생성형 AI를 활용해 수행

- 중국 해커 중에서 AI를 적극적으로 사용하는 단체는 차콜 타이푼(Charcoal Typhoon)과 살몬 타이푼(Salmon Typhoon)으로 이들은 사이버 공격 전에 테스트하는 정찰 단계에서도 AI를 사용해 정확도를 높이고 있다고 함
- 북한의 대표적인 해커 단체로 알려진 '김수키' 역시 생성형 AI를 활용해 다양한 정보를 분석하고 취약점을 파악하는 것으로 알려짐

⑤ AI 자동화 공격

- AI로 미리 공격할 대상을 설정하고 주기적으로 접속 또는 이메일을 발송하여, 상대방이 안심할 때까지 지속적으로 자동화 공격을 시도하는 방식
- AI 자동화 공격의 대표적인 형태는 그리드 퍼즐을 통해 사용자가 로봇인지 사람인지 판별하고, 사용자의 행동 패턴을 분석해 비정상적인 활동을 감지하는 행동 분석 기반 탐지를 실시하며, 웹 애플리케이션을 대상으로 공격
- 포춘 비즈니스 인사이트에 따르면, 2023년 전 세계 사이버 보안 시장 규모는 1,722억 4,000만 달러로 평가되며, 2024년에는 1,937억 3,000만 달러, 2032년까지는 5,627억 2,000만 달러로 연간 14.3%의 성장률을 기록할 것으로 전망

2.2 AI 사이버 보안 이슈 사항

AI 사이버 보안 이슈 사항

- 데이터 보안(Data Security)
  - 문제점: AI 시스템은 대규모 데이터를 학습하여 작동하는데, 학습 데이터가 노출되거나 변조되면 시스템 성능에 직접적인 영향을 미치게 됨. 데이터 중독(Data Poisoning) 공격을 통해 악의적인 데이터가 삽입되면 AI 모델이 잘못된 예측을 하게 만들 수 있음. 예를 들어, 의료 데이터를 사용하는 AI 시스템이 잘못되거나 변조된 데이터를 학습할 경우, 잘못된 진단 결과를 초래할 수 있음
  - 해결 방안: 데이터 암호화, 접근 제어, 안전한 데이터 수집 프로세스 적용 등이 해결 방안이 될 수 있음

- 적대적 공격(Adversarial Attacks)
  - 문제점: 적대적 공격은 AI 모델이 잘못된 결정을 내리도록 설계된 입력 데이터를 의미하며, 이미지 인식 모델에서 특정 픽셀을 조작해 잘못된 결과를 유도하거나, 자율주행 차량이 신호를 오인하게 만드는 공격이 발생할 수 있음. 예를 들어, 자율주행 자동차의 AI가 적대적 공격으로 인해 정지 표지를 무시하고 사고를 초래할 수 있음
  - 해결 방안: 적대적 훈련(Adversarial Training), 모델 견고성 강화, 공격 탐지 시스템 구축 등이 해결 방안이 될 수 있음

- 모델 보안(Model Security)
  - 문제점: AI 모델 자체가 탈취(Stealing)당하거나 역공학(Reverse Engineering)될 경우, 악의적인 목적으로 활용될 수 있음. 모델 도난(Model Theft) 문제는 AI 기술을 상업적, 군사적, 또는 범죄적으로 악용할 가능성이 높음. 예를 들어, 금융 예측 모델이 탈취되어 경쟁사나 범죄 조직이 악용될 수 있음
  - 해결 방안: 모델 암호화, 액세스 제한, 워터마크 삽입 등이 해결 방안이 될 수 있음

- 프라이버시 침해(Privacy Violations)
  - 문제점: AI 시스템은 민감한 개인 데이터를 학습하거나 처리하기 때문에 프라이버시

침해 위험이 존재하며, 데이터 탈취뿐만 아니라 모델 자체가 개인정보를 역추적(Model Inversion)하는 문제도 발생 가능함. 예를 들어, 얼굴 인식 AI가 사용자 사진을 학습하여 민감한 정보를 도용할 수 있음

- 해결 방안: 차등 프라이버시(Differential Privacy), 데이터 최소화 원칙 등이 적용될 수 있음

- AI의 오용(Malicious Use of AI)
  - 문제점: 공격자들이 AI를 활용해 더욱 정교하고 효과적인 사이버 공격을 수행하며, 피싱 이메일 생성, 악성 코드 개발, 네트워크 취약점 탐지 등에 AI 기술이 사용될 수 있음. 예를 들어, AI 챗봇을 활용하여 마치 인간이 하는 듯한 피싱 메시지를 자동으로 생성할 수 있음
  - 해결 방안: AI 감시 체계 강화, 악용 사례 탐지 기술 개발 등이 해결 방안이 될 수 있음

- AI 시스템의 의존성과 복잡성
  - 문제점: AI 시스템이 중요한 인프라(예: 전력망, 의료 시스템 등)에서 사용되면서 보안 사고가 발생할 경우, 피해가 광범위하게 확산될 수 있고 AI 시스템의 복잡성으로 인해 취약점을 사전에 탐지하거나 대응하기 어려울 수 있음. 예를 들어, 전력망을 관리하는 AI 시스템이 공격받아 대규모 정전 사태가 발생할 수 있음
  - 해결 방안: AI 보안 표준 도입, 주기적인 모니터링 및 위협 탐지 시스템 운영

- AI 규제 및 표준화 부족
  - 문제점: AI 시스템에 대한 보안 표준과 규제가 부족하여 조직마다 다른 보안 수준을 유지할 경우, 법적/윤리적 이슈로 인해 보안 체계 개발이 느려지는 경우도 존재함
  - 해결 방안: 국제표준의 개발과 국가적 정책 마련 등이 해결 방안이 될 수 있음

Chapter 03

규제 동향 및 현안

PART 01

글로벌 AI 사이버 보안 규제 동향

1.1 국제기구의 규제 동향

국제기구의 규제 동향

- UN(유엔)
  - UN은 AI 기술이 포함된 무기 시스템과 데이터 보호 관련 이슈를 다루고 있으며, 국가 간 협력을 통해 AI 기반 사이버 위협 대응 방안을 논의 중
- ITU(국제전기통신연합)
  - ITU는 AI와 관련된 글로벌 표준화 작업과 함께 사이버 보안 관점에서 데이터 관리와 신뢰성 보장을 위한 가이드라인을 개발 중
- OECD(경제협력개발기구)
  - OECD는 원칙을 수립하고, AI와 사이버 보안 간의 상호작용을 규제하는 정책 프레임워크를 제시

1.2 지역별 규제 동향

유럽연합

- 인공지능 법안(AI Act)
  - 2021년에 발표된 유럽 최초의 AI 규제법안으로, AI 시스템의 위험 수준에 따라 “금지된 위험”, “고위험”, “제한적 위험”, “취소 위험”의 4단계로 분류
  - AI 사이버 보안과의 관계: 고위험 AI 시스템은 필수적으로 사이버 보안 평가를 포함해야 하며, 데이터 보호와 모델의 신뢰성을 보장하는 조치가 요구됨

- 예를 들어, 의료, 금융, 공공 서비스에서 사용되는 AI 시스템은 사이버 공격으로부터의 안전성을 입증해야 함
- AI 시스템의 개발 단계에서부터 사이버 보안 위협을 고려하도록 "보안 설계(Security by Design)" 원칙을 적용
- 고위험 AI 시스템(예: 의료, 금융, 생체인식)에 대해 엄격한 사이버 보안 요구사항 부과
- 데이터 보안, 적대적 공격 방어, 데이터 정확성 검증 의무화 포함

- 네트워크 및 정보 보안 지침(NIS2 Directive)
  - 필수 서비스 운영자를 포함한 AI 시스템의 보안 및 사이버 복원력을 강화
  - 주요 디지털 인프라 제공자는 적절한 보안 조치를 취해야 함

미국

- 국가 AI 이니셔티브 법안(National AI Initiative Act, 2020)
  - AI 연구 및 개발에서 보안과 윤리적 문제를 고려하도록 규정
  - AI 모델의 보안 평가 및 적대적 공격 방어를 연구 대상으로 지정

- 연방 무역 위원회(FTC, Federal Trade Commission)의 가이드라인
  - AI 기반 시스템이 소비자 데이터를 안전하게 처리할 것을 요구
  - 허위 또는 불완전한 AI 보안 조치에 대한 책임 부과

중국

- 인터넷 정보 서비스 알고리즘 규제 (2021)
  - AI 알고리즘의 보안 검토 및 심사를 의무화
  - 알고리즘이 공공질서, 보안, 데이터 보호 규칙을 준수하도록 규제

- 사이버 보안법 (Cybersecurity Law)
  - 중요 정보 인프라에 사용되는 AI 시스템의 데이터 보호와 보안 강화를 요구
  - 국가 보안 평가 기준 도입

한국

- AI 윤리 기준 (2020)
  - AI 시스템이 인간의 존엄성과 공공의 이익을 침해하지 않도록 설계 및 운영
  - 보안성과 안정성을 필수 요소로 포함
- 정보통신망법 및 개인정보 보호법
  - AI 시스템이 개인정보 처리 시 데이터 암호화 및 접근 통제를 의무화
  - 데이터의 무단 수집 및 사용에 대한 엄격한 처벌 규정

규제 관련 도전과제

- AI 사이버 보안 표준이 국가 및 기관마다 다르며, 국제적으로 통일된 보안 프레임워크가 부재한 상황임
  - AI 기술이 빠르게 발전하여 기존 규제 체계를 빠르게 넘어가는 상황이므로, 엄격한 규제 준수를 위한 비용이 중소기업에 큰 부담이 될 수 있음
  - 현재 대부분의 규제는 사후 대응에 초점을 두고 있으므로 예방적 보안 조치가 부족한 상황인 것이 도전과제가 될 수 있음

PART 02

규제 현안 및 경과

2.1 해외 규제 현안 및 경과

EN 303 645 CIoT 보안 표준

- 인터넷 기반 소비자 제품의 사이버 보안에 대한 국가/지역 표준을 기반
  - 유럽무선기기 지침(RED)과 관련, 사이버 보안 규제가 강화되고 있으며 IoT 기기가 사이버 공격의 주요 대상 중 하나가 되어 보호 표준 중요성이 더 높아짐
  - 소비자 제품에 대한 우수한 보안 기준을 지원
  - 기본 암호 없음, 취약성 공개 정책 구현, 소프트웨어 업데이트 유지 등 상위 3가지 권장 사항 제공 및 소비자 IoT 장치에 대한 특정 데이터 보호 조항이 포함됨

- 경과

  - ETSI TR 103 621, (2022년 3월), Implementation Guide
  - ETSI EN 303 645 V2.1.1, (2020년 6월)
  - ETSI TS 103 645 V3.1.1, (2024년 1월)
  - ETSI TS 103 701, (2021년 8월), Assessment Specification
  - ETSI EN 303 645 보도 자료, (2020년 6월)

영국 AISI(AI Safety Institute) 구축

- 고급 AI 시스템을 주기적으로 평가하여 발생할 수 있는 잠재적 피해를 평가 수행
  - 최근 이미 대중이 사용하고 있는 5개의 대규모 언어 모델에 대한 평가 결과를 제시함
  - 모델 평가에 대한 첫 번째 기술 블로그 게시물 게시
  - AI 위험에 대한 과학적 증거 조사를 위해 30개국을 조율하는 최초의 첨단 AI 안전성에 관한 국제 과학 보고서 발간('24.5.17)

- AI 안전성 평가를 실행하기 위한 플랫폼인 Inspect를 오픈소스로 제공('24.4.21)
- 미국 AI 안전연구소와 상호 운용 협력을 위한 양해각서('24.4.2)에 이어, 캐나다 AI 안전연구소와 협력하기 위한 새로운 파트너십 발표('24.5.20), 이를 통해 테스트 및 평가 작업을 지원하고 각 AISI간 파견을 활성화하기 위한 전문지식을 공유할 수 있도록 구축 중

CEN(유럽표준화위원회) / CENELEC(유럽전기기술위원회)

CEN/CLC/JTC 13(사이버 보안 및 데이터 보호)

- ISO/IEC JTC 1 및 기타 SDO와 ISO, IEC, ITU-T 및 산업과 같은 국제기구에서 이미 발행했거나 개발 중인 문서의 식별 및 채택 가능성이 범위에 포함됨
- AI 사이버 보안에 대한 표준과 규제 관련 작업프로그램은 아직 미진행 상태

CEN/CLC/JTC 21(인공지능)

- ISO/IEC JTC 1 및 SC 42 인공지능과 같은 소위원회와 같은 다른 조직에서 이미 사용 가능하거나 개발 중인 국제표준을 식별하고 채택
- 유럽 시장 및 사회적 요구를 해결하고 EU 법률, 정책, 원칙 및 가치를 뒷받침하는 표준화 결과물을 생산
- AI 사이버 보안 및 안전에 대한 표준과 규제 관련 작업프로그램은 아직 미진행 상태

미국의 사이버 보안 거버넌스

국가 사이버 보안 전략(National Cybersecurity Strategy, NCS) 발표('23.3)

- 국익 증진 및 경쟁력 확보, 향후 글로벌 공동 대응을 위한 방향성을 제시
- 바이든 정부 출범 이후의 사이버 위협 대응 전략들을 통합·계승하는 새로운 종합 전략으로, 연방정부의 역할 강화 및 실질적 보안 수준 강화를 목표로 함
- 국가 사이버안보 및 인공지능 이니셔티브 정책, 사이버안보 개선 행정명령(EO-14028), 5G 보안)을 위한 국가전략 등 주요 내용을 반영
- 전략별 실행계획 및 책임기관, 목표 시기를 공개, 대통령실 소속 국가 사이버 국장실(ONCD) 주도하에 오픈소스 SW 보안 솔루션 개발('23.7)

- CISA(사이버 보안·인프라 보안국)은 사이버 방어, 중요 인프라 보안 및 사이버 회복력 확보 방안을 중심으로 CISA 사이버 보안 전략 계획 발표
  - 「CISA 전략계획('23~'25)」을 발표('22.9), 전담 기관이 가지는 주요 기반 시설 보호 및 주·연방정부와의 협력 역할을 강조
  - 바이든 대통령의 행정명령 후속 조치로 'AI를 위한 첫 번째 로드맵'을 발표, 사이버 보안 관점에서 AI에 대한 5가지의 접근방식을 제시
  - 국토안보부가 전 세계적으로 AI 안전 표준 채택을 촉진, 미국 네트워크와 중요 기반 시설을 보호하며 AI로 인한 위험을 줄이고 숙련된 인재 유치를 지원('23.10)

- 국립 표준기술연구소(NIST)
  - '14년 오바마 정부에서 제시한 사이버 보안 프레임워크(Cyber Security Framework, CSF)를 대외환경 변화에 맞게 현행화하여 CSF2.0을 발표('24)
  - 「국가 주요 기반 시설의 사이버 위협 대응 강화」를 위한 행정명령(EO 13636) → (트럼프 행정부) 「연방 네트워크와 주요 기반 시설의 사이버 보안 강화」를 위한 행정명령(EO13800, '17.5)을 통해 정부 기관의 사이버 보안 위험관리에 CSF 도입을 의무화함
  - 사이버 보안 환경변화와 국내외 활용 수요 반영을 위해 다양한 부문의 의견을 수렴하여 사이버 보안 프레임워크를 최신화(CSF 2.0, '24.2)
  - 제로트러스트의 정의, 원칙, 보안 위협 등을 기술한 '제로트러스트 아키텍처(Zero Trust Architecture, SP800-207)' 발표('20.8)
  - (바이든 행정부) 행정명령(EO10428)*을 통해 연방정부의 사이버 보안 현대화를 위한 제로트러스트 전략 채택('21.5)

    * Executive Order 10428 – Improving the Nation's Cybersecurity
  - (사이버 보안, 인프라보안청 CISA) 정부 기관 도입을 위한 '제로트러스트 성숙도 모델 1.0' 발간

- 안전한 인공지능 법(Secure Artificial Intelligence Act of 2024), '24.5.1
  - 인공지능 관련 보안 · 안전 사고 및 위험추적 처리 절차 개선 등에 관한 「인공지능 관련 보안 안전사고 및 위험 · 추적 관리와 기타 목적을 위한 법률안」 발의
  - 인공지능 취약성 DB 개선 및 보안 취약점의 특성 식별관리 및 개발

- 인공지능 보안 안전, 사고를 추적하고 관리할 수 있도록 사고 구축에 포함할 사고 선별 및 사고 익명화 등 수행
- 공통 취약성 및 노출 프로그램 관련 절차 개선 및 자발적 합의 표준 평가
- 국가안보국은 사이버안보 협력 센터 내에 인공지능 안전센터 설치

영국의 사이버 보안 의무화

- 국가 사이버 보안 센터, NCSC) 제로트러스트 아키텍처 설계·구축의 가이드라인으로 '제로트러스트 아키텍처 설계 원칙 1.0' 발표('21.7)
  - PSTI법(제품 안전 및 통신 인프라 법)에 명시된 요구사항을 의무화 이행('24.4.29)
  - 요구사항은 PSTI 법에 따라 평가될 수도 있지만, "소비자 IoT의 사이버 보안"이라는 ETSI EN 303 645 표준에 따라 평가가 이루어질 수 있음→ 요구사항을 준수하고 자체 신고함

중국의 데이터 보안법과 개인정보 보호법

- 미국의 첨단 기술 기업에 대한 규제가 전방위적으로 확대되면서 ▲데이터 국지화 ▲소스 코드 공개 ▲기술 이전 강요 등 사이버 보안 이슈 부각
  - 기술 안보를 내세워 중국 첨단기업의 수출입 규제, 특히 디지털 무역 활성화에 장애 요소인 데이터 국지화를 반대
  - 「데이터 보안법」('21.09)과 「개인정보 보호법」('21.11) 등 법·제도적 근거를 바탕으로 중국에서 수집한 데이터 및 개인정보의 역외 이전을 제한, 외교적 수단으로 활용
  - 데이터 보안법은 유형별 데이터 제도를 통해 사이버 안전과 디지털 산업의 발전 기반을 마련. 개인정보 보호법은 법률의 개별 규정에서 보호하던 개인정보의 정의와 규정을 구체화

- 국가인터넷정보판공실: 「사이버 보안법」을 5년 만에 개정하며 네트워크 운영 보안의 일반규정을 위반하는 행위에 대한 법적 책임을 명시('22.9)
  - 기존 네트워크 운영 보안에 관한 법적 제도 시행 상황을 고려하여, 네트워크 운영 보안 의무를 저버리거나 사이버 위협을 가하는 행위의 처벌 강도를 조정
  - 핵심 정보 인프라 운영자의 위법 행위에 대한 처벌 규정을 개선 및 네트워크 정보 보안 의무를 위반하는 행위에 대한 법적 책임을 통합

- 개인정보 보호법에서 규정한 법적 책임 제도를 수정하여, 기존의 개인정보 보호 관련 법적 책임 제도가 기타 법률 적용을 받도록 할 방침

일본의 사이버 보안 관련 동향

- 정부가 제정한 상위 법령에 따른 국가적 차원의 거버넌스 구축하고, 「사이버 보안 전략」을 비롯한 주요 정책을 지속해서 현행화 진행
  - ’21년부터 디지털 사회 실현을 위해 「디지털 사회 형성 기본법」 수립, 디지털청 설치 등 추진 중으로 중점 분야로 사이버 보안 중요성 강조
  - 「사이버 보안 기본법」 제정 후, 내각 총리를 최고책임자로 하는 ‘사이버 보안 전략 본부’를 설치·운영 및 안전한 사이버공간 구현을 위해 ‘디지털청’과 협력 중
  - 「사이버 보안 기본법」 제정 전후로, 대내외 사이버 환경변화에 대응하기 위해 핵심 정책인 「사이버 보안 전략」을 3년 단위로 개정

- 사이버 보안 전략본부 산하, 사이버보안센터 「사이버 보안 전략」에 따른 「사이버 보안 2024」 발간(’24.07)
  - 「사이버 보안 기본법」에 명시된 정책 목적과 ’21년 「사이버 보안 전략」의 추진 방향에 따른 ’23년도의 실적과 ’24년도의 중점 추진 계획을 제시
  - 국가의 전반적인 사이버 보안 대응 능력을 유럽과 미국 등 주요 강국 수준으로 확보하기 위해 종합적인 국가전략 수립

- 디지털청에서 제로트러스트 아키텍처 개념, 적용 방침, 적용 순서, 정책 등을 정의한 ‘제로트러스트 아키텍처 적용 정책’ 발표(’22.6)

2.2 국내 규제 현안 및 경과

120대 국정과제

- 윤석열 정부는 「120대 국정과제」를 통해 사이버안보 대응 역량 강화의 국정 방향을 제시하고 「대한민국 디지털 전략」에서 디지털 사회 구현의 핵심으로 정보보호의 중요성을 강조함
  - 국정과제에서 국가 안보 태세 유지와 산업·기술·인재 경쟁력 향상을 위해 사이버 보안 분야에 범정부 차원의 협력체계 공고화 방안 제시
  - (사이버 보안 역량 강화) 보안클러스터 모델의 지역거점 확산으로 기업 성장 지원, 10만 사이버 보안 인재 양성(~'26년)
  - 「대한민국 디지털 전략」 기술 패권에 대응하기 위한 6대 디지털 혁신 기술 중 하나로 사이버 보안을 설정, 최적화된 R&D 협력 방식 및 인력양성 구축 방안 제시
  - 사이버전, 미래 기술(6G, 양자 등)에 대비한 지능형 보안 핵심기술 및 데이터 보안 원천기술 확보 및 4대 방어 기술 개발 목표(미국 대비: 88.6%('20) → 93%('27) 역량 달성)

- 「정보보호산업의 글로벌 경쟁력 확보 전략」 발표('23.9)
  - 제로트러스트, 공급망 보안 등 新 보안 체계 적용·확산, 미래형 융합보안 시장 개척 및 AI 보안 사이버 보안·정보보호 분야의 차세대 기술·산업 경쟁력 제고
  - 「K-시큐리티 얼라이언스」 민·관 협력을 통한 통합보안 모델 개발
  - 「K-시큐리티 클러스터 벨트」 국내 정보 보안 산업의 시설 및 투자 확충, 인재 양성 활성화 「K-시큐리티 랩」 신흥시장 진출 가속화를 위한 현지 플랫폼 구축

- 「2024 국가 사이버안보 전략」을 새롭게 개정하여 고도화된 기술 및 국제 정세 문제로부터 국가 안보를 확보하고자 함('24.2)
  - 생성형 AI와 같은 ICT 신기술에 대응하고, 북한의 사이버 공격을 악의적 행위 및 위협으로 명시하여 안보 관련 대응을 강화하는 새로운 전략
  - (3대 목표) ▲공세적 사이버 방어 및 대응 ▲글로벌 리더십 확장 ▲건실한 사이버 복원력을 설정, 이를 실현할 5대 전략과제 제시

- 5대 전략과제: ①공세적 사이버 방어 활동 강화 ②글로벌 공조 체계 구축 ③국가 핵심 인프라 사이버 복원력 강화 ④신기술 경쟁 우위 확보 ⑤업무 수행 기반 강화

5. 대통령 직속 디지털플랫폼정부위원회

- 국가적 차원의 '제로트러스트 도입 추진 계획'('23.4) 및 과기정통부의 「제로트러스트 가이드라인 1.0」 발표('23.7), 국내 도입을 위한 기반 구축

6. 한국의 「AI 기본법」('24.12.26, 국회 통과)과 EU AI Act('24.8.1. 발효)를 비교

- 한국은 산업 육성과 윤리적 활용에 초점을 맞추는 반면, EU는 위험관리와 안전성 확보를 우선시하였고, EU는 위험 기반 접근법을 통해 AI 시스템을 세분화하여 각기 다른 규제를 적용하지만, 한국은 포괄적 규제와 가이드라인 중심으로 규제를 설계하는 점이 다름
- 투명성 요구 수준도 EU는 AI 투명성 요건을 명확히 규정하며 사용자에게 AI 사용 사실을 반드시 알릴 것을 요구하지만 한국은 투명성을 권장하나 의무화 수준 낮음
- 위험 분류 관점에서 보면, EU는 위험에 따라 금지(prohibited risk)에서 규제 제외(minimal risk)까지 세분화하지만, 한국은 아직 구체적 위험 분류 체계가 도입되지 않음
- 산업 육성 지원 관점에서 보면, 한국은 AI 산업 육성을 위한 지원 정책(R&D, 데이터 공유)을 강조하며, EU는 규제 준수를 강조함
- EU AI Act와의 공통점

▪ AI 윤리 원칙: 공정성, 투명성, 책임성을 강조
▪ 국제표준과의 연계: 국제 AI 표준에 부합하도록 국내 정책 설계
▪ AI 안전성과 신뢰성 확보: AI 시스템의 안전성을 보장하고, 위험 최소화 목표

〈표 7〉 한국의 AI 기본법과 EU AI Act 비교

구분	한국「AI 기본법」	EU AI Act
제정시기	▪ 2024년 12월 26일 제정 ▪ 2026년 1월 1일부터 발효	▪ 2023년 6월 14일 제정 ▪ 2024년 8월 1일 발효
접근방식	▪ 자율 규제 중심	▪ 위험 기반 접근법 (risk-based approach)
목적	▪ AI 기술의 윤리적 사용 및 안전한 개발 보장 ▪ 국가 차원의 AI 산업 육성 및 국제 경쟁력 강화	▪ AI의 안전성 확보 및 윤리적 사용 보장 ▪ EU 단일 시장 내에서 통합 규제 적용

주요 특징	▪ 윤리 원칙 제시: 공정성, 투명성, 책임성 등을 기반으로 AI 개발 및 활용 규범 제정 ▪ 자율 규제 중심: 민간의 자율성을 강조하며 AI 기술 발전을 저해하지 않는 방향으로 설계 ▪ 산업 지원: AI 스타트업 및 기업에 대한 지원 정책 포함 (R&D 투자, 데이터 인프라 지원 등) ▪ 국내 표준화 연계: 국제표준과 조화를 이루는 국내 AI 표준 제정	▪ 위험 기반 접근법: AI 시스템을 4개 위험군으로 분류 - Prohibited risk: 금지 - High risk: 엄격한 규제 - Limited risk: 정보제공 요구 - Minimal risk: 규제 제외 ▪ 투명성 요건: 사용자에게 AI의 사용 사실과 작동 원리를 명시적으로 알릴 것을 요구 ▪ 엄격한 규제: 특히 high risk AI는 데이터 관리, 알고리즘 검증, 사용 환경 평가를 포함한 다중 규제 적용 ▪ 강력한 감독: 각국의 독립적 감독 기관이 시행을 모니터링
규제적용 대상	▪ 모든 AI 시스템, 특히 국민 안전 및 복지에 영향을 미치는 서비스	▪ 위험 군별로 구분하여 차등 적용 ▪ EU 내에서 제공, 사용되는 모든 AI 시스템
위험 분류	▪ 명시적 위험 분류 없음	▪ 4개 위험군 (prohibited, high, limited, minimal risk)으로 분류
규제 초점	▪ 윤리 원칙 준수, 산업 육성 지원	▪ 안전성 보장, 데이터 및 알고리즘 검증
투명성 요건	▪ 일반적 투명성 권장	▪ 사용자에게 사용 사실 및 작동 원리 공개 의무
감독체계	▪ 정부 주도, 민간 협력	▪ EU 차원 감독 + 각국 독립적 기관
표준화노력	▪ 국내 표준화 우선, 국제표준 연계	▪ 국제표준과 완전한 통합
산업지원	▪ R&D 투자, 데이터 인프라 지원 포함	▪ 산업 지원보다는 규제에 중점
운영방식	▪ 정부 주도, 민간 협력 기반	▪ EU 차원의 규제 집행 및 개별 국가의 감독 기관 협력

Chapter 04

향후 일정 및 산업계 대응 방안

PART 01

규제 향후 일정

1.1 EU AI Act 일정

EU AI Act의 추진경과 및 일정

추진 일정

추진 일정		주요 내용
2021	4월	▪ (EC) AI 법안 제안 및 공개 자문 개시
	8월	▪ 유럽의회 시민권 및 헌법 정책국, 윤리적, 법적 관점에서 생체인식 기술 사용 분석 연구 발간
	11월	▪ (EC) 소셜 스코어, 생체인식 시스템, 고위험 앱 관련 변경 사항이 반영된 초안을 이사회, 의회 제출
2022	4월	▪ 유럽의회 내부시장위원회(IMCO)와 시민자유위원회(LIBE) 보고서 초안 발표
	5월	▪ (EU 이사회) 이미지 및 음성 이해, 오디오 및 비디오 생성 등에 관한 수정안 발표
	9월	▪ 유럽의회 법제위원회가 검토, 마지막 위원회로서 AI 법안 채택
	12월	▪ EU 이사회가 AI 법안에 대한 공통 입장 채택
2023	6월	▪ (유럽의회) AI 법안에 대해 찬성 499표, 반대 28표, 기권 93표로 통과
	12월	▪ 유럽의회와 EU 이사회 잠정 합의
2024	2월	▪ 유럽의회 내부시장위원회 및 시민자유위원회가 71대 8로 회원국과 법안 협상 결과 승인
	3월	▪ 유럽의회 최종 채택
	5월	▪ EU 이사회 최종 승인
	6월	▪ 유럽의회, EU 이사회 의장 서명 후 관보 게재 및 발효, AI 법령 EU 감독기구인 AI 사무소설립을 위한 작업 시작, 각 EU 회원국은 AI 규제 샌드박스 제정
	8월	▪ EU AI Act 발효 시작

● 향후 일정

추진 일정		주요 내용
2025년	~1분기	▪ 금지된 AI 시스템 금지조항 발효 및 집행 (Title 1: General Provisions, Title II: Prohibited AI practices)
	2분기~3분기	▪ 파운데이션 모델을 포함한 범용 AI 모델 관련 의무 사항 발효 ▪ (Title III, Chapter 4: Notified authorities and notified bodies, Title VI: EU AI Board/National Regulators, Title VIIIA: GPAI, Title X: Penalties)
	2025년 4분기~ 2026년 3분기	▪ 독립적으로 운영되는 고위험군 AI 관련 의무 사항 발효 + General Application
2026년		▪ AI 법령 모든 의무 사항 발효 - Annex II- High Risk AI system used as a safety component of a product covered by EU Harmonisation legislation

1.2 규제 대응 전략

AI의 양면성과 활용

- AI가 사이버 보안 문제를 한층 더욱 크게 할 수도 있지만, 역설적으로 AI를 활용한 사이버 보안 강화도 가능함
- AI 기술은 한층 정교하고 효율적인 보안 솔루션을 제공
- 비밀번호 생성, 비정상 데이터 탐지, 시뮬레이션 환경 생성 등 다양한 사례에서 생성형 AI는 사이버 보안의 중요한 기반 기술로 자리 잡고 있음
- 앞으로 AI 기술은 빠르게 발전하며, 사이버 위협에 대한 대응력을 더욱 강화할 것

● AI가 사이버 보안의 위협 요소이기도 하지만 역설적으로 사이버 보안을 개선할 수 있는 대안으로도 주목

- 생성형 AI 기술은 사이버 보안으로 악용될 수 있지만, 방패 역할을 수행할 수 있다는 점을 고려해야 할 것

- 이에 많은 글로벌 빅테크 기업은 AI를 이용한 사이버 보안 위협에 대응할 수 있는 사전적 예방 기술도 동시에 개발하고 있음
- 사이버 보안을 위한 AI의 핵심적인 개념은 AI를 사용하여 여러 소스에서 이벤트와 사이버 위협 데이터를 분석하고 상호 연결하여 보안 전문가가 추가 조사, 대응 및 보고에 사용하는 것을 지칭함
- 사이버 공격이 정부 또는 기업의 보안팀에서 정의한 특정 기준을 충족하는 경우 AI는 대응을 자동화하고 피해를 최소화하는 것임
- 최근 발전하고 있는 생성형 AI는 기존 데이터의 패턴을 기반으로 원래 자연어 텍스트, 이미지 및 기타 콘텐츠를 생성하여 대응할 수 있는 다양한 방법을 제시하고 있음

● AI가 사이버 보안을 개선할 수 있는 세 가지 방법

① 사이버 위협 완화

- AI 기술은 취약성과 의심스러운 행동을 식별하여 사이버 공격을 감지하는 데 도움
- IBM의 자료에 따르면, 사이버 공격의 91%는 경고를 생성하지 않으며 기업은 침해를 식별하는 데 평균 207일, 침해를 억제하는 데 73일이 걸리는 반면 AI는 이벤트를 신속하게 분석하여 사이버 보안 위험과 관련 재정 및 평판 손실에 보조를 맞출 수 있도록 지원 가능
- 무엇보다 AI는 사이버 위협을 예측하는 데 도움이 될 수 있으며, 금융기관에는 알고리즘을 사용하여 대규모 데이터 풀을 스캔하고 일반적인 행동 패턴을 식별하며, 잠재적인 사기를 예측하는 고도의 사기 방지 시스템 개발
- AI는 리소스가 부족한 정부 또는 기업의 보안팀을 지원하는 데 도움이 될 수 있으며 AI는 알고리즘을 사용하여 시스템 전반의 사건을 모니터링하고 즉각적인 조치가 필요한 사이버 위협에 플래그를 지정함으로써 도움을 줄 수 있음

② 데이터 보안

- IBM 리서치의 데이터 침해 보고서 2021의 비용 보고서에 따르면 2020년 데이터 유출 비용은 386만 달러(약 46억 원)에서 2021년 424만 달러(약 51억 원)로 10% 증가(IBM 2024)
- 높은 재정적 손실 외에도 이러한 유출은 기업과 고객을 위험에 빠뜨리고 심각한 법적 문제를 야기
- 보안 AI 및 자동화를 갖춘 조직은 AI 기술을 사용하여 데이터 거버넌스 프로세스를

강화할 수 있는데 예를 들어 AI는 다양한 소스를 통해 민감한 데이터를 식별한 다음 기업에서 익명화, 제거, 암호화 또는 외부 또는 내부 위협으로부터 다른 방식으로 보호가 가능

- 이러한 데이터 사용을 통해 기업은 기밀 정보를 안전하게 처리하고 유럽연합 일반 개인정보 보호법(General Data Protection Regulation, GDPR)과 같은 개인정보 표준 및 규정을 준수할 수 있게 됨
- AI는 합성 데이터를 생성하여 시나리오를 생성하고 미래의 사이버 노출을 예측할 수 있는 것

③ AI 기반 생체 인증

- AI는 지정된 범위 내에서 이러한 메트릭 편차를 분석하고 그에 따라 결정을 내리고 지속 학습이 가능
- AI는 키 입력, 스크롤 및 스와이프 패턴과 같은 고유한 행동 생체인식을 분석하여 사용자를 식별하고 봇 및 자동 공격과 구별하는 데 도움이 될 수 있음

PART 02

산업계 영향 및 대응 방안

2.1 국내·외 산업계 영향

IBM의 Security QRadar(IBM 2024)

- IBM의 보안 방어를 가속화 하는 AI 기술
  - 오늘날 많은 기업들의 보안팀은 자체적으로 정교한 해커, 공격 표면 확장, 데이터 폭발, 인프라 복잡성 증가 등 데이터를 보호하고, 사용자 액세스를 관리하고, AI 보안 위협을 신속하게 탐지하고 대응하는 데 방해가 되는 많은 문제에 직면
  - IBM Security는 AI 위협 탐지 및 마이그레이션*을 가속화하고, 대응을 신속하게 처리하며, 사용자 ID와 데이터 세트를 보호하는 등 분석가의 시간을 최적화하는 동시에 사이버보안 팀과 긴밀하게 소통하고 책임감 유지 필요
    * 마이그레이션(Migration)은 시스템, 데이터, 소프트웨어, 애플리케이션, 또는 사용자 환경을 하나의 플랫폼, 환경, 혹은 구조에서 다른 것으로 이동하거나 전환하는 과정을 의미
  - AI 도구는 섀도 데이터를 식별하고, 데이터 접근의 이상 징후를 모니터링하며, 데이터 또는 민감한 정보에 액세스하는 악의적인 공격자의 잠재적 위협에 대해 사이버 보안 전문가에게 경고하여 문제를 실시간으로 감지하고 해결하는 데 드는 시간을 절약
  - AI 기반 위험 분석은 높은 정확도의 알림을 위한 인시던트 요약을 생성하고 대응을 자동화하여 알림 조사 및 분류를 신속하게 진행
  - AI 기술은 위협 환경 전반에서 취약성을 식별하고 사이버 범죄자 및 사이버 범죄를 방어하는 데 도움

- IBM은 사용자 액세스 요구와 보안의 균형 유지
  - AI 모델은 각 로그인 시도의 위험을 분석하고 행동 데이터를 통해 사용자를 확인하여 검증된 사용자의 액세스를 간소화하고 비용을 최대 90%까지 절감함으로써 보안과 사용자 경험의 균형을 유지하는 데 도움
  - AI 시스템은 보안 시스템 내에서 피싱, 멀웨어 및 기타 악성 활동을 방지하여 높은 보안 태세를 유지할 수 있도록 지원

마이크로소프트(MS 2024)

마이크로소프트의 사이버 보안과 AI

- AI 개발 이전 단계부터 사이버 커뮤니티는 1980년대 후반부터 기술 발전이 진행되었으며 2000년대부터 본격적으로 낮은 수준의 AI를 적용하고 있음
- 초기 마이크로소프트에서는 사이버 보안에서 단순하게 정의된 매개 변수에 따라 경고를 하는 규칙 기반 시스템을 사용했으며 2000년대 초부터 대규모 데이터 집합에서 분석하고 학습하는 AI의 하위 집합인 기계 학습을 활용
- 이후 조직 전체의 일반적인 트래픽 패턴 및 사용자 작업을 이해하여 비정상적인 일이 발생할 때 식별하고 대응할 수 있게 개선하였고, AI의 최근 발전으로 기존 대형 데이터의 구조를 기반으로 새 콘텐츠를 만드는 생성형 AI를 적용하는 단계로 발전

공격과 방어의 도구가 된 AI

- AI를 사용하는 것은 사이버 공격자일 수도 있어 이에 대한 대응이 필요함
- 국가 단위 공격자, 대규모 범죄 기업 또는 개인과 관계없이 AI를 악용할 수 있어 악성 행위자는 AI 시스템을 감염시키고, AI를 사용하여 합법적인 사람으로 가장하고, 사이버 공격을 자동화하는 등 사이버 공격에 대한 위험도가 높아짐

사이버 보안과 AI 활용

- 사이버 보안을 위한 마이크로소프트의 AI는 여러 소스에서 대량의 데이터를 평가하여 사람들이 로그인하는 시기 및 위치, 트래픽 볼륨, 직원이 사용하는 디바이스 및 클라우드 앱과 같은 조직 전체의 활동 패턴을 식별하는 기술 적용
- 일반적인 동작을 이해하면 조사해야 할 수 있는 비정상적인 동작을 식별하고 개인정보를 보호하기 위해 조직 내부의 데이터는 다른 조직의 AI 출력에 사용되지 않게 활용함
- AI는 기계 학습 알고리즘을 사용하여 시스템이 평가하는 데이터를 기반으로 지속적으로 학습하므로 생성형 AI는 멀웨어 같은 특정 사이버 위협을 식별할 때 위협 분석을 텍스트화하고 새로운 텍스트 또는 그림을 생성하여 상황을 설명하는 데 도움

AI 사이버 보안의 이점

- 디지털 전환 속도가 빨라지면서 사이버 위협이 점점 더 많아지고, 데이터양이 증가하고, 사이버 공격이 확장됨에 따라 AI는 여러 가지 방법으로 효율성을 높이는 데 도움

① 신속한 사이버 위협 감지에 도움

- AI 보안 솔루션은 잠재적 비정상적 동작을 나타내는 수천 개의 이벤트를 기록하여 의심 활동과 관계있는 경우 잠재적 사이버 위협을 나타내는 동작을 감지

② 생성형 AI를 통한 보고의 간소화

- 생성형 AI를 사용하는 도구는 여러 데이터 원본에서 정보를 가져와 보안 전문가가 이해하기 쉬운 보고서 작성에 도움

③ 취약성 식별

- AI는 알 수 없는 디바이스 및 클라우드 앱, 오래된 운영 체제 또는 보호되지 않는 중요한 데이터와 같은 잠재적인 위험을 감지하는 데 도움

④ 분석가가 기술을 발전시키는 데 도움 제공

- 생성형 AI는 사이버 위협 데이터 및 분석을 자연어로 변환하는 데 도움이 되므로 기술적 능력이 뛰어나지 않은 분석가의 생산성을 높일 수 있으며 생성형 AI는 사이버 공격에 효과적으로 대응하는 방법을 빠르게 학습할 수 있도록 도움

삼성전자

- 삼성전자는 최근 AI 활용 사이버 보안 분야를 강화하고 있음(김재연 2024; 한지연 2024)

  - 2024년 하반기 시장조사기관 가트너에 따르면 세계 정보 보안 서비스 시장은 올해 1,839억 달러(약 245조 원)에서 2025년 2,120억 달러(약 283조 원)로 15.1% 증가할 것으로 전망

  - 가트너는 대규모 언어 모델(LLM)* 등 생성형 AI가 전자기기에 적용되면서 기업들의 보안 소프트웨어 관련 투자가 큰 폭으로 늘어날 것으로 전망했는데 무엇보다 LLM은 외부 데이터센터에 있는 서버를 활용하기 때문에 언제든 사이버 공격을 받을 수 있기 때문임

  * 대규모 언어 모델(LLM, Large Language Models)은 텍스트를 이해하고 생성하는 등의 작업을 수행할 수 있는 인공지능(AI) 프로그램으로 방대한 양의 텍스트 데이터를 학습하여 인간과 유사한 응답을 생성할 수 있는 고급 AI 모델로, 자연어의 복잡성을 이해할 수 있어 기존의 기계 학습 알고리즘보다 정확하다는 평가를 받고 있음

  - 삼성전자는 2024년 10월 3일 '삼성 개발자 콘퍼런스(SDC) 2024'에서 블록체인 기반의 '삼성 녹스'를 통한 개인정보 보호 기능을 모바일 제품을 넘어 TV와 가전제품

으로 확대하겠다고 밝힘

- 삼성 녹스는 삼성전자가 자체 개발한 보안 플랫폼으로 삼성전자는 보안 레벨이 높은 '패스키'를 삼성 계정뿐 아니라 일반 웹 브라우저 로그인에도 쓸 수 있도록 사용 범위를 확장하여 다양한 상품군에 적용할 것으로 전망
- 이와 함께 매년 진행하는 '삼성 보안 기술 포럼'의 2024년 주제를 '생성형 AI와 함께하는 보안: 생성형 지능과 함께 안전한 미래로 (Security with GenAI: Safeguarding the Future with Generative Intelligence)'로 설정하고 AI를 활용한 사이버 보안 부문을 강화하고 있음

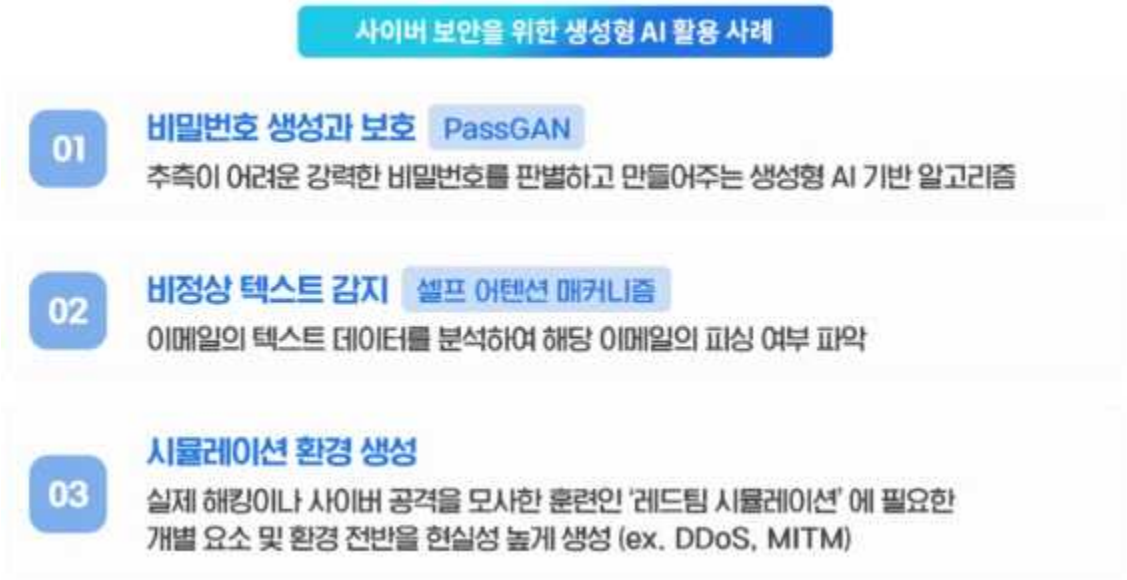
삼성전자의 미래 대응 방향

- 삼성전자는 스마트 기술이 보편화되고 생성형 AI를 악용한 사이버 공격 빈도와 정도가 심화하면서 보안 분야에서 기술적 개발과 적용을 확대하고 있음
- 무엇보다 일반인도 활용할 수 있는 인공지능 시대로 접어들면서 스마트폰과 PC 등에 탑재된 온 디바이스 AI 역시 함께 늘어나며 편리함과 동시에 AI로 악성 코드를 쉽게 만들어 해킹하거나 음성 위변조 등 사이버 공격도 수월한 환경에 직면
- 이 때문에 AI를 활용한 사이버 공격을 해결하기 위해 오히려 보안 분야에서의 AI 기술 중요도가 커지고 있어 삼성전자는 대량의 데이터를 학습한 AI를 활용해 새로운 데이터에서도 분석과 추론을 통해 보안 위협을 미리 감지하고 대응하는데 집중하고 있음
- 장기적으로 삼성전자는 취약점을 탐지한 후 보안패치를 자동화하는 AI 기술을 연구하여 생성형 AI 등을 활용해 다양한 형태의 보안 위협에 대응 가능한 보안 분야 효율성을 높일 것으로 계획(한지연 2024)

생성형 AI를 활용한 사이버 보안 대응

① 비밀번호 생성과 보호

- 대규모 비밀번호 데이터를 생성형 AI가 학습하면 비밀번호의 구조와 패턴을 인식
- PassGAN은 패스워드의 분포를 학습하는 생성적 적대 신경망(Generative Adversarial Network; GAN)을 활용해 안전한 비밀번호의 패턴을 따르는 고유한 비밀번호를 생성할 수 있게 도와줌



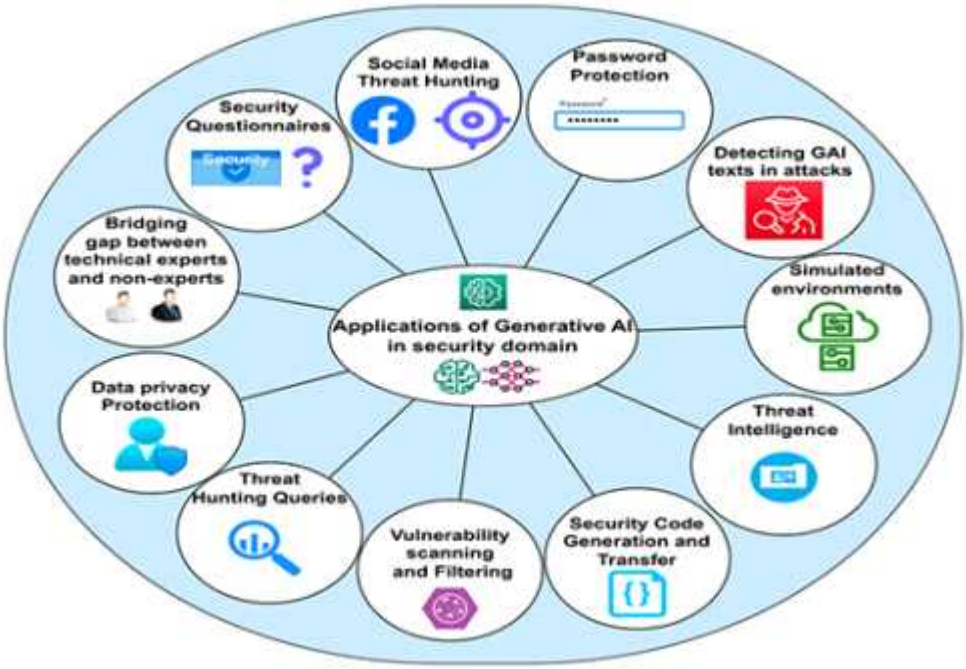
〈그림 2〉 사이버 보안을 위한 AI 활용(임재완 2024에서 재인용)

② 비정상 텍스트 탐지

- 피싱 이메일에는 이메일 주소를 포함해 발신 시간, 이메일 본문, 클릭을 유도하는 링크 등 다양한 텍스트가 포함
- 구글의 Gemini, OpenAI의 GPT 모델, 메타의 Llama 등 초거대 언어 모델(Large Language Models; LLM)을 통해 이메일의 텍스트 데이터를 분석하면 해당 이메일이 비정상(피싱)인지 정상인지 파악 가능
- LLM을 기반으로 한 피싱 탐지 시스템은 지속적인 학습과 업데이트를 통해 새로운 피싱 기법에 대응
- 핵심 알고리즘으로 흔히 언급되는 것은 셀프 어텐션 메커니즘(Self-attention mechanism)

③ 시뮬레이션 환경 생성

- 생성형 AI의 사이버 보안 활용 사례는 시뮬레이션 환경 생성
- 기업들은 사이버 위협 대응력을 키우기 위해 '레드팀 시뮬레이션(red team simulation)'이라 불리는 모의 사이버 공격 실시
- 레드팀 시뮬레이션은 실제 해킹이나 사이버 공격을 모사한 훈련으로 비상시 신속한 대처는 물론 시스템 가용성, 취약점, 효율성 등을 파악하기 위한 목적으로 진행
- 생성형 AI는 레드팀 시뮬레이션에 필요한 개별 요소와 환경 전반을 생성하는데 유용한 역할
- 시뮬레이션 훈련에서 모사하려는 시나리오와 공격 기술을 학습함으로써 생성형 AI는 현실성 높은 피싱 공격, 취약점 탐지, 실시간 대응 훈련 등을 가능하게 해줌



〈그림 3〉 사이버 보안과 AI 활용(Sai et al. 2024; 임재완 2024에서 재인용)

④ 더욱 강력하고 효율적인 방어 시스템

- AI는 방대한 데이터 분석과 패턴 인식 능력을 바탕으로 기존의 방어 시스템을 훨씬 더 강력하고 효율적으로 운영 가능
- 전통적인 사이버 공격에 대한 방어 시스템은 정해진 규칙에 따라 작동하는 반면, AI는 스스로 학습하고 발전하는 능력을 통해 새로운 위협에 대응하고 선제적으로 예방 조치를 취할 수 있음
- AI 기반의 사이버 보안 시스템은 악성 코드를 실시간으로 탐지하고 차단하며, 침입 시도를 예측하여 사전에 차단하는 역할을 수행
- AI는 복잡한 데이터를 분석하여 이상 징후를 감지와 예측에 탁월하며, 이를 통해 테러 공격이나 사이버 공격을 예방하는 데 유용하게 활용

⑤ 첨단 기술 기반의 효율적인 자원 관리

- AI는 방대한 데이터 분석과 최적화 알고리즘을 통해 자원 관리 효율성을 극대화
- AI 기반의 시스템은 군사 작전 계획 수립, 물류 관리, 인력 배치 등 다양한 분야에서 최적의 효율성을 제공
- AI는 복잡한 상황 변화에 유연하게 대응하고 실시간으로 최적의 의사 결정을 지원하는데 탁월하여, 제한된 자원을 최대한 효과적으로 운용하는 데 도움

⑥ 지능형 감시 및 예측 분석

- AI는 다양한 센서 데이터와 영상 분석 기술을 활용하여 감시 및 예측 분석 능력을 향상할 수 있음
- AI 기반의 감시 시스템은 24시간 실시간 모니터링을 수행하면서 이상 징후를 발견하고 위협을 예측하여 선제적으로 대응할 수 있음
- AI는 영상 분석을 통해 군사 기지나 중요 시설에 대한 침입 시도를 예측하고, 드론이나 폭발물을 탐지하는 데 활용
- 또한, AI는 사회 불안 요소를 분석하여 잠재적인 위협을 예측하고 예방 조치에 도움을 줄 수 있음

2.2 주요 국가의 법·제도적 대응

사이버 보안을 위한 주요국 대응 동향

- 디지털 전환이 가속화되면서 사이버 공격이 증가하자, 주요국 정부는 사이버 보안 강화를 위해 내부 조직 및 관련 규정을 정비
- 전통적인 안보 영역과 함께 AI 사이버 보안 문제에 대응하기 위한 정책적·제도적 대응 강화

미국[7)]

- 미국은 1980년대부터 사이버 관련 법·제도를 마련함(문인철 2018, 9)
  - 당시 미국의 사이버 관련 법·제도는 오늘날의 사이버 보안의 개념을 반영하지 못함
  - 지금처럼 인터넷 기술이 발전되지 않은 상황에서 사이버공간의 안보 문제를 고려한다는 것은 시기상조였기 때문임
  - 미국 정부는 여러 차례의 사이버 공격을 경험하면서 사이버 위협의 예방·탐지·평가·해결을 국가 안보 및 경제 안보를 위한 최우선 과제로 삼고 자국의 사이버안보 수준을 꾸준히 격상시켜 왔음

- 미국은 9.11 테러 이후 본격적으로 사이버 관련 법·제도를 마련하기 시작해 2002년 '국토안보법'을 제정
  - 이를 토대로 국토안보부(DHS)를 신설하고, '연방정보보안관리법'을 시행하였음(박상돈 2017)
  - 2014년 사이버안보 법·제도를 체계화하기 위해 관련 법·제도들을 대폭 개편하면서 '국가사이버안보보호법', '연방정보보안현대화법', '사이버안보인력평가법', '국경순찰요원 급여개선법', '사이버안보강화법' 등을 차례로 제정
  - 2015년에는 '사이버안보 정보공유법안', '국가 사이버안보보호 발전법안', '연방 사이버안보강화법안', '연방 사이버안보 인력평가법안' 등 사이버안보 관련 주요 법안들을 새로 구성하여'사이버안보법'을 제정하였음

- 사이버안보 담당 기관

7) 미국의 사이버 보안과 관련한 법·제도적 대응의 주요 내용은 채재병·김일기. 2020. "주요국 사이버안보 전략과 한국에의 시사점."와 임산호. 2023. "사이버안보 위험 확대와 주요국 대응 동향." 을 중심으로 작성하였음.

- 국방부, 국가안보국, 국토안보부, 연방수사국(FBI)이 있으며 특히 국방부는 2010년 5월 사이버 사령부를 개설하여 사이버 공간에 대한 작전 능력을 강화함
- 국가안보국은 미국 국방부 특별활동국 소속으로 암호 작성, 관리, 분석, 해독을 주 임무로 하는 정보수집 기관으로 특화하였음
- 국토안보부도 사이버안보를 담당하는 주요 기관으로, 설립 이유가 9.11 테러를 기반으로 한다는 점에서 국토안보부의 역할은 매우 광범위하며 이러한 맥락에서 사이버안보에 접근하고 있으며 핵심 임무 중 하나가 '사이버공간의 보호 및 안전 확보'임
- 연방수사국은 법 집행기관이지만 수사 목적의 정보활동도 활발히 진행하고 있고, 사이버 보안이나 사이버 테러 등 범죄 활동의 맥락에서 사이버안보에 접근하고 있으며 '사이버범죄수사대(Cyber Crime)'가 담당함

- 2020년대 이후 대응(임산호 2023)
  - 바이든 행정부는 '국가 사이버안보 개선에 관한 대통령 행정명령 140281)(E.O 14028)'을 발표('21.5.12)
  - 행정명령에서는 핵심 인프라에 대한 사이버 공격 대응부터 소프트웨어 공급망 관리 체계를 마련하는 등 적극적인 대응에 나섬
  - 한편, 바이든 행정부는 2023년 3월 새로운 '국가 사이버안보 전략'을 발표하고, 7월에는 '국가 사이버안보 실행계획'을 공개하는 등 국가 차원에서 사이버 보안 분야에 관심을 두고 정책적 대응을 하고 있음

EU[8)]

- EU 집행위는 핵심 인프라에 대한 사이버 공격, 소프트웨어 공급망 위험을 경제 안보 부문의 주요 위험으로 제시
  - EU 사이버보안청(ENISA)을 통한 연구 및 전략 설정, 관련 법안 채택, 개정을 통해 체계를 정비함

- 2022년 9월 제안된 EU 사이버 복원력 법(Cyber Resilience Act, CRA)
  - 제조업체에 소프트웨어 제품의 보안을 보장하도록 책임을 부과
  - 수정안에서는 제조업체가 소프트웨어 취약성을 인지했을 때 보고를 의무화하고 있음
  - 제조물 책임 지침(Product Liability Directive, PLD)은 결함이 있는 제품의 제조

8) EU의 사이버 보안과 관련한 법·제도적 대응의 주요 내용은 임산호. 2023. "사이버안보 위험 확대와 주요국 대응 동향." 을 중심으로 작성하였음.

업체뿐 아니라 결함 부품을 공급한 공급업체의 책임에 대한 지침을 제시

- 2022년 12월 개정된 EU 네트워크·정보 보안 지침(Network and Information Security Directive)
  - 회원국들의 사이버안보 관리 방식을 현대화하기 위함
  - 개정안에서는 사이버 보안 사고에 대한 보고 의무, 네트워크 보안을 위한 위험관리 조치 등을 포함하여 변화하는 기술환경에 대응한 사이버 보안 부분을 보완하고 있음

- 이어 2023년 6월 EU 집행위가 발표한 'EU 경제안보전략'에서는 EU가 직면하고 있는 4가지 경제 안보 위험을 식별
  - 여기에는 사이버 보안 영역에서'핵심 인프라에 대한 물리적/사이버안보 위험'이 포함되었음

일본[9)]

- 일본은 2013년부터 현재까지는 사이버 보안 기본법 제정으로 사이버 위협·공격에 적극적으로 대응
  - 국가안전 보장에서 사이버 보안 영역의 가장 큰 변화는 2014년 11월 사이버 보안 기본법의 제정 후 2015년 1월 전면 시행
  - 기본법 제정을 통해 사이버 보안 정책 추진 체계의 제도적 근간 정립된 상황으로 진화
  - 현재 기본법은 여러 이슈로 인해 2016년 4월과 2018년 12월, 두 번의 개정 진행

- 2015년 1월 사이버 보안 기본법에 근거하여 내각에 「사이버 시큐리티 전략본부」(Cybersecurity Strategic Headquarters)를 설치
  - 전략본부는 일본 사이버 보안 대응의 사령탑 역할을 수행하며, 전반적인 기획·입안·정리·역할을 담당하는 기관으로 일본 사이버 보안 정책 추진의 핵심
  - 사이버 보안 전략 추진 사무국 격으로 내각관방에 「내각관방 사이버 시큐리티 센터」(NISC)를 개편·설립 운영하여 실질적으로 추진하는 주체로서 역할을 하고 있음 (안춘모 2023)

- 일본의 사이버 보안 전략은 전체 정책의 기본전략으로서 큰 틀에서 기본전략의 방향성 혹은 목표는 변화를 보이지 않고 있음

9) 일본의 사이버 보안과 관련한 법·제도적 대응의 주요 내용은 안춘모. 2023. "일본의 사이버 보안 정책 추이와 시사점 연구,"을 중심으로 작성하였음.

- 그러나, 세부적인 시책은 전략 수립 당시의 이슈를 반영하면서 변화가 진행
- 기본전략의 목적은 경제사회, 안전·안심 사회, 국제 및 자국 안전보장 등 크게 3가지 범주에서 일치하며, 목적 달성을 위한 방향성과 세부 시책에서 차별화가 발생

- 본 기본전략은 2015년 9월 4일 기본법에 기반한 최초 사이버 보안 전략이 각의 결정으로 수립
  - 이후 2018년, 2021년 개정안이 수립되었으며, 본 전략에서는 기존 전략의 프레임 범주인 경제, 안심, 협력 등 3가지 목적은 유지하고 신규 방향성으로 ① DX와 사이버 보안 동시 추진, ② 사이버공간 전체를 조망하는 안전·안심 확보, ③ 안전 보장 관점에서 대처 등을 제시

- 동맹국들과 사이버 공격에 공동으로 대응
  - 2021년 7월 미국, EU, 영국, 호주, 뉴질랜드 등 동맹국은 Microsoft Exchange 서버 공격과 관련된 해킹 배후에 중국 국가안전부가 있으며 중국 정부에 이러한 사이버 침해 행위를 중단해야 한다고 공동 성명을 발표하는 등 사이버 보안 영역에서 공동 대응 강화

호주[10]

- 2023년 11월 17일 호주에서 사이버 공격 피해가 급증하면서 호주 정부는 '2023-2030 사이버안보 전략'을 발표
  - 사이버안보 대응 역량 강화를 위해 약 5억 8,700만 호주 달러(약 3억 8,200만 달러) 투자 계획을 밝히고 업계 전반의 임원급이 참여하는 민-관 사이버 위원회 설립
  - 새로운 사이버안보 전략은 기존에 핵심 인프라로 간주하지 않았던 통신 부문의 보안 규정을 호주의 핵심 인프라 보안법(SOCI법, 2018년)에 적용함으로써 주요 통신사들에게 랜섬웨어 보고 의무와 함께 강력한 사이버안보 의무를 적용함
  - 이러한 변화에는 2022년 호주 통신업체인 Optus에서 호주 인구 절반에 해당되는 1천만 명의 개인정보가 노출되는 데이터 도난 사건이 발생하고, 랜섬웨어 공격으로 호주 최대 항만 운영업체인 DP World Australia의 물류 공급망이 중단되는 등 잇따른 대규모 사이버 공격 영향이 있는 것으로 분석

영국

10) 호주의 사이버 보안과 관련한 법·제도적 대응의 주요 내용은 박의례. 2023 "'해킹 피해' 급증한 호주, 5천억원 투자해 '사이버 범죄' 대응." 을 중심으로 작성하였음.

- 영국은 최근 AI 기술 발달로 커지는 사이버안보 위협에 대응하기 위해 AI 안보연구소(LASR)를 신설(현대인 2024)
  - 일부 국가들이 AI를 활용해 악성 소프트웨어 개발을 촉진하고, 사이버 공격에 악용
  - 팻 맥패든 영국 랭커스터 장관은 2024년 11월 25일 런던에서 열린 나토 사이버 안보 회의에서 AI 안보연구소를 설립하여 AI가 국가 안보에 미치는 영향을 평가하고 사이버안보 도구를 만들어내는 중추적 역할을 수행할 것을 제안함
  - AI 안보연구소는 현재 옥스퍼드대에 설치될 예정으로 초기 정부 자금으로 822만 파운드(약 145억 원)가 투입되며 학계와 업계, 정부 정보 전문가들이 참여할 예정
  - 이후 미국·영국·캐나다·호주·뉴질랜드의 정보 동맹인 파이브 아이즈(Five Eyes)와 나토 동맹국을 시작으로 파트너들과 협력을 추진할 계획

다자간 사이버 보안 협력 강화[11)]

- 다자간 공조 추세 강화
  - 외국으로부터의 공격이 잦은 사이버 공급망의 특성상 국가 간 공조가 필수적이라는 인식이 강화
  - 대표적으로 Quad 사이버안보 파트너십으로 2022 도쿄에서 열린 미국, 일본, 인도, 호주 4개국 안보협의체 Quad 정상회의 이후, 4개국은 공동으로 '소프트웨어 보안을 위한 공동원칙'을 발표
  - Quad 사이버안보 파트너십에서 4개국 정상은 ▲위협 정보 공유, ▲디지털 기반 제품·서비스에 대한 잠재적 공급망 리스크 식별 및 평가, ▲정부 조달을 위한 소프트웨어 보안 표준을 조정을 합의

- 동맹국 공동으로 사이버 보안 대응
  - 미국 사이버안보·인프라안보국(CISA), 영국 국가 사이버안보센터(NCSC) 호주 사이버안보센터(ACSC), 캐나다 사이버안보센터(CCCS), 뉴질랜드 국립 사이버 안보센터(NCSC) 등 동맹국의 전담 조직들이 협력하여 사이버안보 강화를 위한 공동 권고안 발표

11) 다자간 협력 대응의 주요 내용은 임산호. 2023. "사이버안보 위험 확대와 주요국 대응 동향." 을 중심으로 작성하였음.

Chapter 05

결론

CHAPTER 05

결론

사이버 보안·AI 사이버 보안 위험성과 국내·외 대응 방향

- 사이버 보안 문제가 가지고 있는 특성을 제시하고 왜 이 시점에서 사이버 보안, AI 사이버 보안 문제가 중요한지를 제시하고자 했음
- 변화하는 사이버 보안 문제의 심각성을 인지하고, 최근 빈번해지는 AI 사이버 보안 문제까지 다각적으로 살펴보고 그 심각성을 확인하고자 함
- 특히 디지털 전환이 가속화되고, EU AI Act가 발효되면서, 미국 영국 등 AI 법안이 마련되어 규제가 강화되는 상황에서, AI를 악용한 사이버 보안 문제의 심각성을 인지하고, AI를 활용한 사이버 공격 예방·차단도 가능하다는 점을 확인함

사이버 보안의 영향력

- 사이버 보안은 계정 관리. 인증, 권한 통제 등 컴퓨터 시스템의 기본 기능에서 시작했고 기술자의 영역으로 간주되었음
- 기업은 인터넷으로 빗장을 열고 개방과 공유를 기치로 내걸었으며 온라인 거래와 비대면 서비스가 급격하게 늘어났고 비즈니스의 전반적인 업무가 디지털 기술에 기반하는 시대가 되면서 사이버 보안은 기술 문제를 넘어서 이제는 경영 리스크가 되고 있음
- 국제적 범죄 조직 혹은 국가에서 직간접적으로 지원하는 국가 안보 문제의 등장은 적대적 국가들 사이에서 빈번하게 나타나고 있음
- 최근에는 국가 간 공격이 더 대담해지고 규모가 커지면서 개인정보 탈취나 디도스 공격에 그치지 않고 더 나아가 랜섬웨어를 이용한 협박, 전력이나 송유관과 같은 기간 시설의 장애 유발, 사회관계망서비스(SNS)를 동원한 사회 혼란, 하이브리드 전쟁, 공급망 파괴, 국제 송금 위조, 암호화폐 탈취 등 민간과 공공, 국방과 금융의 영역을 가리지 않고 공격 범위가 확대되고 있음
- 이와 같은 사이버 공격으로 벌어들인 자산은 핵무기 개발이나 범죄 용도로 사용될 수 있다는 우려감도 커지고 있음

- 민주주의 국가에서도 사이버 보안 문제가 드러났는데 일부 악의적 AI 기술을 활용하여 딥 페이크, 허위 조작정보(가짜뉴스)의 확산 등 민주 질서를 뒤흔들고 국제 정세에 영향을 주는 여론 형성 등 중대한 과제로 등장하였음(벤 뷰캐넌 2023)

디지털 기술 발전에 따른 위협 강화

- AI 발전으로 사이버 보안은 냉전 이후 비전통적인 안보 차원에서 포괄적 안보 개념으로 확장하고 있음
- 향후 사이버 보안은 사이버공간과 현실 공간의 통합적인 개념이라는 점에서 안보 개념의 확대와 재정립을 가져올 것임
- 특히 기술 발전이 고도화됨에 따라 네트워크 연계성을 악용한 새로운 사이버 보안 이슈가 부각되고 있으며, 최근에는 테러 집단과 국가적인 차원에서 공격이 진행되고 있음

- 그러나 한국은 아직도 사이버 보안이 전문가 중심으로 논의되고 있어 전국민적인 대응 체계 또는 국가전략 차원의 접근이 부족한 것이 현실(벤 뷰캐넌 2023)
  - 언론에서도 지적하고 있지만 우리나라의 정치·정부·언론의 오피니언 리더들은 인식론적으로는 사이버 보안 문제의 심각성을 파악하고 있지만 현실 속에서 정책화, 실천 노력은 아직 부족한 것이 사실임
  - 아직 사이버 보안이 자신의 당면 문제라고 생각하진 않는 이유는 사이버 보안이 기술자의 영역이라는 생각에 머물러 있어 '보안이 중요하다'는 원론적인 구호만 제시하고 있음

- 그러나 이런 인식론적인 논의를 넘어 최근 한국에서는 구체적인 사이버 보안에 대한 대응을 논의하고 있다는 점은 긍정적인 변화라고 할 수 있음
  - 한국은 '국가사이버안전관리규정'을 보완 및 강화하여 각 기관에 보안관제센터를 구축하고 대책기구를 구성하는 등 사이버안보에 대한 강화 조치를 시행하고 있음(채재병·김일기 2020)
  - 한국은 2011년에 들어 사이버 위협 대응 체계를 정비하고, 부처별 역할을 정립하기 위해 '국가 사이버안보 마스터플랜'을 수립
  - 2013년에는 '국가 사이버안보 종합대책'을 수립하였고, 2019년에는 '국가사이버안보전략'을 공표

- 2024년 12월에는 AI 기본법 통과로 AI 활성화 기반 체제 마련(AI 안전연구소에 대한 지원 체제 마련됨)
- 그러나 이러한 몇몇 노력에도 불구하고 한국의 사이버 보안은 여전히 미흡한 상태로 국가 사이버 보안 체제에 대한 개선이 요구되는 상황임

- 그런 맥락에서 본 보고서에서 살펴본 사이버 보안을 강화하기 위한 기업 차원의 기술적인 대응과 주요국 정책 대응 동향에서 다양한 시사점을 얻을 수 있을 것임
  - 디지털 전환이 가속화되면서 사이버 공격이 증가하자, 주요국 정부는 사이버 보안 강화를 위해 내부 조직 및 관련 규정을 정비
  - 전통적인 안보 영역과 함께 AI 사이버 보안 문제에 대응하기 위한 정책적·제도적 대응 강화되어야 할 것임

- 보안 강화를 통한 지나친 규제의 위험성
  - 사이버 보안 영역에서 특히 AI의 악용 가능성은 증가하고 있지만 그렇다고 지나친 생성형 AI에 대한 우려감은 자칫 기술적인 규제로 비화될 수 있음
  - 그러나 AI 기반의 악성 코드 탐지 및 차단, AI 기반의 침입 탐지 및 대응 등 AI의 사이버 보안 활용도 가능하다는 점을 생각하면 반드시 AI가 부정적인 현상을 양산하지 않을 것으로 예상됨

- 이상 주요국들의 사이버 보안 전략을 검토해 본 결과, 한국의 사이버 보안 강화전략에 대한 심층적이고 체계적인 고민이 요구되는 시점임
  - 첫째, 사이버 보안 문제가 과거와 다른 새로운 경제적·국가 안보적 이슈임을 인지해야 할 것임
  - 둘째, 사이버 보안은 비즈니스 차원에서만이 아니라 국가 안보 차원에서 민관 협력을 통한 사이버 공격 총괄 대응 체계를 구축해야 할 것임
  - 셋째, 앞서 살펴본 바와 같이 AI가 새로운 방식의 사이버 공격 도구가 되기도 하지만 역으로 예방하고 감시하는 기술로도 발전할 가능성이 있으므로, 기업 차원에서 그리고 국가 차원에서 이를 적극 개발할 필요가 있음
  - 넷째, 사이버 공격에 대응하는 국제 사이버 협력 네트워크에 참여하여 국제간 협력을 통한 사이버 보안 능력 제고에 적극 대응해야 할 것임

참고 자료

1) 김미희. 2017. "쩐의 전쟁, 사례로 살펴보는 사이버 공격의 트렌드." 아이티데일리 2017.12.1

2) 김영명. 2024. "2023년 사이버 위협 결산 키워드 : 디도스, 서버해킹, 랜섬웨어, IP 카메라, 라자루스." 보안뉴스 2024.1.22

3) 김재연. 2024. "삼성·LG, AI 보안에 사활…개인정보 지켜라." 한국경제 2024.10.5일

4) 김홍선. 2023.『보이지 않는 위협』. 서울: 한빛미디어.

5) 김희정. 2024. "생성형 인공지능 기술을 활용한 신종 사이버 범죄 예방과 사이버 보안 법정책적 대응 전략."『법학논문집』제48집 제2호, pp.49-84.

6) 문인철, 2018. "미국의 사이버안보정책과 전략: 한국의 대북사이버안보 정책에 대한 함의." 2018 국제정치학회 하계학술회의 발표논문, p.9.

7) 박상돈. 2017. "미국 2015 사이버 보안법(Cybersecurity Act of 2015)의 의의와 시사점,"『미국헌법연구』, 제28권 제1호, pp.45-49.

8) 박의례. 2023. "해킹 피해 급증한 호주, 5천억원 투자해 사이버 범죄 대응." 연합뉴스 2023.11.22.

9) 벤 뷰캐넌 지음. 강기석 옮김. 2023.『해커와 국가: 사이버 공격과 지정학의 뉴 노멀』.

10) 안영국. 2024. "국가사이버안보 기본계획 발표..양자암호 개발·망분리 개선·사이버보안 R&D 확대." 전자신문 2024.9.1.

11) 안춘모. 2023. "일본의 사이버 보안 정책 추이와 시사점 연구," 2023년도 한국통신학회 하계종합학술발표회.

12) 이상덕. 2024. "다크웹의 위협과 AI 보안: 거세지는 사이버 공격, 어떻게 대비할 것인가." https://www.lgcns.com/blog/it-trend/59127/ .

13) 임산호. 2023. "사이버안보 위험 확대와 주요국 대응 동향." 경제안보 Review Vol 21.

14) 임종인. 2008. "사이버보안 정책 및 법제도 현황." TTA Journal NO. 118.

15) 임재완. 2024. "더 강력한 방패 : 사이버보안과 생성형 AI의 만남." SAMSUNG SDS 블로그
https://www.samsungsds.com/kr/insights/cyber_security_gen_ai_240702.html

16) 전미준. 2022. “인공지능이 사이버보안을 강화할 수 있는 3가지 방법은?” 인공지능신문. 2022.2.7.

17) 채재병·김일기. 2020. “주요국 사이버안보 전략과 한국에의 시사점.” 국가안보전략연구원. INSS 전략보고 No. 73.

18) 한지연. 2024. “AI로 사이버보안 우려 없앤다...미국 홀린 삼성전자 기술은.” 머니투데이 2024.8.20.

19) 현대인. 2024. “영국, AI안보연구소 신설…러시아·북한 AI 사이버 위협 대응.” 2024.11.26.

20) Amazon. 2024. “사이버보안이란 무엇인가요?” https://aws.amazon.com/ko/what-is/cybersecurity/

21) Cloudflare. 2024. “멀웨어(Malware)란” https://www.cloudflare.com/ko-kr/learning/ddos/glossary/malware/

22) IBM. 2024. “알고리즘 안전을 통한 개인과 기업 보호.” https://www.ibm.com/kr-ko/case-studies/united-family-healthcare

23) IBM. 2024. “보안 및 ID”. https://www.ibm.com/kr-ko/topics/malware

24) MicroSoft. 2024. https://www.microsoft.com/ko-kr/security/business/security-101/what-is-ai-for-cybersecurity

25) Fortinet. 2024. https://www.fortinet.com/kr/resources/cyberglossary/recent-cyber-attacks

26) Sai, S., Yashvardhan, U., Chamola, V., & Sikdar, B. 2024. *Generative ai for cyber security: Analyzing the potential of chatgpt, dall-e and other models for enhancing the security space.* IEEE Access.

27) TTA 정보통신용어사전. 2024. http://word.tta.or.kr/dictionary/dictionaryView.do?subject=%EC%82%AC%EC%9D%B4%EB%B2%84+%EB%B3%B4%EC%95%88

28) World Economic Forum. 2022. *World Economic Forum Global Cybersecurity Outlook 2022*. World Economic Forum.

29) AI 기본법, 과학기술정보통신부 자료, 2024.12.27.

30) EU AI Act, https://artificialintelligenceact.eu/

주 의

- 본 보고서는 산업통상자원부 국가기술표준원의 무역기술장벽(Technical Barriers to Trade; TBT) 대응 활동의 일환으로 최신 규제 정보를 제공하기 위해 작성되었습니다.
- 본 보고서는 TBT종합지원센터의 동의 없이 무단 배포 및 변경할 수 없으며, 상업·법률적 판단 근거로 활용될 수 없습니다.
- TBT종합지원센터에서 운영 중인 KnowTBT 포털을 통해 더 많은 해외 기술규제 정보를 제공받을 수 있습니다 (www.knowtbt.kr).

Tel. : 02-3487-7758 Fax : 02-571-0003 E-mail : tbt@kotica.or.kr