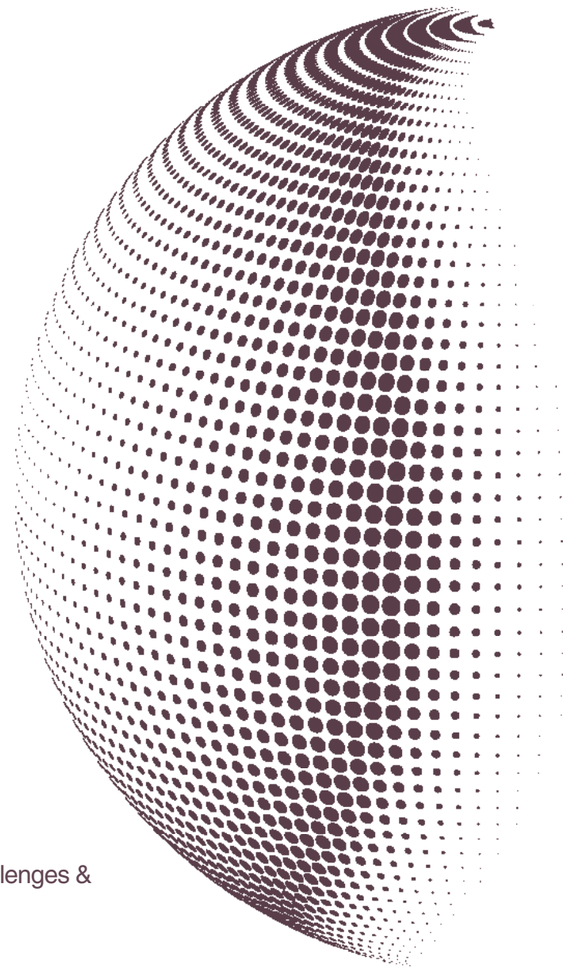


신기술 기반 복합 위협의 국제안보 함의 분석 및 국제협력 방안 연구

Exploration of Emerging Technology-Driven Challenges &
Emerging International Security Issues and
Global Security Collaboration

주관연구기관 | 한국과학기술원 KAIST

외교부

신기술 기반 복합 위협의 국제안보 함의 분석 및 국제협력 방안 연구

KAIST

KAIST

Exploration of Emerging Technology-Driven Challenges &
Emerging International Security Issues and
Global Security Collaboration

Exploration of Emerging Technology-Driven Challenges &
Emerging International Security Issues and
Global Security Collaboration

신기술 기반 복합 위협의 국제안보 함의 분석 및 국제협력 방안 연구

주관연구기관 | 한국과학기술원

신기술 기반 복합 위협의 국제안보 함의 분석 및 국제협력 방안 연구

Exploration of Emerging Technology-Driven Challenges & Emerging International Security Issues and Global Security Collaboration

제출문

외교부 장관 귀하

본 보고서를 '신기술 기반 복합 위협의 국제안보 함의 분석 및 국제협력 방안 연구'과제의 최종 보고서로 제출합니다.

2025.10.

주관연구기관 | 한국과학기술원(KAIST)

연구책임자 | **김용희** (국가미래전략기술정책연구소 소장)

공동연구원 | **김소영** (과학기술정책대학원 교수)

서용석 (문술미래전략대학원 부교수)

최용찬 (국가미래전략기술정책연구소 연구부교수)

참여연구원 | **김승현** (과학기술정책대학원 박사과정)

전준형 (전산학부 학사과정)

Content

신기술 기반 복합 위협의 국제안보 함의 분석 및 국제협력 방안 연구

Exploration of Emerging Technology-Driven Challenges & Emerging International Security Issues and Global Security Collaboration

Exploration of Emerging Technology-Driven Challenges &
Emerging International Security Issues and
Global Security Collaboration

표 차례

그림 차례

ABSTRACT

AI, 양자, 드론 등 신흥 기술이 안보 영역과 결합하면서 하이브리드 위협의 양상은 점점 더 복잡하고 상시화되고 있음. 허위정보, 사이버 공격, 핵심 인프라 교란 등 다양한 차원에서 발생하는 위협은 군사·비군사, 물리·디지털, 국가·비국가 행위자가 복합적으로 결합하는 양상 속에서 국제안보 질서를 흔드는 핵심 요인으로 부상 중임.

특히, 미·중 간 전략 경쟁 심화와 기술패권 구도의 장기화는 자원과 기술을 둘러싼 국제 갈등을 확대시키고 있음. 동시에, 첨단 기술 기반 무기체계의 확산과 인지전 심화는 전쟁 양식을 근본적으로 변화시키고 있음. 이에 따라 기술 주권 확보와 사회적 회복력(resilience) 강화는 국가 안보 전략의 최우선 과제로 부상하고 있음.

이러한 배경 속에서 2025년 세계신안보포럼(WESF)은 “하이브리드 위협의 진화와 국제안보”를 주제로 국내외 전문가들이 인지전, 신기술과 위협 동향, 핵심 인프라 회복력 등 주요 안보 현안을 심도있게 논의하는 자리가 마련되었으며, 앞서 개최된 라운드테이블에서는 국내 민·관·학 전문가들이 참여하여 안보 현안과 관련된 의제를 사전 검토하고 다양한 시각을 공유·조정하는 논의가 진행되었음.

동 포럼에 참여한 국·내외 전문가들은 다층적 안보 위협 환경 속에서 국가 차원의 상황 인식 고도화, 핵심 인프라 회복력 강화, 민·관·학 협력 확대, 국제 규범 정립을 통한 다자적 대응의 중요성을 강조함. 아울러 기술 선도국으로 자리매김한 한국이 국제사회에서 협력의 기반을 마련하기 위한 능동적 역할을 수행해야 함을 강조함.

As emerging technologies such as AI, quantum, and drones increasingly converge with the security domain, the nature of hybrid threats is becoming more complex and persistent. Threats such as disinformation, cyberattacks, and disruptions to critical infrastructure—arising across multiple dimensions—are emerging as key factors destabilizing the international security order, driven by the combined actions of military and non-military, physical and digital, state and non-state actors.

In particular, the intensifying strategic competition between the United States and China and the prolonged dynamics of technological hegemony are amplifying global conflicts over resources and technology. At the same time, the proliferation of advanced technology-based weapon systems and the deepening of cognitive warfare are fundamentally transforming the character of warfare. Consequently, securing technological sovereignty and strengthening societal resilience have emerged as top priorities in national security strategies.

Against this backdrop, the 2025 World Emerging Security Forum(WESF), held under the theme “The Evolution of Hybrid Threats and International Security”, provided a venue for domestic and international experts to engage in in-depth discussions on key security challenges such as cognitive warfare, emerging technologies and threat dynamics, and the resilience of critical infrastructure. A preceding roundtable brought together Korean experts from government, industry, and academia to review relevant security agendas and to share and coordinate diverse perspectives.

Participants at the Forum emphasized the importance of enhancing national-level situational awareness, strengthening the resilience of critical infrastructure, expanding cooperation among government, industry, and academia, and advancing multilateral responses through the establishment of international norms in the face of a multidimensional security environment. They also underscored that Korea, having established itself as a leading technological nation, should play a proactive role in laying the foundation for cooperation within the international community.

Exploration of Emerging Technology-Driven Challenges &
Emerging International Security Issues and
Global Security Collaboration

1 연구 필요성 및 목적

1. 연구 필요성 및 목적

1-1. 연구 필요성

● 신흥 기술이 안보 영역과 결합하면서 하이브리드 위협은 점점 더 복잡하고 상시화되고 있음. 허위정보, 사이버 공격, 핵심 인프라 교란과 같은 다양한 차원에서 발생하는 위협은 군사·비군사, 물리·디지털, 국가·비국가 행위자의 복합적 결합 속에서 국제안보 질서를 흔드는 핵심 요인으로 부상하면서, 이의 안보적 위협 분석 필요성 증대

- 이에 따라 안보의 위협 범위는 기존 영역(지·해·공)을 넘어 사이버·전자기 및 우주 영역에 이어 인지심리 차원으로 안보 위협 확대
- 기술의 비약적 발전과 글로벌 연결성의 심화는 안보 위협을 점점 더 복합적이고 예측 불가능한 형태로 변화시키고 있으며, 이러한 흐름 속에서 기술 발전이 야기하는 하이브리드 위협의 안보적 함의를 정밀하게 분석하는 작업은 필수적임.
- 특히, 기술 기반 위협은 전통적인 군사적 위협을 넘어 사이버 공격, 정보 조작, 경제적 압박, 인프라 마비 등 다양한 비정형·비대칭적 양상의 복합 안보 위협을 증폭시키며, 국가 간 경계를 넘나들며 빠르게 진화하고 있음.
- 따라서, 신기술 기반 위협의 특성과 구조를 분석하는 동시에, 그로 인해 유발되는 안보적 측면의 위협을 식별하고 대응 전략을 제시하는 연구가 필요한 시점임.
- 특히, 사이버 공격은 국가 안보를 위협할 수 있는 주요 공격 수단으로, 유럽 사이버 사건 저장소(European Repository of Cyber Incidents)에서는 사이버 공격의 목표와 특성에 따라 6가지 범주(data theft, doxing, disruption, hijacking, exploitation, ransomware)로 구분함. 2021년 이후 모든 유형의 사이버 공격 발생 빈도가 크게 증가하는 추세를 보이며, 그중에서도 오·남용을 동반한 하이재킹과 서비스 방해 공격의 증가세가 가장 가파름(Romansky *et al.*, 2024).

● 하이브리드 위협의 증폭은 국가 안보 차원을 넘어 사회 전반의 안전, 회복력, 지속 가능성에까지 직접적인 영향을 미치고 있음. 하이브리드 위협은 사회적 인프라(예:보건, 교통, 통신, 에너지 등)를 직접적으로 겨냥하며 사회 혼란을 초래할 수 있으며, 이에 대한 단순 방어를 넘어 위기 발생 이후 사회가 얼마나 신속하게 회복하고 정상화될 수 있는가가 전략의 핵심 과제로 부상하고 있음. 이에 따라 핵심 인프라 복원 능력, 정보 환경의 신뢰 확보, 시민사회의 대응·적응 역량 강화 등 회복력 중심의 안보 전략을 연구할 필요가 있음.

- 하이브리드 위협은 특정 국가나 세력이 군사적 수단과 비군사적 수단을동시에 활용하여 상대 사회를 교란하는 전략적 행위를 의미함. 예컨대, 사이버 공격으로 전력망을 마비시키면서 동시에 허위정보를 퍼뜨려 사회 불안을 증폭시키는 방식이 대표적 사례임.
- 이러한 하이브리드 위협은 높은 불확실성과 파급력으로 국가적·사회적회복력을 정면으로 시험하는 도전으로 부상하고 있음. 따라서, 하이브리드위협을 중점 사례로 심층 분석하고, 그로부터 안보적 함의와 대응 전략을체계적으로 도출할 필요가 있음.
- 아울러, 이러한 흐름은 전통적 안보와 구조적으로 구분되는 신흥 안보 양상의심층적 분석을 요구하며, 신기술이 안보에 미치는 파급효과에 대한 진단이필수적임.
- 최근 급부상하는 신기술의 안보 함의에 통찰을 제공할 국내·외 전문가풀을 구축하고, 이해관계자 인식 조사를 통해 쟁점과 우선순위를 체계적으로 파악·반영하는 노력이 요구됨.

● 기술 기반 하이브리드 위협에 대응하기 위한 국제 협력 체계는 선택이 아니라 필수적인 전략임. 기술 기반 위협은 국경과 조직의 경계를 넘어 전염되며, 단기간 내 통제가 어렵기 때문에 개별 국가 차원의 대응만으로는 한계가 있음. 따라서 국경·조직·기능을 초월한 협력적 구조를 구축하고, 이를 통해 회복력 강화와 공동 대응 역량을 높이는 방안에 대한 연구가 절실히 요구됨.

● 이외에도, 신흥 안보 양상은 국제정세와 기술 발전에 따라 갈수록 다변화·복잡화 되고 있기 때문에 신기술의 안보적 파급효과와 변화 양상을 지속적으로 진단·분석하고, 이에 대응하기 위해 규범 형성, 정보 공유, 공동 실증, 공동 대응 등 국제 협력을 한층 더 강화해야할 필요가 있음. 아울러 한국 정부는 이러한 분야의 국제 협력에서 선도적 위상을 공고히 하며 주도권을 확보를 위해 지속적으로 노력할 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 2021년도부터 세계신안보포럼(WESF)을 개최하여 매년 관련 논의를 심화하고 세계적으로 확대하고 있음.

표1. 지난 세계신안보포럼 (WESF) 행사 요약

개최일자	포럼 주제	주요연사
2021년도 (2021.11.16.)	신안보위협 대응을 위한 다자협력의 미래	정의용(외교부장관), 토마스 헨드릭 일베스(전 에스토니아 대통령), 클라우스 슈밥(WEF 회장), 테드로스 거브레예우스(WHO 사무총장), 유르그 라우버(UN 사이버안보작업반 초대 의장), 세드릭 오 (프랑스 디지털담당 국무장관) 등
2022년도 (2022.6.21.~6.22.)	신흥안보 위협의 과거와 현재, 그리고 미래 - 신뢰에 기반한 국제협력으로의 길	박진(외교부장관), 에후드 올메르트(전 이스라엘 총리크리스토퍼), 크리스토퍼 페인터(전 미 국무부 사이버조정관), 테드로스 거브레예수스(WHO 사무총장), 손영권(하만이사회 의장), 스테판 뒤갱(사이버평화연구소 CEO), 백경란(질병관리청장), 댄 스미스(스톡홀름국제평화연구소 소장) 등
2023년도 (2023.12.5.)	사이버공간과 신기술의 안보 위협 대응을 위한 글로벌 협력 강화	박진(외교부장관), 반기문(제8대 유엔 사무총장), 리차드 폰테인(신미국안보센터 회장), 폴 샤레(신미국안보센터 연구소장 및 총괄 부사장). 마트 누르마(북대서양조약기구 사이버방위센터 -CCDCOE 센터장), 쉬에 란(칭화대 국제학부 및 AI 국제거버넌스 연구소 학장) 등
2024년도 (2024.12.5.)	진화하는 안보 환경 속 국제협력 - 사이버, AI, 신기술을 중심으로	조태열(외교부장관), 이동렬(국제사이버협력대사), 칼 빌트(유럽외교협의회 공동의장), 댄 스미스(스톡홀름국제평화연구소 소장), 이광형 (KAIST 총장), 제임스 앤드류 루이스 (CSIS 수석부회장), 임종인(대통령실 사이버 특보), 조경현(뉴욕대학교 컴퓨터과학과 교수), 마농 르블랑(유럽대외관계청 사이버조정관) 등

개최일자	포럼 주제	주요연사
2025년도 (2025.9.8.)	하이브리드 위협의 진화와 국제안보	조현(외교부장관), 이광형(KAIST 총장), 크리스토프 호이스겐(생갈렌 심포지엄 공동의장), 카림 하가그(SIPRI 소장), 테이야 틸리카이넨(하이브리드 COE 소장), 제임스 설리번(영국 왕립합동군사연구소(RUSI) 사이버·기술국장), 질리언 프로스트(캐나다 외교부 사이버, 핵심기술, 민주회복력국장) 등

- 2025년 9월, 세계신안보포럼(9.8)에 이어 사이버 서밋 코리아(9.9~9.11), 서울안보대화(9.8~9.10) 등이 같은 주간에 연속적으로 개최되며 우리 정부가 국제안보와 사이버 보안 분야에서 국제 협력 체계 구축을 적극 추진하고 있음을 보여줌.
- 진화하는 안보 환경과 변화 양상은 어떠한지 분석하고, 주요국과 이해관계자들의 인식을 지속적으로 파악하는 것이 필요함.

1-2. 연구 목적 및 내용

● 신흥 기술이 안보 영역과 결합하면서 하이브리드 위협은 더욱 복잡해지고 상시화가 가속화 됨되고 있음. 이에 따라 하이브리드 위협의 특성과 신기술 기반 복합 위협의 파급력을 분석하고, 대응전략 수립을 마련하기 위한 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 하이브리드 위협의 진화와 국제안보에 관한 주요 행사 기획과 전문가 네트워크 구축, 신기술 및 안보 정책 현황 분석으로 구성

- (행사 기획 및 운영) 2025 세계신안보포럼의 주제(하이브리드 위협의 진화와 국제안보; The Evolution of hybrid Threats and International Security)를 반영한 포럼 기획 및 운영('25.9), 국내 전문가 라운드테이블 기획 및 운영('25.7.)
- (전문가 네트워크 구축) 인지전, 하이브리드전, 하이브리드 위협 대응 전략 및 사이버 위협 대응 분야에 대한 전문가 조사 및 주요 기술별 전문가 조사 진행. 이어 하이브리드 위협 동향과 신흥 안보·보안·국제 협력을 주제로 전문가 그룹 심층 인터뷰 및 하이브리드 위협 대응 전략을 주제로 전문가 세미나 진행. 이를 통해 하이브리드 위협과 신안보 전반에 관한 전문가 분석과 정책 인사이트를 도출, 국내·외 전문가 네트워크를 구성 및 활용
- (신기술 및 안보 정책 현황 분석) 하이브리드 위협의 주요 특징 분석, 주요 신기술 안보 이슈와 주요국 신기술 안보 관련 정책 현황 분석

표 2 : 주요 연구 내용

I. 주요 행사기획	II. 전문가 네트워크 구축	III. 신기술 및 안보 정책 현황 분석
■ (국제행사) 2025 세계신안보포럼(WESF) 기획 및 공동 운영 ■ (국내행사) 2025 세계신안보포럼 라운드테이블 기획 및 공동 운영	■ 하이브리드 위협 및 대응 전략 국내·외 전문가 조사 ■ 하이브리드 위협 동향과 신흥 안보·보안·국제 협력 분야 전문가 네트워크 마련 (FGI 및 세미나)	■ 하이브리드 위협의 주요 특징 분석 ■ 주요 신기술 분야별 안보 이슈 분석 ■ 주요국 신기술 안보 관련 정책 현황 분석

Exploration of Emerging Technology-Driven Challenges &
Emerging International Security Issues and
Global Security Collaboration

2 하이브리드 위협

2. 하이브리드 위협

2-1. 하이브리드 위협의 개념과 정의

2-1-1. 하이브리드 위협이란

● 21세기 안보 환경은 단일한 군사적 충돌보다는 정치, 경제, 사이버, 정보공간을 포괄하는 다양한 수단을 복합적으로 활용하는 '하이브리드 위협(Hybrid Threats)'이라는 새로운 형태의 도전에 직면해 있음.

- 최근 몇 년간, 이 하이브리드 위협은 유럽 안보 지형에서 중심 주제로 부상해 오고 있었으며, 이제 하이브리드 위협이라는 용어는 국제안보 담론에서 익숙하게 사용되고 있지만 그 개념은 여전히 혼재되어 있음.
- 일반적으로 '하이브리드(hybrid)'는 "서로 매우 다른 두 요소가 혼합된 것"을 의미하며, 이를 안보 위협에 적용할 경우 군사적 및 비군사적 도전 요소의 결합을 뜻하게 됨. 즉, 하이브리드 위협은 한 가지 방식이 아니라 군사·비군사 수단을 복합적으로 섞어 국가나 조직의 취약점을 노리는 위협을 의미함.
- 하이브리드 위협의 내재된 특성들로 전통적인 이분법의 경계를 흐리고, 모호성을 조장하는 것이라 이야기되고 있으며, 평시와 전시의 경계가 허물어진 복합적 상태라고도 이야기하고 있음. 즉, 하이브리드 위협은 표면적으로는 전쟁(무력 충돌)으로 보이지 않지만, 전쟁과 평화의 경계(그레이존)에서 압박을 가해 법적·정치적 대응을 어렵게 만드는 게 특징임.
- 하이브리드 위협은 즉각적 기능 장애(사회 기반시설·금융·의료 마비)와 지속적 침식(신뢰·결속 약화)을 동시에 유발하고, 공격자 식별과 책임추궁이 어려워 억지·제재가 지연된다는 면에서 그 파급력과 위협성이 심각함.
- 최근, 하이브리드 위협이라는 개념이 빠르게 진화하고 있으며, 관련 문헌의 증가, 관련 연구기관 및 연구조직의 확산 및 정책 문서에서 사용되는 언어의 변화를 통해 하이브리드 위협이라는 개념의 빠른 진화 현상 파악 가능함(Giannopoulos *et al.*, 2021). 한편, 아직까지 '하이브리드 위협' 또는 관련 활동에 대해 널리 합의된 정의는 존재하지 않으며, 심지어 EU와 NATO 내부에서도 서로 다른 정의들이 통용되고 있는 실정임(Zandee *et al.*, 2021).

표 3 : 하이브리드 위협의 주요 정의

출처	정의
Giannopoulos *et al.* (2021)	하이브리드 위협이란, 국가 또는 비국가 행위자가 지방, 지역, 국가, 제도 수준 등 다양한 차원에서 특정 표적의 의사결정에 영향을 주거나 이를 방해하여, 해당 표적을 약화시키거나 손상시키려는 활동을 의미
Costigan and Hennessy(2024)	하이브리드 위협이란, 국가 또는 비국가 행위자가 군사적 및 비군사적 수단, 공개적 또는 은밀한 방식을 동원해 대상 사회를 약화시키고 정치적 목표를 달성하려는 잠재적 행동을 의미하고 이러한 행동은 국가 간의 통상적인 상호작용 범위를 넘어서며, 전쟁을 직접적으로 추구하지는 않지만 전쟁과 유사한 영향력을 행사할 수 있음.
European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)[1]	하이브리드 위협은 악의적인 의도를 가지고 계획되고 실행되는 유해한 활동으로, 정보 조작, 사이버 공격, 경제적 압박, 은밀한 정치적 책략, 강압적 외교, 군사력의 위협 등 다양한 수단을 결합해 국가나 제도 등의 대상을 약화시키려는 행위를 말하며, 이러한 위협은 단순한 영향력 행사나 간섭에서부터 실제 하이브리드 전쟁에 이르기까지 다양한 목표와 형태를 지니며, 전통적인 안보 개념의 경계를 넘어서는 복합적이고 포괄적인 위협 유형임.

2-1-2. 기존 문헌 조사

● 유럽연합 집행위원회 산하 과학·지식 서비스 기관인 공동연구센터(Joint Research Centre)와 하이브리드 위협 대응을 위한 유럽 우수센터(Hybrid CoE)가 공동으로 발행한 정책을 위한 과학 보고서(Science for Policy report)에 따르면, 하이브리드 위협이란 국가 또는 비국가 행위자가 지역, 국가, 제도, 또는 국제 차원에서 표적의 의사결정 과정에 영향을 미치거나 이를 약화시키기 위해 수행하는 활동을 의미(Giannopoulos *et al.*, 2021)

- 즉, 하이브리드 위협은 국가 또는 비국가 행위자가 정치적, 경제적, 사회적, 정보적 수단을 복합적으로 활용하여, 지방부터 국가 및 제도 수준에 이르기까지 다양한 차원에서 표적의 의사결정 과정에 영향을 미치거나 이를 방해하려는 활동을 의미함.
- 이러한 위협은 군사적 수단뿐 아니라 사이버 공격, 허위 정보 유포, 경제적 압박 등 다양한 방식으로 전개되며, 목표는 사회 불안 조성, 제도적 마비, 정책 결정 지연 등 표적의 전반적인 기능을 약화시키는 데 있다고 말하고 있음.
- 하이브리드 위협은 간섭, 영향력 행사, 작전, 캠페인, 전쟁/무력 충돌 등 다양한 활동 유형을 포함하는 넓고 포괄적인 개념으로, 이러한 모든 활동은 한 국가의 내부 공간에 대한 원치 않는 개입 행위로 간주될 수 있음.

● NATO(북대서양조약기구)의 정의에 따르면, 하이브리드 위협은 군사적·비군사적 수단뿐 아니라 은밀하고 공개적인 방식까지 결합한 것으로, 허위정보, 사이버 공격, 경제적 압박, 비정규 무장 세력의 투입 및 정규군의 사용 등을 포함함.[2]

- 이러한 하이브리드 방식은 전쟁과 평화의 경계를 흐리게 하고, 표적 국가의 국민들에게 의구심을 심으려는 시도이며, 그 목적은 사회를 불안정하게 만들고 약화시키는 데 있음. 최근 몇 년 사이 하이브리드 위협의 속도, 범위, 강도가 증가하고 있으며, 국가든 비국가 행위자든 하이브리드 공격을 예방하고, 대응하며, 이를 반격할 준비를 갖추는 것은 NATO의 최우선 과제임.[3]

1) Hybrid CoE. (n.d.) "Hybrid threats as a concept" (검색일: 2025.6.25.)
2) NATO OTAN. (2024) "Countering hybrid threats" (검색일: 2025.7.5.)
3) NATO OTAN. (2024) "Countering hybrid threats" (검색일: 2025.7.5.)

- 하이브리드 위협은 국가 또는 비국가 행위자가 특정 사회를 약화시키고 자신들의 정치적 목표를 달성하기 위해 취할 수 있는, 공개적이거나 은밀한 군사적·비군사적 활동을 의미함. 이러한 활동들은 국가 간의 통상적인 상호작용을 넘어서는 것이며, 반드시 전쟁을 목적으로 하는 것은 아님(Costigan and Hennessy, 2024).

● 유럽 하이브리드 위협대응센터(Hybrid CoE)에 따르면, 하이브리드 위협이란 민주주의 국가 및 제도의 구조적 취약점을 표적으로 삼아 다양한 수단을 통해 조정되고 동기화된 행동. 감지 및 귀속의 임계점을 악용하고, 전쟁-평화, 내부-외부 안보, 지방-국가, 국내-국제 관계 등의 경계를 활용하며, 지방/국가/제도 수준의 의사결정에 영향을 주어 행위자의 전략적 목표를 실현하는 활동을 의미함.[4)]

- 하이브리드위협대응센터는 하이브리드 위협을 다음과 같이 특징짓고 있음. 첫째로, 다양한 수단을 통해 민주 국가와 기관의 체계적 취약성을 의도적으로 표적으로 삼는 조정되고 동기화된 행동이고, 둘째로. 탐지 및 귀속의 문턱과 다양한 인터페이스(전쟁-평화, 대내외 안보, 지역 국가, 국가-국제)를 활용하는 활동이며, 셋째로, 지역, 주 또는 기관 차원에서 다양한 형태의 의사 결정에 영향을 미치고, 대상을 약화시키거나 손상시키면서 에이전트의 전략적 목표를 더욱 달성하기 위해 고안된 활동임.

● EU의 '하이브리드 위협 대응 공동 프레임워크'(Joint Framework on Countering Hybrid Threats) 정의에 따르면, 하이브리드 위협은 강압적이며 전복적인 활동의 혼합으로, 외교, 군사, 경제, 기술 등의 전통적 및 비전통적 방법들이 조정되어 사용될 수 있으며, 공식으로 전쟁이 선포되지 않은 선 아래에서 국가 또는 비국가 행위자가 특정 목표를 달성하기 위해 사용하는 활동을 의미함(Zandee *et al.*, 2021).

● EU 대외행동서비스(EEAS) 정의에 따르면, 하이브리드 위협은 국가 또는 비국가 행위자가 특정 정치적 목표를 달성하기 위해 전통적 및 비전통적, 군사적 및 비군사적 활동을 조정된 방식으로 결합한 것으로, 하이브리드 캠페인은 다차원적이며 전통적 및 비전통적 도구와 전술을 활용하여 강압적·전복적 수단을 결합하고 있음. 이러한 위협은 탐지하거나 행위자를 특정하기 어렵도록 설계되어 있으며, 핵심 취약점을 겨냥하고 혼란을 유발하여 신속하고 효과적인 의사결정을 방해하는 것을 목적으로 함(Zandee *et al.*, 2021).

● 미국 국방대학교의 저명한 연구원 프랜시스 호프만(Francis Hoffman)에 따르면, 하이브리드 위협이란 동시에 정규 무기, 비정규 전술, 테러리즘, 범죄적 행동을 맞춤형으로 혼합하여 특정 전장과 시간 속에서 정치적 목표를 달성하려는 모든 적대 세력을 의미함.[5)]

● 김소정(2014) 보고서에 따르면, 하이브리드 위협이란 전통적인 군사적 공격과 비군사적 수단(예:사이버 공격, 경제적 강압, 정보전 등)을 결합하여 특정 국가나 비국가 행위자를 압박하고 혼란을 일으키는 복합적인 위협을 의미하며 하이브리드 위협의 목적은 대상 사회를 불안정하게 만들고, 정부의 의사결정을 방해하며, 국가의 회복력을 약화시키는 데 있음. 또한, 하이브리드 위협의 주요 특징으로는 명확한 경계가 없으며, 사이버공간상 모든 행위가 하이브리드 위협의 대상이자 목표, 수단이 동시에 될 수 있음.

● 송태은(2020) 보고서에 따르면, 하이브리드 위협이란 대규모의 군사력을 사용하지 않고, 공격 주체의 노출을 최소화하며, 공격의도를 은폐하면서 전략적 목적을 달성하려는 '무정형 전략(amorphous strategy)'이고, 하이브리드 위협의 목표로는 공격대상이 되는 적의 전투 및 대항 의지를 좌절시키고, 공격대상 정부와 제도의 정당성(legitimacy) 및 현지 주민 혹은 시민의 정부에 대한 지지를 제거 하는 것임.

● 이외에도, 박지영 및 김선경 (2019) 보고서에 따르면, 하이브리드 위협은 방대한 양의 정보와 정확한 잠재 대상을 타겟팅 할 수 있는 능력으로 위협적이며 인공 지능 개발과 네트워킹 기술이 성숙함에 따라 위험도가 증가함.

2-1-3. 하이브리드 위협 VS 하이브리드 전쟁

● Monaghan(2019)은 하이브리드 위협과 하이브리드 전쟁이 각기 다른 안보 도전 과제임을 전제로, 하이브리드 위협은 비폭력적인 수단들을 광범위하게 결합해, 사회의 전반적인 취약점을 공략함으로써 기존 질서를 약화·전복하고, 국가 기능, 통합성, 국민의 의지를 훼손하는 전략으로, 이러한 전략은 결정적 대응(특히 무력 대응)을 유도하지 않고 점진적으로 목표를 달성하려는 수정주의 행위자들이 주로 사용함. 반면, 하이브리드 전쟁(Hybrid warfare)이란 무장 충돌 상황에서 상대의 정규군 전력을 무력화하기 위해 다양한 전쟁 유형과 비군사 수단을 복합적으로 사용하는 도전 과제라는 정의를 제안함(Monaghan, 2019).

- Monaghan(2019)에 따르면, 하이브리드 위협과 하이브리드 전쟁은 기본적으로 기존 국가 권력을 무력화하려는 시도라는 같은 원인도 있지만, 하이브리드 위협은 국민의 의지와 정부의 의사결정 역량을 주요 타깃으로 삼는데, 반면 하이브리드 전쟁은 군대의 작전 수행 능력을 약화시키는 데 집중하는 전략적 목표의 차이도 있음.

- Monaghan(2019)은 하이브리드 위협과 하이브리드 전쟁은 분쟁의 연속선상(conflict continuum)에서 각기 다른 위치에 놓여 있으며, 분쟁 연속선상에서 조망한 하이브리드 위협과 하이브리드 전쟁 관련 그림1을 제시

- 다만, Monaghan의 주장은 우크라이나-러시아 전쟁과 이스라엘-하마스 분쟁 등 최근 전·분쟁을 통해 최근 현황을 반영하기에는 제한적임. 최근 전·분쟁에서는 하이브리드 위협과 하이브리드전 경향이 전쟁 전·중·후 모두 나타나고 있으며, 군사 분야 뿐만이 아니라 크게는 외교, 정보, 군사 및 경제, 작게는 정치, 군사, 경제, 사회, 정보 및 기반체계에 얽히고 설켜 나타나고 있음(라운드테이블 참여 전문가).

4) Hybrid CoE. (n.d.) "Hybrid threats as a concept" (검색일: 2025.6.25.)
5) Nettis (2020) "Multi-Domain Operations: Bridging the Gaps for Dominance" (검색일: 2025.7.18.)

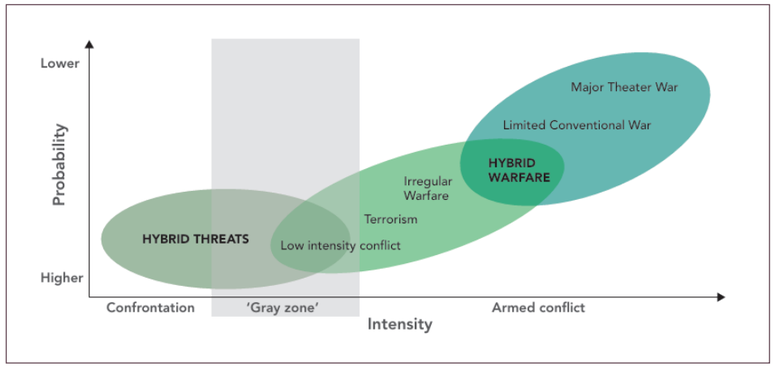


그림1. 분쟁 스펙트럼에서 조망한 하이브리드 위협과 하이브리드 전쟁

출처: Monaghan(2019)

2-1-4. 전쟁수행 영역 (War-fighting Domains)

● 미 합동작전 교리(Joint Operations)에 따르면, 공중·지상·해상·우주 영역(domains)과 더불어 정보 환경(여기에는 사이버 포함)을 작전 환경의 구성 요소로 본다고 명시되어 있음(Joint Publication 3-0, 2011). 아울러, 미국의 다영역작전(MDO, Multi-Domain Operations)은 cyber·space·air·ground·sea의 다섯 영역을 연결 대상으로 본다는 점을 분명히 함.[6)]

- 미 공군 공식교리에 따르면, 합동 전영역 작전(Joint All-Domains operations)은 전통적 공중, 지상, 해상, 사이버, 우주 영역에 더해 전자기 스펙트럼(electromagnetic spectrum)으로 구성됨(U.S. AIR FORCE & U.S. SPACE FORCE, 2021; U.S AIR FORCE, 2025).
- 최근 몇 년간 미국방부(Department of Defense)는 다영역작전의 필요성이 점점 커지고 있다는 점에 주목해 왔으며, 국가방위전략(National Defense Strategy)에서는 "이 복잡하고 경쟁적인 안보 환경에서 경쟁하기 위해, 미국은 전 범위의 분쟁에서 동시에 여러 영역에 걸쳐 작전할 준비가 되어 있어야 한다"고 명시하고 있음.[7)]
- 미 군사 교리에서 작전 영역은 공중, 해상, 육상, 우주, 그리고 사이버 공간 5개로 정립되어 있음. 여기서 영역(domains)이란 "임무 수행에 필요한 자유로운 행동과 우위를 위해 접근하거나 통제하는 것이 필수적인 거시적 기동 공간"이라 할 수 있는데, 이는 접근해야 하며 또한 효과를 창출할 수 있는 공간이며 반드시 물리적일 필요는 없음을 의미함.[8)]
- Nettis(2020) 자료에 따르면, 최근에는 정보작전의 부상으로 인해 여섯 번째 영역으로 인지 영역(cognitive domain)이 논의되고 있으며 미 태평양 육군 사령관 로버트 브라운 장군은 인지 영역이 단순히 고려 대상이 아니라, 가장 중요한 영역이라고 강조함. 인지 영역의 중요성은 우주 및 사이버 기술의 등장과 함께 점점 커지고 있으며, 이 영역은 대중을 더 많은 정보에 노출시켜 전통적인 언론·방송·정부 기관 등 정보의 유통을 통제하던 매개자들을 무력화시키고 있으며, 국가든 비국가든 누구나 어느 영역에서든 효과를 창출하기 쉽게 만들고 있음.[9)]
- Nettis(2020)는 전쟁수행 영역과 이를 가로지르는 교차 기능 영역을 나타낸 다영역작전 체계도(그림2)를 제시. 이 그림에서 도메인은 가로 막대로 표시되며, 여기에는 인지 영역이 포함됨. 사이버 영역은 더 큰 전자기 스펙트럼으로 표현됨. 교차 부문(cross-cutting sectors)은 지역, 주, 연방 수준의 군사, 정부, 상업 주체들의 결합으로 구성됨. 이러한 부문들은 순수한 군사적 활동이나 도메인의 전통적 한계를 넘어선 것으로, 이 교차 부문에는 상업 부문, 민간 부문, 군 인력, 우주 기술, 사이버, 핵, 정보, 정보작전, 전자전 등이 포함됨.[10)]

6) U.S. Department of War. (2019) "Multidomain Operations Rely on Partnerships to Succeed" (검색일: 2025.8.9.)
7) Nettis (2020) "Multi-Domain Operations: Bridging the Gaps for Dominance" (검색일: 2025.7.18.)
8) Donnelly & Farley (2018) "Defining the 'Domain' in Multi-Domain" (검색일: 2025.6.21.)

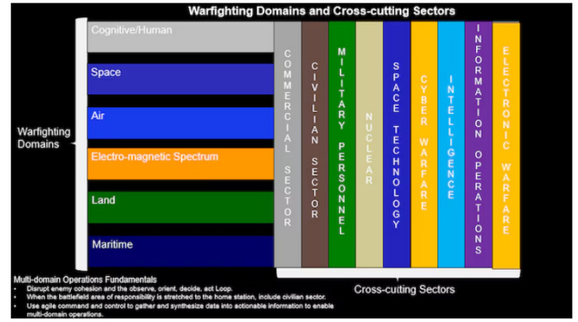


그림2. 다영역작전(MDO) 체계: 전쟁수행 영역과 교차 기능 영역

출처: Nettis (2020)

● NATO의 구조 내에는 해상(Maritime), 지상(Land), 공중(Air), 우주(Space), 사이버(Cyberspace)의 5개 작전 영역이 존재하고 있으나[11)], 인간의 인지·판단·신뢰 체계를 겨냥한 인지전(Cognitive Warfare)이 부상하면서, NATO 내부에서는 이를 '제6의 전장(The Sixth Domain)'으로 개념화하고 교리적 채택을 위한 정책 검토를 진행 중임.

그림3. NATO의 다영역 작전(Multi-Domain Operations, 2023)

출처: NATO OTAN – Welcome to allied Command Transformation. (2023) "Multi-Domain Operations in NATO – Explained" (검색일: 2025.9.12.)

9) Nettis (2020) "Multi-Domain Operations: Bridging the Gaps for Dominance" (검색일: 2025.7.18.)
10) Nettis (2020) "Multi-Domain Operations: Bridging the Gaps for Dominance" (검색일: 2025.7.18.)
11) NATO OTAN – Welcome to allied Command Transformation. (2023) "Multi-Domain Operations in NATO – Explained" (검색일: 2025.9.12.)

- 2020년, NATO의 후원을 받아 인지전이라는 제목의 연구가 발표되었고, 이 연구보고서에서는 인지전을 지상(Land), 해상(Sea), 공중(Air), 우주(Space), 사이버(Cyber)와 함께 NATO의 제6의 작전 영역(The Sixth Domain of Operations)으로 규정. 21세기의 전장은 인간의 뇌가 될 것이고, 인간은 쟁취의 대상 영역이며, 인지전은 우리 개개인의 프로세서인 뇌를 겨냥한 뇌과학의 군사화를 수반하게 될 것이라고 언급하고 있음.[12)]
- NATO 전쟁수행 기본 개념(NWCC, NATO War-fighting Capstone Concept)은 2021년에 승인되었으며, 이는 동맹의 억제 및 방위 태세를 강화하기 위한 노력에 기여하고, NATO의 결정적 군사적 우위를 유지·발전시키기 위한 비전 및 2040년까지 군사력의 지속적 적응 및 발전을 지원하는 방향을 제시하였음.[13)] NWCC의 핵심 발전 요소 중 하나로 인지적 우위(Cognitive Superiority)를 포함[14)]
- NATO는 폭탄이나 미사일이 아닌 거짓과 조작으로 수행되는 새로운 형태의 전쟁에 직면하고 있는데, 적대 세력들은 온라인 공간에서 허위정보(disinformation)와 대립적 수사를 퍼뜨림으로써 NATO에 대한 대중의 신뢰를 훼손하려 시도하고 있음. 이러한 전략은 인지전(Cognitive Warfare)의 일환으로, 동맹 내부의 불화를 조장하고 자기 방어 능력을 약화시키려는 목적을 가짐. 연합전력변환사령부(Allied Command Transformation, ACT)는 '인지전 개념(Cognitive Warfare Concept)'을 개발 중임. 또한, ACT는 인지 영역(cognitive domain)에서 막대한 잠재력과 위험성을 동시에 가진 인공지능의 책임 있는 군사적 활용에 관한 군사적 자문을 제공할 예정임.[15)]

● 우리나라도 미래 안보 환경 변화에 대응하기 위해 지·해·공 영역을 넘어 우주·사이버·전자기 영역에서의 전력체계 준비 중임.

- 합동참모본부는 우주·사이버·전자기 등 전장 영역의 확장에 대응하고, 인지적 차원의 통합정보작전을 수행하기 위한 다영역작전부를 전략본부에 만드는 등 합참 직제 개정안을 입법(2024.11.22.)[16)]
- 국방혁신 4.0 추진 과제에서 우주, 사이버, 전자기 등 신영역 작전수행개념 및 첨단 전력체계 발전안 제시[17)]

12) European Parliament. (2022) "NATO study on the 'weaponisation of brain sciences' for the purposes of 'cognitive warfare'" (검색일: 2025.9.26.)
13) NATO OTAN – Welcome to allied Command Transformation. (n.d.) "The NATO Warfighting Capstone Concept" (검색일: 2025.9.11.)
14) NATO OTAN – Welcome to allied Command Transformation. (2023) "NATO Warfighting Capstone Concept: An Adaptive 20-year Strategy for NATO and its Allies" (검색일: 2025.9.29.)
15) NATO OTAN – Welcome to allied Command Transformation. "Allied Command Transformation develops the Cognitive Warfare Concept to Combat Disinformation and Defend Against "Cognitive Warfare"" (검색일: 2025.10.7.)
16) KBS 뉴스. (2024) "합동참모본부, 우주·사이버·전자전 대비 '다영역작전부' 신설" (검색일: 2025.7.12.)
17) 대한민국 국방부. (n.d.) "국방혁신 4.0 추진 중점 및 과제- 우주, 사이버, 전자기 등 신영역 작전수행개념 및 첨단 전력체계 발전" (검색일: 2025.8.7.)

2-1-5. 하이브리드 위협을 이해하기 위한 모델

● EU-JRC(Joint Research Centre)와 Hybrid Centre of Excellence(Hybrid CoE)에서는 하이브리드 위협을 어떻게 개념화하고 구성요소들을 체계적으로 어떻게 이해할지에 대한 모델 제안(Giannopoulos *et al.*, 2021)

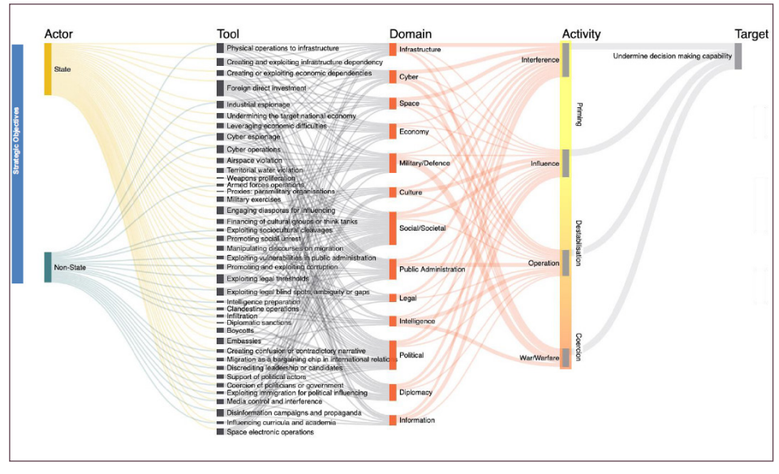
- EU 집행위원회 산하 공동연구센터(JRC)와 하이브리드 위협 대응센터(Hybrid CoE)는 하이브리드 위협 개념 모델과 분석 프레임워크를 공동으로 개발. 다양한 행위자(actors), 도구(tools), 영역(domains), 단계(phases) 같은 요소들을 포함한 개념적 모델을 통해 공통적 이해를 만들고자 함.
- EU-JRC와 Hybrid CoE가 공동 제안한 모델은 위협 예측 및 조기 경보(Early Warning) 시스템 구축, 국가 또는 조직에서 취약점 평가 및 회복력 강화를 위한 전략 수립, 국제기관-EU/NATO-회원국 간-민관 간 공조(cooperation)와 정보공유(sharing) 및 다양한 단계(phases) 및 도구(tools)를 포함한 가상 시나리오를 통해 대응체계 준비도를 높이는 데 도움이 될 것으로 기대함.
- 제안한 이 개념 모델이 응답하고자 한 핵심 질문 중 하나는 바로 "무엇이 위협을 하이브리드로 만드는가?"라는 것임.

표 4. 개념 모델의 4가지 핵심 축

축(Pillar)	설명
행위자(actors)	- 국가(state) 또는 비국가(non-state) 행위자
도구(tools)	- 행위자가 활용하는 수단들: 사이버 공격, 허위정보, 외교, 선전, 경제압박, 불법/비정규전, 심리전, 사회 내부 갈등 조장에서의 행동 등
영역(domains)	- 하이브리드 위협이 작용하는 활동 영역. 기술(tech), 경제(economic), 사회(social), 정치(political), 정보(information), 군사(military) 등 여러 영역이 포함됨. - 국가 권력의 수단을 특징짓기 위한 개념으로, 세분성과 일반화의 분석적 가치를 균형 있게 반영하기 위해 총 13개 영역 고려
단계(phases)	- 하이브리드 위협의 시간적 구성: 준비 → 침투 → 실행 → 후속 효과 등

그림 4. 개념 모델(conceptual model)의 시각화

출처: Giannopoulos *et al.* (2021)



2-2. 하이브리드 위협의 특징

● 하이브리드 위협의 주요 특징은 다음과 같이 정리할 수 있음. 국제기구(NATO, EU, Hybrid CoE)와 주요 연구 문헌에서 공통적으로 강조하는 핵심 포인트를 포함 기준으로 정리

- 수단의 혼합성(Multimodality): 군사와 비군사, 정규와 비정규, 디지털과 물리적 수단이 동시에 또는 순차적으로 사용됨. 예컨대 사이버 공격과 가짜뉴스 유포, 정치 개입, 경제적 압박이 연쇄적으로 전개됨.[18)]
- 은밀성 및 익명성(Plausible Deniability): 공격의 출처가 명확하지 않음. 국가는 직접 개입하지 않고, 대리인(proxy actors) 또는 사이버 공간을 활용함. 즉, 탐지와 추적(책임소재 규명)을 어렵게 함으로써 대응 지연 초래[19)]
- 비대칭성(Asymmetry): 상대방보다 경제력, 군사력 등 전통적 자산이 부족한 행위자도 효과적으로 공격 가능. 기술과 정보조작 등을 통해 비용 대비 높은 효과를 노림 (Bertolini *et al.*, 2023; Weissmann *et al.*, 2021).
- 전쟁과 평화 사이의 회색지대(Grey Zone): 하이브리드 위협은 공식적 전쟁은 아니지만, 국가 안보를 심각하게 위협하고 국제 질서를 교란하는 행위 법적·군사적 대응 기준이 모호하여 정책적 혼란 유발(Bertolini *et al.*, 2023)[20) 21) 22)]
- 사회적 신뢰와 제도적 기반 공격(Targeting Societal Cohesion): 단순한 물리적 파괴가 아닌, 민주주의·공공 신뢰·사회 통합을 약화시키는 것이 목적. 선거 개입, 허위정보 유포, 극단주의 조장 등 포함(Hedling, 2025)[23)]
- 지속적, 저강도 작전(Persistent & Low-Intensity Operations): 일회성 공격이 아니라 장기적으로 다양한 형태로 지속. 특히 사회 시스템의 '피로도'를 높이고, 자가붕괴를 유도하는 전략 사용(Hybrid CoE, 2021; NATO OTAN 2022)
- 기술 활용 및 적응성(Tech-driven & Adaptive): 인공지능, 드론, 위성, 빅데이터 등 첨단 기술을 융합하여 전통적 대응을 무력화. 단순한 기술 사용을 넘어, 공격 전략이 기술 중심으로 빠르게 변화하여 대응하기 어렵게 진화하고 있음. 또한, 적응형 전략 사용으로 공격 방법과 타깃이 빠르게 변함.[24) 25) 26) 26) 27 28)]

표 5 : 하이브리드 위협 신흥 주요 기술 및 전술 사례

① 인공지능(AI)	자동화된 콘텐츠 생성, 대규모 정보공간(뉴스·SNS·포럼)에서 여론 조작·분열 증폭 및 허위정보 확산에 사용, 표적 선정 자동화 (전술 예: LLM/멀티모달 모델로 대량의 현지어 맞춤 선전물·댓글·DM 자동 생성, 감성·주제 모델링으로 지역별 민감 이슈·분열선 탐지 → 메시지 미세조정, 음성·문자·이미지 합성을 결합한 복합 심리전 수행)
② 드론	저비용·저위험으로 물리적 인프라 정찰·교란, 감시, 소규모 정밀타격 등 물리적·비정규전 수행 (전술 예: 변전소, 통신기지국, 연료 저장고 등 중요시설 원거리 정찰·영상 수집 → 사이버/물리 공격 타겟팅 정밀화. 상업용 드론 개조로 익명성 확보)
③ 위성·지리정보 (Sat/GIS)	실시간 타격 또는 인프라 마비 작전에 활용, 제재 회피·병참 추적, 정보전 근거 제공 (전술 예: 상업 위성영상(SAR/EO) 주기 수집 → 부두·군기지·송유관 활동 파악, 물류 흐름 추적, AIS(선박)/ADS-B(항공) 데이터 분석으로 그레이존 활동(깜깜이 항해, 환적) 식별, GIS와 결합해 취약지점(초고압선, 교량, 해저케이블 상륙점) 타겟 리스트화)
④ 빅데이터 분석	사회·경제적 약점, 여론 분열 포인트를 정밀 타깃팅 (전술 예: 대규모 디지털 흔적에서 취약계층·핵심 여론 허브 식별, 메시지·자원 배분 최적화)
⑤ 딥페이크 (영상·음성 합성)	여론 왜곡, 공공 불신 조장, 지도자 발언 위조, 위기 방송 조작, 기업·기관 평판 훼손 등을 통해 신뢰 파괴·혼란 조성 (전술 예: 선거·위기 시기를 노려 긴급 성명 영상/음성 위조 → 금융시장·치안 불안 유발, 유명 언론 포맷·로고·앵커 음성 모사로 진위 식별 비용 크게 상승)
⑥ 소셜미디어·메신저	내러티브 창출–증폭–지속 루프 구축을 통해 정보 확산·사회 분열의 주전장 (전술 예: 해시태그·밈·자동화 계정을 활용해 특정 메시지를 트렌드화. 커뮤니티·비공개 메신저를 통한 장기적 침투 및 극단주의 확산)

18) NATO OTAN. (2024) "Countering hybrid threats" (검색일: 2025.7.5.)
19) Hybrid CoE. (n.d.) "Hybrid threats as a concept" (검색일: 2025.6.25.)
20) Wikipedia. (n.d.) "Grey-zone (international relations)" (검색일: 2025.9.21.)
21) Rühle & Roberts (2021) "Enlarging NATO's toolbox to counter hybrid threats" (검색일: 2025.9.2.)
22) EU Joint Framework on Countering Hybrid Threats (2016)
23) Hybrid CoE. (n.d.) "Hybrid threats as a concept" (검색일: 2025.6.25.)
24) Hybrid CoE. (2021) "Hybrid CoE Trend Report 6: The future of cyberspace and hybrid threats" (검색일: 2025.9.11.)
25) Giannopoulos *et al.*, (2021)
26) Sprengel (2021)
27) Romansky *et al.*, (2024)
28) NATO OTAN. (2024) "Countering hybrid threats" (검색일: 2025.7.5.)

2-3. 하이브리드 위협 주요 사례

● 이스라엘-하마스(Hamas) 교전

- 사이버 공격을 수반한 하이브리드 위협 사례로, 2013년 하마스는 이스라엘에 대해 1,400회 로켓공격과 아울러 4천4백만회의 사이버 공격을 수행(송태은, 2020)
- 이스라엘은 하마스와 지하드(Jihad)의 라디오 방송을 하이재킹(Hijacking)하여 테러리스크를 돕지 말 것을 설득하는 심리전도 수행(송태은, 2020)

● 러시아의 크림 반도 병합

- 2014년 러시아는 무장한 정규군이 아닌 은밀하게 군복 없이 활동하는 병력('리틀 그린맨-little green men'이라 불림[29])을 활용하여 크림반도의 실질적 지배력을 확보함
- 비군사적 수단도 병행됨: 선거(국민투표) 조직, 언론 선전, 정보 조작, 정치적 압박 등이 포함됨.[30) 31) 32)]
- 크림반도 병합은 군사적 충돌 없이 국제법과 주권 원칙을 회피하면서도 국제사회의 직접적인 군사 대응을 유발하지 않는 전략적 하이브리드 위협 사례로 널리 평가되고 있음.[33)]

● NotPetya 공급망 공격

- 역사상 비용과 혼란의 규모 면에서 가장 큰 악성코드 공격은 2017년 러시아의 사이버 작전인 NotPetya였는데, 이는 돈바스 전쟁의 일부였으며 전 세계적으로 치명적인 재정적 타격을 직접 초래(Salt and Sobchuk, 2021)
- 우크라이나 회계 소프트웨어 업데이트(M.E.Doc 소프트웨어를 설치) 경로를 악용해 전 세계로 확산, NotPetya의 의도된 표적은 우크라이나였지만, 이 공격은 FedEx, Merck, 그리고 세계 해상 운송의 약 5분의 1을 담당하는 덴마크의 해운 대기업 머스크(Maersk)와 같은 다국적 기업들의 소프트웨어를 심각하게 훼손시킴(Salt and Sobchuk, 2021; Crosignani *et al.*, 2021).
- 백악관은 이번 공격의 배후가 러시아의 우크라이나 불안정화 시도의 일환임을 확인. NotPetya는 '사이버' 단일 사건만 보면 하이브리드가 아니지만, 러시아의 다영역 혼합 전술 속에서 수행된 '하이브리드 위협'의 핵심 사례로 보는 것이 타당

● 중국의 남중국해 전략(South China Sea Strategy)

- 중국의 남중국해 전략은 대표적인 하이브리드 위협의 국제 사례로 간주될 수 있음. 여러 국제안보 전략 문서와 학술 연구에서 중국의 회색지대 전략(Grey-zone strategy)과 비군사적·비정규전적 수단의 복합 활용 방식이 하이브리드 위협의 전형으로 분석되고 있음(Guilfoyle, 2019; Schultheiss, 2023).
- 중국은 남중국해에서 군사적 강압과 비군사적 수단(법률전, 심리전, 정보전 등)을 결합하여 자국의 영향력 확대와 해양 지배권 주장을 전개하고 있음. 이는 전통적 전쟁이 아닌 '그레이존(gray zone)' 내에서 이루어지며, 명확한 군사 충돌 없이 전략적 목표를 달성하려는 하이브리드 전략으로 해석됨(Yoon & Kim, 2023).

● 이란의 대리전(Proxy Warfare) 전략

- 이란은 시리아, 예멘, 이라크 등지에서 직접 병력을 대규모로 투입하기보다는 현지 민병대, 민간 무장단체, 불규칙 전투 세력 등을 지원하면서, 외교적·정보적·군사적 수단을 혼합하여 지역 영향력을 확대하고 있음(Kazdal, 2025).
- 공식 군대를 전면 배치하지 않고 비정규군 또는 대리 세력을 사용함으로써, 국제법적 책임을 모호하게 만듦. 이는 하이브리드 위협의 중요한 특징 중 하나인 책임 회피성을 갖게 함. 또한, 정보전·정치적 선전, 여론 조작, 외교적 압박을 병행하고 있음.

● 러시아의 서구권 선거 개입

- 러시아는 사이버 해킹(정당·캠프 이메일 탈취 등)과 대규모 정보·심리전(봇·가짜계정·선전·타깃 광고)을 결합해 서구 선거의 여론·의제·신뢰에 영향을 주려 함. 이는 군사·비군사 수단을 결합하는 하이브리드 위협의 전형임.
- 러시아는 해킹·정보공작을 결합해 2016년 미국의 대선에 영향력을 행사(Office of the Director of National Intelligence, 2017). 이외에도, 러시아는 사이버 심리전을 이용 2016년 영국 브렉시트 국민투표, 2017년 독일 총선, 프랑스 대선, 스페인 카탈루냐 독립 투표, 2018년 이탈리아 총선, 2019년 유럽의회선거(EU Parliamentary Election)와 미국 중간선거 등 서구권 소셜미디어 플랫폼에 AI 알고리즘 프로그램인 가짜계정 봇(bots)을 이용한 디지털 허위조작정보의 대규모 유포(송태은, 2020)

29) Wikipedia. (n.d.) "Little green men (Russo-Ukrainian War)" (검색일: 2025.8.29.)
30) Wikipedia. (n.d.) "2014 Crimean status referendum" (검색일: 2025.9.14.)
31) Wikipedia. (n.d.) "Media portrayal of the Russo-Ukrainian War" (검색일: 2025.9.22.)
32) Wikipedia. (n.d.) "Russian occupation of Crimea" (검색일: 2025.7.3.)
33) Wikipedia. (n.d.) "Russian annexation of Crimea" (검색일: 2025.7.2.)

2-4. 하이브리드 위협 대응

2-4-1. 하이브리드 위협 대응이란

● 하이브리드 위협 대응은 이러한 복합적 위협에 맞서기 위해 군사·비군사적 수단을 통합적으로 활용하고, 국가·사회 전반의 복원력과 억제력을 높이는 일련의 전략적·정책적 활동을 의미함.[34)]

- 이는 전통적 억지(deterrence) 개념을 넘어, 사이버·경제·사회·외교 등 전 영역을 포괄하는 포괄적 억지(comprehensive deterrence)로 확장(NATO OTAN, 2022)
- 따라서 하이브리드 위협 대응은 국방·외교뿐 아니라 사이버 보안, 언론·플랫폼 정책, 경제·산업, 시민사회까지 아우르는 통합적 대응 체계가 필요(EU, 2016)
- 하이브리드 위협 대응(Countering Hybrid Threats)이란 이러한 복합적 위협을 인식하고 억제하며, 피해 발생 시 신속한 회복력을 발휘할 수 있도록 군사·외교·경제·정보·사회적 수단을 통합적으로 운용하는 전략적 활동을 의미(EU, 2016)
- 하이브리드 위협 대응의 핵심은 단순한 군사적 방어를 넘어, 사회 전체의 복원력(resilience)을 높이고 범정부적 통합 대응과 국제 협력을 결합하는 새로운 안보 패러다임을 구축하는 것이 핵심[35) 36) 37)]

● 위협 대응의 필요성

- 위협의 빠른 확산과 강도 증가: NATO는 최근 하이브리드 공격의 속도, 규모, 강도가 급증했다고 평가하고 있으며, 최근 기술 변화와 글로벌 상호연결성의 발전이 이를 촉진하는 주요 요인으로 평가[38)]
- 핵심 인프라에 대한 복합 위협: 하이브리드 위협은 사이버·물리·심리 작전을 결합해 주요 기반시설(Critical Infrastructure Systems, CIS)에 치명적 위협을 가함(Vaseashta *et al.*, 2025). NATO 해양 사령부는 천문학적 수준의 인프라에 대한 "해저 하이브리드 전쟁" 가능성을 경고하고, 유럽·북미 인구 10억 명의 안보를 위협한다고 지적[39)]
- 국가 단독 대응의 한계와 국제 협력 필요성: 하이브리드 위협은 전통적 군사력만으로 대응하기 어려운 복합적 도전으로, NATO-EU는 대응 체계 개선과 공동 훈련, 정보 공유 등을 통해 지역의 회복력을 강화하고자 지속해서 노력하고 있음.[40) 41)]
- 복원력이 최우선 전략임: 하이브리드 위협 대응에서 가장 일반적으로 제안되는 대응책이 바로 복원력 강화로, 이는 사회 통합, 인프라 보안, 투명한 정치 시스템 구축에 기반한다는 점에서 대응의 기본 축으로 강조[42) 43)]

● 하이브리드 위협 대응 경보 체계의 진화

- 하이브리드 위협에 대응하는 데 있어 경보 체계는 핵심적인 요소임. 하이브리드 위협은 모호하고 경계가 불분명하며, 이를 적절히 다룰 수 있는 고정된 기준 이 부족하다는 점이 일반적인 문제로 지적됨. 냉전 시대에 사용되던 지표들은 오늘날의 하이브리드 위협을 신호하는 지표를 충분히 포착하지 못함. 하이브리드 위협에서는 군사적 수단과 비군사적 수단이 다양하게 결합되고, 위협 행위자 또한 매우 다양하기 때문에, 이들을 충분히 이해하고 감시해야만 적절한 경보를 제공할 수 있음. 하이브리드 위협이 '난제(wicked problem)'로 간주되기는 하지만, 하이브리드 위협에 대한 경보 시스템이 불가능한 것은 아님(Rietjens, 2020).
- EU의 하이브리드 위협 대응 네트워크(HYBNET;Empowering a Pan-European Network to Counter Hybrid Threats)가 초기 경보·탐지(Early warning & detection) 역량을 코어 주제로 잡고, AI 활용 프로젝트(예: ALIGNER – 인공지능 로드맵/치안) 등을 연계해 조기 경보·탐지에 AI 도구 도입(EU-HYBNET, 2022)
- 미 연방 감사보고서(OIG)는 "허위정보(disinformation)에 대응하는 효과적인 노력이 없으면, 외국 정부가 선거에 성공적으로 영향력을 행사하고 유권자를 오도하며, 미국인의 선거 시스템 신뢰를 훼손할 수 있다"고 명시. 선거 인프라 보안이 강화되었더라도, 허위정보·외국 영향에 대한 조기 탐지/경보와 대응 체계가 필수라고 강조함. 현재 및 진화하는 위험을 다루어 국가의 선거 인프라의 보안과 복원력을 강화할 수 있도록, 허위정보와 인공지능(AI)의 활용을 포함한 위험 기반의 국가 전략 계획을 수립·시행할 것을 권고(Office of Inspector General, 2024)
- 하이브리드 위협 위기관리는 예방-대비-대응-복구의 단계로 전개되어 왔으나, 최근 하이브리드 위협에서는 AI의 발전이 앞단의 예측(anticipation)·조기경보 기능을 크게 끌어올리고 있어 예측-예방-대비-대응-복구의 진행되는 추세임(라운드테이블 참여 전문가).

34) Hybrid CoE. (n.d.) "Hybrid threats as a concept" (검색일: 2025.6.25.)
35) NATO OTAN. (2024) "Countering hybrid threats" (검색일: 2025.7.5.)
36) Hybrid CoE. (n.d.) "Deterrence and resilience" (검색일: 2025.9.18.)
37) European Commission, (n.d.) "Strengthening EU resilience: hybrid threats and critical entities" (검색일: 2025.9.23.)
38) NATO OTAN. (2024) "Countering hybrid threats" (검색일: 2025.7.5.)
39) The Guardian. (2024) "Undersea 'hybrid warfare' threatens security of 1bn, Nato commander warns" (검색일: 2025.9.30.)
40) Brethous & Kovalčíková (2023) "Next level partnership – Bolstering EU–NATO cooperation to counter hybrid threats in the Western Balkans" (검색일: 2025.8.20.)
41) Zandee *et al.*, 2021
42) KERŠANSKAS, 2020
43) European Commission, (n.d.) "Resilience to Hybrid Threats" (검색일: 2025.7.2.)

2-4-2. 하이브리드 위협 주요 대응 전략

● NATO 하이브리드 위협 대응 전략

- NATO는 2015년 공식적으로 하이브리드 전쟁 대응 전략(NATO's Strategy on Countering Hybrid Warfare)을 발표. 이 전략은 준비(preparedness), 억제(deterrence), 방어(defence) 세 축으로 구성. ①(준비) 회색지대 활동의 식별, 평가, 소통, 귀속(attribution), ②(억제) 사회 복원력 강화, 의사결정 과정 적응, 동맹국들의 대응옵션 확대 ③(방어) 동맹국들의 군사·비군사 대응 역량 강화[44) 45)]

- 2016년 바르샤바 정상회의에서 이 하이브리드 전쟁 대응 전략이 공식 확정되었으며, 하이브리드 전쟁은 "정규·비정규, 공개·은밀한 군사·준군사·민간 수단을 통합적으로 활용하는 복합적이고 적응적인 조합"으로 규정하고 있음. 특히, 사회·인프라 복원력 강화가 억지의 핵심으로 확인되었고, NATO는 지원만 하고 주된 책임은 회원국에 있다는 점도 명시. 중요한 합의 중 하나는 하이브리드 행위도 NATO 집단방위조항(제5조) 발동 사유가 될 수 있다는 점임(Piella, 2022).

- NATO의 하이브리드 위협 대응은 단순한 군사적 차원을 넘어선 다층적(total security) 구조로 발전하고 있는데, 이는 조기 식별(Early Warning) → 방어(Defence) → 억제(Deterrence) → 회복(Resilience) → 국제 협력(International Cooperation)으로 이어지는 총체적 프레임워크임.[46) 47) 48) 49)]

● EU 하이브리드 위협 대응 전략

- 하이브리드 위협에 대응할 일차적 책임은 개별 EU 회원국에 있지만, EU는 이러한 위협에 대응하기 위해 공동으로 조정된 행동도 함께 수행하고 있음.

- EU는 하이브리드 위협을 국가 차원을 넘어서는 복합 안보 도전으로 보고, EU 하이브리드 툴박스(hybrid toolbox)를 마련하였음. 이 툴박스는 예방적·협력적·안정성 구축·제한적·지원적 조치로 구성되어 있음. 예로, FIMI Toolbox는 외부 정보조작(Foreign Information Manipulation & Interference) 대응[50)]

- EU 회원국, 파트너 국가, 그리고 CSDP(공동안보·방위정책) 임무 및 작전을 지원하기 위해 하이브리드 신속 대응팀(hybrid rapid response teams)을 마련함.[51)]

- EU는 하이브리드 위협을 "국가 차원을 넘어서는 복합 안보 도전"으로 규정하고, ① 하이브리드 Toolbox(정책·외교·제재·사이버 수단), ② 전담 조직(HFC·신속 대응팀), ③ 국제 협력(EU-NATO·파트너국 지원) 이라는 3축 체계를 중심으로 대응 전략을 운영하고 있음.

44) NATO OTAN. (2024) "Countering hybrid threats" (검색일: 2025.7.5.)
45) Piella (2022) "NATO's strategies for responding to hybrid conflicts" (검색일: 2025.6.27.)
46) Maciata (2025) "Fortifying the Baltic Sea – NATO's defence and deterrence strategy for hybrid threats" (검색일: 2025.10.5.)
47) NATO OTAN. (2024) "Countering hybrid threats" (검색일: 2025.7.5.)
48) Brethous & Kovalčíková (2023) "Next level partnership – Bolstering EU–NATO cooperation to counter hybrid threats in the Western Balkans" (검색일: 2025.8.20.)
49) NIKOLOV (2018)
50) European Council. (n.d.) "Hybrid threats" (검색일: 2025.6.19.)
51) European Council. (n.d.) "Hybrid threats" (검색일: 2025.6.19.)

- EU는 하이브리드 위협을 단순 군사 문제가 아니라 민간, 정부, 산업, 사회 전반을 아우르는 복합적 도전으로 정의하고 있고, 따라서 전(全)정부(All-of-Government) 및 전(全)사회(All-of-Society) 차원의 포괄적 대응을 지향[52) 53)]

● 헤이그 전략연구센터(HCSS) 대(對)하이브리드 대응 프레임워크

- 라이벌 국가들은 점점 더 하이브리드 전술을 사용하여 민주적 절차에 영향을 미치고 상대의 취약성을 악용하고 있으며, 이러한 전술에는 전통적인 무력 충돌의 문턱 아래에서 폭력적·비폭력적 권력 수단을 조정되고 동기화된 방식으로 동원하는 것이 포함되며, 종종 탐지와 귀속을 회피하고 있음.빠르게 진전되는 기술 발전과 심화된 글로벌 상호 연결성은 이러한 국가들에게 놀라운 도구를 제공하고 있는데, 최근 서방 정부들은 상황 인식을 점진적으로 강화하고, 하이브리드 위협으로 인한 피해를 최소화하기 위한 역량을 개발해 오고 있음. 나아가, 단순히 회복력을 높이고 방어를 강화하는 것을 넘어, 억지 조치를 통해 적대국의 행동을 적극적으로 변화시키기 위한 다양한 정책을 시행하기 시작했음(Bertolini *et al.*, 2023).

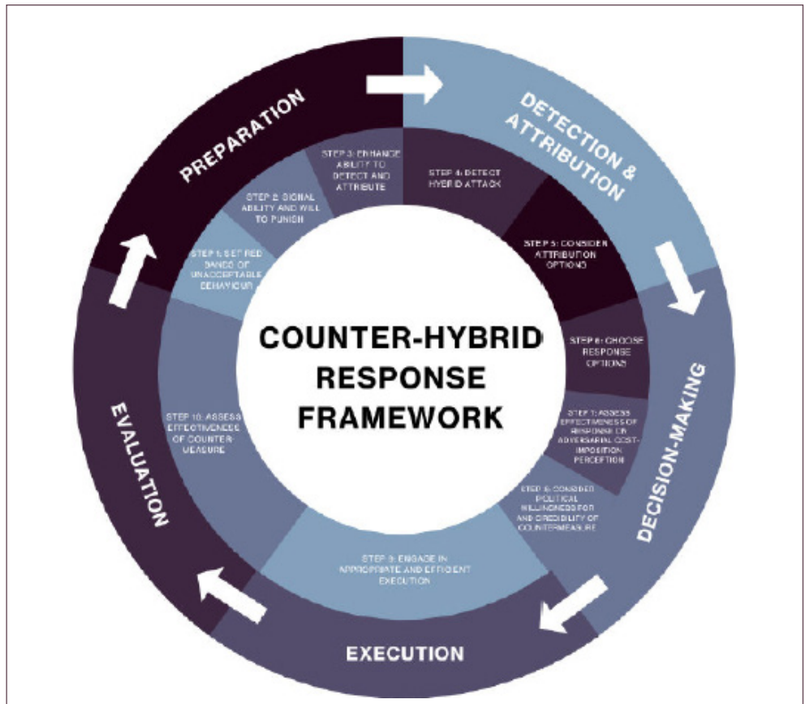
- Bertolini *et al.* (2023)는 하이브리드 위협에 대응하기 위한 다양한 혁신적노력에도 불구하고, 하이브리드 가해자를 억지하는 것이 어려운 이유들을 제시. 첫째, 하이브리드 행위자는 고의적으로 탐지를 회피하고 책임 회피. 둘째, 용인 가능한 행동을 규율하는 명확한 공유 규칙이 없음. 셋째, 방어 측은 대응할 역량이나 의지가 부족. 넷째, 방어 측은 상대방의 유인 구조와 취약 지점을 제대로 이해하지 못해, 효과적이고 맞춤화된 정책을 설계하지 못함. 또한 방어 측은 사전에 대응 정책을 설득력 있게 전달하지 못함. 다섯째, 대응 정책의 설계와 실행은 종종 즉각적으로 드러나지 않는 2차·3차 파급효과를 동반함.

- 헤이그 전략연구센터는 하이브리드 대응 프레임워크(Counter-Hybrid Response Framework) 제안. 하이브리드 대응 프레임워크 5단계 구조는 ① 준비 단계(Preparation Stage), ② 탐지 및 귀속 단계(Detection & Attribution Stage), ③ 의사결정 단계(Decision-Making Stage), ④ 실행 단계(Execution Stage), ⑤ 평가 단계(Evaluation Stage)로 구성됨. 각 단계에는 구체적인 실행 조치가 포함되어 있고 이 프레임워크는 순환 구조를 가지며, 향후 대(對)하이브리드 조치를 지속적으로 개선하기 위한 피드백 루프를 포함하고 있음. 다섯 단계는 편의를 위해 열 가지 세부 단계로 다시 구분되며, 정책결정자들이 대응 방향을 설정하는 데 도움이 되는 통찰을 제공하는 것을 목표하고 있음(Bertolini *et al.*, 2023).

52) EUDefence StrategicCompass. (2024) "COUNTERING HYBRID THREATS" (검색일: 2025.9.24.)
53) European Commission (2016) Joint Framework on countering hybrid threats

그림 5. 5단계·10절차 하이브리드 대응 프레임워크의 피드백 메커니즘

출처: Bertolini *et al.* (2023)



- 비록 용납할 수 없는 행위의 '레드라인(red bands)'을 설정하더라도, 적대 세력이 이를 넘어설 수 있다고 가정하며, 대(對)하이브리드 태세를 구축하는 목표는 상대방의 전략적 행동을 장기적으로 형성하고, 개선된 전략 환경을 마련하는 누적적 억제를 달성하는 데 있음.

표 6. 대응 프레임워크 각 단계별로 요구되는 활동

Stage	Step	Actions
① 준비 단계 (Preparation Stage)	1단계: 용인할 수 없는 행동의 'Red Bands (경계선)'을 설정하라	1. 적대적 하이브리드 작전의 범위를 그 영향에 따라 분석하고, 어떤 것이 대응을 촉발할 것인지 표시 2. 용인할 수 없는 행위의 Red Bands(경계선)를 설정 3. 용인할 수 없는 행위의 Red Bands를 내부적으로, 파트너들과, 그리고 경우에 따라서는 적대 세력과도 공유 4. 안심 제공, 인센티브, 규범 설정(norm-setting)을 통해 긍정적인 행동을 장려
	2단계: 처벌 능력과 처벌 의지를 명확히 표명하라	5. 억지 약속을 이행할 능력과 의지를 신호하라. 이는 능력의 시연과 의지의 발표를 통해 가능
	3단계: 탐지(detect)와 귀속(attribution) 능력을 강화하라	6. 탐지 능력을 향상 7. 정치적으로 의미 있는 시한 내에 귀속 능력을 강화 8. 귀속 결과를 제3자에게 설득력 있게 설명할 준비
② 탐지 및 귀속 단계 (Detection & Attribution Stage)	4단계: 하이브리드 공격을 탐지하라	9. 하이브리드 공격을 탐지
	5단계: 귀속 옵션을 고려하라	10. 귀속할지 여부를 결정(하이브리드 위협이나 공격이 발생했을 때, 행위자를 특정할지 말지를 정치적·전략적 맥락에서 먼저 판단) 11. 효과적인 방식으로 귀속
③ 의사결정 단계 (Decision-Making Stage)	6단계: 대응 옵션을 선택하라	12. DIMEFIL 스펙트럼(외교·정보·군사·경제·금융·정보·법률)에 따른 사용 가능한 대응책을 그 영향력에 따라 분석 13. 대응 목표(타깃)를 다중 도메인에서 식별 — 여기에는 반력(군사·전력) 목표, 가치(경제·사회) 목표, 정치적 목표가 포함 14. 대응 옵션의 법적 정당성을 평가 15. 각 대응책이 발효되는 시점과 지속기간을 평가 16. 대응책의 비례성(비례원칙)을 고려하라. 17. 연계(얽힘) 요소 및 2차·3차 영향(부작용)을 식별 18. 에스컬레이션(확전) 가능성 평가를 수행
	7단계: 대응 조치가 적에게 비용부과(손실부과)로 인식되는지의 효과를 평가하라	19. 심리적 수준에서의 비용을 조사 20. 정치적 수준에서의 비용을 조사 21. 경제적 및 작전적 수준에서의 비용을 조사
	8단계: 대응 조치의 정치적 수용 가능성과 실행 신뢰성을 평가하라	22. 상대방의 시각에서 대응 조치의 신뢰성을 평가 23. 해당 대응 조치를 채택하려는 정치적 의지를 평가 24. 국내적 대응 노력을 동기화하고 조율: 범정부적 및 범사회적 접근 25. 국제적 대응 노력을 동기화하고 조율
④ 실행 단계 (Execution Stage)	9단계: 대응 방안을 실행하고, 대응 조치를 이행하라.	26. 핵심 이익과 처벌 위협을 고려하여 시기적절한 경고 대응을 시행 27. 국내외의 지지 상황을 모니터링 28. 전략적 목표를 중심에 두어라. 29. 정부 전반에 걸친 다층적 전략 커뮤니케이션(StratCom)을 동기화되고 조율된 방식으로 실행
⑤ 평가 단계 (Evaluation Stage)	10단계: 대응 조치의 효과성을 평가하라	30. 비용 부과 목표의 달성 여부를 평가 31. (상황의) 확산 및 고조(에스컬레이션) 동향을 평가 32. 2차 및 3차 효과를 평가

2-4-3. 회복력(Resilience)

● 회복력의 전략적 의미

- 회복력(resilience)은 억제·방어의 선결 조건임. 하이브리드 공격이 임계 기능(전력·통신·교통, 정책결정, 사회신뢰)을 노리기 때문에, 충격을 흡수·격리·복구하는 능력 자체가 공격의 기대효용을 낮추는 사전적 억제로 작동하게 됨.[54)]

- 디스인포·사이버공격·경제강압은 임계값 아래에서 점진적으로 축적되어, 전통적 '공격-보복' 억제가 어려워, 피해를 최소화하고 기능을 유지·복구하는 흡수·적응 능력이 정책의

54) NATO OTAN. (2024) "Resilience, civil preparedness and Article 3" (검색일: 2025.8.19.)

중심축으로 이동(Giannopoulos *et al.*, 2021)

- 하이브리드 공격이 임계기능(전력·통신·정치 의사결정 등)을 노리는 만큼 "버티고 빨리 복구하는 능력"이 곧 억제력의 일부라는 논리(Monaghan, 2022; European Commission, 2023)

● 하이브리드 위협에 대한 핵심 사회기반 시설의 복원 능력의 중요성

- 하이브리드 위협은 전통적인 군사력보다는 사이버 공격, 정보 조작, 사회분열, 에너지 압박, 공급망 교란 등의 비가시적·비군사적 수단을 결합해 공격하며(NATO OTAN, 2022), 이들은 전시가 아닌 평시에도 작동하며, '임계 기능'(critical functions)을 마비시켜 사회적 혼란과 제도 불신을 유도함. 즉, 하이브리드 위협은 인프라와 사회 기반 기능을 복합 위협으로 겨냥함.
- 하이브리드 공격은 완벽하게 막을 수 없는데, 따라서 중요한 것은 "공격 이후에도 빠르게 기능을 복구하는 능력"임. 이러한 회복력이 강하면, 공격자는 정치·전략적 효과를 얻기 어려워지고, 재시도에 대한 유인이 줄어듦. 이는 "억제(denial)" 전략, 즉 공격의 실익(정치적·전략적 효과)을 박탈함으로써 상대의 선택지를 제한하는 억제 개념임(Monaghan, 2022; Bertolini *et al.*, 2023).
- 하이브리드 위협에 대응하는 핵심 사회기반 시설(Critical Infrastructure, CI)의 복원 능력(resilience)은 단순한 재난 대비 차원을 넘어, 복합적이고 지속적인 공격 속에서도 필수 기능을 유지·복구하는 능력을 의미함. 이는 국가 안보와 억제력의 기반 역할을 의미
- 인프라는 물리적 시설, 정보기술, 통신망, 공급망 등으로 정의되며, 이들의 손상이나 파괴는 국가의 사회적·경제적 안녕에 위험을 초래할 수 있으며(호주 정부, 2015), 유엔(UN)은 회복력 있는 인프라를 "예측 가능한 사건이든 예측 불가능한 사건이든, 교란 사건으로부터 견디고, 적응하며, 신속하게 회복할 수 있는 인프라"로 정의(Hammad and Haddad, 2021)
- 복원 능력(Resilience)이란 예상치 못한 충격(사이버·물리·정보·경제 등)에도 핵심 기능을 흡수(absorb) → 적응(adapt) → 복구(recover) 하는 역량으로(National Infrastructure Advisory Council, 2009), 이는 복원력이 단일 대응이 아니라 지속 가능한 시스템 역량임을 보여주며, 하이브리드 위협처럼 예측 불가능하고 복합적인 상황에서 핵심 기반 시설의 안정성을 지키는 데 필수적임을 보여 주고 있음.

● NATO는 사회·국가 차원의 회복력을 "신뢰할 만한 억제·방어의 필수 기반"으로 규정하고, 동맹의 7대 회복력 기준(에너지·통신·교통·식량/물·의료·정부기능·군사 지원)을 제시해 국가·연합 차원의 대비[55]

- NATO는 '회복력 기반의 억제력(Resilience-Based Deterrence)' 개념을 제시, 버티고 빠르게 복구하는 능력이 곧 억제력의 일부로 작동한다는 전략적 관점을 취하고 있음.
- 회복력 기반 억제력은 하이브리드 위협이 전통적인 군사적 충돌이 아닌, 임계값 아래에서 전개된다는 점에 주목하여 등장한 새로운 억제 전략 개념으로, 이러한 위협은 전력망, 통신망, 정책 결정 과정, 시민 여론 등 민간 사회의 임계 기능을 점진적·비가시적으로 약화시키는 방식으로 나타나며, 통상적인 군사력 기반의 억제(예: 보복 위협)만으로는 사전에 차단하거나 대응하기 어려워 전략적 접근이 필요함.
- NATO는 하이브리드 위협과 전통적 군사적 위협 모두에 효과적으로 대응하기 위해, 국가 및 사회 차원의 회복력을 "신뢰할 수 있는 억제 및 방어의 필수 기반"이라고 명시하고 있으며, 이를 위해 7대 회복력 기준(Seven Baseline Requirements for Resilience)을 제시
- NATO는 회복력, 민간 대비, 민군 협력에 점점 더 많은 비중을 두고 있으며, 이러한 요소들은 동맹의 집단방위와 억지력의 핵심 요소로 점점 더 중요하게 간주되고 있음.[56]
- 2023년 정상회의에서 NATO는 회복력에 관한 공통의 동맹 목표를 채택, 목표들은 주로 2016년과 2021년에 마련된 NATO의 회복력 기본 기대치를 기반으로 ①국가 관리 체계의 연속성 보장, ②견고한 전력 공급 보장, ③통제되지 않은 인구 이동에 대응할 수 있는 역량 확보, ④견고한 식량 및 식수 공급 보장, ⑤대규모 인명 피해에 대응할 수 있는 역량 확보, ⑥견고한 민간 통신 체계 보장, ⑦회복탄력적인 교통 체계 확보 등 설정[57) 58)]

표 7. NATO 7대 회복력 기준 (Baseline Requirements)
출처: NATO[59) 60)] and CCOE[61)]

기존 항목	주요 내용
① 정부 및 핵심 공공 서비스의 연속성 보장	위기 상황에서도 결정을 내리고 국민과 소통할 수 있는 능력을 유지하는 것 예시: 위기 시 대체 지휘부, 비상대피 계획, 행정 데이터 백업 시스템, 분산형 행정구조 등
② 에너지 공급의 회복력 확보	에너지 공급의 지속성 보장 및 공급 차질에 대비한 백업 계획 수립 예시: 비상 연료 저장소, 자국 내 발전시설 확보, 다중 공급망 계약, 사이버보안 강화
③ 통제되지 않은 인구 이동에 대한 효과적 대응 능력	난민, 피난민 등 예기치 못한 인구 이동에 효과적으로 대응하고 대규모 인구 이동이 NATO의 군사 배치와 충돌하지 않도록 관리하는 능력 예시: 접경지 난민캠프 계획, 이중국적자 위험평가, 생체정보 등록 시스템
④ 식량 및 식수 자원의 회복력	공급망이 방해나 파괴 없이 유지될 수 있도록 안전하게 확보 예시: 국가 비축 식량·식수, 정수설비 보완, 공급망 다변화
⑤ 대량 사상자 및 보건 위기에 대한 대응 능력	민간 보건 시스템이 위기 상황을 감당할 수 있어야 하며, 충분한 의료물자 확보 및 보관 체계가 마련되어야 함 예시: 임시 병상/의료인력 확보, 전략의약품 비축, 민군의료 협력 체계
⑥ 민간 통신 시스템의 회복력	통신 및 사이버 네트워크가 위기 상황에서도 작동 가능해야 하며, 백업 기능이 확보되어야 함 특히 5G를 포함한 통신 인프라, 위기 시 복구 수단, 국가기관 우선접속 보장, 위험요소의 정기 평가 등이 포함됨 예시: 위성통신 백업망, 암호화된 위기 대응 채널, 긴급경보시스템(공공경보).
⑦ 수송 시스템의 회복력	NATO 병력이 동맹국 영토 내를 신속히 이동할 수 있고, 민간 서비스도 위기 속에서 수송망에 의존할 수 있도록 해야 함 예시: 군민겸용 항만·공항, 대체 노선 확보, 위기 시 우선 운송 프로토콜

55) NATO OTAN. (2024) "Resilience, civil preparedness and Article 3" (검색일: 2025.8.19.)
56) NATO OTAN. (2024) "Resilience, civil preparedness and Article 3" (검색일: 2025.8.19.)
57) NATO OTAN. (2024) "Resilience, civil preparedness and Article 3" (검색일: 2025.8.19.)
58) Roepke & Thankey (2019) "Resilience: the first line of defence" (검색일: 2025.10.4)
59) NATO OTAN. (2024) "Resilience, civil preparedness and Article 3" (검색일: 2025.8.19.)
60) Roepke & Thankey (2019) "Resilience: the first line of defence" (검색일: 2025.10.4)
61) Civil-Military Cooperation Centre of Excellence(CCOE). (n.d.) "Seven baseline requirements" (검색일: 2025.7.9.)

● 하이브리드 위협 대응 전략에서 시민 교육, 사이버 방어, 민군 통합 대응 역량 강화는 NATO와 EU 등 국제기구 및 주요 정책 연구기관들이 강조하는 복원력 강화의 핵심 축 들임.

- 하이브리드 위협 맥락에서 시민 교육, 사이버 방어, 민군 통합 대응 역량 강화를 복원 전략으로 제시[62) 63)]
- 시민 교육 (Civic Education & Media Literacy) 강화를 통해 허위정보, 정치적 공작, 외부 선동에 대한 인식 제고 및 면역력 강화(Anagnostakis, 2023)
- 국가 기반 시스템에 대한 사이버 공격 탐지·방어 및 회복 능력 제고 필요(Klimburg, 2012; European Union Agency for Cybersecurity, 2025)
- 민관 협력 체계 구축 필요, 운영기관·정부·국제 파트너 간 위기관리 네트워크 구축과 비밀 등급·민간 데이터 간 안전한 정보 공유 프로토콜 마련 필요[64)]
- 복원 능력 강화는 기술적 보안-사회적 신뢰-조직적 적응을 통합해야 하며, NATO/EU가 강조하는 것처럼 국가 단독이 아닌 다층·다국적 협력이 필수[65)]

62) NATO OTAN. (2024) “Cyber defence” (검색일: 2025.9.26.)
63) NATO OTAN. (2024) “Countering hybrid threats” (검색일: 2025.7.5.)
64) EUDefence StrategicCompass. (2024) “COUNTERING HYBRID THREATS” (검색일: 2025.9.24.)
65) NATO OTAN. (2024) “Countering hybrid threats” (검색일: 2025.7.5.)

Exploration of Emerging Technology-Driven Challenges &
Emerging International Security Issues and
Global Security Collaboration

3 신기술과 안보

3. 신기술과 안보

3-1. 주요 신기술 분야별 최신 안보 동향

3-1-1. 인공지능

● AI-강화 피싱(phishing)·보이스피싱(vishing)·멀웨어(malware) 확산

그림 6. 여행사 웹사이트를 위조한 피싱 웹페이지

출처: Altukhov (2025) "New trends in phishing and scams: how AI and social media are changing the game" (검색일: 2025.9.25.)

- 보안 솔루션 전문업체 카스퍼스키(Kaspersky)는 2025년 위협 보고서에서, 피싱·사기 공격이 단순 텍스트에서 벗어나 딥페이크 영상, 음성복제(voice cloning), 다중단계 사회공학 등과 결합하여 진화했다고 분석하였음. 이는 2단계 인증(2FA) 우회, 생체정보 탈취 등 전통적인 보안 메커니즘을 위협하는 결과를 낳았음.[66]
- IBM X-Force는 2025년 보고서에서 인포스틸러(infostealer) 공격이 2024년에 전년 대비 84% 증가했고, 2025년 들어서는 주간 기준으로 2023년에 비해 약 180% 증가 조짐을 보인다고 발표하였음. 이는 공격자가 AI를 통해 대규모 공격 자동화를 실현하고 있음을 시사함(IBM X-Force, 2025).
- 보안 전문 기업 Proofpoint는 사이버 범죄자들이 AI 웹사이트 생성 플랫폼 'Lovable'을 악용해 자격 증명 피싱(credential phishing), 멀웨어(malware) 배포, 암호화폐 지갑 탈취 사이트 등을 손쉽게 제작·호스팅하고 있다고 보고했음. 공격자들은 유명 브랜드를 사칭한 가짜 사이트를 만들고, CAPTCHA를 통해 필터링한 뒤 피해자의 로그인 정보나 금융 정보를 수집하여 텔레그램(Telegram)으로 유출하는 수법을 사용하였음. Proofpoint는 "웹 개발 지식이 거의 없어도 AI 서비스 덕분에 범죄 진입 장벽이 크게 낮아졌다"고 평가하며, Lovable 측이 2025년 하반기부터 실시간 탐지와 자동 스캐닝 기능을 도입했다고 전함.[67]

66) Altukhov (2025) "New trends in phishing and scams: how AI and social media are changing the game" (검색일: 2025.9.25.)
67) Proofpoint. (2025) "Cybercriminals abuse AI website creation app for phishing" (검색일: 2025.8.19.)

● AI 시스템 자체 보안: 프롬프트 인젝션(prompt injection)·툴/에이전트 독성(tool poisoning)·데이터 포이즈닝(data poisoning)

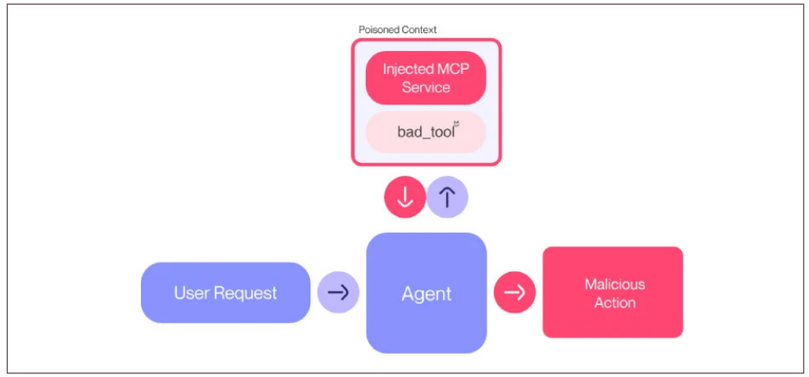


그림 7. 프롬프트 인젝션 공격의 프레임워크

출처: Lakshmanan (2025) "New Reports Uncover Jailbreaks, Unsafe Code, and Data Theft Risks in Leading AI Systems" (검색일: 2025.9.3.)

- 2025년 8월, 레노버 고객지원 챗봇에서 프롬프트 인젝션을 통해 XSS와 세션하이재킹까지 연계될 수 있는 취약점이 발견되었음. 이는 언어 모델 기반 서비스가 기존 웹 취약성과 결합할 경우 심각한 보안 위협이 될 수 있음을 보여줌.[68]
- OWASP GenAI 프로젝트는 2025년 툴 포이즈닝(tool poisoning) 사고 사례를 정리하며, 플러그인 설명이나 메타데이터에 삽입된 악성 지시가 무단 지시 실행을 유발할 수 있다고 경고하였음. 또한 LLM 공급망(supply chain) 위험과 데이터 포이즈닝을 주요 리스크로 지목하였음.[69]
- 2025년 보안 연구자들은 악성 AI 모델이 배포 경로에 섞여 백도어를 삽입하는 AI 공급망 공격(AI supply-chain attack) 가능성을 실증하였음. 이에 따라 모델의 출처 검증(model provenance)과 서명 기반 배포 체계가 중요한 보안 과제로 부상하였음(Sood, 2025).

● 자율살상무기체계(LAWS, Lethal Autonomous Weapons Systems) 최근 동향

- UN 사무총장 보고서 A/79/88(2024): 각국과 국제기구 의견을 모아 자율무기 문제가 사람의 최종 통제 보장, 전시 민간인 보호, 책임소재 명확화에 걸쳐 있음을 정리하고, 국가별 사전 법검토 제도 강화와 새 국제규범 또는 정치적 선언 등 여러 대안을 병렬로 제시함(UN, 2024a).
- CCW 정부전문가그룹 작업문서 WP.10(2024): 10개국 공동 초안으로 자율무기의 사용을 '본질적으로 금지할 범주'와 '조건부 허용할 범주'로 나누고, 표적 구분·과도한 피해 방지 같은 전쟁법 원칙을 실제 운용 요건으로 풀어쓴 조문 틀을 제시하여 협상의 기준점을 마련함(UN, 2024b).

68) Woollacott (2025) "Flaw in Lenovo's customer service AI chatbot could let hackers run malicious code, breach networks" (검색일: 2025.9.25.)
69) Clinton (2025) "OWASP Gen AI Incident & Exploit Round-up, Q2'25" (검색일: 2025.9.29.)

- SIPRI 정책보고서(2024): 실제 상황을 가정한 시나리오 연습 결과를 바탕으로 위원회 협상에 적용할 수 있는 이원 규제 설계를 구체화하고, 금지 목록과 조건부 허용 시 필요한 안전성·검증·책임 요건을 '메뉴형 요소'로 제시하여 국가들이 단계적으로 조합해 채택할 수 있도록 안내함(Laura, 2024).

3-1-2. 양자

● 양자 분야 주요 안보 이슈

- Quantum Threat Timeline Report(2024)에 따르면, 양자컴퓨터 기술 발전을 둘러싼 글로벌 경쟁은 사이버보안에 중대한 도전 과제를 제기하고 있음. 가까운 미래에 양자컴퓨터가 기존 표준 암호화 프로토콜을 무력화할 수준으로 강력해질 것으로 전망되며, 이에 따라 암호체계를 양자 공격에 견딜 수 있도록 업데이트하지 못한 조직들에서 심각한 보안 문제가 초래할 수 있다는 전문가들의 견해가 증가하고 있음(Mosca & Piani, 2024).
- 양자 기술의 발전은 보안·정보전·전략적 억지체계에 새로운 변수로 작용하고 있으며, "Harvest now, decrypt later" 전략은 그 중에서도 양자 컴퓨터 시대의 사이버·정보 안보 핵심 이슈와 직결. 공격자가 현재(양자 컴퓨터가 실용화되기 전)에 암호화된 데이터를 수집해서 저장해 두었다가, 양자 컴퓨터가 등장하면 나중에 복호화(decrypt)하려는 '수확 → 나중에 복호화' 전략이 경고되고 있음. 이로 인해 저장 중인 민감 정보가 미래에 위험에 노출될 수 있음.[70]
- 미국은 국립표준기술연구소(NIST)를 통해 포스트 양자 암호(Post-Quantum Cryptography, PQC)에 대해 체계적이고 표준 우선적인 접근법을 취해 왔음. 2024년 8월, NIST는 세계 최초의 PQC 표준을 공식화하여, 전 세계 조직들이 활용할 수 있는 기반을 마련함. 이 표준은 인증을 위한 디지털 서명과 안전한 통신 채널을 위한 키 캡슐화 메커니즘(Key-Encapsulation Mechanisms)을 포함한 세 가지 양자 내성 알고리즘으로 구성되어 있음.[71]

● 국가 간/산업 간 경쟁 및 전략적 우위 확보를 위한 양자 기술 선도 경쟁

- 양자 컴퓨터 및 양자 기술(quantum sensing, quantum communication 등)에 대한 경쟁이 단순한 기술 경쟁을 넘어 국가안보, 정보우위, 암호깨기 능력, 정보 수집 능력 등의 전략적 우위(strategic advantage) 확보 수단으로 인식됨. 양자 기술 선도 경쟁은 단순한 과학적 자랑이 아니라 경제적 리더십, 군사력, 사이버보안, 규칙 제정 권한에 직결되는 문제임.[72]
- 양자컴퓨팅은 단순히 더 빠른 컴퓨터를 의미하는 것이 아니라, 이는 광범위한 지정학적 함의를 가진 패러다임으로의 전환을 의미함. "누구든 양자컴퓨팅을 먼저 개발하는 국가는 암호학, 탐지, 정보처리에서 명백한 군사적 우위를 가지게 될 것"으로, 이제 양자기술은 암호 해독을 넘어 직접적인 군사적 응용의 예들도 갖고 있음. 양자 센싱의 경우 탐지 능력을 크게 향상시킬 수 있는데, 예를 들어 잠수함이나 스텔스 항공기를 미세한 중력 또는 자기 이상을 감지해 탐지할 수 있어 전통적인 스텔스 및 2차 보복 능력을 무력화할 수 있어 이러한 발전은 군사적 균형을 흔들 수 있음.[73]

3-1-3. 사이버 보안

● 복합적 위협 확산

- **내부자(insider) 위협의 고도화**: 사용자 권한을 악용하거나 위장해 합법적 활동처럼 보이도록 하는 공격이 증가, 조직 내부 계정 탈취와 권한 상승을 결합한 정교한 침투가 확대됨(최정완, 2024).
- **공격 자동화·지능화**: 악성코드(Malware-as-a-Service), 봇넷 자동화, 취약점 스캐닝 툴 등이 발전하면서 탐지 회피형 대규모 공격이 가능해졌고, 이는 단일 기술이 아니라 사이버 도메인 내 자동화·오케스트레이션 기술 발전과 연계됨.
- **사이버 전술과 물리적 교란의 융합**: 중요 인프라를 겨냥한 사이버-물리적(hybrid) 작전이 현실화되면서, 전력·교통·의료 등 운영기술(OT)을 포함한 통합 보안 거버넌스가 요구됨(이세훈 & 이승훈, 2024).
- **종합적 전략적 고려 필요**: 사이버 작전은 단일 침투가 아니라, 심리전·정보전·물리적 교란을 동시 운용하는 복합 전략이므로, 군사 대비·외교·법제도 강화·전문 인력 양성·대국민 인식 제고가 모두 병행되어야 함(서예령 & 이재우, 2021).

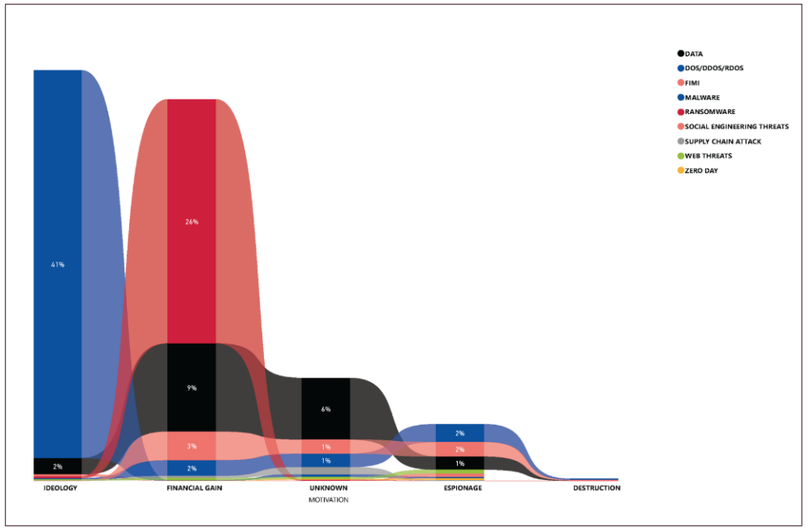


그림 8. 위협 행위자의 동기별 위협 범주
출처: ENISA (2024)

70) Wikipedia. (n.d.) "Harvest now, decrypt later" (검색일: 2025.8.13.)
71) Sanchez (2025) "Regional Approaches To Post-Quantum Cryptography" (검색일: 2025.9.1.)
72) Ivezic (2025) "Quantum Geopolitics: The Global Race for Quantum Computing" (검색일: 2025.9.27.)
73) Ivezic (2025) "Quantum Geopolitics: The Global Race for Quantum Computing" (검색일: 2025.9.27.)

● 위협 대응 체계: 수동 방어에서 전체 시스템 회복력으로

- 전략적 리더십 전환: 기존 “침입 차단 중심”을 넘어, 내부자 위협 조기 탐지, 침해사고 대응 자동화, 공급망 보안(supply chain security) 및 운영기술(OT) 방호를 아우르는 복원력 중심 전략 필요(정태진, 2024)
- 거버넌스 및 규제 정비: 사이버 보안은 단순 기술 운영을 넘어, 위험 정보 공유, 민관 거버넌스, 규제·표준 동기화를 통한 위험 기반 관리(risk-based management)로 확장돼야 함(류지선&박정호, 2023).
- 암호·통신 체계 보호: 미래 양자 환경을 대비해 암호 체계를 점진적으로 전환하되, 이는 사이버 보안의 기반 인프라 차원에서 관리돼야 하며, 인공지능 분야에서 논의되는 위협과 별개로 암호·통신 레이어의 방어 정책으로 자리매김해야 함.

그림 9. 2025년 보안 운영 하이프 사이클의 3가지 핵심 주제

출처: Gartner “Hype Cycle for Security Operations, 2025 ”이글려코퍼레이션 재구성

● 국제협력 및 공동 대응 체계 중요성

- 복잡한 사이버 환경 대응: 사이버 범죄는 특정 기관의 업무를 넘어서 국가와 산업 구분 없이 정보 공유 및 공동 대응의 중요성을 필요로 하고 있는 바, 단일 주체만으로는 새로운 위협을 차단하기 어려움.
- 국경 초월 공격 대응: 사이버 위협이 기반시설·기업·민간 부문 전반으로 확산됨에 따라, 신뢰할 수 있는 국제 공동대응 체계 구축은 필수 전략으로 간주됨(KISA, 2024).
- 글로벌 협력 심화: UN Global Mechanism 출범으로 사이버 규범·국제법 준수·능력 강화·신뢰 구축을 위한 기반이 마련됐으며, EU 역시 회원국 간 공동대응 표준화 및 위기대응 일원화를 추진 중임(송태은, 2021).
- 최근 보안 운영의 초점이 개별 위협 대응을 넘어 노출 관리와 선제적 대응 체계로 전환되고 있는 추세이며(그림 10), 특히 AI 활용 확대와 국제적 협력 기반의 위협 탐지·대응 강화가 향후 사이버 거버넌스의 핵심 방향임을 시사하는 바, 단편적 기술 대응보다 지속적 위험 관리와 통합적 보안 운영 역량 강화가 중요해지고 있음을 확인할 수 있음(그림 11, 그림 12).

그림10. 지속적 위협 노출 관리: 5단계 순환 체계

출처: Gartner. (n.d.) “Cybersecurity Insights & Trends” (검색일: 2025.9.19.)

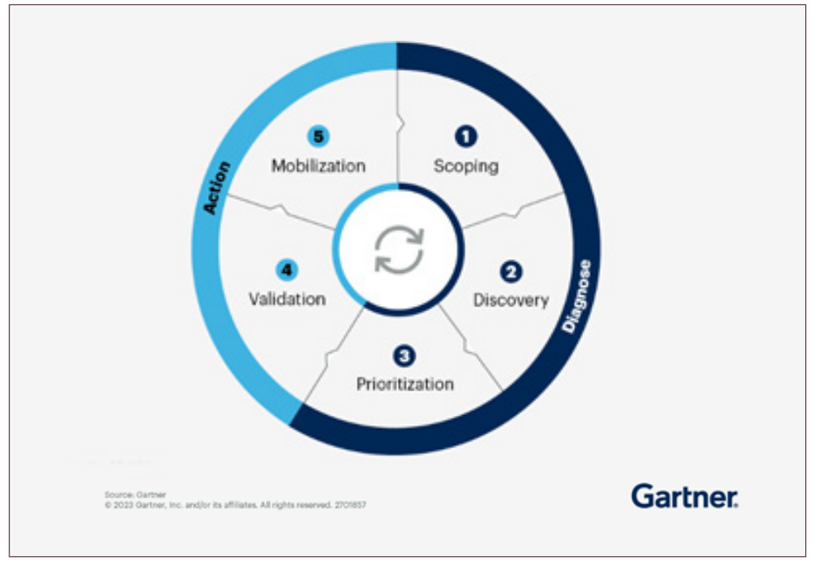
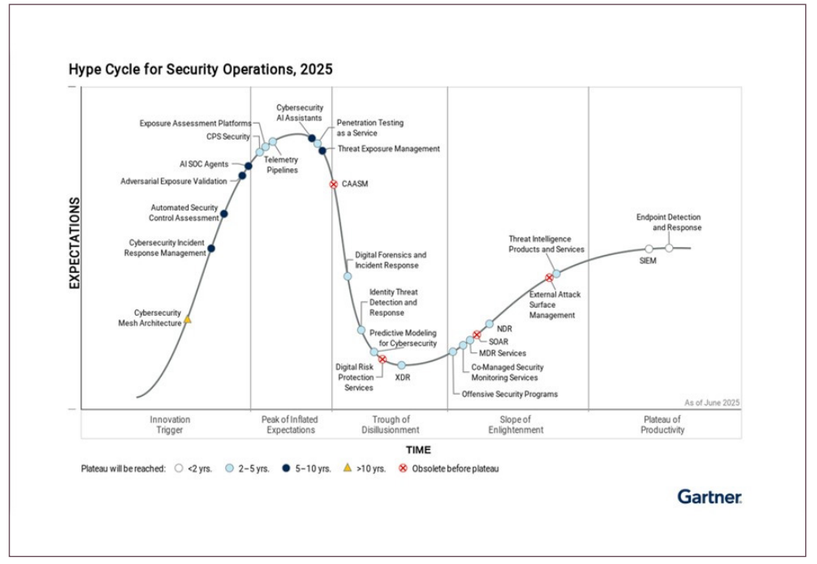


그림 11. 2025년 보안 운영 하이프 사이클

출처: Gartner (2025)



'25년 신규 추가: 파란색 / '24년 제외: 빨간색

구분	발생기		버블기
'25년	• Cybersecurity Mesh Architecture • Cybersecurity Incident Response Management • Automated Security Control Assessment	• Adversarial Exposure Validation • AI SOC Agents	• CPS Security • Exposure Assessment Platforms • Telemetry Pipelines • Cybersecurity AI Assistants • Penetration Testing as a Service • Threat Exposure Management
'24년	• Automated Security Control Assessment(ASCA) • Cybersecurity Mesh Architecture(CSMA) • Cybersecurity AI Assistants	• Adversarial Exposure Validation • Exposure Assessment Platforms • Telemetry Pipelines	• CPS Security • CAASM • Penetration Testing as a Service • Threat Exposure Management • Security Service Edge(SSE)
구분	환멸기	계몽기	안정기
'25년	• CAASM • Digital Forensics and Incident Response • Predictive Modeling for Cybersecurity • Digital Risk Protection Services • XDR	• Offensive Security Programs • Co-Managed Security Monitoring Services • MDR Services • SOAR • NDR • External Attack Surface Management • Threat Intelligence Products and Services	• SIEM • Endpoint Detection and Response
'24년	• Digital Forensics and Incident Response(DFIR) • Digital Risk Protection Services(DRPS) • External Attack Surface Management(EASM) • Identity Threat Detection and Response(ITDR) • XDR • SOAR	• Co-Managed Security Monitoring Services • MDR Services • NDR • Threat Intelligence Products and Services	• SIEM • Endpoint Detection and Response(EDR)

그림 12. 2024, 2025년도 보안 운영 하이프 사이클 속 기술 비교

출처: Gartner (2025)

3-1-4. 우주

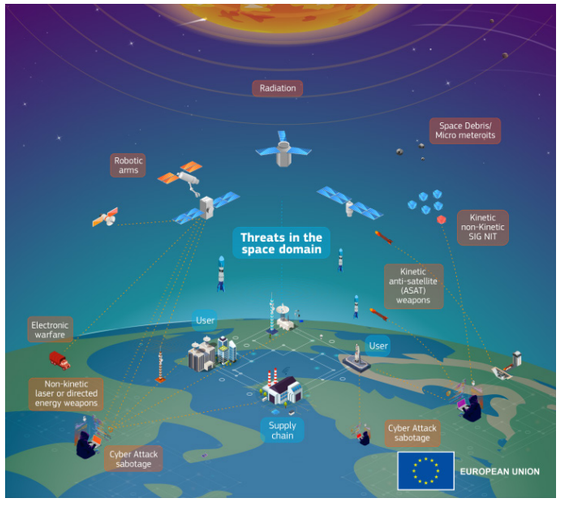


그림 13. 우주 도메인에서의 위협들

출처: European Commission. (n.d.) "Strengthening EU resilience: hybrid threats and critical entities" (검색일: 2025.9.23.)

● 우주 시스템 위협 증대 현황

- 위성, 궤도 인프라, 우주·지상 통신망 등이 국가의 군사·상업·과학 용도로 점점 의존도가 높아짐에 따라 공격 표적으로서의 매력 증가[74]
- 우주 시스템들이 많은 부분 디지털화 및 네트워크화됨으로써 사이버 취약성, 위성 제어 링크의 해킹·압력·스푸핑(spoofing)이나 재밍(jamming) 가능성 증가
- 우주 쓰레기(space debris)와 궤도 혼잡(orbital congestion)의 증가함으로써 위성 충돌 위험, 궤도 유지의 어려움 증대

● 우주 시스템 위협 주요 사례들

- 2022년 스타링크 해킹 시도(하드웨어 췌약성 발견)[75], 보안 취약성 관련 사례 발생 및 스타링크 단말기에 대한 재밍(jamming)시도[76]
- 일본 정부·JAXA(Japan's Space Agency는 2023년 하반기부터 여러 차례 외부 해커로부터 공격을 받고 있다는 사실을 공개.[77] 공격 수단 중 하나로 VPN 장비의 취약성이 악용된 것으로 확인됨.[78]

● 주요국 우주 사이버 보안 정책 강화 현황

- 미국은 2020년 우주 사이버보안 정책 지점(Space Policy Directive-5) 발표,[79] 이를 통해 우주 시스템 자체가 사이버 영역의 위협(target)이 될 수 있다는 점을 연방 정책 수준에서 인정함으로써 우주 시스템의 사이버보안에 대한 국가적 인식 및 우선순위를 상승시키고,[80] 설계-발사(pre-launch)-운용(orbit)-지상 시스템(ground)까지 이르는 전체 주기에 걸쳐 보안 설계 및 대응이 요구되며 정부만이 아닌 전체 우주 산업 생태계(space industrial base)의 보안수준 향상을 도모함.[81] 또한, 미국은 2023년 위성 사이버보안법(Satellite Cybersecurity Act) 발의함.[82]
- 2022년, EU 지도자들은 우주를 전략적 영역으로 규정하고, EU 차원의 우주 안보·방위 전략(EU Space Strategy for Security and Defence) 수립을 요구했으며 이러한 정치적 모멘텀을 바탕으로, 유럽연합 집행위원회와 고위대표는 최초의 EU 우주 안보·방위 전략을 마련.[83] 또한, 유럽 위원회는 2025년 6월 "Space Act"제안, 이를 통해 EU 전체 우주 공간(space) 정책의 규제적 기본틀(regulatory framework)을 조성하려 함.[84]

---

74) Roberts *et al.* (2024) "Stellar safeguards: How organizations can protect space assets from cyberthreats" (검색일: 2025.9.19.)
75) Korth (2022) "Starlink Terminal Hack" (검색일: 2025.7.21.)
76) Insinna (2022) "SpaceX beating Russian jamming attack was 'eyewatering': DoD official" (검색일: 2025.7.4.)
77) Koi (2024) "Japan Space Agency (JAXA) Hit by Cyberattacks" (검색일: 2025.9.19.)
78) Japan Aerospace Exploration Agency. (2024) "Report on Unauthorized Access at JAXA" (검색일: 2025.10.2.)
79) Federal Register – The Daily Journal of the United States Government. (2020) "Cybersecurity Principles for Space Systems" (검색일: 2025.9.18.)
80) Aerospace Security. (2020) "How Does Space Policy Directive-5 Change Cybersecurity Principles for Space Systems?" (검색일: 2025.10.2.)
81) Federal Register – The Daily Journal of the United States Government. (2020) "Cybersecurity Principles for Space Systems" (검색일: 2025.9.18.)
82) Congress.Gov. (2023) "S.1425 – Satellite Cybersecurity Act" (검색일: 2025.8.4.)
83) European Commission, (n.d.) "EU Space Strategy for Security and Defence for a stronger and more resilient European Union" (검색일: 2025.8.30.)
84) Kerr-Shaw *et al.* (2025) "The EU's New Cybersecurity Law for the Space Sector" (검색일: 2025.9.24.)

3-2. 주요국 신기술 안보 관련 정책 동향

3-2-1. 미국

● 미국 연방정부는 AI·사이버·양자·우주를 국가안보, 동맹외교, 공급망 및 수출통제까지 아우르는 단일 프레임으로 통합

- 2025년 7월 발표된 「America's AI Action Plan」은 혁신 가속, AI 인프라 구축, 국제외교 및 안보 리더십 등 세 가지 축에서 90여개 정책행동을 제시(연방 연구, 조달, 국제협력 포함)하였으며, 대통령령을 통해 "미국산 AI 기술 스택의 글로벌 보급"을 국가 정책으로 천명함(White House, 2025).
- 2024년 8월 NIST는 최초로 양자내성암호(FIPS 203/204/205)를 확정 고시하였으며 2025년 3월 추가 알고리즘 (HQC) 표준화를 추진한다고 고시시, 연방 및 국가안보기관 전환의 기준점으로 평가됨(NIST, 2024).
- 국방부는 2024년 4월 「상업우주 통합전략」을 최초 수립하여 상업 역량을 국가안보 우주구조에 본격 흡수하는 정책 기조를 수립하여 미 우주군도 상업우주 전략을 통해 사이버 내구성 및 위협 대응 추구를 원칙으로 확정함(Department of Defense, 2024).

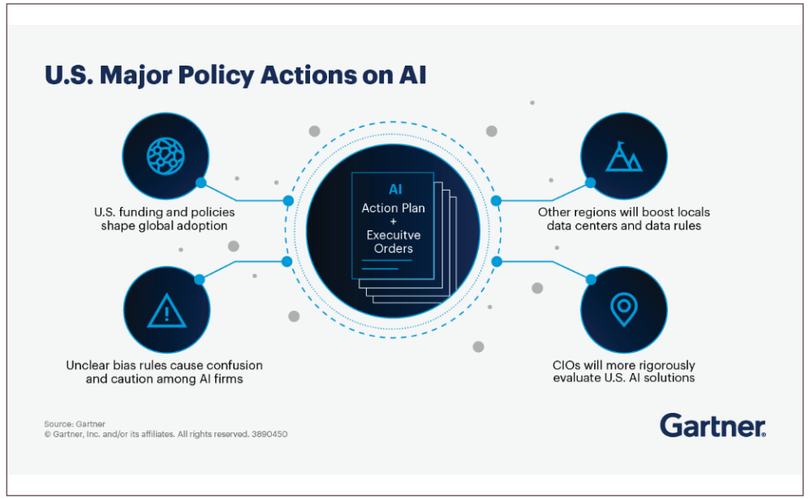


그림 14. 미국의 인공지능 정책 주요 조치

출처: Gartner[85)]

● 미국은 주요 신기술 분야별 주요 정책 수단을 발표하여 선제적 대응 강화

- 인공지능: 각 부처는 안전·보안·탄력성 기준을 충족하지 못하는 고영향(high-impact) AI에 대해 사용 중단 계획을 마련하도록 지시하고, 'AI Action Plan'에서서 연구·평가·안전표준·대국민 서비스 적용을 포괄하는 "미국 AI 기술 스택의 해외 확산 지원"을 명시(White House, 2025)
- 사이버보안: Zero Trust를 핵심 원칙으로 삼아 디지털 서비스 및 인프라 방어를 강화하고, Secure-by-Design (SbD) 생태계화를 촉진하여 공공부문과 산업기반 보안을 보강(Office of the President, 2025)
- 양자보안: NSA의 CNSS 정책 15를 기반으로 국가안보시스템 전환 로드맵을 제시, 첨단 컴퓨팅 통제 규정을 잇달아 고시하여 핵심 기술의 해외 유출을 차단하고 있음(NSA, 2025).
- 우주: 상업데이터 및 플랫폼을 국가안보 우주망에 통합하고. 사이버 내구성 및 리스크 관리 원칙을 명시한 Zero Trust 보고서를 발간(CISA, 2024)

● 범정부 거버넌스를 정비하여 즉각적·탄력적 대응 역량 강화

- 백악관: 국가사이버전략의 범정부 조정, 성과평과를 총괄하며, 예산 지침으로 각 부처 집행을 견인(Zero Trust, AI 도입 통제 등)
- NIST(국립표준기술연구소): AI 안전 및 기술 표준화의 국제연계 허브 역할을 수행
- 집행 및 활동: 사이버보안 및 인프라 보안국(CISA)를 필두로 국방부, 우주군, NSA 등 유관기관 유기적 연계를 통해 인프라 방어, 실전화, 기술 변동 대응, 기술 유출 억제를 통합적으로 추진

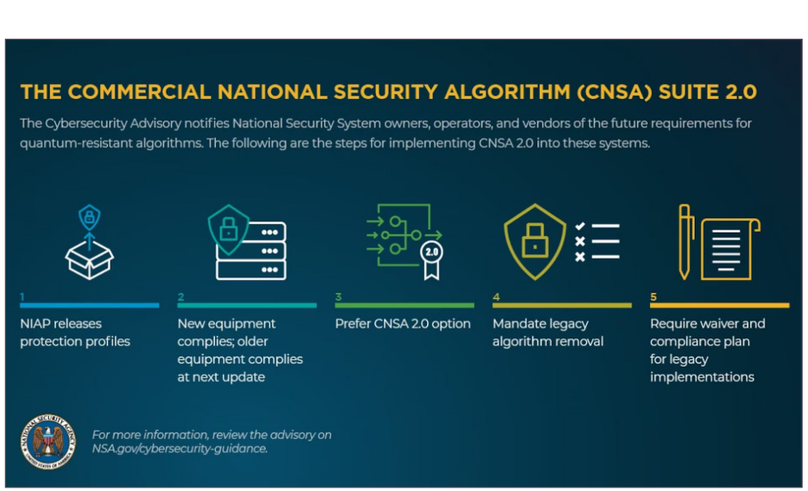


그림 15. 미국 NSA의 국가안보 시스템용 차세대 양자내성(QR) 알고리즘 요구사항

출처: National Security Agency/Central Security Service. (2022) "NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems" (검색일: 2025.9.23.)

3-2-2. 유럽연합(EU)

● 위험 인식과 규제, 투자, 위기대응을 포괄하는 안보 패키지를 추진

- AI Act (2024.8), Cyber Resilience Act (2027.12 적용 예정) 발효를 시작으로 디지털 주권 인프라를 강화를 목표로 함(EU, 2024).

85) Bishop (2025) "us-ai-action-plan" (검색일: 2025.9.25.)

- EU는 IRIS(안보형 위성 통신) 구축을 본격화하고 EuroQCI(양자 통신 인프라)와의 연계, 양자내성암호 전환을 통해 핵심 인프라 보호 추진(EU, 2023)

● 정책 및 거버넌스

- AI Act (위험기반 규제) 단계적 적용: 2024.8. 발효 → 2025.2. 금지행위 및 AI 리터러시 적용 → 2025.8. 범용모델 의무 적용 → 2026.8. 전면적용(EU 2024).
- 집행위원회 (European Commission)과 회원국 공조 구조를 공고히 하고 있으며 AI Office·감독당국·AI Board가 참여하는 다층 협력 구조를 운영, Cyber Solidarity Act로 EU 비상메커니즘을 제도화(EU 2025)

3-2-3. 중국

● (정책) 대만 총통선거(2024) 인지전(cognitive warfare)·심리전(心理戰/psychological warfare) 전개

- 중국은 대만 유권자의 비용·편익 판단과 정체성 프레이밍을 바꾸기 위한 인지전을 집중 전개했으며, 관영·친중 매체와 소셜미디어를 활용해 선거 관련 허위정보를 조직적으로 확산시켰음. 한국 연구기관 분석에 따르면, 압박성 발언·군사 시위와 함께 온라인 영향공작을 병행, 반중 성향 후보의 신뢰를 약화하는 내러티브를 대량 유포했음.[86)]
- 이러한 공작은 '삼전(三戰, Three Warfares)' 교리—심리전·여론전·법리전—의 장기적 적용 사례로, 정보환경 우위를 통해 물리적 충돌 없이 전략적 목적을 달성하려는 중국식 하이브리드전의 전형으로 평가됨(김재엽, 2022)

● (거버넌스) 대만 선거 인지전 수행조직의 지휘·통제

- 이러한 공작은 '삼전(三戰, Three Warfares)' 교리—심리전·여론전·법리전—의 장기적 적용 사례로, 정보환경 우위를 통해 물리적 충돌 없이 전략적 목적을 달성하려는 중국식 하이브리드전의 전형으로 평가됨(김재엽, 2022)

● (정책) 홍콩 국가안전법(National Security Law, 2020)과 디지털 통제

- 홍콩 국가안전법은 분열·전복·테러·외세결탁을 포괄하는 국가안보 위반을 광범위하게 규정하며, 온라인 표현과 조직 활동까지 규율함. 한국 외교 안보 연구기관들은 이 법이 '일국양제(一國兩制)'의 성격을 변화시키고, 기술·플랫폼을 매개로 한 감시·통제를 제도화해 디지털 주권과 안보를 결합했다고 평가함(국립외교원, 2020)
- 미국·영국의 제재와 기업·시민사회의 반발에도 불구하고 법 시행으로 온라인 검열·콘텐츠 삭제·플랫폼 상 협조 의무가 확대, 중국식 '안보 우선' 통치가 홍콩 디지털 공간에 심화되었다는 한국 측 분석이 다수 제시됨(국가안보전략연구원, 2020)

● (정책) 남중국해 회색지대(gray zone) 작전과 해경법(海警法) 연계

- 중국은 해경(China Coast Guard, CCG)·해상민병대(maritime militia)·어선집단을 동원해 분쟁 해역에서 상시 압박·차단·표지물 설치 등 '법집행'과 '현상변경'의 경계를 흐리는 회색지대 전술을 구사함. 한국 국회 보고서는 중국 해경법과 남중국해 활동의 국제법적 우려를 짚으며, 해경·민병대의 법적 권한 주장 확대가 역내 긴장 요인임을 지적함(국회입법조사처, 2021).
- 위성·AIS 자료를 종합한 국제 분석에 따르면, 2024년 중국 해상민병대의 분쟁 해역 상주 규모가 기록적 수준으로 증가했으며(특히 스프래틀리 일대), 필리핀 보급선 차단 과정에서 물대포·근접 기동 등 강압 수단 빈도가 높아졌음(CSIS/AMTI, 2025).

86) EAI. "2024 대만 선거에서의 중국 위협론 공방" (검색일: 2025.9.25.)

Exploration of Emerging Technology-Driven Challenges &
Emerging International Security Issues and
Global Security Collaboration

4 전문가 네트워크 구축

4. 전문가 네트워크 구축

4-1. 전문가 그룹 심층 인터뷰

● 세계신안보포럼 사후 분석 보강을 위해 아래와 같이 국내 전문가 그룹 심층 인터뷰하고 신흥 안보, 기술, 보안, 정책, 거버넌스 및 국제협력 관점의 이슈와 시사점을 도출함. (보다 자세한 심층 인터뷰 내용은 부록 1 참고)

표 8. 국내 전문가 그룹 심층 인터뷰 일정

성명	소속 및 직책	인터뷰 일시	분야
이장욱	KIDA 안보전략연구센터 신흥안보연구실장	2025.9.29.	신흥 안보
김동희	국가보안기술연구소 안보정책연구실장		보안
강경일	합동참모본부 연합검증평가 TF장		하이브리드 위협
이종진	서울대학교 통일평화연구원 선임연구원		국제협력 & 외교

● (신흥 안보 관점) 최근 특정 국가의 수출통제 강화·제재 연동·희소자원 관리 등으로 첨단 기술 공급망의 정치·안보화가 진전되고 있음. 이로 인해, 한국은 기술 의존과 기술 주권 문제에서 전략적 불확실성에 직면하고 있으며, 경제·기술 협력의 다변화 및 공급망 분산 전략 등 이를 완화하기 위한 전략 마련이 필수적임.

- 신흥 안보 위협은 전통 군사력뿐 아니라 기술·경제·사회 전반으로 확장되며, 상시화·복합화되는 추세임.
- 중국은 수출통제·허가제·안보 심사 등을 활용해 반도체·배터리 소재·희토류 등 전략 자원과 소재의 대외 공급을 관리·제한 중임.
- 한국은 경제·기술 의존성과 안보 동맹 사이에서 압박을 받는 이중 구조에 놓여 있으며, 기술 블록화와 신흥 위협의 상시화 속에서 전략적 딜레마가 심화될 가능성이 큼. 이를 완화하기 위한 전략 마련이 시급함.
- 이외에도, 해저 케이블(또는 해저 광케이블)의 절단과 손상 사건은 국제 데이터 흐름과 핵심 인프라의 안정성에 직결되는 위협으로, 해저 케이블은 군사적·비군사적 행위자 모두가 노릴 수 있는 하이브리드 위협의 대표적 표적으로 부상하고 있음.

● (기술 관점) AI 경쟁은 단순한 군사기술 문제가 아니라 데이터·표준·칩·응용기술·인재확보를 둘러싼 총체적 경쟁으로 전개되고 있음. 이에, 각국은 AI 기술력 확보와 안보 리스크 관리를 병행하는 기술안보(techno-security) 전략을 강화하고 있음. 한국 역시 개방성과 자율성을 토대로 AI 표준 참여 확대, 데이터 인프라 고도화, 반도체(칩)·핵심 부품 공급망 다변화를 추진 전략이 필요함.

- 미국·중국은 AI 반도체, 데이터, 알고리즘, 인재 확보 등 전 분야에서 총체적 경쟁을 심화시키고 있으며, 이는 단순한 기술 경쟁을 넘어 경제·산업·안보 전반을 걸쳐 전략적 경쟁으로 확산되고 있음.
- 미국은 AI 관련 데이터 보안과 기술 통제를 강화해 중국의 학습·확산을 차단하려 하며, 동맹국에도 보안 요건을 강화해 협력 압박을 가할 가능성이 큼.
- 중국은 AI, 양자, 우주 등 첨단 기술의 군사적 활용을 적극 추진하고 있으며, 정보전·심리전·인지전을 포함한 비군사적 영향력 수단을 강화하고 있음. 이를 통해 국가 전략목표 달성을 위한 복합적 영향력 확대를 시도하고 있음.
- 최근 기술 경쟁은 미국·중국 중심의 양극화로 심화될 가능성이 높고, 이는 중간국가인 한국의 전략적 취약성을 확대시킬 수 있음. 이에, 한국은 전략적 자율성과 회복탄력성을 강화할 수 있는 대응 전략 마련 필요
- AI 기술의 고도화됨에 따라, 해당기술이 인지전·사이버전에 활용될 경우, 정치·사회적 내정 간섭과 여론 조작이 상시화되고 있음. 이는 국가 간 경쟁이 비군사적·비가시적 영역으로 확장되며 하이브리드 위협 양상을 가속화할 것으로 예상됨.

● (보안 관점) 사이버와 물리 세계의 경계가 사라지고 있으며, 전력·교통·금융 등 핵심 기반시설을 겨냥한 공격이 현실화됨. 이는 국가안보 차원의 리스크로 직결됨.

- AI 기술이 기존 공격 방식을 고도화하는 도구로 악용되며, 자동화·대규모 침투가 가능해져서 위협의 범위와 속도가 과거보다 훨씬 확장됨.
- 국내 사이버 보안은 탐지·대응·복원 전 주기 개선이 요구되며, 특히 복원력(백업·대체 절차·재해복구 체계)이 가장 취약 및 미흡하고, 침해사고 후 신속히 기능을 정상화하지 못하는 점이 구조적 약점으로 지적됨.

● (정책 관점) 신흥 기술별 시급한 정책·제도적 보완이 필요함. 기술 발전 속도에 비해 법·제도·윤리·안전 기준이 미비하여, 각 기술 특성에 맞춘 안전성 기준·책임체계·국제협력 규범 등 선제적 정책 및 규범 정비가 구축되어야 함.

- 기술 개발의 고도화에 초점을 맞춰 정책 또한 고도화할 필요가 있으며, 선진적 국제 기준 규범 도입보다는 정책 정합성이 우선시 되어야 함.
- 사이버안보법 제정, 분산된 법제의 일원화가 시급하며, 기업의 책임성 강화 및 개인정보 유출 처벌 강화도 필요함.
- AI 모델 확산, 양자 전환 비용 등 신기술 관련 리스크를 고려한 정책·제도적 보완이 강조됨.

● (거버넌스 관점) 위협 발생시 국가 차원의 종합적 사이버 안보 대응체계와 컨트롤 타워 부재가 지속되고 있으며, 부처별 파편적 대응이 이뤄지고 있어, 국가 단위의 통합 거버넌스 마련이 필요함.

- 민·관·군 협력 거버넌스 구축과 합동 훈련 정례화가 필요하며, 위기 시 신속한 의사결정 권한 배분 체계 마련도 필요함.
- 위협 발생 시 빠른 대응과 책임 소재 명확화를 위해 국내 법체계 내 신속한 의사결정 권한 부여가 필요하다고 지적됨.

4-2. 전문가 세미나

표 9. 국내 전문가 세미나 일정

성명	소속 및 직책	세미나 일시	분야
박동휘	육군3사관학교 교수 (군사사학과 학과장)	2025.8.25.	사이버 보안 및 하이브리드 대응 전략

그림 16. 국내 전문가 세미나

● (국제협력 관점) 신흥 안보 양상은 국제정세와 기술 발전에 따라 갈수록 다변화·복잡화 되고 있으며, 이에 따라 신기술의 안보적 파급효과와 변화 양상을 지속적으로 진단하고 분석하고, 이에 대응하기 위해 규범 형성, 정보 공유, 공동 실증, 공동 대응 등 국제 협력 강화 필요

- 국가·민간·국제 차원에서 협력 체계가 작동하기 위해서는 정확한 상황 파악과 역할 인식이 전제되어야 함. 이를 위해 정보 공유와 조기 경보 체계 강화가 필수적임.
- UN, 다자회의 등을 통한 규범 정립과 신뢰 구축이 중요하며, 실시간 위협정보 공유 체계 강화가 필요함.
- 국제협력 효과성 제고를 위해 소규모 다자 협력, 전략적 동맹 간 합동 훈련·인재 양성·복원력 강화 협력이 필요함.
- 동맹국 및 파트너 간에는 합동 훈련, 핵심 기반시설 보호 연구·개발, 인재 양성, 복원력 강화 협력 등 전략적 연합 체계를 강화할 필요가 있음.
- 국제 규범 논의에서 한국은 중견국으로서 조정자 역할을 수행할 수 있으며, 이를 위해 전문 인력 양성과 정책적·외교적 자원 투입을 통해 지속적 참여 역량과 협상력 강화가 필요함.

● 세계신안보포럼 세션 준비 및 사후 분석 보강을 위해 국내 전문가 세미나를 진행하고 아래와 같이 하이브리드 위협 대응 전략 관점의 이슈와 시사점을 도출함.

- 세미나 제목: 하이브리드 위협 대응 전략: 회색지대 전술 대응 방안

● 권위주의 국가의 하이브리드 전략

- 타국가 및 비국가 행위자 등 활용으로 제3자를 이용한 대리전 전략 추구
- 대리전의 이점으로는 가성비의 국가이익 극대화 추구 전략, 직접적 비용 절감. 정치·군사적 부담 경감, 행위의 부인 및 보복과 제재 회피 가능
- 사이버 대리전 전략(Cyber Proxy Warfare Strategy) 추구로 익명성, 모호성, 비대칭성 기반 국가는 상대국의 제재 또는 보복 회피 가능
- 권위주의 국가 배후 해킹 조직이 사이버전의 핵심 중 핵심임.

● 위협의 진화 양상

- 사이버 위협의 중요성 증대. 전·평시 구분 모호하고 모든 영역에서 위협
- 현대 위협의 핵심은 ICT 기술의 발전에 기인하고 있음.

● 하이브리드 위협 대응 위한 선결 조건 제시

- 법과 제도 구비, 중앙 및 기관별 조직 구축, 전문 인력 양성 및 활용 및 국민 교육임.

● 하이브리드 위협 대응 방안

- 억제(Deterrence) : 국방분야의 소프트웨어 의존성 증가(소프트웨어는 현대 무기체계의 핵심 구성요소이며 국방 운영 지원하는 다양한 체계에 소프트웨어 필수적 의존 중)로, 소프트웨어 공급망의 투명성, 신뢰성, 보완성 강화 필요
- 지속적 관여(Persistent Engagement): 적의 위협 사전 식별 및 차단을 통해 적의 사이버 역량과 기반시설을 지속적으로 약화. 또한, 과도한 충돌이 아닌 적적한 마찰을 유지하여 전쟁 등의 큰 갈등으로의 비화 방지. 나아가, 동맹 및 파트너와 계속적인 정보 공유를 통해 연속적이로 조율된 대응 체계 유지
- 전방 방어(Defend forward): 적 인프라에 침투해 공격 도구 및 수법 추적 등 선제적 위협 대응. 또한, 법적 권한 범위 내 작전 및 동맹국 및 파크너와 협력해 불필요 충돌 위험 회피
- 회복력(Resilience) 구축 방안: 선제적 대응전략, 신속 대응 전략 및 장기 대응 전략 구축을 통해 회복력 구축 마련 필요. 장기적으로 디지털 안보 리커러시 교육 필요 강조
- 협력방안(Cooperations): 민·관·군 산학연 협력 강화 필요
- 기타 : 국내 토종 민간 사이버 보안 기업 육성 전략 마련 필요, 사이버 예비군 체계 구축 필요, 청소년 사이버 안보 전문가 양성(화이트 해커 등) 필요

4-3. 주요 분야별 전문가 풀

● 세계신안보포럼 및 국내 전문가 라운드테이블 기획을 위해 약 39여 명의 해외 전문가를 발굴함.

– 인지전 분야 전문가는 정보전, 심리전, 인지심리, 인지보안, 사이버·디지털 인지전, 전략 커뮤니케이션 등 관련 9명을 발굴함.

이름	소속·직책 / 전문분야
 Ms. Anja Kaspersen	· Director for Global Markets Development, Frontier Technologies at the IEEE · Senior Fellow, Carnegie Council of Ethics and International Affairs · Former Director of the United Nations Office for Disarmament Affairs in Geneva · Former Head of Strategic Engagement and New Technologies at the International Committee of the Red Cross (ICRC)
 Dr. Florence Gaub	· Director of the Research Division at the NATO Defense College (Rome) · Former, deputy director at the EU Institute for Security Studies, foresight advisor at the EU Council, and special advisor to EU Commissioner **Maroš Šefčovič**
 Prof. Deeph Chana	· Managing Director, NATO Defence Innovation Accelerator for the North Atlantic (DIANA) · Founding Chair, NATO Advisory Group on Emerging and Disruptive Technologies · High-level science advisor to the UK's Ministry of Defence
 Ms. Tanna Krewson	· Subject Matter Expert in Cognitive Warfare, NATO Allied Command Transformation (ACT) · Cognitive security, strategic communications, and information operations
 Mr. Viktors Makarovs	· Special Envoy on Digital Affairs at the Ministry of Foreign Affairs of Latvia · 2024년 민주주의 정상회의 information integrity 관련패널 사회자
 Mr. James Appathurai	· 캐나다 외교관, NATO 혁신, 하이브리드 및 사이버 담당 부사무차관보 · NATO Deputy Assistant Secretary General for Innovation, Hybrid and Cyber
 **Mr. Jānis Sārts**	· Director of the NATO Strategic Communications Centre of Excellence · Former Chair of the Latvian National Cyber Security Board
 **Lt. Col. (Ret.) François du Cluzel**	· Head of Innovative Projects, NATO Allied Command Transformation Innovation Hub; Retired Lieutenant Colonel, French Army · Cognitive warfare concept development and defense innovation strategy
 David Maxwell	· Senior Fellow, Foundation for Defense of Democracies · Associate Director, Center for Security Studies, Georgetown University · Retired U.S. Army Special Forces Colonel

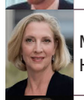
– 하이브리드전 분야 전문가는 하이브리드 위협, 비정규전 및 하이브리드 전쟁 등 관련 8명을 발굴함

이름	소속·직책 / 전문분야
 Frank G. Hoffman	· Distinguished Research Fellow, Institute for National Strategic Studies, National Defense University · Hybrid Warfare and National Security Strategy
 May-Britt Stumbaum	· Professor, College of International Security Studies, George C. Marshall European Center for Security Studies · Hybrid Warfare and Authoritarian Influence Operations
 Seth G. Jones	· Senior Vice President & Director, International Security Program, Center for Strategic and International Studies · Irregular Warfare (Hybrid Warfare) and Defense Strategy
 William Harry McRaven	· Former Commander, United States Special Operations Command · Former Chancellor, The University of Texas System
 Mykhailo Fedorov	· First Deputy Prime Minister of Ukraine · Minister of Digital Transformation of Ukraine
 Max A. Boot	· Author, editorialist, lecturer, and military historian · Worked as a writer and editor for The Christian Science Monitor and then for The Wall Street Journal in the 1990s. · Expert in Predicting Hybrid Threat Patterns in Advanced Science and Technology Fields
 Ralph Thiele	· Chairman, Political-Military Society · President, EuroDefense Germany · CEO, StratByrd Consulting
 Ofer Fridman	· Senior Lecturer in War Studies, King's College London · Director of Operations, King's Centre for Strategic Communications

– 하이브리드 위협 대응 전략 분야 전문가는 하이브리드 위협 대응, 사이버 방위 및 전(全)정부·전(全)사회적 통합 안보 프레임워크전략 등 관련 4명을 발굴함

이름	소속·직책 / 전문분야
 Mr. David Song-Pe-hamberger	· Deputy Director of the Hybrid CoE's Community of Interest for Strategy & Defence · Specialized in Cyber Defence, Emerging Technologies, and matters related to East Asian Security and Defense
 Mr. Tõnis Saar	· Director of NATO Cooperative Cyber Defence Centre of Excellence(CCDCOE)
 Martha Turnbull	· Director, Community of Interest on Hybrid Influence · Former Deputy Head, State Threats Unit
 Rauha-Maija Rannikko	· Special Advisor, European Centre of Excellence for Countering Hybrid Threats · Lecturer / Speaker on Hybrid Threats at NATO Conferences

– 사이버 위협 대응 분야 전문가는 사이버 방어·보안 운영, 위협 정보 분석, 국가보안정책 및 국가보안전략 등 관련 4명을 발굴함

이름	소속·직책 / 전문분야
 Mr. Austin Larsen	· Principal Threat Analyst with Google's Threat Intelligence Group, leading rapid response and investigation coordination for major global cyber events.
 Ms. Melissa Hathaway	· President, Hathaway Global Strategies LLC; former U.S. National Cybersecurity Coordinator · National Cybersecurity Policy and Cyber Threat Response
 Mr. Dmitri Alperovitch	· Executive Chairman, Silverado Policy Accelerator; Co-founder of CrowdStrike · Cyber Threat Intelligence and Cyber Defense Strategy
 Mr. Ciaran Martin	· Professor of Practice, University of Oxford; former CEO, UK National Cyber Security Centre · National Cybersecurity Strategy and Incident Response

– 인공지능 분야 전문가는 AI 기술혁신, 윤리, 정책, 안보 및 보안 관련 2명을 발굴함

이름	소속·직책 / 전문분야
 Ms. Elsa B. Kania	· Adjunct Senior Fellow, Technology and National Security Program, Center for a New American Security · Chinese Military Applications of Artificial Intelligence
 Dr. Margarita Konaev	· Deputy Director of Analysis, Center for Security and Emerging Technology · Military Applications of AI and Emerging Technologies

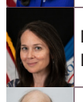
– 우주항공 분야 전문가는 국제우주정책, 우주 안보전략 및 우주 보안 관련 3명을 발굴함

이름	소속·직책 / 전문분야
 Mr. Brian Weeden	· Director of Program Planning, Secure World Foundation · Space Security and Space Situational Awareness
 Ms. Kaitlyn Johnson	· Deputy Director, Aerospace Security Project, Center for Strategic and International Studies · Space Policy, Defense, and Counterspace Threats
 Dr. Bleddyn E. Bowen	· Associate Professor of International Relations, University of Leicester · Space Warfare and Defense Strategy

– 양자분야 전문가는 양자컴퓨터, 양자정보통신, 양자암호 관련 3명을 발굴함이로 조율된 대응 체계 유지

이름	소속·직책 / 전문분야
 Dr. John Preskill	· Richard P. Feynman Professor of Theoretical Physics, California Institute of Technology · Quantum Computing and Quantum Information Science
 Dr. Pan Jian-Wei	· Professor of Physics, University of Science and Technology of China · Quantum Entanglement and Satellite Quantum Communication
 Dr. Stephanie Wehner	· Professor of Quantum Information, Delft University of Technology · Quantum Internet and Communication Technologies

– 사이버 보안, 통신 분야 전문가는 사이버 정책, 사이버 보안 등 관련해 6명을 발굴함

이름	소속·직책 / 전문분야
 Ms. Anne Neuberger	· Payne Distinguished Lecturer at Stanford University; Former Deputy National Security Advisor for Cyber and Emerging Technology (White House) · Cybersecurity strategy and national security technology policy
 Dr. Jen Easterly	· Director of the U.S. Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security · Cyber defense, critical infrastructure protection, and organizational cyber resilience
 Mr. Bruce Schneier	· Security Technologist and Fellow at Harvard University (Berkman Klein Center); Lecturer in Public Policy at Harvard Kennedy School · Cryptography, software security, and public cybersecurity policy
 Mr. Michael Daniel	· President & CEO of the Cyber Threat Alliance; former White House Cybersecurity Coordinator (Obama Administration) · Cybersecurity policy, cyber incident management, and information-sharing initiatives
 Ms. Lindy Cameron	· Chief Executive Officer of the UK National Cyber Security Centre (NCSC) · National cyber defense, cyber incident response, and resilience of critical communication networks
 Dr. Charles Clancy	· Senior Vice President & Chief Futurist at MITRE Labs; former Director of the Hume Center for National Security and Technology at Virginia Tech · Secure wireless communications, cybersecurity for 5G/next-gen networks, and AI-driven security solutions

● 국내 전문가는 인지전 3명, 하이브리드 위협 및 대응 전략 2명, 사이버 보안 7명, 인공지능 4명, 양자분야 2명 을 포함해 총 18명을 발굴함.

– 인지전 분야 전문가 (3명)

이름	소속·직책 / 전문분야
 이호령	· 책임연구위원, 한국국방연구원(KIDA); 회장, 한국세계지 역학회 · 북한 및 동북아 안보전략, 인지전 대응 전략
 김소정	· 국가안보전략연구원(INSS) 책임연구위원 · 하이브리드 위협 및 인지전(認知戰) 대응 정책
 두진호	· 한국국방연구원(KIDA) 연구위원 · 사이버 심리전 및 인지전 전략 분석

– 사이버 보안, 통신 분야 전문가 (7명)

이름	소속·직책 / 전문분야
 권헌영	· 고려대학교 정보보호대학원 교수 (사이버보안정책센터 소장 역임) · 정보보호 법제 및 정책, 개인정보보호와 사이버 안보 정책
 박동휘	· 육군3사관학교 군사사학과 학과장 (육군 중령) · 전쟁사, 사이버전, 군사전략
 이상중	· 한국인터넷진흥원(KISA) 원장 (前 구미대 사이버보안연구원장) · 사이버범죄 수사 및 디지털 포렌식, 국가 사이버보안 정책
 진승헌	· 한국전자통신연구원(ETRI) 정보보호연구본부 본부장 · 인증기술, 네트워크 보안 등 사이버보안 기술 R&D
 손기욱	· 서울과학기술대학교 컴퓨터공학과 교수 (한국사이버안보학회 회장) · 소프트웨어 보안 취약점, 공급망 보안 등 사이버보안 분야
 이대성	· 국립한국해양대학교 교수 (사이버안보공학연구센터 센터장) · 정보통신 시스템 보안, 해양 및 산업 분야의 사이버보안
 박노형	· 고려대학교 법학전문대학원 교수 (국제사이버법연구회 회장) · 국제법 및 사이버 법률 정책, 사이버 공간의 법제와 국가안보

– 하이브리드 위협 및 대응 전략 분야 전문가 (2명)

이름	소속·직책 / 전문분야
 이상민	· 한국국방연구원(KIDA) 현역연구위원 · 북한 핵, 미사일, WMD 등
 손경호	· 국방대학교 교수부 교수 · 전쟁사, 테러리즘, 국가 전략

– 인공지능 분야 전문가 (6명)

이름	소속·직책 / 전문분야
 예종철	· KAIST 전산학부 교수 · 신호처리, 머신러닝, 의료 이미지 영상 처리
 신진우	· KAIST 전산학부 교수 · 대규모 언어 모델, 딥러닝, 인공지능 이론
 김승주	· 고려대학교 정보보호대학원 교수 · 암호학, 국가 사이버안보 정책, 블록체인·AI 보안
 오혜연	· KAIST 전산학부 교수 · 인공지능·정보서비스, 소셜 컴퓨팅, 인터랙티브 컴퓨팅
 김건희	· 서울대학교 컴퓨터공학부 교수 · 컴퓨터 비전, 머신러닝, 자연어 처리
 유영재	· 서울대학교 컴퓨터공학부 교수 · Physical AI, 강화 학습, AI Safety

– 양자 분야 (2명)

이름	소속·직책 / 전문분야
 배준우	· KAIST 전기및전자공학부 &양자대학원 교수 · 양자정보이론
 손영익	· KAIST 전기및전자공학부 &양자대학원 교수 · 광자 기반 양자 컴퓨팅, SiV 센터 기반 양자 중계기

Exploration of Emerging Technology-Driven Challenges &
Emerging International Security Issues and
Global Security Collaboration

5 신기술 안보 관련 포럼

5. 신기술 안보 관련 포럼

5-1. 2025 세계 신안보포럼 라운드테이블 (국내 행사)

● 본 정책연구 과제의 주요 과업인 세계신안보포럼 세션 기획을 위해 사전 국내 전문가 라운드테이블을 아래와 같이 개최함. (보다 자세한 세계신안보포럼 라운드테이블 내용은 부록 2 참고)

- 일시 및 장소: 2025.07.14.(월) 15:00~18:00, 포시즌스 호텔 서울
- 일정 및 패널

표 10. 세계신안보포럼 라운드 테이블 세부 일정

일정	시간	세부주제	참여 패널
개회식	15:00~15:15	개회식, 환영사, 축사	개회사: 이태우 외교부 국제사이버협력대사 환영사: 배중면 KAIST 안보융합원장 축사: 댄 스미스 스톡홀름국제평화연구소(SIPRI) 소장
세션1	15:20~16:30	하이브리드 위협의 실태	발표: 양욱 아산정책연구원 외교안보연구센터 연구위원 토론: 손인근 아주대학교 장위국방연구소 연구교수, 조상근 사단법인 창끝전투 학회장, 김은영 가톨릭관동대학교 경찰학부 부교수 좌장: 손한별 국방대학교 전략학부 교수
세션2	16:40~17:50	하이브리드 위협과 국제안보의 변화	발표: 박보라 국가안보전략연구원 하이브리드위협연구센터장 토론: 안형준 과학기술정책연구원(STEPI) 연구위원, 이동연 한국인터넷진흥원(KISA) 국민피해대응단장, 방준성 한국전자통신연구원(ETRI) 책임연구원 좌장: 김소영 KAIST 과학기술정책대학원 교수

● 세션 1 발표의 주요 내용 : 하이브리드 위협의 실태

- 전쟁은 선형전·화력전·기동전·내러티브 중심전·인지 중심 융합전으로 발전해 왔으며, 탈냉전 이후 다극화·정보화·초연결화 속에서 전쟁 비용과 정치적 부담은 증대하고 하이브리드 위협은 상시적이고 불투명한 방식으로 제도와 신뢰를 잠식하는 새로운 전쟁 양상으로 자리 잡음.
- 2014년 크림 병합은 군사력과 정보·외교·법률·문화·사이버·경제·에너지 수단을 결합한 러시아식 하이브리드 전쟁의 전형적 사례로, 인지전을 활용해 상대방의 판단과 결심을 흐리며 국제사회의 불완전한 대응 속에서 전략적 성과를 거둔 사건으로 평가됨.
- EU의 CORE 모델은 하이브리드 위협이 사회 전영역에 걸쳐 선택적 침투와 연계 확산을 일으킨다는 점을 시각화하며, 중국의 대만 공세와 러시아의 발칸 압박 사례 분석을 통해 전사회적 취약성을 드러냈고 이에 대응하기 위해 조기 탐지, 민관 통합, 가치 기반 회복탄력성이 필요함.
- **시사점 및 제언:**
  ① 회색지대·인지전의 상시화에 대비해 상황 인식과 조기 경보를 고도화하고 탐지–평가–대응 절차를 표준화할 필요가 있음.
  ② 부처 간 권한·책무를 명확히 한 거버넌스를 구축하고 민간 플랫폼·언론·시민사회와의 상시 협력 메커니즘을 제도화해야 함.
  ③ CORE 기반 취약성 진단과 모의훈련을 정례화하고 정치·정보·경제 연계 영역의 억제력과 회복탄력성을 높이기 위한 법제·예산·인력 투입을 지속해야 함.

● 세션 1 주요 토론 내용

- **(핵심 제언)** 하이브리드 위협 대응은 부처 간 자산 공유와 민간 기술 활용, 법·제도적 기반 마련을 통해 이루어져야 하며, 애매모호성과 자유민주 사회의 취약성을 고려한 사례별 접근이 필요함. 인지전의 개념 정립과 내러티브 관리, 범정부 차원의 거버넌스 구축이 요구되며, 기술적 대응과 함께 사회적 공감대 형성과 제도화가 병행되어야 함.
- 토론자별 주요 내용
  ① 손인근 교수: 사이버·전자·우주 영역에서 부처 간 자산 공유 체계가 미비해 협업 실패가 반복되고 있으며, 미국은 5G·AI·클라우드 등 민간 기술을 도입해 위협 대응 속도를 높이고 있음. 네트워크를 넘어선 융합 시스템 구현을 위해 법·제도 정비와 거버넌스 마련이 필요함.
  ② 조상근 학회장: 하이브리드·인지전은 현실을 온전히 반영하지 못하며, 상용 드론·클라우드·통신망 활용은 모호성을 증대시킴. 권위주의 국가는 법·윤리에 구애받지 않으나 자유민주 국가는 제약을 받는 구조적 한계가 있어 사례별 분석과 대응이 필요함.
  ③ 김은영 교수: 하이브리드 전쟁은 전면전과 평시 사이의 회색지대에서 가장 큰 위험을 드러내며, 인지전의 개념과 범위에 대한 국가적 공감대가 부족함. 민간 기술 활용의 잠재력은 크지만 정부의 가이드라인과 거버넌스가 부재해, 사회적 접근을 완성하기 위해서는 국가와 공공기관의 제도 설계와 리더십이 중요함.
  ④ 양욱 연구위원: 모든 위협을 국가가 대응하는 것은 비현실적이며 댓글 공격과 같은 일상적 인지전은 출처와 의도가 다양함. 민·관·군의 역할을 분리하고 생태계 기반 방어체계를 구축해야 하며, 민주주의 국가에서는 정치적 합의를 통해 권한과 책임을 분산시키는 구조가 필요함.

● 세션 2 발표의 주요 내용 : 하이브리드 위협과 국제안보의 변화

- 런던 77 테러와 2017년 웨스트민스터 테러는 소셜미디어를 통한 혐오 내러티브 확산과 러시아 연계 사이버 트롤 계정의 개입으로 기존 국경 중심 대테러 전략의 한계를 드러내며, 하이브리드 위협이 현실화된 대표 사례로 평가됨.
- 국제안보환경은 예측 불가능성과 민주주의 체계 마비를 노린 비물리적 공격이 두드러지는 방향으로 전환되고 있으며, 허위조작정보와 인프라 공격은 사회 기반을 장기간 잠식하는 핵심 위협으로 부상함.
- NATO, EU, 영국, 호주 등은 훈련·정보 공유·제도적 대응을 통해 하이브리드 위협에 대응하고 있으며, 특히 EU는 상황 인식·회복·귀속 판단을 중시하는 다층적 프레임워크를 발전시켜 왔음.

- **시사점 및 제언:**

① 하이브리드 위협은 특정 부처가 단독으로 대응할 수 없는 복합적 성격을 지니므로, 범정부적 협력 프레임워크를 마련하고 상황별로 주도 부처를 유연하게 조정할 수 있는 체계를 구축해야 함.

② 내러티브 관리와 정보 전달 전략은 정부 신뢰를 기반으로 설계되어야 하며, 국민이 수용할 수 있는 메시지와 신뢰할 수 있는 플랫폼을 확보해야 함.

③ 시민 개개인이 대응 주체임을 인식할 수 있도록 미디어 리터러시 교육을 강화하고, 이를 뒷받침할 법적·제도적 기반을 조속히 정비해야 함.

● 세션 2 주요 토론 내용

- **(핵심 제언)** 우주와 사이버 공간은 경계와 책임이 불분명한 영역으로, 하이브리드 위협의 핵심 속성과 맞닿아 있으며 이에 대한 전략적 대응이 필요함. 위성 해킹이나 글로벌 소프트웨어 장애처럼 비의도적 사건도 국가 안보 차원의 위협으로 확산될 수 있어, 민관 협력과 정보 공유, 회복력(resilience) 기반 대응 전략을 강화해야 함. AI의 활용과 기술 민주화는 위협의 정밀성과 보편성을 동시에 확대하고 있어, 독자적 데이터 인프라 구축과 국제 규범 논의 참여, 시민 사회의 연대 문화 형성이 함께 뒷받침되어야 함.

– 토론자별 주요 내용

① 안형준 연구위원: 우주는 주체 식별과 책임 귀속이 어려워 하이브리드 위협에 포함되며, 위성 해킹은 전면전 없이도 국가 기반 인프라를 마비시킬 수 있음. GPS와 위성통신 등 의존도가 높아지는 가운데, 국제 규범 논의와 기술 블록 형성 초기 단계에서 한국의 전략적 판단이 요구됨.

② 이동연 단장: 글로벌 소프트웨어 장애는 고의적 공격이 아님에도 사이버전 수준의 피해를 낳았으며, 랜섬웨어와 대리 공격은 여전히 효과적인 수단임. AI가 접목되며 공격의 정밀성이 강화되고 있어 통합적 대응과 민관 협력이 필수이며, KISA는 CERT 운영과 국제 협력을 통해 사이버 레질리언스를 강화 중임.

③ 방준성 책임연구원: 인터넷 기반 기술 확산으로 누구나 공격자가 될 수 있는 환경이 조성되었으며, 딥페이크와 허위정보 같은 위협은 AI 기반 대응 전략과 새로운 예측 도구가 필요함. 단순 방어가 아닌 회복력 중심 대응이 요구되며, AI 격차 해소와 프로세스 단위 적용을 통해 실질적 보안 역량을 확보해야 함.

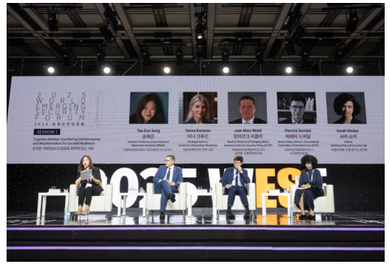
④ 박보라 센터장: 영국·호주는 모호한 '하이브리드 위협' 대신 '국가 안보'나 '해외 영향력' 같은 용어를 사용해 위협을 직관적으로 설명하고 국민적 경각심을 유도함. 혐오 표현 대응은 법적 규제만으로는 한계가 있으며, 사회적 연대와 공동체적 책임 문화를 통해 극복할 수 있음.

그림 17. 2025
세계신안보포럼
라운드테이블(국내 행사)

5-2. 2025 세계 신안보포럼 (국제 행사)

● 2025년 제5차 세계신안보포럼(World Emerging Security Forum, WESF)은 외 교부 주최로 스웨덴 정부의 외교정책연구소인 스톡홀름 국제평화연구소(SIPRI) 및 KAIST 국가미래전략기술 정책연구소가 파트너 기관으로서 함께 개최함.

- 2025 WESF 포럼은 지난 4년간의 성공적인 성과를 토대로, 과학기술의 급속한 발전에 따라 진화하는 국제안보 환경에 초점을 맞추었으며, 특히 인지전, 신기술과 위협 동향, 핵심 인프라 회복력 등을 중심으로 논의가 이루어짐.
- 주제: 하이브리드 위협의 진화와 국제안보 (The Evolution of Hybrid Threats and International Security)
- 일시 및 장소: 2025.09.08.(월) 10:00~17:10, 그랜드 하얏트 서울, 그랜드 볼룸
- 동 포럼에 관한 자세한 보고는 별책에 수록함.



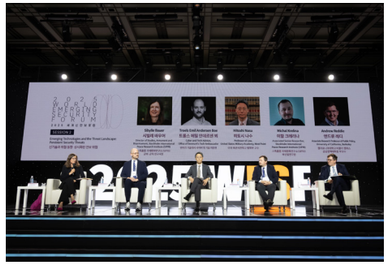


그림 18. 2025
세계신안보포럼(국제 행사)

Exploration of Emerging Technology-Driven Challenges &
Emerging International Security Issues and
Global Security Collaboration

부록

부록 1 : 국내 전문가 주요 자문 내용

한국국방 연구원
안보전략연구센터
신흥안보연구실장
이장욱

1. 과학기술과 연계된 신흥 안보 이슈 및 향후 전망

- 기술 분포는 경쟁 심화에서 양극화로 이동할 가능성이 크며, 이 경우 한국과 같은 중간국가의 포지셔닝이 극도로 중요해지며, 기술 평준화가 이루어질 경우에는 후발국의 도전이 늘고 비대칭 공격 가능성이 증대함.
- 양극화가 고착될 경우 중간국가의 기술적 몰락 위험이 커지고, 불법적 획득 시도가 증가할 수 있는 바, 한국도 기술적 중간국가로서 이러한 위험에 대비할 필요함.
- 기술 확산 시에는 후발국의 도전이 늘어 비대칭 공격 가능성이 확대되며, 기술 정체가 발생하면 기술 의존국이 급격히 쇠퇴할 수 있어 분야별 차별화된 전략 마련이 필요함.
- 한국은 아직 기술적 중간국가 위치에 있으며, 이러한 구도에서 몰락 가능성을 차단하기 위해 선도국과의 협력 강화 및 자국 기술 자립도를 높이는 전략 병행이 필요함.

2. 최근 사이버 보안 환경과 리스트 변화

- 경제적 이익을 노린 공격이 급증하고 있으며, 특히 랜섬웨어와 지적재산권 탈취 시도가 지속적으로 발견되고 있음.
- 국가가 직접 개입하지 않고 대리인(Proxy) 해커를 활용하는 사례가 증가하고 있으며, Dragon 계열 해커나 러시아 후원 KillNet 2.0 등이 대표적 사례로 지목됨.
- 개인정보 유출 후 USIM 칩 삽입, SNS 가상계정 개설, 가짜뉴스 확산으로 이어지는 다단계 공격이 나타나고 있으며, 러시아의 미국·유럽 선거 개입 사례에서 실제 확인됨.
- 중국은 IT·미디어 기업의 지분을 매입해 정보 생태계를 간접적으로 장악하려는 움직임을 보이고 있어, 단순한 기술 문제를 넘어 정보 공간·여론 통제 수단으로 확장될 가능성 상존
- AI·봇을 활용한 자동화 공격이 대규모·초고속으로 이뤄지고 있으며, 국내 모바일 인증 제도의 취약성이 이런 공격에 직접 노출될 가능성이 크다고 지적됨.

3. 미국· 중국의 AI 기술력 경쟁이 국제 안보 환경에 미칠 영향과 전망

- 미국은 AI 관련 데이터 보안과 기술 통제를 강화해 중국의 학습·확산을 차단하려 하며, 동맹국에도 보안 요건을 강화해 협력 압박을 가할 가능성이 큼.
- 중국은 완전하지 않아도 실전 적용이 가능한 기술을 우선 배치하는 전략을 추구하며, 자율 무기체계의 조기 배치 가능성이 높음.
- 미국은 '리플리케이터(Replicator) 이니셔티브'를 통해 군집 드론 전투와 같은 혁신적 전환을 추진하고 있으며, 이는 전략 경쟁자의 억지를 넘어 미래 전쟁양상을 주도하려는 시도로 평가됨.
- 미·중 경쟁은 기술 양극화를 유발해 중간국가와의 군사력 격차를 확대시킬 가능성이 크며, 압도적 군사력을 바탕으로 현상 변경과 강압적 대외정책을 추진할 수 있음.
- AI가 인지전·사이버전에 활용될 경우, 내정간섭과 여론 조작이 상시화되고 하이브리드 전쟁 양상이 고도화될 것으로 전망됨.

4. 최근 신흥 안보 위협의 진화 양상 및 상시화된 안보 위협 현황

- '가난한 국가의 순항미사일'로 불리는 저가형 드론 등 값싼 비대칭 무기 수단이 확산되며 국지적 충돌 위험이 증가함.
- 기후변화로 인한 기상 예측 곤란, 해류·기류 변화는 군사 작전과 어업 분쟁 등 새로운 갈등 요인으로 작용하며, 수단 내전 등 기후 기인 분쟁 사례도 나타남.
- 에너지 안보 차원에서 중동 산유지역 분쟁, 러시아의 에너지 무기화가 지속되고 있음. 이는 공급망 위기를 심화시키고, 전략적 자원(희토류 등)의 무기화 가능성을 확대함.
- 해상 회색지대 분쟁, 무기 불법 거래 등 비정규 주체의 위협이 확산되고 있음.
- SNS와 미디어 발전은 오히려 극단주의 확산과 신(新)파시즘 및 권위주의 부상에 기여하고 있어, 인도주의적 위기와 사회 불안정을 증폭시킴.

5. 기후변화, 에너지, 우주, 양자기술 등 비전통적·복합 위협 영역에서 가장 주목해야 할 새로운 안보 리스크는 무엇입니까?

- 기후변화는 북극항로 개방과 같은 물리적 충돌 위험을 높이고 있으며, 신흥 강대국 간 경쟁 요인으로 부상함.
- 인지전은 기존 국제체제의 근간을 약화시키고, 내정 간섭과 사회적 분열을 상시화시킬 수 있음.
- 중국의 회색지대 전술 고도화와 기회주의적 팽창은 주변국과 국제질서를 불안정하게 만드는 핵심 요인으로 작용함.
- 두뇌공학(예: 뉴럴링크) 상용화는 인간과 무기를 연결해 인지공간·물리공간 이원적 전투를 가능하게 하며, 전장의 개념을 근본적으로 변화시킬 잠재력을 가짐.

6. 기타

- 위협 탐지 단계의 취약성이 가장 크며, 회색지대 공격의 초기 징후를 포착하기 어려움.
- 개인정보 유출에 대한 처벌 강화, 기업 보안 책임성 제고 등 법·제도적 보완이 필요함.
- 민간의 방호 의지를 높일 수 있는 인센티브 설계와 정책적 장치 마련이 필요하며, 국제 협력 약화가 위협을 고도화시키는 상황에서 정보 공유와 예방 중심 훈련 강화가 요구됨.

국가보안기술
연구소 안보정책
연구실장
김동희

1. 과학기술과 연계된 신흥 안보 이슈 및 향후 전망

- 신흥파괴적기술(EDT)은 국가안보를 강화하는 동시에 악용될 경우 심각한 위협이 될 수 있는 양면성을 지녔으며 첨단기술은 억지력 강화와 동시에 새로운 공격수단을 제공함.
- 이러한 기술들은 미·중 간 기술 패권 경쟁을 심화시키며, 군사력의 질적 변화와 함께 국제 질서 재편을 촉발하는 요인이 되고 있음.
- 특히 AI, 양자, 우주기술 등은 단기간 내 국가 간 전략 균형을 흔들 수 있는 잠재력이 크므로 한국은 중장기적 관점에서 새로운 안보 전략을 마련해야 함.

2. 최근 사이버 보안 환경과 리스트 변화

- 사이버와 물리 세계의 경계가 사라지고 있으며, 전력·교통·금융 등 핵심 기반시설을 겨냥한 공격이 현실화됨. 이는 국가안보 차원의 리스크로 직결됨.
- AI 기술이 기존 공격 방식을 고도화하는 도구로 악용되며, 자동화·대규모 침투가 가능해져서 위협의 범위와 속도가 과거보다 훨씬 확장됨.
- 침해사고 발생 이후 정상화로 돌아가는 복원력이 부족한 점이 문제로 지적됨. 공격은 늘어가는데 대응·복구 속도와 체계는 뒤처지는 상황임.

3. 미국· 중국의 AI 기술력 경쟁이 국제 안보 환경에 미칠 영향과 전망

- AI 기술 경쟁은 공급망, 기술표준, 국제규범 전반으로 파급되며, 각국은 자국의 국익을 극대화하기 위해 기술 보호조치를 강화하는 추세임.
- 검증되지 않은 AI 모델의 확산은 데이터 유출, 조작 가능성, 알고리즘 불투명성 등 새로운 리스크를 야기할 수 있음.
- 양자 내성 암호 전환 비용과 같은 파생 리스크도 존재하며, 한국과 같은 국가들은 비용 측면에서 큰 부담을 지게 될 수 있음.

4. "위협 탐지–대응–복원" 단계에서 현재 한국의 가장 취약한 고리는 어디에 있다고 보십니까?

- 세 단계 모두 보완이 필요하지만, 특히 복원력(회복력)이 가장 취약하고, 침해사고 후 신속히 기능을 정상화하지 못하는 점이 구조적 약점으로 지적됨.

5. 사이버 보안 위협에 대한 기술적 대응 외에, 법·제도적 보완이 필요한 지점은 무엇이라고 생각하십니까?

- 사이버안보법과 같은 기본 법제 정비가 필요하며, 현재 분산된 법령을 일원화하고 거버넌스를 재정립해야 함.
- 국제 공조 기반 마련을 위해 관련 법령을 제·개정하고, 사이버 범죄 대응의 사법 공조 체계를 강화할 필요가 있음.

- 위협 발생 시 빠른 대응과 책임 소재 명확화를 위해 국내 법체계 내 신속한 의사결정 권한 부여가 필요하다고 지적됨.

6. 민관 협력(산업계, 학계, 정부)을 통한 보안 강화 방안은 무엇일까요?

- 새로운 기술의 국제 표준화 및 인증 분야에서는 산·학·연 협력이 필수적이며, 국가 차원의 지원도 뒷받침되어야 함.
- 대부분의 사이버 위협이 민간을 경유하거나 민간을 직접 대상으로 하기 때문에, 민간과의 실시간 정보공유 체계를 강화해야 함.
- 핵심 기술과 서비스의 안정적 공급·유통을 위해 공급망 보안 분야에서 민관 협력이 강화될 필요가 있음.

7. 기타

- 국제협력은 국내 거버넌스 정비와 병행되어야 실효를 거둘 수 있음. 내부 의사결정 구조와 위기 시 권한 배분을 미리 확정하는 것이 중요함.
- 기술적 측면에서만 대응하려는 태도에서 벗어나 법·제도·정책·국제협력이 종합적으로 작동해야 지속 가능한 안보 체계가 될 수 있음.

합동참모본부
연합검증평가
TF장
강경일

1. 과학기술과 연계된 신흥 안보 이슈 및 향후 전망

- 미·중 전략경쟁은 과거 냉전처럼 완전한 단절 구도가 아니라 상호 의존과 교류가 남아 있는 구조에서 전개되고 있으며, 이는 권위주의 국가의 초한전 전략 확산을 촉진하고 있음.
- 중국은 반도체, 배터리, 희토류 등 공급망 무기화와 AI·양자·우주 기술의 군사화, 정보전·심리전의 일상화를 통해 영향력을 확대하고 있음.
- 한국은 경제·기술 의존성과 안보 동맹 사이에서 압박을 받는 이중 구조에 놓여 있으며, 기술 블록화와 신흥 위협의 상시화 속에서 전략적 딜레마가 심화될 가능성이 큼.

2. 최근 사이버 보안 환경과 리스트 변화

- 사이버 공간은 군사 충돌을 대신하는 회색지대 압박 수단으로 활용되고 있고, 권위주의 국가에게는 초한전의 핵심 전장으로 자리잡음.
- 북한은 제한된 자원 속에서도 인력을 활용해 사이버 능력을 비대칭 전략으로 발전시키고 있어 한국은 미·중 경쟁과 북한 위협이 중첩된 '3중 도전'에 직면함.
- 중국·북한 해커는 공급망 및 운영체계를 표적으로 삼아 정밀한 해킹을 시도하여 AI 기반 공격까지 결합하면서 억지력 확보가 어려운 구조적 취약성이 드러남.

3. 미국· 중국의 AI 기술력 경쟁이 국제 안보 환경에 미칠 영향과 전망

- AI 경쟁은 단순한 군사기술 문제가 아니라 데이터·표준·칩·응용기술을 둘러싼 총체적 경쟁으로 전개되고 있음.
- 중국은 심리전, 여론조작, 사회통제에 AI를 적극 활용하는 반면 미국은 동맹과 표준 연계를 통해 이를 견제하려 하지만 과거 냉전처럼 완전 통제는 쉽지 않음.
- 한국은 반도체, 2차전지, 차세대 에너지 등 응용기술 분야에 강점을 보유하나, 미·중 전략경쟁 속에서 기술 블록화 압력과 동맹·경제 의존 사이의 전략적 딜레마가 심화될 전망임.

4. 하이브리드 위협의 융합·심화가 국제 안보 환경을 어떻게 변화시키고 있다고 보십니까?

- 군사와 비군사 수단이 융합되며, 무역·금융·외교·정보·법률 등 민간 영역 전체가 전장으로 확장되고 있음.
- 전쟁 발발 시 가장 먼저 민간 인프라와 사회적 신뢰가 공격 대상이 되며, 러시아–우크라이나 전쟁에서 이미 확인된 패턴이 반복될 가능성이 높음.
- 한국은 지정학적 위치와 경제 개방성으로 인해 이러한 하이브리드 위협의 주요 표적이 될 수 있으며, 사회적 갈등을 조장하는 심리전·허위정보 유포에 특히 취약함.

5. 핵심 인프라 회복력을 강화하기 위해 단기적으로 가장 시급히 개선해야 할 영역은 무엇입니까?

- 희토류 등 전략 자원에 대한 공급망 다변화가 필수적이며, 중국 의존도를 줄여야 국가적 충격 흡수력이 커짐.
- 금융결제, 전력망, 통신망, 물류망 등 핵심 기반시설의 복구 프로세스를 강화해야 하며, 사이버 공격 발생 시 신속한 대체체계 가동이 가능해야 함.
- 허위정보·심리전에 대응하기 위한 사회적 신뢰망을 구축하고, 유튜버·미디어를 통한 허위정보 확산에 대한 징벌적 제재 제도도 마련이 필요함.
- 이를 위해 민·군·정부가 유기적으로 연계된 거버넌스를 구축하고, 합동 훈련을 정례화하여 실제 위협 상황에서 대응 능력을 확보해야 함.

6. 기타

- 단순 억지력만으로는 불충분하며, 사이버·공급망·정보 영역에서의 회복력(resilience) 강화를 최우선 과제로 삼아야 함.
- 자유민주주의 국가 특성상 (준)전시가 아니면 군 개입이 제한되므로, 민간과 정부 차원에서 선제적 대비와 협력이 더욱 중요함.
- 미·중 전략경쟁, 북한 위협, 신흥기술 확산이 중첩되는 한국의 안보환경은 복잡성을 높이고 있으므로, '전통 억지 + 하이브리드 대응체계'의 이중 전략이 불가피하다고 지적됨.
- 위협은 국제안보 담론에서 지·해·공 전통 영역을 넘어 사이버·우주·전자기 영역으로 확장되고 있으며, 최근에는 해저(undersea)와 지하(subterranean) 영역에 대한 관심도 빠르게 높아지고 있음.

서울대학교
통일평화연구원
선임연구원
이종진

1. 과학기술과 연계된 신흥 안보 이슈 및 향후 전망

- AI 기반 사이버 공격은 여론조작과 정보왜곡을 통해 사회 혼란을 야기하고 민주주의 제도를 근본적으로 위협할 수 있으며, 민주주의 국가일수록 제도적 개방성을 악용당할 소지가 큼.
- 첨단 기술 공급망은 특정 국가가 이를 무기화하거나 통제수단으로 활용할 가능성이 있는 바, 한국은 기술 의존과 주권 문제에서 전략적 불확실성에 직면하고 있음.
- 기술 주권의 충돌은 국제사회에서 역할 인식의 혼선을 유발하며, 한국은 안보·경제 양 측면에서 동시에 압박을 받는 구조임.

2. 최근 사이버 보안 환경과 리스트 변화

- 사이버 공격의 대상은 대기업에서 중소기업, 개인, 비영리기관까지 확산되며 전 사회적 차원으로 확대되고 있음.
- 공격 방식은 네트워크 해킹뿐 아니라 물리적·오프라인 해킹과 결합하는 형태로 진화하고 있으며, 공급망 취약점을 활용한 공격도 증가하는 추세임.
- 공격 속도와 빈도는 높아지고 있으나 방어·대응 능력은 여전히 분산적이며, 한국은 사이버 생태계 전반의 복합적 위협에 취약한 상태임.

3. 미국· 중국의 AI 기술력 경쟁이 국제 안보 환경에 미칠 영향과 전망

- 미·중은 AI 반도체, 데이터, 알고리즘, 인재 확보 등 전 분야에서 총체적 경쟁을 심화시키고 있어 단순한 기술 경쟁을 넘어 경제·안보 전반을 압박
- AI 모델의 확산은 개인정보 보호와 데이터 안보 문제를 넘어 인지전 발생 가능성으로 이어질 수 있으며, 사회적 갈등과 분열을 유도할 위험이 존재
- AI 모델 개발·운영에는 막대한 전력과 냉각 인프라가 필요하며, 향후 에너지 안보 차원에서 SMR (소형모듈원자로) 등 대체 방안을 고려해야 하는 새로운 과제가 발생하고 있음.

4. 복합적·다면적 위협에 대응하기 위해 국제 사회가 취할 수 있는 전략적 협력 방식에는 어떤 것들이 있다고 보십니까?

- UN 등 국제기구와 다자 회의를 통해 사이버 공간에서 책임 있는 국가행동에 관한 규범을 정립하고 신뢰 구축 메커니즘을 발전시켜야 함.
- 실시간 위협 정보·악성코드·공격 기법 등을 공유하는 국제 정보공유 체계를 구축하여 탐지·대응 속도를 높이고, 조기 경보 시스템을 마련해야 함.
- 동맹국 및 파트너 간에는 합동 훈련, 핵심 기반시설 보호 연구·개발, 인재 양성, 복원력 강화 협력 등 전략적 연합 체계를 강화할 필요가 있음.

5. 신흥 안보 대응 전략을 '상황인식–탄력성–전략적 커뮤니케이션–통합적 정책–국제 협력'의 축으로 본다면, 현 시점에서 가장 우선 강화해야 할 요소와 그 이유는 무엇이라고 생각하십니까?

- 다섯 요소가 유기적으로 작동해야 하지만, 가장 근본적인 출발점은 '상황인식'이며, 위협을 인지하지 못하거나 잘못 인식할 경우 정책 실패와 협력 지연으로 연쇄 위기가 발생할 수 있음.
- AI, 드론, 사이버 공격과 같은 위협은 급격히 변형·확산되므로, 실시간 상황인식이 없다면 탄력적 대응이나 국제 협력이 무력화될 가능성이 큼.
- 국가·민간·국제 차원에서 협력 체계가 작동하기 위해서는 정확한 상황 파악과 역할 인식이 전제되어야 함. 이를 위해 정보 공유와 조기 경보 체계 강화가 필수적임.

6. 기타

- 다자 협력은 절차가 복잡하고 실행력이 낮을 수 있으므로, 협력이 용이한 분야에서 출발해 점진적으로 확대하는 현실적 접근이 필요함.
- 한국은 전략적 협력에서 신뢰 구축과 무임승차 방지 장치를 함께 고려해야 하며, 이는 소다자 협력 네트워크와 연계될 수 있음.
- 국제 규범 논의에서 한국은 중견국으로서 조정자 역할을 수행할 수 있으며, 이를 위해 전문 인력과 정책적 자원 투입이 필요하다고 지적됨.
- 해저 케이블(submarine cable, 또는 해저 광케이블)의 절단과 손상 사건은 국제 데이터 흐름과 핵심 인프라의 안정성에 직결되는 위협으로, 해저 케이블은 군사적·비군사적 행위자 모두가 노릴 수 있는 하이브리드 위협의 대표적 표적으로 부상하고 있음.

부록 2 : 2025 세계신안보포럼 라운드테이블(국내 행사) 상세 내용

행사 개요

- 행사 제목: 2025 세계신안보포럼 라운드테이블
- 행사 일시: 2025년7월14일(월) 15:00 ~ 18:00
- 행사 장소 : 포시즌스 호텔 서울 그랜드볼룸
- 행사 주제: '하이브리드 위협의 진화와 국제안보'주제 하에,
  - 세션1에서는 세계 각지의 하이브리드전의 양상 및 요소 등 하이브리드 위협의 실태에 대해서 발표와 토론을 진행,
  - 세션2에서는 하이브리드 위협의 진화가 국제안보에 미치는 영향에 대한 논의 진행
- 행사 구성 및 주요 참석자

세션	참석자
개회식, 축사	· 개회사: 이태우 외교부 국제사이버협력대사 · 축사: 배중면 한국과학기술원(KAIST) 안보융합원장 · 축사: 댄 스미스 스톡홀름국제평화연구소(SIPRI) 소장
세션 1	· 발제: 양욱 아산정책연구원 외교안보연구센터 연구위원 · 토론: 손인근 아주대학교 장위국방연구소 연구교수 조상근 사단법인 창끝전투 학회장 김은영 가톨릭관동대학교 경찰학부 부교수 · 좌장: 손한별 국방대학교 전략학부 교수
세션 2	· 발제: 박보라 국가안보전략연구원 하이브리드위협연구센터장 · 토론: 안형준 과학기술정책연구원(STEPI) 연구위원 이동연 한국인터넷진흥원(KISA) 국민피해대응단장 방준성 한국전자통신연구원(ETRI) 책임연구원 · 좌장: 김소영 한국과학기술원(KAIST) 과학기술정책대학원 교수

주요 내용

● 개회식

1) **개회사: 이태우 외교부 국제사이버협력대사**

오늘날 안보 위협은 군사·비군사, 물리·디지털, 국가·비국가 행위가 복합적으로 결합된 하이브리드 위협으로 진화하고 있음. 이는 사이버와 우주 공간으로 확장되며, 딥페이크 등 허위 정보는 인지전을 통해 민주주의와 사회적 신뢰를 훼손하고 있음. 우크라이나 전쟁은 드론, AI, 위성, 양자 기술이 전장을 변화시키는 단적인 사례이며, 주요 인프라에 대한 사이버 공격과 랜섬웨어 피해는 사회·경제적 혼란을 일상화하고 있음. 이러한 위협은 단일 국가나 기관만으로는 대응할 수 없기에 우리 정부는 UN을 포함한 국제무대에서 인권 중심 기술 활용, AI 군사적 이용 규범, 자율살상무기 논의에 기여하고 있으며, 사이버 안보 분야에서는 국제법 적용과 신뢰 구축을 위해 양자·다자 협력을 추진하고 있음. 외교부는 세계신안보포럼(WESF)을 통해 정부·기업·학계·시민사회가 함께하는 국제 거버넌스를 강화하고 있으며, 오는 2025년 9월 제5차 포럼에서는 하이브리드 위협의 진화와 국제 안보를 주제로 인지전·신기술·인프라 회복력 논의를 이어갈 예정임.

2) **환영사: 배중면 한국과학기술원(KAIST) 안보융합원장**

2025년 세계신안보포럼의 일환으로 마련된 오늘 라운드 테이블에 참석해 주신 국내외 귀빈과 연사 여러분께 진심으로 감사와 환영의 인사를 전함. 본 포럼은 변화하는 국제 질서 속에서 기술 기반 신안보 전략을 주제로 글로벌 협력을 모색하는 플랫폼으로 자리매김하고 있으며, 안보 개념은 이제 군사 분야를 넘어 기후, 에너지, 사이버, 인공지능(AI) 등 다양한 기술 이슈로 확대되고 있음. 이러한 환경 변화에 대응하고자 KAIST는 과학기술 최전선에서 문제 해결형 연구를 통해 국가 전략기술 확보와 글로벌 공공 가치 증진에 기여하고 있으며, 안보융합원을 중심으로 과학기술 기반의 정책 제안과 안보 생태계 강화에도 힘쓰고 있음. 오늘 회의는 본 포럼의 사전 논의로서 국내 전문가들이 신안보 이슈에 대해 공동의 문제의식을 공유하고 정책적 방향을 점검하는 자리이며, 국내외 시각이 연결되는 이번 만남이 오는 WESF 본회의로 이어지는 심도 있는 논의의 토대가 되기를 기대함.

3) **축사: 댄 스미스 스톡홀름국제평화연구소(SIPRI) 소장**

대한민국과 외교부가 제5차 세계신안보포럼을 준비하며 오늘 라운드 테이블을 개최한 데 대해 축하의 뜻을 전함. WESF는 지난 4년간 기술 중심 안보 이슈에 대한 국제적 논의의 장으로 자리잡았으며, 빠르게 변화하는 안보 환경 속에서 정부가 기술 변화에 창의적으로 대응할 수 있도록 돕는 플랫폼 역할을 해왔음. 최근 10년간 무력 분쟁과 인도적 피해는 증가하고 있으며, 핵확산금지조약(NPT), 포괄적핵실험금지조약(CTBT) 등 다자 군비통제 체제는 위기에 처해 있음. 동시에 전 세계 군비 지출은 사상 최고치를 경신했고, 기후 변화와 생태 위기 등 복합적 요인이 안보 불안을 가중시키고 있음. 기술 발전은 국제 안보 지형을 더욱 복잡하게 만들고 있으며, 인공지능, 자율 무기 체계, 사이버 공간, 우주 공간, 양자 기술 등은 기존의 전쟁과 평화, 국가와 비국가 행위자의 경계를 흐리고 있음. 특히 양자 컴퓨팅, 통신, 센싱 기술은 보안, 감시, 암호화 등 전략적 영역에서 새로운 기회를 제공함과 동시에 불균형적 경쟁과 새로운 군비 경쟁(Quantum Arms Race)을 야기할 가능성이 있음. 이러한 기술의 안보적 영향을 분석할 수 있는 전담 기관의 필요성을 강조하며, 오는 9월 포럼이 실질적이고 혁신적인 논의의 장이 되기를 기대함.

세션 1

1) (발표: 양욱 아산정책연구원 외교안보연구센터 연구위원) 하이브리드 위협의 실태

– 전쟁세대의 발전과 안보환경의 변화

① 전쟁 세대의 구분

그림 19. 전쟁 세대의 발전 과정

· 전쟁은 1세대 선형전, 2세대 화력·소모전, 3세대 기동전, 4세대 비정형·내러티브 중심전으로 발전해왔음. 차세대 전쟁은 인지 중심의 다차원·융합전으로, JADO, DCW, 모자이크전, 에이전트전 등이 대표적이며 정보화·지능화 기술과 결합된 네트워크 기반 양상이 특징임.

② 안보환경의 변화

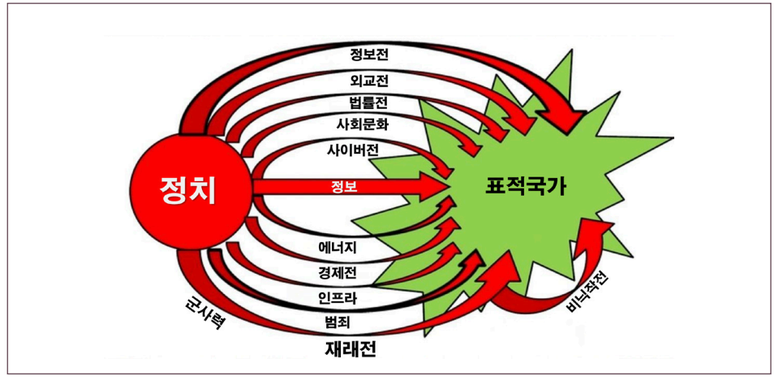
· 탈냉전 이후 이념 대결 구도는 수정 민주주의 체제로 이행되며 다양한 정치 형태가 등장함. 경제·사회는 다극화·정보화가 심화되고 있음. 군사환경은 총력전·국민군 체제에서 신속결정전·전문군 체제로 전환됨. 국제안보체제는 약화되고 일방주의가 대두됨. 미중·미러 패권 충돌, 팬데믹 등 비전통적 위협이 새로운 핵심 위험 요소로 부각됨.

③ 전쟁 비용 및 인명 피해의 부담 증가

· 20세기 전쟁은 수천만 명의 희생을 낳으며 경제·정치적 부담이 막대했음. 현대전은 인명 피해가 감소했으나, 인명의 가치 상승으로 정치적 부담은 오히려 커짐. 비정규전·대테러전에서는 침공 이후 더 큰 피해가 발생해 미국의 쇠퇴 요인으로 작용함

– 크림 병합과 러시아식 전쟁 수행

그림 20. 하이브리드전의 개전 양상



① 전쟁 비용 회피와 하이브리드 접근

· 전면전의 경제·정치적 부담을 회피하기 위해 러시아는 저비용 고효율 전략으로 전환했으며, 2014년 크림 병합은 군사력 외 다양한 수단을 동원한 대표적 하이브리드 전쟁 사례로 국제 질서에 충격을 줌.

② 러시아의 하이브리드 전쟁 방식

· 러시아는 군사력과 함께 정보·외교·법률·사이버·에너지 등 국가 수단을 통합 활용하며, 비인가 병력을 동원한 은폐 작전과 게라시모프 독트린을 통해 비군사적 수단 중심의 무력화를 추구함.

③ 크림 병합의 전개 과정

· 러시아는 정치 공작과 군사작전을 병행해 크림 권력을 장악하고, 무력시위·조작된 투표를 통해 합병을 정당화했으며, 미국·EU는 제재로 대응했으나 군사적 억제에는 실패함.

④ 하이브리드 전쟁 개념의 부상

· 크림 사태는 전쟁과 평화 사이 회색지대를 부각시키며 기존 대응의 한계를 드러냈고, 이후 미국을 중심으로 하이브리드 위협 연구와 개념 정립이 확산됨.

– 하이브리드 위협의 정의

① 위협 스펙트럼상의 위치

· 하이브리드 위협은 사이버 공격, 가짜 뉴스, 선거 개입, 해양 도발 등 전면전 이전 단계의 적대 행위로, 전통적 군사 충돌과 그레이존 사이에 위치함.

· 본격적 군사력 대신 비정규 수단으로 정치적 목적을 달성하며, 크림 합병이나 이스라엘-하마스 충돌 초기 사례에서 확인됨.

② 하이브리드 위협의 구성 요소

· (주체의 확장) 국가뿐 아니라 비국가 행위자도 적극 개입함.

· (수단의 총동원) 군사 충돌 없이 사이버·정보·외교·경제 등 비군사 수단을 종합 활용함.

· (가시성과 책임성의 불투명성) 공격 주체와 피해가 불명확해 책임 규명이 어려움.

③ 재래식 위협과의 비교

· 무력 충돌 없이도 제도와 신뢰를 무너뜨려 정치적 목적을 달성함.
· 국제법의 경계를 회피해 법적 대응이 어렵고, 전통적 억제 수단으로는 대응 한계가 있음.
· 대응에는 민간을 포함한 전사회적·전정부적 통합 접근이 요구됨.

④ 일상화된 위협으로서의 성격

· 평시에도 상시적·비정형적 공격이 지속되며, 반복적 성격을 가짐.
· 한국은 북한과의 관계 속에서 이러한 위협을 구조적으로 경험해온 대표 사례임.

– 대표적 교전형태: 인지전 (cognitive warfare)

① 인지전의 정의와 특징

· 인지전은 상대의 인식과 결심을 교란해 판단 속도와 정확성을 저하시키며 전략적 우위를 획득하려는 공격형태임. 판단 흐림을 통한 의사결정 마비와 정보 신뢰성 저하가 핵심 수단임.

② 하이브리드 위협과의 연결성

· 하이브리드 위협은 법률·문화·제도 등 사회 전반을 겨냥한 내러티브 공격으로 나타나며, 인지전은 그 핵심 축으로 상시적·비대칭적 영향력을 행사함. 물리적 충돌 없이도 사이버·정보 공간을 통해 24시간 전개될 수 있음.

③ 러시아식 인지전의 방식

· 러시아는 재귀통제(recursive control) 등 판단 흐림 기법과 의사결정 교란 전술을 활용해 상대의 리더십과 의사결정 능력을 약화시키는 방식으로 인지전을 수행함. 우크라이나 전개 사례에서처럼 하이브리드 수단과 결합해 전투 이전부터 전략적 우위를 구축하려 함.

– CORE(Comprehensive Resilience Ecosystem) 모델을 통한 하이브리드 위협 분석

① CORE 모델

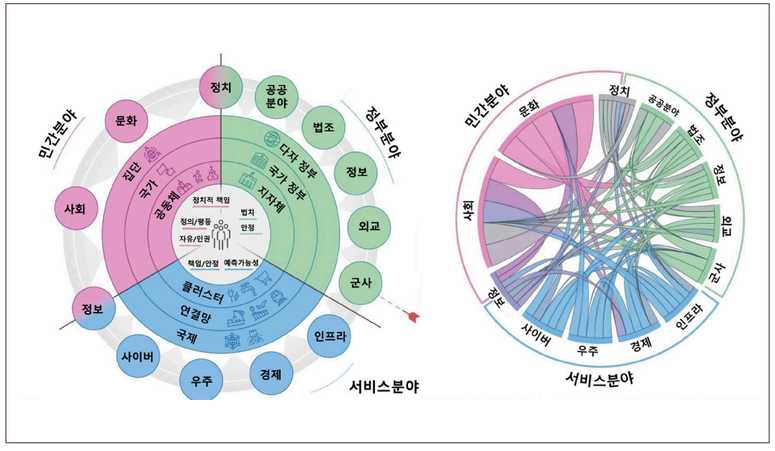


그림 21. EU의 CORE 모델

· CORE 모델은 EU가 사회적·제도적 연결망을 기반으로 하이브리드 위협의 영향 경로를 시각화한 분석 도구임. 서비스·민간·정부 분야 간 상호작용을 원형·연결선 형태로 표현해 취약점과 전이 경로를 한눈에 보여줌.

② 공격 방식과 전달 구조

· 하이브리드 공격은 특정 도메인을 겨냥해 '선택적 침투'를 시도하고, 연결망을 통해 파급효과를 확대해 시스템적 불안정을 유도함. 이러한 전달 구조는 직접적 물리 충돌 없이도 정치·사회적 신뢰를 침식시키는 데 효과적임.

③ 적용 사례의 시사점

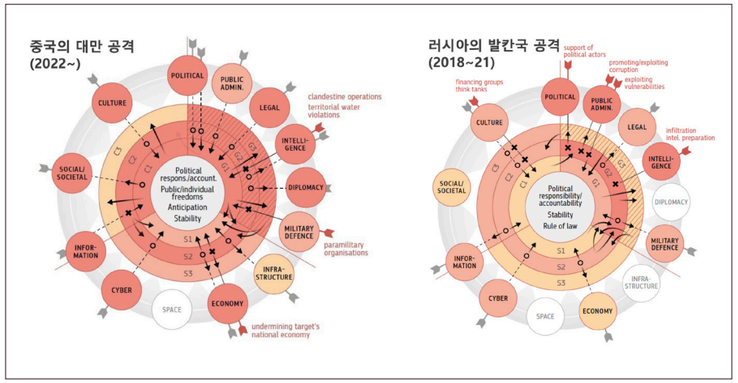


그림 22. 중국과 러시아의 사례에 대한 CORE 모델

· 대만 사례에서 정치·공공행정 취약성이 부각되었고, 발칸 사례에서는 정치·문화·정보 영역이 연결망을 통해 국가 신뢰를 약화시킴. CORE 모델은 우선 방어 대상과 긴급 대응 우선순위를 설정하는 국가 전략 수립에 직접적으로 활용 가능함.

– 결론: 가치 기반 회복탄력성

① 신속한 탐지와 역할 분담

· 위협을 조기에 인지할 수 있도록 감시·정보공유 체계를 강화해야 함과 동시에 정부 부처별 책임과 권한을 명확히 규정해 대응 혼선을 방지해야 함.

② 민관 통합의 필요성

· 사이버·인지 영역을 포함한 하이브리드 위협에 대응하기 위해 민간의 능동적 참여와 협력체계를 구축하고, 민관 합동 시나리오·훈련을 정례화해야 함.

③ 회복탄력적 대응 체계

· 조기 탐지→명확한 책임 분담→즉각적 억제의 순환을 갖춘 억제·대응 메커니즘을 마련하고, 전사회적(total-society) 역량을 총동원하는 체계로 운영해야 함.

④ 하이브리드 위협에 대한 정의

· 하이브리드 위협을 군사·비군사 수단의 창의적 결합으로 규정하고, 법·외교·정보·경제 등 모든 정책수단을 통합한 장기적 회복전략을 수립·적용해야 함.

2) (토론/ 좌장: 손한별 국방대학교 전략학부 교수)

- 손인근 아주대학교 국방외국방연구소 연구교수

① 부처간 자산 공유·협업 부족
사이버·전자·우주 도메인 기반 하이브리드 위협에 대응하려면 각 부처가 보유한 정보와 자산을 상시 공유할 체계가 필요하나, 현재 협업 시스템이 미흡하여 협업 실패 사례가 반복되고 있음.

② 민간 기술 활용 모델
미국방부는 5G·AI·클라우드 등 민간 기술을 적극 도입하여 초연결·초지능 네트워크를 구축하고 있으며, 이러한 민관 협력은 위협 판단·대응 속도를 높이는 데 기여함.

③ 법·제도·거버넌스 선행 과제
네트워크를 넘어선 융합 시스템을 구현하려면 관련 법·제도 정비와 거버넌스 구축이 선행되어야 하며, 미비 시 국가 차원의 하이브리드 위협 대응 능력이 제한될 위험이 있어 조속한 개선이 필요함.

- 조상근 사단법인 창끝전투 학회장

① 하이브리드·인지전 용어의 기원
권위주의 세력이 아니라 자유민주 진영이 제3자 시각으로 붙인 명칭이므로, 당사자 행위를 정확히 반영하지 못해 오해와 시행착오가 발생함.

② 핵심 속성 1: 애매모호성(ambiguity)
상용 드론·클라우드·통신망 등 누구나 쓸 수 있는 상용서비스를 전장에 투입하면 의심이 어려워지며, 리치-백(reach-back) 형태 원격 조종이 전쟁 양상을 재구성함.

③ 핵심 속성 2: 자유민주 취약성 파고들기
권위주의 군은 정치 목적 달성을 위해 법·윤리를 개의치 않는 반면, 자유민주 국가는 인권·법치(ROE)에 묶여 있어 AI전투 알고리즘도 젠틀하게 세팅됨. 동일 잣대에서 충돌 시 자유민주 측이 불리해질 위험이 큼.

④ 정의 남용의 함정·사례별 접근 필요
'모든 것이 하이브리드/인지전' 식의 포괄적 규정은 현실을 흐리므로, 애매모호성·취약성 등 속성을 면밀히 따져 케이스-바이-케이스로 분석·대응해야 함.

- 김은영 가톨릭관동대학교 경찰학부 부교수

① 회색지대의 전략적 중요성과 애매모호성
하이브리드 전쟁에서 전면전과 평시 사이의 회색지대가 핵심 영역이며, 가장 위험한 요소는 그 모호성임. 이 회색지대는 정치 체제(민주주의 vs 권위주의)나 사회의 내러티브 취약성에 따라 위험성이 달라지며, 인지전은 이 회색지대를 통해 침투함.

② 인지전에 대한 국가적 인식 부족
우리 사회는 인지전에 대한 전략적 중요성을 인식하고 있으나, 인지전의 정의, 범위, 적용 방식 등에 대한 명확한 공감대가 부재함. 하이브리드 전쟁의 인간 영역을 다루는 인지전에 대한 개념 정립이 시급함.

③ 정부 거버넌스의 부재
민간 기술의 기여 가능성은 크지만, 기술 활용의 기준과 경계를 설정할 정부의 가이드라인과 거버넌스가 부족함. 손 교수의 지적처럼 무엇을 해야 하고 하지 말아야 하는지에 대한 국가 차원의 규범 마련이 필수적임.

④ 사회적 접근과 국가 역할
하이브리드 전쟁에 대비하기 위한 사회적 접근(society approach)을 완성하기 위해서는 정부 주도의 거버넌스와 제도 설계가 중요함. 민간의 기술 주도성을 인정하되, 전쟁이라는 총체적 상황에서 국가와 공공기관의 리더십이 필수적임.

세션 1 Q&A

좌장 질문 1

하이브리드 위협이 모든 상황을 포함한다면 항상 전쟁 상태에 있는 것인지, 모든 위협에 대응해야 하는지, 그렇지 않다면 어디까지를 위협으로 보고 어떻게 대응할지를 구분해야 하는가?

답변(양욱 발표자)

전쟁이 상시적 현상이라는 인식은 일정 부분 타당함. 그러나 모든 위협을 동일하게 대응하면 사회 전체가 피로해지므로, 일상적 인지전까지 국가가 직접 관리하는 것은 비현실적임. 따라서 민·관·군의 역할을 구분해 생태계 기반 방어체계를 구축해야 함. 정부의 과도한 통제보다는 민주주의 국가에 적합한 정치적 합의와 권한 분산 구조가 마련되어야 하며, 이는 정책 차원이 아니라 정치권이 해결해야 할 구조적 과제임.

좌장 질문 2

사이버전·인지전의 애매모호성을 고려해 인지전 위협을 빠르고 정확히 탐지할 수 있는 시스템을 어떻게 설계해야 하는가?

답변(김은영 토론자)

인지전 탐지는 단순 기술 의존이 아니라 무엇을 탐지할지 규정하는 것이 핵심이므로, 사회공학적 베이스라인(감정·판단 기준·심리적 취약성)을 확보하고 비정상 행위 패턴을 식별하는 맞춤형 AI(예: 트랜스포머 기반 딥페이크·허위정보 탐지)와 인간 전문가의 교차검증 체계를 결합해야 함. 민·관·군의 융합 조직을 구성해 역할을 분담하고, 탐지 모델은 국가·집단별 내러티브 특성을 반영해 설계해야 함.

좌장 질문 3

수많은 하이브리드 위협 중 대한민국이 가장 취약한 분야는 무엇이며, 유럽 등 타국과 비교했을 때 위협 인식에는 어떤 차이가 있는가?

답변(김은영 토론자)

대한민국은 국민·정부·군 간 신뢰를 흔드는 인지전에 특히 취약함. 북한은 허위정보로 내부 분열을 유도하고 있으며, 한국은 무인기 침투 사례에서 보듯 다부처 통합 대응이 미흡함. 반면 우크라이나는 역정보 대응센터, 이스라엘은 총참모부 산하 대변인 부대를 통해 실시간 검증체계를 운영 중임. 동유럽 국가는 다음 차례라는 위기의식 속에 적극적 대응에 나서지만, 한국은 정치적 부담으로 정부·군 모두 주저하는 상황임. 따라서 국민적 공감대 형성과 데이터 축적, 범정부적 조기 대응 체계 제도화가 시급함.

좌장 질문 4

하이브리드 위협 대응을 위한 법·제도 정비에서 한국의 현실적 역량을 고려할 때 어떤 영역에 우선순위를 두어야 하는가?

답변(김은영 토론자)

기존의 경계선 기반 보안은 클라우드·사이버 위협 환경에 적합하지 않으므로, 제로트러스트(Zero Trust) 개념처럼 지속적 검증 구조를 적용해야 함. 하이브리드 위협은 경계 없는 침투가 특징이므로 전통적 부처 분할 체계로는 대응이 불가하며, 협업 중심의 융합 거버넌스 체계가 필요함. 따라서 법·제도 정비는 위협을 감지·판단할 수 있는 종합 시스템 설계에 우선순위를 두고, 그 운용에 맞는 규범과 절차를 단계적으로 보완해야 함.

좌장 질문 5

하이브리드 위협 속에서 전략적 중심(center of gravity)은 여전히 전통적 국력 요소에 있는가, 아니면 인지전 등 비물리적 요소로 이동하고 있는가? 우리가 가장 우선적으로 보호해야 할 영역은 무엇인가?

답변(양욱 발표자)

전략적 중심은 고정된 것이 아니라 위협 구조에 따라 유동적으로 변화하며, 전쟁의 단계별 목표를 붕괴시키기 위해 다차원적으로 탐색·공격되는 개념으로 이해해야 함.

답변(김은영 토론자)

핵무기와 같은 물리적 수단은 여전히 결정적이지만, 미래에는 인간이 사이버와 직접 연결되는 구조로 진화할 가능성이 크므로 사이버 공간이 전략적 중심의 핵심이 될 수 있음.

인지전 역시 뇌와 연결되므로 우선적 대응 영역으로 간주해야 함.

답변(조상근 토론자)

전략적 중심은 각 도메인의 핵심 노드를 제거해 전체를 무력화시키는 개념으로, 물리적·비물리적 방식 모두 가능함. 이스라엘-하마스 분쟁과 러시아-우크라이나 전쟁 사례처럼 시기·상황에 따라 달라지며, 이를 조직·평가하는 주체가 장기적으로 핵심임.

답변(손인근 토론자)

하이브리드전은 전쟁 양상을 변화시키는 수단일 뿐, 승패를 좌우하는 결정적 요인으로 보기는 이르며, 전략적 중심은 여전히 기존 전쟁의 핵심 요소들에 있음.

청중 질문 1

하이브리드 위협 시대에서 정부는 어떤 정보를 공개하고, 어떤 정보를 감춰야 하는가? 외교·안보 정책 변화기에 평화와 안보 균형을 위한 고려사항은 무엇인가?

청중 질문 2

이스라엘 사례처럼 국가의 잠재 능력을 대응력으로 전환하는 정부의 자율성이 중요하다면, 한국 정부가 하이브리드 위협에 맞서 자율성과 동원 능력을 강화할 수 있는 제도적 방안은 무엇인가?

청중 질문 3

한국 정부가 현재 하이브리드 위협에 대해 실행 중인 구체적 대응 조치나 반격 전략이 있는가? 또한 외국발 정보 위협을 조기 탐지·경보할 수 있는 시스템이 마련되고 있는가?

청중 질문 4

러시아-우크라이나 전쟁에서 사망자 통계가 상이한 것은 단순 집계 차이인지, 전략적 정보 왜곡인지 궁금함. 또한 통계 시각화에서 객관성을 보장하기 위한 적절한 기준은 무엇인가?

청중 질문 5

하이브리드 위협과 하이브리드 전쟁은 개념과 주체가 다르다고 보는데, 군 중심인지 정부 전체인지에 따라 대응 체계가 달라질 수 있음. 이에 대한 개념적 정리가 필요하지 않은가?

답변 (양욱 발표자)

한국 정부의 대응은 국익 중심 실용 전략에 기반해야 하며, 방어 주체로서 명확한 입장을 가져야 함. 하이브리드 위협은 범정부적 접근이 필요하지만, 하이브리드 전쟁은 군 개입 단계로 개념을 구분해야 함. 군사적 개입 여부에 따라 대응 주체와 위상이 달라짐.

답변 (조상근 토론자)

우크라이나는 전쟁 장기화 속에 국민 전체를 예비 전력화하고 첨단 기술 교육으로 안보 의식을 고양해 왔음. 한국도 민방위 훈련 등 제도를 실효성 있게 운영해야 함. 또한 러시아발 사망자 통계는 정치적 목적에 따른 왜곡 가능성이 크므로, 자유민주 진영과 권위주의 진영의 통계를 교차 검증해 평균치를 도출하는 방식이 객관적임. 데이터 해석에는 정치적 의도를 고려해야 함.

답변 (김은영 토론자)

한국은 북한발 유튜브 채널 차단, 대북전단 논의 등 인지전 대응 사례가 있으나 정치적 상황으로 제도화와 통합 대응체계 마련은 지연되고 있음. 미국은 글로벌 인게이지먼트 센터, 사이버 커맨드 등 유형별 조직적 대응체계를 운영 중임.

답변 (손인근 토론자)

한국은 해킹·침해사고 대응에서 기관별 사이버 보안 시스템은 운영 중이나, 범정부 차원의 사이버 정보전 대응은 미흡함. 위협 정보의 전략적 분석과 공유, 이를 기반으로 한 정책 대응이 통합적으로 추진되어야 함.

세션 2

그림 23. 2005년 런던 77 테러

출처: BBC News. (2015) "Ken Livingstone: Tony Blair to blame for 7/7 bombings" (검색일: 2025.9.28.)

1) (발표: 박보라 국가안보전략연구원 하이브리드위협연구센터장) 하이브리드 위협과 국제안보의 변화

– 런던, 2017년 3월

① 자생 테러의 충격

· 2005년 런던 7·7 테러는 이주민 1.5·2세대가 자국민을 대상으로 일으킨 자생 테러로, 영국 사회에 큰 충격을 주며 국경 중심 대테러 전략의 한계를 드러냄.

② 웨스트민스터 테러 발생

· 2017년 3월 22일 의사당 인근에서 차량 돌진과 흉기 난동으로 3명 사망, 40명 부상 발생함. 가해자가 영국 태생 무슬림으로 밝혀지며 사회적 공포와 반이민 정서가 재점화됨.

③ 소셜미디어 통한 내러티브 확산

· 테러 발생 2시간 만에 '무슬림 여성이 부상자를 외면했다'는 트윗이 확산되었고, 트럼프 지지 계정으로 위장된 트롤 계정이 주도함. 혐오 이미지와 함께 리트윗되며 반이민·반난민 정서를 자극함.

④ 정보전 형태의 하이브리드 위협

· 문제 계정은 이후 러시아 크렘린과 연계된 사이버 트롤로 확인되었으며, 사건 발생 시 여론을 조작하는 슬리핑 셀 방식으로 활동함. 이 사례는 테러 직후 온라인 내러티브로 사회 분열을 유도한 하이브리드 위협의 대표적 사례로 평가됨.

– 국제안보환경의 전환

① 기존 안보 개념의 한계

· 하이브리드 위협은 유형·수단·범위가 다양해 국가별·사례별로 양상이 달라 단일 대응책으로는 한계가 있으므로 전 정부적 맞춤형 접근이 필요함.

② 예측 불가능한 위협의 부상

· 새로운 위협은 예상 불가능하거나 상상 밖 형태로 나타나 과거의 확실성에 의존할 수

없으므로, 전통적 안보 모델을 재정립해야 함.

③ 국가 시스템과 의사결정에 대한 공격

· 하이브리드 위협은 물리적 피해가 아니라 국가 시스템과 민주주의적 의사결정을 마비시키는 것을 목표로 하며, 이는 전통적 안보 개념을 넘어서는 도전임.

– 하이브리드 위협의 개관

① 담론의 중심에 선 허위조작정보

· 허위조작정보는 하이브리드 위협에서 가장 자주 언급되는 핵심 주제이며, 대안적 진실·기만·소셜미디어 등을 통해 장기간에 걸쳐 제도적 기반을 약화시키는 상시적 위협으로 기능함.

② 진실의 제도적 붕괴: RAND 보고서 분석

· 2018년 RAND 보고서는 인지 편향·정보체계 변화·교육·사회 양극화 등을 '동인'으로 사실·의견 경계의 흐려짐과 신뢰 약화의 '추세'를 거쳐 시민 담론 위축·정치 마비로 이어지는 '결과'로 진실 붕괴 과정을 제시함.

③ 사이버공격과 기반시설 마비 시도: SKT 사례

· 2025년 5월 7일 보도된 SKT 해킹 사건은 단순 정보 탈취를 넘어 에너지·교통 등 핵심 인프라에 대한 사전 준비 공격 가능성을 시사하며, 이는 하이브리드 위협의 물리적 기반 위협 전개 양상과 연계해 해석될 수 있음.

④ 하이브리드 위협의 전략적 양상

· 하이브리드 위협은 국가·비국가·모호한 행위자에 의해 사이버·심리·정보·경제 등 비군사 수단을 단계적·비가시적으로 동원해 국가 시스템과 사회 안정성을 와해하려는 전략적 특성을 보임.

– 하이브리드 위협 대응

① NATO: 준비-억제-방어의 3단계 구조

· NATO는 Prepare-Deter-Defend의 3단계 접근을 채택하며, 내러티브·허위조작정보·사이버공격에 대응하기 위해 훈련·지원팀 운영·정보 공유·연구 참여 등 4가지 축을 중심으로 실행함. 사이버 위협의 초국경적 특성 때문에 동맹국 간 정보 공유가 핵심임.

그림 24. NATO의 준비-억제-방어의 하이브리드 위협 대응법

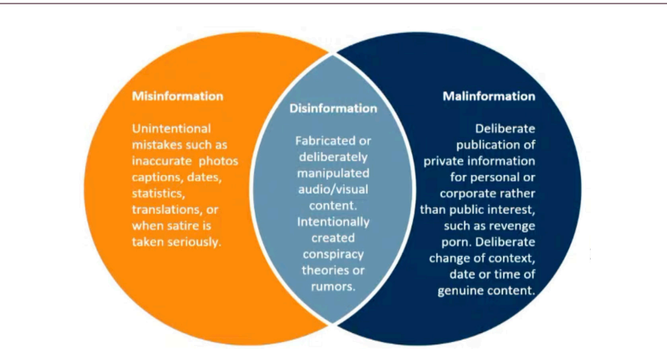
② EU: 상황 인식과 회복 중심의 전 정부적 대응

그림 25. EU의 하이브리드 위협 대응 방안

· EU는 대중의 위협 인식 제고를 출발점으로 삼고, 발생한 위협에 대한 신속 회복 체계를 강조함. 대응은 역내·역외 협력을 전제로 하며, 2023년 헤이그 프레임워크에서는 준비-탐지-의사결정-실행-평가의 5단계 모델을 제시하고, 특히 '귀속(공격 주체 식별)' 문제를 핵심 과제로 지목함.

③ 허위조작정보 대응: EU의 FIMI 프레임워크

그림 26. EU의 FIMI 프레임워크



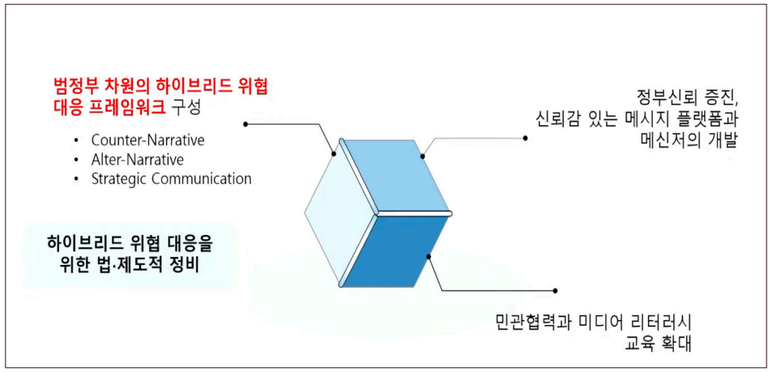
· 허위조작정보는 콘텐츠 자체보다 유포 과정과 효과에 주목해 분석해야 하며, EU의 FIMI 프레임워크는 의도적 유포 행위를 프로파일링 기법처럼 추적·분석함. 표현의 자유와 신속 대응의 균형을 모색하며, 법적 근거와 다부처 협력을 전제로 운영됨.

④ 영국과 호주의 제도 기반 대응

· 영국은 '국가 위협(State Threat)' 개념 하에 총리실-내무부-외무부-MI5가 협력하며, 국가안보법 제정을 통해 형사처벌까지 연계 가능한 체계를 마련함. 호주는 'FIMI' 또는 '국가 위협' 개념을 도입해 정보기관·수사기관·외교부·내무부가 참여하는 다채널 전략을 운영함.

– **對韓 시사점과 고려사항**

그림 27. 하이브리드 위협에 대한 시사점



① 범정부적 프레임워크의 필요

· 하이브리드 위협은 특정 부처가 단독 대응할 수 없으므로, 상황에 따라 외교부·수사기관·행정안전부 등 주도 부처가 달라지는 범정부적 협력 체계를 수립해야 함.

② 내러티브 대응의 중요성

· 내러티브는 위협 확산을 좌우하는 핵심 요인으로, 사회적 기억과 감정을 자극해 허위조작정보보다 강력한 파급력을 가질 수 있음. 다문화·다인종화가 진행되는 한국 사회에서 내러티브 취약성 관리가 중장기 과제가 되어야 함.

③ 정부 신뢰와 메시지 전략

· 전 정부적 대응이 효과를 가지려면 국민 신뢰가 선결 조건이며, 신뢰할 수 있는 메신저와 플랫폼을 통해 사회적 설득 구조를 마련해야 함.

④ 민간 참여와 리터러시 교육

· 시민 개개인이 대응 주체임을 인식시켜야 하며, 이를 위해 온라인 플랫폼 중심의 미디어 리터러시 교육을 강화해 정보 판별 능력을 높여야 함.

⑤ 법·제도 기반 정비

· 한국은 관련 법·제도 기반이 미비하므로, 상황별 대응 권한 배분과 수사·외교·대국민 대응을 포괄하는 총체적 입법과 제도 정비가 시급함.

2) (토론/ 좌장: 김소영 한국과학기술원(KAIST) 과학기술정책대학원 교수

– **안형준 과학기술정책연구원(STEPI) 연구위원**

① 우주를 하이브리드 위협에 포함해야 하는 이유

우주는 인지전·사이버전처럼 평화적 이용과 군사적 활용 간 경계가 불분명하고, 주체 식별·의도 파악·책임 귀속이 어려운 특성을 지님. 이러한 모호성과 비정형성은 하이브리드 위협의 핵심 특징과 부합함.

② 위성 해킹 등 비물리적 공격의 전략적 파괴력

최근에는 고비용 발사체 없이도 해킹 등을 통해 위성 시스템을 교란하거나 정보 탈취가 가능함. 이는 전면전 없이도 국가 사회의 핵심 인프라를 마비시킬 수 있는 비대칭적 수단으로 부상함.

③ 우주 인프라 의존도 증가에 따른 국가 리스크

GPS·항법 시스템·위성통신 등은 군·민을 불문하고 필수 인프라가 되었음. 해당 시스템이 외부 공격이나 지정학적 결정(예: 미국의 GPS 차단)에 의해 중단될 경우, 국제적 혼란 초래 가능성이 큼.

④ 국제 규범 논의와 기술 블록 형성의 초기 움직임

우주 시스템을 둘러싼 규범화 및 국제 협력 논의가 진행 중이나 구체화는 미흡함. 한편, 미국·유럽·일본 간 군집 위성 협력 등 미중 이외의 제3 블록 형성이 나타나고 있어, 한국의 전략적 판단이 요구됨.

⑤ 미국 우주 정책의 불확실성과 대응 필요성

미국의 정치적 불확실성은 국제 우주 질서의 안정성에도 부정적 영향. 한국은 미중 경쟁 구도에만 주목하지 말고, 다자협력·기술 독자화·전략적 외교 등을 병행하는 능동적 대응이 필요함.

– **이동연 한국인터넷진흥원(KISA) 국민피해대응단장**

① 사이버 사고의 파급력과 비의도적 위협 가능성

2023년 글로벌 소프트웨어 업데이트 장애로 공항, 병원, 금융기관, 911 서비스 등이 마비됨. 이는 고의적 공격이 아님에도 불구하고 사이버전 수준의 피해를 초래했으며, 현대 사회의 디지털 기반 시스템이 얼마나 위협에 취약한지를 보여줌.

② 고도화되는 공격 형태와 AI의 활용

랜섬웨어, DDoS 공격은 여전히 비용 대비 효과적인 수단이며, 사이버 용병·익명 해커 집단을 통한 대리 공격도 증가 중임. 특히 AI 기술이 접목되면서 공격의 정밀도와 속도가 급격히 향상되고 있어, 단순 대응을 넘어선 전략적 대응체계 필요함.

③ 디지털 전환과 하이브리드 위협의 결합

코로나 팬데믹 이후 디지털 전환이 급진전되며 사이버 위협 또한 가속화됨. 물리적·사이버 공격에 더해 심리전이 동반되는 복합 위협 양상이 뚜렷해지고 있으며, 국가 안보 차원에서 이에 대한 통합 대응이 필수적임.

④ 민관 협력과 정보 공유 체계의 중요성

KISA는 피싱·스미싱 대응, 통신사 해킹 사고 대응 등에서 정부·기업·금융기관과 협력 체계를 유지 중임. 은밀하고 장기적인 기반시설 공격에 대응하기 위해선, 보안 취약점 정보의 신속한 공유와 공동 대응 체계가 필수적임.

⑤ 사이버 레질리언스를 위한 체계적 대응

국가안보실을 중심으로 한 거버넌스 체계 하에 KISA는 KR-CERT 운영, 민간 보안 대응, 기술개발(R&D) 등을 수행 중임. 특히 기반 인프라 보호와 관련된 협력, 취약점 공개와 대응, 국제 접점 역할 수행이 미래 신뢰사회 구축의 핵심 과제로 강조됨.

– **방준성 한국전자통신연구원(ETRI) 책임연구원**

① 기술의 민주화와 위협의 보편화
인터넷 기반의 기술 공개와 도구의 접근성 향상으로 인해, 누구나 마음먹고 공격할 수 있는 환경이 조성됨. 이제는 단순한 기술 개발보다 어떤 기술을 어떤 방향으로 활용할 것인지, 전략적 판단과 인식의 전환이 더 중요함.

② 알려지지 않았거나 알고도 속는 위협에 대한 대응 필요
하이브리드 위협의 핵심은 비가시적이고 모호한 위협임. 딥페이크나 허위정보처럼 인지하고도 속는 위협은 AI 기반 대응 전략 개발이 필수적이며, AR 시뮬레이션 등 새로운 예측·식별 도구에 대한 연구가 절실함.

③ 회복력(resilience) 중심 대응 전략의 중요성
현대 위협은 패턴화된 공격이 아니며, 개인도 치명적 위협을 가할 수 있음. 기술·조직·인적 차원의 복합 대응이 요구되며, 단순 방어가 아닌 전체 시스템의 회복력 구축이 핵심 전략이 되어야 함.

④ AI 추론 격차와 전략 설계 문제
의사결정이 추론 기반으로 전환되면서, AI 인프라 격차가 전략 수립과 실행에 영향을 미침. 미국 등 AI 선도국과의 격차를 고려해 독자적 데이터 인프라 및 추론형 전략 수립 역량 강화가 요구됨.

⑤ 프로세스 중심의 AI 보안 기술 접근 필요
AI 기술은 단일 기능 대체가 아닌, 위협이 집중되는 프로세스 단위에서의 적용이 효과적임. 노동집약적·위험집중적 공정에 대한 분석을 통해, AI 기반 안보 대응 기술을 실질적으로 연구·개발해야 함.

세션 2 Q&A

청중 질문 1

영국이나 호주가 '하이브리드 위협' 대신 '국가 안보', '해외 영향력' 등의 표현을 사용하는 이유는 무엇이며, 이러한 용어 선택이 국민적 공감대 형성에 도움이 되었는가?

답변(박보라 발표자)

하이브리드 위협은 개념이 모호하고 유형이 다양하기 때문에, 영국·호주는 대응 프레임워크를 명확히 하기 위해 '해외 영향력(foreign influence)'이나 '허위조작정보(disinformation)'처럼 직관적 용어를 사용함. 용어 선택만으로 국민적 공감대가 형성된 것은 아니지만, 정치인 연루 사건 등 구체적 사건이 발생하면서 경각심과 정책 대응 필요성에 대한 공감대가 강화되었음.

청중 질문 2

초고령 사회에서 청년들이 혐오가 만연한 정보 환경 속에서도 미래를 이끌기 위해 긍정적 여론을 형성하려면 어떤 법제화가 필요하고, 정부는 어떤 역할을 해야 하는가?

답변(박보라 발표자)

하이브리드 위협 속 실제 피해자는 평범한 시민임을 간과해서는 안 됨. 혐오 표현에 대한 법적 규제는 필요하지만, 무엇보다 사회가 '레드라인'을 합의하고 이를 넘는 발언에 침묵하지 않고 연대하는 문화가 중요함. 혐오는 연대와 통합을 이길 수 없으며, 시민이 공동체적 책임감을 가지고 대응할 수 있도록 정부는 제도적 장치와 환경을 마련해야 함.

청중 질문 3

사이버 위협이나 국가안보 위협을 조기에 탐지하고 정책으로 연결하기 위한 체계는 실제로 얼마나 실효성 있게 작동하고 있는가?

답변(이동연 토론자)

사이버 보안은 '제로 트러스트(Zero Trust)' 기반으로 전환 중이며, 신원 검증 후 최소 권한만 부여하는 구조를 실증하고 있음. 정부와 민간이 협력해 가이드라인을 마련 중이며, 공급망 보안(SBOM)도 미국 기준을 참고해 국내 적용을 추진하고 있음.

답변(방준성 토론자)

생성형 AI로 이미지·글의 대량 생산이 가능해지면서 진위 판별이 어려워졌음. 전면 검열은 불가능하므로 선거·안보 등 핵심 영역에 워터마크, 태깅, 원본 소스 비교 등을 적용하고 있음. 사실 검증 비용이 크기 때문에 위협 우선순위를 정한 선택적 대응이 이루어지고 있음.

청중 질문 4

북한이 한국에 우주 기반 공격을 감행할 수 있는 능력을 보유하고 있는가? 러시아도 스타링크를 차단하지 못하는 상황에서 북한의 위협 수준은 어느 정도인가?

답변(안형준 토론자)

북한은 위성 신호 교란(재밍) 등 우주 영역에서 하이브리드 위협 활동을 시도한 사례가 있음. 그러나 출처가 불분명하거나 부인되는 경우가 많아 '귀속 문제'가 핵심 난제로 남음. 이러한 특성상 실제 위협 여부를 기술적으로 입증하기는 어렵지만, 우리 정부는 북한의 역량을 실질적 위협으로 인식하고 있음.

참고문헌

[국문]

국립외교원(IFANS). (2020). 2020년 홍콩 국가보안법 통과의 의미와 시사점. 국가안보

국회입법조사처(NARS). (2021). 바이든 시기 미·일 관계 주요 현안과 시사점
(중국 해경법·남중국해 언급).

김소정 (2024). 하이브리드 위협 대응을 위한 정책 고려사항. INSS 이슈브리프, No.612.
국가안보전략연구원.

김재엽 (2022). '전쟁 이외의 전략 도전'으로서 중국의 삼전(三戰): 특징과 사례,
그리고 한반도 안보에의 시사점. 신아세아, 29(1), 94 - 126.

류지선, 박정호 (2023). 방위산업 디지털 전환에 따른 보안위협 분석 및 대응방안. 한국산학기술학회
논문지, 24(10), 682-689.

박지영, 김선경 (2019) 하이브리드 전쟁의 위협과 대응. 이산정책연구원 이슈브리프.

서예령, 이재우 (2021). 복잡한 사이버-물리시스템의 확장성, 안전성 및 보안성 연구.
한국산업보안연구, 11(1), 43-64.

송태은 (2020) 하이브리드 위협에 대한 최근 유럽의 대응. 국립외교원 외교안보연구소
주요국제문제분석 2020-31.

송태은 (2021). 디지털 시대 하이브리드 위협 수단으로서의 사이버 심리전의 목표와 전술:
미국과 유럽의 대응을 중심으로. 세계지역연구논총, 39(1), 69-106.

윤전형 (2023). 양자과학기술의 국가안보적 의미와 대응전략. INSS 전략보고, No.239.
국가안보전략연구원.

이세훈, 이승훈 (2024). 러시아의 하이브리드전을 통해 본 한국의 사이버전 발전방안.
산업진흥연구, 9(4), 65-76.

전략연구원(INSS). (2020). 홍콩 국가안전법 제정의 파급영향과 정책시사점.

정태진 (2024). AI를 이용한 사이버 위협의 해외사례 분석 및 시사점 연구. 융합보안 논문지,
24(5), 123-136.

최정완 (2024). 기업 내 생성형 AI 시스템의 보안 위협과 대응 방안. 융합보안 논문지, 24(2), 9-17.

한국인터넷진흥원 (2024). 2024년 하반기 사이버 위협 동향 보고서. 한국인터넷진흥원.

[영문]

Anagnostakis, D. (2023). Hybrid Threats: A European Response. In: Balomenos, K.P., Fytopoulos, A., Pardalos, P.M. (eds) Handbook for Management of Threats. Springer Optimization and Its Applications, vol 205. Springer, Cham.

Bertolini, M., Minicozzi, R., Sweijs, T. (2023) Ten Guidelines for Dealing with Hybrid Threats A Policy Response Framework, The Hague Centre for Strategic Studies

CISA (2024). Space systems security and resilience landscape: Zero trust in the space environment.

CISA (2025, January 13). Building a secure by design ecosystem.

Costigan, S. S., Hennessy, M. A. (2024) Hybrid Threats and Hybrid Warfare Reference Curriculum (HTHWRC), NATO Headquarters Brussels

Crosignani, M., Macchiavelli, M., Silva, A.F. (2021) Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains. Federal Reserve Bank of New York Staff Reports, no. 937

CSIS/AMTI. (2025, Feb 27). Dropping the Act: China's Militia in 2024.

Department of Defense (2024). Commercial space integration strategy.

EU (2016) Joint Framework on Countering Hybrid Threats

EU-HYBNET (2022) Fourth Six Month Action Report

European Commission (2016) Joint Framework on countering hybrid threats

European Commission (2019) Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats

European Commission(2023) EU-NATO Task Force on the Resilience of Critical Infrastructure: Final Assessment Report

European Union (2023, March 15). Regulation (EU) 2023/588 of the European Parliament and of the Council establishing the Union Secure Connectivity Programme for the period 2023–2027.

European Union (2023, March 16). European Quantum Communication Infrastructure Initiative.

European Union (2024, June 13). Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

European Union (2024, October 23). Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

European Union (2025). Governance and enforcement of the AI Act.

European Union (2025). Shaping Europe's digital future.

European Union Agency for Cybersecurity (2025) Handbook for Cyber Stress Tests

Frank Christian Sprengel (2021) Drones in hybrid warfare: Lessons from current battlefields, Hybrid CoE Working Paper 10

Giannopoulos, G., Smith, H., Theocharidou, M. (2021) The Landscape of Hybrid Threats: A Conceptual Model Public Version. Joint Research Centre of the European Commission (JRC) and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)

Guilfoyle, Douglas. (2019), “Rule of Law and Maritime Security,” International Affairs.

Guillem Colom Piella (2022) NATO’s strategies for responding to hybrid conflicts, CIDOB REPORT # 08- 2022

Hammad, A.W.A., Haddad, A. (2021). Infrastructure Resilience: Assessment, Challenges and Insights. In: Leal Filho, W., Azul, A.M., Brandli, L., Lange Salvia, A., Wall, T. (eds) Industry, Innovation and Infrastructure. Encyclopedia of the UN Sustainable Development Goals. Springer, Cham.

Hammoudeh, M., Essa, A. T., Sherbeeni, A. M., Firth, C. M., & Essa, A. S. (Eds.). (2025). Quantum computing: A journey into the next frontier of information and communication security (1st ed.). CRC Press.

Hedling, Elsa. (2025) Social identities and democratic vulnerabilities: Learning from examples of targeted disinformation, Hybrid CoE Paper 24

Hybrid CoE (2021) The future of cyberspace and hybrid threats, Hybrid CoE Trend Report 6

IBM X-Force. (2025, May 10). IBM X-Force 2025 Threat Intelligence Index. IBM Security.

Joint Publication 3-0. Joint Operations, August 2011

Kazdal, M. (2025). ADAPTING TO CONFLICT: IRAN’S PROXY WARFARE STRATEGY IN SYRIA AND YEMEN (2011–2020). Kafkas Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi, 16(31), 301-323

Keršanskas, V. (2020) DETERRENCE: Proposing a more strategic approach to countering hybrid threats, Hybrid CoE Paper 2

Klimburg, A (2012) National Cyber Security Framework Manual, NATO CCD COE Publication

Laura Bruun. (2024). Towards a Two-tiered Approach to Regulation of Autonomous Weapon Systems: Identifying and Possible Elements. Stockholm International Peace Research Institute (SIPRI)

Monaghan, S. (2019) Countering Hybrid Warfare PRISM, Vol. 8, No. 2, pp. 82-99

Monaghan, S. (2022) Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice, Hybrid CoE Paper 12

Mosca, M., Piani, M. (2024) Quantum Threat timeline report 2024. Global Risk Institute.

National Infrastructure Advisory Council (2009) Critical Infrastructure Resilience final report

NATO OTAN (2022) NATO 2020 Strategic Concept

NIKOLOV, Orlin. (2018) BUILDING SOCIETAL RESILIENCE AGAINST HYBRID THREATS, *Information & Security: An International Journal*

NIST (2024, August 13). NIST releases first 3 finalized post-quantum encryption standards.

NSA (2025, March 4). CNSS Policy 15. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

Office of Inspector General (2024) DHS(Department of Homeland Security) Improved Election Infrastructure Security, but Its Role in Countering Disinformation Has Been Reduced

Office of the Director of National Intelligence (2017) Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution

Office of the President (2025, January 15). Memorandum for heads of executive departments and agencies (M-25-04).

Rietjens, S. (2020) A warning system for hybrid threats – is it possible? Hybrid CoE Strategic Analysis 22 :

Romansky, S., Hoenig, A., Meessen, R., Kruijver, K. (2024) New Technologies, Changing Strategies: Five Trends in the Hybrid Threat Landscape, The Hague Centre for Strategic Studies and TNO.

Salt, A., Sobchuk, M. (2021) Russian Cyber-Operations in Ukraine and the Implications for NATO. Canadian Global Affairs Institute.

Schultheiss, Christian. (2023), “What Has China’s Lawfare Achieved?”, ISEAS Perspective.

Sood, Aditya, K., Zeadally, S. (2025). Malicious AI Models Undermine Software Supply-Chain Security. Communications of the ACM, Vol. 68, No. 6

The White House (2025). Winning the race: America‘s AI action plan.

U.S. AIR FORCE (2025) Operations. Air Force Doctrine Publication 3-0

U.S. AIR FORCE, U.S. SPACE FORCE (2021) The Department of the Air Force role in Joint all-domains operations. Air Force Doctrine Publication 3-99

UN. (2024a, July 1). Lethal autonomous weapons systems : Report of the Secretary-General. UN.

UN. (2024b, October 2). Convention on prohibitions or restrictions on the use of certain conventional weapons which may be deemed to be excessively injurious or to have indiscriminate effects (CCW/GGE.1/2024/WP.11).

Vaseashta, A., Hudișteanu, A. C., Djugumanov, I., Arama, M. H., Vasović, D., Milenković, M., Bolgen, N., Codreanu, M., Maftei, C. (2025) Hybrid Threats, Risks, and Vulnerabilities—Critical Infrastructure Resilience Solutions Toolkit for Cross-Sectoral Applications. In: Radu, D., Hukić, M., Vaseashta, A. (eds) Countering Hybrid Threats Against Critical Infrastructures. ICSIMAT 2024. NATO Science for Peace and Security Series B: Physics and Biophysics. Springer

Weissmann, M., Nilsson, N., Palmertz, B., Thunholm, P. (2021) Hybrid Warfare: Security and Asymmetric Conflict in International Relations

Yoon, S., Kim, W. (2023), “The Import of Hybrid Activities in the South China Sea”, Journal of Indo-Pacific Affairs

Zandee, D., Van der Meer. S., Stoetman, A. (2021), Countering hybrid threats Steps for improving EU-NATO cooperation, Clingendael Report

[온라인]

대한민국 국방부. (n.d.) “국방혁신 4.0 추진 중점 및 과제- 우주, 사이버, 전자기 등 신영역 작전 수행개념 및 첨단 전력체계 발전” https://www.mnd.go.kr/mbshome/mbs/mnd/subview.jsp?id=mnd_011903030000 (검색일: 2025.8.7.)

Aerospace Security. (2020) “How Does Space Policy Directive-5 Change Cybersecurity Principles for Space Systems?” https://aerospace.csis.org/how-does-space-policy-directive-5-change-cybersecurity-principles-for-space-systems/ (검색일: 2025.10.2.)

Altukhova, O. (2025) "New trends in phishing and scams: how AI and social media are changing the game" Secure List by Kaspersky https://securelist.com/new-phishing-and-scam-trends-in-2025/117217/ (검색일: 2025.9.25.)

BBC News. (2015) “Ken Livingstone: Tony Blair to blame for 7/7 bombings” https://www.bbc.com/news/uk-politics-34941658 (검색일: 2025.9.28.)

Bishop, M. (2025) “us-ai-action-plan” Gartner.https://www.gartner.com/en/articles/us-ai-action-plan (검색일: 2025.9.25.)

Brethous, M., Kovalčíková, N. (2023), “Next level partnership - Bolstering EU-NATO cooperation to counter hybrid threats in the Western Balkans” European Union Institute for Security Studies https://www.iss.europa.eu/publications/briefs/next-level-partnership-bolstering-eu-nato-cooperation-counter-hybrid-threats (검색일: 2025.8.20.)

Civil-Military Cooperation Centre of Excellence(CCOE). (n.d.) “Seven baseline requirements” https://www.cimic-coe.org/handbook-entries/welcome-to-the-cimic-handbook/vii-resilience/7-2-seven-baseline-requirements/ (검색일: 2025.7.9.)

Clinton, S. (2025) "OWASP Gen AI Incident & Exploit Round-up, Q2'25" GenAI Security Project https://genai.owasp.org/2025/07/14/owasp-gen-ai-incident-exploit-round-up-q225/ (검색일: 2025.9.29.)

Congress.Gov. (2023) “S.1425 - Satellite Cybersecurity Act” https://www.congress.gov/bill/118th-congress/senate-bill/1425/text (검색일: 2025.8.4.)

Donnelly, J., Farley, J. (2018) “Defining the ‘Domain’ in Multi-Domain” Over the Horizon. https://othjournal.com/2018/09/17/defining-the-domain-in-multi-domain/ (검색일: 2025.6.21.)

EUDefence StrategicCompass. (2024) “COUNTERING HYBRID THREATS” https://www.eeas.europa.eu/sites/default/files/documents/2024/2024-countering-Hybrid-Threats.pdf (검색일: 2025.9.24.)

European Commission. (n.d.) “EU Space Strategy for Security and Defence for a stronger and more resilient European Union” https://defence-industry-space.ec.europa.eu/eu-space/eu-space-strategy-security-and-defence_en (검색일: 2025.8.30.)

European Commission. (n.d.) “Strengthening EU resilience: hybrid threats and critical entities” https://joint-research-centre.ec.europa.eu/projects-and-activities/strengthening-eu-resilience-hybrid-threats-and-critical-entities_en? (검색일: 2025.9.23.)

European Commission. (n.d.) “Resilience to Hybrid Threats” https://joint-research-centre.ec.europa.eu/projects-and-activities/strengthening-eu-resilience-hybrid-threats-and-critical-entities/resilience-hybrid-threats_en (검색일: 2025.7.2.)

European Council. (n.d.) “Hybrid threats” https://www.consilium.europa.eu/en/policies/hybrid-threats/ (검색일: 2025.6.19.)

European Parliament. (2022) “NATO study on the ‘weaponisation of brain sciences’ for the purposes of ‘cognitive warfare’” https://www.europarl.europa.eu/doceo/document/E-9-2022-001093_EN.html (검색일: 2025.9.26.)

Federal Register - The Daily Journal of the United States Government. (2020) “Cybersecurity Principles for Space Systems” https://www.federalregister.gov/documents/2020/09/10/2020-20150/cybersecurity-principles-for-space-systems (검색일: 2025.9.18.)

Gartner. (n.d.) “Cybersecurity Insights & Trends” https://www.gartner.com/en/insights/cybersecurity (검색일: 2025.9.19.)

Hybrid CoE. (2021) “Hybrid CoE Trend Report 6: The future of cyberspace and hybrid threats” https://www.hybridcoe.fi/publications/hybrid-coe-trend-report-6-the-future-of-cyberspace-and-hybrid-threats/ (검색일 2025.9.11.)

Hybrid CoE. (n.d.) “Hybrid threats as a concept” https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ (검색일 2025.6.25.)

Hybrid CoE. (n.d.) “Deterrence and resilience” https://www.hybridcoe.fi/deterrence-and-resilience/ (검색일 2025.9.18.)

Insinna, V. (2022) “SpaceX beating Russian jamming attack was ‘eyewatering’: DoD official” Breaking Defense. https://breakingdefense.com/2022/04/spacex-beating-russian-jamming-attack-was-eyewatering-dod-official/ (검색일: 2025.7.4.)

Ivezic, M. (2025) “Quantum Geopolitics: The Global Race for Quantum Computing” PostQuantum https://postquantum.com/quantum-computing/quantum-geopolitics/ (검색일: 2025.9.27.)

Japan Aerospace Exploration Agency. (2024) “Report on Unauthorized Access at JAXA” https://global.jaxa.jp/press/2024/07/20240705-2_e.html (검색일: 2025.10.2.)

KBS 뉴스. (2024) “합동참모본부, 우주·사이버·전자전 대비 ‘다영역작전부’ 신설” https://news.kbs.co.kr/news/pc/view/view.do?ncd=8112682 (검색일: 2025.7.12.)

Kerr-Shaw, N., Aleksiev, A. J., Anderson, J., Ridgway, W. E., Simon, D. A., Werry, S. (2025) “The EU’s New Cybersecurity Law for the Space Sector” Skadden. https://www.skadden.com/insights/publications/2025/07/the-eus-new-cybersecurity-law-for-the-space-sector (검색일: 2025.9.24.)

Koi, U. (2024) “Japan Space Agency (JAXA) Hit by Cyberattacks” Space Systems CyberSecurity. https://spacesecurity.wse.jhu.edu/2024/06/24/japan-cyberattacks/ (검색일: 2025.9.19.)

Korth, L. (2022) “Starlink Terminal Hack” Space Systems CyberSecurity. https://spacesecurity.wse.jhu.edu/2022/09/21/starlink-terminal-hack/ (검색일: 2025.7.21.)

Lakshmanan, R. (2025) "New Reports Uncover Jailbreaks, Unsafe Code, and Data Theft Risks in Leading AI Systems" The Hacker News. https://thehackernews.com/2025/04/new-reports-uncover-jailbreaks- unsafe.html (검색일: 2025.9.3.)

Maciata, K. (2025) “Fortifying the Baltic Sea - NATO’s defence and deterrence strategy for hybrid threats” NATO OTAN – NATO REVIEW. https://www.nato.int/docu/review/articles/2025/05/05/fortifying-the-baltic-sea-natos-defence-and-deterrence-strategy-for-hybrid-threats/index.html (검색일: 2025.10.5.)

National Security Agency/Central Security Service. (2022) “NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems” https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3148990/nsa-releases-

future-quantum-resistant-qr-algorithm-requirements-for-national-se/ (검색일: 2025.9.23.)

NATO OTAN – Welcome to allied Command Transformation. (2023) “Multi-Domain Operations in NATO – Explained” https://www.act.nato.int/article/mdo-in-nato-explained/ (검색일: 2025.9.12.)

NATO OTAN – Welcome to allied Command Transformation. (2023) “NATO Warfighting Capstone Concept: An Adaptive 20-year Strategy for NATO and its Allies” https://www.act.nato.int/article/nato-warfighting-capstone-concept-an-adaptive-20-year-strategy-for-nato-and-its-allies/ (검색일: 2025.9.29.)

NATO OTAN – Welcome to allied Command Transformation. (2024) “Allied Command Transformation develops the Cognitive Warfare Concept to Combat Disinformation and Defend Against “Cognitive Warfare”” https://www.act.nato.int/article/cogwar-concept/ (검색일: 2025.10.7.)

NATO OTAN – Welcome to allied Command Transformation. (n.d.) “The NATO Warfighting Capstone Concept” https://www.act.nato.int/our-work/nato-warfighting-capstone-concept/ (검색일: 2025.9.11.)

NATO OTAN. (2024) “Countering hybrid threats” https://www.nato.int/cps/en/natohq/topics_156338.htm (검색일: 2025.7.5.)

NATO OTAN. (2024) “Cyber defence” https://www.nato.int/cps/en/natohq/topics_78170.htm (검색일: 2025.9.26.)

NATO OTAN. (2024) “Resilience, civil preparedness and Article 3” https://www.nato.int/cps/en/natohq/topics_132722.htm (검색일: 2025.8.19.)

Nettis, K. (2020) “Multi-Domain Operations: Bridging the Gaps for Dominance” Sixteenth Air Force (Air Forces Cyber) https://www.16af.af.mil/Newsroom/Article-Display/Article/2112873/multi-domain-operations-bridging-the-gaps-for-dominance/ (검색일: 2025.7.18.)

Piella, G. C., (2022) “NATO’s strategies for responding to hybrid conflicts” CIDOB. https://www.cidob.org/en/publications/natos-strategies-responding-hybrid-conflicts (검색일: 2025.6.27.)

Proofpoint. (2025) "Cybercriminals abuse AI website creation app for phishing" https://www.proofpoint.com /us/blog/threat-insight/cybercriminals-abuse-ai-website-creation-app-phishing (검색일: 2025.8.19.)

Roberts, R., Miller, C., Weggeman, C., Burns, W. Eggers, W.D. (2024) “Stellar safeguards: How organizations can protect space assets from cyberthreats” Deloitte Center for Government Insights https://www.deloitte.com/us/en/insights/industry/government-public-sector-services/defending-against-cyber-threats-space-systems.html (검색일: 2025.9.19.)

Roepke, W-D., Thankey, H. (2019) “Resilience: the first line of defence” NATO OTAN – NATO REVIEW. https://www.nato.int/docu/ review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html (검색일: 2025.10.4.)

Rühle, M., Roberts, C. (2021) “Enlarging NATO’s toolbox to counter hybrid threats” NATO OTAN – NATO REVIEW. https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html (검색일: 2025.9.2.)

Sanchez, A. (2025) “Regional Approaches To Post-Quantum Cryptography” Forbes. https://www.forbes.com/councils/forbescommunicationscouncil/2025/09/08/regional-approaches-to-post-quantum-cryptography/ (검색일: 2025.9.1.)

The Guardian. (2024) “Undersea ‘hybrid warfare’ threatens security of 1bn, Nato commander warns” https://www.theguardian.com/world/2024/apr/16/undersea-hybrid-warfare-threatens-security-of-1bn-nato-commander-warns (검색일: 2025.9.30.)

U.S. Department of War. (2019) “Multidomain Operations Rely on Partnerships to Succeed” https://www.war.gov/News/News-Stories/Article/Article/1755520/multidomain-operations-rely-on-partnerships-to-succeed/ (검색일: 2025.8.9.)

Wikipedia. (n.d.) “2014 Crimean status referendum” https://en.wikipedia.org/wiki/2014_Crimean _status_referendum (검색일: 2025.9.14.)

Wikipedia. (n.d.) “Grey-zone (international relations)” https://en.wikipedia.org/wiki/Grey-zone_%28 international_relations%29 (검색일: 2025.9.21.)

Wikipedia. (n.d.) “Harvest now, decrypt later” https://en.wikipedia.org/wiki/Harvest_now,_decrypt_later (검색일: 2025.8.13.)

Wikipedia. (n.d.) “Little green men (Russo-Ukrainian War)” https://en.wikipedia.org/wiki/Little_green_men_(Russo-Ukrainian_War) (검색일: 2025.8.29.)

Wikipedia. (n.d.) “Media portrayal of the Russo-Ukrainian War” https://en.wikipedia.org/wiki/Media_portrayal_of_the_Russo-Ukrainian_War (검색일: 2025.9.22.)

Wikipedia. (n.d.) “Russian annexation of Crimea” https://en.wikipedia.org/wiki/Russian_annexation_of_Crimea (검색일: 2025.7.2.)

Wikipedia. (n.d.) “Russian occupation of Crimea” https://en.wikipedia.org/wiki/Russian_occupation_of_Crimea (검색일: 2025.7.3.)

Woollacott, E. (2025) "Flaw in Lenovo's customer service AI chatbot could let hackers run malicious code, breach networks" IT Pro. https://www.itpro.com/security/flaw-in-lenovos-customer-service-ai-chatbot-could-let-hackers-run-malicious-code-breach-networks (검색일: 2025.9.25.)

Seoul Dialogue:

Exploring Hybrid Threats, Emerging Technologies, and the Resilience of Critical Infrastructure

2025 세계신안보포럼 영문 보고서

Report of the World Emerging Security Forum

TABLE OF CONTENTS

EDITED BY:

Yonghee Kim
So Young Kim
Yong-Chan Choi
Seung Hyun Kim
Junhyeong Jeon

THE EVOLUTION OF HYBRID THREATS AND INTERNATIONAL SECURITY

FORUM SUMMARY

The World Emerging Security Forum (WESF), launched in 2021, has become a pivotal venue for fostering international cooperation to address complex, cross-border security risks in an era of rapid technological change. Building on previous dialogues, WESF 2025 centered on the theme "The Evolution of Hybrid Threats and International Security," reflecting growing concern over strategies that blend military, technological, informational, and economic instruments to undermine stability and erode public trust.

Held on September 8, 2025, in Seoul, the Forum convened senior government officials, international organizations, industry leaders, academics, and media representatives to examine how hybrid tactics exploit the seams between peace and war, civilian and military domains, and physical and digital environments. Discussions underscored that hybrid threats no longer occupy the periphery of security debates: they reshape the strategic landscape, demand adaptive governance, and call for a deeper integration of societal resilience into national and international security planning.

SESSION I:
Cognitive Warfare: Countering Disinformation and Misinformation for Societal Resilience

The opening session highlighted the intensification of cognitive warfare, where malign actors use disinformation, deepfakes, and algorithmic amplification to manipulate perceptions and polarize societies. Experts analyzed how adversaries exploit human psychology, data-driven targeting, and emerging AI tools to fracture social cohesion and weaken democratic discourse. Participants emphasized the need for comprehensive approaches - media literacy, ethical standards for AI, and enhanced cooperation between governments, platforms, and civil society - to safeguard information integrity and build public resilience.

SESSION II:
Emerging Technologies and the Threat Landscape: Persistent Security Threats

This session examined how drones, artificial intelligence, and quantum technologies are reshaping conflict dynamics. Panelists assessed the democratization of airspace through low-cost drones, the use of AI in intelligence, logistics, and targeting, and the promise and perils of quantum computing and communication. They warned that these capabilities blur the lines between offensive and defensive operations, complicate attribution, and expand the risk surface for escalation. Discussions called for updated legal frameworks, better counter-UAS measures, and robust civil–military–private partnerships to anticipate and mitigate these evolving threats.

SESSION III:
Resilience of Critical Infrastructure: Reducing Multidimensional Vulnerabilities

The final session focused on the interdependence of essential services - energy grids, transport, healthcare, finance, and digital networks - and their exposure to cyber and physical attacks. Presentations underscored that resilience depends not only on technical safeguards but also on governance, economic readiness, and community-level adaptability. Case studies from Canada, Southeast Asia, and Africa illustrated the value of public–private trust, cross-border drills, and regulatory harmonization. Speakers advocated embedding resilience in system design, expanding cyber-insurance markets, and prioritizing capacity-building for developing states.

WESF 2025 reaffirmed the Forum's role as a hub for policy innovation and practical collaboration. By linking the study of hybrid threats to concrete measures - ranging from information integrity and technological governance to infrastructure resilience - the event laid a foundation for cooperative strategies that integrate ethics, security, and societal trust in confronting 21st-century risks.

Opening Session

Opening Remarks

Cho Hyun
Minister of Foreign Affairs, Republic of Korea

President Kwang Hyung Lee of KAIST, Excellencies, distinguished guests, on behalf of the Ministry of Foreign Affairs of Korea, I would like to welcome each and every one of you to this forum.

Human nature often resists change, but technology relentlessly drives it forward. In this hyper-connected world, accelerating technology brings both unprecedented opportunities and risks. Addressing these risks demands stronger global governance and international cooperation, making the expertise and commitment in today's forum all the more critical. These risks also justify the assistance of diplomats in these discussions - who know actually nothing about technology.

Today, power is measured not only by armies and territory, but in ideas, information, and innovation. That is why this forum focuses on the rise of hybrid threats - a domain where the battlefield is as much cognitive and digital as it is physical. Hybrid threats combine military and non-military actions. They are hard to detect and even harder to counter.

Recognizing the urgency, today's event will explore three key dimensions:
First, the battlefield of cognition, where disinformation turns trust into target. Disinformation corrodes the foundation of our trust-based democratic society. It sows division among people and weakens confidence in institutions. This is a new threat to our democracies. A single false narrative can reach millions within hours. According to a survey in Korea, over 80 percent of people view online false information as a major threat. The rise of AI and deepfake technologies magnifies this danger - producing fabricated reality so convincing that truth itself is under siege. Every click, every share, every manipulated image has the power to shape perceptions and sway opinions.

Second, technology is redefining how conflicts are fought. When I served as Korean Ambassador to the United Nations in 2020 - together with Ambassador Heusgen - I witnessed debates on the Nagorno-Karabakh conflict. For the first time, the world realized that drones could decide the course of war. Affordable, commercially available drones revealed that traditional military superiority could be overturned by technology. That lesson applies on a larger scale in Ukraine. Just a few days ago, we saw swarms of drones attacking key buildings. Beyond drones, AI-driven analysis compresses decision cycles from days to minutes. Quantum computing also threatens to upend current encryption methods. Together, these technologies expand the battlefield beyond conventional physical spaces, creating new vulnerabilities worldwide.

Third, critical infrastructure remains an exposed target at the heart of our daily lives. Cyber or physical attacks on energy grids, healthcare systems, water supplies, or transportation networks can cascade into economic disruption and global supply-chain instability. National security itself can be jeopardized. Consider the vulnerability of undersea Internet cables - a single act of sabotage could paralyze intercontinental financial flows. These threats do not respect borders; they are global in impact.

The urgency is undeniable. Yet one of our greatest obstacles in countering hybrid threats is the lack of shared understanding, compounded by the rapid pace of technological and societal change. That is why international cooperation is indispensable.

The Republic of Korea has actively advanced this agenda. At the United Nations we spearheaded the first-ever resolution on AI in military domains, affirming that international humanitarian and human-rights law should be applied to AI in military terms. We also led the resolution on new and emerging digital technologies and human rights, emphasizing a human-rights-based approach for digital technologies. These efforts will continue through our AI initiative at the upcoming APEC Economic Leaders' Meeting in Gyeongju, aimed at building AI capacity across all levels of society.

As President Lee Jae-myung of Korea has emphasized, when it comes to security, proactive prevention is more important than reactive measures. Our front line lies not only in technological advancement or military capacity, but in society itself - resilient citizens, discerning minds, safeguarded democratic discourse. These are our defenses. Equally important is cross-sectoral collaboration - among governments, businesses, and academia. Much of the infrastructure we rely on, and the innovation that drives progress, rests in private hands. Only through close cooperation can we build resilience through policy coordination, knowledge-sharing, and technology transfer.

I once told my fellow ambassadors in New York, when I was about to leave: If I could speak about the world right now, I would say that I were the captain of a plane announcing that we are experiencing turbulence - so fasten your seat belt. Indeed, we are vulnerable, but together we can navigate it and find a way through. I look forward to the most fruitful and engaging discussions in today's forum. Thank you very much.

Welcoming Remarks

Kwang Hyung Lee
President, KAIST

Good morning. I am Kwang Hyung Lee, President of KAIST. It is my great honor to welcome you to the 2025 World Emerging Security Forum, a gathering dedicated to addressing the future of global security. I extend my deepest gratitude to Minister Cho of the Ministry of Foreign Affairs and to all the esteemed guests who have joined us today.

The emerging security threats we face are no longer confined to traditional military conflicts. Hybrid threats, created by digital technologies and a hyper-connected society, endanger not only the core functions of a state, but also the values of democracy.

To respond effectively, we need policy insights, a strategic understanding of security, and close international cooperation. Science and technology are the essential foundation supporting every stage of security. As a center of transnational cooperation, KAIST will advance research and disseminate outcomes, leading the way in fulfilling our mission to safeguard humanity.

Finally, I express sincere appreciation to everyone who contributed to making this forum possible. May this gathering serve as a solid foundation for cooperation toward a peaceful and sustainable international order. Thank you very much.

Congratulatory Remarks

Karim Haggag

Director, Stockholm International Peace Research Institute (SIPRI) (Video Message)

Excellency Minister Cho, President Lee, distinguished guests, ladies and gentlemen: It is a great pleasure to address you at the commencement of the 2025 World Emerging Security Forum. While I very much regret not being able to be with you in person, it is my distinct honor that my message coincides with my first day as the incoming Director of SIPRI.

The theme of this year's forum-hybrid threats and their implications for international security-addresses one of the most critical and complex challenges facing today's security environment. The complexity arises from the multifaceted nature of hybrid threats: technological, political, military, and informational. AI and advanced digital communications enable massive disinformation campaigns that threaten to undermine democratic processes and political stability.

Increasingly sophisticated cyber weapons pose a growing risk to critical infrastructure across health, finance, transportation, and energy. The nexus between new technologies-AI, quantum, additive manufacturing, space-based systems-and the old technologies of WMD (nuclear, chemical, biological) presents novel challenges. Risks of proliferation are increasing, undermining the normative and legal restrictions of the global non-proliferation regime.

Pathways for conflict escalation have multiplied as new technologies interact with weapons systems and decision-making in unpredictable ways, potentially impacting crisis and strategic stability profoundly. These challenges unfold amid geopolitical instability, great-power rivalry, and uncertainty in alliance frameworks. Conceptually, hybrid threats are blurring long-standing distinctions: civilian vs. military, war vs. peace, legality vs. illegality, conventional vs. unconventional, state vs. non-state. Cognitive warfare and grey-zone tactics are no longer concepts of the future; they are realities of today's battlefields.

The task before this forum is to assess the evolving challenges posed by hybrid threats while devising a holistic response that brings together political, legal, technological, military, and societal domains. Key questions include: best practices for combining kinetic and non-kinetic responses; how to build resilience in critical infrastructure; how to use emerging technologies to enhance defense while avoiding vulnerabilities of technological dependency; and how to mitigate escalatory risks even below the threshold of conventional war.

SIPRI is proud to be at the cutting edge of research on many of these issues and to partner with MOFA and KAIST in convening this event. I look forward to deepening this partnership in the years ahead, building on what I am confident will be a rich and insightful outcome of this year's forum. Thank you.

Christoph Heusgen

Co-Chairman, St. Gallen Symposium

Good morning, excellencies, ladies and gentlemen. First, I thank the organizing team-the Ministry of Foreign Affairs of Korea, and partners KAIST and SIPRI-for the kind invitation. I also congratulate the Ministry of Foreign Affairs team for the perfect organization of this conference; it reminds me of the G20 Summit in Seoul, which I attended as Chancellor Merkel's National Security Advisor-equally well organized and with important results.

Germany and South Korea have much in common: solid democracies, close political and economic partners, committed to the United Nations and its Charter. Congratulations on your UN Security Council membership and on the September presidency-and best wishes to the foreign minister, whom I worked with in 2019–2020. As he said, in this world situation one has to fasten the seat belt.

After World War II, Germany and Korea were divided. Germany was fortunate to overcome this division; I hope one day Korea will also be reunited. What were the driving principles behind Germany's policy leading to reunification? First, communication-keeping lines open, advancing humanitarian causes, building confidence; Ostpolitik was a cornerstone. Second, targeted sanctions-then easier to implement and harder to circumvent; they were decisive. In 2019–2020, as Germany's Ambassador to the UN, I chaired the Security Council's North Korea Sanctions Committee and tried to stay on a tough line-working closely with your now Director-General for International Security Affairs, Yoon Jong-kwan. Russia and China blocked many efforts, but they didn't boycott the committee. Today, unfortunately, they do-violating international law. Instead of participating in the international effort to prevent North Korea from acquiring nuclear weapons, Russia has engaged in a close partnership with this brutal dictatorship, engaging North Korean mercenaries in its war of aggression against Ukraine.

Those countries that adhere to the UN Charter try nevertheless to keep sanctions in place. A third pillar is military strength-democracy must be stronger than tyranny. German reunification was possible because of military strength and that of its allies. Today, however, strength needs a wider interpretation; it's no longer limited to classical security instruments. We need a wider vision, and here the theme of our conference is timely: hybrid warfare, cybersecurity, electronic warfare, drones, and social-media warfare. Totalitarian countries are way ahead, as seen in systematic, even industrial disinformation from the Kremlin and others-undermining democracy as a global phenomenon.

To confront these new challenges, democracies and all countries adhering to the UN Charter must work together. Thanks again to MOFA for putting these challenges on the forum agenda. I look forward to our discussions and results. Thank you very much.

Teija Tiilikainen

Director, European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) (Video Message)

Excellencies, ladies and gentlemen. It is a great pleasure to address this distinguished forum and to stress the importance of its topic. Allow me a few words on the evolving international security environment and, specifically, on hybrid threats. I speak on behalf of the European Centre of Excellence for Countering Hybrid Threats, located in Helsinki, an expert organization among all 36 EU and NATO members, with both organizations as key participants in our work.

The world is undergoing major geopolitical change. We see growing competition for global leadership, which enhances risks and threats to our overall security and stability. There is a lack of mutual trust among great powers and members of the international community. A key dividing line in this competition is between democratic values and authoritarian rule-with the democratic model being weakened as part of this confrontation.

As global competition gains the upper hand, new tools are constantly developed to weaken competitors. We see direct attacks on vulnerabilities of our democratic societies-against elections, the information space, critical infrastructures, and access to critical commodities. Almost anything can be weaponized and instrumentalized-from energy to migration to social identities-with the human mind and cyberspace becoming battlefields.

This conflict is not limited by borders or governments; it reaches our citizens and domestic spheres in dangerous ways. Given the challenging environment, more cooperation is needed among democracies and like-minded states-and among practitioners and experts. We must learn from each other, share best practices, and enhance the comprehensive resilience of our societies. We must learn to recognize threats and prevent the exploitation of our vulnerabilities.

I therefore welcome fora such as WESF and congratulate it on a high-level program and participation. I wish you all a stimulating and productive discussion. Many thanks and have a nice conference.

Arnold Kavaarpuo

Executive Director, Data Protection Commission, Ghana
(Video Message)

Your Excellencies, distinguished delegates, ladies and gentlemen, warm greetings from the people of Ghana and indeed 1.4 billion Africans. It is an honor to join you virtually in Seoul, a city where tradition meets modernity. It is fitting that we gather at this global crossroads of culture and technology to deliberate on one of the most pressing issues of our age: the evolution of hybrid threats and international security.

I congratulate the Government of the Republic of Korea and the organizers for convening this timely forum-not just a platform for dialogue, but a call to action. Since our independence in 1957, Ghana has positioned itself as the gateway to Africa-not only historically as the first sub-Saharan nation to gain independence, but symbolically as the only country where the Equator and Greenwich Meridian converge. Ghana stands at the crossroads of Africa's past and future. We have built one of the continent's most stable democracies and are writing one of the most encouraging economic-recovery stories.

Hybrid threats are reshaping the security environment-blurring lines between war and peace, domestic and international. We have all witnessed their global cost: the NotPetya (2017) cyberattack, costing over $10 billion; the SolarWinds (2020) intrusion, which showed how supply chains can be weaponized; and ongoing hybrid warfare in Ukraine, combining cyber operations, disinformation, and kinetic force. These threats can paralyze economies, undermine democratic institutions, and destabilize regions.

For Africa, these challenges are equally real. Disinformation campaigns seek to influence elections and erode public trust. Cyberattacks on mobile-money systems, on which millions depend daily, threaten livelihoods and financial stability. Disruptions to ports and sea cables can paralyze trade and connectivity with rippling effects across entire regions.

Africa is home to the world's most youthful population-digitally connected and innovative. This is our greatest strategic advantage, yet also where hybrid threats strike hardest. Young people are targeted by disinformation, radicalization, and economic exploitation. If we do not act, the democratic dividend that should drive innovation risks being weaponized against stability. But if we succeed, Africa's youth will secure our continent and serve as a shield of resilience for the world.

Africa is not only a continent of vulnerabilities; it is a continent of solutions. A new generation of innovators is building platforms to strengthen financial systems, agriculture, health, and governance. The AU Malabo Convention reflects our commitment to cybersecurity and data protection. In Ghana, data-governance reforms, open banking, and trust and accountability are core to our digital economy, making resilience a national priority.

The lesson is clear: No nation or region can confront hybrid threats alone. These threats exploit the spaces between jurisdictions, the gaps between generations, and the divides between regions. Our response must therefore be collective-grounded in stronger cross-border intelligence-sharing, resilient infrastructure, and international norms to ensure emerging technologies are harnessed for peace. This forum brings together bright minds and experienced leaders. I look forward to learning, exchanging insights, and carrying lessons back to Ghana and Africa-to strengthen institutions, empower youth, and deepen our contribution to global security.

The stakes could not be higher. If we fail to act, hybrid threats will define international security by fragility and mistrust. If we act together, we can build a future anchored in trust, resilience, and shared responsibility. Africa is ready. Ghana is ready. The time for decisive collective action is now. Thank you.

Session 1: Cognitive Warfare: Countering Disinformation and Misinformation for Societal Resilience

Moderator:
Dr. Tae-Eun Song
Assistant Professor,
Korea National Diplomatic Academy (KNDA)

Dr. Song opened the first thematic session by describing cognitive warfare as a contest over meaning, one that seeks to manipulate perceptions, disrupt rationality, and corrode trust. She noted that modern hybrid threats increasingly exploit the information domain, blending disinformation, psychological operations, and identity-based narratives to destabilize societies. The advent of AI-generated content, deepfakes, and micro-targeted influence has made these operations faster, cheaper, and more precise. Dr. Song framed the discussion around three questions: how cognitive warfare is evolving as part of hybrid threats; what implications new technologies - particularly artificial intelligence and neuro-tools - pose for information integrity; and how governments, industry, and civil society can strengthen resilience without compromising democratic freedoms.

Tanna Krewson
Tanna Krewson, Strategic Advisor, Centre for Information Resilience

Key Message
Hybrid threats exploit perception rather than firepower—modern conflict is fought in minds and identities, not just on physical battlefields.

Tanna Krewson began her remarks by noting that hybrid threats today exploit one of the simplest truths of modern conflict: it is often far more cost-effective to manipulate perception than to deploy military force. In this space, hybrid threats thrive below the threshold of open war, operating where doubt, division, and distrust take root in societies.

Drawing from her experience in the development sector, she explained that building societies often requires working at the grassroots level, meeting people where they are. Malign actors, however, have learned to reverse this logic. Instead of confronting governments through military action, they target societies directly, breaking them down from the ground up.

According to Krewson, when adversaries fracture trust in institutions, fuel polarization, and erode social cohesion, they can achieve strategic objectives without the need for tanks or missiles. She pointed to Russia's war in Ukraine as an illustration. While kinetic action dominates the headlines, the battle over perception has been constant. Narratives of "liberation" or the "Nazi threat," amplified by AI-driven tools, shaped opinion across Europe. She added that similar dynamics are present in the Middle East, where narratives on religion, sovereignty, and injustice are manipulated in real time.

She highlighted that China is pursuing a systematic approach, combining commercial AdTech, data collection, and psychological profiling into what she described as "intelligentized warfare." Violent extremist groups, she added, are adopting similar methods, leveraging AI manipulation to target societies.

Krewson argued that the traditional threat landscape is rapidly evolving, and that emerging technologies, especially AI, are significant because of their intersection with human psychology. She emphasized that people rarely act through logic alone. Identity and emotion are more powerful drivers of behaviour.

She explained that effective manipulation target's identity. For example, adversaries may exploit cultural values around being a man, a mother, a Christian, or a citizen. Questions such as whether one brings shame to their family or whether one is seen as a leader in the community can be powerful levers. Technology, she observed, now makes it easier to pull these levers at scale, while making them harder to defend against.

Krewson warned that algorithms often reward outrage and grievance, as these emotions generate engagement and profit for social media companies. She added that deepfakes, synthetic media, and tailored microtargeting, based on detailed personal data, create an information environment where individuals disengage from fact-checking and instead rely on what feels right to them—precisely the outcome adversaries seek.

She then described her professional work. For the past several years, she has worked with NATO to develop its approach to cognitive warfare. Beyond this, she has trained militaries and advised governments on understanding influence, building resilience against manipulation, and, when necessary, operationalizing influence effectively. The lesson across these settings, she argued, is the same: hybrid threats are central, not peripheral, to today's security environment.

She concluded by stating that hybrid threats have a profound impact on international security because they move the battlefield into societies, institutions, and even individual identities. Emerging technologies, she stressed, act as accelerants. AI does not invent these strategies, but it makes them scalable and precise. Unless democracies adapt, adversaries and malign actors will continue to gain advantages at minimal cost while democracies remain reactive.

Jean-Marc Rickli
Jean-Marc Rickli, Head of Global and Emerging Risks, Geneva Centre for Security Policy (GCSP)

Key Message
The boundaries of warfare are dissolving—autonomous technologies and AI now serve as surrogates in conflict, expanding the domain of hybrid warfare and challenging traditional responses.

Jean-Marc Rickli began by explaining that the concept of hybrid warfare is difficult to define in academic terms, since different perspectives exist. What is important, however, is the idea of ambiguity and the blurring of lines: between peace and war, between civilians and the military, and between internal and external dimensions. This blurring, he stressed, has a strong impact on how states respond to potential attacks.

He noted that hybrid warfare can be conducted in different ways, one of which is increasingly prominent: the use of surrogates. Unlike proxy warfare, which was widely practiced during the Cold War through human groups fighting

on behalf of larger powers, surrogate warfare expands the category to include technology. Surrogates create plausible deniability. He cited Crimea in 2014 as an example, recalling the “little green men” whose identities could not be confirmed at the time, though they were strongly suspected to be Russian soldiers. This ambiguity shaped how the situation was addressed.

Technology, he continued, now functions as a surrogate actor in its own right. With the rise of autonomy and artificial intelligence, AI can be weaponized in at least three principal ways.

- First, as an analytical enabler, it can process vast amounts of data from multiple sources to generate actionable intelligence.
- Second, as a force multiplier, AI enhances the precision and lethality of existing systems, exemplified by drone warfare in Ukraine.
- Third, as a disruptive force, AI redefines the nature of warfare itself, creating new domains of contestation.

He highlighted two disruptive uses of AI that are especially significant. The first is in swarm technology, which he chose not to elaborate on in detail. The second, more relevant to the panel, is in disinformation and cognitive warfare. Unlike traditional information warfare, which floods targets with messages in the hope of influencing some of them, cognitive warfare goes further. It aims to change the “software” of the target by altering rationality itself.

According to Rickli, this means that the surface of risk is expanding daily as new layers of vulnerability are added. Addressing these risks, he argued, requires the development of resilient systems and approaches to countering hybrid threats.

Pierrick Devidal

Pierrick Devidal, Senior Policy Advisor, International Committee of the Red Cross (ICRC)

Key Message

Hybrid threats are not new - but digital transformation has amplified their speed, scale, and reach. To respond effectively, societies must look beyond technology to the deeper political, economic, and ethical forces that allow manipulation to flourish.

Pierrick Devidal began by acknowledging the difficulty of discussing hybrid warfare, noting that, as Jean-Marc Rickli had mentioned earlier, there is no single agreed definition. The concept, he explained, has evolved in shape and form over the years, making comparative analysis difficult and leaving it unclear whether hybrid threats are intensifying.

He pointed out that there is also a cognitive bias at play, where people tend to believe that current times are worse than the past. This nostalgia bias, he argued, affects perception and can even be instrumentalized to create fear or justify political decisions. Such manipulation itself can be seen as a form of cognitive warfare. He reminded the audience that psychological operations and disinformation are not new, citing the Romans, the Second World War, and the Cold War as historical examples where hybrid forms of conflict were intense.

What has changed, Devidal emphasized, is the qualitative shift brought about by technological innovation. Advances in technology have transformed not just the tools of hybrid warfare but also its speed, scale, and impact. In the past, societies existed within relatively secluded information spaces that were tightly controlled by states and communities. Building networks to influence and manipulate an enemy’s population could take years. Today, however, anyone with a computer and an internet connection can do the same in minutes.

He argued that digital ecosystems are now central to the problem. These networks are global, interconnected, and extremely difficult to control, leaving people constantly exposed to psychological and cognitive manipulation whenever they are online. Disinformation and psychological operations, he observed, have even become legitimate and lucrative business models.

Devidal warned that digital transformation itself has created an environment conducive to hybrid threats. No longer is there a need for armies of secret operatives. Instead, personal data can be purchased from obscure data brokers, hackers can be hired on the dark web, or communities can be manipulated directly through messaging services. These tools can be used to create chaos, sow division, and trigger violence. He stressed that whether these actions are state-sponsored or conducted by loosely organized groups, the same tools and techniques are available, and they serve political, economic, or military goals alike.

To understand hybrid threats, he argued, one must look beyond the moral panic around disinformation and focus on the deeper structural drivers. While technologies such as AI are important, he cautioned against what he described as the “finger-and-moon” problem: focusing too narrowly on the visible technological tools while ignoring the underlying causes.
He identified several drivers of hybrid threats, emphasizing that they:

- spread because digital dependence makes manipulation easy and viral.
- persist because political and economic systems profit from them.
- grow where social inequality and rights violations erode trust.
- endure as legal and ethical safeguards weaken.
- And they thrive because some actors and corporations gain wealth and influence from these dynamics.

He concluded by urging that conversations on hybrid threats must focus not only on the technological aspects but also on the deeper political and economic interests that prevent societies from developing the safeguards needed to protect themselves.

Sarah Shoker

Sarah Shoker, Fellow, Berkeley Risk and Security Lab

Key Message

The challenge of AI-driven disinformation lies not only in technological capability but in human behavior - declining trust, fragmented attention, and blurred boundaries between citizens and influence operators.

Sarah Shoker shared her reflections on artificial intelligence, particularly the rapid advancement of large language models, and noted that these technologies are distinct yet must be understood in the context of broader global changes over the past decade. Their distinctiveness lies in their volume, scale, speed, and ease of use. Unlike earlier technologies, they do not require specialized expertise in machine learning. Anyone can use them, and a wide range of tools are now available, including open-source alternatives accessible to the general public.

Shoker reminded the audience that misinformation and disinformation are forms of labor. Someone must produce them, and whether they are widely adopted depends on

cost-effectiveness. At the same time, she argued, public trust in democratic institutions has declined—sometimes justifiably so. This growing distrust means that AI-generated media is not only the work of foreign influence operators but can also be created by ordinary citizens dissatisfied with their own governments. As a result, it is increasingly difficult to distinguish between citizens legitimately engaging in political expression and actors seeking to exploit or undermine democratic societies.

She also highlighted the role of short-form content in shaping today's information environment. The recent rise of 30-second to one-minute videos represents a shift from the longer recommendation-driven content of platforms like YouTube. Users now spend hours scrolling through infinite feeds, creating conditions of information overload that human cognition is ill-equipped to manage. Within such an environment, it becomes nearly impossible to identify anomalous or malicious pieces of content, such as those planted by foreign influence agents. This, she warned, is a significant risk to public literacy.

Shoker further pointed to political shifts in online content moderation over the last one to two years. Attitudes toward regulating or "policing" online information have changed, making disinformation and misinformation moving targets. This constant evolution, she argued, complicates efforts by policymakers, governments, and civil society to reduce public distrust or build coherent strategies against manipulation, particularly across geographic boundaries.

She concluded by noting that these shifting conditions make it increasingly difficult to establish clear, sustainable responses to the challenges of AI-driven disinformation and hybrid threats.

Following the presentations, Moderator Tae-Eun Song invited the panelists to respond to several questions submitted by the audience in advance and posed additional follow-ups to guide discussion.

Question 1

"The domain of cognitive warfare has established itself as extending beyond the purely military sphere, carrying across non-military threats and traditional modes of warfare. In your view, what efforts and strategic directions should government and the private sector pursue to effectively counter and operate within this new domain?"

Jean-Marc Rickli said governments must bring industry into strategic thinking, since most tools for accessing the brain are developed privately. He contrasted civil–military fusion in China with changing attitudes in Western tech hubs, warned of a US–China tech decoupling, and urged global governance and ethical standards for neuro-AI and synthetic biology. Without oversight, competition may erode safety.

Question 2

"In recent years there have been notable instances of cognitive warfare in various countries and regions. From the perspective of international security, which case do you regard as the most significant, and what key lessons should be drawn from it?"

Tanna Krewson responded that the erosion of support for Ukraine illustrates how influence on domestic audiences can shape strategy. She traced the change in NATO debates since 2022 and said ChatGPT's release made decision-makers realize how fast manipulation could spread. Narratives undermining aid have shifted democratic choices, proving that cognitive warfare threatens internal cohesion as much as external fronts

Question 3

"What are your views on strategic approaches to cognitive warfare - such as establishing an integrated task force - especially for South Korea?"

Tae-Eun Song answered that Korea needs not just a task force but a permanent strategic-communication system. Agencies should jointly collect and analyze threat data, define hybrid operations, and issue coordinated messages at home and abroad, including through Indo-Pacific partnerships.

Pierrick Devidal urged solutions that protect humanitarian neutrality, warning that disinformation campaigns endanger aid workers and operations. Jean-Marc Rickli stressed foresight: dismissing risks as "science fiction" delays action, just as flight was once doubted because planes lack flapping wings. Sarah Shoker, replying to a final audience question on education policy, noted that AI literacy is high among youth, yet distrust in democratic institutions persists; resilience also requires addressing social exclusion and insecurity.

Session 2: Emerging Technologies and the Threat Landscape: Persistent Security Threats

Moderator:
Dr. Sibylle Bauer
Director of Studies, Armament and Disarmament, Stockholm International Peace Research Institute (SIPRI)

Dr. Sibylle Bauer opened the afternoon session by noting that emerging technologies are reshaping the character of conflict, compressing the distance between innovation and the battlefield. She framed the discussion as an effort to map how drones, artificial intelligence, and quantum tools are altering operational realities and strategic calculations. Against a backdrop of geopolitical instability and contested norms, the panel sought to understand both present challenges and forward-looking solutions.

Troels Emil Andersen Boe
Troels Emil Andersen Boe: Cyber and Tech Advisor, Office of Denmark's Tech Ambassador

Key Message
The rise of drones has not changed the nature of war but its character -transforming security from a flat battlefield into a contested, three-dimensional space that challenges state sovereignty and civilian safety alike.

Boe opened he remarked that if he had a dollar for every time someone claimed that drones had changed the nature of war, he would not be rich, but he would have many friends who studied Clausewitz who would laugh at the distinction. The point, he explained, is that drones have not altered the nature of war, but rather its character. This change, he argued, is visible in Ukraine and extends beyond the battlefield into the sphere of homeland security.

To explain this shift, Boe introduced the concept of spatial security, which, in his words, reflects the movement of security from a two-dimensional plane to a three-dimensional volume. His interest in this idea began years earlier, when he was an election observer in Ukraine after the revolution. At that time, he learned that the OSCE used drones to access areas blocked off by unidentified "little green men." This highlighted how drones could reach places inaccessible to human observers, sparking his reflection on the broader implications of aerial accessibility.

Boe outlined four interrelated dynamics shaping the new era of spatial security.

- **First, the democratization of airspace.**
  He explained that drones have dramatically lowered barriers to entry. Where once aviation required state budgets, logistics, and complex organizational structures, today the entire system "fits into a backpack." Commercially available drones now allow virtually anyone to access airspace—whether for legitimate or malicious purposes. Because airspace cannot be sealed with fences or walls, intent becomes invisible, and the same open sky is now shared by hobbyists, activists, criminals, and states alike.

- **Second, the cat-and-mouse race of counter-drone operations.**
  Boe observed that NATO members are struggling in this domain because air defense capabilities were neglected for decades. Drone technologies evolve rapidly, while countermeasures lag behind. Options such as kinetic destruction are often impractical in urban environments, and electronic warfare may disrupt civilian communications. Consequently, rules governing drone use serve more as principles than enforceable laws, creating regulatory gaps that adversaries exploit.

- **Third, the challenge drones pose to state sovereignty in low-altitude airspace.**
  He cited multiple real-world incidents to illustrate how drones complicate protection of critical infrastructure and symbolic sites.In Copenhagen, for example, drones were used for industrial espionage, peering into a law firm's windows on the 11th floor. In Sweden, unidentified drones appeared over nuclear facilities and the royal castle following Russia's 2022 invasion of Ukraine—yet police could not identify or apprehend the operators. These cases, he noted, show how difficult attribution heightens public unease and undermines confidence in state capacity to secure the skies.

- **Fourth, the materialization of spatial security in physical environments.**
  Boe recalled that as early as 2020 he had used examples such as Arctic research stations, greenhouses, and even science-fiction moon bases to illustrate how physical enclosures might emerge as defensive responses to aerial threats. At the time, this seemed speculative. Yet in Ukraine, such enclosed volumes of air have become tangible: tanks covered with cages, roads shielded by nets, and entire facilities protected against overhead attacks. These developments mark the architectural manifestation of spatial defense.

Boe concluded with a warning: the tactics developed in war zones will inevitably migrate into civilian contexts. Drones are so accessible that even children can penetrate military airspace, which makes the threat posed by intentional malicious actors even more serious. He pointed to recent reports of drones spying on military transports to Ukraine and sightings near offshore oil facilities in Denmark.

His final point was that societies must begin preparing for this new reality. Building psychological resilience and doctrinal preparedness is essential to deal with the emerging challenges of spatial security, as the line between wartime and civilian use of drones continues to blur.

Andrew Reddie

Andrew Reddie: Associate Research Professor of Public Policy, University of California, Berkeley

Key Message

Artificial intelligence is already embedded in military operations, but its growing influence exposes new vulnerabilities rooted in data quality, automation bias, and overreliance on machine judgment.

Dr. Andrew Reddie opened his remarks by framing today's security environment as suspended between two eras—"halfway between trench warfare and science fiction." In this space, he argued, artificial intelligence (AI) has become both a strategic asset and a structural risk for modern militaries.

He began by clarifying that AI is not a monolithic concept. Rather, it spans three overlapping categories:

- "good old-fashioned AI," rooted in rule-based systems and symbolic reasoning
- technologies that have been retrospectively labeled as "AI" to attract investment or policy attention
- enuinely new and transformative applications in machine learning and automation

For his presentation, Reddie focused on the second and third categories - AI technologies that are already developed, deployed, and operationally relevant. While discussions about future possibilities five or ten years ahead are valuable, he emphasized that AI is already shaping the battlefield today.

- **Situational Awareness and Intelligence**

  Reddie highlighted that the most widespread military applications of AI lie in situational awareness, not autonomous weapons. Despite popular focus on "killer robots," the core of AI's military utility remains in intelligence, surveillance, and reconnaissance (ISR).

  He explained that increasingly sophisticated sensor networks—in orbit, at high altitude, and beneath the sea—are transforming strategic stability and early-warning systems. AI-powered signal and anomaly detection algorithms can, for instance, identify an object moving at 11.2 kilometers per second as a probable intercontinental ballistic missile (ICBM).

  He also noted that cyber defense has been revolutionized by AI. Algorithms now detect and patch network vulnerabilities far more rapidly than human operators, enhancing resilience across digital infrastructures. However, he cautioned that this dependence introduces new points of failure, since maliciously manipulated data can subvert the very systems designed to protect.

- **Decision Support and Operational Planning**

  Reddie next turned to decision support systems, a domain he described as central to current defense innovation. Although some soldiers quip that they "would prefer reliable email systems to advanced AI," he observed that militaries continue to invest heavily in tools that optimize logistics, predictive maintenance, and command decision-making.

- **Automation Bias and Ethical Risks**

  Moving to kinetic applications, Reddie acknowledged that lethal autonomous weapons dominate policy debates. He referenced the Future of Life Institute's well-known video dramatizing automation bias, where a soldier repeatedly follows AI-generated recommendations without question. The scenario, he argued, captures one of the deepest ethical and operational risks: that human operators may surrender judgment to machines in moments of uncertainty or fatigue.

  He underscored that AI's effectiveness is limited by the quality and availability of training data. Conflict-related datasets remain incomplete, inconsistent, and often contextually outdated. Even widely used resources - such as SIPRI's military databases or the Correlates of War project - lack granularity at higher levels of escalation. This absence of real-world examples, Reddie warned, makes it impossible to reliably model the dynamics of major-power conflict or nuclear signaling.

- **Vulnerabilities and Strategic Implications**

  Drawing on his own experience as a war game designer, Reddie expressed concern that policymakers underestimate these data limitations. AI is being embedded in command-and-control systems without sufficient scrutiny of how it performs in crisis conditions, where incomplete information, adversarial manipulation, and data poisoning are likely.

  He stressed that trust and reliability must therefore be treated as core components of military readiness. The same systems that improve intelligence gathering and targeting efficiency can also introduce cascading errors if compromised.

In his conclusion, Reddie emphasized that while AI is already being integrated into military operations, it simultaneously introduces new vulnerabilities. These include risks such as adversarial manipulation and data poisoning, which undermine trust in even relatively accepted applications like intelligence and surveillance. The challenge, he warned, is to ensure that systems can be trusted to function reliably in the uncertainty of conflict. This issue, he concluded, remains one of the most pressing concerns for both policymakers and militaries.

Michal Krelina

Michal Krelina: Associated Senior Researcher, Stockholm International Peace Research Institute (SIPRI)

Key Message

Quantum technologies represent both an extraordinary scientific frontier and an emerging security challenge - poised to transform encryption, navigation, and sensing long before they reshape computing itself.

Dr. Michal Krelina began acknowledging that quantum technologies, among those being discussed at the forum, are perhaps the most mysterious. Their enigmatic nature, he remarked, makes them both tempting and heavily surrounded by hype. He explained that when most people hear the term "quantum technologies," they think of quantum computing and its potential to break today's encryption systems. Yet this, he stressed, represents only a fraction of what quantum technologies encompass. Broadly, they refer to technologies that function on the principles of quantum mechanics, though they span diverse purposes and applications.

He described how quantum computing is widely known for its potential to undermine asymmetric encryption used in current communication systems. However, he argued that more interesting applications may emerge in other domains, such as chemistry, where quantum computers could simulate chemical behaviours beyond the capabilities of conventional computers. Optimization problems, too, could be transformed. He acknowledged that while there is hype around the intersection of quantum and artificial intelligence, there is no definitive proof yet that such combinations will deliver advantages, at least not in the immediate future.

Krelina then turned to quantum communication, highlighting South Korea's advanced position in this field. Along with China, South Korea is one of the only countries with established standards for quantum key distribution already in practical use. He explained that this progress points toward the eventual creation of a "quantum internet," offering services beyond secure communication, including highly precise timing distribution. Quantum sensing and metrology, he noted, could provide accuracy far beyond what current technologies deliver.

He emphasized quantum sensing as perhaps the most immediately relevant technology. While quantum computing may only become practical in ten years or more, and quantum communication is still in testing stages, quantum sensing could be deployed within one or two years. He pointed to the Ukraine conflict, where satellite navigation has often been jammed, as an example of where quantum navigation could provide a decisive advantage. These technologies, he explained, work at the scale of individual electrons, atoms, and molecules, which makes them fragile but also transformative in how information is transferred, processed, and secured. Rather than delivering entirely new weapons, quantum advances will strengthen existing systems, such as improving navigation and surveillance for drones or enhancing AI performance in fields like linear algebra.

Krelina referenced a report he co-authored in July titled Military and Security Dimensions of Quantum Technologies. He summarized several key findings from that work. The first major concern is encryption. Quantum computing could indeed break today's cryptography, though significant efforts are already underway in developed countries to deploy quantum-safe systems. He cautioned, however, that if developing countries lag in adopting these protections, cyberspace could become asymmetric, allowing advanced states with quantum computers to access classified information from weaker states.
Another important application is navigation. Magnetic-aided and gravity-aided navigation requires global maps of anomalies in the Earth's magnetic and gravitational fields. Satellites, he explained, are critical for building such maps, making them a strategic asset. States with the ability to generate and control this data will hold a significant advantage.

He noted that quantum technologies are inherently dual-use, with potential for both civilian and military applications. His own interest began a decade earlier, when discussions about defense applications, particularly sensing, were already prominent. He identified supply chains as a persistent challenge. Many quantum technologies require cryogenic cooling and rare materials such as helium-3, which is a byproduct of nuclear weapons programs and thus extremely scarce.

Krelina also reflected on the unique relationship between fundamental research, applied research, and commercial development in this field. He described quantum technologies as unusually dynamic, with breakthroughs in basic science rapidly moving into applied domains. Yet, at the same time, he warned that research into the security implications of quantum technologies remains underdeveloped and underestimated.

He concluded with a broader warning. Public debate often frames quantum technologies as either beneficial or military-driven. In the mid- to long-term, however, the real issue will be their accessibility. As quantum systems become cheaper and more widespread, the risk of misuse by non-state actors will increase. He emphasized that societies tend to overestimate the short-term effects of new technologies and underestimate their long-term impacts. For this reason, he argued, it is essential to examine both the positive uses of quantum technologies and their potential exploitation by adversaries.

He ended his remarks by stressing the need for deeper understanding of quantum technologies, both for their promise and for their risks.

Hitoshi Nasu

Hitoshi Nasu: Professor of Law, United States
Military Academy, West Point

Key Message

The nature of war remains constant - lethal, brutal, and destructive - but technology is transforming its character, accelerating its tempo, and widening access to tools of conflict beyond the control of states.

Prof. Nasu, Turning to the subject of hybrid warfare, emphasized that modern technologies are changing the characteristics of warfighting but not its nature. The nature of war, he explained, remains constant: it is lethal, brutal, and destructive, inevitably causing casualties among both civilians and service members. No matter how technologies reshape the methods of fighting, this essential nature does not change. What technology is doing, however, is altering the speed and tempo of warfare.

He referred to observations made by Troels Boe regarding the widespread use of low-cost drones, which, when combined with high-fidelity sensors and big data analysis powered by artificial intelligence, are accelerating the pace of conflict and reshaping the battlefield. Defense leaders and commanders, he said, are closely watching conflicts such as those in Ukraine and Gaza. Their analyses increasingly highlight the importance of dispersal, deception, and the use of attritable assets in future conflicts. This recognition is driving efforts to explore both technological and doctrinal solutions in these areas.

Nasu stressed that militaries no longer have a monopoly over modern technology. As Bøe also observed, these technologies are widely accessible to the general public. This accessibility means that individuals now have the ability to commit acts of violence with far greater destructive effect than ever before. The combination of advanced technological capabilities and their widespread availability create conditions that malicious actors can exploit, leveraging socio-technical vulnerabilities in society to wage hybrid warfare.

Drawing on his previous research, Nasu identified three structural conditions that determine the effectiveness of hybrid warfare:

- Technological capability: the availability of advanced tools that enable low-cost, high-impact operations;
- Use of intermediaries: militias, proxies, or surrogates, including non-state actors
- The target state's adherence to the rule of law and accountability.

Prof. Nasu concluded by warning that if technology continues to enable hybrid threats to succeed, the trend could spiral downward. The more effective these tactics appear, the more states and malicious actors will be incentivized to adopt them. This, he argued, represents one of the central challenges in addressing hybrid warfare today.

Following the presentations, Moderator Sibylle Bauer invited the panelists to engage with several audience-submitted and moderator-framed questions, focusing on the intersection of AI, autonomy, and law in modern warfare.

Question 1

"Biases and limitations of AI systems were mentioned, including Israel's Lavender program. Could you discuss how biases affect AI targeting, and what safeguards or baselines are needed?"

Andrew Reddie explained that bias is a feature, not a bug: every model reflects the choices made during training and fine-tuning. The problem in military contexts is the lack of a performance baseline for novel systems such as Lavender. What mattered most in that case, he said, was not automation itself but how states defined legitimate military targets and civilian-casualty thresholds.

Building on this, Hitoshi Nasu noted that in military settings, training data are curated and labeled internally, so concerns differ from those in civilian AI. Still, law must address how decisions are made and verified.

Reddie added that governments often rush to adopt AI for targeting without clarifying training data quality or oversight. Proper metrics and governance are essential before fielding such tools.

Question 2

"A question for Mr. Boe: what systems could prevent or de-escalate major conflict - cyber capabilities, autonomous systems - and, if deployed, what safeguards should accompany them?"

Troels Emil Andersen Boe described how autonomous drone swarms can create a "fog of death," saturating airspace and acting as a form of non-nuclear deterrence. While they could discourage aggression, they risk becoming weapons of mass destruction if left unchecked. He stressed the need for international humanitarian law (IHL) as a guardrail, plus rigorous cybersecurity to prevent hijacking or accidents. Democratic oversight and clear alignment between political aims and technology developers were also essential to avoid reckless escalation.

Question 3

"Why is there a time lag between technological development and policy or legal responses, and how could it be narrowed?"

Hitoshi Nasu argued that law is not always behind; the Geneva Conventions and principles on new weapons already oblige states to ensure compliance, even for tools not yet invented. International humanitarian law can fill regulatory gaps in advance.

Andrew Reddie agreed, saying verification makes technical arms-control regimes difficult. Governance will likely evolve through behavioral norms, Track-2 and Track-1.5 dialogues, and incremental agreements rather than sweeping treaties.

Adding a technological dimension, Michal Krelina added that quantum technologies offer a rare chance for anticipatory regulation, since deployment is still limited. He used submarine detection and quantum navigation as an example of a "cat-and-mouse" stability problem needing early study.

After the Q&A, Andrew Reddie highlighted the importance of integrating expertise across domains - AI, drones, quantum - and connecting policy and technical communities. Michal Krelina encouraged policymakers to act on quantum issues before they become operationalized. Hitoshi Nasu urged participants to critically reflect on legal advice and craft creative arrangements to address hybrid threats. Troels Boe closed by linking technological democratization to the need for strong democratic participation and trust.

Session 3: Resilience of Critical Infrastructure: Reducing Multidimensional Vulnerabilities

Moderator:
James Sullivan
Director of Cyber & Tech, Royal United Services Institute (RUSI)

James Sullivan opened the forum's final session by situating critical infrastructure at the heart of contemporary security debates. Building on themes from the first two sessions, he cautioned against excessive pessimism about technology, urging participants to embed democratic values into design and governance. Yet, he warned, hospitals, power grids, transport systems, and undersea cables remain exposed to cascading threats. Cyber intrusions, ransomware, outdated software, and accidental outages - such as the recent Red Sea cable damage affecting global cloud services - illustrate how vulnerabilities span technical, organizational, and geopolitical dimensions. Responding requires "multi-dimensional strategies," from regulation and incentives to diplomatic levers and cross-sector partnerships.

Gillian Frost
Gillian Frost: Director General for Cyber, Critical Technology and Democratic Resilience Bureau, Global Affairs Canada

Key Message
Protecting critical infrastructure requires a whole-of-society approach -integrating public-private cooperation, cross-border coordination, and resilience planning - to confront malicious cyber activity that directly threatens national security.

Gillian Frost began her presentation by emphasizing that critical infrastructure sits at the intersection of technology, economy, and society. It not only relies on digital systems but also enables them, creating multiple, interconnected vulnerabilities at the core of modern life. Against this backdrop, she outlined four interrelated dimensions of resilience:

- Cyber threats to critical infrastructure,
- Collaboration between states and the private sector,
- Cooperation among states to mitigate malicious cyber activity
- Strengthening international protection frameworks.

She warned that cyber incidents - whether caused by malign actors, human error, or system malfunction - can have profound economic, political, and societal consequences. State-sponsored cyber threat actors, she said, are targeting critical infrastructure networks in Canada and allied countries both for espionage and to prepare for possible disruptive or destructive operations in the future. She cited Salt Typhoon as an example of a major global cyber espionage campaign that implicated Canada among 80 affected states. Canada, she noted, had been working domestically and internationally with partners to respond to these threats.

Frost underlined that when several states share the same vulnerabilities, the risks increase for all. These campaigns, she continued, destabilize cyberspace, increase the risk of miscalculation, and aim to sow panic and distrust within civilian populations. Over the past decade, Canada has intensified efforts to protect critical infrastructure. The first step, she explained, is to clearly define what constitutes critical infrastructure. In Canada, it refers to processes, systems, facilities, technologies, networks, assets, and services essential to health, safety, security, economic well-being, and the effective functioning of government. She described this as a complex web that spans provinces, territories, and international borders.

She pointed to a 2023 survey showing that 100 of the 193 UN member states had published their own lists of critical infrastructure sectors, with energy, information and communications technology, transportation, finance, public services, and health being the most common. At the UN, she noted, discussions continue on voluntary, non-binding norms to protect critical infrastructure during peacetime. She argued that a threat-by-threat approach to protecting critical infrastructure is insufficient. Instead, the focus must be on resilience, regardless of which specific threats emerge.

Moving to her second theme, Frost highlighted the importance of whole-of-society engagement and collaboration between states and the private sector. Such partnerships, she argued, are essential because it is impossible to prevent all cyber intrusions. Canada's 2025 National Cybersecurity Strategy commits to this approach, with the creation of the Canadian Cyber Defense Collective, which brings together public and private partners to address national cybersecurity challenges, policy priorities, and operations. Governments, she said, need the latest insights from industry and academia to inform effective policy. Building trust is central, both between public and private partners and between governments and citizens. A trusting relationship ensures more effective coordination and communication during cyber incidents and encourages partners to report intrusions rather than concealing them.

Her third theme addressed cooperation to mitigate malicious cyber activity. Frost argued that innovation and cybersecurity are not mutually exclusive but mutually reinforcing. She explained that Canada faces a major shortage of cybersecurity talent, producing fewer than 4,000 graduates annually against a demand of up to 25,000 roles. This gap, she warned, threatens both economic stability and public safety. To address it, Canada is investing in advanced research, digital innovation, and skills development to grow its domestic cybersecurity industry. She highlighted that robust incident response frameworks reduce remediation costs, improve efficiency, and support economic resilience. Canada's federal cyber incident response plan, led by Public Safety and the Canadian Centre for Cyber Security, coordinates responses and ensures situational awareness across government.

Finally, Frost addressed international collaboration. She emphasized the importance of partnerships, legislation, and information sharing to strengthen the protection of critical infrastructure. She referenced Bill C-8, proposed legislation on cybersecurity, which includes mandatory incident reporting to improve understanding of the threat landscape and enable more effective defensive action. Canada is also working closely with international partners to promote the UN's 11 norms of responsible state behaviour in cyberspace and to combat cybercrime. This includes publicly attributing malicious cyber activities to specific states, when necessary, a practice Canada has used against actors such as China in relation to Salt Typhoon.

In conclusion, Frost stated that malicious cyber activity against critical infrastructure represents a direct threat to national security, requiring governments to act in order to protect their populations and interests. By strengthening cooperation, sharing information, and working together, she said, states can build resilience to malicious cyber activity and enhance their protection of critical infrastructure.

Allan Cabanlong

Allan Cabanlong: Regional Director for Southeast Asia Hub,
Global Forum on Cyber Expertise (GFCE)

Key Message

Building resilience in critical infrastructure requires a multidimensional approach - integrating technical, economic, legal, and social strategies - to ensure societies can withstand, absorb, and recover from cascading cyber-physical disruptions.

Allan Cabanlong emphasized that resilience in critical infrastructure is not merely a technical issue but also an economic, social, and legal challenge. Speaking in his capacity as Regional Director for Southeast Asia at the Global Forum on Cyber Expertise (GFCE), he shared observations from the region, where interconnected vulnerabilities expose societies to cascading risks.

Cabanlong explained that today's critical infrastructure—including energy grids, transportation systems, financial networks, health services, and digital platforms—are no longer insulated from one another. They are interdependent and exposed to hybrid threats. A ransomware attack on a hospital, for example, can escalate into a national security crisis. A disruption in energy supply can ripple outward to trigger financial instability. Disinformation campaigns during infrastructure outages, he added, can erode public trust and paralyze effective response.
He stressed that true resilience cannot be reduced to firewalls or technical safeguards alone.

Cabanlong detailed how risks manifest across multiple layers:

- Cyber-technical vulnerabilities - including supply-chain compromises, outdated industrial-control systems, and AI-driven attacks—threaten the operational backbone of infrastructure.
- Economic disruptions can cascade across sectors, undermining trade, production, and investor confidence.
- Legal and governance gaps - fragmented policies, outdated regulations, and disputes over data ownership and cloud storage - slow response and blur accountability.
- Social vulnerabilities amplify crises when misinformation fuels panic and public confidence erodes.

Because of these intertwined risks, Cabanlong argued, cybersecurity alone cannot deliver resilience. Nations must strengthen the broader economic, legal, and social foundations that underpin technical defense.

Cabanlong outlined four pillars essential to modern resilience strategies:

- Technical Fortification and Modernization: integrating cybersecurity into digital-transformation projects, protecting operational technologies, building redundancy, and investing in real-time AI-powered monitoring.
- Cross-Sectoral Collaboration: ensuring governments, industry, academia, and civil society work together under the principle that no single actor owns resilience.
- Economic Preparedness: strengthening continuity planning, cyber insurance, and sectoral risk-sharing models that help operators recover after major disruptions.
- Community-Level Adaptability: extending resilience to citizens and communities through public awareness campaigns, community drills, and trusted communication channels that sustain confidence and prevent panic.

"Resilience," he said, "is not only about withstanding and absorbing attacks, but about recovering and adapting fast-

er than adversaries expect."

Cabanlong then reflected on best practices and lessons learned from the ASEAN region and globally. He noted that ASEAN countries are working to harmonize cyber norms and build regional incident response collaboration, with the ASEAN Cyber Cooperation Strategy as a key framework. Member states are developing stronger critical infrastructure protection laws and policies and sharing practices through platforms such as the ASEAN Ministerial Conference on Cybersecurity, the ASEAN Regional Forum, and annual events like Singapore International Cyber Week. He also highlighted the European Union's progress through the NIS2 Directive and the Cyber Resilience Act, which establish minimum standards across member states. South Korea, he observed, stands as a model of technological leadership and whole-of-society preparedness. Within this global ecosystem, the GFCE acts as a platform for cyber capacity building, helping countries, particularly developing nations translate frameworks into practice.

Looking ahead, he identified three priorities for international cooperation. The first is the development of integrated strategies that embed legal, economic, and social resilience into technical infrastructure protection. The second is cross-border exercises and simulations, noting that ASEAN already conducts periodic cyber drills and collaborates with partners such as South Korea's KSPO, the Asia-Pacific Cybercrime Hub, and the World Bank to build regional capacity. The third is continued capacity building and knowledge sharing to ensure that no country or community is left behind in the global resilience equation.

He concluded by emphasizing that resilience is not built in isolation but cultivated through trust, collaboration, and adaptability. A multi-stakeholder approach, he argued, is essential, and as threats grow more complex, societies' ability to withstand, absorb, and recover will depend not only on systems but also on solidarity.

Adewale Peter Obadare

Adewale Peter Obadare: Founder & Chief Visionary Officer, Digital Encode Limited

Key Message

True resilience begins with the health of digital infrastructure. Most cyber incidents are not caused by sophisticated attackers but by outdated, unprotected systems that lack intelligent, adaptive defenses.

He began by defining cybersecurity as the state of well-being of any digital asset. By this definition, he argued, many critical infrastructures are in poor health. Most incidents involving critical national infrastructure, he observed, are not the result of advanced cyberattacks but of outdated and unprotected systems. He referred to the case of Maersk, the global shipping company, which suffered a major ransomware incident. At the time, its core systems were still running on Windows XP, an operating system that Microsoft had already stopped supporting. This made the company an easy target. Similar conditions exist across energy, aviation, transport, and water sectors, where organizations often treat core applications as untouchable "black boxes" and fail to modernize the systems on which those applications depend.

From his consulting experience in aviation, he recalled being asked to assess a platform and finding the same weakness. The application itself was functional, but it operated on outdated systems still running Windows XP. He noted that operators tend to focus investment on proprietary applications that drive their sectors while neglecting the underlying infrastructure that supports them. This imbalance, he argued, creates systemic vulnerabilities.

Obadare organized his analysis around four interdependent pillars—architecture, design, implementation, and operation.

- Architecture, he said, is the blueprint that defines systemic integrity. "If the architecture is flawed," he explained, "no policy or strategy can compensate."
- Design determines resilience. Poorly designed systems multiply risks, as demonstrated in the Colonial Pipeline Incident in the United States, where an outdated VPN system opened the door to a national disruption.
- Implementation is frequently undermined by overreliance on third-party vendors who deploy solutions but fail to transfer knowledge or accountability to operators.
- Operation depends ultimately on people. Without proper awareness and training, even well-built systems fail under pressure. Human error and social engineering, he warned, remain the most common entry points for attackers.

He stressed that resilience requires strength across all four areas. Yet, many infrastructures lack what he described as "cybersecurity intelligent caution," the ability to detect and respond intelligently to threats. He described three levels of intelligence that should be embedded into systems. Augmented intelligence provides real-time awareness of attacks as they happen. Anticipatory intelligence allows prediction of likely threats before they occur. Assistive intelligence ensures that actions are taken correctly, by asking whether organizations are doing the right things, doing them the right way, and ensuring that they are completed effectively. These layers of intelligence, he explained, are largely absent in many critical infrastructures.

Obadare concluded by observing that most national policies and strategies only describe what should be done but do not explain how to do it. He urged governments and operators to move beyond high-level frameworks and develop practical guidance for implementation. He suggested that the forum should produce recommendations focused on "how to do" rather than only "what to do." He ended by thanking the audience and underlining the urgency of improving resilience in critical infrastructure.

Joanna Kulesza

Joanna Kulesza: Assistant Professor, Department of International Law and International Relations, University of Lodz, Poland

Key Message

International law remains the foundation of stability in both the physical and digital realms. Rather than being outdated, it continues to evolve as a living instrument for governing cyberspace, emerging technologies, and future domains such as outer space.

Joanna Kulesza emphasized the importance of international law and cautioned against dismissing it, warning that such an approach would be dangerous. Since 1945, she explained, international law and international organizations have helped maintain peace, particularly in Europe. As a Polish scholar, she acknowledged her bias but highlighted that institutions such as the European Union, the Council of Europe, and the North Atlantic Treaty Organization had been instrumental in keeping Europe stable for nearly eighty years.

Turning to cyberspace, Kulesza observed that international law has been applied to cyber issues for roughly two

decades. She referred to the recent final report of the UN Open-Ended Working Group, which concluded its work in July, coinciding with Korea's release of its official position on the application of international law in cyberspace. Korea's document was the thirty-third such declaration by a sovereign state and joined similar positions expressed by international organizations, including the African Union and the European Union. These statements, she explained, clarify how states interpret principles of international law in relation to malicious cyber operations.

She outlined several key principles contained in Korea's position. This included state responsibility, a principle codified through years of judicial practice and elaborated by the International Law Commission. She also highlighted the debates on sovereignty, noting that while China often refers to cyber sovereignty, in Europe the concept is expressed through digital or technological autonomy. For Europe, sovereignty also extends to protecting critical infrastructures such as satellites. Kulesza further emphasized the principle of due diligence, explaining that states have an obligation to safeguard their societies and their partners by taking measures to prevent cyberattacks.

Kulesza explained that these principles are reflected in the UN Open-Ended Working Group's final document and will continue to be developed through a newly established permanent mechanism. States will reconvene in March 2026 to discuss responsible state behaviour in cyberspace. While the consensus achieved at the UN level was significant, she noted that it was imperfect. States praised the emphasis on capacity building, but some experts sought more extensive discussion of international law.

She then turned to a European example. The European Union has developed what it calls the "cyber diplomacy toolbox," which provides diplomats with guidance on interpreting and applying international law in response to cyber threats. This framework also includes a system of cyber sanctions, a measure that has attracted considerable international attention. For Kulesza, this demonstrated that international law is not abstract theory but a practical tool for diplomacy and security.

Looking ahead, she suggested that similar frameworks might be needed for outer space. With growing security concerns in space, she argued that the principles of the Outer Space Treaty should be clarified and applied to new threats, potentially through a "space diplomacy toolbox." Finally, she connected contemporary debates to lessons from history. On the eightieth anniversary of the Potsdam Agreement, she and her colleagues published a call urging the development of a normative framework for autonomous weapons systems. The goal, she stressed, was not to ban such systems outright but to ensure that human judgment remains central when human life is at risk. Automated decision-making, she argued, must stop when lives are at stake. She compared this initiative to the 1955 Einstein–Russell call on nuclear non-proliferation and suggested that a similar process could help address emerging technologies.

Kulesza concluded by affirming that future progress must be grounded in trust and capacity building. Drawing on her experience working in academia and with young people, she stressed the importance of building knowledge and resilience for addressing both cyber threats and emerging security challenges.

After the panel presentations, Moderator James Sullivan guided a brief question-and-answer segment, posing questions collected from participants in advance and inviting the panelists to share their perspectives on international cooperation and resilience in critical infrastructure.

Question 1

"We've spoken about choosing suppliers and living in a world where you 'fasten your seatbelts.' Joanna, from a European perspective, how reliable a partner is the United States in cyber and technology cooperation?"

Joanna Kulesza replied that, despite turbulence, long-standing international legal safeguards act as "seat belts" for cooperation. She acknowledged U.S. political challenges but noted similar unpredictability elsewhere. The rules and regimes developed over 80 years - diplomacy, law, multilateral forums - provide stability even during disruptions. She stressed that governments, academia, business, and civil society must work together to sustain reliability and a safe future.

Question 2

"Could you share how Canada is managing tensions or uncertainty in its relationship with the U.S., especially on cyber and technology?"

Gillian Frost said Canada's partnership with the U.S. remains deep and practical, rooted in geography, trade, and shared infrastructure. She cited the Canada–U.S. Cybersecurity Action Plan (2022) covering incident management, information-sharing, and public awareness. Cross-border infrastructure, joint law-enforcement, and intelligence cooperation make resilience a shared imperative. She added that bilateral mechanisms often enable faster coordination and mutual assistance during cyber incidents, complementing Canada's broader engagement in multilateral fora. Frost added that Canada and the U.S. also coordinate in the UN, G7 cyber groups, and other forums, maintaining dialogue even amid political fluctuations.

Moderator Sullivan closed the session by thanking the panel and audience, observing that the discussion highlighted how critical infrastructure sits at the heart of national and international security. Adversaries, he said, exploit it to gather intelligence, stage operations, or undermine democratic confidence. Strengthening technical standards and sharing best practices globally remain essential to defending open societies.

Closing Session

Lee Tae Woo
Ambassador for International Cyber Affairs of the Ministry of Foreign Affairs of the Republic of Korea

Distinguished guests, ladies and gentlemen, as we conclude the 2025 World Emerging Security Forum, I wish to extend my deepest gratitude to all our speakers, panelists, moderators, and participants from across the globe.

Your insights and contributions have made this gathering both rich in substance and meaningful in spirit. Throughout today's sessions, we have addressed some of the most urgent challenges confronting the international community.

First, we examined the growing complexity of cognitive warfare and the urgent need to safeguard truth and trust in an age of disinformation.

Second, we explored how emerging technologies - from drones to artificial intelligence to quantum - are reshaping the threat landscape, bringing both historic opportunities and profound risks to global security.

And third, we reflected on the resilience of critical infrastructure and the shared responsibility to reduce vulnerabilities that could disrupt not just essential services but the very stability of our societies.

The discussion was sobering yet also inspiring. They reminded us that hybrid threats are not distant or abstract - they are immediate, evolving, and deeply interconnected. At the same time, this forum has shown us that when governments, academia, the private sector, and civil society come together, we can chart creative and credible ways forward.

First held in 2021 and now marking its fifth edition, the World Emerging Security Forum has reaffirmed its role as a pivotal platform for dialogue, knowledge-sharing, and cooperation. Each year, we strengthen our collective understanding of emerging threats and sharpen our ability to respond with unity and purpose. For the Republic of Korea, this affirms our commitment to advancing responsible governance of technology, to deepening global cooperation, and to contributing our knowledge and expertise to strengthening resilience.

Ladies and gentlemen, as we close, I encourage you to carry forward the spirit of collaboration that has defined this forum. Let us continue to exchange ideas, build trust, and strengthen partnerships. For hybrid threats cannot be confronted in isolation; they demand sustained cooperation, enduring solidarity, and a shared vision for peace and stability.

I thank you all once again for your active participation and dedication. We look forward to your continued engagement and support in future discussions under the framework of the World Emerging Security Forum.

Thank you very much.

Exploration of Emerging Technology-Driven Challenges &
Emerging International Security Issues and
Global Security Collaboration

신기술 기반 복합 위협의 국제안보 함의 분석 및 국제협력 방안 연구

주관연구기관 | 한국과학기술원