사이버안보연구, 2집 2호 2025 겨울, 099-137

EU 사이버안보의 법적 거버넌스가 주는 국내 시사점 및 국제협력의 방향성

심소연 | 국회도서관 법률자료조사관

논문접수일 2025년 10월 12일 | 논문심사일 2025년 11월 30일 | 게재확정일 2025년 12월 10일

논문 요약

최근 생성형 AI 시스템의 출현과 국가 중요 인프라 시설의 디지털화가 촉진됨에 따라 사이버 위협과 공격이 증가하고 있으며, 이는 개인과 사회를 넘어 국가 안보 전체에 심각한 영향을 미치고 있다. 유럽연합(EU)은 이러한 초국가적 위협에 대응하기 위해 「사이버보안법」, 「사이버 복원력법」, 「사이버 연대법」, 「NIS2 지침」 및 「핵심 조직 복원력 지침」 등 다층적이고 포괄적인 법적 거버넌스 체계를 구축하고 있다. 본 연구는 EU의 이러한 사이버안보 법령들이 어떻게 법적 거버넌스를 구축하고 작동시키는지 종합적으로 검토하고, 이를 통해 국내 사이버안보 체계에 대한 시사점과 국제협력의 방향성을 제시한다.

대한민국은 EU가 이미 법제화된 체계를 갖추고 예방에 주력하는 것과는 대조적으로, 관련 법률 입법 제안 단계에 머물러 있어 일관된 대응에 어려움이 존재한다. EU의 입법례는 대한민국에 '국가 사이버안보 기본법(가칭)' 제정을 통한 거버넌스 명확화, 유럽연합사이버보안청(ENISA)과 같은 중앙 조정기관을 통한 민관 협력 강화, 사이버보안 인증 및 관리 체계의 전문성 제고, 그리고 사후 처벌이 아닌 사이버 복원력 중심의 패러다임 전환 가속화를 위한 개선 과제를 제시한다.

동아시아 지역은 미·중 전략 경쟁과 지정학적 긴장(러시아-북한 신조약) 심화로 사이버안보 협력의 진영화가 불가피한 상황이다. 대한민국은 EU가 「사이버 연대법」을 통해 구축한 '유럽 사이버 방패'와 같은 포괄적인 공동 방어 및 지원 체계를 벤치마킹하여, ICT 강국으로서 사이버보안 ODA를 활성화할 뿐만 아니라, 자유민주주의 진영 내 사이버안보 협력국들과의 공동 훈련 및 경제적 인센티브제 도입을 통해 사이버안보 분야에서 국제 리더십을 증진하고 안정적인 협력 환경을 구축하는 데 중추적인 역할을 해야 한다.

주제어 유럽연합, 사이버안보, 사이버 연대법, 사이버 복원력법, 국제협력

Ⅰ. 머리말

2022년 11월말 오픈AI가 출시한 ChatGPT를 필두로 한 생성형 AI 시스템의 출현은 기존 정보통신기술(ICT)을 고도화하고 국가의 중요 인프라 시설(전력, 수도, 원자력, 정보 통신 등)의 디지털화를 촉진했다. 이에 따라 사이버공간 역시 전통적인 지상, 해상, 공중, 우주와 마찬가지로 공격의 장으로 인식되고 있으며, 국가와 비국가 행위자 모두로부터 다양한 사이버 위협과 공격이 증가하고 있다. 더욱이 군사적, 민간적 인프라 간의 구분이 모호해지고 있고, 에너지, 교통, 우주 기반의 인프라가 점점 더 공격에 노출되면서 사이버 위협은 개인과 사회를 넘어 국가 전체에 영향을 미칠 수 있게 되었다. 특히, 사이버 공격은 은밀하게 광범위한 시공간에서 발생할 수 있기에 국방을 포함한 여러 분야에 걸쳐 물리적 공격 이상으로 국가에 심각한 영향을 줄 수 있다(심승배. 2024). 따라서 사이버 위협과 공격을 예방하고 효과적으로 대응하고, 피해가 발생할 시, 이를 신속히 복구함으로써 정보의 기밀성·무결성·가용성을 보장하는 것이 중요하다.

'Cybersecurity'는 우리말로 사이버안보 또는 사이버보안으로도 번역되는데, 이 둘은 비슷한 개념이지만, 그 초점과 범위에서 차이가 있다. 사이버보안은 주로 기술적 측면에 초점을 맞추며 정보시스템, 네트워크, 프로그램, 데이터 등을 사이버 공격이나 무단 접근으로부터 보호하는 것을 의미한다. 반면에 사이버안보는 사이버보안의 기술적 요소뿐만 아니라, 법적, 정책적, 사회적 측면도 포함하여 국가안보와 관련되며, 국가 간의 사이버 전쟁, 사이버 범죄, 정보 전쟁 등과 같은 더 넓은 범위의 문제를 다룬다(채재병 & 김일기, 2020, 4~5). 즉, 사이버보안은 주로 기술적 방어에 중점을 두고, 사이버안보는 더 포

괄적인 국가 및 조직의 안전을 위한 정책적 접근을 포함하는 개념으로 이해할 수 있다. 따라서, 국가적 인프라를 보호하기 위해서는 개인, 기업, 조직의 IT 환경이 철저하게 관리되어야 하기에 사이버보안은 사이버안보의 중요한 구성 요소로 인식되어왔다. 그러나, 2024년 7월 미국 마이크로소프트(MS)사의 클라우드 서비스 장애가 발생하여 주요 은행, 언론사와 항공사 등 민관 기관뿐만 아니라 공공기관들이 겪은 대규모 IT 중단 사태를 통해 알 수 있듯이(연합뉴스 2024/7/19), 사이버안보와 사이버보안의 경계는 점차 희미해지고 있다. 사물인터넷(IoT) 시대에 'Cybersecurity'의 개념을 네트워크, 정보시스템, 정보의 보호로만 제한하는 것은 시대착오적이며 'Cybersecurity'는 기본권과 자유, 물리적 안전 등의 가치를 유지하는 데 점점 더 중요해지고 있다(Chiara, Pier Giorgio, 2024).

사이버공간은 국가, 비국가행위자, 공공 및 민간 기관에 의도된 기능을 위해 데이터에 의존하고, 이러한 데이터를 사용하는 시스템과 데이터의 기밀성(Confidentiality), 무결성(Integrity) 및 가용성(Availability) 라는 CIA 3요소의 보장을 위해 방어적인 조치를 취해야 하는 보안 문제를 제시한다(Van Puyvelde, Damien & F. Brantly, Aaron(이상현, 신소현, 심상민 옮김), 2023, 175).

유럽연합(이하 EU)은 이러한 사이버공간에서 벌어지는 위협에 대한 포괄적이고 통합적인 법적 거버넌스 체계를 구축함으로써 역내 디지털 복원력과 안보를 강화하고 있다. EU의 이러한 노력은 급변하는 사이버 위협 환경 속에서 개별 국가의 대응을 넘어선 초국가적 차원의 협력과 연대의 중요성을 강조한다. 2022년 러시아의 우크라이나 침공과 같은 지정학적 갈등은 사이버안보의 중요성을 더욱 확산시키는 계기가 되었으며, 이는 EU 회원국을 포함한 동맹국들이 직면한

다양한 사이버 공격 사례를 통해 명확히 드러났다(Carrapico, Helena & Farrand, Benjamin, 2024, 3).

또한, 2022년 2월 말 러시아의 우크라이나에 대한 군사적 공격으로 시작된 러시아-우크라이나 전쟁 등으로 국제적 갈등이 격화되고 국가 중요 인프라 시설과 공급망 등을 대상으로 하는 사이버 위협이 증가하면서 광범위한 지정학적 불안정과 함께 각 국가의 안보도 위협받고 있다. CERT-EU[1]의 2023년 보고서는 '러시아의 우크라이나 침공 이후 EU 회원국 등 우크라이나의 동맹국들은 여러 유형의 사이버 공격에 직면했다'라고 지적했다(CERT-EU, 2024). 실제로, 러시아 해커 조직 클롭(Clop)은 많은 기업이 활용하는 파일 전송 프로그램 '무브잇(MOVEit)'을 랜섬웨어로 감염시켜 전 세계 정부 기관과 기업들에 피해를 줬으며, 특히 유럽에서는 영국, 스위스, 벨기에, 독일 등의 피해가 컸다(보안뉴스 2023/6/18). 대한민국도 2025년 4월 18일 SK텔레콤의 가입자 정보가 담긴 홈 가입자 서버(Home Subscriber Server, HSS)가 해킹된 사이버보안 사고가 있었고 이로 인한 개인 금융정보 탈취, 신원 도용과 같은 2차 피해가 우려되는 상황 속에서 사이버보안의 중요성에 대한 인식이 증가하고 있다.

이러한 맥락 속에서 본 연구는 다양한 EU 사이버안보 법령(「사이버보안법」, 「사이버복원력법」, 「사이버 연대법」, 「NIS2 지침」 및 「핵심 조직 복원력 지침」)을 검토하고 이러한 법령들이 어떻게 EU 사이버안보의 법적 거버넌스를 구축하고 작동시키는지 종합적으로 살펴본 후, 이를 통해

1) CERT-EU는 EU 기관 및 단체를 위한 컴퓨터비상대응팀으로, 모든 EU 기관 및 단체의 정보통신기술(ICT) 인프라를 보호하고 사이버 사고에 대한 대응을 조율한다.

국내 사이버안보 법제에 대한 시사점을 도출하고 사이버안보 국제협력의 방향성을 제시하고자 한다.

Ⅱ. EU의 사이버안보 법제

1. 사이버보안법(Cybersecurity Act)

EU의 사이버보안법(Cybersecurity Act)은 2019년 4월 17일에 제정되어 같은 해 6월 27일부터 시행 중인 법이다(Regulation (EU) 2019/881). 이 법의 주된 목적은 EU 회원국 전체의 사이버보안을 강화하는 것으로, 이를 위해 유럽연합사이버보안청(European Union Agency for Cybersecurity, 이하, ENISA)을 상설기관으로 격상하여 권한을 강화한다. 또한, 정보통신기술(ICT) 제품, 서비스 및 프로세스 인증에 적용되는 포괄적인 규칙을 담은 EU 차원의 '사이버보안 인증 기본체계(Cybersecurity Certification Framework)'를 개발하는 것을 목표로 한다(법률신문 2024/4/22).

2023년 4월 18일, EU 집행위원회는 사이버보안법 개정안을 발표했으며, 이 개정안은 2024년 12월 19일에 개정되었다. 개정안의 주요 내용은 기존의 사이버보안 인증 기본체계 구축에서 한 걸음 더 나아가 '관리형 보안 서비스(Managed Security Services, MSS)'를 사이버보안 인증체제에 포함하는 것이다. 관리형 보안 서비스(MSS)는 사고 대응, 침투 테스트, 보안 감시 및 자문을 포함한 사이버안보 전반에 관한 위험 관리 활동을 수행하거나 지원하는 서비스를 의미한다. 관리형 보안 서비스(MSS) 인증은 공급자(provider)의 기술 역량과 데이터 보호

능력을 평가하고 보장하며, 위험 수준에 따라 기본, 상당, 고급의 세 단계로 구분된다(「사이버보안법」 제52조.).

관리형 보안 서비스(MSS) 업체는 데이터의 기밀성, 무결성, 가용성을 유지하고 사고 발생 시 신속하게 복구해야 하는 의무를 진다. EU 사이버보안 인증 체계는 ICT 제품, 서비스, 프로세스 및 관리형 보안 서비스(MSS)가 낮은 위험의 '기본(basic)' 등급에 해당하는 경우에만 관련 업체의 자체 적합성 평가를 허용한다(심소연, 2025a, 6). 이는 인증의 신뢰성과 효율성을 동시에 확보하기 위한 조치이다.

이 법은 EU 역내 시장의 단일화를 촉진하기 위한 중요한 규정도 포함한다. 회원국은 EU 인증 체계가 이미 적용되는 ICT 제품, 서비스, 프로세스 및 관리형 보안 서비스(MSS)에 대해 새로운 국내 인증제도를 도입할 수 없다. 이를 통해 EU는 인증 중복을 방지하고 EU 역내 시장의 단일화를 촉진할 것으로 기대한다(심소연, 2025a, 6).

관리형 보안 서비스(MSS) 인증은 사이버보안 역량과 서비스 품질에 중점을 둔다. 반면, 개인정보보호 관리 체계 인증은 EU 개인정보보호법(GDPR) 제42조에 별도의 인증제도를 마련하고 있어, 사이버보안 인증과 개인정보보호 인증을 분리하여 관리하는 EU의 접근 방식이 특징이다. 이는 대한민국이 「개인정보보호법」 제32조의2에 근거한 정보보호 및 개인정보보호 관리 체계 인증(ISMS-P)[2]을 획득하면 「정보통신망법」 제47조에 따른 정보보호 관리 체계 인증(ISMS)을 포함하는 것으로 간주하는 것과 대조적이다(심소연, 2025a, 7).

2) Information Security Management System – Personal Information Protection Management System

사이버보안 인증은 각 회원국의 국가 사이버보안 인증 기관이 감독하며, ENISA가 기술적 기반 마련을 담당한다. 개인정보보호 인증은 각국 개인정보보호 감독기관이 기준을 승인하고, 국가 인정기관이 인증기관을 인정하는 구조이다. 이러한 분리 관리는 각 영역의 전문성과 특수성을 존중하면서도, 디지털 경제에서 필수적인 사이버보안과 개인정보보호라는 두 핵심 가치를 효과적으로 보장하기 위한 EU의 전략적 접근법을 반영한다고 볼 수 있다.

이러한 EU 사이버보안법의 체계는 EU가 역내 디지털 생태계 전반에 걸쳐 통일된 보안 표준을 적용하고, 관리형 보안 서비스와 같은 핵심 분야의 신뢰성을 확보하며, 궁극적으로는 광범위한 사이버 위협으로부터 시민과 기업을 보호하려는 의지를 보여준다.

3. 사이버 복원력법(Cyber Resilience Act)

유럽연합의 사이버 복원력법(Cyber Resilience Act, CRA)은 2024년 10월 23일에 공식적으로 제정되었고, 2024년 12월 10일에 발효되었다. 이 법의 주요 의무는 2027년 12월 11일부터 적용된다. 이 법은 디지털 요소가 포함된 제품(제품 및 소프트웨어)의 취약점 및 사이버 위협에 대응하기 위한 EU 최초의 일반 사이버보안 규정으로, EU 내에서 공급되는 제품의 디지털 요소에 대한 수평적 사이버보안 요구사항을 설정함으로써 제품·서비스 전 생애주기에서 사이버보안 수준을 강화하는 것이 목적이다(Regulation (EU) 2024/2847).

1) 적용 대상

사이버 복원력법은 디지털 요소가 포함된 모든 제품(직·간접적으로

네트워크에 연결 가능한 하드웨어·소프트웨어) 판매자·제조사·수입자·유통업자에게 적용되며, 의료기기, 항공, 자동차 등 자체 규제가 있는 분야는 제외된다. 비상업적 오픈소스 소프트웨어는 적용 대상이 아니다(「사이버 복원력법」 제2조~제3조).

2) 주요 내용

- 필수 사이버보안 요건(Essential cybersecurity requirements): 제조사는 위험 기반 접근으로 해킹·침입·취약점 발생 가능성에 대응해야 하며, 안전한 개발·설계·생산·테스트·배포·수정 과정 관리가 요구된다(제10조).
- 제조사는 보안 업데이트 지원 기간을 명시하고 사용자에게 투명하게 고지해야 한다(제11조).
- 취약점 발견 시 대응 프로세스 및 제조사/유통사/수입자의 보고 의무를 규정한다(제12조).
- 고위험·중요 제품은 제3자 인증기관의 적합성 평가를 거쳐야 하며, 기타 제품은 자체 적합성 선언이 가능하다(제16조~제19조).
- 사이버 복원력법상 적합성 평가를 충족한 제품의 경우, CE 인증 마크 부착이 가능하다(제20조).
- 시장 감시체계를 도입하고 회원국 당국 간 협력을 규정한다(제28조~제29조).
- 사이버 복원력법 미준수 시 최대 과징금은 1,500만 유로 또는 전 세계 매출의 2.5%까지 부과가 가능하다(제30조~제31조).

사이버 복원력법의 '브뤼셀 효과'가 어떻게 전개될지는 아직 알 수 없지만, 글로벌 데이터 거버넌스 기본체계의 분열을 악화시킬 뿐만

아니라 다양한 정책 영역에서 지정학적 긴장과 전략적 경쟁을 증가시켜 궁극적으로 원활하게 작동하는 데이터 경제와 그에 따른 최적의 법적 설계에 거의 기여하지 못할 수 있다는 우려도 존재한다(Mira, Burri, & Zaira, Zihlmann, 2023, 45).

2. 사이버 연대법(Cyber Solidarity Act)

사이버 연대법(Cyber Solidarity Act)은 러시아-우크라이나 전쟁의 장기화로 EU 회원국들이 겪는 사이버 위협이 급증함에 따라, 범유럽 차원의 거버넌스를 기반으로 사이버안보 위협을 예측하고 탐지하며 체계적인 관리 및 대응을 강화할 필요성 아래 제정되었다. 이 법은 2023년 4월에 EU 집행위원회가 제정을 제안했으며, 2024년 12월 19일에 제정되어 2025년 2월 4일부터 시행 중이다(Regulation (EU) 2025/38).

이 법은 EU의 사이버안보를 위한 네 가지 핵심 메커니즘을 담고 있다:

- 유럽 사이버보안 경보 시스템(European Cybersecurity Alert System)
- 사이버보안 비상대응 메커니즘(Cybersecurity Emergency Mechanism)
- EU 사이버보안 예비 자원(EU Cybersecurity Reserve)
- 사이버보안 사고 검토 메커니즘(European Cybersecurity Incident Review Mechanism)

첫째, 유럽 사이버보안 경보 시스템은 EU 회원국 및 국경 간 '보안운영 센터(Security Operation Centre, SOC)'를 연결하여 '유럽 사이버 방패(European Cyber Shield)'를 구축함으로써 사이버 위협의 실시간 탐

지 및 정보 공유를 가능하게 한다. 각 SOC는 인공지능(AI)과 데이터 분석 기술을 활용하여 사이버 위협을 탐지하고 회원국과 EU 기관의 사이버보안 태세 강화에 기여하며, 최소 3개 이상의 국가 사이버 허브를 포함하는 국경 간 사이버 허브(Cross-Border Cyber Hubs)로 통합된다. EU 회원국마다 국가 사이버 허브(National Cyber Hub)가 반드시 존재하는 것은 아니다. 국가 사이버 허브의 지정은 의무가 아니라 선택적이며, 국경 간 사이버 허브는 최소 3개 이상 회원국의 국가 허브가 함께 참여하는 컨소시엄 방식으로만 설립 가능하다(「사이버보안법」 제3조).

자금 지원 측면에서 유럽 사이버보안 역량센터(European Cybersecurity Competence Centre, 이하, ECCC)[3]는 회원국의 국가 사이버 허브 설립 및 강화를 위한 도구, 인프라 또는 서비스 공동 조달에 참여할 회원국을 선정하고, 선정된 회원국에 해당 취득 및 운영 비용의 최대 50%를 보조금으로 지원한다. 또한, ECCC는 국경 간 사이버 허브의 도입 및 운영을 위해 호스팅 컨소시엄(hosting consortium)을 선정하여 도구, 인프라 또는 서비스 공동 조달 비용의 최대 75% (취득) 및 50% (운영)를 지원한다(심소연, 2025a, 3).

3) '유럽 사이버보안 역량센터(European Cybersecurity Competence Centre, ECCC)'의 임무는 EU의 사이버보안 연구·산업 역량을 강화해 전략적 자율성을 확보하고, 네트워크·정보시스템 인프라의 복원력과 신뢰성을 지원하며, 사이버보안 산업의 글로벌 경쟁력을 높여 이를 다른 산업의 경쟁우위로 전환하는 것이다. 또한 필요에 따라 유럽사이버보안청과 협력해 임무를 수행한다.

〈표 1〉 유럽 사이버보안 경보 시스템 자금 지원

구분	내용
유럽 사이버보안 역량센터(ECCC)의 공동 조달 참여 회원국 선정 및 보조금 지원	• ECCC는 회원국의 국가 사이버 허브 설립·강화를 위해 도구·인프라 또는 서비스의 공동 조달에 참여할 회원국을 선정하고 선정된 회원국에 해당 도구·인프라 또는 서비스의 취득 비용의 최대 50% 및 운영 비용의 최대 50%를 보조금으로 지원하고 나머지 비용은 선정된 회원국이 부담 • 공동 조달 절차 개시 전에 ECCC와 선정된 회원국은 해당 도구·인프라 또는 서비스의 사용을 규율하는 호스팅 및 사용 계약을 체결해야 함
추가 지원 제한	• 회원국의 국가 사이버 허브는 도구·인프라 또는 서비스를 획득하거나 보조금을 수령한 날 중 빠른 날부터 2년 이내에 국경 간 사이버 허브에 참여하지 않으면 추가적인 지원을 받을 수 없음
ECCC의 호스팅 컨소시엄 선정 및 보조금 지원	• ECCC는 '호스팅 컨소시엄(hosting consortium)'을 선정하여 도구·인프라 또는 서비스의 공동 조달에 참여하게 함. 호스팅 컨소시엄에 해당 도구·인프라 또는 서비스의 취득 비용의 최대 75%, 운영 비용의 최대 50%를 지원하며, 나머지 비용은 호스팅 컨소시엄이 부담 • 공동 조달 절차 개시 전에 ECCC와 호스팅 컨소시엄은 해당 도구·인프라 또는 서비스의 사용을 규율하는 호스팅 및 사용 계약을 체결해야 함
2년 주기 국가·국경 간 사이버 허브 역량·자원 현황 정리	• ECCC는 최소 2년마다 국가 및 국경 간 사이버 허브의 역량과 가용 자원을 정리하여 작성하고, 작성 시 유럽사이버보안청(ENISA), 컴퓨터 보안 사고 대응팀(Computer Security Incident Response Teams, CSIRT) 네트워크, 국경 간 사이버 허브 및 EU집행위원회와 협의해야 함

출처: 심소연. 2025a. "유럽연합(EU)의 사이버 연대 및 보안 입법례" 국회도서관 「최신 외국입법정보」 7호(통권 제270호).

둘째, '사이버보안 비상대응 메커니즘'은 금융, 에너지, 의료 등 중요 공공부문의 조직에 대한 사이버 위협에 대비하여 잠재적 취약점을 상시 평가하고 사고 발생 시 위험을 완화하기 위한 지원 체계이다.

회원국은 요청 시 디지털 유럽 프로그램(Digital Europe Program)[4] 자금으로 지원받을 수 있으며, 유럽 사이버보안 역량센터(ECCC)는 회원국의 조치를 보완하며 국가조정센터 네트워크와 협력하여 운영된다. 지원 조치에는 핵심 분야 (예: 에너지, 금융, 의료, 통신망, 상하수도, 운송, 공공행정 인프라) 기관의 준비 태세 점검, 기타 중요 부문의 준비 조치, 회원국 간 기술적 상호지원이 포함된다(심소연, 2025a, 4).

셋째, 'EU 사이버보안 예비 자원'은 대규모 사이버안보 사고 발생 시 대응, 복구 및 지원을 위해 개별 회원국들이 이용할 수 있는 위탁된 관리형 보안 서비스 업체들로 구성된다. 이 서비스는 회원국 사이버 위기관리 당국, 컴퓨터 보안 사고 대응팀(CSIRT), EU 기관, 기구 및 에이전시를 위한 컴퓨터 비상대응팀(CERT-EU), 그리고 디지털 유럽 프로그램(DEP)에 연계된 제3국의 CSIRT 및 사이버 위기관리 당국이 이용할 수 있다. 'EU 사이버보안 예비 자원' 이용에 관한 전반적인 책임은 EU 집행위원회가 지며, 운영 및 관리는 유럽연합사이버보안청(ENISA)이 전부 또는 일부 위탁받아 수행한다(「사이버 연대법」 제12조).

넷째, '사이버보안 사고 검토 메커니즘'은 유럽연합사이버보안청(ENISA) 주도로 대규모 사이버 사고를 평가하고, 회원국과 EU 기관에 권고하는 체계이다. 이 메커니즘은 사고의 영향을 분석하고 향후 유사 사건에 대비한 개선책을 마련하는 데 기여할 수 있다(「사이버 연대법」 제21조).

이러한 사이버 연대법의 도입은 EU가 사이버 위협에 대한 개별 국

4) 디지털 유럽 프로그램(Digital Europe Programme)은 EU가 디지털 전환을 촉진하고, 고성능 컴퓨팅·인공지능·사이버보안 등 전략 기술 분야에 대한 역량 강화를 위해 마련한 2021~2027년 기간의 주요 투자·지원 정책이다.

가의 대응을 넘어 범유럽 차원의 공동 방어 체계를 구축하고, 특히 지정학적 긴장이 고조되는 상황에서 회원국 간의 실질적인 연대와 지원을 강화하려는 의지를 명확히 보여준다. 또한, 사이버 연대법은 그 적용이 회원국에만 국한되지 않고, EU 기관과 기구로도 확장된다는 점이 주목된다. 이는 유럽의회의 선거 과정을 표적으로 하거나, EU 기밀 문서 등 민감한 정보에 접근하려는 하이브리드 위협이 감지될 경우, EU 사이버보안 예비 자원이 활용될 수 있다는 의미이다.

그러나 사이버 연대법이 보여주는 사이버안보에 대한 초국가적 연대의 개념은 국가 안보 논거에 의해 약화된다. EU 집행위원회가 사이버보안 예비 자원을 활성화할 책임이 있지만, 사이버 연대법에 의해 설립된 도구들은 회원국 국내 사이버보안 시스템을 대체하거나 근본적으로 변형시키도록 설계될 수는 없으며, EU가 긴급 상황에서 활성화할 수 있는 연대 조치는 여전히 회원국의 주권에 구속된다(Villani, Susanna, 2025, 495).

4. NIS2 지침

2016년 7월 6일에 제정된 '네트워크 및 정보시스템(Network and Information Systems, 이하 NIS)' 지침의 목적은 EU 역내 네트워크와 정보시스템의 사이버보안 수준을 전반적으로 강화하며, 중요 인프라의 복원력(Resilience)을 높여 사이버 공격과 사고 시에도 필수서비스가 중단되지 않도록 하고, 회원국 간 사이버보안 역량의 격차를 줄일 뿐만 아니라 각 회원국이 공통된 기준에 따라 사이버 위협을 관리하며, 사고 대응과 정보 공유 시스템을 구축하는 것이다. EU 입법자가 사이버 위협에 대응하기 위해 채택한 여러 법적 수단 중에서도 가장 기본

적인 도구로 꼽히는 이 지침은 회원국뿐만 아니라 일부 경제주체에게도 의무와 역할을 부여한다(Theodoros Karathanasis, 2025, 65~66).

2022년 12월 14일 EU는 기존의 NIS 지침을 NIS2 지침으로 개정했다(Directive (EU) 2022/2555). NIS2 지침의 핵심 방향은 기존에 사이버 공격에 대한 처벌에 초점을 맞추었던 것에서 벗어나 방어적인 보안에 중점을 두는 것으로 전환하는 것이다. 이에 기존의 NIS 지침과 NIS2의 목적은 같으나, NIS2 지침의 경우 그 적용 대상의 범위가 더 확대되고 의무사항이 강화되었다.

EU 법체계상 지침(Directive)은 회원국에 직접 적용되지 않으므로, 각 회원국은 2024년 10월 17일까지 NIS2 지침을 반영한 국내법의 제정 및 개정을 완료하고, 2024년 10월 18일부터 이를 시행해야 한다. 2025년 9월 기준 NIS2 지침을 국내법으로 전환한 회원국은 14개국(완전 이행 완료 7개 회원국: 벨기에, 크로아티아, 헝가리, 이탈리아, 라트비아, 리투아니아, 슬로바키아, 추가 이행 7개 회원국: 덴마크, 에스토니아, 핀란드, 그리스, 몰타, 루마니아, 슬로베니아)으로 파악된다(SECOMEA, 2025).

2025년 5월 7일, EU 집행위원회는 NIS2 지침의 완전한 전환을 하지 못한 19개 회원국에 대해 이유서(reasoned opinion)를 발송했다(European Commission, 2025). 해당 회원국들은 이유서를 받은 지 2개월 내에 필요한 조치를 취해야 하며, 그렇게 하지 않을 시에는 유럽사법재판소(CJEU)에 제소될 수 있다.

NIS 지침 개정으로 인한 주요 변경 사항 및 의무사항은 다음과 같다.

1) 적용 대상의 확대

NIS2 지침은 적용 대상이 기존 NIS 지침에 명시된 7개(에너지, 교통, 의료, 디지털 인프라 등) 분야에서 18개 분야로 확대되어, 제조업, 폐기물 관리, 우주 산업, 공공행정 등이 새롭게 포함되었다(NIS2 지침 제2조~제3조). 특히, 직원 수 50명에서 250명 사이, 매출액 1천만 유로에서 5천만 유로 사이, 또는 연간대차대조표 총액 1천만 유로에서 4천3백만 유로 사이의 중견 기업 이상의 규모이면서, 이 지침의 부속서 I에서 정하는 중요도가 높은 분야 또는 부속서 II에서 정하는 기타 중요 분야에 해당하는 공공 또는 민간 조직에 적용된다. 다만, 국가 안보, 치안, 국방, 법 집행 분야에서 활동하는 공공행정기관은 이 지침의 적용에서 제외된다(심소연, 2024, 8).

2) 주요 의무사항의 강화

NIS2 지침은 기존 NIS 지침의 "필수서비스 운영자(Operator of Essential Services)"와 "디지털 서비스 제공자(Digital Service Provider)"라는 구분을 없애고, 중요도에 따라 필수 기관(Essential Entities)과 중요 기관(Important Entities)으로 나누어 회원국의 감독과 집행 수준을 차등화했다(심소연, 2024, 9).

- 의무 공통 적용: 필수 기관과 중요 기관 모두 사이버 위험 관리 조치, 사고 통지, 정보 공유 등의 의무를 진다. 여기에는 위험분석, 정보시스템 보안 정책, 사고 대응, 공급망 보안, 인적자원 보안, 접근 통제 정책, 자산관리 등이 포함된다(「NIS2 지침」 제21조).
- 사고 통지: 서비스 제공에 중대한 영향을 미치는 사고는 컴퓨터 보안 사고 대응팀(CSIRT)이나 관할 당국에 사고 발생 인지 후 24시간 이내 통지하는 것으로 통지 의무가 강화되었다(제23조).

- 감독 및 집행: 사전 및 사후 감독과 집행 조치에서는 중요 기관보다 필수 기관을 더 엄격하게 다룬다(제32조~제33조).
- 국가 전략 및 기관 지정: 각 회원국은 국가 사이버보안 전략을 수립하고 이를 EU 집행위원회에 보고해야 하며(제5조), NIS2 지침 시행과 사이버보안 사고 대응을 위한 기관도 지정해야 한다(제7조).
- 유럽연합사이버보안청(ENISA)의 역할: ENISA는 DNS(Domain Name System) 서비스, TLD(Top-Level Domain) 네임 등록부, 클라우드 컴퓨팅 서비스, 데이터센터 서비스 제공자 등의 등록부를 만들어 관할 당국이 활용할 수 있게 해야 한다(제27조).
- 최고경영진(C-level)의 개인적 법적 책임 명시: 사이버보안 미준수 시 경영진에게 법적제재가 직접 부과되며, 과징금 수준이 상향되어 최대 연간 매출의 2% 또는 1천만 유로까지 징벌적 과징금 부과가 가능하다(제34조).
- 정기적 보안 교육과 훈련이 필수 법률 요건에 포함되어, 경영진 및 전 직원의 보안 인식과 역량 강화가 강조된다(제20조).

3) 국제협력 강화

NIS2 지침은 국제협력을 강화하는 방안을 포함하고 있다. 회원국은 '유럽 사이버 위기 연락 조직 네트워크(EU-CYCLONe)', 컴퓨터 보안 사고 대응팀(CSIRT) 네트워크, NIS 협력단 간 협업을 통해 사이버안보 위기 대응 기본체계를 구축하고 국제협력을 강화한다(심소연, 2024, 10).

- EU-CYCLONe: 대규모 사이버보안 사고 및 위기관리 지원, 정보교환 촉진을 위해 각 회원국 사이버 위기관리 기관 대표로 구성된다(제14조).
- 컴퓨터 보안 사고 대응팀(Computer Security Incident Response

Teams, CSIRTs): 회원국은 사이버 위협, 취약점, 사고 모니터링, 분석, 조기 경보, 사고 대응 지원 등의 업무를 수행하는 컴퓨터 보안 사고 대응팀(CSIRT)을 1곳 이상 지정하거나 설립해야 한다(제10조).

- CSIRT 네트워크: 회원국 간 기술 및 정책 교류, 사이버 위협, 사고, 취약점 등에 대한 정보 교환 촉진을 위해 각 회원국 CSIRT 대표 및 EU 컴퓨터 비상 대응팀(CERT-EU)으로 구성된다(제15조).

NIS2 지침은 EU가 사이버 위협에 대한 접근 방식을 근본적으로 변화시키고, 전략적이고 예방적인 접근을 통해 EU 전체의 디지털 인프라와 서비스를 보호하려는 노력을 명확히 보여준다. 이는 EU가 사이버보안을 단순히 기술적 문제로 국한하지 않고, 거버넌스, 정책, 국제 협력을 아우르는 포괄적인 접근 방식을 취하고 있음을 의미한다.

〈표 2〉 사이버보안 위기 대응 기본체계

구분	내용
유럽 사이버 위기 연락 조직 네트워크 (EU-CYCLONe)	• 대규모 사이버보안 사고 및 위기관리 지원, 정보 교환 촉진을 위해 각 회원국 사이버 위기관리 기관 대표로 구성
CSIRT 네트워크	• 회원국 간 기술 및 정책 교류, 사이버위협, 사고, 취약점 등에 대한 정보 교환 촉진을 위해 각 회원국 CSIRT 대표 및 EU컴퓨터비상대응팀 (CERT-EU)으로 구성
NIS 협력단	• 회원국은 사이버 위협, 취약점, 사고 모니터링, 분석, 조기 경보, 사고 대응 지원 등의 업무를 수행하는 컴퓨터보안사고대응팀(CSIRT)을 1곳 이상 지정하거나 설립해야 함

출처: 고은아·김홍빈·김진규·윤주연. 2023. "EU의 디지털 미래 구축을 위한 사이버보안(Cybersecurity) 방향과 시사점 - 사이버보안 입법 동향을 중심으로 -,"「INSIGHT Digital & Security Policy」 Vol. 4.

NIS2 지침의 요구사항을 해석하고 이행하는 데에 중소기업이 대기업보다 어려움을 겪는다는 독일에서의 연구 결과가 있다(Joswig, Thomas & Kurz, Walter, 2025). 이는 중소기업의 재정적 제약, 사이버보안 전문성 부족, 의무적 위험 관리 및 보고 의무사항의 복잡성 등에 기인하는 것으로 나타났다. 산업 부분에 따라서도 NIS2 지침의 의무 이행에 있어서 격차가 나타난다. 독일의 경우, IT 부문 기업, 에너지 및 중요 기반시설의 NIS2 지침 이행 수준이 서비스 기반 부문의 기업의 이행 수준보다 상대적으로 높게 나타났다(Joswig, Thomas & Kurz, Walter, 2025).

또한, Niels Vandezande 라는 학자는 NIS2 지침의 네 가지 한계를 지적한다(Vandezande, Niels, 2024). 첫째, NIS2 지침은 정보 공유를 강력하게 권장하지만, 여전히 자발적 성격을 유지하고 있어, 실제로 효과적인 정보 공유가 이루어질지는 불확실하다. 둘째, NIS2 지침은 엄격한 보고 의무와 과도한 행정 부담 사이의 균형을 추구하지만, 유럽의회의 산업연구에너지위원회(ITRE)가 우려했듯이 지나치게 부담스러운 보고 의무는 지키기 어렵고 당국은 무의미한 보고로 업무의 효율성이 저하될 수 있다. 셋째, NIS2 지침은 기관의 경영진에게 사이버보안 교육을 의무화하여 충분한 사이버보안 지식과 기술을 갖추도록 요구하지만, NIS2 지침 적용 대상 기관이 이미 IT 보안 전담 직원이나 부서를 보유하고 있을 가능성이 높다는 점에서 경영진에 대한 사이버보안 교육의 실효성에 의문을 제기한다. 마지막으로, 필수 기관에 대한 표적 감사는 독립 기관 또는 관할 당국이 수행하되, 감사 대상 기관이 그 비용을 부담해야 한다. 이때 지나치게 열성적인 관할 당국에 의해 감사 대상 기관들이 상당한 비용 청구서를 받게 되는 상황이 발생할 수 있다.

NIS2 지침은 EU 사이버보안 정책의 일반법으로 자리 잡으며, 사이

버보안법, 핵심 조직 복원력(CER) 지침, 금융 부문의 사이버보안 강화와 복원력을 위한 '디지털 운영 복원력법(DORA)[5]' 등 사이버안보 관련 기타 법령들과 조화를 이루는 사이버안보 법제 생태계의 중심이라 할 수 있다. 이는 기관들이 여러 사이버안보 관련 법령들을 동시에 준수해야 할 수 있음을 의미하며, 관할 당국 간 긴밀한 협력도 필수적이다.

한편, NIS2 지침은 데이터 센터에 대한 도전과제도 안고 있다. AI 시스템은 방대한 양의 데이터에 크게 의존하며 생성형 AI를 활용한 위협에 점점 더 취약하다. NIS2 지침은 데이터 센터에 대한 보안 요구사항을 강화하지만, 고도로 민감한 AI 관련 데이터 보호를 위한 명시적 지침을 제공하지 않아서 규제의 사각지대를 만든다(Joswig, Thomas & Kurz, Walter, 2025).

5. 핵심 조직 복원력(Critical Entities Resilience, CER) 지침

유럽연합(EU)은 최근 증가하는 사이버 위협과 자연재해, 테러 등의 다양한 위기 상황에 대응하기 위해 포괄적인 법적 거버넌스 체계를 구축하고 있으며, 이러한 노력의 일환으로 「핵심 조직 복원력 지침(Critical Entities Resilience, CER Directive)」을 2022년 12월 14일 제정하였다(Directive (EU) 2022/2557).

5) EU의 디지털 운영 복원력법(Digital Operational Resilience Act, DORA)에 대한 좀 더 자세한 내용은 다음의 발간물을 참고할 수 있다. 심소연. 2025b. "유럽연합의 금융 부문 사이버보안 및 복원력 강화를 위한 「디지털 운영 복원력법(DORA)」." 국회도서관 『최신외국입법정보』 23호(통권 제286호).

이 지침의 핵심 목표는 EU 회원국 전반에 걸쳐 필수적인 서비스를 제공하는 핵심 기반 시설과 조직들이 다양한 위협에 효과적으로 대응하고 신속하게 복구할 수 있는 능력을 갖추도록 하는 것이다. 이는 단순히 사이버 공격뿐만 아니라 자연재해, 테러 공격 등 물리적 위협까지 포함하는 포괄적인 복원력 강화를 지향한다(「핵심 조직 복원력 지침」 제4조).

1) 핵심 조직의 선정 및 의무

이 지침 제2조에 따르면 핵심 조직(critical entites)이란 사회의 필수적 기능이나 경제활동 유지에 필수적인 서비스를 제공하는 조직으로서, 에너지, 교통, 금융, 보건, 식수·식품처리 등 구체적 분야는 제3조에 나열되어 있다. 각 EU 회원국은 2026년 7월 17일까지 자국 내 핵심 조직을 선정하고 그 목록을 EU 집행위원회에 제출해야 한다. 또한 회원국은 선정된 핵심 조직에 이러한 사실과 함께 지침에 따른 의무사항을 통지해야 한다. 핵심 조직으로 지정된 기관들은 다음과 같은 의무를 이행해야 한다(제13조~제14조).

- 지침의 내용을 전달받고 관련 교육에 참여한다.
- 복원력 강화를 위한 지속적인 점검 의무를 이행한다.
- 지침의 활용을 위한 재정 지원 의무를 부담한다.
- 사고 발생 시 관련 당국에 통보해야 한다.

특히, 6개 이상의 회원국에 동일하거나 유사한 필수적인 서비스를 제공하는 조직은 '특별히 중요한 핵심 조직(Critical entities of particular European significance)'으로 지정되어 더욱 엄중한 관리 대상이 된다. 이는 초국가적 중요성을 갖는 서비스의 안정성을 보장하려는 조치이다.

2) 거버넌스 및 국제협력

핵심 조직 복원력 지침은 중요한 핵심 조직들의 원활한 관리를 위해 핵심 조직 복원력(Critical Entities Resilience, CER) 그룹의 설립을 규정한다. 이 그룹은 EU 집행위원회 위원장과 회원국 대표들로 구성되며, 지침 준수 관련 모범 사례를 공유하고 회원국 지원을 위한 국제협력 강화 조치를 포함한다. 이러한 거버넌스 체계는 EU 차원의 일관된 접근 방식을 보장하고, 회원국 간의 정보 공유 및 협력을 촉진하여 전반적인 복원력 수준을 높이는 데 기여한다(제19조).

3) 법적 성격 및 국내 이행

핵심 조직 복원력 지침은 NIS2 지침과 같이, EU 법체계상 '지침(Directive)'에 해당하므로 회원국에 직접 적용되는 것이 아니라 각 회원국이 자국의 국내 입법을 통해 이를 자국 법률로 전환해야 한다. 또한 지침에 명시된 조치를 지키지 않을 경우를 대비하여 각 회원국은 처벌 규정 또한 국내 입법을 통해 마련해야 한다. 이는 EU가 회원국의 법적 자율성을 존중하면서도, 공동의 목표 달성을 위한 최소한의 법적 기본체계를 제시하는 방식이다.

III. 국내 시사점 및 사이버안보 국제협력의 방향성

1. EU 입법례를 통한 국내 사이버안보 체계 강화 방안

EU는 사이버 복원력(Cyber Resilience)과 기술 주권 확보를 목표로 하는 포괄적인 법제 체계를 구축하고, EU 전역에서 통합된 방어 역량을 강화한다. EU의 사이버 보안법, 사이버 복원력법, 사이버 연대법, NIS2 지침 및 핵심 조직 복원력 지침(CER 지침)은 민간과 군사 간 협력을 강조하며, 나토(NATO)와의 협력 등 국제적인 대응 체계까지 포괄하는 구조를 형성함으로써 지엽적인 '사이버보안'의 영역을 넘어 '사이버안보'영역에서의 회원국 간 협력을 강화하고 있다. EU의 사이버안보 분야에서의 이러한 법적 거버넌스는 단일 국가 차원에서도 대한민국의 사이버안보 체계에 여러 시사점을 제공한다.

대한민국은 대통령실 국가안보실을 컨트롤타워로 하여 국가정보원, 과학기술정보통신부, 한국인터넷진흥원, 국방부가 민간 분야, 공공 분야, 국방 분야를 담당하는 민관군 종합 대응 체계를 구축하고 있다. 윤석열 정부의 국가안보전략(2023)은 사이버안보법 제정, 국가사이버안보위원회 설치, 일원화된 대응 체계 구축을 포함한 정책을 내세웠으나 이루어지진 않았다. 이재명 정부는 아직 공식적인 '국가 사이버안보 전략' 문서를 별도로 발표한 바는 없다. 다만, 대선 공약 및 2025년 국정과제 등을 통해 '민·관협력'을 키워드로 하는 사이버보안 로드맵을 제시하면서, 아직 설치되지 않았으나, 대통령 직속 '국가사이버안보위원회'를 중심으로 공공민간 통합 위협 인텔리전스 허브

를 구축하고 AI 기반 보안 관제 시스템을 2027년까지 전 부처에 도입할 계획이다(한국정보기술신문 2025/6/4).

EU가 법제화된 사이버안보 체계를 갖추고 첨단 기술을 활용한 국제 협력과 예방에 주력하는 반면, 대한민국은 2006년 이후 관련 법률 입법 추진 단계에 머물러 있다는 점에서 큰 차이를 보인다. 대한민국에서는 「국가정보원법」, 「전자정부법」, 「정보통신기반 보호법」 및 「정보통신망법」 등 사이버보안 관련 법률이 존재하지만, 국가 사이버안보 전체를 조망하는 기본법 차원의 법률 제정은 아직 이루어지지 않았다. 제21대 국회에서 「사이버안보 기본법안」, 「국가사이버안보법안」, 「사이버보안 기본법안」 등 총 3개의 법안이 발의되었으나, 민간에 대한 감시 권한 확대 우려, 국가정보원 권한 강화에 대한 비판, 과기정통부가 컨트롤 타워로서 적절한지에 대한 선행 논의의 필요성, IT산업 성장 저해 우려 등이 제기되어 제정으로까지 이어지지 못했다[6]. 제22대 국회에는 2개의 법안(국민의 힘 김상훈 의원 등 20인이 발의한 사이버안보 기본법안 및 국민의 힘 유용원 의원 등 10인이 발의한 국가사이버안보법안)이 소관위원회인 정보위원회에 계류 중이다.

이러한 상황에서 EU의 입법례는 대한민국 사이버안보 체계 강화에 다음과 같은 시사점과 개선 과제를 제시한다.

첫째, 포괄적인 기본법 제정을 통한 거버넌스 명확화가 필요하다. EU의 사이버보안법, NIS2 지침과 같이 국가 전체의 사이버안보를 조망하고 민간과 공공부문의 역할을 명확히 하는 기본법 제정이 시급

6) 제21대 국회에서 발의된 3개의 법안과 국가정보원이 제안한 법안에 대한 비교 분석은 다음의 논문을 참고할 수 있다. 유인수 외. (2023). "국내 사이버안보법 입법 현황과 제언사항." 『명지법학』제21권 제2호, 107-131.

하다. 대한민국이 관련 법률 입법 추진 단계에 머물러 있는 것은 사이버 위협에 대한 일관되고 체계적인 대응을 저해할 수 있다. 따라서 국가사이버안보위원회(가칭)를 설치하고 일원화된 대응 체계를 구축하려는 노력은 법제화를 통해 제도적 기반을 마련해야 한다[7].

둘째, 민관 협력 체계를 강화하고 역할 분담을 명확히 해야 한다. 대한민국은 정보통신기술(ICT) 인프라 강국임에도 불구하고 각 부처가 경쟁적이고 산발적으로 법제 및 정책을 추진하여 민관 협력 체계가 취약하다는 평가를 받는다. EU의 유럽연합사이버보안청(ENISA)은 회원국과 민간 부문, 학계 등 다양한 이해관계자 간 협력을 통해 사이버 위협에 대응하는 중앙 조정기관 역할을 한다. 특히 정보 공유, 위협 분석, 대응 체계 구축에서 민관 파트너십을 강화하는 프로세스는 대한민국의 사이버안보 협력 구조 구축에 매우 유용하다. 미국 역시 바이든 행정부의 2023년 국가 사이버안보 전략에서 민간 부문과의 사이버안보 협력을 6대 핵심 범주 중 하나로 포함시켰다. 대한민국도 정보 공유 분석 센터(ISAC)나 민관 합동 훈련을 확대하고, 민간 부문의 전문성과 자원을 사이버안보 대응에 필수적으로 통합하는 거버넌스 모델을 구축할 필요가 있다.

셋째, 사이버보안 인증 및 관리 체계의 효율성을 제고해야 한다. EU는 ICT 제품, 서비스, 프로세스 및 관리형 보안 서비스(MSS)에 대한 사이버보안 인증 체계를 구축하고, 개인정보보호 인증과는 별도로 관리한다. 이는 대한민국이 「개인정보보호법」 제32조의2에 근거

7) 새로운 사이버안보 전담 기관을 국무총리 직속 기관으로 신설 시, 정보공유 측면에서 부처 간 협력에 용이하며, 사이버안보 업무 폭증으로 인한 국가정보원 업무의 불균형도 예방할 수 있고, 대한민국의 국가정보체계를 개편하는 계기가 될 수 있다는 의견이 있다(유인수 외. 2023).

한 정보보호 및 개인정보보호 관리 체계 인증(ISMS-P)을 획득하면 「정보통신망법」 제47조에 따른 정보보호 관리 체계 인증(ISMS)을 포함하는 것으로 간주하는 것과 대조적이다. EU의 접근 방식은 사이버 보안 역량과 서비스 품질에 초점을 맞추어 인증의 전문성과 신뢰성을 높이는 데 기여한다. 대한민국 역시 EU의 사례를 참고하여 국내 인증제도의 효율성과 전문성을 제고할 방안을 검토할 필요가 있다.

넷째, 사이버 복원력 중심의 패러다임 전환을 가속화해야 한다. EU는 NIS2 지침과 사이버 복원력법을 통해 사이버 공격에 대한 사후 처벌에서 벗어나 사전에 방어하는 보안과 사이버 복원력 강화에 중점을 두는 것으로 방향을 전환했다. 이는 국가 중요 인프라 시설의 디지털화가 가속화되고 사이버 위협이 국가 전체에 심각한 영향을 미칠 수 있게 된 현실을 반영하는 것이다. 최근 대한민국 SK텔레콤의 가입자 정보 해킹 사고와 같은 대규모 정보통신기술(IT) 중단 사태는 사이버안보와 사이버보안의 경계가 희미해지고 있음을 보여주는 것이며, 대규모 사고 발생 시 신속한 복구 역량의 중요성을 부각시켰다. 따라서 대한민국도 사이버 공격을 예방하고 효과적으로 대응하며 피해 발생 시 신속히 복구함으로써 정보의 기밀성·무결성·가용성을 보장하는 복원력 중심의 전략적 접근을 강화해야 한다. 또한 이를 가능하게 하는 법적·정책적 기반을 마련할 필요가 있을 것이다.

2. 동아시아 지역 사이버안보 협력의 한계 및 국제협력 방향

동아시아 지역은 사이버 공격의 주요 대상 지역인 동시에 고도의 사이버 역량을 보유한 국가들의 존재에도 불구하고, 사이버안보에 관한 실질적인 협력은 매우 어려운 상황이다.

예를 들어, 대만은 2024년에만 하루 평균 240만 건의 사이버 공격을 받았으며, 에너지, 통신, 반도체 제조, 금융 서비스, 항공 및 해상 물류 등 핵심 인프라가 매우 취약하다. 이러한 시스템의 마비는 대만 내 혼란을 일으킬 뿐만 아니라 전 세계 시장, 특히 기술 부문에 충격을 줄 수 있다. 중국의 사이버 접근 방식은 대만의 국가적 기능과 사회를 약화시키고 대만을 디지털적으로 고립시키며, 사회적 신뢰를 파괴하고 경제를 마비시키는 것을 목표로 한다. 이러한 상황은 동아시아 전반에 걸쳐 사이버 위협이 단순히 개별 국가의 문제를 넘어 지역 전체의 안정과 글로벌 공급망에 영향을 미치는 초국가적 위협임을 보여준다(HSU, Jason & Saunders, Joseph, 2025, 1).

미·중 전략 경쟁은 아시아 국가들이 자체 사이버안보 역량을 강화하도록 자극하지만, 동시에 전략적 불신을 심화시켜 정보 공유와 공동 대응을 제한한다. 또한 사이버공간의 진영화 현상(자유민주주의 진영 vs. 반자유주의·권위주의 진영)을 심화시켜 아시아 국가들이 특정 진영에 편입될 압박을 받게 되며 이는 다자간 협력 환경을 약화시킨다(홍건식, 2023, 3~4).

더욱이 2024년 러시아와 북한 간 체결한 러북 신조약은 러북간 기존 동맹관계가 사이버공간으로까지 확대된다는 점을 분명히 함으로써, 지역 안보 경쟁 구도를 더욱 심화시키고, 대한민국을 포함한 동맹국들에 대한 사이버 공격 가능성을 높인다(김소정, 2024, 4).

사이버 위협은 본질적으로 초국가적 형태로 진행되므로 단일 국가의 대응으로는 한계가 있어 국제협력 및 협력 거버넌스 구축이 필수적이다. 이와 관련하여 EU의 사이버보안 및 연대 관련 입법례를 통해 동아시아 지역에 대한 시사점을 도출하고, 사이버안보 국제협력에 있어 대한민국의 주도적 역할을 위한 방안을 다음과 같이 제시하

고자 한다.

첫째, 국제협력 이전에 국내 협력을 위한 사이버안보 거버넌스가 마련되어 정권이 바뀌는 것과 관계없이 사이버안보 영역만큼은 일관성 있는 정책과 대응이 이루어질 필요가 있다. 단일 국가로서는 영국의 사이버안보 거버넌스 체계가 가장 잘 되어 있다고 평가받고 있으므로 이를 벤치마킹할 필요가 있다.

둘째, EU의 사이버보안 협력 거버넌스를 참고하여 지정학적 리스크를 고려한 사이버보안 국제협력 체계를 마련할 필요가 있다. EU는 사이버 연대법을 통해 '유럽 사이버 방패'를 구축하여 EU 회원국 및 국경 간 보안 운영 센터(SOC)를 연결하고 사이버 위협의 실시간 탐지 및 정보 공유를 가능하게 한다. 또한 '사이버보안 비상대응 메커니즘'과 'EU 사이버보안 예비 자원'을 통해 대규모 사이버 사고 발생 시 회원국 간 지원 체계를 마련하고, 유럽연합사이버보안청(ENISA) 주도로 사고를 평가하고 권고하는 '사이버보안 사고 검토 메커니즘'을 운영한다. 비록 동아시아 지역에 EU와 같은 구속력 있는 법체계를 갖춘 초국가기구는 존재하지 않지만, 이러한 EU의 포괄적인 협력 모델은 동아시아 지역에서 적어도 사이버보안 영역에서의 협력 거버넌스 구축에 중요한 참고가 될 수 있다.

실제로, '아세안 사이버보안 협력 전략 2021-2025'는 역내 협력을 위한 주요 지침 문서로, 사이버 준비 태세 협력 증진, 역내 사이버 정책 조정 강화, 사이버공간 신뢰 증진, 역내 역량 강화 및 국제협력 증진을 목표로 한다(ASEAN Cybersecurity Cooperation Strategy 2021-2025, 2). 아세안은 2024년 10월부터 싱가포르에 본부를 둔 지역 컴퓨터 비상 대응팀(Computer Emergency Response Team, CERT)을 운영하며, 말레이시아가 첫 조정 역할을 맡았다. CERT는 회원국 간 실시간 사이

버 위협 정보를 공유하고 민관 협력을 확대하는 것이 목적이다. 기술 및 역량 강화 측면에서 아세안은 인터폴(INTERPOL)의 글로벌 경찰 통신망과 아세안폴(ASEANAPOL) 데이터베이스로 데이터 공유를 촉진한다. 또한, 2016년 싱가포르에서 시작된 사이버 역량 프로그램은 정책 담당자, 외교관, 기술 인력 등에 사이버 사고 대응·정책 수립 등 다양한 교육을 제공하고 있다.

셋째, 대한민국은 ICT 강국으로서 '브릿지(bridge) 국가'로서의 역할을 하며 사이버보안 국제협력을 주도할 수 있을 것이다. 사이버보안 후발국에 대한 지원을 위해 사이버 공적개발원조(ODA)를 시행하고 이를 통해 국제협력을 확대하며 사이버보안 국제규범화 및 국제 사이버공간 리더십 확보에 기여할 수 있다. 특히, 중국발 사이버 공격이 동남아시아 국가들을 우회해서 들어오는 현상을 고려할 때, 사이버안보 목적의 ODA 사업을 활성화하여 전략적 이익 달성과 사이버안보의 국제적 기여를 동시에 이루는 것을 기대해 볼 수 있을 것이다.

넷째, 사이버 범죄 및 랜섬웨어 대응을 협력의 점화제로 삼아 실질적인 사이버보안 및 안보 협력을 강화할 필요가 있다. 대규모 사이버 공격 발생 시 대응, 복구 및 지원을 위해 관리형 보안 서비스 업체들로 구성된 'EU 사이버보안 예비 자원'과 같은 모델을 참고할 수 있다. 이를 위해 대한민국은 동맹국을 포함한 사이버안보 강국들과 공동 훈련 및 공격 시뮬레이션과 같은 시범 사업을 통해 신뢰와 공동 대응 능력을 강화해야 한다. 실제로 대한민국은 2022년 5월 아시아 국가 최초로 나토(NATO) 사이버방위센터(CCDCOE) 정회원으로 가입하여 국제협력 역량을 강화한 경험이 있다. 또한, 2024년부터 대한민국 주도로 NATO, 일본, 싱가포르 등 인도·태평양 20~24개국의 사이버안보 전문가들이 참여하는 국제협력형 훈련 APEX(Allied Power EXercise)

를 개최하였다. 올해도 국가정보원 주관으로 2025년 9월 8일부터 11일까지 이어진 Cyber Summit Korea 2025 행사 기간 동안 APEX가 진행된 바 있다. 이러한 경험을 바탕으로, 대한민국 정부는 사이버안보 강국들과 정보 공유 및 공동 대응을 위한 공식 협력 체계를 공고히 하고, UN 정부전문가그룹(GGE) 등 다자간 국제규범 협의체에서 리더십을 더욱 강화할 필요가 있다.

사이버안보 국제협력은 참여자 간 신뢰가 핵심이다. 따라서, APEX 같은 사이버안보 협력 훈련에 중국이나 북한을 참여시킨다면, 미국을 비롯한 사이버안보 강국들은 참여를 꺼리게 될 수 있다. 일례로 미국 오바마 정권은 2015년 중국 시진핑 주석이 미국을 방문했을 때, 지적재산권 분야만이라도 사이버 공격으로 취득한 정보를 산업에 활용하지 않도록 하는 사이버안보 협정을 체결하였으나 여전히 중국 국가기관이 사이버공간에서 불법적으로 취득한 미국의 정보들을 중국 산업에 활용하고 있다(김년수 외, 2024, 218; Remarks by Vice President Mike Pence(2019.10.24.)).

다섯째, EU의 사례를 벤치마킹하여 자유민주주의 진영의 사이버안보 협력국 간 사이버보안 통합을 위한 경제적·정치적 인센티브 제도를 도입할 수 있다. 예를 들어 공통 사이버보안 인증 기준을 마련하고 협력국 간 CERT 및 관련 인증서에 대한 상호인정협정을 활성화하여 인증 비용 절감과 시장 접근성을 향상할 수 있다. 또한 공동 조달 시장을 형성하고 인증된 사이버보안 제품·서비스에 대해 우대 조달 정책 및 협력 프로그램을 운영하여 시장 규모 확대와 경제적 효율성을 확보하며 중소기업의 참여를 유도할 필요가 있다. 공동 연구개발(R&D) 및 투자 촉진을 위해 사이버보안 강화 투자에 대한 세금 감면, 보조금, 금융 지원 등을 정책적으로 제공하는 것도 중요하다.

여섯째, AI, 5G/6G, 양자암호 등 신흥 기술(emerging technologies) 기반의 협력을 강화해야 한다. AI, 5G/6G, 양자암호와 같은 신흥 기술은 역내 협력 의제와 우선순위에서 핵심 요소로 빠르게 반영될 전망이며, 기술 개발, 표준화, 보안, 인력 양성, 공급망 안정성 확보 등 여러 방면에서 협력을 확대해야 한다. 특히 AI 기반 보안 시스템 구축 및 양자암호통신 기술 개발은 사이버안보 역량 강화에 필수적이다. 대한민국 정부, 민간, 군 및 학계는 이러한 신흥 기술 분야의 공동 연구 및 인력 양성 프로그램을 확대하고 국제 표준 개발 주도권 확보를 위한 협력 플랫폼을 구축하여 사이버안보 협력 강화에 기여할 필요가 있다.

IV. 맺음말

EU는 법제화된 사이버안보 체계를 갖추고 첨단 기술을 활용한 국제 협력과 예방에 주력하는 반면, 대한민국은 관련 입법 추진 단계에 머물러 있으며, 북한의 사이버 공격에 대한 대응에 상대적으로 집중된 전략을 취하고 있음을 알 수 있다. 또한, EU는 민간과 군사 간 협력을 강화해 사이버 방어를 다층적으로 구축하는 데 반해, 대한민국은 사이버안보 실무 차원에서는 국가정보원이 중심이 되어 공공·민간 분야를 종합 관리하는 체계를 갖추고 있다. 이러한 차이는 각국의 사이버 위협 환경과 지정학적 특수성에 따른 차별화된 전략에서 기인한다고도 볼 수 있을 것이다.

사이버 위협은 동아시아 지역뿐만 아니라 전 세계적으로 점점 더 복잡하고 초국가적인 양상을 띠고 있으며, 이는 개별 국가의 대응만

으로는 한계가 있음을 시사한다. 미·중 전략 경쟁 국면에서 기술 주권의 확보 측면에서도 EU는 추가적인 사이버안보 법제화 논의를 지속해 갈 것이다.

대한민국도 사이버안보 기본체계를 강화하는 법적 틀을 조속히 마련하고, 대한민국의 ICT 역량과 그간의 국제협력 경험을 바탕으로 동아시아라는 지역에 국한하지 않고, 지역을 넘어 자유민주주의 진영 협력국들과의 신뢰 구축과 공동 대응 역량 강화를 통해 안정적이고 견고한 사이버안보 국제협력 환경을 구축하는 데 중추적인 역할을 해야 할 것이다.

〈참고문헌〉

강진규. 2025. "'사이버안보기본법' 끝날 때까지 끝난 것이 아니다?...국정원 올해 하반기 재추진." 『Digital Today』 (1월 29일).

강진규. 2024. "'국가사이버안보기본법' 재추진...직속 연구기관도 설립." 『Digital Today』 (3월 6일).

고은아·김홍빈·김진규·윤주연. 2023. "EU의 디지털 미래 구축을 위한 사이버보안(Cybersecurity) 방향과 시사점 – 사이버보안 입법 동향을 중심으로 –." 『KISA INSIGHT Digital & Security Policy』 Vol. 4.

김년수·김세일·김종욱·류재수·백운호·신경수·신진·이은수. 2024. 『공공외교와 사이버 미래전』대전: 충남대학교출판문화원.

김성훈·김정덕. 2024. "침해사고 등 사이버 공격 대응 관점에서의 사이버 복원력(Cyber Resilience) 정책 이슈 분석 및 시사점." 한국인터넷진흥원. 『KISA INSIGHT』 Vol. 5.

김소정. 2024. "한미 대북 사이버안보 협력의 현황과 과제." 국가안보전략연구원(INSS) 『INSS 전략보고』 December. No. 310.

문가용. 2023. "초대형 공급망 공격? 클롭 랜섬웨어, 무브잇 통해 일 저질러." 『보안뉴스』 (6월 18일).

심소연. 2025a. "유럽연합(EU)의 사이버 연대 및 보안 입법례." 국회도서관 『최신외국입법정보」』 7호(통권 제270호).

심소연. 2025b. "유럽연합의 금융 부문 사이버보안 및 복원력 강화를 위한 「디지털 운영 복원력법(DORA)」." 국회도서관 『최신외국입법정보」』 23호(통권 제286호).

심소연. 2024. "유럽연합(EU)의 사이버안보 법제 동향 - NIS 지침을 개정한 NIS2 지침을 중심으로 –." 한국법제연구원 『최신외국법제정보』 현안발굴형 외국법제 제8호.

심승배. 2024. "[심승배의 국방&디지털⑧] AI는 사이버전의 창과 방패." 『ZDNET KOREA』 (10월 6일).

유인수 외. 2023. "국내 사이버안보법 입법 현황과 제언사항." 『명지법학』 제21권 제2

호, 107-131.

이소미. 2023. "사이버 보안 중심의 EU 디지털 정책, 우리에게 시사하는 바는?" 『보안뉴스』 (9월 25일).

이준삼. 2024. "전세계 IT 대란에 발칵…공항 멈추고 통신·방송·금융 차질" 『연합뉴스』 (7월 19일).

조남준. 2025. "SKT해킹, 재난급 사고인데 경보도 없었다" 『에너지데일리』 (5월 7일).

차동언 외. 2024. "해외규제 리포트 – 유럽 연합(EU), 사이버 보안 인증 제도(EUCC) 도입." 『법률신문』 (4월 22일).

채재병·김일기. 2020. "주요국 사이버안보 전략과 한국에의 시사점." 『INSS 전략보고』 No. 73.

한국정보기술신문(2025.6.4.) "이재명 정부가 내건 '디지털 대전환' 로드맵은 무엇인가"

홍건식. 2023. "사이버 공간의 진영화와 영향 공작." 국가안보전략연구원(INSS) 『이슈브리프』 501호(12월 29일).

ASEAN Cybersecurity Cooperation Strategy 2021-2025. 2023. https://cil.nus.edu.sg/wp-content/uploads/2023/08/2021-2025-ASEAN-Cybersercurity-Cooperation-Strategy.pdf (검색일: 2025.10.1.).

Burri, Mira & Zihlmann, Zaira. 2023. "The EU Cyber Resilience Act - An appraisal and contextualization." *Zeitschrift für Europarecht.* doi: 10.36862/eiz-euz015 (검색일: 2025.10.1.).

Carrapico, Helena & Farrand, Benjamin. 2024. "Cybersecurity Trends in the European Union: Regulatory Mercantilism and the Digitalisation of Geopolitics." *Journal of Common Market Studies.* Annual Review, 1-12.

HSU, Jason & Saunders, Joseph. 2025. "Resilience is deterrence: Why Taiwan's Cyber Weakness is a strategic risk." (August) Hudson Institute.

Joswig, Thomas & Kurz, Walter. 2025. "Empirical Analysis of NIS2 Adoption in EU SMEs: Challenges for Critical Infrastructure in Germany."

Journal of Next-Generation Research 5.0, 1(3). https://doi.org/10.70792/jngr5.0.v1i3.99 (검색일: 2025. 12. 8.).

Karathanasis, Theodoros. 2024. Cybersecurity and EU Law. Adopting the network and information security directive. London: Routledge.

Oleksiewicz, Izabela & Civelek, Mustafa Emre. 2023. "Where are the changes in eu cybersecurity legislation leading?." *Research Journal of Humanities and Social Sciences* 30, No. 4 (October-December), 183-197. doi: 10.7862/rz.2023.hss.50 (검색일: 2025.10.1.).

Pence, Mike. 2019. "Remarks by Vice President Pence at the Frederic V. Malek Moemorial Lecture,"Conrad Hotel, Washington, D.C. 2019.10.24., https://trumpwhitehouse.archives.gov/briefings-statements/remarks-vice-president-pence-frederic-v-malek-memorial-lecture/ (검색일: 2025.10.1.).

Chiara, Pier Giorgio. 2024. "Towards a right to cybersecurity in EU law? The challenges ahead." *Computer Law & Security Review*, Vol. 53. https://doi.org/10.1016/j.clsr.2024.105961 (검색일: 2025. 12. 8.).

Van Puyvelde, Damien & F. Brantly, Aaron(이상현, 신소현, 심상민 옮김). 2023.『사이버안보. 사이버공간에서의 정치, 거버넌스, 분쟁』서울: 명인문화사.

Vandezande, Niels. 2024. "Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor." *Computer Law & Security Review*, Vol. 52. https://doi.org/10.1016/j.clsr.2023.105890 (검색일: 2025. 12.8.).

Villani, Susanna. 2025. "The Cyber Solidarity Act: Framework and Perspectives for the New EU-Wide Cybersecurity Solidarity Mechanism Under the EU Legal System." *European Journal of Risk Regulation*. 16(2), 485-497. doi:10.1017/err.2025.24 (검색일: 2025. 12.8.).

제394회 국회(임시회) 제1차 과학기술정보방송통신위원회 사이버보안 기본법안 검토

보고 – 윤영찬 의원 대표발의(의안번호 제2113670호), 2022년 3월.

제382회 국회(정기회) 제2차 정보위원회 사이버안보기본법안 검토보고 – 조태용 의원 대표발의(의안번호 제2101220호), 2020년 9월.

CERT-EU. 2024. "'Russia's War on Ukraine: One Year of Cyber Operations – 24 February 2022 – 24 February 2023." https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf (검색일: 2025.10.1.).

European Commission·High Representative of the Union for Foreign Affairs and Security Policy. 2022. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL EU Policy on Cyber Defence (JOIN/2022/49 final) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022JC0049 (검색일: 2025.10.1.).

European Commission·High Representative of the Union for Foreign Affairs and Security Policy. 2020. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade (JOIN/2020/18 final). https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (검색일: 2025.10.1.).

Regulation (EU) 2025/37 of the European Parliament and of the Council of 19 December 2024 amending Regulation (EU) 2019/881 as regards managed security services, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202500037 (검색일: 2025.10.1.).

Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202500038 (검색일: 2025.10.1.).

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 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), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02024R2847-20241120 (검색일: 2025.10.1.).

Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0887 (검색일: 2025.10.1.).

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881 (검색일: 2025.10.1.).

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), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504 (검색일: 2025.10.1.).

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557 (검색일: 2025.10.1.).

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), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02022L2555-20221227 (검색일: 2025.10.1.).

The Domestic Implications and International Cooperation Directions of the EU's Legal Governance on Cybersecurity

Soyeon Shim | National Assembly Library, EU Law Research Officer

The rise of generative AI systems and the accelerating digitalization of critical national infrastructures have led to an escalation of cyber threats and attacks, posing profound risks not only to individuals and societies but also to national security as a whole. The European Union (EU) has responded to these transnational risks by establishing a multi-layered and comprehensive legal governance framework, including the Cybersecurity Act, the Cyber Resilience Act, the Cyber Solidarity Act, the NIS2 Directive, and the Critical Entities Resilience Directive. This study provides an integrated analysis of how these EU cybersecurity instruments construct and operationalize legal governance, drawing implications for South Korea's cybersecurity framework and future directions for international cooperation.

In contrast to the EU's established and preventive governance system, South Korea remains at the legislative formation stage, facing challenges in implementing a coherent cybersecurity approach. The EU's legislative model offers valuable insights for South Korea, including the need to clarify governance through an overarching National Cybersecurity Basic Act, strengthen public-private cooperation via a central coordinating body similar to the European Union Agency for Cybersecurity (ENISA), enhance the professionalism of certification and management systems, and accelerate the shift from post-incident punitive measures toward a resilience-oriented cybersecurity paradigm.

In East Asia, intensifying U.S.-China strategic competition and increasing geopolitical tensions—exemplified by the new Russia-North Korea treaty—have made the bloc-based alignment of cybersecurity cooperation inevitable. South Korea should benchmark the EU's comprehensive joint defense and support framework embodied in the Cyber Solidarity Act's "European Cyber Shield" to activate ICT-based cybersecurity Official Development Assistance (ODA), promote joint exercises with democratic cybersecurity partners, and introduce economic incentives. By doing so, South Korea can reinforce its international leadership and foster a stable cooperative environment in global cybersecurity governance.

Keyword European Union, Cyber Security, Cyber Solidarity Act, Cyber Resilience Act, International Cooperation