글로벌정책리포트

외교안보정책실
이윤식 수석연구위원

(엔비디아 사태로 본)
마중 AI 패권경쟁의 쟁점과 과제

2026년 11월 19일

여의도연구원
THE YEOUIDO INSTITUTE

(엔비디아 사태로 본) 미·중 AI 패권경쟁의 쟁점과 과제

- 수출통제의 실효성, 기업의 안보책임, 기술방첩의 중요성 중심 -

2026. 11. 19. (목) 외교안보정책실장 이 윤 식

□ **엔비디아 사태는 전략기업의 핵심 인물과 거래망에 대한 접근이 첨단 AI 역량 확보와 국가 의사결정에 대한 영향력 행사로 이어질 수 있다는 국가안보 문제를 제기**

○ 수출통제·기업 책임·기술방첩은 이번 사태를 통해 미·중 AI 패권경쟁의 실상을 살펴볼 핵심 쟁점으로, 통제 우회와 경영진 감독, 정보공작에 대한 차단능력이 핵심

□ **한국도 반도체 공정정보와 정보요원 신원 유출의 문제를 겪고 있으며, 경쟁국이 확보한 기술과 훼손된 정보망은 사후 처벌만으로 회복하기 어려움**

○ 그러나 민주당이 추진한 국정원 대공수사권 이관과 이재명 정부의 수사·기소 분리로, 정보 탐지부터 증거 확보·기소까지 연결해야 할 부담이 커진 상황

○ 정부는 공조체계의 존재를 넘어 실제 차단 및 검거능력을 입증해야 하며, 관대한 선고와 외국 개입 입증의 한계도 해소할 필수적 과제

□ **향후 핵심 인물의 조기 신고·보호와 경영진 관련 거래의 독립 심사를 추진하고, 정부의 해외정보를 기업의 거래 점검과 연결할 필요**

○ 아울러 국정원 대공수사 기능과 기술안보 전문수사 및 직접 보완수사 역량 회복을 위한 정상화 입법, 고의적 해외 유출의 가중처벌 및 범죄수익 환수 등을 추진

○ 정부에 30일 이내 위험·대응 공백·조치계획 보고를 요구하고, 경고 묵살과 대응 지연의 책임을 규명해 기술·기밀 유출 이전에 개입하는 국가 역량을 확보

I. 서론: 엔비디아 사태의 확산과 기술안보 문제의 부상

○ 젠슨 황의 사생활과 중국 정보기관 연계를 둘러싼 엔비디아 사태가 첨단 AI 역량 확보와 미국의 통제·감독 책임을 묻는 국가안보 문제로 확대

- 뉴욕타임스(NYT)는 11월 6일 미 정보당국자를 인용해, 앨리스 황이 '중국 국가안전부에 포섭됐다'고 보도. 그가 경영에 관여했던 싱가포르 데이터센터 기업 메가스피드의 반도체 거래도 조사 대상으로 부상
- 핵심은 최고경영진에 대한 접근이 기술·거래정보 수집과 첨단 칩 확보, 나아가 미국의 對中 수출정책에 대한 영향력 행사로 이어졌는지에 관한 것

○ 엔비디아는 11월 12일 젠슨 황의 CEO·사장·이사직 사임과 콜레트 크레스 최고재무책임자의 임시 CEO 선임을 발표했으나, 기업의 내부통제가 적절히 작동했는지와 정부의 대응 책임을 둘러싼 논란은 지속

- 미 하원 정보위·외교위·중국특위는 젠슨 황의 12월 1일, 엔비디아 법무총괄 팀 테터의 12월 2일 비공개 면담 일정을 확정하며, 개인의 행위와 기업의 안보·거래 관리에 대한 검증을 본격화
- 미국은 제3국 데이터센터를 통한 첨단 AI 연산능력의 원격 이용을 겨냥한 통제 규칙도 공개하며, 반도체의 물리적 이동을 넘어 실제 이용 경로까지 통제를 확대

○ 이번 사태는 미·중 AI 패권경쟁의 여러 쟁점 가운데 ①수출통제의 실효성, ②전략기업의 국가안보 책임, ③핵심 인물에 대한 기술방첩의 중요성을 드러낸 사례

- △수출통제의 우회는 중국의 AI 역량 확보로, △기업의 관리·감독 실패는 전략기술 보호의 허점으로, △핵심 인물에 대한 포섭은 정보 유출과 정책 영향력 행사의 통로로 이어질 수 있음
- 기업의 사업 이해와 정부의 외교·통상 판단이 안보상 경고보다 앞설 경우, 위험을 파악하고도 차단하지 못한다는 점에서 대응의 실효성과 의사결정 책임이 중요

○ 한국 역시 반도체·AI·방산 등 전략산업을 보유한 만큼, 핵심 인력과 거래망에 대한 외국 정보기관의 접근을 기업만의 보안 문제로 돌릴 수 없는 상황

- 기술과 기밀의 유출은 군사·정보 역량과 산업 경쟁력을 함께 훼손하며, 사후 처벌만으로 이미 넘겨진 정보와 기술적 우위를 되돌리기 어려움
- 이에 본 보고서는 세 쟁점을 토대로 한국의 대응체계를 평가하고, 정보·수사 권한 재편 이후의 공백과 정부 책임을 검토해 당이 추진할 보호·차단 과제를 제시

II. 엔비디아 사태에서 드러난 미·중 AI 패권경쟁의 세 쟁점

① 수출통제: 우회 조달과 첨단 연산능력 접근의 차단

○ 메가스피드 관련 의혹은 미국이 지키려는 첨단 AI 역량의 우위가 제3국 거래망을 통해 잠식될 수 있다는 문제를 제기

- 핵심은 해외 데이터센터용으로 공급된 첨단 칩이 신고된 목적대로 사용됐는지, 중개 거래망을 거쳐 중국으로 이전됐는지에 있음
- 싱가포르 당국도 서버가 자국을 거쳐서 말레이시아로 수출된 뒤 신고했던 곳과 다른 목적지로 이동했는지 조사했다고 발표해, 서류상 목적지와 실제 사용처 사이의 간극을 드러냄[1)]

○ 나아가, 통제의 사각지대는 반도체 밀반출뿐 아니라 중국 기업이 제3국 데이터센터의 첨단 연산능력을 원격으로 이용하는 경로에도 존재

- 칩이 허용된 국가에 남아 있더라도 중국 기업이 이를 첨단 AI 개발에 활용한다면, 중국의 첨단 AI 역량 확보를 제한하려는 통제 목적은 훼손
- 미국의 새 원격접속 통제 규칙은 이러한 우회를 겨냥한 조치로, 미·중 경쟁의 통제 대상이 칩의 이동에서 첨단 연산능력에 대한 접근으로 확대되고 있음을 의미[2)]
- 엔비디아도 11월 17일 실적설명회에서 허가받은 호퍼 계열 데이터센터 제품의 대중국 출하 중단을 밝혀, 대중 사업의 조정이 실제 공급 단계로 이어지는 상황

○ 이처럼 물리적 이동과 원격 이용을 함께 통제해야 하는 만큼, 수출통제의 실효성은 최종 이용자를 확인할 집행능력과 위험 거래를 차단할 정부의 판단에 달려 있음

- 조지타운대 안보·신흥기술센터(CSET)는 칩의 위치 확인만으로 실제 이용자를 식별할 수 없으며, 탐지된 단서를 추적할 인력과 자원이 부족하면 통제 효과도 제한된다고 분석[3)]
- 미 상원의원들의 수출정책 문서와 트럼프-젠슨 황 접촉 기록 보존 요구도 이러한 판단을 검증하려는 조치로, 안보상 경고가 외교·통상 또는 기업의 이해 때문에 후순위로 밀렸는지가 책임 규명의 핵심[4)]

② 전략기업의 책임: 사업적 이해와 국가안보 책임의 충돌

○ 엔비디아는 미국의 AI 우위를 뒷받침하는 전략기업으로, 고객 심사와 경영진 감독의 실패가 국가의 기술통제까지 약화시킬 수 있는 위치

- 고객사 경영에 관여했던 앨리스 황과 젠슨 황의 사적 관계는 거래 심사와 위험 보고가 최고경영자로부터 독립적으로 이루어졌는지 검증해야 할 사유
- 중국 시장을 유지하려는 사업적 이해가 의심 거래의 묵인으로 이어지지 않도록, 이사회와 법무·준법 조직이 최고경영자의 의사에 반해서도 추가 확인과 거래 보류를 요구할 수 있었는지가 중요

○ 이러한 문제에 대응해 엔비디아는 젠슨 황 퇴진 이후 '국가안보·수출통제'를 이사회 차원에서 감독하는 체계로 개편

---

1) 싱가포르 내무부, "Singapore's Investigations into Alice Huang (Huang Le) and Megaspeed International Pte Ltd", 2026.11.12.
2) 미국 상무부 산업안보국(BIS), "BIS Issues Rule Addressing Remote Access to American Super Intelligence Technology", 2026.11.16.
3) Jacob Feldgoise, Kyle Miller and Hanna Dohmen, "Tracking AI Chips: Assessing Location Verification as an Export Control Enforcement Tool", *CSET*, 2026.9.
4) 신효령, "美 민주, 트럼프·젠슨 황 접촉 기록 보존 요구… 엔비디아 수출 문서도", 『뉴시스』, 2026.11.12.

- 11월 17일 이사회 상설 「국가안보·수출통제 감독위원회」를 설치하고, 기존 국가안보팀과 글로벌 무역준수팀이 임시 CEO와 위원회에 직접 보고하도록 조치[5)]
- 이는 안보 위험을 기업 실적과는 별도의 감독 대상으로 삼은 변화로, 향후 거래 심사와 위험 보고가 실제로 독립성을 확보하는지가 개편의 실효성을 좌우

③ 기술방첩: 핵심 인물 포섭과 국가 의사결정에 대한 접근

○ 11월 6일 NYT의 중국 국가안전부 포섭 보도는 이번 사건을 전략기업의 기술뿐 아니라 핵심 인물의 정보와 영향력을 겨냥한 '정보공작' 문제로 부각[6)]
- 최고경영자는 △기술·고객정보와 공급 계획, △규제 대응 전략, △정부와의 협의 내용에 접근하므로 외국 정보기관이 확보하려는 정보의 범위도 넓음
- 특히, 젠슨 황처럼 수출정책 논의에 영향력을 행사하는 인물에 대한 접근은 정보 수집과 정책 영향력 행사를 동시에 겨냥할 수 있다는 점에서 방첩상 중요성이 큼

○ 기술방첩은 정보기관의 접근을 탐지하고, 경고·보호·수사·차단으로 연결하는 국가의 실행능력을 요구
- 전략국제문제연구소(CSIS)는 핵심 경영진이 민감정보 유출과 국가안보 관련 영향력 행사의 경로가 될 수 있다고 지적. 위협 평가와 비밀보장 신고체계를 제안[7)]
- 싱가포르 내무부가 서버 거래 수사에 필요한 슈퍼마이크로 관련 미국 측 정보·협조가 제한적이었다고 밝힌 것은, 위험 인지 이후에도 기업 자료와 해외 증거를 확보하지 못하면 규명과 차단이 지연될 수 있음을 보여줌

○ 종합하면, 세 쟁점을 관통하는 변화는 AI 패권경쟁이 첨단 칩 확보를 넘어 △연산능력의 이용, △전략기업의 의사결정, △핵심 인물의 보호를 둘러싼 경쟁으로 확대되고 있다는 점
- 시진핑은 11월 18일 선전 APEC CEO 서밋에서 AI 협력 확대를 제안했으나, 미국은 제3국 데이터센터의 원격 이용까지 통제를 확대하고 있어 협력 논의와 기술안보 경쟁이 병행되는 양상[8)]
- 향후 우회 경로를 차단하려는 미국의 통제는 거래 상대와 실제 이용자 확인을 강화하는 방향으로 전개될 가능성이 있으며, 기업과 정보·수사 당국의 협력도 기술

---

5) NVIDIA, "NVIDIA Board of Directors Establishes National Security and Export Control Oversight Committee", 2026.11.17.
6) The New York Times, "China's Top Spy Agency Recruited Woman Who Targeted Jensen Huang", 2026.11.6.
7) Matt Pearl & A'ndre Gonawela, "The Nvidia Controversy Should Put Corporations on High Alert About Threats to U.S. National Security", *CSIS*, 2026.11.16.
8) 중국 국무원 홈페이지, "Full text: Keynote speech by Chinese President Xi Jinping at the APEC CEO Summit 2026", 2026.11.18.

안보의 핵심 조건으로 부상

- 한국 역시 수출규정 준수에 머물지 않고, 자국 기업의 기술·인력·의사결정이 외국의 접근에 얼마나 노출돼 있는지 함께 평가할 필요

[표 1] 엔비디아 사태의 3가지 쟁점과 한국의 점검 과제

쟁점	국가안보 위험	한국의 점검 과제
수출통제	우회 거래·원격 이용을 통한 첨단 AI 역량 확보	최종 이용자와 실제 용도를 확인할 수 있는가?
기업 책임	사업적 이해와 경영진 이해충돌에 따른 감독 약화	최고경영자도 견제하고 위험 거래를 중단할 수 있는가?
기술방첩	핵심 인물 포섭을 통한 정보 수집·정책 영향력 행사	위험 탐지가 경고·수사·차단으로 연결되는가?

III. 한국의 기술안보 피해와 정부 대응체계의 취약점

① 핵심 인력을 통한 기술·기밀 유출과 회복하기 어려운 안보 손실

○ 엔비디아 사태에서 제기된 핵심 인물 접근과 기술 확보의 위험은 한국에서도 이미 현실화했으며, 피해는 기업의 영업비밀 상실을 넘어 경쟁국의 기술개발 역량 강화와 국가 정보자산의 훼손으로 연결

- 삼성전자의 18나노 D램 공정정보 유출 사건에서는 해당 정보가 중국 창신메모리(CXMT)의 제품 개발에 사용. 전직 직원에게 2025년 2월 1심 징역 7년이 선고
- 수년간 축적한 공정정보가 경쟁기업에 넘어가면 상대가 시행착오에 투입할 시간과 비용을 줄여주게 되며, 유출자를 처벌하더라도 이미 습득된 기술을 회수하거나 기존 격차를 원상복구하기는 어려움[9)]

○ 정보요원의 포섭은 기술 경쟁력뿐 아니라 해외 정보망과 요원의 안전도 직접 위협

- 정보사 군무원의 '블랙요원 정보 유출' 사건에서는 중국 정보요원 추정 인물에게 요원 신원 등 군사기밀이 넘어갔으며, 해당 군무원에게 징역 20년이 확정
- 재판부는 요원들의 생명·신체에 명백한 위험이 발생하고, 기존 정보수집에 투입한 시간과 노력을 더 활용할 수 없게 됐다고 지적해 인적 정보자산은 유출 이후의 검거만으로 복구할 수 없다는 사실을 확인[10)]

9) 한주홍, "'중국에 반도체 기술 유출' 삼성전자 전 직원 1심서 징역 7년", 『연합뉴스』, 2025.2.19.
10) 이미령, "'중국에 블랙요원 명단 유출' 정보사 군무원 징역 20년 확정", 『연합뉴스』, 2026.1.20.

○ 두 사건은 접근 대상과 수법이 다르지만, 핵심 인력이 가진 정보와 조직 내 지위가 국가안보적 손실의 통로가 됐다는 점에서 공통

- 보호 대상은 기술자료뿐 아니라 고객정보와 요원 신원·공작망까지 포함. 이에 자료 반출 단속을 넘어 핵심 인물에 대한 의심 접촉과 이해충돌을 조기에 포착할 필요
- 따라서 정부는 핵심 인력에 대한 포섭·협박과 의심 접촉을 조기에 탐지하고, 위험 징후가 발견되면 당사자 보호와 정보 접근 제한, 수사로 연결해 유출 이전에 개입할 수 있는 기술방첩 체계를 갖춰야 함

② 정부·여당의 정보·수사 기능 분리와 기술안보 대응의 단절 위험

○ 민주당이 추진한 제도 변화는 정보를 수집한 기관이 직접 수사하거나, 기소를 담당할 검사가 필요한 증거를 직접 보충하던 기능을 분리하는 방향으로 진행

- 2020년 민주당이 주도한 국정원법 개정에 따라 2024년부터 국정원의 대공수사권이 경찰로 이관돼, 국정원은 관련 첩보를 확보하더라도 압수수색 등 강제수사를 직접 수행할 수 없게 됨[11)]
- 이어 이재명 정부·민주당이 추진한 2026년 10월 형사사법체계 개편으로 검찰청이 폐지되고 수사와 기소가 분리됐으며, 검사는 직접수사 대신 수사기관에 보완수사를 요구하는 구조로 전환[12)]

○ 기술안보 사건에서는 정보와 수사 기능의 분리가 '대응 지연'의 위험을 키울 수 있다는 문제가 있음

- 앞선 D램 사건은 국정원이 유출 정황을 포착해 검찰에 수사를 의뢰한 사례로, 해외 첩보와 전문수사가 결합해 범행을 규명했으나, 현재는 수사기관과 공소기관 사이의 추가적인 연결까지 관리해야 하는 상황
- 국정원 대공수사권 이관과 산업기술 유출 수사는 적용 법률이 다르지만, 해외에서 포착한 인물·거래의 맥락을 수사기관이 이어받고 법정 증거로 전환해야 한다는 과제는 공통
- 관련자가 출국하거나 해외 자료가 삭제되는 사건에서 이첩·재확인·보완수사가 반복된다면 그 손실은 단순한 처리기간 증가에 그치지 않으며, 국가는 절차를 진행하는 동안 기술과 증거를 동시에 잃을 수 있음

○ 정부의 공조체계 설명은 이러한 위험을 해소했다는 충분한 답변이 되지 못함

- 산업부는 11월 12일 합동 대응단·국가방첩전략회의·신속 정보지원 채널을 운영한

11) 윤보람, "국정원 대공수사권 경찰로 완전 이관…안보공백 관련 우려 씻을까", 『연합뉴스』, 2023.12.31.

12) 국가법령정보센터, 「검사와 사법경찰관의 상호협력과 일반적 수사준칙에 관한 규정」 제정·개정 이유, 2026.10.2. 시행; 「공소청법」 부칙 제1·2조 등.

다고 해명했으나, 앞선 국감에서는 기술보호 인력·예산과 기관별 기술유출 통계의 종합 관리 필요성이 제기됐고 정부도 보완 필요성을 수용[13)]

• 국정원법 개정(12.30 시행)으로 경제안보 정보수집 범위는 확대되지만, 이는 수사권 회복과는 별개로 확보한 첩보를 증거 수집과 유출 차단으로 연결할 과제는 여전히 남음

- 정부·여당은 '공조하고 있다'는 설명에 그칠 것이 아니라, 위험 첩보의 접수부터 기업 경고·수사 착수·유출 차단까지 누가 책임지는지 밝혀야 함. 권한 분리의 명분이 실제 차단능력의 입증을 대신할 수는 없음

③ 처벌 강화에도 남아 있는 관대한 선고와 외국 개입 입증의 한계

○ 기술유출의 국가안보상 피해에 비해 실제 선고가 충분한 억제력을 갖추는지도 문제

- 주진우 의원실에 따르면, 2025년 판결이 내려진 기술유출 범죄 100건 중 73건에 집행유예가 선고됐으며, 집행유예 비율은 2023년 48%, 2024년 62%에서 상승[14)]
- 이 집계는 전체 기술유출 범죄에 관한 것으로, 국가핵심기술 해외 유출·경영진 가담·조직적 범행의 선고와 환수 결과를 별도로 분석해 중대한 안보 침해에 상응하는 처벌이 이루어지는지 확인할 필요

○ 선고의 책임은 법원에 있으나, 반복되는 문제를 해소할 입법·수사·환수체계를 정비할 책임은 정부·여당에도 존재

- 정부·민주당은 국가안보상 피해가 큰 유출 범죄에 현행 가중처벌이 충분한지, 유출 대가를 추적·보전할 수 있는지, 피해와 외국 측 개입을 입증할 전문인력이 확보돼 있는지를 구체적으로 제시해야 함
- 법정형을 높이고도 입증 부족으로 중대한 범행의 실체를 밝히지 못하거나 범죄수익을 남겨둔다면, 기술유출을 통해 얻는 이익을 꺾기 어려움

○ 외국을 위한 간첩죄의 적용 확대 역시 정보·수사의 연결 문제를 해결하지 않고서는 충분한 방어수단이 되기 어려움

- 형법 제98조의2는 외국 등을 위한 국가기밀 탐지·수집·누설 등을 처벌하지만, 산업기술 유출 모두에 자동 적용되는 것은 아니며 국가기밀 해당성과 외국 측의 지령·사주·의사 연락 등을 입증해야 함
- 결국 외국 정보기관의 개입을 처벌하려면 그 개입을 추적할 정보역량과 법정 증거를 확보할 수사역량이 함께 필요하며, 두 기능의 연결을 어렵게 하는 제도적 장애를 방치한 채 처벌 강화만 내세워서는 기술안보를 지킬 수 없음

---

13) 산업통상부, 「산업기술 유출 방지를 위해 관계기관은 긴밀히 협력하고 있습니다」, 2026.11.12.; 「산업부, 국감 지적 반영해 산업기술 유출 방지 총력」, 2026.10.7.

14) 이태성·이혜수·오석진, "주진우 '기술유출 여전히 처벌 약해…집행유예가 73%'", 『머니투데이』, 2026.10.16.

Ⅳ. 결론: 기술·기밀 유출의 선제적 차단과 향후 추진과제

○ 엔비디아 사태 관련 향후 대응은 △핵심 인물·거래망 보호, △기술안보 수사역량 회복, △고의적 해외 유출의 처벌·환수에 집중

① 핵심 인물·거래망 보호와 경영진 감독 강화

○ 반도체·AI·방산 분야의 의심 접촉을 고객·투자·기술협력 관계와 함께 점검하고, 기존 신고체계를 조기 보호와 연결

- 국정원 111 신고·상담과 현행 신고자 보호제도를 활용하되, 기술유출 이전의 포섭·협박 단계에서도 보호 상담을 받을 수 있는지 점검하고, 접수 후 위험평가·당사자 보호·기업 경고의 담당과 처리 절차를 명확화
- 포섭·협박을 받은 사람이 조기에 신고할 수 있도록 상담 이후의 보호 절차를 명확히 하고, 고의적 가담과 피해 차단을 위한 협력을 구분해 대응
- 해외 중개업체의 실소유자와 데이터센터의 실제 이용자를 확인하되, 기업이 파악하기 어려운 배후 관계는 정부의 해외정보와 관계국 공조로 보완

○ 특히, 경영진이 자신과 관련된 위험 보고와 거래 심사를 통제하지 못하도록 독립적인 감독 절차 마련

- 이해충돌이나 포섭 징후가 발견되면 해당 경영진을 심사에서 배제하고, 이사회·감사기구가 관련 거래와 정보 접근을 재검토
- 이사회 직접 보고와 거래 보류·정보 접근 제한의 판단 권한을 명확히 해, 위험 경고가 실제 차단으로 이어지도록 조치

② 기술안보 수사역량 회복을 위한 정상화 입법 추진

○ 우리는 정보·수사 기능을 분절시키고 긴급 증거 확보를 어렵게 하는 조항을 폐지·개정하는 「국가 기술안보 수사체계 정상화」 입법 패키지를 추진할 필요

- 기존 대공수사권 복원 발의안의 내용과 심사 경과를 점검해 입법을 추진하되, 외국 정보기관 연계 국가핵심기술 유출 사건에 대한 국정원의 직접 수사 참여 범위와 권한도 함께 명확화
- 형사소송법과 수사·공소기관 법률을 함께 정비해 기술안보 사건의 직접 보완수사 기능을 회복하고, 첩보 확보부터 증거 수집·기소까지 추적의 연속성을 보장
- 대상 범죄, 기관별 주도권과 중복수사 조정, 영장·감독 절차를 함께 규정해 권한 회복과 책임 있는 집행을 제도화

○ 입법과 병행해 기존 사건의 이첩·증거 확보 지연을 점검하고, 현행법으로 가능한 합동 추적·긴급 공조는 즉시 시행

- 기존 합동 대응단과 신속 정보지원 채널의 사건별 처리 과정을 점검하고, 최초 탐지기관과 주관 수사기관이 경고 전달·증거 확보·차단 조치의 진행 및 지연 사유를 함께 관리하도록 운영기준을 구체화
- 안보상 경고 이후에도 거래·허가가 유지됐다면 판단 근거와 결정 책임자를 확인해, 경고 묵살과 대응 지연의 원인을 규명

③ 고의적 해외 유출의 엄정 처벌과 외국 개입 입증 강화

○ 현행 몰수·추징 규정과 정부가 발표한 범죄수익 환수 확대방안의 집행·추진 상황을 점검하고, 외국 정보기관 연계·경영진 지위 악용·조직적 해외 유출에 대한 처벌과 환수의 미비점을 정비

- 국가핵심기술 해외 유출 사건의 범죄수익 산정액·보전액·실제 환수액을 구분해 확인하고, 해외재산 추적과 증거 확보를 가로막는 장애를 우선 해소
- 해외 자금·통신·기술자료를 연결해 외국의 지시·대가 관계와 안보상 피해를 입증할 전문인력을 확보하고, 그 결과가 기소와 양형에 반영되도록 지원

○ 향후 우리는 '전략산업 핵심 인물·거래망 기술안보 점검'을 정부에 요구하고, 정상화 입법과 현장 조치의 이행을 관리

- 점검 착수 후 30일 이내 우선 위험·대응 공백·조치계획을 보고하도록 요구하고, 추후 필요한 법률 개정과 전문인력·예산 확보를 추진
- 정보·수사 권한을 나눈 정부·여당에 대응 공백의 해소 책임을 개별 상임위에서 집중적으로 묻고, 확인된 경고 묵살과 지연에는 책임을 추궁

[표 2] 한국의 기술안보 대응과제와 추진 방향

우선 과제	핵심 대응	추진 방향
핵심 인물·거래망 보호	조기 신고·보호와 경영진 관련 거래의 독립 심사	기업 보호체계와 정부 위험정보 지원 점검
기술안보 수사역량 회복	정보·수사의 연속성과 직접 보완수사 기능 확보	관련 조항 폐지·개정을 통한 정상화 입법
엄정 처벌·범죄수익 환수	조직적 해외 유출의 책임 강화와 외국 개입 입증	가중처벌·범죄수익 환수 법제 및 전문인력 정비