

원저

경찰의 방산안보 전문수사관 제도 도입 방안: 기술·안보 융합수사 역량 강화를 중심으로

강전석¹, 오진수², 류연승³

¹경기북부경찰청 일산서부경찰서

²경기북부경찰청 고양경찰서

³명지대학교 방산안보학과 교수

교신저자: 류연승 (ysryu@mju.ac.kr)

요약

오늘날 글로벌 안보 환경이 기술 패권 경쟁 체제로 재편됨에 따라, 국가방위의 근간인 방위산업기술을 보호하기 위한 경찰 안보수사 역량의 고도화는 국가 생존 전략으로 부상하였다. 방위산업기술 자산은 일반 산업기술과 달리 무기체계 설계 프레임워크 및 복잡한 국방 R&D 프로세스와 결합되어 있어 군사적 특수성에 기반한 법제와 획득 절차에 대한 고도의 전문지식이 요구된다. 본 연구에서 다루는 ‘방산안보 전문수사관’은 방산기술·무기체계·방위산업 공급망·국방획득체계 및 관련 법제도에 대한 전문성을 바탕으로 방산기술 유출, 산업기밀 침해, 방산비리 및 공급망 위협 등 방산안보 관련 범죄를 전문적으로 탐지·수사하는 경찰 전문인력이다.

그러나 현행 경찰 전문수사관 체계는 일반 죄종 중심의 단기·정량적 실적에 편중되어, 장기적 추적과 정밀 검증이 필수적인 방산 안보 직무와 극심한 ‘제도적 미스매치’를 야기하고 있다. 아울러 단기 순환보직 관행은 인적 전문성과 첨단 기술 자산이 결합하지 못하는 기술 비대칭성을 심화시키고 있다.

이에 본 연구는 단순한 인력 확충을 지양하고 전문수사관의 인사·평가 구조를 전환하기 위해, 일반 수사 트랙과 분리된 독자 트랙 신설을 제안한다. 세부 대안으로는 무기체계 기술 가치 및 국방 획득 절차 이해도를 검증하는 정성적 직무 특화 지표 도입, 국가직무능력표준(NCS)을 준용한 기술·안보 융합형 교육 프레임워크 구축, 전문직위 지정을 통한 장기 보직 유인책 마련을 제시한다. 결론적으로 본 연구는 기술 가치 분석 기반의 ‘정보주도형 치안(ILP)’ 모델을 방산 영역에 투영하고, 다변화된 사법 관할권 내에서 군·정보기관과의 상호 운용성을 보장하는 통합 방산안보 거버넌스 공조 체계의 방향성을 제안한다.

핵심어

방산안보, 방산안보 전문수사관, 안보수사, 정보주도형 치안(ILP), 기술·안보 융합

차례

1. 서론
2. 이론적 배경 및 선행연구 고찰
3. 현행 안보수사관 자격 관리 체계 분석
4. 경찰의 방산 안보 전문수사관 제도 도입 및 고도화 방안
5. 결론 및 향후 연구 과제

Open Access

접수일: 2026년 8월 10일
수정일: 2026년 9월 09일
게재승인일: 2026년 9월 16일
출판일: 2026년 9월 30일

Copyright © 2026 Author(s).

This is an Open Access article distributed under the terms of the Creative Commons CC BY 4.0 license (<https://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Original Article

A Study on Introducing the Specialist Investigator System for Defense Security in the Police: Focusing on Strengthening Tech-Security Convergence Investigation Capabilities

Jun-seok Kang¹, Jinsu Oh², Yeon-seung Ryu³

¹Ilsan Seobu Police Station, Gyeonggi Bukbu Provincial Police Agency, Republic of Korea

²Goyang Police Station, Gyeonggi Bukbu Provincial Police Agency, Republic of Korea

³Professor, Department of Defense Industrial Security, Myongji University, Republic of Korea

Corresponding Author: Yeon-seung Ryu (ysryu@mju.ac.kr)

ABSTRACT

As the global security environment is restructured into a technological hegemony competition, advancing police security investigation capabilities to protect defense technology assets has emerged as a vital national survival strategy. Unlike general industrial technologies, defense technology assets are inherently intertwined with weapon system design frameworks, closed military network isolations, and complex defense R&D acquisition processes. In this study, a “Defense Security Specialist Investigator” is defined as a specialized police investigator who professionally detects and investigates defense security crimes—such as technology leaks, trade secret infringements, defense procurement fraud, and supply chain threats—based on profound expertise in defense technologies, weapon systems, defense supply chains, defense acquisition frameworks, and specialized legal systems.

However, the current police specialist investigator qualification framework remains heavily biased toward short-term, quantitative outputs centered on conventional criminal offenses, triggering a severe “institutional mismatch” with defense security duties that demand long-term tracing and rigorous validation. Furthermore, the practice of short-term rotational assignments exacerbates a technological asymmetry gap, preventing cutting-edge science policing assets from organically integrating with human professional expertise.

To overcome these structural defects and shift the focus from merely expanding headcounts to restructuring the personnel system, this study proposes the establishment of an independent qualification track for “Defense Security Specialist Investigators,” completely separated from the general criminal investigation track. As key policy alternatives, this paper derives: (1) introducing qualitative, job-specific evaluation indicators assessing weapon system technology values (ROC disruption) and defense acquisition governance; (2) constructing a tech-security convergence educational framework adapted from the National Competency Standards (NCS); and (3) establishing institutional incentives for long-term assignments through designated specialized positions. In conclusion, this study projects an Intelligence-Led Policing (ILP) model onto the defense domain and underscores the necessity of follow-up research to establish an integrated governance cooperation system that ensures operational interoperability with military and intelligence agencies.

KEYWORDS

Defense Security, Defense Security Specialist Investigator, Police Security Investigation, Intelligence-Led Policing (ILP), Tech-Security Convergence

1. 서론

1.1. 연구의 배경 및 목적

현대 국제 정세는 단순한 군사적 대립이나 영토적 패권 경쟁의 구도를 넘어, 국가의 첨단 기술 자산과 지식재산권을 얼마나 확보하고 철저히 보호하느냐가 국가 존립의 핵심 변수가 되는 ‘경제안보(Economic Security)’ 시대로 빠르게 이행하고 있다. 과거 방위산업이 국가 방위력 건설 및 군사력 증강이라는 전통적 안보 목적에 국한된 특수 분야로 인식되었다면, 현대의 방위산업은 반도체, 인공지능(AI), 우주항공, 양자 컴퓨터 등 국가 최첨단 전략기술이 총망라되어 집약된 경제적 핵심 자산이자 국가 미래 성장 동력으로 그 가치와 패러다임이 전면 재정립되었다. 특히 대한민국은 독자적이고 세계적인 국방과학기술력을 바탕으로 글로벌 시장에서 ‘K-방산’의 위상을 확고히 다져왔으며, 최근 역대 최고 수준의 방산 수출 성과를 잇달아 달성하며 국가 경제 발전과 신안보 체계의 핵심 축으로 급부상하였다.[1]

그러나 이러한 K-방산의 비약적인 성장과 국방과학기술의 가치 상승은, 역설적이게도 해외 정보기관과 글로벌 산업 스파이 집단, 경쟁 국가들의 집중적인 표적이 되는 심각한 안보적 부작용을 초래하였다. 글로벌 기술패권 경쟁 하에서 방산기술 유출 사범의 범죄 양상은 국가 간 하이브리드 전쟁의 성격을 띠며 날로 고도화되고 있다. 과거의 기술 유출 범죄가 단순한 서류 복사나 저장매체의 물리적 반출 수준에 머물렀다면, 오늘날 방산 범죄는 내부 조력자의 권한을 악용한 지능형 기술 유출이나 글로벌 공급망의 허점을 노린 전략물자 불법 우회 수출 등 그 양상이 고도로 첨단화·지능화되어 급격히 진화하고 있다. 이에 따라 방위산업 영역에서의 사이버 방첩 활동과 제도적 정비는 더 이상 미룰 수 없는 국가적 당면 과제이다. 또한, 기술 보호의 대상을 명확히 하고 법적 규제력을 확보하기 위해서는 산업기술 전반을 아우르는 체계적인 법제적 이해가 선행되어야 한다.[2]

이와 같은 고도화된 특수 인프라 환경에서 발생하는 기술 유출 범죄는 일반적인 사이버 범죄나 지능 범죄 수사와는 법적·기술적 접근 방식을 완전히 달리해야 한다. 방위산업 기술 보호는 사후적 조치나 단일 기관의 단편적인 대응만으로는 불가능하며, 고도의 전문성을 갖춘 전문인력 양성과 국가 차원의 안보 거버넌스 확립이 필수적이다. 특히 방산데이터가 철저히 업무망 내부에서만 통제되는 폐쇄적 인프라 환경의 특수성을 고려할 때, 수사 주체 역시 무기체계 전반의 기술적 특수성과 국방 보안 훈령에 대한 깊은 식견을 공유해야 한다. 변화하는 위협에 효과적으로 대응하기 위해서는 기존의 통제 방식을 탈피하여 방산보안 패러다임의 혁신적 전환을 이룩해야 하는 이유가 바로 여기에 있다.[3]

그러나 대공·안보 수사관 다변화 시대를 맞아 국가 안보 사범 책임수사의 핵심 주체로 부상한 경찰의 현행 인력 양성 및 자격 평가 시스템은 여전히 일반 죄종의 송치 건수나 영장 신청률 등 단기적·정량적 실적에 지나치게 편중되어 있다. 이는 장기적인 기술 분석과 고도의 전문지식이 필수적인 방산 안보 수사의 특수성을 포괄하지 못하는 ‘제도적 미스매치’를 야기하고 있으며, 결과적으로 우수한 안보 특화 인력이 조직 내에 안정적으로 잔류하지 못하고 이탈하는 심각한 인력 공백을 낳고 있다.[4,5] 더욱이 정보주도형 치안(Intelligence-Led Policing) 관점에서 볼 때, 안보 수사는 범죄 발생 이후의 단편적인 검거를 넘어 고도화된 정보 분석 역량이 유기적으로 결합되어야 함에도, 현재의 인사 구조는 수사관들의 전문지식적 요소를 안정적으로 축적하기 어려운 환경이다. 이는 일반 경찰 조직뿐만 아니라 유사한 책임수사 기능을 수행하는 타 수사기관의 전문수사관 운영 제도에서도 공통적으로 지적되는 고질적인 한계점이다.[6]

이러한 맥락에서 본 연구는 학계에서 지속적으로 강조해 온 ‘융합형 방산안보 거버넌스 이론’과 ‘네트워크형 거버넌스 인재 육성’의 필요성에 사법적 실행력을 결합하고자 한다. 방산기술 보호는 단일 기관의 차원을 넘어 기술과 안보를 융합하여 해석할 수 있는 국가 차원의 거버넌스 확립이 핵

십이며, 이를 실무적으로 뒷받침할 수 있는 표준화된 직무 역량 체계의 확립이 시급하다.[7]

따라서 본 연구는 급변하는 경제·안보 환경 속에서 경찰이 방산 안보 수사의 책임 주체로서 실질적 대응력을 확보할 수 있도록, 국가직무능력표준(NCS) 기반의 방산 안보 직무 설계 원리를 경찰 수사 자격 체계에 이식한 ‘방산 안보 특화 전문수사관 시스템’의 구체적인 도입 방안과 제도적 실효성 제고 방안을 제시하는 것을 목적으로 설정한다.[8]

구체적으로는 현행 경찰 전문수사관 인증제도의 실태와 문제점을 명확히 진단하고, 국내 현행 안보수사관들을 대상으로 한 실증적 조사 분석을 바탕으로 기술·안보 융합형 직무 역량 모델을 도출하고자 한다. 나아가 폐쇄 보안망 환경에 대응하는 기술 역량 내재화 방안과 함께, 전문직위 지정 및 보직 관리의 연속성 확보 등 전문 인재들이 안정적으로 방산 안보 분야에 정착하여 민·관·학 협력 플랫폼을 주도할 수 있는 실행 가능한 대안을 도출함으로써, 국가 경제·안보를 수호하는 경찰 안보수사의 전문수사관 실효성을 확립하고자 한다.

1.2. 연구의 필요성 및 문제 제기

첫째, 현행 일반 수사 분야 중심의 책임수사관 제도와 안보 수사 고유의 특수성 간의 제도적 mismatch를 극복해야 한다. 현재 경찰청은 수사 인력의 전문성 강화를 위해 ‘수사관-전문수사관-책임수사관’으로 이어지는 자격 체계를 고도화하여 운영하고 있다. 그러나 이러한 제도적 혜택과 역량 인증 기준은 형사, 경제, 지능 등 일반 죄종별 수사 부서에 편중되어 있어, 독자적인 영역과 안보적 가치를 지닌 안보 수사 분야의 특수성을 제대로 포괄하지 못하고 있다.[4] 일반 수사 체계 중심의 평가 기준은 고도의 기술 보호와 안보적 판단이 요구되는 방산 안보 수사관들의 전문성을 공인하는 데 한계가 있으며, 단기 순환보직 위주의 인사 운용은 전문지식의 장기적 축적을 저해하여 결과적으로 안보 특화형 책임·전문수사관 트랙의 공백을 야기하고 있다.[5] 따라서 기존의 뼈대를 활용하되 안보 분야의 특성을 조화롭게 수용한 전문수사관 제도의 도입이 필요하다.

둘째, 네트워크 보안 체제 및 국가 안보망의 기술적 메커니즘을 규명할 ‘융합형 전문인재 양성’의 제도적 기반이 필요하다. 방산 안보 수사는 높은 보안성이 요구되는 인프라의 특수성, 그리고 철저히 통제된 안보망 내에서 일어나는 비정상적인 데이터 흐름이나 우회 경로를 추적해야 하는 고난도의 과학수사 영역이다. 현대 방산·보안 환경은 고도화된 정보통신기술이 집약되어 있어 전통적인 보안 통제나 수사 방식으로는 한계가 명확하다.[3] 단기 순환보직 체계 중심의 인력 운용 하에서는 이러한 진입장벽 높은 특수 보안 인프라를 깊이 있게 이해하고 수사에 접목하기 어려우며, 인재가 체계적으로 안보 분야에 정착하여 전문성을 고도화할 수 있는 유인 기제가 부족하다. 이는 타 책임수사 주체의 전문수사관 제도 운영에서도 공통적으로 나타나는 한계점으로, 조직적 안정성과 특화된 인사 트랙의 확보가 선행되어야 함을 시사한다.[9] 이에 방산기술 유출 범죄는 단순 기술 탈취를 넘어 국가 안보적 파급효과를 동반하므로, 특수 보안망의 구조적 특성을 규명해낼 수 있는 기술적 식견과 안보 수사 역량을 동시에 겸비한 전문인재 양성이 조직 안정화와 거버넌스 확립의 핵심 과제이다.

셋째, 과학치안(Science Policing) 역량의 내재화와 기술 비대칭성 문제를 해결해야 한다. 최근의 방산 기술 유출은 다크웹을 통한 정보 거래, 가상자산을 활용한 자금 세탁 등 첨단 ICT 기술을 매개로 발생하고 있다. 이에 따라 방위산업을 둘러싼 사이버 영역에서의 방첩 활동과 법제도적 대응력을 확보하는 것은 매우 중대한 제도적 과제이다.[2] 이에 대응하여 경찰 조직 차원의 첨단 기술 자산과 과학치안 R&D 투자는 지속되고 있으나, 정작 현장의 안보수사 인력이 이러한 첨단 기술 자산을 네트워크 내부 환경 등 실제 수사 과정에 유기적으로 결합하여 활용하는 역량은 정체되어 있다. 특히 기술 유출의 사법적 입증을 위해서는 산업기술 보호 방안의 표준화된 기술 유출 판단 기

준과 법적 통제 메커니즘에 대한 명확한 이해가 수사관에게 내재화되어야 한다.[10] 즉, 기술 인프라의 발전 속도와 이를 운용할 전담 인력의 전문성 간의 비대칭성이 발생하고 있으며, 이는 전문수사관 제도 내에 기술 활용 역량 인증과 실무 연계형 고도화 교육이 강하게 결합되어야 할 이유가 된다.

넷째, 민·관·학 협력 네트워크를 아우르는 거버넌스 중심형 인재 인프라가 마련되어야 한다. 방산 안보 사범은 국경을 초월한 글로벌 네트워크를 형성하고 있어 외국의 전문 수사기관과의 실시간 공조가 필수적이며, 기술 유출의 1차 접점인 민간 방산업체 및 전문 연구기관과의 긴밀한 협업이 필수적이다. 방산 안보 환경의 급격한 변화는 단일 사법기관의 단편적인 사후 조치로는 대응이 불가능하며, 민·관·학의 유기적 연계가 수반되어야 한다.[1] 하지만 현재의 대응 체계는 부서 간, 기관 간의 칸막이식 운영으로 인해 통합적인 정보 환류와 유기적인 협력이 원활하지 못하다. 따라서 방산 안보 전문수사관을 단순히 ‘수사 전문가’에만 한정 짓지 않고, 정보주도형 치안(Intelligence-Led Policing) 관점에 기반하여 고도화된 정보 분석 능력을 토대로, 민·관·학 협력 플랫폼을 매개하고 주도할 수 있는 ‘네트워크형 거버넌스 인재’로 육성할 전략적 방안 마련이 학술적·정책적으로 필요하다.[6]

1.3. 연구의 범위 및 방법론

본 연구는 경찰 경제 등 첨단 안보수사 분야의 전문수사관 전문성 강화에 대한 주요국의 선진 수사 인력 양성 방안을 비교 대상에 포함한다. 내용적으로는 경제안보 관점에서의 방산 범죄 유형 분류, 국외 전문 수사기관의 인재 양성 현황 분석, 국내 경찰 전문수사관 시스템의 자격 관리 및 교육 체계 진단, 그리고 실증 분석을 통한 정책 대안 도출을 범위로 확정한다.

연구의 타당성을 확보하기 위해 본 연구는 이론적 고찰과 실증적 분석을 병행하는 다각적 분석 방법론(Triangulation)을 채택한다. 첫째, 국내외 학술 논문 및 관련 법령을 심층 분석하는 문헌 연구를 수행하며, 특히 방산안보의 개념을 확장하고 재정립한 선행 연구들을 중점적으로 고찰하여 이론적 기틀을 다진다.[1] 둘째, 정보주도형 치안(Intelligence-Led Policing, ILP)¹⁾ 모델 등 국외의 선진 안보 분야 지침 및 인력 운용 모델의 시사점을 분석한다.[6,7] 셋째, 실무적 대안 제시를 위해 국가직무능력표준(NCS) 기반의 직무 설계 및 교육 프레임워크 이론을 접목하여, 경찰 조직에 실질적으로 적용 가능한 방산 안보 특화 교육 모델을 도출하고자 한다.[8]

2. 이론적 배경 및 선행연구 고찰

2.1. 방산 안보 환경의 특성

2.1.1. 경제안보 패러다임으로의 개념적 확장

전통적인 안보 개념이 군사력 중심의 영토 주권 수호와 군사적 위협에 대한 물리적 방어에 국한되었다면, 현대의 안보 환경은 국가의 핵심 첨단 기술 자산과 공급망을 보호하는 ‘경제안보(Economic Security)’의 개념으로 급격히 이행하고 있다. 이러한 패러다임의 변화 속에서 방위 산업은 단순히 국가 방위력을 건설하는 보조적 수단을 넘어, 반도체, 우주항공, 인공지능(AI) 등 국

1) ILP 모델은, 사후 검거 위주의 전통적인 경찰 활동이 아닌, 범죄 정보(Intelligence)의 수집과 분석을 토대로 자원을 효율적으로 배치하고 범죄를 선제적으로 차단, 예방하는 치안 관리 방식이다. 여기서 범죄 정보란 수집된 여러 첩보를 정밀 분석, 평가, “사범 지휘부가 정책적, 전략적 결정을 내릴 수 있도록 가치 있게 가공한 지식”이며, 현대 경찰은 한정된 인력과 예산이라는 제약을 안고 있어 ILP 모델은 고위험 사범이나 상습 범죄 지역, 혹은 고도화된 안보 위협 등 ‘가장 위험도가 높은 곳’에 경찰 자원을 집중 투자함으로써 치안 효율성을 극대화하고자 한다.

가의 최첨단 전략기술이 총망라된 경제적 자산이자 미래 국가 성장 동력으로 그 가치가 전면 재정립되었다.

특히 대한민국 방위산업은 국방과학기술의 비약적인 발전을 바탕으로 글로벌 시장에서 'K-방산'의 독자적인 위상을 공고히 구축하였으나, 이러한 급성장은 역설적이게도 해외 정보기관 및 산업 스파이 집단의 집중적인 표적이 되는 안보적 취약성을 동반하게 되었다. 그렇기에 현대의 방산 안보는 단순히 침입자를 막는 사후적·방어적 통제 개념에 머무는 것이 아니라, 국가의 거시적 경제 자산과 국가 경쟁력을 능동적으로 수호하는 포괄적 안보 거버넌스로 정의된다.[7] 국가 간 기술패권 경쟁이 심화됨에 따라, 방산 안보 정책은 군사적 차원을 넘어 기술 유출이 국가 안보 및 거시 경제에 미칠 파급효과를 종합적으로 고려하여 수립되어야 한다.[1]

2.1.2. 기술적 특수성과 폐쇄적 인프라 환경

방산 안보 환경을 구성하는 가장 차별화된 고유한 특성은 방산 기업 및 연구 유관 기관들이 운용하고 있는 고도의 기술적 특수성과 독점적 보안 인프라의 폐쇄성에 있다. 일반 산업 기술과 달리 방산 기술은 무기체계의 설계 프레임워크, 체계 통합 기술, 군사 작전 요구성능(Required Operational Capability, ROC)²⁾ 등이 복합적으로 얹혀 있어, 법적 규제력과 통제 메커니즘을 명확히 판단하기 위해서는 고도의 전문지식이 선행되어야 한다.[3]

이러한 국가 핵심 자산을 보호하기 위해 국내 방산 영역은 외부 인터넷망과 업무용 내부 네트워크를 원천적으로 차단하는 '네트워크 보안 체제(Network Isolation)'와 강력한 '국가 안보망'을 상시 가동하고 있다. 이러한 고보안·폐쇄적 인프라 환경은 외부로부터의 단순 접근을 차단하는 데는 효과적이지만, 내부 조력자가 정상 권한을 오·남용하여 기술을 은닉 반출하거나 변칙적인 경로로 데이터를 우회시키는 지능형 범죄가 발생했을 시 외부에서 혐의를 포착하기가 극도로 어렵다는 맹점을 지닌다. 즉, 정보통신기술(ICT)의 고도화는 역설적으로 방산 보안의 기술적 진입장벽을 가중시켰으며, 이를 분석하고 규명해야 하는 사법 당국으로 하여금 단순한 수사 기법을 넘어 무기체계의 특수성과 국방 보안 훈령, 폐쇄망의 로그 데이터 메커니즘을 완벽히 이해할 것을 요구하고 있다.[3]

2.1.3. 사이버 영역에서의 안보 위협 고도화 및 방첩의 난해성

현대의 방산 범죄는 국경의 한계를 소멸시킨 사이버 공간을 무대로 전개되고 있으며, 그 수법 또한 다크웹을 통한 첩보 거래, 가상자산을 활용한 추적 회피형 자금 세탁, 고도화된 지능형 지속 위협(Advanced Persistent Threat, APT)³⁾ 공격 등 첨단 ICT 기술과 유기적으로 결합되어 진화하고 있다. 과거의 아날로그식 문서 탈취나 물리적 저장매체 반출과 달리, 사이버 공간에서의 기술 유출은 범죄의 실행과 결과 사이에 시차가 존재하고 증거의 인멸 및 변조가 순식간에 이루어지기 때문에 실체적 진실을 규명하는 데 막대한 사법적 난제가 뒤따른다.

방위산업을 겨냥한 적대 세력의 위협이 군사기밀 유출을 넘어 공급망 전반을 마비시키는 하이브리드전 형태로 전개되고 있음을 지적하며, 방위산업 사이버 방첩을 위한 제도적 과제와 전담 사법 인력의 고도화가 결코 지체될 수 없는 시급한 당면 과제임을 역설하였다.[2] 철저히 폐쇄된 보안망

2) 미래의 전장 환경에서 승리하기 위해 새로운 무기체계에 장비에 요구하는 구체적인 성능, 기능, 그리고 규격을 의미한다. 특히 방산·안보 수사의 기술적·보안적 특수성을 고려할 때, 수사 주체에게는 고도의 기술적 식견과 국방 획득 절차에 대한 깊이 있는 이해 등 전문성 확보가 필수적으로 요구된다.

3) 지능형(Advanced), 지속성(Persistent), 위협(Threat)은 특정 대상을 겨냥해 장기간에 걸쳐 다양한 방식으로 공격 대상의 시스템 취약점을 분석, 알려지지 않은 보안 취약점(Zero-Day)을 악용하는 등 첨단 수단을 동원하여 지속적으로 해킹 공격을 감행하는 고도화된 사이버 공격 기법이다.

내부 환경과 고도화된 글로벌 사이버 위협 사이의 비대칭성을 극복하기 위해서는, 범죄 발생 후 사후적으로 개입하는 형사 사법 패러다임에서 벗어나야 한다. 다양한 민간 플랫폼 및 첩보 채널을 통해 유입되는 불명확한 징후들을 사전에 포착하고 유기적으로 분석해내는 정보주도형 치안(ILP) 관점의 방첩 수사 체계 구축이 필수적이며[6], 이는 곧 기술적 식견과 정보 분석 역량을 동시에 내재한 안보 특화 전문수사관의 양성을 강력히 뒷받침하는 배경이 된다.

2.2. 방산 안보 거버넌스 이론 및 선행연구 검토

방산 안보 수사의 전문성 공백을 메우기 위한 이론적 토대는 학계에서 지속적으로 논의되어 온 융합형 방산안보 거버넌스 이론에서 찾아볼 수 있다. 선행 연구에 따르면 방산 기술 보호는 단일 사법기관이나 보안 부서의 단편적인 통제 정책만으로는 불가능하며, 군·경·민·학을 아우르는 국가 차원의 통합·융합형 거버넌스가 확립되어야 한다. 특히 방산 안보 범죄는 첨단 기술 탈취라는 실정법 위반의 사법적 성격과 국가 안보 시스템 및 국익을 위협하는 안보 저해 행위의 성격을 동시에 지니고 있다. 따라서 수사 주체 역시 법리적 판단을 넘어 무기체계의 특수성과 군사 작전 요구성능(ROC), 그리고 국방 보안 훈령 등 기술과 안보를 체계적으로 융합하여 해석할 수 있는 다차원적 역량을 갖추어야 한다.[2]

또한 글로벌 기술 패권 경쟁 속에서 발생하는 방산 기술 유출 사범의 진화 양상에 대한 실증적 연구들을 살펴보면, 최신 방산 범죄는 단순한 개인의 일탈을 넘어 국가 간 하이브리드 전쟁의 성격을 띠며 고도로 첨단화되고 있다.[1] 이에 따라 방산업체 및 유관 연구소가 운용 중인 폐쇄적 망분리 체계를 무력화하기 위해 내부 조력자를 정밀 포섭하거나, 지능형 지속 위협(APT) 공격 및 고도화된 공급망 해킹을 시도하는 등 기술적 우회 수법이 날로 다변화되는 추세이다.[2]

이러한 위협 환경의 변화는 현장의 안보수사관이 단순히 사후에 피의자를 신문하고 디지털 포렌식 결과만을 확인하는 전통적 수사 방식에서 전면 탈피해야 함을 시사한다. 즉, 정보통신기술(ICT) 기반의 방산 인프라 취약점을 선제적으로 진단하고 유관 기관과 실시간으로 안보 정보를 환류할 수 있는 혁신적인 ‘방산보안 2.0’ 패러다임 기반의 수사 체계로 전환되어야 한다.[3] 이는 본 연구가 제안하는 기술·안보 융합형 전문수사관 제도 도입의 가장 강력한 학술적 당위성이 된다.

2.3. 현행 경찰 수사 자격 체계와 안보수사의 한계

2.3.1. 일반 최종 중심 책임수사관 제도의 한계

경찰청은 현재 수사 역량의 상향 평준화와 전문성 공인을 위해 ‘수사관-전문수사관-책임수사관’으로 이어지는 수사관 자격 등급 제도를 운영하고 있다. 그러나 현행 제도는 형사, 경제, 지능, 사이버 등 일반 최종별 분류와 정량적 평가 기준에 편중되어 설계된 한계를 지닌다. 현재의 자격 인증 체계는 송치 건수, 영장 신청률, 일반 형사법리 해석 능력 등 단기적 성과에 치중되어 있어, 장기적 분석과 정성적 가치 평가가 핵심인 안보 분야의 직무 특성을 올바르게 반영하지 못하는 ‘평가 지표의 불일치’를 야기한다.[4]

방산 안보 수사는 단 한 건의 내사 및 사건 처리를 위해 수개월 동안 폐쇄망 내부의 복잡한 로그 데이터를 추적하고, 국방 획득 절차 및 산업기술보호법상의 위법성을 면밀히 검토해야 하므로 정량적 실적 위주의 평가 체계에서는 안보수사관의 전문성이 구조적으로 저평가되는 모순이 발생한다. 이는 결국 ‘자격의 전문성 공백’으로 이어진다. 수사관이 일반 사이버 분야의 전문수사관 자격을 보유했다 하더라도, 국가 안보망의 폐쇄적 거버넌스 체계나 방산 기술 고유의 특수성 및 무기체계 설계 프레임워크를 심층적으로 이해하지 못하면 실질적인 방산 유출 범죄의 실체적 진실을 입

증하는 데 명백한 한계에 부딪힐 수밖에 없다.[10]

2.3.2. 제도적 연속성 부족과 인재 양성의 한계

경찰 내부적으로 방산·안보·대공 수사권 다변화 국면에 발맞추어 안보 분야 인력의 독자성을 확보하려는 시도는 지속되고 있으나, 이를 실질적인 수사 역량과 연계하여 최고 단계의 베테랑으로 공인하고 우대해 주는 안보 특화형 전문수사관 독립 트랙은 여전히 부재한 상태이다. 안보 수사는 축적된 안보 정보 자산과 인적 네트워크, 그리고 기술 보안 인프라에 대한 숙련도가 수사의 성패를 좌우하기 때문에, 범죄 발생 전후의 정보 분석력을 토대로 자원을 집중하는 정보주도형 치안(ILP) 관점의 지속성 있는 인재 축적이 필수적이다.[6]

그러나 전문성을 체계적으로 검증하고 보장해 주는 독자적인 자격 인증 제도의 부재와 수사관의 전문지식적 요소를 장려하지 못하는 현행 제도의 미비는 안보 수사관들의 직무 사기 저하와 일반 수사 부서로의 이탈(순환보직)을 가중시키는 핵심 원인이 되고 있다.[5] 이러한 전문 인력의 불안정성과 인센티브 부족으로 인한 경험 자산의 손실은 일반 경찰 조직뿐만 아니라, 독자적인 책임수사 기능을 수행하는 해양경찰 등 유사 기관의 전문수사관 운영 실태에서도 공통적인 제도적 한계이자 개선 과제로 지적된다.[9]

결과적으로, 태동기에 접어든 방산 안보 전문인재 양성 기조를 안정적으로 뒷받침하고 기술적 진화에 선제적으로 대응하기 위해서는 기존의 일반 책임수사관 제도와 완전히 차별화된, 그리고 국가직무능력표준(NCS) 기반의 직무 설계 원리를 조화롭게 수용한 ‘안보 특화 전문수사관 자격 제도’의 신설이 정책적으로 필요하다.[8]

3. 현행 안보수사관 자격 관리 체계 분석

3.1. 방산 안보 수사의 기술·제도적 한계

3.1.1. 방산 기술의 고유한 특수성

방산 안보 수사가 일반 형사 및 사이버 수사와 구별되는 가장 큰 차이점은 수사 대상이 되는 기술 자산이 ‘무기체계 설계 프레임워크’ 및 ‘군사 작전 요구성능(ROC)’과 직접 결합되어 있다는 점이다. 일반 기업의 산업기술은 상업적 가치와 시장 독점성을 기준으로 평가되지만, 방산 기술은 국가 안보 및 군사력 비대칭성과 직결되는 최고 등급의 군사기밀적 성격을 내포한다.[10]

그러나 현행 경찰의 안보수사 체계는 기술 유출 혐의를 포착하더라도 유출된 데이터가 군사적으로 어떤 치명적인 가치를 가지는지, 혹은 국방과학 R&D 단계 중 어느 공정에서 유출되었는지 법적으로 유효하게 증명하는 데 한계를 드러낸다. 방산 기술 고유의 법적·기술적 메커니즘을 심층적으로 해석할 수 있는 안보수사관의 전문지식 부재는 법정에서 범죄 혐의를 입증하는 과정에서 가장 큰 걸림돌로 작용하고 있다.[7]

3.1.2. 방산 안보 특수성 및 기술·제도적 이해 부족

방산 비리 및 기술 유출 범죄의 흐름을 추적하기 위해서는 소요 제기부터 연구개발, 시험평가, 양산 및 도태에 이르는 복잡한 ‘국방 획득 절차(Defense Acquisition Process)’와 군·방사청·방산업체 간의 정부 주도형 안보 거버넌스 구조를 완벽히 이해해야 한다.[1]

그러나 일반적인 죄중 중심의 훈련만 받은 안보수사관은 방위사업법, 국방보안훈령 등 방산 전반을 규율하는 독자적인 법제와 절차적 규범에 대한 이해가 부족하여 수사의 초기 단계를 설계하

는 데 난항을 겪는다. 안보 수사 주체가 이러한 특수한 행정·군사적 메커니즘을 사전에 인지하지 못할 경우, 단순한 문서 유출 수준의 지엽적인 수사에 머무르게 되며 국가 간 하이브리드 전쟁 형태로 진화하는 조직적 기술 스파이 범죄의 실체적 진실을 규명하는 것은 불가능에 가깝다.[2]

3.2. 현행 수사관 자격 등급제의 제도적 한계

3.2.1. 일반적 경과 중심 정량 평가 체계의 한계

현재 경찰청이 수사 역량 상향 평준화를 위해 운용 중인 ‘수사관-전문수사관-책임수사관’ 자격 체계는 형사, 경제, 지능 등 일반 죄종별 실적 지표를 기준으로 설계되어 있어 안보 수사의 특수성을 포괄하지 못한다. 일반 수사 부서의 자격 인증 및 심사는 ‘사건 송치 건수’, ‘체포·영장 신청률’ 등 단기적·정량적 실적에 치중되어 있다.[4]

반면, 방산 안보 수사는 단 한 건의 유출 혐의를 규명하기 위해서도 수개월 동안 방대한 기술 자료를 분석하고 국방 법제의 위법성을 정밀 검토해야 하는 장기적·정성적 노력이 투입된다. 결과적으로 현행 평가 체계 하에서는 방산 안보 수사관들의 고도의 전문성이 정량적 지표에 밀려 저평가 되는 구조적 모순이 발생하며, 이는 안보 수사관들이 전문 자격을 취득하거나 안보 부서에 장기 잔류하는 것을 저해하는 요인이 된다.

3.2.2. 경과 인증 체계 내 안보 특화 트랙의 전문성 부재

현행 제도하에서는 일반 사이버 분야나 경제 분야의 전문수사관 자격을 보유하고 있더라도 방산 기술의 특수성이나 안보 법제를 이해하지 못해 실질적인 방산 범죄 수사에서 한계를 드러내는 경우가 많다. 안보 분야 수사는 일반적인 디지털 증거 분석 역량뿐만 아니라 안보적 판단력과 방산 기술 보호 법제에 대한 이해가 결합한 ‘융합형 역량’이 필수적이기 때문이다.[5]

그러나 현재 경찰의 자격제도 내에는 이러한 기술·안보 융합형 전문성을 공인해 주는 ‘안보 특화 전문수사관’ 독자 트랙이 부재하다. 이로 인해 안보 수사의 전문성이 객관적으로 인증받지 못하면서 우수 인력이 일반 수사 부서로 이탈(순환보직)하는 현상이 지속되고 있으며, 결과적으로 고도화 되는 경제안보 위협에 체계적으로 대응할 베테랑 인적 자원의 축적 체계가 단절되는 결과를 초래하고 있다.

3.3. 과학치안 R&D 자산과 인적 운용 체계 간의 비대칭성

경찰 조직 차원에서 기술 패권 경쟁에 대응하기 위해 첨단 ICT 인프라 확충과 과학치안(Science Policing) R&D 투자는 지속해서 확대되어 왔다. 그러나 정작 현장 안보수사 인력의 선발과 보직 운용은 여전히 전통적인 단기 순환보직 체계에 머물러 있어, 범죄 발생 전후의 징후를 토대로 수사력을 집중하는 정보주도형 치안(ILP) 관점의 전문성이 정제되어 있다.[6]

방산 기술 유출 패러다임의 고도화 속도와 이를 분석할 현장 수사 인력의 인적 전문성 간에 심각한 ‘비대칭성’이 발생하고 있는 것이다. 국가직무능력표준(NCS) 등을 활용한 전문 직무 설계나 자격 인증 기준이 마련되지 않은 채 인프라에만 의존하는 현행 방식은 과학치안 거버넌스의 거대한 공백으로 지적된다.[8] 따라서 인프라 투자에 걸맞은 ‘방산 안보 특화 전문수사관 자격 제도’의 설계가 정책적으로 필요하다.

4. 경찰의 방산 안보 전문수사관 제도 도입 및 고도화 방안

4.1. 안보 특수성을 반영한 전문수사관 자격 체계 다변화

4.1.1. 방산 안보 전문수사관 자격 트랙의 독자적 신설

현행 경찰 수사관 자격 체계의 일반 죄종별 편중성을 극복하고 방산 안보 범죄에 효과적으로 대응하기 위해서는, 기존의 형사·사이버 트랙과 분리된 ‘방산 안보 전문수사관’ 인증 트랙을 독자적으로 신설해야 한다.[5]

단순히 일반 수사 경력에 안보 부서 근무 기간을 가산하는 소극적 방식에서 탈피하여, 기술과 안보가 복합된 영역의 직무 역량을 공인할 수 있는 독립적 평가 제도가 수립되어야 한다. 이를 위해 자격 인증 요건에 군사기밀보호법, 방위사업법, 산업기술보호법 등 관련 법령의 다차원적 해석 능력과 무기체계의 특수성을 고려한 정성적 수사 난이도를 평가 지표에 명시해야 한다.[10] 아울러, 지원자의 안보적 판단력과 방산 법제 적용 능력을 정밀 검증할 수 있는 심층 서류 심사 및 구술 면접 제도를 결합하여 운영할 필요가 있다.

4.1.2. 방산 분야 이해도 중심의 정성적 평가 지표 도입

정량적인 ‘사건 송치 건수’와 ‘영장 신청률’ 중심의 현행 평가 지표는 장기적인 내사와 정밀한 기술 가치 평가가 요구되는 방산 안보 수사의 특성과 명백한 미스매치를 일으킨다.[4] 따라서 안보 전문수사관 및 책임수사관 자격 심사 시 다음과 같은 정성적·직무 특화형 기술 지표가 중심이 되는 평가체계의 고도화가 요구된다.

첫째, ‘무기체계 기술 가치 및 안보 저해성 입증도’이다. 수사 과정에서 유출된 방산 기술이 군사 작전 요구성능(ROC)이나 비대칭 군사력에 미치는 치명성을 논리적으로 규명하고, 그것이 국가 안보에 초래할 위협 수준을 정성적으로 입증해 낸 기여도를 평가에 반영한다.[7]

둘째, ‘국방 획득 절차 및 거버넌스 분석 역량’이다. 연구개발, 시험평가, 소요 제기 등 복잡한 방위사업 R&D 공정 단계 중 어느 지점에서 위법 행위나 기술 탈취가 발생했는지 범죄 혐의 간의 인과관계를 체계적으로 재구성한 실적을 공인하고, 이를 특별 승진 및 포상 기제와 긴밀히 연계해야 한다.[1]

4.2. 기술·안보 융합형 전문인재 양성 과정 신설

4.2.1. 국방 R&D 및 방산 특화 실무 교육 도입

태동기에 접어든 방산 안보 인재 양성 기초가 실효성을 거두기 위해서는 단순한 이론 중심 교육이나 일반 형사법 위주의 훈련에서 벗어나, 국가직무능력표준(NCS)의 직무 체계를 조화롭게 수용한 ‘기술·안보 융합형 실무 교육 프레임워크’로 전면 전환되어야 한다.[8]

경찰수사연수원 및 안보 전문 교육기관 내에 방산 R&D 프로세스, 군사기밀 관리 메커니즘, 국방보안훈령 실무를 포괄하는 전문 교육 과정을 상설화해야 한다. 이를 통해 수사관들이 무기체계 설계도면 해석법, 방산 기술 보호 표준 통제 기법, 하이브리드전 양상으로 진화하는 글로벌 스파이 조직의 범죄 프로파일링 기법을 실시간으로 학습하고 수사에 대입할 수 있는 ‘실무 연계형 고도화 과정’을 체계화할 필요가 있다.[2]

4.2.2. 과학치안 R&D 자산과 인적 역량의 유기적 연계

조직 내 기술 자산과 현장 수사 인력 간의 비대칭성을 해결하기 위해, 국가 과학치안 R&D 사업을 통해 개발된 첨단 기술 수사 소프트웨어와 데이터 분석 장비를 전문수사관 자격 제도와 유기적으로 결합해야 한다.

단순히 장비를 도입하는 것에 그치지 않고, 정보주도형 치안(Intelligence-Led Policing) 관점에서 범죄 징후를 사전에 분석하고 차단할 수 있는 인적 역량을 갖추도록 장비 운용 자격과 전문수사관 자격 기준을 연계해야 한다.[6] 또한 신규 방산 안보 수사 기법 개발 단계부터 현장 안보수사관들을 테스트베드(Test-bed) 요원으로 적극 참여시켜 과학치안 인프라의 현장 수용성을 높이고, 전문 직무 기술을 장려하는 조직 문화를 구축해야 한다.

4.3. 민·관·학 협력 및 거버넌스 기반의 인프라 구축

4.3.1. 통합 정보 환류 네트워크 주도형 인재 육성

방산 안보 전문수사관은 단방향적인 수사권 행사의 주체에 머무르지 않고, 기술 유출의 1차 접점인 민간 방산업체, 정부 유관기관(방위사업청, 국방기술진흥연구소 등), 그리고 학계 연구소의 보안 책임자들과 상시 소통할 수 있는 ‘네트워크형 거버넌스 주체’로 육성되어야 한다.[1]

독자 트랙을 통해 공인된 전문수사관들에게 민·관·학 합동 방산안보 콘퍼런스나 방산기술보호 실무 협의체의 경찰 측 전담 패널 역할을 부여하는 것이 효과적이다. 이를 통해 방산 기술 유출의 최신 트렌드와 고도화되는 위협 징후에 대한 고가치 첩보를 실시간으로 환류받고, 유관 기관과의 신뢰를 바탕으로 사전에 취약점을 진단·대응할 수 있는 제도적 소통 채널을 안보 수사의 핵심 자산으로 정착시켜야 한다.[3]

4.3.2. 지속 가능한 조직 안정화 및 인센티브 체계 고도화

전문수사관 제도가 실질적인 실효성을 발휘하려면 자격 취득이 경력 발전과 직결되는 강력한 유인 기제가 보장되어야 한다.[4] 방산 안보 전문수사관 및 책임수사관 자격을 취득한 인력에 대해서는 안보 경과 내부의 핵심 보직 임용 시 우선권을 부여하고, 전문직위(Professional Position) 지정을 통한 장기 보직을 부여하여 순환보직으로 인한 전문성 단절을 원천적으로 막아야 한다.

이와 함께 안보 특화 수사비 특별 편성, 인사 가점 등 인사 및 재정적 인센티브를 패키지 형태로 제공함으로써 전문지식을 갖춘 베테랑 인재들이 안보 수사 부서에 안정적으로 잔류하여 정성적 경험 자산을 지속해서 축적할 수 있는 토대를 마련해야 한다.[5]

5. 결론 및 향후 연구 과제

5.1. 연구 결과 요약 및 시사점

5.1.1. 연구 결과 요약

본 연구는 급변하는 기술 패권 경쟁 및 경제안보 환경 속에서 국가 안보의 핵심 자산인 국방과학 기술을 보호하기 위한 경찰 안보수사 역량의 고도화 방안을 논증하고자, 현행 자격 관리 체계의 실태를 분석하고 ‘방산 안보 전문수사관 제도’ 도입의 당위성을 학술적으로 확인하였다.

이론적 고찰 및 선행연구 분석을 통해 방산 안보 수사의 핵심 대상이 되는 기술 자산은 일반 산업 기술과 달리 군사 작전 요구성능(ROC) 및 무기체계 설계 프레임워크와 유기적으로 결합되어 있음

을 확인하였다.[10] 이러한 특수성으로 인해 방산 안보 범죄는 국방 R&D 프로세스와 방산 거버넌스의 고유한 맥락을 파고들며 지능화되고 있으나, 일반 죄종 중심의 사후적 수사 기법이나 파편화된 디지털 포렌식 역량만으로는 복잡한 기술적 유출 경로와 안보 저해성을 법적으로 유효하게 증명하는 데 명백한 한계가 존재함을 도출하였다.[7]

제도적 실태 분석 결과, 현재 경찰청이 운용 중인 ‘수사관-전문수사관-책임수사관’ 자격 체계는 형사, 경제, 지능 등 일반 죄종의 정량적 실적(사건 송치 건수, 영장 신청률 등)에 편중되어 있어, 장기적·정성적 분석이 필수적인 방산 안보 수사의 특수성을 포괄하지 못하는 ‘제도적 미스매치’를 야기하고 있음이 확인되었다.[4] 또한, 조직 차원의 과학치안(Science Policing) R&D 투자는 확대되고 있으나 현장 인력의 단기 순환보직 체계로 인해 첨단 정보 자산과 인적 전문 역량이 유기적으로 결합하지 못하는 ‘기술 비대칭성’ 문제 역시 심각한 거버넌스의 공백으로 식별되었다.[6]

이러한 구조적 한계를 치유하기 위해 본 연구는 4장에서 일반 수사 트랙과 완전히 분리된 ‘방산 안보 전문수사관’ 독자 트랙의 신설과 무기체계 기술 가치 및 국방 획득 절차 이해도를 평가하는 정성적 직무 특화 지표 도입을 제안하였다.[5] 아울러 국가직무능력표준(NCS)을 준용한 기술·안보 융합형 실무 교육 프레임워크 구축과 민·관·학 협력 기반의 거버넌스 인프라 확립, 그리고 전문직 위 지정을 포함한 장기 보직 유인책 마련을 최종 정책적 대안으로 도출하였다.[8]

5.1.2. 학술적 및 정책적 시사점

본 연구가 가지는 학술적·정책적 시사점은 다음과 같다.

첫째, 학술적 측면에서 전통적 안보학 및 국방행정학 영역에 국한되어 논의되던 융합형 방산안보 거버넌스 이론을 경찰학·수사학의 인적 자원 관리 메커니즘(수사관 자격 등급제)과 유기적으로 결합함으로써 관련 학문의 외연을 실무적으로 확장하였다.[1] 단순한 범죄 진압 이론을 넘어 기술 가치와 국가 안보를 동시에 수호하는 정보주도형 치안(Intelligence-Led Policing)의 이론적 토대를 방산 안보 영역에 투영했다는 점에서 의의가 있다.

둘째, 정책적 측면에서 단순히 안보 수사 인력의 정원 확대나 예산 증액이라는 단편적 처방에서 벗어나, 무기체계의 기술적 특수성과 방산 특화 법제의 융합적 해석 능력을 공인할 수 있는 구체적인 역량 인증 모델을 설계함으로써 실효성 있는 방산 안보 전문인재 양성의 마스터플랜을 제공하였다.[2]

5.2. 연구의 한계점 및 향후 연구 과제

5.2.1. 연구의 한계점

본 연구는 학술적 타당성과 정책적 대안을 정교하게 도출하였음에도 불구하고 다음과 같은 한계점을 지닌다.

본 연구는 현행 제도와 보안 인프라의 실태를 법령 및 선행 문헌 분석을 중심으로 규명하였으나, 경찰 조직의 보안 지침상 현직 안보수사관들의 실제 직무 수행 데이터나 인사 평정 자료를 전수 확보하여 정량적 상관관계를 정밀하게 계량화하는 데는 이르지 못했다.

또한, 안보 특화 전문수사관 트랙 신설을 위한 경찰 내부 지침 개정안은 제시하였으나, 대공·안보 수사권 다변화 환경 속에서 국가정보원, 국군방첩사령부, 방위사업청 등 타 안보·조사 기관과의 사법적 관할권 충돌이나 공동 수사 거버넌스 구축 시 발생할 수 있는 법제도적 마찰을 세부적으로 조율하는 데까지는 논의를 확장하지 못했다.[2]

5.2.2. 향후 연구 과제

앞서 언급한 한계점을 보완하고 방산 안보 전문수사 체계를 더욱 고도화하기 위해 향후 다음과 같은 연구가 지속되어야 한다.

첫째, 경찰의 독자적 자격 체계 고도화를 넘어, 안보 수사 주체 간의 다변화된 환경 속에서 경찰과 군·정보기관 간의 기술·안보 융합형 방산 수사 공조 모델과 고가치 정보 공유 플랫폼의 법적 가이드라인을 정밀하게 규명하는 거버넌스 연구가 뒤따라야 한다.[1]

둘째, 본 연구가 제안한 안보 특화 전문수사관 자격 표준이 실제 제도화된 이후, 장기 근속률 향상, 방산 유출 사건의 사법적 유죄율(혐의 입증 성공률) 변화, 전문지식적 요소의 현장 기여도 등을 정량적으로 추적 평가하는 후속 종단 연구(Longitudinal Study)가 수행되어야 할 것이다.[5]

참고문헌

- [1] 류연승 등. 방위산업 안보환경 변화에 따른 방산안보정책 검토. 한국과 세계, 제4권 제2호, pp. 207-232. 2022. <https://doi.org/10.22743/kwr.2022.4.2.207>
- [2] 이수인. 방위산업 사이버 방첩의 제도적 과제. 방산안보연구, 제1권 제2호, pp. 1-19. 2025. <https://doi.org/10.64227/jdis.2025.1.2.1>
- [3] 류연승. 방산보안 2.0. 정보보호학회지, 제28권 제6호, pp. 6-12. 2018.
- [4] 정혜란. 경찰 전문수사관 인증제도 개선방안에 관한 연구. 중앙대학교 행정대학원, 석사학위논문. 2017.
- [5] 현세준. 전문수사관 인증제의 활성화 방안에 관한 연구: 전문지식적 요소를 중심으로. 한국치안행정논집, 제13권 제3호, pp. 179-202. 2016.
- [6] Ratcliffe JH. Intelligence-Led Policing, 2nd ed. Routledge. 2016.
- [7] 유인수, 류연승. 방산안보의 개념에 관한 고찰. 국방과 보안, 제5권 제2호, pp. 271-284. 2023.
- [8] 강태영, 류연승. NCS를 활용한 방산안보 교육 모델 연구. 한국국방기술학회 논문지, 제6권 제3호, pp. 1-4. 2024.
- [9] 손영태. 해양경찰청 전문수사관 운영제도의 개선방안에 관한 연구. 한국해양경찰학회보, 제9권 제2호, pp. 89-121. 2019.
- [10] 류연승 등. 산업보안학 2판. 박영사. 2022.