방산안보연구
Journal of Defense Industrial Security

방산안보연구, 1권 1호, 2025년 3월, 1-17면.
Journal of Defense Industrial Security, Volume 1, Issue 1, March 2025, Pages 1-17.
https://doi.org/10.?????/jdis.2025.1.1.1

Print ISSN 3091-5546
Online ISSN 3091-5554

원저

방산안보 연구의 한계에 관한 고찰: 국가정보학의 정보수집 및 분석, 방첩의 관점에서

박은열

명지대학교 대학원 방산안보학과, 방산안보학 박사

교신저자: 박은열 (dmsfuf2@empal.com)

요약

방위산업(방산)은 무기체계를 연구·개발·생산하는 산업으로, 무기체계는 군사정보 수집 및 분석의 주요 목표가 될 가능성이 높다. 그러나 기존 방산안보 연구는 정보기관이 활용하는 5대 정보출처를 기반으로 한 정보수집 및 분석 위협을 충분히 다루지 못하고, 주로 정책적 접근과 부분적인 방어적 방첩 연구에 집중되어 있다. 이에 본 논문은 국내외에서 수행된 다양한 방산안보 연구를 검토하고, 해외 정보기관이 실제로 수행한 무기체계 분석 사례를 종합적으로 분석하여 기존 연구의 추세와 한계를 국가정보학의 정보수집, 분석, 방첩 관점에서 진단하였다. 이후, 이러한 한계를 보완하기 위해 방산안보학이 무기체계 관련 정보수집 및 분석 위협에 대한 심층적 연구를 수행해야 하며, 공격적 방첩 개념을 포함한 통합적 방첩 접근으로 확장될 필요가 있음을 제안한다. 기존 방산안보 연구의 한계와 이를 극복하기 위한 방산 방첩 개념을 도식화하여 제시하는 본 논문은 다차원적 방산 방첩 연구의 방향성을 제시하고, 실질적이고 체계적인 방산안보 전략 수립을 위한 기초를 제공하고자 한다.

핵심어

방산안보, 정보수집, 정보분석, 기술정보, 방첩

차례

접수일: 2024년 11월 14일
수정일: 2024년 12월 08일
게재승인일: 2025년 03월 17일
출판일: 2025년 03월 31일

Original Article

Reflections on the Limitations of Defense Industrial Security Research: Perspective of Intelligence Collection, Analysis, and Counterintelligence in National Intelligence Studies

Eunyeol Park

Ph.D. in Defense Industrial Security, Graduate School of Myongji University, Republic of Korea

Corresponding Author: Eunyeol Park (dmsfuf2@empal.com)

ABSTRACT

The defense industry focuses on the research, development, and production of weapon systems, which are significant targets for military intelligence collection and analysis. However, existing defense industrial security research has largely overlooked threats posed by intelligence collection based on the five primary sources used by intelligence agencies, focusing instead on policy and defensive counterintelligence. This paper reviews domestic and international studies on defense industrial security and analyzes real-world cases of weapon system analysis by foreign intelligence agencies to identify trends and limitations. It highlights the need for in-depth research on intelligence threats to weapon systems and proposes expanding defense industrial security studies to include integrated counterintelligence approaches with offensive counterintelligence. The findings aim to guide multidimensional counterintelligence research and support the development of systematic defense industrial security strategies.

KEYWORDS

Defense Industrial Security, Intelligence Collection, TECHINT, Counter Intelligence

1. 서론

1.1. 연구의 배경 및 필요성

방위산업은 첨단 과학기술이 집약된 분야이므로, 국가안보는 물론 경제적 자립과 국제적 위상에도 직접적인 영향을 미치는 중요한 산업이다. 따라서 방산안보 연구는 이러한 방위산업을 보호하고 외부 위협을 예방하며, 방산 위협감소에 핵심적인 역할을 수행하는 국가안보의 중요한 학문적 영역이 되어야 한다.

또한 방산안보 연구는 방산이 무기체계 등을 생산하는 산업의 영역으로 군사 분야와 매우 밀접한 관련이 있다는 특성과, 방산의 대표적인 생산품이라 할 수 있는 무기체계는 해외 정보기관에서 수행하는 군사정보(Military Intelligence) 수집 및 분석의 주된 표적이 될 가능성이 매우 높은 객체라는 특성을 가지고 있다는 점을 충분히 고려한 가운데 연구를 수행하여야 한다.

그러나 현재의 방산안보 연구 추세는 이러한 특성을 기초로 국가정보학에서 제시되는 다양한 정보출처와의 직접적인 연관성과 위협을 고찰하는 형태의 연구가 부족한 상황이며, 주로 법률 및 제도적 검토와 같은 전반적 개념을 주로 연구하고 있다.

특히 방산 방첩 분야의 연구 역시 사이버 보안·기술 보호 등 방어적 방첩의 영역에 가까운 연구가 중점적으로 이루어지는 경향이 있고, 방첩수집과 공격을 포함한 방첩 전반에 관한 연구는 드문 상황이다. 이러한 연구의 한계는 장기적으로 국가안보와 방산안보 전반에 걸쳐 위협을 초래할 뿐 아니라, 국제 방산시장에서 대한민국의 경쟁력 저하를 초래할 수 있는 중요한 문제로, 반드시 보완되어야 한다.

이에 본 논문은 국가정보학에서 제시하는 정보수집 및 분석, 방첩의 관점에서 각각 방산안보의 연구 한계를 진단하고 대응의 필요성을 제시하기 위해 작성되었다.

1.2. 연구 목적과 구성

본 연구는 상기한 1절의 배경 및 필요성을 바탕으로 기존 방산안보 연구 추세를 종합적으로 검토하고, 국가정보학의 정보수집 및 분석, 방첩의 관점에서 연구 한계를 분석하여, 대응방안을 제시하는 것을 그 목적으로 한다. 이를 위해 2장 '방산안보학의 연구 추세'에서는 ① '국내·외의 방산안보 연구'로부터, ② '방산안보 연구 종합 및 추세 분석'으로 구분하여 2024년까지의 방산보안 및 방산안보 연구를 검토하고 분석하였다.

3장 '정보수집 및 분석, 방첩 관점에서의 방산안보 연구 한계'에서는 ① '정보수집 위협과 대응 연구의 한계'를 통해 국가정보학에서 제시하는 정보수집 및 분석의 관점에서 5대 정보출처(HUMINT, SIGINT, GEOINT, MASINT, OSINT)를 중심으로 무기체계를 대상으로 수행된 정보수집 및 분석 관련 사례와 위협을 제시하고, ② '통합적 방첩 연구의 한계'를 통해 기존 연구의 부족함을 진단하며, ③ '연구의 한계가 초래할 위협'을 통해 상기 2개의 연구 한계가 불러올 수 있는 문제점을 제시하였다.

4장 한계의 대응 방안에서는 ① '정보수집 위협 연구의 수행' 필요성을 제시하고, ② 총체적 방첩(MDCI)의 개념이 적용된 '통합적 방첩 연구의 수행' 필요성을 제시하였다.

5장 결론에서는 위에서 살펴본 다양한 문제점과 대응 방안을 정리하고 연구 시사점과 한계를 기술하였다. 또한, 기존 방산안보 연구의 한계를 극복하며, 보다 다각적이고 통합적인 방산안보 체계를 구축하기 위한 실질적인 연구 제언을 기술하였다.

2. 방산안보의 연구 추세

2.1. 국내·외의 방산안보 연구

방산안보학은 신생 학문으로 그 역사가 길지는 않으나, 방산안보의 개념 정립 이전에 명지대학교의 류연승 교수가 2014년 방산보안협의회와 MOU를 체결하고 2015년 연구소를 개소함에 따라 방산보안이 학문으로 인식되었으며 방산보안을 주제로 하는 다양한 연구들이 진행되었다.[1]

이후 방산보안과 관련하여 다양한 연구를 확인할 수 있었으며, 국내부터 살펴보면, 첫 번째로, 류연승(2018)이 정보보호학회지를 통해 "방산보안 2.0"을 제시하며, 방산보안의 발전과 변화에 대해 논하였고, 방산이 발전함에 따라 정의 또한 변화해 왔으며, 방산기술보호법 제정 이후를 방산보안 2.0의 시대라고 구분하여 민간과의 정보공유·상호교류 및 지원을 통한 개방적 선진 방산보안 제도의 지원과 구축이 필요하다고 주장하였다. 주된 위협으로는 사이버 침해 · 역공학 등을 제시하였다.[2]

두 번째로, 허아라와 류연승(2018)이 한국정보보호학회를 통해 "국방과학기술 정보의 분류체계 고찰"을 발표하였으며, 현행 과학 기술정보 분류체계와 미 국방부의 과학기술 정보의 분류체계를 비교하고 발전 방향을 제시하였다.[3]

세 번째로, 박흥순(2018)이 한국정보보호학회지를 통해 "방위산업 사이버 보안을 위한 방산 정보 공유·분석센터(ISAC) 설립 방안"을 발표하였으며, 정보공유 및 분석센터 설립 사례와 국내 방산업체 보안관제 환경 분석을 통해 방산 정보공유 및 분석센터 설립 방안을 제안하였다. 주된 위협으로 제시한 것은 사이버 공격 분야이다.[4]

네 번째로, 박흥순, 김세용, 김용환(2019)이 융합보안 논문지를 통해 "체계적인 방위산업기술보호를 위한 보호체계 우선순위"를 발표하였으며, 기존 기술 보호지침과 방위산업기술 보호지침에 대한 비교를 수행하고, AHP 기법을 활용하여 보호 체계 세부 항목에 대한 우선순위 분석을 수행하였다.[5]

다섯 번째로, 송경호, 허아라, 류연승(2021)이 한국방위산업학회지를 통해 "무기체계 안티탬퍼링을 위한 기술 식별 및 위험평가 방안"과 "체계공학 기반 안티탬퍼링 프로세스"를 연속으로 발표하였으며, 무기체계 역설계 방지를 위한 안티탬퍼링의 적용 필요성을 논하였다.[6][7]

여섯 번째로, 오광환, 김권일, 차정훈(2021)은 한국산업보안연구를 통해 "방산인력 기술유출 방지를 위한 실태분석 및 개선방안"을 발표하였으며, 기술유출 문제를 분석하고 이를 예방하기 위한 법적·제도적 개선 방안과 인력관리 방안을 제시하였다.[8]

2022년에는 상기한 각종 연구와 발전을 토대로 방산보안의 영역을 넘어 방산안보의 영역으로 학문을 확장시키기 위해 명지대학교 "방산보안 연구소"가 "방산안보연구소"로 개칭되었고, 명지대학교 "방산안보학과"가 개설되었으며, 이를 통해 방산안보학이 학문으로서 정립될 수 있었다.[9]

이후 국내의 방산 관련 분야의 연구는 방산보안의 영역을 넘어 방산안보의 영역까지 다루게 되었다. 이와 관련한 연구의 첫 번째로, 류연승, 김영기, 송은희(2022)가 한국과 세계를 통해 "방위산업 안보환경 변화에 따른 방산안보정책 검토"라는 주제의 논문을 발표하였으며, 방산 침해 보호라는 관점에서 환경과 정책을 검토하였다. 현 보호 정책이 기술 탈취에 중점이 맞춰져 있지만, 방산이 국가안보 등에 미치는 영향을 고려 시 안보 전략적 관점에서 정책의 검토가 필요하고, 국가 대응 시스템 정비, 전문가 양성, 사회적 인식 확대, 국제 협력 관계 증진 등의 필요성과 향후 방산방첩 차원의 정책 모색이 필요하다고 주장하였다.[10]

두 번째로, 같은 해 김영기(2022)가 동중아아시아연구를 통해 “방위산업과 방산안보 발전방안”을 발표하였다. 이를 통해 방산 정책·사건·안보 활동 등을 검토하여 방산안보 발전방안을 제시하였고, 정보수사기관 협력을 통한 기술유출 침해 신고의 대응 체계화와 국정원 안보수사역량의 전환 및 전문화, 방산 정보 지원 조직의 신설 등을 주장하였다. 또한, 주된 위협으로 공급망과 사이버 위협을 언급하였다.[11]

세 번째로, 2023년에 주영진, 손창근 등(2023)이 한국방위산업학회지를 통해 “무기체계 기술보호를 위한 안티탬퍼링 시험평가 방안”을 발표하였다. 이를 통해 수출용 무기체계의 기술 보호 필요성이 증가하고 있으므로, 안티탬퍼링 시험평가 프로세스의 필요성을 주장하였다.[12]

네 번째로, 허아라(2023)는 명지대학교의 학위논문인 “직무분석을 통한 방위산업 기술보호 인력 교육 모델”을 통해 방산기술 보호 인력의 교육 모델을 제시하였다. 이를 통해 NICE(미국 사이버 보안 교육), 국가직무 능력표준(NCS)의 직무체계의 분류와 통합실태조사·CMMC 이행과제 등을 활용하여 방산기술보호 관련 학위 과정의 안을 설계하였고, 주된 위협을 기술 유출로 설정하였다.[13]

다섯 번째로, 2024년에는 김영기(2024)가 단행본인 “방산안보와 국가정보연구”를 통해 법령을 논거로 하는 광·협의의 방산안보, 방위사업 ·산업, 국가안보·정보, 국방정보·방첩, 방산 보안·기술보호 등의 개념을 제시하였다. 더하여 방산 발전과 수출증대는 외국이 한국 방산에 대한 첩보 수집 활동을 증가시킴으로써 방산 위협 역시 증가하고 있다고 하였고, 방산안보란 방위산업·사업을 학문적으로 보호하는 학문이고, 외국의 국·내외 정보활동에 대한 방산업체·기술 보호의 필요성을 주장하였다.[14]

여섯 번째로, 김진경과 류연승(2024)이 한국방위산업학회지를 통해 “무역안보(전략물자) 법제 동향과 방산안보 시사점”을 발표하였다. 방산 수출의 증대 현황, 미·일의 수출통제 관련법 등을 살피고 대외무역법과 방위사업법의 수출입 관련 조항과 벌칙 규정을 비교하였으며, 양 법의 벌칙 규정을 형평성 있게 개정할 필요성을 제안하였다.[15]

일곱 번째로, 유인수와 류연승(2024)이 국방과보안을 통해 “방산안보의 개념에 관한 고찰”을 발표하였다. 이를 통해 방어·수동적 (보호·보안) 외 공격·능동적(개척·육성) 방산안보를 주장하였고, 방산의 범주 역시 협의와 광의로 구분하여 방산안보의 연구 분야를 제시하였다.[16]

여덟 번째로, 배정석(2024)은 박사학위논문인 “방위산업 보호를 위한 방첩의 역할과 범위: 방위산업체와 정보기관의 협력체계를 중심으로”를 발표하였으며, 방첩을 광의의 방첩과 협의의 방첩으로 구분하고, 개념을 제시하였다. 또한, 정보적 위협의 주체로 외국정보기관, 외교관 및 무관, 외국 방위산업체, 외국 협력사 및 합동연구기관, 내부자를 제시하였다. 또한, HUMINT에서는 OC·NOC·AGENT를 포함하였고, TECHINT에서는 해킹·도청·검색·리버스엔지니어링으로 구분하여 제시하였다.[17]

아홉 번째로, 류연승, 김영기 등(2024)이 단행본인 방산안보학 개론을 통해 개관, 방산 침해, 법제, 발전, 트렌드, 보호, 방첩, 국가정보 활동 등을 종합적으로 제시하고 정리하였다.[18]

해외에서도 방산 관련 연구가 다양하게 수행되고 있었으며, 관련한 연구들까지 확장하여 살펴보면, 먼저, Levy와 Gafni(2022)가 “Online Journal of Applied Knowledge Management”를 통해 “Towards the quantification of cybersecurity footprint for SMBs using the CMMC 2.0”를 발표하였는데, 미국 국방부가 CMMC 2.0을 통해 중소기업이 자가 평가를 할 수 있는 지침을 제공하였으며, 이를 기반으로 실무를 기반으로 사이버 보안 발자국의 정량적 평가 방법론을 제안하였다.[19]

Farkas(2023)는 “2023 IEEE 21st Jubilee International Symposium on Intelligent

Systems and Informatics (SISY)"를 통해 "The Challenges for the European Defense Industry"를 발표하였으며, 유럽의 안보를 보장하는 핵심은 유럽의 방위산업이며, 방산 진흥을 창출하기 위해서는 국제 협력과 방산 간 협력이 필수적이라고 주장하였다.[20]

Fonfria(2023)는 "Informacion Comercial Espanola Revista de Economia"를 통해 "LA INDUSTRIA DE DEFENSA EUROPEA FRENTE A LA AUTONOMÍA ESTRATÉGICA"를 발표하였으며, 팬데믹 이후 공급망 문제를 중점으로 하는 방위산업에의 영향을 분석하였다.[21]

Brown(2024)이 연속간행물인 "Global Security & Intelligence Studies"를 통해 "Industrial Security Policy Application in High Tech Defense Industry"를 발표하였으며, 공공-민간 협력을 통해 보안 표준화를 강화하고 방위산업 기반을 효과적으로 보호할 필요가 있다고 주장하였다.[22]

Baydarov 와 Faikov(2024)는 정기 간행물인 "Управление"를 통해 "Обоснование комплекса мер по формированию институциональной среды и системы управления диверсификацией оборонно- промышленного комплекса"를 발표하였다. 방산의 발전을 위해 민간 제품 분야로의 다각화를 수행 시 기술 주권 강화와 기술 선도 달성을 가능하게 한다고 주장하였으며, 러시아 방위산업의 다각화를 위한 제도적 환경 및 관리 체계 구축 방안을 제시하고, 효과적인 실행을 위한 법적·제도적 기반과 단계적 접근이 필요하다고 강조하였다.[23]

2.2. 방산안보 연구 종합 및 추세 분석

위에서 살펴본 바와 같이 국내·외의 연구 모두 전반적으로 사이버 보안, 공급망 문제, 법률적 검토, 안티탬퍼링 등 각개 분야에서 집중적인 연구가 진행되고 있었다. 또한, 위의 문헌 외에도 다양한 논문 등의 학술 자원이 존재하나, 해외의 최근 연구까지 모두 포함해서 고찰해 보아도 방산안보 연구는 국가정보학에서 제시되는 5대 정보출처 전 분야에 걸친 대응과 공격적 방첩을 포함하는 통합적 방첩 개념에서의 접근으로 연구가 확장되지 못하였음을 확인할 수 있었다.

기존의 방산보안 연구를 포함하여 연구를 종합하고 추세를 분석해 보면, ① 인간·사이버 공격에 의한 기술 유출 및 대응, ② 수출 장비 등의 안티탬퍼링, ③ 방산 보호 인력양성, ④ 방산 분야 법제 검토, ⑤ 방산안보의 개념 정립 및 연구 분야 제시 등이 주된 연구 방향과 추세를 이루고 있었다. 2024년의 최신 연구를 포함하여도 해외 정보기관 등이 활용하는 5대 정보출처의 일부만이 포함되거나 개괄적으로만 포함되어 전 출처에서의 정보수집 및 분석의 가능성과 공격적 방첩을 포함한 통합적 방첩 측면에서의 대응으로 접근하는 문헌을 찾아볼 수 없었다. 이를 정리한 내용은 아래의 표 1과 같다.

표 1. 방산안보 연구가 제시하는 위협(문제점)과 대응하는 방첩의 영역

구 분	제시 위협(문제점)	방어적 방첩	공격적 방첩
류연승(2018)	사이버, 역공학	O	X
허아라, 류연승(2018)	정보분류 체계	X	X
박흥순(2018), 박흥순 외(2019), Levy, Gafni(2022), Brown(2024)	사이버	O	X
송경호 외(2021), 주영진 외(2023)	역공학	O	X

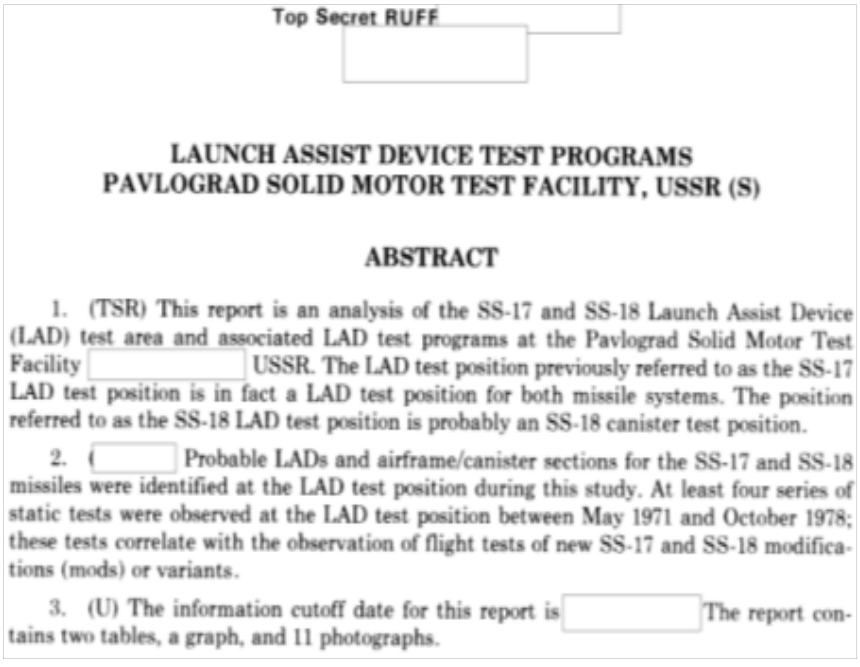
오광환 외(2021)	인력에 유출	O	X
류연승 외(2022)	기술 탈취, 발전된 위협	O	△
허아라(2023)	사이버, 인력에 의한 유출	O	X
Fonfria(2023)	공급망	△	X
김영기(2022)	공급망, 사이버	O	X
김영기(2024)	외국 등의 정보활동	O	△
김진경, 류연승(2024)	법률적 검토	X	X
유인수, 류연승(2024)	방산안보 개념	△	△
배정석(2024)	5대 정보출처 일부	O	△
류연승 외(2024)	사이버, 역공학 및 5대 정보출처 일부	O	△
Baydarov , Faikov(2024)	민간 개방 및 다각화	X	X

3. 정보수집 및 분석, 방첩 관점에서의 방산안보 연구 한계

3.1. 정보수집 및 분석의 위협과 대응 연구의 한계

국가정보학의 정보수집에 따르면 정보기관은 크게 5개의 정보출처를 활용하여 정보를 수집하고 분석을 진행하고 있다. 무기체계에 대한 정보수집과 분석 역시 수행 중인데, 이는 CIA FOIA 등을 통해 확인할 수 있다.

각 출처에 의한 무기체계의 정보분석 사례를 간략하게 살펴보면, 첫 번째로, 아래의 그림 1과 같이 U.S NPIC(1979)이 작성하고 비밀 해제된 “LAUNCH ASSIST DEVICE TEST PROGRAMS, PAVLOGRAD SOLID MOTOR TEST FACILITY, USSR”에서 IMINT (GEOINT)를 활용하여 USSR의 LAD를 식별하고 분석한 사실을 확인할 수 있다.[24]



Top Secret RUFF

LAUNCH ASSIST DEVICE TEST PROGRAMS
PAVLOGRAD SOLID MOTOR TEST FACILITY, USSR (S)

ABSTRACT

1. (TSR) This report is an analysis of the SS-17 and SS-18 Launch Assist Device (LAD) test area and associated LAD test programs at the Pavlograd Solid Motor Test Facility USSR. The LAD test position previously referred to as the SS-17 LAD test position is in fact a LAD test position for both missile systems. The position referred to as the SS-18 LAD test position is probably an SS-18 canister test position.

2. (Probable LADs and airframe/canister sections for the SS-17 and SS-18 missiles were identified at the LAD test position during this study. At least four series of static tests were observed at the LAD test position between May 1971 and October 1978; these tests correlate with the observation of flight tests of new SS-17 and SS-18 modifications (mods) or variants.

3. (U) The information cutoff date for this report is The report contains two tables, a graph, and 11 photographs.

그림 1. NPIC(1979)의 소련 고체 로켓 모터 관련 보고서 中

두 번째 사례로, U.S. CIA DI(1970)는 “Basic Imagery Interpretation Report”를 통해 모스크바 퍼레이드에서 촬영된 공개 사진(OSINT)을 바탕으로 선형 치수 ±2%, 또는 0.05ft 이내의 오차 수준을 언급할 정도로 정밀하게 분석하였으며, 사진 원형과 분석된 내용은 아래의 그림 2와 같다.[25]

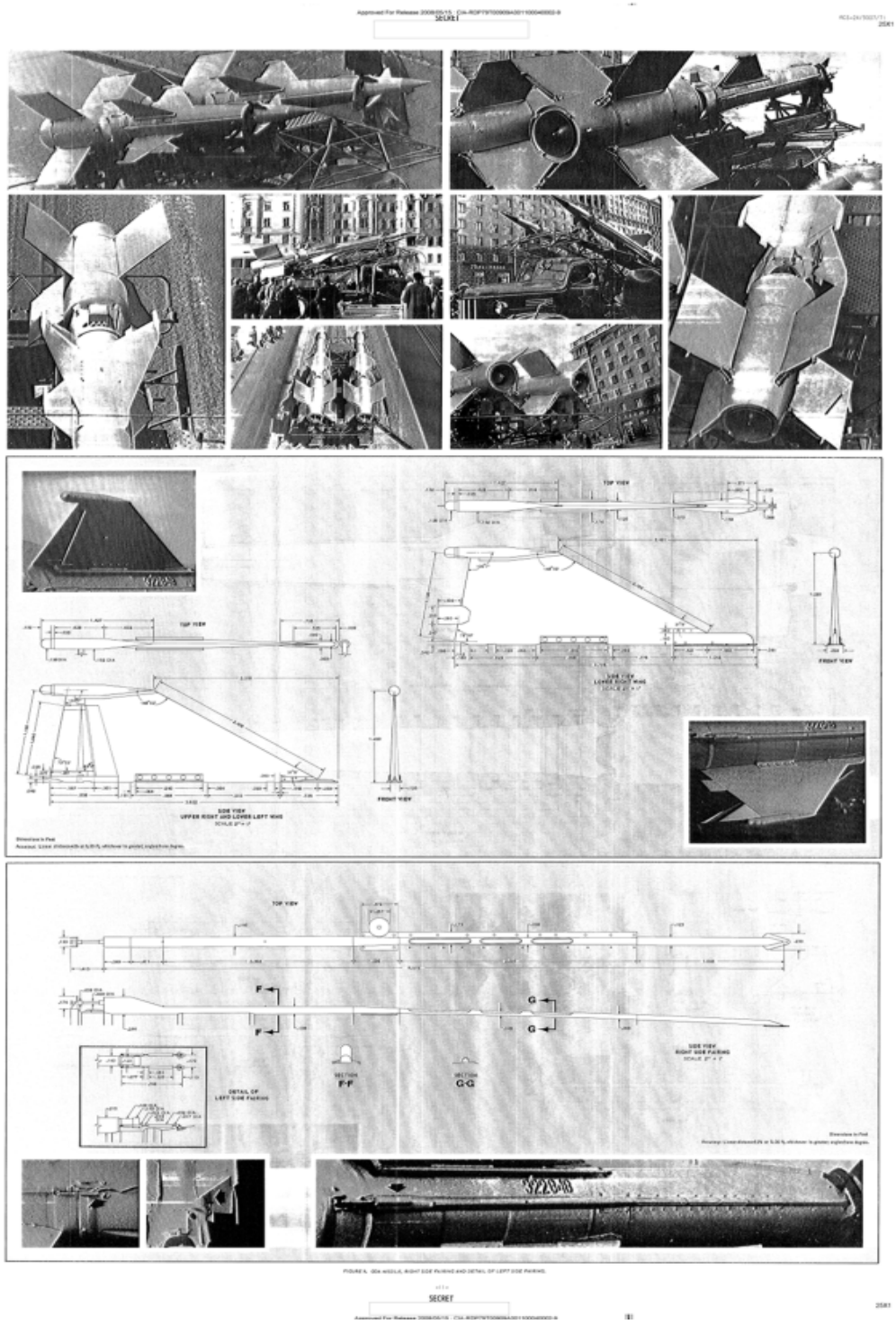
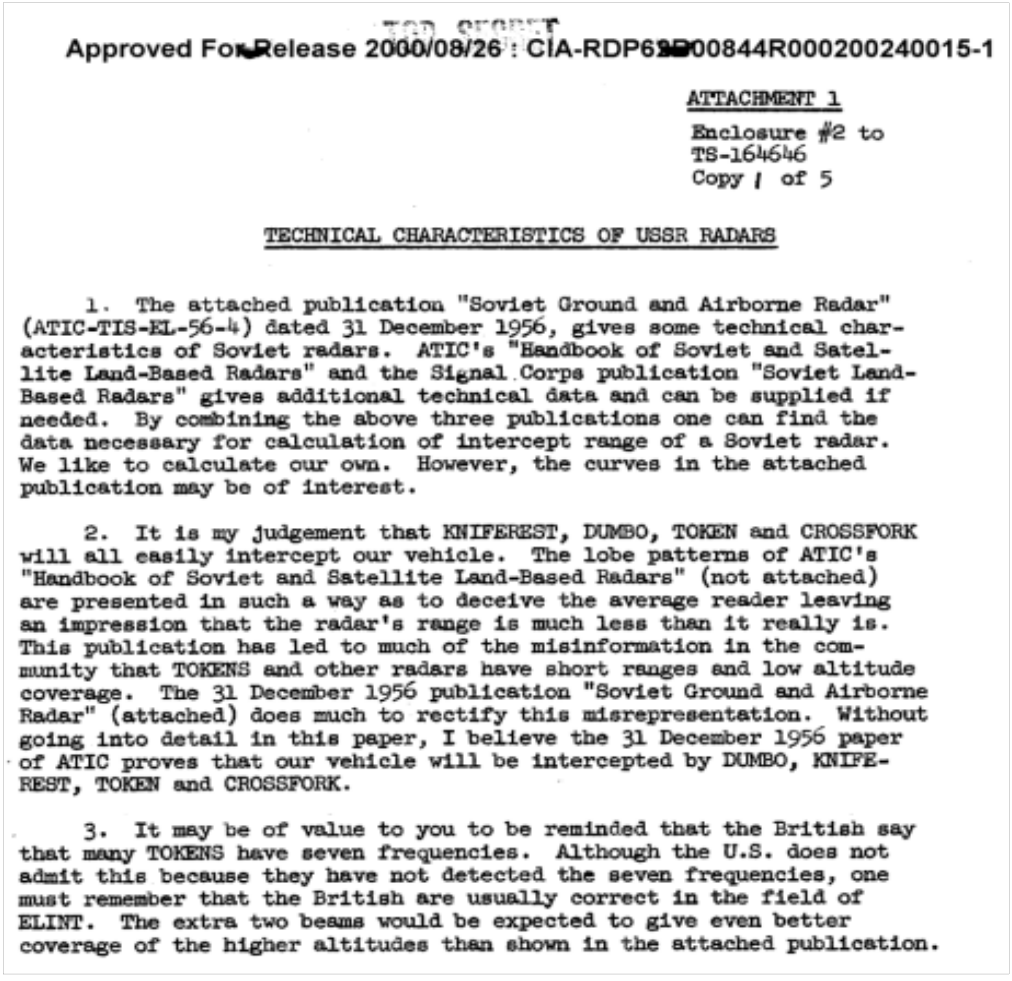


그림 2. U.S CIA DI(1970)의 SA-3 영상 통합 보고서 中

세 번째 사례로, U.S. CIA가 작성하고 비밀 해제된 “TECHNICAL CHARACTERISTICS OF USSR RADARS”를 살펴보면 아래의 그림 3과 같이 SIGINT를 활용하여 소련의 레이더들에 대한 기술적 특성을 분석하였다는 사실을 확인할 수 있다.[26]



TOP SECRET

Approved For Release 2000/08/26 : CIA-RDP6[illegible]00844R000200240015-1

ATTACHMENT 1
Enclosure #2 to
TS-164646
Copy 1 of 5

TECHNICAL CHARACTERISTICS OF USSR RADARS

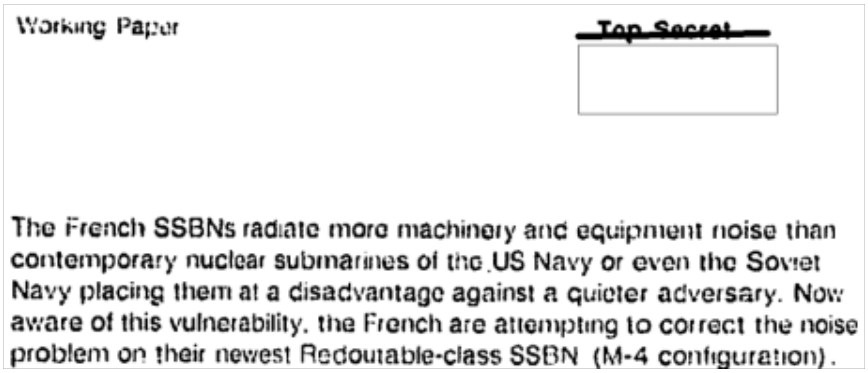
1. The attached publication "Soviet Ground and Airborne Radar" (ATIC-TIS-EL-56-4) dated 31 December 1956, gives some technical characteristics of Soviet radars. ATIC's "Handbook of Soviet and Satellite Land-Based Radars" and the Signal Corps publication "Soviet Land-Based Radars" gives additional technical data and can be supplied if needed. By combining the above three publications one can find the data necessary for calculation of intercept range of a Soviet radar. We like to calculate our own. However, the curves in the attached publication may be of interest.

2. It is my judgement that KNIFEREST, DUMBO, TOKEN and CROSSFORK will all easily intercept our vehicle. The lobe patterns of ATIC's "Handbook of Soviet and Satellite Land-Based Radars" (not attached) are presented in such a way as to deceive the average reader leaving an impression that the radar's range is much less than it really is. This publication has led to much of the misinformation in the community that TOKENS and other radars have short ranges and low altitude coverage. The 31 December 1956 publication "Soviet Ground and Airborne Radar" (attached) does much to rectify this misrepresentation. Without going into detail in this paper, I believe the 31 December 1956 paper of ATIC proves that our vehicle will be intercepted by DUMBO, KNIFEREST, TOKEN and CROSSFORK.

3. It may be of value to you to be reminded that the British say that many TOKENS have seven frequencies. Although the U.S. does not admit this because they have not detected the seven frequencies, one must remember that the British are usually correct in the field of ELINT. The extra two beams would be expected to give even better coverage of the higher altitudes than shown in the attached publication.

그림 3. TECHNICAL CHARACTERISTICS OF USSR RADARS 中

네 번째 사례로, U.S. CIA DI(1984)의 보고서 “Foreign Submarine -Launched Ballistic Missiles”를 살펴보면, 아래의 그림 4와 같이 프랑스의 SSBN에 대한 상세한 정보분석이 수행되었으며, 특히 ‘프랑스의 SSBN은 미국과 소련의 핵잠수함 대비 기계 장비 소음의 방사 수준이 높고, 최신 Redoutable급 잠수함에서는 이러한 문제를 수정하려 한다.’는 내용이 포함되어 있다. 이러한 문건은 미국의 정보기관이 냉전 당시 2세계 뿐만 아니라 우호국 프랑스 등에도 정보수집과 분석을 수행하였으며, 특히 소음수준 등을 측정하는 MASINT를 활용한 DB의 구축이 진행되어 있었음을 확인할 수 있는 대목이다.[27]



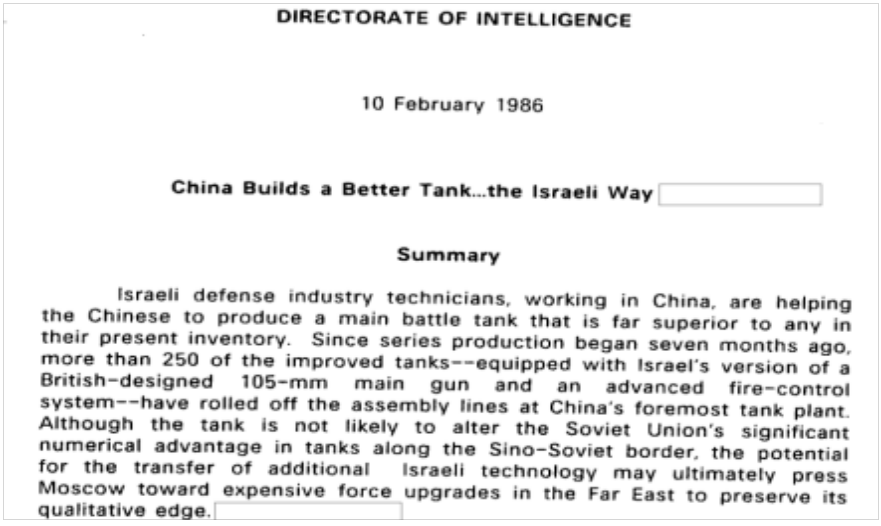
Working Paper

Top Secret

The French SSBNs radiate more machinery and equipment noise than contemporary nuclear submarines of the US Navy or even the Soviet Navy placing them at a disadvantage against a quieter adversary. Now aware of this vulnerability, the French are attempting to correct the noise problem on their newest Redoutable-class SSBN (M-4 configuration).

그림 4. U.S CIA DI(1984)의 프랑스 SSBN 관련 보고서 中

다섯 번째 사례로, 아래의 그림 5와 같이 중국의 전차 개량 동향과 관련한 U.S. CIA DI(1986)의 보고서 "China Builds a Better Tank…the Israeli Way"가 있으며, CIA DI는 중국이 이스라엘과의 협력을 통해 전차의 주포 개량 등을 추진하고 있다고 분석하였고, 보고서에서 사용된 출처로는 OSINT와 HUMINT 등이 원 출처로 추정될 수 있는 내용들이 직·간접적으로 언급되었다.[28]



DIRECTORATE OF INTELLIGENCE

10 February 1986

China Builds a Better Tank...the Israeli Way

Summary

Israeli defense industry technicians, working in China, are helping the Chinese to produce a main battle tank that is far superior to any in their present inventory. Since series production began seven months ago, more than 250 of the improved tanks--equipped with Israel's version of a British-designed 105-mm main gun and an advanced fire-control system--have rolled off the assembly lines at China's foremost tank plant. Although the tank is not likely to alter the Soviet Union's significant numerical advantage in tanks along the Sino-Soviet border, the potential for the transfer of additional Israeli technology may ultimately press Moscow toward expensive force upgrades in the Far East to preserve its qualitative edge.

그림 5. U.S CIA DI(1986)의 중국의 개량형 전차 관련 보고서 中

이렇듯 다양한 정보출처를 활용하여 무기체계에 대한 정보분석을 수행한 상기 사례들은 해외 정보기관들이 사용하는 다양한 정보수집 분야에서의 위협과 대응 연구의 필요성을 시사한다. 하지만 2장 현 방산안보 연구 추세에서 살펴본 바와 같이 기존 방산안보 연구에서는 해당 분야의 본격적인 연구가 수행되지 못하고 있는데, 방산 법제·개념 정립 연구는 전반적 개념을 다루는 연구이므로 별개로 상정하고, 인간에 의한 기술 유출 대응 연구가 HUMINT(OC·NOC), 사이버 공격에 의한 기술 유출 대응 연구가 SIGINT(COMINT) 및 OSINT(Public Data, Gray Literature), 안티탬퍼링 연구가 MASINT(Material)의 부분적인 대응이 가능할 것으로 예측되므로, 박은열(2025)이 주장한 바와 같이 정보출처별 수집수단이 방산안보에 미치는 연구와 대응에 있어 아래의 그림 6의 회색 음영 부분과 적색 실선 부분과 같은 한계와 위협이 잔존하고 있음을 확인할 수 있다.[29]

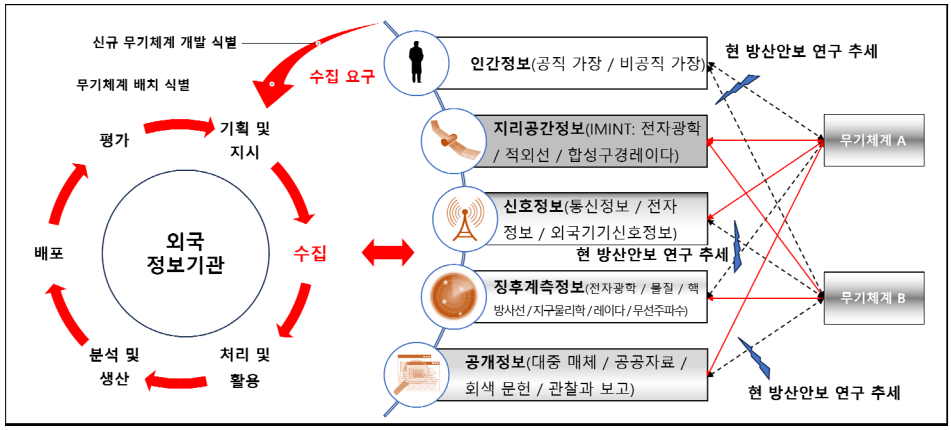


그림 6. 정보수집 관점에서의 현 방산안보 연구 추세와 한계 분석

3.2. 통합적 방첩 연구의 한계

국가정보학의 기존 연구와 학자들의 저서, 법령 등의 방첩 분야를 고찰해 보면 기존 방산안보 연구의 한계를 또 다른 관점에서 확인할 수 있다. 방첩의 개념과 관련하여 첫 번째로, Shulsky 등(2002)은 방첩의 영역을 '정보의 분류', '보안', '대간첩 활동', '총체적 방첩활동(이하 MDCI)' 등의 형태로 구분하여 설명하였으며, "MDCI는 적국의 정보수집 능력의 효율성을 평가하고, 자국의 정보와 통신 활동 중 취약한 부분을 찾아 효과적인 보호 대책을 강구하는 형태"라고 정의한 바 있다.[30]

두 번째로, 윤정석(2014)은 방첩 활동이 세 가지로 구분된다고 하였으며, '정보수집', '방어적 조치', '공격적 조치'로 구분하여 성명하였고, 우호국 역시 적대국과 유사한 수준의 방첩활동인 경계 및 감시 또는 저지의 필요성을 언급하였다.[31]

Aucff 등(2021)은 방첩을 '방어적'·'공격적' 방첩으로 구분하였고, 방어적 방첩은 위협의 탐지·억지 등 능동적 조처가 가능하며, 공격적 방첩은 기만 · 무력화로 구분하여 설명하였다. 또한, 공격적 방첩은 방어적 방첩과 같이 진행해야 한다고 주장하였으며, 방첩 위협평가와 관련하여 "위협 = 능력(지식+자원) + 의도(욕망+기대)"로 평가할 수 있다고 제시하였다.[32]

Zegart(2022) 역시 '방어적·공격적 방첩'으로 구분하여 제시하였으며, 방어적 방첩에서 특수정보시설(SCIF: Sensitive Compartmented Information Facilities)을 포함한 인원·시설 보안 등을 예시로 설명하였고, 공격적 방첩에서는 외국의 정보기관에 스파이를 침투시키거나 이중간첩을 활용하는 등 다양한 형태와 사례를 제시하였다.[33]

Lowenthal(2022)은 방첩을 자국을 목표로 할 수 있는 상대방의 수집 능력에 대한 첩보를 수집하는 '수집', 적대적 정보기관이 자국 기관에 침투 하려는 시도를 방해하는 '방어', 자국 체계 안으로 침투 시도를 파악한 후 상대 요원을 이중스파이로 전환하거나 본국에 보고하도록 허위 첩보를 제공하는 '공격'으로 구분하였다.[34]

더하여 국가정보원법 제4조(직무) 1항과, 방첩업무규정의 제3조(방첩 업무의 범위) 에서도 방첩의 '수집'에 관한 내용을 찾아볼 수 있다.[35][36]

상기한 문헌과 법령들을 종합 해보면, 방첩이란 외국 등의 정보기관이 능력과 의도를 가지고 수행하는 정보수집 활동에 대해 대응하는 것으로, 크게 '수집', '방어적 방첩', '공격적 방첩'으로 나뉘는 것을 확인할 수 있다. 상세 활동으로는 '수집'을 통해 외국정보기관의 수집 능력을 평가하고, 자국 정보의 취약점을 확인하여 효과적인 보호 대책을 강구 하며, '방어적 방첩'을 통해 정보 유출

을 최소화하고, '공격적 방첩'을 통해 외국정보기관 등의 수집을 기만하거나 정보의 오염을 유발하는 활동이라고 할 수 있다.

이들의 활동은 독립적으로 수행되는 것이 아니며, 병행하여 수행되어야 하는 일련의 과정이라고 할 수 있으나, 현 방산안보 연구의 추세는 2장에서 살펴본 바와 같이 전반적으로 '방어적 방첩'에 중점을 두고 있으며, 방첩이라는 개념의 과반에 해당할 수 있는 '수집'과 '공격적 방첩'에 대한 연구에 한계가 존재하는 것으로, 이를 분석해보면 박은열(2025)이 주장한 바와 같이 아래 그림 7의 회색 음영과 점선으로 표시된 것과 같은 위협과 취약점이 잔존하고 있다.[37]

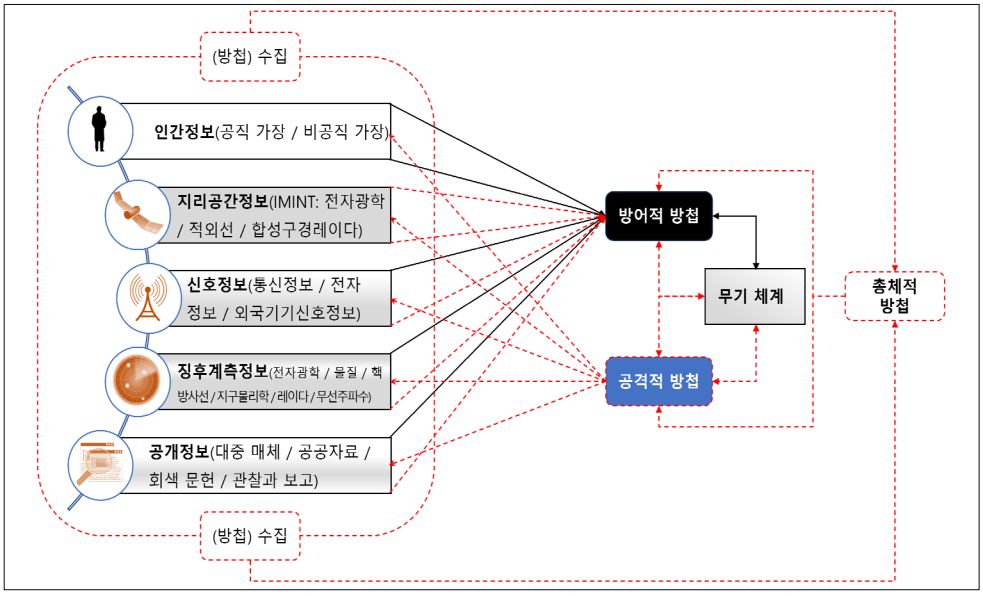


그림 7. 방첩 관점에서의 현 방산안보 연구의 한계 분석

3.3. 연구의 한계가 초래할 위협

위에서 살펴본 바와 같이 방산과 방산이 생산하는 최종 산물인 무기체계에 있어서 정보위협과 취약성의 발현은 기술 유출과 사이버 영역서만 발생하지 않는다. 다양한 국가의 정보기관은 냉전을 겪으며 상대국의 군사정보 수집과 분석을 위한 막대한 노력과 체계를 구축하여 그 능력과 효율성을 높여왔으며, 특히 무기체계 등의 제원 및 특성, 취약성을 집중적으로 분석하는 '기술정보(이하 TECHINT)'라는 개념을 정립해 두었고, 이는 각종 법령과 문헌을 통해 확인할 수 있다.

관련하여 법령부터 살펴보면, 대한민국 국방부 훈령 "적성물자 획득 ·관리 및 기술정보 업무 훈령"의 제2조(정의)에서 "기술정보"라는 단어를 찾아볼 수 있으며, 동 조항에서는 "기술정보라 함은 북한을 포함한 외국에서 개발한 기술과 그 기술을 이용 또는 응용하여 생산된 외국 물자의 작전적 능력 및 기술적 특성에 관한 것으로서 현재 또는 미래의 군사목적에 적용할 정보를 말한다." 라고 정의하였다. 국방부 훈령 "국방전력발전업무 훈령" 제2조(정의)와 관련된 별표 1 용어의 정의에서 역시 "기술정보란 군사목적을 위해 현재 또는 결과적으로 실제 적용될 수 있는 외국 기술 발전 및 외국 군수물자의 질과 운용 능력에 관한 정보를 말하며, 이것은 첩보의 수집 및 처리로 획득되는 최종 완성자료이다."라고 정의하였다.[38][39]

외국의 군사 교리에서 역시 이러한 내용을 찾아볼 수 있었는데, 미 합참(2013)의 합동교범인 JP 2-0 합동 정보와 미 육군(2019)의 ADP 2-0에 해당 내용이 기술되어 있었으며, "TECHINT란 기술적 기습 방지와 외국의 과학 기술적 능력의 평가, 신규 장비에 대한 대책

개발 및 사용 지원 등의 목적을 위해 외국 장비와 재료 관련 데이터를 수집, 처리 분석 및 활용하여 파생된다."라고 정의한다. 영국 역시 U.K MoD가 발간한 JDP 2-00에 따르면 "TECHINT는 외국의 기술 개발과 관련된 정보, 군사적 목적으로 실제 적용되었거나 향후 적용될 가능성이 있는 외국 물자의 성능 및 운용 능력에 관한 정보."라고 설명하고 있다.[40][41][42]

국가정보학의 단행본인 Acuff 등(2021)의 "국가 정보학 개론" 역시 군사정보 분석관들이 "다종의 수집 플랫폼을 사용하여 외국 군대의 능력을 확인하는 작업을 TECHINT라 부른다." 라고 설명하였으며, U.S DNI(2013)의 "National Intelligence an Overview"에 따르면 다양한 군사 정보기관은 외국군의 과학 및 기술적 정보와 능력을 분석하고 생산하는 조직이 있음을 명시하고 있다. 더하여 미 의회 조사국(2021)의 보고서에 따르면 러시아군은 정보총국 제9국이 군사기술에 대한 정보를 담당하고 있는 것으로 기재되어있다.[43][44][45]

위에서 살펴본 바와 같이 법령과 교리, 각종 문헌 등에서 다양한 국가들이 'TECHINT'라는 영역을 구축하고 수행하고 있음을 확인할 수 있었으며, 종합적으로 정의에 보자면 군사정보의 하부 분류에 속하는 TECHINT는 외국의 기술적 기습 방지와 신규 장비에 대한 대책 개발 등을 위해 군사적 목적으로 실제 적용되었거나 향후 적용될 가능성이 있는 외국의 장비·물자 및 재료와 관련된 첩보의 수집과 처리로 획득되는 최종 완성자료라고 정의할 수 있다. 여기서 말하는 군사 목적의 외국 장비·물자란 표준국어대사전에서 정의하는 군수품을 의미하고, 군수품이란 방위사업법 제3조(정의)에서 명시된 무기체계 등을 의미한다.[46][47]

결국, TECHINT는 외국군 무기체계의 약점을 분석하고, 대응책과 대응 전술을 개발하여 자국 군대와 무기체계의 우위를 확보하기 위해 수행되며, TECHINT의 절차와 목적에 대한 개념은 아래의 그림 8과 같다.

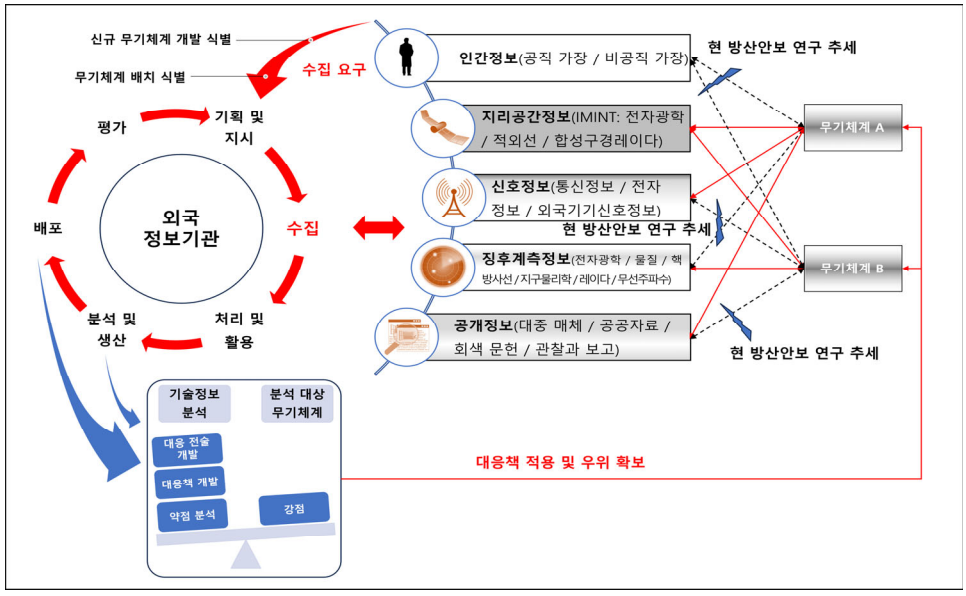


그림 8. TECHINT의 절차와 개념

위의 그림 8과 1·2절에서 살펴본 기존 방산안보의 연구 한계를 토대로 대응 연구의 부재가 초래할 위협을 고찰해 보면 아래와 같다.

먼저, 학술적으로는 국가정보학에서 제시하는 정보출처별 수집 수단이 방산의 최종 생산품인 무

기체계에 미칠 영향에 대한 연구가 수행되지 않았기에, 우리의 무기체계가 외국정보기관 등이 수행할 수 있는 정보수집과 분석이 어떤 식으로 노출되었는지도 모르는 채 대응연구들이 발전하거나 아예 수행되지 않을 가능성이 있다. 또한, 방첩 분야에서도 '방어적 방첩'에 치중한 가운데, 방첩 영역에서 과반이 넘는 '수집'과 '공격적 방첩'의 연구가 미약하여 국가정보학과 방산안보학의 학술적 괴리와 방산안보학의 학술적 대응능력 부족 등이 발생할 가능성이 있다.

두 번째로, 실제 위협과 관련하여 우리의 무기체계가 외국으로부터의 정보수집과 TECHINT의 목표가 될 가능성에서 자유롭지 않은 가운데, 대응연구 등이 발전하지 못하는 현상이 지속될 경우 장기적으로 해외 정보기관 등으로부터 우리 무기체계의 약점이 분석되고 대응 전술과 대응책이 개발될 수 있다. 이는 우리 무기체계의 강점 약화, 약점 보완 등의 추가 예산 및 시간 소모, 무기체계 교체 주기 단축, 무기체계의 무력화 등을 시사하고, 이는 종국적으로 국제시장에서의 K-방산 경쟁력 저하의 단초가 될 수 있다.

그러므로 방산안보 연구에서 국가정보학에서 제시되는 정보수집 관련 연구와 통합적 방첩을 위한 연구의 한계가 지속되는 것은 대한민국을 상대로 수행될 수 있는 TECHINT 가능성에 절반 이상의 연구가 수행되지 않고 방치하는 것으로, 장기적으로 연구와 대응 부족 등의 사유로 국가안보와 방산안보 모든 영역에서 위의 1절에서 확인한 형태와 같은 외국정보기관의 정보수집과 분석을 허락하여 다양한 문제를 초래할 가능성을 내포하고 있다.

4. 연구 한계의 대응 방안

4.1. 정보수집 위협 연구의 수행

위의 3장에서 살펴본 바와 같이, 다양한 정보출처로부터 유효하게 수집된 정보는 무기체계를 대상으로 TECHINT를 가능하게 하며, 이는 곧 위협으로 간주 될 수 있다. 또한, Acuff와 Craft 등이 저서에서 "위협 = 능력 + 의도"라고 설명한 바와 같이 위협을 연구하기 위해서 먼저 그 능력에 대한 연구가 선행되어야 하며, 이는 Shulsky와 Schmitt(2002)가 제시한 MDCI의 시작점이기도 하다.[30][43]

그러므로 방산안보 연구에서는 우리의 무기체계 등에 위협으로 작용할 수 있는 정보출처별 정보수집 능력을 국가정보학과 연계한 가운데 수행하여야 한다. 하지만 이의 연구가 중점적으로 수행되지 않아 그 기반이 미약하므로, 이의 근거를 마련하기 위한 연구부터 시작하여야 하며, 국가정보학의 정보수집 및 분석 분야의 연구자들이나 해당 분야에서 장기간 근속한 인원 등을 통하여 정보출처별 수집 수단의 능력과 장·단점을 집중적으로 연구하여 그 기틀을 만들어야 한다.

또한, 정보출처별 수집 수단이 우리의 어떤 무기체계를 상대로 유효한 정보수집을 수행할 수 있는지에 대한 연구가 여러 관점에서 수행되어야 하며, 이러한 연구를 바탕으로 도출된 결과는 향후 다양한 방향으로 수행될 방산안보 연구에서 위협의 기준으로 삼아 그 초석이 될 필요성이 있다.

4.2. 통합적 방첩 연구의 수행

방산 방첩 역시 방어적 방첩과 공격적 방첩이 모두 연구되어야 할 주제임에도 불구하고, 위의 3장에서 확인한 바와 같이 연구의 불균형이 존재하는 상태이다. 이는 장차 학술적·실질적 취약점 모두를 초래할 수 있는 사안이므로, 향후 방산안보학에서의 방첩 연구는 통합적 방첩 연구 수행이라는 기조 아래 공·방 공히 수행하여 기존의 연구 불균형이라는 상태에서 벗어나야 한다.

이를 위해 방산 방첩 연구가 추구해야 할 방향은 박은열(2025)이 주장한 바와 같이 위의 1절에서 수행한 정보수집 위협을 토대로 MDCI의 개념을 도입하고 적용한 가운데, 아래 그림 9의 검은색 부분과 같이 방어적 방첩을 통해 정보수집을 차단하고, 청색 부분과 같이 공격적 방첩을 통해 정보를 오염시키는 형태의 통합적 방첩 체계를 추구하는 방향이다.[37]

또한, 이러한 연구의 방향을 유지한 가운데, 공격적 방첩과 방어적 방첩 모두의 대책을 마련해야 한다.

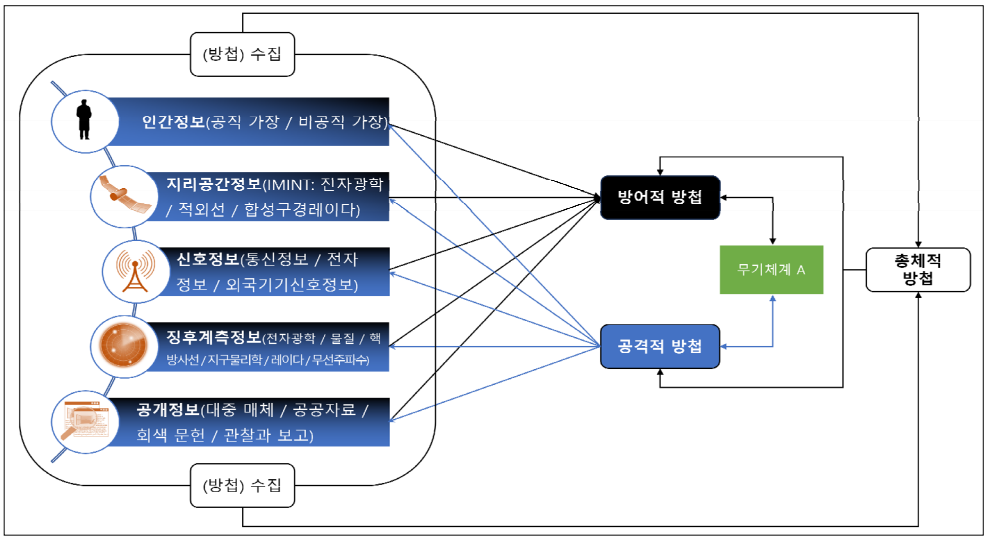


그림 9. 방산안보 연구에서 추구해야 할 방산 방첩 개념

5. 결론

방산안보학은 1장에서 기술한 바와 같이 방산 위협감소에 핵심적인 역할을 수행하는 국가안보의 중요한 학문적 영역이 되어야 한다. 기존의 학자들이 방산보안으로부터 방산안보에 이르는 다양한 연구를 수행하여 왔으나, 위의 2장에서 고찰한 바와 같이 학문의 역사가 짧고 연구자 수가 적어 기존의 전반적인 연구가 정책과 방어적 방첩 연구에 집중되는 현상을 보이고 있었으며, 정보출처별 수집 위협과 대응의 측면에서 다양한 연구 한계가 존재한다.

특히 K-방산이라는 표현이 등장할 만큼 세계 각국으로부터의 다양한 관심을 받고있는 현재의 방산은 정보위협이라는 측면에서의 짙은 음영을 만들어 내기 시작했으며, 이는 우리의 무기체계가 3장에서 제시된 다양한 정보출처별 수집과 TECHINT 위협에 노출될 가능성이 비례하여 증가함을 시사한다. 따라서 향후 방산안보 연구는 4장에서 논한 바와 같이 국가정보학과의 학제 간 연구를 활성화한 가운데 전 출처에 걸친 정보수집 위협의 연구를 수행해야 하며, 이러한 연구를 토대로 총체적 방첩(MDCI) 개념을 적용한 통합적 방첩의 연구 역시 수행하여야 한다.

연구의 한계점으로는, 해외의 정보분석 사례를 중심으로 위협을 제시한 본 논문의 특성상 방산의 주된 생산품인 무기체계를 중심으로 기술하여 방위산업 물자 및 전략물자 등에 대한 연구를 수행하지 못하였다는 것이다. 또한, 연구 한계의 고찰과 관련하여 정보출처별 세부 분류는 총 18종에 달하나, 지면상 이에 관하여 세부적인 고찰을 수행하지 못하였다.

향후 연구 제언으로 18종에 달하는 세부 수집 수단이 우리의 무기체계에 어떠한 위협을 미칠 수 있는지 각각 연구되어야 하며, 이러한 위협으로부터 어떠한 통합적 방첩이 수행될 수 있는지 연구

할 필요성이 있다. 저자는 본 논문에서 제시된 연구의 결과물이 방산안보학의 개념 정립과 발전에 기여하기를 희망한다.

참고문헌

[1] 방산안보연구소. https://idis.mju.ac.kr/ridis/8232/subview.do (검색일 2024. 10. 2).

[2] 류연승. 방산보안 2.0. 한국정보보호학회지, 제28권 제6호, pp. 78-86. 2018.

[3] 허아라, 류연승. 국방과학기술 정보의 분류체계 고찰. 한국정보보호학회지, 제28권 제6호, pp. 25-32. 2018.

[4] 박흥순. 방위산업 사이버 보안을 위한 방산 정보 공유 · 분석센터(ISAC) 설립 방안. 한국정보보호학회지, 제28권 제6호, pp. 56-62. 2018.

[5] 박흥순 등. 체계적인 방위산업기술보호를 위한 보호체계 우선순위 분석 연구. 융합보안논문지, 제19권 제4호. 2019.

[6] 송경호 등. 무기체계 안티탬퍼링을 위한 기술 식별 및 위협평가 방안. 한국방위산업학회지, 제28권 제2호, pp. 41-50. 2021.

[7] 송경호 등. 체계공학 기반 안티탬퍼링 프로세스. 한국방위산업학회지, 제28권 제3호, pp. 77-91. 2021.

[8] 오광환 등. 방산인력 기술유출 방지를 위한 실태분석 및 개선방안. 한국산업보안연구, 제11권 제1호, pp. 435-458. 2021.

[9] 방산안보연구소. https://idis.mju.ac.kr/ridis/8232/subview.do (검색일 2024. 10. 2).

[10] 류연승 등. 방위산업 안보환경 변화에 따른 방산안보정책 검토. 한국과 세계, 제4권 제2호, pp. 207-232. 2022.

[11] 김영기. 방위산업과 방산안보 발전방안. 동중앙아시아연구, 제33권 제1호, pp. 23-39. 2022.

[12] 주영진 등. 무기체계 기술보호를 위한 안티탬퍼링 시험평가 방안. 한국방위산업학회지, 제30권 제3호, pp. 47-58. 2023.

[13] 허아라. 직무분석을 통한 방위산업 기술보호 인력 교육 모델. 명지대학교 대학원, 박사학위논문. 2023.

[14] 김영기. 방산안보와 국가정보연구. 진영사. 2024.

[15] 김진경, 류연승. 무역안보 (전략물자) 법제 동향과 방산안보 시사점. 한국방위산업학회지, 제31권 제2호, pp. 73-86. 2024.

[16] 유인수, 류연승. 방산안보의 개념에 관한 고찰. 국방과 보안, 제5권 제2호, pp. 271-284. 2023.

[17] 배정석. 방위산업 보호를 위한 방첩의 역할과 범위: 방위산업체와 정보기관의 협력체계를 중심으로. 명지대학교 대학원, 박사학위논문. 2024.

[18] 류연승 등. 방산안보학 개론. 박영사. 2024.

[19] Levy, Gafni. Towards the Quantification of Cyber Security Footprint for SMBs using the CMMC 2.0. Online Journal of Applied Knowledge Management (OJAKM), Vol. 10, No. 1, pp. 43-61. 2022.

[20] Farkas. The Challenges for the European Defense Industry. Proceedings of the 2023 IEEE 21st Jubilee International Symposium on Intelligent Systems and Informatics, pp. 457-462. 2023.

[21] Fonfria. La industria de defensa europea frente a la autonomia estratigica. ICE, Revista de Economia, (930), pp. 145-155. 2023.

[22] Brown. Industrial Security Policy Application in High Tech Defense Industry. Global Security & Intelligence Studies, Vol. 9, No. 1, pp. 111-136. 2024.

[23] Baydarov, Faikov. Обоснование комплекса мер по формированию институциональной среды и системы управления диверсификацией оборонно-промыш

ленного комплекса. Управление, Vol. 12, No. 2, pp. 5-16. 2024.

[24] CIA FOIA. LAUNCH ASSIST DEVICE TEST PROGRAMS, PAVLOGRAD SOLID MOTOR TEST FACILITY, USSR. https://www.cia.gov/readingroom/docs/CIA-RDP80T00250A000100100001-3.pdf (검색일 2024. 7. 22).

[25] CIA FOIA. BASIC IMAGERY INTERPRETATION REPORT. https://www.cia.gov/readingroom/docs/CIA-RDP79T00909A001100040002-9.pdf (검색일 2024. 7. 22).

[26] CIA FOIA. TECHNICAL CHARACTERISTICS OF USSR RADARS. https://www.cia.gov/readingroom/docs/CIA-RDP62B00844R000200240015-1.pdf (검색일 2024. 7. 22).

[27] CIA FOIA. Foreign Submarine-Launched Ballistic Missiles. https://www.cia.gov/readingroom/docs/DOC_0000962878.pdf (검색일 2024. 7. 22).

[28] CIA FOIA. China Builds a Better Tank...the Israeli Way https://www.cia.gov/readingroom/docs/CIA-RDP86T01017R000605590001-5.pdf (검색일 2024. 7. 22).

[29] 박은열. 방산안보를 위한 무기체계별 정보수집 대응 방안 연구. 명지대학교 대학원, 박사학위논문. 2025.

[30] Shulsky et al(김계동 역). 국가정보의 이해: 소리없는 전쟁. 명인문화사. 2007.

[31] 윤정석. 국가정보학의 이해: 정보와 국가안보. 오름. 2014.

[32] Acuff et al(김계동 역). 국가정보학 개론: 제도, 활동, 분석. 명인문화사. 2022.

[33] Zegart(유인수 역). 스파이, 거짓말, 그리고 알고리즘: 미국 정보기구의 역사와 미래. 한울엠플러스. 2024.

[34] Lowenthal. Intelligence: From Secrets to Policy. Ninth edition. CQ Press. 2022.

[35] 법제처 국가법령정보센터. 국가정보원법. https://www.law.go.kr/법령/국가정보원법/(20240101,17646,20201215)/제4조 (검색일 2024. 10. 4).

[36] 법제처 국가법령정보센터. 방첩업무 규정. https://www.law.go.kr/법령/방첩업무규정/(20240423,34435,20240423)/제3조 (검색일 2024. 10. 4).

[37] 박은열. 방산안보를 위한 무기체계별 정보수집 대응 방안 연구. 명지대학교 대학원, 박사학위논문. 2025.

[38] 법제처 국가법령정보센터. 적성물자 획득·관리 및 기술정보업무 훈령. https://www.law.go.kr/행정규칙/적성물자획득·관리및기술정보업무훈령/(2342,20191120)/제2조 (검색일 2024. 7. 22).

[39] 법제처 국가법령정보센터. 국방전력발전업무훈령, https://www.law.go.kr/행정규칙/국방전력발전업무훈령/(2924,20240502)/제2조 (검색일 2024. 7. 22).

[40] U.S JCS. Joint Publication 2-0 Joint Intelligence. U.S JCS. 2013.

[41] U.S Army. ADP 2-0 INTELLIGENCE. U.S Army. 2019.

[42] U.K MoD. Joint Doctrine Publication 2-00 Intelligence, Counter-intelligence and Security Support to Joint Operations(Fourth Edition). U.K MoD. 2023.

[43] Acuff et al(김계동 역). 국가정보학 개론: 제도, 활동, 분석. 명인문화사. 2022.

[44] U.S DNI(이길규, 이함구, 장재복 역). 미국 국가정보 이해. 박영사. 2013.

[45] U.S Congress Research Service. Russian Military Intelligence: Background and Issues for Congress. 2020.

[46] 국립국어원 표준국어대사전. 군수품. https://stdict.korean.go.kr/search/searchView.do?pageSize=10&searchKeyword=%EA%B5%B0%EC%88%98%ED%92%88 (검색일 2024. 7. 22).

[47] 법제처 국가법령정보센터. 방위사업법. https://www.law.go.kr/법령/방위사업법/(20240717,20023,20240116)/제3조 (검색일 2024. 7. 22).