

국가핵심기술 해외유출 대응 제도개선 토론회

일시 2025. 9. 2. (화) 14:00 ~ 16:00

장소 국회의원회관 제1세미나실

주최/주관 한국형사·법무정책연구원, 국회의원 송재봉·김남근·김기표

후원 산업통상자원부, 특허청

CONTENTS

개회사

- 정웅석 원장 (한국형사·법무정책연구원) 4

인사말

- 송재봉 국회의원 6
- 김남근 국회의원 8
- 김기표 국회의원 10

축사

- 이학영 국회의원 (국회 부의장) 12
- 김원이 국회의원 (산업통상자원중소벤처기업위원회 민주당 간사) 14
- 문신학 1차관 (산업통상자원부) 16
- 목성호 차장 (특허청) 18

발제

- 기술안보의 관점에서의 국가핵심기술 해외유출에 대한
형사정책적 대응 방안 21
- 김유근 선임연구위원 (한국형사·법무정책연구원)

사례발표

- 첨단전략산업 분야 핵심기술 해외유출 수사사례 83
- 김은정 기획수사팀장 (특허청 기술디자인특별사법경찰과)

토론

- 이상홍 실장 (기아 정보보안2실) 93
- 손용하 과장 (산업통상자원부 기술안보과) 95
- 전우정 교수 (한국과학기술원 지식재산대학원) 97
- 심미량 실장 (한국지식재산연구원 법제도연구실) 99



정웅석

한국형사·법무정책연구원 원장

안녕하십니까.

한국형사·법무정책연구원 원장 정웅석입니다.

오늘 「국가핵심기술 해외유출 대응 제도개선 토론회」라는 뜻깊은 자리를 국회의원 송재봉 의원님, 김남근 의원님, 김기표 의원님과 함께 마련하게 되어 더욱 기쁘게 생각합니다.

또한, 이번 토론회의 개최에 축사를 전해주시는 이학영 국회부의장님, 국회의원 김원이 의원님과 산업통상자원부 문신학 1차관님, 특허청 목성호 차장님께도 감사의 말씀을 전하며, 좌장을 맡아주시는 법무법인 율촌의 손승우 상임고문님을 비롯 발표 및 토론자분들과 오늘 이 자리를 함께해 주신 모든 참석자 여러분께 깊은 감사의 말씀을 드립니다.

국가핵심기술은 단순한 산업 자산을 넘어, 우리 경제의 미래와 국가안보의 토대가 되는 소중한 자산입니다.

그러나 기술유출은 갈수록 지능화·다변화되고 있으며, 국제 경쟁이 치열해질수록 그 위험성은 더욱 커지고 있습니다.

이에 따라 우리 연구원은 국회와 관계 기관, 전문가들과 함께 제도적 보완책을 모색하고자 합니다.

오늘 토론회가 형사·법무 정책적 대응과 산업적 보호 장치를 유기적으로 결합하는 출발점이 되기를 기대합니다.

특히, 국가핵심기술의 해외유출을 대응하기 위해서는 산업통상자원부와 특허청을 비롯한 정부 부처, 그리고 학계와 전문가 여러분의 다양한 의견이 모여야 실효성 있는 정책 대안이 마련될 수 있습니다.

오늘 논의된 결과는 반드시 정책 현장에 반영되어, 국민의 신뢰를 지키고 국가 산업경쟁력을 강화하는 밑거름이 될 것입니다.

오늘 이 자리가 국가핵심기술 보호를 위한 제도개선의 중요한 전환점이 되기를 바라며, 바쁘신 와중에도 자리를 빛내주신 내외 귀빈 여러분께 다시 한번, 감사의 말씀을 드립니다.

감사합니다.

2025년 9월 2일

한국형사·법무정책연구원 원장 **정 응 석**



송재봉

더불어민주당 국회의원

〈국가핵심기술 해외유출 대응 제도개선 토론회〉에 참석해주신 여러분, 반갑습니다.

더불어민주당 국회의원 송재봉입니다.

먼저 뜻깊은 자리 마련에 힘을 모아주신 김남근·김기표 국회의원님, 한국형사·법무정책연구원 정웅석 원장님을 비롯한 관계자분께 깊이 감사드립니다. 아울러, 바쁘신 중에서 함께해주신 이학영 국회부의장님, 국회 산업통상자원중소벤처기업위원회 김원이 간사님, 산업통상자원부 문신학 1차관님, 특허청 목성호 차장님께도 진심으로 감사의 말씀을 드립니다.

오늘 우리가 논의할 주제는 대한민국의 산업경쟁력과 미래를 좌우할 국가핵심기술 보호입니다. 반도체, 배터리, 디스플레이 등 첨단산업을 둘러싼 국제 경쟁은 이미 경제안보의 영역으로 확장되고 있습니다. 기술 유출은 단순한 기업의 피해를 넘어 국가 전체의 안보와 미래성장 동력을 위협하는 심각한 사안입니다.

그럼에도 현장에서는 피해 기업이 입증의 어려움과 절차적 한계로 인해 충분히 구제받지 못하는 사례가 적지 않습니다. 「산업기술보호법」, 「국가첨단전략산업법」, 「방산기술보호법」 등 여러 법률이 존재하지만, 체계의 정합성이 미흡해 제도적 공백과 불균형이 여전히 발생하고 있습니다. 이제는 사후적 처벌에 그치는 대응을 넘어, 사전적·예방적 보호 장치를 정비하는 것이 시급합니다.

이번 토론회가 바로 그 대안을 모색하는 뜻깊은 자리가 되기를 기대합니다. 저 역시 국회 산업통상자원중소벤처기업위원회의 일원으로서, 우리 기업들이 안심하고 연구개발에 전념할 수 있도록 관련 법제 개선과 입법적 보완에 최선을 다하겠습니다.

다시 한번 뜻깊은 자리에 함께해주신 모든 분께 감사드리며, 오늘 논의가 우리나라 기술 안보를 한층 더 강화하는 출발점이 되기를 기원합니다.

감사합니다.

2025년 9월 2일

더불어민주당 국회의원 **송재봉**



김남근

더불어민주당 국회의원

안녕하십니까.

국회의원 김남근입니다.

국가핵심기술은 단순한 산업 자산을 넘어, 대한민국의 경제 안보를 지키는 전략적 기반입니다. 그러나 최근 빈번하게 발생하는 기술유출 사건은 기존 제도의 실효성에 큰 의문을 던지고 있습니다. 기술을 지켜내지 못하면 산업 경쟁력은 물론, 국가 안보까지 위협받게 됩니다. 이제는 보다 강력하고 정합적인 대응 체계를 갖춰야 할 때입니다.

기술유출은 날로 지능화되고 있습니다. 외국계 사모펀드의 인수합병, 비식별 수법을 활용한 AI 기반 정보 수집 등 신종 수법이 등장하고 있지만, 제도와 수사는 여전히 뒤따라가는 수준에 머물러 있습니다. 최근 6년간 기술유출 사건 중 절반 이상이 집행유예에 그쳤고, 30%는 무죄 판결을 받았습니다. 유출된 기술의 65%가 중국으로 넘어갔다는 점도 매우 우려스럽습니다.

기술보호는 더 이상 민사 중심의 분쟁 대응에 머물 수 없습니다. 형사정책과 안보전략이 결합된 새로운 국가적 보호체계가 필요합니다. 기술이전, 외국인 투자, 합작법인 등 유출 통로에 대한 선제적 차단은 물론, 외국의 입법 사례에 대한 비교·분석도 본격적으로 추진해야 합니다.

오늘 토론회에서 논의되는 다양한 현장의 목소리와 정책 제안이, 법적 사각지대를 해소하고
실효적인 제도 개선으로 이어질 수 있도록 국회도 최선을 다하겠습니다.

끝으로, 오늘 자리를 마련해주신 한국형사·법무정책연구원 정웅석 원장님과 관계자
여러분께 깊이 감사드립니다. 공동주최를 맡아주신 송재봉 의원님, 김기표 의원님, 그리고
산업통상자원부와 특허청 관계자, 발제와 토론을 맡아주신 전문가 여러분께도 진심으로
감사드립니다.

2025년 9월 2일

더불어민주당 국회의원 **김 남 근**



김기표
더불어민주당 국회의원

안녕하십니까,

더불어민주당 국회의원 김기표(부천시을, 법제사법위원회)입니다.

존경하는 정웅석 한국형사·법무정책연구원 원장님과 관계자 여러분, 그리고 오늘 <국가핵심 기술 해외유출 대응 제도개선 토론회>를 함께 준비해 주신 송재봉 의원님, 김남근 의원님께 깊이 감사드립니다.

또한 참석해 주신 이학영 국회 부의장님, 김원이 의원님, 산업통상자원부·특허청 관계자분들, 그리고 산·학·연 전문가 여러분께도 진심으로 환영과 감사의 말씀을 드립니다.

최근 5년간 산업기술 유출 건수는 100여건에 달하며, 경제적 피해 규모는 약 23조 원에 이릅니다. 수년간, 수백 명의 땀과 노력으로 결실을 맺은 기술이라 할지라도 단 한 번의 유출로 물거품이 됩니다. 기술 탈취 수법은 빠른 속도로 진화하고 있지만, 현행 제도로는 입증 요건이 까다로워 처벌이 어려운 실정입니다. 범죄가 앞서가고 제도는 뒤쫓는 것입니다.

국가핵심기술 해외유출은 개별 기업 손실을 넘어, 국가 경제를 위협하는 중대한 범죄입니다. 국가핵심기술 유출을 철저히 차단하고, 자국 내 산업 기반을 더욱 강력히 다져 대한민국의 기술 주권을 확립해야 합니다.

오늘 토론회에서 논의될 다양한 제안들이 입법과 정책 개선으로 이어져, 국가 핵심기술을 지키고 대한민국을 보호하는 초석이 되기를 기대합니다.

다시 한번 <국가핵심기술 해외유출 대응 제도개선 토론회>에 참석해 주신 모든 분께 감사드리며, 저 역시 법제사법위원회 국회의원으로 국가핵심기술 해외유출 대응 제도 마련에 끊임없이 고민하고 힘쓰겠습니다.

감사합니다.

2025년 9월 2일

더불어민주당 국회의원 **김 기 표**



이학영
국회 부의장

안녕하세요. 국회 부의장 이학영입니다.

「국가핵심기술 해외유출 대응 제도개선」 토론회 개최를 축하드립니다. 뜻깊은 자리를 마련해주신 동료 의원님들과 한국형사·법무정책연구원 그리고 발표와 토론을 맡아 주신 전문가 여러분께 깊은 감사의 말씀드립니다.

국가핵심기술은 단순한 산업 자산이 아니라 대한민국의 미래를 결정하는 전략적 자산입니다. 반도체, 이차전지, 조선, 방위산업, 인공지능 등 한국의 유능한 기술들은 세계에서 주목받는 만큼, 동시에 해외유출의 위협에도 노출되어 있습니다.

특히 인재의 해외 순유출은 심각한 문제로 지적됩니다. 2024년 우리나라 인공지능(AI) 분야 인재가 해외로 빠져나간 규모가 인구 1만 명당 0.36명 수준으로 경제협력개발기구(OECD) 38개국 중 네 번째로 높다고 합니다. △단기 실적 중심의 평가 체계 △연공서열식 보상 시스템 △부족한 연구 인프라 △국제 협력 기회의 부족 등의 구조적 한계가 누적되면서 성과가 뛰어난 인재일수록 한국을 떠나는 안타까운 현실에 직면하고 있습니다.

국가핵심기술을 보호하는 것은 단지 기업의 문제가 아니라, 미래 세대에게 안전하고 지속 가능한 산업환경을 물려주기 위한 우리의 의무이자 책임입니다. 국가핵심기술 해외유출을 막기 위해서는 성과 중심의 보상 체계로의 전환을 강화하고 인재가 다시 유입·순환되는 구조를 마련해야 할 것입니다.

오늘 토론회가 현행 제도의 미비점을 점검하고, 입법적·정책적 보완책을 마련하는 데 중요한 밑거름이 되었으면 좋겠습니다. 다시 한번 토론회 개최를 축하드리며, 참석해 주신 모든 분의 건강과 행복을 기원합니다.

감사합니다.

2025년 9월 2일

국회 부의장 **이 학 영**



김원이

국회 산업통상자원중소벤처기업위원회 여당 간사

반갑습니다.

국회 산업통상자원중소벤처기업위원회 여당 간사이자 더불어민주당 목포시 국회의원 김원이입니다.

먼저 「국가핵심기술 해외유출 대응 제도개선 토론회」 개최를 진심으로 축하드립니다.

뜻깊은 자리를 마련해주신 정웅석 원장님과 연구원 관계자 여러분, 그리고 공동주최를 맡아주신 의원님들께도 감사드립니다.

국가핵심기술은 단순한 산업 자산을 넘어, 우리 경제의 주권이자 국가 안보의 근간입니다. 그러나 기술 탈취와 핵심기술 해외유출은 중소기업과 소상공인의 존립을 위협할 뿐만 아니라, 국가의 미래 성장 동력을 근본적으로 흔드는 심각한 문제입니다.

현행 제도는 피해 기업의 실질적 구제와 예방적 보호에 미흡한 점이 있어, 보다 실효성 있는 제도 개선과 강력한 대응 체계 마련이 절실합니다.

오늘 토론회에서 제시될 전문가 여러분의 고견이 향후 정책과 입법으로 이어져, 현장에서 체감할 수 있는 변화를 만들어 내기를 기대합니다. 저 역시 국회에서 우리 기업과 산업의 경쟁력을 지키고 미래를 준비하기 위해 최선을 다하겠습니다.

다시 한 번 토론회 개최를 축하드리며, 오늘의 논의가 우리 산업 발전과 국가 경쟁력 강화로 이어지길 기원합니다.

감사합니다.

2025년 9월 2일

국회 산업통상자원중소벤처기업위원회 여당 간사 **김 원 이**



문신학

산업통상자원부 1차관

반갑습니다. 먼저 오늘의 토론회를 준비해주신 송재봉 의원님, 김남근 의원님, 김기표 의원님, 한국형사·법무정책연구원 정웅석 원장님께 감사드립니다. 또한, 바쁘신 와중에도 정책 논의를 위해 참석해주신 이학영 국회 부의장님, 김원이 의원님, 그리고 내외빈 여러분들께도 깊은 감사를 드립니다.

우리는 지난 수십년간 기적과도 같은 산업 발전을 이뤄왔습니다. 섬유와 철강, 조선, 자동차 산업을 시작으로 반도체, 이차전지와 같은 첨단산업에 이르기까지 수많은 도전과 변화를 거치며 세계를 주도하는 산업 강국으로 도약했습니다. 이러한 발전은 우리 국민과 기업, 그리고 정부의 노력이 한데 합쳐져 이뤄낸 눈부신 성과입니다. 하지만 이제 우리는 세계화와 자유무역 시대가 이끈 고도성장의 시기를 지나, 기술패권과 보호무역이 새로운 경제질서로 등장하고 각국이 산업의 경쟁력을 확보하기 위해 치열한 전쟁을 벌이는 경제안보 시대에 살고 있습니다. 산업 경쟁력의 핵심이 기술인 상황에서 우리의 기술을 지키는 기술안보가 무엇보다 중요한 시대가 되었습니다. 이러한 상황 속에서 반도체, 이차전지, 자동차, 조선, 바이오, 에너지 등 우리 산업의 첨단 핵심기술은 곧 국가의 전략 자산입니다. 수조원을 들여 개발한 우리 핵심 기술들이 개인의 일탈과 사익 추구로 제3국에 복제 공장이 설립되고, 학술교류와 공동연구라는 포장 아래 우리 기술과 핵심 인재가 외국으로 유출되는 것은 단지 기업과 연구현장의 문제를 넘어 우리 대한민국의 국가 경쟁력에 대한 심각한 위협입니다. 따라서 우리의 기술을 보호하는 것은 국가의 미래와 직결되며 세계와의 기술 경쟁에서 승리하기 위한 범국가적 과제로서 접근하여야 합니다.

정부는 이러한 인식을 바탕으로 산업기술보호법, 국가첨단전략산업법 등 기술보호를 위한 법과 제도를 운영하고 지속적으로 보완해 왔습니다. 하지만 이러한 기술보호 법제들이 기술의 중요도 만큼이나 다양한 형태로 운영되고 있어, 제도 간 정합성에 대한 논의 필요성이 제기되어 온 것도 사실입니다. 우선, 제도별로 보호하는 기술의 수준이 상이하고 보호 방식에도 차이가 있습니다. 그리고 법을 위반했을 시 받을 수 있는 제재나 기술유출범에 대한 처벌 기준도 일부 다르게 설정된 부분이 있어, 유사한 기술유출 범죄라도 적용되는 법률에 따라 처벌의 강도와 방식이 달라지는 경우도 있습니다. 이에 기술 보호 관련 법제 전반에 대한 체계적인 정비와 통합적 접근을 통해 보호제도의 실효성을 높여야 한다는 목소리가 제기되고 있습니다. 오늘 이 자리는 이러한 현장의 목소리를 바탕으로, 기술보호 법제 간의 정합성을 높이고 우리의 핵심기술 유출을 방지하는 기술보호 법제의 목적이 실현될 수 있도록 개선 방안을 모색하는 매우 중요한 자리입니다. 정부는 오늘 토론회에서 제안되는 소중한 의견들을 경청하고, 기술보호 정책과 법제 개선에 적극 활용하겠습니다.

세계 주요국이 각자가 보유한 핵심기술을 지키는 것을 경제안보의 최우선 과제로 생각하고 있습니다. 기술을 잃는다는 것은 단순한 자산의 손실이 아닙니다. 우리가 그동안 기술과 사람으로 세우고, 이룩한 현재의 산업 강국의 지위와 미래의 성장 기회를 함께 잃는 것입니다. 오늘의 이 토론회가 산업 경쟁력의 핵심이자 미래 산업 발전의 제1 동력인 국가핵심기술과 국가첨단전략기술을 더욱 강력하게 보호하기 위한 실질적이고 실행력 있는 대안을 도출하는 뜻깊은 자리가 되리라 믿어 의심치 않습니다. 마지막으로, 오늘 이 자리를 마련해 주신 의원님들과 한국형사·법무정책연구원장님, 그리고 기술안보의 초석을 세우기 위해 귀중한 시간을 내어주신 토론자 여러분께 다시 한번 감사의 말씀을 드립니다.

감사합니다.

2025년 9월 2일

산업통상자원부 1차관 **문 신 학**



목성호
특허청 차장

안녕하십니까? 특허청 차장 목성호입니다.

금일 국가핵심기술 해외유출 대응을 위한 제도개선 토론회를 준비해 주신 송재봉의원님, 김남근의원님, 김기표의원님과 한국형사·법무정책연구원 정웅석 원장님께 감사의 말씀을 올립니다.

국가핵심기술의 해외 유출은 개별 기업의 피해이기도 하지만, 국가적으로도 심각한 피해입니다. 국정원 발표에 따르면 최근 5년간('20~'24) 적발된 산업기술 해외유출 사건 105건 중 국가핵심기술 사건이 32건이며 피해액은 23조원에 이른다고 합니다.

기술유출 수법도 나날이 지능화·고도화 되고 있습니다. 종전에는 국내 기업의 연구 인력에게 외국 기업으로 곧바로 이직을 제안하는 방식이 대부분이었다면, 이제는 외국 기업이 직접 자금을 투입하여 국내 자회사를 설립한 후 주요 연구자를 영입하거나, 미국 등 주요국에 본사를 설립한 후 한국에 지사를 만들어 국내 연구진을 이직시키는 사례 등 마치 국내 기업간 인력이동인 것처럼 보이는 방식이 발견되고 있습니다.

우리나라는 인적자원과 기술력으로 선진국 반열에 올랐습니다. 우리나라 기술력의 총아(寵兒)인 반도체, 디스플레이, 이차전지 및 바이오 분야의 기술들과 관련 연구자들은 우리나라의 미래이자 반드시 지켜야 할 국가의 소중한 자산입니다.

우리나라의 국부인 첨단기술이 해외로 유출되는 것을 막는 일은 정부는 물론 개인과 기업 모두가 함께 경각심을 갖고 적극적으로 대응해야 할 사안입니다.

특허청은 우리의 첨단기술이 해외로 유출되는 것을 방지하기 위한 노력을 지속해 오고 있습니다. 특허청은 정부부처 중 유일하게 박사, 기술사, 변리사 등 1,400명에 이르는 기술 전문가가 근무하고 있으며, 전세계 6억건 이상의 특허 빅데이터를 보유하고 있습니다. 이러한 인적·물적자원을 적극 활용하여 기술유출 사건의 신속하고 정확한 해결을 위해 노력하고 있습니다.

특허청 기술경찰은 2019년에 출범하여 2023년말 기준 전체 지식재산 침해 사건의 27.5% (178건 / 647건)를 담당하고 있으며, 기술경찰의 송치결과와 검찰처분의 일치도는 91.6%에 달하고 있습니다. 지난 7월에는 이차전지분야 첨단전략기술을 해외로 유출하려던 침해 사범을 사전에 검거하여 수조원 이상의 피해를 예방하는 성과도 이루어낸 바 있습니다. 향후에도 지속적으로 기술경찰의 규모를 확대하고, 첨단산업 중심으로 수사를 확대할 예정입니다.

그리고 올해 4월부터는 첨단기술 유출사건을 수사하는 검찰·경찰·무역위 등 유관기관의 기술적 판단에 도움이 되도록 기술자문을 실시하고 있습니다. 현재 경찰과 검찰은 특허청의 기술자문에 대해 높은 만족도를 보이고 있으며, 기술자문은 특허청의 고유 업무로서 자리잡아가고 있습니다.

뿐만 아니라 2021년부터 기술유출 사건에 대한 양형기준을 대폭 강화하기 위해 많은 노력을 경주하였고, 그 결과 지난해 7월부터는 영업비밀 해외유출사범의 최대 형량을 12년까지 부과할 수 있도록 강화한 양형기준이 시행되고 있습니다.

오늘 토론회는 국가핵심기술의 해외유출 방지를 위해 국회 및 정부의 그간의 노력들을 돌아보고, 향후 개선방안을 심도 있게 논의하기 위해 마련된 자리라고 알고 있습니다. 매우 시의적절하고, 매우 의미 있는 자리라고 생각합니다. 오늘 발표를 준비해 주신 한국형사·법무정책연구원 김유근 선임연구위원님과 토론에 참여해 주신 이상홍 실장님, 산업부의 손용하 과장님, 전우정 교수님과 심미랑 박사님께 감사의 말씀을 드립니다.

마지막으로 이번 행사준비를 위해 애써주신 모든 분들에게 다시 한번 감사드립니다.

2025년 9월 2일

특허청 차장 **목성호**

발제

기술안보의 관점에서의 국가핵심기술 해외유출에 대한 형사정책적 대응 방안

– 「산업기술보호법」, 「국가첨단전략산업법」 그리고
「방산기술보호법」의 체계정합성을 중심으로 –

| 김유근 선임연구위원 (한국형사·법무정책연구원)

기술안보의 관점에서의 국가핵심기술 해외유출에 대한 형사정책적 대응방안

- 「산업기술보호법」, 「국가첨단전략산업법」 그리고
「방산기술보호법」의 체계정합성을 중심으로 - *

김유근 **

목 차

- I. 서론
- II. 국가핵심기술의 해외유출·침해에 대한 형사정책적 대응의 현대적 의의
- III. 국가핵심기술 등 해외유출·침해행위의 규정형식의 문제점
 - 1. 개관
 - 2. 「산업기술보호법」상 국가핵심기술과 「국가첨단전략산업법」상 전략기술의 구별의 어려움으로 인한 법적용의 곤란
 - 3. 「산업기술보호법」, 「국가첨단전략산업법」 그리고 「방위기술보호법」의 기술유출·침해행위의 규정 형식의 문제점
- IV. 벌칙규정의 문제점
 - 1. 목적범에서 단순고의범으로의 전환
 - 2. 형벌의 불균형
 - 3. 미수범 및 예비·음모
 - 4. 몰수·추징규정
 - 5. 양벌규정의 문제점
- V. 결론 및 정책제언
 - 1. 결론
 - 2. 정책제언 - 개선안 제시
 - 가. 「산업기술보호법」 개정안
 - 나. 「국가첨단전략산업법」 개정안
- VI. 참고문헌

* 본 발표문은 현재 2025년 한국형사·법무정책연구원에서 수행 중인 『기술안보의 관점에서의 국가핵심기술 해외유출에 대한 형사정책적 대응방안』의 연구보고서의 일부를 그대로 발췌하여 작성된 것임을 밝혀 둔다. 『기술안보의 관점에서의 국가핵심기술 해외유출에 대한 형사정책적 대응방안』의 연구보고서는 2025년 12월 31일 발간예정이다.

** 한국형사·법무정책연구원, 선임연구위원.

I

서론

본 발표는 최근에 지정학적 안보위기에 직면하여 경제안보 또는 산업안보라는 관점에서 집중적인 조명을 받고 있는 국가핵심기술 등의 해외유출·침해에 대한 형사법적 대응과 관련하여 특히 「산업기술의 유출방지 및 보호에 관한 법률」(이하 “산업기술보호법”이라 한다), 「국가첨단전략산업 경쟁력 강화 및 보호에 관한 특별조치법」(이하 “국가첨단전략산업법”이라 한다) 그리고 「방위산업기술 보호법」(이하 “방산기술보호법”이라 한다)의 체계정합성을 중심으로 논의를 진행하고자 한다.

이들 세 법률들은 국가핵심기술, 국가첨단전략기술(이하 “전략기술”이라 한다) 그리고 방산기술의 해외유출·침해행위의 유형을 비롯하여 처벌규정들까지 동일·유사규정들을 공유하고 있어서 어떤 기술의 해외유출·침해사건이 발생하더라도 일관적인 법적용을 가능하도록 해 준다.

그러나 다른 한편으로 동일·유사규정들을 공유하는 법률들의 경우 일방 법률에 대한 일방적인 개정은 타방 법률에 규율의 공백이나 가벌성의 흠결을 발생시킬 수 있다는 문제가 있다. 이것은 일방의 법률에 대한 개정이 다른 법률에 어떤 영향을 미치게 될 것인가에 대한 입법평가가 결여되는 경우에 극명하게 나타난다.

그런데 바로 여기에서 다루게 될 세 법률들에서 이러한 문제를 발견할 수 있다. 즉 2006년 10월 27일 「산업기술보호법」¹⁾이 제정된 후 18년이 지나 2022년 2월 3일에 「국가첨단전략산업법」²⁾이 제정되었는데 동법은 당시 시행되던 「(구)산업기술보호법」³⁾을 참고하여 이에 상응하여 입법된 것으로 추측된다. 그래서 기술 유출·침해의 금지를 정한 「(구)국가첨단전략산업법」 제15조의 유출·침해 행위유형의 규정형식과 열거순서가 「(구)산업기술보호법」 제14조와 유사하며 벌칙규정의 경우에도 「(구)국가첨단전략산업법」 제50조와 「(구)산업기술보호법」 제36조에서의 규정형식과 규정순서가 유사하다. 또한 「방산기술보호법」⁴⁾은 「국가첨단전략산업법」의 제정에 앞서 2015년 12월 29일에 제정되었는데 「(구)방산기술보호법」도 당시 시행되던 「(구)산업기술보호법」⁵⁾의 것을 참고한 것으로 추측되지만 유출·침해행위유형과 관련해서는 매우 간소화된 형태로 규정되었다.

그런데 2025년 1월 21일 「산업기술보호법」이 개정⁶⁾되었음에도 불구하고 이에 상응한 「국가첨단전략산업법」과 「방산기술보호법」의 개정이 이루어지지 않아 특히 기술유출·침해행위의 유형과 형벌

1) 법률 제8062호, 2006.10.27. 제정, 2007.4.28. 시행.

2) 법률 제18813호, 2022.2.3. 제정, 2022.8.4. 시행.

3) 2023년 1월 3일 법률 제19166호에 의하여 개정되기 이전의 것.

4) 법률 제13632호, 2015.12.29. 제정, 2016.6.30. 시행.

5) 2016년 3월 29일 법률 제14108호에 의하여 개정되기 이전의 것.

6) 법률 제20694호, 2025.1.21. 일부개정, 2025.7.22. 시행.

규정에 규율의 공백과 가별성의 흠결이 발생하게 되었다.

본 발표는 이러한 문제점을 분석·검토하여 개선방안을 제시하기 위하여 국가핵심기술 등 해외유출·침해행위의 규정형식의 문제점(III.)을 살펴본 다음 해외유출·침해행위에 상응하는 별칙규정의 문제점(IV.)을 분석하고 검토한 다음 이러한 분석·검토로부터 도출되는 시사점을 개선방안으로 제시하고자 한다(V).

우선 본격적으로 논의에 들어가기에 현재 직면하고 있는 지정학적 안보위기, 특히 경제안보 또는 산업안보라는 관점에서 집중적인 조명을 받고 있는 국가핵심기술 등의 해외유출·침해에 대한 대응의 중요성에 관하여 간략하게 살펴보고자 하는데(II.) 이것은 국가핵심기술 등의 해외유출·침해에 대한 대응의 방향성을 결정해 주는 중요한 단서를 제공해 줄 것이라고 판단된다.

II

국가핵심기술의 해외유출·침해에 대한 형사정책적 대응의 현대적 의의

전통적으로 산업기술 또는 지적 재산권은 민간영역에서의 기업의 영업비밀의 문제로 다루어지면서 민사법의 영역에서 민간재로서의 의미를 가지고 있어서 영업비밀침해는 단순히 기업의 이유창출 침해의 문제로서 재산·경제범죄의 영역으로만 인식되어 왔으며 기껏해야 산업스파이에 대한 형사처벌과 수사기법의 효율화의 문제로서 다루어져 왔던 것이 사실이다.

또한 다른 한편으로 기업의 영업비밀보호에 대한 범국가적 보호정책 혹은 무역보호주의는 민간영역에 대한 국가후견주의로서 그리고 특정 기업 및 산업에 대한 특혜 또는 더 나아가서는 부정부패의 문제나 외국 경쟁기업 혹은 투자자에 대한 불공정한 경쟁으로서 국제분쟁과 외교문제와 연결되어 논의되기도 했다.

그러나 (1) 최근의 지정학적 안보위기와 글로벌 기술패권경쟁(특히 미국·중국 간)은 국가주도적인 “기술통제”의 추세를 심화시키고 있으며⁷⁾ 지금까지의 인식과 국가정책의 패러다임에 대한 근본적인 변화를 요구받고 있다. (2) 또한 새로운 유출·침해유형들이 등장하면서 대응에 어려움을 가중시키고 있다. (3) 이러한 상황 하에서 최근에 급증하고 있는 고부가가치의 산업기술들의 해외유출사건들은 인식의 변화와 국가정책의 패러다임의 변화를 가속화시키고 있는 것이 사실이다. 이러한 상황 하에서 산업기술에 대한 보호는 단순한 민간영역에서의 보안의 강화와 손해배상의 확실성의 보장의 문제에 그치는 것이 아니라 인식 하에 국가의 안전보장 및 국민경제의 발전에 중대한 영향을 미칠 수 있는 산업기술들을 국가주도적으로 국가핵심기술⁸⁾ 혹은 국가첨단전략기술⁹⁾로 규정하여 새로운 경제안보의 영역으로 편입시키고 전통적인 안보개념에 근본적인 변화를 촉발하고 있다. (4) 이러한 새로운 도전에 대하여 우리나라의 기존의 보호법제와 대응체계의 한계가 분명해 지고 있다.

7) 산업기술보호위원회, 『제5차 산업기술의 유출방지 및 보호에 관한 종합계획(‘25~’27)』, 2024.12.31., 1면 (<https://kcg.korea.kr/common/download.do?fileId=198001265&tblKey=GMN>; 최종접속일: 2025년 5월 26일).

8) 「산업기술의 유출방지 및 보호에 관한 법률」 제2조 제2호 “‘국가핵심기술’이라 함은 국내외 시장에서 차지하는 기술적·경제적 가치가 높거나 관련 산업의 성장잠재력이 높아 해외로 유출될 경우에 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 기술로서 제9조의 규정에 따라 지정된 것을 말한다”.

9) 「국가첨단전략산업 경쟁력 강화 및 보호에 관한 특별조치법」 제2조 제1호 “‘국가첨단전략기술’(이하 ‘전략기술’이라 한다)이란 공급망 안정화 등 국가·경제 안보에 미치는 영향 및 수출·고용 등 국민경제적 효과가 크고 연관산업에 미치는 파급효과가 현저한 기술로서 제11조에 따라 지정된 기술을 말한다”.

1. 세계적인 보호주의적 “기술통제”의 추세

최근의 지정학적 안보위기와 글로벌 기술패권경쟁(특히 미국·중국 간)이 촉발시킨 세계적인 국가 주도적 “기술통제”의 추세는 전통적인 민간영역과 공공영역 간의 경계를 모호하게 만들고 국가의 안전보장 및 국민경제의 발전에 중대한 영향을 미칠 수 있는 산업기술들의 보호의 문제는 이제는 민간영역의 경계를 넘어 공공영역으로의 이행을 가속화시키고 있다.

즉 최근 세계정세를 변화시키고 있는 지정학적 안보위기, 예컨대 미·중 기술패권경쟁,¹⁰⁾¹¹⁾ Covid-19 팬데믹¹²⁾ 상황 하에서의 가치사슬(Value Chain)·산업공급망의 교란 및 핵심기술패권을 둘러싼 국제산업스파이의 암약 그리고 2016년 주한미군 THAAD 배치로 인한 한국에 대한 중국의 무역규제와 2019년 (외관상으로는) 우리나라 대법원의 강제징용배상판결로 촉발된 우리나라에 대한 일본의 반도체 소재·부품·장비(소부장)의 수출규제를 통한 우리나라 반도체산업에 대한 견제 등¹³⁾은 개별 기업 또는 특정 산업의 산업기술 또는 지적 재산권이라는 민간재는 더 이상 개별 기업의 이윤창출도구로서 민간영역의 문제(예컨대 영업비밀침해, 특허분쟁 등)에 머무는 것이 아니라 공공재로서 국가의 존립까지도 위협할 수 있는 국가안보¹⁴⁾의 문제와 직결되어 범국가적인 대응방안이 필요하다는 것을 인식시켜준 사건들이라고 볼 수 있으며,¹⁵⁾ 이제 국가핵심기술은 중요한 “외교전략 무기”¹⁶⁾로 부각되고 있다고 말해지기도 한다(민간재의 공공재화).

이러한 가운데 기존의 기술·자원·물류¹⁷⁾의 가치사슬의 상호의존성으로부터의 탈피와 더불어 자국

10) ICT 정보통신 인프라를 제공하는 중국 기업 화웨이에 대한 미국의 경제제재로 촉발된 미·중 기술패권경쟁은 반도체분야 뿐만 아니라 우주항공, 조선 등 다른 산업으로 확대되고 있다. 박성준, “미중 기술패권경쟁과 우리나라의 전략 - 반도체”, 『Futures Brief』, 국회미래연구원, 2023.1., 1면 이하(<https://www.nafi.re.kr/new/report.do?mode=view&articleNo=4134>; 최종접속일: 2025년 6월 3일).

11) 경제와 관련해서는 북태평양지역에서의 경제블록, 즉 중국 주도의 AIIB와 일본 주도의 TPP 간의 경쟁구도를 들 수 있다.

12) 이렇게 본다면 팬데믹은 우리에게 범국가적인 감염병정책과 의료시스템에 대한 변혁을 가져왔을 뿐만 아니라 개별 기업의 기술(백신개발 및 생산기술)은 이제 민간재로서가 아니라 공공재로서의 성격을 강하게 가지도록 함으로써 산업기술의 해외유출방지 및 보호에 대한 패러다임을 근본적으로 변화시키고 새로운 기술패권경쟁이 대두될 수 있는 토대를 만든 사건이라고 볼 수 있다.

13) 그 밖에 이에 더하여 세계의 공장이라고 불리던 중국으로부터의 공급망의 디커플링, 우크라이나-러시아 전쟁으로 인한 군비확충 등은 각국의 방산기술 및 산업기술에 대한 정보전을 치열하게 만듦으로써 제2의 냉정시대의 도래를 암시하고 있다고 평가되고 있다.

14) 예컨대 대만 파운드리 반도체생산기업인 TSMC가 대만-중국의 양안대립 그리고 미국·중국 간 기술패권경쟁의 중심에 있다는 점은 많은 설명을 필요로 하지 않을 것이다.

15) 조용래·김현수·성경모, 『경제안보·기술안보 법제 진단·분석 프레임워크 개발과 적용방안』, STEPI Insight, 제318호(2023.12.20.), 과학기술정책연구원, 1면 이하 (<https://www.stepi.re.kr/site/stepiko/report/View.do?reIdx=328&pageIndex=1&cateCont=A0501&searchYear=&searchCondition=&searchKeyword=&searchSort=>; 최종접속일: 2025년 6월 3일).

16) 조용래·김현수·성경모, 앞의 보고서, 14면.

17) 물류와 관련해서는 우크라이나-러시아 간 전쟁, 이스라엘-하마스 간 전쟁, 후티반군의 홍해 민산상선·군함 공격, 남중국해의 영토분쟁 등이 지정학적 안보위기로 거론됨.

우선주의 및 보호주의의 대두는 기술종속성을 탈피하기 위한 각국의 기술패권주의와 자국우선주의를 더욱 가속화시키고 있으며 이러한 배경 하에서 방산기술을 비롯한 국가핵심기술 및 지적 재산권의 해외유출 및 침해는 국가의 존립을 좌우하는 중요한 요인으로 인식되고 있는 것이 세계적 추세이다.

예컨대 2022년 엔비디아(그래픽카드 칩 및 인공지능 커퓨팅 칩 설계에 특화된 팹리스기업)가 마이크로프로세서, GPU, NPU 등 연산유닛 아키텍처를 설계에 있어서 독보적인 기술을 가진 영국 팹리스 반도체기업인 ARM의 인수를 시도했을 때 영국 정부는 국가핵심기술의 유출 및 안보위협을 이유로 해당 인수·합병을 불허한 사건¹⁸⁾ 국가주도적 기술통제의 단적인 예라고 볼 수 있다.

2. 국가핵심기술의 해외유출의 급증

우리나라에서 산업기술의 해외유출은 이미 오래 전부터 사회적으로 문제가 되어 왔던 것이 사실이며 현재도 진행 중이다. 예컨대 종종 스마트폰, 메모리반도체,¹⁹⁾ LCD·LED 디스플레이²⁰⁾ 그리고 리튬배터리²¹⁾ 등의 영역에서 중국의 기술적 추격을 허용하고 경우에 따라서는 특정 영역의 산업기술은 생산성과 생산효율성의 악화로 해당 산업을 포기할 수밖에 없었던 경험이 있는데 이것은 중국으로의 핵심기술의 유출이 그 원인들 중의 하나로 지목되기도 한다. 또한 이러한 국가핵심기술의 해외유출은 앞서 언급한 반도체나 디스플레이 혹은 리튬배터리 분야에 국한되지 않으며 의료,²²⁾

18) 『ZDNet Korea』 2022년 2월 9일 기사 “48조원짜리 엔비디아 ARM 인수, 왜 불발됐나 [이슈진단+] 반도체 패권 경쟁 속 반발·각국 정부 규제로 불확실성 증폭”
(<https://zdnet.co.kr/view/?no=20220208160541>; 최종접속일: 2024년 3월 20일).

19) 예컨대 『중앙일보』 2025년 3월 13일 보도 “반도체 기술 중국 빼돌려 4조원대 피해…기술유출범 역대 최다 검거”(https://www.joongang.co.kr/article/25320356; 최종접속일: 2025년 6월 20일); 『매일경제』 2025년 5월 25일 보도 “中에 위장회사 세워 韓인재 영입 동료 연구원 20명 통째 빼가기도”
(https://www.mk.co.kr/news/society/11325970; 최종접속일: 2025년 6월 20일).

20) 예컨대 『한겨레』 2023년 7월 23일 보도 “‘곡면 패널’ 기술 중국에 유출한 삼성 협력업체 대표 유죄 확정”
(https://www.hani.co.kr/arti/society/society_general/1099942.html; 최종접속일: 2025년 6월 3일); 『매일경제』 2023년 11월 2일 보도 ““中BOE가 영업비밀 침해” 삼성디스플레이, 美ITC 제소”(https://www.mk.co.kr/news/business/10865043; 최종접속일: 2025년 6월 3일); 『YTN』 2024년 11월 21일 보도 “10년 격차 기술' 중국 유출... 전 삼성디스플레이 연구원 기소”(https://www.ytn.co.kr/_ln/0103_202411212243556879; 최종접속일: 2025년 6월 3일); 『ChosunBiz』 2025년 6월 19일 보도 ““참을만큼 참았다”... 삼성·LG, 中 OLED 특허 침해에 칼 뽑은 이유는”(https://biz.chosun.com/it-science/ict/2025/06/19/KGMKO65KJZFBVLWPM4UXZ25DCQ/; 최종접속일: 2025년 6월 20일).

21) 예컨대 『동아일보』 2024년 8월 21일 보도 ““中서 韓배터리 특허 빼껴도 입증 어려워... LCD처럼 당할 판””(https://www.donga.com/news/Economy/article/all/20240821/126610259/2; 최종접속일: 2025년 6월 20일); 『중앙일보』 2024년 11월 21일 보도 “中 특허 무임승차에 韓 칼 뽑았다... '배터리 특허전쟁' 터질까”(https://www.joongang.co.kr/article/25293657; 최종접속일: 2025년 6월 20일); 『머니투데이』 2025년 6월 11일 보도 “中장성차, 직접 산업스파이 지휘... 'K배터리' 핵심기술 털렸다”(https://news.mt.co.kr/mtview.php?no=2025052814520025000; 최종접속일: 2025년 6월 20일).

22) 『동아일보』 2023년 6월 8일 보도 “한국 근무 中연구원, 의료로봇 기술 1만건 유출”
(https://www.donga.com/news/Society/article/all/20230608/119665869/1#:~:text=%5B%EA%B8%B0%EC%88%A0%20%EC%9C%A0%EC%B6%9C%20%EB%B9%A8%EA%B0%84%EB%B6%88%5D%20

(구)산업부에 따르면 2018년부터 2023년까지 6년간 기술 해외유출은 140건에 이른다고 함. 즉 산업기술이 총 104건 국가핵심기술이 36건이며 모두 반도체관련기술이 가장 많았다고 함.²³⁾ 그러나 법령상 처벌수위가 높음에도 불구하고 유출사건에 대한 법원의 판결은 무죄가 30.3% 그리고 집행유예가 54.5%에 이른다고 한다.²⁴⁾ 또한 유출된 산업기술의 65%가 중국으로 유출된 것으로 파악되고 있다.²⁵⁾

또한 산업통상자원부는 2024년 6월 최근 5년 간(2019년부터 2023년)의 산업기술 유출시태를 발표한 바 있는데 총 96건의 기술유출이 적발되었는데 그 중에서 반도체관련 기술의 유출이 38건 (39.6%)으로 가장 많았으며 디스플레이(16건·16.7%), 자동차(9건·9.4%) 등이 뒤를 이었다고 함.²⁶⁾ 또한 유출된 산업기술 중 국가핵심기술로 지정된 것이 33건으로 전체의 34%를 차지했다고 함.²⁷⁾

이러한 상황에 대하여 산업통상자원부는 현재 외국인이 국내기업을 인수·합병할 경우 인수되는 국내기업만 신고하면 되던 것을 인수하려는 외국인에게도 신고의무를 부과하도록 산업기술보호법을 개정하려고 함.²⁸⁾ 그러나 문제는 이 개정으로 인하여 외국인의 국내투자를 위축시킬 우려가 있다는 점이 지적되고 있다.²⁹⁾

이것은 산업기술의 보호(목적)의 “방식”(수단)이 자칫 경제의 성장동력을 멈추게 할 위험이 있는지에 대한 신중한 검토와 적절한 보호수단에 대한 숙고의 중요성을 알려주는 좋은 예라고 볼 수 있다. 이 문제는 주요 외국 간의 상호주의의 문제와도 연결되어 주요 외국의 정책에 대한 심도있는 검토가 필요함. 또한 이 문제는 외국인 투자의 위축의 문제로만 그치는 것이 아니라 뿐만 아니라 국제적 자유경쟁의 저해로 인한 각종 국제중재재판소나 ISDS 제소, 국제조약 및 협약에 반하는 민간기업에 대한 보조금지급이나 국가조달사업에서의 특혜의 문제 등(비관세장벽)과도 관련됨.

%EA%B5%AD%EB%82%B4%20%EB%8C%80%ED%98%95%EB%B3%91%EC%9B%90%20%EC%97%B0%EA%B5%AC%EC%86%8C%EC%84%9C%20%EC%9D%BC%ED%95%98%EB%A9%B0,%EC%9E%90%EB%A3%8C%201%EB%A7%8C%EC%97%AC%20%EA%B1%B4%EC%9D%84%20%EC%A4%91%EA%B5%AD%EC%9C%BC%EB%A1%9C%20%EC%9C%A0%EC%B6%9C%ED%95%9C%20%ED%98%90%EC%9D%98%EB%A5%BC%20%EB%B0%9B%EB%8A%94; 최종접속일: 2025년 6월 20일).

23) 한국무역협회 『무역뉴스』 2023년 8월 29일 보도 “6년간 기술 해외유출 140건…정부, 연내 처벌강화 등 규제개선” (https://www.kita.net/board/totalTradeNews/totalTradeNewsDetail.do;JSESSIONID_KITA=ECFBD9B7AFC505896FA3CC7E51CC3422.Hyper?no=77735&siteId=1; 2024년 3월 20일). 그 밖에 국정원 기술유출 분석자료에 따르면 『서울경제』 2023년 9월 24일 보도 “20년간 100조…'國富기술' 줄줄 샀다[경제안보 흔드는 산업스파이]”(<https://www.sedaily.com/NewsView/29UT3YHD42>; 최종접속일: 2024년 3월 20일).

24) 앞의 한국무역협회 『무역뉴스』 2023년 8월 29일 보도.

25) 『연합뉴스』 2023년 10월 9일 보도 “해외 유출 산업기술 65% 중국으로…5년여간 225명 검거” (<https://www.yna.co.kr/view/AKR20231008038100004>; 최종접속일: 2023년 3월 20일).

26) 『동아일보』 2024년 2월 7일 보도 “5년간 산업기술 96건 해외 유출, 반도체 38건으로 가장 많아” (<https://www.donga.com/news/Economy/article/all/20240207/123421696/1>; 최종접속일: 2024년 3월 21일); 『연합뉴스』 2024년 2월 6일 보도 “5년간 산업기술 해외 유출 96건 적발…반도체 최다”(<https://www.yna.co.kr/view/MYH20240206010500641>; 최종접속일: 2024년 3월 21일)..

27) 『동아일보』 앞의 2024년 2월 7일 보도.

28) 『동아일보』 앞의 2024년 2월 7일 보도.

29) 『동아일보』 앞의 2024년 2월 7일 보도.

그리고 최근의 국가핵심기술 유출 사례로는 국산 차세대 초음속 스텔스 전투기 KF-21 개발과정에서 공동개발국인 인도네시아 기술자가 한국항공우주국 연구실에서 개발관련 데이터가 담긴 USB를 유출하려고 한 사건이 있었다.³⁰⁾

3. 새로운 유출·침해유형의 등장

국가핵심기술의 유출·침해유형은 종래 내부자에 의한 유출 및 침해가 상당수를 차지했었으며³¹⁾ 이러한 의미에서 종래 민사상 전직·이직·경업금지나 막대한 손해배상 그리고 부정경쟁방지법상 영업 비밀침해나 형법상 배임·횡령에 의하여 대응할 수 있었으며 산업스파이의 문제는 오래전부터 논의되어 오기는 했으나 직접적·인적 스파이행위보다는 오히려 해킹 등 정보통신망 등을 이용한 유출·침해행위가 대부분을 차지하면서 일반적인 컴퓨터범죄의 범주에서 자주 논의되어 온 것이 사실이다.

국내핵심기술의 해외유출·침해와 관련하여 많이 논의되어 왔던 것으로는 예컨대 1) 불법적 수단을 통한 해외유출·침해로서 대표적인 것으로는 무엇보다도 ① 내부자 유출로서 그 목적은 영리나 가해 목적인 경우가 많을 것이다. 또한 계약상 경업금지를 위반한 경우도 생각할 수 있다. ② 그리고 전통적인 산업스파이도 여기에 포함될 것이다.

2) 또한 외부적 합법성을 가장한 해외유출로서 ① 전직·이직 혹은 경업금지 기간이 경과한 후의 경업 또는 헤드헌팅 등 인재유출이 곧 국가핵심기술의 유출이 되는 경우도 생각할 수 있다. ③ 그 밖에 기술수출·이전이나 외국에 합자회사를 설립하면서 이루어지는 기술유출(예컨대 중국의 경우 중국 내 진출하기 위해서는 반드시 중국기업과 합자회사를 설립하여야 함), ④ 타국 정부나 군이 쉽게 개입할 수 있는 사모펀드에 의한 첨단기술 기업의 인수·합병 등이 있다.

3) 그러나 국가핵심기술의 유출·침해유형들은 정교하고 교묘해지고 있고 그 탈취행위의 은밀성은 고도화되고 있을 뿐만 아니라 새로운 유형들이 등장하면서 기존의 보호법제와 대응체계가 새로운 도전에 직면하게 된 것이 사실이다.

예컨대 ① 정부·보안기관·군이 실질적 소유자인 민간기업에 의한 또는 해당 민간기업과의 합자회사 설립 등으로 인한 유출·침해,³²⁾³³⁾ ② 일상화된 그러나 보안위협이 있는 외국 정보통신기기(외국산

30) 『조선일보』 2024년 2월 2일 보도 “USB에 KF-21 자료들이...KAI 파견 인도네시아인들, 기술 빼내다 들통”(https://www.chosun.com/politics/diplomacy-defense/2024/02/02/5J7SK4ZBAVH3BGWYRZM3Q2IA/; 최종접속일: 2024년 3월 21일). 2025년 6월 검찰은 인도네시아 기술자 5명에 대하여 방산기술보호법·방위사업법·대외무역법 위반 혐의에 대해서는 무혐의처분을 그리고 부정경쟁방지법 위반 혐의에 대해서는 기소유예 처분을 내렸다고 한다. 『조선일보』 2025년 6월 4일 보도 “‘한국형 전투기 자료유출’ 인도네시아 기술자, 형사 처분 면했다”(https://www.chosun.com/national/national_general/2025/06/02/5IGNZY5WJZCKPF2E5R2IP6LSUU/; 최종접속일: 2025년 6월 5일).

31) 『자유일보』 2025년 3월 19일 보도 “돈 때문에 승진 떨어져...산업기술 유출 88%가 내부자 소행”(https://www.jayupress.com/news/articleView.html?idxno=38710; 최종접속일: 2025년 6월 20일).

32) 『시사IN』 2014년 3월 14일 보도 “화웨이, ZTE... 진짜 주인은 정부?”(https://www.sisain.co.kr/news/artic

스마트기기, 특히 정부부처·군·방산기업 그리고 민간기업에 설치되어 있는 외국산 CCTV나 인터넷 프로토콜 카메라(IP Camera))의 영상자료의 해외로의 송출 등³⁴⁾의 사용으로 인한 유출·침해(특히 해당 외국에 데이터센터가 설치되어 있는 경우 등),³⁵⁾ ③ 해외에서 원격통제가능한 산업설비를 통한 기술유출,³⁶⁾ ④ 정부기관 또는 군기지 인근의 부동산 매입 등을 통한 산업스파이활동 그리고 ⑤ OpenAI의 소스코드 이용과 관련한 사용이력 감시 및 개인정보 탈취(예컨대 DeepSeek 등) 또는 AI를 활용한 국가핵심기술의 탈취, ⑥ 범용 앱을 통한 빅데이터 수집(예컨대 미국 정부가 공무원의 Tiktok 사용을 중지) 등을 생각할 수 있다. ⑦그 밖에도 자율주행차량의 급속한 보급으로 인하여 자율주행차량에 탑재된 카메라의 영상·위치·지리정보 그리고 LiDAR(Light Detection and Ranging)에 의하여 수집된 지리정보의 해외유출이 문제될 수 있는데 특히 수집된 정보들이 외국 데이터센터에 저장될 경우 해당 데이터센터에 대한 통제가 국내에서는 용이하지 않다는 문제가 있다. 실제로 2021년 중국은 안보문제를 이유로 군·국영회사 임직원들의 자율주행 전기차 테슬라 사용을 제한한 바 있으며,³⁷⁾ 미국도 중국산 전기차에 대하여 안보상 문제를 이유로 규제를 시사한 바 있다.³⁸⁾

leView.html?idxno=19603; 최종접속일: 2025년 6월 20일); 『한겨레』 2020년 6월 26일 보도 “미, 화웨이 등 중 거대기업 20곳 ‘군 소유’ 지정”(https://www.hani.co.kr/arti/international/china/950939.html; 최종접속일: 2025년 6월 20일); 『VOA Korea』 2020년 12월 2일 보도 “미 국방부, 군 통제기업 목록에 중국 회사 4곳 추가”(https://www.voakorea.com/a/world_asia_dod-blacklists-chinese-military-companies/6049413.html; 최종접속일: 2025년 6월 20일).

- 33) 예컨대 중국군이 퇴역 미군조정사를 외국에 소재하는 민간항공학교에 영입한 후 중국 공군조정사의 항공모함 이착륙 교육을 담당하도록 한 사건과 관련해서는 『중앙일보』 2024년 6월 6일 보도 “‘엄청난 돈으로 유혹’…中, 서방 전·현직 조종사 빼내 중국군 훈련”(https://www.joongang.co.kr/article/25254610; 최종접속일: 2025년 6월 20일).
- 34) 『한겨레』 2024년 9월 13일 보도 “최전방에 ‘보안 우려’ 중국산 CCTV …군은 10년간 모르고 있었다”(https://www.hani.co.kr/arti/politics/defense/1158352.html; 최종접속일: 2025년 6월 3일).
- 35) 예컨대 미국 정부가 공무원의 중국산 휴대폰 사용을 제한하거나 미국 및 유럽이 중국 기업인 화웨이의 5G장비 사용을 규제하고 있는 것을 들 수 있다.
- 36) 미국은 조선소에 설치되어 있는 중국산 선적 크레인에 대하여 보안위협 경고한 바 있으며 우리나라 조선소에도 중국산 크레인이 설치되어 있는 것으로 알려져 있다. 『한겨레』 2024년 3월 8일 보도 “미국 항구 크레인에 ‘정체불명’ 통신장비…보안문제 제기 크레인, 중국 업체서 제작된 걸로 확인”(https://www.hani.co.kr/arti/international/america/1131498.html; 최종접속일: 2024년 3월 20일); 『연합뉴스』 2024년 2월 21일 보도 “트로이 목마?…美, 중국산 크레인 등 항만시설 사이버보안 강화”(https://www.yna.co.kr/view/AKR20240221065000071; 최종접속일: 2025년 6월 3일); 『한겨레』 2024년 3월 8일 보도 “미국 항구 크레인에 ‘정체불명’ 통신장비…보안문제 제기크레인, 중국 업체서 제작된 걸로 확인”(https://www.hani.co.kr/arti/international/america/1131498.html; 최종접속일: 2025년 6월 3일).
- 37) 연합뉴스 2021년 3월 20일 보도 “중국, 군·국영회사 임직원들의 테슬라 차 사용제한”(https://www.yna.co.kr/view/AKR20210320004300072; 최종접속일: 2024년 3월 20일).
- 38) 머니투데이 2024년 3월 2일 보도 “‘미국 안보 위협에 처할 것’ 바이든, 중국산 스마트카에 칼 뽑았다”(https://news.mt.co.kr/mtview.php?no=2024030213320480780; 최종접속일: 2024년 3월 20일).

앞서 언급한 국가핵심기술 등의 유출·침해유형들을 간략하게 정리하면 아래와 같다.

1. 불법적 수단을 통한 해외유출·침해

가. 내부자 유출

- 1) 영리목적 또는 가해목적
- 2) 경업 - 해외에 회사설립
- 3) 외국, 외국인(외국단체를 포함)을 “위한” 행위 - 전형적인 내부자에 의한 경제스파이 행위

나. 산업스파이

2. 외부적 합법성을 가장한 해외유출·침해

가. 내부자 유출

- 1) 전직·이직 - 헤드헌팅(군인 포함)
- 2) 경업 - 해외에 외국 회사와의 합자회사 설립

나. 기술수출

다. 국내외 합자회사의 설립

라. 기업의 인수·합병

마. 외국자본(특히 사모펀드)의 국내투자 - 지배구조의 문제 발생

3. 새롭게 대두되고 있는 위협·침해

가. 민간기업 배후에 정부·정보기관·군이 관여하고 있는 경우

- 전통적인 해킹의 범주와는 다른 것으로서 보안위협이 있는 통신기기(스마트폰, 태블릿 등. 예컨대 미국 정부가 공무원의 중국산 휴대폰 사용을 제한하거나 미국 및 유럽이 중국 기업인 화웨이의 5G장비 사용 규제)
- 정부 또는 군이 투자자이거나 실질적인 소유자인 기업이 생산하는 보안장비들 - 예컨대 미국의 화웨이 제재의 주요 원인으로 알려지고 있다

나. 일상화된 수입 정보통신기기의 사용과 국외 데이터센터

- 전통적인 불법감청설비의 사용이나 해킹이 아니라 해외에서 원격조정이 가능한 일상화된 수입 정보통신기기의 사용
- 자율주행차량의 시스템에 저장되는 데이터의 해외 데이터센터에의 송출 - 영상·위치·지리정보의 해외 유출
- 국가기간시설에 설치되어 있는 CCTV(특히 인터넷 프로토콜 카메라(IP Camera))의 영상자료의 해외로의 송출 등
- 드론
최근에 중국인이 군사기지 인근에서 드론을 띄워 군사기지 및 인근지역을 촬영하는 사건이 빈발하자 보호 구역에서 금지 또는 제한행위를 위반한 경우 군사재판을 받을 수 있도록 하는 법률안이 발의되기도 하였다.³⁹⁾
- 범용 앱을 통한 빅데이터 수집(예컨대 미국 정부가 공무원의 Tiktok 사용을 중지) 및 AI 기술의 고도화(중국 DeepSeek의 사용 금지(우리나라 2025년 2월 17일))
- 결제시스템의 협업을 통한 개인정보의 해외유출(2025년 1월 23일 카카오, 애플 등이 중국 알리페이에 4천건 이상의 개인정보 이전함으로써 중국 정부 및 군에 개인정보가 유출될 수 있는 위험을 초래(중국 국가정보법 제7조 제1항 “모든 조직과 공민은 모두 법에 따라 국가정보업무를 지지·협조·호응하여야 하고, 국가정보업무를 통하여 알게 된 비밀을 지켜야 한다”))

다. 해외에서 원격통제가 가능한 산업설비

- 미국은 조선소에 설치되어 있는 중국산 선적 크레인에 대하여 보안위협 경고⁴⁰⁾
- 군 등이 배후에 있는 외국 기업에 의한 원격감시·데이터송출 등의 문제

라. 정부기관 또는 군기지 또는 방산기업, 국가핵심기술 또는 전략기술 대상기관 인근의 부동산 매입

마. 시를 통한 유출·침해

4. 기타

4. 안보개념의 패러다임의 변화

최근의 지정학적 안보위기와 글로벌 기술패권경쟁(특히 미국·중국 간)이 촉발시킨 세계적인 국가 주도적 “기술통제”의 추세 그리고 새로운 국가핵심기술의 유출·침해유형의 등장은 전통적인 안보개념의 패러다임을 근본적으로 변화할 것을 요구받고 있다는 점은 이미 앞서 언급하였다. 즉 현재의 국제정세 및 지정학적 위기를 살펴볼 때 자유진영 또는 서방동맹 혹은 군사동맹이라는 개념은 더 이상 외교관계의 신뢰와 의리에 의하여 규정되지 않고 경제적 이익에 의하여 좌우된다는 점은 부인할 수 없는 사실일 것이다. 그러한 서방진영 간 갈등의 단적인 예가 바로 2025년 미국이 촉발시켰고 현재 진행 중인 중국뿐만 아니라 서방진영을 대상으로 한 관세전쟁⁴¹⁾을 들 수 있을 것이다. 즉 종래 안보개념이 적국이나 반국가단체를 전제로 발전되어 왔고 우리나라에 외교적·군사적으로 적대적인 국가에 대한 개념이었던 것에 대하여 이제는 경제적 이익과 경제 및 산업안보에 위협이 되는 외국, 외국인 외국인단체 개념으로 확대되면서 안보개념은 새로운 패러다임의 변화를 겪게 되었다.

또한 기술통제의 경향은 또 다른 관점, 즉 국가핵심기술의 보호는 경제성장동력이 된다는 점을 반영한 것이라고 말할 수 있다. 즉 “기술혁신이 법·제도의 변화를 촉발시키고, 다시 법·제도가 기술혁신을 촉진하는 선순환으로서 기술혁신-법·제도 간의 ‘공진화(共進化: Co-evolution)’가 형성”⁴²⁾될 수 있다면 그리고 이러한 선순환이 경제성장동력으로서 기능한다면 산업기술혁신의 촉진 및 지원정

39) 2025년 5월 26일 (의안번호: 2210604) 「군형법 일부개정법률안(강대식의원 등 11인)」.

40) 『한겨레신문』 2024년 3월 8일 보도 “미국 항구 크레인에 ‘정체불명’ 통신장비…보안문제 제기 크레인, 중국 업체서 제작된 걸로 확인”(https://www.hani.co.kr/arti/international/america/1131498.html; 최종접속일: 2024년 3월 20일).

41) 그 밖에도 2013년 미국 국토안보국의 전세계적 감시망의 존재를 폭로했던 스노던 사건 참조. *Reuters* June 2, 2025, “How Trump's trade war is upending the global economy”(https://www.reuters.com/business/autos-transportation/how-trumps-chaotic-trade-war-has-evolved-2025-05-12/; 최종접속일: 2025년 6월 3일); 『연합뉴스』 2025년 2월 16일 보도 “[트럼프 스톱 한달] 글로벌 관세전쟁·신평창주의로 국제질서 지각변동”(https://www.yna.co.kr/view/AKR20250215031800071; 최종접속일: 2025년 6월 3일); *Satter, Raphael*, “U.S. court: Mass surveillance program exposed by Snowden was illegal”, in: *Reuter*, September 3, 2020(https://www.reuters.com/article/world/us-court-mass-surveillance-program-exposed-by-snowden-was-illegal-idUSKBN25T3CJ/; 최종접속일: 2025년 6월 3일).

42) 조용래·김현수·성경모, 앞의 보고서, 16면.

외국, 외국인, 외국인단체를 위한 경제스파이까지를 포괄하는 간첩죄를 신설하고 다만 경제스파이에 대해서는 적국이나 반국가단체에 대한 국가기밀의 간첩에 비하여 경한 형량을 규정하고 있다.

물론 국가핵심기술 해외유출 범죄를 형법상 간첩죄로 의율하는 것에 대해서는 많은 문제들이 산재하고 있다. 예컨대 무엇보다도 공안범죄로서의 형법상 간첩죄 자체에 대한 반감을 불식시키기가 쉽지 않다는 점과 경우에 따라서는(특히 계엄 시) 군사재판을 받게 된다는 문제도 해결하여야 할 과제가 된다.

그리고 특정 산업기술 및 지적 재산을 “핵심전략기술”, “국가전략기술”, “국가첨단전략기술”, “국가핵심기술” 등(여기에서는 “국가핵심기술”이라 한다)으로 지정하여 육성과 동시에 제한도 부과되어 기업의 입장에서는 실질적으로 일종의 규제로 인식될 수 있음을 간과해서는 안 되며 경제안보 혹은 산업안보와의 조화를 도모하는 것이 중요한 과제로 남게 된다.

5. 주요 외국 입법례의 변화

주요 외국 입법례를 살펴보면 예컨대 독일과 같이 국가핵심기술의 해외유출·침해범죄를 여전히 영업비밀의 하나로서 다루고 있는 입법례가 있는가하면 예컨대 미국, 영국, 중국 그리고 대만과 같이 민간영역의 일반적인 영업비밀 침해범죄의 범주를 넘어 공안범죄로서의 경제안보범죄로서 다루고 공안범죄 담당 특별수사기관이 수사하는 입법례도 찾아볼 수 있다. 우리나라는 후자에 속하기는 하지만 공안범죄만을 담당하는 특별수사기관이 존재하지 않는다는 점에서 구별된다.

미국의 경우 일반적인 영업비밀을 보호하는 「통일영업비밀법(Uniform Trade Secrets Act)」 외에 1996년에 「경제스파이법(Economic Espionage Act of 1996)」⁴⁵⁾을 제정하여 경제안보범죄로서 경제스파이행위를 규율하고 있다. 또한 2022년 8월에는 「반도체와 과학법(The Chips and Science Act)」 제정되기도 하였다.

영국은 2023년 7월 「국가안전보장법(National Security Act 2023)」을 제정하여 일반적인 영업비밀 침해범죄와 구별되는 외국을 위한 불법한 영업비밀에 대한 스파이활동을 국가안전보장을 해하는 첫 번째 범죄로 규정하였다(Sec. 2).

대만은 일반적인 영업비밀은 「영업비밀법」에 의하여 보호되고 있었으나 중국기업이 허가없이 대만에 회사를 설립하여 반도체 관련 인력을 빼내는 한편 이를 통하여 영업비밀이 유출되는 사건 등이 빈발하자 2019년부터 영업비밀법 등의 개정을 추진하다 2022년 5월 「국가안전법」을 제정하여 경제안전보장의 관점에서 국가안전보장에 관련되는 국가핵심중요기술에 관한 영업비밀의 보호

안번호: 2204555)(2024.10.4.), 구자근 의원안(의안번호: 2204278)(2024.9.25.), 윤상현 의원안(의안번호: 2203041)(2024.8.21.), 인요한 의원안(의안번호: 2202437)(2024.7.31.), 장경태 의원안(의안번호: 2201388)(2024.7.4.) 등을 들 수 있다.

45) 18 U.S.C. §§ 1831.

를 신설하였다(대만 「국가안전법」 제3조).⁴⁶⁾

일본은 본래 국가핵심기술을 영업비밀의 하나로써 다루어 부정경쟁방지법(不正競争防止法)상 영업비밀 침해죄와 형법상 횡령죄로 대응하였으나 경제안보의 중요성이 대두되면서 2024년 5월 10일 「중요경제안보정보의 보호 및 활용에 관한 법률(重要經濟安보情報の保護及び活用に関する法律)」⁴⁷⁾을 제정하여 국가핵심기술을 중요경제안보정보로 다루어 강한 보호를 제공하고 있다. 이러한 경제안보에 대한 인식의 변화는 이미 2022년에 제정된 「경제시책의 통일적 시행에 의한 안전보장의 확보의 추진에 관한 법률(經濟施策を一体的に講ずることによる安全保障の確保の推進に関する法律)」⁴⁸⁾에 나타나 있다.⁴⁹⁾ 또한 「형법전」에 간첩죄가 없는 일본은 2013년 12월 6일 「특정비밀의 보호에 관한 법률(特定秘密の保護に関する法律)」을 제정하여⁵⁰⁾ 각 부처의 장이 지정한 특정비밀의 유출·침해행위를 처벌하고 있는데 이 특정비밀에는 국가핵심기술은 포함되어 있지 않다.⁵¹⁾

중국의 경우 일반적인 영업비밀은 「반부정당경쟁법(中华人民共和国反不正当竞争法)」에 의하여 보호된다. 그런데 2014년에 제정된 「반간첩법(中华人民共和国反间谍法)」은 국가안전보장에 위해를 가하거나 인민의 이익을 해할 수 있는 국가기밀 또는 정보에 대한 간첩행위를 그 적용대상으로 정하고 있다. 그런데 국가안전보장에 위해를 가하거나 인민의 이익을 해할 수 있는 정보는 불확정 개념으로서 어떤 것인가에 관하여 명확히 규정하고 있어서 자의적인 법적용의 위험이 있는 것이 사실이다. 이와 관련하여 중국 「국가안전법(中华人民共和国国家安全法)」의 근본이념인 이른바 “총체적 국가안전관(总体国家安全观)”에 따를 경우 경제안보도 국가안보의 하나가 되기 때문에 경제안보를 해할 수 있는 국가핵심기술의 해외유출·침해범죄에 대해서도 「반간첩법」이 적용될 가능성이 있다고 해석될 수 있다.

이에 대하여 독일의 경우 국가핵심기술의 해외유출·침해범죄를 민간영역의 영업비밀 침해범죄로 다루고 있다. 종래 영업비밀침해범죄는 부정경쟁방지법상 영업비밀침해죄나 형법상 비밀침해죄 혹은 배임·횡령죄로 처벌되었으나 영업비밀 보호 및 공정거래에 관한 유럽연합의회의 지침(2016/943)의 이행입법⁵²⁾으로서 새로운 「영업비밀의 보호에 관한 법률(Gesetz zum Schutz von

46) 이에 관한 상세한 것은 제〇〇장 제〇〇절 “대만” 참조. 그 밖에 湯野基生, “台湾：国家安全法の改正”, 『外国の立法』, No. 296(2023. 6), 国立国会図書館 調査及び立法考査局, 1頁以下(<chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://dl.ndl.go.jp/view/prepareDownload?itemId=info:ndljp/pid/12888736>; 최종접속일: 2025년 5월 3일).

47) 令和六年法律第二十七号, 2024년 5월 10일 제정, 2025년 5월 16일 시행.

48) 令和4年法律第43号, 2022년 5월 11일 제정, 단계적 시행.

49) 동 법률에 관한 상세한 것은 일본 내각부 홈페이지 참조(https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/suishinhou.html; 최종접속일: 2025년 5월 3일).

50) 平成二十五年法律第八号, 2013년 12월 6일 제정, 2014년 12월 10일 시행.

51) 각 행정기관이 지정한 특정비밀에 관한 것은 일본 내각관방장관실 홈페이지 참조(<https://www.cas.go.jp/jp/tokuteihimitsu/nyou.html>; 최종접속일: 2025년 5월 3일).

52) BGBl. 2019 S. 466 ff.(Gesetz zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung

Geschäftsgeheimnissen (GeschGehG))」을 제정하여 통일적으로 영업비밀을 보호하고 있다.⁵³⁾ 다만 「대외경제법」 등 무역 등의 관련법령을 통하여 국가핵심기술의 해외유출에 대응하고 있다.

6. 우리나라의 국가핵심기술에 대한 미흡한 보호법제와 대응

우리나라의 경우 국가핵심기술의 해외유출은 과거 경제안보의 관점에서가 아니라 단순히 기업의 영업비밀 유출·침해 혹은 특허침해라는 재산범죄의 영역의 문제로서 인식되어 왔던 것이 사실이다.

그러나 2004년에 “산업기술의 불법 해외유출이 심각한 수준에 있으나 ‘부정경쟁방지및영업비밀 보호에관한법률’이 민간 기업비밀 누설에만 처벌이 한정되어 있고 각종 법률에 산재해 있는 관련 규정으로는 산업기술유출 방지 및 근절에 큰 효과를 내지 못[하여]” “국가안보에 직접적인 영향을 미치는 국가핵심기술의 해외유출을 규제하고, 산업기술의 부정한 유출을 방지하기 위한 보안의식 확산 및 제도적 기반의 구축을 통해 국내 핵심기술을 보호하고 전문과학·산업 기술인 및 연구개발자를 보호지원하여 국가산업경쟁력을 강화하고 국가의 안전과 국민경제의 안정을 보장”하기 위하여 「산업기술의 유출방지 및 보호에 관한 법률안」이 발의되어⁵⁴⁾ 2006년 10월 27일에 제정되기도 했다.⁵⁵⁾

그러나 이러한 근본적인 패러다임의 전환, 즉 민간영역에서의 기업의 영업비밀 보호의 관점에서부터 경제안보의 관점으로의 전환에도 불구하고 당시 「산업기술의 유출방지 및 보호에 관한 법률」(이하 “산업기술보호법”이라 한다) 제정법률은 ①국가핵심기술의 해외유출을 목적범으로 규정하고 있었을 뿐만 아니라⁵⁶⁾⁵⁷⁾ ②동법에 정한 최고형량은 7년 이하의 징역 또는 7억원 이하의 벌금에 불과하여 국가핵심기술을 영업비밀 침해로서 형법상 배임·횡령 및 「특정경제범죄 가중처벌 등에 관한 법률」(이하 “특정경제범죄법”이라 한다) 제3조에 따라 “특정재산범죄의 가중처벌”하는 경우 이득액에 따라 최고 무기 또는 5년 이상의 징역 그리고 이득액 이하의 벌금에 처할 수 있었던 것에 비하면 매우 경한 법정형이었다.⁵⁸⁾ ③또한 단순유출·침해범에 대한 과실범처벌규정이 존재하지 않는다. 즉 「산업기술보호법」 제36조 제4항은 제3자가 국가핵심기술의 부정취득행위 등(제14조 제1항 및

vom 18. April 2019).

53) BT-Drucksache 19/4724 2019, S. 1 ff.

54) 2004년 11월 9일 「산업기술의 유출방지 및 보호 지원에 관한 법률안(이광재의원등 34인)」(의안번호: 170764).

55) 법률 제8062호, 2006.10.27. 제정, 2007.4.28. 시행.

56) 「산업기술보호법」 제36조 제1항 “산업기술을 외국에서 사용하거나 사용되게 할 목적으로”.

57) 2025년 1월 21일 개정에 의하여 비로소 목적범이 단순고의범으로 개정되었다. “국가핵심기술이 외국에서 사용될 것을 알면서”.

58) 「산업기술보호법」의 법정형(제36조 제1항)은 2008년 3월 14일 개정에 의하여 10년 이하의 징역 또는 10억원 이하의 벌금으로, 2016년 3월 29일 개정에 의하여 15년 이하의 징역 또는 15억원 이하의 벌금으로, 2019년 8월 20일 개정에 의하여 3년 이상의 유기징역 또는 15억원 이하의 벌금으로 그리고 2025년 1월 21일 개정에 의하여 3년 이상의 유기징역 또는 65억원 이하의 벌금으로 상향되었다.

제2항)이 있다는 사실을 중대한 과실로 알지 못하고 그 산업기술을 취득·사용 및 공개하는 행위(제14조(산업기술의 유출 및 침해행위 금지) 제4호를 처벌하고 있으나 정범이 과실로 국가핵심기술을 유출·침해한 경우에 대한 과실범 처벌규정이 존재하지는 않는다. 물론 제정법률 제36조 제1항이 목적범을 그리고 현행 제36조 제1항의 구성요건이 “외국에서 사용될 것을 알면서”라는 고의범만을 규정한 것이어서 어쩔 수 없다고는 하지만 단순유출·침해범을 정한 제정법률 제36조 제2항 및 현행법 동조 제3항의 경우 경제안보 침해범죄라는 중요성을 고려할 때 과실범 처벌규정을 두지 않을 합리적인 이유를 찾아보기는 쉽지 않을 것이다. 참고로 「산업기술보호법」과 유사한 체계를 가지고 있는 「방위산업기술 보호법」(이하 “방산기술보호법”이라 한다)에도 단순유출·침해범에 대한 과실범 처벌규정은 존재하지 않는다. ④그리고 가능한 국가핵심기술의 유출·침해행위를 모두 포괄하고 있는가에 대해서도 의문이다. 예컨대 알선행위를 어떤 유형으로 처벌할 것인가에 대해서도 명문규정이 없어서 형법상 공범이론에 의존할 수밖에 없게 된다.

그리고 「산업기술보호법」상 국가핵심기술들 중 보다 강한 보호의 필요성이 요구되는 국가첨단전략기술의 보호를 위하여 2022년 2월 3일 「국가첨단전략산업 경쟁력 강화 및 보호에 관한 특별조치법」⁵⁹⁾(이하 “국가첨단전략산업법”이라 한다)을 제정하고 「산업기술보호법」의 경우보다 중한 법정형을 규정하고 있으나 「산업기술보호법」상 국가핵심기술보다 강한 보호의 필요성이 요구되는 만큼 「국가첨단전략산업법」상 국가첨단전략기술 해외유출·침해행위에 대한 법정형은 산업기술보호법보다 중하기는 하지만(5년 이상의 유기징역. 이 경우 20억원 이하의 벌금 병과(「국가첨단전략산업법」 제50조 제1항)) 「산업기술보호법」이 예비·음모죄를 처벌하고(동법 제37조) 양벌규정을 두고 있는 것에 반하여(동법 제38조) 「국가첨단전략산업법」에는 이러한 처벌규정들이 존재하지 않는다. 더욱이 「산업기술보호법」이 2025년 1월 21일 15억원 이하의 벌금을 65억원 이하의 벌금으로 상향했음에도 불구하고 「국가첨단전략산업법」의 벌금형은 20억원 이하의 벌금에 머무르고 있어서 병과되는 벌금형과 관련해서는 오히려 「산업기술보호법」의 경우가 더 중한 모순이 발생하게 되었는데 두 법률의 소관부처가 산업통상자원부(산업정책과, 기술안보과)라는 점을 고려할 때 이러한 모순이 소관부처가 상이하여 발생된 문제로 치부하기도 쉽지 않을 것이다. 「국가첨단전략산업법」의 제정으로 인하여 국가핵심기술 개념 외에 국가첨단전략기술 개념이 신설되고 그런 만큼 후자의 보호의 강도가 보다 강해야 한다는 것이 당연한 귀결이라고 한다면 앞서 언급한 모순은 해소되어야 할 것으로 보인다.

그런데 산업기술의 해외유출·침해에 대해서는 해당 산업기술이 국가핵심기술과 국가첨단전략기술인가에 대한 판단기준이 명확한 이상 적용법령을 정하는데 아무런 문제가 발생하지 않을 것으로 생각되지만 문제는 국가핵심기술과 국가첨단전략기술에 적용되는 「산업기술보호법」과 「국가첨단전략산업법」 외에도 경합하는 많은 법령들과 규정들이 산재해 있어서⁶⁰⁾ 기소를 담당하는 검찰의 입장

59) 법률 제18813호, 2022.2.3. 제정, 2022.8.4. 시행.

60) 예컨대 앞서 언급한 형법상 업무상배임·횡령 및 「특정경제범죄법」 외에도 「부정경쟁 방지 및 영업비밀 보호에 관

에서는 입증의 용이성과 법정형의 경중에 따라 적용법조를 찾아야 해서 법적용상 혼란을 초래할 위험이 있다는 점이다. 즉 ① 「산업기술보호법」상 국가핵심기술⁶¹⁾과 「국가첨단전략산업법」상 국가첨단전략기술⁶²⁾인가의 여부, ② 「부정경쟁방지법」상 영업비밀에 해당하는지의 여부 그리고 ③ 행위자가 비밀유지의무자인가의 여부 등에 따라 경합관계가 발생한다.

또한 대응체계와 관련해서도 정책적 컨트롤타워는 각 법률에 정한 각종 위원회가 담당하기는 하지만 실무상 구체적인 수사의 컨트롤타워가 어디에 있는가의 문제도 제기된다.

한 법률」 및 형법상 비밀침해죄를 비롯하여 각종 지적 재산권 보호법(특히 「특허법」, 「지식재산 기본법」 등), 「중소기업기술 보호 지원에 관한 법률」, 「반도체집적회로의 배치설계에 관한 법률」, 「독점규제 및 공정거래에 관한 법률」 등이 있다. 또한 방위산업기술과 관련해서는 「방위산업기술 보호법」, 「방위사업법」, 「군사기밀 보호법」, 「국방과학기술혁신 촉진법」 등이 있다. 그리고 보안과 관련해서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「사이버안보 업무규정」, 형법상 비밀침해죄 등이 있으며 무역통제와 관련해서는 「대외무역법」, 「전략물자 수출입고시」 「외국인투자촉진법」, 「남북교류협력에 관한 법률」, 「원자력법」, 「방위사업법」, 「화학무기·생물무기의 금지와 특정화학물질·생물작용제 등의 제조·수출입 규제 등에 관한 법률」 그리고 「관세법」 등을 들 수 있으며, 범죄수익환수와 관련해서는 「범죄수익은닉의 규제 및 처벌 등에 관한 법률」, 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」, 「관세법」 등이 있다.

61) 「산업기술보호법」 제9조 관련 「국가핵심기술 지정 등에 관한 고시」[별표](산업통상자원부고시 제2024-114호, 2024.7.5. 일부개정, 2024.7.5. 시행).

62) 「국가첨단전략산업법」 제11조 관련 「국가첨단전략기술 지정 등에 관한 고시」[별표](산업통상자원부고시 제 2025-71호, 2025.5.12. 일부개정, 2025.5.18. 시행).

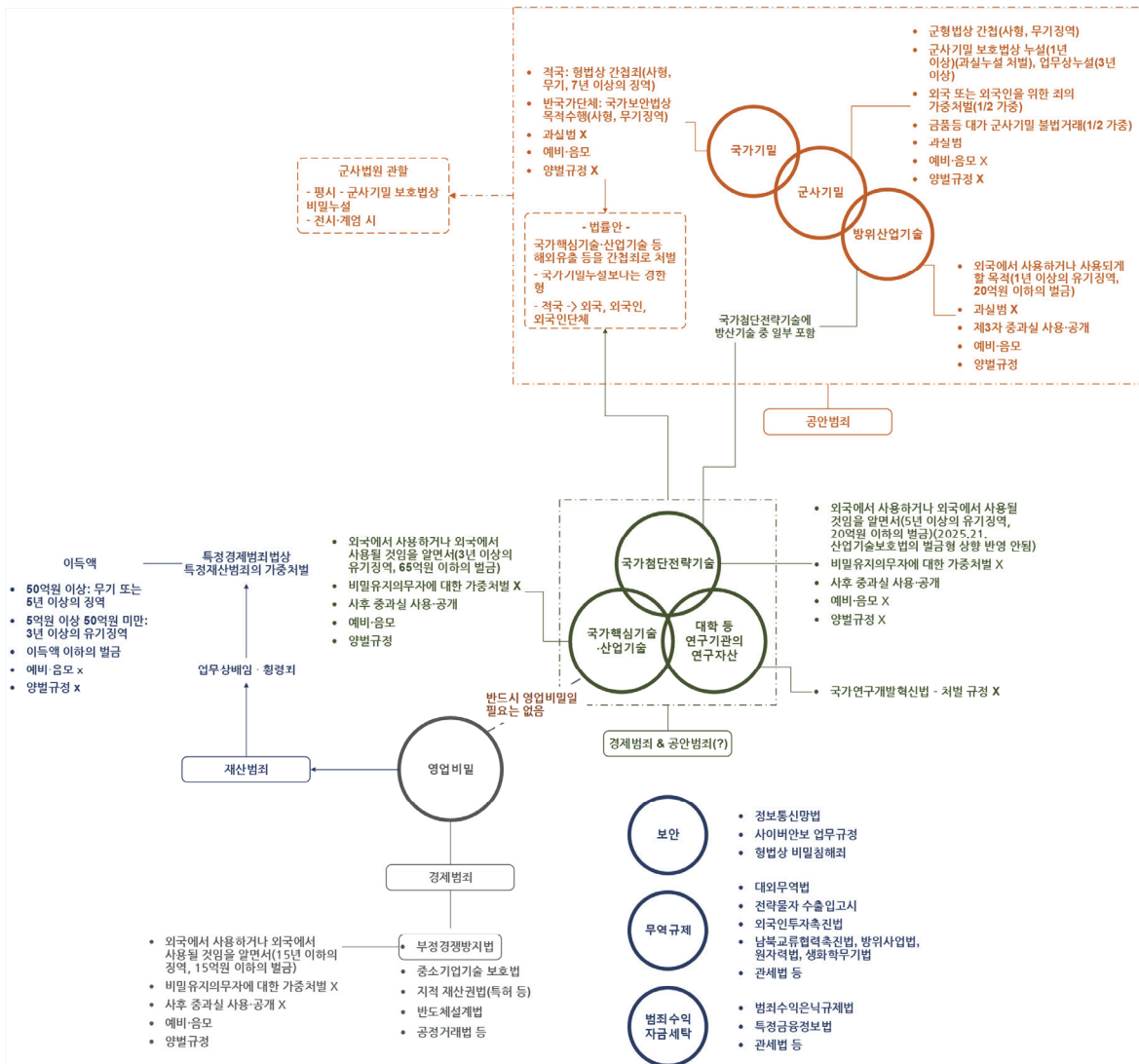
III

국가핵심기술 등 해외유출·침해행위의 규정형식의 문제점

1. 개관

현재 국가핵심기술 등 해외유출·침해에 대응하기 위한 법령체계는 매우 복잡하여 다고 이를 개관하기는 쉽지 않다.

아래의 그림은 본 발표의 대상이 되는 「산업기술보호법」, 「국가첨단전략산업법」 그리고 「방산기술보호법」 외에 국가핵심기술 등 해외유출·침해에 대응하기 위한 법령들의 체계를 간략하게 나타낸 것이다.



[그림 1] 국가핵심기술 해외유출에 대한 형사법적 대응체계

이 그림을 살펴보면 여러 법률들이 그 적용에 있어서 서로 경합하게 되어 법적용자로 하여금 착오를 일으키게 할 정도로 복잡하다는 것을 알 수 있다.

또한 아래의 표는 「부정경쟁방지법」, 「산업기술보호법」, 「국가첨단전략산업법」 그리고 「방산기술보호법」이 어떻게 상호 상응하여 규정되어 있는가를 나타낸 것이며 “〈표 1〉 산업기술 및 국가핵심기술의 유출 및 침해행위에 대한 형사처벌 비교”와 후술하는 “〈표 3〉 「산업기술보호법」, 「국가첨단전략산업법」 그리고 「방산기술보호법」의 기술유출·침해행위 비교”는 앞으로의 논의에서 많이 참조될 것이다.

〈표 1〉 산업기술 및 국가핵심기술의 유출 및 침해행위에 대한 행사차별 비교

내용	「부정경쟁방지법」	「산업기술보호법」	「국가첨단전략산업법」	「방산기술보호법」	비고
보호대상	영업비밀	지정 산업기술 및 국가핵심기술 (산업통상자원부장관) ※ 방산기술 제외	지정 국가첨단전략기술 (산업통상자원부장관) ※ 「산업기술보호법」상 국가핵심기술보다 상위첨단전략기술 - 그러나 벌금형은 「산업기술보호법」보다 경함. ※ 방산기술 포함 「동법 고시」 제3조 별표 ⑥ 방산과 「방산기술보호법」상 고출력 가스터빈엔진시스템 기술 중 고성능 유·무인 항공기용 15,000lb급 이상 첨단 항공 가스터빈엔진만을 포함	지정 방위산업기술 (방위산업청장) ※ 벌금형은 「산업기술보호법」보다 경함. ※ 「동법 고시」 별표 「방위산업기술 목록」 "추진(10개) / 공기출입 추진(3개) / 고출력 가스터빈엔진시스템 기술" 중 「국가첨단전략산업법」이 적용되는 경우가 있음.	- 일분의 경우 각 부처 장관이 지정
유출 및 침해유형 (「산업기술보호법」에 따라 정리)	▶ 제2조제3호 가. 영업비밀의 부정취득·사용·공개 라. 계약 등에 따라 영업비밀 유자의 무자가 보정한 이익 취득 목적 또는 영업비밀 보유자에게 손해를 입힐 목적으로 사용·공개	▶ 제14조 1. 산업기술의 부정취득·사용·공개 2. 계약 등에 따라 비밀유자의무자의 산업기술 유출·사용·공개·제3자로 하여금 사용하도록 하는 행위 ※ 목적으로 규정되어 있던 것(「부정한 이익을 얻거나 그 대상기관에게 손해를 발생시키는 것을 알면서도」)을 삭제 (2025.1.21. 개정)	▶ 제15조 1. 국가첨단전략기술의 부정취득·사용·공개 2. 계약 또는 「산업기술」의 유출방지 및 보호에 관한 법률, 제34조 등에 따른 전략 기술에 대한 비밀유자의무자가 보정한 이익을 얻거나 그 대상기관에 손해를 가할 목적으로 산업기술 유출·사용·공개·제3자로 하여금 사용하도록 하는 행위	▶ 제10조 1. 방산기술의 부정취득·사용·공개	- 결합문제 발생: 국가핵심기술인가 아니면 국가첨단전략기술인가에 따라 그리고 영업비밀에 해당하는지의 여부에 따라
	3. 계약 등에 따른 비밀유자의무자가 보유 또는 사용권한 소멸 후 대상기관으로부터 산업기술에 관한 자료 등의 반환·삭제 요구를 거부·기피 또는 그 사본의 보유	7. 계약 또는 「산업기술」의 유출방지 및 보호에 관한 법률, 제34조 등에 따른 비밀유자의무가 보유 또는 사용 권한 소멸 후 해당 전략기술보유자로부터 전략기술에 관한 자료 등의 반환·삭제 요구를 부정한 이익을 얻거나 그 보유자에 손해를 가할 목적으로 거부 또는 기피·그 사본의 보유(목적법)	4. 계약 등에 따른 비밀유자의무자가 방위산업기술에 대한 보유 또는 사용 권한이 소멸됨에 따라 대상기관으로부터 방위산업기술에 관한 자료 등의 반환·삭제를 요구 받고도 이를 거부 또는 기피하거나 그 사본을 보유하는 행위	- 「방위산업기술보호법」 제10조제5호는 계약 등에 따른 비밀유자의무자가 중대한 과실로 자료 등의 반환 등을 거부한 경우 침해행위로 규정 - 비밀유자의무자 또는 직원 - 형법상 업무상 배임죄(대법원 2009. 10. 15. 선고 2008도9433 판결) ⁶³⁾	

내용	「부정경쟁방지법」	「산업기술보호법」	「국가첨단전략산업법」	「방산기술보호법」	비고
	X	X	X	5. 4호의 행위를 중대한 과실로 행한 경우	
	X	4. 계약 등에 따라 산업기술에 대한 접근 권한이 있는 자가 산업기술을 지정된 장소 밖으로 무단으로 유출·목적 외 사용·공개(2025. 1. 21. 신설) ※ 「부정경쟁방지법」의 경우 침해행위로 정의되어 있지 않으나 형사처벌대상(동법 제18조 제1항제1호 나목(목적범))	X	X	
나. 부정취득 등의 사실을 알거나 조 대한 과실로 알지 못하고 취득·사용·공개		5. 제1호부터 제4호까지의 행위가 개입된 사실을 알고 그 산업기술을 취득·사용·공개하거나 취득 후 그 사실을 알고 그 산업기술을 사용·공개	3. 제1호 또는 제2호에 해당하는 행위가 개입된 사실을 알고 그 전략기술을 취득·사용·공개하거나 취득 후 그 사실을 알고 그 전략기술을 사용하거나 공개하는 행위	2. 부정취득 등의 사실을 알고 방위 산업기술을 취득·사용·공개	
X	X	6. 제1호부터 제4호까지 소개·알선·유인(2025. 1. 21. 신설)(「부정경쟁방지법」에는 없음)	X	X	
		7. 승인없이 또는 부정한 방법으로 승인을 얻어 국가핵심기술을 수출 8. 제11조제4항에 따른 신고를 하지 아니하거나 부정한 방법으로 신고하여 국가핵심기술을 수출하는 행위	5. 승인없이 또는 부정한 방법으로 승인을 받아 전략기술을 수출하는 행위		
		9. 제11조의2(해외인수·합병등)제1항에 따른 승인없이 또는 부정한 방법으로 승인을 받아 해외인수·합병등	6. 전략기술을 외국에서 사용하거나 사용되게 할 목적으로 제13조제1항에 따른 승인없이 또는 부정한 방법으로 승인을 받아 해외인수·합병등(목적범)		
	X	10. 제11조의2제5항 및 제6항에 따른 신고를 하지 아니하거나 부정한 방법으로 신고를 하고서 해외인수·합병등			

내용	「부정경쟁방지법」	「산업기술보호법」	「국가첨단전략산업법」	「방산기술보호법」	비고
<p>나. 부정취득 등의 사실을 알거나 조대한 과실로 알지 못하고 취득·사용·공개</p> <p>다. 영업비밀 취득 후 부정취득행위가 개입된 사실을 알게 되거나 중대한 과실로 알지 못하고 사용·공개</p> <p>마. 영업비밀이 라목에 따라 공개된 사실 또는 그러한 공개행위가 개입된 사실을 알거나 중대한 과실로 알지 못하고 취득·사용·공개</p> <p>바. 영업비밀을 취득 후 그 영업비밀이 라목에 따라 공개된 사실 또는 그러한 공개행위가 개입된 사실을 알거나 중대한 과실로 알지 못하고 사용·공개</p> <p>※ 직접 부정취득행위(가, 라목)를 행하지 않았다고 하더라도 (1) 그 사실을 알고 해당 영업비밀을 사용·공개하거나 (2) 중대한 과실로 그 사실을 알지 못한 경우에 침해행위(나, 다, 마, 바목)</p> <p>- 타인의 영업비밀 훼손 등(제9조의8) - 비밀유지명령 위반(제14조의4)</p>	<p>제11조제6항·제8항(국가핵심기술의 수출금지·수출금지·원상회복 등의 조치) 및 제11조제2제8항·제10항(해외인수·합병 등에 대하여 중지·금지·원상회복)에 따른 산업통상자원부장관의 명령을 이행하지 아니하는 행위</p> <p>12. 산업기술 관련 소송 등 대통령령으로 정하는 적법한 경로를 통하여 산업기술이 포함된 정보를 제공받은 자가 정보를 제공받은 목적 외의 다른 용도로 사용·공개</p> <p>13. 제1호부터 제4호까지에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 그 산업기술을 취득·사용 및 공개하거나 산업기술을 취득 후 그 산업기술에 대하여 제1호부터 제4호까지에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 그 산업기술을 사용·공개</p>	<p>제11조제6항·제8항(국가핵심기술의 수출금지·수출금지·원상회복 등의 조치) 및 제11조제2제8항·제10항(해외인수·합병 등에 대하여 중지·금지·원상회복)에 따른 산업통상자원부장관의 명령을 이행하지 아니하는 행위</p> <p>12. 산업기술 관련 소송 등 대통령령으로 정하는 적법한 경로를 통하여 산업기술이 포함된 정보를 제공받은 자가 정보를 제공받은 목적 외의 다른 용도로 사용·공개</p> <p>13. 제1호부터 제4호까지에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 그 산업기술을 취득·사용 및 공개하거나 산업기술을 취득 후 그 산업기술에 대하여 제1호부터 제4호까지에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 그 산업기술을 사용·공개</p>	<p>8. 전략기술 관련 소송 등 대통령령으로 정하는 적법한 경로를 통하여 전략기술이 포함된 정보를 제공받은 자가 정보를 제공받은 목적 외의 용도로 그 정보를 사용하거나 공개하는 행위</p> <p>4. 제1호 또는 제2호에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 그 전략기술을 취득·사용·공개하거나 전략기술을 취득 후 그 전략기술에 대하여 제1호 또는 제2호에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 그 전략기술을 사용·공개</p>	<p>3. 부정취득 등의 사실을 중대한 과실로 알지 못하고 방위산업기술을 취득·사용·공개</p>	

내용	「부정경쟁방지법」	「산업기술보호법」	「국가첨단전략산업법」	「방산기술보호법」	비고
일선	<p>X</p> <p>(공범관계의 경우만 형사처벌)</p>	<p>O</p> <p>(제14조제6호)</p>	<p>X</p> <p>(공범관계의 경우만 형사처벌)</p>	<p>X</p> <p>(공범관계의 경우만 형사처벌)</p>	
<p>형벌</p>	<p>▶ 제18조</p> <p>① “영업비밀을 외국에서 사용하거나 외국에서 사용될 것임을 알면서” - 15년 이하의 징역 15억원 이하의 벌금(재산상 이득액의 10배에 해당하는 금액이 15억원을 초과하는 경우 그 재산상 이득액의 2배 이상 10배 이하의 벌금)(2019.1.8. 개정)</p> <p>1. 부정한 이익을 얻거나 영업비밀 보유자에게 손해를 입힐 목적으로(목적범) 영업비밀을 취득·사용·제3자가 영업비밀을 지정된 장소 밖으로 무단 유출</p> <p>다. 영업비밀 보유자로부터 영업비밀의 식재·반환을 요구받 고도 이를 계속 보유</p> <p>2. 절취·기망·협박, 그 밖의 부정 한 수단으로 영업비밀 취득</p> <p>3. 제1호 또는 제2호에 해당하는 행위가 개입된 사실을 알면서도 그 영업비밀을 취득·사용</p>	<p>▶ 제36조</p> <p>① 국가핵심기술이 외국에서 사용될 것 을 알면서 제14조제1호부터 제12호의 어느 하나에 해당하는 행위를 한 경우 - 3년 이상의 유기징역 그리고 65억원 이하의 벌금 병과(2019.8.20. 신설, 2025.1.21. 시행)</p> <p>② 산업기술이 외국에서 사용될 것을 알 면서 제14조제1호부터 제6호까지 및 제12호의 어느 하나에 해당하는 행위 를 한 경우(제1항에 해당하는 행위를 한 자는 제외) - 15년 이하의 징역 또 는 30억원 이하의 벌금 또는 병과</p>	<p>▶ 제50조</p> <p>① 전략기술을 외국에서 사용하거나 사용 되게 할 목적으로 제15조제1호부터 제 3호까지의 어느 하나에 해당하는 행위 를 한 경우(목적범) - 5년 이상의 유기징 역(단독형), 20억원 이하의 벌금 병과</p> <p>② 전략기술을 외국에서 사용하거나 사용 되게 할 목적으로 제15조제5호부터 제 8호까지의 어느 하나에 해당하는 행위 를 한 경우(목적범) - 20년 이하의 징역 또는 20억원 이하의 벌금</p> <p>※ 그러나 제15조제6호가 “외국에서 사용하거나 사용되게 할 목적”을 규정하고 있는데 동 목적은 제50조제2항과 관련해서는 중복 적 표기.</p>	<p>▶ 제21조</p> <p>① 방위산업기술을 외국에서 사용하거나 사용되게 할 목적으로 제10조 제1호, 제2호 및 제4호에 해당 하는 행위를 한 경우(목적범) - 1년 이상의 유기징역(단독형), 20억원 이하의 벌금 병과</p> <p>※ 「군사기밀 보호법」 제15조(외국 또는 외국인에 의한 죄에 관한 가중처벌) - 1/2 가중</p>	<p>- 목적범을 인식범으로 개정</p> <ul style="list-style-type: none"> 「산업기술보호법」: 2025.1.21. (제36조제1항 및 제2항: “사용하거나 사용 되게 할 목적으로” → “사용될 것을 알 면서”) 「부정경쟁방지법」: 2019.1.8. 64(규) 제18조 제1항 본문 및 제2항) <p>- 정역형 및 벌금(징벌 적 배상) 상향</p> <ul style="list-style-type: none"> 「부정경쟁방지법」 - 2019.1.8. 개정 (10년 이하의 징역 또는 1억원 이하의 벌금 → 15년 이하 의 징역 또는 15억 원 이하의 벌금; 재 산상 이득액의 10 배에 해당하는 금액 이 15억원을 초과 하면 그 재산상 이 득액의 2배 이상 10 배 이하의 벌금) 「산업기술보호법」 <ul style="list-style-type: none"> 2019. 8. 20. 개 정: 정역형 상향 (15년 이하 → 3년 이상의 유기) <ul style="list-style-type: none"> 2025.1.21. 개 정: 벌금 상향(15억원 이하 → 65억원 이하)

내용	「부정경쟁방지법」	「산업기술포호법」	「국가첨단전략산업법」	「방산기술포호법」	비고
	유자에게 손해를 입힐 목적으로 타인의 영업비밀을 훼손·멸실·변경(목적범) - 10년 이하의 징역 또는 5억원 이하의 벌금(2024.2.20. 신설)	③제14조제1호부터 제11호까지의 어느 하나에 해당하는 행위를 한 경우 - 10년 이하의 징역 또는 10억원 이하의 벌금 또는 병과 ④제14조제12호 및 제13호의 어느 하나에 해당하는 행위를 한 경우 3년 이하의 징역 또는 3억원 이하의 벌금 또는 병과	③제15조 각 호(제4호·제6호 및 제8호는 제외한다)의 어느 하나에 해당하는 행위를 한 경우 - 15년 이하의 징역 또는 15억원 이하의 벌금 ④제15조제4호 또는 제8호에 해당하는 행위를 한 경우 - 5년 이하의 징역 또는 5억원 이하의 벌금	②제10조제1호·제2호 및 제4호에 해당하는 행위를 한 경우 - 10년 이하의 징역 또는 10억원 이하의 벌금 ③제10조제3호 및 제5호(종과실 법)에 해당하는 경우 - 5년 이하의 징역 또는 5억원 이하의 벌금	역원 이하) 「부정경쟁방지법」, 「산업기술포호법」 - 일반인과 계약 등 영업비밀 유지의무자간에 형벌의 차이가 없음. - 비밀유지의무자 또는 직원의 경우 → 형법상 업무상배임죄 → 「특정경제범죄법」 제3조 제1항에 따라 • 이득액이 5억원 이상 50억원 미만일 때 무기 또는 5년 이상의 징역 • 5억원 미만 - 3년 이상의 유기징역 • 제14조(일정 기간의 취업제한 및 인가·허가 금지 등)
	※ 「부정경쟁방지법」 제9조의8(영업비밀 훼손 등의 금지)(2024.2.20. 신설) 위반(단순 영업비밀훼손 등)은 불가벌(제18조 제3항) - 타인의 영업비밀 훼손 등 - 형법상 비밀침해죄 적용 - 비밀유지 의무자에 의한 영업비밀 훼손 등 - 형법상 업무상배임죄(대법원 2009.10.15. 선고 2008도9433 판결)	③ 제36조의2 - 비밀유지명령 위반죄(친고죄) - 5년 이하의 징역 또는 5천만원 이하의 벌금			
적용범위(외국에서의 행위)	▶ 제18조의4 - 비밀유지명령 위반죄(친고죄) - 5년 이하의 징역 또는 5천만원 이하의 벌금 - 내국인의 국외범 O(「형법」 제3조) - 외국인의 국외범 X(제5조) - 대한민국과 대한민국 국민에 대한 국외범 O(제6조)	- 외국에서의 행위에 대한 적용(제14조의4)(2025.1.21., 2025.7.22. 시행) - 형법 적용	- 형법 적용	- 형법 적용	
벌금의 병과	선택적 (제18조제6항)	필요적(제36조제1항) ·선택적(제36조제8항)	필요적(제50조제1항) ·그 외의 경우 병과규정 X	O (제21조제7항)	

내용	「부정경쟁방지법」	「산업기술포호법」	「국가첨단전략산업법」	「방산기술포호법」	비고
물수 「범죄수익은닉 규제법」 적용여부	물건 또는 그 행위로부터 생긴 물건 (제18조의5)(2024.2.20. 신설) ※장발적인지 이득발적인지 불명확	이득재산의 물수 (제36조제5항)	x	이득재산의 물수 (제21조제5항)	「범죄수익은닉규제법」 제2조제1호 가목(사형 무기 또는 장기 3년 이상의 징역이나 금고에 해당하는 죄)(2022.1.4. 개정) ⁶⁵⁾
미수	제18조 제1항 및 제2항(제18조의2) - 제외 • 과실범의 미수범 포함: 중대한 과 실로 침해·유출행위가 개입된 사 실을 알지 못하고 사용·공개의 미수범 처벌 • 부정한 이익을 얻거나 영업비밀 보유자에게 손해를 입힐 목적으 로 영업비밀 훼손·멸실·변경(제 18조제3항)의 미수범 불가벌 - 제18조제3항은 2024년 2월 23 일 신설되었음에도 미수범 처벌 규정은 개정되지 못함.	제36조제7항 - 제외 • 과실범의 미수범 제외: 중대한 과 실로 침해·유출행위가 개입된 사 실을 알지 못하고 사용·공개(제14 조제13호) 불가벌 • 적법한 경로를 통하여 산업기술이 포함된 정보를 제공받은 자가 정보 를 제공받은 목적 외 사용·공개(제 14조제12호)의 미수범 불가벌	x	제21조제6항 - 제외 • 과실범(제10조제3호·제5호) 의 미수범 제외(제21조제6항)	
예비·음모	제18조의3 - 미수범의 적용범위와 동일 - 제18조 제1항 - 3년 이하의 징역 또는 3천만원 이하의 벌금 - 제18조 제2항 - 2년 이하의 징역 또는 2천만원 이하의 벌금	미수범의 적용범위와 동일 - 3년 이 하의 징역 또는 3천만원 이하의 벌금	x	제22조 - 미수범의 적용범위와 동일 - 제21조제1항 - 5년 이하의 징 역 또는 5천만원 이하의 벌금 - 제21조제2항 - 3년 이하의 징 역 또는 3천만원 이하의 벌금	

내용	「부정경쟁방지법」	「산업기술포호법」	「국가첨단전략산업법」	「방산기술포호법」	비고
과실유출 증과실	X X - 영업비밀 침해행위에는 선의취득자의 중과실을 포함시키고 있으나 형사처벌규정 없음. - 다만 제13조제2항이 "제1항에서 "영업비밀을 정당하게 취득한 자"란 제2조제3호다목 또는 바목에서 영업비밀을 취득할 당시에 그 영업비밀이 부정하게 공개된 사실 또는 영업비밀의 부정취득행위나 부정공개행위가 개입된 사실을 중대한 과실 없이 알지 못하고 그 영업비밀을 취득한 자를 말한다"고 규정하고 있음	X O - 부정취득 등 행위가 개입된 사실을 중대한 과실로 알지 못하고(제36조 제4항)	X O - 부정취득 등 행위가 개입된 사실 중대한 과실로 알지 못하고(제15조제4호)	X O - 부정취득 등 행위가 개입된 사실을 중대한 과실로 알지 못하고(제10조제3호) - 계약 등에 따른 비밀의무자가 중대한 과실로 반환·삭제 등 거부·기피·보유(제10조제13호)	
양벌규정	제19조 (법인: 본조의 벌금형의 3배 자연인: 본조의 벌금형)	제38조 (법인·자연인: 본조의 벌금형)	X	제23조 (법인·자연인: 본조의 벌금형)	
범인에 대한 공소시 효 특례	제18조 제1항 및 제2항의 경우 범인의 공소시효 10년	X	X	X	

- 63) 대법원 2009.10.15. 선고 2008도9433 판결: "회사 직원이 영업비밀을 경쟁업체에 유출하거나 스스로의 이익을 위하여 이용할 목적으로 무단으로 반출하였다면 그 반출 시에 업무상배임죄의 기수가 되고, 영업비밀이 아니더라도 그 자료가 불특정 다수의 사람에게 공개되지 않았고 사용자가 상당한 시간, 노력 및 비용을 들여 제작한 영업상 주요한 자산인 경우에도 그 자료의 반출행위는 업무상배임죄를 구성하며, 회사 직원이 영업비밀이나 영업상 주요한 자산인 자료를 적법하게 반출하여 그 반출행위가 업무상 배임죄에 해당하지 않는 경우라도 퇴사시에 그 영업비밀 등을 회사에 반환하거나 폐기할 의무가 있음에도 경쟁업체에 유출하거나 스스로의 이익을 위하여 이용할 목적으로 이를 반환하거나 폐기하지 아니하였다면, 이러한 행위는 업무상배임죄에 해당한다(대법원 2008.4.24. 선고 2006도9089 판결)". 그 밖에 대법원 2017.6.29. 선고 2017도 3808 판결; 대법원 2019.9.10. 선고 2016도1241 판결.
- 64) 법률 제16204호, 2019.1.8. 일부개정, 2019.7.9. 시행.
- 65) 법률 제18672호, 2022.1.4. 일부개정, 2022.1.4. 시행.

2. 「산업기술보호법」상 국가핵심기술과 「국가첨단전략산업법」상 전략기술의 구별의 어려움으로 인한 법적용의 곤란

「산업기술보호법」상 국가핵심기술과 「국가첨단전략산업법」상 전략기술은 그 고도의 전문성으로 인하여 일반인 그리고 법적용자가 구별하는 것은 그리 쉬운 것은 아니다. 그러나 이러한 불가피성을 감안하더라도⁶⁶⁾ 양 기술은 경우에 따라서는 동일한 것이 지정되어 있어서 서로 구별되지 않음으로써 애초부터 법적용 자체가 가능하지 않은 경우가 있다.

아래의 표는 국가핵심기술 지정 등에 관한 고시⁶⁷⁾ 별표에 지정된 국가핵심기술(법 제9조 관련)과 「국가첨단전략기술 지정 등에 관한 고시」⁶⁸⁾ 별표에 지정된 국가핵심기술(법 제9조 관련) 중 상호 동일한 것이 지정된 경우를 나타낸 것이다.

〈표 2〉 국가핵심기술과 국가첨단전략기술의 중복적 지정

구분	국가핵심기술 「국가핵심기술 지정 등에 관한 고시」 별표 (법 제9조 관련)	국가첨단전략기술(전략기술) 「국가첨단전략기술 지정 등에 관한 고시」 별표 (법 제11조 관련)
반도체	시스템반도체용 첨단 패키지 (FO-WLP, FO-PLP, FO-PoP 등) 조립·검사 기술	시스템반도체용 첨단 패키지에 해당하는 FO-WLP, FO-PLP, FO-PoP, SiP 등 공정조립·검사기술
	디스플레이 패널 구동을 위한 OLED용 DDI(Display Driver IC) 설계기술	디스플레이 패널 구동을 위한 OLED용 DDI(Display Driver IC) 설계 기술
전기·전자·이차전지	리튬이차전지 Ni 함량 80% 초과 양극소재(전구체 포함) 설계, 제조 및 공정기술	리튬이차전지 고용량 양극소재 설계, 제조 및 공정기술(니켈함량 80% 초과)
	차세대 리튬 이차전지(600mAh/g 이상의 초고성능 전극 포함) 설계, 공정, 제조 및 평가기술	600mAh/g 이상 초고성능 전극(실리콘그래파이트 복합 음극, 황 양극, 리튬금속 음극) 또는 ----- 설계, 공정, 제조 및 평가기술
방산	x	유·무인기용 15,000lbf급 이상 첨단 항공엔진 핵심 소재 및 부품 기술

이 표를 살펴보면 알 수 있듯이 국가핵심기술로도 그리고 국가첨단전략기술(전략기술)로도 지정된 것이 4개나 있다. 즉 이들 기술들은 국가핵심기술로서 「산업기술보호법」의 적용대상이 되거나 혹은 「국가첨단전략산업법」의 적용대상이 된다.

그런데 문제는 어떤 기술이 국가핵심기술인지 아니면 전략기술인지에 따라 그 유출·침해에 대하여 적용되는 벌칙규정과 형벌이 상이하게 된다는 데에 있다. 보다 큰 문제는 산업통상자원부장관이 동일한 기술을 국가핵심기술로 지정할 것인지 아니면 전략기술로 지정할 것인지는 지극히 임의적인

66) 이에 관한 평석으로는 선종수, “산업기술유출의 개념과 형사책임 - 헌법재판소 2013.7.25. 자 2011헌바39 결정 -”, 『과학기술법연구』, 제20권 제2호(2014), 78면 이하; 하지현·이현희, “산업기술유출 사건에서 산업기술의 개념과 형사책임에 관한 소고-2011헌바39 결정을 중심으로-”, 『법학논총』, 제37권 제4호(2013), 단국대학교 법학연구소, 521면 이하; 신알찬·권솔, “한국 산업의 기술유출 방지를 위한 현행 법제 검토 및 개선방안에 대한 고찰- 형사적 규제 확대를 중심으로 -”, 『한국산업보안연구』, 제5권 제1호(2015), 한국산업보안연구학회, 29면 이하. 그 밖에 김정환, 앞의 논문, 51면 이하.

것이 되는데 그렇다면 유출·침해행위의 가별성이 산업통상자원부장관의 임의적인 지정에 의하여 결정되어 벌칙에서의 가별성을 결정하는 핵심적인 내용인 기술의 종류 자체가 명확성을 결여하게 됨으로써 법적용의 확실성을 저해하여 법적 안정성을 심각하게 저해하게 된다.

그리고 위의 표와 같이 하나의 기술이 국가핵심기술로도 그리고 전략기술로도 지정된 경우에는 어떤 법률을 적용할 것인가와 관련하여 혼란을 초래하게 된다. 여기에서 법적용자의 자의적인 선택적 법적용의 문제가 발생하게 된다.

3. 「산업기술보호법」, 「국가첨단전략산업법」 그리고 「방위기술보호법」의 기술유출·침해행위의 규정형식의 문제점

가. 개요

법적용을 어렵게 만드는 것은 무엇보다도 산업기술 등 유출·침해행위에 대한 처벌규정들이 여러 법률에 산재해 있을 뿐만 아니라 바로 그로 인하여 법령들 간 동일·유사규정들 간에 상응성이 결여되어 전체 법체계에서의 체계정합성까지도 해치고 있다는 점에 있다.

특히 문제가 되는 것은 이른바 3대 기술보호법이라고 말할 수 있는 「산업기술보호법」, 「국가첨단전략산업법」 그리고 「방산기술보호법」 간의 관계이다.

우선 2006년 10월 27일 「산업기술보호법」⁶⁷⁾이 제정된 후 18년이 지나 2022년 2월 3일에 「국가첨단전략산업법」⁶⁸⁾이 제정되었는데 동법은 당시 시행되던 「(구)산업기술보호법」⁶⁹⁾을 참고하여 이에 상응하여 입법된 것으로 추측된다. 이것은 아래의 표를 살펴보듯이 기술 유출·침해의 금지를 정한 「(구)국가첨단전략산업법」 제15조의 유출·침해행위유형의 규정형식과 열거순서가 「(구)산업기술보호법」 제14조와 유사하다는 점 그리고 벌칙규정의 경우에도 「(구)국가첨단전략산업법」 제50조와 「(구)산업기술보호법」 제36조에서의 규정형식과 규정순서가 유사하다는 점에서도 쉽게 알 수 있다.

또한 「방산기술보호법」⁷⁰⁾은 「국가첨단전략산업법」의 제정에 앞서 2015년 12월 29일에 제정되었는데 「(구)방산기술보호법」도 당시 시행되던 「(구)산업기술보호법」⁷¹⁾의 것을 참고한 것으로 추측되지만 유출·침해행위유형과 관련해서는 매우 간소화된 형태로 규정되었다.

아래의 표는 「(구)국가첨단전략산업법」이 제정될 당시 참고했을 것으로 추측되는 「(구)산업기술보호법」과 현행 「산업기술보호법」 그리고 「방산기술보호법」 제정 당시의 기술 유출·침해행위와 그 벌칙규정을 비교한 것이다.

67) 법률 제8062호, 2006.10.27. 제정, 2007.4.28. 시행.

68) 법률 제18813호, 2022.2.3. 제정, 2022.8.4. 시행.

69) 2023년 1월 3일 법률 제19166호에 의하여 개정되기 이전의 것.

70) 법률 제13632호, 2015.12.29. 제정, 2016.6.30. 시행.

71) 2016년 3월 29일 법률 제14108호에 의하여 개정되기 이전의 것.

〈표 3〉 「산업기술보호법」, 「국가첨단전략산업법」 그리고 「방산기술보호법」의 기술유출·침해행위 비교(「(구)산업기술보호법」을 기준으로 정리)

<p>(현행)「산업기술보호법」 (2025.1.21. 개정)</p>	<p>「(구)산업기술보호법」 (2023년 1월 3일 법률 제19166호에 의하여 개정되기 이전의 것)</p>	<p>「(구)국가첨단전략산업법」 (2022.2.3. 제정)</p>	<p>「(구)방산기술보호법」 (2015.12.29. 제정)</p>
<p>※ 2025.1.21.에 제14조의 열거순서를 전면개정</p>	<p>- 「국가첨단전략산업법」 제정 당시의 것임.</p>	<p>- 제15조 및 제50조는 법률이 제정된 이래 현재까지 개정되지 않아 현행과 같음.</p>	<p>- 제10조는 법률제정된 이후 현재까지 개정되지 않음. - 제21조는 제1항의 법정형이 상향되고 각 항의 적용대상 범주가 변경됨.</p>
<p>제14조(산업기술의 유출 및 침해행위 금지)</p>	<p>제14조(산업기술의 유출 및 침해행위 금지)</p>	<p>제15조(전략기술 유출 및 침해행위 금지)</p> <p>- 현행과 같음</p>	<p>제10조(방위산업기술의 유출 및 침해 금지)</p> <p>- 2024.12.3.에 제10조제4호 및 제5호 신설(법률 제20540호, 2025.6.4. 시행, 현행)</p>
<p>1. 절취·기망·협박 그 밖의 부정한 방법으로 대상기관의 산업기술을 취득하는 행위 또는 그 취득한 산업기술을 사용하거나 공개(비밀을 유지하면서 특정인에게 알리는 것을 포함한다. 이하 같다)하는 행위</p>	<p>1. 절취·기망·협박 그 밖의 부정한 방법으로 대상기관의 산업기술을 취득하는 행위 또는 그 취득한 산업기술을 사용하거나 공개(비밀을 유지하면서 특정인에게 알리는 것을 포함한다. 이하 같다)하는 행위</p>	<p>1. 절취·기망·협박 또는 그 밖의 부정한 방법으로 대상기관의 전략기술을 취득하는 행위 또는 그 취득한 전략기술을 사용하거나 공개하는 행위</p>	<p>1. 부정한 방법으로 대상기관의 방위산업기술을 취득, 사용 또는 공개(비밀을 유지하면서 특정인에게 알리는 것을 포함한다. 이하 같다)하는 행위</p>
<p>2. 제34조의 규정 또는 대상기관과의 계약 등에 따라 산업기술에 대한 비밀유지의무가 있는 자가 대상기관의 산업기술을 유출하거나 그 유출한 산업기술을 사용 또는 공개하거나 제3자가 사용하게 하는 행위</p> <p>※ 2025.1.21.에 개정 - 목적 삭제</p>	<p>2. 제34조의 규정 또는 대상기관과의 계약 등에 따라 산업기술에 대한 비밀유지의무가 있는 자가 부정한 이익을 얻거나 그 대상기관에게 손해를 가할 목적으로 유출하거나 그 유출한 산업기술을 사용 또는 공개하거나 제3자가 사용하게 하는 행위</p>	<p>2. 제14조에 따른 전략기술보유자와의 계약 또는 「산업기술의 유출방지 및 보호에 관한 법률」 제34조 등에 따라 전략기술에 대한 비밀유지의무가 있는 자가 부정한 이익을 얻거나 그 대상기관에 손해를 가할 목적으로 전략기술을 유출하거나 그 유출한 전략기술을 사용 또는 공개하거나 제3자가 사용하게 하는 행위</p>	<p style="text-align: center;">x</p>
<p>5. 제1호부터 제4호까지에 해당하는 행위가 개입된 사실을 알고 그 산업기술을 취득·사용·공개하거나 산업기술을 취득한 후에 그 산업기술에 대하여 제1호부터 제4호까지에 해당하는 행위가 개입된 사실을 알고 그 산업기술을 사용하거나 공개하는 행위</p>	<p>3. 제1호 또는 제2호의 규정에 해당하는 행위가 개입된 사실을 알고 그 산업기술을 취득·사용 및 공개하거나 산업기술을 취득한 후에 그 산업기술에 대하여 제1호 또는 제2호의 규정에 해당하는 행위가 개입된 사실을 알고 그 산업기술을 사용하거나 공개하는 행위</p>	<p>3. 제1호 또는 제2호에 해당하는 행위가 개입된 사실을 알고 그 전략기술을 취득·사용 및 공개하거나 전략기술을 취득한 후에 그 전략기술에 대하여 제1호 또는 제2호에 해당하는 행위가 개입된 사실을 알고 그 전략기술을 사용하거나 공개하는 행위</p>	<p>2. 제1호에 해당하는 행위가 개입된 사실을 알고 방위산업기술을 취득·사용 또는 공개하는 행위</p>
<p>13. 제1호부터 제4호까지에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 그 산업기술을 취득·사용 및 공개하거나 산업기술을 취득한 후에 그 산업기술에 대하여 제1호부터 제4호까지에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 그 산업기술을 사용하거나 공개하는 행위</p>	<p>4. 제1호 또는 제2호의 규정에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 그 산업기술을 취득·사용 및 공개하거나 산업기술을 취득한 후에 그 산업기술에 대하여 제1호 또는 제2호의 규정에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 그 산업기술을 사용하거나 공개하는 행위</p>	<p>4. 제1호 또는 제2호에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 그 전략기술을 취득·사용 및 공개하거나 전략기술을 취득한 후에 그 전략기술에 대하여 제1호 또는 제2호에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 그 전략기술을 사용하거나 공개하는 행위</p>	<p>3. 제1호에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 방위산업기술을 취득·사용 또는 공개하는 행위</p>

<p>〔현행〕「산업기술보호법」 (2025.1.21. 개정)</p>	<p>「(구)산업기술보호법」 (2023년 1월 3일 법률 제19166호에 의하여 개정되기 이전의 것)</p>	<p>「(구)국가첨단전략산업법」 (2022.2.3. 제정)</p>	<p>「(구)방산기술보호법」 (2015.12.29. 제정)</p>
<p>7. 제11조제1항의 규정에 따른 승인을 얻지 아니하거나 부정한 방법으로 승인을 얻어 국가핵심기술을 수출하는 행위</p>	<p>5. 제11조제1항의 규정에 따른 승인을 얻지 아니하거나 부정한 방법으로 승인을 얻어 국가핵심기술을 수출하는 행위</p>	<p>5. 제12조제1항에 따른 승인을 받지 아니하거나 부정한 방법으로 승인을 받아 전략기술을 수출하는 행위</p>	<p style="text-align: center;">x</p>
<p>8. 제11조제4항에 따른 신고를 하지 아니하거나 거짓이나 그 밖의 부정한 방법으로 신고를 하고 국가핵심기술을 수출하는 행위</p>	<p style="text-align: center;">-</p>	<p style="text-align: center;">-</p>	<p style="text-align: center;">-</p>
<p>9. 제11조의2제1항에 따른 승인을 받지 아니하거나 거짓이나 그 밖의 부정한 방법으로 승인을 받아 해외인수·합병등을 하는 행위</p>	<p>6. 국가핵심기술을 외국에서 사용하거나 사용되게 할 목적으로 제11조의2제1항에 따른 승인을 받지 아니하거나 거짓이나 그 밖의 부정한 방법으로 승인을 받아 해외인수·합병등을 하는 행위</p>	<p>6. 전략기술을 외국에서 사용하거나 사용되게 할 목적으로 제13조제1항에 따른 승인을 받지 아니하거나 거짓이나 그 밖의 부정한 방법으로 승인을 받아 해외인수·합병등을 하는 행위</p>	<p style="text-align: center;">x</p>
<p>10. 제11조의2제5항 및 제6항에 따른 신고를 하지 아니하거나 거짓이나 그 밖의 부정한 방법으로 신고를 하고서 해외인수·합병등을 하는 행위</p>	<p>6의2. 국가핵심기술을 외국에서 사용하거나 사용되게 할 목적으로 제11조의2제5항 및 제6항에 따른 신고를 하지 아니하거나 거짓이나 그 밖의 부정한 방법으로 신고를 하고서 해외인수·합병등을 하는 행위</p>	<p style="text-align: center;">-</p>	<p style="text-align: center;">-</p>
<p>3. 제34조 또는 대상기관과의 계약 등에 따라 산업기술에 대한 비밀유지의무가 있는 자가 산업기술에 대한 보유 또는 사용 권한이 소멸됨에 따라 대상기관으로부터 산업기술에 관한 문서, 도화(圖畵), 전자기록 등 특수매체기록이나 원시코드 등의 반환이나 산업기술의 삭제를 요구받고도 이를 거부 또는 기피하거나 그 사본을 보유하는 행위</p>	<p>6의3. 제34조 또는 대상기관과의 계약 등에 따라 산업기술에 대한 비밀유지의무가 있는 자가 산업기술에 대한 보유 또는 사용 권한이 소멸됨에 따라 대상기관으로부터 산업기술에 관한 문서, 도화(圖畵), 전자기록 등 특수매체기록의 반환이나 산업기술의 삭제를 요구받고도 부정한 이익을 얻거나 그 대상기관에 손해를 가할 목적으로 이를 거부 또는 기피하거나 그 사본을 보유하는 행위</p>	<p>7. 제14조에 따른 전략기술보유자와의 계약 또는 「산업기술의 유출방지 및 보호에 관한 법률」 제34조 등에 따라 전략기술에 대한 비밀유지의무가 있는 자가 전략기술에 대한 보유 또는 사용 권한이 소멸됨에 따라 해당 전략기술보유자로부터 전략기술에 관한 문서, 도화(圖畵), 전자기록 등 특수매체기록의 반환이나 전략기술의 삭제를 요구받고도 부정한 이익을 얻거나 그 보유자에 손해를 가할 목적으로 이를 거부 또는 기피하거나 그 사본을 보유하는 행위</p>	<p style="text-align: center;">x</p> <p>※2024.12.3. 개정으로 제4호로 신설되는데 이때에도 현행 「산업기술보호법」 제14조제3호와 같이 목적범을 삭제. ※2024.12.3. 개정으로 제4호의 종과실범을 신설(제5호) - 현행 「산업기술보호법」이나 「국가첨단전략산업법」에는 없는 규정임.</p>
<p>4. 대상기관의 계약 등에 따라 산업기술에 대한 접근 권한이 있는 자가 산업기술을 지정된 장소 밖으로 무단으로 유출하거나 목적 외로 사용·공개하는 행위</p> <p>※2025.1.21.에 개정 - 신설</p>	<p style="text-align: center;">x</p>	<p style="text-align: center;">x</p>	<p style="text-align: center;">x</p>
<p>6. 제1호부터 제4호까지의 어느 하나에 해당하는 행위를 소개·알선·유인하는 행위</p> <p>※2025.1.21.에 개정 - 신설</p>	<p style="text-align: center;">x</p>	<p style="text-align: center;">x</p>	<p style="text-align: center;">x</p>

<p>〔현행〕「산업기술보호법」 (2025.1.21. 개정)</p>	<p>「(구)산업기술보호법」 (2023년 1월 3일 법률 제19166호에 의하여 개정되기 이전의 것)</p>	<p>「(구)국가첨단전략산업법」 (2022.2.3. 제정)</p>	<p>「(구)방산기술보호법」 (2015.12.29. 제정)</p>
<p>11. 제11조제6항·제8항 및 제11조의2제8항·제10항에 따른 산업통상자원부장관의 명령을 이행하지 아니하는 행위</p> <p>12. 산업기술 관련 소송 등 대통령령으로 정하는 적법한 경로를 통하여 산업기술이 포함된 정보를 제공받은 자가 정보를 제공받은 목적 외의 다른 용도로 그 정보를 사용하거나 공개하는 행위</p>	<p>7. 제11조제5항·제7항 및 제11조의2제7항·제9항에 따른 산업통상자원부장관의 명령을 이행하지 아니하는 행위</p> <p>8. 산업기술 관련 소송 등 대통령령으로 정하는 적법한 경로를 통하여 산업기술이 포함된 정보를 제공받은 자가 정보를 제공받은 목적 외의 다른 용도로 그 정보를 사용하거나 공개하는 행위</p>	<p style="text-align: center;">x</p> <p>8. 전략기술 관련 소송 등 대통령령으로 정하는 적법한 경로를 통하여 전략기술이 포함된 정보를 제공받은 자가 정보를 제공받은 목적 외의 용도로 그 정보를 사용하거나 공개하는 행위</p>	<p style="text-align: center;">x</p> <p>※ 「방위사업법」에도 관련규정을 찾을 수 없음.</p>
<p>제36조(벌칙)</p>	<p>제36조(벌칙)</p>	<p>제50조(벌칙)</p>	<p>제21조(벌칙)</p>
<p>- 2025.1.21. 목적범 삭제 - 벌금형 상향</p>		<p>- 현행과 같음</p>	<p>- 목적범으로 규정된 것은 현행과 같음 - 2024.12.3. 법정형이 상향되고 일부 대상법조 변경</p>
<p>①국가핵심기술이 외국에서 사용될 것을 알면서 제14조제1호부터 제12호까지의 어느 하나에 해당하는 행위를 한 자는 3년 이상의 유기징역에 처한다. 이 경우 65억원 이하의 벌금을 병과한다. <신설 2019.8.20., 2025.1.21.></p>	<p>①국가핵심기술을 외국에서 사용하거나 사용되게 할 목적으로 제14조제1호부터 제3호까지의 어느 하나에 해당하는 행위를 한 자는 3년 이상의 유기징역에 처한다. 이 경우 15억원 이하의 벌금을 병과한다. <신설 2019.8.20.></p> <p>※2019.8.20. 이전에는 법정형이 15년 이하의 징역 또는 15억원 이하의 벌금이었음.</p>	<p>①전략기술을 외국에서 사용하거나 사용되게 할 목적으로 제15조제1호부터 제3호까지의 어느 하나에 해당하는 행위를 한 자는 5년 이상의 유기징역에 처한다. 이 경우 20억원 이하의 벌금을 병과한다.</p> <p>②전략기술을 외국에서 사용하거나 사용되게 할 목적으로 제15조제5호부터 제8호까지의 어느 하나에 해당하는 행위를 한 자는 20년 이하의 징역 또는 20억원 이하의 벌금에 처한다.</p>	<p>①방위산업기술을 외국에서 사용하거나 사용되게 할 목적으로 제10조제1호 및 제2호에 해당하는 행위를 한 사람은 15년 이하의 징역 또는 1억5천만원 이하의 벌금에 처한다.</p> <p>※2017.11.18. 개정으로 법정형이 20년 이하의 징역 또는 20억원 이하의 벌금으로 상향됨. ※2024.12.3. 개정으로 법정형이 1년 이상의 유기징역으로 상향되고 20억원 이하의 벌금을 병과하도록 상향됨. ※2024.12.3. 개정으로 제10조 제4호가 적용대상에 포함됨.</p>
<p>②산업기술이 외국에서 사용될 것을 알면서 제14조제1호부터 제6호까지 및 제12호의 어느 하나에 해당하는 행위를 한 자(제1항에 해당하는 행위를 한 자는 제외한다)는 15년 이하의 징역 또는 30억원 이하의 벌금에 처한다. <개정 2008.3.14., 2016.3.29., 2019.8.20., 2025.1.21.></p>	<p>②산업기술을 외국에서 사용하거나 사용되게 할 목적으로 제14조 각 호(제4호를 제외한다)의 어느 하나에 해당하는 행위를 한 자(제1항에 해당하는 행위를 한 자는 제외한다)는 15년 이하의 징역 또는 15억원 이하의 벌금에 처한다.</p> <p>※2019.8.20. 이전에는 법정형이 7년 이하의 징역 또는 7억원 이하의 벌금이었음.</p>		
<p>③제14조제1호부터 제11호까지의 어느 하나에 해당하는 행위를 한 자는 10년 이하의 징역 또는 10억원 이하의 벌금에 처한다. <개정 2011.7.25., 2016.3.29., 2019.8.20., 2025.1.21.></p>	<p>③제14조 각 호(제4호·제6호·제6호의2 및 제8호는 제외한다)의 어느 하나에 해당하는 행위를 한 자는 10년 이하의 징역 또는 10억원 이하의 벌금에 처한다.</p>	<p>③제15조 각 호(제4호·제6호 및 제8호는 제외한다)의 어느 하나에 해당하는 행위를 한 자는 15년 이하의 징역 또는 15억원 이하의 벌금에 처한다.</p>	<p>②제10조제1호 및 제2호에 해당하는 행위를 한 사람은 7년 이하의 징역 또는 7천만원 이하의 벌금에 처한다.</p> <p>※2017.11.18. 개정으로 법정형이 10년 이하의 징역 또는 10억원 이하의 벌금으로 상향됨. ※2024.12.3. 개정으로 제4호가 적용대상에 포함됨.</p>

「(현행)산업기술보호법」 (2025.1.21. 개정)	「(구)산업기술보호법」 (2023년 1월 3일 법률 제19166호에 의하여 개정되기 이전의 것)	「(구)국가첨단전략산업법」 (2022.2.3. 제정)	「(구)방산기술보호법」 (2015.12.29. 제정)
④제14조제12호 및 제13호의 어느 하나에 해당하는 행위를 한 자는 3년 이하의 징역 또는 3억원 이하의 벌금에 처한다. <개정 2019.8.20., 2025.1.21.>	④제14조제4호 및 제8호의 어느 하나에 해당하는 행위를 한 자는 3년 이하의 징역 또는 3억원 이하의 벌금에 처한다.	④제15조제4호 또는 제8호에 해당하는 행위를 한 자는 5년 이하의 징역 또는 5억원 이하의 벌금에 처한다.	③제10조제3호에 해당하는 행위를 한 사람은 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. ※2017.11.18. 개정으로 5억원 이하의 벌금으로 상향됨. ※2024.12.3. 개정으로 제5호가 적용대상에 포함됨.
⑤제1항부터 제4항까지의 죄를 범한 자가 그 범죄행위로 인하여 얻은 재산은 이를 몰수한다. 다만, 그 전부 또는 일부를 몰수할 수 없는 때에는 그 가액을 추징한다. <개정 2019.8.20.>	⑤제1항부터 제4항까지의 죄를 범한 자가 그 범죄행위로 인하여 얻은 재산은 이를 몰수한다. 다만, 그 전부 또는 일부를 몰수할 수 없는 때에는 그 가액을 추징한다.	X (현행법에도 없다)	⑤제1항부터 제3항까지의 죄를 범한 사람이 그 범죄행위로 인하여 얻은 재산은 몰수한다. 다만, 그 재산의 전부 또는 일부를 몰수할 수 없는 때에는 그 가액을 추징한다.
⑥제34조의 규정을 위반하여 비밀을 누설하거나 도용한 자는 5년 이하의 징역이나 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다. <개정 2016.3.29., 2019.8.20.>	⑥제34조의 규정을 위반하여 비밀을 누설하거나 도용한 자는 5년 이하의 징역이나 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다.	⑤제10조제5항 각 호의 어느 하나에 해당하는 행위를 한 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.	④제19조를 위반하여 비밀을 누설·도용한 사람은 7년 이하의 징역이나 10년 이하의 자격정지 또는 7천만원 이하의 벌금에 처한다.
⑦제1항부터 제3항까지의 미수범은 처벌한다. <개정 2019.8.20.>	⑦제1항부터 제3항까지의 미수범은 처벌한다.	X (현행법에도 없다)	⑥제1항 및 제2항의 미수범은 처벌한다.
⑧제2항부터 제4항까지의 규정에 따른 징역형과 벌금형은 이를 병과할 수 있다. <개정 2019.8.20.>	⑧제2항부터 제4항까지의 규정에 따른 징역형과 벌금형은 이를 병과할 수 있다.	X (현행법에도 없다)	⑦제1항부터 제3항까지의 징역형과 벌금형은 병과할 수 있다. ※2024.12.3. 개정으로 제1항의 벌금형이 필요적 병과로 개정됨에 따라 제7항에서도 제1항을 삭제되었어야 함.
제36조의2(비밀유지명령 위반죄)	제36조의2(비밀유지명령 위반죄)	-	-
제37조(예비·음모)	제37조(예비·음모)	X (현행법에도 없다)	제22조(예비·음모)
제38조(양벌규정)	제38조(양벌규정)	X (현행법에도 없다)	제23조(양벌규정)

나. 각 법률에 규정된 기술유출·침해유형들 간의 상응성의 문제점

그런데 이상의 3개 법률의 비교표에서 알 수 있는 것은 동일·유사규정들이 여러 법률에 산재되어 규정될 경우 일방 법률에 대한 일방적인 개정은 타방 법률에 예기치 않은 규율의 공백과 가별성의 흠결이 발생하게 된다는 점이다.

물론 「산업기술보호법」, 「국가첨단전략산업법」 그리고 「방산기술보호법」은 입법취지나 목적 그리고 각 법률에 도입된 특수한 제도들 등에 상응하여 각 법률에 맞는 규정들을 입법하는 것이 당연하다.

그러나 문제는 기술유출·침해 유형이 특단의 사정이 없는 이상 일반적으로 행위유형들이 각 법률에 따라 동일·유사한 것은 아닌가 그리고 어떤 기술유출·침해행위가 형사처벌의 대상이 될 정도로 죄질의 경중에 있어서 중한 것이라면 이러한 가치평가는 다른 법률에서 이와 동일·유사한 기술유출·침해 행위를 규정하고 있다면 그대로 적용되어야 하는 것은 아닌가라는 의문이 제기된다.

여기에서는 「산업기술보호법」과 「국가첨단전략산업법」 및 「방산기술보호법」 간의 기술유출·침해 유형들 간의 상응성과 전체 법체계에서의 체계정합성에 관하여 검토하고자 한다.

1) 「산업기술보호법」과 「국가첨단전략산업법」 간의 상응성

우선 「산업기술보호법」과 「국가첨단전략산업법」에 규정된 기술유출·침해 행위유형들 간의 상응성에 관하여 살펴보면 다음과 같다.

「국가첨단전략산업법」이 제정될 당시 동법 제14조에 규정된 전략기술의 유출·침해유형들은 위의 표에서도 알 수 있듯이 「(구)산업기술보호법」 제15조와 거의 동일했다.

그런데 문제는 「국가첨단전략산업법」이 제정된 2022년 이래 「산업기술보호법」의 경우 3차례에 걸쳐 유출·침해행위와 이에 상응하는 벌칙규정이 개정되었음에도 「국가첨단전략산업법」의 유출·침해행위와 벌칙규정은 현재까지 단 한 번도 개정되지 못했다는 점이다. 그 결과 「국가첨단전략산업법」상 전략기술이 「산업기술보호법」상 산업기술 또는 국가핵심기술보다 보호의 강도가 더 강해야 함에도 불구하고 「산업기술보호법」의 일방적인 개정에 의하여 경우에 따라서는 전략기술의 보호에 공백이 발생하는 결과를 초래하게 되었다.

특히 「산업기술보호법」은 특히 최근인 2025년 1월 21일 개정에서 유출·침해행위뿐만 아니라 벌칙규정에 대하여 폭넓은 개정을 단행했는데 주요 개정내용으로는 유출·침해행위와 관련하여 ①(구)제2호가 비밀유지의무자의 행위에 대하여 “부정한 이익을 얻거나 그 대상기관에게 손해를 가할 목적”을 요구하던 것을 이를 삭제하여 단순고의범으로 개정했다는 점, ②전략기술 보유 대상기관의 미승인 해외인수·합병((구)제6항)의 경우와 ③미신고 해외인수·합병(제6항의2)의 경우에 “외국에서 사용하거나 사용되게 할 목적”을 삭제하고 이를 단순고의범으로 개정한 점, ④산업기술에 대하여 접근권한이 있는 자가 해당 권한의 소멸 후 자료 등의 반환을 거부 등의 행위와 관련하여 종래(구)제6항의3이 “부정한 이익을 얻거나 그 대상기관에 손해를 가할 목적”을 요구하던 것을 삭제하여 단순고의범으로 개정한 점, ⑤새롭게 신설된 유출·침해행위로서는 산업기술에 대하여 접근권한이 있는 자가 지정된 장소 밖으로 무단으로 유출하거나 목적 외 용도 등으로 사용·공개하는 행위(현행 제4호), ⑥유출·침해행위에 대한 소개·알선·유인하는 행위(현행 제6호) 그리고 ⑦미신고 등 수출(현행 제8호) 등이 있으며 ⑧이러한 개정에 따라 제14조에 열거된 유출·침해행위의 규정순서도 대대적으로 수정되었다는 점이다. 그 결과 「산업기술보호법」 제14조에 정한 기술유출·침해행위는 13개로 증가한데 대하여 「국가첨단전략산업법」 제15조에 정한 전략기술 유출·침해행위(제15조)는 동 법률

제정 이래로 개정되지 못하여 여전히 8개의 기술유출·침해행위만이 규정되어 있을 뿐만 아니라 법문언도 변경된 것이 없다.

물론 그렇다고 하여 「산업기술보호법」 제14조에 신설된 5개 유출·침해행위들 모두가 「국가첨단전략산업법」과 관련될 수 있는 것은 아니어서 「국가첨단전략산업법」에 모두 도입되어야 하는 것은 아닐 것이다. 예컨대 「산업기술보호법」 제14조 제8호는 승인대상 외의 국가핵심기술의 수출과 관련된 것인데 전략기술의 수출 승인 등에 관하여 정한 「국가첨단전략산업법」 제12조는 모든 전략기술에 대하여 승인을 요구하고 있기 때문에 승인대상 외의 전략기술의 수출문제는 발생하지 않을 것이다. 이것은 「산업기술보호법」 제14조 제10호에 정한 승인대상 외의 국가핵심기술을 보유한 대상기관의 미신고 인수·합병의 경우(제11조의2 제5항 및 제6항)에도 동일한 것이 적용된다.

가) 계약 등 비밀유지의무자의 기술 유출·침해행위에 있어서의 “부정한 이익을 얻거나 그 대상기관에 손해를 가할 목적으로”

「산업기술보호법」은 종래 계약 등 비밀유지의무자의 산업기술 유출·침해행위와 관련하여 비밀유지의무자가 “부정한 이익을 얻거나 그 대상기관에게 손해가 발생하는 것을 알면서” 산업기술을 유출할 것을 요구함으로써 고의 외에도 부정한 이익을 얻을 목적이나 대상기관의 손해의 발생에 대한 인식이 있을 것을 요건으로 하고 있었다((구)제14조 제2호). 그러나 2025년 1월 21일 개정에 의하여 이 행위자의 추가적인 주관적 요건을 삭제함으로써 주관적 구성요건의 입증을 용이하게 하여 가벌성의 문턱을 낮추어 보호의 강도를 높였다. 그리고 마찬가지로 계약 등 비밀유지의무자의 권한 소멸 후 자료 등의 반환 등의 거부에 있어서 “부정한 이익을 얻거나 그 대상기관에 손해를 가할 목적”을 요구하던 (구)제14조 제6호의3도 동 개정에 의하여 목적이 삭제되었다(현행 제14조 제3호).

그런데 마찬가지로 계약 등 비밀유지의무자의 전략기술의 유출에 관하여 정한 「국가첨단전략산업법」 제15조 제2호는 여전히 “부정한 이익을 얻거나 그 대상기관에 손해를 가할 목적”을 요구하고 있는데 이것은 계약 등 비밀유지의무자의 권한 소멸 후 자료 등의 반환 등의 거부에 있어서도 동일하다(동조 제7호).

이 문제도 동일·유사규정을 공유하는 여러 법률들 가운데 일방 법률이 일방적으로 개정되었을 때 타방 법률에 규율의 공백이 가벌성의 흠결이 발생하는 현상들 중의 하나라고 볼 수 있다. 즉 2025년 1월 21일 「산업기술보호법」이 일방적으로 개정됨에 따라 「산업기술보호법」상 산업기술 또는 국가핵심기술의 유출·침해행위에 대하여 고의 외에 추가적으로 요구하던 주관적 요건, 즉 목적을 삭제하여 유출·침해행위의 입증을 용이하게 함으로써 가벌성의 문턱을 낮춤에 따라 보다 강한 보호의 강도가 요구되는 「국가첨단전략산업법」상 전략기술의 유출·침해행위에 대한 가벌성의 문턱이 높아져 전략기술에 대한 보호의 강도가 상대적으로 약해진 것이라고 볼 수 있다.

따라서 이러한 보호의 강도의 역전현상을 방지하기 위해서는 「산업기술보호법」의 개정에 상응하여 「국가첨단전략산업법」의 관련규정들을 정비할 필요가 있다.

나) 전략기술 유출·침해행위에서의 “외국에서 사용하거나 사용되게 할 목적”

「국가첨단전략산업법」 제15조 제6호는 제13조제1항에 따른 승인을 받지 아니하거나 거짓이나 그 밖의 부정한 방법으로 승인을 받아 대상기관의 해외인수·합병등을 하는 행위를 전략기술의 유출·침해행위로 규정하면서 다른 유출·침해행위와 달리 추가적으로 “외국에서 사용하거나 사용되게 할 목적”을 요구하고 있는데 문제는 제50조 제2항이 이미 형벌구성요건에서 “외국에서 사용하거나 사용되게 할 목적”을 요구하고 있기 때문에 유출·침해행위에 관하여 정한 제14조 제6호에서 추가적인 목적에 관하여 규정하는 것은 중복이며 불필요한 것이라고 볼 수 있다.

2025년 1월 21일에 의하여 개정되기 이전의 「(구)산업기술보호법」도 별칙규정인 제36조 제2항이 유출·침해행위가 처벌되기 위한 추가적인 주관적 요건으로서 “외국에서 사용하거나 사용되게 할 목적”을 요구하고 있는데도 불구하고 (구)제14조 제6호(미승인 등 인수·합병)와 제6호의2(미신고 등 인수·합병)에서 반복적으로 “외국에서 사용하거나 사용되게 할 목적”을 요건으로 정하고 있었으나 동 개정에 의하여 별칙규정이 목적범에서 단순고의범으로 전환되면서 함께 정비되었다.

물론 현행 「국가첨단전략산업법」 제50조(별칙)가 「산업기술보호법」에서도 요구하지 않는 형벌규정에서 추가적인 목적을 향후에도 형벌구성요건으로 규정할 것인가에 대해서는 의문이 제기된다는 것은 별칙규정에 관하여 서술하면서 언급하도록 하겠다.

다) 전략기술 유출·침해행위의 알선 등 행위

「산업기술보호법」은 종래 산업기술 등 유출·침해행위의 알선 등 행위에 관하여 정하고 있지 않아 「형법」 제31조에 정한 교사범이나 제32조에 정한 중범 그리고 공범이론으로 해결하여 왔으나 2025년 1월 21일 개정에 의하여 산업기술 등 유출·침해행위의 알선 등 행위(제14조 제6호)를 신설하였다. 이러한 개정은 문제는 모든 알선 등 행위, 특히 브로커 등의 행위가 반드시 공범의 성립요건을 충족하는 것은 아니라는 점에서 한계를 가지고 있다는 점에서 적절한 개정이라고 판단된다.

그런데 기술 등 유출·침해행위의 알선 등 행위에 관하여 정하고 있지 않은 「국가첨단전략산업법」에도 앞서 언급한 공범규정의 적용의 한계의 문제는 동일하게 발생될 수 있다는 점에서 알선 등 행위를 기술유출·침해행위의 하나로 규정할 필요가 있다.

라) 전략기술의 무단 반출 등 행위

「산업기술보호법」은 종래 계약 등 비밀유지의무자 등의 산업기술 등의 유출·침해행위와 관련해서는 부정한 이익을 얻거나 그 대상기관에게 손해가 발생하는 것을 알면서도 산업기술을 유출하는

행위((구)제14조 제2호)와 권한소멸 후 자료 등 반환거부 등((구)제14조 제6호의3)만을 규정하고 있었으나 산업기술 등의 무단 반출 행위는 정확히 이들 행위유형에 포섭되지 않는다는 점에서 2025년 1월 21일 개정으로 계약 등 비밀유지의무자 등의 산업기술 등의 무단 반출 등의 행위(「산업기술보호법」 제14조 제4호)를 신설하였다.

이러한 「산업기술보호법」에서 발생하는 문제는 동일하게 「국가첨단전략산업법」에서도 발생될 수 있다는 점에서 관련규정이 신설될 필요가 있다.

마) 전략기술의 유출·침해를 방지하기 위한 산업통상자원부장관의 제한조치에 관한 명령에 대한 불이행

「산업기술보호법」은 국가핵심기술(신고대상 국가핵심기술)의 수출과 국가핵심기술을 보유하는 대상기관의 인수·합병 시 해당 국가핵심기술의 유출·침해를 방지하기 위한 산업통상자원부장관의 제한조치에 관한 명령을 이행하지 않는 행위를 직접적으로 국가핵심기술의 유출·침해의 결과를 초래하는 행위로 규정하고 있는데 대하여 「국가첨단전략산업법」은 마찬가지로 산업통상자원부장관의 제한조치에 관하여 정하고 있으면서도 법률제정 당시부터⁷²⁾ 현재까지도 그 불이행을 전략기술의 유출·침해행위로 규정하고 있지는 않다.⁷³⁾ 이에 관한 규정들을 비교해 보면 아래의 표와 같다.

〈표 4〉 기술유출·침해방지를 위한 산업통상자원부장관의 제한조치에 관한 명령에 관한 규정들의 비교

(현행)「산업기술보호법」 (2025.1.21. 개정)	「(구)산업기술보호법」 (2023년 1월 3일 법률 제19166호에 의하여 개정되기 이전의 것)	「국가첨단전략산업법」 (아래의 규정들은 제정 이래 개정된 바 없음)
제14조(산업기술의 유출 및 침해행위 금지) (생략) 11. 제11조제6항·제8항 및 제11조의2 제8항·제10항에 따른 산업통상자원부장관의 명령을 이행하지 아니하는 행위 (생략)	제14조(산업기술의 유출 및 침해행위 금지) (생략) 7. 제11조제5항·제7항 및 제11조의2제7항·제9항에 따른 산업통상자원부장관의 명령을 이행하지 아니하는 행위 (생략)	x
제11조(국가핵심기술의 수출 등) ⑥ (구법 제7항과 같음).	제11조(국가핵심기술의 수출 등) ⑤산업통상자원부장관은 제4항의 신고대상인 국가핵심기술의 수출이 국가안보에 심각한 영향을 줄 수 있다고 판단하는 경우에는 관계중앙행정기관의 장과 협의한 후 위원회의 심의를 거쳐 국가핵심기술의 수출중지·수출금지·원상회복 등의 조치를 명할 수 있다.	제12조(전략기술의 수출 승인 등) - ※ 전략기술의 수출은 승인대상이기 때문에 「산업기술보호법」의 신고에 관한 규정에 상응하는 「국가첨단전략산업법」의 규정은 없음.

72) 「국가첨단전략산업법」의 제정 당시 시행되던 「(구)산업기술보호법」에도 국가핵심기술의 수출 및 대상기관의 인수·합병 시의 산업통상자원부장관의 명령의 불이행을 국가핵심기술의 유출·침해행위로 규정하고 있었다.

73) 이에 대한 비판으로는 조용순, “국가첨단전략산업법상 전략기술의 유출·침해행위 및 형사처벌 규정에 대한 문제점과 개선방안”, 『산업재산권』, 한국지식재산학회, 제72호(2022), 510면 이하.

<p>(현행)「산업기술보호법」 (2025.1.21. 개정)</p>	<p>「(구)산업기술보호법」 (2023년 1월 3일 법률 제19166호에 의하여 개정되기 이전의 것)</p>	<p>「국가첨단전략산업법」 (아래의 규정들은 제정 이래 개정된 바 없음)</p>
<p>⑧ 산업통상자원부장관은 국가핵심기술을 보유한 대상기관이 다음 각 호의 어느 하나에 해당하는 경우에는 해당 국가핵심기술의 수출중지·수출금지·원상회복 등 필요한 조치를 명할 수 있다. (생략)</p>	<p>⑦산업통상자원부장관은 국가핵심기술을 보유한 대상기관이 제1항의 규정에 따른 승인을 얻지 아니하거나 부정한 방법으로 승인을 얻어 국가핵심기술의 수출을 한 경우 또는 제4항의 규정에 따른 신고대상 국가핵심기술을 신고하지 아니하거나 허위로 신고하고 국가핵심기술의 수출을 한 경우에는 정보수사기관의 장에게 조사를 의뢰하고, 조사결과를 위원회에 보고한 후 위원회의 심의를 거쳐 해당 국가핵심기술의 수출중지·수출금지·원상회복 등의 조치를 명령할 수 있다.</p>	<p>④산업통상자원부장관은 전략기술보유자가 제1항에 따른 승인을 받지 아니하거나 부정한 방법으로 승인을 받아 전략기술의 수출을 한 경우 정보수사기관의 장에게 조사를 의뢰하고, 조사결과를 산업기술보호위원회에 보고한 후 산업기술보호위원회의 심의를 거쳐 해당 전략기술의 수출중지·수출금지·원상회복 등의 조치를 명할 수 있다.</p>
<p>제11조의2(국가핵심기술을 보유하는 대상기관의 해외인수·합병등)</p> <p>⑧ (구법 제7항과 같음).</p> <p>⑩산업통상자원부장관은 국가핵심기술을 보유한 대상기관이 다음 각 호의 어느 하나에 해당하는 경우에는 해외인수·합병등의 중지·금지·원상회복 등 필요한 조치를 명할 수 있다. (생략)</p>	<p>제11조의2(국가핵심기술을 보유하는 대상기관의 해외인수·합병등)</p> <p>⑦산업통상자원부장관은 제1항, 제5항 및 제6항에 따른 국가핵심기술의 유출이 국가안보에 심각한 영향을 줄 수 있다고 판단하는 경우에는 관계 중앙행정기관의 장과 협의한 후 위원회의 심의를 거쳐 해외인수·합병등에 대하여 중지·금지·원상회복 등의 조치를 명할 수 있다.</p> <p>⑨산업통상자원부장관은 국가핵심기술을 보유한 대상기관이 제1항에 따른 승인을 받지 아니하거나 거짓이나 그 밖의 부정한 방법으로 승인을 받아 해외인수·합병등을 진행한 경우 또는 제5항 및 제6항에 따른 신고를 하지 아니하거나 거짓이나 그 밖의 부정한 방법으로 신고를 하고서 해외인수·합병등을 한 경우에는 정보수사기관의 장에게 조사를 의뢰하고, 조사결과를 위원회에 보고한 후 위원회의 심의를 거쳐 해당 해외인수·합병등에 대하여 중지·금지·원상회복 등 필요한 조치를 명할 수 있다.</p>	<p>제14조(전략기술의 보호조치 등)</p> <p>⑤ 산업통상자원부장관은 해외인수·합병등에 따른 전략기술의 유출로 국가·경제안보에 심각한 영향을 줄 수 있다고 판단하는 경우에는 관계 중앙행정기관의 장과 협의한 후 산업기술보호위원회의 심의를 거쳐 해당 해외인수·합병등에 대하여 중지·금지·원상회복 등의 조치를 명할 수 있다.</p> <p>⑦산업통상자원부장관은 전략기술보유자가 제1항에 따른 승인을 받지 아니하거나 거짓이나 그 밖의 부정한 방법으로 승인을 받아 해외인수·합병등을 진행한 경우 정보수사기관의 장에게 조사를 의뢰하고, 조사결과를 산업기술보호위원회에 보고한 후 산업기술보호위원회의 심의를 거쳐 해당 해외인수·합병등에 대하여 중지·금지·원상회복 등 필요한 조치를 명할 수 있다.</p>

그런데 이와 같이 「국가첨단전략산업법」이 제정 당시에도 그리고 현행법에서도 전략기술 유출·침해의 방지를 위한 산업통상자원부장관의 제한조치에 관한 명령의 불이행을 유출·침해행위로 규정하지 않은 것은 이를 전략기술의 유출·침해행위로 보지 않는다는 것을 의미하는 것인지 아니면 「국가첨단전략산업법」상 전략기술도 「산업기술보호법」상 국가핵심기술의 하나인 이상 「산업기술보호법」이 그대로 적용되기 때문에 중복적인 규정을 두지 않으려는 의도적인 것인지 아니면 단순한 입법상의 누락인지에 관해서는 명확하지 않다.

그러나 앞서 언급한 바와 같이 「산업기술보호법」상 국가핵심기술의 수출과 국가핵심기술을 보유하는 대상기관의 인수·합병 시 해당 국가핵심기술의 유출·침해를 방지하기 위한 산업통상자원부장관

의 제한조치에 관한 명령을 이행하지 않는다는 것은 곧 국가핵심기술의 유출·침해의 결과를 초래한다는 것을 의미하는 것이라면 국가핵심기술보다 강한 보호의 강도가 요구되는 전략기술의 경우에는 더욱 더 이러한 행위들이 기술유출·침해행위로 규정되어야 할 것이다.⁷⁴⁾

물론 「국가첨단전략산업법」상 전략기술은 「대외무역법」상 이중용도품목이나 군용물자품목(동법 제19조, 시행령 제32조의2, 「전략물자 수출입고시」 별표 2 및 3) 등의 전략물자에 해당되어 「대외무역법」의 적용도 받아 수출입이 통제되기는 하지만 그렇다고 하여 「국가첨단전략산업법」상 모든 전략기술이 「대외무역법」상 전략물자가 되는 것은 아니라는 점 그리고 「대외무역법」은 전략기술을 보유한 대상기관의 인수·합병에 관해서는 상세한 규정을 두고 있지 않다는 점에서 다른 법률에 의한 보충도 그리 쉽지는 않다.

2) 「산업기술보호법」과 「방산기술보호법」 간의 상응성의 문제

2015년 12월 29일에 「방산기술보호법」이 제정되었을 당시 방산기술 유출·침해유형은 3개에 불과했는데((구)제10조) 당시 시행되고 있었던 「(구)산업기술보호법」(2015.1.28. 개정)⁷⁵⁾이 8개 유형을 규정하고 있었던 것에 비하면 매우 간소하게 규정되어 있었다. 또한 최근인 2024년 12월 3일 개정에서도 계약 등에 따른 비밀유지의무자의 권한 소멸 후 고의에 의한 반환거부 등(제10조 제4호)과 그 중과실범(동조 제5호) 등 2개 유형들만 신설되는데 그쳤다. 그리고 「산업기술보호법」은 2025년 1월 21일 개정에 의하여 그 유형들이 13개로 확대된 것에 비하면 「방산기술보호법」의 방산기술 유출·침해유형은 매우 간소하다고 말할 수 있으며 이것은 앞서 제시된 “표 2 산업기술 및 국가핵심기술의 유출 및 침해행위에 대한 형사처벌 비교”와 “표 4 「산업기술보호법」, 「국가첨단전략산업법」 그리고 「방산기술보호법」의 기술유출·침해행위 비교”를 보더라도 쉽게 알 수 있다.

이러한 점에서 앞서 「산업기술보호법」과 「국가첨단전략산업법」에 대하여 논의했던 양 법률들 간의 상응성의 결여의 문제는 「방산기술보호법」에도 그대로 적용될 수 있을 뿐만 아니라 특히 「방산기술보호법」의 경우에는 현행 제10조에 정한 방산기술 유출·침해행위만으로 모든 행위유형들을 포괄할 수 있는가에 대하여 의문이 제기된다.

가) 기술취득 후 인식있는 사용·공개행위

「방산기술보호법」 제10조 제2호는 “제1호에 해당하는 행위가 개입된 사실을 알고 방위산업기술을 취득·사용 또는 공개하는 행위”를 방산기술 유출·침해행위의 하나로 규정하고 있는데 이것은 「산업기술보호법」 제14조 제5호에 상응하는 것이기는 하지만 그렇다고 하여 양 규정의 법문언이 정확히 일치하는 것은 아니다.

74) 조용순, 앞의 논문(2022), 510면 이하.

75) 2016년 3월 29일 법률 제14108호에 의하여 개정되기 이전의 것.

즉 「산업기술보호법」 제14조 제5호는 「방산기술보호법」 제10조 제2호와 달리 “제1호부터 제4호까지에 해당하는 행위가 개입된 사실을 알고 그 산업기술을 취득·사용·공개”하는 행위 외에 “산업기술을 취득한 후에 그 산업기술에 대하여 제1호부터 제4호까지에 해당하는 행위가 개입된 사실을 알고 그 산업기술을 사용하거나 공개하는 행위”까지 규정하고 있다.

그런데 이 두 규정들의 법문언을 구체적으로 살펴보면 「산업기술보호법」 제14조 제5호는 ①인식 있는 취득·사용·공개와 ②인식 없는 기술취득 후 인식있는 사용·공개를 구분하고 있는데 대하여 「방산기술보호법」 제10조 제2호는 첫 번째 유형만을 규정하고 있는데 이러한 「산업기술보호법」의 규정형식은 동법 제정당시부터 큰 변동 없이 유지되어 왔다.

그리고 「산업기술보호법」과 같이 두 가지 유형을 모두 규정하고 있는 것으로는 예컨대 「국가첨단전략산업법」 제15조 제3호와 「부정경쟁방지법」 제2조 제3호 나목부터 바목 중 고의범에 해당하는 것들을 들 수 있다. 또한 「산업기술보호법」 제14조 제13호와 「국가첨단전략산업법」 제15조 제4호 그리고 「부정경쟁방지법」 제2조 제3호 나목부터 바목 중 중과실에 관한 행위들도 유사한 규정형식(①중대한 과실로 인한 인식 없는 취득·사용·공개와 ②기술취득 후 중과실로 인한 인식 없는 사용·공개)을 취하고 있다. 이에 대하여 「방산기술보호법」 제10조 제2호와 같이 한 가지 유형만을 규정하고 있는 것으로는 「부정경쟁방지법」 제18조⁷⁶⁾ 제1항 제3호가 있으며 중과실과 관련해서는 「방산기술보호법」 제10조 제3호가 있다. 아래의 표는 이들 규정들의 규정형식을 비교한 것이다.

〈표 5〉 인식 있는 기술유출·침해와 인식 없는 기술취득 후 인식있는 기술유출·침해에 관한 법률규정들 비교

	「방산기술보호법」 제10조	「산업기술보호법」 제14조	「국가첨단전략산업법」 제15조	「부정경쟁방지법」 제2조 제3호
①인식있는 취득·사용·공개 / 인식 없는 기술취득 후 인식있는 사용·공개	2. 제1호에 해당하는 행위가 개입된 사실을 알고 방위산업기술을 취득·사용 또는 공개하는 행위	5. 제1호부터 제4호까지에 해당하는 행위가 개입된 사실을 알고 그 산업기술을 취득·사용·공개하거나 산업기술을 취득한 후에 그 산업기술에 대하여 제1호부터 제4호까지에 해당하는 행위가 개입된 사실을 알고 그 산업기술을 사용하거나 공개하는 행위	3. 제1호 또는 제2호에 해당하는 행위가 개입된 사실을 알고 그 전략기술을 취득·사용 및 공개하거나 전략기술을 취득한 후에 그 전략기술에 대하여 제1호 또는 제2호에 해당하는 행위가 개입된 사실을 알고 그 전략기술을 사용하거나 공개하는 행위	나. 영업비밀에 대하여 부정취득행위가 개입된 사실을 알거나 중대한 과실로 알지 못하고 그 영업비밀을 취득하는 행위 또는 그 취득한 영업비밀을 사용하거나 공개하는 행위 다. 영업비밀을 취득한 후에 그 영업비밀에 대하여 부정취득행위가 개입된 사실을 알거나 중대한 과실로 알지 못하고 그 영업비밀을 사용하거나 공개하는 행위
중대한 과실로 인한 인식 없는 취득·사용·공개 / 인식 없는 기술취득 후 중과실로 인한 인식 없는 사용·공개	3. 제1호에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 방위산업기술을 취득·사용 또는 공개하는 행위	13. 제1호부터 제4호까지에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 그 산업기술을 취득·사용 및 공개하거나 산업기술을 취득한 후에 그 산업기술에 대하여 제1호부터 제4호까지에 해당하는 행위가 개입된 사실을 중대한 과실로 알	4. 제1호 또는 제2호에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하고 그 전략기술을 취득·사용 및 공개하거나 전략기술을 취득한 후에 그 전략기술에 대하여 제1호 또는 제2호에 해당하는 행위가 개입된 사실을 중대한 과실로 알지 못하	다. 영업비밀이 라목에 따라 공개된 사실 또는 그러한 공개행위가 개입된 사실을 알거나 중대한 과실로 알지 못하고 그 영업비밀을 취득하는 행위 또는

76) 「부정경쟁방지법」 제2조 제3호에 규정된 모든 “영업비밀 침해행위”가 동법 제18조(벌칙)에 의하여 형사처벌의 대상이 되는 것은 아니다.

	「방산기술보호법」 제10조	「산업기술보호법」 제14조	「국가첨단전략산업법」 제15조	「부정경쟁방지법」 제2조 제3호
		지 못하고 그 산업기술을 사용하거나 공개하는 행위	고 그 전략기술을 사용하거나 공개하는 행위	그 취득한 영업비밀을 사용하거나 공개하는 행위 바. 영업비밀을 취득한 후에 그 영업비밀이 라목에 따라 공개된 사실 또는 그러한 공개행위가 개입된 사실을 알거나 중대한 과실로 알지 못하고 그 영업비밀을 사용하거나 공개하는 행위 ※ 「부정경쟁방지법」 제18조 (벌칙) 제1항 제3호 “제1호 또는 제2호에 해당하는 행위가 개입된 사실을 알면서도 그 영업비밀을 취득하거나 사용(제13조제1항에 따라 허용된 범위에서의 사용은 제외한다)하는 행위”

그런데 이때 제기되는 의문은 그렇다면 첫 번째 유형만을 규정하고 있는 「방산기술보호법」 제10조 제2호에 의해서는 두 번째 유형인 기술취득 후 인식있는 사용·공개행위를 포섭할 수 없어서 규율의 공백이나 가벌성의 흠결이 발생하는가라는 것이다. 그런데 결론부터 말하면 첫 번째 유형은 이미 두 번째 유형을 포함하고 있어서 두 번째 유형에 관하여 규정하지 않는다고 하더라도 규율의 공백이나 가벌성의 흠결은 발생하지 않는다는 것이다. 그 이유는 다음과 같다.

첫 번째 유형과 관련하여 “취득·사용·공개”에서 중간점을 “또는”이라는 접속부사로 해석할 경우 이 유형은 제○호부터 제○호까지에 해당하는 행위가 개입되었다는 사실을 알고 그 산업기술을 ‘취득하거나 또는 사용하거나 또는 공개하는 행위’로 해석될 수 있다. 이것은 예컨대 「산업기술보호법」 제15조 제1호가 “절취·기망·협박 또는 그 밖의 부정한 방법으로 ……”라는 표현을 사용하면서 이때의 중간점을 “또는”이라는 접속부사로 밖에 해석될 수 없는 것과 같다.⁷⁷⁾ 그러면 첫 번째 유형에서의 사용과 공개는 인식있는 취득이든 아니면 인식없는 취득이든 이를 불문하고 사용과 공개에 있어서 위법사실의 개입에 대한 인식만 있으면 된다는 의미가 되는데 그렇다면 인식 없는 취득을 전제하는 두 번째 유형, 즉 적법하게 취득 후 위법사실의 개입을 인식하게 되어 사용 또는 공개하는 행위와 첫 번째 유형과는 구별되지 않게 된다.

그렇다고 두 유형의 구분을 견지하기 위하여 두 번째 유형은 인식없는 취득을 전제로 한 인식있는 사용·공개와 관련된 것이고 첫 번째 유형에서의 사용·공개는 인식있는 취득을 전제로 한 인식있는 사용·공개에 관한 것이라고 해석할 경우 이제 첫 번째 유형에서의 중간점의 해석(“또는”)은 더 이상 견지될 수 없게 될 뿐만 아니라 취득행위를 전제하지 않는 인식 있는 사용이나 공개에 대해서는

77) 그렇지 않으면 해당 유출·침해행위는 “절취·기망·협박”이 누적적 요건이 되기 때문이다.

첫 번째 유형이 적용될 수 없게 되는 문제가 발생하게 된다. 물론 기술을 물건이나 문서로만 이해할 경우 사용과 공개를 위해서는 취득이 전제되어야 하지만 기술이 네트워크상에서 접근할 수 있는 전자정보의 형태를 가지고 있는 경우 이에 대하여 접근하는 행위가 취득에 해당하는지 아니면 취득이 전제되지 않은 사용에 불과한 것인지의 경계가 명확하지 않아 또 다른 해석의 문제를 발생시키게 된다.

결론적으로 「방산기술보호법」 제10조 제2호는 「산업기술보호법」 제14조 제5호와 같이 취득 후 인식있는 사용·공개에 관하여 정하지 않았다고 하여 규율의 공백이나 가벌성의 흠결이 발생되지 않는다고 말할 수 있으며 이것은 「부정경쟁방지법」 제18조 제1항 제3호에 대해서도 그리고 중과실과 관하여 정하고 있는 「방산기술보호법」 제10조 제3호에도 그대로 적용된다.

물론 「산업기술보호법」 제14조 제5호와 「국가첨단전략산업법」 제15조 제3호가 두 가지 유형을 모두 정하고 있다고 하여 특별한 문제는 발생하지 않을 것이다.

나) 기술 유출·침해행위의 알선 등 행위

「방산기술보호법」은 방산기술 유출·침해행위의 알선 등 행위에 관하여 정하고 있지 않는데 「국가첨단전략산업법」과 관련하여 논의했던 문제점, 즉 브로커 등은 형법상 공범의 처벌규정에 의해서는 완전히 포섭될 수 없다는 문제점이 여기에서도 그대로 적용된다는 점에서 방산기술 유출·침해행위의 알선 등 행위를 유출·침해행위로 규정할 필요가 있다.⁷⁸⁾

다) 방산기술의 무단 반출 등 행위

「방산기술보호법」은 방산기술의 무단 반출 등 행위에 대하여 규정하고 있지 않는데 마찬가지로 「국가첨단전략산업법」에서 논의했던 문제점이 여기에서도 그대로 적용된다. 즉 「방산기술보호법」 제10조 제4호는 권한소멸 후 자료 등 반환거부 등을 그리고 제5호는 그 중과실범만을 규정하고 있어서 비밀유지의무자에 의한 방산기술의 무단 반출 행위는 여기에 정확히 포섭되지 않는다는 점에서 이에 관한 규정의 신설이 필요하다.

라) 방산기술의 수출 및 기술보유 대상기관의 인수·합병

「방산기술보호법」 제10조에는 방산기술의 수출 및 방산기술 보유 대상기관의 인수·합병과 관련한 방산기술 유출·침해행위에 대하여 규정하고 있지 않는데 이것은 「산업기술보호법」 제14조 제7호부터 제11호와 「국가첨단전략산업법」 제15조 제5호 및 제6호가 별도로 미승인·미신고 수출·기술보유 대상기관의 인수·합병을 기술유출·침해행위로 규정하고 있는 것과는 구별된다.

78) 같은 견해로는 송승은, 앞의 논문, 315면 이하; 조용순, 「「방위산업기술보호법」 개정안에 대한 검토: 정의규정, 침해 행위, 형사처벌 규정을 중심으로」, 『한국산업보안연구』, 제13권 제3호(2023), 한국산업보안연구학회, 60면 이하.

그러나 이것은 추측컨대 「산업기술보호법」과 「국가첨단전략산업법」은 해당 법률에 기술의 수출 및 기술보유 대상기관의 인수·합병에 관하여 상세한 규정을 두고 있는데 대하여 「방산기술보호법」은 그렇지 않은데 기인하는 것 같다. 그런데 방산기술의 수출, 기술보유 방산기업의 인수·합병을 포함한 그 지배구조에 관해서는 「방위사업법」에 상세한 규정을 두고 있을 뿐만 아니라 방산기술을 포함한 전략물자의 수출에 관해서는 「대외무역법」이 규율하고 있다. 예컨대 「방위사업법」은 외국기업을 위해 중개 또는 대리하는 행위를 하는 업으로서 군수품무역대리업에 관한 것(제3조 제12호, 제57조의2), 절충교역(제20조), 방산업체의 매매·경매 또는 인수·합병의 승인(제35조 제3항),⁷⁹⁾ 수출제한(제57조 제4항), 외국인의 국가 전략무기사업 등 참여에 관한 것(제50조의2) 등에 관하여 정하고 있고 「대외무역법」은 “국제평화 및 안전유지와 국가안보를 위하여 필요”한 물자인 전략물자⁸⁰⁾의 수출통제 등에 관하여 상세하게 정하고(동법 제19조 이하) 전략물자의 수출입과 관련한 위반행위에 대하여 상세한 처벌규정들을 두고 있다(제53조 및 제53조의). 따라서 「방산기술보호법」에 방산기술의 수출 및 방산기업의 인수·합병에 관하여 규정할 경우 이것은 「방위사업법」이나 「대외무역법」과 유사·중복규정이 될 수 있을 뿐만 아니라 자칫 일방 법률의 일방적 개정이 타방 법률에 규율의 공백이나 가별성의 흠결을 발생시킬 우려가 있는 것이 사실이다.

그러나 그렇다고 하여 방산기술의 수출 및 방산기업의 인수·합병과 관련하여 전혀 문제가 없는 것은 아니다.

즉 「산업기술보호법」 제15조 제11호는 국가핵심기술보유 대상기관의 인수·합병과 관련하여 산업통상부장관의 제한조치에 관한 명령을 이행하지 않는 경우 이를 국가핵심기술의 유출·침해행위로 규정하고 형사처벌까지 하고 있는데 대하여 「방산기술보호법」이나 「방위사업법」 그리고 「대외무역법」에는 이에 관하여 규정하는 바가 없다.

또한 「방위사업법」 제57조 제4항은 “방위사업청장은 대통령령이 정하는 바에 따라 관계행정기관의 장과 협의하여 방산물자 및 국방과학기술의 수출을 제한하거나 조정을 명할 수 있다”고 정하고 있으나 해당 명령에 대한 불이행에 대해서는 제재가 규정되어 있지 않다. 그리고 「대외무역법」 제53조에 전략물자의 승인 없는 수출 등에 관한 광범위한 처벌규정을 두고 제53조의2가 산업통상자원부장관의 전략물자등 이동중지명령에 대한 불이행에 대한 처벌규정을 두고 있으나(동조 제1항 제1호) 전략물자 등의 이동을 제한하는 궁극적인 목적이 기술보호에 있다고 하기 보다는 오히려 “국제평화 및 안전유지와 국가안보를 위하여 필요”하기 때문이라고 본다면 「방위사업법」이나 「대외무역법」으로는 「방산기술보호법」의 규율의 공백과 가별성의 흠결을 메우는 것은 충분하지 않을 것으로 판단된다.

79) 「방위산업 발전 및 지원에 관한 법률」 제11조 제5항 참조.

80) 전략물자에는

IV

별칙규정의 문제점

별칙규정에서도 동일·유사규정을 공유하는 법률들 가운데 일방 법률에 대한 일방적인 개정이 타방 법률에 규율의 공백이나 가별성의 흠결을 발생시키는 현상이 발생한다.

1. 목적범에서 단순고의범으로의 전환

2025년 1월 21일 「산업기술보호법」이 개정됨에 따라 가장 중요한 변화를 가져온 것들 중의 하나가 바로 동 개정이 종래 산업기술 또는 국가핵심기술의 유출·침해범에 대하여 고의 외에 추가적으로 요구하던 목적을 삭제하여 이를 목적범에서 단순고의범으로 전환하여 가별성의 문턱을 낮추고⁸¹⁾ 그 결과 보다 강한 보호의 강도가 요구되는 「국가첨단전략산업법」상 전략기술이나 「방산기술보호법」상 방산기술의 유출·침해범에 대한 가별성의 문턱이 높아짐으로써 보호의 강도가 상대적으로 약해졌다는 외관을 가지게 되었다는 점일 것이다.

즉 앞의 “표 4 「산업기술보호법」, 「국가첨단전략산업법」 그리고 「방산기술보호법」의 기술유출·침해행위 비교”에서도 알 수 있듯이 「산업기술보호법」은 2025년 1월 21일 개정에 의하여 종래 별칙에서 고의 외에 추가적으로 요구하던 “기술 등이 외국에서 사용하거나 사용되게 할 목적”이나 “부정한 이익을 얻거나 그 보유자에 손해를 가할 목적”을 삭제하고 행위자에게 “외국에서 사용될 것을 알면서”라는 단순한 인식만 있으면 처벌이 가능하도록 했을 뿐만 아니라 종래 “부정한 이익을 얻거나 그 보유자에 손해를 가할 목적”을 추가적으로 입증하도록 요구했던 것을 삭제하였다.

물론 「산업기술보호법」의 개정이 「국가첨단전략산업법」이나 「방산기술보호법」의 개정을 필연적으로 수반하여야 하는가에 대해서는 각 법률의 입법목적이나 취지를 고려하여 판단하여야 할 아닐 뿐만 아니라 여전히 「국가첨단전략산업법」이나 「방산기술보호법」에 규정된 법정형은 「산업기술보호법」의 것보다 높기는 하다. 그러나 문제는 유사·동일한 기술유출·침해범에게 요구하는 추가적인 주관적 요소의 존재의 여부는 입증의 정도에 영향을 미친다는 점에서 보호의 강도에도 직접적으로 영향을 미친다.

81) 이러한 평가로는 산업기술보호위원회, 『제5차 산업기술의 유출방지 및 보호에 관한 종합계획(’25~’27)』, 2024.12.31., 22면 참조(<https://kcg.korea.kr/common/download.do?fileId=198001265&tblKey=GMN>; 최종접수일: 2025년 5월 26일).

2. 형벌의 불균형

또한 벌금형과 관련해서도 「산업기술보호법」의 2025년 1월 21일 개정에 의하여 형벌의 불균형이 발생하게 되었다.

즉 동 개정에 의하여 동법 제36조 제1항에 정한 국가핵심기술의 해외유출·침해행위에 대한 벌금형은 15억원에서 65억원으로 상향되었으나 정작 국가핵심기술보다 보호의 강도가 강해야 하는 「국가첨단전략산업법」(제50조 제1항)이나 「방산기술보호법」(제21조 제1항)의 경우 「산업기술보호법」에 정한 해외유출·침해행위와 동일·유사한 행위에 대하여 20억원 이하의 벌금을 부과하고 있어서 벌금형과 관련하여 형벌의 역전현상이 발생하게 되었다.

그런데 「산업기술보호법」의 개정으로 인하여 보다 심각한 결과를 초래하게 된 것은 바로 「국가첨단전략산업법」 제50조 제2항이다.

「국가첨단전략산업법」 제50조 제2항은 “전략기술을 외국에서 사용하거나 사용되게 할 목적으로 제15조제5호부터 제8호까지의 어느 하나에 해당하는 행위를 한 자는 제1호부터 제3호의 경우(제1항)와 달리 20년 이하의 징역 또는 20억원 이하의 벌금에 처한다”⁸²⁾고 규정하고 있는데 이와 동일·유사 유출·침해행위에 대하여 「산업기술보호법」 제36조 제1항은 3년 이상의 유기징역과 65억원 이하의 벌금을 병과하도록 정하고 있어서 보다 강한 보호의 강도가 요구되는 「국가첨단전략산업법」의 형벌이 「산업기술보호법」의 형벌보다 경한 것이 되었다.

그런데 이것은 「국가첨단전략산업법」 제50조 제2항에 상응하는 「(구)산업기술보호법」 제36조 제2항⁸³⁾(15년 이하의 징역 또는 15억 이하의 벌금)이 2025년 1월 21일 일방적으로 개정되면서 예기치 않게 「국가첨단전략산업법」 제50조 제2항의 법정형이 동일·유사 유출·침해행위를 정한 「산업기술보호법」의 것보다 경한 것이 된 데에 기인한다. 종래 「(구)산업기술보호법」은 국가핵심기술의 해외유출·침해행위와 관련하여 (구)제14조 제1호부터 제3호까지의 행위에 대하여 벌칙에서 가장 중한 형벌을 부과하면서도(3년 이상의 유기징역과 15억원 이하의 벌금의 병과) 동조 제4호 이하의 행위에 대해서는 국가핵심기술이든 산업기술이든 이를 불문하고 경한 형벌을 부과했었다(15년 이하의 징역 또는 15억원 이하의 벌금). 그런데 2025년 1월 21일 개정은 국가핵심기술의 해외유출·침해

82) 앞의 “표 4 「산업기술보호법」, 「국가첨단전략산업법」 그리고 「방산기술보호법」의 기술유출·침해행위 비교”를 살펴보면 「국가첨단전략산업법」 제50조 제2항이 적용대상으로 하는 전략기술 유출·침해행위는 미승인 등 전략기술의 수출(제15조 제5호), 외국에서 사용하거나 사용되게 할 목적 미승인 등 대상기관의 해외인수·합병(동조 제6호), 계약 등 비밀유지의무자의 권한소멸 후 자료 등 반환거부 등(제7호) 그리고 적법한 경로를 통하여 전략기술이 포함된 정보를 제공받은 자의 목적 외 사용·공개(제8호)인데 이에 상응하는 「산업기술보호법」상 산업기술 또는 산업기술 유출·침해행위는 각각 동법 제14조 제7호, 제9호, 제3호 그리고 제12호이다.

83) 「(구)산업기술보호법」 제36조

“①국가핵심기술을 외국에서 사용하거나 사용되게 할 목적으로 제14조제1호부터 제3호까지의 어느 하나에 해당하는 행위를 한 자는 3년 이상의 유기징역에 처한다. 이 경우 15억원 이하의 벌금을 병과한다. <신설 2019. 8. 20.>

②산업기술을 외국에서 사용하거나 사용되게 할 목적으로 제14조 각 호(제4호를 제외한다)의 어느 하나에 해당하는 행위를 한 자(제1항에 해당하는 행위를 한 자는 제외한다)는 15년 이하의 징역 또는 15억원 이하의 벌금에 처한다. <개정 2008. 3. 14., 2016. 3. 29., 2019. 8. 20.>”.

행위와 산업기술의 해외유출·침해행위를 명확히 구분하여 전자에 대해서는 제14조에 정한 거의 모든 유출·침해행위(제1호부터 제12호까지의 행위(신설된 규정들을 포함))에 대하여 벌칙에서 가장 중한 형(3년 이상의 유기징역과 65억원 이하의 벌금의 병과)을 그리고 후자에 대해서는 제14조제1호부터 제6호까지 및 제12호의 행위에 대하여 경한 형(15년 이하의 징역 또는 30억원 이하의 벌금)을 부과하도록 개정되었다.

만약 국가핵심기술이 관건이 되는 한 그 해외유출·침해를 발생시키는 제14조 제1호부터 제12호까지의 행위에 대해서는 어떤 유형의 행위인지를 구별하지 않고 모두 벌칙에서 중한 형을 부과하도록 한 「산업기술보호법」에 대한 입법자의 정책적 결단이 특별히 부당한 것이 아니라면 이러한 가치판단은 「국가첨단전략산업법」에 대해서도 그대로 적용되어야 하는 것이 일관적일 것이다. 즉 「국가첨단전략산업법」이 「산업기술보호법」의 것과 동일·유사한 유출·침해행위를 전략기술의 유출·침해행위로 규정할 것이라면 각 기술유출·침해행위의 죄질의 경중에 대한 「산업기술보호법」의 가치판단은 「국가첨단전략산업법」에 대해서도 그대로 적용되어야 한다.⁸⁴⁾ 그렇다면 현행 「국가첨단전략산업법」 제50조가 전략기술의 해외유출·침해행위를 제15조 제1호부터 제3호의 경우와 제15조제5호부터 제8호까지의 경우로 구분하여 각기 다른 형을 부과하고 있는 것은 개정되어야 할 것으로 판단된다.

3. 미수범 및 예비·음모

「산업기술보호법」⁸⁵⁾과 「방산기술보호법」⁸⁶⁾은 기술의 해외유출·침해행위에 대한 미수범과 예비·음모를 처벌하고 있는데 대하여 「국가첨단전략산업법」에는 미수범과 예비·음모에 대한 처벌규정을 두고 있지 않은데⁸⁷⁾ 그 이유는 명확하지 않다.

물론 일견 전략기술은 「산업기술보호법」상 국가핵심기술이나 산업기술에 포섭된다는 의미에서 (대는 소를 포함한다, Argumentum a fortiori) 일반법인 「산업기술보호법」에 대하여 「국가첨단전략산업법」은 특별법의 지위에 있기 때문에 「국가첨단전략산업법」에 관련규정이 없다고 하더라도 전략기술에는 (특별히 다른 규정이 없는 한) 일반법인 「산업기술보호법」이 당연히 적용될 수 있으며 「국가첨단전략산업법」에 미수범 및 예비·음모에 대한 처벌규정이 명문으로 규정되어 있지 않더라도 「산업기술보호법」의 미수범 및 예비·음모 처벌규정을 적용할 수 있는 것처럼 보인다. 그리고 「형법」 제25조 제2항은 따라 “미수범의 형은 기수범보다 감경할 수 있다”고 규정하고 있기 때문에 예비·음모 처벌규정과 같이 법정형을 특정할 필요도 없다.

그러나 「국가첨단전략산업법」에 미수범 및 예비·음모에 대한 처벌규정을 두지 않는 경우 미수범의

84) 물론 각 법률에서 보호하고자 하는 기술의 보호의 강도에 따라 구체적인 법정형의 수치는 상이할 것이다.

85) 「산업기술보호법」 제36조(벌칙) 제7항(미수범); 제37조(예비·음모).

86) 「방산기술보호법」 제21조(벌칙) 제6항(미수범); 제22조(예비·음모).

87) 이에 대한 비판으로는 조용순, 앞의 논문(2022), 515면 이하.

형량의 기준은 「국가첨단전략산업법」상 전략기술 유출·침해범의 기수범이 아니라 「산업기술보호법」상 국가핵심기술의 유출·침해범의 기수범이 될 수밖에 없는데 그렇게 되면 전략기술에 대한 보호의 강도는 국가핵심기술의 것과 동일하게 되는 문제가 발생하게 된다. 전략기술의 보호의 강도가 국가핵심기술의 보호의 강도와 동일하게 되는 문제는 예비·음모의 경우에도 마찬가지로 발생한다.

더욱이 「산업기술보호법」과 「국가첨단전략산업법」은 각기 다른 법률일 뿐만 아니라 후자의 법 적용에 있어서는 전자에 종속되어야 한다는 원칙도 존재하지 않는 이상 전략기술 유출·침해범죄의 미수·예비·음모를 검사가 기소재량에 따라 기소하지 않는다고 하더라도 해당 기소는 「국가첨단전략산업법」 위반에 해당되지 않아 공소기각의 사유도 되지 않는다(「형사소송법」 제327조(공소기각의 판결) 제2호).

물론 기수범도 아닌 미수범·예비·음모의 경우에 전략기술과 국가핵심기술에 대한 보호의 강도가 동일하게 되는 문제는 애초부터 전략기술과 국가핵심기술의 유출·침해행위에 대한 법정형이 높기 때문에 부당하게 낮은 형량을 선고받는 경우는 없을 것이라고 말할 수도 있을 것이다. 그러나 전략기술과 국가핵심기술을 별개의 다른 법률에 개별적으로 규율하고 있는 입법목적과 취지를 고려한다면 아무리 기수범도 아닌 미수범·예비·음모의 경우라고 하더라도 죄질의 경중에 상응하는 형량이 규정되는 것이 타당하다.⁸⁸⁾

4. 몰수·추징규정

「국가첨단전략산업법」에는 전략기술을 유출·침해한 자에 대한 몰수·추징규정을 두고 있지 않다. 물론 이것은 범죄행위로 인하여 얻은 재산의 몰수·추징은 전략기술의 유출·침해행위의 경우에는 포기하겠다는 입법자의 의도적인 부작위는 아닐 것이다. 여기에서도 이러한 몰수·추징규정의 부재는 「산업기술보호법」의 관련규정의 적용을 염두에 둔 입법경제에 기인하는 것으로 추측된다.

물론 일견 몰수·추징은 가벌성을 창설하는 것도 그리고 책임귀속의 시간적 범위(미수·예비·음모)를 결정하는 것도 아닐 뿐만 아니라 이미 앞서 언급한 바와 같이 전략기술은 「산업기술보호법」상 국가핵심기술이나 산업기술에 포섭된다는 의미에서 일반법인 「산업기술보호법」에 대하여 「국가첨단전략산업법」은 특별법의 지위에 있기 때문에 「국가첨단전략산업법」에 관련규정이 없다고 하더라도 전략기술에는 (특별히 다른 규정이 없는 한) 일반법인 「산업기술보호법」이 당연히 적용될 수 있으며 이것은 몰수·추징규정의 경우에도 동일한 것이 적용되는 것처럼 보인다. 또한 설령 몰수·추징규정이 존재하지 않는다고 하더라도 「범죄수익은닉규제」의 적용대상인 이상 범죄로부터 유래하는 경제적 이익은 몰수할 수 있다고도 말할 수도 있을 것이다.

그러나 「국가첨단전략산업법」에 특별한 준용규정이 존재하지 않을 뿐만 아니라 「국가첨단전략산업법」은 「범죄수익은닉규제법」 제2조 제2호 나목에 열거된 대상범죄에 포함되지 않아 동호 가목에

88) 같은 취지로는 조용순, 앞의 논문(2022), 502면 이하.

따라 “사형, 무기 또는 장기 3년 이상의 징역이나 금고”에 처해지는 경우에만 「범죄수익은닉규제법」의 적용대상이 되기 때문에 일부 전략기술의 유출·침해행위에 대해서만 동법이 적용될 수 있을 뿐이다.

더욱이 「산업기술보호법」과 「국가첨단전략산업법」은 각기 다른 법률일 뿐만 아니라 후자의 법적 용에 있어서는 전자에 종속되어야 한다는 원칙도 존재하지 않는 이상 전략기술 유출·침해범죄에 대하여 몰수·추징을 하지 않는다고 하더라도 「국가첨단전략산업법」 위반이 되지 않아 항소의 대상(「형사소송법」 제361조의5(항소이유) 제1호)이 되지도 않는다.

또한 「형법」 제41조 제9호에 의하여 「형벌」의 하나로 규정되어 있는 만큼(학설상으로는 단순히 형벌의 부수효과로 이해하려는 견해도 있기는 하지만) 어떤 형벌을 부과할 것인가 혹은 이를 통하여 어떤 법률효과를 발생시키도록 할 것인가는 개별적으로 해당 법률에 규정하는 것이 타당하다.

5. 양벌규정의 문제점

양벌규정의 실효성에 관한 문제, 특히 개인과 동일한 벌금형의 실효성의 문제, 공소시효의 문제,⁸⁹⁾ 벌금형의 승계에 관한 문제⁹⁰⁾는 비단 「산업기술보호법」, 「국가첨단전략산업법」 혹은 「방산기술보호법」만의 문제가 아니라 양벌규정 전반에 관한 문제이다.

특히 일반적으로 양벌규정에 정한 법인에 대한 벌금형은 자연인에 대한 벌금형과 동일한 벌금형을 부과하도록 하는 경우가 많은데 벌금형에 대한 자연인의 감수성과 법인의 감수성은 동일하지 않을 것이다. 이러한 점을 고려할 때 최근에 법인처벌에 소극적이던 독일이 「2020년 단체재법(안) (“Entwurf des Gesetzes zur Sanktionierung von verbandsbezogenen Straftaten, Verbandssanktionengesetz – VerSanG”)⁹¹⁾을 발의하면서 기업의 매출을 기준으로 벌금형을 정하고 있는데 예컨대 다국적기업의 경우 최근 3년 간의 평균 매출의 30% 이하의 벌금을 부과하도록 한 것은 시사하는 바가 크다고 볼 수 있다.⁹²⁾

다만 우리나라의 경우 벌금형을 법인의 매출을 기준으로 정하고 있는 경우를 찾아볼 수 없다는 점을 고려할 때 적어도 「부정경쟁방지법」 제19조에 정한 바와 같이 법인에 대하여 본조에 정한 벌금형의 3배 이하의 벌금에 처하는 방안도 생각할 수 있을 것이다.

89) 이에 관한 상세한 것은 김유근·박성민·유주성·정배근(김유근), 『법인처벌을 위한 형사소송절차에 관한 연구』, 한국형사법무정책연구원, 2024, 152면 이하 참조.

90) 이에 관한 상세한 것은 김유근·박성민·유주성·정배근(김유근), 앞의 보고서, 177면 이하 참조.

91) BT-Drucksache 19/23568, S. 1(Entwurf eines Gesetzes zur Stärkung der Integrität in der Wirtschaft Art. 1 “Gesetz zur Sanktionierung von verbandsbezogenen Straftaten (Verbandssanktionengesetz – VerSanG)”). 다국적기업인 경우의 법인에 대한 형벌은 독일 「법인처벌법안」 제9조 제1항 제2문 참조. 이에 관한 상세한 것은 김유근·박성민·유주성·정배근(김유근), 『법인처벌을 위한 형사소송절차에 관한 연구』, 한국형사법무정책연구원, 2024, 20면 이하.

92) 다국적기업인 경우의 법인에 대한 형벌은 독일 「법인처벌법안」 제9조 제1항 제2문 참조. 이에 관한 상세한 것은 김유근·박성민·유주성·정배근(김유근), 앞의 보고서, 20면 이하.

V

결론 및 정책제언

1. 결론

◆ 법적용에 있어서의 혼란을 방지하기 위한 대책의 필요성

가. 동일·유사규정들을 공유하는 서로 다른 법률들에서 일방 법률에 대한 일방적인 개정은 타방 법률에 규율의 공백 또는 가벌성의 흠결을 발생시킬 위험이 있음.

○ 「산업기술보호법」, 「국가첨단전략산업법」, 「방산기술보호법」 그리고 더 나아가서는 「부정경쟁방지법」(영업비밀에 관련된 규정들에 한함) 등의 경우 보호객체(예컨대 산업기술·국가핵심기술, 전략기술, 방산기술 그리고 영업기술)의 유출·침해행위, 그 처벌규정의 규정형식(예컨대 목적범으로 규정할 것인가의 여부 등) 그리고 책임귀속의 수준(어느 행위까지 형사처벌의 대상으로 할 것인가, 예컨대 미수·예비·음모(시간적 수준), 과실범까지 처벌할 것인가(어느 정도의 주관적 구성요건이 요구되는가의 여부), 자연인을 넘어 법인까지 행위주체로 볼 것인가(행위주체의 범위) 등의 문제) 등에서 동일·유사 규정들을 공유할 뿐만 아니라 규정순서도 공유함.

○ 그런데 이와 같이 동일·유사규정들을 공유하는 서로 다른 법률들에서 일방 법률에 대한 일방적인 개정은 타방 법률에 규율의 공백 또는 가벌성의 흠결을 발생시킬 위험이 있으며 실제로 「산업기술보호법」의 최근의 개정으로 인하여 미쳐 이에 상응하는 개정이 뒤따르지 못한 「국가첨단전략산업법」이나 「방산기술보호법」에 규율의 공백이나 법적용에 있어서 모순이 발생하게 됨(예컨대 보호의 강도에 상응하지 않은 형벌의 역전현상 등).

○ 적어도 「산업기술보호법」과 「국가첨단전략산업법」의 소관부처(산업통상자원부)가 동일한 만큼 일방 법률의 개정이 타방 법률에 어떤 영향을 미치는가에 대한 입법평가가 필요함.

나. 규율의 공백의 보충을 위한 법률들 간의 상호보충적 법적용에는 한계가 존재함.

○ 「산업기술보호법」에서의 산업기술은 동법에 따르는 국가핵심기술, 「국가첨단전략산업법」상 전략기술 그리고 「방산기술보호법」상 방산기술을 모두 포괄하는 개념이어서 원칙적으로 일방 법률에 발생하는 규율의 공백은 다른 법률에 의하여 상호보충될 수 있음.

○ 이러한 상호보충적 법적용은 입법정책적 관점에서는 규율의 경제성을 기할 수 있고 행정절

차 또는 산업육성이라는 관점에서는 규율의 효율성을 제고할 수 있으나 형사책임의 확정에 있어서는 죄형법정주의의 원칙, 특히 법률주의(가벌성의 기준), 명확성의 원칙 그리고 이를 통한 수범자들의 예측가능성의 담보라는 관점이 규율의 경제성에 우선함.

- 따라서 예컨대 「국가첨단전략산업법」이나 「방산기술보호법」에서의 규율의 공백, 특히 가벌성의 창설이나 형사책임의 귀속에 중요한 핵심적인 내용은 「산업기술보호법」의 관련규정을 단순히 원용하여 적용될 수 있는 것은 허용되지 않는다고 보아야 함.
- 이러한 의미에서 특히 「국가첨단전략산업법」에 누락되어 있는 미수범·예비·음모, 몰수·추징, 양벌규정 등의 규정들은 「산업기술보호법」에 의존할 것이 아니라 「국가첨단전략산업법」 자체에 규정될 필요가 있으며, 「방산기술보호법」의 경우에도 누락된 규정들이 있다면 동일한 것이 적용됨.

다. 가벌성을 확정하는 기준이 되는 국가핵심기술과 전략기술의 명확한 구별의 필요성

- 특정 기술유출 침해행위에 대하여 「산업기술보호법」을 적용할 것인지 아니면 「국가첨단전략산업법」을 적용할 것인지는 해당 기술이 국가핵심기술인지 아니면 전략기술인지의 여부에 따라 결정되며 형사책임과 관련해서는 이 결정은 가벌성의 핵심적인 내용을 결정하는 중요한 기준이 됨.
- 죄형법정주의의 원칙에 따라 원칙적으로 포괄적인 위임입법은 허용되지 않으나 발달속도가 매우 빠른 국가핵심기술이나 전략기술을 법률에 빠짐없이 열거하는 것은 현실적으로 가능하지 않다는 점을 고려할 때 어느 정도의 포괄적인 위임입법은 불가피하며 가벌성을 확정할 수 있을 정도의 명확성과 특정성 그리고 상세화가 담보되는 한 죄형법정주의에 반하지 않는다고 보는 것이 타당함(헌법재판소 결정).
- 그러나 하위입법인 「국가핵심기술 지정 등에 관한 고시」[별표]와 「국가첨단전략기술 지정 등에 관한 고시」[별표]에 열거된 국가핵심기술과 전략기술의 목록이 죄형법정주의의 원칙을 충족시킬 수 있을 정도로 명확하고 상세화된 것인가에 대해서는 의문이 제기됨.
- 특히 문제가 되는 것은 동일한 내용의 기술이 동시에 국가핵심기술로도 그리고 전략기술로도 지정되어 있어서 (행정규제 및 산업기술육성장 효율성을 제고할 수는 있어도) 해당 기술에 대하여 어느 법률을 적용하여야 하는지가 명확하지 않게 되어 법적용자는 자의적인 적용법조의 선택을 강요받게 될 뿐만 아니라 죄형법정주의의 파생원칙인 명확성의 원칙에 전면으로 반하고 수범자에게 예측가능성도 제공하지 못함.

◆ 각 법률에서 요구되는 보호의 강도에 상응하는 기술의 해외유출·침해행위에 대한 법정형의 차등화의 필요성

- 산업기술 및 국가핵심기술, 전략기술 그리고 방산기술을 각기 다른 법률, 즉 「산업기술보호법」, 「국가첨단전략산업법」 그리고 「방산기술보호법」으로 규율하는 궁극적인 이유는 각 기술들의 보호의 강도가 다른데 기인하며 이에 상응하여 행정절차 및 육성정책이 상이함.
- 이것은 이들 기술들의 유출 침해행위에 대한 형사책임을 정하는 경우에도 동일한 것이 적용되며 특히 어느 정도의 보호의 강도가 요구되는가에 따라 해당 기술의 유출·침해행위에 대한 법정형이 정해져야 함.
- 목적범이나 비밀유지의무자의 행위는 죄질의 경중이 일반인의 경우보다 중하다는 점을 고려한다면 법정형에 차등을 두는 방안도 고려할 만함.

2. 정책제언 - 개선안 제시

이상의 문제의식을 바탕으로 「산업기술보호법」과 「국가첨단전략산업법」에 대한 구체적인 개선방안을 제시하면 다음과 같음.

다만 이 개선안은 법률의 체계정합성의 관점에서 제시된 것임을 밝혀둔다. 주요 해외 입법례로부터 얻을 수 있는 시사점이나 새로운 기술유출 침해행위의 등장으로 인한 규율의 공백이나 가벌성의 흠결의 보충의 문제는 추후에 다루도록 한다.

가. 「산업기술보호법」 개정안

1) 제14조(산업기술의 유출 및 침해행위 금지)

현행법	개정안	설명
제14조(산업기술의 유출 및 침해행위 금지) 1. ~ 13. (생략)	제14조(산업기술의 유출 및 침해행위 금지) 1. ~ 13. (현행과 같음)	
제14조의4(외국에서의 행위에 대한 적용) (생략)	제14조의4(외국에서의 행위에 대한 적용) (현행과 같음)	

2) 제36조(벌칙)

현행법	개정안	설명
제36조(벌칙) ① ~ ④ (생략)	제36조(벌칙) ① ~ ⑧ (현행과 같음)	
<p>※ 다만 「부정경쟁방지법」 제18조(벌칙)이 재산상의 이득에 따라 벌금액을 차등화하고 있기는 하지만 동법이 개인적 법익의 보호에 그 초점이 맞추어져 있다는 점에서 국가적·사회적 법익의 보호가 전면에 있는 「산업기술보호법」에서는 신중한 검토가 필요함.</p> <p>※ 2025.1.21. 개정 당시 목적범을 단순고의범으로 전환 시 단순고의범의 형량을 하향조정하고 목적범의 가중처벌규정을 신설하면서 법정형을 현행 형량으로 정함으로써 구법의 입법취지를 살리는 한편 죄질의 경중을 구분할 수 있도록 하는 방안도 고려할 만함.</p> <p>※ 일반인에 비하여 비밀유지의무자의 위법행위는 죄질의 경중이 중하다고 본다면 가중처벌의 필요성이 있음.</p> <p>※ 제7항에서 명령불이행죄의 경우 미수와 기수를 구별하는 것이 가능한지 의문이기는 하다.</p>		
제36조의2(비밀유지명령 위반죄) ① ~ ② (생략)	제36조의2(비밀유지명령 위반죄) ① ~ ② (현행과 같음)	
제37조(예비·음모) ① ~ ② (생략)	제37조(예비·음모) ① ~ ② (현행과 같음)	- 다만 명령불이행죄의 예비·음모의 성립여부에 대한 검토가 필요함.
제38조(양벌규정) 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제36조 제1항부터 제4항까지의 어느 하나에 해당하는 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인에게도 해당 조문의 벌금형을 과(科)한다. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.	제38조(양벌규정) ----- ----- ----- ----- ----- 제36조제1항부터 제4항까지의 ----- ----- ----- 그 법 인에게는 해당 조문에 규정된 벌금형의 3배 이하의 벌금형을, 그 개인에게는 해당 조문 의 벌금형을 과(科)한다. ----- ----- ----- -----	- 신설한 과실범 처벌규정(제4항의2) 추가 - 개인에 대한 벌금형이 애초부터 매우 높기는 하지만 법인과 개인에 대한 벌금액을 차등함으로써 법인의 관리감독책임을 강화함. - 법정형은 영업비밀 침해·유출과 관련한 「부정경쟁방지법」 제19조 양벌규정의 것에 따른 것임. 이상적으로는 최근 3년간의 매출의 30% 정도가 적절하다고 판단됨(최근 독일 법인 처벌법 법률안).

나. 「국가첨단전략산업법」 개정안

「국가첨단전략산업법」에 정한 국가첨단전략기술(이하 “전략기술”이라 한다)은 「산업기술보호법」에 정한 산업기술 또는 국가핵심기술에 비하여 보다 강한 보호가 요구된다는 점에서 전략기술의 유출·침해행위는 적어도 「산업기술보호법」상 유출·침해행위유출·침해행위를 내포하고 있어야 할 것이다. 이러한 관점에서 「산업기술보호법」에 비추어 누락된 유출·침해유형들을 보완하였다.

1) 제15조(전략기술 유출 및 침해행위 금지)

이하의 정책제언은 장기적인 관점에서 전략기술 유출 및 침해행위를 「산업기술보호법」 제14조와 별칙인 제36조에 상응시킨 것으로서 경우에 따라서는 각호를 이동시켰다.

2) 제50조(벌칙)

현행법	개정안	설명
<p>제50조(벌칙) ① 전략기술을 외국에서 사용하거나 사용되게 할 목적으로 제15조제1호부터 제3호까지의 어느 하나에 해당하는 행위를 한 자는 5년 이상의 유기징역에 처한다. 이 경우 20억원 이하의 벌금을 병과한다.</p>	<p>제50조(벌칙) ① 전략기술이 외국에서 사용될 것을 알면서 제15조제1호부터 제10호까지의 ----- ----- ----- ----- 85억원 ----- -----.</p>	<ul style="list-style-type: none"> - 목적법을 단순고의범으로 개정. - 적용대상 유출·침해행위를 「산업기술보호법」 제36조제1항에 상응시킴. - 동조에 상응하는 「산업기술보호법」 제36조제1항(국가핵심기술)의 법정형이 2025. 1.21. 개정으로 15억원에서 65억원으로 상향된 것을 반영한 것임(약 4.3배).
<p>② 전략기술을 외국에서 사용하거나 사용되게 할 목적으로 제15조제5호부터 제8호까지의 어느 하나에 해당하는 행위를 한 자는 20년 이하의 징역 또는 20억원 이하의 벌금에 처한다.</p>	<p>〈삭제〉</p>	<ul style="list-style-type: none"> - 종래의 제2항의 적용대상을 제1항으로 옮김.
<p>③ 제15조 각 호(제4호·제6호 및 제8호는 제외한다)의 어느 하나에 해당하는 행위를 한 자는 15년 이하의 징역 또는 15억원 이하의 벌금에 처한다.</p>	<p>② 제15조제1호부터 제9호까지의 어느 하나에 해당하는 행위를 한 자는 15년 이하의 징역 또는 15억원 이하의 벌금에 처한다.</p>	<ul style="list-style-type: none"> - 「산업기술보호법」 제36조제2항에 상응시킴.
<p>④ 제15조제4호 또는 제8호에 해당하는 행위를 한 자는 5년 이하의 징역 또는 5억원 이하의 벌금에 처한다.</p>	<p>③ 제15조제10호 또는 제11호에 ----- ----- -----.</p>	
<p>〈신설〉</p>	<p>④ 제1항부터 제3항까지의 죄를 범한 자가 그 범죄행위로 인하여 얻은 재산은 이를 몰수한다. 다만, 그 전부 또는 일부를 몰수할 수 없는 때에는 그 가액을 추징한다.</p>	<ul style="list-style-type: none"> - 몰수·추징규정 신설 - 「산업기술보호법」 제36조제5항에 상응시킴.
<p>⑤ (생략)</p>	<p>⑤ (현행과 같음)</p>	
<p>〈신설〉</p>	<p>⑥ 제1항 또는 제2항까지의 미수범은 처벌한다.</p>	<ul style="list-style-type: none"> - 미수범 처벌규정 신설 - 다만 다만 명령불이행죄의 경우 미수와 기수를 구별하는 것이 가능한지 의문이기는 하다. - 「산업기술보호법」 제36조제7항에 상응시킴.
<p>〈신설〉</p>	<p>⑦ 제2항 또는 제3항까지의 규정에 따른 징역형과 벌금형은 이를 병과할 수 있다.</p>	<ul style="list-style-type: none"> - 벌금의 병과규정 신설 - 「산업기술보호법」 제36조제8항에 상응시킴.
<p>〈신설〉</p>	<p>제50조의2(예비·음모) ① 제50조제1항의 죄를 범할 목적으로 예비 또는 음모한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.</p>	<ul style="list-style-type: none"> - 예비·음모 규정 신설 - 「산업기술보호법」 제37조(예비·음모)에 상응시킴.

현행법	개정안	설명
	<p>②제36조제2항의 죄를 범할 목적으로 예비 또는 음모한 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.</p>	
<p>〈신설〉</p>	<p>제50조의3(양벌규정) 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제50조제1항부터 제3항까지의 어느 하나에 해당하는 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인에게도 해당 조문의 벌금형을 과(科)한다. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.</p>	<ul style="list-style-type: none"> - 양벌규정 신설 - 「산업기술보호법」 제38조(양벌규정)에 상응시킴.

[참고문헌]

- 김동준, “영업비밀 성립요건 중 경제적 유용성”, 『강원법학』, 제52호(2017), 강원대학교 비교법학연구소, 561-595면.
- 김정환, ‘산업기술의 유출방지 및 보호에 관한 법률’에 대한 형사법적 검토, 『형사정책연구』, 한국형사법무정책연구원, 제78호(2009), 29-58면.
- 노태악(편), 『주석 형사소송법(I)』, 한국사법행정학회, 2022(“주석 형사소송법(2022)(저자)”로 인용한다).
- 박상기·전지연, 『형법5학』, 제5판, 집현재, 2021.
- 박성준, “미중 기술패권경쟁과 우리나라의 전략 - 반도체”, 『Futures Brief』, 국회미래연구원, 제23-1호(2023.1.)(<https://www.nafi.re.kr/new/report.do?mode=view&articleNo=4134>; 최종접속일: 2025년 6월 3일).
- 박찬걸, 『형법각론』, 박영사, 2022.
- 산업기술보호위원회, 『제5차 산업기술의 유출방지 및 보호에 관한 종합계획('25~'27)』, 2024.12.31. (<https://kcg.korea.kr/common/download.do?fileId=198001265&tblKey=GMN>; 최종접속일: 2025년 5월 26일).
- 선중수, “산업기술유출의 개념과 형사책임 - 헌법재판소 2013.7.25. 자 2011헌바39 결정 -”, 『과학기술법연구』, 제20권 제2호(2014), 77-106면.
- 송승은, “방위산업기술 유출에 대한 형사법적 대응방안”, 『법률실무연구』, 제13권 제1호(2025), 사단법인 한국법이론실무학회, 297-327면.
- 신알찬·권솔, “한국 산업의 기술유출 방지를 위한 현행 법제 검토 및 개선방안에 대한 고찰- 형사적 규제 확대를 중심으로 -”, 『한국산업보안연구』, 제5권 제1호(2015), 한국산업보안연구학회, 7-42면.
- 임웅·이현정·박성민, 『형법각론』, 제14판, 법문사, 2025.
- 정성근·박광민, 『형법각론』, 제3판, 삼영사, 2011.
- 조용래·김현수·성경모, 『경제안보·기술안보 법제 진단·분석 프레임워크 개발과 적용방안』, STEPI Insight, 제318호(2023.12.20.), 과학기술정책연구원(<https://www.stepi.re.kr/site/stepiko/report/View.do?reIdx=328&pageIndex=1&cateCont=A0501&searchYear=&searchCondition=&searchKeyword=&searchSort=>; 최종접속일: 2025년 6월 3일).
- 조용순, 「「방위산업기술보호법」 개정안에 대한 검토: 정의규정, 침해행위, 형사처벌 규정을 중심으로」, 『한국산업보안연구』, 제13권 제3호(2023), 한국산업보안연구학회, 47-71면.
- 조용순, “국가첨단전략산업법상 전략기술의 유출·침해행위 및 형사처벌 규정에 대한 문제점과 개선방안”, 『산업재산권』, 한국지식재산학회, 제72호(2022), 473-527면.
- 차승민·김우리나라, “산업기밀유출에 대한 법적 제재: 방위산업을 중심으로”, 『한국산업보안연구』, 제1권 제11호(2017), 191-222면.
- 최진태·정유한, “국가주요기술 해외유출 특징 분석 및 과제 : 주요 기술유출 사례연구를 중심으로”, 『한

- 국산업보안연구』, 제12권 제2호(2022), 한국산업보안연구학회, 137-160.
- 하지현·이현희, “산업기술유출 사건에서 산업기술의 개념과 형사책임에 관한 소고-2011헌바39 결정을 중심으로-”, 『법학논총』, 제37권 제4호(2013), 단국대학교 법학연구소, 521-552면.
- 法律時報社, “資料 国家秘密法案新旧条文对照表”, 『法律時報』, 59卷5号 (通卷721号) (1987.4.1.), 54-55頁.
- 湯野基生, “【中国】食糧安全保障法の制定”, 『外国の立法』, No. 299-2(2024.5), 国立国会図書館 調査及び立法考査局(chrome-extension://efaidnbmnnnibpcajpcgicfindmkaj/https://dl.ndl.go.jp/view/prepareDownload?itemId=info:ndljp/pid/13586435; 최종접속일: 2025년 6월 3일).
- 湯野基生, “台湾：国家安全法の改正”, 『外国の立法』, No. 296(2023. 6), 国立国会図書館 調査及び立法考査局(chrome-extension://efaidnbmnnnibpcajpcgicfindmkaj/https://dl.ndl.go.jp/view/prepareDownload?itemId=info:ndljp/pid/12888736; 최종접속일: 2025년 5월 3일).
- 『글로벌이코노믹』 2024년 11월 4일 보도, “美 재무부, 군사 기지 인근 중국의 토지 매입 규제 강화”(https://www.g-enews.com/article/Global-Biz/2024/11/202411040743076951fbbec65dfb_1; 최종접속일: 2025년 5월 30일).
- 『노컷뉴스』 2023년 2월 17일 보도, “軍기지 옆이 중국땅? 미국 또 '깜짝'”(https://www.nocutnews.co.kr/news/5897044; 최종접속일: 2025년 5월 30일).
- 『동아일보』 2024년 8월 21일 보도 ““中서 韓배터리 특허 빼려고 입증 어려워… LCD처럼 당할 판””(https://www.donga.com/news/Economy/article/all/20240821/126610259/2; 최종접속일: 2025년 6월 20일)
- 『동아일보』 2024년 2월 7일 보도 “5년간 산업기술 96건 해외 유출, 반도체 38건으로 가장 많아”(https://www.donga.com/news/Economy/article/all/20240207/123421696/1; 최종접속일: 2024년 3월 21일).
- 『동아일보』 2023년 6월 8일 보도 “한국 근무 中연구원, 의료로봇 기술 1만건 유출”(https://www.donga.com/news/Society/article/all/20230608/119665869/1#:~:text=%5B%EA%B8%B0%EC%88%A0%20%EC%9C%A0%EC%B6%9C%20%EB%B9%A8%EA%B0%84%EB%B6%88%5D%20%EA%B5%AD%EB%82%B4%20%EB%8C%80%ED%98%95%EB%B3%91%EC%9B%90%20%EC%97%B0%EA%B5%AC%EC%86%8C%EC%84%9C%20%EC%9D%BC%ED%95%98%EB%A9%B0,%EC%9E%90%EB%A3%8C%201%EB%A7%8C%EC%97%AC%20%EA%B1%B4%EC%9D%84%20%EC%A4%91%EA%B5%AD%EC%9C%BC%EB%A1%9C%20%EC%9C%A0%EC%B6%9C%ED%95%9C%20%ED%98%90%EC%9D%98%EB%A5%BC%20%EB%B0%9B%EB%8A%94; 최종접속일: 2025년 6월 20일).

- 『매일경제』 2025년 5월 25일 보도 “中에 위장회사 세워 韓인재 영입 동료 연구원 20명 통째 빼가기도”
(<https://www.mk.co.kr/news/society/11325970>; 최종접속일: 2025년 6월 20일).
- 『매일경제』 2023년 11월 2일 보도 ““中BOE가 영업비밀 침해” 삼성디스플레이, 美ITC 제소”(<https://www.mk.co.kr/news/business/10865043>; 최종접속일: 2025년 6월 3일).
- 『머니투데이』 2025년 6월 11일 보도 “中장성차, 직접 산업스파이 지휘…'K배터리' 핵심기술 털렸다”
(<https://news.mt.co.kr/mtview.php?no=2025052814520025000>; 최종접속일: 2025년 6월 20일).
- 『머니투데이』 2024년 3월 2일 보도 ““미국 안보 위협에 처할 것” 바이든, 중국산 스마트카에 칼 뽑았다”
(<https://news.mt.co.kr/mtview.php?no=2024030213320480780>; 최종접속일: 2024년 3월 20일).
- 『서울경제』 2023년 9월 24일 보도 “20년간 100조…'國富기술' 줄줄 샀다[경제안보 흔드는 산업스파이]”
(<https://www.sedaily.com/NewsView/29UT3YHD42>; 최종접속일: 2024년 3월 20일).
- 『시사IN』 2014년 3월 14일 보도 “화웨이, ZTE… 진짜 주인은 정부?”(<https://www.sisain.co.kr/news/articleView.html?idxno=19603>; 최종접속일: 2025년 6월 20일).
- 『연합뉴스』 2025년 2월 16일 보도 “[트럼프 스톱 한달] 글로벌 관세전쟁·신팽창주의로 국제질서 지각 변동”(<https://www.yna.co.kr/view/AKR20250215031800071>; 최종접속일: 2025년 6월 3일).
- 『연합뉴스』 2024년 2월 6일 보도 “5년간 산업기술 해외 유출 96건 적발…반도체 최다”(<https://www.yna.co.kr/view/MYH20240206010500641>; 최종접속일: 2024년 3월 21일).
- 『연합뉴스』 2024년 2월 21일 보도 “트로이 목마?...美, 중국산 크레인 등 항만시설 사이버보안 강화”
(<https://www.yna.co.kr/view/AKR20240221065000071>; 최종접속일: 2025년 6월 3일).
- 『연합뉴스』 2023년 10월 9일 보도 “해외 유출 산업기술 65% 중국으로...5년여간 225명 검거”(<https://www.yna.co.kr/view/AKR20231008038100004>; 최종접속일: 2023년 3월 20일).
- 『연합뉴스』, 2021년 4월 11일 보도 “100여명 이직이 촉발한 LG-SK 배터리 전쟁, 713일만에 종지부”
(<https://www.yna.co.kr/view/AKR20210411016351003>; 최종접속일: 2025.05.30.).
- 『연합뉴스』 2021년 3월 20일 보도 “중국, 군·국영회사 임직원들의 테슬라 차 사용제한”(<https://www.yna.co.kr/view/AKR20210320004300072>; 최종접속일: 2024년 3월 20일).
- 『자유일보』 2025년 3월 19일 보도 “돈 때문에 승진 떨어져...산업기술 유출 88%가 내부자 소행”(<https://www.jayupress.com/news/articleView.html?idxno=38710>; 최종접속일: 2025년 6월 20일).
- 『조선일보』 2025년 6월 4일 보도 ““한국형 전투기 자료유출' 인도네시아 기술자, 형사 처분 면했다”
(https://www.chosun.com/national/national_general/2025/06/02/5IGNZYSWJZC KPF2E5R2IP6LSUU/; 최종접속일: 2025년 6월 5일).
- 『조선일보』 2024년 2월 2일 보도 “USB에 KF-21 자료들이...KAI 파견 인도네시아인들, 기술 빼내다

- 들통”(https://www.chosun.com/politics/diplomacy-defense/2024/02/02/5J7SK4ZBAVH3BGWYRZMZB3Q2IA/; 최종접속일: 2024년 3월 21일).
- 『중앙일보』 2025년 3월 13일 보도 “반도체 기술 중국 빼돌려 4조원대 피해…기술유출범 역대 최다 검거”(https://www.joongang.co.kr/article/25320356; 최종접속일: 2025년 6월 20일).
- 『중앙일보』 2024년 11월 21일 보도 “中 특히 무임승차에 韓 칼 뽑았다…'배터리 특허전쟁' 터질까”(https://www.joongang.co.kr/article/25293657; 최종접속일: 2025년 6월 20일).
- 『중앙일보』 2024년 6월 6일 보도 ““엄청난 돈으로 유혹…中, 서방 전·현직 조종사 빼내 중국군 훈련””(https://www.joongang.co.kr/article/25254610; 2025년 6월 20일).
- 『한겨레』 2024년 9월 13일 보도 “최전방에 ‘보안 우려’ 중국산 CCTV …군은 10년간 모르고 있었다”(https://www.hani.co.kr/arti/politics/defense/1158352.html; 최종접속일: 2025년 6월 3일).
- 『한겨레』 2024년 3월 8일 보도 “미국 항구 크레인에 ‘정체불명’ 통신장비…보안문제 제기 크레인, 중국 업체서 제작된 걸로 확인”(https://www.hani.co.kr/arti/international/america/1131498.html; 최종접속일: 2024년 3월 20일).
- 『한겨레』 2023년 7월 23일 보도 “‘곡면 패널’ 기술 중국에 유출한 삼성 협력업체 대표 유죄 확정”(https://www.hani.co.kr/arti/society/society_general/1099942.html; 최종접속일: 2025년 6월 3일).
- 『한겨레』 2020년 6월 26일 보도 “미, 화웨이 등 중 거대기업 20곳 “군 소유” 지정”(https://www.hani.co.kr/arti/international/china/950939.html; 최종접속일: 2025년 6월 20일).
- 『한국경제』 2024년 3월 6일 보도, “구멍 뚫린 간첩법에 기승 부리는 산업스파이”(https://www.hankyung.com/article/2024030620061; 최종접속일: 2025년 5월 23일).
- 한국무역협회 『무역뉴스』 2023년 8월 29일 보도 “6년간 기술 해외유출 140건…정부, 연내 처벌강화 등 규제개선”(https://www.kita.net/board/totalTradeNews/totalTradeNewsDetail.do; JSESSIONID_KITA=ECFBD9B7AFC505896FA3CC7E51CC3422.Hyper?no=77735&siteId=1; 2024년 3월 20일).
- 『ChosunBiz』 2025년 6월 19일 보도 ““참을만큼 참았다”… 삼성·LG, 中 OLED 특허 침해에 칼 뽑은 이유는”(https://biz.chosun.com/it-science/ict/2025/06/19/KGMKO65KJZFBVLWPM4UXZ25DCQ/; 최종접속일: 2025년 6월 20일).
- 『VOA Korea』 2020년 12월 2일 보도 “미 국방부, 군 통제기업 목록에 중국 회사 4곳 추가”(https://www.voakorea.com/a/world_asia_dod-blacklists-chinese-military-companies/6049413.html; 최종접속일: 2025년 6월 20일).
- 『YTN』 2024년 11월 21일 보도 ““10년 격차 기술' 중국 유출...전 삼성디스플레이 연구원 기소”(https://www.ytn.co.kr/_ln/0103_202411212243556879; 최종접속일: 2025년 6월 3일).

『ZDNet Korea』 2022년 2월 9일 기사 “48조원짜리 엔비디아 ARM 인수, 왜 불발됐나 [이슈진단+] 반도체 패권 경쟁 속 반발·각국 정부 규제로 불확실성 증폭”(https://zdnet.co.kr/view/?no=20220208160541; 최종접속일: 2024년 3월 20일).

『朝日新聞』 2025년 8월 5일, “2ナノ半導体祕密持ち出しか、TSMC元社員ら拘束・日本企業も捜索”(https://www.asahi.com/articles/AST85323QT85UHBI01MM.html; 최종접속일: 2025년 8월 6일).

『産経新聞』 2025년 8월 8일, “台湾半導体大手TSMCの機密情報が東京エレクトロンに・台湾紙報道、ラピダスにも漏洩か”(https://www.sankei.com/article/20250806-MNZDJDB2DNIHDP5GXDULLQRPD4/; 최종접속일: 2025년 8월 8일).

Bloomberg August 8, 2025, “TSMC Secrets Leak Puts Japan's Tokyo Electron on Hot Seat” (https://www.bloomberg.com/news/articles/2025-08-07/tsmc-trade-secrets-leak-puts-japan-s-tokyo-electron-on-hot-seat; 최종접속일: 2025년 8월 8일).

Reuters August 8, 2025, “Tokyo Electron confirms Taiwan unit employee's involvement in intellectual property case”(https://www.reuters.com/markets/emerging/tokyo-electron-confirms-taiwan-unit-employees-involvement-intellectual-property-2025-08-07/; 최종접속일: 2025년 8월 8일).

Reuters June 2, 2025, “How Trump's trade war is upending the global economy”(https://www.reuters.com/business/autos-transportation/how-trumps-chaotic-trade-war-has-evolved-2025-05-12/; 최종접속일: 2025년 6월 3일).

Satter, Raphael, “U.S. court: Mass surveillance program exposed by Snowden was illegal”, in: *Reuter*, September 3, 2020(https://www.reuters.com/article/world/us-court-mass-surveillance-program-exposed-by-snowden-was-illegal-idUSKBN25T3CJ/; 최종접속일: 2025년 6월 3일).

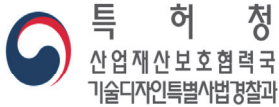
사례발표

첨단전략산업 분야 핵심기술 해외유출 수사사례

| 김은정 기획수사팀장 (특허청 기술디자인특별사법경찰과)

2025. 9. 2. (화)

반도체 국가핵심기술 (CMP) 국외유출 사건 수사결과 발표



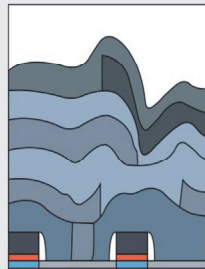
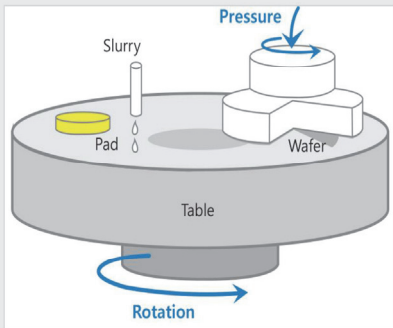
피해 기업

- A社 : 반도체 웨이퍼 연마제·패드(CMP 슬러리·패드) 제조 국내 업체
- B社 : 연마제(CMP 슬러리) 제조 국내 업체
- C社 : 메모리 반도체 제조 국내 업체

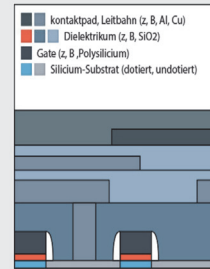
* A·B·C社는 시가총액 약 66조원, 코스피/코스닥 상장사



반도체 웨이퍼 연마(CMP) 기술



CMP 공정 前



CMP 공정 後

출처: MOS 홈페이지-CMP 공정소개 (http://www.e-mos.kr/page/sub03_01.html)

- 반도체 웨이퍼 연마공정(CMP, Chemical Mechanical Polishing)

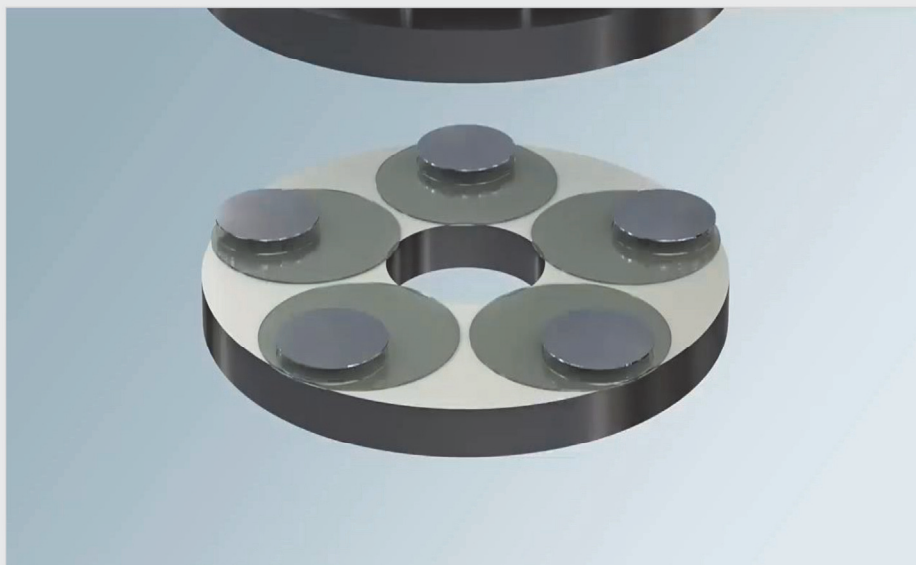
: 반도체 웨이퍼 표면의 미세한 요철을 평탄화(연마)하는 공정

- 연마패드(Pad) : 연마가 잘 되도록 반도체 웨이퍼와 접촉하는 패드

- 연마액(Slurry) : 연마공정에서 반도체 웨이퍼와 연마패드 사이로 흘러보내는 용액



반도체 웨이퍼 연마(CMP) 기술



해당영상은 본 사건과 무관한 영상입니다.

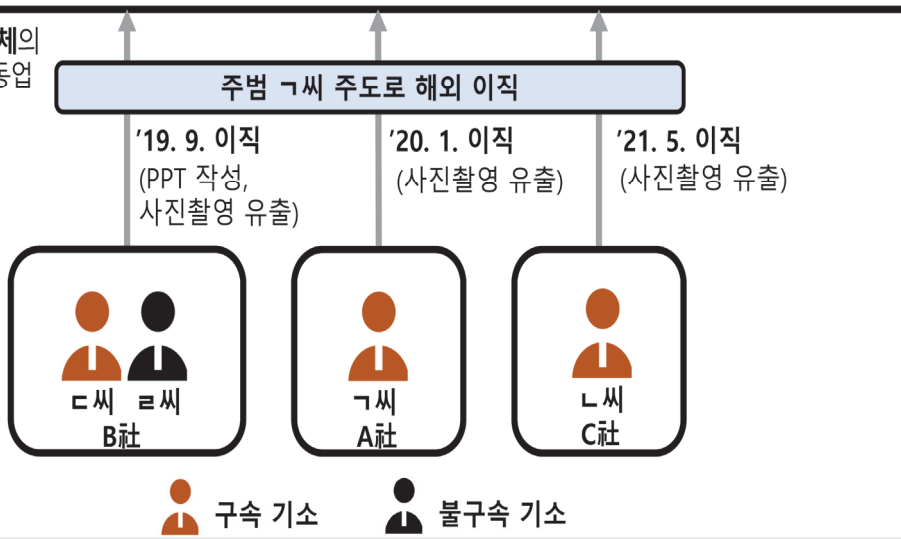
주요 피고인

- ㄱ씨 (55세, 구속): '20. 1.경 A社 퇴사, 외국 업체 **사장급** 이직
 기술유출 전체를 설계한 **주범**
- ㄴ씨 (52세, 구속): '21. 3.경 C社 퇴사, 외국 업체 **부사장급** 이직
- ㄷ씨 (42세, 구속): '19. 9.경 B社 퇴사, 외국 업체 **팀장급** 이직
- ㄹ씨 (35세, 불구속): '19. 9.경 B社 퇴사, 외국 업체 **팀원급** 이직

사건 관계도



ㄱ씨와 해외업체의
CMP 슬러리 동업
약정('19.6)



구속 기소 불구속 기소



주요 범행 (산업기술보호법위반 및 부정경쟁방지법위반)

❖ B社の 반도체 웨이퍼 연마제 관련 첨단기술 유출

- '19. 6.~9.경 B社の 반도체 웨이퍼 연마제(CMP 슬러리) 관련 기술자료(영업비밀) 활용
→ 외국 내 연마제 사업계획 PPT 제작 → 외국 업체의 직원들에게 제공

❖ A社の 연마제·패드 관련 첨단기술 유출

- '19. 8.~'20. 1.경 B社の 연마제·패드(CMP 슬러리·패드) 관련 보안자료를 컴퓨터 화면에 띄워 놓고 휴대전화로 촬영·유출

❖ C社の 연마 공정 관련 국가핵심기술 유출

- '20. 4.~'21. 1.경 C社の 연마 공정(CMP 공정) 관련 보안자료를 업무용 휴대전화 화면에 띄워 놓고 다른 휴대전화로 촬영·유출



특허청 기술경찰의 주요 수사 경과

- '22. 3. 21. 국정원 산업기밀보호센터 첩보 (ㄷ씨 및 ㄹ씨 영업비밀침해 수사 착수)
- '22. 4. 외국 체류 ㄷ씨 및 ㄹ씨의 귀국 즉시 신병 확보
- '22. 4.~5. 주거지 등 압수수색 6차례
- '22. 4.~5. 기술유출 전체를 설계한 주범 ㄱ씨, 중간간부 및 브로커 등 4명 피고인 발견
대기업 A社, C社の 국가핵심기술, 첨단기술 유출에 대한 추가 인지
- '22. 5.~10. 디지털포렌식을 통한 압수물 분석 → 피고인들·관련자 조사
- '22. 11. 2. ㄷ씨에 대한 구속영장 집행
- '22. 11. 28. B社 퇴사자 ㄷ씨 등 2명 1차 기소(1명 구속, 1명 불구속)
- '22. 12. 28. ㄱ씨, ㄴ씨에 대한 구속영장 집행
- '23. 1. 20. A社 퇴사자 주범 ㄱ씨 등 2차 기소(2명 구속, 3명 불구속)



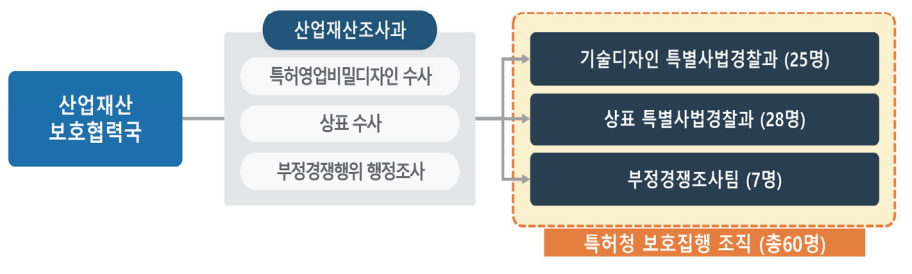
기술경찰 출범경과

특허청 보호집행조직 확대개편· 기술경찰 출범

- 산업재산조사과 내 수사관 6명(19.3) → 15명(21.3) → 기술경찰과 22명(21.7) → 24명(24.2) → 25명(25.1)
- 국회·BH 설득, 행안부·기재부 협의를 통하여 **기술경찰 조직·인력 확대 개편(+2과, +11명) 출범**(21.7.27)
- 법무부 수사자문검사 특허청 파견(22. 2. 7)



보호집행 확대개편 조직도



감사합니다



토론

| 이상홍 실장 (기아 정보보안2실)

| 손용하 과장 (산업통상자원부 기술안보과)

| 전우정 교수 (한국과학기술원 지식재산대학원)

| 심미랑 실장 (한국지식재산연구원 법제도연구실)

