Institute For National Security Strategy
www.inss.re.kr

March 2026
No. 375

INSS 전략보고

국가핵심기술 보호를 위한 산업 스파이 대응방안: 연구 안보를 중심으로

박보라
borapark@inss.re.kr

국가안보전략연구원

March 2026
No. 375

CONTENTS

국가핵심기술 보호를 위한 산업 스파이 대응방안: 연구 안보를 중심으로

국가핵심기술 보호를 위한 산업 스파이 대응방안: 연구 안보를 중심으로

저자 | 박보라

국문 초록

국가핵심기술은 해외로 유출 시, 국가의 안전보장과 국민경제의 발전에 중대한 악영향을 미칠 수 있는 우려가 있는 기술을 의미한다. 현재 우리나라는 국가핵심기술을 보호하기 위하여 노력을 기울이고 있으나, 기술 유출 사건은 지속적으로 발생하고 있으며, 최근 5년간 해외로 유출된 국내 산업기술 110건 중 국가핵심기술은 33건 및 그 피해 규모는 약 23조, 2,700억 원으로 추정되고 있다. 우리 정부는 과학기술의 외교 · 안보적 측면까지 고려한 「국가전략기술 육성방안」을 수립하여 글로벌 수준의 연구 협력 이행전략 마련과 핵심연구자산의 유출 방지를 위한 연구보안 체계 강화에 나서고 있다. 그러나 지금까지의 전략은 사후적 보호의 성격이 강하며, 연구과정 전반의 대응이라 하더라도 외국 영향력 및 연구 간섭 등 한국 사회의 변화하는 인력 구조에서 파생되는 연구 위험을 반영하지 못한다는 한계점이 있다. 해외 주요국과 국제사회는 기존 산업 스파이의 논의를 확정하여 연구 안보의 개념을 도입하였고, 물리적 · 인적 보안과 함께 외국의 악의적인 영향력이 연구 활동에 미치려 하는 시도를 차단 및 연구 생태계 보호에 적극적으로 나서고 있다. 국가안보에 경제안보 및 산업 스파이의 논의를 확장한 연구 안보 개념을 도입한 대표적인 사례는 영국이다.

이 보고서는 영국의 「국가안보법」과 「국가안보 및 투자법」 등 주요 법령과 연구 안보 전담 기구 및 주요 이니셔티브를 살펴보고, 이를 바탕으로 한국에의 시사점을 도출하였다.

주제어: 산업 스파이, 산업 보안, 기술 유출 범죄, 연구 안보(research security), 해외 영향력

Ⅰ 서론

▪ 국가핵심기술은 국내외 시장에서 차지하는 기술적 · 경제적 가치가 높거나, 관련 산업의 성장 잠재력이 높아 해외로 유출될 경우 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 기술[1]을 의미

▪ 우리나라의 국가핵심기술 보호를 위한 노력에도 불구하고, 기술 유출 사건은 지속 발생하고 있으며 최근 5년간 해외로 유출된 국내 산업기술 110건 중 국가핵심기술은 33건 및 피해 규모는 약 23조 2,700억 원으로 추정[2]

※ 유출 기술은 △ 반도체(38%) △ 디스플레이(20%) △ 전기 · 전자(8%) 등 국가전략산업에 집중

- 2025년 한 해에만 국가핵심기술 유출 8건을 포함한 총 179건의 기술 유출 범죄가 적발되었으며 기술 유출의 주체는 피해기업 임직원 등 내부인(148건, 82.7%)이 대다수를 차지하는 것으로 파악[3]

최근 5년간 기술 유출 범죄 국내 · 외 유출 현황

(단위: 검찰 송치 건수)

구분	2021년	2022년	2023년	2024년	2025년
계	89	104	149	123	179
국내	80	92	127	96	146
해외	9	12	22	27	33

* 출처: 경찰청 국가수사본부, "경찰청, 2025년 기술유출 범죄 단속 결과", 「보도자료」 2026년 1월 20일.

1 「산업기술의 유출방지 및 보호에 관한 법률」 제2조 2항.

2 이현주, "반도체 등 산업기술 유출 피해, 5년간 23조 원", 『뉴시스』 2026년 1월 14일.

3 경찰청 국가수사본부, "경찰청, 2025년 기술유출 범죄 단속 결과", 「보도자료」 2026년 1월 20일.

▪ 세계 선도 분야의 국내 기술 유출 시도가 지속될 것으로 예측되는 가운데, 우리 정부는 미래 성장과 기술 주권 확보를 위한 「국가전략기술 육성방안」을 발표 및 관련 입법[4]에 나서는 한편, 기업의 기술 유출 방지를 위한 '기술 보호 4중 안전장치'를 본격 시행

- 동 방안은 △ 과학기술의 외교 · 안보적 측면까지 고려 △ 산학연관의 협력 유인 및 글로벌 수준의 연구협력을 고려한 이행전략 마련 △ 핵심 연구 자산의 유출 방지를 위해 '연구 보안' 체계 강화에 특징[5]
- 2024년부터 시행 중인 '기술 보호 4중 안전장치'는 기술 유출 위험 정보수집 · 분석 → 기술 유출 혐의 수사 → 기술 유출 범죄 처벌의 기술 유출 대응 활동의 전(全) 주기를 모두 강화한 조치[6]

▪ 우리 당국은 기술 유출자 대상 실질적 처벌 강화 및 유출 차단을 위한 제도적 노력 강화를 통해 산업기술 보호에 나서고 있으나, 사후적 보호의 성격이 강하며 기술 개발과 연계된 연구 과정 전반의 대응은 아직 부족한 편

▪ 선제적인 기술 유출 예방을 위해 기술 개발과 관련된 과학지식의 생산 과정 전반을 고려할 필요성 제기, 그 근거로 △ 기술패권 경쟁의 무대가 기업뿐만 아니라 대학 캠퍼스와 기초연구 현장까지 확대 △ 모든 과학기술 연구는 국제 활동[7]이라는 점이 해당

- 기술 경쟁이 심화되면서 연구자의 국제 연구협력활동이 기술 · 연구정보 탈취의 주요 경로로 악용되는 추세로, 非보안연구 및 원천연구 분야 대상 불법적인 연구 탈취 및 해외기관의 부적절한 연구간섭 사례 증가[8]
- 美 하버드大 「찰스 리버」 교수 사건[9](2020)을 계기로 주요국은 연구의 보호가 국가안보와 직결될 수 있음을 인식, 기술 유출 방지 이상의 연구 개발 과정 전반에 대한 선제적인 보호책 마련

  ※ 세계적인 나노 과학자인 「리버」 교수는 중국의 「천인계획」에 참여하고 관련 수입을 숨긴 혐의로 2023년 유죄 확정

4 「국가전략기술 육성에 관한 특별법」 및 「국가전략기술 육성에 관한 특별법 시행령」

5 김지혜 · 정유한, "공공부문의 연구보안 프로그램 운영에 대한 연구현장 인식 연구", 『한국산업보안연구』 제13권 제3호 (2023), p. 132.

6 특허청, "우리 기술 지킬 '4중 안전장치' 완성, 올해 본격 가동", 「대한민국 정책 브리핑」 2024년 5월 13일.

7 선인경, "연구안보의 쟁점과 시사점", 「과학기술정책 Brief」 Vol. 39 (2024), p. 1.

8 Manjulika E. Robertson, Samantha M. Chu, Anika Cloutier, Philippe Mongeon, Don A. Driscoll, Tej Heer & Alana R. Westwood, "Interference in Science: Scientists' Perspectives on Their Ability to Communicate and Conduct Environmental Research in Canada", FACETS, November 30, 2023, https://www.facetsjournal.com/doi/full/10.1139/facets-2023-0005

9 강영진, "노벨상 후보 하버드 교수 중국 천인계획 참여 유죄 평결", 『뉴시스』 2021년 12월 22일.

▪ 그동안 국내에서 과학기술 및 연구의 보안을 다루는 논의는 △ 산업기술 유출 방지 △ 연구부정행위 방지 목적의 연구 윤리를 중심으로 진행되어 왔으며, 산업 보안의 관점에서 '연구 보안'을 접근[10]

- 산업 보안은 과학 · 기술 연구 전반이 아닌 산업기술에 정책 초점이 맞춰져 있으며, 국익의 관점에서 접근하고 있으나 산업기술의 유출 방지에만 국한된 소극적 접근법이라는 한계 존재[11]
- 또한 기술 유출을 다루는 산업 스파이차원의 논의는 경제 안보의 부상과 국내 인구구조 변화를 반영하는 연구 생태계 내 잠재적 위험 요인 대응 방안 마련에 대한 논의가 상대적으로 부족한 편

▪ 숄정부적으로 합일되고 포괄적인 대응이 필요한 상황에서 연구 생태계 위험 요인 대응을 위해 기존 산업 스파이 대응 논의를 확장하여 연구 안보 위협에 대한 대처 방안 마련 필요

10 한소영 · 장항배, "연구보안제도 개선을 위한 비교탐색적 연구: 미국의 연구보안 사례를 중심으로", 『한국전자거래학회지』 제27권 제1호 (2022), pp. 111-126.

11 선인경 · 이다은 · 장용석 · 정헌주, 『글로벌 연구 생태계에서의 안보와 자율성 충돌: 해외 사례 분석』, 기초연구 2022-07 (세종: 과학기술정책연구원, 2022), pp. 9-10.

Ⅱ 연구 안보 논의의 이론적 배경

1. 연구 안보의 개관

가. 연구 안보의 논의 배경

▪ 지정학적 긴장 심화 등 국제질서의 변화가 국내외 경제 환경에 영향을 미치면서 그간 산업 스파이 대응 측면에서 논의된 연구 성과물 및 기술 유출 방지 목적의 '연구 보안'에 안보적 접근의 필요성 제기

- 기존 반도체 · 방위산업기술 외 디지털 경제 전환에 따른 빅데이터 분석 · flow 기술, 인공지능(AI) 등 첨단기술의 중요성이 증대되면서 해당 기술 개발 및 확보를 위해 국가간 갈등 고조
- 일부 국가의 적대적인 경제 관행에 기반한 정부 주도의 산업 정책 및 기술 탈취는 타국의 국가안보, 특히 경제안보를 위협하고 있으며, 글로벌 통상 질서에 위협을 제기[12]
- 미 · 중 전략경쟁 심화와 같은 지정학적 긴장은 개방과 협력을 핵심 가치로 내세운 연구 생태계와 연구 목적의 국제협력에 내재된 위험성을 인식하는 계기로 작용

▪ 주요국은 산업 스파이 활동에 대응하는 산업 보안을 확장한 '연구 안보' 개념을 제시하는 한편, 자국의 경제안보 전략에 연구 안보를 포함 및 변화하는 위협 양상에 대응하는 정책 및 법 · 제도 마련에 나선 상황

- 미국은 연구 · 기술 개발을 전담하는 고등교육기관과 연구기관에 대한 외국의 영향력을 차단하기 위해 「NSPM-33 시행 지침(2022/2024)」[13] 및 「CHIPS 및 과학법」[14]을 각각 제정[15]

12 오현석, "외국인투자 안보심사제도 개선방안에 관한 제언: 기술안보를 중심으로", 『국제거래법연구』 제33권 제1호 (2024), pp. 37-38.

13 NSPM-33 Implementation Guidance (2022/2024), 동 지침은 매년 5천만 달러 이상 연방 기금 지원이 집행되는 연구기관은 포괄적인 연구 안보 프로그램을 수립하도록 의무화하고 있다. 연구 안보 프로그램의 핵심 요소로는 사이버보안, 학술 목적을 포함한 해외 여행 · 체류 시 보안 정책, 연구 보안 훈련 등이 제시되고 있다.

14 CHIPS and Science Act of 2022. 미국 내 반도체 제조 시설 투자 촉진과 對중국 기술 경쟁력 우위 공급망 확보를 목적으로 제정된 동 법은 R&D 지원 132억 달러를 포함하여 총 520억 달러 규모의 자금 지원과 미국 내 공장을 건설하는 기업에 25%의 투자 세액 공제를 제공하는 것 등이 주요 내용이다. 단, 보조금을 받은 기업은 중국 내 첨단 반도체 생산 능력을 10년간 확장할 수 없고, 보조금 프로그램에 참여하는 사람은 악의적인 외국의 육성 프로그램(malign foreign talent programs)에 참가할 수 없으며, 보조금 프로그램 참가자와 외국의 연계성을 공개하는 것 등이 의무 조항으로 규정되어 있다.

15 Office of the Director of National Intelligence, "Research Security", https://www.dni.gov/index.php/safeguarding-science/research-security#:~:text=In%20July%202024%2C%20the%20White%20House%20Office,their%20unique%20needs%2C%20challenges%2C%20and%20risk%20profiles. 검색일: 2026년 1월 15일.

- 「경제 스파이 법」[16] 개정을 통해 처벌조항 강화 및 「외국인 투자와 국가안보법」[17]을 통해 외국 자본의 첨단기술 관련 품목 인수합병은 '외국인투자위원회'(CFIUS)의 관리 · 통제를 의무화[18]
- 국립과학재단(NSF) 산하 연구 안보 · 연구 진실성 전담 기구(RSI-ASIO)[19]를 설치한 후 미국 내 · 외 연구 생태계의 안전 확보 목적의 SECURE 프로그램 시행 중[20]
- 美 FBI는 최우선 과제 중 하나로 경제 방첩을 제시, 외국 정부 기관 및 단체의 첨단 기술 탐지행위 대상 수색 활동을 전개하는 한편, CIA, 국방부 등 관계기관간 유기적인 방첩 공조 체계 구축[21]
- 일본은 △ 외국 자본의 직접 투자에 의한 기업 매수 △ 외국의 유학생 · 연구자 파견 등 자국의 첨단기술 유출 경로 다양화에 맞서 「경제안전보장추진법」을 제정, 사회 · 경제 요인에 영향을 줄 수 있는 해외 요인 차단[22]

■ 주요국은 연구 안보의 범위에 자국의 연구 정보 및 신기술 유출 방지뿐만 아니라 해외 영향력 활동 대응까지 포함, 연구 안보는 기존 산업 스파이 활동 대응에서 하이브리드 위협 대응 전략 수립까지 연계 가능

- 하이브리드 위협의 주요 양상에서 목격된 △ 공격 수단의 융합 및 초연결성 △ 디아스포라를 활용한 외국 영향력 활동 등이 연구물 · 기술 유출에 국한되지 않고, 자국의 정치 개입 및 가치 훼손으로 연결 가능하다는 지적[23]

나. 연구 안보의 정의

■ 산업 스파이 대응은 연구 결과물 또는 혁신 기술 등 즉시 상용화하여 경제적 가치를 창출할 수 있는 대상을 다루었으나, 산업 스파이 활동이 지정학적 갈등과 연계되면서 집합적인 위협 제기[24]

■ 영국, 미국, EU 등 주요국과 국제 사회는 기존 산업 스파이 논의를 확장하여 '연구 안보'(research security)를 새로운 의제로 제시, 연구 안보는 기존 산업 스파이 또는 경제 스파이 활동을 모두 포괄

16 Economic Espionage Act (EEA).

17 The Foreign Investment and National Security Act of 2007 (FINSA).

18 한정무, "국가연구개발에서의 연구보안 법제 연구", (단국대학교 박사학위 논문, 2023), pp. 128-129.

19 Research Security and Integrity Information Sharing Analysis Organization.

20 Safeguarding the Entire Community in the U.S. Research Ecosystem (SECURE) Program.

21 https://www.fbi.gov/investigate/counterintelligence (검색일: 2026년 1월 15일).

22 임지영, "일본 경제안전보장추진법(안)의 주요 내용과 쟁점", 「세계 에너지시장 인사이트」 제22-8호 (2022) pp. 1-6.

23 Andrea Christou & Chad Damro, "Research Security and the European Union", *EU-RENEW*, June 13, 2025, https://eu-renew.eu/research-security-and-the-european-union/ (accessed: February 20, 2026).

24 Goldsmith University of London, "Economic Espionage, Q&A with Dr Nicola Searle", July 11, 2025, https://www.gold.ac.uk/news/2025/economic-espionage/ (accessed: January 22, 2026).

▪ OECD는 2020년 국제 사회 최초로 '연구 안보'를 연구 주제로 채택, OECD 회원국의 관련 동향 및 정책을 분석하고 회원국간 사례 공유와 대응 방향을 논의하기 시작[25]

- OECD는 연구 안보를 "연구 활동에 대한 외국 정부나 비국가 행위자의 바람직하지 않은 영향력(interference)을 방지하는 것"[26]으로 정의하고 '외국 영향력'을 "글로벌 연구 생태계의 규범을 준수하지 않는 외국 정부 및 비국가 행위자의 연구 간섭 행위"로 규정[27]
- OECD의 정의는 △ 연구 투자 △ 연구 수행 △ 연구 결과로 연결 되는 연구 활동의 全주기를 대상으로 외부 행위자가 불법적으로 접근 또는 탈취 시도, 스파이 활동을 파악하여 연구 생태계를 보호 하고자 하는 목적[28]

▪ G7은 과학기술 국제협력의 핵심 가치 중 하나로 연구 안보를 지목, '연구안보 워킹그룹'[29]을 신설하고 연구 안보를 "경제적 · 전략적 위험 또는 국가안보 및 국제안보에 위험을 제기하는 행위자와 행위로부터 연구 커뮤니티를 보호하는 활동"[30]으로 정의

▪ EU는 연구 안보를 "제3국 또는 비국가 행위자의 과학적 활동 오용 및 과도한 영향력 행사 방지를 위한 산업 보호"로 규정[31], 유럽 내 디아스포라를 통한 외국 영향력 대응에 초점을 두면서 하이브리드 위협과 연계성을 제시

- EU가 제시하는 연구 안보의 개념은 연구 활동에 가해지는 위험(risk) 전반에 해당, 신기술 유출과 같은 기존 산업 스파이 활동 영역과 더불어 EU 안보 및 가치에 위협을 가할 가능성이 있는 지식 · 기술의 불법적 전달까지 포함

---

25 OECD, "What Is Research Security and Why Does It Matter for Global Science?", November 21, https://www.oecd.org/en/blogs/2025/11/what-is-research-security-and-why-does-it-matter-for-global-science.html (accessed: January 10, 2026).

26 원문 표현은 다음과 같다: "preventing undesirable foreign state or non-state interference with research", OECD 홈페이지 참조.

27 선인경 · 이다은 · 장용석 · 정헌주, 『글로벌 연구생태계에서의 안보와 자율성 충돌』 기초연구 2022-07 (세종: 과학기술정책연구원, 2022), pp. 10-11.

28 상게 보고서, p. 11.

29 G7 Working Group on the Security and Integrity of the Global Research Ecosystem(SIGRE). 관련 내용은 이민정, "G7 오픈사이언스 정책 담론과 시사점", 「KISTEP 브리프」 No. 13 (2024), pp. 1-3. 참조.

30 원문은 "actions that protect our research communities from actors and behaviours that pose economic, strategic, and/or national and international security risks". G7, "Annex to the G7 Science Ministers' Communiqué 2022: Further Implementation and G7 Science Working Groups" 참조.

31 EU Commission, "Council Recommendation of 23 May 2024 on Enhancing Research Security", C/2024/3510, May 30, 2024.

- 국내에서 주로 사용되는 '연구 보안'은 "연구를 수행하는 연구기관 · 연구자가 연구 준비 단계부터 수행 과정과 종료 이후 발생한 연구 개발 산출물이 무단 유출되지 않도록 방지하기 위한 제반 활동"을 의미[32]
  - 결과물에 대한 보안 수준을 넘어 연구 개발 전 과정에 대한 보안 활동으로 확대된 측면은 바람직하나, 연구물의 유출 차단에 중점을 맞추고 있으며 외국의 영향력 대응 차원은 미포함

- '연구 안보' 용어를 제시한 한국과학기술정책연구원(STEPI)은 "국제화 및 연구 개방과 관련된 위험으로부터 연구자와 연구 자산을 보호하고 연구 생태계 가치를 수호하는 것"으로 연구 안보를 정의[33]

- 상기 논의를 종합하여 이 보고서에서는 연구안보를 "기존 산업 스파이 활동 영역을 포함, 국가안보 및 우리의 가치에 위협을 가할 가능성이 있는 정보의 불법적 전달 방지와 연구 활동 전반에 대한 외국 · 비국가 행위자의 영향력으로부터의 연구 생태계 보호"로 정의하고자 함

다. 연구 안보와 유사 개념의 비교

- 연구 안보는 국가의 생존과 직결되는 과학기술의 안보위협化 가능성을 대비하기 위해 수립된 개념이라는 점에서 과학적 기준에 근거하여 지식 생성의 신뢰성 및 정직성 보호 목적으로 수립된 '연구 진실성'(research integrity)과 구별

- 연구부정행위 방지 목적의 연구 윤리는 연구자 개인 및 연구기관 차원의 규범적 덕목을 강조하는 차원에만 논의가 국한되어 국가 차원의 안전과 이익을 고려하는 연구 안보를 도입한 주요국과 차이 존재[34]

- 연구의 유출이라는 측면에서 연구 안보는 산업 스파이와 중첩 부분 존재, 산업 스파이는 개념 정의상 △ 행위적 측면에서 산업기술 유출 여부 △ 동기적 측면에서 경제성의 유무에만 초점을 맞춰 논의가 진행

32 국가과학기술연구회 · 국가정보원, 『연구자를 위한 연구보안 길잡이』 (세종 · 서울: 국가과학기술연구회 · 국가정보원, 2022).

33 선인경 외, (2022) pp. 11-12.

34 상게 연구보고서, pp. 9-10.

국내 주요 연구진의 '산업 스파이' 개념

연구진	정의
정덕영 · 정병수 (2007)	파견 주체가 누구인지 상관없이 경제적 목적으로 상대국의 기업이나 회사가 소유하고 있는 물품의 제조 및 판매방법, 산업과 영업상의 유용한 기술이나 경영정보 등의 산업체 비밀이나 영업비밀과 산업기밀을 불법적으로 입수하거나 정탐하는 행위를 자행하는 사람
신성균 · 박상진 (2009)	특정 국가의 경제적인 경쟁력 제고를 위하여 지시와 지원을 조정하는 첩보수집 활동
이훈재(2011)	고의적인 범의를 가지고 실행되며, 경제적 이익을 목적으로 하는 행위
성용은 · 박준호 · 박준기(2019)	경제적인 목적으로 상대국의 기업 혹은 단체가 소유하고 있는 산업 및 경영정보 등의 기밀을 불법적으로 입수하거나 정탐하는 일체의 행위를 자행하는 사람
조성구(2020)	경쟁국이나 기업이 비밀로 관리하는 중요경제 및 산업정보를 부정한 목적과 수단으로 정탐하고 유출하는 일체의 행위를 하는 사람
최판암(2021)	경제적인 이익을 목적으로 상대 산업체의 핵심기술 및 주요 정보 등을 불법적인 방법으로 취득하기 위하여 해당 정보를 필요로 하는 기업체로부터 지원 또는 협조를 받아서 정탐하거나 정보를 입수하는 사람

- 산업보안 및 관련 학계에서 사용되어 온 '연구 보안'은 기술 유출 및 정보 탈취 방지라는 소극적 보안 활동에 국한되어 있어 연구 개발의 전 과정과 외국의 영향력 대응이라는 적극적인 예방 개념 적용 필요
  - 특히 주요국은 신기술 등 개발이 완료된 연구물뿐만 아니라 '가치 있는 정보' 전반을 연구 안보 개념의 적용 대상으로 하고 있다는 점에서 잠재적인 위험성을 적극 차단

2. 연구 안보 위험 요소와 국내 연구 안보 환경

가. 연구 안보의 위험 요소

- 국제 연구협력에서 발생하는 악의적인 연구활동 관행은 데이터 · 샘플 · 노하우(know-how)의 탈취 및 오용, 기만 또는 강압 등이 해당[35], 연구 안보 관련된 논의는 국제 연구협력에 잠재된 위험(risk)에 초점
  - 연구 안보상 위험은 불법적 · 불투명한 연구활동을 의미,[36] G7은 연구 안보에 위협을 가하는 위험을 ① 위협 행위 ② 범죄 행위 ③ 기타 활동 및 잠재적 위험이라는 3가지의 유형으로 제시[37]

35 OECD, "Integrity and Security in the Global Research Ecosystem", *OECD Science Technology and Industry Policy Paper*, Vol. 130 (2022) pp. 24-29.

36 선인경, "G7, '디리스킹(de-risking)' 강조한 연구안보 위험관리방안 제시", 「과학기술정책 Brief」 Vol. 11 (2023) p. 3.

37 이하 내용은 G7 Working Group on the Security and Integrity of the Global Research Ecosystem(SIGRE)을 참조.

G7의 연구 안보 위협활동

위협 행위	연구 활동에 부당하게 간섭 또는 압박을 가하거나, 연구를 탈취하는 행위를 의미
범죄 행위	정부, 군, 공공기관 또는 비국가 행위자가 연구 아이디어, 연구 산출물 또는 지적재산권을 도용 또는 탈취하는 행위
기타 활동 및 잠재적 위험	한 국가의 경제적 · 전략적 · 안보적 이익을 해하는 행위

※ 출처: 선인경 외, 『글로벌 연구생태계에서의 안보와 자율성 충돌: 해외사례 분석』 기초연구 2022-07 (세종: 과학기술정책연구원) p. 11 재구성.

- 상기 위험은 △ 물리적 · 디지털 인프라 △ 연구자 △ 연구 기금이라는 3가지 차원에서 발생 가능[38]하며, 이에 연구 안보 제반 정책 분야는 사이버보안, 국방 및 정보(intelligence), 외국인 투자, 이민, 법집행을 비롯한 교육, 국제통상 · 수출통제 등 다양한 분야와 상호 연계

- 이러한 이유로 美 국가정보장실(ODNI)은 연구 안보에 관련된 요소로 △ 학문 자원 △ 사이버안보 △ 운영보안 △ 방첩 △ 내부자 위험 △ 공급망 위험 관리 △ 위협 정보 △ 정보보안 △인적 보안 △ 물리적 보안을 함께 포함하여 제시[39]

나. 국내 연구 안보 제반 환경

- 주요국의 연구 안보 논의를 종합 시, 기존 산업 스파이 논의를 확장한 연구 안보 환경은 △ 연구 인력(연구 · 개발 분야의 외국인 유학생 · 전문 인력) △ 기금(외국인 투자)을 기준으로 제시 가능

- 2025년 기준 국내 외국인 유학생 수는 253,434명[40]이며, 이 중 이공계 외국인 유학생 수는 2021년 8,321명에서 2024년 9,001명으로 매년 증가 및 산업계에서도 개발 등 외국인 전문 인력 채용은 지속 증가

38 G7 Security and Integrity of the Global Research Ecosystem(SIGRE) Working Group, "G7 Best Practices for Secure and Open Research Security", (May 2023) p. 4.

39 Office of the Director of National Intelligence, "Research Security", https://www.dni.gov/index.php/safeguarding-science/research-security (accessed: January 10, 2026).

40 e-나라지표, https://www.index.go.kr/unity/potal/main/EachDtlPageDetail.do?idx_cd=1534 (검색일: 2026년 2월 19일).

▪ 이공계 등 연구개발 관련 분야의 외국인 인력 채용 증가는 국내 연구 정보 · 기술의 해외 유출 가능성을 우려하는 배경으로 작용, 외국인 유학생의 핵심기술 유출사례[41] 등이 대표적 사례

- 연구 비자(E-3)로 체류자격을 취득하는 연구 개발 외국인 인력은 2025년 10월 기준 3,420명이 국내 체류 중, 비자 취득 후 근무지 및 근무 분야 등 현황은 체계적 관리 미비[42]

▪ 기술 유출 방식과 관련, 최근 국내에서도 △ 외국의 국내 기업 인수합병을 악용한 기술 유출 △ 위장법인을 통한 공동 연구 제안 및 기술 유출 등 적발 사례가 증가하는 상황[43]

▪ 반면 국내 외국인 투자 안보 심의는 매우 제한적인데 △ 소수 지분 취득도 심사하는 외국과 달리 지분율 50% 이상 취득 시에만 심사 △ 간접지배 투자 및 '그린필드' 투자는 심사 대상 제외 등이 그 이유

※ 그린필드 투자: 외국인 투자자가 대상국에 공장 · 사업장을 새로 설립해 직접 운영하는 형태

▪ 2025년 연간 외국인 직접투자는 전년 대비 4.3% 증가한 360.5억 달러로 역대 최대 실적을 기록하였으나[44], 선진기술 도입 및 고용 창출과 같은 긍정적인 측면과 동시에 기술 유출 등 부작용도 우려[45]

▪ 현재 국내에서 연구 안보와 관련된 법 · 제도적 대응은 연구 안보적 관점보다는 연구 보안적 측면에서 신기술의 보호와 유출 차단에 중점, 2024년 「방첩업무규정」 개정을 포함한 '기술보호 4중 안전장치' 시행

- 2024년부터 시행 중인 '기술보호 4중 안전장치'는 기술 유출 위험 정보수집 · 분석 → 기술 유출 혐의 수사 → 기술 유출 범죄 처벌의 기술 유출 대응 활동의 전(全) 주기를 모두 강화한 조치[46]

41 이강준 · 박상호 · 박진호, ""돌연 자퇴하고 연락 뚝"…베트남 대학원생, 韓 전기차 핵심기술 빼갔다", 『머니투데이』 2025년 4월 30일.

42 안승진, "[단독] 외국인 연구 인력 3400명…개인정보 · 기술 유출 사고에도 현황 파악 없다", 『세계일보』 2026년 1월 10일.

43 이용권, "K - 첨단기술 유출 피해 5년간 23조… 30%가 반도체", 『문화일보』 2026년 1월 14일.

44 산업통상부, "연간 외국인직접투자 360.5억 달러, 역대 최대 실적 달성", 「보도자료」 2026년 1월 7일.

45 한국무역협회 무역정책지원실, "최근 외국인투자기업의 수출입 및 주요국의 외국인투자심사 동향", 「Trade Voice」 Vol. 5 (2025), pp. 1-15.

46 특허청, "우리 기술 지킬 '4중 안전장치' 완성, 올해 본격 가동", 「대한민국 정책 브리핑」 2024년 5월 13일.

기술보호 4중 안전장치 주요 내용

주요 내용	시행일
①「방첩업무규정」 개정 및 특허청의 방첩기관 지정	2024.04.23.
②「사법경찰직무법」 개정, 기술 유출 범죄의 경찰 수사 범위가 모든 영업비밀 범죄로 확대 (영업비밀 부정취득 · 사용 · 누설만 수사 → 예비 · 음모, 부당보유 · 무단유출도 수사 대상化)	2024.01.16.
③「지식재산 · 기술침해범죄 양형기준」 개정으로 처벌 강화	2024.07.01.
④「부정경쟁방지 및 영업비밀보호에 관한 법률」 개정, 최대 5배 징벌적 배상	2024.08.21.

- 연구 안보와 관련된 형사 처벌은 「산업기술의 유출방지 및 보호에 관한 법률」('산업기술보호법') 및 「부정경쟁방지 및 영업비밀보호에 관한 법률」의 이원적 체계로 구성
  - 「산업기술보호법」상 국가가 지정한 국가핵심기술 및 산업기술의 국외 유출은 가중처벌 대상이며, 「부정경쟁방지법」은 영업비밀의 해외무단 사용 및 누설 시 최대 15년 이하의 징역형으로 처벌 강화
  - 해외 기술유출에 대한 국내 형벌 수준은 높아졌으나, 법체계의 분산 및 중복으로 인한 문제점[47]과 최근 한국에서 발생한 첨단기술 해외 유출 사건의 형법상 간첩죄 규정 불가능 등 문제점 지속
  - 이에 형법 제98조 '적국을 위하여 간첩행위를 하거나 적국의 간첩을 방조한 자'를 '적국을 위하여 적국의 지령, 사주 하에 국가기밀을 탐지 · 수집 · 누설 · 전달 · 중개하거나 이를 방조한 자'로 구체화하고(1항),
  - '외국 또는 이에 준하는 단체를 위하여 외국 등의 지령, 사주 하에 국가기밀을 탐지 · 수집 · 누설 · 전달 중개하거나 이를 방조한 자'도 처벌 대상에 포함(2항 신설), 법정형을 사형, 무기 또는 7년 이상의 징역에 처하는 개정안이 2월 26일 통과

47 김다은, "경제 · 기술안보 시대 간첩죄 개정안의 제도적 함의와 향후 과제 고찰", 『한국민간경비학회보』 제24권 5호 (2025), p. 21.

Ⅲ 영국의 연구 안보 접근 사례

1. 연구 안보 접근의 기본 방향

가. 기본 방향

▪ 영국의 연구 안보 접근은 EU의 연구 안보 접근 방향과 유사한 관점을 채택, 이는 연구 안보에만 국한된 것이 아니라 허위조작정보(FIMI) 대응 등 위협 대응에서도 동일하게 나타나는 방식

▪ EU는 EU 경제 안보 전략의 일환이자 EU 회원국과 유럽 내 연구 · 혁신 분야 지원을 목적으로 2024년 「연구 안보 강화를 위한 EU 이사회 권고안」을 상정, 경제 안보와 연구 안보를 연계하여 대응 전략 수립

- △ 기술 개발과 기술 유출 방지 중심에서 외국의 영향력 공작 대응까지 논의 확장 △ 디아스포라 發 위협의 범위 확대를 통해 유럽의 안보 및 가치 보호에 주력하였다는 점이 특징
- EU는 제3국에 의한 △ 신기술 · 핵심기술 유출 △ 악의적 영향력 △ 연구 윤리 위반과 연계된 위험 요소 관리에 중점, 연구 안보의 근본적인 목적을 개방적이고 안전한 연구 활동과 연구의 자유 보호로 제시

나. 연구 안보 논의의 배경

▪ 기술 · 방산 등 고가치 산업에 크게 의존하는 영국의 경제 구조상 기술 유출은 심각한 경제적 손실뿐만 아니라 영국의 국가안보 및 민주주의에 영향을 미치는 행위로 인식

- 과거 예상가능한 형태의 물리적 · 일차원적 방식에서 스파이, 기술 유출, 허위조작정보 유포, 외국의 내정 간섭, 사이버공격 등 다양한 형태로 안보위협이 진화하고 있음을 인식, 이를 '국가위협'으로 명명

▪ 영국은 △ 인터넷의 대중화와 신기술의 상용화를 악용한 위협 제기 △ 정부-민간기간 경계의 모호화에 따른 위협 대상의 확대 △ 스파이 활동의 주체 및 '가치 있는 정보'의 범위 확대라는 상황에 직면[48]

- 기존에 개발이 완료되어 사용가능한 기술에서 원천 연구 분야까지 '가치 있는 정보'의 범위가 확대되었으며, 이에 따라 연구 결과물 뿐만 아니라 연구 정보도 위험 관리 대상으로 포함될 필요 제기

48 정제용 · 김학경, "영국의 국가안보법 제정과 그 의미에 관한 고찰: 경제안보 및 산업보안 중심으로", 『범죄수사학연구』 제20호 (2024), p. 181.

- 영국 대학에 대한 중국 내정 간섭 이슈(2019)[49] 및 중국 「화웨이」의 케임브리지 대학 침투[50] 등 문제 제기를 기점으로 연구자에 대한 위험 관리 이슈 제기
- 2021년 기준 영국의 연구 개발 중 60.1%가 국제협력을 통해 진행, 이공계 분야 영국 내 유학생 수 지속 증가 등 연구의 초기 단계에서부터 위험 관리가 이루어져야 한다는 필요성이 제기된 배경[51]

2. 연구 안보 관련 법제 동향

가. 「국가안보법」(2023) 제정

▪ 기존 영국의 국가방첩활동상 법적 근거인 「공공비밀법」(Official Secrets Act)은 '하나의 특정 관할 내에서 적대적 행위를 하는 국가'라는 개념에 기반, 변화하는 스파이 활동 대응에 한계점 존재

- 동법 적용 시 △ 국방·군사 정보 외 산업 기밀 유출 행위 △ 사이버해킹 등으로 인한 영국 외 지역에서 발생하는 정보 유출 행위를 처벌하지 못한다는 한계점 존재
- 「공공비밀법」만으로 산업기술 유출 활동과 중요정보의 무단 유출 방식 변화를 반영하지 못하며 국가-기업간 경계 모호화 추세에 대응하기에 역부족이라는 상황 인식이 공유, 대체 입법의 필요성 공감[52]

▪ △ 스파이 활동의 성격 변화 △ 스파이 활동 대상 선정 및 접근 방식의 현대화 등 산업기술 유출 추세 대응이 필요하다는 공감대가 형성된 후 「국가안보법」(National Security Act 2023) 입법안 통과(2023.12. 시행, 7년 소요)

▪ 국가방첩활동의 주요 대상에 해당하는 국가를 '적'이라는 이분법적 접근 대신 오늘날 다양한 행위로 나타나는 광범위한 위협과 피해를 포괄하는 방향으로 입안되었다는 점이 특징

▪ 「국가안보법」은 상호 연결된 세계에서 '적대국'이라는 이분법적 개념에서 벗어나 오늘날의 다양한 행위로 나타나는 광범위한 위협과 피해를 포괄하는 방향으로 입법, 스파이 행위를 새롭게 범죄화[53]

---

49 Patrick Wintour, "'Alarming' Chinese Meddling at UK Universities Exposed in Report", *The Guardian*, November 5, 2019.

50 UK-China Transparency, *Cambridge-Huawei Report*, Charity No. 1201902, https://ukctransparency.org/data/media/2023/10/Cambridge-Huawei-Report.pdf (accessed: February 23, 2026).

51 National Protective Security Authority, "Trusted Research", https://www.npsa.gov.uk/specialised-guidance/trusted-research (accessed: February 23, 2026).

52 정제용·김학경, "영국의 국가안보법 제정과 그 의미에 관한 고찰: 경제안보 및 산업보안 중심으로", 『범죄수사학연구』 제20호 (2024), pp. 181-182.

53 Part 1, Sec. 1, Sec. 3, Sec. 18에서 범죄화한 행위 규정

英「국가안보법」상 새롭게 범죄화된 스파이 행위

해당 조항	세부 내용
Section 1. 보호된 정보의 스파이 행위	누군가가 (a) 보호된 정보를 획득, 복사, 기록, 보유, 공개 혹은 접근 제공을 하는 행위여야 하고; (b) 영국의 이익 혹은 안전에 위험을 초래한다는 것을 인지하거나 그에 알려진 다른 사항들을 고려할 때, 합리적으로 인지할 수 있는 경우; (c) 그러한 행위가 다른 국가에 이익을 가져다 줄 의도를 가지거나 가져다 줄 것으로 인지하고 이행되거나, 그에 알려진 다른 사항들을 고려할 때 합리적으로 알 수 있는 경우
Section 2. 산업기술유출행위[54]	누군가가 (a) 산업기밀을 획득, 복사, 기록, 보유, 공개 혹은 접근 제공을 하는 행위여야 하고; (b) 그러한 행위는 승인받지 않은 행위이며, (c) 그러한 행위가 승인받지 않은 행위라는 것을 인지하거나, 그에 알려진 다른 사항들을 고려할 때 합리적으로 인지할 수 있는 경우; (d) 그러한 행위가 다른 국가에 이익을 가져다 줄 의도를 가지거나, 가져다 줄 것으로 인지하고 이행되거나, 그에 알려진 다른 사항들을 고려할 때 합리적으로 알 수 있는 경우
Section 18. 사전준비행위	(a) Section 1 혹은 2와 같은 스파이 행위 중 하나를 저지르려는 의도를 가지거나, 또는 그러한 행위가 다른 사람에 의해 자행되려는 의도가 있는 경우에 (b) 그러한 행위의 실행을 사전에 준비하는 어떠한 행동에 착수한 경우

※ 출처: 정제용 · 김학경, "영국의 국가안보법 제정과 그 의미에 관한 고찰: 경제안보 및 산업보안 중심으로", 『범죄수사학연구』 제20호 (2024), pp. 187-190 재구성.

■ 「국가안보법」 Part 1의 적용 대상인 스파이 관련 범죄유형은 아래와 같이 정리할 수 있으며, Part 2에서는 제한적 조치의 일환인 스파이 활동의 '예방 및 수사 조치'를 규정하고 있음

英「국가안보법」 적용 대상 스파이 행위 유형

① 첩보활동으로부터 민감한 장소(금지된 장소) 보호와 관련, 드론이나 전자적으로 이러한 장소에 접근하는 것
② 산업 기밀 유출 행위
③ 영국 내외를 막론하고 영국의 국가안보와 국익을 해치며 외국정보기관을 원조하는 행위
④ 외국의 지시를 받고, 영국의 안전이나 이익을 해하는 고의적인 방해 행위
⑤ 영국의 정치체제 등에 대한 외국의 간섭, 방해 활동
⑥ 영국에서 신고되지 않는 외국 스파이로서 외국 정보기관의 활동을 물질적으로 돕는 행위

※ 출처: UK Home Office, "A Guide to the National Security Act 2023 for Security Professionals", January 24, 2025 및 UK National Security Act 2023 Part 1. 재구성.

54 Sec 2. 〈산업기술유출행위〉 동 규정은 영국의 산업기술과 기업들의 상업적 및 경제적 가치를 가지고 있는 정보를 보호하기 위한 것으로 기존의 「공공비밀법」에서는 관련된 규정이 존재하지 않았다. 즉 스파이 행위의 진화된 위협 방식이 국가에 대한 위협뿐만 아니라 주요 산업 및 기술에 대한 위협도 포함하고 있다는 점을 고려하여 기존 「공공비밀법」의 법률적 공백을 메우기 위한 입법이다. 정제용 · 김학경, "영국의 국가안보법 제정과 그 의미에 관한 고찰: 경제안보 및 산업보안 중심으로", 『범죄수사학연구』 제10권 제2호 (2024), pp. 189-190.

- 「국가안보법」 Part 2에서 규정된 '예방 및 수사조치'(Prevention and Investigation Measures, PIMs)는 영국 정보기관이나 수사 기관에서 영국에 국가 위협을 가하는 개인의 활동 또는 계획을 식별했으나, 용의자 기소가 현실적이지 않을 때 사용될 수 있음[55]
- 예방 및 수사조치는 용의자 검거 및 처벌보다 「국가안보법」상 '국가 위협활동'으로 정의된 행위에 해당인의 추가 참여를 방지하여 위협의 감소 및 예방에 목적, 다른 방법이 불가능할 경우에만 제한적으로 활용해야 함[56]

英 「국가안보법」 상 예방 · 수사 조치

① 대상자의 거주 장소 제한
② 대상자의 특정 장소 출입 제한
③ 대상자 개인의 무기 및 폭발물 접근 제한
④ 특정 장소에의 접근 또는 대상자가 일하거나 연구하는 장소 제한,
⑤ 대상자가 어떤 사람과 어울릴 수 있는지 또는 대화할 수 있는지 제한
⑥ 대상자 개인의 금융 서비스 접근 또는 전자 통신 장비의 사용 제한,
⑦ 대상자가 영국을 떠나거나, 영국 내 특정 지역을 이탈하는 것을 제한

※ 출처: UK Home Office, "State Threats Prevention and Investigation Measures (STPIMs): National Security Bill Fact Sheet", June 24, 2025 재구성.

나. 외국인 투자 관련 법제 개정

- 영국의 외국인 투자 규제 근거인 「기업법」(Enterprise Act)은 정부가 외국인 투자에 개입 가능한 범위가 비교적 제한되는 한계점 존재[57], 이에 2021년 「국가안보 및 투자법」(National Security and Investment Act)을 개정하여 외국인 투자 심사를 강화
  - 개정된 「국가안보 및 투자법」은 기업 · 에너지 · 산업전략부 산하 외국인의 투자심사를 전담하는 투자안보국(Investment Security Unit, ISU)을 신설, 국가안보에 대한 위협이 있다고 판단될 경우 영국 정부가 기업의 국내외 인수합병 과정에 직접 개입 가능[58]

55 Explanatory Memorandum to the National Security Act 2023, Prevention and Investigation Measures, (POLYGRAPH) Regulations 2023, No. 1249. https://www.legislation.gov.uk/

56 Explanatory Note "The government anticipates such measures will be used sparingly and as a measure of last resort to mitigate the immediate threat an individual poses while they continue to be investigated"

57 KOTRA, "영국, 외국인투자 심사제도 강화", 「KOTRA 해외시장뉴스」 2021년 6월 7일. https://dream.kotra.or.kr/kotranews/cms/news/actionKotraBoardDetail.do?SITE_NO=3&MENU_ID=100&CONTENTS_NO=1&bbsGbn=322&bbsSn=322&pNttSn=188924 (검색일: 2026년 2월 5일).

58 KOTRA, "영국, 외국인투자 심사제도 강화".

- 투자안보국은 ① (대상) 인수 대상 기업 또는 자산이 국가안보 위험을 초래하는지 여부 ② (인수자) 인수 기업 또는 자산에 대한 지배권을 사용할 수 있는 특정 인수자가 국가안보 위험을 초래하는지 여부 ③ (통제) 인수자가 얻는 지배권의 정도를 검토하여 구분[59]

외국인 투자의 국가안보 위험 고려 요소

구분	고려 요소	
대상 위험	기업	· 의무신고 대상 분야에서 사업을 영위하거나 밀접하게 연관된 기업의 인수 · 정부와 밀접한 관계를 맺고 있는 기업의 인수 · 특정 부문 또는 연계 부문에 걸친 누적 인수 거래 · 새로운 법인 설립에 기존 자산 또는 기업에 대한 지배권 변경이 포함되는 경우[60]
	자산	· 기타 경제적 가치가 있는 아이디어, 정보 또는 기술과 같은 무형자산을 포함한 자산에 대한 지배권 취득 · 의무신고 대상 분야 또는 밀접하게 연관되어 사용되거나 사용 가능한 자산 · 해당 자산의 수출통제 대상 여부를 고려 및 수출통제통합국(ECJU)이 발급한 모든 수출허가를 고려하여 신고 여부 결정 · 중요한 국가기반 시설이나 정부 건물 등의 토지
인수자 위험	· 자금 출처[61] 등 관련 당사자의 의도와 과거 행동 · 인수자와 영국의 적대국 또는 적대적 단체와 관련된 유대관계[62]를 고려하고, 정치적, 군사적 또는 국가가 지원하는 영향력이나 의무를 검토하기 위해 관련 당사자가 인수자에게 부과한 요건 고려 · 인수자가 영국 또는 외국의 제재를 받고 있거나, 받은 적이 있는지 여부와 제재 대상자가 대상 기업 또는 자산에 대해 가지게 될 지배권의 수준 고려	
통제 위험	· 인수를 통해 획득하였거나, 획득하게 될 지배권 고려[63] · 인수자가 이사회에 대한 접근권이나 기타 의사결정을 통해 인수 대상의 정책에 영향을 미칠 수 있는 지배력을 확보할 수 있는지 여부	

※ 출처: 임정현, "英 국가안보투자법(NSIA) 관련 지침 개정 발표", 「수출통제 Issue Report」 (전략물자관리원, 2024년 6월) 2024-43. p. 2 재구성.

- 동 법 개정을 통해 △ 의무 사전 신고 △ 자발적 신고 △ 콜인(call-in) 제도 도입, 「국가안보 및 투자법」에서 지정한 17대 민감 분야의 경우 의무 사전 신고 대상[64]

59 임정현, "英 국가안보투자법(NSIA) 관련 지침 개정 발표", 「수출통제 Issue Report」 (전략물자관리원, 2024년 6월), p. 2.

60 특정 합작투자, 그린필드 투자의 지적재산권 이전 등이 해당된다.

61 투자 컨소시엄의 개별 구성원, 펀드 매니저 및 최종 수익 소유자 포함 등

62 출신 국가에만 근거하여 판단하는 것은 아님

63 지배권이 높아질수록 국가안보 위협 초래 가능성이 높아짐

64 UK Cabinet Office, "National Security and Investment Act: Details of the 17 types of notifiable acquisitions", Updated February 6, 2024.

의무 사전 신고 대상 17대 민감 분야

① 첨단 소재	② 첨단 로봇	③ 인공지능65	④ 민간 원자력
⑤ 통신	⑥ 컴퓨터 하드웨어	⑦ 정부 핵심 공급업체	⑧ 암호화 인증 기술
⑨ 데이터 인프라	⑩ 국방	⑪ 에너지	⑫ 군사용 · 민군 겸용 기술
⑬ 양자 기술	⑭ 인공위성 · 우주 기술	⑮ 위기 관련 공급업체	⑯ 합성생물학
⑰ 수송			

- 「국가안보 및 투자법: 고등교육 및 연구 부문 지침」을 통해 △ 주요 개정 사항 및 자문 제공 가능 대상 △ 「국가안보 및 투자법」 적용 대상과 사례 △ 17대 민감 분야 해당 시 신고 및 승인 취득 절차 △ 영국 정부 심사 결정 시 절차 등을 별도로 안내[66]

3. 연구 안보 관련 기구 신설과 이니셔티브

가. 영국 정보기관의 연구 안보 전담조직 신설

- 기업 · 에너지 · 산업전략부의 투자안보국 외 연구 안보와 관계된 정부 부처에서 전담 조직을 개설, 연구 · 기술 및 연구자, 연구 생태계 보호를 위한 全정부적인 접근법 추진
  - 외무 · 英연방부(FCDO)는 첨단재래식무기 등 민감 분야에 수학하려는 외국인 유학생 대상 학술기술승인제도(ATAS)를 운영, 2021년부터 유학생 외 외국인 연구자까지 스크리닝 절차 강화[67]
  - 과학 · 혁신 · 기술부(DSIT)는 연구협력자문팀(RCAT)에게 민감 · 신흥연구 분야 국제협력시 연구자에게 국가안보 관련 자문 제공 역할 지정, 2025년 7월 기준 국제 연구협력 시 '외국 영향력 등록제도' 도입[68]

65 2026년 1월 기준으로 생성형 AI를 포함 예정으로 공지되고 있음.

66 UK Cabinet Office, National Security and Investment Act: Guidance for the Higher Education and Research-Intensive Sectors, Updates May, 2024.

67 UK Foreign, Commonwealth & Development Office, "Academic Technology Approval Scheme (ATAS)", November 26, 2025, https://www.gov.uk/guidance/academic-technology-approval-scheme (accessed: February 24, 2026).

68 Research Collaboration Advice Team (UK DSIT), "Foreign Influence Registration Scheme: check if you need to register", July 3, 2025, https://www.gov.uk/government/publications/foreign-influence-registration-scheme-check-if-you-need-to-register (accessed: February 24, 2026).

▪ 국내 정보를 담당하는 영국 보안국(MI5)은 국가기반보호센터(CPNI)의 소관 범위를 대폭 확대한 '국가보호안보국'(National Protective Security Authority)을 신설, 물리적 보안과 인적 보안을 통합[69]

- 기존 국가기반보호센터는 테러 및 기타 위협으로부터 영국의 국가 인프라를 보호하는 역할 담당, 조직 확대 · 개편을 통해 민간 · 공공 조직에 안보 교육 · 자문 및 지침을 제공하는 등 업무 범위 확대[70]
- CPNI와 마찬가지로 국가보호안보국도 대테러 업무를 포함[71], 연구 안보와 관련된 기업 · 연구 기관 대상의 안보 위협에 대한 인식을 제고하는 한편 대상별로 활용 가능한 다양한 지침과 도구를 개발

▪ 국가보호안보국은 연구 안보와 관련, '혁신의 보호'(Secured Innovation) 프로그램을 운영하는 한편 국가사이버안보센터(NCTC)와 공동으로 '신뢰할 수 있는 연구'(Trusted Research) 프로그램, 기업통상부(DBT) 등과 공급망 지침 프로그램(Supply Chain Guidance)을 각각 운영

나. 신뢰할 수 있는 연구(Trusted Research) 이니셔티브

▪ 2019년 중국의 영국 내 대학 침투 논란 이후 영국 내 대학들은 연례 총회에서 '신뢰할 수 있는 연구' 프로그램을 개시, 국가보호안보국과 국가사이버안보센터와 밀접한 협력을 통해 안보 위협으로부터 안전한 국제협력 문화 조성 추진[72]

▪ '신뢰할 수 있는 연구'(Trusted Research)는 "영국의 지적재산권, 민감분야 연구, 연구자 및 인프라를 적대적 행위자의 간섭을 포함, 잠재적 탈취, 조종 및 착취로부터 보호"하는 이니셔티브[73]

- '신뢰할 수 있는 연구'는 △ 국제협력 대상 연구의 잠재적 위험 요소 파악 △ 국제 연구협력 신뢰 제고 및 정보 기반 의사결정 지원 △ 연구 탈취 및 연구의 오용 · 악용으로부터 연구와 연구자 보호라는 3가지 요소로 구성[74]

---

69 https://www.npsa.gov.uk/ (accessed: February 24, 2026).

70 https://www.npsa.gov.uk/about-npsa/who-we-work (accessed: February 24, 2026).

71 영국은 대테러 관련 법령에 사이버공격('사이버테러')이 포함되어 있기 때문임.

72 National Protective Security Authority & National Cyber Security Centre, *Trusted Research Guidance for Academics*, (2025).

73 UK Research and Innovation, "Trusted Research and Innovation", January 19, 2026. https://www.ukri.org/manage-your-award/good-research-resource-hub/trusted-research-and-innovation/ (accessed: February 22, 2026).

74 선인경 · 이다은 · 이동우 · 양현채 · 김은지, 『연구안보에 관한 주요국 정책 비교 분석과 국내 대응 방향 연구』 정책연구

▪ 동 이니셔티브는 연구 · 기술 분야의 혁신 주체별 특성에 따른 맞춤형 지침을 개발, 혁신 주체별로 처할 수 있는 연구 안보 위험환경과 의사결정 시 참고 사항을 구분하여 제시하고, 이를 통해 연구 안보에 대한 인식 제고와 연구 안보의 현장 정착을 노력

혁신 주체별 연구 안보 점검사항[75]

주체	발간 유형	주요 내용
학계	학계 점검사항	① 연구협력 파트너 제반 사항 ② 업무협력 성과 관련 사항 ③ 기존 연구협력 파트너와 이해충돌 사항
	고위급 관리자용 지침	고위급 관리자 차원에서 연구 안보 관련 의사결정 시 고려사항
	학계 지침	① 국제협력 시 안보위협 요소 ② 수출통제, GDPR 등 관련 법제 안내 ③ 연구 및 연구자 보호 방안
	신뢰받는 연구 이행 지침	① 안보위협 교육 ② 교육훈련을 통한 대응능력 강화 ③ 보안 강화 환경 조성 ④ 보안 강화에 대한 인센티브 ⑤ 보안 강화에 대한 평가
	해외활동 이행 지침	회의 및 컨퍼런스, 현장 방문, 주관연구 수행, 방문 연구자, 컨퍼런스 발표 및 강의, 해외 협력 연구자 방문, 해외 연구기관 방문 등 해외활동 시 주의사항
산업계	산업계 점검사항	① 기술성숙도, 지식재산권 등 연구 포트폴리오 점검 ② 협력 기관 점검 ③ 협력 프로젝트 점검
	산업계 지침	연구협력 파트너로서 학계와 협력 시 주의 및 참고사항

※ 출처: https://www.npsa.gov.uk/specialised-guidance/trusted-research 내용 재구성.

2023-14 (세종: 과학기술정책연구원, 2023), p. 19.

75 영국 국가보호안보국(NPSA) 홈페이지 내용 재구성. https://www.npsa.gov.uk/specialised-guidance/trusted-research (accessed: February 3, 2026).

Ⅳ 對韓 시사점과 고려 사항

1. 연구 안보 관련 대국민 인식 제고 노력 및 공감대 형성 필요

- 해외의 경우, 핵심기술의 개발뿐만 아니라 유출 방지가 향후 국가의 생존과 직결된다는 인식 속에서 산업 스파이의 범위를 특정한 국가에 유리한 방향의 연구 수행, 신기술의 불법 이전까지 포함하는 추세

- 기존 산업 스파이를 확장한 '연구 안보' 개념을 제시하게 된 배경에는 국제 연구협력에 내재된 잠재적 위협과 함께 자국 내 디아스포라 증가와 외국 영향력 공작의 연계 양상이 지속 적발되는 데 기인

- 국내의 경우, 연구 보안 정책을 통해 연구 결과물 · 기술 유출 차단과 연구 과정의 전 단계의 보안관리에 나서고 있으나, 유출 방지 중심의 정책 초점과 디아스포라 대응에는 소극적이라는 한계점 지적
  - 국내 대학도 외국인 유학생 · 연구원을 적극 유치하고 있으나, 인적요소를 통한 연구 · 기술 유출의 잠재적 위험성은 논의 및 대응책 마련이 소극적으로 이루어지는 편
  - 대학의 자체적인 연구 안보 지원체계 및 전문가 육성과 함께 연구 개발 현장에서 연구 진실성 외 연구 안보의 인식 제고 필요성 제기 및 외국인 연구원 전용 규정 마련과 이행을 의무화할 필요[76]

- 기존의 연구 보안 정책도 문서뿐인 규정으로 인식하는 것이 아닌, 대학을 포함한 연구 개발 현장에서 실제 보안 문화로 정착될 수 있도록 연구 종사자의 전반적인 인식 전환을 유도할 수 있는 노력 필요

- 연구 안보와 관련된 입법 노력도 전국민적 공감대 형성과 인식 제고가 필수적인 부분, 영국의 「국가안보법」 입법 당시 약 7년에 걸쳐 인식 제고 캠페인 진행 및 충분한 공감대 형성을 거쳤다는 점에 주목
  - 연구 안보와 관련된 법제 정비는 필연적으로 국가의 공권력 범위 확대 및 강화 등을 수반하게 된다는 점에서 관련 법률의 제 · 개정 필요성에 대한 충분한 공감대 형성이 입법 지지의 기반으로 작용

76 이대권 · 김태건 · 박준석, "대학기관의 실태조사를 통한 연구보안 강화방안: 연구보안 규정을 중심으로", 『한국산업보안연구』 제14권 3호 (2024), pp. 183-187.

2. 연구 안보 제반 위협의 안보범죄 인식 및 관련 제도 연계 필요

▪ 기존 형법은 국내에서 발생한 첨단기술 유출 사건의 상당수가 북한이 아닌 제3국을 향한 것임에도 법리상 간첩죄(제98조) 적용이 불가능하여 「산업기술보호법」 위반 혐의로 처벌

▪ 2026년 핵심기술 보호는 단지 특정 기업의 손실이 아닌 국익 위해 요소 차단과 직결된다는 인식에서 「형법」상 '간첩죄'의 적용 대상을 '외국'으로 확대하는 형법 제 98조의 2를 신설(2.26)

- 기존 간첩죄의 적용 대상을 적국에서 '외국과 이에 준하는 단체'로 확대 및 산업 스파이의 처벌 기준 대폭 강화 등 성과가 있으나, '국가기밀'에만 적용되는 점은 다소 아쉬운 부분
- 이번 개정을 통해 반도체 · 디스플레이 등 국가안보와 직결되는 분야는 간첩죄 적용이 가능해졌으나, 일반적인 산업 기밀 유출 사건은 「산업기술보호법」만 적용되기 때문임
- 첨단기술 유출은 인력 포섭 및 장기간의 공작을 통해 이루어진다는 점에서 스파이 행위와 사실상 동일하며, 연구 안보 위협 행위는 우리의 개방적인 연구 생태계와 국가안보를 위협한다는 점에서 경제범죄보다는 안보범죄로 규정 및 대응 노력 필요

▪ 기술 유출 사건 관련 수사 및 재판 절차의 전문화를 위한 제도 연결 강화도 시급, 전문법원이 기술 유출 사건을 담당하는 일본 · 대만과 달리 우리는 현재 전문법원 없이 일반 형사재판부가 기술 유출 사건을 담당[77]

- 일반 형사재판부의 기술 유출 사건 담당 시 기술적 쟁점에 대한 이해 부족이나 담당 판사의 잦은 교체로 인한 노하우 축적 미흡 등 문제 제기[78]
- 이번 간첩죄 개정을 통해 경찰은 안보수사국 내 산업기술보안수사대의 방첩 기능을 별도의 조직으로 분리 · 재편한 테러방첩수사대를 설치한 만큼 수사 단계 이후 재판 단계의 전담 부서 지정을 통한 전문성 강화 필요

▪ 연구 안보의 강화를 위해 연구 관련 기관의 연구 보안 업무는 연구물의 유출 차단을 넘어서는 외국 영향력 및 연구 간섭 대응을 위한 지침 및 점검사항 등 수립 · 배포까지 확대 검토 필요

77 김은환, "대만 개정 국가안전법에 관한 공법적 고찰: 국가핵심기술 유출방지에 관한 사항을 중심으로", 『공법학연구』, 제26권 4호 (2025), pp. 359-386.

78 황경준 · 권헌영, "기술유출 형사사건의 처리 실태와 개선 고려사항 논의: 무죄사건을 중심으로", 『융합보안논문지』 제22권 3호 (2022), pp. 41-55.

참고문헌

강영진. “노벨상 후보 하버드 교수 중국 천인계획 참여 유죄 평결”. 『뉴시스』 2021년 12월 22일.

경찰청 국가수사본부. “경찰청, 2025년 기술유출 범죄 단속 결과”. 「보도자료」 2026년 1월 20일.

국가과학기술연구회 · 국가정보원. 『연구자를 위한 연구보안 길잡이』 세종 · 서울: 국가과학기술연구회 · 국가정보원. 2022.

「국가전략기술 육성에 관한 특별법」.

「국가전략기술 육성에 관한 특별법 시행령」.

김지혜 · 정유한. “공공부문의 연구보안 프로그램 운영에 대한 연구현장 인식 연구”. 『한국산업보안연구』 제13권 제3호 (2023), pp. 131-152.

김다은. “경제 · 기술안보 시대 간첩죄 개정안의 제도적 함의와 향후 과제 고찰”. 『한국민간경비학회보』 제24권 5호 (2025), pp. 1-31.

김은환. “대만 개정 국가안전법에 관한 공법적 고찰: 국가핵심기술 유출방지에 관한 사항을 중심으로”. 『공법학연구』, 제26권 4호 (2025), pp. 359-386.

「산업기술의 유출방지 및 보호에 관한 법률」.

산업통상부. “연간 외국인직접투자 360.5억 달러, 역대 최대 실적 달성”, 「보도자료」 2026년 1월 7일.

선인경 · 이다은 · 장용석 · 정헌주. 『글로벌 연구 생태계에서의 안보와 자율성 충돌: 해외 사례 분석』 기초연구 2022-07. 세종: 과학기술정책연구원. (2022).

선인경. “G7, ‘디리스킹(de-risking)’ 강조한 연구안보 위험관리방안 제시”. 「과학기술정책 Brief」 Vol. 11 (2023), pp. 1-4.

선인경 · 이다은 · 이동우 · 양현채 · 김은지. 『연구안보에 관한 주요국 정책 비교 분석과 국내 대응 방향 연구』 정책연구 2023-14. 세종: 과학기술정책연구원. (2023).

선인경. “연구안보의 쟁점과 시사점”. 「과학기술정책 Brief」 Vol. 39 (2024), pp. 1-4.

안승진. “[단독] 외국인 연구 인력 3400명…개인정보 · 기술 유출 사고에도 현황 파악 없다”. 『세계일보』 2026년 1월 10일.

오현석. “외국인투자 안보심사제도 개선방안에 관한 제언: 기술안보를 중심으로”. 『국제거래법연구』 제33권 제1호 (2024), pp. 37-66.

이강준 · 박상호 · 박진호, ““돌연 자퇴하고 연락 뚝”…베트남 대학원생, 韓 전기차 핵심기술 빼갔다”. 『머니투데이』 2025년 4월 30일.

이대권 · 김태건 · 박준석. “대학기관의 실태조사를 통한 연구보안 강화방안: 연구보안 규정을 중심으로”/ 『한국산업보안연구』 제14권 3호 (2024), pp. 167-192.

이민정. “G7 오픈사이언스 정책 담론과 시사점”. 「KISTEP 브리프 13」 (2024), pp. 1-3.
이용권. “K - 첨단기술 유출 피해 5년간 23조… 30%가 반도체”. 『문화일보』 2026년 1월 14일.
이현주. “반도체 등 산업기술 유출 피해, 5년간 23조원”. 『뉴시스』 2026년 1월 14일.
임정현. “英 국가안보투자법(NSIA) 관련 지침 개정 발표”. 「수출통제 Issue Report」 No. 43 (2024), pp. 1-5.
임지영. “일본 경제안전보장추진법(안)의 주요 내용과 쟁점”. 「세계 에너지시장 인사이트」 제22-8호 (2022), pp. 1-6.
정제용 · 김학경. “영국의 국가안보법 제정과 그 의미에 관한 고찰: 경제안보 및 산업보안 중심으로”. 『범죄수사학연구』 제10권 제2호 (2024), pp. 179-198.
한국무역협회 무역정책지원실. “최근 외국인투자기업의 수출입 및 주요국의 외국인투자심사 동향”. 「Trade Voice」 Vol. 5 (2025), pp. 1-15.
한소영 · 장항배. “연구보안제도 개선을 위한 비교탐색적 연구: 미국의 연구보안 사례를 중심으로”. 『한국전자거래학회지』 Vol. 27 No. 1 (2022), pp. 111-126.
한정무. “국가연구개발에서의 연구보안 법제 연구”. 단국대학교 박사학위 논문, 2023.
황경준 · 권헌영, “기술유출 형사사건의 처리 실태와 개선 고려사항 논의: 무죄사건을 중심으로”, 『융합보안논문지』 제22권 3호 (2022), pp. 41-55.
특허청. “우리 기술 지킬 ‘4중 안전장치’ 완성, 올해 본격 가동”. 「대한민국 정책 브리핑」 2024년 5월 13일.
e-나라지표. https://www.index.go.kr/
KOTRA. “영국, 외국인투자 심사제도 강화”. 「KOTRA 해외시장뉴스」 2021년 6월 7일.

Robertson, Manjulika E., Samantha M. Chu, Anika Cloutier, Philippe Mongeon, Don A. Driscoll, Tej Heer & Alana R. Westwood. “Interference in Science: Scientists’ Perspectives on Their Ability to Communicate and Conduct Environmental Research in Canada”. *FACETS*. November 30, 2023.
CHIPS and Science Act of 2022.
Christou, Andrea & Chad Damro. “Research Security and the European Union”, *EU-RENEW*, June 13, 2025.
Economic Espionage Act.
EU Commission. “Council Recommendation of 23 May 2024 on Enhancing Research Security”. C/2024/3510, May 30, 2024.
Explanatory Memorandum to the National Security Act 2023. *Prevention and Investigation Measures*. (POLYGRAPH) Regulations 2023. No. 1249.

Federal Bureau of Investigation. https://www.fbi.gov/

Goldsmith University of London. "Economic Espionage, Q&A with Dr Nicola Searle", July 11, 2025.

G7. "Annex to the G7 Science Ministers' Communiqué 2022: Further Implementation and G7 Science Working Groups". 2022.

G7 Security and Integrity of the Global Research Ecosystem(SIGRE) Working Group. "G7 Best Practices for Secure and Open Research Security". May 2023.

NSPM-33 Implementation Guidance (2022/2024)

OECD, "Integrity and Security in the Global Research Ecosystem", OECD Science Technology and Industry Policy Paper, Vol. 130 (2022) pp. 24-29.

OECD. "What Is Research Security and Why Does It Matter for Global Science?". November 21, 2025.

Office of the Director of National Intelligence. https://www.dni.gov/

Research Collaboration Advice Team (UK DSIT), "Foreign Influence Registration Scheme: check if you need to register".

The Foreign Investment and National Security Act of 2007.

The Official Home of UK Legislation. https://www.legislation.gov.uk/

UK Cabinet Office. "National Security and Investment Act: Details of the 17 types of notifiable acquisitions". February 6, 2024.

UK Cabinet Office. "National Security and Investment Act: Guidance for the Higher Education and Research-intensive Sectors". May, 2024.

UK-China Transparency. https://ukctransparency.org/

UK Foreign. Commonwealth & Development Office, "Academic Technology Approval Scheme (ATAS)". November 26, 2025.

UK National Protective Security Authority. https://www.npsa.gov.uk/

UK National Protective Security Authority & National Cyber Security Centre. *Trusted Research Guidance for Academics*. 2025.

UK Research and Innovation. https://www.ukri.org/

Wintour, Patrick. "'Alarming' Chinese meddling at UK universities exposed in report". *The Guardian*. November 5, 2019.

Abstract

Countering Industrial Espionage to Protect National Core Technologies : From the Perpective of Research Security

Bora Park
(Institute for National Security Strategy)

National core technologies refer to technologies whose leakage overseas could significantly harm national security and the development of the national economy. While Korea is currently making efforts to protect its national core technologies, incidents of technology leakage continue to occur. Among the 110 cases of domestic industrial technology leaked overseas in the past five years, 33 involved national core technologies, with the estimated damage amounting to approximately 23 trillion 270 billion Korean won. The ROK government has established the “National Strategic Technology Promotion Plan,” which considers the diplomatic and security aspects of science and technology. It is now working to develop a global-level research cooperation implementation strategy and strengthen the research security system to prevent the leakage of core research assets. However, existing strategies have been largely reactive in nature, and even when addressing the entire research process, they fail to reflect research risks stemming from changing personnel structures in Korean society, such as foreign influence and research interference. Major overseas nations and the international community have solidified discussions on traditional industrial espionage to introduce the concept of research security. They are actively working to block attempts by foreign malicious influence to impact research activities and protect the research ecosystem, alongside physical and human security measures. The case of UK is a prime example of introducing the concept of research security, expanding the discussion of economic security and industrial espionage into national security.

This report examines key UK legislation such as the National Security Act and the National Security and Investment Act, along with dedicated research security agencies and major initiatives, and derives implications for Korea based on the analysis.

Keywords: Industrial Espionage, Industrial Security, Crime of Economic Espionage, Research Security, Foreign Malign Influence/Interference

Institute For National Security Strategy

www.inss.re.kr

INSS 전략보고

March 2026
No. 375

06295 서울시 강남구 언주로 120 인스토피아 빌딩
02-6191-1000 02-6191-1111 www.inss.re.kr

국가안보전략연구원