

Emerging Technologies and Emerging Security Issues:
Global Collaboration for Responsible Development and
Deployment of Emerging Technologies

신기술의 안보적 함의 분석 및 책임있는 신기술의 개발·사용을 위한 국제협력 방안 연구

KAIST

신기술의 안보적 함의 분석 및 책임있는 신기술의 개발·사용을 위한 국제협력 방안 연구

Emerging Technologies and Emerging Security Issues:
Global Collaboration for Responsible Development and
Deployment of Emerging Technologies

주관연구기관 | 한국과학기술원(KAIST)

KAIST



외교부

신기술의 안보적 함의 분석 및 책임있는 신기술의 개발·사용을 위한 국제협력 방안 연구

Emerging Technologies and Emerging Security Issues:
Global Collaboration for Responsible Development and
Deployment of Emerging Technologies

주관연구기관 | 한국과학기술원(KAIST)

제출문

외교부 장관 귀하

본 보고서를 ‘신기술의 안보적 함의 분석 및 책임있는 신기술의 개발·
사용을 위한 국제협력 방안 연구’ 과제의 최종 보고서로 제출합니다.

2023.12.

- 주관연구기관

| 한국과학기술원(KAIST)
- 연구책임자

| 김소영(과학기술정책대학원 교수)
- 공동연구원

| 서용석(문술미래전략대학원 부교수)
박경렬(과학기술정책대학원 조교수)
- 참여연구원

| 코넬리우스 칼렌지(국가미래전략기술정책연구소 연수연구원)
백단비(국가미래전략기술정책연구소 연구원)
양문열(과학기술정책대학원 석사과정)

Content

요약	008
----	-----

1. 연구 필요성 및 목적

1-1. 연구 필요성	010
1-2. 연구 목적 및 내용	011

2. 신기술과 안보

2-1. 신기술의 정의	012
2-2. 신기술의 안보적 함의	013
2-3. 신기술 분야별 안보 이슈	015
2-3-1. 인공지능	016
2-3-2. 양자과학기술	019
2-3-3. 첨단바이오기술	021
2-3-4. 나노기술	023

3. 정책 및 인식

3-1. 신기술 안보 관련 정책 현황	025
3-1-1. 미국	025
3-1-2. 유럽연합(EU)	027
3-1-3. 중국	028
3-2. 신기술 안보 관련 국민 인식	029
3-2-1. 신기술 일반 인식	029
3-2-2. AI 기술 인식	030
3-2-3. 한국의 신기술 안보 국민 인식	033

4. 전문가 네트워크 구축

4-1. 전문가 인터뷰	035
4-2. 기술별 전문가 풀	036

5. 신기술 안보 관련 포럼

5-1. 국내 신기술 안보 라운드테이블	044
5-2. 세계신안보포럼 라운드테이블	046

부록 1 : 국내 전문가 주요 자문 내용	048
부록 2 : 국내 전문가 라운드테이블 상세 내용	054
부록 3 : 신기술 안보 관련 주요 국내외 보고서 목록	062
참고문헌	068
별책	072

표 차례

표 1 : 신기술의 학술적 정의	012
표 2 : 신기술 안보 관련 주요 회의	014
표 3 : 주요 신기술 정의와 파급 효과	015
표 4 : 알고리즘 전쟁 분야와 예시	018
표 5 : 미국 20대 핵심 신흥기술	025
표 6 : 중국의 디지털·사이버 법제도 정비 상황	028
표 7 : 중국 산업정책 내 주요 어휘의 출현	029
표 8 : 국내 전문가 인터뷰	035
표 9 : 국내 신기술 안보 라운드테이블 프로그램	044

그림 차례

그림 1 : 주요 연구 내용	011
그림 2 : 신기술 속성의 변화	012
그림 3 : 신기술로 인한 최근 안보의 변화	014
그림 4 : 사이버 안보의 주요 영향 분야	015
그림 5 : AI 기술 가트너 하이프 사이클, 2021~23	017
그림 6 : GPT 모델의 진화	017
그림 7 : 구글딥마인드의 일반인공지능(AGI) 레벨 분류	018
그림 8 : 자율살상무기 사례	006
그림 9 : 각국의 양자과학기술정책 현황	020
그림 10 : 위성 양자암호통신	020
그림 11 : 양자과학기술의 안보 활용 사례	021
그림 12 : 양자과학기술의 전쟁 적용 시 예상도	021
그림 13 : 미래유망기술(6T)별 국가연구개발사업 집행 추이	022
그림 14 : 1~4차 나노기술종합발전계획 경과 및 성과	023
그림 15 : EU의 디지털 미래 구축을 위한 사이버보안 정책과입법 추진현황	027
그림 16 : 신기술 대중 인식의 중요성	029
그림 17 : 14개 기술 인식 조사 결과	030
그림 18 : 국가별 기술 긍정인식 조사 결과	030
그림 19 : 일상생활의 AI 활용 인식의 주요 이유	031
그림 20 : AI 활용 인식 변화	031
그림 21 : AI 기술 가능성과 가치 평가	032
그림 22: 미국인 및 중국인의 AI R&D 수준 인식	033
그림 23 : 응답 집단별 미국의 AI 군사역량 확보 인식	033
그림 24 : AI 기술로 인한 변화 인식	034
그림 25 : 국내 신기술 안보 라운드테이블 모습	044
그림 26 : 세계신안보포럼 라운드테이블 모습	047
그림 27 : 생성형 AI의 한계와 안보 리스크	056
그림 28 : 생성형 AI 시대의 안보 위협 전망 1	057
그림 29 : 생성형 AI 시대의 안보 위협 전망 2	057

Abstract

전 세계적으로 인공지능(AI), 반도체, 양자, 첨단 바이오 등 파괴적인 신기술의 안보적 파급효과가 점차 다양하게 전개되면서 이들 신기술의 잠재적 위험성에 대한 정교한 분석이 필요함. 본 과제는 AI의 군사적 활용 등 신기술의 안보적 활용 양상과 국내외 외교안보 정세 변화에 따른 함의 분석을 통해 글로벌 중추국가로서 신기술의 책임있는 개발 및 활용에 있어 한국의 국제적 리더십 제고를 위해 기초자료를 수집하고 전문가 네트워크를 구축하는 것을 목표로 함. 주요 과업은 (1) 제3차 세계신안보포럼(World Emerging Security Forum) 내 신기술 관련 세션 기획·운영, 사전 국내 전문가 라운드테이블 기획·운영, (2) 주요 신기술별 안보 이슈 분석과 관련 정책 현황 및 신기술 안보 관련 시민인식 분석, (3) 신기술과 안보 접면의 전문가 발굴 및 전문가 인터뷰를 정책 인사이트 도출임.

세계신안보포럼('23.12.5) 신기술 세션은 “Navigating New & Emerging Security Paradigms in AI-Driven World”라는 제목으로 8명의 전문가 패널로 진행됨. 주요 논의와 제언으로는, AI와 같은 신기술에 대한 과도한 규제를 지양하되 실제적 안보 위험을 구체적·과학적으로 분석할 수 있는 역량 제고, 신기술의 점증하는 복잡성과 융합성으로 인한 다주체 거버넌스(multistakeholder governance)의 중요성 증가, 기술과 정책·거버넌스의 동시 설계(Co-design) 관점에서 최고 수준의 과학기술 전문가들이 신기술 안보 정책·전략 개발에 참여할 수 있는 체계 및 과정의 필요성이 거론됨.

아울러 신기술과 안보 접면의 전문가는 인공지능, 사이버안보, 양자과학기술, 첨단바이오, 나노기술을 중심으로 국내외 총 110여 명을 발굴하고, 이 중 20여 명을 세계신안보포럼 신기술 세션 및 사전 국내 라운드테이블에 초청해 발표와 토론을 진행함. 특히 국내 라운드테이블과 신기술 안보 관련 국내 전문가 인터뷰에서는 신기술의 급속한 발전과 군사적 활용에 따라 신기술 안보에 관한 다부처 협력이 시급하며 미중 패권경쟁에서 중견국으로서 차별화된 전략과 기술 역량별, 지정학적 상황을 고려한 종합적 전략이 필요함이 지적됨.

As the security ramifications of destructive new technologies such as artificial intelligence (AI), semiconductors, quantum, and advanced biotechnology are rapidly unfolding around the world, a sophisticated analysis of the potential risks of these new technologies is needed. This project puts together various data and analyses to enhance Korea's international leadership in the responsible development and use of new technologies as a global pivotal country by analyzing the security use of new technologies, such as the military use of AI, as well as the implications of changes in domestic and international diplomatic and security situations. It also and aims to build a network of experts in the interface of emerging technologies and security issues.

The technology session of the World New Security Forum on 5th of December 2023 was held with a panel of eight experts under the title “Navigating New & Emerging Security Paradigms in AI-Driven World.” Key discussions and recommendations include: avoiding excessive regulation of new technologies such as AI, but improving the ability to analyze actual security risks in a concrete and scientific manner, and establishing multistakeholder governance due to the increasing complexity and convergence of new technologies. With the ever-greater entanglement of technology and policy/governance, the following recommendations were made: (i) Make a sober assessment of emerging technologies, while avoiding alarmism, (ii) Raise capacity for agile governance with multi-stakeholder collaboration, and (iii) Involve scientists seriously in the decision making involving technologically complex issues.

In addition, about 110 international and domestic experts in the interface of emerging technologies and security were identified, focusing on artificial intelligence, cyber security, quantum science technology, advanced biotechnology, and nanotechnology, with 20 of them engaged in in new technology session at the World New Security Forum and the domestic expert roundtable. In particular, the domestic expert roundtable and interviews with domestic experts on security implications of emerging technologies emphasized multi- or cross-ministerial cooperation on new technology security in view of the rapid development and military use of new technologies and noted the need for the South Korean government to develop a comprehensive strategy as a middle power in light of US-China rivalry in the technological and military domains, differentiated by technological capabilities and geopolitical contexts.

1. 연구 필요성 및 목적

1-1. 연구 필요성

- 전 세계적으로 인공지능(AI), 반도체, 양자, 첨단 바이오 등 파괴적인 신기술의 안보적 파급효과가 점차 다양하게 전개되면서, 이들 신기술의 잠재적 위험성에 대한 정교한 분석이 필요함.

- WEF(2023)은 향후 10년 동안 신흥 기술(emerging technologies)에 대한 국가 R&D 투자와 강력한 산업 정책 시행, 민간 투자가 지속되며 AI, 양자컴퓨팅, 생명공학 기술이 크게 발전할 것으로 전망함.
- AI는 방대한 데이터를 신속하게 처리해 국가 차원의 정보 수집 및 분석 능력 향상에 영향을 미치고 있으며, 미래전의 주요 쟁점인 자율무기체계(AWS)의 기반 기술로 군사 안보에 직접적으로 영향을 주고 있음.
- 양자 과학기술의 발전은 기존의 암호체계를 무력화해 국가 주요 기밀 유출 위험을 높이는 반면, 국방 분야 감시 및 정찰 능력을 획기적으로 향상시킬 수 있음.
- 바이오 안보는 전세계를 세기적 위기로 몰아넣은 코로나19 이후 크게 부각되면서, 전염병을 비롯한 다양한 생물학적 위협에 대한 국가 차원의 대비 필요성이 대두되고 있음.

- 신기술의 군사 분야 적용과 위험성은 우크라이나-러시아 전쟁, 이스라엘-하마스 전쟁을 통해 생생히 드러나고 있으며, 이들 전쟁에 대한 글로벌 빅테크의 개입으로 국제 안보의 이해관계자 범위가 확장되고 미래 안보 지형에도 큰 변화를 일으키고 있음.

- 우-러 전쟁은 무인항공기(UAV, 드론)의 활용부터 AI와 데이터를 활용한 첨단 AI 기술의 실험장이 되면서 미래전의 양상과 안보 변화 추세를 가늠할 수 있는 테스트베드가 되고 있음.
- 이스라엘 또한 공습 대상 선택 시 AI를 활용한 방대한 양의 데이터 분석을 비롯해 첨단 기술을 활용하며 미래전 양상의 변화를 실시간으로 보여주고 있음.
- 한편, 사회관계망서비스(SNS)를 활용한 여론 주도, 스타링크의 저궤도위성(LEO)을 이용한 우주 와이파이 네트워크 활용 등 글로벌 빅테크의 직접적 전쟁 개입이 전세 전환에 상당한 영향을 미치고 있음.

- 군사 안보뿐만 아니라 사이버 위협 또한 국가 차원의 안보 문제로 부상하면서, 주요국은 자국의 국가 전략 수립뿐만 아니라 동맹국 체제의 공동 대응 체제를 마련하고 글로벌 규범을 모색하는 추세임.

- 미국, EU, 영국, 프랑스, 일본 등 주요국은 2022년을 전후로 하여 사이버 보안과 국가 안보에 대한 국가 전략을 수립함.

1-2. 연구 목적 및 내용

그림 1 : 주요 연구 내용

- 제1차 차세대 핵심·신흥기술 대화 개최(‘23.4.)를 통한 한미 핵심신흥기술 동맹의 확장으로 첨단기술의 우위 확보가 경제·안보 차원에서 핵심 현안으로 부상함.
- 우리 정부는 글로벌 중추국가 비전을 바탕으로 세계신안보포럼(WESF), 인공지능의 책임있는 군사적 이용에 관한 고위급회의(REAIM) 등 글로벌 아젠다 형성에 주도적으로 참여하며 가치 기반 신기술 글로벌 규범 모색에 적극 참여 중임(유준구, 2023).

- 이러한 흐름에 따라 전통적 안보와 구조적으로 다른 신안보 양상에 대한 분석을 비롯해 신기술의 안보적 파급효과를 진단하는 연구가 필요함.

- 최근 급부상하는 신기술과 관련 안보적 함의에 대한 통찰을 제공할 수 있는 국내외 전문가들을 파악하고, 관련 이슈에 관한 이해관계자들의 인식을 파악하는 연구가 필요함.

- 본 연구의 주요 목적은 AI의 군사적 활용 등 신기술의 안보적 활용 양상과 국내외 외교안보 정세 변화에 따른 함의 분석을 통해 글로벌 중추국가로서 신기술의 책임있는 개발 및 활용에 있어 한국의 국제적 리더십 제고를 위해 기초자료를 수집하고 전문가 네트워크를 구축하는 것임.

- 주요 연구 내용은 신기술의 안보적 활용에 관한 주요 행사 기획과 전문가 네트워크 구축, 주요국 대응 및 인식 분석으로 구성됨.

- (행사 기획 및 운영) 제3차 세계신안보포럼의 주제(Advancing Global Cooperation in Response to Security Threats in Cyberspace and New Technologies)를 반영한 글로벌 전문가 라운드테이블 기획 및 운영(‘23.12.), 국내 전문가 라운드테이블 기획 및 운영(‘23. 9.)
- (전문가 네트워크 구축) 주요 신기술별 전문가 조사, 전문가 인터뷰(서면 및 대면, 개인 및 그룹) 진행, 신기술과 안보 접면에 관한 전문가 분석 및 정책 인사이트 도출, 국내외 전문가 네트워크 구성 및 활용
- (정책 및 인식 분석) 주요 신기술 안보 이슈와 관련된 주요국 정책 및 거버넌스 현황에 관한 분석 및 주요국 일반 인식 분석

I. 신기술 안보 주요 행사 기획

- 제3회 세계신안보포럼 기획 및 공동운영
- 국내 전문가 라운드테이블 기획 및 공동운영

II. 신기술안보전문가네트워크구축

- 신기술 분야별 국내외 전문가 조사
- 신기술과 안보 연계 분석 전문가 네트워크 마련

III. 신기술 안보 정책 및 인식 분석

- 신기술 안보 관련 주요국 대응 분석
- 신기술에 관한 주요국 일반 시민 인식 분석

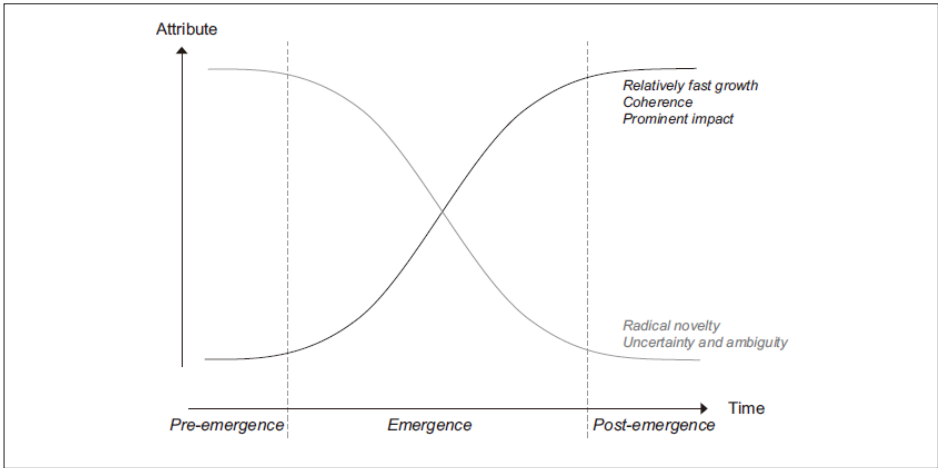
2. 신기술과 안보

2-1. 신기술의 정의

● **신흥기술 혹은 신기술(emerging technologies)은 학술적으로 다양한 정의가 있으나 대체로 신규성(novelty), 급진성(disruption), 불확실성 등이 주요 특징임.**

- 신기술은 신산업을 창출하거나 경쟁의 기반 자체를 바꾸는 혁신적 기술이지만 동시에 그 가능성이 여전히 잠재적이고 불확실하다는 이중적 성격을 지님.
- 신기술에 대한 대표적인 메타 연구(Rotolo, et al., 2015)에 따르면, 신기술의 대표적 5대 속성 중 신규성과 불확실성은 시간의 경과에 따라 줄어들지만 성장세와 일관성, 파급효과는 늘어남.

그림 2 : 신기술 속성의 변화
(출처 : Rotolo, et al., 2015)



2-2. 신기술의 안보적 함의

● **최근 신기술은 민간영역 산업 창출을 넘어 안보 영역에서 큰 파장을 낳으며, 신기술 등장에 따른 신안보 위협의 확산은 국가 안보전략의 중요 현안으로 등장함.**

- 특히 전략기술(critical technologies)의 주도권 확보는 경제·산업적 필요성을 넘어 국가안보에 사활적인 이슈로 부상하고 있음(윤정현, 2023).
- 신기술의 등장에 수반되는 신안보 위협의 확산은 국가전략의 중요 현안으로서, 주요 선진국에서는 신기술의 개발·획득을 위한 국가전략 수립 시 포괄적인 국가 안보전략 차원에서 수립하고 있음.
- 급변하는 국제정세 속에서 중견국으로서 한국의 신기술 안보전략 수립이 그 어느 때보다 중요해지고 있으나 신기술에 관한 포괄적 안보전략이 부재한 상황에서 국제협력이 분절적으로 추진되고 있음(김상배 외, 2023). 전통적 안보를 넘어 포괄적 안보에 신기술이 미칠 파장을 예측하고 글로벌 흐름에 대응하며 국가 이익을 확보하기 위한 노력이 시급함.

● **최근 당면한 신기술의 안보적 함의와 현안은 다음 세 가지로 정리할 수 있음. 첫째, 외교와 동맹 변수 부상으로 개별 국가 차원이 아닌 특정 쟁점에 대한 우방국 중심 연대 경향 속에서 신기술·사이버 안보 분야 협력은 가치 기반 동맹의 새로운 축으로 등장함. (참고로 신기술 안보 관련 주요 국내외 보고서는 부록 3 참조)**

Boon W and Moors E (2008) Exploring emerging technologies using metaphors: a study of orphan drugs and pharmacogenomics. Social Science & Medicine 66(9): 1915-1927

“유망기술(emerging technologies)은 아직 개발 초기단계에 있는 기술이다. 기술의 특징과 기술 행위자 네트워크의 형태 및 이들의 관련 역할 등 여러 측면에서 아직 불확실하고 구체적이지 않다.” (1915쪽)

Srinivasan (2008) Sources, characteristics and effects of emerging technologies: Research opportunities in innovation. Industrial Marketing Management 37(6): 633-640

“유망기술(emerging technologies)의 개념은 기술의 원천(source), 특성(characteristics) 및 영향력(effects)으로 3가지 부문으로 정리해 볼 수 있다. 먼저 기술의 원천은 릴레이 경주와 같은 진화이거나 응용을 통한 혁명과 같다. 유망기술의 특성은 클록 속도(clockspeed nature), 융합, 지배적인 디자인, 네트워크 효과, 4가지로 살펴볼 수 있으며, 유망기술의 영향력은 가치사슬의 변화, 제품의 디지털화, 혁신 발생지의 변화로 나타날 수 있다.”(633-634쪽)

Cozzens S, Gatchair S, Kang J, Kim KS, Lee HJ, Ordonez G, and Porter A (2010) Emerging technologies: quantitative identification and measurement. Technology Analysis & Strategic Management 22(3): 361-376

유망기술(emerging technology)은 높은 잠재력은 가지고 있으나 아직 기술의 가치는 입증되거나 어떠한 형태의 합의도 이루어지지 않은 기술이다.”(364쪽)
“유망기술은 (1) 최근에 빠른 성장을 하고 (2) 변천(transition) 혹은 변화(change)가 진행 중이며 (3) 시장·경제적 잠재성이 아직까지는 완전하게 이용되지 않았고, (4) 마지막으로 점점 더 과학을 기반으로 한다.”(365-366쪽)

표1 : 신기술의 학술적 정의

출처	정의
Day George S and Paul JH Schoemaker (2000) Avoiding the pitfalls of emerging technologies. California Management Review 42(2): 8-33	“유망기술(emerging technologies)은 신산업 창출하거나 기존산업을 변화시킬 잠재력을 가진 과학 기반의 혁신을 말한다. 이전에는 관련 없던 서로 다른 독립 연구 분야가 만나 기술의 진화를 이끌어 내는 점진적 혁신뿐만 아니라 기존에는 존재하지 않았던 급진적 혁신(radical innovation)을 포함하기도 한다.” (30쪽)
Porter AL, Roessner JD, Jin, X-Y, Newman NC (2002) Measuring national emerging technology capabilities. Science and Public Policy 29(3): 189-200	“유망기술(emerging technologies)은 향후 (대략) 15년 후 경제적 발전을 가져올 수 있는 기술로 정의된다.” (189쪽)
Hung SC, and Chu YY (2006) Stimulating new industries from emerging technologies: challenges for the public sector. Technovation 26(1): 104-110	“유망기술(emerging technologies)은 곧 경쟁의 기반(basis)을 바꿀 수 있는 핵심 기술이다.” (104쪽)

그림 3 : 신기술로 인한 최근 안보의 변화
(출처 : 김상배, 2021)

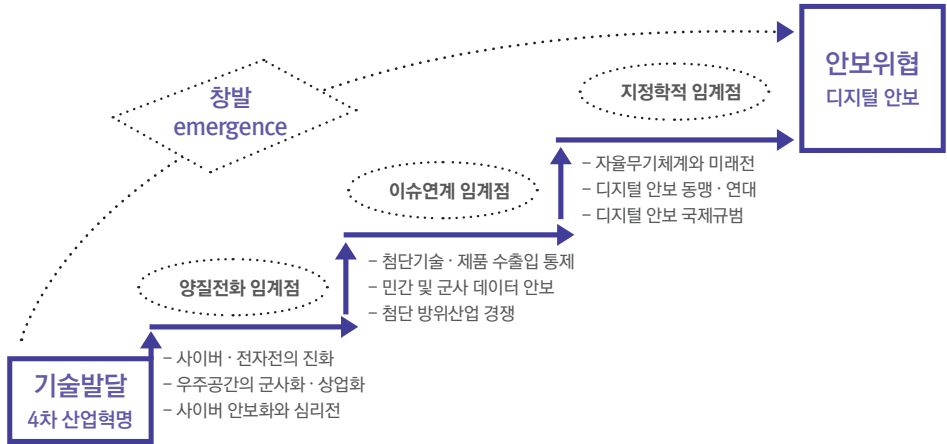


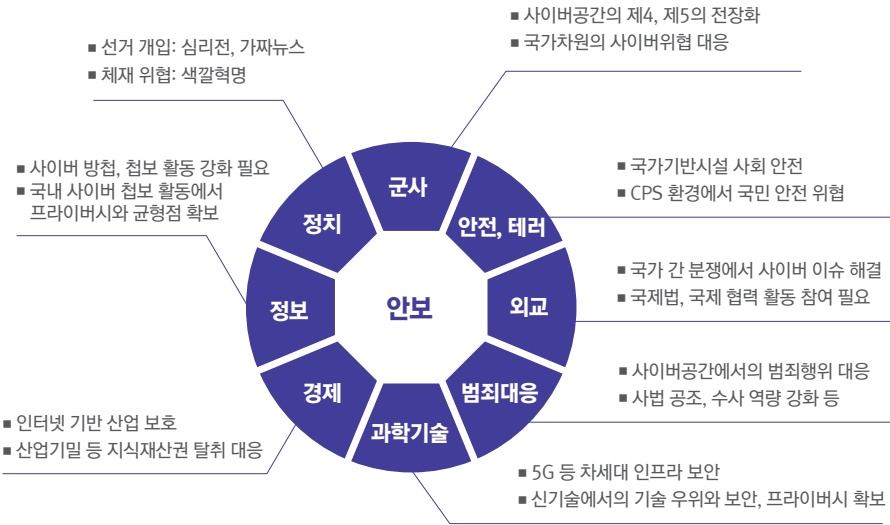
표 2 : 신기술 안보 관련 주요 회의

신기술 안보 관련 주요 회의	내용
제1차 차세대 핵심·신흥기술 대화(‘23.12.)	한미동맹을 군사와 경제에 이어 기술까지 포괄하는 전략 동맹으로 확대하고 핵심 신흥기술 정책을 안보 정책의 중요한 축으로 선언
북한 사이버 위협 대응 한미일 외교당국간 실무그룹(‘23.12.)	한미일 정상회담의 후속조치의 일환으로 도쿄에서 개최
군사적 영역의 책임 있는 인공지능에 관한 장관급 회의(REAIM, ‘23.02.)	60개국 정부 고위 인사 및 이해관계자가 모여 ‘REAIM 공동 행동 촉구서(call to action)’를 발표, 2024년 회의는 한국 개최 예정, 내년 AI 안정성 미니 정상회의(AI Safety mini virtual summit, ‘24.05) 역시 한국 개최

● **둘째, 국가안보의 모든 영역에서 사이버 안보가 중요해지면서 최근 한국을 포함한 주요 국에서는 사이버 보안을 국가전략 수준으로 격상시키며 사이버 안보 전략을 강화 중임**

- 미국 백악관은 국가사이버안보전략(National Cybersecurity Strategy, ‘23.03.)과 시행안(National Cybersecurity Strategy Implementation Plan, ‘23.07.), CISA의 사이버보안 전략계획(Cybersecurity Strategic Plan FY 2024–2026, ‘23.08.)을 연이어 발표하며 국가 주요 기반시설의 보호 체계 강화와 국제협력을 통한 대응 활동 강화에 대한 구체적인 시행 계획을 발표함.
※ CISA(Cybersecurity and Infrastructure Security Agency): 미 국토안보부 산하 사이버보안 및 인프라 보안국
- EU는 사이버 방어 정책(EU Policy on Cyber Defence, ‘22.11.), 독일은 사이버보안전략 2021(Cybersicherheitsstrategie fur Deutschland 2021, ‘21. 09.)을 수립, 호주 2023–2030 호주 사이버 안보 전략(2023–2030 Australian Cyber Security Strategy, ‘23.11.)을 발표함.
- 한국은 ‘19년 「국가 사이버안보 전략」을 수립했고, ‘23년 「윤석열 정부의 국가안보 전략」을 수립하며 그중에서도 국가 사이버안보 역량 강화를 신안보 이슈에 대한 능동 대응의 주요 현안으로 다룸(국가안보실, 2023). 또한 사이버 안보법 제정을 추진 중에 있으며 국가 사이버 위기 통합대응조직인 국가사이버위기관리단을 공식 출범시킴(‘23.05.).

그림 4 : 사이버 안보의 주요 영향 분야
(출처: 임종인, 2023)



● **셋째, 신기술의 급속한 발전과 적용에 따라 신안보 영역이 확장되면서 이들 기술의 군사적 적용이 빠르게 확대되고 있음.**

- 최근 생성형 AI의 빠른 발전은 사이버 안보에 파괴적 영향을 미칠 것으로 예측되며, 랜섬웨어, 디지털자산과 자금세탁, 주요 기반시설·생산시설 대상 위협, 공급망 보안과 경제 안보, 정보유출까지 신안보 영역이 확장되는 추세임.
- 특히 AI 기술의 군사적 적용이 가속화되면서 정부에서는 AI 기반 유·무인 복합전투체계로의 단계적 추진 계획을 발표했으며 북한의 무인기 위협에 대응하는 드론작전사령부 조기 창설 계획을 발표함(국가안보실, 2023).
- 그 외에 AI와 빅데이터의 적용이 범분야로 확산되며 나타나는 안보적 이슈 뿐만 아니라 양자 과학기술, 첨단바이오, 나노 등 미래기술로 불리었던 핵심 기술들의 발전 속도가 가속화되며 새로운 안보 위협을 제기하고 있음.

● **신기술의 범위와 종류, 유형은 매우 다양하나 본 연구에서는 인공지능, 양자과학기술, 첨단바이오기술, 나노기술을 중심으로 기술적 특성과 현황, 안보 관련 이슈를 살펴봄.**

기술 분류	기술 정의	안보 관련 주요 세부 기술	파급 효과
인공지능 (Artificial Intelligence)	인공지능은 인지, 사고, 학습 등 인간의 지적능력을 컴퓨터를 통해 구현하는 시스템(IBM, 2024., 한국전자통신연구원, 2019)	일반인공지능(AGI) 빅데이터 생성형 AI(멀티모달, 온디바이스 등) *AI의 군사적 이용 가능 분야: C4ISR(지휘, 통제, 통신, 컴퓨터, 정보, 감시 및 정찰)	좁은 인공지능(ANI)에서 인간지향적 인공일반지능(AGI)과 특이점을 넘어서는 슈퍼 인공지능(ASI)을 향해 빠르게 발전함에 따라 자율무기체계의 급속한 발전과 위험성 또한 증대, 제도 통제의 속도 보다 더 빠르게 진화되며 사이버 안보에 영향(박영숙 외, 2023., 민욱기 외, 2020)

2-3. 신기술 분야별 안보 이슈

표 3 : 주요 신기술 정의와 파급 효과

양자과학기술 (Quantum Science & Technology))	양자과학기술은 양자물 리학적 특성을 컴퓨팅, 통신, 센서 등 정보기술 에 적용하여 “초고속 연 산”, “초신뢰 통신”, “초 정밀 계측”을 가능하게 하는 기술(과기정통부, 2023)	양자 암호 양자 컴퓨팅 양자 센서 양자 통신	기존의 암호체계를 무력화할 수 있는 강 력한 기술로 시, 슈퍼컴퓨팅 등으로 첨단 화된 국가방어체계의 교란에 가장 큰 영 향력을 미칠 수 있는 기술(WEF, 2023)
바이오기술(Bio technology)	생물체의 기능과 정보를 이용해 각종 유용한 물 질을 생산하는 기술이며 바이오안보는 병원균, 바이러스, 곰팡이 등 미 생물의 유입을 차단 및 봉쇄하는 모든 조치를 뜻함(김재호, 2023)	유전자·세포치료 디지털헬스 데이터 분 석·활용(고성능컴퓨팅 (HPC) 활용) 합성생물학 생물학 무기 (OECD, 2023., 박상민, 2023)	첨단바이오는 AI·빅데이터 등 디지털 기 술과의 융합으로 기존 의료 분야의 난제 해결 및 생산 효율 확대로 폭발적 잠재력 을 보유(박상민, 2023) 바이오안보는 데이터베이스화와 연계되 며 사이버 안보 차원으로 확대 전망(김 재호, 2023)
나노기술(Nanotechnology)	나노미터 크기의 범주 에서 조작·분석·제어 함으로써 새롭거나 개선 된 물리적·화학적·생 물학적 특성을 나타내는 소재·소자 또는 시스템 을 만들어내는 과학기술 (나노기술개발 촉진법, 2018).	나노 센서 나노 소재 나노 로봇	나노 기술은 무기 및 전투복의 경량화, 의료지원 분야의 연계로 첨단 국방과학 기술(무기체계 분야, 군수분야, 광학분 야)의 향상을 가속화 가능(김용, 2009)

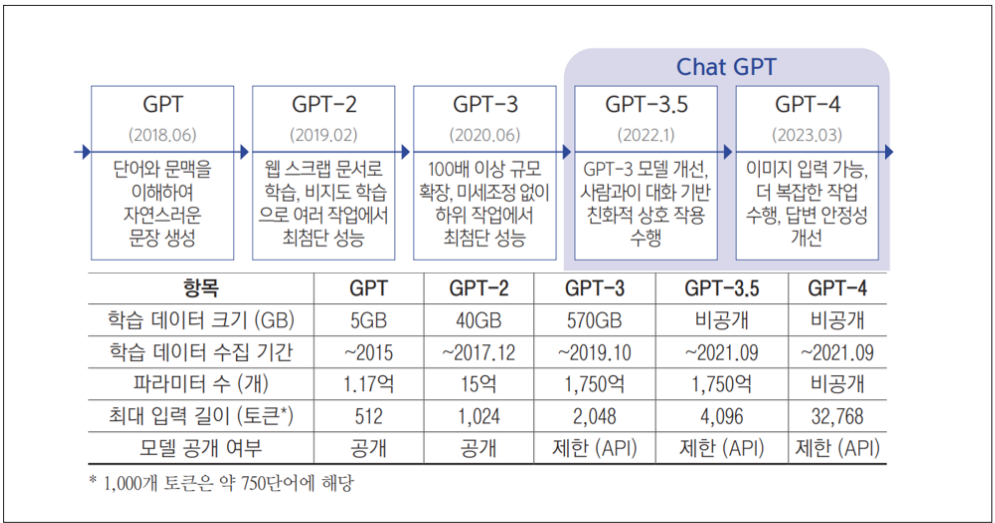
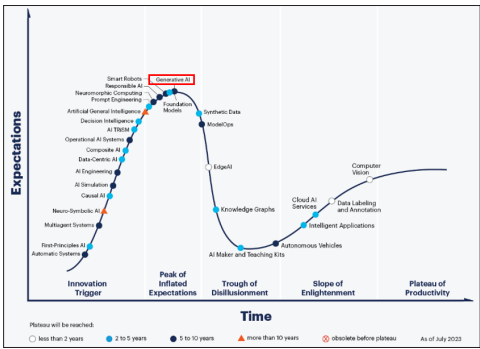
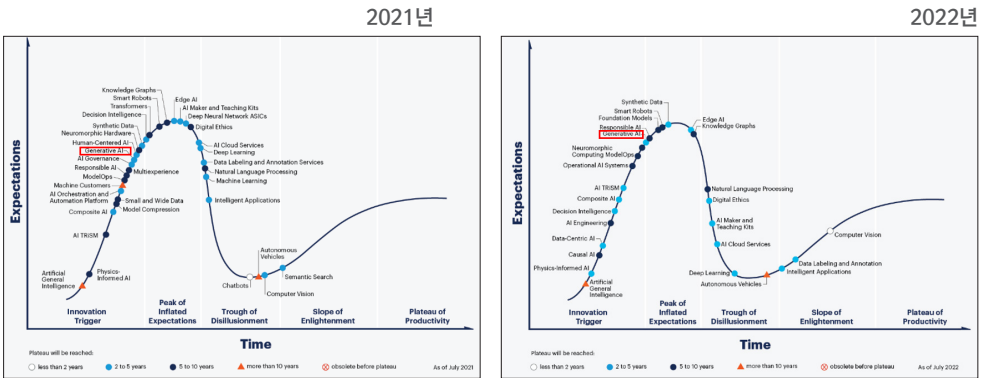
2-3-1. 인공지능

● 2016년 알파고 충격과 함께 산업, 서비스, 문화, 교육, 교통, 보건 등 다양한 분야에 접
목되기 시작한 AI 기술은 2022년 말 챗GPT로 대표되는 생성형 AI의 등장으로 더욱 빠
르게 확산 중임.

- AI 기술에 관한 지난 3년간의 가트너 하이프 사이클을 비교해 보면 생성형 AI는 2021년과
2021년에는 혁신 촉발(innovation trigger) 단계에서 상승 중이었으나 2023년 기대의 정
점(peak of inflated expectations) 단계에 진입함.
- 국내 AI 분야 시장은 ‘22년 2조 6천억원에서 ‘27년에는 4조 4천억원 규모로 연평균 15%
성장할 것으로 전망되며, 전세계적으로는 ‘22년 869억 불에서 ‘27년 4,100억 불로 크게 늘
어날 것으로 예상됨(한국IDC, 2023).
- 대표적 생성형 AI 모델인 챗GPT는 2018년 OpenAI에서 처음 개발하였으며 지속적인 버전
업그레이드를 통해 성능과 활용 범위가 비약적으로 증가하고 있고, 최근 OpenAI는 맞춤형
AI를 사고 팔 수 있는 GPT스토어를 공개함.
- 최근 구글 답마인드는 자율주행차 단계처럼 일반인공지능(AGI)을 단순 연산능력 수준의 레
벨 0부터 슈퍼휴먼에 가까운 레벨 5 단계로 구분하면서 AGI가 철학적 개념에서 이제 실용적
개념으로 진화했다고 주장함(Google DeepMind, 2023).

그림 5 : AI 기술 가트너 하이프 사이클,
2021~23
(출처 : Gartner.com)

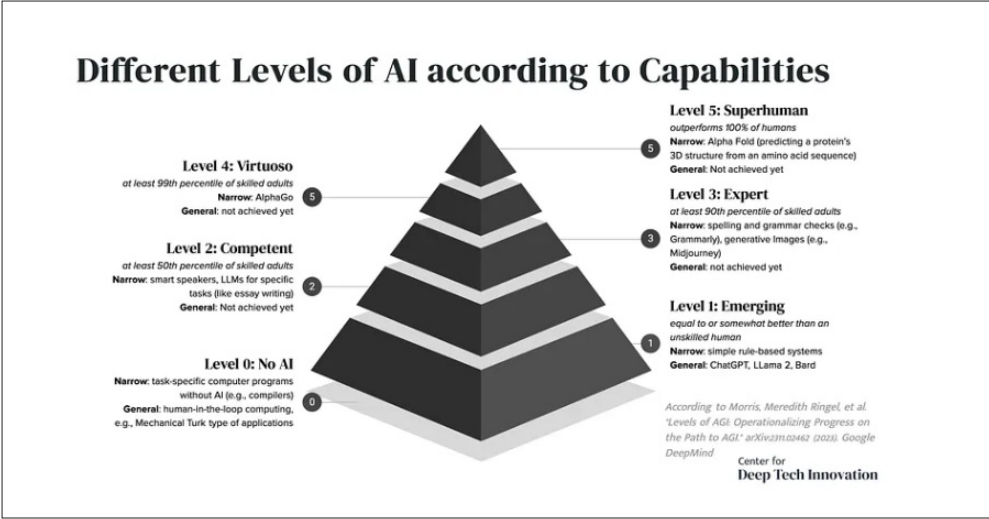
그림 6 : GPT 모델의 진화
(출처 : 국가정보원 외, 2023)



● AI 기술은 가장 대표적인 범용기술(general purpose technology, GPT)로서 민간 영역
만이 아니라 무기체계에나 전력지원체계, 실제 및 가상 전투 수행 등 국방 및 군사 분야에서
도 미래전의 양상을 바꾸는 혁신을 이끌고 있음.

- 시는 근자의 미중 기술패권 경쟁의 핵심 기술로서 AI 슈퍼파워로서 중국의 부상은 국제질
서에 근본적 도전을 제기하고 있음(Lee, 2018; Allison, et al., 2021; Allison & Schmidt
2020; Stokes, et al. 2023).

그림 7 : 구글딥마인드의 일반인공지능 (AGI) 레벨 분류
(출처 : Google DeepMind, 2023)



- AI 기술은 알고리즘 전쟁(Algorithmic Warfare)을 가능케 하는데, AI 알고리즘으로 무인 로
봇체계를 운용하면서 유인 플랫폼이 수행하기 어려운 전시 임무를 수행하거나 AI 기반으로
전투 역학·전력 소모 분석에 광범위하게 활용될 것으로 예측됨(유기현, 2023).
※ 알고리즘 전쟁은 미 공군 메이븐 프로젝트(Project Maven)에서 본격적으로 사용되기 시작된 개념으로 AI와 빅
데이터, 머신러닝, 데이터마이닝, 자율주행 등 을 활용한 군사전략과 작전 개념을 일컬음

표 4 : 알고리즘 전쟁 분야와 예시
(출처 : 유용원, 2020)

분야	내용	예시
정찰 및 정보 수집	항공우주 감시 영상 등 군 데이터를 머신러닝 으로 분석, AI를 활용해 지능형 객체식별·인식· 분석 기능 등을 구현하여 전투 수행체계 향상	Project Maven
예측을 통한 의사결정 지원	군수나 무기체계 데이터 기반 예지 정비나 다 영역(cross-domain) 전투 지원을 위한 소프 트웨어 등	DARPA의 MARS(Multi- Domain Adaptive Request Service)
자동화를 통한 장비 운영	무인항공기, 무인지상로봇 등의 자율 주행· 비행	미 육군의 차세대 장갑차 (OMFV)

● AI 기술의 안보적 이슈와 관한 자세한 논의는 세계신안보포럼 기술 세션 보고서(별책) 및
국내 라운드테이블, 전문가 인터뷰(부록 1 및 부록 2) 참조.

그림 8 : 자율살상무기 사례
(출처 : 안성원, 2022)

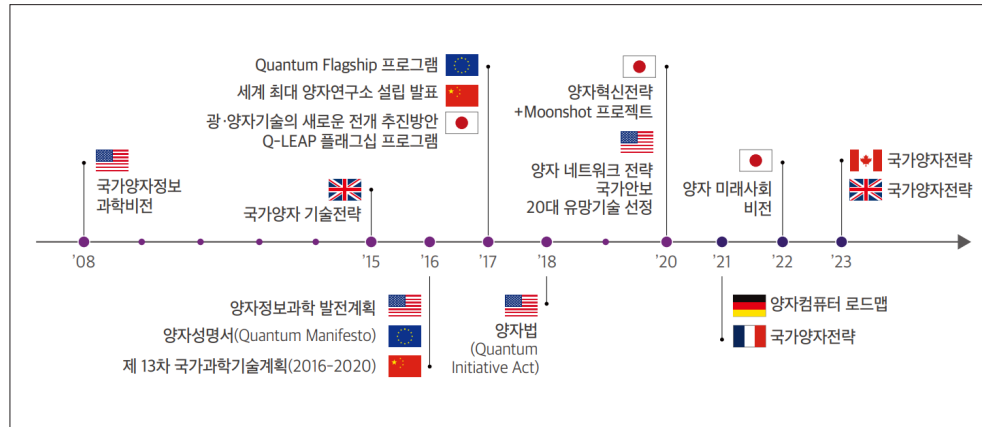


2-3-2. 양자과학기술

● 양자과학기술(Quantum Science & Technology)은 양자물리학적 특성을 컴퓨팅, 통
신, 센서 등 정보기술에 적용하여 초고속 연산, 초신뢰 통신, 초정밀 계측을 가능하게 하
는 기술임(과기정통부, 2023).

- 양자과학기술 분야는 양자컴퓨팅, 양자 시뮬레이션, 양자암호, 양자인터넷 등으로 분류되며,
우리 정부에서는 양자컴퓨팅, 양자통신, 양자센서를 3대 양자과학기술로 분류해 정부 R&D
를 추진 중임.
※ 주요국 양자과학기술 진흥 분야: EU - 양자통신, 양자 시뮬레이션, 양자 센싱 및 계측, 양자 컴퓨팅, 양자 기초과
학 / 영국 - 양자컴퓨팅, 양자 센싱 및 이미징, 양자통신 / 캐나다 - 양자 하드웨어와 소프트웨어, 양자통신, 양
자센서)
- 현 시장 기준 연 평균 20% 이상의 높은 성장을 예고하며 상용화의 경우 양자컴퓨팅은
10~15년 사이, 양자통신은 이미 초기 상용화 단계에 진입, 양자센싱은 향후 7~9년 사이로
전망함(과기정통부, 2023).
- 미국, 중국, 영국, EU 등 주요국은 양자과학기술을 국가 주요 전략 기술로 선정하여 전략을
수립했으며, 특히 미국은 양자 네트워크 전략에서 양자과학기술을 국가안보 20대 유망기술
로 선정(‘20)
- WEF는 2030년 양자컴퓨팅 기술 발전으로 모든 암호가 기능을 상실하는 세계적 보안 위기

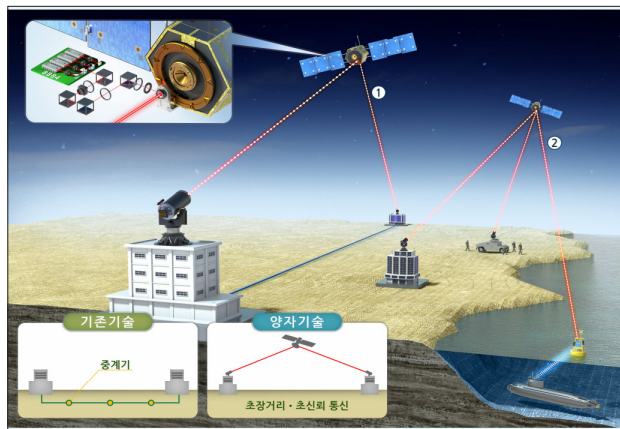
그림 9 : 각국의 양자과학기술
정책 현황
(출처 : 과기정통부, 2023)



● 양자과학기술의 발전에 따른 주요 안보 위협과 리스크는 세부 기술별로 다음과 같음.

- (양자컴퓨팅) 양자컴퓨팅은 빠른 연산으로 기존 슈퍼컴퓨터의 기술 수준을 넘어설 것으로, 양자 컴퓨팅을 통해 구현된 고급 감지 기술은 이동식 핵무기 등에 대한 실시간 표적 및 제거가 가능함(WEF, 2023).
- (양자측정) 상대진에 대한 정찰, 감지, 전장에 대한 파악 및 무기의 유도를 위해 가장 필요한 연구 분야이며, 이러한 양자 측정을 가능하게 하는 센서를 양자센서로 정의함(조성완, 2023).
- (양자통신) 주로 국방 분야에서는 유선 양자암호통신(물리적으로 해킹이 불가능한 암호키를 공유하고, 암호화된 데이터 송수신이 가능, 적의 해킹시도 여부 실시간 모니터링 및 파악 가능), 무선 양자암호통신(지상통제소-무인체계, 무인체계 간에 양자기반의 암호통신을 통해 제어·센서 데이터를 안전하게 송수신 가능), 위성 양자암호통신(초신뢰 보안성 제공, 초장거리 양자 네트워크 구성 가능), 양자 네트워크(통신 거리의 제한 없이 데이터 송수신 가능) 기술이 사용됨(김종영 외, 2022).

그림 10 : 위성 양자암호통신
(출처 : 김종영 외, 2022)



- (양자센서) 국방 분야에 적용 가능한 양자센서의 주요 연구로는 양자중력계(지하의 터널 및 수로 탐색 가능), 양자 RF 센서(레이저의 투과영역에 변화를 주는 양자역학적인 특성 이용), 양 가속도계 및 관성항법계(물체의 위치 정보 제공)이 있음(조성완, 2023).
- (양자암호) 양자컴퓨팅이 기존 암호 체계를 무너뜨리는 위협을 방지하기 위해 어떠한 양자 기술로도 뚫기 어려운 양자내성암호, 포스트-양자 암호(PQC※), 양자키분배기술(Quantum Key Distribution) 등을 국가 차원에서 관련 기술 R&D 지원을 강화 중임.

※ 양자암호: 현대의 암호체계와 같은 디지털 정보를 이용하지 않고, 양자컴퓨터에서 사용되는 물리적 양자상태를 이용하는 암호 방식

※ 포스트-양자 암호: 양자컴퓨터로도 풀 수 없도록 수학 문제의 복잡도를 높은 형태의 암호 알고리즘으로 해당 수학 문제 기반으로 크게 5가지 종류로 나뉨(격자, 해시, 다변수, 코드, 타원곡선)

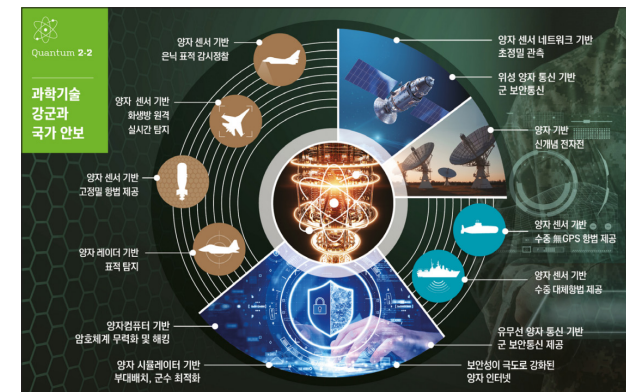


그림 11 : 양자과학기술의 안보 활용 사례
(출처 : 과기정통부, 2023)

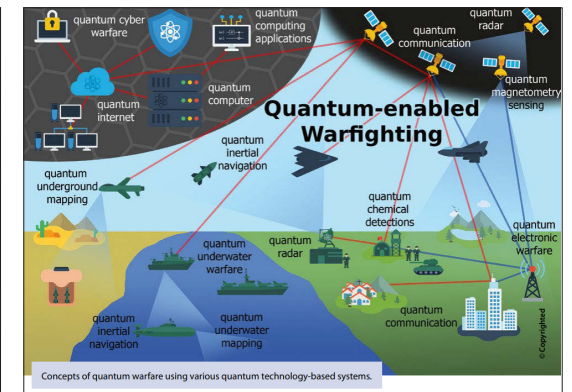


그림 12 : 양자과학기술의 전쟁 적용 시 예상도
(출처 : Michael Krenlina et al., 2023)

2-3-3. 첨단바이오기술

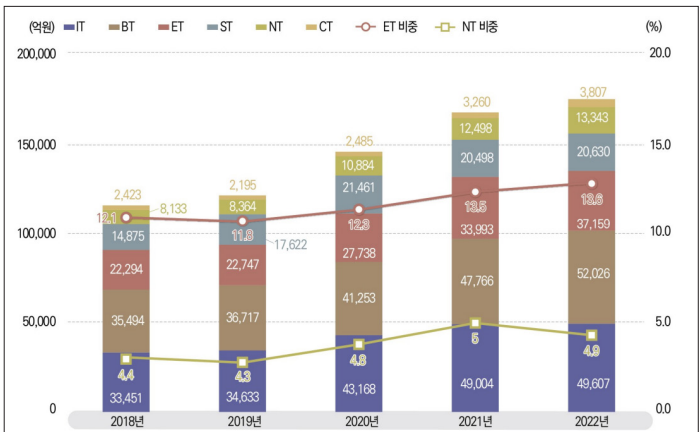
● 첨단바이오기술의 기반이 되는 생명공학은 각종 생물체의 생물학적 시스템, 생체, 유전체 또는 그들로부터 유래되는 물질·정보를 연구하고 활용하는 학문과 기술을 말하며, 기초의과학까지 포함함(생명공학육성법, 2022).

- 바이오 분야는 최근 기술 혁신 및 융합이 가장 활발한 영역으로 AI, 로봇, 빅데이터 등 디지털 기술과 바이오 기술의 결합은 새로운 가치사슬과 성장 기회를 창출하고 있음. 특히 유전체 기술과 빅데이터의 결합으로, 신약 후보물질 발굴, 단백질 구조해독, 유전자가위 예측 등 기존 바이오 기술의 한계를 극복하는 새로운 혁신 성과가 지속적으로 창출되고 있음(제4차 생명공학육성기본계획('23~'32), 2023).
- 첨단바이오기술은 기후 변화, 식량 부족 등 글로벌 이슈에 대응하기 위한 기술로서 그 중요성이 증대하고 있으며, 특히 코로나19 팬데믹 등 감염병 리스크 증가로 공공성이 강조되는 바이오 R&D가 확대되고 있고, 첨단바이오기술 기반 산업 역시 새로운 성장 산업으로 부상 중임.
- 바이오산업의 경우 R&D 성과가 시장 성공으로 직결되는 과학 및 기술집약적 산업으로 CT·나노기술 등 다른 과학기술과의 융합을 통해 새로운 부가가치를 만들며 R&D 전과정에서

그림 13 : 미래유망기술(6T)별
국가연구개발사업 집행 추이
(출처 : 과기정통부 · KISTEP, 2023)

기술창업 · 기술이전 · 연구개발서비스업 등 경제적 효과를 창출하나 윤리 · 규제 문제가 두드러진 산업임(김홍열 외, 2021).

- 현재 우리 정부는 22년 기준 미래유망기술(6T) 예산 17조 6,571억 중 바이오기술 분야에 가장 많은 5조 2,026억원(19.1%)을 투자하고 있음.



※ 미래유망기술(6T) : 정보기술(IT), 생명공학기술(BT), 나노기술(NT), 에너지환경기술(ET), 우주항공기술(ST), 문화기술(CT)

● **바이오기술은 오래전부터 생화학무기 위협과 같은 군사적 활용 이슈가 존재했으나 최근 전세계적 감염병 위기와 유전자 조작 기술 혁신으로 그 중요성이 더욱 증가하고 있음.**

- 바이오기술의 군사적 활용을 규제하는 1972년 발표 생물무기금지협약(Biological and Toxin Weapons Convention)에 따라 각국은 생물학 무기와 관련된 위험을 방지하기 위해 수출 및 수입 통제, 생물안전 및 바이오안보에 대한 법률과 규정을 시행 중임.
- 선진국은 기존의 규제 범위를 벗어나는 바이오기술의 새로운 개발로 군사적 활용이 어려워지고 있는 반면, 기술 수준이 낮은 국가는 진입장벽이 낮은 바이오기술을 손쉽게 획득해 적은 비용으로 무기화할 수 있고 상기 협약의 미가입 국가들이 자국 방어를 위해 바이오기술을 오용하는 도미노 현상도 우려됨.

● **특히 다음과 같은 첨단바이오기술은 새로운 차원의 안보 리스크를 제기함.**

- (유전자 조작 및 생화학적 에이전트 개발) 바이오기술의 발달로 미생물, 식물, 동물 유전자의 조작이 가능해지면서 특정 병원체를 더 치명적이거나 전파력이 강하게 만들 수 있을 뿐만 아니라, 이미 개발된 백신이나 치료법을 무력화시키는 형태로 변형이 가능함.
- (생물학적 감지기술) 생물학적 감지기는 화학적·생물학적 물질을 신속하고 정확하게 검출할 수 있어, 전장에서 생물학 공격을 감지하고 보호조치를 취하는데 이용할 수 있음.
- (인공지능+로봇공학+바이오기술) 자율화된 로봇에 생물학 무기를 개발 및 탑재하여 최소한의 아군 기동으로 생물학적 공격이 가능함. 또한 디지털화된 생명 관련 데이터에 충분한 사이버보안이 수반되지 않을 경우 치명적 취약점이 될 것임(Ryan Fedasiuk, 2022; Kolja

2-3-4. 나노기술

그림 14 : 1~4차 나노기술종합
발전계획 결과 및 성과
(출처 : 국가과학기술자문회의, 2021)

Brockmann et al., 2019).

● **나노기술은 물질을 나노미터 크기의 범주에서 조작 · 분석하고 이를 제어함으로써 새롭거나 개선된 물리적 · 화학적 · 생물학적 특성을 나타내는 소재 · 소자 또는 시스템을 만들어내는 과학기술과 소재 등을 나노미터 크기의 범주에서 미세하게 가공하는 과학기술임(나노기술개발 촉진법, 2018).**

- 나노는 머리카락의 10만분의 1정도의 아주 미세하고 작은 단위로, 대상을 나노 크기로 자를 때 부피 대비 표면적이 기하급수적으로 상승하고 그 결과 나노 크기로 자르면 대상의 본연의 물리적 성질이 변화함.
- 나노기술은 나노공정(nano-processing), 나노소재(nano-materials), 나노기능(nano-functions), 나노부품 및 시스템(nano-components & systems), 나노기반(nano-structures) 등으로 나뉨(정희태 외, 2019)
- 나노기술은 범용기술(General Purpose Technology)로서 파급력이 크고 소재 · 부품 · 장비, 반도체, 배터리 등 주요 제조업과도 다각도로 연계되어 있음. 산업적으로 자성나노입자 · 나노와이어를 이용한 인체 실시간 모니터링으로 당뇨병·심혈관 등 각종 정밀검사에 활용할 수 있고, 고집적 반도체, 고용량 배터리, 유해가스 탐지 센서 등 Si와 로봇 기술에도 활용됨.
- (정부계획) 우리 정부는 2003년 나노기술개발 촉진법을 제정하고 현재까지 제5차 나노기술종합발전계획('21~'30) 포함 총 다섯 차례 나노기술종합발전계획을 수립해 범부처 차원에서 세부 추진계획과 실적을 점검 중임.



● **나노기술은 그 범용성으로 국방·군사 분야에서도 다양하게 활용되고 있음.**

- (나노소재 강화 전투복) 나노 센서를 부착하여 생화학 위험 요소를 선제적으로 식별하여 군인의 생존성 강화가 가능하며, 소재 개발을 통해 운동에너지를 흡수할 수 있는 전투복 개발이 가능함. 또한 높은 유연성과 기동성을 보장할 수 있는 경량화 방탄복과 전투원의 건강 상태를 실시간 모니터링하는 센서를 부착하여 작전 실시간 전투지휘의 효율성을 높일 수 있음.

- (나노소재 강화 폭발물) 부피는 소형화되었으나 폭발력이 증대되고 세부 성형을 통한 관통력 이 향상된 전통적 미사일을 개발할 뿐만 아니라, ‘미니핵’도 개발할 수 있음.
- (자가복제 스마트 나노로봇) 나노로봇과 인공지능이 결합되어 나타난 자가복제 스마트 나노 로봇은 극소단위에서 자가 복제가 가능하며, 연결된 인공지능을 통해 부여된 임무를 효율적 으로 수행할 수 있음. 이를 통해 기존의 장거리 정밀타격을 뛰어넘어 극비리에 초정밀 표적을 타격할 수 있음(Kosal, 2014; Maj Patrick M., 2019).

● 눈에 보이지 않는 나노기술의 불투명성으로 나노기술 규제는 매우 어렵고, 민간에서 국 방 분야로 빠르게 이식 중이나 국방 분야에 한정된 규제로는 효과적인 통제가 어려움.

- 공기 중 분포한 독성 입자의 크기가 작을수록 그 독성은 강해지므로 나노기술의 환경과 인체 에 대한 독성에 대한 우려는 점증하고 있는데 군사 분야에서 나노기술은 안보딜레마 속 군비 경쟁에서 국방 분야에 빠르게 확산 중이고 국가간 기술의 수준 차이로 일부 선도국의 기술 독 점이 발생하고 있음(Kosal, 2014; Maj Patrick M., 2019).

3-1. 신기술 안보 관련
정책 현황

3-1-1. 미국

표 5 : 미국 20대 핵심 신흥기술
(출처 : 글로벌 과학기술정책정보 서비스, 2020)

3. 정책 및 인식



● 미국은 「핵심 신흥 기술에 대한 국가 전략(National Strategy for Critical and Emerging Technologies, ‘20.10.)」의 핵심 축 중 하나로 국가 안보 혁신을 촉진하도록 설계했으 며, 이를 비롯해 신기술과 사이버 중점의 주요 안보 정책·전략·법을 고도화하는 추세임.

- 미국 국가안보위원회(National Security Council, NSC)는 정부 부처와 산하 기관에 미국의 안보 우위를 위한 중요한 기술을 제시하도록 하여 20개의 핵심 신흥 기술을 선정, 지식재산 및 기술 우위를 보호하고 국가안보 혁신 기반을 강화하는 전략을 구축함.

첨단 컴퓨팅	선진 재래식 무기 기술	첨단 공학 소재	첨단 제조
첨단 센싱	항공 엔진 기술	농업 기술	인공지능
자율화 체계	바이오 기술	화학, 생물, 방사능, 핵(CBRN) 억제 기술	통신 및 네트워킹 기술
데이터 과학 및 저장	분산 원장 기술	에너지 기술	인간-기계 인터페이스
의료 및 공공 보건 기술	양자정보과학	반도체 및 마이크로일렉트로닉스	우주 기술

● (정책) 사이버 안보에 관한 국가 전략을 구체화하여 전략을 고도화 중이며, AI, 양자과학 기술을 비롯한 ‘신기술’과 연계된 안보 대응책 마련부터 나아가 글로벌 규범까지 선점하 기 위한 정책을 추진 중임.

- 미국은 경제 전반과 각종 사회서비스, 정책에 기술 활용도와 의존도가 높아 사이버 위협으 로 인한 잠재적 피해 가능성이 상대적으로 높은 편이고, 기존의 수많은 사이버 공격으로 인 해 사이버안보에 대한 정책과 대응 조직 마련에 매우 적극적임(Damien Van Puyvelde 외, 2023).
- 2000년대부터 미국은 사이버안보의 중요성을 지속적으로 강조하며 「국가안보전략(National Security Strategy, ‘22.10.)」에서 사이버범죄 및 위협에 대한 복원력 확보를 위해 국제협력 을 통한 공동 대응을 강조한 이후, ‘사이버 안보’를 중점으로 한 「국가 사이버 안보전략(개정 판, National Cybersecurity Strategy, ‘23.3.)」, 「국가 사이버 안보전략 시행안(National Cybersecurity Strategy Implementation Plan, ‘23.7.)」을 차례로 수립하며 정책 전략을 고도화함(김도원 외, 2023).

3-1-3. 중국

역량 강화, 우수 모범 사례 공유 등을 필두로 국제 파트너십 체결 및 강화(‘23.12.), 우크라이나(‘23.11.), 한국 과기부(‘22.12.) 등 주요국과 국제 협력 강화 중

● (정책) 경제안보 이면의 ‘데이터’와 ‘국가안보’ 중심의 안보 체계 강화, 공급망 확보, 글로벌 표준 확립까지 연계

- 중국 국무원 국무조정실의 「국가 경제 안보의 기본 요소 및 보호 조치에 관한 규정」 발표(‘22.1.): 중국의 국가 경제 안보를 보호하기 위한 기본 요소와 보호 조치를 규정하며, 신기술 관련 안보 분야에서는 핵심 기술의 수출 통제, 기술 유출 방지, 사이버 보안 강화 등을 강조
- 중국은 「국가안전법(国家安全法)」을 제정(‘15)하고 사이버 공간을 국가안보 영역으로 확장하며, 「네트워크안전법(网络安全法)」 제정(‘17)을 통해 사이버 안보영역을 구체화·명확히 하고, 「개인정보 보호법(个人信息保护法)」 시행을 통해 사이버 보안 및 네트워크에 관한 법률체계를 마련(장은정, 2023)
- 중국이 매년 3월 양회(兩會)에서 발표하는 정부업무보고(政府工作報告)와 2015년 발표된 〈중국제조 2025〉 문건 및 13차 5개년 계획(2016~2020) 및 14차 5개년 계획(2021~2025)에 따르면 안보와 산업망·공급망 어휘가 다수 출현(최필수, 2022)

표 7 : 중국 산업정책 내
주요 어휘의 출현
(출처 : 최필수, 2022)

	2015	중국제조 2025	2016	13-5	2017	2018	2019	2020	2021	14-5	2022
제조 강국 制造强国	제조대국에서 제조강국으로	세계를 선도하는 제조강국	품질강국, 제조강국, 지재권 강국	품질강국, 제조강국, 지재권 강국	제조강국을 위한 정책 시스템 개선	제조강국	제조강국	-	-	품질강국, 제조강국, 지재권 강국	품질 강국
안보安全	식량안보	국제경쟁력을 갖춘 제조업이 곧 국가의 안전을 보장하는~ 길이다	-	외국인 투자자가 안보심사, 국가경제 안보	식량안보	-	-	식량과 에너지 안보	에너지 안보, 국가경제 안보, 식량안보	국제산업 안보협력, 식량안보, 자원안보, 외국인 투자자가 안보심사, 국가기술 안보 리스크 관리, 국가 경제 안보	식량 에너지 안보
산업망 공급망 产业链 供应链	-	산업망 구축 공급망 관리 등	산업망 구조조정, 공급망 재구성 등	디지털 산업망, 녹색 공급망 등	농업 산업망 확장 등	-	-	산업망 공급망 안정	산업망 공급망 안정	산업망 공급망 안정	산업망 공급망 안정

표 6 : 중국의 디지털·사이버
법제도 정비 상황
(출처 : 장은정, 2023)

법률명	발표/ 시행	주요내용
네트워크안전법 (网络安全法)	2016.11.7./ 2017.6.1.	■ 네트워크안전법은 중국 내에서의 네트워크 구축, 운영, 유지와 사용 및 인터넷 안전의 감독 관리를 목적으로 제정됨 ■ 외국기업에 대한 데이터 중국 내 저장 의무화, 개인정보 수집 제한 및 유출·판매 규제, 인터넷 제품 및 서비스 보안 심사 의무 등
데이터3법		
데이터 안전법 (数据安全法)	2021.6.10./ 2021.9.1.	■ 데이터 분류 관리, 데이터 안전 평가 및 심사 등 관리 제도 확립
개인정보보호법 (个人信息保护法)	2021.8.20./ 2021.11.1.	■ 개인정보 수집, 저장 사용, 가공, 전송, 제공, 공개, 삭제 및 보호 전반에 대해 포괄적으로 규정한 개인정보보호제도의 기본법
사이버안전심사방법 (网络安全审查办法)	2021.12.28./ 2022.2.15.	■ 100만명이 넘는 이용자의 개인정보를 보유한 인터넷 플랫폼 사업자는 해외 상장 전 중국 당국으로부터 허가·심사받도록 의무화
핵심정보인프라안전보호조례 (关键信息基础设施安全保护条例)	2021.7.30./ 2021.9.1.	■ 국가사이버보안당국, 공안당국 및 관련 부처, 핵심 정보 인프라 안전보호체계공동구축
데이터역외이전안전평가방법 (数据出境安全评估办法)	2022.5.19./ 2022.9.1.	■ 데이터 처리자가 데이터를 해외로 이전하고자 하는 경우, 중요 데이터 및 법에 따라 안전평가를 진행해야 하는 개인정보에 대해 안전평가를 진행하는 대상, 평가내용, 데이터 해외 이전 계약 내용 등 안전평가방법을 규정
인터넷데이터안전관리조례 (网络数据安全管理条例) (의견수렴안)	2021.11.14.	■ 데이터의 종류별등급별 보호제도 수립 및 VPN(가상사설망)에 대한 단속 강화

3-2. 신기술 안보 관련
국민 인식

3-2-1. 신기술 일반 인식

그림 16 : 신기술 대중 인식의 중요성
(출처 : RAND, 2022)

● 미국 국토안보부(Department of Homeland Security, DHS)는 자국 국민의 안전과 국가 안보에 직접적 영향을 미칠 수 있는 신기술에 대한 대중 인식(public perceptions)의 중요성에 주목하며 이들 신기술에 대한 대중의 지지가 확보되지 않을 경우 신기술의 안보적 활용이 용이치 않음을 지적함(RAND, 2022).

- 국토안보부 지원으로 신설된 RAND 연구소 내 국토안보운용센터(Homeland Security Operation Center) 보고서에서는 신기술의 안전성, 투명성, 정확성 등에 대한 대중의 신뢰와 지지가 확보되어야 하며 다음과 같은 분석 프레임워크를 제시함.

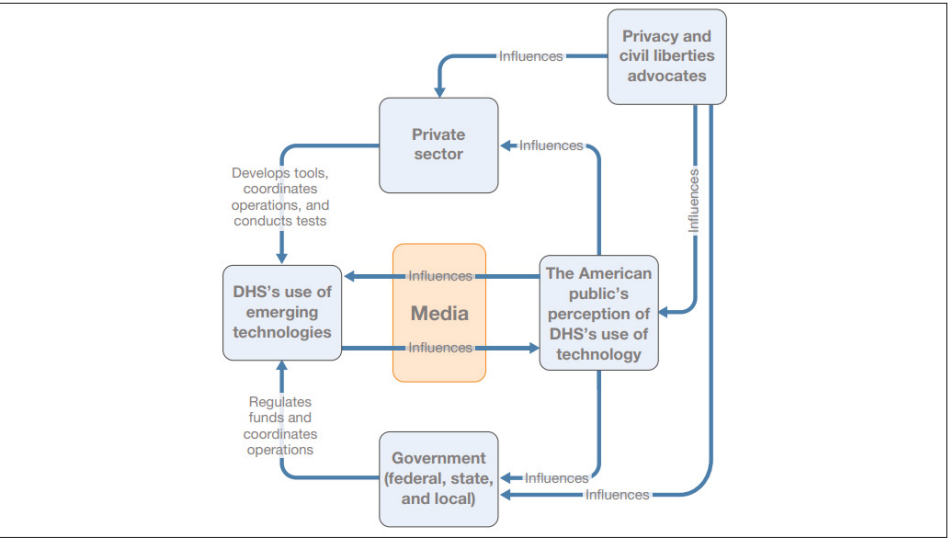
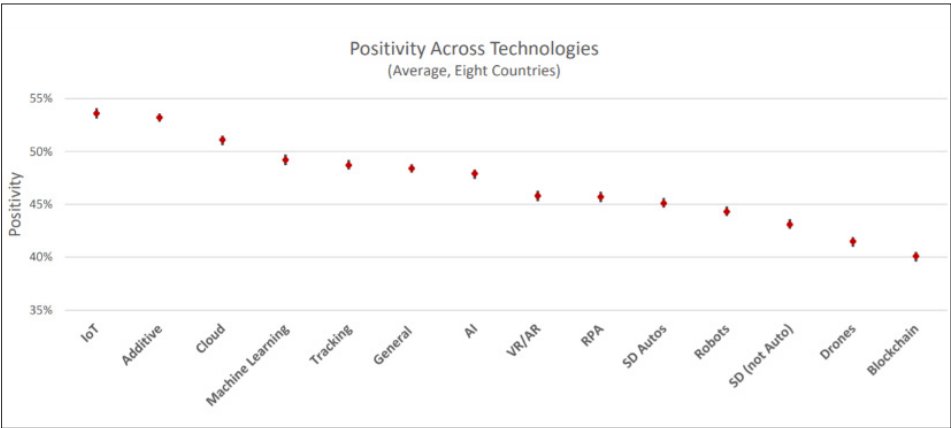
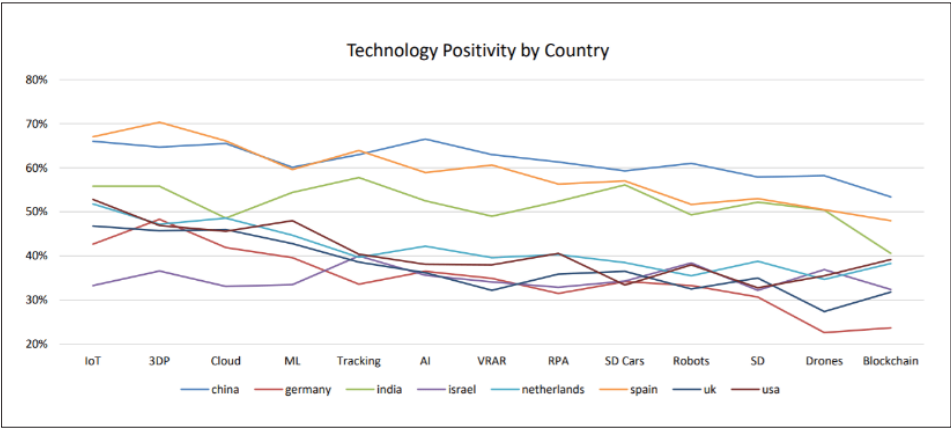


그림 17 : 14개 기술 인식 조사 결과
(출처 : Robinson, 2019)



3-2-2. AI 기술 인식

그림 18 : 국가별 기술
긍정인식 조사 결과
(출처 : Robinson, 2019)



- AI의 긍정적 효과로 조사되는 내용은 주로 생활의 편리성 증대, 생산성 향상, 삶의 질 제고 등이며, 부정적 효과는 일자리 소멸, 윤리적 문제, 인간 존엄성 상실, 프라이버시 침해 등으로, AI의 안보적 함의에 대해 직접 묻는 문항은 거의 없음.

● 미국의 대표적 여론조사·연구기관인 Pew Research Center의 2021년 AI 인식 조사에 따르면 일상생활에서 AI 사용 증대에 대해 37%가 기대되기보다는 우려된다(more concerned than excited)고 응답했으며, 기대와 우려가 반반이라는 응답은 45%, 우려보다 더 기대된다는 응답은 18%에 머물렀음.

- 동 조사에서 기대보다 우려된다는 응답 중에서는 일자리 소멸(19%), 감시·해킹·디지털 프라이버시(16%), 인간 유대감 상실(12%)가 주요 이유였으며, 예기치 않은 결과와 감독·규제의 부재를 이유로 든 응답도 각각 2%로 나타남.

- 한편 동 기관에서 2022, 2023년 이어 수행한 AI 인식 조사에서는 기대보다 우려가 된다는 응답이 증가했는데 특히 2023년 결과는 응답자 과반수 이상(52%)이 기대되기보다 우려된다는 인식을 보여줌. 이는 2022년 말 생성형 AI의 등장으로 이전 분석형 AI를 훨씬 뛰어넘는 성능과 파괴적 잠재력을 경험한 데 따른 것으로 보임.

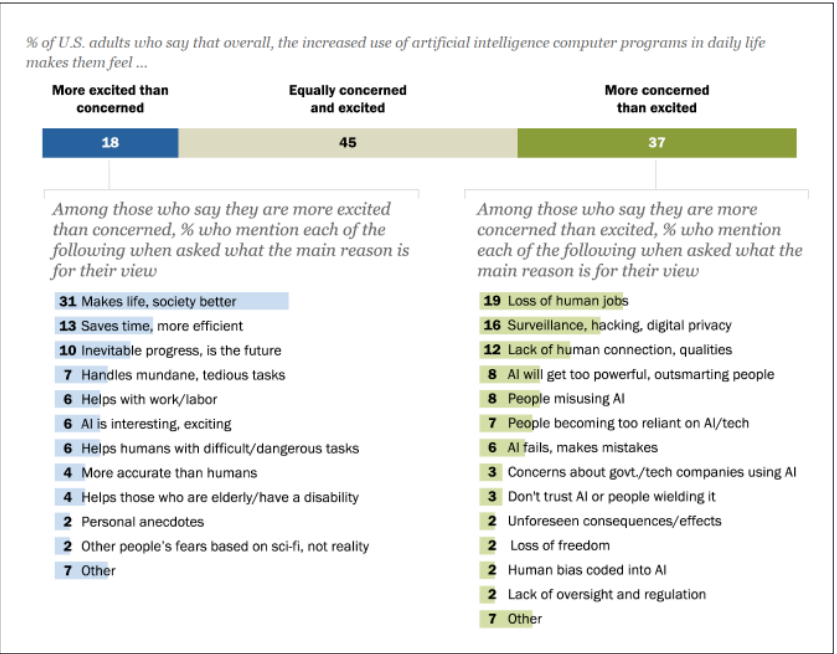


그림 19 : 일상생활의
AI 활용 인식의 주요 이유
(출처 : Pew Research Center, 2021)

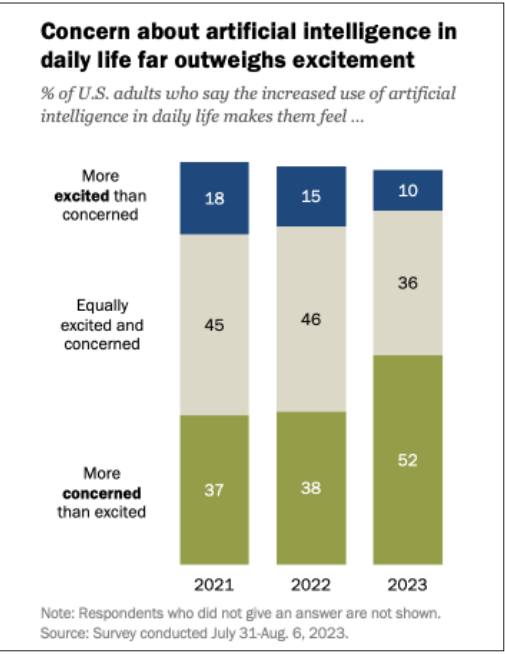


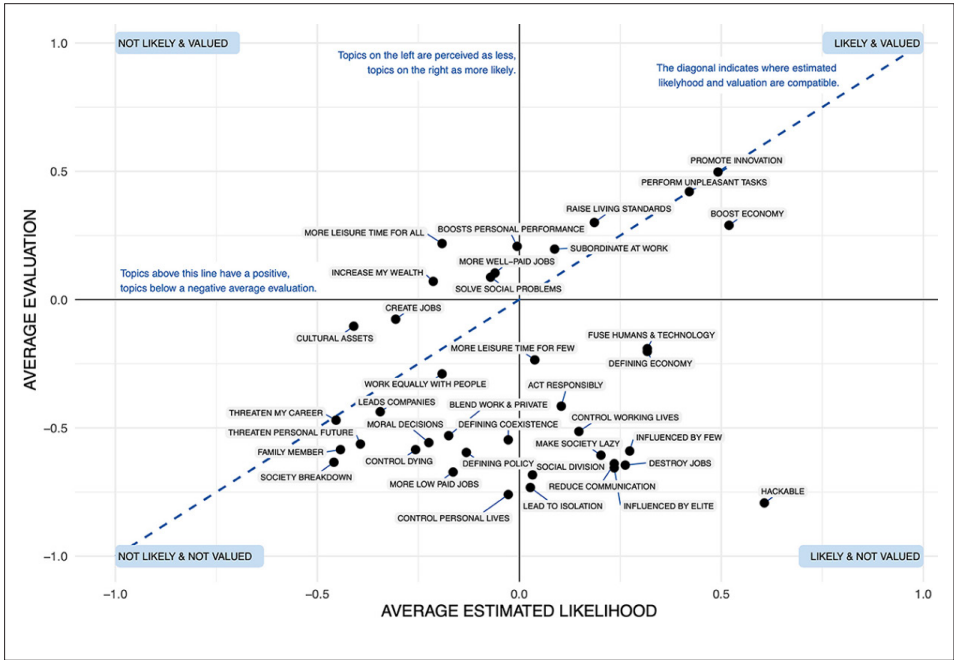
그림 20 : AI 활용 인식 변화
(출처 : Pew Research Center, 2023)

● 전문가 및 시민을 대상으로 한 독일의 최근 조사 연구에서는 전문가 워크샵에서 도출한 38개 질문에 대해 122명에 대한 심층 인식조사 결과를 발생 가능성(likelihood)과 가치(valuation) 차원으로 정리함.

- 발생 가능성이 높고 가치가 큰 AI의 효과로는 혁신 창출, 경제 촉진, 생활 수준 향상 등이 있는데 안보적 차원과 가장 가까운 효과로서 해킹은 가치 차원은 낮으나 발생 가능성이 높은 것

그림 21 : AI 기술 가능성과 가치 평가
(출처 : Brauner et al., 2023)

으로, 사회 붕괴는 가치와 발생 가능성이 모두 낮은 것으로 나타남.



● 옥스퍼드 Future of Humanities Institute에서 2019년 실시한 AI 관련 설문은 미국인 (988명)과 중국인(1,012명)을 대상으로 미국과 중국의 AI 기술 및 군비경쟁에 관한 의견을 조사함.

- AI R&D 수준에 관해서 미국인보다 중국인이 자국의 수준이 좀 더 높은 것으로 응답했는데 5 점 리커트 척도에서 미국인 응답은 1.66, 중국인 응답은 1.74점을 기록함.
- 한편 동 조사에서는 응답자들을 통제집단과 실험집단으로 나눠 실험집단의 경우 AI 우위 확보를 위한 국가주의적 지문(Treatment 1 그룹), 군비경쟁 위험에 관한 지문(Treatment 2 그룹), 인류 공통의 평화 유지에 관한 지문(Treatment 3 그룹)으로 나눠 각각 미국의 AI 군사능력 확보에 더 투자해야 하는지 아니면 중국과 협력해야 하는지를 조사했는데, 군비경쟁 위험과 인류 평화를 강조한 그룹에서 미중 협력 필요성을 강조하는 비율이 가장 높았음.

그림 22 : 미국인 및 중국인의
AI R&D 수준 인식
(출처 : Zhang & Dafoe, 2019)

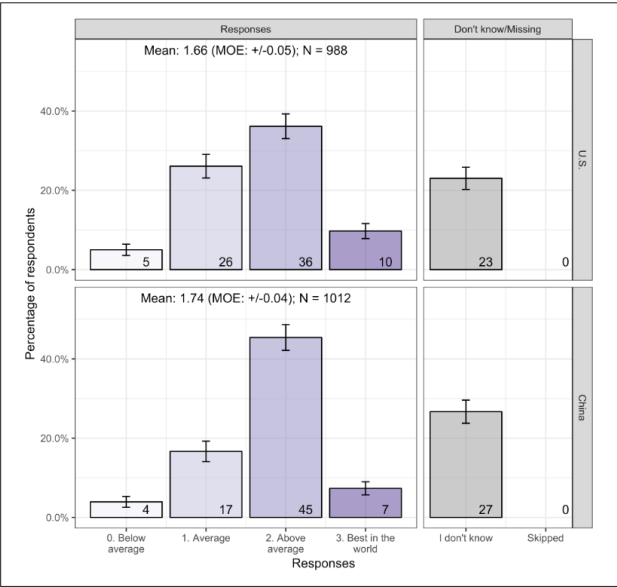
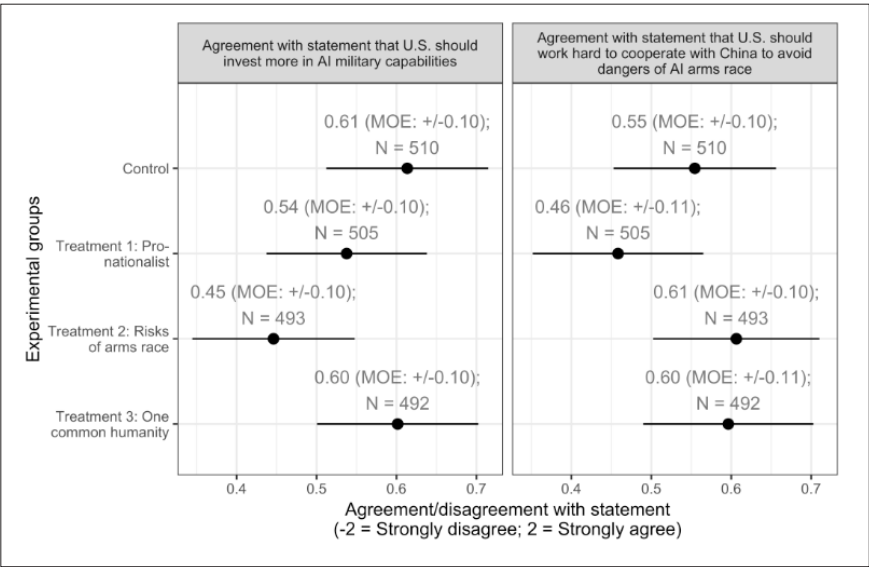


그림 23: 응답 집단별 미국의
AI 군사역량 확보 인식
(출처 : Zhang & Dafoe, 2019)



3-2-3. 한국의 신기술
안보 국민 인식

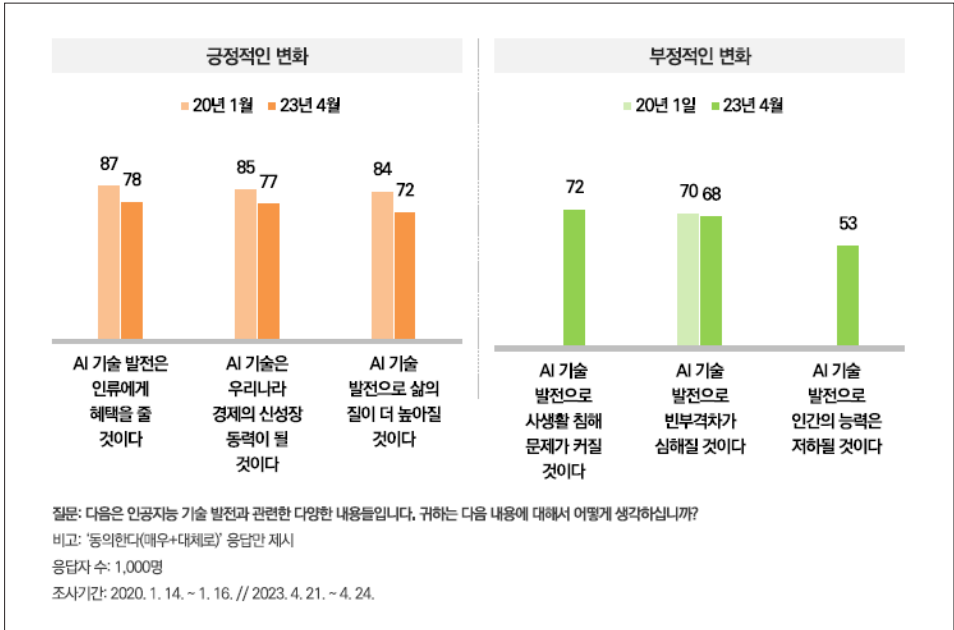
● 해외 여론조사와 마찬가지로 국내에서도 신기술의 안보적 함의를 직접적으로 묻는 설문 조사는 드물어 신기술의 일반적 인식 설문조사에서 유추하거나 신기술 인식과 안보 인식에 관한 조사를 병렬적으로 검토하는 방법이 있음.

● 한국리서치는 국가안보 분야는 정기조사, 기술과학 분야는 기획조사를 수행하고 있는데, 기술과학 분야에서는 AI, 자율주행, 로봇저널리즘, 디지털 격차 등에 관한 조사를 실시함.

- 특히 AI 기술은 2020년부터 매년 기획조사를 실시했는데 4년 사이 AI 기술의 혜택에 대한 긍정적 인식이 점진적으로 감소한 것이 주목할 만함.

그림 24 : AI 기술로 인한 변화 인식
(출처 : 한국리서치, 2023)

- 참고로 대통령직속4차산업혁명위원회에서 2021년 실시한 <인공지능 이용 인식조사>에서 는 AI 기술을 신뢰하는 비율이 37.1%, 신뢰하지 않는 비율7이 6.4%로 2년 전만 해도 부정 인식이 매우 적었던 것으로 판단됨(대통령직속4차산업혁명위원회, 2021).
- 또한 AI 발전으로 이전에 없던 다양한 문제가 발생하고 있는데 이에 대해 우리나라가 준비 를 잘 하지 못하고 있다는 응답이 57%로, 준비를 잘 하고 있다는 응답(12%)의 4배가 넘음.



4-1. 전문가 인터뷰

표 8 : 국내 전문가 인터뷰

4. 전문가 네트워크 구축

- 세계신안보포럼 세션 준비 및 사후 분석 보강을 위해 아래와 같이 국내 전문가를 인터뷰 하고 아래와 같이 기술, 정책, 거버넌스 국제협력 관점의 이슈와 시사점을 도출함. (보다 자세한 인터뷰 내용은 부록 1 참고)

성명	소속 및 직책	인터뷰 일시	분야
심승배	한국국방연구원 국방데이터연구단 국방정책SI연구센터장	2023.11.28.	국방 AI
권현	육군사관학교 AI데이터학과장	2023.11.28.	국방 AI, 데이터
이상우	인하대학교 법학전문대학원 연구교수 및 AI·데이터법센터 책임연구원	2023.11.28.	국제법
정구연	강원대 정치외교학과 부교수	2023.12.15.	국제정치

- (기술 관점) 현 국방부의 AI 수준은 적용 및 활용 단계에 못 미치고 있기 때문에 AI 활용 에 필요한 빅데이터 구축 및 활용 방안에 대한 선제적 준비가 필요하며, 미국을 비롯한 기 술 선진국과의 경쟁 우위 확보 및 동맹국 협력을 위한 유사 수준의 독자적 기술을 확보할 필요가 있음.

- 현 국방 데이터 운용은 강력한 보안 및 투명한 사업관리에 중점이 맞춰진 관계로 기술개발 속 도가 저하되고 있는 바, 클라우드 환경 전환에 따른 데이터 보호 정책을 수립하고 한국어 기 반의 텍스트 음성 데이터 운용시스템 등 독자적인 기술이 필요함.
- 러-우 전쟁 사례를 통해 탄력적인 군수 공급망이 원활하지 않은 것을 볼 때, 한국이 특히 군 사 분야에 있어 선점해야 할 주제는 군수 공급망(AI-driven defense supply chain)이며 물 리적인 무기 공급뿐만 아니라 향후 보안체제까지 확장되는 사안이기에 선제적인 준비가 필 요함.

- (정책 관점) 너무 앞선 규범 수립보다는 기술 개발의 고도화에 초점을 맞춰 정책 또한 고 도화할 필요가 있음.

- 기존 법령의 하드웨어 중심의 무기체계 연구개발 또는 구매 절차에 AI와 같은 소프트웨어 연 구 추진을 위한 제도가 부재한 상황임. 이들 제도 설계 시 선부른 규제 도입과 윤리라는 명목 하에 기술 발전 저해에 영향을 미치면 안됨.
- AI 기술 역량이 국가별로 편차가 매우 커서 일괄적인 규제 이니셔티브를 글로벌 차원에서 마

련하기에는 한계가 있으며, 현재 글로벌 규범 수립의 움직임 또한 AI 기술 리더십 공고화 목적이 내포되어 있어, 당장 구속력 있는 규제보다는 AI 기술의 다양한 사회·정책적 영향에 대한 협의체 수준으로 접근하는 것이 현실적이고 바람직함.

● (거버넌스 관점) 국가 차원의 종합적인 사이버 안보 대응이 시급하며 다양한 이해관계자의 협의를 통한 거버넌스를 마련할 필요가 있음.

- 현재 거버넌스의 맹점은 사이버 안보 기본법제가 미비하며, 사이버 안보와 AI를 통할하는 국가 차원의 컨트롤 타워가 없어 부처별로 사이버 안보 이슈에 파편적으로 대응 중임.
- 국가 차원의 통합적 대응을 위해서는 AI 핵심·원천기술 확보와 기술개발을 지원할 수 있는 환경을 조성하고, 민·관·군이 함께 하는 유기적인 거버넌스 구축이 필요함. 이에 각 부처별 민간 전문가를 포함하는 민관협의체가 효과적인 시작점이 될 수 있음.

● (국제협력 관점) 미중 패권 사이의 중견국으로서의 차별화된 전략과 AI 기술 역량별, 지정학적 학별 상황을 고려한 종합적인 전략이 필요함.

- 한국은 북한, 중국, 러시아 등 다층적 위협(AI의 일반적 위협, AI의 군사적 위협, AI와 핵 위협)에 노출되어 있는 상황으로 유사입장 국가들과의 소·다자협력을 통한 군사훈련 및 군사협력 상황을 통해 위협 가능성 축소와 최소한의 규제에 대한 합의 노력 필요
- 균형잡힌 시각을 바탕으로 한국이 양분된 국제협력 거버넌스의 연결고리 역할을 담당해야 하며, 지정학적, AI 기술 역량별로 동맹국들과의 협의체제를 신속하게 가동할 필요성이 있음.

4-2. 기술별 전문가 풀

● 세계신안보포럼 및 국내 전문가 라운드테이블 기획을 위해 약 90여 명의 해외 전문가를 발굴함.

- 인공지능 분야 전문가는 AI 기술 혁신, 윤리, 정책, 거버넌스, 안보 및 보안 관련 30여 명을 발굴함.

이름		소속 · 직위 / 전문분야
	Dr. Marietje Schaake	· International Policy Director, Cyber Policy Center, Stanford University · Human-Centered Artificial Intelligence
	Dr. Ng Seek Kiong	· Director of AI Technology, AI Governance, Singapore · AI and National Innovation System
	Ms. Beena Ammanath	· Global Head of Deloitte AI Institute, Deloitte · AI Ethics

	Mr. Joris Cyizere	· Strategy Lead & Deputy Director, WEF Center for the Fourth Industrial Revolution, Rwanda · AI Governance at WEF
	Mr. Alain Ndayishimiye	· Head of AI, WEF Center for the Fourth Industrial Revolution, Rwanda · AI Tech Development
	Dr. Rediet Abebe	· Fellow at Harvard Society of Fellows & Assistant Professor at UC Berkeley · AI and Inequality
	Dr. Anu Bradford	· Professor of Law, Columbia Law School · AI and Big Tech Regulation
	Ms. Stephanie Ifayemi	· Head of Policy, Partnership on AI (PAI) · AI Standards and Policy
	Mr. Anir Chowdhury	· Policy Advisor of Government of Bangladesh / United Nations Development Programme · AI and Digital Promotions Policy
	Dr. Hammam Riza	· President of KORIKA - Indonesia · Artificial Intelligence in Indonesia
	Dr. Renee Cummings	· Professor of AI Governance, Columbia University · AI for Social Good and Social Justice
	Mr. Jacob Stokes	· Senior Fellow of the Indo-Pacific Security Program, Center for a New American Security · AI and Great Power Competition
	Dr. Lance Menthe	· Senior Physical Scientist; Professor of Policy Analysis, RAND Corporation · Military Application of AI
	Dr. V.S. Subrahmanian	· Walter P. Murphy Professor of Computer Science, Northwestern University · Deepfakes, Machine Learning for Security Problems
	Dr. Vincent Boulanin	· Director of the Governance of Artificial Intelligence Programme, Stockholm International Peace Research Institute (SIPRI) · Autonomous Weapons Systems
	Dr. Darren J. Lim	· Senior Lecturer of Australian National University · Defence Studies, Politics and International Relations
	Dr. Urs Gasser	· Dessor of Public Policy, Technology University of Munich & Harvard Berkman Klein Center · Technology Governance

	Mr. Onni Aarne	<ul style="list-style-type: none">· Consultant of Institute for AI Policy and Strategy· Compute and Governance of AI
	Dr. Paul Scharre	<ul style="list-style-type: none">· Executive Vice President and Director of Studies, Center for a New American Strategy (CNAS)· Unmanned and Autonomous Systems
	Ms. Ainikki Riikonen	<ul style="list-style-type: none">· Policy Analyst of Office of Science and Technology Policy (OSTP)· AI and Information Systems in the International Competition
	Dr. Li Ang Zhang	<ul style="list-style-type: none">· Codirector of Center for Scalable Computing and Analysis, RAND Corporation· Applying Machine Learning on Defense and Military Technology Policy
	Dr. Edward Geist	<ul style="list-style-type: none">· Dressor of Policy Analysis, Pardee RAND Graduate School· Potential Impact of Emerging Technologies on Nuclear Strategy
	Dr. Aaron B. Frank	<ul style="list-style-type: none">· Acting Associate Director of Acquisition and Technology Policy Program, RAND Corporation· Analytic Tradecraft, Decision-Support Tools for Analyzing Complex Security Issues
	Dr. William Marcellino	<ul style="list-style-type: none">· Senior Behavioral and Social Scientist, Professor of Policy Analysis, Pardee RAND Graduate School· AI Technology Application, Acqusition
	Dr. John Villasenor	<ul style="list-style-type: none">· Professor of Department of Electrical Engineering, UCLA· Information Technology, Artificial Intelligence
	Mr. Fabio Rugger	<ul style="list-style-type: none">· Deputy Permanent Representative of Italy, NATO· Cyber Security, Artificial Intelligence
	Dr. Andrew Lohn	<ul style="list-style-type: none">· Director of Emerging Technology, National Security Council, The White House· Policy in AI and Cybersecurity
	Dr. Diana Gehlhaus	<ul style="list-style-type: none">· Defense Department Fellow of Center for Security and Emerging Technology; Department of Defense· Human Resource Management in Artificial Intelligence
	Dr. Margarita Konaev	<ul style="list-style-type: none">· Deputy Director of Analysis, Center for Security and Emerging Technology· Military Applications of Artificial Intelligence



- 바이오기술 분야 전문가는 바이오안보, 생화학무기, 글로벌 보건 안보, 팬데믹 대응 등 관련 해 10여 명을 발굴함.

이름	소속 · 직위 / 전문분야
	Mr. Matthew McKnight <ul style="list-style-type: none">· General Manager of Ginkgo Bioworks· Biosecurity
	Dr. Sam Weiss Evans <ul style="list-style-type: none">· Research Fellow of Harvard University· Biosecurity, Biorisk, Management
	Dr. Brandon Hatcher <ul style="list-style-type: none">· Acting Director and Deputy Director of Center for Disease Control and Prevention· Biosafety
	Dr. James Revill <ul style="list-style-type: none">· Programme Lead at Weapons of Mass Destruction, UN Institute for Disarmament Research· Biological and Toxins Weapons
	Dr. Filippa Lentzos <ul style="list-style-type: none">· Associate Dressor of Kings College London· Biomedical and Life Science, Security, and Policy
	Dr. Piers Millett <ul style="list-style-type: none">· Senior Fellow of Future of Humanity Institute· Biotech
	Dr. Audrey Bowden <ul style="list-style-type: none">· Dressor of Vanderbilt University· Biophotonics
	Dr. Lane Warmbrod <ul style="list-style-type: none">· Biological and Chemical Weapons Policy Analyst of Pacific Northwest National Laboratory· Biosecurity and Pandemic Preparedness & Response
	Dr. Nancy Connell <ul style="list-style-type: none">· Dressor of Department of Medicine, Institute for Health, Health care Policy and Aging Research· Antibacterial Drug Discovery
	Dr. Sana Zakaria <ul style="list-style-type: none">· Research Leader of RAND Corporation· Biotechnologies converging with Machine Learning and Quantum Technologies
	Dr. Jennifer Bouey <ul style="list-style-type: none">· Senior Policy Researcher of Tang Chair in China Policy Studies, RAND Corporation· Global Health Security, Health Equity
	Dr. Timothy Marler <ul style="list-style-type: none">· Senior Research Engineer of Professor of Policy Analysis, Pardee RAND Graduate School· Health Biotechnology, Bioeconomy Strategy
	Mr. John V. Parachini <ul style="list-style-type: none">· Senior International and Defense Researcher of RAND Corporation· Biological Weapons and Warfare






	Dr. Patricia A. Stapleton	· Associate Director of Infrastructure, Immigration, and Security Operations Program, RAND Corporation · S&T Policy, Food Security
	Dr. James Andrew Lewis	· Senior Vice President and Director of Strategic Technologies Program, Center for Strategic and International Studies (CSIS) · International Security, Quantum Technology
	Dr. Sujai Shivakumar	· Director and Senior Fellow of Renewing American Innovation Project, Center for Strategic and International Studies (CSIS) · Technology and Innovation, Quantum Technology
	Dr. Charles Wessner	· Research Professor of Science, Technology and International Affairs Program at Georgetown · Semiconductor R&D and National Security

- 양자과학기술 분야 전문가는 양자 하드웨어, 교육, 양자안보, 양자외교 등 관련해 10여 명을 발굴함.

이름	소속 · 직위 / 전문분야
	Mr. Robert Burns · Chief Product Security Officer of Thales CPL · Cloud Computing and Quantum Computing
	Dr. Ronald Hanson · Chairman Executive Board of Quantum Delta NL · Quantum Technology
	Dr. Hartmut Neven · Vice President of Engineering of Google · Quantum Technology
	Dr. Abe Asfaw · Researcher of Google Quantum · Quantum Hardware and Education
	Dr. Michael J. D. Vermeer · Senior Physical Scientist, RAND Corporation · Cybersecurity Risks Created by Quantum Computing
	Dr. Edward Parker · Physical Scientist of Professor of Policy Analysis, Pardee RAND Graduate School · Emerging Quantum Technologies
	Dr. Salil Gunashekar · Senior Research Leader at Associate Director of Science and Emerging Technology, RAND Europe · AI, Quantum Technology Regulation
	Dr. Daniel Gonzales · Senior Scientist, Professor of Technology Analysis, Pardee RAND Graduate School · Advanced Communications Systems, Quantum




	Dr. Chad Heitzenrater	· Senior Information Scientist of RAND Corporation · Economics of Information Systems, Cyber Warfare
	Dr. Kiron K. Skinner	· Taube Professor of International Relations and Politics, Pepperdine University · Quantum Technology on Foreign Policy

- 바이오기술 분야 전문가는 바이오안보, 생화학무기, 글로벌 보건 안보, 팬데믹 대응 등 관련해 10여 명을 발굴함.




이름	소속 · 직위 / 전문분야
	Dr. Shanhui Fan · Professor of the Dressor School of Engineering, Stanford University · Nanophotonic for Energy
	Dr. Karl K. Berggren · Professor of Electrical Engineering, MIT · Nanofabrication
	Dr. Adrian Mihai Inonescu · Professr of Nanoelectronic Devices Laboratory, Swiss Federal Institute of Technology Lausanne · Nanoelectronic devices, nanoelectrics for sustainability
	Dr. Bernard C. Kress · Director of XR Hardware, Google · Nano Optics
	Dr. Richard Silbergliitt · Senior Physical Scientist, Professor of Policy Analysis, Pardee RAND Graduate School · R&D Portfolio Assessment and Nanotechnology

● 국내 전문가는 인공지능 및 사이버안보 20명, 양자 및 나노기술 각 5인을 포함해 총 25 명을 발굴함.






·인공지능

이름	소속 · 직위 / 전문분야
	유기현 · 한국국방연구원 군사발전연구센터 책임연구위원 · 국방기획 · 혁신, 인공지능
	노용만 · KAIST 전기및전자공학부 교수 · 국방 · 보안 AI 딥러닝 공격 방어
	이정민 · 카네기국제평화연구소 선임연구위원 · 신기술의 국방 무기체계 적용, 국방기획






	윤정현	· 국가안보전략연구원 부연구위원 · 국방 분야 인공지능 기술 도입
	김상배	· 서울대학교 정치외교학부 교수 · 신형 안보의 디지털 기술 연관성
	조원영	· 소프트웨어정책연구소 SI 정책연구팀 책임연구원 · 인공지능 신뢰체계 정립
	유준구	· 외교안보연구소 연구교수 · 신기술의 군사적 활용규제, 자율살상무기
	하정우	· 네이버클라우드 시럽 소장 · 대규모 언어모델, 디지털플랫폼정부
	안성원	· 소프트웨어정책연구소 AI정책연구실장 · 인공지능, 국가안보, 전략기술
	김용대	· KAIST 전기및전자공학부 · 정보보호대학원 교수 · 블록체인, 가상화폐, 사이버보안
	김영진	· 고려대 인공지능사이버보안학과 초빙교수 · 사이버보안, 사업기술보호
	하태정	· 과학기술정책연구원 국가연구개발분석단 선임연구원 · 사이버보안, 사업기술보호
	윤명근	· 국민대학교 소프트웨어학부 교수 · 인공지능연구, 금융보안, 사이버보안, 보안관제
	정구연	· 강원대학교 정치외교학과 부교수 · 미래전, 인공지능, 자율무기체계
	차정미	· 국회미래연구원 국제전략연구센터장 · 중국 군사혁신, 군사지능화, 군민융합
	손광수	· KB경영연구소 북한연구센터 연구위원 · 북한 가상자산 탈취
	민경식	· 한국인터넷진흥원 디지털정책팀장 · 정보보호, 블록체인 기술 표준화
	박성수	· 카스퍼스키 책임연구위원 · 가상화폐 및 사이버 공격

	김성배	· 국가안보전략연구원 책임연구위원 · 신기술의 국제정치, 해외 정보
	임종인	· 고려대 사이버국방학과 석좌교수 · 사이버안보 기술 · 정책, 암호학
	김정호	· KAIST 전기및전자공학부 교수 · 반도체, 신호무결성, 상호연결성

·양자기술

	이름	소속 · 직위 / 전문분야
	이준구	· KAIST 전기및전자공학부 교수 · 양자보안통신, 양자기계학습, 광통신
	곽기호	· 국방과학연구소 국방첨단과학기술연구원장 · 첨단무기체계 연구개발, 양자기술
	김재완	· 고등과학원 부원장, 계산과학부 교수 · 양자 얽힘, 양자정보, 큐디트
	한상욱	· 한국과학기술연구원 양자정보연구단 단장 · 양자 암호, 양자컴퓨팅, 양자정보기술
	정연욱	· 정연욱 성균관대 나노공학과 교수 · 초전도 큐비트 기반 양자 컴퓨팅

·나노기술

	이름	소속 · 직위 / 전문분야
	유룡	· 한국에너지공과대학교 석학교수 · 나노구조, 물리화학, 촉매
	현택환	· 서울대 화학생물공학부 석좌교수 · 기능성 무기 나노 소재
	김필립	· 하버드대 물리학과 교수 · 응집물질 물리학, 그래핀
	이영희	· 성균관대 물리학과 석좌교수 · 나노물질 합성 및 물성연구
	이건재	· KAIST 신소재공학과 석좌교수 · 박막증착, 반도체공정, 반도체센서

5-1. 국내 신기술 안보
라운드테이블

표 9 : 국내 신기술
안보 라운드테이블 프로그램

5. 신기술 안보 관련 포럼

● 본 정책연구 과제의 주요 과업인 세계신안보포럼 세션 기획을 위해 사전 국내 전문가 라운드테이블을 아래와 같이 개최함.

- 일시 및 장소: 2023.09.15.(금) 10:30~14:40, 포시즌스 호텔 서울
- 일정 및 패널

일정	시간	세부 주제	참여 패널
개회식	10:30~10:45	개회사, 축사	▪ 개회사: 박용민 외교부 다자외교조정관 ▪ 축사: 이승섭 KAIST 안보·대외협력 자문역 ▪ 사회: 김수라 외교부 국제안보과장
세션 1	10:50~12:00	생성형 인공지능의 세계안보적 함의	▪ 발표: 윤정현 국가안보전략연구원 신흥안보연구실 부연구위원 ▪ 토론: 조상근 KAIST 국가미래전략기술정책연구소 연구교수, 차정미 국회미래연구원 국제전략연구센터장, 안성원 소프트웨어정책연구소 AI정책연구실장 ▪ 좌장: 송윤선 국민대학교 정치대학원 겸임교수 ▪ 사회: 김수라 외교부 국제안보과장
오찬(12:00~13:00)			
세션 2	13:30~14:40	사이버해킹과 사이버안보의 미래	▪ 발표: 김용대 KAIST 정보보호대학원 교수 ▪ 토론: 박춘식 아주대학교 사이버보안학과 교수, 손광수 KB금융지주경영연구소 북한연구센터 연구위원, 조은정 국가안보전략연구원 국제질서연구센터장 ▪ 좌장: 임종인 고려대학교 정보보호대학원 석좌교수

그림 25 : 국내 신기술
안보 라운드테이블 모습



● 세션 1 발표의 주요 내용: 생성형 AI의 세계안보적 함의

- 인공지능은 국가안보에 있어 범용적 파급력을 가진 기술로, 경제·사회·군사 등 다양한 분야에서 활용중이며, 특히 생성형 AI는 기존 콘텐츠 정보를 토대로 새로운 콘텐츠를 창작하는 AI 모델로, 다차원·복합 문제해결에 적합하며 결과의 다양성과 활용 용이성을 갖고 있음.
- 그러나 생성형 AI는 편향성과 환각, 불안정한 기술발전 단계, 상시적 Prompt Hacking 위험성 등의 한계점을 가지고 있으며, 이는 국가안보에 부정적인 파급력을 미칠 수 있음.
- 생성형 AI 시대의 국가안보 위협은 단기·중장기적으로 발생할 수 있으며, AI의 범용적 측면과 신흥파괴적 측면, 미중 경쟁 시대의 정치안보적 쟁점 및 수단화, 차세대 보안 패러다임 전환 과정에서의 불확실성 등을 고려하여 대응해야 함.
- 시사점 및 제언:
 - ① 진화된 AI가 제기하는 신종 위협에 대한 능동적 대응 인프라/기반 마련, 편향성과 환각 등 AI의 구조적 한계점 보완을 위한 데이터 활용 기준 개선 필요
 - ② 생성형 AI의 안전한 이용 인증 및 장기적 연구지속을 위한 민관협력 대화체제 수립, 인간/기계협업 구조를 보장하는 제도적 원칙과 환류체계 마련 필요
 - ③ 진화된 AI 제기하는 글로벌 안보 도전에 대응하는 거버넌스 논의 주도, 사회 구성원의 AI 문해력 강화 및 올바른 생산/활용 준수 가이드라인 마련 필요

● 세션 1 주요 토론 내용

- (핵심 제언) 생성형 AI는 기존 AI 기술보다 더욱 정교하고 현실적인 가짜 콘텐츠를 생성할 수 있어, 정보전, 심리전, 사이버 공격 등 다양한 분야에서 국가안보에 위협이 될 수 있음. 따라서 생성형 AI의 위험성 인식과 대응 방안 마련을 위한 국제 협력이 필요함. 또한, 생성형 AI의 기술 확보와 더불어 기술 신뢰성 확보 필요
- 토론자별 주요 내용:
 - ① 윤정현 부연구위원: 생성형 AI는 군사 분야에서의 활용이 급속도로 증가하고 있어, 새로운 전쟁 양상을 야기할 수 있음. 따라서 생성형 AI의 기술 확보와 더불어 기술 신뢰성 확보가 필요함. 또한, 생성형 AI의 위험성 인식과 대응 방안 마련을 위한 국제 협력이 필요함.
 - ② 조상근 연구교수: 생성형 AI의 활용에 있어서 알고리즘뿐만 아니라 구현하는 이동통신, 반도체 등이 매우 긴밀하게 연결되어 있음. 따라서 그것을 구현하는 역량을 키워 지렛대로 활용 필요함. 또한, 국제 사회의 냉엄한 현실에 따라 AI가 군사적인 목적으로 활용되는 경우가 굉장히 많음. 이에 따라 AI 오남용 방지 측면에서 안보 전략 및 정책 방향 필요
 - ③ 차정미 센터장: 생성형 AI로 인해 새로운 국제 질서와 안보 위기를 불러올 수 있으며, 복합 안보 위기라고 불리는 기술과 가치구범, 군사, 외교, 글로벌 리더쉽 경쟁을 구체화하고 심화시킬 수 있음. 또한, 주요국에서는 생성형 AI를 안보 측면에서 기술패권을 유지하는데에 핵심이 있음. 따라서 우리의 안보는 어디에 방점이 있고, 그러면 우리는 어떤 것을 지켜야 하기 때문에 어떻게 안보 전략을 구성하고, 어떻게 외교 전략을 구성해야 되는지에 대한 한국식 생성형 AI 시대의 안보 외교 전략 필요
 - ④ 안성원 실장: AI 오남용 방지 측면에서 안보 전략 및 정책 방향을 제시하였음. 생성형 AI 기술은 우리나라가 기술력을 확보하지 못하면 글로벌 사회에서 도태될 수밖에 없는 핵심적인 기술임. 따라서 국가 차원의 기술 확보와 더불어 기술 신뢰성 확보 필요

● 세션 2 발표의 주요 내용: 사이버해킹과 사이버 안보의 미래

- 사이버해킹의 발생 원인은 인간의 실수와 디지털 트랜스포메이션으로 인한 새로운 애플리케이션과 플랫폼의 등장이며, 해킹의 트렌드는 제로 트러스트 보안의 확산과 공급망 공격의 증가로 이어지고 있음.
- 신기술의 보안 문제는 신기술 개발자의 보안 이해 부족, 표준에서의 보안 고려 부족, 설계상의 문제점, 기존 보안 취약점 등으로 인해 발생함.
- 사이버안보는 모든 ICT의 핵심이며, 기술의 발전에 따라 취약점도 증가하기 때문에 보안의 플랫폼 내재화, 공격과 수비 기술의 중요성, 표준에서의 보안 요소를 고려해야 함.
- 시사점 및 제언:
 - ① 사이버해킹은 국가 안보뿐만 아니라 개인의 안전과 재산에도 심각한 위협이 되고 있기 때문에 사이버안보의 중요성은 더욱 커지고 있음. 이에 따라 사이버안보를 강화하기 위해서는 기술적인 측면뿐만 아니라 법적, 제도적, 인적 측면에서도 종합적으로 접근할 필요가 있음.
 - ② 신기술의 등장에 따른 보안 문제에 대한 대비가 필요하며 신기술의 개발 단계에서부터 보안을 고려하는 것이 중요하며, 기존 보안 취약점도 지속적으로 점검하고 보완해야 함.

● 세션 2 주요 토론 내용

- (핵심 제언) 사이버 안보는 국가 차원의 단독 대응으로는 한계가 있기 때문에 국제 사회의 협력과 다양한 분야의 전문가들이 모여 사이버 안보에 대한 정책과 전략을 논의하는 것이 중요함. 또한, AI 및 신기술을 통한 효율성 확보와 책임 강화 방식 도입 등을 통해 사이버 안보 역량을 강화해야 함
- 토론자별 주요 내용:
 - ① 조은정 센터장: 사이버 안보는 국가 이니셔티브 차원의 안보 문제로 고려되어야 하며, 국제 사회의 협력과 다양한 분야의 전문가들이 모여 사이버 안보에 대한 정책과 전략을 논의하는 것이 중요함.
 - ② 손광수 연구위원: 북한은 사이버 공격을 주요 대남 도발 수단으로 활용하고 있으며, 최근에는 가상 자산 탈취를 통해 외화벌이를 목적으로 하는 공격이 증가하고 있음. 이에 한미일 3국은 사이버 안보 협력을 더욱 강화할 필요가 있음.
 - ③ 박춘식 교수: 한국은 사이버 안보 선진국이지만, 사이버 범죄 협약 가입, 사이버 안보 관련 인력 확충, 사이버 안보 역지력 강화 등의 분야에서 개선이 필요함.
- 동 라운드테이블에 관한 상세 보고는 부록 2에 수록함.

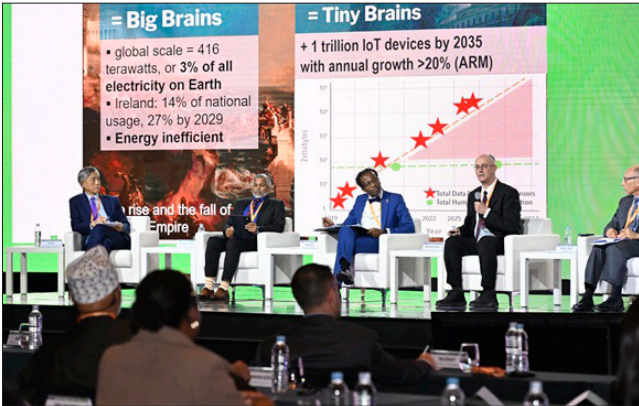
● 2023년 제3차 세계신안보포럼(World Emerging Security Forum, WESF)은 외교부 주최로 미국의 대표적 중립적 싱크탱크인 신미국안보센터(CNAS) 및 KAIST 과학기술정책대학원이 함께 개최함.

- 최근 생성형 AI 기술의 급속한 발전과 함께 AI 기술의 군사적 사용 위험이 국제안보 이슈로 대두됨에 따라 미국, 영국을 비롯한 주요국은 AI 관련 국제규범 개발에 앞장서고 있는 바, 본 포럼에서는 과학기술의 안보화 추세 속에서 한국이 신기술의 무기화에 대응하는 글로벌 협

력과 공조를 선도할 수 있는 방안을 모색함.

- 주제 : 사이버공간과 신기술의 안보 위협 대응을 위한 글로벌 협력 강화(Advancing global cooperation in response to security threats in cyberspace and new technologies)
- 일시 및 장소 : 2023. 12. 5(화), 9:00 ~ 16:30, 그랜드 하얏트 서울, 그랜드볼룸
- 동 포럼에 관한 보고는 별책에 수록함.

그림 26 : 세계신안보포럼
라운드테이블 모습



부록 1

국내 전문가 주요 자문 내용

〈한국국방연구원 국방데이터연구단 국방정책AI연구센터 심승배〉

1. 국방 분야 인공지능 연구개발 및 활용을 위한 제한점은 무엇인가요?

- 기존 법령의 하드웨어 중심의 무기체계 연구개발 또는 구매 절차는 인공지능과 같은 소프트웨어 연구 추진을 위한 제도가 부재함.
 - 국방전력발전업무훈령에서 제시하는 소요제기서의 형태에 군사요구도(ROC: Required Operational Capability)가 특정 기준 제시가 필요하므로 신기술은 이를 맞추기 어려움.
 - * 전차 사거리 00km, 항속거리 000km vs. 인공지능 임무 성공률 00 % 등(국방전력발전업무훈령 별지 제10호 참조)
 - 현재 국내 방위산업 추진이 최선의 무기체계 획득보다는 투명한 사업관리에 중점이 맞춰져 빠른 속도의 기술개발에 제한이 있음.

2. 국내 민간분야 AI의 발전상황과 이에 대한 국방분야 적용 가능성에 대해서는 어떻게 생각하나요?

- 국내 AI 업계는 초거대 AI 모델을 바탕으로 빠른 속도로 개발 중, 초거대 AI는 중국·미국에 이어 3위, 전 분야 또한 7~8위 판단
- 선행되어야 할 국방 관련 데이터의 비밀 또는 공개 등급 불분명, 이로 인한 데이터 분류 제한으로 빅데이터 구축의 전제조건 미달성
- 군대 내 폐쇄적인 보안환경으로 민간을 선도하는 것 뿐만 아니라 따라가는 것 또한 어려운 상황 --> Data Lake에서 Data Fabric(데이터 위치기반 공유)으로 개념 진화 중

3. 국제 수준에서의 AI 발전 동향과 우려되는 점은 어떤 것이 있을까요?

- 기존 법령의 하드웨어 중심의 무기체계 연구개발 또는 구매 절차는 인공지능과 같은 소프트웨어 연구 추진을 위한 제도가 부재함.
 - 미국의 AI 관련 박사급 인력 대다수 사기업 시장으로 이동하고 있고, 한국은 계약학과, 국방과학기술 사관학교 등으로 인력 획득을 추진하고 있으나 필요인력에 비해서는 낮은 수준임.
- 반면, 러시아-우크라이나·이스라엘-하마스 전쟁 등에서 공격권의 자율성을 가진 AI 기반 무기체계의 출현이 우려됨.

- 하마스의 거대 땅굴을 이스라엘군이 적탐지 및 사격 기능을 가진 무기체계를 이용하여 수색 중일 것이라 의심됨.

● AI 관련 국제규범 또는 군비통제가 시행되기 전, 주요행위자 자격을 갖추기 위한 기술개발이 필수적임.

- NPT와 같이, 미국이 빠른 속도로 기술을 개발한 이후 경쟁국의 개발을 제한하려 할 경우를 대비해 유사수준의 기술 확보가 필요, 이를 위해 Fast-Follower 전략으로 한국 AI 기술 발전이 요망됨.

4. 기타 의견

- 한국군은 징병 가능 인구 감소로 자율화·자동화가 피할 수 없는 만큼 인공지능 기술의 도입이 필요함.
- 국가계약에 대기업의 소프트웨어 분야 참여는 기술력으로는 큰 차이가 없을지 몰라도 사업관리 분야에서 안정성을 보일 것으로 기대함.

* 참고 : 국방전력발전업무훈령 별제 제10호

■ 국방전력발전업무훈령 [별지 제10호서식] <개정 2022. 3. 18.>

소요제기서(00품목)

1. 사업개요

2. 필요성
가. 현실태 및 문제점

3. 편성·운용개념
가. 용도
나. 편성
다. 운용개념

4. 소요기준 · 소요량
가. 총 소요량
나. 소요기준

5. 전력화시기

구분	기획 소요	중장 목표	F	국방중기계획 대상기간						F+6 이후
				계	F+1	F+2	F+3	F+4	F+5	
수량()										
금액(억 원)										

6. 군사요구도와 기술적·부수적 성능

가. 구성(항상)

나. 세부내용

구 분	요 구 성 능	선 정 근 거
군사요구도		
기술적·부수적 성능		

7. 전력화지원요소

8. 비용 대 효과분석

9. 획득방법(안)

10. 선행연구 필요성

11. 소요제기 부서 및 담당자

210mm×297mm[백상지(80g/㎡)]

〈육군사관학교 AI데이터과학과 권현 교수,
인하대학교 AI·데이터법센터 이상우 책임연구원〉

1. (사이버 안보) 국방 분야의 사이버 안보를 위한 현 주요 정부 전략의 핵심과 거버넌스 현황에서의 맹점은 무엇이라고 생각하십니까?

- 현재 거버넌스의 맹점은 사이버 안보 기본법제 미비로, 사이버 안보와 AI를 통할하는 국가 차원의 컨트롤 타워 구축 필요
 - 사이버 안보 기본법제 입법의 난항, 다수의 인공지능법안 논의 중, 딥페이크 등 기술에 기반한 AI 콘텐츠 가짜뉴스의 증가로 국가 안보 위협이 증가 중, 대통령 직속 국가인공지능위원회(가칭)을 신설하여 파편화된 사이버 보안 지휘 체계를 통합하고, AI에 관한 외교 경제 안보 이슈를 통할할 수 있는 명실상부한 국가 컨트롤 타워 설립
- 현재는 부처별로 사이버 안보 이슈에 대응 중이나 국가 차원에서 효과적으로 대응할 수 있도록 통합할 필요가 있음. 국방 분야의 특성상 과도한 보안 규제로 인해 연구 추진을 저해함.

2. (AI) AI의 개발과 사용에 대한 잠재적 위험을 고려하고 윤리적 원칙을 구체화할 수 있는 국방부의 주요 이니셔티브에 대한 의견은 무엇입니까?

- AI 기술의 윤리적 문제를 다루기에 앞서 전제 조건인 기술 자체의 성숙도가 낮은 단계임. 현재 국방부의 AI 수준은 적용 및 활용할 수 있는 단계에 못미치며, 이를 위한 데이터 수집 및 관련 시스템 구축을 진행하는 단계임. 우선적으로 AI 활용을 위한 데이터가 필요하므로 현재 국방부에서 AI 데이터센터를 설립하고 데이터 구축과 활용 방안에 대해 논의 중임.
- 선제적으로 윤리적 원칙을 높여 한국 스스로 기술 개발의 장벽을 세우는 우를 범하지 않도록 유의할 필요가 있음, 국제협력이라는 명목 아래 해당 기술을 제한하는 규제 조약 추진 시 우리에게 득과 실이 무엇인지에 대한 명확한 분석 필요

3. (데이터) 해외 주요국의 국방 데이터 확보 및 보호 경쟁 전략 대비 국내 전략의 차별점과 보완 사항은 무엇이라고 생각하십니까?

- 기존의 규제 ICT·샌드박스를 데이터 개인정보 분야로 확대하여 국방 분야에서 원본데이터(개인정보)를 그대로 학습할 수 있는 ‘국방 데이터 규제 샌드박스(가칭)’ 도입 고려를 제안

- 해외 주요국의 국방 데이터 확보 및 보호 경쟁에서 그 차이를 좁힐 수 있는 현실적인 보완책으로 활용 가능

- 클라우드 환경 전환을 대비한 데이터 보호 정책 수립과 한국어 기반의 텍스트 음성 데이터 등에 대한 독자적인 기술 필요, 선부른 규제 도입과 윤리라는 명목하에 기술 발전을 저해하면 안될 것

4. (국제협력) AI 및 신기술을 적용하는 군사 안보 측면에서 국제협력을 주도하기 위한 방안과 주안점은 무엇이라고 생각하십니까?

- 균형 잡힌 시각을 바탕으로 한국이 양분된 국제협력 거버넌스의 연결고리 역할 담당 필요, 미국을 중심으로 한 국제협력에 참여함과 동시에 중국을 위시하는 국제협력 체계의 동향도 쫓는 커뮤니케이션 채널 유지 필요
- 국제협력을 주도하기 위한 독자적인 기술 보유와 이를 전폭적으로 지원해주는 정책의 정착화 필요, 궁극적으로 AI 관련된 방산업체까지 연계하여 수출까지 선순환 구조 마련 필요

5. (기타 의견)

- 우려될 수 있는 투명성을 제고하기 위해서 대통령 직속 국가인공지능위원회(가칭)의 기본계획 및 주요 정책, 예산 등과 관련하여 국회의 관리 감독을 받는 체계 수립이 필요함.
 - AI 분야의 핵심·원천기술 확보를 국방력 강화라는 관점에서 바라보고 기술개발을 지원할 수 있는 환경 조성 및 민관군이 함께하는 유기적인 거버넌스 구축 고려
- 범용기술 중 국방 분야에 AI가 적용될 수 있는 영역을 명확히 하여 해당 기술의 규율에 있어서 안보 공백이 발생하지 않도록 하는 노력이 뒷받침되어야 할 것임.
- 정책을 수립할 때 민관군이 함께 국가 역량을 한 곳에 집중할 수 있는 워킹그룹 설립과 실효성 확보 필요
- AI를 활용한 의사결정 시 오판할 가능성이 있기 때문에 사람의 개입이 반드시 필요, 관련해 AI 활용 및 서비스를 위한 명확한 평가 기준, 가이드라인이 필요함.

〈강원대학교 정치외교학과 정구연 교수〉

1. (AI) AI의 개발과 사용에 대한 잠재적 위험을 고려하여 윤리적 원칙을 구체화하는 것이
필요한 상황에서 이러한 맹점을 극복하기 위한 한국의 주요 규제 이니셔티브는 무엇입
니까?

● 현재로서는 없으며 사실상 AI 기술 역량의 국가별 편차로 일괄적인 글로벌 규제 이니셔티브를 마련하기는 한계가 있음. 다만, 국가별 역량과 규제 방향이 유사한 입장국들 사이에 서만 소다자협력 수준으로 나타날 것

- REAIM을 비롯한 공동의 원칙, 군비통제 형식의 합의 등이 장기화 될수록 기술 발전과 규범 제정 속도 사이의 격차가 커져 규제 조항에 관한 합의를 도출하기는 어려울 것으로 전망됨.

● 한국의 경우 지정학 특성상 북한, 중국, 러시아로부터 다층적 군사 위협에 노출되어 있기 에 이러한 위협에 각각 AI가 접목될 상황과 그로부터의 위협을 모두 예측한 규제 방안을 마련할 필요가 있음.

- AI의 일반적 위험: AI의 자율성 범위와 그로부터 노정되는 불확실성
- AI와 군사적 위험: 전투 속도의 배가, 역량과 의도에 대한 오인(misperception), 전장 및 위 기고조 과정에 대한 인간의 통제 약화, 비국가 행위자로의 AI기술 확산 등
- AI와 핵 위험: 선제공격 유인 확대, 우발적 위기고조, 군비경쟁 등

● AI 기술 역량에서의 소통이 가능한 국가들과의 협의체제 신속 가동, 유사입장국(공동군 사훈련 실시 동맹국 및 파트너 국가들)과의 소다자협력을 통해 예측 가능한 위험성을 줄 이며 최소한의 규제에 대한 합의 노력 필요

- AI 기술 역량 기반 소통 가능 국가간의 협의 단계 제시: ① 규제에 관한 분야별 모범사례 공유, ② AI 역량과 진화 수준/경로에 대한 정보 공유, ③ 지속적인 규제 방안 마련, ④ 수출통제 방 안 모색, ⑤ 군비통제 단계로의 진화

2. (국제협력) AI 및 신기술을 적용하는 군사 안보 측면에서 국제협력을 주도하기 위한 방안 과 주안점은 무엇이라고 생각하십니까?

● 강대국 경쟁 국면에서 독자적인 영향력을 낼 수 있는 영역 식별과 자국의 영향력을 높이 기 위한 실질적인 협의체 운용이 중요

- 최근 전세계적인 AI 거버넌스 회의 개최는 사실상 규제 창출 보다는 정치적 입지 공고와 첨단 기술 개발과 규제를 선도한다는 리더쉽 보여주는 일환(미국의 경우 자국법을 수정하지 않

는 수준에서 AI 규제조치 주장 중)

- AI 및 주요 신기술은 글로벌 기술패권 경쟁의 핵심 요소이며 이에 따라 AI 전략과 규범, 안전 조치 마련도 역시 경쟁의 요소가 되는 것이 사실이며, 동시에 글로벌 차원의 위험을 줄이기 위한 실질적 규제조치에 대한 국가간의 합의도 필요. 이에 따라 두가지를 해결하기 위한 민 관협의체 필요
- 국가 차원에서 외교부, 국방부, 과기정통부, 산업부 등 유관 부처와 다양한 이해관계자가 참 여하는 형식의 협의체 설립 필요

● AI-driven defence supply chain(군수 공급망)에 대한 선점 필요

- 현재 탄력적인 군수 공급망 운용이 원활하지 않으며 이러한 물리적인 무기공급 뿐만 아니라 AI 차원으로 확장되었을 때 보안체제의 문제까지 연계됨.
- AI는 군수 공급망의 효율성과 정확도를 향상시킬 뿐만 아니라 실제 무인항공기, 자율주행차 량, 사이버 전쟁에 있어서도 중요한 역할을 수행함.
- 군수공급망 차원에서의 AI 활용과 적용에 관한 논의를 한국이 선점해야 할 필요가 있음.

부록 2

국내 전문가 라운드테이블 상세 내용

WESF 라운드테이블

■ 행사 개요

- 행사 주제: 신안보위협 미래와 해법: 사이버, 인공지능을 중심으로
- 일시 및 장소: 2023.09.15.(금) 10:30~14:40, 포시즌스 호텔 서울
- 구성: 개회식, 세션 1·2

- 세션 1 주제: 생성형 인공지능의 세계안보적 함의
- 세션 2 주제: 사이버해킹과 사이버안보의 미래

* 주요 참석자(발표·토론): 박용민 외교부 다자외교조정관, 이승섭 KAIST 안보·대외협력 자문역, 윤정현 국가안보전략연구원 신흥안보연구실 부연구위원, 조상근 KAIST 국가미래전략기술정책연구소 연구교수, 차정미 국회미래연구원 국제전략연구센터장, 안성원 소프트웨어정책연구소 AI정책연구실장, 송윤선 국민대학교 정치대학원 겸임교수, 김용대 KAIST 정보보호대학원 교수, 박춘식 아주대학교 사이버보안학과 교수, 손광수 KB금융지주경영연구소 북한연구센터 연구위원, 조은정 국가안보전략연구원 국제질서연구센터장, 임종인 고려대학교 정보보호대학원 석좌교수

■ 주요 내용

● 개회식

- 1) (개회사: 박용민 외교부 다자외교조정관) 국가에 대한 사이버 공격 위협의 다양화, 증대, 진화가 지속되고 있음. 특히 최근의 생성형 AI의 빠른 진화를 비롯한 첨단 기술의 빠른 발전으로 안보적 리스크에 대한 이해와 규범에 대한 국제적 논의가 시급해짐. 이에 따라 한국 정부는 지난 2월 ‘인공지능의 책임있는 군사적 이용에 관한 고급회의’를 네덜란드와 공동 주최하고, 추후 2차 회의를 한국에서 개최할 것임. 또한 내년부터 안보리 비상임 이사국으로서 사이버 안보를 안보리에서 중점 의제로 다룰 예정이며, 올해 12월 개최 예정인 제3차 세계신안보포럼에서 사이버 신기술과 국제안보에 대한 국제사회의 논의 진전에 기여하고자 함. 제 3차 포럼의 주요 주제로는 사이버, AI 등 신기술 관련 신안보 위협을 다룰 예정이며 미국의 싱크탱크인 신안보센터와 카이스트와 협력하여 준비 중임.
- 2) (축사: 이승섭 KAIST 안보·대외협력 자문역) 챗GPT의 확산 및 발전으로 가장 혁신적인 디지털 전환을 야기했지만 신종 사이버 공격 알고리즘 등 첨단 과학기술의 발전에 따른 다양한 안보 이슈 확산과 국제정치의 불확실성을 심화시킴. 따라서 첨단 과학기술과 국제 공조가 교차하는 현 상황에서 외교부와 카이스트가 함께 라운드 테이블 행사를 마련했다는 점이 뜻깊음.

● 세션 1

1) (발표: 윤정현 국가안보전략연구원 부연구위원) 생성형 AI의 세계안보적 함의

- 인공지능과 국가안보:

- ① 인공지능의 지속적인 주목 이유: 4차 산업혁명과 디지털 전환을 주도하고 있는 인공지능의 범용적 파급력, 경제·사회 분야 뿐만 아니라 미래전의 양상을 바꾸는 군사혁신의 기반, 고도화된 정보심리전의 공격과 방어를 위한 핵심 수단, 미·중의 인공지능 기술혁신과 안보적 활용을 위한 갈등 심화, 경쟁의 진영화
- ② 안보 관점에서의 중점 사항: 급속히 진화하는 인공지능 기술 혁신이 초래하는 위협의 변화와 신흥안보적 의미, 하이브리드전 시대의 진화된 인공지능 공격이 갖게 될 공간초월적 파급력, 기술지정학 측면에서의 제약과 한국적 맥락의 의미
- ③ 진화된 인공지능의 미래 위협 대응을 위한 초점: 생성형 AI 시대의 전사·비전시 위협 발생 시나리오 및 부문별 파급효과 전망, 주요국 정부 및 정보기관의 대응 동향과 기술·제도적 시사점 진단, 글로벌 AI 거버넌스 의제 주도과 국익 확보를 위한 방향 탐색

- 생성형 AI의 부상과 진화적 의미

- ① 생성형 AI의 개념과 진화적 특징: 생성형 AI는 기존 콘텐츠 정보를 토대로 텍스트, 이미지, 음악, 영상 등 사용자가 요구하는 형태의 새로운 콘텐츠를 창작하는 AI 모델로 기능적 측면(데이터 학습을 통한 또다른 결과물 생성)과 활용적 측면(인터페이스의 혁신체)에서의 진화 중
- ② GPT 모델: 생성가능한, 사전 학습된 거대언어모델(LLM)로서 많은 데이터를 학습하고 단어 간 연관성 파악이 가능한 혁신적 심층신경망 모델임. 주로 크롤링 방식으로 데이터를 수집하거나 데이터셋으로 구축해 스스로 지속적 학습 수행함. 생성형 AI 모델은 분석형 인공지능과 비교 시 다차원·복합 문제해결에 적합하며 결과의 다양성과 활용 용이성을 갖고 있으나 높은 데이터 편향 가능성과 예상 결과물의 불확실성을 갖고 있음.

- 생성형 AI의 한계와 안보 리스크

- ① 진화된 생성형 AI의 주요 한계점: 편향성과 데이터 지체에 따른 환각, 불완전한 기술발전 단계에 있는 생성형 AI의 한계점들, 상시적 Prompt Hacking 위험성
- ② 국가 안보 차원의 부정적 파급력: 영향공작/ 악의적 시도에 따른 거짓·유해 정보 제공, 국가가 통제·주도하는 정보심리전의 고도화된 무기로의 활용 가능성, 사이버 공격의 고도화 수단
- ③ 생성형 AI의 보안이슈가 초래하는 국가안보 위협 발생요소
- ④ AI의 의사결정 가능성 증대와 우려 사항: 국방 분야 적용 확대의 난제였던 ‘의사결정’ 역할로의 진일보 가능성, 생성형 AI 및 인공 초지능 등의 규제 여부

- 생성형 AI 시대의 안보위협 전망

- ① AI 기술성숙도 측면에서 본 단기·중장기 위협 가능성 고려: 가트너의 하이프 사이클에 따라 생성형 AI로 인한 위협들을 장단기 차원의 국가 안보 차원에서 대응 고려 필요

- ② AI가 가진 범용적 측면과 신형파괴적 측면 고려: AI의 광범위한 활용 영역과 전력화 시 AI의 책무성을 은폐할 수 있는 가능성 존재
- ③ 미중 경쟁 시대의 정치안보적 쟁점 및 수단화 고려: 지정학 갈등 구도를 심화시키는 군사안보적 무기로 활용되는 AI, 정보기관의 영향력 공작, 심리전, 방첩활동에 적극 도입되는 AI
- ④ 차세대 보안 패러다임 전환 과정에서의 불확실성 고려: 진화된 AI 모델에 기반한 사이버-물리공간의 결합과 대응체계 변화, 생성형 AI 모델을 활용한 보안체계 변화와 선제적 대응
- ⑤ 생성형 AI에 대한 통제와 규범의 차이 고려: AI의 군사적 책무성 적용에 따른 간극을 어떻게 조정할 것인가가 문제이며, AI 신뢰성에 대한 국가별 입장차로 인해 비대칭적인 활용도가 나타남
- ⑥ 평시 생성형 AI 기반 치명적 유해 알고리즘의 파급효과 시나리오(단기)
- ⑦ 준전시 생성형 AI 기반 물리적 피해 가능성과 군사적 충돌 시나리오(중장기)

그림 27 : 생성형 AI의 한계와
안보 리스크

취약점	촉발 경로	예상 피해
AI 모델 악용	- 적대적 시스템 메시지	- 유해한 답변과 오인식 만연 - 가짜뉴스로 인한 비이성적 여론형성과 사회적 혼란, 잘못된 의사결정 유도
유사 AI 모델 서비스 방자	- 유사 악성 서비스 접근 유도	- 신뢰할 수 있는 AI이름을 도용한 스쿼팅 URL, 가짜 앱 등을 통해 개인정보 대량 유출 가능
데이터유출	- 데이터 합성 과정의 문제 - 과도한 훈련 데이터 암기 문제 - 대화 속 개인정보 등 민감정보 작성	- 민감한 훈련 데이터나 기밀 유출 - 데이터베이스 해킹 시, 과거 이용자 중 주요 대상에 대한 표적 추론공격도 가능
플러그인 취약점	- AI 모델의 적용 범위 확장 - 안정성 확인 미흡 - 해커 공격 범위 확장 - 취약점이 있는 서비스와 연결	- 에이전트화된 AI를 악용한 악성코드 전파 - 새로운 도메인에서의 모델 오작동 유도 - 취약점 서비스와의 연결을 통한 해커의 공격 범위 확장
확장 프로그램 취약점	- 확장 프로그램 내 악성서비스 설치 - 서비스 제공업체의 보안조치 미흡	- 사용자 권한을 남용한 사용자시스템 공격 - 대량 좀비PC 생성 및 DDos 피해 발생 - 호스팅 서버 및 스토리지 시스템 위협
API 취약점	- 미흡한 API 키 관리 - 제어불가한 악의적 프롬프트 주입	- 인증수단 약화로 데이터 및 시스템 보안 피해 - 유해 알고리즘, 불법적 무기제조 설계 등

- 시사점 및 제언

- ① AI의 정치안보 무기화에 따른 비대칭적 위협 경감 수단 필요: 진화된 AI가 제기하는 신종 위협에 대한 능동적 대응 인프라/기반 마련 필요, 편향성과 환각 등 AI의 구조적 한계점 보완을 위한 데이터 활용 기준 개선
- ② 생성형 AI의 불확실성에 대응하는 민관협력 및 인간/ 기계협업 구조의 안착: 생성형 AI의 안전한 이용 인증 및 장기적 연구지속을 위한 민관협력 대화체 수립, 인간/기계협업 구조를 보장하는 제도적 원칙과 환류체계 마련
- ③ 진화된 AI 제기하는 글로벌 안보 도전에 대응하는 거버넌스 논의 주도: 국제 규범 적용을 위한 쟁점 분야의 주체범위, 기술수준에 대한 면밀한 검토 필요, 산업 진흥과 사용자 보호, 국가안보적 논리를 종합적으로 고려한 국제공조 의제 발굴
- ④ 사회공학적 영향력을 최소화하는 국민 차원의 ‘윤리 방화벽’ 필요: 사회 구성원의 AI 문해력 강화 및 올바른 생산/ 활용 준수 가이드라인 마련, 인간과 AI와의 건강한 공존을 위한 기본원칙 및 윤리강화 교육 확대

그림 28 : 생성형 AI 시대의
안보 위협 전망 1

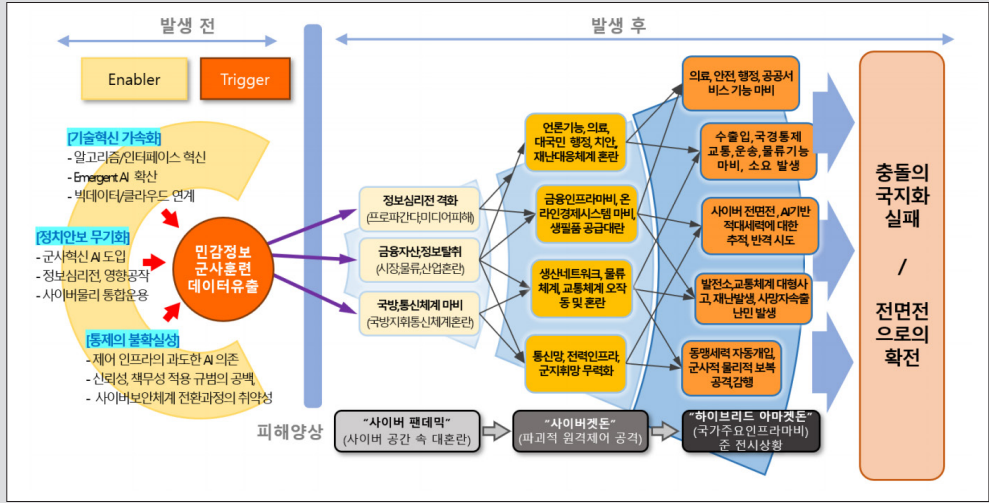
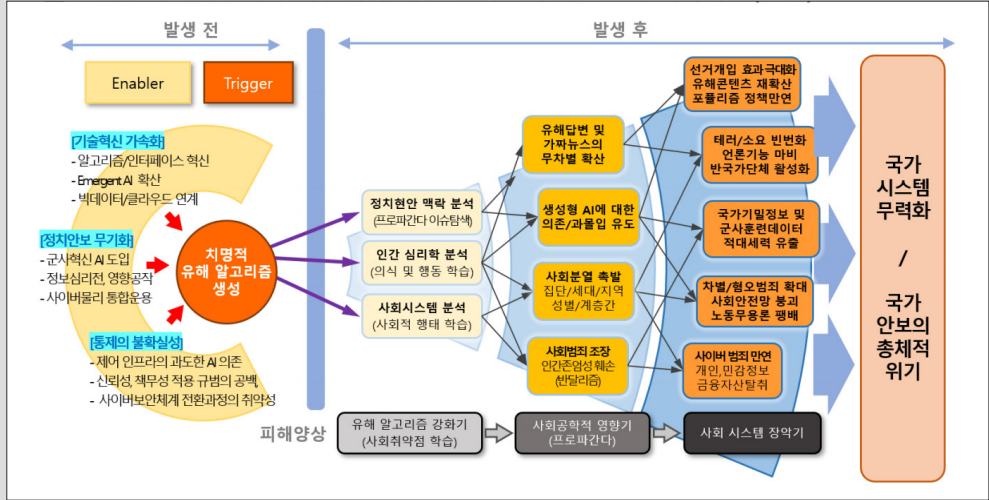


그림 29 : 생성형 AI 시대의
안보 위협 전망 2



2) (토론/ 좌장: 송윤선 국민대 교수)

- 조상근 KAIST 연구교수

- ① 안보적 측면에서 생성형 AI 사용 시 통신 위성 보유의 중요성: 발표에서 언급한 빅데이터의 편향성 보다는 실시간 정보 수집의 통합 및 융합을 통한 좌표화 및 정밀 타격 조준이 상대적으로 더 중요(전쟁의 AI 적용 사례: 우크라이나의 IT 통합 플랫폼을 통한 적진의 위치 파악, 자폭 드론 및 정밀 타격 등)
- ② 인공지능 윤리의 필요성과 국제적 합의의 필요성: 국내에서의 윤리 기준 수립이 가이드 수준이기에 법적 구속력도 있지 않으며, 권위주의 국가의 경우 정치적 목적을 위해서는 고려할 가능성이 낮으므로 국제적인 합의를 통한 수립이 필요하며 무엇보다 각 기술적 특성에 맞는 AI 윤리 및 보완책 수립 필요

- **차정미 국회미래연구원 국제전략연구센터장**: 생성형 AI로 인해 새로운 국제 질서와 안보 위기를 불러올 수 있으며, 복합 안보 위기라고 불리는 기술과 가치규범, 군사, 외교, 글로벌 리더십 경쟁을 구체화하고 심화시킬 수 있다고 생각함.

주요국에서는 생성형 AI를 안보 측면에서 기술패권을 유지하는데에 핵심이 있음.

- ① 최근에 중국이 생성형 AI 서비스 관리 잠정 방법을 지난 8월부터 실시하고 있는데 해당 문구를 보면 여러가지 복합 안보 경쟁의 구조를 그대로 담고 있음. 우리는 해당 잠정 방법을 규제 조치라고 하지만 규제 조치는 아니며 혁신안에 가까움. 국내 수요자들에게 국내 서비스를 하는 업자들에게만 규정하며 대중 대상이 아닌 경우에 어떠한 것도 규제하지 않게 되어 있음. 즉, 중국은 생성형 AI가 어떻게 공산주의를 수호하면서 기술 혁신을 주도할 수 있는지 이 두 가지 고민을 다 담고 있음. 중국이 글로벌 리더십 경쟁, 기술 안보 경쟁, 가치 규범 경쟁을 주도하겠다는 의지를 담고 있음. 또한 국제적으로도 브릭스 협력, 중·러 AI 협력 등 의지를 표명함. 결론적으로 중국 주도의 자치 기술 생태계를 모색 중임.
- ② 미국 또한 기술 패권 전략이 명확하고, 유럽은 최근에 규범 주도로 하겠다는 의지가 굉장히 명확함. 따라서 향후 복합안보 위기, 가치 규범 경쟁 등이 강화될 것으로 예상됨. 그래서 생성형 AI 안보를 논할 때 우리의 안보는 어디에 방점이 있고, 그러면 우리는 어떤 것을 지켜야 하기 때문에 어떻게 안보 전략을 구성하고, 어떻게 외교 전략을 구성해야 되는지에 대한 한국식 생성형 AI 시대의 안보 외교 전략 필요

- **안성원 소프트웨어정책연구소 AI정책연구실장**: 국제사회의 냉엄한 현실에 따라 AI가 군사적인 목적으로 활용되는 경우가 굉장히 많음. 이에 따라 AI 오남용 방지 측면에서 안보 전략 및 정책 방향을 크게 두 가지 차원에서 제시

- ① 국가 차원의 기술 확보 필요: AI 기술은 우리나라가 기술력을 확보하지 못하면 글로벌 사회에서 도태될 수밖에 없는 핵심적인 기술임. AI 기술을 확보하기 위해서는 반도체, 클라우드를 비롯한 인프라 단의 기술을 확보할 필요가 있음. 특히 우리나라는 반도체의 제조 측면에 강점이 있으므로 장중단기의 R&D 체계를 면밀히 검토하고 대중소기업의 컨소시엄을 국가차원에서 지원할 필요가 있음. 또한 다양한 시행착오를 겪어볼 수 있는 플레이그라운드를 마련, 규제 완화 등 전체적으로 생태계 확장 필요
- ② 기술 신뢰성 확보: G7 정상회담에서도 성명문을 통해 법적 구속력을 갖는 프레임워크를 만드려는 움직임이 있지만 윤리적 강조가 현실 세계에서는 사실 비현실적이고 비합리적인 선택이 될 수도 있음. 기술의 완성도 측면과 고도화 측면, 에러 레질런스 측면의 완성을 위한 신뢰성을 높이는 여러 가지 법적 제도 및 장치 마련 필요

- **청중 질문 1**: 첨단 기술을 선점하기 위한 국제적 주도권 확보 경쟁 상황에서 우리가 어떤 논의를 주도해 나갈 수 있겠는가? 즉 AI를 비롯한 첨단 기술들을 우리가 빠르게 발전시키면서도 우리에게 유리한 식으로 어떻게 발전을 주도할 수 있는지?

- **청중 질문 1 답변(윤정현 발표자)**: AI의 활용에 있어서 알고리즘 뿐만 아니라 구현하는 이 동통신, 반도체 등이 매우 긴밀하게 연결되어 있음. 따라서 그것을 구현하는 역량을 키워 지렛대로 활용 필요. 특히 미중의 기술패권 상황이 신흥 기술의 육성에 있어서 기회적 측면도 있다고 생각함. 예를 들어 공급망 재편 과정에서 중국 의존도를 낮출 수 있었고, 우호국과의 동맹을 통해 대안적 네트워크를 확보하게 됨. AI 뿐만 아니라 양자 과학 기술 같은 경우도

한·미, 한·미·일 정상회담에서 언급된 바와 같이 대단히 전략적인 협력이 가능한 것으로 정책 결정자들의 서포트를 받을 수 있는 여지가 있음.

- **청중 질문 2**: 생성형 AI와 같은 급진적 AI 기술이 안보 위협을 가하고 있는데 그것을 통제하기 위해서 국제적 차원의 지침이나 규범이 만들어진다면 정부, 기업, 시민사회 등 다중 이해관계자들이 이를 준수할 수 있도록 할 수 있는 요소는 무엇인가? 예컨대 글로벌 시장 점유 그리고 이윤 창출 이런 것이 목적인 빅테크 기업들을 위한 인센티브나 패널티를 포함할 수 있겠는가?

- **청중 질문 2 답변(윤정현 발표자)**: 지금 현재 유럽 같은 경우에는 EU AI ACT에서 패널티를 강제 중임. 생성형 AI에 대한 인증 표시를 확실히 하지 않을 경우 수익금의 2%를 벌금으로 받거나 아니면 천억 유로 혹은 천만 유로를 부과하는 중임. 미 정부 역시도 안보적 측면에서 AI에 대한 규제와 통제의 필요성을 인식하고 있고, 빅테크 기업들이 관련 내용을 준수하길 원함. 따라서 빅테크 기업들이 갖고 있는 기득권을 어떻게 통제할 것인가에 대해서는 유럽 차원 뿐만 아니라 정부 차원의 협력 보다 필요

- **청중 질문 3**: 생성형 AI의 발전에 따른 리스크에 대한 협력이 필요하다는 원론적인 수준의 합의가 국제사회에서 논의가 제기가 되고 있으며 그럼에도 불구하고 서구에서 생각하는 AI 생태계 인식과 중국의 인식이 다름으로 인해서 진영화가 심화될 가능성에 대해서 말씀해주셨음. 그럼에도 불구하고 협력이 진행이 돼야 한다고 한다면 가장 먼저 협력이 진행될 가능성이 가장 높은 그 스타팅 포인트가 어디라고 생각하시는지?

- **청중 질문 3 답변(윤정현 발표자)**: 근 미래에 발생 가능한 허위 조작, 허위 정보에 대한 악영향을 미국과 EU 공통적으로 고위험 AI 리스크로 분류함. 허위성에 대한 신뢰성을 정부가 담보하기 위해서 인증 방법을 실행할 수 있을 것으로 고려됨.

- **청중 질문 3 답변(차정미 토론자)**: 생성형 AI는 오픈소스 등의 운영 형태로 인해 국가가 통제하지 못하는 단계가 올 것으로 예상하며, 그것이 글로벌 위기라는 인식이 팽배해질 경우 국가간의 협력이 가능할 것으로 고려됨.

● 세션 2

1) (발표: 김용대 KAIST 정보보호대학원 교수) 사이버해킹과 사이버안보의 미래

- **해킹의 이해**:

- ① 해킹의 발생 이유: 가장 큰 이유는 패치되지 않은 혹은 앞으로 영원히 패치되지 않을 취약점들이 굉장히 많기 때문임. 인간이 프로그램을 개발을 하기 때문에 인간은 실수로 많은 취약점들이 나타남. 디지털 트랜스포메이션에 따라 새로운 애플리케이션들이 새로운 플랫폼에 구현되며 새로운 보안 취약점들이 계속해서 나타나고, 그에 따른 해킹이 계속 일어남.

- ② 해킹의 트렌드 변화: 다층 방어를 나타내는 제로 트러스트가 떠오르고 있으며 공급망을 공격하는 경우가 많아지고 있음. 따라서 미국 및 우방국들과의 공조가 필요하며 이에 따른 우월 기술이나 정보 보유가 필요한 현황
- 신기술의 과거 보안 문제: 신기술 개발자의 보안에 대한 이해 부족, 표준에서 보안의 고려 필요, 설계상의 문제점 개선 필요, SDL 등 개발 프로세스 개선, 기존 보안 취약점에 대한 점검 필요
- 신기술의 신규 보안 문제: 5G 표준화가 거의 다 진행된 시점임에도 지금까지 패치되지 않아 발생하는 많은 설계 취약점 존재
- 결론: 모든 ICT에서 보안은 핵심이며 기술의 발전에 따라 취약점도 많아짐. 따라서 보안의 플랫폼 내재화가 필요하며, 기술의 중립성에 따라 공격과 수비 기술 모두 중요함. 또한, 표준에서의 보안 요소 고려 필요

2) (토론/ 좌장: 임종인 고려대 교수)

- 조은정 국가안보전략연구원 국제질서연구센터장: 단순한 보안 문제가 아닌 국가 이니셔티브 차원의 안보 문제로 고려됨. 최근 미국에서 발표된 사이버 전략이 기존의 사이버 안보 전략에서 국가 전략으로 한 레벨 승격화된 것을 살펴 볼 수 있음. 영국 또한 격상한 사례가 있음. 해당 전략의 공통점은 신기술의 등장과 빠른 발전으로 개인의 보안 문제가 아닌 국가 시스템을 위협하는 세계적 안보 문제로 격상. 국가 사회적 기반의 인프라 공격 시 국가 전체의 섣다운 야기 가능
- 손광수 KB금융지주경영연구소 북한연구센터 연구위원: 한국은 정보화 국가로서 사이버 기술을 기반으로 한 행정 서비스와 인프라를 갖추고 있으나 이러한 발전은 사이버 공격의 위험을 증가시켰음. 북한은 사이버 공격을 주요 대남 도발 수단으로 활용하고 있음. 특히, 최근에는 가상자산 탈취를 통해 외화벌이를 목적으로 하는 공격이 증가하고 있음. 이러한 북한의 사이버 공격은 단순한 금융 범죄를 넘어 안보 위협으로 인식되고 있음. 이에 따라 한미일 3국은 사이버 안보 협력을 강화하고 있음. 또한, 사이버 공격은 국경을 초월하기 때문에 국가 차원의 단독 대응으로는 한계가 있음. 따라서 국제 사회의 협력이 필요하며, 사이버 공격에 대한 국제적 법적 구속력을 마련하고, 각국이 공동 대응 체계를 구축하는 것이 중요함.
- 박춘식 아주대 교수: 한국은 사이버 안보 선진국이며, 정부 차원의 사이버 안보에 대한 관심과 노력을 기울이고 있지만, 아직도 부족한 점이 있음. 특히, 사이버 범죄 협약 가입, 사이버 안보 관련 인력 확충, 사이버 안보 역지력 강화 등의 분야에서 개선이 필요함. 사이버 범죄 협약 가입은 한국의 사이버 안보 역량을 강화하고, 국제사회에서의 위상을 높이는 데 도움이 될 것임. 사이버 안보 관련 인력 확충은 사이버 공격에 대한 대응 능력을 향상시키는 데 필수적임. 사이버 안보 공동 민관 전문가 포럼은 다양한 분야의 전문가들이 모여 사이버 안보에 대한 정책과 전략을 논의하는 데 도움이 될 것임. 사이버 공격에 대한 퍼블릭


어트리뷰션 강화는 가해자를 신속하게 식별하고, 그에 따른 책임을 묻는 데 도움이 될 것임.

- 청중 질문 1: 개인정보 수집과 관련하여 기업과 정부 간에서 과연 기업이 소유한 개인 정보를 정부에게 제공하게 되는지 정부의 권한과 기업의 개인정보 보호라는 권한 중에서 어떤 것이 더 우선하는지에 대한 논의가 굉장히 미비한 상황이라고 알고 있음. 특히 해당 기업과 정부가 다를 때(예를 들어 한국인 구글 사용자가 많은데, 미국 정부가 구글에게 한국인의 데이터를 요구했을 때) 한국인의 데이터가 미국 정부에게 들어갈 위험이 있기 때문에 외교적 취약점이 존재할텐데, 이에 대한 국가간 논의 사항이 궁금함.
- 청중 질문 1 답변(임종인 좌장): 구글은 멀티내셔널 기업이기 때문에, 단일 국가의 법률만으로는 이를 규제하기 어려운 실정이며 이러한 문제에 대한 해결책은 국가 간 협력과 국제기구의 역할이 필요함. EU 방식의 정부의 강한 드라이브 혹은 미국 차원으로 시장의 판단에 맡기는 것이 좋은지, 가이드라인을 만드는 것이 좋을지 여러 방안이 있겠지만 당분간은 명확한 대안이 없을 것으로 생각됨.
- 청중 질문 1 답변(박춘식 토론자): 국제간에 적용되는 GDPR과 같은 차원이 아니라 외교적 차원에서는 미국과 유럽간의 프라이버시 쉴드라던지 별도로 협약을 맺어 해결할 것으로 추측됨.
- 청중 질문 2: 사이버 분야의 고도화에 따라 과연 정부 조직이나 업체 같은 경우 실제 현장에서 어떻게 고도화 하는 것이 좋을지?
- 청중 질문 2 답변(임종인 좌장): AI 및 신기술을 통한 효율성 확보 필요(인력으로 모든 사이버 위협을 탐지하고 대응하기에 한계 존재), 추후 사이버 안보법이 통과될 경우 정부의 조직을 최신화하여 여러 가지 대응 태세와 능력 고도화 견인 가능할 것. 책임 강화 방식 도입 필요
- 청중 질문 2 답변(김용대 발표자): 포지티브 규제가 오히려 허점을 만들어 문제라고 여겨짐. 현재의 제도 자체가 투자에 대한 충분한 인센티브가 부재


부록 3

신기술 안보 관련 주요 국내외 보고서 목록

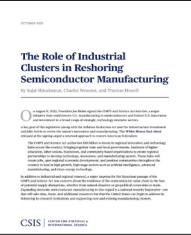
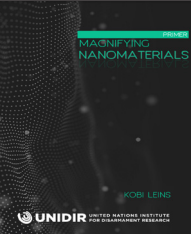
· 인공지능

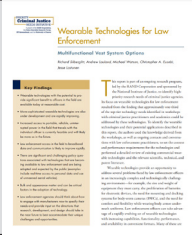
	Aarne, Onni, Tim Fist, and Caleb Withers. “Secure, Governable Chips,” CNAS, January 8, 2024.
	Bouey, Jennifer, Lynn Hu, Keller Scholl, William Marcellino, James Gazis, Ammar A. Malik, Kyra Solomon, Sheng Zhang, and Andy Shufer. “China’s AI Exports: Developing a Tool to Track Chinese Development Finance in the Global South — Technical Documentation.” RAND Corporation, December 11, 2023.
	Byman, Daniel L., Chongyang Gao, Chris Meserole, and V.S. Subrahmanian “Deepfakes and international conflict,” Brookings Institution, January, 2023.
	Gehlhaus, Diana, Ron Hodge, and Jonathan Rotner. “DOD’s Emerging Digital Workforce.” Center for Security and Emerging Technology, October 2023.
	Hicks, Marie-Laure, Ella Guest, Jess Whittlestone, Jacob Ohrvik-Stott, Sana Zakaria, Cecilia Ang, Chryssa Politi, Imogen Wade, and Salil Gunashekar. “Exploring Red Teaming to Identify New and Emerging Risks from AI Foundation Models.” RAND Corporation, October 31, 2023.
	Konaev, Margarita, Ryan Fedasiuk, Jack Corrigan, Ellen Lu, Alex Stephenson, Helen Toner, and Rebecca Gelles. “U.S. and Chinese Military AI Purchases.” Center for Security and Emerging Technology, August 2023.

	Lohn, Andrew. “Scaling AI.” Center for Security and Emerging Technology (blog), December 2023.
	Reinsch, William Alan, Emily Benson, Thibault Denamiel, and Margot Putnam. “Optimizing Export Controls for Critical and Emerging Technologies,” CSIS, May 31, 2023.
	Stokes, Jacob, Alexander Surlivan, Noah Greene. “U.S.-China Competition and Military AI,” CNAS, July, 2023.
	Menthe, Lance, Li Ang Zhang, Edward Geist, Joshua Steier, Aaron B. Frank, Erik Van Hegewald, Gary J. Briggs, Keller Scholl, Yusuf Ashpari, and Anthony Jacques. “Understanding the Limits of Artificial Intelligence for Warfighters: Volume 1, Summary,” RAND Corporation, Sep 23, 2022.
	Binnendijk, Anika, Timothy Marler, and Elizabeth M. Bartels. “Brain-Computer Interfaces: U.S. Military Applications and Implications, An Initial Assessment.” RAND Corporation, August 27, 2020.
	Scharre, Paul, Ainikki Riikonen. “Defense Technology Strategy,” CNAS, Nov 17, 2020.
	Muro, Mark, Maxim Robert, and Jacob Whiton. “Automation and Artificial Intelligence: How Machines Are Affecting People and Places.” Brookings Institution, January 24, 2019.



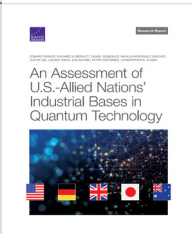
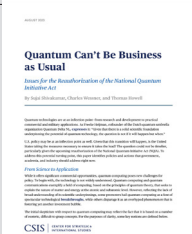
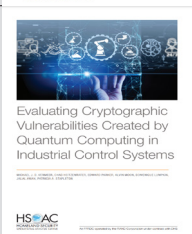
	Rugge, Fabio, John R. Allen, Giampiero Massolo, Gabriele Rizzo, Tom Wheeler, David Simpson, Tom Stefanick, John Villasenor, Mariarosaria Taddeo, and Samuele Dominioni. “The Global Race for Technological Superiority: Discover the Security Implications.” ISPI, and Brookings, November 26, 2019.
	국가정보원. “국가사이버안보센터 2022 연례보고서.” 국가사이버안보센터, 2023년.
	유기현. “AI는 전쟁의 양상을 어떻게 바꿀 것인가?: 알고리즘 전쟁(Algorithmic Warfare)을 중심으로.” 한국국방연구원, 제1938호(23-13), 2023년 3월 28일.
	홍성민, 황은혜. “인공지능시대의 본격 개막에 따른 인력 수급 정책의 미래 방향 제언.” 과학기술정책연구원, 2023년 12월 27일.

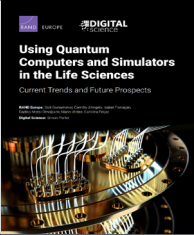
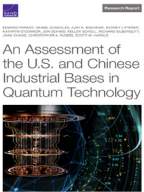
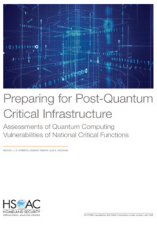
· 나노기술

	Shivakumar, Sujai, Charles Wessner, and Thomas Howell. “The Role of Industrial Clusters in Reshoring Semiconductor Manufacturing.” CSIS, October 10, 2023.
	Leins, Kobi. “Magnifying Nanomaterials.” UNIDIR, October 2, 2020.



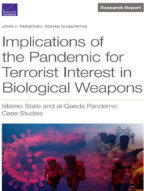
	Silbergliitt, Richard, Andrew Lauland, Michael Watson, Christopher A. Eusebi, and Jesse Lastunen. “Wearable Technologies for Law Enforcement: Multifunctional Vest System Options.” RAND Corporation, September 8, 2017.
---	--


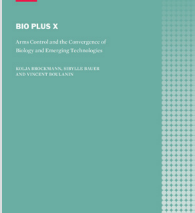
· 양자기술

	Carmack, Dustin. “Beating China in the Race for Quantum Supremacy,” The Heritage Foundation, April 5, 2023.
	Lewis, James Andrew, and Georgia Wood. “Quantum Technology: Applications and Implications,” CSIS, May 25, 2023.
	Parker, Edward, Richard Silbergliitt, Daniel Gonzales, Natalia Henriquez Sanchez, Justin W. Lee, Lindsay Rand, Jon Schmid, Peter Dortmans, and Christopher A. Eusebi. “An Assessment of U.S.-Allied Nations’ Industrial Bases in Quantum Technology.” RAND Corporation, November 16, 2023.
	Shivakumar, Sujai, Charles Wessner, and Thomas Howell. “Quantum Can't Be Business as Usual: Issues for the Reauthorization of the National Quantum Initiative Act,” CSIS, August 17, 2023.
	Vermeer, Michael J. D., Chad Heitzenrater, Edward Parker, Alvin Moon, Domenique Lumpkin, Muhammad Jalal Awan, and Patricia A. Stapleton. “Evaluating Cryptographic Vulnerabilities Created by Quantum Computing in Industrial Control Systems.” RAND Corporation, October 4, 2023.

	Gunashekar, Salil, Isabel Flanagan, Camilla d' Angelo, Immaculate Dadiso Motsi-Omoijiade, Mann Virdee, Carolina Feijao, and Simon Porter. "Using Quantum Computers and Simulators in the Life Sciences: Current Trends and Future Prospects." RAND Corporation, October 5, 2022.
	Parker, Edward, Daniel Gonzales, Ajay K. Kochhar, Sydney Litterer, Kathryn O'Connor, Jon Schmid, Keller Scholl, et al. "An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology." RAND Corporation, February 2, 2022.
	Vermeer, Michael J. D., Edward Parker, and Ajay K. Kochhar. "Preparing for Post-Quantum Critical Infrastructure: Assessments of Quantum Computing Vulnerabilities of National Critical Functions." RAND Corporation, August 18, 2022.

· 바이오기술

	Zakaria, Sana, Timothy Marler, Mark Cabling, Suzanne Genc, Artur Honich, Mann Virdee, and Sam Stockwell. "Machine Learning and Gene Editing at the Helm of a Societal Evolution." RAND Corporation, October 23, 2023.
	Fedasiuk, Ryan. "Regenerate: Biotechnology and U.S. Industrial Policy," CNAS, July, 2022.
	Parachini, John V., and Rohan Kumar Gunaratna. "Implications of the Pandemic for Terrorist Interest in Biological Weapons: Islamic State and al-Qaeda Pandemic Case Studies." RAND Corporation, May 31, 2022.

	Warmbrod, L., James Revill, and Nancy Connell. "Advances in Science and Technology in the Life Sciences," UNIDIR, August 19, 2020.
	Brockmann, Kolja, Sibylle Bauer, and Vincent Boulanin "Bio Plus X: Arms Control and the Convergence of Biology and Emerging Technologies," SIPRI, March, 2019.

참고문헌

[국문]

고은아 외. 2023. “EU의 디지털 미래 구축을 위한 사이버보안 방향과 시사점: 사이버보안 입법 동향을 중심으로”. KISA Insight 2023 Vol. 4. 한국인터넷진흥원.

국가과학기술자문회의. 2021. 「제5기 나노기술종합발전계획(2021~2030, 5+5 계획)」.

국가정보원·국가보안기술연구소. 2023. “챗GPT 등 생성형 AI 활용 보안 가이드라인”.

과학기술정보통신부(융합기술과). 2018. 「나노기술개발 촉진법」.

과학기술정보통신부. 2022. 「생명공학육성법」.

과기정통부·한국과학기술평가원. 2022. “2021년도 국가연구개발사업 조사·분석보고서”.

과학기술정보통신부·국가양자비전 TF. 2023. “대한민국 양자과학기술 비전: 양자시대를 여는 우리의 도전과 전략”.

국가안보실. 2023. 「윤석열 정부의 국가안보 전략」.

글로벌 과학기술정책정보 서비스(S&T GPS). 2020. “미국, 핵심 유망 기술 국가 전략 제시”. 주요동향. 178호.

김경준. 2023. “유엔사·우주·사이버 훈련 강화... “질적·양적 도약””. 한국일보, 11월 1일.

김도원·하병욱·김성훈. 2023. “미국·EU·영국 등의 사이버보안 전략 분석 및 시사점”. Kisa Insight 2023 Vol. 1. 한국인터넷진흥원.

김상배. 2021. 「디지털 안보의 세계정치: 미중 패권경쟁 사이의 한국」. 한울엠플러스: 서울

김상배 외 22인. 2023. 「신흥기술·사이버 안보의 국가전략: 국제정치학적 어젠다의 발굴」. 서울 대학교 국제문제연구소 총서 52. 사회평론아카데미.

김소정. 2023. “2023 미국 사이버안보 전략 주요내용과 한국에의 시사점”. Issue Brief. Vol. 423. 국가안보전략연구원.

김용. 2009. “나노기술의 군사 분야 적용”. 국방과학논단

김재호. 2023. “바이오안보 연구 동향 및 팬데믹 전후 변화”. BRIC View 2023-T21. 교수신문.

김종영 외. 2022. “미래 전장양상을 바꾸는 국방 양자기술 10선”. Issue Paper. Vol. 04. 국방 기술진흥연구소.

김홍열 등. 2021. 「바이오 헬스 분야 중장기 R&D 투자전략 수립 연구」. 한국생명공학연구원.

대통령직속4차산업혁명위원회. 2021. “대국민 인공지능 이용 인식조사”.

민옥기 외 5인. 2020. “ATL 1.0: 인공지능 기술 수준 정의”. 전자통신동향분석. 35(3). 한국전자통신연구원.

박상민. 2023. “경제·안보 관점에서 AI와 첨단바이오 기술 우선순위 설정: 국가전략기술 임무 중심 전략로드맵 II. 미래혁신 분야: 인공지능(AI), 첨단바이오”. 경제정책해설. 과학기술정보통신부

박영숙·제롬 글렌. 2023. 「세계미래보고서 2024-2034」. 교보문고: 서울

법무법인 화우. 2023. “미국 정부, 2023 정보보호 전략 발표: 책임의 재분배, 협력강화, 적극적인 대응, 투자의 확대”.

생명공학종합정책심의회. 2023. 「제4차 생명공학육성 기본계획 ('23~'32)」.

안성원. 2022. “국가 안보를 위한 인공지능(AI)과 3대 전략 기술”. Issue Brief. Vol. IS-140. 소프트웨어정책연구소.

유기현. 2023. “AI는 전쟁의 양상을 어떻게 바꿀 것인가?: 알고리즘 전쟁(Algorithmic Warfare)을 중심으로”. 국방논단 제1938호. 한국국방연구원.

유용원. 2020. “AI와 머신러닝을 사용한 ‘알고리즘 전쟁’”. 조선일보, 8월 27일.

유준구. 2023. “파괴적 신기술로서 인공지능의 책임있는 군사적 이용 논의 동향과 시사점”. 주요국제문제문석 2023-33. 국립외교원

윤정현. 2023. “양자과학기술의 국가안보적 의미와 대응전략”, INSS 전략보고, 국가안보전략연구원.

이지은·이지선·류종수. 2023. “해외 주요국의 국방 AI 현황 연구”. 한국국방기술학회. 5(1). 019-024.

임종인. 2023. “대한민국 사이버안보 확립 방안”. 국제 대학생 사이버보안 경진대회 및 컨퍼런스 발표자료.

장은정. 2023. “중국의 경제안보 최신 동향: 디지털·사이버 분야 법제를 중심으로”. 전문가 오피니언. 대외경제정책연구원.

정희태·전경주. 2019. 「나노 기술의 국방 응용 가능성 탐색」. 국방논단 제1770호. 19-31. 한국국방연구원.

조성완. 2023. “국방 분야에 적용 가능한 양자·양자향상 센서 연구 동향”. 주간기술동향 2019호. 정보통신기획평가원.

최필수. 2022. “경제안보 시대 중국의 대응”. 아시아 브리프 통권 79호. 서울대 아시아연구소.

한국리서치. 2023. “2023년 인공지능 인식조사: 인공지능, 양날의 검?”.

한국IDC. 2023. “국내 인공지능 시장 전망, 2023-27”.

한국전자통신연구원 표준연구본부. 2019. “인공지능”. ETRI Insight. 표준화동향 2019-01. 한국전자통신연구원.

홍락환. 2023. “글로벌 기술 패권 경쟁 관점의 국방 기술 혁신 동향”. ICT Standard Weekly. Vol. 1139. 정보통신기획평가원.

Damien Van Puyvelde·Aaron F. Brantly. 2023. 「사이버안보: 사이버공간에서의 정치, 거버넌스, 분쟁」. 명인문화사: 서울

IBM. 2024. “인공지능(AI)이란 무엇인가요?”. <https://www.ibm.com/kr-ko/topics/artificial-intelligence> (검색일: 2024.1.9.)

[영문]

Maj Patrick M. 2019. Nanoweapons: A Growing Threat to Humanity. Air University.

Allison, Graham, Kevin Klyman, Karina Barbesino, & Hugo Yen. 2021. “The Great Tech Rivalry: China vs. the US. Harvard Belfer Center for Science and International Affairs.”

Allison, Graham, Eric Schmidt. 2020. “Is China Beating the US to AI Supremacy?” Harvard Belfer Center for Science and International Affairs.

Boon W, Moors E. 2008. “Exploring emerging technologies using metaphors: a study of orphan drugs and pharmacogenomics”. Social Science & Medicine 66(9): 1915-1927

Brauner, Philipp, Hick, Alexandr, Philipsen, Ralf, & Zielfe, Martina. 2023. What does the public think about artificial intelligence? - A criticality map to understand bias in the public perception of AI. Frontiers in Computing Science 5. <https://doi.org/10.3389/fcomp.2023.1113903>.

Center for Security and Emerging Technology. 2020. “Artificial Intelligence and National Security.”

Cozzens S, Gatchair S, Kang J, Kim KS, Lee HJ, Ordonez G, and Porter A . 2010. Emerging technologies: quantitative identification and measurement. Technology Analysis & Strategic Management 22(3): 361-376

Day George S and Paul JH Schoemaker. 2000. “Avoiding the pitfalls of emerging technologies”. California Management Review 42(2): 8-33

Forbes. 2023. What The Quantum Computing Cybersecurity Preparedness Act Means For National Security. January 25th.

Gartner. 2023. The Gartner Hype Cycle for Artificial Intelligence.

Google DeepMind. 2023. “Levels of AGI: Operationalizing Progressson the Path to AGI.” arXiv:2311.02462v2.

Hung SC, and Chu YY. 2006. “Stimulating new industries from emerging technologies: challenges for the public sector”. Technovation 26(1): 104-110

Kosal, Margaret E. 2014. Military Applications of Nanotechnology: Implications for Strategic Security I. PASCC(Project on Advanced Systems and Concepts for Countering WMD).

Kolja Brockmann, Sibylle Bauer, Vincent Boulanin. 2019. Bio Plus X: Arms Control and the Convergence of Biology and Emerging Technologies. SIPRI(Stockholm International Peace Research Institute).

Lee, Kai-Fu. 2018. AI Superpowers: China, Silicon Valley, and the New World Order. Harper Business.

Michael Krenlina, Lieutenant Colonel Denis Dúbřavčík. 2023. “Quantum Technology for Defence: What to Expect for the Air and Space Domains”, JAPCC.

National Quantum Coordination Office. 2022. Summary of The Workshop on Cybersecurity of Quantum Computing.

OECD. 2023. OECD Science, Technology and Innovation Outlook 2023: Enabling Transitions in Times of Disruption. <https://doi.org/10.1787/0b55736e-en>.

Pew Research Center. 2021. How Americans think about artificial intelligence.

Pew Research Center. 2023. Growing public concern about the role of artificial intelligence in daily life.

Porter AL, Roessner JD, Jin, X-Y, Newman NC. 2002. “Measuring national emerging technology capabilities.” Science and Public Policy 29(3): 189-200

RAND. 2022. The Department of Homeland Security`s Use of Emerging Technologies: Why Public Perception Matters. Homeland Security Operation Analysis Center.

Robinson, Dan. 2019. Analyzing the public perception of artificial intelligence and what leaders can do about it.

Rotolo, Daniele, Diana Hicks, Ben R. Martin. 2015. “What is an emerging technology?” Research Policy 44: 1827-1843

Ryan Fedasiuk. 2022. Regenerate: Biotechnology and U.S. Industrial Policy. CNAS(Center for a New American Security).

Srinivasan. 2008. “Sources, characteristics and effects of emerging technologies: Research opportunities in innovation.” Industrial Marketing Management 37(6): 633-640

Stokes, Jacob, Alexander Sullivan, Noah Greene. 2023. US-China Competition and Military AI. Center for a New American Security. CNAS(Center for a New American Security)

WEF. 2023. Global Risk Report 2023 (18th edition). World Economic Forum.

Zhang, Baobao, Dafoe, Allan. 2019. Artificial Intelligence: American Attitudes and Trends. Center for the Governance of AI, Future of Humanity Institute, University of Oxford.

별책

세계신안보포럼 신기술 세션 영문 보고서

Report of
Navigating New
and Emerging
Security Paradigms
in AI-Driven World

2023 WORLD EMERGING SECURITY FORUM REPORT

Session on Navigating New and Emerging Security Paradigms
in AI-Driven World
December 2023
KAIST



Executive Summary

Today, emerging security threats ranging from cyber threats and new technologies to climate change are rapidly on the rise. Raising awareness and strengthening international cooperation to address such threats has never been more important.

Given the multifaceted nature of emerging security threats, mobilizing the expertise and capabilities of all relevant actors including governments, the private sector, international and regional organizations, and academia is critical.

In this context, the Republic of Korea launched the World Emerging Security Forum (WESF) in 2021 to promote a shared understanding of today’s changing international security environment and shape global discussions on ways to effectively tackle emerging security threats. By bringing together a wide array of stakeholders, WESF aims to promote neutral and balanced discussions that anchor collective interests.

In this year's report, WESF builds on the discussions of previous years and seeks to delve deeper into the impact of threats on the international security environment, with an emphasis on cyber threats and artificial intelligence (AI), and possible ways to address them.

Contents

076	1. The Brave New World of Technology-Security Coupling
078	2. Report Methodology
079	3. Assessing, Securing, and Governing Generative AI and Emerging Technologies for National and Global Security and Prosperity
081	4. Biosecurity and Emerging Technologies: Reflections on Emerging Questions for National and Global Security
088	5. Emerging Nanotechnology and Artificial Intelligence: Challenges, Threats and Opportunities
093	6. Emerging Technologies & Security Issues in Emerging Economies
096	7. Shaping Regulatory Frameworks in The Era of Disruptive Emerging Technologies
098	8. Cyber Security Risks in The Era of Emerging Quantum Computing
099	9. AI Technologies and Benefits Vs Risk Discourse: Why We Need A Balanced Approach
101	10. Emerging Security Questions and Expert Views
103	Conclusions
106	Notes and References
107	Appendix 1: Roundtable Program
107	Appendix 2: Panel Biographies

1.
The Brave
New World of
Technology-
Security
Coupling

No single day goes by without technological invention or innovation within and across nations. When confined to university or corporate labs, novel technologies remain only as ideas and imaginations. Like the genie out of the bottle, however, new technologies bring about unexpected consequences of often enormous magnitude and scope, nationally and internationally.

For instance, the rise of AI-generative deepfake has fueled disinformation, posing far-reaching ramifications for national geopolitical information securityⁱ ⁱⁱ. Drone warfare has become so conventional that it is hard to imagine how future wars can be waged without drones. Furthermore, while quantum computing is hailed for its potential to speed up new drug discovery, financial analytics/trading, and other cutting-edge applications, it poses unfathomable security threats to the integrity of the digital world. Nano-scale fabrication of organic and synthetic materials has opened up new possibilities for medical and industrial production; ironically, the same technologies invented for life and prosperity can be deployed to make new toxins or chemicals to cause death and harm.

Indeed, what is really at stake is humanity's broader rethinking of the meaning of security in this brave new world of technology-security coupling. We need to ask whether there is a need to redefine the meaning of security in the era where the fast-paced development of AI and emerging technologies is not only promising to revolutionize various sectors of both national and global economies but also introducing new risks and threats. In the political arena, for example, the world needs to rethink political security and the future of democracy, when powerful algorithms are used to influence political outcomes. The role of Cambridge Analytica and the 2018 US elections underscore the scale of the threat and risks in politicsⁱⁱⁱ.

Similarly, the emerging AI-powered technologies call for rethinking economic security. As governments in major economies embark on unhinged investments in AI and underlying technologies such as semiconductors, they should also begin to ask how they will safeguard economic security in the age of AI-powered automation because of its impacts on productivity, livelihoods, and standards of living now and in the foreseeable future^{iv}. Nations need to ask whether they are investing and developing the wrong kind of AI and if there is a need to refocus on investing in the “right kind of AI” to guarantee better economic and social security^v ^{vi}. Governments need to ask what they are going to do with the productivity paradox raised by AI and automation, whether they should start preparing for a world without work, and its potential implications for economic security.

Furthermore, AI-powered tools are reshaping the very foundations of our societies and nations, impacting their social and cultural fabrics. The ongoing transformations raise new questions and threats to nations’ social and cultural security. Currently, AI-powered

applications permeate virtually every aspect of individuals’ daily lives, from shopping to transportation, profoundly influencing social interactions and even determining outcomes such as who remains incarcerated or is released from jail^{vii}.

The breadth of these applications is as extensive as our personal experiences, yet our understanding of their consequences and the emerging risks associated with such technologies remains limited. There is an urgent need to deepen our comprehension of AI's effects at the individual level and understand its implications for the future of social justice. In this era characterized by the dominance of “surveillance capitalism,”^{viii} governments must expedite the redefinition of individual privacy, safety, and data ownership and storage. Furthermore, governments must reconsider their approaches to technology governance and regulation of AI technologies. What is worrying (or should be a point of concern across the board) is that current governance structures are struggling to keep pace with the rapid advancements in AI technologies.

This report focuses on in-depth discussion and understanding of emerging security implications, threats, and risks inherent to new emerging technologies. The report while avoiding “alarmism,” makes a sober assessment of emerging security risks and challenges from disruptive technological innovations to foster a greater understanding of the multifaceted security landscape associated with these innovations. We hope that through collaboration and knowledge-sharing on the potentials and pitfalls of new emerging technologies, nations can work towards proactive solutions to safeguard our societies, economies, and global stability in an increasingly tech-driven world.

The report broadly focuses on the following questions:

- What are new technological innovations coming out of labs or in the market that need particular attention from policymakers and relevant stakeholders?
- What are specific risks and threats that those innovations may pose for national and global security?
- What are emerging regulatory and governance best practices to safeguard the security of various dimensions from those potential harms? How can we benchmark and proliferate them globally?

2.
Report
Methodology

Table 1. Key Experts in
Each Technology Domain

With a focus on shaping a new understanding of emerging security issues posed by AI and emerging technologies such as biotechnology, nanotechnology, and quantum among others, we invited world-leading experts to share their insights through the roundtable and extensive interviews. Their in-depth insights are critical in shaping global understanding of new technological-security paradigms.

NAME	Title	Technology Domain
Prof. Xue Lan	Dean of the Schwarzman College and Dean of the Institute, Institute for AI International Governance of Tsinghua University	AI Global Governance Expert
Prof. Landry Signé	Executive Director and Professor, Thunderbird School of Global Management in Washington, D.C.; Co-Founder, Fourth Industrial Revolution Global Initiative; Senior Fellow, The Brookings Institution; Distinguished Fellow, Stanford University	Fourth Industrial Revolution Expert
Prof. Gerald Epstein	Contributing Scholar, Johns Hopkins Center on Health Security, Former Advisor, White House	Biotechnology and Emerging Technologies
Prof. Adrian Mihai Ionescu	Professor, École Polytechnique Fédérale de Lausanne (EPFL)	Quantum Computing Thought Leader
Dr. Vikram Sharma	CEO and Founder of Quintessence Labs	Quantum Computing and Cyber Security Thought Leader
Dr. Youssef Travalay	Executive Chairman of AllSightsAfrica	AI, Semi-Conductors, and Emerging Technologies Expert
Hon. Mohamed Shareef	Former Minister of State for Environment, Climate Change and Technology, Maldives	Expert on Emerging Technology Government Policy
Prof. Jaejin Lee	Dean, Graduate School of Data Science, Seoul National University	AI Technology Expert
Dr. James Revill	Head of the Weapons of Mass Destruction and Space Security Programmes at the United Nations Institute for Disarmament Research (UNIDIR)	Expert on Emerging Technologies and Space
Dr. Andraz Kastelic	Researcher at the United Nations Institute for Disarmament Research (UNIDIR)	Expert on Cyber Stability
Prof. Duk Choi	Associate Professor of Quantum Science and Technology, Australia National University	Quantum Computing and Global Collaboration

Please see the appendix for a detailed bio of the experts.

3.
Assessing,
Securing, and
Governing
Generative AI
and Emerging
Technologies
for National and
Global Security
and Prosperity

By Prof. Landry Signé



“Today, I stand before you to discuss a phenomenon reshaping our world – the Fourth Industrial Revolution. This revolution is not just an evolution; it’s a transformational shift, marking a new era where digital, physical, and biological realms converge, epitomized by groundbreaking developments like generative AI and the metaverse. As we navigate this moment of “punctuated equilibrium,” it’s essential to understand the monumental changes, opportunities, and challenges it brings”.

- Prof. Landry Signé, Executive Director and Professor, Thunderbird School of Global Management in Washington, D.C.; Co-Founder, Fourth Industrial Revolution Global Initiative; Senior Fellow, The Brookings Institution; Distinguished Fellow, Stanford University

Key Message

The 4IR is a way to acknowledge, describe, and understand a range of ongoing changes in how the world functions, including the convergence of frontier digital, physical, and biological technologies epitomized by generative AI and the metaverse. These changes are driven by a shift in the pace, velocity, and scope of co-evolution in technological developments, production systems, and social behaviors, a moment of “punctuated equilibrium” as socio-technological beings.

While generative AI and the emerging technologies associated with the 4IR are positively transforming the world and generating benefits for humanity, they also come with fast-

growing and ever-changing national and global security implications, harms, threats, and risks. What are some of the most consequential emerging and frontier technologies associated with the 4IR? What are the emerging harms, threats, risks, security, and cybersecurity challenges related to these technologies, particularly generative AI? How can policymakers, business leaders, and stakeholders collaborate to build a safer and more secure world during this rapid technological revolution? How can we better regulate generative AI and emerging technologies globally and use them more effectively to create a safer, more secure, better governed, inclusive, and prosperous world?

Professor Landry Signé systematically examined key trends, opportunities, risks, and strategies concerning generative AI, emerging technologies, security risks, and their implications for technology governance. He provided insights to shape understanding, assessing, securing, and governing emerging technologies and generative AI for advancing national and global security and prosperity. He gave special attention to the imperative of agile governance, technology policy, and multistakeholder collaboration, whether nationally or worldwide, including the partnership between the Global South and the Global North, recognizing their crucial role in navigating the challenges and harnessing the opportunities presented by the 4IR.

The major challenge is pacing challenge where technology such as Generative AI overtakes the ability to govern the technology. Further, generative AI has shown that it is possible to hack in a couple of minutes the government's digital infrastructure in developing countries. Similarly, technologies are now shaping public policy and democracy, and it's important to get governance right.

He emphasized that with great power comes great responsibility. The rapid growth of these technologies brings with them significant national and global security implications. For instance, the use of AI in autonomous weapons systems raises ethical and strategic concerns. The proliferation of deep fakes, enabled by generative AI, pose a threat to the integrity of information and has significant implications for personal and national security.

The risks associated with these technologies are diverse and evolving. Cybersecurity threats are escalating in complexity and scale, targeting critical infrastructure, financial systems, and personal data. The misuse of AI in surveillance and data manipulation pose threats to individual freedoms and democratic institutions.

To address these challenges, collaboration is the key. Policymakers, business leaders, and stakeholders must work together to develop frameworks that ensure the safe and ethical use of these technologies. This involves creating regulations that are adaptable to the fast-paced

4.
Biosecurity
and Emerging
Technologies:
Reflections
on Emerging
Questions for
National and
Global Security

evolution of tech, promoting transparency and ensuring accountability.

Effective regulation of generative AI and emerging technologies is crucial. This means establishing global standards and practices that balance innovation with security and ethical considerations. It's about harnessing the potential of these technologies while mitigating their risks.

Our shared goal as “humanity” should be to use these technologies to create a more inclusive, secure, and prosperous world. This involves leveraging AI for sustainable development, improving healthcare access, and driving economic growth while safeguarding against potential harm.

All these call for agile governance and multi-stakeholder collaboration, which are increasingly essential in this rapidly changing landscape. We need policies that are flexible and responsive to technological advancements. Multi-stakeholder collaboration, including partnerships between the Global South and Global North, is critical in sharing knowledge, resources, and best practices.

“As we stand at the cusp of this technological revolution, the decisions we make today will shape our future. It's not just about adopting new technologies but about adapting our societies, economies, and policies to harness their potential responsibly. By working together, we can navigate the complexities of the Fourth Industrial Revolution and steer toward a future that is secure, inclusive, and prosperous for all”.

By: Prof. Gerald Epstein



“Canadian author Margaret Atwood once said, “With all technology, there is a good side, a bad side, and a stupid side you weren’t expecting”. I’m not so sure about the “stupid” side, but she was right about “unexpected”. What we’ve learned is that unexpected or unforeseen effects of a new technology may dominate over whatever effects had been anticipated”.

- Dr. Gerald Epstein, Contributing Scholar, Johns Hopkins Center on Health Security, Former Advisor, White House

SUMMARY

Modern technologies are not required to produce biological weapons, but they can widen the set of people able to produce such weapons and exacerbate the harm that can result. The fact that all biology is based on a digital system – the genetic code – is driving a convergence between biotechnologies and information technologies, a convergence that is not only supercharging the development of biotechnology, but is also introducing some new dangers. In particular, there are some very concerning scenarios regarding how artificial intelligence (AI) can intensify biological risks. Artificial intelligence developers are working with biosecurity professionals – those people who are working to mitigate biological risk, especially the risk of deliberate misuse -- to explore these risks and to consider safeguards that might mitigate them. At this point, however, neither the magnitude of the risks nor the potential effectiveness of the safeguards is well understood. It is clear, however, that some actions that might be taken today – such as putting advanced AI models completely into the public domain – are not only irreversible, but might preclude the ability to implement some of these safeguards. Given the incredible benefits that AI and biotechnology can bring, we need to be very careful before imposing measures that might slow these fields down. On the other hand, slowing down something growing at an explosive pace could still leave it growing at a slightly less explosive pace. If that delay buys us all some safety, it’s a good tradeoff.

ASSESSING EMERGING TECHNOLOGIES

Canadian author Margaret Atwood once said “With all technology there is a good side, a bad side, and a stupid side you weren’t expecting”. Whether or not she was right about the “stupid” side, she was absolutely correct about “unexpected”.¹ What we’ve learned is that unexpected or unforeseen effects of a new technology may dominate over whatever effects had been anticipated.

For example, the initial estimates of the demand for photocopiers were vastly underestimated

2
Jeffrey Ding and Allan Dafoe, Engines of Power: Electricity, AI, and General Purpose Military Transformations, Cambridge University Press, February 2023, <https://www.cambridge.org/core/journals/european-journal-of-international-security/article/engines-of-power-electricity-ai-and-generalpurpose-military-transformations/7999C41177B0C2A7084BD3C1EAC0E219>

because they were based largely on the size of the carbon paper market – estimates that totally missed the transformational value of having the recipient of a document able to copy it, not just the originator. Similarly, when electricity first came on the scene, most predictions of how it would affect warfare envisioned electric weapons – say, directed lightning bolts.² But its most significant effects proved to be more subtle, and yet more transformational – in logistics, in communications, and in increased industrial productivity, which greatly improved the ability to produce all types of military hardware.

CONVERGENCE

Perhaps the most significant transformation in the field of biotechnology has come from the recognition that all biology is based on a digital system – the genetic code. Every organism on earth is defined by its RNA or DNA – and in particular the sequence of the chemical base units -- the As, Cs, Gs, and Ts that, when strung together, constitute that full RNA or DNA genome. This digital nature of life is not confined to the genome. Proteins – those molecules within living cells that build structures and perform essential functions such as catalyzing critical chemical reactions can also be characterized by a string of letters, each one corresponding to one of 20 amino acid building blocks that make up all proteins. These amino acids, when strung together in a particular linear sequence, determines a protein’s structure and therefore its function.

This recognition that life is digital at heart is driving convergence between the biological sciences and the information sciences. We can now bring all of the statistical and artificial intelligence (or AI) tools that have been developed to analyze large datasets to bear on genomic and other biologic datasets, allowing us to decipher – and increasingly to predict and to program – the operations of life. This ability is tremendously empowering, but it also means that whatever vulnerabilities are inherent to cyber systems, or to artificial intelligence operations, now can extend into the biological world as well.

BENEFITS AND HARMS OF BIOTECHNOLOGY

Biotechnology is a perfect example of a so-called “dual use” technology – meaning that the same science and technology base that underlies its legitimate applications can also be used for harm. Furthermore, attempts to constrain those harmful applications have the potential to constrain legitimate use as well.

Biotechnologies are developing at an explosive rate because of their hugely beneficial role – not just in medicine and health care, but in agriculture, in environmental protection, and increasingly in a whole range of industrial processes, in many cases displacing older, dirtier,

1
Rebecca Mead, “Margaret Atwood, the Prophet of Dystopia,” The New Yorker, April 10, 2017, <https://www.newyorker.com/magazine/2017/04/17/margaret-atwood-the-prophet-of-dystopia>

and more carbon intensive production technologies. But the ability to manipulate living organisms in these ways also confers the ability to modify them for harm, such as by creating more dangerous pathogens.

Modern technology is not required to use biology for harm, although it can exacerbate that harm. Long before much of today’s biotechnology had been developed, several nations were able to mobilize major biological weapons programs. More recently, nations around the world have organized to ban biological weapons by treaty – a treaty that the entire world has an interest in preserving. Moreover, and increasingly over time, the ability to use biology for harm has not required the resources of a nation-state. Therefore, preventing malicious use by nonstate groups or even individuals must also be a high priority – especially since – as the world has experienced – a single disease outbreak, starting off in a single location, can spread to become a global catastrophe. There is a vast range of human technologies that can be used for harm, but very few of them have potential consequences as severe, and as accessibly attained, as those that biology can cause.

CYBERSECURITY AND BIOSECURITY

In addition to what might be called “traditional” cybersecurity threats such as cyberespionage, ransomware, or theft of intellectual property, the biotech sector’s heavy dependence on huge genomic or proteomic datasets opens up additional vulnerabilities. These datasets may be at risk of denial of service or corruption. Furthermore, the product of advanced biotechnical manipulation – an engineered organism designed to have a specific function or to make a specific product – might effectively be stolen just by theft of its genetic code, without having to take the physical organisms at all.

Consider what might have happened if the genetic sequence used to manufacture mRNA vaccines like the Moderna and Pfizer COVID vaccines had somehow been hacked, so that they were no longer effective at triggering the body to make antibodies against COVID -- or worse, led the body to produce something dangerous. It is important to emphasize at this point that multiple safeguards exist to make sure that such an attack could never happen, but this example does illustrate one mechanism by which a cyber vulnerability could lead to a biological consequence.

Similarly, the automation of laboratory operations -- another aspect of information technology that is being increasingly utilized in the biotech sector -- could offer additional vulnerabilities to cyberattack. So effective cybersecurity is essential to mitigate potential harms from biotechnology. And we all know that no country can defend its cyberspace by itself, given our global connections.

ARTIFICIAL INTELLIGENCE AND BIOSECURITY

Looking at other applications of information technology, a great deal of attention has recently been devoted to how artificial intelligence could exacerbate biosecurity challenges, including by the barriers to development, production, and delivery of known types of biological weapon, or by facilitating the creation of more insidious pathogens than nature has yet come up with.

Large Language Models. Many of these risks are not well understood at present. AI developers and biosecurity professionals have been exploring the extent to which AI tools such as Large Language Models --- for example, OpenAI’s ChatGPT -- can provide roadmaps for those seeking to identify, acquire, and use biological weapons, making them more accessible to those who are not sufficiently technically trained to develop them without help.

One explanation I like for what these models effectively do is from Dr. Natasha Bajema, at the James Martin Center for Nonproliferation Studies. As she explains it, “It’s like having hundreds of thousands of graduate students conducting Internet research at the same time, putting together their unsourced, unverified, and outdated results (2021 or earlier), applying advanced statistics to determine the most probable correct response, and writing up a generic summary of the average outcome—all of this in mere minutes or seconds. It is not the “what” (information from the Internet), it is the “how” that matters (breadth of the research and speed).” These models are not necessarily completely trustworthy today, but they are improving rapidly.

Even with such a roadmap, would-be bioterrorists would likely need a considerable amount of “tacit knowledge” – knowledge that can only be acquired by doing something, rather than reading about it – to pull off an attack. Yet AI can help with this problem as well. If a would-be attacker gets stuck at some point in the process, Large Language Models can be very useful for troubleshooting -- but it’s not clear to what extent they would be sufficient to navigate “tacit knowledge” barriers.

It is also important to remember developing a biological weapon is not just obtaining a pathogen, but growing it, preparing it for release, disseminating it, and having it able to cause consequences. (Of course, spreading a contagious agent eliminates many of these steps, since the agent itself takes care of dissemination.) An attack also requires mastery of logistics, security, and other operational issues that have nothing to do with biology. A Large Language Model could help anywhere along this spectrum.

Right now, AI model developers and biosecurity experts are evaluating the extent to which these models really do lower barriers for users ranging from novices to those with advanced

skills in at least some of the necessary disciplines. We also have to anticipate how those evaluations might change as these models improve. In response to Dr. Bajema’s analogy above for how Large Language Models work, another biosecurity expert responded that if these models act like hundreds of thousands of graduate students today, not too far off they will act like that many PhDs, and at some point, they will act like that many world experts. Others, of course, disagree that the AI models will improve to that extent.

A number of potential safeguards might help deal with the use of AI to develop or improve biological weapons, ranging from controlling access to the huge amounts of computational power needed to train the models; limiting the types of data used to train them; or controlling who is allowed to access the models themselves. Developers are also considering building technical “guardrails” into the models that would not allow them to answer dangerous questions. It’s not yet clear, however, how feasible any of these safeguards would be, or what limitations they would place on those attempting to use these models for legitimate purposes. Recall that combating natural disease involves similar biological questions.

One thing that seems clear now, however, is that to the extent these models might pose dangers, allowing them to be released into the public domain without control – as some models have been to date -- precludes the ability to implement many of these safeguards, since there would be no ability to control who used them, and public release would likely make it possible to engineer around any technical guardrails governing what these models would be allowed to say.

Biodesign Tools

In addition to broadening the pool of those who can use biological systems, AI tools could also be used to help experts design pathogens or toxins having features more harmful than those nature has, or is likely to, come up with. A range of expert AI systems known as “biodesign tools” have been able to solve longstanding biological problems that have eluded decades of scientific effort, such as the ability to predict the structure of a protein when given its amino acid sequence. This ability, in turn, might allow biologists to determine a protein’s function from its sequence. Ultimately it may be possible to turn that around, starting with a desired function and from that deriving the amino acid sequence necessary to achieve it. Generalizing from proteins to genomes, it is conceivable, although if so still off in the future, that AI tools might one day be able to generate the genome for a novel pathogen with desired characteristics.

Unlike Large Language Models, AI-powered biodesign tools require substantial expertise to use, and only a fraction of the designs they come up with are successful. So the extent to

which they could be reliably used in this scenario is not well not known at present. To the extent these biodesign tools are thought to pose problems, many of the technical safeguards being envisioned for Large Language Models could be utilized for them as well.

Furthermore, before an AI-generated protein or genomic sequence can affect the world, it has to be embodied into a physical molecule. The point at which that happens --the so-called “digital-to-physical interface”— provides additional opportunities for control. For example, vendors of synthetic DNA– who are given DNA sequence information and produce the corresponding DNA molecules – today are being asked to screen both the DNA sequences they are asked to make and the customers they are making them for. If the DNA appears to be a so-called “sequence of concern” – something that could facilitate a biological weapon – the vendors are asked to make sure that their customers have legitimate need for those sequences.

Since DNA molecules are easy to ship across national borders – and DNA sequences even easier -- these controls would be of limited effectiveness unless they were implemented around the world. The same would go with any controls on the AI systems themselves.

CONCLUSION

It is encouraging that AI developers, biosecurity professionals, and policymakers are working together on issues at the intersection of AI, cybersecurity, and biotechnology. Thinking through these issues now is absolutely essential – particularly since, as has been stated above, some actions that might be taken today, such as putting material into the public domain, are irreversible. Five years from now, we don’t want to be in the position of desperately wishing we had done something five years previously– in other words, right now.

It is also important to note that, given the incredible benefits that AI and biotechnology can bring, any measures that might slow these fields down need to be considered very carefully before being implemented. On the other hand, slowing down something growing at an explosive pace could still leave it growing at a slightly less explosive pace. If that delay buys us all some safety, it’s a good tradeoff.

5.
Emerging
Nanotechnology
and Artificial
Intelligence:
Challenges,
Threats and
Opportunities

By: Prof. Gerald Epstein



“We are currently immersed in the digital era, marked by the progress of silicon nanoelectronics, which created the most abundant artificial object on Earth: the transistor. We have fabricated ten to power ten more transistors by humankind than the 400 Billion stars of the Milky Way”.

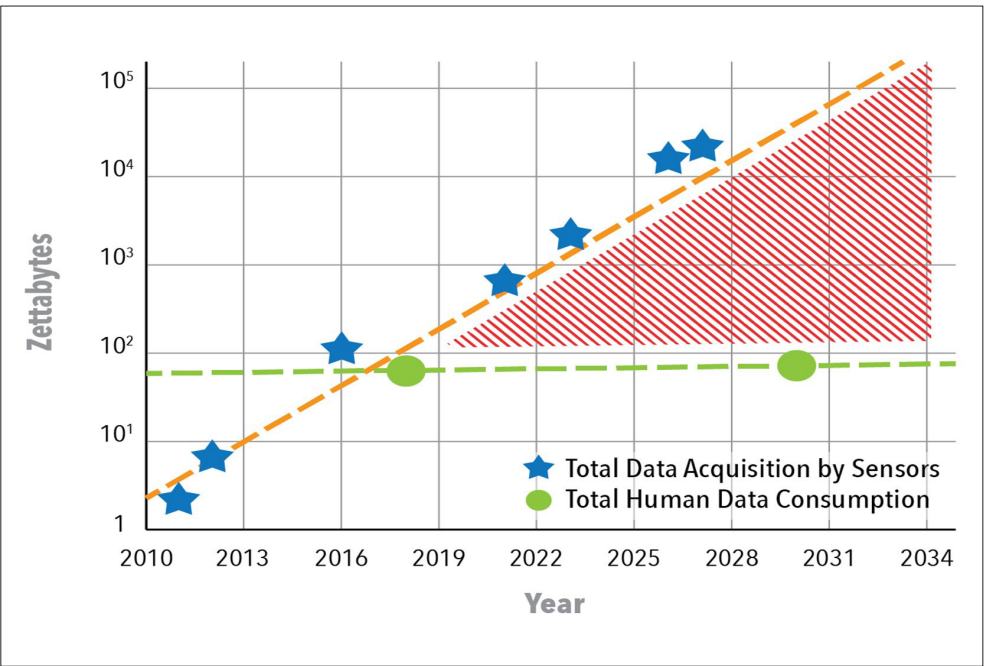
- Prof. Adrian Mihai Ionescu, Professor, École Polytechnique Fédérale de Lausanne (EPFL)

Key Message

Prof. Adrian Mihai shared his insights and provided a global view of where nanotechnology and Artificial Intelligence are strongly interconnected and their challenges, threats, and opportunities. He emphasized that the convergence of these technologies should be jointly considered. Below is his presentation on nanotechnology and AI:

The exponential progress of this technology during more than fifty years has been predicted in Moore’s law by one of the founders of Intel, Gordon Moore, who, from only 5 data points made a famous prediction of doubling the density of transistors every eighteen months. Today, we fabricate more than 100 million transistors per millimeter square, with dimensions 10 times smaller than a virus, working without any error for ten years. The related industry has one of the highest added value rates, of about 10 million, starting from an abundant material like sand (quartz) and ending in digital products.

Figure 1.
Internet of Things Nodes =
Tiny Brains



+1 trillion IoT devices by 2035 with annual growth > 20% (ARM)

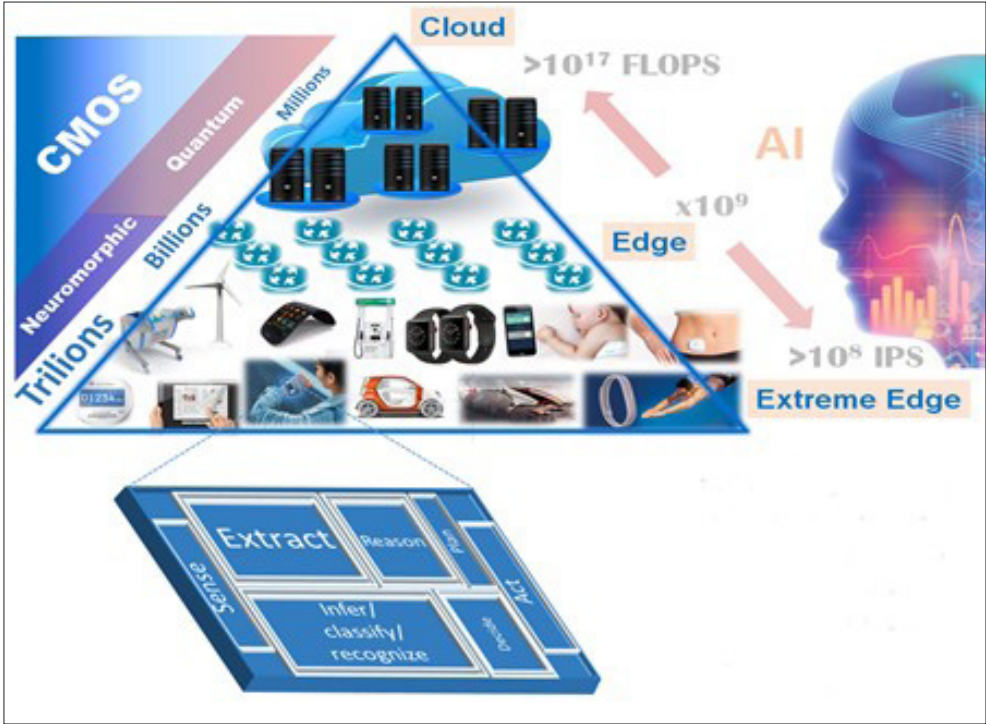
So, then why this nanotechnology is considered today by some a victim of its success? This is because it was primarily designed for performance and it’s facing big challenges like poor energy efficiency and large data proliferation. Data centers, the big brains of the cloud, are today responsible for more than 3% of the global energy consumption but their fraction is increasing exponentially and the projected trillion of Internet of Things nodes, the tiny brains, are expected to explode by a factor of one thousand the hundreds of zettabyte data generated by the middle of 21st century, making the sustainability of these technologies questionable.

In the last decade, we have experienced a profound change in the processing the digital information enabled by nanotech, which is the Edge to Cloud ecosystem. Here, due to the proliferation of Edge AI and low-latency autonomous systems, there is a trend of bringing much more intelligence to the Edge. So, what is the future of edge-to-cloud processing and related threats and challenges?

Let us first focus on the challenges of TINY BRAINS, essentially an Edge technology. Here a bright future is foreseen by taking inspiration from nature, going fully analog, and building neuromorphic spiking systems, end to end, inspired by the world of insects. By processing spikes with amplitudes near one hundred millivolts. This will able to detection and classification of events at the edge without storing or transmitting all the data, with increased security and privacy.

Figure 2.
Edge to Cloud Information
Processing in the Digital Era

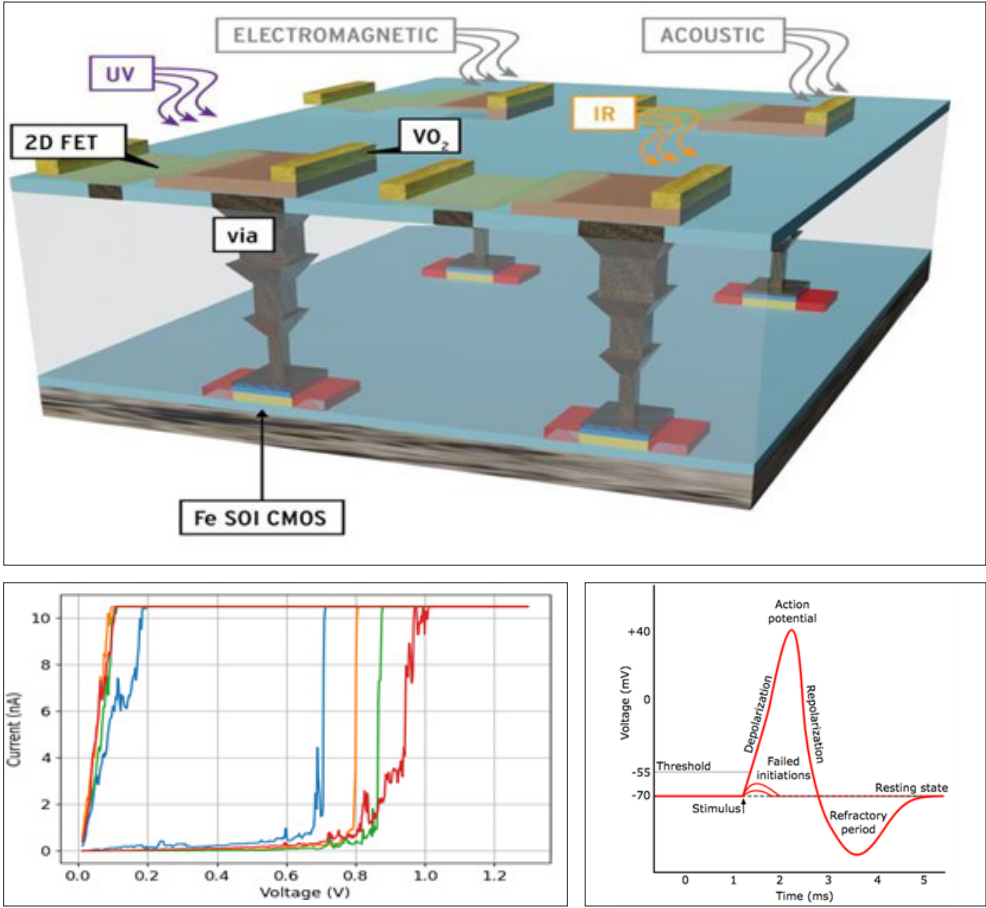
Source: Prof. Adrian Mihai



Imagine a new era of stochastic adaptive electronics that can learn over time and can be one thousand times more energy efficient than the one of today, systems that are integrated in 3D on top of existing silicon chips and will integrate new classes of nanoscale permissive devices based on functional oxides and 2D semiconductors to build artificial neurons and synapses. Such future Edge AI neuromorphic electronics will learn and improve their functionality based on sensed data sets on focused customized applications.

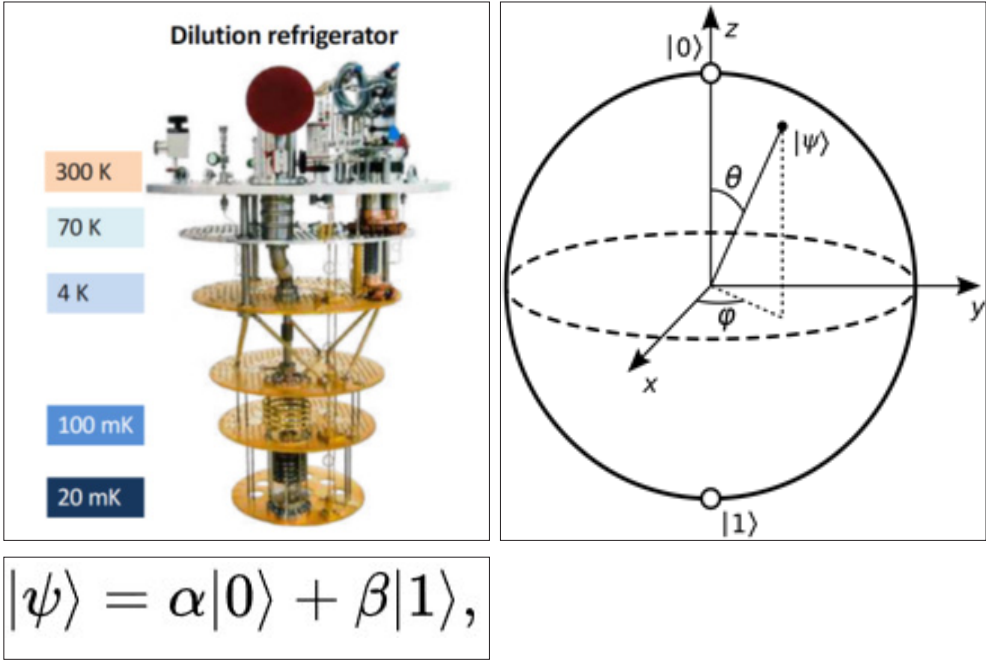
A major consequence and paradigm change enabled by Nano-AI concerns Digital Twin deployment. Digital Twins are digital replicas of complex systems of systems with unrivaled prediction capability. They can be applied in many domains like smart countries and cities, lean factories in Industry 4.0, battlefields, space exploration and, finally, to revolutionize the healthcare of humans from reactive to proactive. This involves understanding and quantifying to support reliable predictions of the future, which can be extended at the planetary level and would involve global cooperation and data sharing to efficiently address all the major sustainable development goals of the United Nations.

Figure 3:
Stochastic electronics that can learn,
1000x more energy efficient:
enabled by new sustainable
nanomaterials



On the other hand, there is a tremendous revolution that is happening now in the technology of BIG BRAINS staying in the cloud: quantum technology. Quantum is based on the concept of qubits, alternatives to classical binary bits of information, capable of exploiting the superposition of zero and one at the same time and in the same physical space. Entangling N qubits will allow a computer to achieve simultaneously two power N states, which for N higher than hundreds means a fantastic computational power, impossible to tract in a classical digital processor. Quantum is foreseen today as a cryogenic technology staying in the cloud and complementing traditional computing for complex tasks. In the future, expectations are enormous concerning its role in cybersecurity, quantum simulations, financial models, and the discovery of new drugs.

Figure 4:
Rise of Quantum Computing



About the future of quantum, the challenge relates to developing the full quantum stack, from the base quantum processors up to the microarchitecture and algorithms. This may be scaled up with the help of an existing nanotechnology platform, offering integration solutions for millions of nano-qubits, based on semiconductors and integrated nanomagnets.

Finally, the most exciting paradigm change for the BIG BRAIN technology is the resulting Quantum AI, bringing together the two words to achieve a possible singularity and offer the possibility to build artificial systems with much beyond human capability. This is a field where fears should be put apart and think BIG about the future of humanity and all kinds of implications, including expanding humanity's understanding and addressing the most urgent planetary issues. It will involve exponential AI, enhanced data security by quantum cryptography (both software and hardware), a combination of digital classic and quantum technology, and even the creation of powerful future Quantum Metaverse.

There are several challenges and risks. Such Quantum AI will have the capability to break any factoring encryption codes and will pose post-quantum cryptography challenges and both technical and ethical concerns about the creation of artificial entities beyond human intelligence. In this context, global policies should identify and agree on the right balance between regulatory aspects and preserving open innovation, which necessitates global cooperation and democratizing fair access to emerging technologies.

In conclusion, the future of AI is even brighter in the context of emerging nanotechnologies

6.
Emerging
Technologies &
Security Issues
in Emerging
Economies

and will involve many expected and non-expected paradigm changes from Edge to Cloud! These are exciting times for science and technology, think Big and Responsible, and don't be afraid!

By: Prof. Gerald Epstein



While emerging technologies present tremendous benefits, the unbalanced access and adoption of these emerging technologies by emerging economies lead to a loss of sovereignty in critical economic sectors such as banking and finance, infrastructure, energy, healthcare, trade, and logistics. Such a loss in sovereignty over financial, energy, healthcare systems, etc. leads to serious security risks for emerging economies.

Dr. Youssef Travaly, Executive Chairman of AllSightsAfrica

Key Message

The advent of emerging technologies such as Big Data Analytics, Cybersecurity, Machine Learning/AI, Cloud Computing, Blockchain, the Internet of Things (IoT), API, Biotech, Robotics, and Energy Storage is rapidly reshaping the global economic and social landscape. Dr. Youssef's presentation offers a comprehensive examination of these technologies, particularly focusing on their implications for emerging economies.

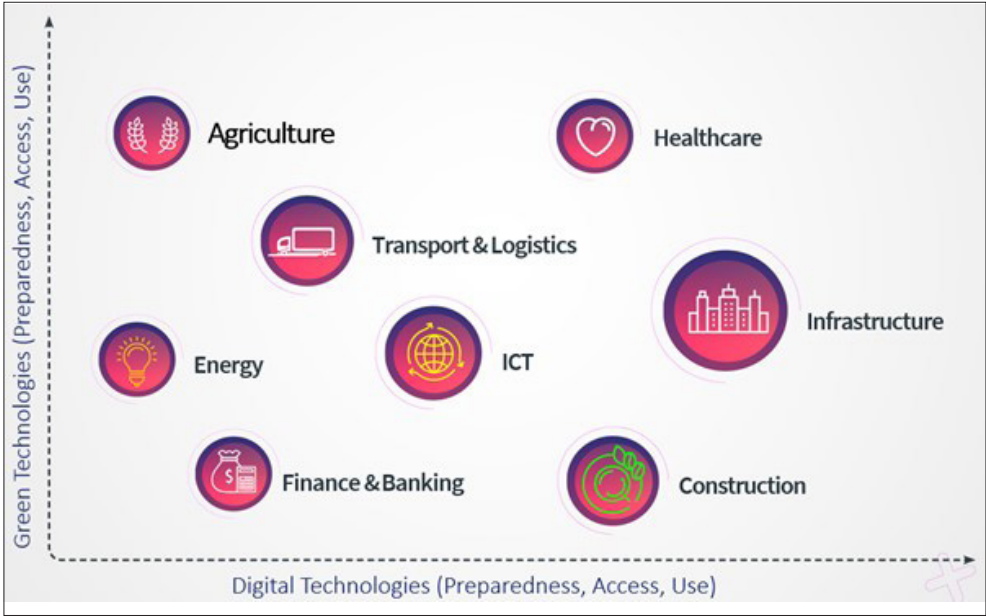
Emerging technologies such as Big Data Analytics and Machine Learning/AI are pivotal in processing vast amounts of data to glean valuable insights. For instance, in agriculture, AI-driven predictive analytics have the potential to significantly increase crop yields in developing

economies. However, the digital divide in data analytics capabilities between developed and emerging economies poses a threat to data sovereignty and economic independence. Emerging economies must develop their technological ecosystem for emerging technologies as well as proper governance frameworks.

Since countries are dependent on digital infrastructure, cybersecurity is increasingly becoming a critical issue. Emerging economies face increased risks of cyberattacks, as seen in the widespread impact of the WannaCry ransomware attack, which affected numerous countries including India, Russia, African countries among others. This highlights the vulnerability of these nations to digital threats.

Energy Storage: This is crucial for the transition to renewable energy. Countries like South Africa are investing in energy storage technologies to stabilize their grids, but access to energy technologies is often limited, posing a challenge to energy sovereignty. This also has an impact on data centers where the majority of data centers store African data outside Africa.

Figure 5.
Emerging Economies Are
Losing Their Sovereignty in All
Economic Sectors.

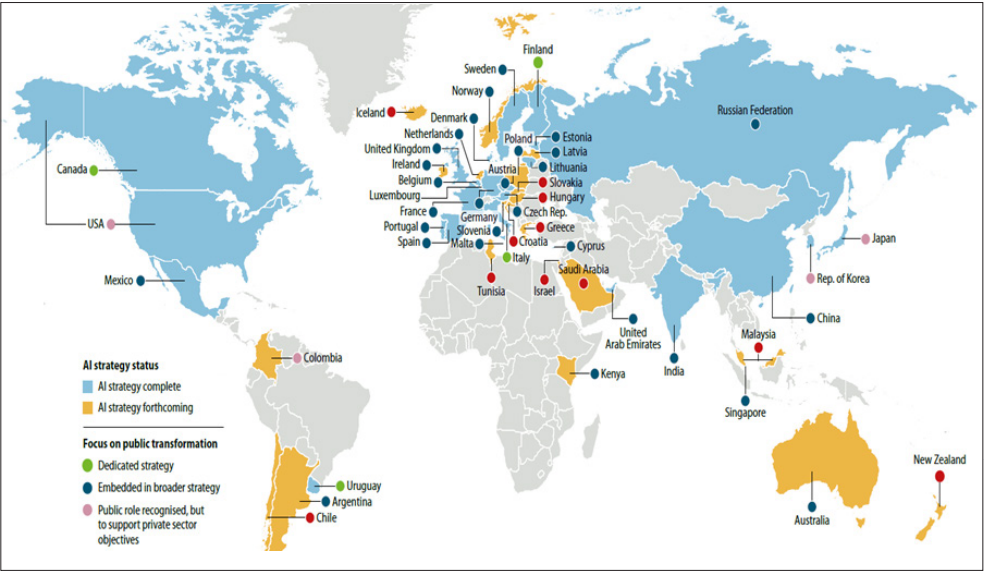


Dr. Youssef emphasized that while these technologies provide substantial benefits, their unequal access and adoption can lead to a loss of sovereignty in critical sectors like banking, finance, infrastructure, energy, healthcare, trade, and logistics. This technological disparity can result in serious security risks for emerging economies.

Real-world examples highlight the consequences of this technological divide. For instance, the over-reliance on foreign technology in the African banking sector has raised concerns about financial sovereignty.

Figure 5.
Few Developing Countries Have
Adopted a National AI Policy.

Source: OECD
(Organization for Economic
Cooperation and Development)



He concluded by emphasizing that the development of national digital economies and by extension of national data/AI economies depends to a large extent on implementing a collaborative digital regulatory and policy framework at both national and regional level in emerging countries. The lack of cross-institutional coordination represents a critical barrier to the development of policy coherence and regulatory consistency. Policy harmonization at national and regional levels is a pre-requisite to the involvement of African nations in international cooperation aiming to addressing new and emerging security paradigms in AI-driven world. In the short term, the Sub-Saharan African countries that could be meaningfully involved in such collaboration and dialogue include Ghana, Kenya, Nigeria, Rwanda, South Africa, Malawi, Mauritius, Senegal and Uganda.

7.
Shaping
Regulatory
Frameworks
in The Era of
Disruptive
Emerging
Technologies

Hon. Mohamed Shareef



“Now is the time to enhance collaboration and knowledge-sharing among various stakeholders, including governments, private sectors, and civil societies. This cooperative approach is essential to develop globally applicable regulations that can effectively govern AI and data-driven technologies”.

- Hon. Mohamed Shareef, Former Minister of State for Environment, Climate Change and Technology, Maldives

Key Message

The rapid advancement of Artificial Intelligence (AI) and data-driven technologies has ushered in a new era marked by remarkable opportunities and significant challenges. Hon. Mohammed’s critical examination focused on the imperative role of regulatory frameworks in balancing the risks and benefits of these disruptive technologies. He discussed the swift evolution of AI, the escalating significance of data, and the emerging security threats accompanying these developments.

Starting with AI advancements, AI technologies have seen exponential growth, transforming sectors from healthcare to finance. For example, AI-driven diagnostic tools have revolutionized medical imaging, enabling early detection of diseases like cancer. However, the fast pace of AI development raises concerns over unintended consequences and ethical dilemmas.

Relatedly, the rise of AI has heightened data security issues. This is because the surge in digital

data has escalated security threats, evidenced by incidents like the Equifax data breach, which exposed the sensitive personal information of millions of people. Such events highlight the vulnerabilities in current data management and protection systems.

Similarly, privacy and ethical concerns now dominate every government agenda in both advanced and emerging economies. The controversies over facial recognition technology used in public spaces, for instance, underscore the tension between technological advancement and individual rights.

The above underscores the need for robust regulations. Hon. Mohamed Shareef emphasized the urgent need for comprehensive regulatory frameworks. He advocates for regulations that are adaptable to the rapidly evolving technology landscape while ensuring the protection of individual rights and societal values.

He also highlighted various ongoing government digital initiatives to promote digital transformation and cybersecurity. The European Union’s General Data Protection Regulation (GDPR) is a prime example, setting a global standard for data protection and privacy.

Such initiatives highlight why countries must pursue proactive regulation and international cooperation. In his remarks, Mr. Shareef argues for proactive regulatory approaches and international collaboration in developing these regulations. The cross-border nature of digital data and AI applications necessitates a unified global response to effectively manage these technologies.

He further called for enhanced collaboration and knowledge-sharing among various stakeholders, including governments, private sectors, and civil societies. This cooperative approach is essential to develop globally applicable regulations that can effectively govern AI and data-driven technologies.

In summary, Mr. Shareef provided a comprehensive view of the challenges and opportunities presented by AI and data-driven technologies. He highlights the need for robust, adaptable regulatory frameworks and international cooperation to ensure that these technologies are harnessed responsibly and ethically, contributing positively to global progress while safeguarding fundamental human rights and social values.

8.
Cyber Security
Risks in the Era
of Emerging
Quantum
Computing

Dr. Vikram Sharma



Key Message

In the contemporary digital landscape, cybersecurity remains a critical concern, with traditional cryptographic methods forming the backbone of data protection. However, the advent of quantum computing poses new challenges and risks to these existing security protocols. Dr. Vikram Sharma, Founder and CEO of QuintessenceLabs and an expert in quantum cybersecurity, provides insights into this evolving domain.

Quantum computing, leveraging the principles of quantum mechanics, represents a significant leap in computational power. This new computing paradigm can process complex computational problems at unprecedented speeds, including potentially rendering current encryption methods obsolete. Quantum computers, with their ability to rapidly solve mathematical problems that are intractable today, could easily break widely-used cryptographic algorithms, such as RSA and ECC, jeopardizing the security of digital communications and long-lived data.

The emergence of quantum computing at a “cryptographically relevant scale” necessitates the re-evaluation of current cybersecurity strategies. The potential for quantum computers to break existing cryptographic codes could lead to a scenario often referred to as the "quantum apocalypse," a point in time when the confidentiality and integrity of digital information are compromised globally.

9.
AI Technologies
and Benefits
vs Risk Discourse:
Why We Need
a Balanced
Approach

To counter these threats, Dr. Sharma emphasizes the development of quantum-resilient cryptographic techniques. These include a new generation of cryptographic algorithms that are resistant to quantum computing attacks, thereby ensuring long-term data protection. Quantum key distribution (QKD), which uses the properties of quantum physics to secure communication channels, is another promising technology.

The era of quantum computing necessitates a paradigm shift in cybersecurity approaches. Dr. Sharma's contributions highlight the urgency for developing quantum-resistant cryptographic methods to safeguard against future quantum computing threats. His company represents a critical step in ensuring data security in the quantum age, emphasizing proactive adoption of emerging technologies.

Prof. Jaejin Lee



“There are too many threats and some people are writing novels of the threats of AI ... AI at its current level is only able to mimic only 3 percent of human's ability”. We shouldn't be too swayed by doomers who are writing fiction about the threats of AI. Essentially, AI will augment human capability”

- Jaejin Lee, Professor of AI and Hyperscale Computing Department, Seoul National University

Key Message

In the rapidly evolving landscape of Artificial Intelligence (AI), there is an increasing tendency to focus on potential risks and negative impacts. However, Prof. Jaejin Lee, a leading expert in AI technology, argues for a more balanced approach that emphasizes the significant benefits of AI. Prof. Lee's perspective on AI-powered technologies and their positive implications calls for a constructive and balanced discourse.

He highlighted that AI encompasses a wide range of technologies, including machine learning, natural language processing, robotics, and computer vision. Machine learning, a core component of AI, utilizes algorithms that learn from and make decisions based on data. Natural language processing enables machines to understand and interact with human language, while robotics integrates AI into physical tasks performed by human. Computer vision, another crucial aspect, allows machines to interpret and act on visual data. These technologies are rapidly advancing, driven by increased data availability, computational power, and algorithmic innovations.

AI technologies offer transformative benefits across various sectors. In healthcare, AI can improve diagnoses, personalize treatments, and enhance patient care. In education, AI-powered tools can offer personalized learning experiences and assist educators in curriculum design. In the business realm, AI enhances efficiency, optimizes supply chains, and drives innovation. AI also plays a crucial role in addressing global challenges, such as climate change, by improving energy efficiency and aiding in environmental monitoring. Furthermore, AI contributes to public safety through predictive analytics and emergency response optimization.

Prof. Lee highlighted people writing about the threats of AI in the same level as an atomic bomb. He suggested that governments in general handled nuclear threats and risks through regulatory regime and global coordination mechanisms. The same models could be applied in cases where AI poses a threat to humanity. Prof. Lee emphasized that the doomers may be exaggerating the risks posed by AI.

While acknowledging the risks associated with AI, such as privacy concerns, job displacement, and ethical dilemmas, Prof. Lee argues that a disproportionate emphasis on these aspects can hinder the development and adoption of beneficial AI technologies. A risk-centric narrative creates fear and resistance, potentially limiting progress and innovation. It is crucial to have a balanced view that acknowledges both benefits and risks of AI while actively working to mitigate the latter through ethical guidelines, regulatory frameworks, and responsible AI development practices.

10.
Emerging
Security
Questions and
Expert Views

Prof. Lee emphasizes the importance of education in understanding AI technologies. Increased public awareness and knowledge about AI can demystify the technology and foster informed discussions. He advocated for a balanced approach to AI technologies, emphasizing their numerous benefits while responsibly addressing potential risks. Embracing AI's positive potential can lead to significant advancements in various fields, contributing to societal progress and global well-being.

Prof. Landry Signé

In the context of the Fourth Industrial Revolution, how should the global tech governance be involved to address the intensifying AI competition between major powers and the urgent need for regulatory clarity in cross-border data and technology sharing?

*“First, I fully agree with the positive assessment by Prof. Lee on the prospect of AI. People look more at the risks and not enough at the benefits. The points he raises on the positive benefits of the technologies are critical and bring important opportunities globally and in emerging countries. I addressed some of these issues in my recently published book **“Africa Fourth Industrial Revolution”** (Cambridge University Press, 2023). I want to bring a global south perspective: people think about privacy, sovereignty, revenue sharing, inclusion, tech transfer, developing technologies, and not just consuming, sharing benefits of technologies. These issues suggest that the global south must be included in conversations regarding technology policy and governance. But with regards to your question Prof. Xue Lan, permit me to extend an invitation to all of us to download our recent publication through Brookings, **“A Blueprint for Technology Governance in Post-Pandemic World”** on emerging technology governance where we lay out steps on emerging tech agile governance, including AI. Thank you.”*

Dr. Gerald Epstein

Drawing from your experience at the OSTP and the Department of Homeland Security, what are the key lessons learned in managing biosecurity risks in the face of rapidly evolving technological landscapes?

“Before I answer, we need to know what should be regulated and who should regulate technology. We need to look at models and control models, can we control access to computing power; limit access to models, limit access to data? Another thing to look at is data, we have to know that by itself, it cannot influence the real world unless it is attached to a physical instrument/object to propagate harm.

If we refer to the DNA sequence, someone has to take that sequence and turn it into a DNA molecule. If people who are ordering it will create harm, then we need to regulate ...
Potential benefits ---If regulation is going to slow growth and slow innovation we will have a field that is growing slowly but still fast, which means that regulation is just buying time.
We need global cooperation to ensure proper regulations”.

Prof. Adrian Mihai Ionescu

How does the advancement of nanotechnology impact global security, particularly in the context of defense and surveillance? And what is your view on global regulatory trends?

“I’m coming from Switzerland and Europe which are very sensitive to human rights aspects and governance of emerging technologies. First, I would highlight to convergence between AI and Nanotechnology. The question in Europe is how to balance regulation and promote innovations. Europe in general is a pioneer leader in regulations. We learned that you need a right balance to regulate and anticipate risks while not jeopardizing innovation and benefit for humanity. If you look at some of applications, whole set regulations will not work. We need to have a public-private partnership. Consider digital technology and digital twin, and how it is promoting all the sustainable development goals based on data AI and other emerging technologies. Maybe the focus should be more on promotion at this point instead of regulation”.

Dr. Vikram Sharma

How should global cybersecurity policies evolve in response to advancements in quantum computing?

“I agree with your assessment that treating AI as an isolated domain doesn't make sense because of the convergence of technologies. There are many AI implications across various domains. For example, AI and Quantum. Governments and organizations that cross-cut across these technologies should collaborate to create cross-cutting regulations and standards for convergence technologies, in my view. Separating them as an individual technology doesn’t make sense and will not be effective”.

Dr. Youssef Travalý

How can the uneven adoption and adaption of 4IR technologies be addressed to ensure a broader access in emerging countries? How would you advise the secretary general of the UN in this regard?

“Accelerate policy development and institutional reform, which will force collaboration, especially between governments and the private sector: This is embedded in ITU models. Such collaboration will drive technology adoption and diffusion, and African governments need to develop their institutions to catch up”.

Prof. Jaejin Lee

How to make people understand science and technology to avoid doomsday scenarios of emerging technologies?

“It seems like a simple question but actually, it is very hard to answer because people are sensitive to media reports which propagate the risks of emerging technologies. First, we need to educate media houses about these technologies. Second graduates and undergraduates need to be educated well because even they hallucinate about the dangers of these emerging technologies ... Education is the key”.

Hon. Mohamed Shareef?

What advice would you give to governments to promote the adoption of emerging technologies?

“AI is advancing and will keep advancing towards general AI. It is part of us and will continue to be part of us ... So, we need to know this technologies ... We need to start with digital, AI and data literacy and build a generation that will be able to anticipate technologies and take a proactive action to a principle-based, right-based approach to developing our AI-driven societies”.

CONCLUSION

With in-depth discussions on rising security implications of the latest emerging technologies, the 2023 World Emerging Security Forum proposed the following recommendations and suggestions so as to foster a greater understanding of the multifaceted security landscape associated with the latest technological breakthroughs, thereby avoiding alarmism while guarding against threats, risks, and pitfalls of disruptive technologies.

1. Make a sober assessment of emerging technologies while avoiding alarmism

- As the pace of the development of emerging technologies overtakes the ability to govern them, it is critical for policymakers to have the most up-to-date understanding of the status of the latest technological breakthroughs and assess the potentials and pitfalls thereof.

- The risks associated with emerging technologies are diverse and evolving. Cybersecurity threats are escalating in complexity and scale, targeting to endanger critical infrastructure, financial systems, and personal data. The misuse of AI in surveillance and data manipulation pose threats to individual freedom and democratic institutions. However, disproportionate emphasis on risks and hazards of technological innovations will jeopardize the opportunities of harnessing the potentials of those technologies for greater safety and benefit of humanity.
- The unprecedented rapid success of large language models (LLMs) such as ChatGPT and ERNIE, has renewed interests in the risks and security issues of AI and has led to wide-spread fears of emerging technologies in different sectors. Emerging evidence across different domains and sectors suggests that AI and other emerging technologies can cause real harms including cyber-attacks, misinformation and disinformation, and potential loss of human control. Policymakers need to conduct an in-depth assessment of risks in each domain and take a risk-based approach to regulating and governing AI. Consider AI models in bioengineering (bio economy) or in autonomous driving (transportation sector).
- There are real and perceived fears of technological dominance by AI and emerging technologies. Some countries with large private players dominate the AI field, which is leading to serious questions on data ownership and sovereignty. Those with computing powers and dominant expertise in AI and data processing and utilization possess disproportionate power over “weak-on-AI- economies”. Policymakers need to seriously consider how their countries and regions can become active participants instead of just being “consumers of AI services”, data colonies for others, and likely to become victims of AI bad actors.
- Relatedly, the dominance by a handful of countries and a few monopolistic AI and tech companies raises new questions on “data colonialism” and the ability of “weak-on-AI” economies in both advanced and emerging countries to respond individually to threats to their security and sovereignty in different sectors. EU, for example, is able to present a united front to regulate AI through the General Data Protection Regulation (GDPR), the proposed AI act (AIA), and the Carbon Border Adjustment Mechanism, and digital taxation regimes, among others of regulatory and policy schemes. But how can “weaker” countries respond to this emerging AI technological dominance? Regional collaboration is becoming increasingly important to address these issues.

2. Build capacity for agile governance with multi-stakeholder collaboration

- Generative AI has shown that it is possible to hack in a couple of minutes government’s digital infrastructure. The era of quantum computing necessitates a paradigm shift in cybersecurity approaches. The advent of the fourth industrial revolution technologies such as machine learning, blockchain, robotics, and IoT is rapidly reshaping the global

economic and social landscape.

- New technologies call for agile governance with multi-stakeholder collaboration, by which those critically affected – whether individuals, groups or countries – can collectively make informed decisions in swift response to the latest developments of technologies.
- While the latest ideas floating around about the global regulation of AI often make a reference to nuclear technology governance such as the NPT, one can also take note of another kind of more distributed governance such as CERN.

3. Complexities in regulation and governance of AI and emerging technologies

- While the consensus on the benefits and risks of AI and other emerging technologies is becoming clear, there are diverse views on how to reap the benefits of AI while regulating its risks. The convergence of AI with other technologies including nanotech, biotech, and quantum among others, increases the complexities of proper regulatory and governance responses. While some quarters are advocating for self-regulation and governance, “risk-based approaches”, “hard regulations”, or “multi-stakeholder and regional interventions”. These debates are likely to remain in the foreseeable future. Policymakers in different jurisdictions should update themselves of these emerging discussions. They should also consider establishing guardrails as well as safety and usage standards to safely guide consumers/users from AI harm.

4. Engage scientists seriously in the decision making process involving technologically complex issues

- With all complexities and uncertainties emanating from the latest technological developments, it would be risky for only policymakers to make a final decision on the use and misuse/abuse of the latest technologies.
- Whether for promotion or regulation of technologies, the best expertise must be sourced from the most credential segment of the scientific communities around the world. This would greatly relieve the anxiety of general citizens as a result of emerging technological manipulation or misuse, especially at the time of securitization of science and technology.

Notes and
References

i. See, Christian and Chadwick (2020), “Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News”, available at <https://journals.sagepub.com/doi/full/10.1177/2056305120903408>

ii. See, Robert and Danielle (2019), “Deepfakes and the New Disinformation War”, available at <https://aloinstitute.org/images/Library/DeepfakesAndDisinformationWar.pdf>

iii. See, Nicholas Confessore, “Cambridge Analytica and Facebook: The Scandal and the Fallout So Far”, New York Times, April 4, 2018, available at <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>

iv. See, Jason Furman and Robert Seamans (2019), “A1 and the Economy”, available at <https://www.journals.uchicago.edu/doi/epdf/10.1086/699936>

v. See, Daron Acemoglu and Pascual Restrepo (2019), “The Wrong Kind of AI? Artificial Intelligence and the Future of Labour Demand”, available at <https://academic.oup.com/cjres/article/13/1/25/5680462>

vi. See, Erik Brynjolfsson, Daniel Rock, and Chad Syverson (2017), “Artificial Intelligence and the Modern Productivity Paradox: A Clash of Expectations and Statistics”, available at https://edisciplinas.usp.br/pluginfile.php/5239446/mod_resource/content/6/w24001_Brynjolfsson_AI_Artificial_Intelligence.pdf

vii. See, Karen Hao, “AI is sending people to jail—and getting it wrong”, available at <https://www.technologyreview.com/2019/01/21/137783/algorithms-criminal-justice-ai/>

viii. See, Shoshana Zuboff (2019), “The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power”.

Appendix 1.
Roundtable
Program:
Navigating New
& Emerging
Security
Paradigms in
AI-Driven World
(14:50– 16:10)

Appendix 2:
Panel Biographies



Run of Show

TIME	APPROVED PROGRAM	SPEAKERS
14:50 PM ~ 14:55 PM	Tour De Table/Introductions of Panelists	Session Chair (Prof. Xue Lan)
14:55 PM ~ 15:03 PM	Generative AI, Emerging Security Risks and Implications for Technology Governance	Prof. Landry Signé
15:03 PM ~ 15:10 PM	Biosecurity and Emerging Technologies: Reflections on Emerging Questions for National and Global Security	Dr. Gerald Epstein
15:10 PM ~ 15:17 PM	Nanotechnology and New Questions for Global Security	Prof. Adrian Mihai Ionescu
15:17 PM ~ 15:24 PM	Cyber Security Risks in the Era of Emerging Quantum Computing	Dr. Vikram Sharma
15:24 PM ~ 15:31 PM	Emerging Technology & Securities Issues in Emerging Economies	Dr. Youssef Travalý
15:31 PM ~ 15:38 PM	Shaping Regulatory Frameworks in the Era of Disruptive Emerging Technologies	Hon. Mohamed Shareef
15:38 PM ~ 15:42 PM	AI and Emerging Issues in Korea	Prof. Jaemin Lee
15:42 PM ~ 16:10 PM	Roundtable Questions to Panelists, Q&A and Closing	Session Chair (Prof. Xue Lan)

Prof. Xue Lan, Dean of the Institute for AI International Governance of Tsinghua University

Prof. Lan is noted for both his positions on many research and educational councils as well as his work in global governance, crisis management, and science, technology, and innovation policy. He sits on the World Economic Forum Steering Committee on AI Governance. He serves as the Director of China's National Expert Committee on Next Generation AI Governance, a member of the UN Committee of Experts on Public Administration, and a member of the Internet Governance Forum Leadership Panel. He is also an adjunct professor at Carnegie Mellon University and a Non-Resident Senior Fellow at Brookings Institution.



Dr. Landry Signé, Executive Director and Professor, Thunderbird School of Global Management in Washington, D.C.; Co-Founder, Fourth Industrial Revolution Global Initiative; Senior Fellow, The Brookings Institution; Distinguished Fellow, Stanford University

Professor Landry Signé is a world-renowned professor, extraordinary global leader, award-winning author, disruptive innovator, and pre-eminent future-oriented thinker who bridges ideas and actions, and private and public sectors to solve some of the world’s most complex challenges and maximize some of the most promising opportunities, winning over 80 prestigious awards and distinctions; with over 200 academic and professional publications; and over 1,000 keynotes, speaking and thought leadership engagements. He received the fastest reported tenure and promotion to the highest rank of full professor in the history of the U.S. universities for a scholar who started at an entry-level position in his discipline, and cumulates over 20 years of distinguished experience as Managing Director, Executive Director, Executive Chairman, Extraordinary Professor, Distinguished Fellow, and Senior Fellow, among others, including in top institutions such as Thunderbird School of Global Management, the Brookings Institution, Stanford University, the University of Oxford, the World Economic Forum, the Wilson Center, and Georgetown University. He often briefs top global leaders, including heads of state, heads of international organizations, and CEOs of global multinationals, and often briefs or testifies before the United States Senate, the U.S. House of Representatives, and the U.S. International Trade Commission, among others.

Professor Signé’s achievements have been recognized internationally with dozens of distinctions for his academic, policy, business, and leadership accomplishments, including as an extraordinary professor, prolific author, cutting-edge scholar, exemplary and dedicated academic leader, innovative entrepreneur, sought-after strategic thinker, problem-solver, board member, and keynote speaker. He was named one of the World Economic Forum “[top 50] foremost future-oriented thought leaders” in the world, a World Economic Forum Young Global Leader for “finding innovative solutions to some of the world’s most pressing issues;” one of “Apolitical’s 100 Most Influential Academics in Government” in the world; one of the “100 Most Influential Africans in the World” and “Thought Leader Extraordinaire” by New Africa Magazine; and one of the “most creative thinkers” by the Carnegie Corporation of New York; among others.



Dr. Gerald Epstein, Contributing Scholar, Johns Hopkins Center on Health Security

Dr. Epstein is a Contributing Scholar at the Johns Hopkins Center for Health Security. He joined the center after retiring from his position as Distinguished Fellow at the National Defense University’s (NDU’s) Center for the Study of Weapons of Mass Destruction, where he addressed challenges posed by nuclear, chemical, and biological weapons, particularly the security implications of advanced life sciences, biotechnologies, and other emerging and converging technologies. He came to NDU from the White House Office of Science and Technology Policy (OSTP), where he was Assistant Director for Biosecurity and Emerging Technologies, serving on detail from his position as Deputy Assistant Secretary for Chemical, Biological, Radiological, and Nuclear Policy at the Department of Homeland Security.



Dr. Adrian Mihai Ionescu, Professor, École Polytechnique Fédérale de Lausanne (EPFL)

He is the founder and director of the Nanoelectronic Devices Laboratory (Nanolab: <http://nanolab.epfl.ch/>) of EPFL. His group pioneered steep slope transistors (tunnel FETs and ferroelectric FETs), MEMS, and NEMS devices with a main emphasis on low-power resonator concepts (vibrating body transistors) to achieve novel energy-efficient digital, analog, radio frequency, and low-power sensing functions. He is the recipient of the IBM Faculty Award 2013 for contributions to Engineering of the recipient of the André Blondel Medal 2009 of the Society of Electrical and Electronics Engineering, France. Ionescu has been a Scientific Board Member for the Semiconductor Companies Associations MEDEA+ and CATRENE. He was the leader of the strategic report “Towards and Beyond 2015: technology, devices, circuits and systems” provided to the European Commission and served as a roadmap to semiconductor industries. Ionescu was involved in the preparation of the FP6, FP7, and H2020 Calls of the European Commission in the fields of Nanoelectronics, Micro/nanosystems, and Future Emerging Technologies.



Dr. Vikram Sharma, CEO and Founder of QuintessenceLabs,

Dr. Vikram Sharma is the CEO and founder of QuintessenceLabs, a global leader in quantum cybersecurity. He has over 20 years of experience in building and managing technology companies. Before founding Quintessence Labs, he founded two successful start-up ventures in the information technology infrastructure and services spaces. He started his career as a programmer analyst and went on to work as a consultant with several leading professional services firms in Australia. He holds a Master of Science in computer science from The Australian National University, a Master of Science in management (Sloan Fellow) from

Stanford University, and a doctorate in quantum physics from The Australian National University. He was presented with the Pearcey State Award for Entrepreneurship in 2013. In 2014, Vikram was invited by the UK Government to join an expert panel for its flagship Quantum Technology Hubs program. He is a member of the Advisory Board of the Sydney Quantum Academy and serves on the World Economic Forum's Global Future Council on Cybersecurity. He is a regular contributor to journals and a frequent speaker at conferences. His TED Talk on "How Quantum Physics Can Make Encryption Stronger" has had over 1.2 million views.



Youssef Travaly, Executive Chairman of AllSightsAfrica

Dr. Youssef Travaly is the Executive Chairman of AllSightsAfrica and a Senior Fellow at Friends of Europe. He formerly served as the Vice President of the Next Einstein Forum and the African Institute for Mathematical Sciences – Next Einstein Initiative (AIMS-NEI) global network, and as the President of AIMS Senegal. He is a senior executive with over 20 years of experience working in the USA, Europe, and Africa with universities, research institutions, the private sector, and regional organizations, as well as national and international NGOs, at both strategic and operational levels in science, innovation, and public policy design, including innovative product policies. He holds a Ph.D. in Materials Science and an MBA and has demonstrated leadership in bringing advanced technologies and innovations from the laboratory to the market in an economically sustainable manner.



Jaejin Lee is a professor in the Dept. of Data Science/Graduate School of Data Science (Dean) and the Dept. of Computer Science and Engineering/College of Engineering at Seoul National University (SNU).

He is also the director of the Centre for Optimizing Hyperscale AI Models and Platforms (CHAMP) and the leader of the Thunder research group. He received his Ph.D. in Computer Science from the University of Illinois at Urbana-Champaign (UIUC) in 1999. His Ph.D. study was partly supported by graduate fellowships from IBM and the Korea Foundation for Advanced Studies. He received an M.S. in Computer Science from Stanford University in 1995 and a B.S. in Physics from SNU in 1991. After obtaining the Ph.D., he spent half a year at UIUC as a visiting lecturer and postdoctoral research associate. He was an assistant professor in the Department of Computer Science and Engineering at Michigan State University from January 2000 to August 2002 before joining SNU. He is an IEEE fellow and a member of ACM.