국가전략연구위원회 이슈브리핑 42호 (발간일: 2025. 12. 8.)

유럽의 사이버안보 전략 심화와 전략적 자율성: 글로벌 질서 변화 속 EU의 규범·산업·군사적 대응

김주희 (국립부경대)

I. 서론 – 글로벌기술질서 변화 속 EU 사이버안보 전략의 구조적 심화

디지털 전환이 사회·경제·안보 전반을 재구조화하면서 사이버 공간의 전략적 중요성은 국제정치의 핵심 변수로 부상하고 있다. 정보·통신·금융·에너지·교통 등 주요 기반시설은 고도화된 상호연결성을 바탕으로 하나의 통합된 디지털 생태계를 형성하고 있으며, 이러한 환경 속에서 사이버 위협은 기술적 침해를 넘어 국가 경제의 안정성, 공공서비스의 연속성, 민주주의 제도의 신뢰성, 군사작전의 효율성에 영향을 미치는 복합적 위협으로 진화하고 있다(Lella et al. 2021).

특히 글로벌 기술 질서는 미국과 중국의 기술패권 경쟁, 글로벌 공급망의 지정학화, AI·반도체·플랫폼 등 전략 기술의 고도화에 따라 기존 규범·제도적 기반이 흔들리고 있다(European Commission. 2020a). 이 가운데 사이버안보는 기술·산업·군사 영역을 가로지르는 핵심 전략 분야로 자리 잡으며, 국가 간 경쟁과 협력의 주요 매개가 되고 있다.

유럽연합(EU)은 기본권, 데이터 보호, 투명성, 법치주의를 중심으로 한 가치 기반 규범정치의 전통을 유지해 왔다. GDPR은 이러한 전통을 대표하는 제도적 성취이며, 데이터 자기결정권과 투명성을 중심으로 디지털 권리를 보호하는 규범적 토대를 제공한다(European Union 2016a). 그러나 점증하는 사이버 위협, 기술경쟁의 심화, 산업데이터의 전략적 중요성 확대는 기존의 규범 중심 접근만으로는 충분한 안정성과 자율성을 확보하기 어렵다는 문제의식을 확산시켰다(Bendiek and Schallbruch 2019). 플랫폼 생태계의 집중, 산업데이터의 전략적 가치 상승, AI 기술의 사회적 영향 확대는

규범정치가 기술·산업·안보 영역과 긴밀히 연계되어야 한다는 새로운 구조적 요구를 만들어냈다(European Commission 2020b).

특히 미국이 플랫폼, AI, 데이터 정책에서 민간자율 중심의 혁신 모델을 유지하는 반면, 유럽은 공공성·투명성·기본권을 강조하는 규범 중심 모델을 강화하고 있다. 이러한 정책적 차이는 EU 내부에서 "유럽적 기준을 강화해 스스로의 자율성과 영향력을 확보해야 한다"는 논의를 촉진하는 배경 요인으로 작용하였다(Houalla and Portuese 2023). 그러나 유럽의 대응은 미국 정책에 대한 단순한 반작용이 아니라, 변화하는 글로벌기술질서 속에서 EU가 규범·산업·안보 대응을 구조적으로 확장해 온 장기적 흐름으로 이해하는 것이 타당하다.

이와 같은 환경 속에서 유럽의 사이버안보 전략은 규범·기술·산업·군사안보가 상호 연동되는 다층적 구조로 진화해 왔다. GDPR, NIS2, CRA, DSA, DMA, Data Act, AI Act로 대표되는 규범 기반 대응은 유럽적 가치에 기초하면서도 전략적 자율성과 경제안보의 요소를 포함하고 있다(European Union. 2016a; European Union. 2022c; European Commission. 2022a; European Union 2022a; European Union 2022b; European Union 2023; European Union 2024). GAIA-X, 디지털 단일시장(Digital Single Market), 유럽 반도체 법(European Chips Act) 등은 유럽이 기술·산업 기반의 자율성을 확보하기 위해 추진해온 전략적 조치이며(European Union 2022b; European Commission 2025), NATO의 집단방위 체계는 증가하는 사이버 위협 속에서 유럽의 억제력과 대응능력을 보완한다(NATO 2016).

결과적으로 유럽의 사이버안보 대응은 단일한 정책의 집합이 아니라 가치 기반 규범정치, 전략 기술정책, 산업·공급망 대응, 집단안보 대응이 결합된 복합적 체계로서 이해할 필요가 있다. 이는 유럽이 디지털 시대의 정치경제적 행위자로서 자율성을 유지하고 변화하는 국제질서 속에서 안정성을 확보하려는 장기적 전략적 선택의 결과이기도 하다(European Commission 2020).

본 연구는 이러한 문제의식을 바탕으로, 변화하는 글로벌기술질서 속에서 EU의 규범·기술·산업·안보 대응이 어떻게 심화되었는지를 구조적으로 분석하고자 한다. 이를 위해 다음 장에서는 규범 기반 사이버안보 대응(2장), 기술·산업·공급망 대응(3장), NATO와의 협력을 중심으로 한 군사·집단안보 대응(4장)을 차례로 검토한 뒤, 마지막으로 한국이 유럽과의 관계에서 직면하는 협력과 경쟁의 복합적 구조를 분석한다(5장). 이러한 분석은 한국이 변화하는 글로벌기술질서 속에서 전략적 선택 공간을 확대하는 데 필요한 이론적·정책적 함의를 제공할 것이다.

Ⅱ. 유럽의 규범 기반 사이버안보 전략의 심화: 가치·전략·경제안보의 다층적 결합

유럽연합(EU)의 규범 기반 사이버안보 전략은 기본권, 투명성, 책임성, 법치주의라는 유럽의 핵심 가치에서 출발하지만, 최근의 디지털 전환 과정에서 그 방향과 성격이 크게 확장됐다. 유럽은 오랫동안 가치 중심의 규범정치를 디지털 정책의 기초로 삼아 왔으며, GDPR은 이러한 전통을 대표적으로 보여주는 규범이다(European Union

2016a). 그러나 기술 경쟁의 심화, 공급망 불안정 증가, 민관 경계가 모호한 하이브리드 위협의 지속은 기존의 규범 중심 접근만으로는 유럽의 안정성과 자율성을 확보하기 어렵다는 문제의식을 확산시켰다. 이러한 환경 변화는 유럽 내부에서 규범정치와 기술·산업·안보 정책이 유기적으로 결합되어야 한다는 새로운 구조적 요구를 형성하였다(Lella et al. 2021).

특히 미국이 플랫폼, AI, 데이터 정책에서 민간주도·시장 중심 모델을 유지하는 반면, 유럽은 공공성·안정성·기본권을 강조하는 규범 중심 모델을 지속 강화하고 있다. 이러한 정책적 차이는 유럽이 스스로의 규범 체계를 유지·확대해야 한다는 논의를 촉진하는 외부적 배경 요인으로 작용하였다(European Commission 2020b). 그러나 유럽의 대응은 미국 정책에 대한 직접적 반작용이라기보다, 변화하는 글로벌기술질서 속에서 유럽이 장기적으로 자율성과 회복력을 확보하기 위한 구조적 흐름으로 이해되는 것이 타당하다.

1. GDPR: 가치 기반 규범정치의 출발점에서 전략적 자산으로

GDPR은 EU 디지털 정책의 철학과 방향을 결정짓는 핵심 규범으로, 정보 최소수집, 목적 제한, 투명성, 삭제권, 자동화된 의사결정 설명 등 기본권 중심의 원칙을 디지털 환경에 적용한 제도적 성취이다. GDPR은 개인정보 보호라는 전통적 가치에서 출발했지만, 역외 적용 조항을 통해 유럽 외 기업에도 동일 기준을 요구함으로써 규범의 외연을 글로벌로 확대하였다. 이러한 성격 때문에 GDPR은 단순한 인권 규범을 넘어 EU가 디지털 질서에서 “규범 설정자”로서 영향력을 행사할 수 있게 하는 전략적 자산으로 재정의되고 있다(Bendiek and Schallbruch 2019).

GDPR이 자리 잡으면서 유럽은 데이터 가치사슬의 초기 단계에서부터 자율적 통제권을 확보했고, 이는 이후 산업데이터 규범, 플랫폼 규제, AI 규범 등으로 확장되는 디지털 규범체계의 기초가 되었다. 미국이 민간 자율성을 중시하는 환경 속에서 GDPR의 전략적 의미는 더 분명해졌고, 유럽 내부에서도 규범정치를 강화해야 한다는 공감이 깊어졌다.

2. NIS2: 사이버보안을 산업·공급망 안보로 확장

NIS2 지침은 유럽의 사이버보안 정책이 기존의 정보보호 중심 접근을 넘어 경제 기반시설과 산업 전반의 안정성까지 포괄하는 구조로 확장되었음을 보여준다. NIS2는 에너지, 교통, 금융, 보건 등 전통적 기반시설뿐 아니라 반도체, 클라우드 서비스, 데이터센터, 우주, 제조업 등 전략 산업까지 포괄하여 규제 범위를 대폭 확대하였다. 이는 사이버보안이 단순한 기술 문제가 아니라 유럽 경제 기반과 공급망 회복력의 핵심 요소라는 인식에 기초한 변화이다(European Union 2022c).

또한 NIS2는 침해 보고 의무 강화, 공급망 위험평가 제도화, 이사회 책임성 명문화, 제재 강화 등 강력한 조치를 도입했다. 이러한 내용은 사이버보안이 산업정책, 경제안보, 공급망 안정과 긴밀히 연결되어 있음을 반영하며, 유럽 내부에서 공급망 취약

정에 대응하기 위한 구조적 요구가 강화되었음을 보여준다. 국제 공급망 재편과 기술 패권 경쟁이 촉발된 환경 역시 NIS2의 방향 설정에 중요한 배경적 요인으로 작용하였다(European Union 2021).

3. CRA: 설계 단계에서의 보안 의무화

사이버 복원력 법(Cyber Resilience Act, CRA)은 유럽이 기술제품 보안을 규범으로 제도화하기 위한 핵심 조치이다. CRA는 소프트웨어 및 IoT 제품 등 디지털 제품 전반에 대해 설계 단계에서 보안 요건을 내재화하도록 규정하고, 취약점 보고와 패치 제공을 의무화하였다. 또한 제품군을 위험도에 따라 분류하여 고위험 제품에는 보다 강력한 규제를 적용한다. 이는 시장 자율에 맡겨온 기존 보안 모델에서 벗어나 기술 제품의 안전성을 유럽 기준 아래에서 균질적으로 관리하겠다는 의지를 보여준다(European Commission 2022a).

CRA가 외부 기업에도 동일하게 적용된다는 점은 EU가 보안 기준을 '수입 규범'이 아니라 '수출 규범'으로 전환시키는 효과를 가진다. 다시 말해 CRA는 EU 내 시장 접근을 위해 기업들이 유럽의 보안 기준을 준수하도록 함으로써, EU가 기술표준 형성 과정에서도 영향력을 행사할 수 있게 한다. 이는 미국식 시장 중심 보안 모델과 구별되는 유럽식 전략의 일환이다.

4. 플랫폼 규율(DSA/DMA): 공정경쟁과 민주주의 보호

유럽의 플랫폼 규제는 온라인 플랫폼을 단순한 기술 기업이 아니라 민주주의, 공공성, 시장 구조에 영향을 미치는 사회적 행위자로 인식하는 관점에서 출발한다. 디지털 서비스법(Digital Services Act, DSA)은 불법 콘텐츠 확산 방지, 알고리즘 투명성 강화, 위험 평가, 외부감사 등 플랫폼의 책임성을 제도화하였다(European Union 2022a).

디지털시장법(Digital Markets Act, DMA)은 시장지배력을 가진 '게이트키퍼' 플랫폼이 자사 우대 서비스 제공, 데이터 결합, 경쟁사 배제 등 불공정 행위를 하지 못하도록 규정한다(European Union 2022b). 두 규범 모두 시장경쟁뿐 아니라 디지털 공간에서의 민주주의 원칙, 사회적 책임성, 투명성을 보호하기 위한 유럽식 접근을 보여준다.

이러한 규범적 개입은 미국의 혁신·경쟁 중심 규제 모델과의 차이를 명확히 하며, CRA는 외부 기업에도 유럽 기준을 준수하도록 요구하기 때문에, EU가 보안 표준을 사실상 국제화하는 효과를 가진다. 이는 미국의 자율·시장 중심 보안 모델과 대비되는 유럽식 접근이며, 기술 기반 경제안보 전략의 일환이라 할 수 있다.

5. 산업데이터 규범(DGA·Data Act): 기술주권의 핵심 기반

유럽은 산업데이터를 기술주권과 경제안보의 핵심 자산으로 보고 있다. 데이터거버넌스법(Data Governance Act, DGA)은 공공데이터의 안전한 재사용과 데이터 중개자 규율을 통해 산업데이터 순환을 촉진하고(European Union 2022c), Data Act는

IoT 기반 산업데이터를 사용자 중심으로 재배분하여 제조기업의 독점을 완화하고 데이터 이동성을 강화한다(European Union 2023).

이 규범들은 유럽 제조업, 모빌리티, 에너지 등 전략 산업에서 생성되는 데이터를 유럽 기준 아래에서 통제하는 구조를 만들며, 글로벌 플랫폼 기업에 대한 의존도를 줄이고 산업 기반의 회복력을 강화한다. 미국 기반 빅테크의 데이터 생태계 영향력이 커지는 환경은 유럽 내부에서 산업데이터 자율성을 강화해야 한다는 논의를 촉진하는 요인으로 작용하였다.

6. AI Act: 위험 기반 규율과 규범적 선점 전략

인공지능법(AI Act)은 AI 기술을 위험도에 따라 분류하고, 특히 고위험 AI에 대해 투명성, 품질, 안전성, 책임성 등 강화된 기준을 적용하는 세계 최초의 종합적 AI 규범이다(European Union 2024). 유럽은 기술혁신과 기본권 보호 사이의 균형을 강조하며, AI 규범을 통해 사회적 위험을 사전에 관리하려는 철학을 구현했다.

또한 인공지능법(AI Act)은 규범적 선점을 통해 유럽이 글로벌 기술 표준 형성과정에서 영향력을 행사하려는 전략적 시도로 해석된다(Crum 2025). 미국이 민간 혁신 중심의 느슨한 규제 모델을 유지하는 상황에서, 유럽의 규범 기반 접근은 국제적 차별성을 강화하는 전략이 되고 있다.

7. 규범에서 전략·경제안보로의 구조적 확장

유럽의 규범 기반 사이버안보 전략은 가치 기반 규범정치에서 출발했지만, 점차 기술·산업·경제안보와 결합되면서 다층적 전략 체계로 확장되었다. GDPR은 규범정치의 기초를 마련했으며, 네트워크 및 정보 체계 지침(Network and Information Systems Directive 2, NIS2), 사이버복원력법, 디지털서비스법, 디지털시장법, 데이터법, 인공지능법은 규범정치가 산업·기술·안보정치와 연결되는 과정에서 유럽의 방향성을 구체화하였다.

미국의 정책 변화는 유럽 전략의 직접적 원인이라기보다 변화하는 글로벌기술질서 속에서 유럽 내부의 규범·산업·안보 논의를 강화하는 배경적 요인으로 작용하였다. 이러한 맥락에서 유럽의 규범 기반 사이버안보 전략은 단순한 규제의 집합이 아니라, 가치·기술·정치·경제안보가 결합된 유럽식 디지털안보 모델의 핵심축으로 이해해야 한다.

Ⅲ. 유럽의 기술·산업·공급망 기반 사이버 대응: 전략적 자율성 확보를 향한 구조적 심화

유럽연합(EU)의 기술·산업·공급망 대응은 디지털 전환이 가속화되는 가운데 기술경쟁, 공급망 재편, 산업데이터 중요성 증가가 결합된 구조적 환경 속에서 발전해 왔다. 이는 단순한 산업정책이 아니라 유럽이 장기적으로 전략적 자율성을 확보하기 위해 구축한 다층적 대응 체계로 이해할 수 있다(European Commission 2020a). 글로벌 기술 질서가 미국과 중국 중심으로 재편되는 과정에서 유럽은 기술·산업 기반의 취약

성과 종속성을 인식하게 되었고, 이에 따라 역내 공급망 회복력 강화, 핵심 기술 자립, 데이터 기반 산업 생태계 구축이 필수적 전략 목표로 부상하였다(OECD 2022). 이러한 정책은 외부 충격에 대한 반응이라기보다 유럽 내부에서 제기된 구조적 요구에 의해 형성된다는 점에서 특징적이다.

1. 기술주권 논의의 심화와 GAIA-X의 전략적 의미

유럽 기술주권(technological sovereignty) 논의는 유럽 경제가 미국 기반 클라우드·플랫폼 생태계에 구조적으로 의존하고 있다는 문제의식에서 출발한다. 데이터가 산업 가치사슬의 핵심 자원으로 자리 잡는 상황에서, 유럽은 산업 데이터의 저장·처리·유통 과정이 역외 사업자 중심으로 전개되는 구조를 전략적 위험으로 인식했다(European Commission 2025b).

GAIA-X는 이러한 문제의식이 구체화된 프로젝트로, 유럽이 신뢰 가능한 데이터 및 클라우드 인프라 생태계를 구축하기 위한 공동의 시도이다. GAIA-X는 단순히 EU 자체 클라우드를 구축하는 것이 아니라, 제조, 에너지, 모빌리티, 헬스케어 등 산업별 데이터 공간(European Data Spaces)을 상호운용적 방식으로 연결하려는 목적을 가진다. 이는 유럽 산업이 생성하는 데이터를 유럽 기준 아래에서 안전하게 공유하고 활용하도록 지원함으로써, 기술적 종속을 줄이고 산업경쟁력을 높이는 기반이 된다(European Commission 2025b).

특히 미국 hyperscale 클라우드의 시장 지배적 구조는 유럽 내부에서 기술주권 확보 논의를 강화하는 배경 요인으로 작용했다. GAIA-X는 기술 자립을 위한 상징적 조치이자, 유럽 디지털 생태계를 하나의 규범·기술적 틀로 통합하는 장기 전략의 일환이다(European Commission 2022b).

2. European Chips Act와 반도체 공급망의 구조적 재편

반도체 공급망 재편은 유럽 기술정책의 중심에 자리한다. 팬데믹 기간 동안 발생한 반도체 공급 부족과 지정학적 긴장 고조는 반도체가 유럽 경제와 산업안보에서 얼마나 결정적 역할을 하는지 드러냈다.

European Chips Act는 이러한 구조적 취약성을 해결하고 유럽이 핵심 기술 기반을 자립적으로 확보하기 위해 도입된 전략이다. 이 법은 크게 세 가지 축으로 구성된다. 첫째, ‘Chips for Europe Initiative’를 통해 첨단 공정 기술, 설계 역량, 연구개발(R&D)을 강화하고, 파일럿 라인을 구축하며 전문 인력을 양성한다. 둘째, 민관 협력을 통한 반도체 생산시설(fab) 확대를 촉진해 유럽 내 제조 역량을 강화한다. 셋째, 반도체 공급망 위기 시 조기경보와 공동대응을 가능하게 하는 EU 차원의 위기관리 메커니즘을 마련한다(Haramboure et al. 2023).

유럽의 반도체 전략은 미국의 Chips and Science Act나 중국의 반도체 육성 정책과 병렬적으로 전개되고 있지만, 기본적으로 유럽 내부의 장기적 산업 기반 취약성에 대한 문제의식에서 출발했다. 국제기술 질서 변화는 유럽의 전략적 방향성을 강화하

는 배경적 요인으로 작용했을 뿐, Chips Act의 핵심 설계는 유럽 내부 논리에 근거한다는 점이 중요하다.

3. 디지털 단일시장(DSM) 전략과 산업경쟁력 기반의 구조화

디지털 단일시장(Digital Single Market, DSM) 전략은 유럽 디지털 경제를 단일한 정책 체계로 통합하기 위한 구조적 프로젝트이다. DSM은 데이터 이동성, 플랫폼 규제, 전자상거래, 디지털 서비스 등 다양한 정책 분야를 유럽 내부 시장 논리로 통합함으로써, 유럽 기업이 대규모 단일 디지털 시장에서 효율적으로 경쟁할 수 있도록 하는 기반을 제공한다(European Union 2015).

DSM은 단순한 시장 통합을 넘어 유럽 디지털정책의 지주 역할을 수행한다. 일반정보보호규정, 디지털서비스법, 다자톨사정보와 같은 규범 기반 전략뿐 아니라 GAIA-X, 데이터법, 반도체법과 같은 기술·산업 기반 전략이 모두 디지털 단일시장(DSM)이라는 구조적 틀 속에서 통합되고 조정된다. 이 과정에서 유럽 디지털 생태계는 규범·기술·산업정책이 서로 결합된 하나의 정책군(policy cluster)으로 진화하였다(Kommerskollegium 2024).

4. 산업데이터 규범(DGA·Data Act)의 전략적 함의

산업데이터는 유럽 제조업, 모빌리티, 에너지, 스마트 인프라 등 핵심 산업의 경쟁력을 좌우하는 핵심 자원으로, 유럽은 산업데이터가 특정 글로벌 기업 생태계에 종속되는 것을 심각한 전략적 위험으로 인식하고 있다. 이에 따라 유럽은 데이터 거버넌스 법(Data Governance Act, DGA)과 데이터법(Data Act)을 통해 산업데이터의 생산·이동·공유·활용을 유럽 기준에 따라 재구조화하고 있다.

DGA는 공공데이터의 안전한 재사용과 데이터 중개 서비스의 투명성과 독립성을 규정하며, 산업데이터 활용 생태계의 신뢰 기반을 구축한다. Data Act는 IoT 기기에서 생성되는 데이터를 사용자 중심으로 재배분하고 제조기업의 데이터 독점을 제한한다. 이를 통해 산업데이터가 특정 기업 생태계에 갇히지 않고 다양한 산업 행위자 간에 순환할 수 있도록 제도적 기반을 마련한다.

이 두 규범은 기술주권을 확보하기 위한 핵심 축으로서, 유럽이 자국 산업의 경쟁력과 공급망 회복력을 강화하는 데 기여한다(European Union 2023). 글로벌 플랫폼의 시장 지배력이 확대되는 가운데 유럽이 산업데이터 자율성을 강화해야 한다는 논의를 촉진하는 배경 요인으로도 작용하였다(European Union 2022c).

5. AI Act와 유럽식 기술정치의 확장

인공지능법(AI Act)은 AI 기술을 위험 기반으로 분류하고 고위험 AI에 대한 엄격한 규제를 도입함으로써, 기술 발전을 사회적 가치와 조화시키려는 유럽식 기술정치의 방향성을 보여준다. AI Act는 투명성, 안전성, 책임성, 품질관리 등 다양한 규범을 포

함하며, 세계 최초의 포괄적 AI 규범이라는 점에서 규범적 선점 효과를 갖는다(European Union 2022c).

유럽의 접근은 미국의 민간 주도 혁신 중심 기조와 차별화되며, 국제규범 논의에서 유럽의 영향력을 확대하는 데 기여한다(Crum 2025). 인공지능법(AI Act)은 단순한 규제가 아니라, AI 기술 발전이 민주주의, 기본권, 사회신뢰와 조화를 이루도록 하는 유럽의 규범정치가 기술정치로 확장된 사례라고 할 수 있다.

6. 기술·산업·공급망 전략의 구조적 성숙

유럽의 기술·산업·공급망 대응은 규범정치, 기술정치, 산업정책, 경제안보가 결합된 복합적 구조로 발전해 왔다. GAIA-X를 통한 데이터 기반 자율성 확보, Chips Act를 통한 공급망 회복력 강화, 디지털 단일시장을 통한 제도적 통합, 디지털 거버넌스 법과 데이터법을 통한 산업데이터 생태계 재편은 모두 유럽 내부의 구조적 요구에 의해 형성된 대응이다.

글로벌기술질서의 변화와 미국·중국의 전략 환경은 유럽 내부의 논의를 촉진하는 외부적 배경 요인이었지만, 유럽의 전략은 반응적 접근이 아니라 유럽식 기술주권을 구축하려는 축적적 과정이었다. 결과적으로 유럽의 기술·산업·공급망 대응은 유럽식 디지털안보 모델의 핵심 축으로 자리 잡았다.

Ⅳ. 유럽의 집단안보 기반 사이버 대응: NATO와 EU의 다층적 안보 구조 형성

EU의 사이버안보 전략은 규범·기술·산업 정책만으로는 완결되지 않으며, 전통적으로 EU와 NATO가 병존하는 이중적 안보 구조 속에서 작동해 왔다. 사이버 위협은 민·군 영역을 넘나들며, 정보전·전력망 공격·금융 교란·허위정보 확산 등 다양한 형태로 나타나는 만큼 단일한 제도나 기구만으로 효과적으로 대응하기 어렵다. 이러한 현실은 EU의 규범·비군사적 대응과 NATO의 군사·집단방위 기반 대응이 상호보완적으로 결합되어야 한다는 합의를 강화해 왔으며, 유럽식 사이버안보 모델이 다층적 구조로 형성되는 배경이 되었다(Howorth 2017).

1. 사이버 공간의 군사적 위상 확립: NATO의 전략적 전환

NATO는 2016년 사이버 공간을 육·해·공·우주와 동등한 독립적 작전 영역으로 공식 규정함으로써 사이버안보 정책의 구조를 크게 전환시켰다(NATO 2016). 이는 사이버 공격이 물리적 무력행사와 유사한 수준의 전략적 효과를 초래할 수 있다는 인식 아래, 사이버를 NATO의 전통적인 군사작전 틀 안에 통합하려는 의지를 반영한다.

이 결정 이후 NATO는 군사작전과 사이버작전의 연계를 체계화하기 시작했으며, 사이버 위협을 단순 기술 문제로 보지 않고 군사적 억제력의 일부로 재정의했다(Nye 2017). 사이버 공격의 식별 어려움과 공격·방어 간 비대칭성이 존재함에도 불구하고, NATO의 작전 영역 지정은 사이버 분야에서도 억제력이 작동할 수 있음을 공식화하는 조치였다. 이는 사이버 공격의 심각성을 국제사회에 명확히 보여주는 전략적 메시

지이기도 하다.

2. 집단방위(Article 5) 적용 가능성과 억제력 강화

NATO는 특정 수준의 사이버 공격이 집단방위조약(Article 5)의 발동 요건에 해당할 수 있음을 명시하였다. 비록 실제 적용 사례는 없지만, 이 선언은 사이버 공격을 물리적 공격과 유사한 전략적 위협으로 간주할 수 있다는 점을 분명히 했다(NATO 2014; 2016). Article 5 적용 가능성 그 자체가 공격자의 계산에 영향을 미치며, 사이버 공격을 '군사적 도발'로 간주할 수 있다는 신호를 제공해 억제 효과를 강화한다. 특히 유럽의 핵심 기반시설—전력망, 통신망, 금융시스템, 교통망—은 상호연결성이 높아 단일 국가의 방어 역량만으로 보호하기 어렵다(Lella et al. 2021). NATO는 사이버공간을 동맹의 작전 영역으로 공식화한 이후, 사이버 공격이 특정 조건하에서 집단방위조약(Article 5)에 해당할 수 있음을 강조해 왔다. 이는 러시아의 회색지대 전술, 중국의 기술·산업 전략, 신흥기술 확산에 대응하여 NATO가 억제력과 위기관리 기능을 재정립하고 있다는 점에서 중요한 의미를 가진다(전혜원 2022).

3. NATO 사이버방어체계: COC와 CCDCOE

NATO는 복합적인 사이버 위협에 대응하기 위해 지휘·조정 기능을 통합하는 사이버작전센터(Cyber Operations Centre, COC)를 설립하였다. COC는 군사작전과 사이버작전을 동기화하고, 위기 상황에서 신속한 결정을 내릴 수 있도록 지원하며, 회원국 간 정보 공유와 위기 대응을 조정하는 핵심 기구이다(CCDCOE 2025).

한편 에스토니아 탈린의 협력 사이버방위센터(CCDCOE)는 NATO의 연구·훈련·기술개발 역량을 결집하는 중심 역할을 한다. CCDCOE가 주관하는 Locked Shields 훈련은 세계 최대 규모의 실전형 사이버 방어 연습으로, 전력망 붕괴, 통신 장애, 금융 혼란, 허위정보 확산 등 실제적 위협 시나리오를 포괄한다(CCDCOE 2023). 이 훈련은 기술 전문가뿐 아니라 군사 지휘관, 법률 자문관, 외교·전략 담당자 등 다양한 행위자가 동시에 참여해야 하는 구조로 설계되어, 현대 사이버 방어가 단순 기술 대응이 아니라 정치·군사·법·전략이 결합된 종합적 역량임을 확인시킨다. 게다가 Locked Shields는 한국·일본·호주·뉴질랜드(IP4)와의 파트너십이 강화되는 맥락에서 더욱 중요성이 커지고 있다. NATO는 최근 신전략개념에서 파트너국과의 협력을 사이버·신흥기술·회복력 증진의 핵심 요소로 규정하고 있으며, 한국의 참여 확대는 NATO의 글로벌 파트너십 구조의 핵심 사례로 평가된다(전혜원 2024).

4. EU-NATO 협력의 제도화와 상호보완성

EU와 NATO는 회원국 구성에서 상당 부분 중첩되지만 기능적 역할은 명확히 구별된다. EU는 규범·법제·산업정책을 중심으로 비군사적 사이버안보를 담당하고, NATO는 군사적 억제력과 방위 역량을 제공한다. 이러한 역할 분담은 하이브리드 위협과 사이버 공격이 점차 복잡해지는 가운데 상호보완적 안보 체계를 구축하는 데 핵심적

이다.

2016년 이후 EU-NATO 공동선언을 통해 양측은 위협정보 공유, 기반시설 보호, 위기 대응 프로토콜 조정, 허위정보 대응 등에서 협력을 제도화해 왔다. EU는 민간·산업 기반의 회복력과 규범 기반 대응을 강화하는 데에 집중하고, NATO는 군사작전 수행능력과 고위협 대응 역량을 제공함으로써 기능적 분업이 이루어진다. 이러한 구조는 사이버 위협의 다층적 특성과 민·군 경계의 모호성을 고려할 때 필수적이다(EU and NATO 2016; NATO. 2023).

또한 국제안보 환경의 불확실성이 높아지고 미국 전략의 기조 변화가 반복되는 상황은 유럽이 자율적 방위 역량을 강화하는 동시에 NATO와의 협력도 심화해야 한다는 논의를 촉진했다. 이로 인해 유럽의 집단안보 기반 사이버 대응은 단순한 군사동맹 차원을 넘어, EU의 규범정치와 NATO의 방위정치가 통합되는 혼합적 구조로 발전해 왔다.

5. 다층적 안보 구조로서의 유럽식 사이버안보 모델

전체적으로 볼 때 유럽의 집단안보 기반 사이버 대응은 EU의 규범·산업 기반 대응과 NATO의 군사·집단방위 기반 대응이 결합된 다층적 구조로 이루어져 있다. EU는 민간 기반시설의 안정성과 시장·산업 구조의 회복력을 확보하는 방향으로 규범·제도 기반을 강화하고, NATO는 고위협 환경에서 억제력과 방위 능력을 제공한다(European Commission 2020).

이 두 체계는 중복이 아니라 상호보완적 구조로서, 민간 영역과 군사 영역이 긴밀히 얽힌 현대 사이버 위협의 특성을 효과적으로 관리하는 데에 기여한다(EU and NATO 2016; NATO. 2023). 글로벌기술질서 변화, 하이브리드 위협 증가, 미국·중국 전략 변화 등은 유럽 내부에서 이러한 다층적 모델을 더욱 강화하는 요인으로 작용했다. 결국 유럽의 집단안보 기반 사이버 대응은 유럽식 디지털안보 모델의 핵심적인 축으로 자리매김하며, 유럽이 국제질서 속에서 자율성과 안정성을 유지하기 위한 전략적 기반을 제공한다.

Ⅴ. 나가며: 협력과 경쟁이 공존하는 전략 환경

트럼프 2기 미국 행정부는 전임 정부와 마찬가지로 혁신 중심·민간자율 모델을 유지하면서도 사이버 억제력, 핵심기술 보호, 공급망 방어를 강화하는 방향으로 정책 기조를 조정하였다. 사이버 규범의 구속력 있는 제도화보다는 민간 부문의 기술 역량과 시장 경쟁력을 우선시하는 미국의 접근은 유럽과의 정책적 간극을 다시 확대시켰고, 이러한 변화는 유럽 내부에서 규범 기반 디지털 질서와 기술주권 강화의 필요성을 재확인시키는 배경 요인으로 작용했다.

이 같은 국제 기술·안보 환경 속에서 유럽의 사이버안보 전략은 규범, 기술, 산업, 군사안보가 상호 연동되는 다층적 구조로 심화되었다. GDPR, AI Act, NIS2 등 규범 기반 정책은 유럽적 가치와 책임성을 제도화하는 한편, GAIA-X와 European Chips

Act는 데이터·클라우드·반도체 등 핵심 기술에서의 자율성을 확대하는 기반을 구축하였다. NATO의 전략개념과 CCDCOE·COC 중심의 군사적 대응체계는 EU의 규범·산업 중심 접근과 결합해 유럽식 다층적 사이버안보 모델을 형성하였다.

이와 같은 유럽의 구조적 변화는 한국에게 협력 가능성과 경쟁 요인을 동시에 제공한다. 한국과 유럽은 민주주의, 법치주의, 기본권 보호라는 공통의 가치 기반을 공유하며 규범·법제 영역에서는 높은 정합성을 지니지만, 기술주권 강화와 산업데이터 자율성 확보 등 유럽의 전략이 확장될수록 한국 기업과 정부는 새로운 기회와 함께 구조적 부담에도 직면하게 된다. 따라서 한국은 유럽을 단순한 협력 파트너로 보기보다 협력과 경쟁이 공존하는 복합적 전략 행위자로 인식할 필요가 있다(Ministry of Science and ICT, Republic of Korea 2022).

디지털 규범·법제 영역의 협력 가능성 확대

한국은 GDPR 적정성 결정을 확보하여 EU와 데이터 이전이 자유롭게 이루어지는 몇 안 되는 국가 중 하나씩, 이는 한국 기업에 규제 안정성과 시장 접근성을 제공하는 중요한 제도적 기반이다(European Commission 2022). AI Act, DSA, DMA 등 유럽 규범이 글로벌 표준 형성 과정에서 영향력을 확대함에 따라, 한국은 규범 동조(regulatory alignment)를 통해 규제 부담을 낮추고 선제적 대응 역량을 강화할 필요가 있다(이효영 2022).

특히 한-EU 디지털 파트너십은 AI, 반도체, 데이터, 클라우드, 사이버보안 등 핵심 분야에서 제도적 협력을 심화할 수 있는 공식적 장치로, 한국이 글로벌 디지털 규범 논의에 실질적으로 참여할 수 있는 통로로 기능한다.

기술·산업·공급망 기반에서의 상호보완성과 경쟁요인

기술·산업 차원에서 한국과 유럽은 강한 상호보완성을 가진다. 반도체에서 한국은 제조 기반을, 유럽은 장비·설계 기술을 보유하고 있어 공동 연구개발과 공급망 연계 협력이 용이하다. 배터리 산업에서도 한국 기업들의 유럽 현지 생산 확대는 EU의 Green Deal 산업전략 및 Net-Zero Industry Act와 결합해 상호이익을 창출할 수 있다(Haramboure et al. 2023).

그러나 이러한 상호보완성은 동시에 경쟁 요인을 내포한다. 유럽의 기술주권 전략은 반도체, 배터리, AI, 클라우드, 산업데이터 분야에서 역내 기술·생산기반 육성을 강조하고 있으며, 이는 장기적으로 한국 기업에게 역내 규제 준수 비용 증가, 기술경쟁 심화, 현지화 요구 확대 등의 압력으로 작용할 수 있다(European Union 2021).

또한 Data Act와 Data Governance Act가 산업데이터 접근·이동·공유 규칙을 강화함에 따라, 한국 기업은 유럽 데이터 생태계의 규범에 맞춘 사업 모델과 기술 전략을 재정비해야 한다. 데이터 주권이 강화될수록 유럽 내 한국 기업의 활동은 유럽 기

준에 더욱 깊이 종속될 가능성이 커진다(김현수 외 3명 2023).

사이버·군사안보 영역에서의 협력 기회 확대

한국은 NATO 회원국은 아니지만 공식 파트너 국가로서 사이버방위·신흥기술·회복력 등 핵심 분야에서 협력을 확대해 왔다. 특히 2022년 이후 NATO가 IP4(한국·일본·호주·뉴질랜드)와의 연계를 강화하면서, 한국의 참여는 단순한 안보 협력을 넘어 유럽의 다층적 사이버안보 구조에 접속하는 중요한 경로가 되고 있다(Pardo 2023). 이러한 참여는 기술·전략·법적 대응을 통합하는 복합적 사이버 위협 환경 속에서 한국의 역량을 실질적으로 강화하는 데 기여할 수 있다. 또한 한국이 NATO와 체결한 개별 맞춤형 파트너십 프로그램(ITPP)는 사이버안보·신흥기술·국방표준 등에서 구체적 협력 계획을 담고 있으며, 이는 유럽의 사이버안보 전략과의 연계에서 중요한 의미를 갖는다(전혜원 2023).

EU 역시 Cyber Solidarity Act와 Joint Cyber Unit을 중심으로 위협정보 공유, CERT 협력, 기반시설 공동방어, 허위정보 대응 등 다층적 협력 구조를 강화하고 있어 한국과의 협력 여지가 확대되고 있다(European Union. 2023a). 한국은 미국·유럽·아시아를 연결하는 전략적 위치를 바탕으로 사이버안보 협력에서 조정자 역할을 수행할 수 있으며, 이는 점증하는 하이브리드 위협 환경 속에서 중요한 전략적 자산이 된다.

한국의 전략적 접근: 조정자·연결자·협상자의 역할

미국과 유럽의 디지털·기술·규범 체계는 서로 다른 방향성을 갖고 있으며, 한국은 이들 사이에서 중첩된 규범 환경을 효과적으로 관리해야 하는 도전에 직면해 있다. 미국은 기술혁신과 민간주도 모델을 중시하는 반면, 유럽은 규범 중심·공공성·책임성을 강조하는 모델을 추구한다. 이러한 차이는 한국이 어느 한쪽 모델에 일방적으로 정렬하는 방식이 아니라, 양 체계 간 균형을 유지하며 정책을 조정해야 하는 구조적 환경을 만든다(Houalla and Portuese 2023).

따라서 한국은 디지털 규범·기술·산업·안보 전반에서 조정자(coordination agent), 연결자(connector), 협상자(negotiator)의 역할을 동시에 수행할 필요가 있다. 규범 영역에서는 EU와의 조기 조율을 강화해 규제 대응 비용을 줄이고, 산업 영역에서는 협력 기회를 활용하되 경쟁 요인을 장기적으로 관리할 수 있는 산업·기술 전략을 마련해야 한다. 사이버안보 영역에서는 NATO·EU·아시아 각국과의 협력 구조를 확대하여 한국의 전략적 영향력을 강화할 수 있다.

결론적으로 EU의 다층적 사이버안보 전략은 한국에게 광범위한 협력 가능성을 제공하는 동시에 복합적인 경쟁 요인도 함께 제시한다. 규범·기술·산업·안보가 결합된 유럽식 접근은 한국에게 신뢰 기반 협력의 기회를 제공하지만, 기술주권 강화와 산업 내재화 전략은 한국 기업의 부담을 증가시키는 요소로도 작용한다(EU and NATO

2016; NATO. 2023).

특히 NATO의 전략개념 변화와 글로벌 파트너십 확대는 한국의 대유럽 전략적 선택 공간을 넓히는 동시에, 유럽의 다층적 사이버안보 체계가 한국에게 제공하는 협력·경쟁 요인의 구조를 보다 복합적으로 만들고 있다(전혜원 2022). 따라서 한국은 유럽을 협력과 경쟁이 공존하는 전략적 행위자로 인식하고, 변화하는 글로벌기술질서 속에서 자율성과 안정성을 확보할 수 있는 다층적 대응 전략을 마련해야 한다. 이는 한국이 디지털 전환과 기술 경쟁의 시대에 지속 가능한 국가 전략을 구축하는 데 중요한 기반이 될 것이다.

참고문헌

김현수·예상준·강민지. 2023.『글로벌 디지털플랫폼의 데이터 집중화에 따른 경제적 영향 분석』. 세종: KIEP.

이효영. 2022.『경제안보의 관점에서의 디지털무역 규범과 우리의 디지털경제외교 전략』. 서울: 국립외교원 외교안보연구소.

전혜원. 2024. "NATO-인도태평양 4개 파트너국 협력."『IFANS』2024(21): 1-21.

_____. 2023. "2023 NATO 정상회의와 한국·NATO 협력 한국 NATO ITPP를 중심으로."『IFANS』2023(22): 1-27.

_____. 2022. "2022년 NATO 신전략개념 및 정상회의 분석과 향후 전망."『IFANS』2022(22): 1-29.

Bendiek, Annegret and Martin Schallbruch. 2019. "Europe's Third Way in Cyberspace: What Part Does the New EU Cybersecurity Act Play?" *SWP Comment* (52): 1-8

CCDCOE. 2023. "World's largest cyber defense exercise Locked Shields kicks off in Tallinn." https://ccdcoe.org/news/2023/worlds-largest-cyber-defense-exercise-locked-shields-kicks-off-in-tallinn (검색일: 2025. 11. 07).

_____. "Cyber defence at the 28th NATO Summit in Brussels, 11-12 July 2018." https://ccdcoe.org/incyder-articles/cyber-defence-at-the-28th-nato-summit-in-brussels-11-12-july-2018 (검색일: 2025. 11. 07).

Crum, Ben. 2025. "Brussels effect or experimentalism? The EU AI Act and global standard-setting." *Internet Policy Review* 14(3): 1-21.

EU and NATO. 2016. "Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization." (July 8) https://www.europarl.europa.eu/delegations/en/dnat/documents/eu-texts (검색일: 2025. 11. 08).

European Commission. 2025a. "European Chips Act." (September 29) https://digital-strategy.ec.europa.eu/en/policies/european-chips-act (검색일: 2025. 11. 13).

_____. 2022a. "Cyber Resilience Act." (September 15) https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act (검색일: 2025. 11. 10).

_____. 2022b. "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee

and the Committee of the Regions – A European Strategy for Data." *Official Journal of the European Union* COM(2022). 45 final.

_____. 2022c. "Adequacy decision for the Republic of Korea." (June 16) https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964 (검색일: 2025. 11. 16).

_____. 2020a. *Shaping Europe's Digital Future*. Luxembourg: Publications Office of the European Union.

_____. European Commission. 2020b. *The EU's Cybersecurity Strategy for the Digital Decade*. Brussels: European Commission.

_____. 2020c. "New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient." (December 16) https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391 (검색일: 2025. 11. 16).

_____. "A European strategy for data." https://digital-strategy.ec.europa.eu/en/policies/strategy-data (검색일: 2025b. 11. 13).

European Union. 2024. "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)." *Official Journal of the European Union* L(202).

_____. 2023a. "Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)." *Official Journal of the European Union* L series.

_____. 2023b. "Proposal for a Regulation of the Europena Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents." *Official Journal of the European Union* COM(2023) 209.

_____. 2022a. "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)." *Official Journal of the European Union* L 333.

_____. 2022b. "Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA

relevance).” *Official Journal of the European Union* L 277/1.

_____. 2022c. “Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance).” *Official Journal of the European Union* L 265/1.

_____. 2022d. “Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance).” *Official Journal of the European Union* L 152/1.

_____. 2021. “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.” *Official Journal of the European Union* COM(2021) 350 final.

_____. 2016. “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).” *Official Journal of the European Union* L 119/1.

_____. 2015. “A Digital Single Market Strategy for Europe.” *Official Journal of the European Union* COM(2015) 192.

Haramboure, Antton et al. 2023. “Vulnerabilities in the semiconductor supply chain.” *OECD Science, Technology and Industry Working Papers* 2023(05): 1-35.

Houalla, Hadi and Aurelien Portuese. 2023. “The Great Revealing: Taking Competition in America and Europe Seriously.” *ITIF* (May) https://www2.itif.org/2023-us-eu-competition.pdf (검색일: 2025. 11. 15).

Howorth, Jolyon. 2017. “EU-NATO Cooperation: The Key to Europe’s Security Future.” *European Security* 26(3): 454-459.

Lella, Ifigeneia et al.(eds). 2021. *ENISA Threat Landscape 2021*. Attiki: ENISA.

Kommerskollegium. 2024. *The EU Single Market in the Digital Era: From legislative complexity to clarity*. Sweden: Stockholm.

Ministry of Science and ICT, Republic of Korea. 2022. *Korea and the EU Launch the ROK-EU Digital Partnership*. Seoul: Ministry of Science and ICT.

NATO. 2023. “Joint Declaration on EU-NATO Cooperation by the President of

the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization." (January 10) https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2023/01/10/joint-declaration-on-eu-nato-cooperation (검색일: 2025. 11. 07).

_____. 2016. "Warsaw Summit Communiqué: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016." (July 9) https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique (검색일: 2025. 11. 07).

_____. 2014. "Wales Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales." (September 5) https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2014/09/05/wales-summit-declaration (검색일: 2025. 11. 05).

Nye, J. S. 2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41(3): 44-71.

OECD. 2022. *Going Digital to Advance Data Governance for Growth and Well-being*. Paris: OECD Publishing.

Pardo, Ramon. 2023. "South Korea-NATO cybersecurity cooperation: learning to work together in the face of common threats." *ARI* 89/2023.