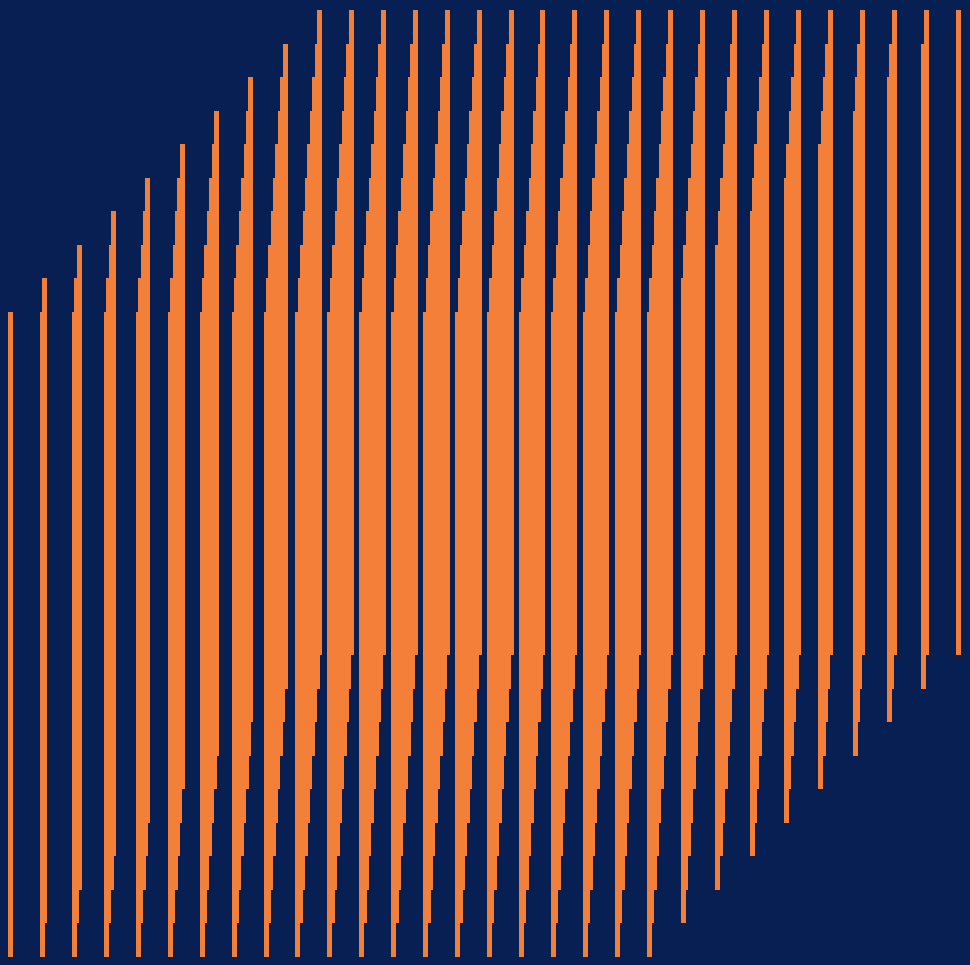
Exploration of Emerging Technologies &
Emerging International Security Issues and
Expansion of Global Networks

신기술의 국제안보에 대한 함의 분석 및 국제 네트워크 확대 방안연구

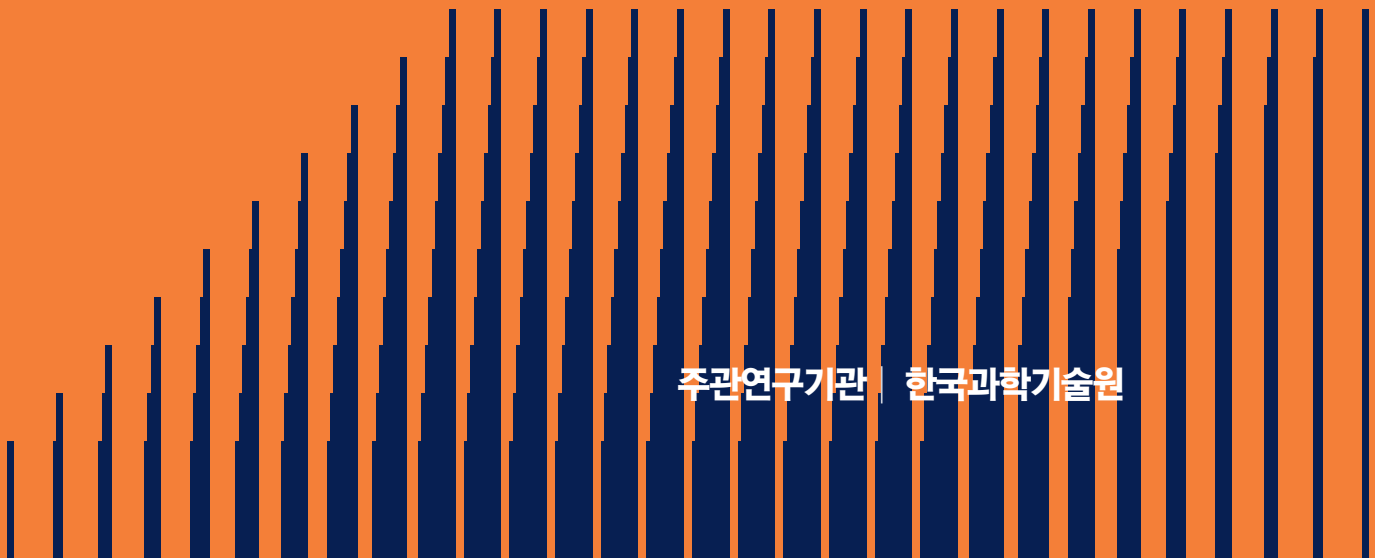


주관연구기관 | 한국과학기술원 KAIST

외교부

Exploration of Emerging Technologies &
Emerging International Security Issues and
Expansion of Global Networks

신기술의 국제안보에 대한 함의 분석 및 국제 네트워크 확대 방안연구



주관연구기관 | 한국과학기술원

신기술의 국제안보에 대한 함의 분석 및 국제 네트워크 확대 방안연구

Exploration of Emerging Technologies &
Emerging International Security Issues and
Expansion of Global Networks

제출문

외교부 장관 귀하

본 보고서를 '신기술의 국제안보에 대한 함의 분석 및 국제 네트워크 확대 방안 연구' 과제의 최종 보고서로 제출합니다.

2024.12.

주관연구기관 | 한국과학기술원(KAIST)

연구책임자 | 과학기술정책대학원 **김소영**(교수)

공동연구원 | 문술미래전략대학원 **서용석**(부교수)

과학기술정책대학원 **박경렬**(조교수)

과학기술정책대학원 **우석균**(조교수)

디지털인문사회과학부 **김태균**(조교수)

참여연구원 | 국가미래전략기술정책연구소 **백단비**(연구원)

전산학부 **전준형**(학사조교)

과학기술정책대학원 **Minahir Shahid Qumar Aali**(석사조교)

마케레레대학교(우간다) 전산학과 **Cornelius Kalenzi**(강사)

신기술의 국제안보에 대한 함의 분석
및 국제 네트워크 확대 방안연구

Exploration of Emerging Technologies &
Emerging International Security Issues and
Expansion of Global Networks

Content

3. 정책 및 인식

4. 전문가 네트워크 구축

5. 신기술 안보 포럼 운영

표 차례

그림 차례

AI, 양자, 첨단바이오 등 신기술 기반 파괴적 혁신이 전세계적으로 확산되면서 국제정세와 세계경제의 구조적 변화가 감지되는 가운데, 신흥 안보 양상도 빠르게 변화 중임.

특히 신냉전의 촉발 기제로서 기술패권주의의 부상은 앞으로도 지속될 전망인 가운데, 첨단기술 기반 새로운 무기체계와 인지전 등 전쟁 양상의 변화로 인해 최신기술에 대한 주도면밀한 분석을 통한 기술주권 확보의 중요성이 고조됨.

이러한 배경 속에 2021년 시작한 세계신안보포럼(WESF)은 급변하는 세계 안보 환경에 대한 이해와 핵심 도전과제 식별을 위한 글로벌 논의의 장을 제공해왔음. 올해는 AI 기술 고도화에 따른 각종 글로벌 안보 위협과 사이버 위협의 진화와 함께 기술패권 경쟁의 핵심으로 부상한 핵심광물, 배터리, 칩 등의 확보를 둘러싼 전세계적인 자원 경쟁 양상을 분석하는 자리로 마련됨.

동 포럼에 참여한 국내외 전문가들은 글로벌 정치경제의 불확실성 확대에 따라 다차원적으로 급변하는 안보 위협에 대한 회복력(resilience) 제고 속에 인류 공통의 가치와 평화를 위해 과학기술의 무한한 가능성을 활용할 수 있는 국제적 연대의 중요성을 강조함. 아울러 기술 선도국의 반열에 오른 한국이 국제사회에서 중견국으로서 국제사회 갈등 조정을 위한 적극적 역할도 주문함.

Summary

As disruptive innovations based on emerging technologies such as AI, quantum, and advanced biotechnology spread globally, structural changes in international relations and the world economy are facing structural changes, with emerging security patterns also rapidly changing.

In particular, the rise of technological hegemony is triggering the so-called new Cold War and expected to continue in the future. The importance of securing technological sovereignty through careful analysis of the latest technologies is thus increasing with changing environments and patterns of wars and militarized conflicts such as autonomous weapons or cognitive warfare.

Against this background, the World New Security Forum (WESF), which started in 2021, has provided a global forum for understanding the rapidly changing global security environment and identifying key challenges. This year, along with the evolution of various global security threats and cyber threats due to the advancement of AI technology, the event was prepared to analyze the global resource competition surrounding securing key minerals, batteries, chips, etc., which have emerged as the core of the competition for technological hegemony.

Domestic and foreign experts who participated in this forum emphasized the importance of international solidarity in utilizing the infinite potential of science and technology for common human values and peace. In particular, they all highlighted the importance of resilience to rapidly changing security threats of multiple dimensions, as uncertainty in the global political economy expands. In addition, South Korea, which has risen to the ranks of technologically leading countries, is requested to play a more active role in mediating conflicts in the international community as a middle power in international relations.

1. 연구 필요성 및 목적

1-1. 연구 필요성

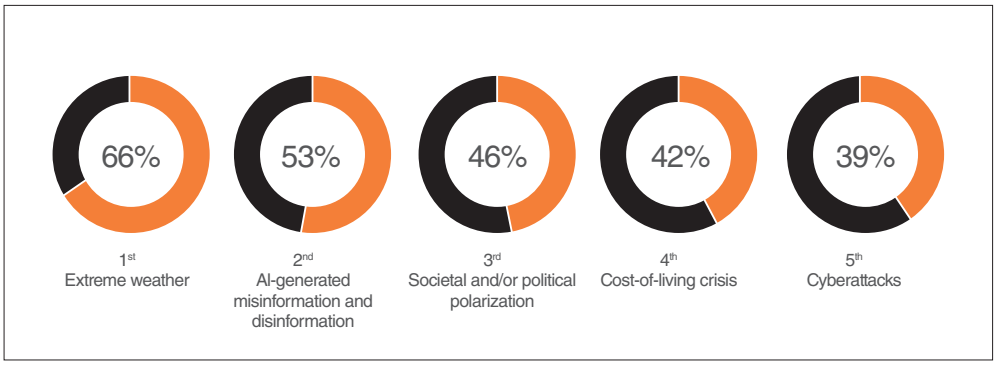
● **신기술의 파급력이 전 세계적으로 확대됨에 따라 신기술로 인해 변화되는 안보 양상을 분석하던 기존 추세에서, 이제는 신기술의 핵심 자원 확보를 통해 국가의 경제력 강화도 함께 꾀하는 등 더욱 다차원적인 외교·안보 전략을 수립하는 추세로 변화됨**

- WEF(2024)에서 발표한 글로벌 리스크 보고서에서는 빠르게 가속화되는 기술 변화와 경제적 불확실성이 팽배해지는 배경 속에 현재와 향후 10년 내의 위험요인으로 주로 AI와 사이버 공격을 논함
- 미국 국가과학기술위원회(NSTC)(2024)에서는 미국의 국가 안보와 경제에 있어 중요한 첨단 기술의 하위 집합으로 중요 신흥 기술(critical and emerging technologies, CET) 리스트를 업데이트했고, AI, 사이버 보안, 양자, 우주항공 등의 기술들이 포함되어 있음
- AI는 전통적 군사 안보의 변화를 일으켜 자율무기체계(AWS), 인지전, 허위 정보 교란 등의 신흥 안보 위협을 만들고 있는 것 뿐만 아니라, 글로벌 AI 규범 및 표준 마련의 추세에 따른 국제 평화와 연대를 맺는 신흥 외교 추세를 만들며 외교 안보 지형을 바꾸고 있음
- 사이버 공격은 국가 안보를 크게 위협할 수 있는 기술로 최근에는 국가를 배후로 한 사회 기반 시스템 마비, 주요 공급망 공격, 중요 정보 유출 등으로 사회 불안 조장부터 국가 안보의 위기까지 초래할 수 있게 됨
- 양자 기술은 상대적으로 응용·산업화 수준에는 미치지는 못하였으나, 복잡한 암호를 해독(양자컴퓨팅)하고, 빠르게 정보를 전달(양자통신)하게 함으로써 안보와 경제적 측면 모두에 파급력이 제일 클 것으로 예고되는 기술임
- 우주 기술은 통신 위성, 군 감시정찰위성 등의 무기체계로 개발되고 있고, 주요국에서는 미래 기술로 선정해 외교·안보·경제적 도구로 적극 활용하며 동맹 형태를 통해 기술 협력을 넓히며 기술력을 확보하고 있음
- 배터리는 핵심광물 공급망에 큰 영향을 받는 분야로 특정 국가에 집중된 리튬, 리켈 등의 공급망을 지속적으로 확보하기 위해 글로벌 협력 강화를 비롯한 전략적인 외교 안보 대응이 필요한 기술 분야임
- 광물은 신재생 에너지, 전기차, 방위산업 등에 사용되어 공급 리스크가 존재할 수 있으며, 주요 자원에 대한 확보와 국제 협력체계 구축을 통한 글로벌 시장에서의 영향력 확대가 중요한 분야임

● **트럼프 2.0. 시대의 개막과 주요국 리더의 강성화(시진핑 주석·푸틴 대통령의 종신집권화, 트럼프의 재선) 추세에 따른 자국 우선주의 팽배가 글로벌 공급망 재편과 기술 우위 확보로 연계되어 글로벌 외교·안보 지형의 불가측성을 확대하고 있음**

- 시진핑의 중장기 국정 운영 방향을 논의하는 국가 회의(2024)에서 국가 중심 전략을 기존의 '경제건설'에서 미국의 전략을 견제한 '안보·기술 확보'로 확대하며 '초장기전략'을 세움(이벌찬, 2024)

그림 1 : WEF 글로벌 리스크 보고서에 나타난 위험
(AI, 사이버 공격)
(출처 : WEF, 2024)



- 트럼프의 주요 기술 관련 정책은 기존의 바이든 정부의 규제 중심 정책을 완화하고 진흥 측면을 강화하는 정책으로, 이는 향후 AI를 비롯한 기술 혁신 속도를 앞당기며 여러나라의 AI 및 첨단기술 자국 우선주의 강화에도 영향을 미칠 것으로 예측됨
- 우리 정부는 공급망 다자협력체 핵심광물안보파트너십(MSP) 의장국 수임을 통해 첨단산업의 핵심광물 공급망 안정화를 추진하는 등 글로벌 아젠다 형성에 주도적으로 참여 중임

● **이외에도 신안보 양상은 국제정세와 기술 발전에 쉽게 영향을 받아 다변화·복잡화되기 때문에 신기술의 안보적 파급효과와 변화 양상을 지속적으로 진단하고 분석할 필요가 있음**

- 우리 정부는 AI 서울 정상회의(AI Seoul Summit, '24.5.), AI의 책임있는 군사적 이용에 관한 고위급 회의(REsponsible AI in the Military domain (REAIM) Summit 2024, '24.9.) 등 글로벌 규범 및 표준 마련에 적극 참여하고 있음
- 또한 글로벌 중추국가 비전을 바탕으로 세계신안보포럼(WESF)을 개최하여 매년 관련 논의를 심화하고 세계적으로 확대하고 있음

  ※ WESF 연차별 주제 : 2021년-신안보 위협 대응을 위한 다자협력의 미래, 2022년- 신흥안보 위협의 과거와 현재, 그리고 미래 - 신뢰에 기반한 국제협력으로의 길, 2023년-사이버공간과 신기술의 안보 위협 대응을 위한 글로벌 협력 강화

- 진화하는 안보 환경과 변화 양상은 어떠한지 분석하고, 주요국과 이해관계자들의 인식을 지속적으로 파악하는 것이 필요함

1-2. 연구 목적 및 내용

● **본 연구의 주요 목적은 AI와 신기술의 다분야 연계가 긴밀해짐에 따른 국제 평화와 안보에 미칠 위험과 파급력을 분석하고, 신기술 개발 및 기술 고도화를 통한 국가 경쟁력 강화를 이루기 위한 관련 국제 네트워크 현황 분석 등을 통해 융복합적 함의를 도출함으로써 한국의 국제적 리더십 제고를 위한 정책 방안 마련 및 전문가 네트워크를 확대하기 위함임**

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

- (행사 기획 및 운영) 제4차 세계신안보포럼의 주제(진화하는 안보 환경 속 국제협력 – 사이버, AI, 신기술을 중심으로)를 반영한 포럼 기획 및 운영('24, 12.), 국내 전문가 라운드테이블 기획 및 운영('24. 10.)
- (전문가 네트워크 구축) 주요 신기술별 전문가 조사, 전문가 인터뷰(그룹 인터뷰, 서면 자문) 진행, 신기술과 안보 전면에 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 네트워크 현황에 관한 분석 및 주요국 일반 인식 분석

표1 : 주요 연구 내용

Ⅰ. 신기술 안보 주요 행사 기획	Ⅱ. 신기술안보전문가네트워크구축	Ⅲ. 신기술 안보 정책 및 인식 분석
■ (국제 행사) 제4회 세계신안보 포럼 기획 및 공동운영 ■ (국내 행사) 제4회 세계신안보 포럼 라운드테이블 기획 및 공동 운영	■ 신기술 분야별 국내외 전문가 조사 ■ 신기술 안보 연계 분석 전문가 네트워크 마련(FGI, 서면 자문으로 연계)	■ 신기술 안보 관련 주요국 대응 분석 ■ 신기술에 관한 주요국 일반 시민 인식 분석

2. 신기술과 안보

2-1. 신기술 분야별 안보 이슈

2-1-1. 인공지능

● **AI는 국가의 안보를 위협할 수 있는 핵심 기술로 자리매김했고, 특히 작년 말부터 올해(2024)는 전세계적인 AI 안전·신뢰에 관한 글로벌 규범 수립부터 AI 혁신 혹은 규제 추세가 외교 안보 측면에도 연계되며 다변화하는 양상을 나타냄**

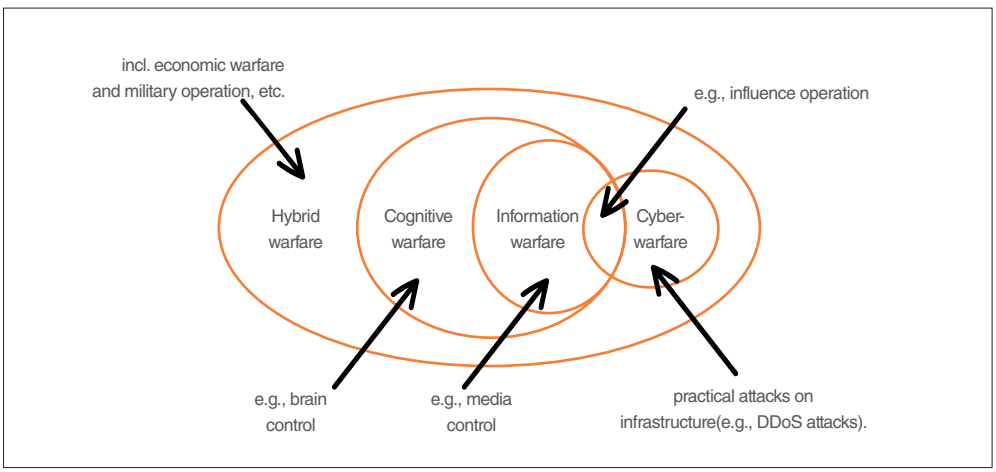
- 미국은 최초의 AI 행정명령(백악관, 2023)에 안전과 법적 규제에 대해 명시하고 있고, 미 사상 처음으로 AI에 관해 다룬 「국가 안보 각서(NSM)(2024)」에도 국가의 안보 목표 달성을 위한 AI 활용 시 AI를 군사적·안보적 활용 뿐만 아니라 전략 자산으로 여기는 경제적 측면과 AI의 안전, 보안, 신뢰를 강조하는 규범 측면을 함께 명시하고 있음
- 영국 정부의 주도로 전 세계 첫 AI 정상회의('23.11.)가 개최된 이후 미국, 영국은 앞다투어 국가 차원의 AI 안전연구소(AISI)를 설립하고, 뒤이어 일본, 우리나라 등 주요국에서도 AISI를 설립하며, 최근에는 미국 주도로 10개국이 참여한 '국제 AI 안전연구소 네트워크(International Network of AI Safety Institutes)'를 출범함('24.11.)
- 우리 정부는 올해(2024) 네덜란드, 싱가포르 정부와 인공지능의 책임있는 군사적 이용에 관한 고위급 회의(REAIM)와 아시아 지역 협의회를 개최한 이래로 외교부와 국방부의 공동 주관으로 한국에서 한 차례 더 개최함

● **러시아-우크라이나 전쟁을 기점으로 AI의 군사적 활용이 본격화되었고, 미·중 패권 경쟁, 중·대 갈등, 중동 지역 분쟁 등 팽배해진 국가간 대치 상황에 향후 군사적으로 더욱 활용되고 보편화될 것으로 여겨지며, 주요 활용 기술로는 '자율무기체계'와 '인지전(Cognitive Warfare)'이 계속해서 대두됨**

- 자율무기체계는 인간 조작자(operator)의 추가 개입 없이 목표를 선택하고 공격할 수 있는 무기 시스템으로, 대표적 무기에는 드론(군집 드론)이 있으며, 기술 특성상 규제가 쉽지 않기 때문에 UN(2023)과 같은 국제기구에서 결의안을 채택하거나 고위급 회의(ex: REAIM)를 개최하는 등의 노력을 이어오고 있음(전재성, 2024)
- 인지전은 미래 시대에 더욱 주목받는 분야로 AI를 비롯한 인터넷, 정보 통신 기술을 기반으로 상대방의 의사결정 과정에 영향을 미칠 수 있고, 딥페이크, 허위정보, 편향적 알고리즘 노출, 데이터 조작으로 잘못된 예측 정보 제공 등에 활용되며, 이는 정보전을 포함하고 사이버전과 연계되는 개념임
- 특히 이러한 인지전은 대규모 감시와 검열을 통해 정보를 조작 가능하고 잘못된 정보를 배포할 수 있으며, 높은 AI와 디지털 인프라 생태계를 갖춘 중국에서 유리하게 사용될 수 있어 미 백악관에서도 이러한 점을 경계하고 있음을 로이터 통신에서 밝힌 바 있음(Reuters, 2024)

그림 2 : 우크라이나전의 사이버 인지전 실행 목표
(출처 : 양정윤, 2024(전문가 자문), 원문: Microsoft, 2022, RAND, 2022)

그림 3 : 인지전의 영역
(출처 : 전재성, 2024, 원문: Hung, Tzu-Chieh, and Tzu-Wei Hung, 2020)



● 주요국에서는 거버넌스를 통해 AI 기술과 외교 안보를 강화하고 있는 가운데, 우리나라도 우리의 강점을 기반으로 거버넌스 지형의 급변 타이밍에 맞춰 빠르게 대응 전략을 취할 필요성이 있음

- 중국은 다자 협력 체계를 갖고 있고, 제조 강점을 활용하여 전세계의 공장에 AI를 적용해 산업화까지 꾀하고 있음. 우리나라도 우리나라가 주도할 수 있는 동아시아, 동북아 협력 체계 수립 전략을 세울 필요가 있음(조은교, 2024(전문가 자문))
- 최근 글로벌 AI 동맹의 흐름은 서방 가치의 동맹(자금 조달, 인재 양성)으로 북미 AI 동맹이 급부상하고 있고, AI 국제 표준 또한 서방에서 빠르게 차지하려하는 움직임을 나타내고 있음. 우호적 국가와의 협력을 벗어나 많은 나라와 다자 협력이 필요함(이원태, 2024(전문가 자문))

● 단편적인 국제협력 전략이 아닌 보다 넓은 시각의 전략 수립이 필요

- 우리나라는 중국의 AI 기술력 발전과 심각성은 인지하고 있으나, 미국을 중심으로 한 AI 기술 경쟁력 강화와 국제협력에 가깝고, 또다른 AI 기술 선도국인 중국은 간과하며 고려하지 않는 경향이 있음(조은교, 2024(전문가 자문))
- 브루킹스 연구소에서 발표한 내용에는 미국은 애초에 AI를 국가 안보적 측면 보다는 상업적

측면에서 민간(OpenAI, 구글, 마이크로소프트 등)에 의지해서 발전한 경향이 있는 반면, 중국은 국가 주도의 대규모 투자와 중국의 상업 발전을 군사 작전에 빠르게 통합하며 안보적 측면과 산업적 측면 동시에 급속하게 발전하는 추세를 보이는 것을 명시하며 미국의 중국 글로벌 리더쉽의 견제 필요성이 담겨있음(Sarah Kreps, 2024)

- 중국 정부는 도시에 데이터 센터를 건설하여 주요 지역의 컴퓨팅 파워를 결합하고, 광동과 선전의 지방 정부와는 AI 파운데이션 모델을 개발하며, 국가연구소와 선도 기업 간 협력을 통해 중국의 독자적 AI 생태계를 구성해나가고 있음(이승주, 2024)

2-1-2. 사이버 보안

● 사이버 공격은 공격 방식, 공격 주체, 공격 목적 등이 다양화·복잡화되며 양적·질적으로 변화되고 있으며, AI, 양자과학기술과도 밀접하게 연계되며 위협성이 커지고 있고, 현 전장과 미래전까지 영향을 미치며 국가 안보에 있어 매우 중요한 기술로 대두되고 있음

- 사이버전은 육·해·공·우주 공간에 영향을 미치며 전쟁의 승패를 좌우할 수 있고, 기존의 전통적인 전쟁과 연계되며 다영역 작전의 임무를 수행하며 승패를 좌우할 수 있음(김상배 외, 2024)
- WEF(2024)의 보고서에 따르면 AI, 양자컴퓨팅을 포함한 200여개의 신흥 기술이 사이버 보안에 신규 위협으로 대두되고 있고, 전통적인 보호 방식으로는 기술 발전으로 인해 나타나는 새로운 취약성과 복잡성에 대응하기 어렵다고 서술함
- 국가 배후의 사이버 공격이 확대되고 있으며 대표적인 예로 러시아의 트롤(Troll)은 우크라이나 뿐만 아니라 NATO 회원국을 대상으로 인터넷의 허위 정보나 선동성 발언을 퍼트려 회원국의 연대를 훼손하고 있음(동아일보, 2023)

● 사이버 보안 정책은 발전되고 변화되고 있으며 정책 추진에 따른 국제협력이 지속적으로 중요하게 인식되고 있음

- 올해 국내의 관련 정책으로는 국가안보실에서 「국가사이버안보전략('24.2.)」을 개정한 이후 국가안보실과 정보 부처 합동으로 「국가 사이버안보 기본계획('24.9.)」을 발표했고, 사이버안보 3법(사이버안보 기본법, 국가사이버안보법, 사이버보안기본법)은 국회 계류중에 있음
- 바이든 정부가 발표한 「국가사이버보안전략('23.3.)」은 공급망 보안 중심의 민관협력을 통해 취약성 감소와 회복력 강화에 집중하고 있으며, 트럼프 전 정부때보다 동맹국과의 협력을 더욱 강조하며 사이버 안보에 따른 시장 개입 비용을 전가하는 전략을 취한 것으로 보임(김상배 외, 2024)
- 미국은 23년 7월 발표했던 이행 계획을 「국가 사이버 안보 전략 이행 계획('24.2.)」으로 업그레이드해 발표하며 사이버 보안과 회복력에 대한 장기적 투자 확보와 긴밀한 주체간의 협력을 강조함(백악관, 2024)

그림 4 : 주요국 사이버안보 현황 및 정책
(출처 : 국회도서관, 2024)

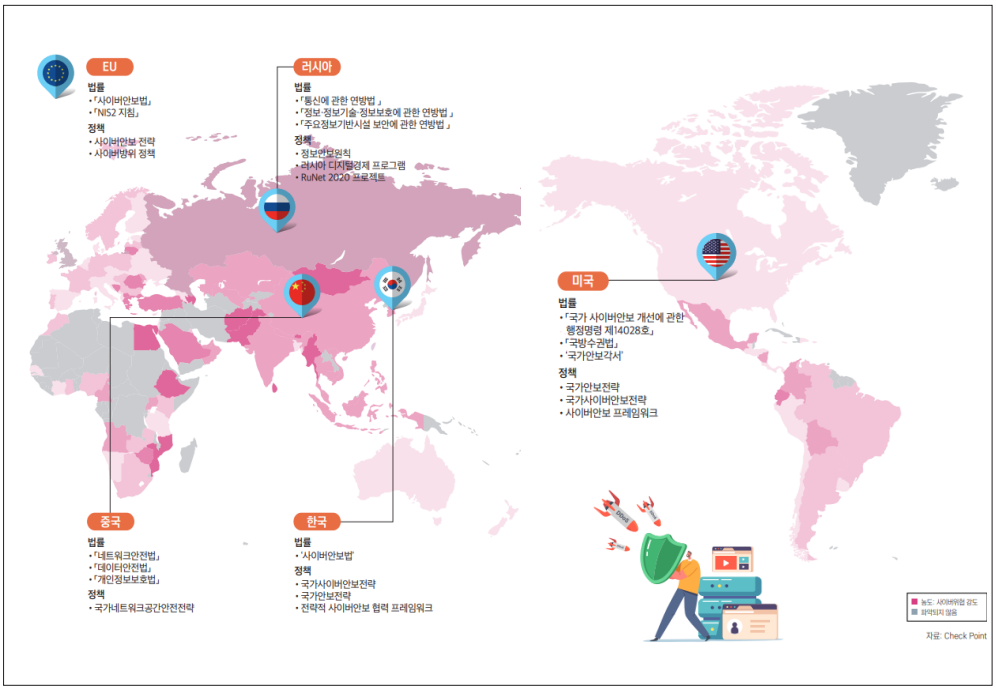
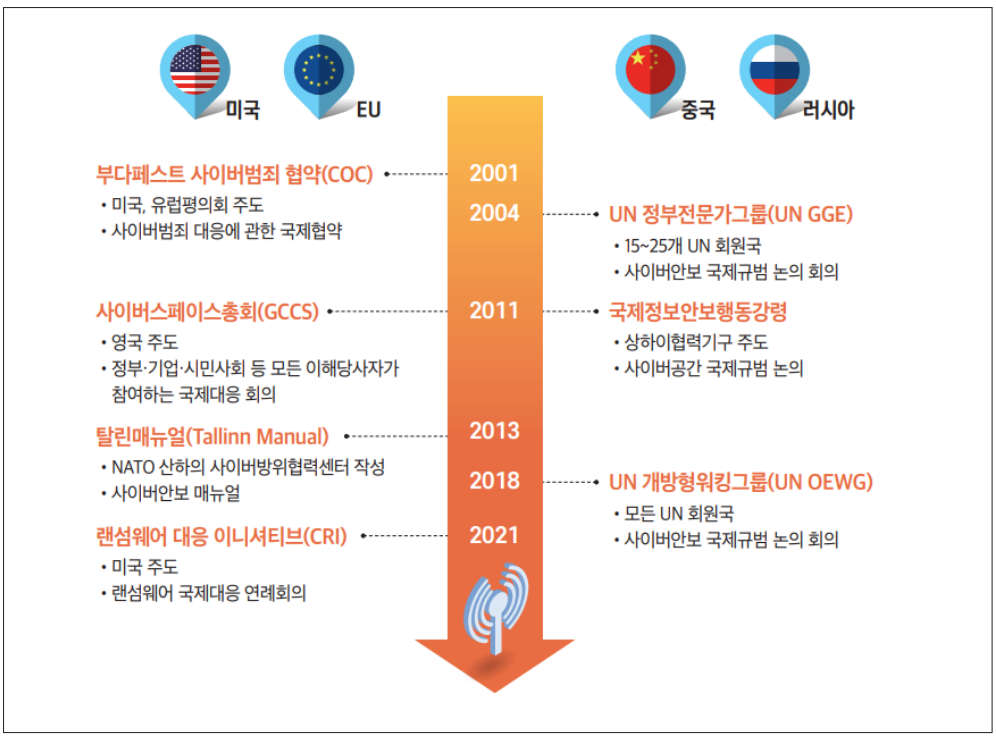


그림 5 : 사이버안보를 위한 국제협력
(출처 : 국회도서관, 2024)



● **사이버 안보 측면의 국제협력 추세로 우방국간의 동맹 기조가 이어지고 있는 반면, 한국은 다소 고립되는 형태를 보임**

- 주로 미국, 영국, 중국, NATO에서 주도하는 협력이 주를 이루어 왔음(국회도서관, 2023)
- (우방국간의 동맹기조) 글로벌 협의체(형태: 소다자, 다자, 지역)의 형태로 동맹 기조가 이어지고 있으며 동맹 서열화 현상이 나타남(이원태, 2024(전문가 자문))
- (안보적 고립) 우리나라는 한미 정상회담에서 「전략적 사이버안보 협력 프레임워크(Strategic Cybersecurity Cooperation Framework, 2023)」를 채택하고, 국가안보실에서 국가사이버안보전략(2024)을 수립하며 국제협력을 넓히고자 하나, 아직까지는 정식 회원국이 아닌 일부 분야로 참여중임

※ 관련 소다자 협의체: Five Eyes, QUAD, AUKUS, G7 / 지역 협의체: ASEAN, ARF, SCO, NATO, EU, OAS / 다자 협의체: UN, UN GGE, UN OEWG, CRI

표 2 : 사이버 안보 관련 전세계 협력 협의체 현황
(출처 : 양정윤, 2024(전문가 자문))

	Five Eyes	NATO	AUKUS	QUAD	OAS	ANZUS	G7
미국	●	●	●	●	●	●	●
영국	●	●	●	●			●
캐나다	●	●			●		●
호주	●		●	●		●	
뉴질랜드	●					●	
일본				●			●
한국							

2-1-3. 양자과학기술

● **양자과학기술은 군사적 용도와 상업적 용도 모두 갖춘 이중 용도 기술로서 국가 안보와 경제에 큰 영향을 미칠 수 있으며, 주요국과 국제조약기구에서는 안보 측면의 전략과 정책을 수립하고 있음**

- 미 백악관(2024)에서는 첨단 기술 규제 최종안을 확정지으며 「우려 국가 내 특정 국가 안보 기술 및 제품에 관한 미국 투자에 관한 행정명령(Executive Order on Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern, '24.10.)」을 발표했고, 이는 양자컴퓨터, 반도체, AI에 미국 자본의 중국 투자를 통제하는 것을 주요 골자로 하며, 군사, 사이버 보안, 감시 측면의 핵심 기술로 여기고 있음을 나타냄
- NATO(2024)에서는 자체적으로 첫 번째 양자 전략을 수립하며 해당 전략을 바탕으로 정부, 산업계, 학계와 협력하는 협력 체계(Transatlatic Quantum Community)를 운영하는 등 동맹국과의 기술 지원, 사이버 안보 보호 동맹 등을 강조함

– 중국 또한 양자과학기술 연구에서도 특히 양자통신 분야에 있어서 세계적으로 선두하고 있으며, 이는 군사적으로 사용 시 적으로부터 통신 보안을 차단하고 기능을 향상시킬 수 있으며, 이외에 군사적 응용 분야로 양자컴퓨팅, 양자센싱 기술도 활용될 수 있음(Edward Parker, 2024)

그림 6 : 미래전에 사용 가능한 양자과학기술
(출처 : NATO, 2023)

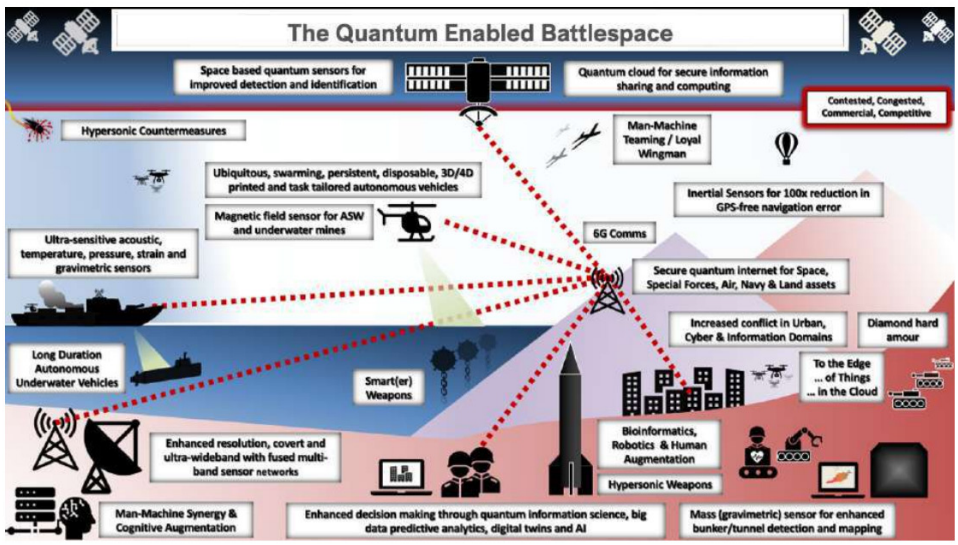


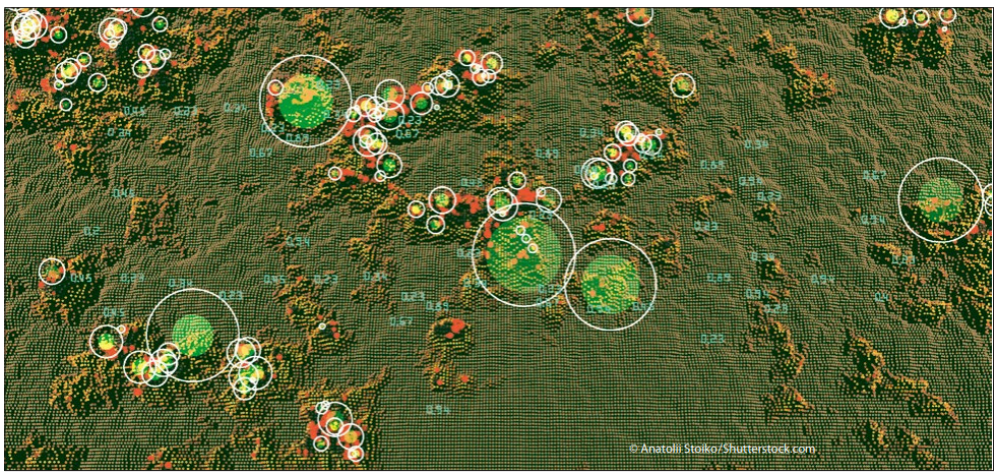
표 3 : 국방 분야에 양자과학기술 활용 시 발생 가능한 위험 요소
(출처 : Nature, 2024)

Type	Risk	Example
Known knowns	Privacy	Quantum computers could break encryption standards, resulting in unauthorized access to sensitive data.
Known knowns	Security	Breaking of encryption standards could reveal government secrets, with national security implications.
Known knowns	Oversight	Quantum algorithms could be difficult to reverse-engineer, hindering transparency and auditing.
Known knowns	Sustainability	Energy-intensive computing will have a negative impact on the environment.
Known unknowns	Just war	The synthesis of new molecules might create chemical or biological weaponry that could breach just-war requirements.
Known unknowns	Compound risks	Quantum tools will exist in an ecosystem with other technologies, such as artificial intelligence, compounding the risks posed by those technologies(including undue discrimination, responsibility gap and limited transparency).
Known unknowns	Strategic autonomy	Quantum tools will rely on specific materials and hardware that might not be available domestically. This could create a dependence on exports from another country, undermining strategic autonomy.
Known unknowns	Security	Quantum sensors could undermine the invulnerability of submarines and weaken nuclear-deterrence regimes.

● **양자과학기술의 주요 기술인 양자컴퓨팅, 양자통신 외에도 군사 영역에서는 아래 세부 기술들이 해당 작전에서 엄청난 잠재력을 갖고 있는 것으로 나타남(Michal Krelina et al., 2024)**

- 양자 이미징 시스템(Quantum Imaging Systems)은 비행 조정사가 장거리와 까다로운 기상 조건에서도 감시 및 표적 식별에 매우 유용하고, 우주 항공 영역에서 위성과 같은 우주 작전의 상황을 빠르게 인지할 수 있음
- 양자 중력기(Quantum Gravimetry) 같은 경우에는 지하 구조의 자원 파악과 잠수함 위치 파악 등을 파악하여 해전에서 널리 사용될 수 있고, GPS 없이도 탐색과 새로운 정보 수집, 표적 탐색에 능함

그림 7 : 전장에 활용 가능한 양자 중력기 모습
(출처 : Michal Krelina et al., 2024)

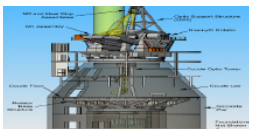
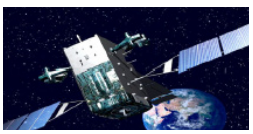
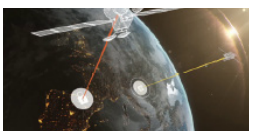


2-1-4. 우주

● **주요국은 군사적 우주기술과 자산 개발을 확대하고, 한국은 독자적 군사위성과 발사체 기술을 확보하며 우주 개발을 진행 중임(김대원 외, 2023)**

- (국내·외 우주 무기체계 개발 동향) 한국은 군 감시정찰위성, 통신위성, 고출력 레이저 추적 시스템 등을 개발 중이며, 미국은 스타링크와 GPS 현대화에 집중, 유럽은 갈릴레오 시스템과 자율적 우주 접근을 목표로 함
- (기술 수준 평가 결과) 국내 국방 기술 수준은 선진국 대비 약 58.8%로 격차는 9.1년, 민간 기술 수준은 약 61.9%로 격차는 8.8년으로 평가되며, 기술 협력 및 도입이 필요한 상황임
- (우주 분야 기술 발전방향) EO/IR, SAR 등의 감시정찰 기술 고도화, 군용 KPS 기반 초정밀 항법 기술 개발, 레이더·레이저 기반 통합 우주영역 인식체계 구축, 재진입·재사용 가능한 발사체 개발이 필요함

그림 8 : 국외 주요 우주 무기 체계
(출처 : 김대원, 2023)

Space surveillance	Solar Telescope(USA)	
Satellite early warning and reconnaissance system	Space Based InfraRed System(USA)	
Satellite communication system	GOVSATCOM(Europe)	
Satellite navigation system	Galileo system 2nd Generation FESA48(Europe)	
Space control	Falcon Heavy Space X(USA)	

● **미중 전략 경쟁 심화 속에서 우주는 글로벌 리더십과 영향력 경쟁의 핵심 공간으로 부상하며, 양국은 동맹 강화와 기술 협력을 통해 우주외교를 외교·안보·경제적 도구로 적극 활용하고 있음(차정미, 2024)**

- (21세기 미중 전략 경쟁) 미중 간 경쟁이 심화되며 우주는 미래 글로벌 리더십과 안보 경쟁의 중심 공간으로 부상함. 우주 기술을 활용한 외교는 국가 위상을 높이고 글로벌 협력 또는 경쟁을 촉진하는 주요 도구임
- (미국) 미국은 아르테미스 협정과 동맹국과의 협력을 강화해 중국 견제와 글로벌 리더십 유지를 목표로 함
- (중국) 중국은 국제달연구기지와 글로벌 남반구 협력을 통해 우주 기술을 외교적 자산으로 활용하고 있음
- (미중 경쟁의 국제 질서 영향) 미중 경쟁은 우주 외교를 중심으로 국제 협력의 진영화와 다극화 추세를 가속화하며 국제질서를 재편하고 있음

2-1-5. 배터리

● **전기차 배터리 핵심광물의 공급망은 특정 국가와 중국에 집중되어 있어 한국은 자원 확보와 공급망 다변화를 위해 민관 협력, 정·제련 기술 내재화, 재활용 확대, 글로벌 협력 강화 등의 전략이 필요함(한국과학기술기획평가원, 2023)**

그림 9 : 미중 양국 주도의 우주협력 네트워크
(출처 : 차정미, 2024)

미국 ARTEMIS 협정국 36개국(2024.2 현재)

우루과이, 앙골라, 아르헨티나, 호주, 바레인, 벨기에, 브라질, 불가리아, 캐나다, 콜롬비아, 체코, 에콰도르, 프랑스, 독일, 그리스, 아이슬란드, 인도, 이스라엘, 이탈리아, 일본, 룩셈부르크, 멕시코, 네덜란드, 뉴질랜드, 나이지리아, 폴란드, 대한민국, 루마니아, 르완다, 사우디아라비아, 싱가포르, 스페인, 우크라이나, 아랍에미리트, 영국, 미국

중국 아태우주협력조직 9개국(2024.2 현재)

방글라데시, 중국, 이란, 몽골, 파키스탄, 페루, 태국,터키

중국 국제달연구기지(ILRS) 10개국(2024.2 현재)

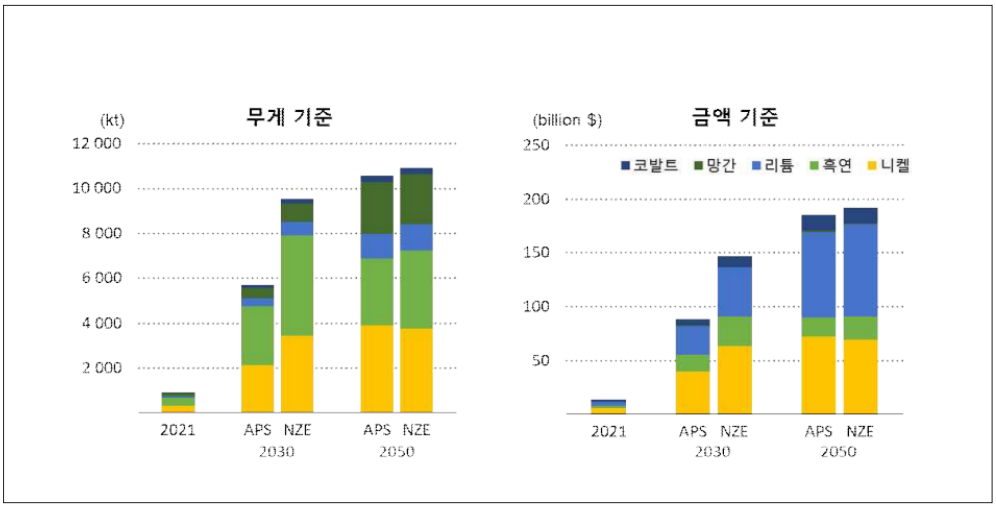
중국, 러시아, 베네주엘라, 남아프리카공화국, 아제르바이잔, 파키스탄, 벨라루스, 이집트, 태국, 니카라과(크로라티아, 아랍에미리트, 키르기스탄, 등은 대학 등이 참여, 터키는 4월에 참여 신청서 제출)

- (공급망 특성 및 과제) 전기차 배터리 핵심광물은 특정 국가에 매장 및 생산이 집중(리튬: 칠레·호주, 니켈: 인도네시아·호주, 코발트: 민주콩고·호주)되어 있으며, 정·제련은 중국이 주도(리튬 52.7%, 니켈 32.8%, 코발트 67.1%)하여 공급망 안정화가 어려운 상황임
- (국내 공급망 현황 및 한계) 한국은 전기차 배터리용 핵심광물(리튬, 니켈, 코발트, 망간 등)을 대부분 수입(리튬 87.9% 중국 의존)하며, 전구체 공정 내재화와 공급망 다변화를 추진 중이나 정·제련 기술 및 생산 설비가 부족함
- (주요 국가 및 기업의 자원 확보 동향) 중국은 남미·아프리카에서 대규모 자원 확보를 진행하고 있으며, 미국은 우방국 중심의 핵심광물안보파트너십(MSP)을 통해 공급망을 강화하며, 한국 기업은 LG에너지솔루션·포스코·SK온 등 주도로 리튬, 니켈 자원 다변화와 제련 시설 구축에 힘쓰고 있음
- (수요-공급 전망) 2025년 이후 리튬·니켈·코발트의 공급 부족이 심화될 것으로 예상되며, 망간은 배터리 수요 대비 공급이 원활하나 하이망간 배터리 개발 시 지정학적 이슈가 될 가능성 있음
- (공급망 안정화 전략) 국내외 자원 확보와 공급망 다변화를 위한 민관 협력, 정·제련 기술 내재화, 재활용 확대, 글로벌 협력 강화, 그리고 ESG 기반의 자원 개발을 통해 안정적 공급망을 구축해야 함

● **전기자동차로의 전환이 가속화되면서 핵심 광물 자원의 수요가 증가하고, 특정 국가에 대한 광물 의존도가 높은 현실을 배경으로 사용후 배터리 재활용 정책이 중요하게 대두되고 있음(김태헌 외, 2024)**

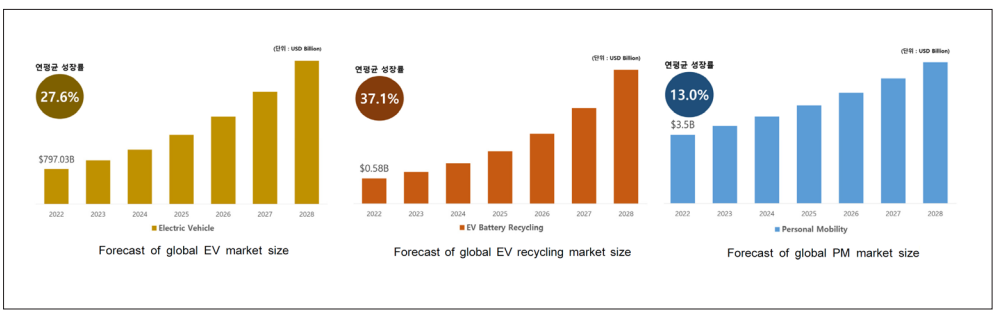
- (글로벌 재활용 배터리 전망) EV: 2022년 시장 규모 약 58억 달러, 연평균 성장률 37.1%로 자원 회수 기술 및 정책 강화 중. PM: 2022년 시장 규모 약 35억 달러, 짧은 배터리 수명으로 재활용 시장의 조기 대응이 필요함

그림 10 : 배터리 핵심광물 수요 현황 및 전망
(출처 : 이승필, 2023)



- (미국 인플레이션 감축법(IRA)) EV 배터리 소재의 재활용 비율 충족 시 세액 공제 혜택 부여. 미국 및 자유무역협정 국가에서의 소재 추출 및 가공 의무화. 자국 내 EV 공급망 재편으로 중국 의존도 감소를 추진함
- (EU 배터리법(Battery Regulation) 및 핵심원자재법(CRMA)) 배터리 재활용 의무화 및 원자재 회수 비율 규정(2030년 기준 리튬 80% 등). 역내 채굴 10%, 가공 40%, 재활용 25% 목표로 전략 자원 확보. 특정 국가에 대한 원자재 수입 의존도를 65% 이하로 감축함

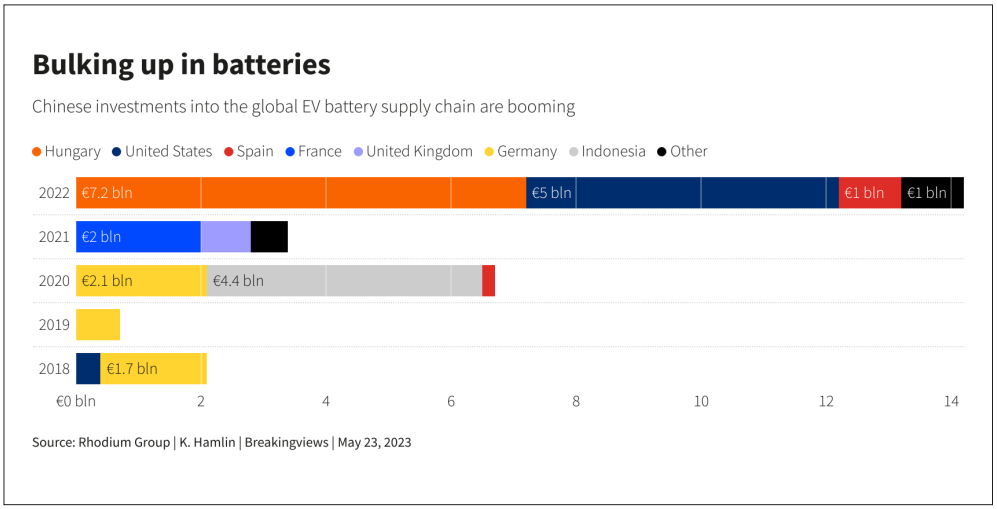
그림 11 : 글로벌 EV 및 PM 시장의 예상 규모
(출처 : 김태헌, 2024)



● EU는 미-중 갈등 이후 중국 의존도를 낮추기 위해 배터리 공급망 정책을 재정립하고 있음(안상욱, 2023)

- (EU의 배터리 산업 육성정책) 전기자동차와 배터리 산업 중심의 탄소중립 실현을 목표로 「유럽핵심원자재법」을 통해 채굴, 가공, 재활용 목표를 설정함
- (EU의 배터리 공급망 정책) EU는 배터리 핵심 원자재(리튬, 희토류 등)의 공급원을 다변화하고, 순환경제와 역내 자립도를 강조하며, 캐나다, 멕시코 등과 FTA를 추진함
- (EU 회원국의 배터리 공급망 정책) 독일과 프랑스 등은 EU 정책과 달리 중국과 경제협력을 강화하며, CATL, 르노 등 중국 기업과의 배터리 협력을 지속하고 있음
- 한국 기업은 EU 진출을 위해 핵심 원자재의 중국 의존도를 줄이고, EU 환경기준 충족 및 기술 경쟁력 확보 전략이 필요함

그림 12 : 글로벌 전기자동차 배터리 분야의 중국 투자
(단위: 10억 유로)
(출처 : REUTERS, 2023)

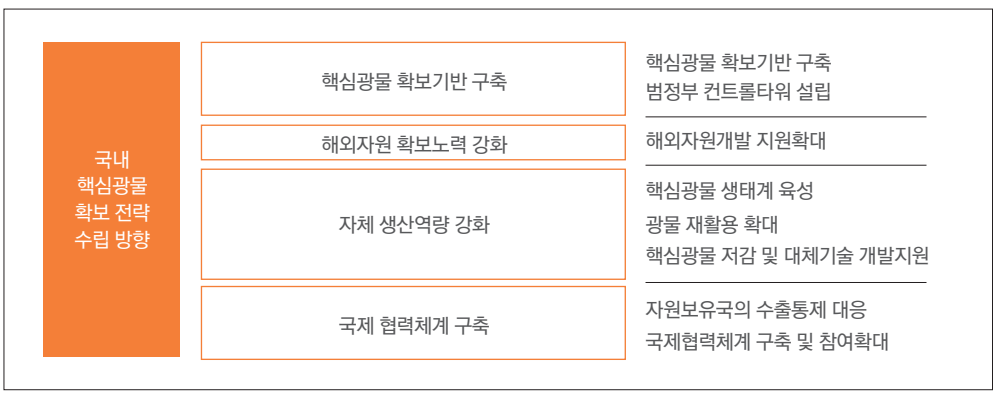


2-1-6. 광물

● **핵심광물은 신재생에너지, 전기차 등 첨단산업에 필수적이며, 각국은 안정적 공급망 구축과 자원 확보를 위해 국내 생산 확대, 국제 협력, 재활용 및 기술 개발을 강화하고 있음(글로벌공급망분석센터, 2022)**

- (핵심광물 정의와 활용) 핵심광물은 경제·안보 필수 원료로 신재생에너지, 전기차, 배터리, 방위산업 등에 사용되며 공급 리스크가 큼
- (공급망 이슈) 수급불안과 가격변동 심화, 생산·가공의 특정국 편중, 신규 광산개발의 낮은 성공률, 자원 민족주의 강화 등이 문제로 부각됨
- (미국의 핵심광물 전략) 자국 생산 역량 강화와 우방국 중심의 공급망 구축을 목표로 인프라 투자법(IIJA), 인플레이션 감축법(IRA) 등을 시행하며, 재활용 및 R&D 확대와 국제협력을 강화하고 있음
- (EU의 핵심광물 전략) '개방된 전략적 자율성' 아래 범유럽 협의체 및 공공기금을 활용해 역내 생산을 촉진하며, 국제협력을 통한 공급망 안정성과 자원 순환성을 강화하고 있음
- (중국의 핵심광물 전략) 희토류 등 주요 자원의 국내 통제 강화 및 해외 자원 지분 확보를 통해 글로벌 시장에서의 영향력을 확대하고, 고부가가치 자원의 해외 유출을 제한함

그림 13 : 국내 핵심광물 확보 전략 수립 방향
(출처 : 박가현, 2022)



- (한국의 대응 방안) 핵심광물 확보를 위해 국내 공급망 안정화 기반 마련, 범정부 컨트롤타워 설립, 재활용 및 대체 기술 R&D 확대, 국제 협력 체계 참여, 민간 지원 확대, 자체 생산 역량 강화를 추진해야 함

● 글로벌 공급망 재편과 자국우선주의로 핵심광물 수요가 폭증하며 주요국은 경제안보 강화를 위한 자원 집약적 구조로 변화하고, 한국도 독자적 핵심광물 전략 필요(김대용, 2024)

- (미국) 「핵심광물 확보를 위한 국가 전략(2010, 2019, 2021)」 발표, 자국 생산 확대와 우방국 중심 공급망 구축, IRA 및 CHIPS Act를 통한 법적 지원, 핵심광물안보파트너십(MSP) 활용
- (EU) 「핵심원자재법(CRMA)」을 통해 공급망 다각화, 핵심광물 자체 공급 강화, 대체물질 기술 개발 및 글로벌 협력(미국, 일본 등) 확대
- (중국) 광물자원을 국가 안보의 범위로 포함하고 일대일로 정책 아래 국제 협력 체제 구축, 민관 협력(PPP) 활성화, 전략적 광물 목록 관리
- (일본) 자원외교를 명시적으로 활용하며, 핵심광물 확보를 위한 개발원조, 정책금융, 무역보험 등을 통합하여 자원국과의 전략적 협력 추진
- (한국의 시사점) 국가적 핵심광물 지정 및 특정국 의존 완화를 포함한 공급망 안정화 전략 수립, 국제협력 플랫폼 활용 및 민간 참여 확대, 공급망 3법 기반의 법적 지원 강화
- (결론 및 제언) 범정부 컨트롤타워를 구축하고 글로벌 협력에 적극 참여하여 지속 가능한 자원 확보 및 경제안보 강화를 위한 정책 마련 필요

2-2. 신기술의 안보적 함의와 리스크 이슈 변화 양상

● 트럼프 2.0. 개막에 따른 MAGA(Make America Great Again) 전략에 따라 신기술 관련 외교 안보 환경의 변화에 큰 영향력을 미칠 것으로 예고됨

- 트럼프의 기조에 따르면 우크라이나군 지원 중단, 나토 탈퇴 등 글로벌 분쟁 개입 축소 시 전 세계 각국의 자체 방위력 강화 시도가 이어질 것이며, 실제로 이전 바이든 정부 때의 방위 산업 관련 ETF(AMS:ITA)보다 트럼프 행정부 취임 시기의 ETF 상승률이 훨씬 높은 것으로 나타남(매일경제 글로벌경제부, 2024)
- 최근의 미·중 과학기술협정(STA)의 5년 갱신 합의('24.12.)에는 국가 안보에 잠재적으로 중요한 AI와 양자컴퓨팅 등의 핵심 기술 영역의 협력은 제외되는 한계성을 나타냄(Natasha Gilbert et al., 2024)
- 미국 내 반도체 제조시설의 부재가 가져올 수 있는 안보 위협을 대응하기 위해 제정된 「반도체와 과학법(CHIPS ans Science Act, '22.8.)」 을 통해 미국 내 관련 시설 건립 시 보조금을 주었으나, 트럼프는 이러한 법이 대만의 TSMC 지원과 경쟁력 강화로 이어질 수 있는 것으로 보고 해당 법에 부정적 의견을 갖고 있음을 표한 바 있으며, 전기차, 배터리 등에 관세를 강화할 것을 표해 향후 산업의 발전에 많은 영향이 예고됨(매일경제 글로벌경제부, 2024)

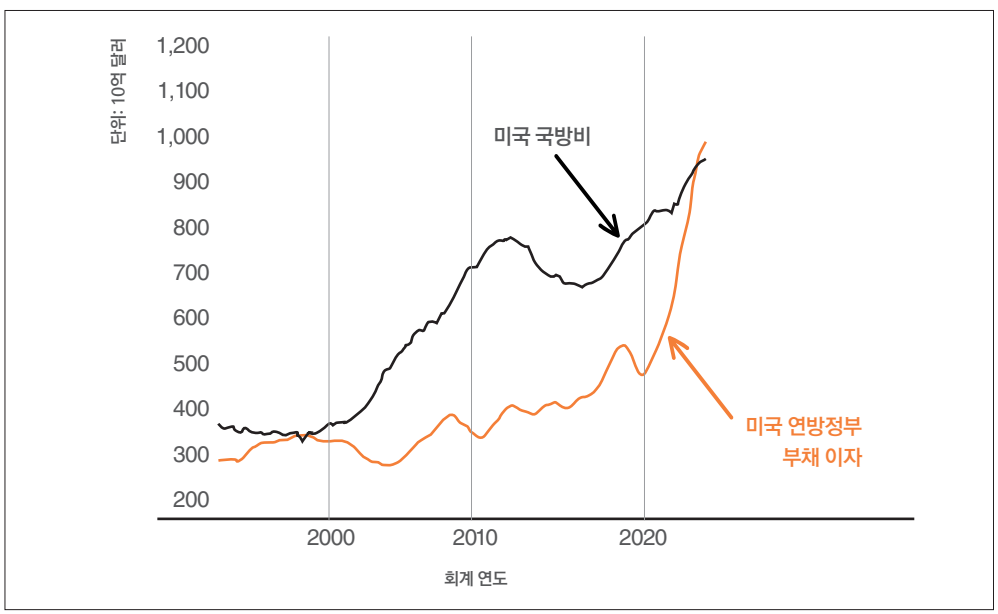
● AI 동맹체제의 다극화를 비롯한 신기술 분야의 글로벌 거버넌스 다극화·분극화 현상이 나타나고 있음(이원태, 2024(전문가 자문))

- 미국은 북미 중심의 동맹을 강화하고 있고, 트럼프 시대에는 다자 협력 보다는 1:1 관계의 협력을 선호하는 경향으로 분석되고 있으며, AI 분야에서는 최근 AISI 협력체계(글로벌 AI 안전연구소 협력체계)를 통해 거버넌스를 이루어가고 있는 모습을 보임
- 중국은 다자협력(사우디, 동북아 등)을 넓히며 중국 중심의 글로벌 공급망을 재편하고 있음(이원태, 조은교, 2024(전문가 자문))
- 미국과 중국으로 인해 Freind-shoring 국가 중심의 공급망이 구축되고, 기술블록화 심화 현상이 일어나는 반면, 각국의 기술 주권을 확보하기 위한 소버린 AI 현상이 나타남

● 국내외로 정세가 불안정성과 불확실성이 확대되며 국내의 정치 안보 환경에 미치는 위험성이 증가되고 있음

- 현재 미·중 양국관계는 cold peace(나라 간의 긴장과 갈등이 존재하나 직접적인 군사 대결이나 극단적 이념 대립, 전쟁으로는 이어지지는 않는 상태, Michael W. Doyle)에 가까우며 이런 상태는 지속될 것으로 전망(이원태, 2024(전문가 자문))
- 트럼프 2기 행정부 출범을 앞서고 국내에서 발생된 비상계엄과 탄핵 사태는 방위비분담특별협정(SMA)의 재협상(방위비 분담금, 주한미군 철수 등) 요구 가능성을 증가시키며, 한미동맹 악영향 등 트럼프 정부의 출범을 대비하지 못하는 사태로 우리나라에 큰 타격이 될 것으로 예상됨(연합뉴스, 2024)
- 미국의 정부 부채로 인한 이자가 미국의 국방비를 넘어서고 있기 때문에 미국의 국가안보전략도 점차 재정적 압력에 직면하며 방위비 분담금 증액, 주한미군의 임무 변화, 관세 등의 전략으로 향할 것이라는 분석이 있음(이만석, 2024)

그림 14 : 미국 연방정부 부채 이자의 추이와 미국 국방비
(출처 : 이만석, 2024)



3. 정책 및 인식

3-1. 신기술 안보 관련 정책 현황

3-1-1. 미국

● (정책) 미국은 중요 신흥 기술(CET)을 중심으로 산업적 측면과 안보를 연계해 정책을 추진하고 있음

- 바이든 행정부는「국가안보전략(National Security Strategy), 2022)」과 제이크 설리반 미국 국가안보보좌관의 발언('22) 등을 통해 신기술(AI, 양자, 바이오, 청정에너지 등) 관련 산업의 미국의 주도권 확보가 국가안보의 우선 순위이자 핵심요소로 인식하기 시작한 것이 나타남(정해영 외. 2024)
- CSIS(2024)에서는 중요 신흥 기술(CET)이 국가 안보에 필수적이며 특히 경제적 경쟁력과 국방이 밀접하게 연계되는 환경에서 기술 혁신을 리더하는 것이 국가 안보의 초석이 될 것이라고 밝히고 있음(Thibault Denamiel et al., 2024)
- 미국의 중요 신흥 기술(CET)은 '20년에 최초 발표된 이후 '24년까지 지속적으로 업데이트 되고 있으며 이 기술들의 주요 필러는 국가안보 혁신 기반 강화와 기술 우위 보호로 나뉨

● (거버넌스) 대중 체제의 강화와 양자 협력, 동맹국 강화를 통한 기술과 안보를 동시에 확보하는 전략으로 강화될 것으로 분석됨

- 미국의 대중국 전략은 중국의 산업적 육성과 군사적 용도 사용을 동시에 차단하기 위한 수출통제, 중국 첨단산업 관련 투자 제한으로 중국의 AI 추격을 지연시켜 미국과의 현 격차를 유지하고자 함(이승주, 2024)
- 미국은 유럽과 핵심광물자원 파트너쉽(미국 국무부 주도,'22.6.)을 맺으며 회원국 외에도 비회원국까지 관련 MSP 포럼에 참여 가능토록 협력 체제를 마련함
- 미국은 싱가포르와 전략적 파트너쉽을 맺어 주요 신흥기술(CET) 관련 핵심 인프라 및 기술 공급망 확보, 국방 혁신 등에 관해 두 차례('23.10, '24.8.) 대화를 진행함(미국 국방부, 2024)
- 미국은 트럼프 2.0. 시대에 신산업과 방위전략을 연계하며 방향을 바꿀 것으로 예고하고 있는데, 특히 우주 방위 산업에 있어 민간 부문과의 협력 강화, 동맹국과 민간 인트라를 포함한 파트너쉽 강화, 인공지능 연계를 위한 인공지능 혁신 지원 등을 골자로 함(김광석 외. 2024)

시대	주요내용
냉전 시대	소련의 핵심 군사용 기술에 대한 접근 저지 목적 – 나토 동맹국과 COCOM을 통한 對 공산권 수출통제 정책 · 통제 품목 조율
냉전 후	대량살상무기 제조에 필요한 물자 기술에 대한 불량국가 및 테러단의 접근 저지 – 최종사용자 기반 통제제도로 전환 – 핵공급그룹, 호주그룹, 미사일기술통제체제, 바세나르체제 등 다자수출통제체제 강화
트럼프 · 바이든 행정부	경제안보의 국가안보화 – 과학 · 기술 · 공학 · 제조 분야 글로벌 리더십 유지 및 국내 경제번영 목적을 국가안보 이익과 연결

표 4 : 미국의 수출통제 제도의 진화과정
(출처 : 정해영 외, 2024)

3-1-2. 유럽연합(EU)

● **(정책) EU는 경제안보를 중시하며 핵심 신흥 기술에 대한 잠재적 이중용도 기술(민간 산업, 국방)의 R&D를 촉진하고 투자를 확대하며, 포괄적 중심 전략으로 '전략적 자율성(strategic autonomy)'을 강화하며 주요국 의존도를 낮추고자 함**

- 유럽연합집행위원회(EC)는 「'23년 유럽경제안보전략 발표 이후 올해 유럽의 경제안보 강화를 위한 5대 계획(Advancing European economic security: an introduction to five new initiatives, '24.1.」을 발표하며 공급망 복원력, 핵심 인프라에 대한 물리적·사이버 보안, 기술안보 및 유출, 경제 의존성의 무기화 및 위협 등의 위험에 대응하기 위한 전략을 '촉진, 보호, 협력 측면'에서 마련함(한국과학기술기획평가원, 2024)
- EU의 경제안보의 핵심은 공급망의 안정성 확보로 특히 전기차, 배터리, 핵심 원자재에 대한 중국 의존도를 낮추고 자국 중심의 글로벌 공급망 재편을 향해 디리스킹(de-risking) 전략을 취하고 '개발된 전략적 자율성' 제고를 목표로 하고 있음(김경숙, 2024)
- EU는 '23년 「우주 안보 방위전략, '23.3.」 을 세우며 미국에 대한 높은 안보 의존도를 줄이고, 우주 안보를 사이버, AI, 핵, 공급망 등 다양한 안보 이슈를 포괄하는 복합 분쟁의 장으로 보며, 민간용 우주자산과 서비스를 군사용으로 전환하고, 위협탐지 역량을 제고해 '전략적 자율성'을 강화하고자 함(조은정, 2024)

표 5 : 주요 자원 의존국을 파악할 수 있는 주요국의 경제지표(2022)
(출처 : François CHIMITS et al., 2024)

	Market size (GDP, billion USD)	Trade openness (%)	Military expenses (share of GDP, %)	Nr of dependent products...	...in strat sec	...3 main origins	3 largest importers	Nr of dominant products	in strat sectors
USA	23315	19	3.5	494	155	1)CHN(63%) 2)EU(10%) 3)CAN(7%)	1)EU(17%) 2)CAN(15%) 3)MEX(15%)	68	28
China	17820	30	1.6	205	67	1)AUS(45%) 2)BRA(13%) 3)IDN(6%)	1)EU(17%) 2)USA(16%) 3)HKG(10%)	704	220
Japan	5006	30	1	538	168	1)CHN(55%) 2)AUS(12%) 3)EU(10%)	1)CHN(21%) 2)USA(17%) 3)EU(10%)	26	15
Republic of South Korea	1818	69	2.8	561	183	1)CHN(44%) 2)AUS(21%) 3)EU(7%)	1)CHN(25%) 2)USA(14%) 3)EU(10%)	6	4
European Union	17316	30	0.0*/1.5**	430	143	1)CHN(65%) 2)VNM(5%) 3)GBR(4%)	1)USA(18%) 2)GBR(13%) 3)CHN(11%)	289	94

Source: World bank WDI, SIPRI, Lefebvre and Wibaux(forthcoming) based on CEPII-BACI
Note: *EU level **Weighted average at Member State level.

● **(거버넌스) EU는 국제 협력 체제를 다극화하면서도 안보적 관점과 경제적 측면에서 주요국에 대한 의존도는 낮추면서 파트너 체제는 놓지 않는 전략을 지속하고 있음**

- EU는 핵심원자재법(CRM) 수립 이후 호주, 캐나다, 칠레, 미국 등 주요국과 긴밀히 협력해 CRM 공급망을 통합하고, 관련 포럼(Minerals Security Partnership Forum)을 통해 공급망의 다각화를 꾀함(Pawel Swieboda, 2024)

- 유럽은 러시아발 우크라이나 전쟁 이후 러시아에 대응하기 위한 수출 통제와 제재 측면을 고려해 전략을 세우고 있으며, 동시에 중국과의 디커플링을 피하며 디리스킹을 취하는 전략을 추진하고 있음. 미국도 마찬가지로 파트너 관계를 유지하면서도 의존하지는 않으려고 하는 전략적 자율성을 지속적으로 추진하고 있음(Emily Benson et al., 2024)

3-1-3. 중국

● (정책) 중국은 경제 안보를 국가 안보 핵심 요소로 여기며 광물 자원을 포함한 공급망 확보, 우주 안보, 기술 국산화 등 여러 안보 분야를 포괄하는 '종합적 국가 안보' 를 마련함(François CHIMITS et al., 2024)

- 중국은 「AI Plus 계획(AI plus initiative, 2024)」를 발표하며 미래 산업을 발전시키기 위해 다양한 산업에서의 AI의 적용을 심화하며 경제 성장을 촉진시키는 계획을 세움(조은교, 2024(전문가 자문))
- 중국 정부는 미국의 대중 반도체 제재에 맞서 '23년부터 1, 2차에 걸쳐 갈륨, 게르마늄, 흑연 관련 품목에 핵심광물 수출통제를 진행함(김경숙 외, 2023)
- 중국은 2000년대 이후 로켓, 인공위성 등 개발과 발사에 전폭적으로 지원하며 주요 성과를 내며 미래전에 대응하고 있음. 중국은 강군몽 전략의 핵심으로 '군사지능화'를 내세우며 AI와 정보통신체계를 연계하는 전략을 적극적으로 모색하고 있음(이동규, 2023)

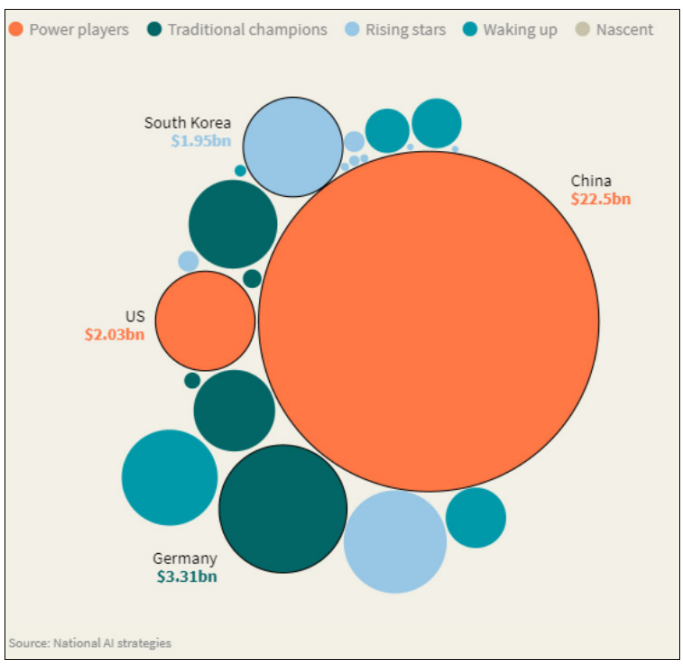
● (거버넌스) 미국 중심의 국제협력 거버넌스에만 국한할 것이 아니라 AI 강대국이자 핵심 광물 자원을 보유한 중국을 고려한 협력 체제 마련도 필요함

- 우리나라가 중국과의 관계를 신중하게 관리해 경제적 이익과 안보를 균형 있게 고려해 국익을 극대화하면서도 중국에 대한 경제의존도를 낮춰 글로벌 공급망의 안정적 위치를 확보하고 자립적 역량을 강화하는 것이 필요함(이만석, 2024)
- 바이든 정부의 첨단기술 관련 제재가 오히려 중국의 국산화를 촉진시켰고, 기술의 산업화 전략을 강조하며, 막강한 자본과 정책 지원으로 트럼프 정부에 대응 가능한 체제가 갖춰짐. 중국이 AI를 비롯 신기술 분야의 글로벌 리더쉽을 차지할 가능성도 배제할 수 없기에 우리정부의 대응 마련이 필요함(조은교, 2024(전문가 자문))
- 중국은 미국과 AI 경쟁력을 다투며 양회를 통해 미국이 제재한 기술을 본격 양성하겠다며 정책을 발표했고, 중동 자본 확보부터 동남아 전자상거래 진출까지 글로벌 확장을 꾀하며 기술의 산업화·응용화를 빠르게 이루어나가고 있음(조은교, 2024(전문가 자문))
- 핵심광물의 공급망 회복력 강화와 수입선 다변화를 위한 국제협력 파트너 참여 확대가 필요함(김경숙 외, 2023)

그림 15 : 세계 주요국 AI 역량내 중국이 2순위 차지
(출처 : 이승주, 2024)

	Overall	Talent	Infrastructure	Operating Environment	Research	Development	Government Strategy	Commercial	Scale	Intensity
United States	1	1	1	28	1	1	8	1	1	5
China	2	20	2	3	2	2	3	2	2	21
Singapore	3	4	3	22	3	5	16	4	10	1
United Kingdom	4	5	24	40	5	8	10	5	4	10
Canada	5	6	23	8	7	11	5	7	7	7
South Korea	6	12	7	11	12	3	6	18	8	6
Israel	7	7	28	23	11	7	47	3	17	2
Germany	8	3	12	13	8	9	2	11	3	15
Switzerland	9	9	13	30	4	4	56	9	16	3
Finland	10	13	8	4	9	14	15	12	13	4
Netherlands	11	8	16	15	10	13	28	20	11	8
Japan	12	11	5	10	20	6	18	23	6	25
France	13	10	11	25	15	18	13	10	9	20
India	14	2	59	12	30	21	38	13	5	51
Australia	15	14	44	62	6	16	14	22	15	14
Denmark	16	19	15	1	18	19	21	17	18	11
Sweden	17	15	21	2	13	17	44	16	19	12
Luxembourg	18	31	6	14	19	22	31	14	33	9
Ireland	19	17	26	19	27	10	29	15	28	13
Austria	20	25	34	5	16	23	33	27	22	18
Spain	21	18	18	16	24	26	4	32	12	28
Belgium	22	26	43	24	14	25	36	25	23	19
Italy	23	22	35	6	21	28	9	35	14	33
Norway	24	24	22	29	22	20	39	21	30	16

그림 16 : 주요국 AI 투자 규모 및 형태
(출처 : 이승주, 2024)



3-2. 신기술 안보 관련 인식

3-2-1. 인공지능 관련 인식 조사(국내)

● 한국리서치의 인공지능 기획 설문 시리즈에 따르면 인공지능 기술에 대한 관심도와 체감도는 모든 세대·학력에서 7-80% 상회, 반면 인공지능 기술 발전으로 사생활 침해 문제가 커지고(71%), 빈부격차가 늘고(64%), 인간 능력이 저하될 것(52%)으로 예상

- 작년 대비 인공지능 관심도는 30대, 50대, 고졸 이하에서 10%p 이상 증가, 인공지능 체감도는 40대, 50대, 고졸 이하에서 10%p 이상 증가
- 인공지능에 대한 감정은 호기심과 기대감이 매우 높은 동시에 의심스러움과 두려움도 높은 편, 연령별 차이도 두드러진데 50대 이상은 65% 이상이 두려움을 표한 반문, 20대는 56%로 10%p 차이 보임, 반면 친근감의 경우 60대 이상이 50%인 데 비해 20대는 37%로 현격히 낮음
- 특히 인공지능 기술 발전 체감도에 따른 차이가 가장 두드러지는데, 체감하는 그룹은 의심스러움과 두려움이 각각 44%, 50%로 체감하지 못하는 그룹(65%, 64%)에 비해 15%p 이상 높음

표 6 : 한국리서치 인공지능 설문조사 기획 시리즈 주요 결과 (2019~24)
(출처: 한국리서치, 2024)

조사연월	조사 제목	주요 조사 결과
2019.07	로봇 저널리즘과 기자의 역할 변화	인공지능 작성 기사 증가가 바람직하지 않다는 의견(42%)과 달리 인공지능이 쓴 기사가 기자가 쓴 기사보다 중립성, 신뢰성에서 더 낫다는 평가
2020.02	AI 시대와 우리의 미래	10명 중 9명, AI에 대해 들어본 적 있음, AI 이해도는 남자, 40대 이하, 고학력자에서 높아
2021.04	AI와 인간의 공존, 그리고 윤리성	10명 중 9명, AI가 도덕성을 갖춰야 한다고 생각, 81%가 AI의 차별적 표현 심각하다고 인식
2021.05	인공지능(AI)이 우리 사회에 미치는 영향과 직업별 역할 수행	10명 중 9명, 인공지능 기술 발전이 개인 및 사회에 긍정적이라 인식, 인공지능 기술 발전으로 생활의 편리성 및 삶의 질 증대(65%) 가장 기대되고 일자리 감소(39%)가 가장 우려돼
2022.10	자율주행 기술에 대한 엇갈린 시선 – 높은 기대감과 불완전한 신뢰	응답자 3분의 2(66%), 20년 내 완전 자율주행 자동차 보편화 예상, 자율주행 차량에 탑승해도 언제든 자동차를 제어할 수 있도록 준비할 것 72%
2023.05	주요 영역별 인공지능(AI) 발전 평가 및 직업 수행 전망	논리수학지능, 음악지능, 시공간지능 등은 AI가 인간보다 뛰어나다는 평가가, 자연지능, 실존지능, 인간친화지능 등은 AI가 인간을 따라잡지 못했다는 평가가 다수
2023.06	인공지능, 양날의 검? 발전 체감도와 미래 변화 예측	인공지능이 '나의 삶'에 미치는 영향은 '긍정도 부정도 아냐'(57%), '우리 사회'에는 '긍정적(61%), AI 기술 발전으로 사생활 침해 문제가 커질 것(72%)
2023.06	생성형 인공지능 사용 경험 및 예술 분야에서의 활용 전망	LLM 기반 대화형 인공지능 서비스 사용 경험 있는 사람은 34%, 일상생활(51%), 업무나 학업(48%), 자기계발이나 학습(41%) 등 다양한 상황에서 대화형 인공지능 사용, 대화형 인공지능 서비스 사용 경험자 중 75%가 결과물에 만족, 대화형 인공지능의 결과물, 실사용자의 평가가 미사용자의 예상보다도 20%p 이상 높음
2024.01	인공지능 시대의 도래, 우리는 무엇을 두려워하고 무엇을 기대하나	대화형 인공지능 사용 경험은 아직 인공지능 번역기나 음성인식 시스템보다는 낮아, 인공지능이 상용화된 미래 긍정적으로 보는 편 76%, 그러나 인공지능으로 인해 '해킹 발생 가능성(87%)', '인간의 노동력 대체(85%)', '행위주체 설정 문제(83%)', '불평등 심화(80%)' 등 다양한 문제 발생 염려

2024.06	인공지능 관심 및 발전 체감도, 미래 변화 인식	인공지능에 관심 있으면서 이를 체감하는 사람은 86%, AI 기술 발전으로 사생활 침해 문제가 커질 것(71%), 빈부격차가 심해질 것(64%)', 인간 능력이 저하될 것(52%)으로 예상, 10명 중 6명 우리나라가 인공지능으로 인한 문제 발생 대처를 잘하고 있지 못하다고 인식
2024.10	AI 기술의 도입과 업무 활용 인식	근로자 78%, AI 기술 활용 능력 떨어져 경쟁력 떨어지고 저평가 될 수 있다는 불안감 느껴, 사업체 단위 AI 기술 도입 비율 30%, 개인 단위 활용 비율 31%로 비슷한 수준, AI 기술이 업무 효율성 개선에 긍정적 영향 64%, 업무 처리 시간 단축 77%, 기술 보안 및 개인정보 유출 우려에도 64%가 공감

그림 17 : 인공지능 체감도 변화
(출처: 한국리서치, 2024)

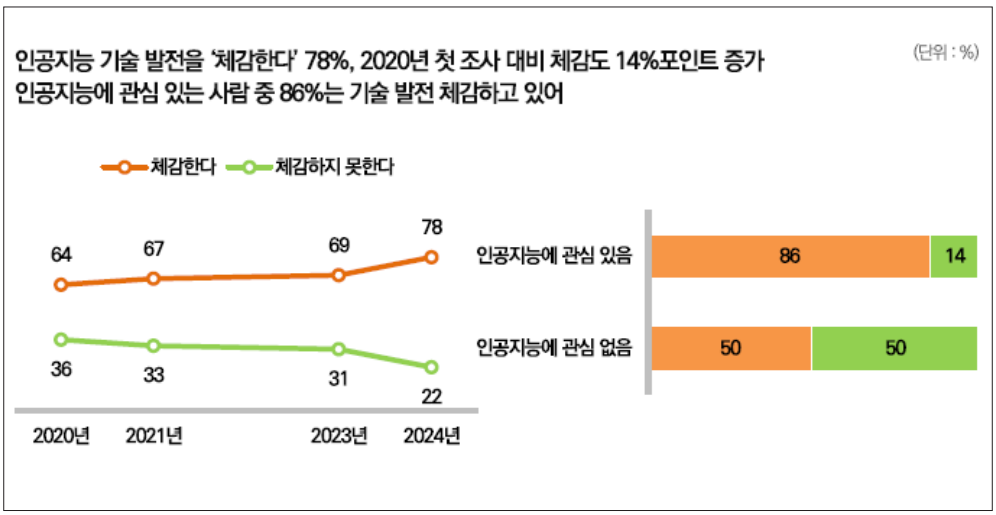


표 7 : 인공지능 기술 발전에 대한 감정
(출처: 한국리서치, 2024)

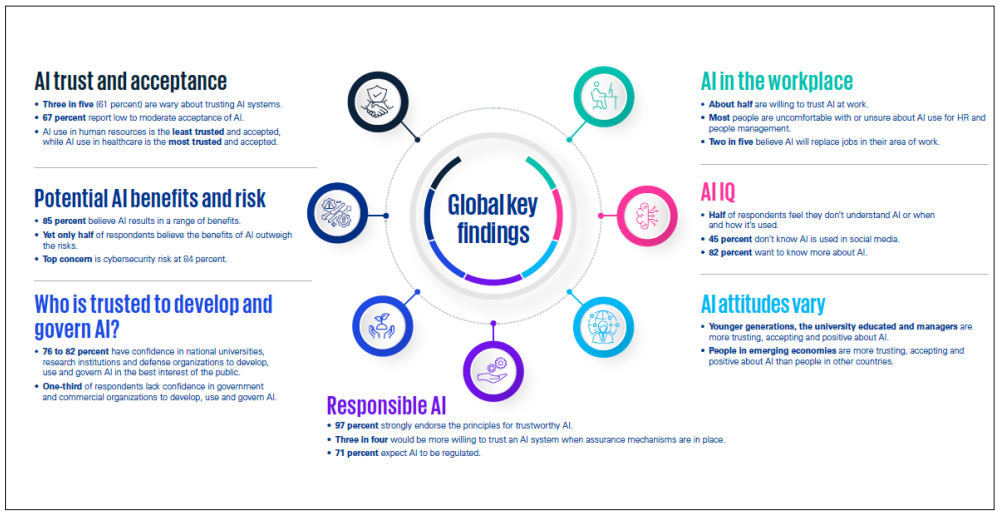
2024년 6월 조사	사례수 (명)	호기심	기대감	의심스러움	두려움	친근감	적대감
전체	(1,000)	83	82	61	61	45	36
연령							
18-29세	(159)	80	79	63	56	37	36
30대	(149)	83	80	62	50	38	34
40대	(177)	86	84	61	60	48	35
50대	(196)	78	77	59	65	42	38
60대	(173)	86	84	60	68	54	38
70세 이상	(146)	84	88	59	65	53	34
인공지능 관심도							
관심 있다	(793)	90	88	64	65	51	38
관심 없다	(207)	56	59	50	47	25	28
인공지능 기술 발전 체감도							
체감한다	(782)	89	87	65	64	50	37
체감하지 못한다	(218)	63	65	44	50	28	31

3-2-2. 인공지능 관련 인식 조사(해외)

● KPMG와 University of Queensland가 호주, 브라질, 캐나다, 독일, 프랑스, 핀란드, 이스라엘, 싱가폴, 인도, 중국, 일본, 한국 등 17개국 17,000명 이상 조사한 비교국가 설문조사(2020년 실시, 2023년 분석결과 발표)에 따르면 5명 중 3명(61%)가 AI 시스템 신뢰성에 의구심을 가지는 것으로 나타남

- 앞선 국내 설문조사와 비슷하게 85%가 AI의 혜택에 동의하나 73%가 리스크도 존재한다고 응답, 특히 가장 큰 우려로 사이버보안을 거론(84%)
- 5명 중 4명이 AI에 대해 알고 있으나 실제로 AI가 어떻게 작동하는지에 대해서는 절반 이상이 모른다고 답, 한편 젊은 세대와 고학력자들이 AI에 대한 신뢰나 수용성이 높음

그림 18 : AI 신뢰성에 대한 다국가 설문조사
(출처 : KPMG & University of Queensland, 2023)



3-2-3. 사이버 보안 관련 인식 조사

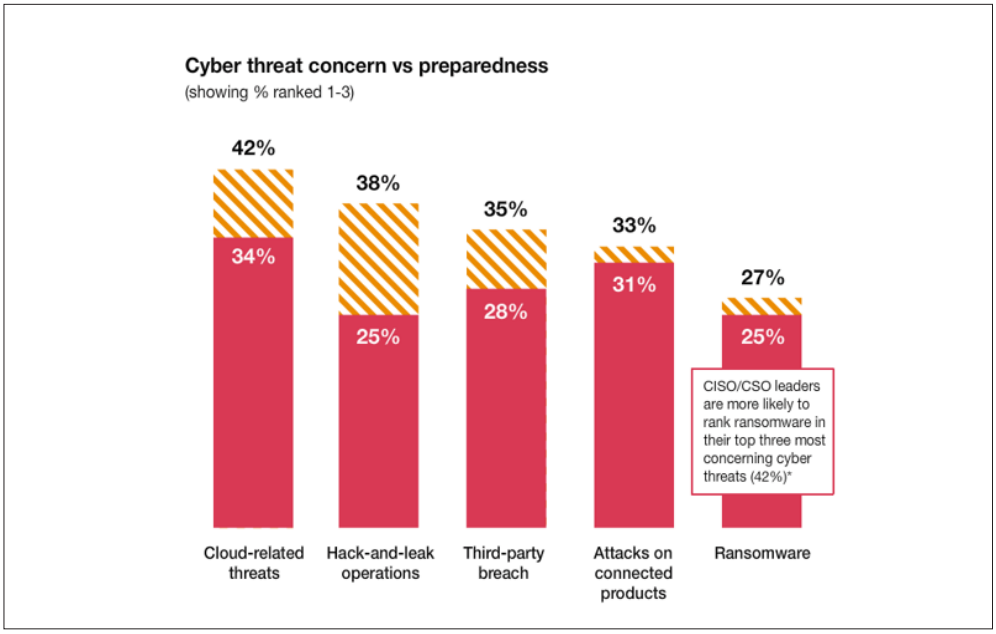
● Ernest & Young LLP가 2022년에 이어 올해 실시한 <2024 Human Risk in Cybersecurity Survey>에 따르면 85%가 AI로 인해 사이버 공격이 더욱 치밀해졌다고 응답

- 미국 공공 및 민간 부문 종사자 1,000명을 대상으로 실시한 동 조사에서는 세대간 차이도 두드러지게 나타남
- 디지털 네이티브임에도 Z 세대는 31%만이 피싱 공격을 자신있게 식별해낼 수 있다고 응답했는데 이 수치는 22년에 비해 무려 9%p가 낮은 결과임, 또한 Z 세대는 의심스러운 링크를 열어보는 비율이 72%에 달했는데, 이는 다른 세대(M 세대-51%, X 세대-36%, 베이비부머-26%)보다 현저히 높음

● 77개국 4,042명의 비즈니스/테크 리더들을 대상으로 실시한 PwC의 <2025 Global Digital Trust Insights>에 따르면, 사이버 위협 증가에도 불구하고 2%만이 소속기업에서 사이버 회복력 관련 대책을 마련하고 있다고 응답

- 동 조사에서는 가장 취약한 사이버 위협으로서 클라우드 기반 위협(42%)이 가장 많이 거론하였고, 해킹(38%), 제3자 침입(35%), 연계 상품 공격(33%), 랜섬웨어(27%) 순이었음. 반면, 사이버 위협에 대한 준비 정도는 해킹과 랜섬웨어 공격이 가장 덜 준비된 것으로 나옴

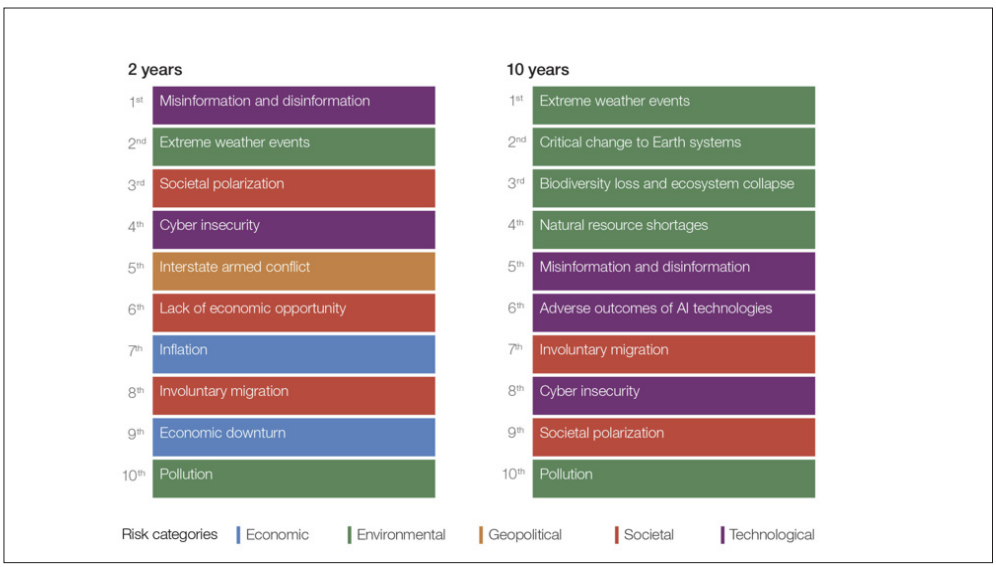
그림 19 : 비즈니즈/테크 리더들의 사이버 위협 우려 vs 준비 정도 인식
(출처 : PwC, 2024)



● 세계경제포럼(WEF)의 <2023-24 Global Risks Survey>에서는 허위정보와 사이버 불안이 향후 2년 내 가장 심각한 리스크 리스트에서 각각 1위, 4위 차지

- 10년 내 가장 심각한 리스크에서도 허위정보, AI 기술 부작용, 사이버 불안이 각각 5위, 6위, 8위 차지

그림 20 : WEF 10대 리스크 중 사이버 보안 관련 순위
(출처 : WEF, 2024)



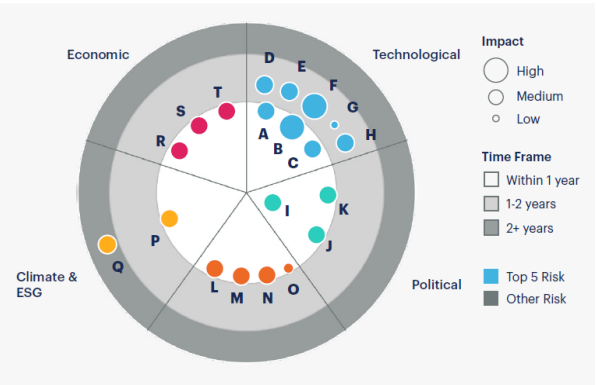
● **미국의 대표적 정보기술 컨설팅 기업인 Gartner에서는 분기별로 20개의 신흥 리스크 관련 사건·원인·결과 등의 분석을 제공하는데, 2024년 3분기 <Quarterly Emerging Risk Report>에 의하면 기술 관련 리스크가 8개로 가장 많을뿐더러 1~2년 내 도래할 것으로 예상**

- 10년 내 가장 심각한 리스크에서도 허위정보, AI 기술 부작용, 사이버 불안이 각각 5위, 6위, 8위 차지
- 지난 1년간 분기별 상위 5개 신흥 리스크에서도 AI 및 사이버 보안 관련 리스크가 1~2위 차지, 특히 AI로 인한 악성 공격이 지난 세 분기 동안 계속 1위를 차지해 사이버 보안에서 AI의 중요성에 대한 인식이 매우 높음을 시사함

그림 21 : 2024년 3분기 신흥 리스크 지형
(출처 : Gartner, 2024)

3Q24 Emerging Risk Universe Map

#	Risk category	Risk Name	
A	Technological	AI-Assisted Misinformation	
B	Technological	AI-Enhanced Malicious Attacks	
C	Technological	AI Intellectual Property Control	
D	Technological	Energy Shortages	☆
E	Technological	Information-Governance-Driven AI Risks	☆
F	Technological	IT Vendor Criticality	☆
G	Technological	Misaligned AI Ambition	
H	Technological	Soft Ransomware Targets	
I	Political	Globally Consequential Elections	
J	Political	New Geopolitical Partnerships	
K	Political	Unsettled Regulatory and Legal Environment	☆
L	Talent	Decline in Employee Productivity	
M	Talent	Employee Misuse of AI	
N	Talent	Misaligned Organizational Talent Profile	
O	Talent	Shifting Attitudes About In-Person Work	☆
P	Climate & ESG	Climate Activism	
Q	Climate & ESG	Extreme Heat Consequences	
R	Economic	Consumer Spending Slowdown	☆
S	Economic	Delayed Interest Rate Lowering	
T	Economic	Stagflation Expectations	



Note: Bubble placement within a ring does not indicate absolute time frame value.
Source: 3Q24 Gartner Emerging Risks Survey, n = 286. ☆ = new to emerging risk universe in 3Q24

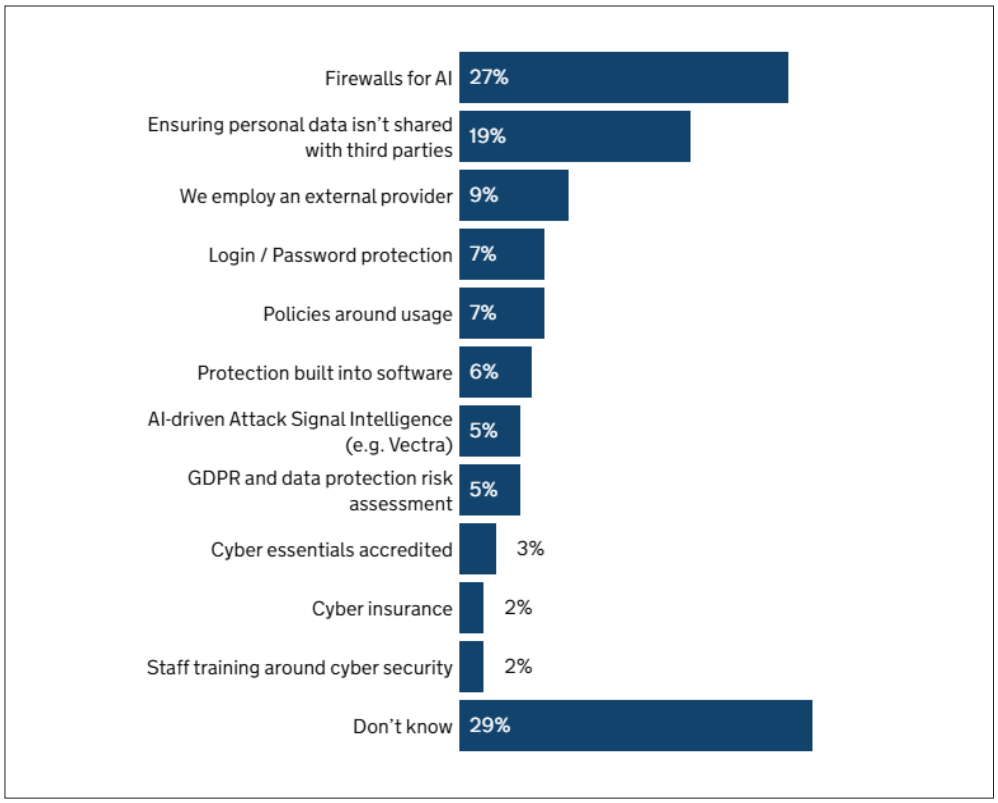
그림 22 : 2023년 4분기~ 2024년 3분기 5대 신흥 리스크 순위
(출처 : Gartner, 2024)

Rank	4Q23	1Q24	2Q24	3Q24
1	Mass Generative AI Availability	AI-Enhanced Malicious Attacks	AI-Enhanced Malicious Attacks	AI-Enhanced Malicious Attacks
2	Escalating Political Polarization	AI-Assisted Misinformation	Soft Ransomware Targets	IT Vendor Criticality
3	Cloud Concentration Risk	Escalating Political Polarization	Escalating Political Polarization	Unsettled Regulatory and Legal Environment
4	Overzealous Cost Cutting	Globally Consequential Elections	Misaligned Organizational Talent Profile	Globally Consequential Elections
5	Market Effects From Higher Borrowing Costs	Misaligned Organizational Talent Profile	AI-Assisted Misinformation	Misaligned Organizational Talent Profile

● **영국 정부가 350여개 영국 내 업체를 인터뷰해 올 상반기 발표한 <AI Cybersecurity Survey>에 따르면, 현재 40% 업체가 AI를 쓰고 있고, 50% 업체가 쓸 계획이 있다고 답한 반면, AI 기술과 관련된 사이버 보안 조치를 취한 비율은 매우 낮은 것으로 나타남**

- AI 방화벽이 27%로 비교적 높으나 다른 조치들은 개인 정보의 제3자 미공유(19%), 로그인 정보 보호(7%), AI 기반 공격 탐지(5%), 사이버 보안 관련 직원 교육·훈련(2%)로 매우 미흡한 수준

그림 23 : AI 활용 중이거나 계획 중인 업체의 AI 관련 사이버 보안 조치 수준
(출처 : UK Government, 2024)



4. 전문가 네트워크 구축

4-1. 전문가 자문 진행

● 세계신안보포럼 세션의 사후 분석 보강을 위해 아래와 같이 국내 전문가를 인터뷰하고 아래와 같이 기술, 정책, 거버넌스 국제협력 관점의 이슈와 시사점을 도출함 (보다 자세한 인터뷰 내용은 부록 1 참고)

표 8 : 국내 전문가 자문 진행

성명	소속 및 직책	자문 형태	자문 일시	분야
이원태	아주대학교 소프트웨어융합대학 사이버보안학과 연구교수 (前 한국인터넷진흥원 원장)	전문가 그룹 인터뷰(FGI)	2024.12.06.	정치학, 사이버안보
조은교	산업연구원 산업통상연구본부 글로벌산업실 연구위원		2024.12.06.	산업경제·정책, 중국경제
양정윤	국가보안기술연구소 안보정책연구실 선임연구원		2024.12.06.	외교, 사이버안보
김양규	동아시아연구원(EAI) 사무국장, 수석연구원, 서울대 정치외교학부 강사	서면 진행	2024.12.17.	국제안보, 외교정책
이중구	한국국방연구원 안보전략연구센터 연구위원		2024.12.17.	전략외교, 외교정책

그림 24 : 전문가 그룹 인터뷰(FGI) 운영 모습

● (기술 관점) AI 개발이 특정 국가에 집중되면서 기술 의존성과 글로벌 불균형이 심화될 가능성이 높아짐. 산업 전반에 걸친 AI 융합이 가속화되며 국가 경쟁력의 핵심으로 부상하고 있음. 또한, AI 기술은 안보와 평화에 복합적 영향을 미치므로 인간 통제와 설명 가능성을 강화해야 함

- AI 개발이 특정 국가 중심으로 이루어지면서 기술 의존성이 증가하고, 이로 인해 글로벌 불균형과 지정학적 갈등이 심화될 가능성이 높아짐. 특히, 중국과 미국 간의 기술 패권 경쟁이 글로벌 AI 생태계를 블록화하는 양상을 띠고 있음
- AI와 제조업, 자율주행, 스마트 팩토리와 같은 산업 간 융합이 가속화되고 있으며, 이는 산업 전환을 주도하는 핵심 기술로 자리 잡고 있음. 이러한 기술적 융합은 국가 경쟁력의 핵심 요소로 작용하나, 이에 대한 준비와 정책적 대응이 미흡한 국가는 경쟁에서 뒤처질 가능성이 있음

- AI를 비롯한 신기술의 다분야 연계는 국제 평화 및 안보에 복합적인 영향을 미치며, 특히 '핵 얽힘'과 '블랙박스 문제'로 인해 재래식 및 핵 무기 시스템에서 오판 가능성을 증가시키므로, 기술 개발 과정에서 인간 통제 유지 및 설명 가능성 개선이 필수적임

● **(정책 관점) 한국은 AI 거버넌스 주도권 상실과 법제 부재로 경쟁력 저하 우려가 있음. AI를 전통 산업에 접목해 산업 혁신을 추진하고, 중소기업 지원 정책을 강화해야 함. 또한, 미국과의 협력을 통해 글로벌 리더십을 강화하고 기술 정책 플랫폼을 구축해야 함**

- 한국은 AI 거버넌스 논의에서 주도권을 상실하고 있으며, 관련 법제 및 정책의 부재로 인해 AI 경쟁력이 저하될 우려가 있음. 글로벌 AI 표준 설정과 관련된 정책적 준비와 법제 정비가 시급히 요구됨
- 한국은 AI 기술을 전통 산업에 접목하여 스마트 제조 전환 및 산업 혁신을 추진할 필요가 있음. 이를 위해 AI 산업 정책을 신속히 수립하고, 중소·중견 기업을 지원하는 정책적 기반을 강화해야 함
- 한국은 신기술 분야에서 미국 주도 질서와의 조기 협력을 통해 글로벌 리더십을 강화하며, 한미 국방 및 과학기술 네트워크를 기반으로 최신 기술 정책 동향을 공유하는 플랫폼을 구축해야 함

● **(거버넌스 관점) 각국은 소버린 AI 정책을 강화하며 AI를 둘러싼 국가 경쟁이 심화되고 있음. 다자간 협력으로 새로운 국제 규범을 수립하고, 중소 국가의 역할을 강화할 거버넌스 개선이 필요함. 또한, 민·관·학 협력을 통해 융합적 교육 플랫폼과 지속 가능한 기술 거버넌스를 마련해야 함**

- 각국은 AI 기술의 국가적 활용을 목표로 소버린 AI 정책을 강화하고 있으며, AI를 핵무기처럼 통제하려는 논의도 진행 중임. 이러한 흐름은 AI를 둘러싼 국가 간 경쟁을 심화시키고 있음
- AI 기술과 사이버 보안 이슈에 대해 다자간 협력 체계를 강화하여 새로운 국제 규범을 수립해야 함. 특히, 강대국 중심의 AI 동맹을 견제하고, 중소 국가의 역할을 강화할 수 있는 거버넌스 개선 방안이 필요함
- 민·관·학·투자·시민사회 간 협력을 통한 융합적 교육 플랫폼을 설계하고, 신기술의 경제·안보적 활용을 위한 국가 전략과 시험적 연구환경을 조성하여 지속 가능한 기술 거버넌스를 확립해야 함

● **(국제협력 관점) 미·중 기술 패권 경쟁은 국제 질서를 다극화시키고 있으며, 글로벌 AI 생태계를 블록화하는 양상으로 전개되고 있음. 국제 사회는 이러한 경쟁 속에서 협력의 필요성을 제기하며, AI 격차 해소를 위한 지원 방안을 모색하고 있음**

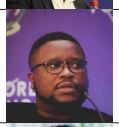
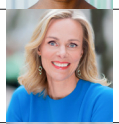
- AI 기술의 확산이 국제 평화와 안보에 잠재적 위험 요소로 작용하지 않도록, 평화적 활용을 촉진하는 국제 협력이 필요함. 특히, AI 기술을 통한 군사적 긴장 고조를 방지하기 위한 다자 협약이 요구됨

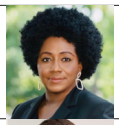
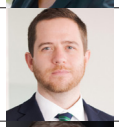
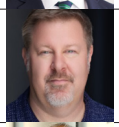
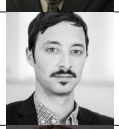
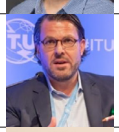
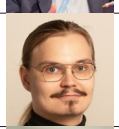
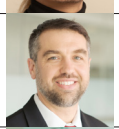
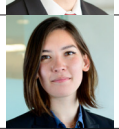
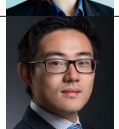
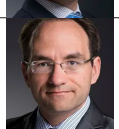
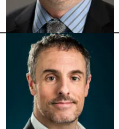
- 한국은 중동 및 동남아와의 협력을 통해 AI 및 사이버 보안 인프라를 강화하고 있으며, 이를 통해 글로벌 AI 생태계에서의 경쟁력을 확보할 수 있음. 이러한 협력 모델은 국제적 대응 방안으로 주목받고 있음

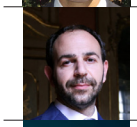
4-2. 기술별 전문가 풀

● 세계신안보포럼 및 국내 전문가 라운드테이블 기획을 위해 약 80여 명의 해외 전문가를 발굴함

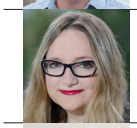
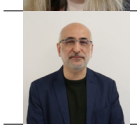
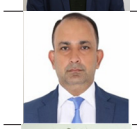
- 인공지능 분야 전문가는 AI 기술 혁신, 윤리, 정책, 거버넌스, 안보 및 보안 관련 30여 명을 발굴함

	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, Government of Bangladesh / United Nations Development Programme · AI and Digital Promotions Policy
	Dr. Hammam Riza	· President, 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 in 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, Australian National University · Defence Studies, Politics and International Relations
	Dr. Urs Gasser	· Dressor of Public Policy, Technology University of Munich & Harvard Berkman Klein Center · Technology Governance
	Mr. Onni Aarne	· Consultant, Institute for AI Policy and Strategy · Compute and Governance of AI
	Dr. Paul Scharre	· Executive Vice President and Director of Studies, Center for a New American Strategy (CNAS) · Unmanned and Autonomous Systems
	Ms. Ainikki Riikonen	· Policy Analyst, Office of Science and Technology Policy (OSTP) · AI and Information Systems in the International Competition
	Dr. Li Ang Zhang	· Codirector, Center for Scalable Computing and Analysis, RAND Corporation · Applying Machine Learning on Defense and Military Technology Policy
	Dr. Edward Geist	· Dressor of Policy Analysis, Pardee RAND Graduate School · Potential Impact of Emerging Technologies on Nuclear Strategy
	Dr. Aaron B. Frank	· Acting Associate Director, Acquisition and Technology Policy Program, RAND Corporation · Analytic Tradecraft, Decision-Support Tools for Analyzing Complex Security Issues
	Dr. William Marcellino	· Senior Behavioral and Social Scientist, Professor of Policy Analysis, Pardee RAND Graduate School · AI Technology Application, Acqusition

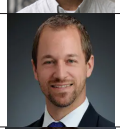
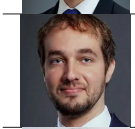
	Dr. John Villasenor	· Professor, Department of Electrical Engineering, UCLA · Information Technology, Artificial Intelligence
	Mr. Fabio Rugge	· Deputy Permanent Representative of Italy, NATO · Cyber Security, Artificial Intelligence
	Dr. Andrew Lohn	· Director of Emerging Technology, National Security Council, The White House · Policy in AI and Cybersecurity
	Dr. Diana Gehlhaus	· Defense Department Fellow, Center for Security and Emerging Technology; Department of Defense · Human Resource Management in Artificial Intelligence
	Dr. Margarita Konaev	· Deputy Director of Analysis, Center for Security and Emerging Technology · Military Applications of Artificial Intelligence

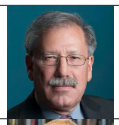
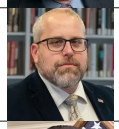
– 사이버 보안 분야 전문가는 사이버 정책, 사이버 보안, 디지털 포렌식 등 관련해 15여 명을 발굴함

	이름	소속 · 직위 / 전문분야
	Dr. Jason Healey	· Senior Research Scholar at Columbia University's School of International and Public Affairs · Cyber conflict history and policy
	Dr. Gregory Falco	· Assistant Professor at Johns Hopkins University · Aerospace security and cybersecurity for space systems
	Dr. Andrea M. Matwyshyn	· Professor of Law and Engineering at Penn State University · Intersection of law, technology, and cybersecurity policy
	Dr. Hamid Jahankhani	· Professor at the University of East London · Cybersecurity, privacy, and digital forensics
	Dr. Arshad Jamal	· Researcher at the University of East London · Cyber defense tactics and countermeasures
	Dr. Shaun Lawson	· Professor at Northumbria University · Human-computer interaction and cybersecurity
	Dr. Eileen Donahoe	· Special Envoy for Digital Freedom at the U.S. State Department · Digital policy and human rights
	Mr. Nathaniel Fick	· U.S. Ambassador-at-Large for Cyberspace and Digital Policy · Cyber diplomacy and international cybersecurity policy

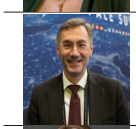
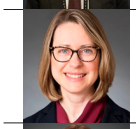
	Mr. Colin Ahern	· Chief Cyber Officer for New York State State-level cybersecurity initiatives and public-private partnerships
	Mr. George Kurtz	· CEO of CrowdStrike · Cyber threat intelligence and incident response
	Mr. Neil J. Walsh	· Regional Representative for Eastern Africa, United Nations Office on Drugs and Crime (UNODC) · Cybercrime, anti-money laundering, counter-terrorism
	Ms. Allison Pytlak	· Senior Fellow and Director of the Cyber Program, Stimson Center · Inter-state cyber operations, international cyber governance, United Nations processes
	Ms. Manon Le Blanc	· Coordinator for Cyber Issues, European External Action Service (EEAS) · Cyber diplomacy, European Union cyber policies
	Ms. Irene Corpuz	· Strategic Steering Committee Member, Global Forum for Cyber Expertise (GFCE) · Cyber capacity building, cybersecurity policy

– 양자 기술 분야 전문가는 양자 하드웨어, 교육, 양자안보, 양자외교 등 관련해 10여 명을 발굴함

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

– 우주 기술 분야 전문가는 국제 우주 정책, 우주 안보 전략, 우주법 등 관련해 10명을 발굴함

	이름	소속 · 직위 / 전문분야
	Dr. Scott Pace	· Professor of Practice of International Affairs; Director, Space Policy Institute, Elliott School of International Affairs, George Washington University · Space policy, international space cooperation, space security
	Dr. Pascale Ehrenfreund	· Research Professor of Space Policy and International Affairs, Space Policy Institute, George Washington University · Space policy, astrobiology, space exploration
	Dr. Pascale Ehrenfreund	· Research Professor of Space Policy and International Affairs, Space Policy Institute, George Washington University · Space policy, international space cooperation, space exploration
	Dr. Frédéric Ouattara	· Assistant Professor, School for the Future of Innovation in Society, Arizona State University · Space science education, international space collaboration
	Mr. George A. Danos	· President, Cyprus Space Exploration Organisation (CSEO) · Space exploration, international space cooperation, space innovation
	Dr. Nicolas Peter	· Acting President, International Space University · Space policy, international space cooperation, space education
	Prof. Krystyn Van Vliet	· Professor of Engineering and Vice President for Research and Innovation, Cornell University · Advanced materials for space technologies, innovation in engineering systems
	Dr. Kai-Uwe Schrogl	· President, International Institute of Space Law (IISL) · Space law, global space governance, international cooperation in space
	Dr. Jessica West	· Senior Researcher, Project Ploughshares · Space security, weaponization of space, emerging technologies in space
	Ms. Victoria Samson	· Washington Office Director, Secure World Foundation · Space sustainability, space situational awareness, policy for space traffic management

– 배터리 분야 전문가는 리튬 이온 전지, 전지 재활용 등 관련해 5명을 발굴함

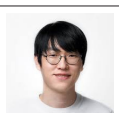
	이름	소속 · 직위 / 전문분야
	Dr. Linda L. Gaines	· Systems Analyst, Center for Transportation Research, Argonne National Laboratory · Battery recycling policies, life cycle analysis of batteries, sustainable materials management
	Dr. Hans Eric Melin	· Founder and Managing Director, Circular Energy Storage · Market analysis and policy development for battery recycling and second-life applications
	Dr. Paul Anderson	· Professor of Strategic Elements and Materials, University of Birmingham · Recycling of lithium-ion batteries, policy implications of battery supply chains
	Prof. Jeff Dahn	· Professor of Physics and Atmospheric Science, Dalhousie University · Lithium-ion battery development, energy storage technologies, collaboration with industry on battery research
	Dr. Ethan Elkind	· Director of the Climate Program at the Center for Law, Energy & the Environment (CLEE), UC Berkeley School of Law · Legal and policy aspects of electric vehicle battery supply chains, sustainability in energy storage

– 광물 분야 전문가는 국제 자원법, 지속 가능한 발전 등 관련해 5명을 발굴함

	이름	소속 · 직위 / 전문분야
	Prof. Ana Elizabeth Bastida	· Lecturer in Global Energy and Resources Law, University of Dundee · International mineral law, sustainable development in mining, governance of mineral resources
	Dr. Robert Pritchard	· Executive Director, Energy Policy Institute of Australia · Energy and mineral policy, international investment in mining, legal frameworks for resource development
	Prof. Peter Cameron	· Director, Centre for Energy, Petroleum and Mineral Law and Policy (CEPMLP), University of Dundee · Energy and mineral law, international energy policy, regulatory aspects of natural resources
	Dr. Günter Tiess	· Editor, Encyclopedia of Mineral and Energy Policy · Mineral policy, sustainable resource management, international mineral economics
	Dr. Michael Lodge	· Secretary-General, International Seabed Authority · Law of the sea, regulation of deep seabed mining, international maritime policy

● 국내 전문가는 인공지능 및 사이버안보 10명, 양자, 우주 각 5명, 배터리·광물 10인을 포함해 총 30명을 발굴함

· 인공지능 및 사이버안보

	이름	소속 · 직위 / 전문분야
	김창익	· KAIST 전기및전자공학부 교수 · 사이버안보, 영상처리
	유지연	· 상명대학교 휴먼지능정보공학 부교수 · 인간 심리, 사이버안보, 공학 융합
	유인태	· 단국대학교 정치외교학과 조교수 · 정치 외교학, 국제 관계, 사이버안보
	정경두	· 사이버안보연구소 대표 · 사이버안보
	채재병	· 국가안보전략연구원 신안보연구실 수석연구위원 · 신흥 안보, 국가 안보 전략, 사이버안보
	오일석	· 국가안보전략연구원 신흥안보연구실 연구위원 · 사이버안보, 신기술 법제, 인공지능
	윤두식	· 이로운앤컴퍼니 대표 · 기업 경영, 사이버안보, 사이버보안
	성경모	· 과학기술정책연구원 과학기술외교안보연구단장 · 과학기술 외교, 안보 정책, 인공지능, 반도체
	하정우	· 네이버클라우드 AI 이노베이션 센터장 · 인공지능, 클라우드 기술
	김준연	· 소프트웨어정책연구소 산업정책연구실 책임연구원 · 소프트웨어 산업 정책, 인공지능
	배영자	· 건국대 정치외교학과 교수 · 정치 외교학, 국제 관계, 외교안보, 인공지능
	강민석	· 카네기국제평화연구소 선임연구위원 · 신흥기술의 국방 무기체계 적용, 국방기획

	양정윤	· 국가보안기술연구소 안보정책연구실 선임연구원 · 사이버전쟁, 국제관계
	류석영	· KAIST 전산학부 교수 · 프로그래밍 언어, 인공지능, 사이버안보
	이원태	· 아주대학교 소프트웨어융합대학 사이버보안학과 연구교수 · 인공지능, 사이버보안, 신기술정책

· 양자기술

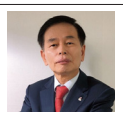
	이름	소속 · 직위 / 전문분야
	이준구	· 카이스트 전기및전자공학부 교수 · 양자보안통신, 양자기계학습, 광통신
	곽기호	· 방과학연구소 국방첨단과학기술연구원장 · 첨단무기체계 연구개발, 양자기술
	김재완	· 고등과학원 부원장, 계산과학부 교수 · 양자 얽힘, 양자정보, 큐디트
	한상욱	· 한국과학기술연구원 양자정보연구단 단장 · 양자 암호, 양자컴퓨팅, 양자정보기술
	정연욱	· 성균관대 나노공학과 교수 · 초전도 큐비트 기반 양자 컴퓨팅

· 우주기술

	이름	소속 · 직위 / 전문분야
	조일연	· 한국전자통신연구원(ETRI)인공지능컴퓨팅연구소장 · 인공지능, 군사학, 우주, 사이버보안
	곽기호	· 국방과학연구소(ADD) 국방AI센터장 · 국방 인공지능, 군사 기술 개발
	윤여선	· 한화시스템 기반기술연구소장 · 첨단 방산 기술, 사이버 보안
	최한림	· KAIST 항공우주공학과 교수 · 항공우주공학, 무인기 기술

	양병희	· KAIST 미래국방AI특화연구센터 초빙교수 · 대드론(anti-drone) 체계, 국방 인공지능

· 배터리 및 광물

	이름	소속 · 직위 / 전문분야
	김진수	· 한양대학교 공과대학 자원환경공학과 교수 · 에너지 및 자원 경제학, 국제 자원 시장 분석
	김연규	· 한양대학교 국제학부 교수 · 에너지 안보, 핵심 광물 지정학
	김동수	· 산업연구원 산업통상연구본부 선임연구위원 · 산업통상 정책, 산업 경제
	박준혁	· 한국지질자원연구원 광물자원연구본부 선임연구원 · 광물 자원 개발, 자원 탐사
	오일석	· 국가안보전략연구원 신흥안보연구실 연구위원 · 신흥 안보 연구, 국가 안보 전략
	김태헌	· 에너지경제연구원 석유정책연구실 선임연구위원 · 석유 정책, 에너지 경제
	유희준	· KAIST 전기및전자공학부 교수 · 전기 및 전자 공학, 반도체 소자
	안기현	· 한국반도체산업협회 전무 · 반도체 산업 정책, 산업 협력
	박재범	· 포스코경영연구원 수석연구원 · 경영 전략, 산업 분석
	조은교	· 산업연구원 산업통상연구본부 글로벌산업실 · 반도체, 전략외교, 산업통상

5. 신기술 안보 포럼 운영

5-1. 2024 세계신안보 포럼 라운드 테이블(국내 행사)

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

- 일시 및 장소: 2024.10.08.(금) 15:00~19:00, 포시즌스 호텔 서울
- 일정 및 패널

일정	시간	세부 주제	참여 패널
개회식	15:00~15:15	개회사, 축사	■ 개회사: 이동렬 외교부 국제사이버협력대사 ■ 축사: 이승섭 KAIST 안보·대외협력 자문역 ■ 사회: 이현승 외교부 국제안보사이버협력팀장
세션 1	15:20~16:30	핵심기반시설에 대한 사이버 위협과 미래	■ 발표: 최광희 법무법인(유) 세종 고문 ■ 토론: 문종현 지니언스 이사, 신소현 아산정책연구원 부연구위원, 송태은 국립외교원 교수, 박찬암 스틸리언 대표이사 ■ 좌장: 김상배 한국사이버안보학회(KACS) 회장
오찬(12:00~13:00)			
세션 2	16:40~17:50	인공지능과 국제안보의 변화	■ 발표: 양병희 KAIST 미래국방AI특화연구센터 교수 ■ 토론: 윤종권 외교부 국제안보국장, 윤여선 세종대학교 국방시스템공학과 교수, 성경모 과학기술정책연구원 과학기술외교안보연구단장, 김재오 인하대학교 데이터사이언스학과 교수 ■ 좌장: 배영자 건국대학교 정치외교학과 교수

● 세션 1 발표의 주요 내용: 핵심기반시설에 대한 사이버 위협과 미래

- 최근 정치적 목적뿐만 아니라 실질적 피해를 유발하려는 사이버 공격이 늘어나고 있으며, 전력망과 같은 주요 기반 시설이 공격의 주요 표적이 되고 있음. 특히 러시아와 이란 관련 사이버 조직이 미국 기반 시설을 대상으로 공격을 수행해 전력망, 급수 시스템 등 다양한 영역에 위협을 가하고 있음
- 코로나19로 인한 디지털 전환은 사이버 보안 취약점을 확대했으며, 기후 변화와 지정학적 충돌 등 복합적인 요소가 사이버 위협을 가중시키고 있음. 빅테크 기업의 인력 감축과 같은 변화는 고급 기술력이 해킹으로 악용될 가능성을 높이며, 공격 조직은 웨일링 어택과 같은 대규모 공격 전략을 통해 주요 기반 시설에 위협을 가함
- 국가마다 기반 시설 보호를 위한 접근 방식이 다르며, 미국은 '잠재적 위험 기반 접근(All-hazard)'을, 한국은 '사이버 위험 기반 접근(cyber risk)'을 중심으로 대응하고 있음. 미국은 민간 기반 시설에 대한 규제를 강화하며 공공과 민간의 협력적 방어 모델을 제시하고, 한국은 제로 트러스트 전략과 같은 기술적 대응을 강화하고 있음

- **시사점 및 제언:**
  ① 글로벌 환경에서 기반 시설의 보호는 단순한 기술적 접근을 넘어선 제도적, 재정적 지원을 포함해야 하며, 민간 사업자가 공격 탐지 및 방어에 적극 나설 수 있도록 법적 지원이 필요함
  ② 국가와 민간, 공공 부문 간 협력을 통해 특화된 방어 모델을 마련하고, 이를 통해 분산형 방어 체계를 구축할 필요가 있음. 이는 글로벌 규범을 기반으로 한 기반 시설 보호 체계를 확립하는 데 기여할 것임
  ③ 각 분야의 사이버 위협을 분석하고 대응할 수 있는 전문 조직을 신설하고, 기반 시설 운영 조직에 재정적, 기술적 지원을 강화하여 보안 수준을 높여야 함

● 세션 1 주요 토론 내용

- **(핵심 제언)** 사이버 보안 강화는 민간과 정부의 협력, 국제 규범 마련, 법적·제도적 보완을 통해 이루어져야 하며, 기반 시설 보호와 정보 보안은 규모와 상관없이 위험도와 중요성에 따라 유연하게 접근해야 함. 법 제정 지연과 국제 규범의 한계를 보완하기 위해 전략 수립과 실질적인 작전 수행이 병행되어야 하며, 민간의 적극적인 참여와 폐쇄성 완화를 통해 보안 역량을 높이는 것이 필요함. 특히, 기술 발전 속도에 맞춘 지속적인 법 개정과 세부적인 제도 개선이 중요하며, 정보 공유와 협력 강화를 통해 국가적·국제적 안보 위협에 대응해야 함
- **토론자별 주요 내용:**
  ① 문종현 이사: 사이버 공격은 생명과 국가 안보에 직접적인 영향을 미칠 수 있는 중요한 문제임. 플로리다 수돗물 해킹과 콜로니얼 파이프라인 사건은 사이버 공격의 파괴적 결과를 보여주는 대표적인 사례이며, AI와 딥페이크 기술이 이러한 공격에 활용될 가능성이 있음. 국내에서도 기반 시설에 대한 공격 사례가 발생하고 있으며, 이를 방지하기 위한 국가 차원의 대응과 대비가 시급함
  ② 신소현 연구위원: 한국의 사이버 안보 법 제정이 지연되고 있어, 구체적인 전략 수립과 민간 참여를 통한 협력적 접근이 필요함. 국제사회와의 소통을 강화해 한국의 성과를 알리고 피드백을 수용해야 하며, 리뷰 커뮤니티를 통해 사이버 안보 전략의 주기적 검토와 개선을 이행하는 체계적인 구조를 마련해야 함
  ③ 송태은 교수: 사이버 공격은 주로 지정학적 갈등에서 비롯되며, 주요 타겟은 보건과 통신 부문임. 북한은 최근 공격 대상을 미국으로 확대하고 있으며, 공격 기술이 RaaS(랜섬웨어 서비스) 같은 구독 모델로 발전하면서 민간과 핵심 기반 시설이 심각한 위협에 노출되고 있음. 이러한 공격은 경제적으로 중소기업과 국가 경제에 치명적인 피해를 줄 수 있음
  ④ 박찬암 대표이사: 민간과의 협력은 사이버 보안 강화를 위한 핵심 요소이며, 규제를 통해 국가 차원의 보안을 체계적으로 강화해야 함. 폐쇄성이 기반 시설의 보안 약점으로 작용할 수 있으므로, 정기적인 보안 점검과 같은 예방적 접근이 필요하며, 이러한 노력을 통해 랜섬웨어와 같은 위협에 효과적으로 대응할 수 있음

● 세션 2 발표의 주요 내용: 인공지능과 국제안보의 변화

- AI 기술은 여러 차례의 터닝포인트를 통해 발전했으며, 최근에는 생성형 AI와 대규모 언어 모델(GPT-4) 같은 기술이 주요 흐름을 주도하고 있음. 특히 AI는 2024년 10대 전략적 기술 중 절반을 차지하며, 다양한 산업과 사회적 변화를 이끄는 핵심 기술로 자리 잡음

- AI는 전통적 군사 전략을 넘어 새로운 형태의 지능 중심 전장(ICW)을 만들어내고 있음. AI 기반 무기와 자율 시스템은 전쟁의 시간과 공간 제약을 없애며, 네트워크 단절 상황에서도 군사 작전을 수행할 수 있는 모자이크 워페어로 발전하고 있음. 특히 중국은 AI 기술을 기반으로 군사적 패권을 강화하고 있으며, 이는 AI 기술 경쟁의 심화와 함께 국제 안보의 불확실성을 높임
- AI는 국가 간 군사 경쟁을 부추길 뿐 아니라, 자율 살상 무기와 같은 새로운 형태의 위협을 창출하고 있음. 이는 예측 불가능한 국제적 위기를 초래할 가능성을 높이며, AI 기술의 군사적 사용과 관련된 사회적 우려를 증폭시키고 있음. 이를 해결하기 위해 국제사회는 AI의 책임 있는 군사적 사용을 논의하며, 윤리적 기준과 강력한 통제 방안을 마련하고 있음
- **시사점 및 제언:**
  ① 국제사회는 AI의 윤리적이고 신뢰 가능한 개발을 위해 법적·정책적 가이드라인을 마련하고, 기술의 투명성, 형평성, 안전성을 강화해야 함. 이를 통해 AI가 국제 안보와 군사적 이용에서 책임감 있는 역할을 할 수 있도록 보장해야 함
  ② AI 기반 군사 기술의 위험성을 통제하기 위해 UN과 국제기구 차원의 AI 감시 체계 구축과 국가 간 협력이 필요함. AI 사용 시 발생할 수 있는 윤리적, 법적 문제를 해결하기 위한 다자간 논의와 합의가 요구됨
  ③ AI 윤리 가이드라인을 기반으로 정책을 마련하고, 신뢰 가능한 AI 연구를 촉진해야 함. 또한, AI 윤리에 대한 교육을 강화해 기술을 올바르게 이해하고 활용할 수 있는 환경을 조성해야 함

● 세션 2 주요 토론 내용

- **(핵심 제언)** AI 기술의 발전과 활용은 국제적 거버넌스 구축, 책임 있는 개발, 그리고 기술적·제도적 보완을 통해 신중하게 이루어져야 하며, 특히 군사와 민간 양측에서 AI의 책임성과 신뢰성을 확보하는 것이 중요함. 국제 사회는 AI 기술을 규제하는 동시에 이를 효율적이고 윤리적으로 활용할 수 있는 제도적 기반을 마련해야 하며, AI 알고리즘의 취약성을 보완하고 투명한 모니터링과 강력한 패널티 체계를 통해 악용 가능성을 억제해야 함. 대한민국은 국방, 외교, 과학기술, 보건 등 다양한 분야에서 안전하고 책임 있는 AI 사용을 확산시키기 위한 국내외 협력과 거버넌스를 적극적으로 구상하고 실현해야 함
- **토론자별 주요 내용:**
  ① 윤종권 국장: 외교부는 제2차 REAIM를 통해 AI와 관련된 국제적 거버넌스와 원칙 수립의 중요성을 강조하며, AI 기술이 국가 경제력과 군사력에 미치는 영향을 평가함. AI는 민군 양면에서 국가 안보의 핵심 요소로 작용하고 있으며, 국제적 규제와 균형이 필요함을 지적함. 특히 기술 발전 속도에 맞춘 법적 체계 마련이 중요하며, 국제적인 감시 기구와 규제 논의가 가속화될 것으로 전망함
  ② 윤여선 교수: 국내 방산업체와 연구소는 AI 기술을 국방에 도입하려 하고 있으나, 법적·제도적 제약으로 인해 어려움을 겪고 있음. AI 무기체계는 지속적 학습과 발전이 필요한데, 현재는 고정된 평가 체계와 정량적 기준이 이를 제한하고 있음. 또한, 소프트웨어 가치 산정의 미비로 인해 산업적 개발과 적용이 저조함. 변화하는 국제 안보 환경에 맞춰 제도적 변화와 AI 기술의 적극적 활용 기반 마련이 필요함
  ③ 성경모 단장: AI는 국가 안보의 게임 체인저로서 작용하고 있으며, 미중 디지털 경제 갈등 속에서 글로벌 디지털 경제와 안보 간 긴장이 증가하고 있음. 유럽연합은 AI 규제와 기술

개발 간의 균형을 목표로 가이아-X 프로젝트와 EU AI 액트를 통해 디지털 주권을 강화하고 있으며, 프랑스는 군사 AI 개발을 촉진하기 위해 2024년에 국방 인공지능부를 신설함. AI 규제와 혁신의 균형을 위한 국제 협력이 강조됨

④ 김재오 교수: AI 기술은 전문가 개입 기반, 순수 데이터 기반, 복합 지능 기반으로 구분되며, 최근에는 멀티 모달 모델을 활용한 복합 지능 기반 기술이 주목받고 있음. 러시아-우크라이나 전쟁과 이스라엘-하마스 전쟁에서도 AI 기반 기술이 군사적으로 활용되며 효율성을 높였으나, 설계 오류와 데이터 편향으로 인한 위험도 존재함. 복합 지능 기술은 미래 전장에서 중요한 역할을 할 가능성이 크며, 이를 도입할 때는 법적, 인도주의적 측면에서 신중한 접근이 필요함

그림 25 : 2024 세계신안보포럼 라운드테이블(국내 행사) 모습

5-2. 2024 세계신안보 포럼(국제 행사)

● 2024년 제4차 세계신안보포럼(World Emerging Security Forum, WESF)은 외교부 주최로 스웨덴 정부의 외교정책연구소인 스톡홀름 국제평화연구소(SIPRI) 및 KAIST 과학기술정책대학원이 파트너 기관으로서 함께 개최함

- 지난 3년간의 성공적인 포럼 성과에 기반하여, 지정학적 긴장과 기술 개발 간 상호작용의 영향 하에 진화하는 국제안보 지형에 초점을 맞춰, 특히 지정학과 AI 등 신기술 간 상호 작용, 진화하는 사이버 위협 환경, 기술 개발을 위한 심화하는 자원 경쟁에 대해 논의함
- 주제 : 진화하는 안보 환경 속 국제협력 – 사이버, AI, 신기술을 중심으로(Global Cooperation in the Evolving Security Environment: Cyber, AI, and New Technologies)
- 일시 및 장소 : 2024. 12. 5(목), 10:00 ~ 17:10, 그랜드 하얏트 서울, 그랜드볼룸
- 동 포럼에 관한 보고는 별책에 수록함

그림 26 : 2024 세계신안보포럼
(국제 행사) 모습

부록 1

국내 전문가 주요 자문 내용

〈아주대학교 소프트웨어융합대학 사이버보안학과 연구교수 이원태〉

1. 신기술(AI 포함)의 다분야 연계 강화와 국제 평화 및 안보에 미칠 위험과 잠재적 파급력

- AI와 같은 신기술의 발전으로 경제, 안보, 기술 간 경계가 무의미해지고 통합적인 접근이 필요하며, 이는 사이버 보안에서도 동일하게 적용됨
- AI 기반 사이버 공격 및 허위 정보 확산, 특히 딥페이크를 이용한 인지전 등으로 정치적·군사적 긴장이 증가할 가능성이 있음
- AI 기술의 빠른 변화와 오픈소스 AI의 확산으로 비국가 행위자나 테러 단체에 의한 악용 위험이 커지고 있음

2. 미·중 기술패권 경쟁과 글로벌 리더십 제고 방안

- AI 중심의 신기술 경쟁으로 인해 글로벌 질서가 다극화·분극화 양상을 보이며, 이는 국제 안정과 평화를 저해할 수 있음
- 미국과 중국의 경쟁이 글로벌 사우스를 대상으로 한 AI 격차 해소 및 지원 명분으로 더욱 치열해지고 있음
- 글로벌 사우스 국가들은 기술 종속을 경계하며 데이터 주권과 독자적인 AI 개발을 주장, AI 국제 거버넌스 체계가 복잡해질 전망임

3. 과학기술과 연계된 신안보 이슈 및 전망

- AI를 중심으로 한 신기술 안보는 기존 안보 체계를 무력화하고 새로운 위협으로 부각됨
- 윤리적이고 신뢰할 수 있는 AI 개발과 국제 규범 논의가 진행 중이나, 첨단 AI 기술의 악용 가능성으로 인해 안보 지형의 변화가 예상됨
- AI 개발이 특정 국가 중심으로 이루어지면서 기술 의존성이 증가하고, 이에 따른 국제적 불균형이 지정학적 갈등을 초래할 가능성이 있음

4. 중국의 AI 기술력과 향후 전망

- 미국과 중국의 AI 경쟁 양상
  - 바이든 정부는 디리스킹 전략(경쟁적 공존)을 추구했지만, 트럼프 2기에서는 더 강경한 중국 견제가 예상됨
  - AI와 반도체 분야에서 디커플링이 가속화되고, 관세 및 기술 통제가 강화될 것임
- 중국의 대응
  - 미국의 강력한 통제와 제재가 오히려 중국의 AI 발전을 촉진했다는 역설적 평가가 존재함
  - 국제기구 및 다자 거버넌스 내에서 중국의 영향력이 상대적으로 커질 가능성 있음
  - 글로벌 리더십 공백 상황에서 중국이 이를 차지할 가능성이 우려됨

- 미국의 전략
  - 북미 중심의 AI 동맹(미국, 캐나다, 영국)을 통해 AI 안전 연구 및 글로벌 표준 선점에 집중함
  - 반도체 동맹 및 AI 기술 제재를 통해 중국과의 기술 격차를 유지하려고 노력중에 있음

5. 소버린 AI와 국제 거버넌스

- AI의 글로벌 거버넌스 체계는 서방 국가(미국, 영국 등)가 주도할 가능성이 큼
- AI를 핵무기처럼 통제할 수 있을지에 대한 논의는 이미 시작되었으며, AI 안전 연구소 네트워크가 주요 역할을 수행 중임
- 한국은 AI 거버넌스 국제 논의에서 충분한 역할을 하지 못하고 있으며, 관련 법제도 및 정책이 미흡한 상태임

6. 사이버 보안과 리스크 변화

- 트럼프 2기에서는 미중 간 기술 전쟁과 사이버 안보 갈등이 더욱 심화될 전망임
- 미국은 사이버 보안 동맹(5 Eyes 등)을 강화하며, 중국의 영향력을 차단하려는 전략을 지속할 것임
- 한국은 중동 등 제3국과의 협력을 통해 사이버 보안 인프라 및 AI 기술의 독립성을 강화하고 있는 사례가 점차 늘고 있음

7. 기타 의견

- AI 기술의 확산은 전통적인 억지 전략 및 방어 체계에 큰 도전을 주며, 이를 대응하기 위한 제도적 통제와 글로벌 협력이 필요함
- 한국은 AI 국제 표준 및 거버넌스 논의에서 경쟁력을 잃고 있으며, AI 기본법 등 정책적 준비가 미흡해 AI 경쟁력 순위가 하락할 가능성이 큼
- 글로벌 AI 생태계는 다각화 및 블록화되는 추세로, 한국의 대응력 부족이 장기적으로 경쟁력을 약화시킬 위험이 있음

〈산업연구원 산업통상연구본부 글로벌산업실 연구위원 조은교〉

1. 신기술(AI 포함)의 다분야 연계 강화와 국제 평화 및 안보에 미칠 위험과 잠재적 파급력

- 중국은 미국의 AI 제재에도 불구하고 중동 자본 유치와 동남아 시장 진출 등을 통해 AI 기술 생태계를 글로벌로 확장하고 있음
- 중국 AI 생태계는 전자상거래와 핀테크, 디지털 물류 및 데이터 센터 구축을 통해 지역의 디지털 생태계를 장악하려는 의도를 보이고 있음

- AI 기반의 자율주행 기술, 딥페이크, 데이터 활용 등에서 빠른 발전을 이루고 있으며, 이는 글로벌 평화와 안보에 잠재적 위험 요소로 작용할 가능성이 있음

2. 미·중 기술패권 경쟁과 글로벌 리더십 제고 방안

- 미국의 대중국 AI 제재 강화로 인해 자본시장의 디커플링이 발생, 중국은 이를 중동 및 러시아와의 협력으로 보완하고 있음
- 중국의 AI 기술 확장은 단순히 경제적 이익을 넘어 디지털 생태계 장악과 데이터 확보를 목표로 하고 있으며, 글로벌 AI 경쟁에서 블록화된 양상을 띠고 있음
- 중국의 AI 기술 자립은 AI 반도체 분야에서 한계를 보이고 있지만, 자체 기술 및 공정을 통해 이를 극복하려는 노력을 지속 중임

3. 국가 경쟁력과 안보 동시 강화 방안

- 한국의 AI 국가전략은 빅3 국가로 도약하겠다는 비전은 제시했지만, 기술 및 경제 안보 측면에서의 구체적 전략이 부족함
- 중국과의 기술 경쟁에서 한국은 강점을 기반으로 AI 기술과 생태계 발전을 집중적으로 육성할 필요가 있음
- 글로벌 AI 생태계에서 경쟁력을 유지하기 위해서는 기술 안보와 경제 안보를 고려한 구체적인 대응 전략 마련이 필요함

4. 중국의 AI 기술력과 향후 전망

- 미국 제재에 대한 중국의 대응
  - 바이든 정부와 트럼프 1기의 제재를 학습하며, 중국은 독립적인 제조 생태계와 국산화율을 빠르게 구축하고 있음
  - 미국의 제재(드론, 플라잉카, 우주항공, 자율주행 등)는 중국이 해당 기술 분야에 더 많은 자원을 투자하고 산업화 속도를 높이는 계기로 작용됨
- 중국의 AI와 제조 융합 전략
  - AI 기술을 제조업에 접목해 스마트 팩토리와 같은 응용 산업을 확장함
  - AI와 제조의 융합으로 폭발적 성장이 예상되며, 플라잉카는 내년 초 발표 목표로 준비 중임
- 중국의 정부 역할
  - 기술 산업화를 경제정책의 최우선 과제로 설정함
  - 과기부 내 기술 산업화 부서를 공업정보화부로 통합해 효율성을 강화하고, 산업별로 AI를 적용하는 세부 정책을 신속히 실행함

5. 우리나라의 AI 정책과 시사점

- 현재 한국의 상황
  - 한국은 AI 기술 정책은 있으나, AI 산업 정책은 부재함
  - 스마트 제조 관련 정책이 단순 자동화를 넘어선 실질적 산업 전환으로 이어지지 못하고 있음
  - AI를 산업 응용으로 확장하는 국가 전략이 부족하며, 관련 법제·조세·인프라 등의 기반이 미흡함

● 필요한 대응 전략
- 전통 산업에 AI를 접목하는 AI 산업 정책의 신속한 수립 및 실행이 필요함
- 정부 차원의 AI와 제조 융합 정책 확대와, 중소·중견 기업의 스마트 제조 전환 지원 강화가 필요함
- 글로벌 AI 생태계 변화에 맞춘 선제적 대응과 국가 경쟁력 강화를 위한 통합적 접근 필요함

6. 소버린 AI와 국제 거버넌스

● 중국의 전략
- AI 플러스 전략을 통해 모든 산업에 AI를 적용하며, 지방정부 차원의 세부 정책도 신속히 마련 중임
- 중국은 제조 강국의 강점을 활용해 AI와의 융합을 통해 글로벌 경쟁력을 강화하고 있음

● 한국의 과제
- AI 기술의 국가 차원 산업화와 글로벌 거버넌스 변화에 맞는 정책적 정비 필요
- AI 기술을 기반으로 한 제조업 혁신을 통해 경쟁력 있는 국가 전략을 수립해야 함

7. 기타 의견

- AI 기술이 블록화된 세계에서 제3국 시장 진출 및 중국 시장과의 경합은 새로운 기회와 비용을 동시에 요구함
- 중국은 러시아, 중동 등 다양한 국가와의 협력을 통해 인재를 유치하고 AI 기술을 지속적으로 확장하고 있어, 이에 대한 국제적 대응 방안이 필요함

〈국가보안기술연구소 안보정책연구실 선임연구원 양정윤〉

1. 신기술(AI 포함)의 다분야 연계 강화와 국제 평화 및 안보에 미칠 위험과 잠재적 파급력

● 미중 전략 경쟁과 함께 신기술로 인해 불확실성이 증가하고 있으며, 전통적 안보 개념에서 정치, 경제, 사이버, 사회 안보 등 포괄적 안보 개념으로 확장됨

● 비국가 행위자 및 국가 배후의 행위자들이 사이버 안보 환경을 더욱 복잡하게 만들고 있으며, 러시아-우크라이나 전쟁 사례에서 이러한 양상이 두드러짐

● AI 기반 기술(딥페이크, 오정보, 컴퓨터 바이러스 등)은 비대칭적 위협을 증대시키며, 기존 안보 체계를 무력화할 가능성이 큼

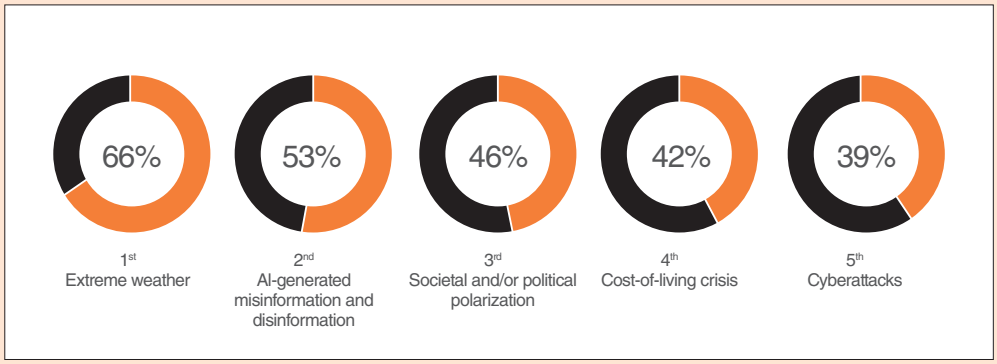
2. 과학기술과 연계된 신안보 이슈 및 전망

● 미국 국가 위협 평가 보고서에서는 AI와 생명공학 등의 신기술 발전이 주요 위협으로 언급되며,

AI 발전이 의도하지 않은 결과와 새로운 비대칭 위협을 초래할 가능성이 있음

- 세계경제포럼(Global Risks Report)에서는 단기적으로 잘못된 정보 및 허위 정보가 1위 위협, 장기적으로는 AI 생성 오정보가 5위 위협으로 나타남
- 러시아-우크라이나 전쟁에서 AI 기반 인지전과 사이버전이 중요한 위협 요소로 등장, 국제 안보 환경의 복잡성과 위험을 가중시키고 있음

그림 27 : WEF 글로벌 리스크 보고서에 나타난 위험 (AI, 사이버 공격)
(출처: WEF, 2024)



3. 사이버 보안과 리스크 변화

- 러시아-우크라이나 전쟁에서의 사이버 보안 교훈
  - 사이버 물리 시스템을 활용한 공격의 기대와 달리, 전쟁의 양상은 전통적인 재래식 전쟁의 형태를 띰
  - 사이버 공간은 전쟁의 대체 수단이기보다는 보조적 역할을 수행하며, 전장 내 정보 공유 및 집단지성 활용 사례로 주목받음
- 사이버의 대중성과 포용성 증가
  - 사이버 기술은 모든 공간에서 활용되며 점차 보편적이고 포괄적인 역할을 수행할 수 있음
  - 드론, 실시간 정보 공유 등 사이버와 물리적 공간의 인터페이스가 더욱 긴밀해지고 있음
- 새로운 사이버 위협 양상
  - 인지전, 심리전, 영향력 작전 등 사이버의 비물리적 영향력이 강화되고 있음
  - 전통적인 물리적 공격보다는, 사람들의 인식과 행동을 변화시키는 데 초점이 맞춰지고 있음

4. 소버린 AI와 국제 거버넌스

- 사이버와 AI의 융합
  - 언맨드(Unmanned) 기술과 사이버 작전이 결합하여, 전쟁 비용을 줄이고 전투 방식을 변화시킬 가능성이 있음
  - 예: 원격으로 조종하는 군사작전과 인지전이 융합, 전쟁의 성격을 근본적으로 변화시킬 가능성이 있음

5. 기타 의견

- 현재 국제 질서는 불확실성이 커지고 있으며, 강대국들의 경쟁과 신기술의 결합으로 새로운 안보 도전 과제가 지속적으로 발생함

- AI와 같은 첨단 기술의 윤리적, 책임 있는 개발이 필수적이며, 기존 안보 체계를 강화하기 위한 국제 협력이 필요함
- 미래 사이버 전쟁의 위험성
  - 기술의 발전으로 전쟁 비용이 낮아지면서, 전쟁 발발 가능성이나 빈도가 증가할 우려가 있음
  - 사이버 영향력 작전과 같은 비물리적 전쟁 수단이 전통적인 전쟁 방식과 병행되어 사용될 가능성 큼

〈동아시아연구원(EAI) 수석연구원 김양규〉

1. 신기술(AI 포함)의 다분야 연계 강화와 국제 평화 및 안보에 미칠 위험과 잠재적 파급력

- AI는 데이터를 처리하고 학습하며, 인간 지능이 필요한 작업(예: 상황 분석, 패턴 인식, 의사소통 등)을 수행할 수 있는 기술
- AI는 범용 기술로 다양한 분야에 적용 가능하며, 기술 변화의 중심에서 문제를 악화시키거나 새로운 해결책을 제시하는 역할을 수행
- AI와 핵무기 결합 시, '핵 얽힘(nuclear entanglement)'과 '블랙박스 문제'로 인해 심각한 결과를 초래할 위험
  - (핵 얽힘) 재래식 전력과 핵 전력이 결합된 무기 시스템에서 오판 가능성 증가
  - (블랙박스 문제) AI의 결론 도출 과정을 인간이 이해하지 못할 경우, 잘못된 판단으로 핵전쟁 확전 위험
- AI 기술 경쟁은 세계 경제의 분절화, 불평등 심화, 노동시장 불균형, 사회적 분열 등을 초래할 가능성이 있음
- 지정학적 분쟁지점(대만, 북한, 남중국해 등)에서 AI가 무력충돌 가능성을 증대시킬 우려가 있음

2. 미·중 기술패권 경쟁과 글로벌 리더십 제고 방안

- AI 발전의 핵심은 반도체 기술이며, 첨단 반도체 생산 능력이 AI 산업의 기반임
- 미국은 반도체 공급망 통제를 통해 중국의 기술 발전을 저지하려는 전략을 추진함
- 중국은 반도체 국산화와 독자적 AI 기술 발전을 목표로 개도국과 협력하여 독자적 생태계를 구축 중임
- AI 기술 질서가 미국과 중국 중심으로 양분되며, 한국의 선택지는 점점 제한될 가능성이 있음
- 한국은 미국 주도 질서에 조기에 편입하여 국제 네트워크 내에서 위상을 강화해야 함

3. 국가 경쟁력과 안보 동시 강화 방안

- 한국은 미국과 첨단 기술 분야 협력을 강화해야 하며, 이는 국방력 강화를 위한 핵심 과제임
- 오커스(AUKUS) 필라 2 가입 검토 필요
  - AI, 양자기술, 자율무기체계 등 미래 전장을 지배할 기술 협력 포함
  - 한국의 국방혁신 4.0과 연계 가능
- 2024년 REAIM 회의를 통해 AI의 군사적 사용에서 '인간 통제 유지'와 '설명 가능성 개선 규범 수립'에 기여
- 자체 핵무장은 국익에 부정적이며, AI 중심의 미래 전략 자산 개발로 북핵 위협에 대응 필요
- 국민 신뢰를 얻기 위해 미래 군사 기술 발전 방향과 북핵 대안을 효과적으로 소통해야 함

〈한국국방연구원 안보전략연구센터 연구위원 이중구〉

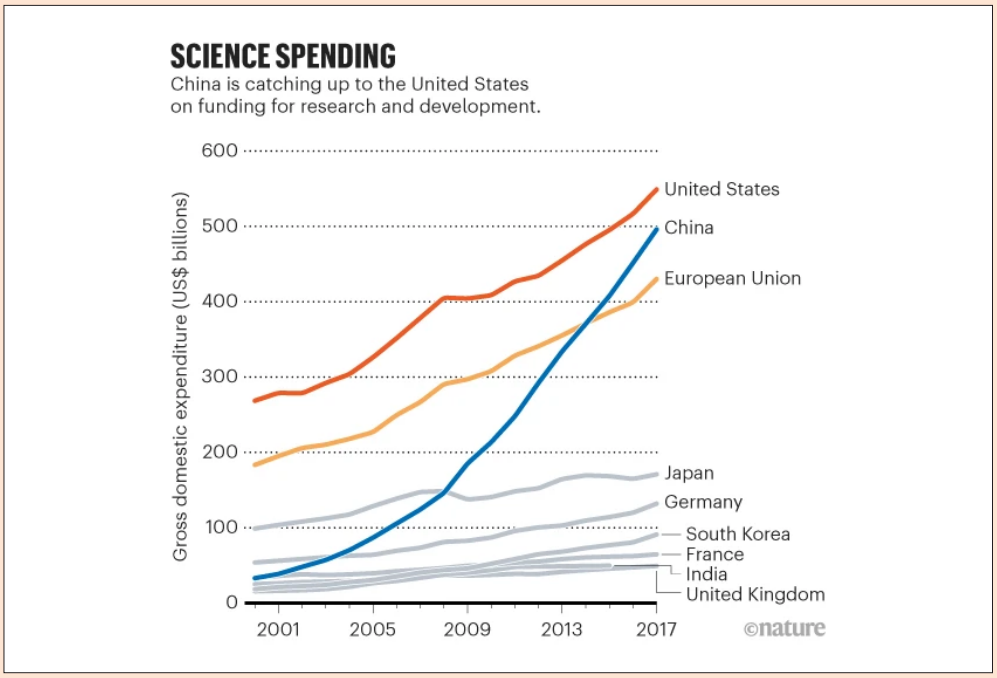
1. 신기술(AI 포함)의 다분야 연계 강화와 국제 평화 및 안보에 미칠 위험과 잠재적 파급력

- AI, 양자, 드론, 나노, 우주, 극초음속 등의 신기술은 기존 군사력의 세력균형을 변화시켜 국제적 안정보다는 불안을 야기할 가능성이 큼
- 신기술 활용 여부에 따른 국가 간 격차는 확대되지만, 기술 전파와 수렴으로 약소국들도 강대국의 전유물이었던 군사적 능력을 확보하게 될 것으로 전망됨
- 군사작전에서 나타날 5가지 주요 특징
  - (사거리 구식화) 드론과 순항미사일의 사거리 증가로 전투기 등이 후방으로 배치되어야 함
  - (공격면역력 상실) 미국 해외기지 등이 비국가행위자의 공격으로부터 자유롭지 않음
  - (방어의 전술적 우위) 건물 지하에 숨겨진 방어체계를 탐지하기 어려움
  - (물량의 귀환) 다량의 무기로 정확성 있는 공격이 가능
  - (동원요건) 3D 프린팅 등으로 군사용 동원이 빠르게 가능하지만 준비가 필요함

2. 미·중 기술패권 경쟁과 글로벌 리더십 제고 방안

- 미국은 군사혁신을 주도하며 동맹국 및 우방국과 혁신 아이디어를 공유
- 한국은 한미 국방·과학기술·산업 간 네트워크를 강화하고 외교채널을 통해 최신 신기술 정책 동향을 공유하는 플랫폼을 마련해야 함
- 글로벌 리더십 확보를 위해 과학기술 투자 확대 및 연구 성과를 기반으로 존재감을 강화해야 함
- 한국의 경험(예: AI를 통한 비무장지대 감시)을 활용하여 국제 다자회의에서 의미 있는 의견을 제시해야 함

그림 28 : 각국의 R&D 지출
(출처: Viglione, 2020)



3. 국가 경쟁력과 안보 동시 강화 방안

- 신기술 개발과 경제·안보 전략을 융합한 국가 전략을 수립
- 시험적 아이디어를 위한 연구환경 조성 필요(예: 보수교육, 고위연수 과정에서 신기술과 경제 혁신 관련 과목 신설)
- 민·관·학·투자·시민사회가 협력하는 교육과정 및 플랫폼을 설계하여 조직 간 융합을 촉진
- 국방 혁신과 경제 혁신 교육과정에 다양한 분야의 인원을 혼합하여 신기술 적용을 촉진

4. 신안보 변화 전망

- 양자 및 AI 기술 연구가 지속되면서 미래 전쟁은 저비용·소형 무기가 중심이 될 전망(예: 드론, 유조선 개조 미사일 발사선 등)
- AI와 우주 기술이 미중 경쟁의 핵심으로 자리 잡음. 한국도 관련 법제화와 역량 강화 필요
- 기후변화 문제도 안보 차원에서 대응해야 하며, 에너지 위기에 대한 대책 마련 필요

5. 기타 의견

- 신기술 자체보다 활용 목적에 대한 명확한 아이디어를 제시해야 함

부록 2

국내 전문가 라운드테이블 상세 내용

■ 행사 개요

- 행사 주제: 사이버, 인공지능 그리고 진화하는 국제안보
- 일시 및 장소: 2024.10.08.(화) 15:00~19:00, 포시즌스 호텔 서울
- 구성: 개회식, 세션 1·2
  - 세션 1 주제: 핵심기반시설에 대한 사이버 위협과 미래
  - 세션 2 주제: 인공지능과 국제안보의 변화

* 주요 참석자(발표·토론): 이동렬 외교부 국제사이버협력대사, 이승섭 KAIST 안보·대외협력 자문역, 최광희 법무법인(유) 세종 고문, 문종현 지니언스 이사, 신소현 아산정책연구원 부연구위원, 송태은 국립외교원 교수, 박찬암 스틸리언 대표이사, 김상배 한국사이버안보학회(KACS) 회장, 양병희 KAIST 미래국방AI특화연구센터 교수, 윤종권 외교부 국제안보국장, 윤여선 세종대학교 국방시스템공학과 교수, 성경모 과학기술정책연구원 과학기술외교안보연구단장, 김재오 인하대학교 데이터사이언스학과 교수, 배영자 건국대학교 정치외교학과 교수

■ 주요 내용

- 개회식

1) **(개회사: 이동렬 외교부 국제사이버협력대사)** 사이버 공간과 AI 기술의 발전이 일상에 혁신을 가져오는 동시에, 초국경적인 리스크를 관리해야 하는 새로운 과제가 대두되고 있음. 최근 발생한 클라우드 스트라이크(CloudStrike) 사태로 인해 공항, 병원 등의 주요 기반 시설에 막대한 손실이 발생한 사례는 사이버 보안의 중요성을 보여주고 있으며, 악의적 의도를 가진 사이버 공격의 위협은 더욱 증가하는 추세임. 또한, AI를 활용한 딥페이크(Deepfake) 등 허위 정보가 민주주의와 인권을 위협하고 있음. AI의 군사적 응용 가능성은 크지만 비윤리적 사용에 대한 우려가 있으며, AI 시장의 급성장 속에서 국제 논의의 필요성이 커지고 있음. 이에 따라 한국 정부는 사이버 안보 전략을 발표하고, 국가 AI 위원회를 출범하는 등 전략적 대응을 강화해 나가고 있음. 대한민국 외교부는 UN 안보리 비상임이사국으로서 사이버 안보를 주요 의제로 다루고, UN 사이버 범죄 협약 협상에 참여하며 관련 논의를 선도 중임. 또한, AI 서울 정상회의와 DM Summit을 통해 AI 담론에 주도적으로 참여하고 있음. 올해 12월에 개최될 세계신안보포럼(WESF)은 사이버 및 AI와 같은 신기술로 인한 융복합적, 초국경적 안보 위협에 대응하기 위한 국제적 협력을 강조할 예정이며, 정부와 다양한 이해관계자 간의 연대와 협력의 중요성을 다룰 계획임.

2) **(축사: 이승섭 KAIST 안보·대외협력 자문역)** AI와 사이버 보안 기술의 발전에 따른 국가 안보 위협의 다변화를 강조하며, 국제 공동 대응의 중요성을 언급함. 최근 한국 정부는 AI 3대 강국 비전을 선포하고 국가 인공지능위원회를 출범, AI 기술을 국가 경쟁력의 핵심으로 인식하고 있음. 9월에 한국에서 열린 '2024 인공지능의 책임있는 군사적 이용에 관한 고위급 회의(REAIM)'는 90여 개국이 참여하여 AI의 국제적 역할을 재확인하는 계기가 되었음. 카이스트는 머신러닝과 딥러닝 분야에서 세계적 학술기관으로 자리하고 있으며, 사이버 보안 역시 국가 안보에 직결되는 중요한 요소로 부각되고 있음. 최근 미국에서 열린 국제 랜섬웨어 대응 회의(CRI)에서는 북한의 가상 자산 탈취 문제가 주요 의제로 논의됨. 이번 WESF 포럼에서 다양한 전문가들이 복합적 위협에 대한 통찰을 공유하는 기회의 장이 될 것임

● 세션 1

1) **(발표: 최광희 법무법인(유) 세종 고문) 핵심기반시설에 대한 사이버 위협과 미래**

- **기반 시설에 대한 사이버 공격**

① 국가 핵심 기반 시설은 정치적 사이버 공격의 첫 번째 타격 목표
최근 주요 기반 시설을 대상으로 한 사이버 공격이 증가하고 있으며, 국가별로 기반 시설의 정의는 다르지만, 2023년부터 정치적 목적을 넘어 실질적 피해를 주려는 공격 양상이 두드러지고 있음. 특히 전력망에 대한 공격이 급증하여 디지털 기반 시설 전체의 마비를 유도할 수 있는 잠재적 위험이 커지고 있음

② 이란, 러시아 관련 사이버 조직이 5개월 동안 36개 미국 내 기반 시설을 공격
미국 DNI 산하 사이버 위협 인텔리전스 통합 센터(CTIIC)는 미국 정보기관들이 수집한 사이버 위협 정보를 통합하여 관리하고 분석하는 기관임. CTIIC는 지난 2023년 11월부터 2024년 4월까지 미국 내 주요 기반 시설을 대상으로 한 사이버 공격 통계를 발표했으며, 이 기간 동안 에너지, 급수, 식품 등 다양한 기반 시설이 공격 대상이 되었음을 보고함. 특히 러시아와 이란의 해킹 그룹들이 주요 공격 주체로 밝혀졌으며, 러시아 해킹 그룹은 주로 급수 시스템을 타겟으로 삼는 등 각 그룹이 자신들의 전문 분야와 취약점을 이용해 특정 시설을 집중적으로 공격하는 경향을 보임

- **사이버 위협 환경 변화: 디지털 트랜스포메이션 (Digital Transformation)**

① 코로나로 인한 기반 시설의 급격한 디지털 전환은 취약점과 공격 표면을 급증시킴
코로나19로 디지털 전환이 급격히 이루어지며 사이버 보안 취약점이 늘었고, WEF는 디지털 기반 시설에 대한 사이버 위험이 계속 증가할 것으로 전망함

② 냉전, 신냉전, N개의 냉전: 국가 지원을 받는 해킹조직 증가
'N개의 냉전 시대' 속 국가 간 갈등이 사이버전을 촉발하며, 사이버 공격이 원전이나 기반 시설을 마비시킬 수 있는 주요 수단이 됨

③ 인플레이션, 기후변화, 지정학적 충돌 등 다양한 위험이 동시에 발생
WEF 보고서에 따르면 인플레이션과 자연재해 같은 단기 위험과 더불어 사이버 범죄가 장기적 위험으로 부상하고 있음

④ 사이버 범죄 국가 간 충돌, 가짜뉴스, 불법 경제의 성장 등이 큰 영향을 미침. 사이버 위협은 허위 정보, 국가 간 갈등, 불법 경제와 결합해 더욱 심각해지고 있음

⑤ 빅테크 기업의 감원은 고급 기술력을 빼내어 해커를 증가시킬 수 있는 요인. 대규모 감원으로 일부 기술 인력이 해커로 전향하고, 제로데이 취약점이 다크웹에 판매되며 기반 시설의 위험이 증가함

⑥ 공격 그룹의 전술 변화: 웨일링 어택 (Whaling Attack)
공격 조직들은 대형 목표를 노리는 'Big Whaling Attack'을 통해 큰 자금을 노리며 주요 기반 시설까지 표적으로 삼음

⑦ 더 많은 에너지 생산을 요구하는 지구 온난화의 영향
기후 변화로 전력 수요가 증가하며 발전 시설에 대한 사이버 공격 위협이 증가하고, 신재생 에너지 시설은 여전히 취약한 상황임

– 기반 시설 보호 정책 및 대응

① 접근 방식: 잠재적 위험 (All-hazard) v.s. 사이버 위험 (cyber risk)
국가별로 기반 시설 보호에 대한 접근 방식이 다르며, 미국, 영국, 호주는 물리적·사이버 위협을 포괄하는 잠재적 위험 기반 대응 방식(All-hazard)을, 한국, 프랑스, 싱가포르는 사이버 위험 기반 대응 방식(cyber risk)을 채택하고 있음

그림 29 : 기반 시설 보호에 대한 두 가지 접근법

구분	잠재적 위험 기반 대응	사이버 위험 기반 대응
주요위협	▪ 자연재해 및 재난 ▪ 시스템 실패 및 장애 ▪ 공급망 위험, 테러 ▪ 사이버 공격 등	▪ 시스템 실패 및 장애 ▪ 악성코드 감염, DDoS 등 사이버 공격
법률/규정	▪ 미국 PPD-21, EO-13636 ▪ 영국 NIS Regulations ▪ 호주 Security Legislation Amendment Act of 2022	▪ 우리나라 정보통신기반보호법 ▪ 프랑스 CIIP Law ▪ 싱가포르 Cybersecurity Act 2018
전략/계획	▪ 미국 국가기반보호 계획 및 분야별 보호 계획 ▪ 호주 CIR strategy and plan ▪ 영국 CIR Strategy	▪ 우리나라 부처별 기반시설 보호계획 ▪ 일본 주요기반 시설 사이버보안대책 이행계획

② 기반 시설의 사이버 공격 증가로 인한 사이버 보안 강화 정책 확대
국가별 기반 시설 보호 대책은 각국의 상황에 맞춰 선택되고 있으며, 주로 세 가지 접근 방식이 활용됨

- 위험도 기반 접근 방식: 미국의 NIST 사이버 보안 프레임워크처럼 사이버 위험을 분석해 공격을 방어하고 서비스의 생존성을 보장하는 것이 일반적이며, 한국도 기반 보호법에 따라 매년 취약점 분석을 시행함
- 둘째, 이해자 간 공동 협력: 정부와 다른 이해 당사자들이 협력해 보호 대책을 수립하고 추진하는 방식이 채택됨
- 셋째, 운영 주체에 대한 의무 부과: 한국은 법률에 따라 기반 시설 운영자에게 보호 책임을 부여하며, 최근 미국도 유사한 양상을 보임

③ 미국의 '국가 사이버안보 전략'에서의 기반 시설 보호 방향: 의무 부과와 협력
미국의 최신 국가 사이버 안보 전략에서는 민간 기반 시설에 대한 보호 규제를 신설하여 인프라 안전을 강화하겠다는 목표가 명시됨. 기존에는 민간 운영자가 자율적으로 정부와 협력해 보호 대책을 마련하는 방식이었으나, 이번 전략에서는 정부가 규제 역할을 강화할 것임을 분명히 하였음. 이를 구체화하기 위해 한국의 기반보호법과 민간 참여 사례에 대한 관심도 높아지고 있음
또한, 정부는 민간 운영자가 보안 비용을 감당할 수 있도록 지원을 약속하였으며, 이 부분은 대형 사업자에 대한 지원이 부족한 한국에도 시사점을 줌. 두 번째 전략으로는 민간과 공공 부문이 각자의 장점을 활용해 네트워크화된 분산형 사이버 방어 모델을 구축하겠다는 방침이 포함되었으며, 이는 협력적이고 특화된 접근을 통해 국가 방어력을 강화하는 방안을 제시함

- **기반 시설의 미래는?**

① OT 악성코드가 말해주는 미래
기반 시설의 사이버 위협은 점점 고도화되며, 초기의 스턱스넷 (Stuxnet)처럼 특정 시스템을 목표로 하던 악성코드는 피패드림 (Pipedream)과 인더스트리얼2 (Industroyer2) 같은 다기능 모듈 형태로 진화해 여러 제어 시스템을 동시 타격할 수 있음

② 우리 기반 시설은 안전할 것인가
한국은 딜로이트 사이버 스마트 스코어 (Deloitte Cyber Smart Score)에서 높은 해킹 노출도를 보이며, 반도체 등 주요 산업이 타겟이 될 가능성이 큼. 이는 기반 시설의 보호 강화가 필요함을 시사함

③ 국가 기반 시설을 더욱 안전하게 만들기 위한 제언
· 민간 사업자가 자신의 역량을 사이버 공격 탐지 및 방어에 적극 활용할 수 있는 법·제도적 장치 마련
· 각 분야별 사이버 위험 분석 및 대응을 지원할 수 있는 전담 조직 신설
· 기반시설을 운영하는 조직에 대한 재정적, 기술적, 인력적 직접 지원방안 마련
· 기반시설 보호제도에서 민간 기반시설 운영기관의 참여 기회 확대
· 글로벌 기반시설 지정과 관리 규범 마련

2) (토론/ 좌장: 김상배 한국사이버안보학회(KACS) 회장)

- **문종현 지니언스 이사**

① 기반 시설 공격 사례: 플로리다 수돗물 해킹과 콜로니얼 파이프라인 사건
2021년 플로리다의 수도 시설이 해킹되어 치사량에 가까운 수산화나트륨 농도가 조정되었고, 같은 해 콜로니얼 파이프라인이 다크사이드 해킹 조직에 의해 공격받아 미국 동부에 주유 대란이 발생. 이러한 사건들은 사이버 공격이 생명과 국가 안보에 직결될 수 있음을 시사함

② 사이버 공격의 진화: AI와 딥페이크 활용
북한 사이버 공작원이 AI 기반의 딥페이크 기술을 통해 신분을 위장하여 미국 보안

회사에 취업을 시도한 사례가 있었음. 이는 향후 AI가 기반 시설 공격에도 활용될 가능성을 보여줌

③ 국내 기반 시설 공격 사례와 국가 차원의 대응 필요성
2023년 건설 기계 관련 사이트가 해킹되어 악성코드가 유포된 사례가 있었으며, 이는 민간 시설 정보 유출과 국가 안보 위협으로 확대될 가능성을 내포함

- **신소현 아산정책연구원 부연구위원**

① 법 제정의 지연과 사이버 안보 전략의 중요성
법이 기술 발전에 비해 뒤처지면서 사이버 안보법과 같은 필수 법안들이 오랜 기간 통과되지 않고 있음. 이에 따라 법적 공백을 메우기 위해 전략 수립이 중요한데, 한국은 2019년과 2024년에 사이버 안보 전략을 발표했으나, 내용이 구체적이지 않음

② 국제사회와의 소통 및 민간 참여 필요성
전략 수립 시 민간의 협력과 인센티브를 제공해 의견을 반영하는 민주적 절차가 필요함. 또한, 전략을 국제기구 및 시민단체에 적극적으로 공유해 한국의 성과를 알리고 피드백을 받을 필요가 있음

③ 리뷰 커뮤니티와 체계적 검토의 중요성
국가 사이버 안보 전략의 주기적 검토를 위한 리뷰 커뮤니티가 필요하며, 전략의 이행을 체계적으로 평가하고 개선점을 반영해 향후 전략 수립에 반영하는 구조가 요구됨

- **송태은 국립외교원 교수**

① 사이버 공격의 주요 원인과 목적
현재 사이버 공격의 86%가 지정학적 갈등에서 비롯되며, 러시아와 우크라이나, 중국, 미국 등이 주요 공격 국가로 등장함. 이러한 갈등은 기반 시설 공격을 통해 국가 안보와 국민 생명에 위협을 주고 있음

② 공격 대상과 빈도
기반 시설 공격 중 보건과 통신 부문이 가장 큰 타겟이 되고 있으며, 미국과 영국이 랜섬웨어 및 멀웨어 공격의 주요 표적이 되고 있음. 특히 미국은 영국에 비해 9배 이상 많은 멀웨어 공격을 받고 있음

③ 북한의 공격 대상 변화
북한은 과거 한국을 주로 공격했으나 최근에는 미국을 대상으로 한 공격 비율이 40% 이상 증가, 미국이 주된 목표가 되는 양상을 보임

④ 사이버 공격이 경제에 미치는 영향
중소기업은 사이버 공격을 당한 뒤 60%가 1년 내 폐업하며, AI와 같은 첨단 기술의 악용이 더해지면 경제적 피해가 심각해질 전망임

⑤ 신종 사이버 공격 모델: RaaS (랜섬웨어 서비스)
공격자가 다크웹에서 구독 방식으로 공격 기술을 구매하는 RaaS 모델이 등장하여 민간과 핵심 기반 시설 모두 심각한 위협에 노출되고 있음

- **박찬암 스틸리언 대표이사**

① 민간 협력의 중요성
사이버 보안 강화를 위해 민간과의 협력이 필수적이며, NSA 역시 협력의 중요성을 강조함. 랜섬웨어 대응에서도 국제 협력과 민간 협력이 실질적인 성과를 보여주고 있어 이러한 협력을 더욱 강화할 필요가 있음

② 기반 시설의 폐쇄성과 보안 취약성
한국의 헌법 기관에서 발생한 해킹 사례처럼, 기반 시설의 폐쇄성이 보안의 약점이 될 수 있음. 이를 해결하기 위해 "해킹 예방 주사"와 같은 정기적인 보안 점검을 통해 면역력을 높이는 접근이 필요함

③ 규제 강화를 통한 보안 이행
일부 산업 분야에서 사이버 보안에 대한 중요성을 체감하지 못하고 있어, 규제와 같은 강제성을 통해 국가 차원의 보안 강화를 이행할 필요가 있음

Q. 청중 질문 1
국내외에서 사이버 보안 규범이 정립되지 않은 이유는 무엇인가? 특히 국내에서 사이버 안보법 제정이 20년째 지연되는 이유와 유엔 중심의 국제 규범 논의 최신 현황은?

A. 청중 질문 1 답변(신소현 토론자)
사이버 안보 기본법의 통과가 중요한 것은 사실이나, 이를 통과시키는 것이 모든 사이버 문제를 해결할 것이라는 오해는 경계해야 함. 기본법이 각 분야의 문제를 포괄적으로 다루지는 못하며, 국방, 정보 등 각 분야에서 개별적으로 법률을 개정하거나 신설하는 노력이 필요함. 따라서 사이버 안보 기본법의 통과와 함께 세부적으로 고쳐 나가야 할 법들을 개선해 나가는 것이 중요하고, 기술 발전 속도에 대응하기 위해 법이 따라가기 어려운 부분은 전략 수립을 통해 보완해야 함

A. 청중 질문 1 답변(송태은 토론자)
국제 사이버 규범이 만들어진다 해도 국가 배후의 해커 조직들은 여전히 활동하며, 사이버 공격을 비즈니스 모델로 수행하고 있어 규범의 한계가 있음. 따라서 사이버 규범 마련과 더불어 해커들에 대한 억지력을 보여주는 실제 작전 수행이 중요함. 예로 한국과 미국 간의 사이버 동맹 훈련 이후 다른 국가들이 한국과의 훈련을 요청하는 사례가 늘어났으며, 규범 마련과 동시에 방어 및 공격 능력을 실질적으로 투사하는 것이 필요함

Q. 청중 질문 2
민관 협력에서 기반 시설의 폐쇄성을 완화할 기준과 기업의 참여 범위는 어떻게 설정할 수 있는가? 폐쇄성 완화와 협력 강화를 위한 구체적인 방안은 무엇인가?

A. 청중 질문 2 답변(문종현 토론자)
기반 시설과 특정 기관의 폐쇄성에 대해 민관 협력이 실제로는 긴밀하게 이루어지고 있으나, 외부에 잘 알려지지 않아 오해가 있을 수 있음. KISA, 국정원, 경찰청 등과의 협력 사례를 언급하며 정부와 민간 간의 협력이 은밀하게 진행되고 있다고 설명함. 현재 보안 전문가 간의 정보 공유와 정부 차원의 개방적 태도 변화로 상황이 점차 나아지고 있음

Q. 청중 질문 3
대기업과 민간 기업 중 제한된 자원으로 어디에 정보 보호 지원을 집중하는 것이 더 효과적인가?

A. 청중 질문 3 답변(최광희 발표자)
기반 시설 보호 지원은 단순히 기업의 규모에 따라 결정되는 것이 아니라, 위험도와 국민 생활에 미치는 영향을 고려해 필요하다면 대기업에도 지원이 이루어져야 함. 정부는 기업의 규모보다는 위험도, 기술의 중요성, 시급성 등을 기준으로 유연한 지원 정책을 도입하고, 대기업에 대한 지원은 장기적으로 회수하는 방식도 고려할 수 있음

A. 청중 질문 3 답변(박찬암 토론자)
금융 부문에서는 범죄자, 북한의 사이버 테러 등 여러 보안 도전 과제에 직면하고 있으며, 금융감독원, 금융보안원, 경찰, 국정원 등과 협력해 대응하고 있음. 반면 국가 중요 인프라나 헌법 기관들은 폐쇄성과 독립성으로 인해 보안 챌린지가 적어 취약한 부분이 있었음. 따라서 중요한 기관일수록 민간과의 협력을 확대하고, 외부 검증을 통해 보안성을 강화해야 함

● 세션 2

1) **발표: 양병희 KAIST 미래국방AI특화연구센터 교수) 인공지능과 국제안보의 변화**

- **인공지능(AI)의 현주소**

① 인공지능 기술의 발전
인공지능(AI)의 발전은 여러 차례의 주요 터닝포인트를 통해 이루어져 왔음. 1950년대에 인간 지능을 기계가 대신한다는 개념이 처음 나왔지만, 컴퓨터 기술의 부족으로 침체기를 겪음. 2006년 제프리 힌튼(Geoffrey Hinton) 교수가 딥 빌리프 네트워크(DBN) 구조를 발표하면서 AI 연구가 활성화되었고, 2009년 스탠포드에서 열린 영상 인식 대회가 AI 연구의 기폭제가 됨. 2016년 알파고(AlphaGo)가 이세돌을 이긴 사건이 두 번째 터닝포인트로, 이후 AI의 발전이 가속화되어 현재는 생성형 AI와 대규모 언어 모델 등의 시대에 도달함

② Top Strategic Technology Trends
가트너(Gartner, Inc.)는 매년 전략적 기술 트렌드를 발표하며, 2022년에는 AI 관련 기술로 데이터 패브릭, AI 엔지니어링, 생성형 AI 등이 포함됨. 2023년에는 디지털 면역

체계, AI 신뢰성 등 다양한 기술이 주목받았으며, 2024년에는 10대 전략적 기술 중 5개가 AI와 관련된 기술로, AI 증강 개발, 지능형 애플리케이션 등이 주요 기술로 선정됨

③ 생성형 AI의 수준 – GPT: Generative Pre-trained Transformer
GPT는 대규모 데이터를 사전 학습해 인간처럼 문자와 지식을 추론하고 생성하는 AI 모델로,GPT-4는 멀티모달 기능을 추가해 텍스트와 이미지를 함께 처리하며, 성능이 크게 향상됨. 2024년에는 더 빠르고 효율적인 모델이 출시될 예정으로, 이는 더 높은 정교함과 멀티모달 처리 능력을 갖춘 것으로 기대됨

- **국제 안보의 변화**

① AI로 인한 세계 안보 정세 흐름의 급변
미중 경쟁 심화, 러시아-북한 전쟁, 이스라엘-하마스 갈등 등으로 인해 국제 안보의 불확실성이 높아지고 있음. 전통적 안보 위협뿐만 아니라 기후변화, 감염병 등 비전통적 위협도 심화되고 있으며, 이를 해결하기 위해 국제 공조와 협력이 필수적임

② AI 발전에 따른 미래 전장의 변화
AI의 발전으로 전장의 모든 영역이 연결되어 시간과 공간의 제한이 없어지고 있으며, AI가 의사결정 과정에 참여함. 우크라이나-러시아 전쟁처럼 비군사적 수단까지 통합해 전장을 주도하는 시대가 도래함

그림 30 : AI 기반 통합 네트워크 체계: 우주, 사이버, 공중, 지상, 해상 연결

③ 미래 지능중심전(ICW) 개념
미래 전장은 네트워크 중심전에서 지능 중심전으로 진화 중이며, AI 기반 무기와 자율 시스템을 통해 네트워크 단절 상황에서도 효율적으로 군사 작전을 수행할 수 있는 모자이크 워페어로 발전하고 있음

④ 中國 지능화軍 건설 중점 추진분야
중국은 AI, 우주, 사이버 전력 강화를 통해 2030년대 세계 최강의 AI 강국을 목표로 하며, 미국과의 기술 패권 경쟁에서 우위를 점하기 위한 국방 개혁을 추진 중임

⑤ 로봇, 자율시스템(RAS) 개발 촉진
미국, 중국뿐 아니라 유럽, 호주, 캐나다 등도 AI 기반 자율살상무기 개발에 주력 중이며, 이는 병력 감소와 고위험 임무 수행을 위한 필수적인 기술로 부각되고 있음.

이로 인해 자율살상무기와 AI 범죄에 대한 사회적 우려가 증가하고 있음

⑥ 인공지능이 국제안보에 미치는 영향 (제2차 REAIM)
서울에서 열린 제2차 인공지능의 책임있는 군사적 이용에 관한 고위급회의(REAIM)에서 AI가 국가 안보에 미치는 영향을 논의함. AI는 예측 불가능한 위협과 대량살상무기에 접근할 수 있는 위험을 야기할 수 있으며, 이를 방지하기 위한 강력한 통제와 정책적 관심이 필요함

- **국제 사회의 대응 방안**

① 누구나 예측 가능한 '인공지능'
인공지능(AI)은 미래 사회의 핵심 기술로 자리 잡았으며, 이에 대응하지 않으면 안 된다는 공감대가 형성됨. AI 발전으로 인해 예상치 못한 사건이 발생할 가능성에 대비해야 함

② 신뢰 가능한 인공지능 구현을 위한 국제사회의 노력
유럽연합(EU), 미국, 영국 등은 신뢰 가능한 인공지능(AI) 구현을 위해 법과 가이드라인을 마련했으며, 민간에서는 IBM이 투명성(Transparency), 설명 가능성(Explainability), 공정성(Fairness), 강건성(Robustness), 프라이버시(Privacy)의 다섯 가지 원칙을 제시함. 이러한 원칙들은 AI 시스템이 신뢰성을 확보하고, 투명하고 공평하며 안전하게 작동할 수 있도록 보장하기 위한 요소들로 구성됨

③ AI의 군사적 사용에 대한 국제사회의 최근 동향
1차 및 2차 인공지능의 책임있는 군사적 이용에 관한 고위급회의(REAIM)에서 AI의 군사적 이용에 대한 조치가 논의되었으며, UN에서는 국제 AI 감시 기구 설립을 검토 중임. AI 사용 시 윤리적, 법적 책임을 보장해야 한다는 결론이 도출됨

④ 美 국방성 AI 개발 윤리기준 ('20.2.)
미 국방성은 AI 개발 시 책임성, 형평성, 추적 가능성, 신뢰성, 통제성을 핵심 윤리 기준으로 삼아 AI 개발 지침을 제시함됨

⑤ 맺음말: AI 시대, 국제안보 변화 방향
미래 국제 안보의 변화에 대응하기 위해 정책적으로 AI 윤리 가이드라인을 설정하고, 신뢰 가능한 AI 연구를 촉진하며, AI 윤리 교육을 강화하는 것이 필요함

2) (토론/ 좌장: 배영자 건국대학교 정치외교학과 교수)

- **윤종권 외교부 국제안보국장**

① REAIM과 주요 과제
외교부는 제2차 REAIM를 준비하며 AI와 관련된 국제적 거버넌스(governance) 및 원칙 수립의 중요성을 강조함. 각국이 이러한 원칙을 어떻게 받아들이고 국제적 거버넌스 체제를 수립하는지가 향후 AI가 국제 관계에 미칠 영향을 결정할 것이라고 평가함

② AI와 국제 정치: 국력과 군사력
AI 기술의 발전은 국가적 경제력(national economic power)과 군사력(military power)에 큰 영향을 미치며, AI 기술 보유 국가가 전략적 우위(strategic advantage)를

점할 가능성이 높음. 특히 미국과 중국의 기술 통제 및 개발 우위 확보 경쟁이 첨단 기술 분야에서 중요한 요소로 작용하고 있음

③ AI의 군사적 활용과 중요성
AI는 군사적으로 결정을 신속히 내릴 수 있는 결정적 우위(decision advantage)와 자원의 효율적 배치를 통한 분산적 우위(distributed advantage)를 제공해 군사력 증진에 기여함. 따라서 AI는 군사와 민간 구분 없이 국가 안보 문제에서 중요한 역할을 차지하고 있음

④ AI와 국제 규제의 필요성
AI의 책임 있는 이용을 위한 통제 및 균형(control and balance)이 중요하며, 각국은 기술 발전과 안보를 고려한 균형을 모색 중임. 국제적인 감시 기구나 법적 체계는 기술 발전 속도를 따라가지 못할 가능성이 크지만, AI의 사회적 영향이 커질 경우 규제 논의가 빠르게 발전할 수 있을 것으로 전망함

- **윤여선 세종대학교 국방시스템공학과 교수**

국내 방산업체와 연구소에서는 AI 기술을 국방에 도입하기 위해 노력하고 있으나, 현장 적용에 있어 법적, 제도적 한계가 존재함

① 진화적 개발 제한: AI는 지속적인 학습과 데이터 축적을 통해 발전해야 하지만, 현재 무기체계는 개발 후 고정된 상태로 평가받아야 하는 구조임

② 시험 평가의 정량적 기준: AI 무기체계는 정량적 수치로 평가하기 어려우나, 현재의 시험 평가 체계는 모든 기능을 수치화해 평가하는 방식을 고수하고 있음

③ 소프트웨어 가치 산정의 미비: AI 무기체계의 핵심인 소프트웨어는 하드웨어와는 달리 적절한 가치 산정 기준이 없어 적극적인 개발과 적용이 이루어지지 않음

변화하는 국제 안보 환경에 대응하기 위해 AI 무기 체계를 준비해야 하며, 이를 위해 연구뿐만 아니라 제도적 변화가 선행되어야 함. AI 소프트웨어의 가치를 인정하고 산업적 이윤을 확보할 수 있는 기반이 마련되어야 함

- **성경모 과학기술정책연구원 과학기술외교안보연구단장**

① AI의 국가안보 역할: 게임 체인저
AI는 국가안보에 있어 중요한 변화 요인으로 작용할 수 있으며, 미중 디지털 무역 전쟁 이후 글로벌 디지털 경제와 국가 안보 간의 긴장이 증가하고 있음. 유럽연합은 '안보에 의한 설계' 원칙을 통해 디지털 제품과 서비스의 안전성을 강화하려고 노력하고 있음

② 유럽연합과 AI 기술 규제
유럽연합은 가이아-X 프로젝트와 같은 디지털 주권 정책을 통해 산업 데이터 시장을 보호하고 있으며, EU AI 액트를 통해 AI 기술 개발과 규제의 균형을 추구하고 있음. 이는 AI의 이중 용도성과 오남용 위험을 고려한 조치임

③ 프랑스의 디지털 주권과 AI 정책
프랑스는 디지털 주권 강화를 위해 클라우드 기술 개발에 중점을 두고 있으며, 신뢰할

수 있는 클라우드 개발을 위해 기업 간 협력을 추진하고 있음. 또한, 2024년에 국방 인공지능부를 신설하여 군사 AI 개발을 촉진하고 있음

④ AI 규제와 혁신의 균형 필요성
AI의 책임 있는 이용을 위한 국제 협력과 규범화를 위해서는 AI 규제와 혁신 정책 간의 균형이 필요하며, 새로운 국가 아젠다 설정과 법적·제도적 기반 마련이 시급하다는 점이 강조되고 있음

- **김재오 인하대학교 데이터사이언스학과 교수**

① AI 기술 분류와 발전 트렌드
AI 기술은 전문가 개입 기반, 순수 데이터 기반, 복합 지능 기반으로 크게 세 가지로 구분됨. 전문가 개입 기반 기술은 컴퓨터 비전과 설명 가능한 AI와 같은 기술을 포함하며, 많은 양의 데이터와 인간의 노동력이 필요함. 순수 데이터 기반 기술은 생성형 AI와 같은 기술로, 학습 데이터를 생성하거나 증강할 수 있어 더 폭발적인 활용 가능성을 가짐. 복합 지능 기반 기술은 멀티 모달 모델을 활용하여 다양한 정보를 동시에 처리함으로써 더 정교한 추론을 가능하게 함

② AI 기술의 군사적 활용
러시아-우크라이나 전쟁과 이스라엘-하마스 전쟁에서 AI 기술이 활용된 사례가 있음. 예를 들어, 자폭형 드론과 라벤더(Lavender) 및 개스페리(Gaspari) 같은 추천 시스템이 군사적 목적에 사용됨. 이러한 기술들은 군사적 효율성을 높이지만 동시에 설계상의 오류나 데이터 편향으로 인해 예측 불가능한 위험을 초래할 수 있음

③ 복합 지능 기술과 전장 활용
복합 지능 기반의 멀티 모달 모델은 텍스트, 이미지 등 다양한 형태의 정보를 동시에 처리해 더 정확한 판단을 가능하게 함. 이러한 기술이 전장에 도입될 경우, 기계 간 전투와 같은 상상 속의 군사 체계가 실현될 가능성이 있으며, AI의 군사적 활용이 인도주의적, 법적, 기술적 측면에서 신중하게 고려되어야 함

Q. 청중 질문
발표자의 말에 따르면, AI 규제를 할 때 상대측이 규정을 지키지 않을 가능성이 있으며, 이는 국가 안보에 취약성을 초래할 수 있음. 이를 방지하기 위해서는 모니터링과 패널티 체계가 필수적인데, AI 사용에 대한 투명한 모니터링 시스템과 규정 위반에 대한 강력한 패널티를 통해 위반의 이익보다 높은 대가를 치르게 해야 함. 이러한 체계를 어떻게 구축하고 실행 가능하게 만들 수 있을지?

A. 청중 질문 답변(양병희 발표자)
2018년 카이스트와 한화 시스템이 AI 융합연구센터를 설립하자, 일부 국제 사회에서는 킬러 로봇 개발을 우려하며 제재 서명을 보냈고, 이는 큰 논란을 불러일으킴. 이에 카이스트는 해당 연구가 군사적 킬러 로봇 개발이 아닌 기초 연구임을 강조하며, AI의 책임 있는 군사적 이용을 위해 통제가 필요함을 설명함. 특히 AI 무기체계의 개발은

미 국방 AI 윤리 원칙을 적용해 사람의 통제가 가능하도록 진행되며, AI의 사회적 긍정적 활용을 권장해야 한다는 입장을 밝힘

A. 청중 질문 답변(윤종권 토론자)

군사 분야에서 AI 사용의 가장 어려운 문제는 결정적 의사결정(lethal decision-making)과 이에 따른 책임성(accountability)을 어떻게 보장할 것인가임. 신뢰성(reliability)과 추적 가능성(traceability) 등 다른 원칙들도 결국 책임성을 담보하기 위한 요소로 작용함. 무기 사용과 관련해서는 기존의 국제 인도법(International Humanitarian Law)을 적용하는 것이 일반적이며, 이는 사이버전에도 유사하게 적용됨. 국제 사회는 전장에서 질서를 유지하기 위한 노력을 지속하며, 이러한 원칙들은 전쟁 상황에서 질서를 잡아내는 데 중요한 역할을 함. 우크라이나 전쟁에서 AI 기술은 신속한 의사결정과 군사적 자산 활용을 가능하게 해, 전쟁에서 중요한 역할을 수행함

A. 청중 질문 답변(윤여선 토론자)

국방 분야에서 책임감 있고 신뢰할 수 있는 AI 개발을 목표로 지속적인 노력이 필요함

A. 청중 질문 답변(성경모 토론자)

디지털 기술 기반의 공격은 공격과 방어의 경계가 모호하며, 대한민국은 책임 있는 AI 개발을 통해 더 큰 전쟁을 피하는 방식으로 역할을 해야 함. 군사 AI를 비롯해 외교, 과학기술, 교육, 보건 등 다른 분야로 안전한 AI 사용의 범위를 확산시키기 위한 국내 거버넌스 구상도 필요함

A. 청중 질문 답변(김재오 토론자)

AI 알고리즘은 매우 취약하며, 작은 노이즈로도 인식 결과가 크게 달라질 수 있다는 점을 지적함. AI가 국가 주요 기술로서 안보의 게임 체인저 역할을 하는 만큼, 알고리즘의 장단점을 인식하면서 국제 안보 문제를 다루어야 함

참고문헌

[국문]

국가안보실. 2024.「국가 사이버안보 전략」.

국회도서관. 2023. 사이버안보 한눈에 보기. FACT BOOK 2023-8호 통권 108호.

김경숙. 홍건식. 2023. 중국의 핵심광물 수출통제와 시사점. INSS 전략보고. No.243. 국가안보전략연구원.

김경숙. 2024. EU의 공급망 디리스킹(de-risking) 전략과 전망. INSS 전략보고. No.278. 국가안보전략연구원.

김광석, 박세익, 박정호, 오태민. 2024.「트럼프 2.0. : 트럼프의 귀환, 놓쳐서는 안 될 정책 변화와 산업 트랜드」. 이든하우스 출판: 서울.

김대원 외. 2023. “국방 우주 분야의 무기체계 개발동향 및 국방전략기술 발전방향”. 한국산학기술학회 Vol. 24(9).

김대용. 2024. “무역안보 시대의 핵심광물 공급망 전략 비교 연구”. 무역안보관리원.

김상배 외. 2024.「사이버 안보의 국제정치학」. 사회평론아카데미: 서울.

김태헌 외. 2024. “사용후 배터리 재활용 국내·외 시장동향 및 에너지정책 분석”. 에너지기후변화학회지, Vol. 19(1).

박가현 외. 2022. “주요국의 핵심광물 확보전략과 시사점”. 글로벌공급망분석센터 상하이지부.

매일경제 글로벌경제부. 2024.「트럼프 2.0 또 다른 미국」. 매경출판: 서울.

안상욱. 2023. “EU와 주요 EU회원국의 배터리 공급망 정책의 차이점: 대중국 전략”. 유럽연구, Vol. 41(3).

강병철. 2024. “‘트럼프 폭풍’ 목전에 두고 리더십 공백... 한미동맹에도 악영향”. 연합뉴스, 12월 14일.

이동규. 2023. 중국 우주력 발전의 군사안보적 함의. 중국전문가포럼 전문가 오피니언. 대외경제정책연구원.

이만석. 2024.「미국의 동맹전략: 미국은 왜 한미동맹을 필요로 하는가」. 플래닛미디어: 서울.

이벌찬. 2024. “中“안보·과학기술을 쌍두마차로… 美 봉쇄 뚫겠다”, 조선일보, 7월 19일.

이승주. 2024. 경제도전 1: 미중 인공지능 생태계 디커플링. 스페셜리포트. EAI 동아시아연구원.

이승필 외. 2023. “전기차 배터리 핵심광물”. 한국과학기술기획평가원.

전재성. 2024. “군사도전 2: AI 기반 자율무기체계, 인지전의 발전과 군사안보질서의 변화”. AI와 신문명 표준 스페셜 리포트. 동아시아연구원.

정성택. 2023. “푸틴의 트롤부대 ‘ 나토가 전쟁 일으켰다’ 세뇌”, 동아일보, 6월 30일.

정해영, 이정아, 한주희, 고성은. 2024. 미국의 경제안보·핵심기술 통제 전략 강화 및 시사점. KITA 통상리포트. Vol.3. 한국무역협회통상지원센터.

조은정. EU「우주안보 및 방위전략」: '전략적 자율성'과 '상호운용성'의 동반 제고. INSS 전략보고. No. 266. 국가안보전략연구원.

차정미. 2024. 미중 전략경쟁과 우주외교(Space Diplomacy) 경쟁. 국가전략, Vol. 30(3).

한국과학기술기획평가원. 2024. 유럽 경제안보 강화를 위한 5가지 이니셔티브 제안. 주요 동향. 글로벌 과학기술정책정보 서비스(S&T SPS).

한국리서치. 2024. 2024 인공지능 인식조사.

[영문]

Benson, Emily, Federico Steinberg, and Pau Alvarez-Aragones. 2024. *The European Union's Economic Security Strategy Update*. Center for Strategic & International Studies.

Ernest & Young LLP. 2024. *2024 Human Risk in Cybersecurity Survey*.

François CHIMITS, Conor McCAFFREY, Juan MEJINO LOPEZ, Niclas Frederic POITIERS, Vincent VICARD, Pauline WIBAU. 2024. *European Economic Security: Current practices and further development*. European Parliament.

Gartner. 2024. *Quarterly Emerging Risk Report – Third Quarter.*

Giuliana Viglione. 2020. *China is closing gap with United States on research spending.* Nature.

Gilbert, Natasha & Smriti Mallapaty. 2024. *US and China sign new science pact but with severe restrictions.* News. Dec 13. Nature

Gillespie, N., Lockey, S., Curtis, C., Pool, J., & Akbari, A. 2023. Trust in Artificial Intelligence: A Global Study. The University of Queensland and KPMG Australia. doi: 10.14264/00d3c94.

Mariarosaria Taddeo, Alexander Blanchard, Kate Pundyk. 2024. *Consider the ethical impacts of quantum technologies in defence before it's too late. News. Oct 22. Nature*

Michal Krelina, Lieutenant Colonel Denis Dúbravčík. 2024. *Quantum Technologies for Air and Space (Part 3 of 3), Quantum for ISR and PNT: Use Cases and Timelines.* Journal Edition 38. JAPPC.

National Science and Technology Council. 2024. *Critical and Emerging Technologies*

List Update. Executive office or the President of the United States.

North Atlantic Treaty Organization. 2024. *Summary of NATO's Quantum Technologies Strategy*. News. Jan 16.

North Atlantic Treaty Organization. 2024. *Science & Technology Trends 2023-2043*, NATO Science&Technology Organization. Vol 2.

Parker, Edward. 2024. *The Chinese Industrial Base and Military Deployment of Quantum Technology*. The Rand Corporation.

Pawel Swieboda. 2024. *Europe needs a 360° Economic security policy.* European policy center.

Reuters. 2024. *US concerned about China's use of AI, says it could make countries vulnerable to coercion*. Oct 24.

REUTERS, 2024.'*Chinese battery cash will fuel Europe's EV drive*,' https://www.reuters.com/breakingviews/chinese-battery-cash-will-fuel-europes-ev-drive-2023-05-31/.

The White House. 2024. *Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence.*

The White House. 2024. *FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence.*

The White House. 2024. *FACT SHEET: Addressing U.S. Investments in Certain National Security Technologies and Products in Countries of Concern.*

The White House. 2024. *National cybersecurity strategy implementation plan*. Version 2.

Thibault Denamiel, Taylar Rajic, William Alan Reinsch, James Andrew Lewis, and Julia Brock. 2024. *Beyond Economics: How U.S. Policies Can Undermine National Security Goals*. Center for Strategic & International Studies.

UK Government. 2024. *AI Cybersecurity Survey - Main Report*

World Economic Forum. 2024. *Global Risk Report 2024 (19th edition)*. World Economic Forum.

World Economic Forum. 2024. *Navigating Cyber Resilience in the Age of Emerging Technologies: Collaborative Solutions for Complex Challenges.*

Sarah Kreps. 2024. ***T****he global AI race: Will US innovation lead or lag?*. Commentary. Dec 6. Brookings institute.

Seoul Dialogue: Advancing Global Cooperation in Cyber and AI Technologies

Report of the World Emerging Security Forum

Edited by: So Young Kim, Cornelius Kalenzi, Danbee Back, Jeon Junhyeong, Minahir Shahid Qumar Aali

Table of Contents

Forum Summary

The World Emerging Security Forum (WESF), launched in 2021, served as a critical platform for fostering international cooperation to address emerging and cross-border security threats. Amid a hyper-connected world, rapid technological developments, such as artificial intelligence (AI) and digital innovations, presented new and complex security challenges.

WESF advocated for multilateral dialogue and cooperation to develop inclusive, coordinated solutions that prevented fragmentation in global security efforts.
WESF 2024, held on December 5, 2024, in Seoul, explored the intersection of geopolitics and emerging technologies, specifically focusing on AI, cyber threats, and the competition for technological resources. The event brought together governments, international organizations, industry leaders, academics, and the media to deliberate on security challenges stemming from technological convergence and geopolitical rivalries.

Session I: AI and Emerging Technologies

AI's rapid integration into key domains like military operations, nuclear weapons, and space exploration raised significant security concerns. Building on frameworks like the Blueprint for Action adopted at REAIM 2024, the session highlighted the dual nature of AI—its potential benefits and risks. Key concerns included AI's potential to disrupt deterrence strategies, shift power dynamics in space with enhanced capabilities, and amplify the threat posed by chemical and biological weapons.

The session emphasized the need for proactive, agile policies to govern AI's convergence with other technologies, mitigate misuse, and anticipate long-term risks. Participants addressed how AI had begun to affect nuclear deterrence strategies, space militarization, and the importance of international cooperation in aligning technological growth with security frameworks.

Session II: Defending Cyberspace

The evolution of cyber threats—ransomware, hacking, spyware, and cryptocurrency theft—posed significant risks to global security. State and non-state actors increasingly used cyber tools for military aims and to compromise critical infrastructure, such as energy, transportation, and healthcare systems. Events like the 2024 UN Convention Against Cybercrime and warnings from initiatives such as the Five Eyes alliance regarding threats like the Volt Typhoon hacking group highlighted the growing urgency.

The session addressed how emerging technologies like AI and quantum computing exacerbated cyber threats, complicating cybersecurity measures. Participants discussed the geopolitical implications of cybercrime, its impact on critical infrastructure, and the role of multilateral mechanisms in mitigating risks. A key focus was understanding cybercrime as a

'threat multiplier' in conflicts.

Session III: Competition for Technological Dominance

The session examined the battle for technological dominance driven by competition over critical minerals, semiconductors, and batteries. Geopolitical tensions—evident in US-China export restrictions on semiconductors and China's control over mineral supply chains—highlighted vulnerabilities in interdependent global supply chains. Critical components like rare earth elements remained vital for advanced military systems, navigation tools, and AI-driven energy demands.

The discussion focused on how resource strategies interacted with goals for technological competitiveness, the risks to defense industries, and supply chain resilience. Issues like stockpile depletion, reliance on Taiwan's semiconductor production, and energy transition minerals amplified security concerns. Participants explored international frameworks to balance competition with global stability.

WESF 2024 succeeded in bridging policy gaps and promoting cooperation on these pressing security issues. The forum laid the foundation for adaptive strategies to address evolving challenges in AI, cybersecurity, and technological competition.

Welcome Remarks

RHEE Dong-yeol, Ambassador for International Cyber Affairs, Ministry of Foreign Affairs, Republic of Korea

Excellencies, Distinguished Guests, Ladies and Gentlemen,

Good morning.

It is my great honor to welcome you to the 2024 World Emerging Security Forum. My sincere thanks go to SIPRI, and KAIST for their tremendous contributions to this forum.

Just months ago, the Nobel Prize Committee recognized the extraordinary era we live in by awarding not one but two prizes to pioneers in artificial intelligence. One celebrated the breakthrough in AI-driven protein folding, unlocking possibilities in medicine, and the other

recognized the transformative power of generative AI.

These accolades represent the essence of our time—an age where technological innovation is reshaping the very fabric of our world, offering unprecedented opportunities as well as risks. The tectonic plates of global security are shifting beneath us, and emerging technologies are redefining the fundamentals of our national security—who, what, where, and when.

Let us put this into perspective.

In the 1940s, the advent of air as a new domain of warfare overwhelmed strategists, who suddenly had to think three-dimensionally to defend their nations. Today, multi-domain challenges extend beyond the physical into cyberspace and even into space itself, all enabled by digital and space technologies. Meanwhile, cutting-edge technologies are changing the how of warfare in profound ways.

The lines between state and non-state actors are blurring as off-the-shelf, dual-use technologies become readily available. Autonomous systems further challenge the distinction between humans and machines. In cyberspace, anonymity makes answering the question of who is responsible nearly impossible.

Furthermore, the when—a new kind of threat now permeates our daily lives. The traditional distinction between wartime and peacetime is fast disappearing. Malicious cyber activities, such as cryptocurrency theft, data breaches, and disinformation campaigns, target our daily lives and the democratic institutions underpinning our societies. Even activities once considered purely commercial, like securing raw materials for industrial growth, have transformed into matters of strategic urgency.

Finally, what—the nature of the threats we face—is evolving. In the past, technological advancements displaced old systems: bows gave way to guns, horses to tanks. Today, however, new technologies coexist and integrate. The rise of drones has not rendered nuclear stockpiles obsolete. Instead, technologies synthesize, adding exponential complexities to both threats and defense.

This brings us to a critical question:

What will be the impact of AI, the ultimate enabler of everything, and quantum technology, the ultimate accelerator of everything? Will the world be more secure or less secure with these technologies? And what does the nexus between AI, cyber, and weapons of mass destruction mean for global security?

Distinguished Guests,

This brave new world calls for both vigilance and vision—vigilance to clearly understand the threats and their complexities, and vision to imagine a better and safer tomorrow. A tomorrow we can only achieve by working together.

Progress has been made. UN members adopted the UN Framework for Responsible State Behavior in the Use of ICT, even though ambiguities persist regarding the application of international law and accountability. Agreements like the recent U.S.-China accord on maintaining human control in nuclear decision-making—on the sidelines of the last two APEC meetings—show that multilateral understanding is possible on such critical issues as AI's role in weapons of mass destruction.

But we must act fast. Technological advancements will not wait for us. If we fail to create robust norms and governance fit for our time, we risk catastrophic consequences for security and human dignity.

The Republic of Korea stands ready to lead in this effort, in line with our foreign policy vision as a Global Pivotal State. Korea seeks to lead global cooperation on emerging technologies and security challenges, playing a triple role as initiator, facilitator, and supporter.

- As an initiator, we have spearheaded global conversations on new norms and governance. Hosting the second LE AIM Summit in September, we provided momentum for the UN General Assembly to adopt the first-ever resolution on responsible AI use in the military domain. As an elected member of the UN Security Council, we enhanced the Council's engagement on cybersecurity and hosted an open debate on the issue in June.
- As a facilitator, we champion collaboration on core emerging technologies—such as semiconductors, batteries, AI, quantum, and space. As a founding member of the growing global network of AI Safety Institutes, launched during the AI Seoul Summit this past May, and as chair of the Mineral Security Partnership since July, we are leading efforts to stabilize and diversify critical supply chains.
- As a supporter, we are actively bridging the digital divide across all regions and promoting an open, free, and secure cyberspace. We leverage our growing Official Development Assistance (ODA) to fortify cybersecurity capacity in nations most vulnerable, recognizing that strengthening these links is crucial for global network resilience.

Our work is guided by the principle of inclusivity, equal in priority to safety and innovation. This principle was recognized in the Seoul Declaration, adopted during the AI Seoul Summit 2024.

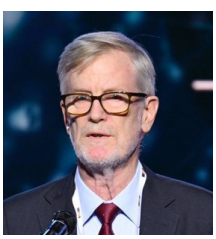
At home, we lead by example. Korea's Cybersecurity Strategy, adopted in February, its implementation plan in September, and the launch of our National AI Committee in October, underscore our unwavering commitment to safety, inclusivity, and innovation.

Distinguished Guests,

Since 2021, the World Emerging Security Forum has catalyzed global discourse on international security, recognizing the importance of multi-stakeholder engagement in our evolving security landscape. It is deeply encouraging to see the collaborative spirit among the broad spectrum of leaders and experts in this room—governments, international organizations, academia, industry, and civil society. Each of us holds a critical piece of a larger puzzle.

By working together with vigilance and vision, we can harness the opportunities of emerging technologies while minimizing their risks. As we come together to share our insights, let us leverage this opportunity to chart a path forward toward a safer world for generations to come.

Thank you.



Dan SMITH, Director, Stockholm International Peace Research Institute (SIPRI)

Thank you very much, Ambassador Rhee. Excellencies, friends, colleagues, ladies and gentlemen, it is truly my pleasure to join in welcoming you all to the World Emerging Security Forum 2024. Allow me to begin by saying that it has been both an honor and a privilege for the Stockholm International Peace Research Institute (SIPRI) to assist and collaborate with the Ministry of Foreign Affairs of the Republic of Korea in preparing for this forum and to participate here today.

I must also acknowledge that Tuesday night's events have created an unusual backdrop for our meeting. While I do not wish to comment in detail, I will say that I am glad to see

democratic institutions and culture in the Republic of Korea standing strong under this test.

World security today faces an array of challenges that include aggression and provocative behaviour by some states, intractable local and regional conflicts, ecological disruptions—particularly climate change—and emerging technologies that present both opportunities and threats. Some of these challenges are immediate and require urgent responses, while others are longer-term but demand our attention without delay. One difficulty we face, both as researchers and policymakers, is balancing priorities. We must address urgent challenges without neglecting the long-term issues that shape the future. This is one of the reasons I find the World Emerging Security Forum so valuable: it provides a platform to move beyond immediate threats and focus on what is changing and unfolding before us.

The war in Ukraine reminds us how different timeframes can converge within a single crisis. It is both an old-fashioned war of aggression, reminiscent of battles from the First World War, and a hypermodern war, where tools like drones, hybrid warfare, and cyber battles—once considered science fiction—are now a reality. In essence, tomorrow has already arrived, even as yesterday still lingers.

We have seen the consequences of delay before. Scientists outlined the global challenge of climate change over 40 years ago. In fact, the foundations of climate science go back to the 19th century, when Swedish scientist Svante Arrhenius predicted the impact of carbon dioxide on global temperatures in 1896. His work was well-researched and remains valid today. Yet we did not act soon enough. Similarly, consider a book published by SIPRI and Oxford University Press in 1987, titled "Arms and Artificial Intelligence." It examined the potential of AI in weapons development and arms control, offering insights into many of the very problems we are discussing today. The publication date was 1987. How long did it take us to engage meaningfully with these issues? Even now, our governments struggle to develop cross-governmental approaches, align with allies, and understand the interconnections between fields like AI, strategic stability, and security.

This forum, therefore, plays a crucial role: it can help cut down the time it takes for us to identify, grapple with, and address emerging challenges. Advances in quantum science are poised to revolutionize areas such as sensing, imaging, navigation, computing, and information sciences, among others. The benefits could be profound, including faster detection of chemical, biological, radiological, and nuclear threats, as well as improved climate modelling and ecosystem monitoring—all of which have clear implications for peace and security.

However, as with all technologies, downsides will emerge. Quantum advances could

undermine encryption, jeopardizing the security of communications and financial systems. Quantum sensors could detect submarines or underground objects previously hidden, which would destabilize the security of submarine-based nuclear deterrence. Do we want to repeat the mistakes we made with AI—failing to act until years or decades later? My colleagues at SIPRI are now studying the peace and security implications of the quantum revolution. Let us not wait 30 to 40 years to act on their findings.

Arms control frameworks are collapsing, and a new nuclear arms race is unfolding. Unlike the Cold War arms race, this one is likely to focus less on warhead numbers and more on cyberspace and outer space. It may also involve three major powers instead of two. If we are fortunate enough to arrive at a moment—after a dangerous decade—when all sides see the value of agreeing to guardrails and limits, the technological challenges of arms control will be dauntingly different.

The research community must become better at addressing risks, where uncertainty is inherent, rather than waiting for "proof" that often comes too late. Similarly, the policy community must improve at balancing priorities, ensuring that future challenges receive adequate attention alongside immediate crises. This is why the World Emerging Security Forum is such an important event. By bringing together the policy and research communities, it enables us to explore critical dimensions of the evolving security landscape.

With that, I want to thank you again for your attention and extend my gratitude to the Ministry of Foreign Affairs for their excellent cooperation. I hope that today's discussions will be engaging, productive, and forward-looking. Welcome once again to the World Emerging Security Forum 2024.

Thank you very much.

Kwang Hyung LEE, President of Korea Advanced Institute of Science and Technology (KAIST)

Minister of Foreign Affairs, Cho Tae-yeol, Mr. Stefan Löfven, Chair of the Governing Board of the Stockholm International Peace Research Institute, distinguished guests, and participants both online and offline,

I am Professor Kwang-Hyung Lee, President of KAIST, and it is my honor to welcome you to the 2024 World Emerging Security

Forum here in Seoul. Allow me to express my gratitude to the Ministry of Foreign Affairs for organizing this forum in partnership with the Stockholm International Peace Research Institute (SIPRI) and KAIST. Now in its fourth year, the World Emerging Security Forum continues to serve as a critical platform for governments, international organizations, academia, businesses, and civil society to advance global cooperation in addressing the complex and rapidly evolving security challenges of our time.

Today, we gather in a world that is both hyper-connected and deeply fragmented. Rapid technological advancements in artificial intelligence, cyber capabilities, and other emerging domains have unlocked unprecedented opportunities but also pose profound risks. Coupled with geopolitical tensions, these developments challenge traditional approaches to security, demanding innovative approaches.

The theme of this year's Forum, *"Global Cooperation in the Evolving Security Environment – Cyber, AI, and New Technologies,"* underscores the critical intersection of geopolitics, technology, and global security. Our discussions today aim to address not only the risks but also the transformative potential of these technologies. Allow me to highlight a few pressing areas where intensified international cooperation and innovative thinking are urgently needed.

First, preparing for global security challenges posed by AI and emerging technologies.

AI is reshaping global security in ways we are only beginning to understand. From autonomous weapons systems to AI-driven surveillance, these technologies have the potential to shift the balance of power, disrupt military strategies, and redefine international norms.

The first step to creating effective governance frameworks for AI at the global level is to gain a clear understanding of what we are trying to govern. I propose that through our respective countries and organizations, we invest time and resources in examining the meta-convergence of AI with other domains such as nuclear technology, space exploration, and quantum computing. Based on such understanding, nations will be able to craft agile, forward-thinking policies and governance systems that balance innovation with accountability and safety.

Second, fostering cooperation to address geopolitical rivalry and resource competition.

We must confront the reality that minerals, semiconductors, and batteries—the backbone of AI and emerging technologies—are now focal points of geopolitical rivalry. Dependencies between critical mineral supply chains and technological advancement threaten not only progress but also global security and economic stability. Such competition creates dangerous resource scrambles and hegemonic struggles that jeopardize peace and stability.

Through this forum, I hope we can explore the complex relationship between national strategies for resource security and the broader goals of technological sovereignty. I also hope our discussions will focus on strengthening multilateral frameworks to mitigate risks and foster equitable access to critical resources.

Third, defending cyberspace against advanced threats.

Cyber threats are growing in sophistication, frequency, and impact. Attacks on critical infrastructure, from energy grids to healthcare systems, threaten not only national security but also the livelihoods of billions. Here in South Korea, groups like the Lazarus Group have persistently targeted digital infrastructure, including satellite launch facilities, court systems, and defense contractors.

AI's ability to generate disinformation and misinformation poses significant threats to democratic processes and international stability. Recent experiences, such as those in the US presidential elections, serve as a stark reminder of the technological challenges facing democratic systems worldwide. I hope this forum will help us forge a common understanding of emerging threats and enhance cooperation to address the rapidly evolving cyber landscape.

Finally, the role of KAIST.

Permit me to acknowledge the significant role of KAIST in driving innovation and thought leadership in these domains. KAIST stands at the forefront of cutting-edge research in AI, cybersecurity, and advanced technologies, contributing to both academic advancements and practical solutions. By fostering interdisciplinary collaboration, KAIST not only develops technical expertise but also cultivates the technical and ethical frameworks necessary to navigate the challenges of emerging technologies. Our university's contributions to forums such as WESF are invaluable in bridging the gap between science, policy, and global security.

Conclusion

Ladies and gentlemen, the challenges before us demand bold vision and resolute action. The discussions we engage in today will shape the strategies of tomorrow. Let us seize this opportunity to strengthen international collaboration, responsibly harness the potential of innovation, and build a more secure and equitable future.

Together, we can ensure that the rapid evolution of technology becomes a catalyst for peace rather than a source of division. I look forward to the insights and partnerships that will emerge from this pivotal forum.

Thank you.

Carl BILDT, Co-Chair, European Council on Foreign Relations (ECFR) /Former Prime Minister, Sweden

Excellencies, Ladies and Gentlemen,

Let me begin by saluting this important international gathering. I deeply regret not being able to join you physically in Seoul today. We live in a world that has become more competitive, more confrontational, and more conflicted than it was just a few years ago.

In Europe, we are faced with the harsh reality of Russia's large-scale aggression against Ukraine. Violating every principle of international law and the global order, Russia has unleashed its full military force against a sovereign nation whose only desire was to shape its own future. This war is both brutal and technologically sophisticated. Human wave assaults reminiscent of past world wars are occurring alongside advanced drone warfare. Industrial mobilization has merged with ballistic missiles, space operations, and information warfare. Hundreds of thousands of lives have already been lost, and the destruction is enormous. The outcome of this war will shape both European and global security for years to come. The emerging link between the regimes in Moscow and Pyongyang further illustrates these evolving security dynamics.

The global security landscape is fraught with challenges. Alongside conflicts and confrontations, we cannot ignore climate change and global health threats. At the same time, we stand at a critical juncture where accelerating technological advancements intersect with intensifying geopolitical competition, creating unprecedented security challenges. Among the most critical of these challenges is the governance of artificial intelligence (AI), particularly where it intersects with nuclear command and control systems.

AI is being integrated into early warning systems, threat assessments, and decision-support tools for nuclear forces. While AI promises faster response times and improved threat detection, it also brings significant risks, including algorithmic bias, system vulnerabilities, and the potential for catastrophic errors such as “flash crashes” in crisis situations. The November 16th joint statement by the leaders of China and the United States is therefore significant. It underscored “the need to maintain human control over the decision to use nuclear weapons.” Equally important is their call to “consider carefully the potential risks and develop AI technology in the military field in a prudent and responsible manner.” Other nuclear powers should follow this example.

There are many promising initiatives aimed at addressing AI governance and security. These

include the AI Safety Summit in Bletchley Park and its follow-ups in Seoul and San Francisco, the G7 Hiroshima Process, the UN High-Level Advisory Board on AI, and the upcoming AI Action Summit in Paris this February. Additionally, the Frontier Model Forum, which brings together leading AI companies, represents a step toward industrial self-regulation—something that should be welcomed.

Beyond AI, synthetic biology has emerged as another critical security concern. Advances in CRISPR gene-editing technology and automated biolabs have dramatically lowered barriers to modifying organisms. While these tools promise groundbreaking medical advancements, they also introduce risks, including the potential creation of engineered pathogens with enhanced transmissibility and lethality.

Traditional boundaries between physical and digital security have dissolved. Today's threats are hybrid, interconnected, and often amplified by emerging technologies. For example, advanced AI can generate highly convincing deepfakes, manipulate public discourse, and design sophisticated cyberattacks. The democratization of these technologies means that capabilities once reserved for resource-rich nation states are now potentially accessible to a much broader range of adversaries.

Our critical infrastructure has never been more vulnerable. The rapid expansion of the Internet of Things (IoT) has created attack surfaces that did not exist before. Power grids, transportation systems, and healthcare facilities are increasingly networked, exposing them to cyberattacks, ransomware incidents, and sophisticated state-sponsored intrusions targeting industrial control systems.

These challenges are daunting, but they are not insurmountable. They require a fundamental shift in how we approach security. We need robust international frameworks for AI governance. This includes developing shared protocols for testing and validating AI systems, establishing "human-in-the-loop" requirements for critical decision-making, and creating verification mechanisms to ensure AI safety claims. We need a coordinated global approach to biosecurity. This means strengthening the Biological Weapons Convention and developing early warning systems for detecting engineered pathogens, while protecting vital research. We must integrate our responses across domains. Modern threats span cyber, physical, and biological domains and demand integrated responses. We need unprecedented cooperation between governments, private sector partners, and international allies.

Absolute security may be an illusion. What we must prioritize is the resilience of our societies and economies in the face of diverse security challenges. Technological change will only accelerate. Quantum computing is on the horizon, with far-reaching consequences for security

and stability. The critical question is not whether to embrace emerging technologies—they are already here and offer tremendous promise for scientific discovery and progress. The real choice is this: will we shape the development and deployment of these technologies in line with our values and security interests, or will we allow others to set the terms?

We must act decisively yet thoughtfully, balancing innovation with security, and individual liberty with collective safety. Thank you for your attention, and I wish you all a productive and insightful discussion here at the World Emerging Security Forum. Thank you.

James Andrew LEWIS, Senior Vice President, Center for Strategic & International Studies (CSIS)

Thank you. It's good to see everyone, and congratulations on this forum, which marks yet another milestone in Korea's emergence as a global power. I want to discuss the political context surrounding the issues we've been exploring today, as well as those we'll continue to address. While technology is undoubtedly reshaping the world, there are other forces we must consider.

The rise of China is arguably the most significant geopolitical development, accompanied by the decline—hopefully temporary—of Europe and the emergence of a multipolar world order. For over a decade, we've spoken of this multipolarity, but it is becoming increasingly evident that the new powers do not necessarily share the visions or values of the old order. They certainly do not view the United States as the singular leader of the global system. Additionally, we face the revanchism of former communist states. The year 1990, once celebrated as a turning point, was not the final victory many believed it to be. Instead, we are now confronting the consequences of unresolved tensions from that era.

And then there's the disinterest of the United States—not to be mistaken for decline. A country cannot lose two wars and expect its citizens to be content. That is the reality America grapples with today. Yet the U.S. remains primus inter pares—first among equals. How it chooses to engage with the world in the coming years will be influential, though not necessarily decisive, in shaping the global order. I'm not taking an entirely Eurocentric or U.S.-centric view, but the role of the United States will indeed be tested in the years ahead.

The world is experiencing a knowledge revolution, enabled by technology. This is not the first time humanity has faced such a transformative shift. The first knowledge revolution

began when Gutenberg introduced movable typewriter to Europe. It took 200 to 300 years to resolve the political challenges it created. By the 19th century, parliamentary democracy had emerged as the solution to those disruptions. Today, we are witnessing early signs that our current systems—built on the democratic frameworks of the 19th century—are increasingly inadequate. Reconstructing our political systems, both nationally and internationally, will be critical as we adapt to the connectivity and challenges created by technology.

History offers us valuable precedents to consider. The First Industrial Revolution—which began in the late 17th century—ultimately led to global conflict. In the aftermath of that conflict, the global order established in 1945 was built on rules and institutions designed to prevent future catastrophes. Those rules and institutions are now being challenged. They must be reinforced, rethought, or perhaps even replaced. Consider the Kitchen Debate of 1959 between Nikita Khrushchev and Richard Nixon. It was not just about two systems competing for dominance; it was a contest over whose system could best foster innovation and meet the needs of their citizens. That debate took 30 years to resolve. We now find ourselves at the beginning of a similar process. Hopefully, it will not take another 30 years, but we must accept that this will be a long and complex contest.

Where does Korea fit into this evolving landscape? This is a crucial question. Korea is a middle power, and middle powers have responsibilities. I recall a conversation I had years ago with a German general who asked, “Why can’t we be like Switzerland?” My initial response was lighthearted: “You don’t have enough cows or chocolate.” But the deeper answer is this: when a nation is among the largest economies, when it is a hub of technological innovation, and when it serves as an inspiration for democracy, neutrality is not an option. That applies to Germany, and it applies equally to Korea.

Technology has fundamentally altered the global dynamic. Its connectivity, the spread of knowledge, and the political tensions it generates mean that neutrality is no longer possible. So, what are our responsibilities as a global community? Rebuilding or restructuring the global order is essential. The framework established in 1945 remains fundamentally valid, particularly its emphasis on respect for individual rights and the use of democracy and markets to guide national policy. However, this framework clearly needs rethinking to address the challenges of the modern world. Dialogue and negotiation are also crucial. History has shown us the importance of engagement—whether during the Kitchen Debate, the Cuban Missile Crisis, or the post-war agreements of 1945. We must find ways to engage with adversaries, negotiate, and, hopefully, reach agreements that promote stability.

Reconstructing a democratic, rules-based global order amid unprecedented challenges to democracy and individual rights is no small task. It will require engagement, dialogue, and

a commitment to shared principles. Today's forum offers a vital opportunity to explore these issues and move closer to solutions. I thank you all for your attention, and I look forward to the discussions ahead. Thank you.

LIM Jong-in, Special Advisor to the President for Cyber, Republic of Korea

Good morning, everyone. As introduced, I am LIM Jong-In, Special Advisor to the President of the Republic of Korea for Cyber. I advise the President on AI, cybersecurity, and emerging security issues.

Previous speakers have eloquently highlighted the revolutionary impact of AI and other emerging technologies. I would like to build on these insights and explore both the opportunities and risks posed by these transformative changes. In October, as Ambassador Lee mentioned, I attended an AI academic conference in Amsterdam. The next day, Korean media widely reported that Jeffrey Hinton and Demis Hassabis—CEO of Google DeepMind—won Nobel Prizes in recognition of breakthroughs in AI and chemistry. This moment symbolized a turning point: the world realized we had entered the AI era. Since the launch of generative AI on November 30, 2022, we have witnessed its disruptive potential across every aspect of life. AI is transforming society at a rapid pace, and its applications continue to astonish us.

Take, for example, advancements in space exploration. For decades, progress in space stagnated after the Apollo missions. Yet today, thanks to AI, technologies like Falcon Heavy and Starship have redefined what is possible. The idea of human settlements on Mars by 2040—once science fiction—is now a serious consideration. In the realm of science, AI is solving problems humanity has struggled with for decades. A prime example is AlphaFold. For years, understanding the atomic structure of a single protein took enormous time and effort, with only 0.1% of protein structures known. In 2022, Google's AlphaFold revealed the structure of virtually all human proteins, achieving a breakthrough that scientists had waited decades for. These are transformative advancements that inspire hope and ambition.

However, with these advances come significant risks. As was emphasized at the Munich Security Conference this year, we must acknowledge the dual nature of AI—its potential for immense benefit and disruption. AI is not just a civilian tool; it is transforming the military domain as well. Autonomous weapons, such as AI-powered fighter jets, are under active development. In the Russia-Ukraine war, we saw how cyberattacks preceded kinetic conflict. Just two hours before Russia's invasion, Ukrainian satellite systems were disrupted

by a successful cyberattack. This incident underscores a key reality: cyber, AI, and space technologies are deeply interconnected, with profound implications for global security.

AI-driven technologies, including Starlink and other space systems, are expanding rapidly. However, this expansion also creates vulnerabilities. Tests conducted on satellites by organizations like NASA and the Enlight Project revealed that direct cyberattacks on satellites are not only possible but likely. In South Korea, we have faced consistent cyber threats over the past two decades, often from North Korea. Reports from the UN confirm that North Korea has engaged in cyberattacks to fund its nuclear weapons programs, targeting cryptocurrency exchanges and critical infrastructure. The interconnected nature of cyberspace, AI, and space systems means that risks can proliferate globally, affecting everything from financial systems to national security.

While the risks posed by AI and emerging technologies are real, I remain optimistic. History teaches us that humanity has always risen to challenges posed by new technologies. When nuclear fusion was discovered, the world faced both the devastation of the Manhattan Project and the benefits of nuclear energy. Similarly, AI and other emerging technologies are dual-use tools: they bring risks, but also opportunities. We need a balanced approach that fosters global cooperation to manage these risks while maximizing the benefits. Encouragingly, we are already taking steps. South Korea emphasized the importance of safety, innovation, and inclusivity during the Seoul AI Summit this year. At the AI Safety Institute Summit in San Francisco, 10 countries agreed to collaborate on global AI governance and information sharing.

As the challenges in cybersecurity, AI, and space technologies grow, forums like this become ever more significant. Since 2021, the Ministry of Foreign Affairs has hosted this important platform for dialogue, and its relevance continues to increase. I would like to highlight one key point. We cannot afford to respond to AI and emerging technologies with fear or inaction. Instead, we must foster understanding, research, and global consensus to identify risks, share solutions, and seize opportunities. Demis Hassabis, in an interview with the New York Times, expressed hope that AI tools like AlphaFold would lead to medical breakthroughs. At the same time, he warned of the technology's potential misuse—for example, in the creation of bioweapons. This duality requires us to engage in meaningful dialogue—just like the one we are having today. By sharing knowledge and fostering international cooperation, we can ensure that AI and emerging technologies benefit humanity.

As we approach the end of the year, I want to express my gratitude to the Ministry of Foreign Affairs of the Republic of Korea for hosting this invaluable forum. I encourage all participants here to engage in productive discussions that help us navigate the challenges and

opportunities ahead. Christmas is near, so I wish you all a joyful holiday season and a Happy New Year.

AI and Technologies: Anticipating Global Security Challenges

YOUN Jong Kwon, Director General for International Security, Ministry of Foreign Affairs, Republic of Korea and Session Moderator

Brief Introduction

The key question of the session “Quantum and Space: How Can We Boldly Go?" draws inspiration from a famous phrase while posing a central question: How can we leverage critical emerging technologies to enhance, rather than compromise, international peace, security, and stability? Since its inception in 2021, this forum has aimed to explore such pressing challenges.

The discussion focused on three transformative domains: artificial intelligence (AI), quantum technologies, and outer space. AI has become a pivotal enabler across various fields, including military applications, where modern battlefields are increasingly adopting AI-driven systems. As noted by Henry Kissinger, computing power, driven by AI, is becoming the cornerstone of national power. Quantum technologies hold the potential to revolutionize fields like cryptography and remote sensing, with the prospect of quantum-powered AI models on the horizon. Similarly, outer space serves as a critical infrastructure for telecommunications and information systems, yet it is increasingly contested, with disruptions carrying significant terrestrial consequences.

All three domains share a dual-use nature, serving both civilian and military purposes, while simultaneously operating in an increasingly "gray" conflict environment. To navigate the rapid evolution of these technologies responsibly, it is essential to go beyond understanding their risks, adopting agile and forward-thinking solutions to address the complex challenges they present. The forum invited thought leaders to provide insights on and expertise on shaping the responsible redevelopment and adoption of these consequential technologies.

AI and Humanity: Centering the Human Role in Technology's Future

Ariel CONN, Subject Matter Expert (SME) and Consultant, Institute for Defense Analysis (IDA)

"I really appreciate the theme "How Can We Boldly Go?" because I believe the key to answering this question lies not in technology alone, but in us—the humans behind it. While we are here to discuss technology, I want to encourage us to keep our focus on people"

Key Message

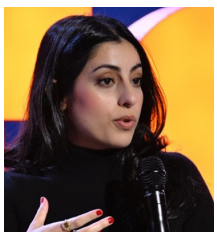
In her remarks Ms. Ariel CONN emphasized the importance of keeping humans at the center of conversations about artificial intelligence (AI). While acknowledging the transformative power of AI, the speaker highlighted that its development, deployment, and impact were entirely shaped by human decisions.

The key message was that AI did not exist in isolation; it is conceptualized, developed, managed, and utilized by humans across its entire life cycle. From idea generation to monitoring its performance, every step involved human accountability and responsibility. However, the speaker noted that discussions often focused on the post-deployment stage, asking alarming questions about AI's role in nuclear weapons or biological warfare, which risked overlooking the significant human activity preceding deployment.
Ariel stressed the need for a human-centric approach, advocating for a framework—like the one developed by IEEE for autonomous weapons systems—that brought decision-makers to the forefront. By addressing human involvement early and throughout the AI timeline, they believed society could better navigate ethical challenges and risks.

The takeaway: AI's challenges and opportunities ultimately depended on human decisions, values, and accountability. By focusing on human responsibility at every stage, the speaker argued that it was possible to shape AI systems that aligned with ethical and societal goals.

Human-Centered AI: Addressing Safety, Security, and Domain-Specific Regulation

Zena ASSAAD, a Senior Lecturer at Australian National University



"AI, at this moment, is everywhere. We see it embedded across almost every industry and domain, and we have witnessed tremendous benefits as a result. These technologies offer enormous opportunities. However, along with those opportunities come significant safety and security implications. Importantly, these implications are not the same across all domains. If we were to implement the same technology in the medical field and in the space sector, for instance, the resulting safety and security risks would look quite different. The Need for Domain-Specific Regulation"

Key Message

Zena Assaad delivered a speech emphasizing the critical role of human involvement across the life cycle of artificial intelligence (AI) systems. She began by agreeing with the broader point that discussions on AI often neglect the essential human element. While AI technologies have become pervasive, appearing in nearly every industry and domain, and delivering tremendous benefits, their implementation also introduces significant safety and security challenges. These challenges, she explained, are not uniform and vary significantly depending on the domain where AI is applied. For example, AI technologies in the medical field and those in the space sector involve vastly different safety and security risks. This variability underscores the need for regulatory frameworks tailored to the specific requirements of each domain.

Assaad argued against the feasibility of a single, overarching AI regulation that could equally address the diverse and complex needs of every industry. She highlighted that each domain has its own unique requirements, benchmarks, and risk thresholds, making a one-size-fits-all approach ineffective. Moreover, the expectations and impacts of AI differ widely depending on the context in which it operates. As a result, the development of domain-specific safety frameworks and regulations becomes essential for addressing the challenges and risks posed by AI. Assaad noted that this domain-specific approach is often overlooked in discussions about AI policy and governance.

She also addressed the ongoing debate over whether AI is even capable of being regulated. Some argue that AI has advanced so rapidly that it is now beyond the control of human governance. Assaad attributed this belief to misunderstandings and misinterpretations of AI's capabilities. Over recent years, rapid advancements in AI technology have been accompanied by exaggerated narratives that have shaped public discourse. These narratives often portray AI

as systems capable of independent decision-making, acting autonomously, or even working against human interests. While such stories are not technically accurate, they have permeated public understanding and shaped expectations about what AI can and cannot do.

Assaad emphasized the importance of managing these public expectations, as they play a crucial role in the success of regulatory efforts. If regulations fail to meet public expectations—whether those expectations are grounded in reality or not—the public response may be overwhelmingly negative, which could hinder the effectiveness of governance measures. She pointed out that part of her work involves clarifying what AI is and is not capable of, while also repositioning humans as central to the conversation about AI governance.

A key theme in her speech was the human role in AI across its entire life cycle. She outlined that every technical system, including AI, follows a life cycle that begins with its conception and moves through stages of design, development, and implementation before eventually being decommissioned. At every stage, humans are the dominant actors, making decisions and shaping the trajectory of these systems. Therefore, regulating AI is not just about overseeing the technology but also about addressing human roles and responsibilities throughout the system's life cycle. It also involves regulating the industries that design, develop, and deploy AI systems.

Assaad also discussed the increasing intersection between technology and national security, noting that the connection between these two domains has never been stronger. She cited Meta’s recent announcement about collaborating with U.S. defense and national security entities to apply their large language models and datasets as a clear example of how technology is now deeply entwined with international security. This intersection, she argued, must be considered when developing safety regulations for AI.

To conclude, Assaad highlighted that AI offers immense potential for innovation across industries, but it also comes with safety and security risks that need to be addressed through domain-specific, human-centered regulations. She reiterated the importance of recognizing human involvement at every stage of AI's life cycle and ensuring that governance frameworks reflect both the technical realities of AI and public expectations. By focusing on these principles, she believed society could navigate the opportunities and challenges presented by AI in a responsible and effective way.

Embracing Uncertainty: Equity and Justice in AI Decision-Making

**Kyunghyun CHO, Professor of Computer Science and Data Science,
New York University (NYU)**

'The inherent uncertainty in technology, whether we are talking about artificial intelligence, quantum computing, or any other emerging technology, there is an inherent uncertainty that we simply cannot eliminate"

Key message

Prof. Kyunghyun Cho delivered remarks on the critical concept of uncertainty in emerging technologies. He took the opportunity to reflect on the inherent uncertainty that underlies artificial intelligence (AI), quantum computing, and other advanced technologies.

Cho highlighted that despite advances in data, algorithms, and computational power, uncertainty is a persistent and unavoidable aspect of these systems. This uncertainty cannot be systematically or algorithmically resolved, and it carries significant implications for the deployment and decision-making processes of AI systems. When these systems are deployed, they must resolve uncertainty in some manner, often doing so in ways that appear arbitrary or opaque.

To illustrate this point, Cho used the example of large language models like ChatGPT. He noted that these models provide answers to questions even when the full context is unobservable or unknown, which is a major source of uncertainty. While humans might use context, judgment, and experience to make decisions, AI systems resolve uncertainty in ways that are often unintelligible to us, even though we design and deploy them. This creates a fundamental disconnect, as humans rely on considerations of societal impact and consequences, while AI systems' resolutions may lack this depth of understanding.

Cho emphasized the importance of addressing this disconnect, pointing out that the resolution of uncertainty matters greatly. Human decision-making, although not always explicit in its rationale, is driven by an understanding of societal consequences and the potential impacts of choices on people and communities. In contrast, AI decision-making is typically guided by algorithms that lack this human nuance and societal perspective.

He also touched upon the commonly proposed solution of putting "humans in the loop"

or establishing safety frameworks to govern AI decision-making. While these are valuable measures, Cho argued that they often overlook a crucial question: who are the humans in the loop? He noted that the individuals involved in building these technologies, designing frameworks, and establishing rules are rarely the ones directly impacted by the systems' decisions. This exclusion of stakeholders most affected by AI decisions creates a fundamental issue of equity and justice.

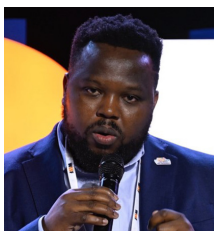
Cho urged the audience to reflect on the question of "who" in discussions about AI and emerging technologies. He stressed the importance of identifying the individuals and communities who will bear the consequences of these technologies and ensuring that their voices are included in the decision-making process. He argued that addressing this question is vital for creating systems and frameworks that resolve uncertainty in ways that are equitable and beneficial for all, not just for those in positions of power.

Cho concluded by reiterating the unavoidable nature of uncertainty in AI and other technologies. He emphasized that how uncertainty is resolved—whether through human decision-making or automated systems—has profound implications for society. He warned against concentrating power and decision-making in the hands of a small group, as this risks exacerbating inequities and excluding those most affected by technological decisions. Instead, he called for frameworks that prioritize societal benefit and inclusivity, ensuring that the power of emerging technologies serves everyone, not just a privileged few.

In his closing remarks, Cho shared his concern about the risk of centralized decision-making and power in the development and deployment of AI. He hoped that the discussions at the forum would address these issues and explore ways to ensure that technologies like AI are developed and governed in ways that prioritize societal equity and justice.

AI and Global Security: Human Control, Equity, and Decolonizing the Balance of Power

Thompson CHENGETA, Professor of International Law and AI Technologies, School of Law, Liverpool John Moores University



Key message

Prof. Thompson focused his discussion on the intersection of artificial intelligence (AI) technologies with weapons of mass destruction, including chemical, biological, and nuclear weapons. His remarks highlighted on four key areas: the relevance of existing international laws, the principle of human control over AI, the impact of AI on smaller weapons in the Global South, and the need for a decolonial perspective on global security.

Existing Prohibitions Under International Law

Prof. Thompson emphasized that international laws, such as the Chemical Weapons Convention and the Biological Weapons Convention, already prohibit the use of certain weapons. These existing frameworks provide a legal and ethical foundation for addressing the emerging risks posed by the integration of AI technologies into such weapons. Recognizing these prohibitions helps anchor discussions about AI within established legal norms, reminding stakeholders that the international community is not starting from scratch in regulating these technologies.

AI's Impact on the Principle of Human Control

The principle of human control over decisions to use force has been vital in preventing catastrophic outcomes, particularly with weapons of mass destruction. Thompson highlighted that this restraint, maintained by the direct involvement of humans, has played a critical role in averting global-scale disasters. However, the integration of AI technologies threatens to undermine this principle, enabling the deployment of such weapons without meaningful human oversight. To address this existential risk, the Thompson advocated for codifying the principle of human control over AI as a non-negotiable norm in international law, particularly when AI intersects with nuclear, chemical, and biological weapons.

AI's Impact on Small and Light Weapons in the Global South

The focus then shifted to smaller and lighter weapons, which disproportionately affect communities in the Global South. While much attention is given to major military capabilities like nuclear or biological weapons, the speaker argued that the proliferation of small arms also warrants urgent attention. AI technologies have the potential to accelerate the production and spread of such weapons, exacerbating insecurity in already vulnerable regions. The

2024 UN Secretary-General's Advisory Board on Disarmament Matters has highlighted this concern, stressing that weaponization, whether on Earth or in outer space, creates security infrastructures that disproportionately harm struggling populations. The speaker called for greater attention to these dynamics in discussions about global AI governance.

A Decolonial Perspective on Global Security

The final point focused on adopting a decolonial perspective in global security discussions. The speaker critiqued the "balance of power" narrative, arguing that it often reinforces the dominance of certain states while marginalizing others. Using Africa as a case study, the speaker pointed to the continent's abundance of minerals critical to developing AI and quantum technologies. While these resources drive technological advancements globally, their extraction has fueled conflict and exploitation, leaving African voices largely excluded from global security dialogues. This raises important questions about Africa's role in the global security infrastructure and the marginalization of communities that bear the brunt of resource-related conflicts while others reap the benefits of technological progress.

Prof. Thompson concluded by emphasizing the importance of building upon existing international laws to regulate AI's convergence with prohibited weapons. Codifying the principle of human control over AI, addressing the disproportionate impact of AI-accelerated small weapons in the Global South, and adopting a decolonial perspective were identified as key steps toward creating a more just and inclusive global security framework. The speaker urged stakeholders to ensure that these frameworks truly reflect the needs of all people, not just the powerful few. His remarks ended with a call for equity, justice, and inclusivity in navigating the complex challenges posed by AI in global security.

The New Space Era: Innovations, Connectivity, and Transforming Global Challenges

Jongjin KIM, Senior Vice President, Hanwha Systems

Key message:

Mr. Jongjin Kim highlighted the privilege of witnessing the transformative advancements occurring in the space industry. His remarks centered on the unprecedented innovations in the "New Space Era" while briefly acknowledging the challenges and threats associated with this period of rapid development.

AI, Quantum Technology, and Space: A Transformative Era

Mr. Kim highlighted the convergence of artificial intelligence (AI), quantum technologies, and space exploration as some of the most transformative areas of research today. These fields have garnered significant global attention and investment, sparking optimism and controversy. The space industry, in particular, is experiencing rapid innovation, shifting from its traditional model to a more commercially viable one driven by private companies.

Reusable Launch Systems: A Game-Changer

One of the most groundbreaking achievements in the New Space Era is the development of reusable launch systems. Companies like SpaceX have pioneered this innovation, drastically reducing the cost of launching payloads into space and enabling commercial sustainability for the industry. The speaker also highlighted emerging companies like SpinLaunch, which has developed an electric-powered rotating arm to launch payloads into Low Earth Orbit (LEO). Such novel ideas are attracting investment and fostering healthy competition, pushing the boundaries of innovation.

Satellite Connectivity: Revolutionizing Communication

Mr. Kim described the rapid expansion of the LEO satellite industry, which is revolutionizing global communication. SpaceX's Starlink has launched over 7,000 satellites, bringing internet connectivity to underserved areas and playing a critical role in strategic situations, such as providing communication infrastructure during the conflict in Ukraine. Other players in the industry include Amazon's Project Kuiper, aiming to launch a constellation of 30,000 satellites, and OneWeb, which operates over 600 satellites for government and business services.

The speaker also highlighted AST Space Mobile's innovative approach to direct-to-mobile communication from space. AST successfully demonstrated its technology by connecting a Samsung Galaxy S22 directly to a test satellite, achieving download speeds of 10 Mbps. This breakthrough, in partnership with T-Mobile, has the potential to transform global mobile connectivity by eliminating the need for intermediary ground infrastructure.

Emerging Applications of Satellites

Satellites are also being used for Earth observation to tackle global challenges like climate change. By monitoring greenhouse gas emissions and environmental changes, satellites offer valuable tools to support global efforts in combating climate change and achieving sustainable development goals. This represents another promising application of satellite technology beyond communication.

Mr. Kim concluded by emphasizing the ongoing transformation of the space industry, driven

by innovative ideas, significant investment, and intense competition. Reusable launch systems, LEO satellite networks, and advancements in direct mobile communications exemplify the industry's potential to reshape global connectivity and address pressing challenges. While the speech primarily focused on these advancements, the speaker expressed a willingness to discuss the associated challenges and risks during the event's broader discussions.

2.1. Emerging Questions and Expert Insights on Emerging Questions

Dan Smith

Dan revisited key points about the intersection of military domains and emerging technologies, emphasizing the importance of addressing a "tech-domain interface" in arms control. Instead of aiming for a general regulatory framework for all security-related technologies, the speaker advocated for domain-specific approaches targeting areas such as AI deployment in nuclear weapons systems, outer space, maritime operations, and other strategic domains. Two examples—ballistic missiles and small arms—illustrated these complexities.

Ballistic Missiles and Submarine-Based Weapons

Submarine-based ballistic missiles have traditionally been viewed as the ultimate "weapon of last resort," offering a strategic deterrent due to their ability to remain hidden in the depths of the ocean for extended periods. This deterrent effect has shaped arms control policies and the development of strategic forces for decades. For instance, China's focus on building a submarine-based ballistic missile force reflects this logic.

However, emerging technologies, such as quantum sensing, and broader challenges like climate change, threaten to erode this deterrence. If submarines become more detectable, their invulnerability as a last-resort deterrent diminishes, raising critical questions about the future of these systems. The speaker posed two key questions:

- Can these vulnerabilities be countered with technological solutions?
- Is it possible to intervene early in the technology life cycle to prevent these challenges?

The speaker expressed scepticism about pre-emptive measures, deeming them unrealistic. Instead, they argued for greater dialogue and transparency among major powers and with the global community. Transforming the way security issues are discussed—fostering openness and cooperation—was identified as essential. However, the speaker acknowledged that arms development competition would persist, underscoring the importance of ensuring such competition stays within safe boundaries.

Small Arms, Light Weapons, and Emerging Technologies

On the other end of the spectrum, emerging technologies could offer transformative solutions to the proliferation of small arms and light weapons. AI-driven monitoring systems, for instance, could make arms trafficking riskier and more challenging, aligning with initiatives such as the African Union's "silencing the guns" campaign for peace and stability on the continent.

Quantum sensing technologies were also highlighted as potentially revolutionary for ceasefire monitoring. These advanced systems could detect and report military actions, such as the firing of an artillery shell, almost instantaneously. This capability would enable quicker responses, improved compliance with ceasefire agreements, and greater accountability, fostering trust and stability.

Dan concluded by emphasizing the dual nature of emerging technologies. On one hand, they challenge traditional security assumptions, as seen with submarine-based weapons. On the other hand, they provide unprecedented opportunities to address longstanding issues, such as arms trafficking and ceasefire enforcement. The key challenge lies in harnessing these technologies responsibly, balancing security needs with transparency and cooperation. By fostering dialogue and managing competition effectively, the speaker argued that it is possible to navigate these complexities and build a safer, more stable future.

Ariel Conn

Could you offer your perspective on the current state of international and domestic policies in this area? Specifically, how can we ensure appropriate human involvement in the development and deployment of these technologies?

Additionally, are there any proposals you'd like to make or particular points you'd like to emphasize that go beyond what you shared in your opening remarks?

Ariel Conn highlighted the importance of improving regulatory frameworks for AI by addressing key issues. First, she emphasized focusing on the entire lifecycle of AI technologies, advocating for early-stage interventions to ensure accountability and responsibility. She referenced IEEE's work on norms and standards for documenting accountability, which she believes should be adopted more widely, along with verification and validation standards.

Second, Conn stressed the need to shift the discourse from hypothetical, large-scale existential risks to immediate, tangible challenges posed by AI technologies. Third, she called for greater inclusion of perspectives from those directly impacted by AI in regulatory processes, ensuring risk-based approaches are effective and inclusive.

Echoing Zena's point, Conn advocated for domain-specific regulations tailored to the unique challenges of sectors like healthcare and the military. Finally, she urged stakeholders to avoid treating AI as a single entity and to instead regulate its distinct technologies and applications in context-specific ways.

Zena Assaad

Delving deeper into the issue of AI safety and AI security. To draw a parallel from the nuclear field: in that context, nuclear safety involves ensuring the safe operation of facilities to protect humans from harm caused by the technology, while nuclear security focuses on protecting the facilities and technology from humans with malicious intent. The distinction there is quite clear.

When it comes to AI, however, the lines between safety and security appear much more blurred. For instance, the process of training AI systems exists within the digital and cyber realms, where vulnerabilities in security can directly impact safety. Without robust AI security, ensuring AI safety becomes almost impossible. This inherent interdependence makes it challenging to separate these two concepts.

Do you have any specific views on how we can effectively address both AI safety and security simultaneously? How can we navigate the overlap while ensuring clarity in our discussions and policies?

Zena Assaad highlighted the distinction between safety and security in AI, noting their overlap but emphasizing their differences. Security involves protecting a system's technical vulnerabilities from compromise or misuse, while safety focuses on minimizing harm to humans or the environment. These concepts often come into tension, especially in military

applications, where securing systems to neutralize threats can cause harm to others.

She raised concerns about transparency in AI training data, referencing Meta's partnership with U.S. defense agencies. This collaboration demonstrates how the coupling of the tech and defense industries blurs lines between end-user safety and security, potentially exposing users to privacy risks or data misuse.

Assaad called for regulation that reduces harm not only for those deploying AI but also for end users, incorporating the entire AI lifecycle. She emphasized the need for transparent, inclusive frameworks to balance safety and security, ensuring neither is compromised.

Prof. Kyunghyun Cho

Let's suppose you were advising a national leader on AI policy and governance. What would be the first priorities you would emphasize in your guidance?

Additionally, if you were tasked with training junior officers or staff under your guidance, where would you begin? What foundational knowledge or principles would you prioritize in their education? The floor is yours.

Prof. Kyunghyun Cho reflected on the evolution of AI technologies, noting that foundational work, like his research on the attention mechanism in 2014, laid the groundwork for current tools like ChatGPT. He highlighted a key issue: a decade-long lag between innovation and realization of its broader applications, emphasizing that new advancements will soon surpass today's technologies.

Cho advised policymakers to adopt a long-term perspective, focusing on the next wave of innovations rather than solely regulating existing technologies. He stressed the need for governments to prioritize funding for frontier research rather than areas already dominated by the private sector. Such investment ensures a robust pool of experts capable of shaping future technologies.

In training junior staff, Cho emphasized critical thinking, understanding innovation lifecycles, and ethical considerations over immediate tool familiarity. He concluded by urging governments to invest in foundational research to maintain leadership in the ever-evolving technological landscape.

Prof. Thompson

Just a few weeks ago, the United Nations First Committee adopted its first-ever resolution on the use of AI in the military domain and its implications for international peace and security. You may already be familiar with this development, and we're expecting the UN Secretary-General to publish a substantive report on this topic by next year.

As an expert in this field, what are your expectations for these efforts? What do you think would be the best way forward for ensuring the responsible use of AI in the military domain, particularly once this report is published? The floor is yours.

Prof. Thompson Chengeta highlighted the significance of the recent UN First Committee resolution on AI in the military domain, noting its overwhelming support with 166 votes in favour and its grounding in international law. This foundation, particularly emphasizing international human rights law, is seen as critical for developing robust policy frameworks.

Two key reasons were provided for grounding discussions in international law:

- Preventing Dilution of Protections: The speaker cautioned against new terminologies, like "mitigating bias," that could dilute existing legal protections, such as the obligation to eliminate discrimination under human rights law.
- Identifying Gaps Without Undermining Norms: Using international law as a starting point ensures existing norms are upheld while addressing gaps posed by emerging technologies.

Looking forward, Thompson expressed hope for a legally binding agreement by 2026 and anticipates the UN Secretary-General's report to build on the resolution by providing concrete guidance for states to create accountable policies for AI in military applications.

Mr. Jongjin Kim

From a business perspective, what do you see as the key areas for collaboration between the space industry, AI, and quantum technologies?

I know you've already touched on some of these points, but if you could, please also highlight the risks associated with such collaborations. Could you wrap that up in about two minutes?

Mr. Kim focused on quantum technologies, emphasizing their division into two areas: quantum computing and quantum communication.

Quantum Computing promises immense computational capabilities but raises concerns about encryption vulnerabilities, which could affect industries like space. As quantum computers advance, encryption methods currently in use may become obsolete.

Quantum Communication, on the other hand, offers a potential solution through unbreakable encryption based on quantum principles. In 2016, Chinese researchers successfully demonstrated quantum communication via a low Earth orbit (LEO) satellite, highlighting its feasibility. However, making this technology practical and scalable remains a challenge, with researchers actively working to overcome technical barriers.

Mr. Kim ended by expressing optimism about the collaboration between the space industry and quantum technology, believing that ongoing efforts will resolve these challenges and lead to impactful advancements in the near future.

Zena Assaad

We are now living not only in the physical world but also in the cyber world, and yet we are increasingly aware of the uncertainties that exist in cyberspace. While we have well-established norms and regulations in the physical world, it seems that regulations in cyberspace are still lacking or unclear, particularly for those of us who are not experts in this area.

I was reassured by the congratulatory remarks earlier, as well as by the mention of the recent United Nations resolution, which was adopted by an overwhelming majority of states. While that resolution addressed AI in the military domain, I wonder if there are broader discussions underway about the regulation of cyberspace. Considering the diverse areas it encompasses, are there efforts to establish norms or regulations for cyberspace in general?

Zena Assaad

It's important to recognize that there are already regulations around cybersecurity, but these are typically domain specific. For instance, there are cybersecurity regulations tailored to the military domain, as well as others designed for civil domains.

That said, cybersecurity concerns are not new—they predate the current wave of AI innovation. Many of the measures we have today were developed and implemented well before the advent of AI as a dominant technology. However, what we're facing now are unique cybersecurity challenges posed by AI-enabled systems, which weren't a significant consideration when earlier frameworks were established.

The task before us is to augment existing regulations to address these new challenges. AI brings with it distinct safety concerns, such as vulnerabilities in data integrity, the potential for malicious use, and the difficulty of predicting or controlling system behaviours. These factors will require us to rethink and expand our cybersecurity measures to ensure they remain relevant and effective in this new landscape.

Dan Smith

Mr. Dan further addressed ongoing discussions at the United Nations regarding global cybersecurity measures, highlighting the challenge of reconciling diverging proposals.

Two primary sets of proposals dominate the conversation:

- Proposals from Russia and China, which offer valuable ideas and merit consideration.
- Proposals from the U.S., U.K., France, Germany, and Japan, which are also well-crafted with significant strengths.

However, these two approaches lack full alignment, and geopolitical tensions complicate efforts to bridge the gap. Despite this divide, the speaker emphasized that extensive thought and negotiation are ongoing at the UN and in other forums. Cybersecurity remains a critical area of discussion, and efforts to find common ground persist amid the challenging international climate.

AI-WMD Nexus: Risks and Responses

Winfred WAN, WMD Programme Director and Senior Researcher, Stockholm International Peace Research Institute (SIPRI) and Session Moderator

Brief Introduction

This session examined the transformative role of AI in the realm of weapons of mass destruction (WMD), focusing on its potential to influence critical aspects such as development, acquisition, transfer, and use. Additionally, we will explore how advancements in AI are reshaping how states and other stakeholders perceive and address these weapons.

With an esteemed panel of experts joining, the panel delved directly into the discussion. To set the stage, our first round of questions focused on understanding the risks associated with AI's integration into WMD-related domains.

Emerging Technologies and the Strategic Effect: Rethinking Deterrence and Impact

James Andrew LEWIS, Senior Vice President, Center for Strategic & International Studies (CSIS)

Key message:

James emphasized three key points to frame the discussion on emerging technologies:

1. Technology is Not Determinative: Using a thought experiment, he illustrated that technological superiority does not always guarantee victory in war. Historical and recent conflicts reveal that wars are shaped by factors beyond technological advantage.
2. Circumventing Classic Deterrence and Arms Control: Emerging technologies like space systems, quantum computing, cyber capabilities, and electronic warfare enable states to achieve strategic effects without nuclear weapons. This creates opportunities to bypass traditional deterrence and arms control mechanisms, reinforcing the need for negotiation to address these new dynamics.
3. Defining Strategic Effect: Strategic effect involves advancing national interests, coercing opponents, or inflicting economic or military damage. When assessing technologies like AI or cyber tools, the critical question is whether they can deliver a

strategic effect on the battlefield today. If not, they lack true strategic impact.

He concluded by encouraging clear thinking about the strategic implications of these technologies.

AI and Nuclear Deterrence: Amplifying Risks, Balancing Stability, and Ensuring Accountability

Nobumasa AKIYAMA, Professor, Hitotsubashi University / Director, Center for Disarmament, Science and Technology, Japan Institute of International Affairs (JIIA)

As someone coming from a non-nuclear weapon state and with a background in arms control, I initially questioned whether I was the right person to discuss the relationship between artificial intelligence (AI) and nuclear deterrence. However, instead of providing definitive thoughts, I would like to share some questions that I believe are central to this intersection of AI and nuclear weapons.

Key message:

Prof. Nobumasa, coming from a non-nuclear weapon state with a background in arms control, explored the complex relationship between artificial intelligence (AI) and nuclear deterrence by posing key questions rather than providing definitive answers.

Is AI a Game-Changer or an Amplifier?

The speaker questioned whether AI fundamentally changes nuclear deterrence or simply amplifies existing challenges. They argued that AI acts more as an amplifier, magnifying pre-existing issues rather than introducing entirely new dynamics. For instance, during the Ukraine conflict, Russia manipulated escalation dynamics, a deliberate exploitation of nuclear stability unrelated to AI. This raised the question of whether AI could truly reduce nuclear risks. The speaker expressed scepticism, given the ongoing dynamics of nuclear deterrence and competition, doubting AI's ability to meaningfully lower these risks.

AI's Impact on Nuclear Operations and Stability

AI's potential to influence nuclear deterrence lies in improving operational capabilities, such as enhancing intelligence, surveillance, and reconnaissance (ISR) systems and accelerating decision-making processes. These capabilities could theoretically strengthen stability or give a state perceived superiority over its adversaries. However, the simultaneous development of

such technologies by multiple states could lead to mutual suspicion. For example, a "use it or lose it" scenario might arise if one side perceives the other's AI-enhanced decision-making as a destabilizing threat. This raises critical questions about how AI will affect the delicate balance of power in nuclear stability and whether arms control frameworks can reconcile the conflicting goals of maintaining stability while pursuing superiority.

The Concept of "Human in the Loop"

Prof. Nobumasa highlighted the often discussed but poorly defined idea of keeping "humans in the loop" in AI decision-making, particularly concerning nuclear weapons. They rephrased the issue to focus on responsibility: who bears the consequences of AI use in the nuclear context? Unlike conventional weapons, the catastrophic consequences of nuclear use make accountability far more pressing. The ultimate responsibility lies with state leaders. However, the speaker questioned whether leaders, especially those lacking technological understanding, could truly grasp the consequences of deploying AI in weapons of mass destruction (WMD). Ensuring informed decision-making by state leaders is a significant challenge.

Key Questions for Consideration

Prof. Nobumasa concluded his remarks by outlining four critical questions:

1. Is AI amplifying existing nuclear challenges, or is it a game-changer?
2. How does AI affect the balance between stability and superiority in nuclear deterrence?
3. What does "human in the loop" mean in practice, and who is responsible for the consequences?
4. How can we ensure state leaders are equipped to make informed decisions regarding AI and WMD?

While these questions are difficult to answer, they are essential for understanding and navigating the intersection of AI and nuclear stability. He emphasized the need to address these issues to ensure that AI's role in the nuclear domain does not compromise global security.

AI and Nuclear Weapons: Navigating Risks in a Time-Compressed and Vulnerable System

Laura GREGO, Senior Scientist and Research Director, Union of Concerned Scientists

Laura Grego, highlighted the intersection of artificial intelligence (AI) and nuclear weapons, focusing on how AI and emerging technologies could impact nuclear risks. She emphasized three

key concerns: miscalculation or inadvertent escalation, time-compressed decision-making pressures, and the challenge of halting nuclear escalation once it begins. Her remarks explored two interconnected aspects: the speed of decision-making and the vulnerability of strategic systems.

Speed of Decision-Making

Grego underscored the risks posed by time-compressed decisions under nuclear postures like "launch on warning" or "launch under attack," maintained by the U.S., Russia, and possibly considered by China. These postures require leaders to make civilization-altering decisions within minutes, often based on incomplete or incorrect information.

AI is being explored to improve intelligence, surveillance, and reconnaissance (ISR), early warning systems, and command processes. While AI could theoretically process complex data faster to assist decision-makers, Grego questioned whether AI could truly improve decision-making under extreme pressure. Historical near misses in nuclear history were caused by human mistakes and technical failures. Adding AI systems, which bring their own biases and limitations, risks compounding these dangers. Moreover, the belief that AI can make nuclear decision-making "safe" and "reliable" may encourage states to rely more on risky postures.

She further noted that new technologies like cyber weapons, anti-satellite systems, and hypersonic delivery systems could compress decision times even further, increasing the temptation to integrate AI into nuclear decision-making processes. While the U.S. and China recently agreed to keep humans in the loop for nuclear decisions, Grego emphasized that this addresses only a small part of a broader issue.

Vulnerability of Strategic Systems

Grego explained how policies like "launch on warning" arise from perceived vulnerabilities of land-based missiles, command systems, and other strategic assets. She raised a critical question: will AI and machine learning increase actual or perceived vulnerabilities of these systems? Perceptions of increased vulnerability, even if technically untrue, could pressure states to adopt riskier postures.

For example, AI-enhanced cyberattacks might target nuclear command and control systems, or AI could improve tracking of ballistic missile submarines, undermining their second-strike survivability. Such developments could drive states toward "use it or lose it" postures, escalating nuclear risks.

Key Reflections

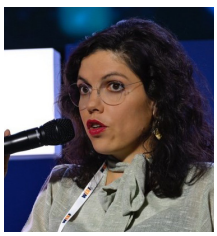
Grego concluded with broader reflections:

- Incorporation of New Technologies: Careful consideration is needed regarding how and when AI and emerging technologies should be integrated into nuclear systems to avoid exacerbating risks.
- Disarmament Obligations: Focusing on improving nuclear systems may lead to complacency, overshadowing obligations to reduce and eliminate these weapons.
- Arms Control: It is essential to explore how AI and emerging technologies can be addressed in future arms control agreements.

Grego urged a holistic and cautious approach to integrating AI into nuclear systems, emphasizing the importance of thoughtful and responsible actions to avoid exacerbating risks in an already fragile nuclear landscape.

Redefining Weapons of Mass Destruction: The Role of AI and Drone Swarms in Modern Warfare

Jimena VIVEROS, Managing Director and CEO, IQuilibriumAI



Jimena Viveros discussed the evolving definition of weapons of mass destruction (WMDs) in the context of AI and emerging technologies. She began by highlighting the lack of a universally clear definition of WMDs, despite efforts like the 1977 UN General Assembly Resolution and the UN Office for Disarmament Affairs (UNODA) guidance. These frameworks broadly classify nuclear, chemical, and biological weapons as WMDs, with potential inclusion of future weapons capable of comparable destruction. Judicial insights, such as those from the International Court of Justice, further define WMDs as inherently indiscriminate and incompatible with international humanitarian law (IHL).

Viveros emphasized the increasing relevance of drone swarms, an AI-related technology, as potential WMDs. Drone swarms are autonomous systems capable of coordinated, large-scale operations, acting as a single weapon system. She cited China's 2018 demonstration of a 1,374-drone swarm, where technical errors caused deviations in one-third of the drones, underscoring the risks of unintended consequences.

Labelling drone swarms as WMDs is critical, according to Viveros, as this designation carries a stigma that encourages deterrence and non-proliferation, aligning with the 2004

UN resolution on preventing WMD proliferation. She concluded by urging the need for AI governance frameworks to acknowledge the dual-use nature of AI technologies and consider innovations like drone swarms as meeting WMD thresholds.

Viveros called for careful deliberation in addressing these challenges to ensure responsible governance of AI-enabled systems.

AI in Military Strategy: Adoption, Challenges, and International Cooperation

Ylli BAJRAKTARI, President and CEO, Special Competitive Studies Project (SCSP)

Mr. Ylli Bajraktari, provided insights into the military adoption of AI, addressing why and how militaries are leveraging AI and the pace of its adoption. He categorized the benefits of AI in the military into four areas:

- Back-office responsibilities: AI enhances administrative processes, cyber defense, and logistics, offering low-risk, cost-effective solutions.
- Indications and warnings (IW): AI improves early detection systems for disasters and risks, enhancing preparedness for both military and civilian scenarios.
- Decision-making: AI provides better analysis and options, supporting human decision-makers with clearer risk and opportunity assessments.
- AI-enabled weapons systems: This contentious category raises critical questions about testing, evaluation, and deployment frameworks, emphasizing the need for modernized acquisition processes and international legal frameworks.

Bajraktari stressed the importance of addressing the challenges posed by AI's development primarily in the private sector. He called for stronger public-private partnerships to ensure accountability and transparency, especially as adversaries like China and Russia operate under different norms.

He concluded by emphasizing the need to:

- Tackle infrastructure challenges such as data centers and energy demands.
- Strengthen international cooperation to ensure AI systems are developed responsibly while countering adversarial misuse.

Defending Cyberspace: Understanding The Evolution of Cyber Threats

Sohyun SHIN, Research Fellow, Asan Institute for Policy Studies and Session Moderator

Brief Introduction

As nations progressed further into the digital age, cyber threats became increasingly pervasive and sophisticated. South Korea, like many other countries, faced cyber threats across various sectors and from diverse actors. Notably, North Korea consistently conducted cyberattacks targeting government agencies, the military, defense industries, and the private sector. These attacks often involved information theft, system disruption, and even the paralysis of critical systems.

In recent years, North Korea shifted its focus toward economic gains, engaging in activities such as stealing cryptocurrencies and infiltrating cryptocurrency exchanges. Beyond these acts, foreign information manipulation and interference in cyberspace by both state and non-state actors emerged as significant threats, jeopardizing democracy and the integrity of public discourse.

The breadth and complexity of threats in today's hyperconnected cyberspace posed considerable challenges. To address this, the session focused on key objectives:

1. Examining the evolving global cyber threat landscape.
2. Sharing regional and organizational approaches, strategies, policies, and legal frameworks for countering these challenges.
3. Fostering mutual understanding of global cybersecurity issues.
4. Exploring ways to strengthen capacities for effective responses to cyber threats.

Additionally, the session sought to deliberate on establishing accountability for cyber threats and breaches, fostering collaboration for enhanced cybersecurity.

Bridging the Gap: Addressing Evolving Threats Through Inclusive Communication and Strategic Intelligence

Neil J. WALSH Executive Secretary - Globe Anti-Corruption Network, UN Office on Drugs and Crime (UNODC) / Chief, Law Enforcement and Strategic Networks

Neil J. Walsh emphasized the interconnected nature of modern threats, cautioning against oversimplification and overly securitizing

issues like cybercrime. He highlighted how events such as the COVID-19 pandemic exposed vulnerabilities, leading to increased online sexual exploitation, fraud, and financial crime, which intersect with broader security and national challenges.

To effectively address these evolving threats, Walsh called for comprehensive strategic threat intelligence at national, regional, and global levels. However, he stressed the critical importance of effective communication. Risks must be explained in clear, relatable terms that resonate with ordinary people. The messaging should also be culturally nuanced, gender-inclusive, and age-sensitive.

Using the example of online sexual extortion, Walsh noted a demographic shift toward older adults as targets, who often lack mechanisms to seek help. He concluded by underscoring that treaties, legislation, and policies are only effective if understood and applied by the public, highlighting the need for inclusive and practical communication strategies.

Cybersecurity in a Geopolitical Era: Protecting Societies Amid Evolving Statecraft

Manon LE BLANC, Coordinator for Cyber Issues, European External Action Service (EEAS)

Manon Le Blanc, Coordinator for Cyber Issues at the European External Action Service (EEAS), highlighted the evolving role of state actors in the cyber threat landscape, emphasizing its intersection with geopolitics and societal vulnerabilities. She noted that the COVID-19 pandemic accelerated global digital connectivity, expanding the attack surface and exacerbating security vulnerabilities.

Le Blanc discussed the escalating sophistication of cyber threats, which now target critical infrastructure, disrupt access to essential resources like water and energy, and compromise systems like GPS. Ransomware attacks have intensified, affecting vital services such as hospitals, while cyber tools increasingly play a strategic role in military conflicts.

State actors now integrate cyber tools into broader statecraft strategies, using them alongside tactics like foreign interference, information manipulation, and sabotage to exploit societal vulnerabilities. This approach has made cyber threats deeply interconnected with geopolitical dynamics, destabilizing societal functions.

The Evolving Cyber Threat Landscape: Implications for Security, Democracy, and Human Rights

Alison PYTLAK, Senior Fellow and Cyber Program Director at the Stimson Center

Ms. Alison Pytlak highlighted the multidimensional nature of the evolving cyber threat landscape and its implications for international peace and security. Drawing from her involvement in the UN's Open-Ended Working Group on cybersecurity, she outlined key areas of concern:

- Cyber Operations in Armed Conflicts: Cyber activities, as extensions of political and military strategies, pose significant risks to civilians, infrastructure, and humanitarian efforts, as seen in Ukraine and Gaza. These operations increase the risk of escalation in volatile conflicts.
- Hybrid Warfare and Coercion: Cyber tools are used below the threshold of armed conflict for coercive tactics, raising questions about governance and the responsible use of offensive cyber capabilities.
- Critical Infrastructure Attacks: Increasingly digitized critical systems like power grids and hospitals are vulnerable, with disruptions threatening public safety, societal stability, and confidence in essential services.
- Foreign Influence and Information Operations: Cyber-enabled influence operations jeopardize elections, democratic processes, and public trust, particularly in a critical election year like 2024.
- Human Rights and Freedoms: The misuse of ICTs disproportionately affects marginalized communities, with surveillance and intrusion technologies eroding privacy and fundamental rights in cyberspace.

Pytlak emphasized the interconnectedness of these threats with broader geopolitical dynamics and the need for evolving international governance to foster stability, accountability, and human rights protection in cyberspace.

Cybersecurity in the MENA Region: Addressing Threats to Critical Infrastructure and Regional Stability

Irene CORPUZ Strategic Steering Committee (SSC) Member, Global Forum for Cyber Expertise (GFCE)

Irene Corpuz highlighted the unique cyber risks in the MENA re-

gion, shaped by geopolitical tensions, economic instability, and rapid technological advancements. She outlined key threats and their implications:

- Targeting Critical Infrastructure: The oil, gas, and energy sectors are prime targets for state-sponsored cyberattacks like ransomware and supply chain compromises. These deliberate attacks aim to destabilize economies and erode public trust.
- Role of social media: Social media platforms are weaponized for disinformation during political unrest. Activist groups, such as Anonymous, use cyberattacks like DDoS to manipulate public opinion and disrupt services.
- Geopolitical Implications: Cyber threats transcend borders, with rival nations engaging in espionage and offensive cyber operations that exacerbate regional instability.
- Impact on Critical Infrastructure: Notable attacks, like the Shamoon incident on Saudi Aramco, illustrate the evolving and persistent nature of threats targeting key industries.
- Emerging Technologies: AI and quantum computing present opportunities for defense but also introduce new vulnerabilities, enabling sophisticated cyberattacks.

Corpuz proposed a three-pillar approach to address these threats:
I. Capacity Building: Enhance workforce cybersecurity skills.
II. Policy Implementation: Establish robust regulatory frameworks.
III. Capable Resources: Invest in advanced tools and skilled professionals.

She stressed the need for a holistic approach to safeguard critical infrastructure and build resilience in the region.

Emerging key questions

Allison Pytlak

What strategies are being implemented, what might still be needed, and how effective these efforts are. You may answer from a regional perspective, such as the EU, or from a sectoral focus, like cybercrime or UN-led responses.

Allison Pytlak emphasized that despite various responses at national, regional, multilateral, and local levels to counter cyber threats, current measures remain insufficient. The evolving cyber threat landscape, characterized by new actors, enhanced capabilities, and severe impacts, necessitates stronger actions.

At the multilateral level, the UN Framework for Responsible State Behaviour in the Use of ICTs provides a foundational baseline. Established in 2015, it includes key agreements such as the application of international law to state conduct in cyberspace and 11 voluntary norms guiding responsible state behavior. However, the framework struggles to deter state-sponsored cyberattacks effectively, contributing to a growing accountability gap.

Complementary initiatives aim to address these challenges, including:

- Cyber sanctions to penalize malicious actors.
- Targeted coalitions like the Pall Mall Process (regulating cyber intrusion technologies) and the International Counter Ransomware Initiative (tackling ransomware).

Pytlak advocated for a shift toward positive accountability mechanisms, focusing on incentivizing compliance and fostering collaborative resilience. Instead of solely punishing bad behaviour, states and organizations should be rewarded for implementing cyber resilience measures and adhering to norms. She concluded that rethinking deterrence, emphasizing shared responsibilities, and integrating positive incentives are essential to building a safer, more resilient cyberspace.

Manon

I know you have significant experience in this field, particularly from a regional perspective like the EU. I'd love to hear your thoughts on how we're responding to cyber threats and what measures are necessary.

Manon Le Blanc emphasized a three-pronged EU approach to tackling cyber threats, focusing on resilience and preparedness, response and deterrence, and international cooperation.

- **Resilience and Preparedness:**
  - Capacity Building: Building robust and secure systems globally, ensuring all states, regardless of resources, enhance cyber defences.
  - Whole-of-Society Approach: Involving governments, private sector, and end-users. The EU's Cyber Resilience Act promotes secure-by-design products.
  - Foresight and Threat Intelligence: Anticipating and mitigating risks through forward-looking approaches.
- **Response and Deterrence:**
  - Sanctions and Accountability: Using sanctions and attribution to hold malicious actors accountable.
  - Asymmetric Measures: Employing economic and political tools to influence and deter persistent threat actors. Cybersecurity extends beyond defense to behaviour modification.
- **International Cooperation:**
  - Information Sharing: Collaboration between nations to develop effective responses and understand threats.
  - Norms and Accountability: The 2015 UN framework on responsible state behaviour provides a foundation. Implementation and enforcement of global norms are essential.
  - Action-Oriented Cooperation: Moving beyond discussions to enforce agreements and frameworks.

Le Blanc concluded that resilience, deterrence, and international collaboration are key to addressing the evolving cyber threat landscape effectively.

Irene

Irene, you have extensive experience in capacity building. How do you think we should respond to cyber threats on a more practical level? How do you approach training and capacity building in your respective fields?

Irene CORPUZ

Irene Corpuz emphasized the importance of accessible and inclusive capacity building in cybersecurity, focusing on practical steps to empower individuals without overwhelming them with complexity. She outlined three key strategies:

I. Leverage Existing Standards and Frameworks:

a. Utilize proven frameworks like ISO 27001, the NIST Cybersecurity Framework, and regional standards such as the EU's NIS Directive.

b. Prioritize critical controls based on organizational needs rather than implementing everything at once.

II.Create Awareness and Knowledge Sharing:

a. Raise foundational awareness through introductory training, relatable case studies, and real-world examples.

b. Highlight opportunities for growth in cybersecurity to attract newcomers.

c. Utilize region-specific training programs, such as those by the GFCE, to align with local needs and realities.

III. Diversity and Inclusion:

a. Address diversity gaps by actively involving women through training, mentorship, and participation in global conferences.

b. Success stories, such as the Middle East having the highest number of women speakers at the Black Hat conference, highlight the impact of targeted efforts.

Corpuz concluded that effective capacity building requires using existing frameworks, promoting awareness, and fostering diversity to ensure a sustainable and confident workforce in cybersecurity.

Neil

Given your extensive experience in the cybercrime field, international cooperation is clearly essential—whether for investigation, evidence collection, or prosecution. How do you see this playing out? What are the challenges and solutions for building an effective international response to cybercrime?

Neil J. Walsh emphasized that addressing cybercrime requires a comprehensive alignment across politics, policy, strategy, tactics, and operations. He highlighted that cybercrime is not merely a technical challenge but a political and policy issue, requiring leaders and policymakers to fully understand its nature and scale. A key example is the UN Cybercrime Convention, where 155 states negotiated a framework criminalizing 11 cyber offenses, ensuring legal equivalency across nations, and embedding strong human rights protections. This demonstrates the necessity for strategies to translate into actionable measures.

The tech sector also bears responsibility. Developers and engineers must anticipate how their innovations might be misused. Walsh cited an example from 2017 when a tool intended for

music artists was exploited for harmful purposes, illustrating the dual-use nature of technology. Similarly, he dismissed calls to ban cryptocurrencies, noting their vast economic role and emphasizing the need for targeted solutions instead of outright bans.

Capacity building, Walsh argued, cannot be one-size-fits-all. He shared his experiences in Eastern Africa, where varying political and technical capabilities required tailored training and resources to address disparities effectively.

Human factors remain a key challenge, as behaviors often compromise cybersecurity. For instance, language models primarily trained in English fail to address risks in regions speaking other languages, creating critical gaps in addressing threats globally.

Lastly, Walsh noted that organizations with both offensive and defensive cybersecurity capabilities risk internal competition, advocating for clearer roles to enhance resource use.

He concluded that tackling cybercrime demands political will, tech sector accountability, tailored capacity building, a focus on human behaviors, and better coordination between offensive and defensive responses. Collaboration and targeted action are essential to improving global resilience against cyber threats.

Manon

Given your experience in developing EU cybersecurity strategies and the EU Cyber Diplomacy Toolbox, could you explain the recent institutional preparations and efforts that the European Union has been implementing to address cyber threats as a leading regional and international organization?

Manon Le Blanc outlined the EU's comprehensive, multi-dimensional strategy to counter cyber threats, emphasizing prevention, resilience, response, and global cooperation. She highlighted that cyber threats are evolving and complex, requiring continuous, tailored efforts.

On prevention and resilience, the EU focuses on raising awareness among citizens and organizations through campaigns and legislative frameworks, such as the NIS2 Directive, which strengthens critical infrastructure protection and establishes uniform security requirements across member states. The EU has also enhanced rapid response capabilities via the updated Cyber Diplomacy Toolbox and introduced a cross-institutional task force to bolster threat intelligence and coordination.

Regarding response and deterrence, the EU employs cyber sanctions to deter and hold malicious actors accountable, particularly state-sponsored threats like those from Russia. Enhanced cyber defense policies ensure resilience in military systems and improve cooperation across member states.

Global cooperation is central to the EU's approach. Internally, it fosters collaboration among its 27 member states, while externally, it engages with global partners through multilateral platforms like the UN Open-Ended Working Group. The EU is also advancing a UN Program of Action for international cybersecurity cooperation, promoting national capacity building, international law application in cyberspace, and knowledge-sharing to protect critical infrastructure.

Le Blanc concluded that the EU's holistic approach aims to build a safer, more resilient cyberspace through prevention, response, deterrence, and strong international partnerships.

Your mention of global cooperation brings to mind Korea's own cybersecurity strategy. Have you had a chance to look at the Korean National Cybersecurity Strategy?

Manon acknowledged the similarities between Korea's and the EU's approaches to cybersecurity, highlighting shared priorities such as resilience, capacity building, critical infrastructure protection, and fostering public-private collaboration. They emphasized the strong partnership between Korea and the EU and expressed enthusiasm for the upcoming EU-ROK Cyber Dialogue. This dialogue presents an opportunity to deepen cooperation and explore ways to jointly enhance cyber resilience and security.

Neil

Let's dive into a specific issue that has sparked serious concern in Korea recently. Just a few months ago, there was a significant case involving deepfake technologies used for sexual exploitation and online crimes. Alarmingly, many of the perpetrators were minors, and they didn't even recognize their actions as criminal. Even more concerning was that the victims were often people close to them—classmates, teachers, fellow students, or even younger sisters.

Since the Budapest Convention and with the recent draft of the UN Cybercrime Convention, which is now in the process of adoption, I want to hear your views on two key aspects:

1. How do you see the relationship between deepfake technologies and AI, both as

tools for cybercrime and for enhancing cybersecurity?

2. ***What impact do you anticipate the UN Cybercrime Convention will have on preventing and punishing such crimes, particularly cases like these?***

Neil emphasized the dual nature of technology like deepfakes and AI, noting that while the technology itself is neutral, its misuse, particularly for harm, is alarming. They highlighted the lack of awareness among perpetrators, especially minors, about the legal and ethical consequences of their actions, which points to a failure in societal education about responsible digital behaviour. Globally, issues like online sexual exploitation and sibling-based abuse have risen, showcasing the amplified risks brought about by technology.

To address this, the speaker argued for a focus on education and social awareness, rather than solely criminalizing offenders, especially minors. Parents, teachers, and community leaders must engage in difficult but necessary conversations about digital ethics. Proactive education programs and parental involvement are essential.

On the international front, the upcoming UN Cybercrime Convention was commended as a landmark in multilateral cooperation. It establishes a framework to criminalize key cybercrimes, balances human rights with enforcement, and aims to harmonize global legislation. However, its success hinges on effective implementation. Many nations face gaps in either political will, technical capacity, or policy coordination, underscoring the need for tailored capacity-building efforts.

Neil also noted the potential of AI and similar technologies to combat cybercrime, such as detecting deepfakes and enhancing investigative capabilities. They stressed the importance of leveraging these tools responsibly.

Lastly, he called for a more unified approach within multilateral systems, arguing that the fragmented handling of cybercrime and cybersecurity in separate UN bodies is ineffective. Criminals exploit hybrid threats, and responses must similarly be flexible, coordinated, and integrated across disciplines. Collaboration, education, and capacity-building were identified as key to staying ahead of cybercriminals.

Allison

Enhancing cyber accountability is likely key to reducing cyber threats and safeguarding cybersecurity.

Could you share your thoughts on:

I. Why we need to enhance cyber accountability?

II. What are the biggest barriers or obstacles to achieving it?

III. How can we effectively enhance cyber accountability?

Allison discussed the challenges of achieving cyber accountability and highlighted the complexity of the issue. She noted that the distinction between crime and security in cyberspace is often unclear, as criminal activities can have significant national or international security implications. Overemphasis on security risks neglecting the human-centric impacts, making a rights-based approach to cybersecurity essential.

Pytlak emphasized the accountability gap, pointing out that the persistence of cyber threats signals the inadequacy of current measures. Drawing lessons from other domains like arms control and climate initiatives, she outlined three key themes for improving cyber accountability: inclusivity, cross-regional collaboration, and a toolbox approach that combines peer reviews, incentives, and sanctions. These measures are more effective than one-size-fits-all solutions.

She identified political will as the greatest barrier, citing examples from disarmament agreements where initial momentum waned over time. To address this, Pytlak advocated for combining deterrence with incentives to encourage compliance and foster global resilience in combating cyber threats.

Irene

With your extensive experience in AI, quantum technologies, and cybersecurity capacity building, especially in the MENA region, I'd like your insights on bridging capacity building and cybersecurity.

Additionally, you've been instrumental in advancing women's participation in cybersecurity, particularly through the Women in Cybersecurity Middle East initiative. This is a crucial yet under-discussed topic, especially in regions like South Korea. Could you share your experience, and the progress made in this field?

Irene highlighted the significant progress made by Women in Cybersecurity Middle East (WiCSME) since its founding in 2018, growing from nine members to nearly 3,000 today. This growth reflects increased awareness of the need for women's participation in cybersecurity, with women now accounting for 25% of the workforce, compared to just 12% a few

years ago.

WiCSME prioritizes encouraging young women to enter the field by tracking how many pursue IT and engineering degrees and secure employment. To amplify its impact, WiCSME collaborates with global initiatives such as the Global Forum on Cyber Expertise (GFCE) and its Women in Cyber Capacity Building (WiCCB) program, which tailors capacity-building efforts to regional and cultural needs. Partnering with the International Telecommunication Union (ITU), WiCSME translated materials into Arabic for the Women in Cyber Mentorship Program, increasing MENA participation from negligible levels to 30% of global participants.

The group also promotes inclusion through initiatives like the Capture the Flag hacking competition, mandating teams include at least one woman, which boosted female participation from 30% to 60%. However, Irene stressed the importance of not only attracting women to cybersecurity but also retaining and developing their careers to ensure long-term contributions to the industry.

What about leadership roles? Women shouldn't just enter the cybersecurity field—they need to rise to leadership levels. Do you have any data on how many women hold leadership positions?

Irene Corpuz highlighted that while WiCSME has made significant progress in increasing women's participation in cybersecurity, their next major goal is to focus on leadership representation. Initially, WiCSME concentrated on supporting recent graduates, providing them with opportunities to grow, such as participating in panels, earning certifications, publishing research, and completing academic degrees. The organization ensures that these achievements are celebrated and made visible, as this visibility helps drive change.

Corpuz noted that companies are starting to acknowledge WiCSME's impact, with some reporting that women now make up 50% of their cybersecurity workforce. However, WiCSME is now challenging these organizations to go further by asking how many of these women hold leadership roles. Moving forward, WiCSME's target is to ensure that women are not only entering the field but are also taking on leadership positions to shape its future.

Allison, do you have any comments on this issue?

Allison Pytlak emphasized the importance of continued dialogue on cybersecurity issues, particularly their gendered impacts. She highlighted research showing how cyber operations, like internet shutdowns, disproportionately affect individuals based on societal gender roles.

Pytlak also linked deepfake technology to technology-facilitated gender-based violence, underlining the harmful intersections of technology and societal dynamics.

She shared that Stimson Center is launching a project next year to study the interplay of gender disinformation, elections, and national security, noting how these factors increasingly reinforce each other negatively. Additionally, Pytlak pointed out the unintended consequences of technological innovation, such as benign apps being repurposed into malicious tools like stalkerware.

While she acknowledged progress in raising awareness and capacity building in cybersecurity, she stressed the need for further research and efforts to understand and mitigate the differentiated harms of cyber operations.

Open floor questions

I'm interested in digital security and cyber threats, and I'd like to bring up a topic that hasn't been fully discussed today. It's about intervention.

Foreign intervention is one aspect, but there seems to be a certain muddiness when it comes to cyber threats. Domestic actors and foreign actors often overlap, especially in cases of manipulating social or political sentiments. How do experts view this "blurring" of actors, and what approaches are being taken to address this intermixing?

On this question, Manon Le Blanc emphasized the growing challenge of blurred lines among cyber actors, including state-sponsored groups, private companies, activists, and criminal organizations. This overlap complicates attribution and effective responses to malicious cyber activities, as these entities often cooperate, directly or indirectly, for varying motives. Addressing this issue requires a dual focus on accountability and strengthening the international normative framework.

She highlighted the United Nations framework, which sets norms and principles for states, such as preventing their territories from being used for cybercrime, protecting critical infrastructure, and avoiding harm to other states' systems. However, enforcement and accountability remain challenging, especially for states like North Korea or Russia, which often lack the political will or incentive to act against such activities.

Le Blanc stressed the importance of global cooperation in addressing this gap. By collective-

ly imposing consequences, such as sanctions or adherence to norms, the international community can encourage accountability and deter malicious cyber activities. Despite political differences among states, enforcing international frameworks and holding states responsible for actions within their jurisdictions is key to tackling this issue effectively.

What changes do you expect from women's inclusion in cybersecurity, especially compared to the nuclear policy field?

Irene CORPUZ: We rely on global surveys conducted regularly by private entities to track progress. While organizations like WKSMY and GFCE don't conduct these surveys directly, we closely monitor the results to measure the impact of our efforts.

It's also important that these surveys cover all industries and regions, not just critical infrastructure sectors like energy or defense, but also education, healthcare, banking, transportation, and telecommunications. A broader scope gives a clearer picture of women's participation and growth in cybersecurity.

As I mentioned earlier, the most recent survey, published last year, showed significant progress, which is very encouraging. This growth is not limited to one group; there are various organizations globally working towards this goal, such as WiCyS (Women in Cybersecurity) in the U.S. and many others across different regions.

Our focus goes beyond simply "ticking the box" for inclusion. We need programs that attract, retain, and promote women in cybersecurity. For example, we celebrate women's achievements—certifications, research publications, and advanced degrees—to inspire others.

Looking ahead, the next step is to expand beyond cybersecurity into other emerging fields like quantum computing. The Women in STEM initiative, which encompasses science, technology, engineering, and mathematics, is critical to achieving broader gender parity.

So, in summary, while progress has been made, there is much more to be done, particularly in ensuring women move into leadership roles and are fully integrated into decision-making processes.

The Battle for Technological Dominance A Competition In Mineral Chips And Batteries

Ingdong YUAN Director, China and Asia Security Programme, Stockholm International Peace Research Institute (SIPRI) and Session Moderator

Brief Introduction

This panel discussion focused on the upstream and midstream dimensions of critical minerals—specifically their extraction, refinement, and production. Critical minerals are indispensable for a broad array of applications, including electronics, electric vehicles (EVs), and military technologies.

The ongoing U.S.-China strategic rivalry looms large over these areas. However, in sectors like batteries and critical minerals, there remains an opportunity for cooperation among the U.S., China, and the European Union, particularly in light of the global push toward a green transition. If this competition is weaponized or overly politicized, we risk creating two parallel, fragmented ecosystems, which could have detrimental consequences for all stakeholders. This dynamic is evident in recent actions: U.S. restrictions on Chinese chip-making companies and efforts to curtail exports of chip-making equipment have prompted retaliatory measures from China, including export controls on critical minerals. Such tit-for-tat responses threaten to escalate tensions further.

With discussions of steep tariffs resurfacing—particularly under a potential future Trump administration—these policies could deepen the trajectory set during the Biden administration and previously initiated under Trump in 2018-2019.

China's current dominance in critical minerals stems from decades of strategic planning and investment, often at environmental and financial costs. Meanwhile, OECD countries, including the U.S. and Europe, have limited critical mineral extraction due to regulatory and environmental concerns. This imbalance has created challenges not only for the U.S. and China but also for the European Union, Japan, and South Korea. Intensifying this rivalry may lead to a lose-lose scenario for all involved.

This discussion delved into these issues, examining the broader context and exploring potential paths forward.

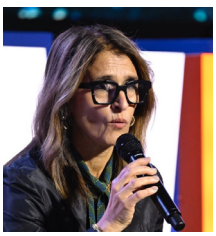
Sophia.

You have written extensively about China's involvement in critical mineral development

and highlighted the growing competition between China and the U.S. There is a perception—and to some extent, reality—those countries in Europe, Asia, and elsewhere rely heavily on China for critical mineral supplies.
Given this competitive environment, concerns are growing about supply chain resilience. There is also fear that China could leverage its dominant position to coerce recipient countries, especially if it faces punitive actions.
This situation risks undermining the mutually beneficial economic relations built over decades and could distract us from shared priorities, such as the green transition, where cooperation would be far more beneficial than competition.
While restrictions on advanced chips are understandable, the scope has expanded to include even legacy chips (like 28-nanometer memory chips). This raises the question:
Do you think we are locked into this competitive dynamic, where cooperation is no longer possible? Or do you see opportunities to move toward a more collaborative approach?

Fostering Collaboration Amid Geopolitical Rivalries: Navigating the Green Transition and Building Global Trust

Sophia KALANTZAKOS, Global Distinguished Professor, Environmental Studies and Public Policy, New York University (NYU) Abu Dhabi



"I'd like to lower the "realist volume" a bit because, throughout the day, we've been focused heavily on security, threats, and competition—almost to the point of creating a sense of inevitability about this situation. Now I'm being asked whether there's hope for collaboration, particularly for something as critical as the green transition"

Key Message

Prof. Sophia Kalantzakos emphasized the need to shift the focus from security and competition to hope and collaboration, especially concerning the green transition. She highlighted the significance of the 2015 Paris Agreement, which aims to limit global temperature rise to 2°C, ideally 1.5°C, by reducing emissions, electrifying transportation, and deploying renewable energy solutions. This transition represents an industrial transformation with significant challenges.
Kalantzakos revisited her earlier analysis of China and the geopolitics of rare earths, questioning how the global community could commit to a green transition without ensuring access to critical materials. Initially, it was believed the market would address these issues,

but geopolitics has since overshadowed economic solutions, intensifying competition and impeding cooperation.

She also touched on the digital transition, noting its entanglement in geopolitical rivalries over control, freedom, and norms, which disrupt global supply chains and economic interdependence. This competition risks undermining trust, a crucial element in addressing divides between the Global North and South and fulfilling promises made to developing nations.

Kalantzakos concluded by urging a shift in focus toward trust-building and collaboration to meet global challenges, particularly in the context of the green transition.

Frank.

Europe, like many others, is heavily dependent on critical minerals and, to some extent, on semiconductors, producing only about 10% of the chips it requires. This reliance on a few suppliers creates vulnerabilities.
In recent years—particularly before discussions of de-risking under President von der Leyen—what strategies has Europe implemented to mitigate these risks? Specifically, how has Europe approached access, investment, and production in critical minerals, including extraction and refinement?
Additionally, how well have these efforts been coordinated with the United States, especially through mechanisms like the Transatlantic Trade and Technology Council (TTC) under the Biden administration? Has this cooperation yielded meaningful results, or are there still unresolved tensions, such as disagreements over trade terms?

Securing Critical Minerals: Addressing Geopolitical Risks and Building Resilient Supply Chains for Energy and Security Goals

Frank UMBACH, Head of Research of European Cluster for Climate, Energy and Resource Security (EUCERS), Center for Advanced Security, Strategic and Integration Studies (CASSIS), University of Bonn

Frank Umbach emphasized the urgent need to recognize the dramatic shifts in the global geopolitical landscape, where leaders like Xi Jinping and Vladimir Putin openly challenge the rules-based international order. This is particularly relevant to the escalating demand for critical minerals necessary for achieving climate and energy goals. Minerals like copper, essential for modernizing electrical

grids, highlight the scale of the challenge: global copper demand for grid upgrades over the next few decades is set to exceed all historical production, yet mining projects face long timelines of up to 20 years due to bureaucratic hurdles.

The geopolitical factor compounds the issue. China has successfully reduced its dependence on the West while increasing Western reliance on Chinese resources. Beyond mining, China dominates refining and reprocessing capacities, posing a significant risk to Western supply chains. In response, the European Commission, since 2010, has developed strategies to secure critical raw material supplies. These include managing demand, enhancing domestic production, and promoting recycling and alternative materials. The EU's Critical Raw Materials Act sets ambitious 2030 targets, but bureaucratic and political challenges hinder implementation.

Umbach highlighted the importance of transatlantic cooperation, which began in 2012, involving the US, EU, Japan, and now Australia, Canada, and the G7. Under the Trump administration, the US recognized critical materials as a national security issue, driven by reliance on China for military technologies. Similarly, Europe discovered vulnerabilities during the pandemic and Ukraine conflict, with 80% of raw materials for ammunition sourced from China.

Despite concerns about potential trade conflicts, Umbach remains optimistic about cooperation. Securing resilient supply chains is vital not only for energy security but also for industrial competitiveness and defense capabilities. Europe must align with models like Japan's focus on economic security to mitigate dependencies and build a robust future framework.

Junhyeok Park.

You're an expert in mineral extraction and supply chain security, so I'd like to ask: Given the proposals and action plans for diversifying critical mineral supplies, how quickly and affordably can alternative critical minerals be extracted, refined, and produced? What challenges do you foresee, and how might these efforts impact global supply chain security?

Securing the Future: Strategies for Sustainable Critical Mineral Supply Chains

Junhyeok PARK, Senior Researcher, Korea Institute of Geoscience and Mineral Resources (KIGAM)

"Let me start with a basic definition: What are critical minerals, and why are they important? Critical minerals are irreplaceable in the near future and vital to economic and national security. They are essential to emerging technologies, yet vulnerable to supply disruptions, as defined by the US Geological Survey (USGS)."

Junhyeok Park, emphasized the growing importance of critical minerals, defining them as irreplaceable resources essential for economic and national security. These minerals, vital to emerging technologies, are increasingly in demand due to green energy policies, advancements in batteries, and AI technologies. For instance, the shift to electric vehicles (EVs) has exponentially increased the need for minerals, with EV batteries requiring 1,000 times more lithium than an iPhone.

The real challenge lies in the supply side. Prior to 2020, critical minerals were peripheral to global markets, with production limited and heavily outsourced to developing countries. This reliance on low-level manufacturing and the geographical concentration of deposits, especially in China, has resulted in an unbalanced and vulnerable supply chain. China dominates every stage of the critical mineral supply chain, especially in sectors like graphite, gallium, and germanium, raising significant supply security risks.

Countries are responding with short- and long-term strategies. Short-term measures include stockpiling minerals, forming bilateral agreements, and incentivizing investments. Long-term strategies focus on multilateral cooperation, resilient systems, and advancing production technologies. Scaling production is hindered by lengthy mining project timelines, particularly in the West, where processes can take over a decade compared to China's shorter timelines. Streamlined permitting and stakeholder coordination are essential to address these delays.

Stockpiling remains a critical short-term buffer against disruptions. While oil stockpiling is common, applying the concept to minerals is more complex due to their diversity. Only a few nations, including Korea and Japan, engage in mineral stockpiling, often for defense purposes.

In the long term, technological innovation is paramount. Breakthroughs in exploration, eco-friendly production, smart mining, and recycling can significantly reduce dependencies.

Technologies like AI and raw material substitution, akin to advancements in shale gas production, hold transformative potential. However, countries must create specific roadmaps for each mineral, addressing technological gaps and focusing R&D investments strategically.

In conclusion, Park outlined four key steps for a sustainable critical mineral supply chain: scaling up production via vertical integration, reducing project timelines through improved regulations, building stockpiles for immediate resilience, and investing in technology to enhance production efficiency and sustainability.

Zainab

With the rising focus on critical minerals, the African continent has become a major target for global powers scrambling to gain access to resources, invest in extraction, and potentially refine them.
Could you provide a general overview of this competition? Specifically, we see China and the US as key players, with the EU also trying to secure its place. What are the characteristics of this scramble for critical minerals in Africa, and which countries—Beijing or Washington—have been more effective in achieving their stated goals?

Strategic Minerals: Africa's Role in the Global Transition and the Path to Equitable Development

Zainab USMAN, Senior Fellow and Director, Africa Program, Carnegie Endowment for International Peace

"This is indeed a critical topic, especially for African nations. However, I want to stress that while the focus on critical minerals feels like a new scramble, the issue of harnessing natural resources—minerals specifically—for economic development is not new for Africa."

Zainab Usman highlighted the historical context of Africa's role in global resource extraction, now reframed around "transition" or "strategic" minerals vital for economic and technological development. She stressed that while demand for these minerals, driven by economies like the US, China, and South Korea, is rising, supply remains geographically dispersed, with Africa playing a pivotal role. Industrial policies from consuming countries, such as China's "Made in China 2025" and the US Inflation Reduction Act, illustrate aggressive strategies to

secure supply chains and dominate value chains.

On the producer side, countries like Indonesia and several African nations have employed export bans to retain value and capture midstream benefits, although with mixed success. Usman underscored the risks of repeating historical asymmetries, where resource-rich regions gain little economic benefit. She noted that while industrial and trade policies are largely bilateral, the lack of robust multilateral cooperation undermines global stability in critical mineral supply.

She concluded with an emphasis on Africa's opportunity to leverage its resources for economic development and prosperity while avoiding past pitfalls. However, challenges remain in balancing resource extraction with sustainability and ensuring African nations benefit equitably from the global scramble for these strategic resources.

Yu Jie

I'm sure many in Europe have been discussing the concept of de-risking over the past few years. In fact, we recently produced a report comparing EU and Japanese de-risking policies.
My sense is that while Brussels recognizes the risks and vulnerabilities in areas like critical minerals and chips, it's not particularly eager to engage in an all-encompassing competition with China.
Where possible, there still seems to be hope for collaboration—especially in areas like the green transition, where cooperation could benefit not only both players but also the broader fight against climate change and the shift toward a post-fossil fuel economy?

Barriers to EU-China Collaboration: Structural Rivalries, Geopolitical Divides, and the Global South Pivot

YU Jie, Senior Research Fellow on China, Chatham House

"Over the past two decades, China has heavily pursued the upgrading of its manufacturing capabilities through strong industrial policies. This has enabled Chinese products—whether in electric vehicles (EVs), renewable energy equipment, or other sectors—to compete directly with European counterparts"

Key message

YU Jie presented a pragmatic and somewhat pessimistic assessment of the prospects for EU-China collaboration, highlighting three main barriers:

Structural Economic Challenges: Over the last two decades, China has advanced its manufacturing sector through industrial policies, eroding the economic complementarity it once had with Europe. Chinese global champions, such as BYD in EVs and SAIC Motor (owner of MG Rover), have created direct competition with European companies. President Xi's goal of transforming China into a "larger version of Germany" adds to this structural rivalry, making economic cooperation increasingly challenging.

Political and Geopolitical Realities: Events like the COVID-19 pandemic and the war in Ukraine have prompted Europe to reconsider its dependencies on external powers, particularly China for manufacturing and Russia for energy. Meanwhile, China's focus on economic self-reliance is driven by perceptions of a US-led containment strategy, backed by strengthened US-EU ties. Additionally, Beijing perceives hypocrisy in the EU's trade protectionism, particularly when Chinese contributions to climate change mitigation, such as EVs and renewables, are met with trade barriers instead of collaboration.

The Role of the Global South: China's engagement with the Global South, fueled by initiatives like the BRI and GDI, has strengthened its partnerships with non-Western nations. By offering affordable renewable energy solutions and infrastructure development, China has positioned itself as a preferred partner in these regions, both as a market and a source for critical minerals. This focus is reinforced by tensions with Western economies.

YU Jie concluded that structural competition, political divides, and China's pivot toward the Global South limit meaningful EU-China collaboration. While selective cooperation may be feasible, these dynamics underline the growing divisions in the global geopolitical landscape

Emerging questions

Sophia

I think you've raised critical points about the role of both public and private sectors in addressing the challenges surrounding critical minerals and supply chains.

To follow up, the reality is that much of the extraction, refinement, and production of these minerals is carried out by private enterprises, who invest and take on significant risks. These companies naturally seek government support—be it in the form of regulation or subsidies.

So, how do you see public-private partnerships working to manage and mitigate these challenges? And, in terms of strategic foresight, what's your projection for the next five years? Will the situation worsen, or is there hope for some guardrails to ensure competition remains stable and manageable?

Sophia Kalantzakos highlighted the missed opportunities by OECD countries in building green transition infrastructure, which allowed China to leap ahead in sectors like electric vehicles and renewable energy. China's success stems from aggressive industrial policies, subsidies, and long-term planning, reminiscent of past Western strategies.

Public-Private Dynamics: The private sector has historically prioritized profits, overlooking strategic risks like overdependence on China for supply chains. After the 2010 rare earth crisis, businesses returned to cost-driven practices once prices stabilized. Governments now intervene to close these gaps, using taxpayer funds and subsidies to incentivize domestic production. For example, the U.S. Inflation Reduction Act supports EV production and adoption. However, Western countries still lag behind China's affordable green technologies, leading to tariffs on Chinese goods not just for trade fairness but to address competitiveness gaps.

Strategic Foresight: Two major challenges lie ahead:

- U.S. Global Role: Policies under Biden, like "Made in America" initiatives, aim to integrate allies such as South Korea into the U.S. market. A shift in administration, like a return of Trump, could signal more unilateral actions, compelling Europe to reconsider its strategies. Europe might pragmatically engage with China on green transitions if transatlantic relations falter.
- Geopolitics and the Global South: Developing nations prefer flexibility, avoiding alignment with either the West or China. Both Europe and China maintain ties with these regions through initiatives like the Belt and Road and Global Gateway, offering opportunities for collaboration rather than polarization.

Climate at the Center: The urgency of the climate crisis should unify global leadership. China's vision of "ecological civilization" aligns with Europe's goal of "living well within planetary boundaries." In an increasingly fragmented world, climate action offers common ground to bridge divides. Ignoring the climate crisis would make other competitions, like cyberspace or military advancements, secondary to the planet's existential challenges.

Frank,

looking into your crystal ball—can Europe realistically compete and address its vulnerabilities in critical minerals?

Frank Umbach emphasized that China's geoeconomic and geopolitical strategy involves controlling the entire supply chain for green technologies, from mineral extraction to end-product manufacturing. This deliberate strategy has been seen before, such as during the rare earth crisis when China drove Western competitors out of the market, ultimately controlling 97% of global production by 2010. The same oversupply tactics are now being used in areas like EV exports to Europe, aimed at undercutting Western industries.

Europe's Dilemma: Europe faces two conflicting priorities:

1. Accelerating the green energy transition to combat climate change.
2. De-risking and reshoring production to reduce dependence on China.

Pursuing the green transition necessitates increased imports of Chinese technologies like solar cells and green hydrogen equipment, as 60% of green hydrogen electrolysis production is based in China. Conversely, focusing on reshoring would drive higher costs and potentially slow down the green transition. Achieving both objectives simultaneously is unrealistic.

The Path Ahead: Governments and industries must make strategic choices and communicate them clearly to the public:

- Accept higher costs to rebuild local, secure supply chains.
- Fast-track the energy transition, even if it deepens reliance on China.

Ultimately, these decisions involve not just economic and environmental considerations but also long-term strategic priorities.

Emerging questions

Dr. Park.

Any final thoughts?

Junhyeok PARK

Dr. Park highlighted three examples of public-private partnerships from the Korean experience:

1. Technological Support: State-owned companies and national labs provide technical expertise to assist the private sector, particularly in feasibility studies where experts are scarce in consuming countries.
2. Financial Support: This year, Korea established the Supply Chain Stabilization Fund, providing $8 billion annually in loans to companies building critical mineral supply chains.
3. Bilateral Cooperation: Governments play a crucial role in securing mining rights and claims, facilitating international agreements that benefit the private sector.

Dr. YU Jie, please share your final insights

YU Jie highlighted China's strategic increase in research and innovation funding, the only budget category to grow by around 12% last year, despite other sectors remaining flat or declining. This funding is directed towards fostering "little giants," private sector companies specializing in niche technologies and cutting-edge innovations. This state-led strategy demonstrates China's unique approach to driving technological breakthroughs. While its success remains uncertain, it underscores a distinct model of leveraging public-private

Closing Remarks

Dong-yeol

Distinguished guests,

I would like to begin by thanking all the speakers for their insightful and enriching discussions today, as well as the moderators for skilfully coordinating each session. My special gratitude goes to SIPRI and KAIST, our esteemed partners, for their intellectual and professional contributions in preparing this forum.

When this forum was first launched in 2021, discussions on today's themes were still in their early stages within the international community. Back then, the idea of hosting initiatives like the AI Summit or the RIM Summit—or adopting foundational documents on AI governance—might have seemed far-fetched.

However, these developments are both natural and necessary as we adapt to the evolving security landscape. We must remain vigilant and agile in addressing emerging challenges. We are all aware that new technologies impact numerous sectors—from science, economy, and military to intangible areas like our values and ways of thinking. These changes are actively reshaping the dynamics of global security.

To navigate this complex journey, cooperation among multiple stakeholders is essential. Governments, international organizations, academia, businesses, and civil society each play a vital role in identifying the missing pieces of this global puzzle.

With this in mind, today's sessions tackled a wide range of issues—from technological advancements to their implications for international security and geopolitics. We expanded our discussions to include the intersections of cybersecurity, AI, weapons of mass destruction, quantum technologies, space exploration, and critical minerals.

These conversations provided a valuable platform to examine both the potential benefits and risks that accompany evolving technologies and to discuss how we can enhance global cooperation to address these challenges. Korea remains committed to contributing to these ongoing discussions. As part of this dedication, Korea will continue to host this forum, developing it further into a unique multi-stakeholder platform where participants can exchange candid ideas and build relationships that contribute meaningfully to addressing emerging security threats.

Allow me to conclude with a quote from the winner of our forum's catchphrase competition: "Borderless threats call for borderless cooperation." This captures the essence of what we are striving for. Let us continue to think together, dialogue together, and collaborate. I look forward to welcoming you all again at this forum in Seoul next year.

Dan SMITH

Thank you very much. I would also like to express my deep gratitude to the speakers, moderators, participants, and the Korean Ministry of Foreign Affairs for organizing such an excellent and timely forum. I must admit, I feel a bit regretful now that I didn't start by recording everything said today, running it through an AI program to produce a transcript, and then

feeding it into ChatGPT for a full summary. It would have been a nice shortcut to capture the depth and richness of today's discussions! Of course, I won't attempt to summarize everything because the conversations have been far too rich and comprehensive for that. But I'd like to share just a few key takeaways.

First, we are facing a number of dilemmas. One is the tension between short-term priorities and long-term goals, which both Ambassador Rhee and I highlighted in our opening remarks this morning. Another major dilemma, which came through most clearly in Session Three, is the balance between the need for cooperation to solve complex global issues and the realities of geopolitical competition. This is a critical challenge. The increasing need for global cooperation is colliding with a declining appetite for cooperation on a broad enough scale.

Second, we need to continue doing our homework. We must keep improving our understanding of interconnections, assess risks more accurately, and most importantly, identify the opportunities that exist. Throughout today's discussions, it became clear that cooperation and action are needed—both now and for the long term—on issues like AI and cybersecurity, critical and strategic minerals, and the green transition toward a just and peaceful future. However, simply talking about cooperation does not solve the problem. We need an approach that both encourages and incentivizes cooperation.

This leads to key questions: Who is most advanced in transitional technologies and the extraction of natural resources? Who is the "we" we are referring to? Is it a collective humanity "we", or a Western "we", or even smaller subsets—Europe, Northeast Asia, or individual countries? These questions remind me of an important point raised in the first panel this morning: the need to decolonize our approach. This is not just an ethical issue or a matter of historical justice; it is also pragmatic. The world order is shifting, and we must address these challenges in a way that reflects and responds to these changing realities.

Another significant point is that outlawing something does not automatically solve the problem. While regulation is essential, especially given the rapid advancements in technology and shifting geopolitics, it is a complex challenge. That said, we are not starting from scratch. We already have a foundation in international law, including humanitarian and human rights law, existing treaty commitments, and a starting point in the United Nations Charter. While innovation is vital, we must recognize that progress comes not by discarding what we already have but by building on it.

Finally, I want to thank everyone once again for a truly engaging and productive forum. I hope this marks the beginning of continued discussions and collaboration in the years to come. Thank you all, and I look forward to seeing you at future forums.

Exploration of Emerging Technologies & Emerging International Security Issues and Expansion of Global Networks

신기술의 국제안보에 대한 함의 분석 및 국제 네트워크 확대 방안연구