방산안보연구
Journal of Defense Industrial Security

방산안보연구, 1권 2호, 2025년 9월, 1–19면.
Journal of Defense Industrial Security, Volume 1, Issue 2, September 2025, Pages 1–19.
https://doi.org/10.64227/jdis.2025.1.2.1

Print ISSN 3091-5546
Online ISSN 3091-5554

원저

방위산업 사이버 방첩의 제도적 과제

이수인

국방부 육군준위

교신저자: 이수인 (silee868@gmail.com)

요약

방위산업은 국방력 증진을 위한 연구 · 개발(R&D), 생산 · 정비, 공급하는 산업을 의미한다. 이는 단순한 무기 제조업을 넘어 국가안보와 주권 수호에 있어 핵심 전략 자산으로 자리매김하고 있다. 본 연구는 2019~2023년 공개된 국내외 방위산업 관련 사이버 침투 사례 30건을 TTPs(전술 · 기법 · 절차) 분석 틀로 정량 · 정성 분석하고, 현행 보안법 · 제도 문헌을 검토하였다. 분석 결과, 공급망 최말단의 탐지 역량 부재와 '기술 보호' 중심 법제가 능동적 기만 · 역추적 활동과 같은 적극적 방어 개념을 수용하고 지원하기 어려운 구조적 한계가 확인되었다. 이에 본 연구는 해외 선진국의 방산 안보 모델을 벤치마킹하여, 사이버 방첩 독립법 제정, 방산 사이버 방첩센터 설립, 허니팟 · 위협 인텔리전스 플랫폼 등 능동형 방어 기술 도입, 다자간 정보 공유 메커니즘 구축을 제도적 과제로 제안한다.

핵심어

방위산업, 사이버 방첩, TTPs 분석, 공급망 보안, 제도적 과제

차례

Open Access

접수일: 2025년 7월 18일
수정일: 2025년 8월 13일
게재승인일: 2025년 8월 27일
출판일: 2025년 9월 30일

Original Article

Institutional Challenges for Cyber Counterintelligence in the Defense Industry

Sooin Lee

Warrant Officer, Ministry of National Defense, Republic of Korea

Corresponding Author: Sooin Lee (silee868@gmail.com)

ABSTRACT

The defense industry refers to the sector engaged in the research and development (R&D), production, maintenance, and supply of goods and services essential for enhancing national defense capabilities. Beyond the mere manufacturing of weapons, it has emerged as a core strategic asset in safeguarding national security and sovereignty. This study analyzes 30 publicly disclosed domestic and international cyber intrusion cases targeting the defense industry between 2019 and 2023, employing the Tactics, Techniques, and Procedures (TTPs) framework for both quantitative and qualitative assessment, and reviews existing laws and regulations related to security. The analysis identifies structural limitations, notably the absence of detection capabilities at the terminal points of the supply chain and a legal framework predominantly focused on “technology protection,” which is insufficient to accommodate and support proactive defense concepts such as active deception and counter-infiltration measures. Accordingly, this study benchmarks advanced defense security models from leading countries and proposes institutional measures including the enactment of an independent cyber counterintelligence law, the establishment of a dedicated defense cyber counterintelligence center, the adoption of active defense technologies such as honeypots and threat intelligence platforms, and the development of multilateral information-sharing mechanisms.

KEYWORDS

Defense Industry, Cyber Counterintelligence, TTPs Analysis, Supply Chain Security, Institutional Challenges

1. 서론

한국 방위산업은 첨단 기술력과 적극적인 시장 개척을 바탕으로 급성장하며 세계 방산 강국으로의 도약을 추진하고 있다. 그러나 방위산업의 위상 강화에 비례하여 사이버 공간에서의 첨단기술 유출 위협도 함께 증대되고 있다. 특히 북한을 비롯한 외국 정보기관의 해킹과 사이버 첩보활동이 방위산업 기밀을 노린 사례가 지속적으로 보고되고 있으며, 이러한 사이버 위협은 국가안보와 경제적 이익에 중대한 위험을 초래한다.

실제로 2024년 초 진행된 경찰청 · 방위사업청 · 국가정보원 등의 합동조사에서는 북한의 해커 조직 라자루스, 안다리엘, 김수키 등이 국내 방산업체 83곳을 대상으로 사이버 공격을 감행하여 이 중 10여 곳에서 방위산업 기술자료를 탈취한 사실이 확인되었다.[1] 더 심각한 것은 일부 피해 업체가 당국의 통보 전까지 해킹 피해 사실조차 인지하지 못할 정도로 공격이 은밀하고 정교하게 이루어졌다는 점이다. 이는 현재의 대응체계로는 고도화되는 사이버 첩보전에 효과적으로 대응하기 어려울 수 있음을 시사한다.

방위산업은 국제적 위상이 증대됨에 따라 북한 등 적대 세력의 핵심 표적이 되고 있으며, 이는 단순한 사이버 공격을 넘어 대한민국의 국가안보와 방산기술 보호에 중대한 위협이 되고 있다. 방산기술 유출은 연구개발 투자 손실, 기술적 우위 상실, 국가 기술 혁신 저해를 야기하며, 궁극적으로 국가의 생존과 직결되는 문제로 발전할 수 있다. 또한, 이러한 기술 유출은 해외 고객사의 신뢰도 저하를 초래하여 방위산업의 글로벌 경쟁력에 부정적인 영향을 미치고, 한국의 방산 수출 성장세에 제동을 걸 수 있다. 사이버 공격으로 인한 경제적 손실은 2024년 전 세계적으로 9.5조 달러에 달할 것으로 추정되며, 실제로 사이버보안에 취약 기업은 주식 시장에서 저조한 성과를 보여 기업 가치 하락으로 이어지는 경향이 있다. 한편, 이러한 위협 환경속에서 2023년 기준 글로벌 군사(국방) 사이버보안 시장은 약 164억 5천만 달러로 평가되었으며, 2032년에는 연평균 성장률(CAGR)[1] 16.1%를 기록하며 약 633억 8천만 달러까지 성장할 것으로 전망된다. 현재 이 시장은 General Dynamics, Raytheon Technologies, Lockheed Martin, SAIC, CACI International 등 대부분 미국계 글로벌 방산 · IT 기업들이 주도하고 있다. 미국의 국방 사이버보안 또는 사이버 방첩 역량이 발전하게 된 바탕에는 미군의 사이버보안 역량 모델 인증(CMMC: Cybersecurity Maturity Model Certification) 제도가 있다. CMMC는 미국 국방부(DoD)가 국방 관련 계약업체 및 그 하위 공급망 전체에 요구하는 사이버보안 역량 평가 · 인증 제도로, 방위산업 공급망에 참여하는 모든 기업이 일정 수준 이상의 사이버보안 통제를 갖추고 있음을 인증받아야 하는 제도이다.[2]

우리 정부도 위협의 심각성을 인식하고 대응책을 마련해 왔다. 2016년에는 방위산업 기술 보호법을 제정 · 시행하여 방위산업기술을 체계적으로 보호하기 위한 법적 기반을 구축하였다. 동 법의 시행으로 방산기술 보유 기관들은 기술 보호 체계 구축과 임직원 대상 기술 유출 방지 교육을 의무화하게 되었으며, 이는 방산 보안 수준을 한 단계 격상시키는 전환점이 되었다. 류연승(2018)은 2016년 법 제정 이후의 시대를 '방산보안 2.0' 시대라고 규정하면서, 이전의 1.0 시대와 대비되는 체계적 보안 환경의 도래를 강조하였다.[3] 한편 방사청 등 관계 부처는 2021년 말 「2022~2026 방위산업기술보호 종합계획」을 수립하여, 국가정보원 · 검찰 등 유관기관 공조 체계를 강화하고 방산기술보호 역량을 높이는 종합대책을 발표하였다. 이 계획에는 방위산업 사이버 위협에 대응하기 위한 범정부 협의체 마련, 방위산업기술보호센터 설립 등의 내용이 담겨 있어, 기존의 개별 기관 대응을 넘어 제도적 · 조직적 대응체계를 구축하려는 노력으로 평가된다.[4]

1) 연평균 성장률(CAGR, Compound Annual Growth Rate) 일정기간 동안 투자나 사업의 가치가 매년 일정한 비율로 성장했다고 가정할 때의 연평균 성장률을 의미

그럼에도 불구하고 여전히 방위산업을 겨냥한 사이버 첩보활동에 대한 대응은 미흡하다는 지적이 있다. 국가정보원이 주최한 2024년 방산안보 국제컨퍼런스에서도 “세계 4대 방산 수출국으로 성장하기 위해서는 핵심 기술 보호와 정보유출 방지에 더욱 많은 관심과 노력이 필요하다”는 업계의 목소리가 나왔다. 이는 단순한 방어 차원의 보안 대책만으로는 부족하며, 보다 능동적이고 전략적인 사이버 방첩(cyber counterintelligence, CCI) 접근이 필요함을 시사 한다.[5] 사이버 방첩 전략이란 전통적 방첩의 개념을 사이버 공간에 적용하여, 적대적 사이버 위협에 대한 탐지, 기만, 교란 및 대응 등의 적극적 조치를 포함하는 포괄적 대응 전략을 의미한다. 이러한 전략은 사이버 공격의 사전 차단과 침투자 색출, 나아가 공격 주체에 대한 역대응까지 포괄함으로써, 방위산업 기밀 유출을 근본적으로 억제하는 것을 목표로 한다.

본 연구는 방위산업의 사이버 위협에 대응하기 위한 사이버 방첩 전략의 필요성을 제기하고, 이를 뒷받침할 제도적 과제를 심층 분석하고 그 발전 방안을 제시하는 것을 목적으로 한다. 이를 위해 제2장에서 방첩과 사이버 방첩의 개념 및 이론적 배경을 살펴보고, 제3장에서 방위산업을 둘러싼 사이버 위협의 현황과 국내외 대응 실태 및 시사점을 분석하며 제4장에서는 이를 바탕으로 사이버 방첩 전략 강화를 위한 법 · 제도적 개선 과제를 제언한다. 마지막으로 제5장 결론에서는 연구 내용을 종합 정리하고 정책적 함의를 제시하고자 한다.

2. 사이버 방첩의 개념과 이론적 배경

사이버 방첩의 개념은 전통적인 방첩에서 대부분 차용되었다. 전통적인 방첩(counterintelligence, CI)은 적대 세력의 첩보활동을 탐지하고 차단함으로써 자국의 기밀과 이익을 보호하는 정보 활동의 한 분야이다. 전통적으로 방첩은 방어적 조치와 공격적 조치를 모두 포괄하는데, 전자는 적의 정보수집을 억제하고 탐지하는 것을, 후자는 적의 첩보 활동을 기만하고 교란하는 적극적 대응을 의미한다. Prunckun(2019)의 이론적 틀에 따르면 방첩은 수동적 방첩(defensive counterintelligence)과 공격적 방첩(offensive counterintelligence)으로 구분된다. 전자는 정보 및 자산에 대한 접근을 차단하고 적의 침투 시도를 발각하는 “거부(Denial)” 전략인 반면, 후자는 적을 오도하고 자원을 소모시키며 첩보 시도를 무력화하는 “기만(Deception)” 전략에 해당한다. 요컨대, 방어적 방첩이 침투 차단과 억지에 초점을 둔다면, 공격적 방첩은 적의 첩보망 교란 및 와해를 목표로 하는 것이다.[6]

사이버 방첩은 이러한 방첩 개념을 사이버 공간에 적용한 것으로, 사이버상에서 이루어지는 스파이 활동, 해킹, 내부자 배신 등에 대응하는 모든 조치를 포괄한다. 이는 전통적인 사이버보안(cyber security) 조치와는 그 접근 방식과 지향점에서 차이가 있다. 사이버보안이 주로 방화벽 설치나 취약점 패치, 접근통제 등 시스템과 네트워크를 방어하는 데 주력하는 반면, 사이버 방첩은 한 걸음 더 나아가 적대적 행위자의 식별과 무력화에 초점을 맞춘다. 예를 들어 사이버 방첩 전략에는 침입 징후를 면밀히 탐지하여 해커의 정체와 의도를 파악하고, 필요시 허위 정보를 심는 등 기만 전술을 구사하거나 법 집행기관 및 정보기관과 공조하여 적의 공격 인프라를 역추적 · 차단하는 등의 적극적 대응이 포함된다.[7] 이러한 측면에서 사이버 방첩은 사이버 공간의 특성을 통해 적의 사이버 공격을 수동적으로 막는데 그치지 않고 능동적으로 역이용하거나 선제 대응하는 “공격이 최선의 방어”가 될 수 있는 보다 높은 수준의 안보를 도모한다.

사이버 방첩 개념을 뒷받침하는 이론적 논의는 아직 진화 단계에 있으나, 국내외 학계와 실무에서 그 중요성에 대한 인식이 높아지고 있다. 특히, 미국의 국가방첩전략(National Counterintelligence Strategy)에서는 “외국의 사이버 첩보활동에 대한 통합적 · 공세적 대응”을 핵심 과제로 천명하고 있으며, 미 국방부 산하 국방방첩보안국(DCSA) 또한 “국방산업기반을

노리는 복잡한 위협에 대응하기 위해 기존의 방식에서 과감한 전환이 필요"하다고 강조한다.[8] 이는 사이버 공간에서의 방첩이 더 이상 부수적인 고려 사항이 아니라, 국가안보 전략의 중심축으로 부상하고 있음을 보여준다. 한편, 국내 연구에서는 방산 분야 방첩 활동이 지금까지 주로 사이버보안이나 기술 보호 등 방어적 방첩 영역에 집중 되어왔으며, 첩보 수집 · 공격 등 적극적 방첩은 상대적으로 미흡하다는 지적이 제기된 바 있다. 박은열(2025)은 방산 안보 연구의 한계를 논하면서, 방산 방첩 연구가 수동적 대응 위주에 머무르지 말고 능동적 정보수집과 공격적 방첩 전략까지 아우를 필요성을 역설하였다. 이러한 논의는 사이버 방첩 전략의 중요성을 학문적으로 뒷받침해 주며, 앞으로 이 분야의 이론 발전과 모범 사례 분석이 활발히 이루어져야 할 것을 시사한다.[9]

사이버 방첩 활동의 핵심은 위협 탐지, 분석, 예측, 그리고 공격자 귀속(attribution) 역량을 혁신적으로 강화하는 것이다. 최근 첨단정보통신 기술의 최대 화두로 떠오른 인공지능(AI)은 기술은 이러한 목표 달성에 결정적인 역할을 수행 할 수 있는 기술로 평가된다. AI는 대량의 데이터(로그, 네트워크 트래픽, 행동 데이터)를 인간 분석가보다 훨씬 빠르고 정확하게 처리하며, 방대한 정보 속에서 미묘한 패턴, 추세, 이상 징후를 식별하는 데 탁월한 능력을 발휘한다. 이러한 능력은 사이버 방첩의 본질적 목표인 적의 첩보활동 탐지 및 차단을 고도화하는 데 필수적이다.[10]

구체적으로, AI는 실시간으로 시스템 로그나 네트워크 트래픽을 분석하여 비정상적인 활동을 신속하게 감지하고, 과거 데이터와 공격 패턴을 학습하여 미래 위협을 예측할 수 있다. 이는 사이버 공격이 발생하기 전에 선제적으로 대응할 수 있는 기반을 마련한다. 또한, AI는 복잡한 사이버 공격의 출처를 추적하고 책임 주체를 식별하는 '귀속' 능력 강화에 기여할 수 있다. 공격자 귀속은 외교적, 법적 대응의 기반이 되므로, AI를 통한 귀속 역량 강화는 국가의 사이버안보 대응력을 한 층 높이는데 기여한다.[11]

더 나아가, AI는 내부자 위협 탐지에도 중요한 역할을 수행한다. AI 기반 예측 모델링은 직원의 행동 데이터, 통신 패턴, 심리적 요인까지 분석하여 잠재적 내부자 위협을 예측할 수 있으며, 민감 정보에 대한 비정상적인 접근이나 비업무 시간 활동 등 이상 행동을 감지하여 내부자 위협을 신호할 수 있다. 이는 전통적인 방첩 활동의 중요한 영역인 내부자 위협 관리를 AI 기반으로 더욱 정교하게 수행할 수 있음을 의미한다. 또한, AI는 공개 출처 및 기밀 채널에서 정보수집을 자동화하여 방첩 활동의 효율성과 도달 범위를 향상 시킬 수 있다. 이러한 AI의 다각적인 활용 가능성은 사이버 방첩의 '눈과 귀' 역할을 고도화하여, 수동적 방어에 머물던 기존 방첩 체계를 능동적이고 예측 가능한 시스템으로 전환하는 데 필수적인 기술적 기반을 제공한다.

3. 방위산업 사이버 위협의 현황 및 국내외 대응 실태 분석

3.1. 국내 사이버 위협 양상

21세기 들어 물리적 전장을 넘어선 '제5의 전장'[2]인 사이버 공간이 첩보전의 최전선으로 부상하고 있으며, 이러한 변화 속에서 전 세계적으로 위상을 높이고 있는 한국 방위산업 역시 북한 등 적대 세력에게 매력적인 핵심 표적이 되고 있다. 특히 북한의 사이버 공격 조직들은 지난 20여 년간 일관되게 한국의 군사기밀과 방산기술을 탈취하는 데 주력해 왔다. 북한은 2000년대 초반부터 현재까지 지속적으로 한국 방산업체를 대상으로 공격을 벌여왔으며, 방위산업기술의 보호는 단순한 산업 보안을 넘어 국가의 핵심 기술과 군사 주권을 지키는 것은 민 · 관 · 군의 유기적인 협력이 필수적으로 요구되는 고도의 '국가 방첩(Counterintelligence)' 영역에 해당한다. 이러한 위협의

2) 미국은 기존의 육 · 해 · 공 · 우주에 이어 사이버공간을 제5의 전장으로 규정하였으며, 국가안보와 군사전략에서 매우 중요한 영역으로 부상

심각성은 단순한 예측을 넘어 현실화 되고 있으며, 실제로 2024~2025년 사이 북한, 중국, 러시아 등 국가 지원 해커 그룹의 공격으로 인해 전 세계 방위, 금융 산업 등이 입은 공급망 피해 규모는 약 30억 달러(약 4조 원)에 달하는 것으로 분석되었다.

특히 국내 사례를 살펴보면, 최근의 위협은 과거의 방식을 뛰어넘어 더욱 조직적이고 지능적으로 진화하고 있으며, 2019년부터 2020년에는 대북 정책 등 국내 정보를 탐색할 목적이었으나 2021년부터 국내 방산업체 등 민간 분야까지 공격을 확대하였으며, 2022년에는 북한 정찰총국이 한국의 대형 조선사를 해킹하여 첨단 함정 설계도면 등을 탈취한 사건이 발생하였다. 이는 방산 핵심 협력업체까지 사이버 공격의 예외가 아님을 보여주는 사례이다. 또한 2023년에는 북한 해커들이 합동으로 한국 방산업계를 겨냥한 전방위 사이버 공격을 감행하여, 다수의 기업에서 대량의 기술자료가 유출되는 피해가 발생했다. 2024년 초 경찰청, 방위사업청, 국가정보원의 합동조사 결과, 각자의 영역에서 활동하던 북한의 대표적 해킹조직인 라자루스, 안다리엘, 김수키가 하나의 목표, 즉 '대한민국 방위산업'을 겨냥해 최소 1년 6개월 이상 조직적인 협공으로 국내 방산업체를 공격해 온 사실이 확인되었다. 과거에는 김수키가 정부기관, 라자루스가 금융기관, 안다리엘이 국방기관을 주로 노리는 것으로 알려졌으나, 최근에는 이 세 조직이 각 조직의 전문 기술을 결합하여 방어체계를 무력화하려는 전례 없는 연합 작전으로, 위협의 수준을 질적으로 변화시키는 변곡점이 되었으며, 공격 주체도 북한뿐만 아니라 기타 국가 및 산업 스파이까지 광범위하다. 2024년 유형별 침해사고 신고 통계에 따르면 이러한 위협의 고도화는 서버 해킹 공격이 전년 대비 약 2배 급증한 것으로 나타났으며, 2020년부터 2023년 8월까지 방위산업기술 유출 · 침해사고 신고센터에 접수된 건수는 82건에 달해, 피해가 이미 광범위하게 발생하고 있음을 보여준다.[12,13]

표 1. 북한 해커조직별 국내 침투 사례 및 TTPs (2019-2024)[3)]

연도	공격 조직	침투 기법	주요 탈취 정보	공격의 특징 및 시사점
2019	리자루스, 김수키, APT45 등	피싱 · 악성코드 · 워터링 홀 시스템 취약점 공격	국회 외통위 · 정보위 · 국방위 의원 정보	대북 정책 및 전략 탐색 목적
2020	탈륨(김수키), 리자루스 등	피싱 · 이메일 · 랜섬웨어	외교 · 안보 라인 정보	남북관계 악화 시점 정보수집 강화
2021	라자루스 · 안다리엘 · 김수키	스피어 피싱 · 내부망 침투 · 악성코드 · 랜섬웨어	한국원자력연구원, KAI, 대우조선해양 등 첨단기술	첨단기술·의료·방산 등 민간 분야까지 공격 확대
2022	북한 정찰총국	해킹(선박 설계도 해킹)	첨단 함정 설계도면 탈취	방산 핵심 협력업체까지 사이버 공격의 표적이 됨을 보여줌.
2023	라자루스 · 안다리엘 · 김수키	APT(지능형 지속 위협) · 피싱 이메일 · 악성코드 · 공급망 공격	연구개발 기술자료 대량 유출	– 과거 역할 분담 없이 공동의 첩보 목표 하에 협공. – 협력업체 계정 탈취를 통한 우회 침투. – 기업 이메일 서버 취약점 악용 (로그인 없이 대용량 파일 접근). – 장기간 은밀히 활동하며 핵심 자료 탈취(일부 기업은 당국 통보 전까지 해킹 피해 인지 못함).

3) 국가안보전략연구원. 김정은시대 북한의 사이버위협과 주요 대응. 2021, 한국인터넷진흥원. 2024 하반기 사이버 위협 동향 보고서. 2025. 참조하여 재작성

2024	라자루스 · 안다리엘 · 김수키	외부 인터넷망 서버 해킹 후 악성코드 심기, 내부망 진입, 개발팀 컴퓨터 자료 국외 클라우드 유출, 협력업체 직원 이메일 계정 탈취 (동일 ID/PW 허점 악용), 협력업체 그룹웨어 이메일 서버 취약점 악용	방위산업 기술 자료	- 최소 1년 6개월 전부터 공격 집중. - 세 조직의 공동 목표 하 총력전 확인. - 공격의 은밀성과 지속성 (수사 시작 시점까지 악성코드 활동).

방위산업에 대한 사이버 위협의 가장 큰 특징은 국가 차원의 조직적 공격이라는 점이다. 우리나라 방산기술 탈취의 배후에는 북한이 있다. 그밖에 중국, 러시아를 비롯하여 다른 국가 들의 개입 정황도 지속적으로 포착되고 있다. 나아가 사이버 공간에서는 동맹 관계와 무관하게 자국의 이익을 위한 첩보전이 전개될 수 있으므로, 잠재적 위협은 특정 적대국에 국한되지 않는다. 북한의 경우 라자루스, 안다리엘, 김수키 등 전문 해커 조직들을 총동원하여 공동의 첩보 목표 하에 협공을 벌이고 있다. 이러한 합동 사이버 첩보전 양상은 공격의 치밀함과 범위를 한층 확대시키고 있다. 2024년 초 밝혀진 사건에서도 세 조직이 각기 다른 경로를 통해 동시다발적인 침투로 기업 내부망 깊숙이 스파이웨어를 설치하고, 상당 기간 은밀히 활동하면서 핵심 자료를 탈취한 것으로 나타났다.

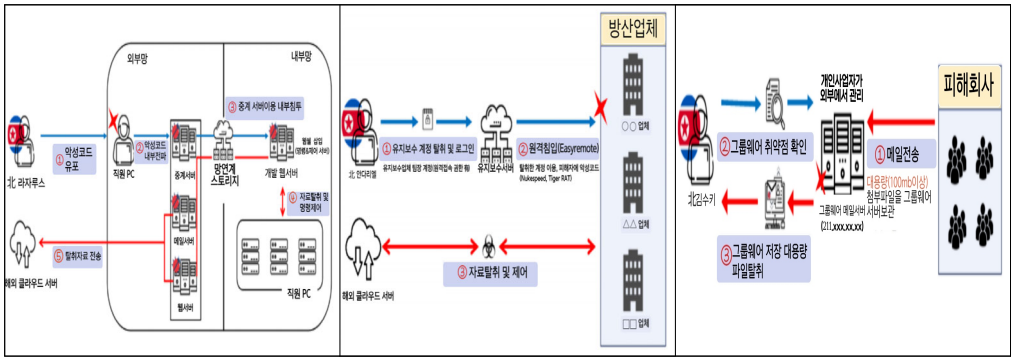

그림 1. 북한 해킹조직별 방산기관 침투 사례[4)]

이러한 공격은 내부망과 외부망 분리 등 기존 보안 대책을 우회하거나, 협력업체의 계정 정보를 탈취해 우회 경로로 목표 기업에 침투하는 등 교묘한 수법을 사용하였다. 또한 기업의 이메일 서버 취약점을 악용해 로그인 없이도 대용량 파일에 접근하는 등의 수법으로 협력업체 자료까지 탈취한 정황도 포착되었다. 요컨대, 현재의 사이버 위협은 단발적이거나 개별 해커 수준을 넘어 국가 차원의 자원과 인력이 동원된 지속적이고 정교한 첩보 공격으로 진화하고 있다.[14]

방위산업의 복합화된 공급망은 핵심 기술 정보 유출의 주요 통로가 된다. 특히 중소 협력업체들은 기술적, 재정적, 인력적 한계로 인해 사이버보안의 가장 취약한 고리가 되고 있으며, 이는 전체 방산 생태계의 핵심 기술 유출 및 국가안보 위협으로 직결된다. 공격자들은 이러한 약점을 체계적으로 파고들어 공급망 전체의 신뢰성을 훼손하고 있다. 2022년 북한 정찰총국이 한국의 대형 조선사를 해킹하여 첨단 함정 설계도면 등을 탈취한 사건은 방산 핵심 협력업체까지 사이버 공격의 예외가 아님을 보여주는 명백한 사례이다.[15]

4) 경찰청 보도자료 2024. 4. 23. (검색일 2025. 6. 25). 참조하여 재작성

최근에는 생성형 AI와 딥페이크 같은 신기술이 사이버 공격의 속도, 규모, 정교함을 전례 없이 가속화 시키고 있으며, 이는 기존의 방어 중심 보안 체계로는 탐지 및 대응이 매우 어려운 '기만' 요소를 강화한다. 2025년 사이버보안 분야에서는 AI · 딥페이크 악용 공격, 국가 주도 공급망 공격, 다변화된 랜섬웨어 공격, 크리덴셜 탈취 공격 증가가 예상된다. 생성형 AI의 발전으로 악성 거대언어모델(LLM) 서비스, 딥페이크 등 신기술을 누구나 활용할 수 있게 되면서 이를 악용한 사이버 위협이 증가할 것으로 전망된다. 공격자들은 LLM 모델을 사용 하여 신뢰할 수 있는 개체를 사칭하고 대규모 피싱 및 사회 공학 공격을 자동화하며, AI 기만 기술을 사용하여 가짜와 실제를 구별하기 어렵게 만들고 있다. 이처럼 AI 기반 사이버 공격은 취약점 탐지 및 공격 실행 시간을 대폭 단축시키고, 의료 영상 변조, 자율주행 차량 안전 위협, 딥페이크를 이용한 금융권 해킹, 스피어피싱을 통한 민감 정보 유출 등 다양한 형태로 진화하고 있다. 이와 같은 AI 기반 공격은 예측 불가능하게 변이하고 기존 패턴 기반 탐지를 우회하며, 보안 팀이 알아채기 전에 시스템을 침투할 수 있어 대응을 더욱 어렵게 만든다. 또한, 랜섬웨어 공격은 데이터 암호화, 기업 자료 유출 · 공개, DDoS 공격을 가하는 3중 갈취 전술을 통해 고도화되고 있다. 따라서 방위산업은 이러한 AI 기반의 고도화된 위협에 대응하기 위해 단순한 방어를 넘어 AI를 활용한 능동적 탐지, 기만, 역대응 기술 개발에 박차를 가해야 한다. 이는 끊임없는 기술 혁신과 적응을 요구하는 새로운 차원의 사이버 전쟁을 의미한다.

3.2. 국내 대응체계 현황과 한계

방산기술 탈취를 목표로 하는 사이버 위협에 대응하기 위해 한국 정부와 민간 부문은 여러 노력을 기울여 왔다. 방위산업기술보호법 시행 이후 방산업체들은 내부 보안 조직을 두고 기술 유출 방지 체계를 마련하는 한편, 국가정보원 산하 산업기밀보호센터와 긴밀히 협조하며 기술 보호 수준 제고에 힘쓰고 있다.

국가정보원은 방첩 전담 기관으로서 방산 분야 보안 강화를 위한 다양한 조치를 추진해 왔다. 방산업체 임직원을 대상으로 기술 유출 사례와 대처 방안을 교육하고, 방위산업 침해대응센터를 신설하여 방산 분야 사이버 사고 대응 및 침해분석 기능을 강화하였다. 또한 2023년과 2024년 두 차례에 걸쳐 주요 방산기업 대표들과의 협의를 통해 북한 해킹 위협에 대한 경각심을 제고하고 대응 협력을 당부하는 등, 민 · 관 협력 기반의 예방적 조치에도 나서고 있다.

방위사업청은 방산기술 보호 업무의 주무 기관으로서, 국방부 · 국정원 등과 공조하여 제도 구축 및 관리 감독을 수행한다. 방사청은 사이버보안 전문 인력 양성과 함께, 미국 국방부의 사이버보안 기준을 도입한 한국형 RMF(Risk Management Framework)[5] 개발을 추진해 왔다. RMF는 군사 무기체계 개발과 운영 전 주기에 걸쳐 보안 위험을 체계적으로 관리하는 프로세스로, 미국에서는 사이버보안 성숙도 평가의 척도로 활용된다.

우리 국방부는 2020년부터 미 RMF를 벤치마킹한 K-RMF를 개발하여 2024년 하반기부터 적용할 예정이며, 우선 무기체계 전산 관리 분야에 시범 도입한 후 점차 범위를 확대할 계획이다. RMF는 준비-분류-통제선정-통제구현-통제평가-인가-모니터링의 7단계 프로세스로 구성되어 있어, 시스템 개발 단계에서부터 폐기까지 지속적인 보안 통제와 검증이 이루어지도록 한다.

이처럼 정부와 업계의 노력으로 방위산업 사이버 보안 거버넌스가 점차 구축되고 있으나, 여전히 여러 한계가 노정되고 있다.

5) RMF(위험 관리 프레임워크) : 미국의 NIST (National Institute of Standards and Technology)에서 제시한 정보시스템 보안 리스크 관리 절차

표 2. 국내 방산 사이버보안 대응체계의 주요조직 및 한계점[6)]

조직	주요 기능	한계점
국가정보원	위협정보 수집 · 분석 · 공유, 방산 분야 보안 강화조치, 침해대응센터 신설, 민 · 관 협력	중소기업 현장 지원 부족
방위사업청	방산기술보호 주무기관 K-RMK 개발 추진, 관리 감독	법적 근거 미비로 능동 대응 제한
국방부	K-RMF 개발 주도, 무기체계 보안 전 주기 관리체계 추진	적용 초기 단계, 범위 확대까지 시간 소요
방산기업	내부 보안 조직운영 · 기술보호 체계 구축, 산업기밀보호센터 협조	전문인력 · 자원 부족으로 탐지 역량 약함 초동 탐지 및 대응 부족
경찰청	합동조사, 해킹 공격 규명 및 보호 조치	사건 발생 후 수사 위주, 예방 및 능동적 방첩 활동에 한계

첫째, 초동 탐지와 대응의 부족이다. 상당수 기업들이 사이버 침해 사고 발생 사실 자체를 알아채지 못했고, 외부 기관의 점검이나 수사를 통해서야 비로소 파악한 경우가 있었다. 이는 기업 차원의 보안관제 능력과 침해사고 탐지 역량이 미흡함을 보여주며, 특히 중소 협력업체일수록 전문 인력과 시스템이 부족하여 위험이 크다. 국내 방산 대기업 18곳의 보안 인력 비율이 1% 미만에 불과하다는 점은 이러한 탐지 역량 부족의 핵심 원인 중 하나이며, 이는 중소 협력업체의 상황은 더욱 열악할 것임을 시사한다. 2016년 9월 발생한 국방망 해킹 사건 당시 국군사이버사령부의 미흡한 대응으로 PC 3,200대가 악성코드에 감염된 사례는 초동 탐지 실패의 심각성을 보여준다.[16]

둘째, 정보 공유와 공조 체계의 한계이다. 현재 국정원 · 방사청 · 경찰청 등 여러 기관이 관여하고 있으나, 사건에 따라 임시 조직이 구성되는 등 일관되고 상시적인 공조 플랫폼은 아직 발전 단계이다. 이는 위협 정보의 적시 공유 및 통합적 대응을 어렵게 만들며, 복잡한 디지털 공급망에서 더욱 두드러진다.

셋째, 능동적 대응 수단의 부족이다. 현재 법제도 하에서는 기업이 스스로 해커를 추적하거나 역대응을 펼치는 것은 현실적으로 불가능하며, 방첩 차원의 적극적 조치는 주로 국정원 등 정보기관에 의존한다. 그러나 사이버상에서의 신속한 공격원 추적과 차단, 역이용 등의 활동은 법적 근거와 전문 인력, 국제 공조가 복합적으로 뒷받침되어야 하는바, 국내에는 이를 전담할 수 있는 사이버 방첩 전담 조직이나 법령 기반이 아직 미흡하다. 한국의 사이버안보 관련 법률은 2020년 제정된 대통령령 「사이버안보 업무규정」과 2001년 제정된 「정보통신기반 보호법」 등 분야별로 존재하지만, 사이버 방첩의 전략적 기능을 직접 규율하는 독립된 법적 근거는 미비한 상태이다.

3.3. 해외 주요국 사례 분석 및 시사점

3.3.1. 주요국 사례

미국은 국방산업기반(DIB: Defense Industrial Base)을 보호하기 위해 강력한 사이버 방첩 체계를 구축하고 있다. 미 국방부 산하 방첩보안청(DCSA: Defense Counterintelligence and Security Agency)은 국방 산업체들의 보안 및 방첩 업무를 통합 관리하며,[17] 특히 사이버보안 성숙도 모델(CMMC: Cybersecurity Maturity Model Certification)[7)]을 도입하여 모든 국방부 계약업체가 일정 수준 이상의 사이버보안 역량을 갖추도록 의무화하고 있다.[18]

6) 사이버보안 대응 주요 조직도를 참고하여 저자 재작성

7) CMMC(Cybersecurity Maturity Model Certification) : 미국 국방부 계약업체 및 하청업체의 사이버 보안 역량을 평가하고 인증하기 위한 모델로 국가 기밀 정보와 민감한 데이터를 보호가 핵심

CMMC는 5단계의 성숙도 레벨로 구성되어 있으며, 기업들은 계약 유형에 따라 요구되는 레벨을 충족해야 한다. 이는 대기업뿐만 아니라 중소 규모의 협력업체까지 포괄하여 공급망 전반의 보안 취약점을 최소화하는 데 기여한다. 미국 국방부(DoD)는 국방 산업기반(DIB)의 사이버보안 및 복원력 강화를 위한 전략을 수립하며, DIB 기업들이 악의적인 사이버 활동의 위험에 노출되어 있으며, 중소기업도 주요 표적임을 강조한다. 이에 따라 미국의 사이버보안 성숙도 모델(CMMC)은 국방부 계약업체가 일정 수준 이상의 사이버보안 역량을 갖추도록 의무화하며, 이는 대기업뿐만 아니라 중소 협력업체까지 포괄하여 공급망 전반의 보안 취약점을 최소화하는 기여한다. 그러나 CMMC 이행의 주요 난관은 비용과 복잡성으로, 특히 중소기업에게는 큰 부담이 될 수 있다. 이를 완화하기 위해 CMMC 2.0은 레벨 1 계약업체에 대해 자율 평가 옵션을 허용하여 비용 부담을 줄이려 하고 있다. DoD의 Project Spectrum은 중소기업의 사이버보안 인식 제고 및 CMMC 준수 지원을 위한 포괄적인 플랫폼을 제공하며, 이는 중소기업의 보안 역량 강화를 위한 정부 차원의 실질적인 지원 방안의 중요성을 보여준다.[19] 또한 미국은 국가방첩안보센터(NCSC: National Counterintelligence and Security Center)를 통해 범정부 차원의 사이버 방첩 전략을 수립하고, 다양한 정보기관 및 법 집행기관 간의 정보 공유와 공조를 강화하고 있다.

이스라엘은 '국가 사이버국(National Cyber Directorate)'을 중심으로 군, 정보기관, 민간 산업체가 긴밀히 협력하는 독특한 사이버안보 생태계를 구축하고 있다.[20,21] 이스라엘은 공격과 방어를 아우르는 '통합 사이버 전략'을 추구하며, 특히 능동 방어 및 사이버 위협에 대한 역대응 역량을 강조한다. 이는 민간 기업의 혁신적인 기술력을 적극 활용하고, 정부가 강력한 지원과 규제를 통해 전체적인 사이버안보 수준을 높이는 방식으로 이루어진다. 이스라엘은 또한 사이버 공격의 출처를 추적하고 책임 주체를 식별하는 '귀속(attribution)' 능력을 매우 중요하게 여기며, 이를 통해 외교적, 법적 대응의 기반을 마련한다.[22]

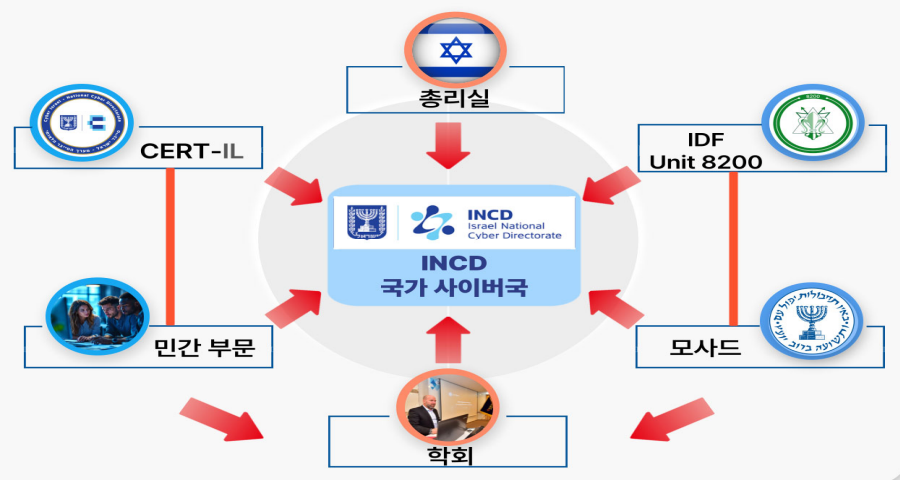

그림 2. 이스라엘 국가 사이버국 조직 거버넌스 구조도[8)]

이외에도 영국, 독일, 프랑스 등 주요 선진국들의 사이버 방첩 법제도 및 거버넌스 모델을 비교분석해 보면 이들 국가들은 단순한 사이버보안을 넘어 국가안보의 핵심 요소로서 사이버 방첩의 중요성을 인식하고, 이를 위한 법적, 조직적, 기술적 투자를 아끼지 않고 있다. 특히, 국방 산업 공급망 전반의 보안 강화, 능동적 대응 역량 확보, 그리고 민 · 관 · 군을 아우르는 통합적 거버넌스 구

8) Center for Security Studies (CSS), ETH Zurich. Israel's national cybersecurity and cyberdefense posture. 2020 참조하여 재작성

축은 공통된 특징이다.

영국(UK): 영국은 '국가사이버전략 2022'를 통해 사이버 공간에서의 국가 거버넌스를 강화하고, 사이버 전략을 국가 전략 수준으로 격상시켰다. 특히 사이버 공격자에 초점을 맞춘 '책임 귀속(attribution)' 입증 역량 강화를 강조한다. 영국의 국방 전략 검토(SDR)는 2025년 11월까지 국방 정보국(DI) 내에 사이버 방첩 전담 부서(Counter-Intelligence Unit, CIU) 설립을 권고하며, 이 CIU는 적대적 정보기관으로부터 영국 국방을 보호하고, 산업과의 단일 접점 역할을 수행할 것이다. 영국의 GCHQ(사이버 및 신호 정보 기관)는 러시아 군사 정보 기관의 악의적인 사이버 활동을 반복적으로 폭로하며 능동적 방어의 사례를 보여주었다. 또한, NCSC(National Cyber Security Centre)는 '능동적 사이버 방어(Active Cyber Defence, ACD)' 프로그램을 통해 대규모 일반 사이버 공격으로부터 영국을 보호하며, 이는 예방적 도구와 서비스를 제공한다.[23]

독일(Germany) : 독일은 사이버 보안을 전담하는 독자적인 거버넌스인 연방정보기술보안청(BSI)을 보유하고 있다. BSI는 IT 보안에 관한 강력한 권한을 가지며, 예방적 사이버보안, 중요 인프라 보호, 스파이 활동 및 방첩, 보안 제품 인증 등을 담당한다. 독일은 사이버보안을 위해 공적 영역과 사적 영역의 상호 협력을 강화하고 있으며, 최근에는 이스라엘 기술을 활용한 국가 사이버 방어 시스템 '사이버 돔(Cyber Dome)' 구축 계획을 발표했다. 이는 정보기관 간 협력 심화, 공동 사이버 연구 센터 설립 등을 포함한다. 연방국방부(BMVg)는 사이버 안보 정책의 국방적 측면을 담당하며, 군사 방위와 사이버 공간 방위가 핵심 임무 영역이다.[24]

프랑스(France) : 프랑스는 국가정보시스템보안청(ANSSI)을 국가 사이버 보안 당국으로 설립하여 정보시스템 보호 관련 능동적인 방어 전략을 취해왔다. ANSSI는 정부 부처 및 중요 기반 시설 운영자(OIV)에 전문 기술 지원 및 자문을 제공하며, 사이버 공격 모니터링, 탐지, 경고 및 대응 역할을 수행한다. 프랑스 국방부는 자체 네트워크 보호 및 디지털 전쟁 통합을 위한 이중 임무를 수행하며, 2017년 사이버 방어 작전 사령부(COMCYBER)를 창설하여 사이버 방어역량을 강화하고 있다.[25]

표 3. 주요 해외국의 사이버 방첩 법제도 및 거버넌스 비교[9)]

국가	주요 법제/정책	전담조직/거버넌스	주요특징/시사점
미국	방위산업기반(DIB) 보호, 사이버 보안 성숙도 모델 (CMMC), 국가방첩전략	DCSA, NCSC	공급망 전반의 보안 인증 의무화, 범정부 차원 사이버 방첩 전략 수립 및 정보 공유 강화
이스라엘	통합 사이버 전략	국가 사이버국(National Cyber Directorate)	공격과 방어를 아우르는 능동적 방어 및 역대응 역량 강조, 민간 기술력 활용, 공격자 귀속(Attribution) 능력 중요시
영국	국가사이버전략 2022, 능동적 사이버 방어(ACD) 프로그램, 국방 전략 검토(SDR)	GCHQ, NCSC, 국방정보국(DI) 내 CIU 설립 추진	사이버 전략을 국가 전략 수준으로 격상, 공격자 귀속 역량 강화, 국방 분야 특화 방첩 조직 추진
독일	연방정보기술보안청(BSI)법, IT 보안법 2.0, 사이버 돔 계획	연방정보기술보안청(BSI), 연방국방부(BMVg)	사이버 보안 전담 독자 거버넌스, 공적/사적 영역 협력 강화, 이스라엘 기술 벤치마킹 사이버 방어 시스템 구축
프랑스	국가정보시스템보안청(ANSSI) 설립 법령, 국방백서의 능동 방어 전략	국가정보시스템보안청(ANSSI), 사이버 방어 작전 사령부(COMCYBER)	정보시스템 보호 능동적 방어 전략, 중요 기반 시설 보호 및 기술 지원, 국방부의 디지털 전쟁 통합

9) 앤소니 온체 등(2021), 국가안보전략연구원. 영국 「국가사이버전략 2022」의 특징과 시사점. (2022), 양천수, 김중길(2022), 박우경(2019) 등 참조하여 재작성

3.3.2. 시사점

위의 해외 사례들은 방위산업 사이버 방첩 전략에 다음과 같은 중요한 시사점을 제공한다. 첫째, 공급망 전체를 포괄하는 강력한 보안 인증제의 도입이 필수적이다. 대기업뿐만 아니라 중소 협력업체의 보안 취약점이 전체 시스템의 가장 약한 고리가 될 수 있음을 인지하고, 미국 CMMC와 같은 한국형 모델 도입을 적극적으로 검토해야 한다. 둘째, 민 · 관 · 군을 아우르는 통합적이고 상설적인 사이버 방첩 거버넌스를 구축해야 한다. 정보 공유와 실시간 공조가 가능한 플랫폼을 제도화하여 위협 정보를 즉각적으로 공유하고, 합동 대응체계를 상시 가동할 필요가 있다. 셋째, 능동적 사이버 방첩 역량 강화가 시급하다. 단순한 방어를 넘어선 위협 인텔리전스 분석, 사이버 기만전술 도입, 공격 주체에 대한 역추적 및 무력화 역량 확보 등 적극적인 방첩 수단을 개발하고 활용해야 한다. 이는 전문 인력 양성과 법적 근거 마련을 통해 뒷받침되어야 한다.

요컨대, 해외 선진국들은 단순한 사이버보안을 넘어선 전략적인 사이버 방첩의 중요성을 인식하고 있으며, 이를 위한 제도적 · 기술적 · 인력적 투자를 아끼지 않고 있다. 한국은 이러한 선진국들의 경험을 벤치마킹하여, 공급망 전반을 포괄하는 보안 인증제 도입, 민 · 관 · 군을 아우르는 통합적 사이버 방첩 거버넌스 구축, 능동적 대응 역량 강화, 그리고 이를 뒷받침할 법적 기반 마련에 시급히 나서야 할 시점이다.

4. 방위산업 사이버 방첩 전략 강화를 위한 제도적 과제

방위산업을 겨냥한 사이버보안 위협은 단순한 해킹이나 기술 유출을 넘어 적대세력의 조직화 된 정보수집과 장기적 첩보작전의 일환으로 전개되고 있다. 기존의 기술 보안이나 침해대응 중심의 사이버보안 체계는 이러한 전략적 위협을 사전에 탐지하거나 효과적으로 저지하는 데 한계를 보이고 있다. 사이버 방첩은 침투 이후의 사후 대응이 아닌 선제 조치로서 정보수집 기획 단계부터 적의 시도를 식별하고 차단하며, 나아가 기만 전략과 대응 작전을 수행하는 전략적 패러다임을 요구한다. 따라서 방위산업 보호를 위한 사이버 방첩 전략은 기술적 조치나 기업 보안 역량 강화에 그치지 않고, 국가 차원의 제도적 기반 재설계가 필요하다.

4.1. 사이버 방첩 법 제 정비 및 임무 규정화

현행법 제도는 산업기술 보호, 국가정보 보호, 사이버보안 등 다양한 요소를 포함하고 있으나, 사이버 방첩이라는 전략적 기능을 직접 규율하는 독립된 법적 근거는 미비한 상태이다. 한국의 사이버안보 관련 법률은 2020년 제정된 대통령령 「사이버안보 업무규정」과 2001년 제정된 「정보통신기반 보호법」 등 분야별로 존재하지만, 사이버 방첩의 전략적 기능을 직접 규율하는 독립된 법적 근거는 미비한 상태이다. 이로 인해 민간 방산기업과 정보기관 간의 협조 체계가 실효성을 갖지 못하고, 사이버 첩보 행위에 대한 국가 차원의 정당한 대응이 법적 논란에 노출될 위험이 존재한다. 국가 사이버안보 역량 강화를 위한 정책 개발 과제 중 하나로 '사이버안보 유관기관별 역할과 각급 기관 간 협력 활성화 등을 규정한 법령 제정 추진'이 포함되어 있으며, 대통령 직속 '국가사이버안보위원회' 설치 및 컨트롤타워 운영체계를 갖추기 위한 국가사이버안보 기본법 제정의 필요성도 제기되고 있다.

이에 따라 사이버 방첩 활동에 대한 법적 근거 마련이 요구된다. 기존 방위산업기술보호법 국가사이버안보 관련 법령에 사이버 방첩 조항을 신설하거나, 별도의 법적 근거를 통해 다음 사항들을 명문화해야 한다: 첫째, 사이버상 국가 전략 자산을 겨냥한 첩보 행위에 대한 방첩 활동 근거, 둘째, 국정원 등 지정 정보기관의 조사 · 식별 · 추적 권한, 셋째, 민간 기업과 정보기관 간 위협 정보 실시

간 공유 체계, 넷째, 정보보호와 기업 책임 제한 장치. 이러한 법제도 정비는 사이버 방첩이 단순한 기술적 보안의 연장이 아닌, 국가 전략정보 기능의 일부로 작동함을 제도적으로 보장하는 조치이다.

능동적 사이버 방첩 활동은 '공격이 최선의 방어'라는 전략적 필요성에도 불구하고, 공격자 귀속의 어려움, 국제법상 무력 사용 기준의 모호성, 그리고 '평시/전시' 경계의 불분명함이라는 법적·윤리적 딜레마에 직면해 있다. 사이버 공격은 발신자 정보 위조, 반사 호스트 이용 등으로 공격자 식별이 매우 어려우며, 이는 국제법상 국가 책임의 전제 조건인 '귀속(attribution)'을 복잡하게 만든다. 국제법(UN 헌장 제2조 4항, 제51조)은 사이버 공격이 '무력 공격'에 해당하는지, 복잡한 법적 쟁점을 야기하며, 이는 국가의 정당한 방어권을 행사하는 데 법적 불확실성을 초래한다. 사이버 작전의 윤리적 규칙은 '전쟁 중인가?', '누구와 전쟁 중인가?', '무엇을 표적으로 삼을 수 있는가?'라는 세 가지 질문에 대한 답변이 모호해지면서 혼란을 겪는다. 사이버 공간에서는 평시와 전시의 경계가 모호해져, 평시에는 범죄적 행위로 간주 될 수 있는 활동이 전시에는 '정보수집'이라는 명분으로 이루어지는 윤리적 문제가 발생한다. 미국 국방부는 '능동적 방어(defend forward)' 전략을 통해 적대적 사이버 활동에 지속적으로 관여하고 교란하며, 대통령은 국가 이익에 반하는 적대적 사이버 작전을 지시할 권한이 있음을 명확히 하고 있다. 국제법은 사이버 공간에도 적용되며, 국가 책임에 관한 기존 규칙(ARSIWA)이 사이버 맥락에도 적용될 수 있다는 의견이 지배적이다. 따라서 한국은 사이버 방첩 독립법 제정을 통해 능동적 대응의 국내 법적 근거를 명확히 하는 동시에, 국제 사회에서 사이버 공간에서의 국가 행동 규범 및 국제법 적용에 대한 논의에 적극적으로 참여하여 법적 불확실성을 해소하고 국제적 공감대를 형성하는 데 기여해야한다.[26]

사이버 방첩 활동은 국가안보라는 중대한 공익을 추구하지만, 이 과정에서 발생하는 개인 정보 침해 및 프라이버시 문제는 심각한 법적, 윤리적 논란을 야기할 수 있다. 사이버 스파이 활동으로부터 보호하기 위해서는 강력한 사이버보안 조치, 국제 협력, 위협 정보 공유, 그리고 명확한 법적 프레임워크가 필요하다. 사이버 방첩은 광범위한 정보수집과 분석을 수반하며, 이는 필연적으로 개인의 디지털 흔적과 민감 정보에 접근할 가능성을 내포한다. 정부의 데이터 수집에 대한 대중의 우려가 높으며, 부적절한 감시 방법은 프라이버시 권리 침해로 이어질 수 있다. HUMINT(인적 정보) 전술은 산업 스파이, 기밀 유지 위반, 공모, 부패 등 심각한 법적 결과를 초래할 수 있으며, 내부자 위협 프로그램은 시스템 접근 모니터링을 넘어 행동 위험을 다루어야 한다.

국제 데이터 보호 및 프라이버시 법률(예: GDPR[10])은 목적 제한, 데이터 최소화, 투명성, 책임성 등 엄격한 원칙을 요구한다. '프라이버시 바이 디자인(Privacy by Design)'은 시스템 설계 단계부터 개인 정보 보호를 고려하는 접근 방식으로, 사전 예방적, 기본 설정으로서의 프라이버시, 설계에 내재 된 프라이버시, 종단 간 보안, 가시성 및 투명성, 사용자 중심성 등 7가지 원칙을 제시한다. 따라서 '프라이버시 바이 디자인' 원칙을 적용하고, 정보 공유 시 익명화 및 최소화 조치를 의무화하며, 기업의 선의의 정보 공유에 대한 법적 책임 제한 장치를 마련하여 국가안보와 개인의 기본권 보호 간의 균형점을 찾아야 한다. 정보 처리 과정의 투명성을 확보하고, 독립적인 감독 기관을 통한 감시를 강화하여 오남용을 방지하는 것도 중요하다. 사이버 방첩의 실효성을 확보하면서도 민주주의 사회의 기본 가치를 훼손하지 않기 위해서는, 프라이버시 보호를 최우선으로 고려하는 법적·기술적·제도적 안전장치 마련이 필수적이다.[27]

10) GDPR(General Data Protection Regulation) 일반 데이터 보호 규정이며, 유럽 연합(EU)에서 제정한 개인정보 보호 법률로, 2018년 5월 25일부터 시행

4.2. 조직 구조 혁신: 사이버 방첩 거버넌스 설계

민간 영역의 정보보호 조직 체계는 정보보안 조직 체계에서 발전하였으나 대부분 침해대응(CERT) 중심, 보안관리(CISO) 중심 구조에 머물러 있다. 그러나 사이버 방첩은 국가안보의 가장 중요한 군사기밀과 첨단 방위산업 기술 보호를 담당한다. 단순한 기술 관리를 넘어 국가 안보적 차원의 전략적 정보 수집 · 분석 · 작전 수행을 수반하는 통합적 접근을 요구한다. 국가 단위에서는 방산 사이버 방첩센터(가칭) 설립을 검토할 필요가 있다. 이 조직은 국가정보원 · 방위사업청 · 국방부가 합동으로 운영하며, 기술 보호, 내부자 위협 탐지, 위협 예측, 대응 전략 개발을 총괄하는 통합 기능을 수행해야 한다. 이는 단순히 정보수집에 그치지 않고, 방산기업 대상으로 하는 첩보활동을 조기에 탐지하고 능동적으로 대응하는 전략적 정보기관으로 설계되어야 한다.

신규 국가 조직 설립은 한국의 공공기관 효율화 기조 및 부처 간 칸막이 문화라는 현실적 난관에 직면할 수 있다. 한국 정부는 공공기관 신설을 최소화하고 기존 기관의 효율화를 추진하는 경향이 있으며, 공공기관 기능 조정 및 조직 · 인력 효율화 이행으로 10,721명 정원 감축, 1.4조 원의 자산 매각 등 사례가 있다. 이는 새로운 센터 설립 시 예산 확보 및 조직 통합 과정에서 상당한 저항과 난관에 부딪힐 수 있음을 의미한다.

성공적인 거버넌스 모델은 강력한 법적 권한, 통합된 정보 흐름, 그리고 민간 부문과의 유기적인 협력을 특징으로 한다. 영국의 국방 전략 검토(SDR)는 2025년 11월까지 국방 정보국(DI) 내에 사이버 방첩 전담 부서(CIU) 설립을 권고하며, 이 CIU는 국방 산업과의 단일 접점 역할을 수행할 것이다.[28] 독일은 연방정보기술보안청(BSI)을 통해 사이버보안을 전담하는 독자적인 거버넌스를 갖추고 있으며, BSI는 사이버보안에 관한 강력한 권한을 가진다. 프랑스 ANSSI는 정부 부처 및 중요 기반 시설 운영자(OIV)에 전문 기술 지원 및 자문을 제공하며, 사이버 공격 모니터링, 탐지, 경고 및 대응 역할을 수행한다. 이러한 해외사례들은 통합성, 강력한 권한, 산업과의 연계가 성공적인 거버넌스 모델의 핵심임을 보여준다.

따라서 방위산업 사이버 방첩센터 설립은 단순한 조직 신설을 넘어, 기존 부처 간 역할 재정립, 예산 확보 전략, 그리고 해외 선진 사례를 참고한 유기적이고 강력한 거버넌스 모델 설계가 동반되어야 한다. 특히, 초기 단계에서는 기존 기관 간의 협의체 강화 및 유기적 연계를 통한 '가상 센터' 운영을 고려하고, 점진적으로 독립 조직으로의 전환을 모색하는 현실적인 로드맵이 필요하다.

민간기업 측면에서는 방산기업 내 사이버 방첩 전담관(POC) 제도 도입을 고려해야 한다. 각 기업이 국정원 또는 정부 기관과 직접 소통하는 공식 채널을 확보하여, 기업 내 위협 징후를 수집 · 분석하고 유관기관과 협력하여 신속한 보고와 대응이 가능한 체계를 구축해야 한다. 국방 산업 기반(DIB) 기업들은 악의적인 사이버 활동의 위험에 노출되어 있으며, DoD는 DIB의 사이버보안 및 복원력 강화를 위한 전략을 수립하고 있다. 미국 CMMC는 계약업체가 일정 수준 이상의 사이버보안 역량을 갖추도록 의무화하며, 이는 대기업뿐만 아니라 중소 협력업체까지 포괄한다. DoD의 Project Spectrum은 중소기업의 사이버보안 인식 제고 및 CMMC 준수 지원을 위한 포괄적인 플랫폼을 제공하며, 이는 민간 기업의 보안 역량 강화를 위한 정부의 지원 중요성을 강조한다.

방위산업 사이버 방첩의 성공은 단순히 조직을 신설하는 것을 넘어, 기존 정부 부처 간의 '칸막이'를 허물고 실질적인 정보 공유와 협력 문화를 제도화하는 데 달려 있다. 한국 정부 부처 간 협업 과제 선정 노력에도 불구하고, 실제 협업은 그만큼 잘 이루어지지 않는 경향이 있으며, 특정 부처 간에는 응집 지수가 높아 타 부처와의 협업 연계가 상당히 낮은 경향을 보인다. 이는 정보 공유와 통합적 대응에 구조적 장애물로 작용한다. 사이버안보의 국가 전략적 접근에 있어 체계적이고 효과적인 컨트롤타워 운영체계 구축은 국가사이버안보기본법 제정을 통해 이행해야 할 우선 과제이며, 이는 협업의 강제성을 부여하고 책임 소재를 명확히 할 수 있다. 법제화와 더불어, 기관 간의 신

뢰를 구축하고 공동의 위협 인식을 공유하는 문화적 변화를 유도하는 것이 장기적인 성공의 열쇠이다. 따라서 방위산업 사이버 방첩 거버넌스 설계는 법적 · 제도적 기반 마련과 함께, 부처 간의 정보 공유 및 협력에 대한 문화적 장벽을 극복하기 위한 지속적인 노력이 요구된다.

4.3. 능동적 대응 중심의 기술체계 확립

사이버 방첩은 공격을 단순 차단하는 것을 넘어 적의 행동을 역추적하고 분석하는 능동적 대응 전략을 포함한다. 이는 위협 인텔리전스 강화, 허니팟(honeypot)[11] 운용, 행동 패턴 분석 등 선제적 대응 기술 체계와 연결되어야 한다.

방산 분야 특화형 사이버 위협 탐지 플랫폼 개발과 배치가 필요하다. 중요 무기체계 개발기업의 핵심 인프라와 유사한 구조의 가상 모니터링 시스템을 구축하여, 침투 시도와 공격 수법을 실시간으로 추적할 수 있다. 이 과정에서 수집된 정보는 적의 TTPs(전술 · 기술 · 절차)를 파악하고, 차기 공격 대비 시나리오 개발에 활용할 수 있다. AI는 네트워크 트래픽 및 시스템 로그 분석을 통해 비정상적인 활동을 신속하게 감지하고, 과거 데이터 및 공격 패턴 학습을 통해 미래 위협을 예측할 수 있다. AI 기반의 차세대 보안관제센터 자동화(NextGen Automation SOC) 구축에 대한 수요가 늘어날 것으로 예상되며, 이는 SIEM, SOAR, TI 등이 적용된 시스템을 포함한다.

사이버 기만 기술(cyber deception) 도입도 검토되어야 한다. 가상 자산을 통한 공격자 유인, 의도적 정보 노출을 통한 공격 방향 파악 등은 방첩 활동의 핵심 방식 중 하나이다. 사이버 기만은 공격자를 유인하고, 속이고, 함정에 빠뜨리는 효과적인 방법으로, AI의 빠른 처리 능력은 적의 전술과 도구를 분석하여 존재를 식별하고 목표를 이해하는 데 활용될 수 있다. AI는 디코이(허위 자산)를 생성하여 공격자를 유인하고, 공격자의 행동 패턴을 분석하여 비정상적인 움직임을 탐지하는 데 활용될 수 있다. 다만 이러한 기술 운용이 관련 법령 위반으로 간주 되지 않도록, 방첩 목적의 기만 기술 운용에 대한 법적 근거 마련이 병행되어야 한다.

AI 기반 허니팟 및 사이버 기만 기술은 방위산업의 능동적 사이버 방첩 역량을 획기적으로 강화할 수 있는 잠재력을 지니지만, 동시에 AI가 공격자에게도 활용되어 위협의 복잡성을 증대시키는 '양면성'을 가진다. AI 기반 딥페이크 기술은 공격자가 신뢰할 수 있는 개체를 사칭 하고 피싱 및 사회 공학 공격을 자동화하는 데 사용될 수 있으므로, 방어 측면에서도 딥페이크 저항 보안 프로토콜 개발 및 AI 기반 사기 탐지 방법론이 필요하다. AI는 동시에 공격자에게도 활용되어 딥페이크, 자동화된 피싱, 악성코드 생성 등 고도화된 기만 공격을 가능하게 한다. 이러한 기술을 효과적으로 운용하기 위해서는 기술적 고도화뿐만 아니라, 기만 활동의 법적 정당성을 확보하고 윤리적 문제를 해결하는 것이 필수적이다. 기만 기술의 운용은 '해킹' 또는 '정보 조작'으로 간주 될 수 있어 법적 논란의 소지가 있으며, 프라이버시 침해, 오인 공격 등 윤리적 문제도 발생할 수 있다. 방위산업은 AI 기반 기만 기술을 적극 도입하되, AI의 '양면성'을 인지하고 AI 기반 공격에 대한 방어 기술을 지속적으로 개발해야 한다. 또한, 이러한 능동적 방첩 활동이 법적 · 윤리적 테두리 안에서 이루어지도록 명확한 법적 근거와 가이드라인을 마련하는 것이 중요하다.

AI 기반 위협 인텔리전스 분석 및 공격자 귀속(Attribution) 기술 고도화도 필수적이다. AI는 대량의 데이터 처리, 패턴, 추세, 이상 징후 식별에 탁월하며, 인간 분석가가 놓칠 수 있는 부분을 찾아낸다. AI 알고리즘은 온라인 및 오프라인 개인행동 분석을 통해 의심스러운 패턴이나 정상 활동에서 벗어나는 행동을 감지하여 위협이 확대되기 전에 식별할 수 있다. AI 기반 예측 모델링은 행동 데이터, 통신 패턴, 심리적 요인 분석을 통해 잠재적 내부자 위협을 예측할 수 있으며, 비정상적

11) 허니팟(honeypot)은 공격자를 유인하기 위해 고의로 설정한 가짜 정보시스템, 서버, 파일 또는 네트워크 리소스를 말한다.

인 민감 정보 접근이나 비업무 시간 활동을 감지하여 내부자 위협을 신호할 수 있다. AI는 공개 출처 및 기밀 채널에서 정보수집을 자동화하여 방첩 활동의 효율성과 도달 범위를 향상 시킬 수 있다. 공격자 귀속(Attribution)은 사이버 공격의 출처를 기술적, 정치적, 법적 차원에서 특정하는 것으로, 국제법상 국가 책임의 근거가 된다. 기존의 귀속 기술은 로그 저장, 허니팟 관찰, 침입 탐지 시스템(IDS) 활용 등이 있으나, IP 스푸핑, 리플렉터 호스트 사용 등으로 공격자 식별이 어려움을 겪고 있다. AI는 위협 인텔리전스 분석 및 공격자 귀속에 혁신적인 도구를 제공하지만, 사이버 공격의 익명성 기술 고도화와 법적 귀속의 높은 증거 기준이라는 본질적인 한계에 직면해 있다. 공격자들은 IP 스푸핑, 프록시 서버, VPN, '위장 작전(false flags)' 등을 사용하여 자신의 신원을 숨기며, 이는 기술적 귀속을 매우 어렵게 만든다. 국제법상 법적 귀속을 위해서는 정치적 책임보다 훨씬 높은 수준의 증거가 요구된다. 따라서 AI 기술 발전과 함께 국제적 협력 및 법적 · 외교적 노력을 병행하여 귀속 역량을 강화해야 한다.

블록체인 기반 공급망 보안 및 위협 정보 공유 시스템 구축도 중요한 과제이다. 블록체인 기술은 거래 기록을 유지하는 협력적이고 변조 불가능한 원장(ledger)으로, 데이터의 변경 여부를 모든 사용자가 알 수 있게 하여 변조 증거를 제공한다. 블록체인은 국방부(DoD) 공급망 네트워크의 "단일 진실 공급원(single source of truth)"을 제공하여 데이터 단편화, 오류 가시성 부족 문제를 해결할 수 있다. 공급망 내 각 단계에서 상품을 스캔하고 블록체인을 업데이트하여 실시간 가시성을 확보하고 문제를 즉시 식별할 수 있다. 블록체인 기반 사이버 위협 인텔리전스 공유는 조직 간 안전하고 투명한 정보 공유를 가능하게 하여 집단 방어를 촉진한다. TrustShare와 같은 블록체인 기반 프레임워크는 안전하고 프라이버시를 보호하며 신뢰할 수 있는 CTI(사이버 위협 인텔리전스) 공유를 가능하게 한다. 블록체인의 불변성, 투명성, 추적 가능성, 탈중앙화 특성은 보안 애플리케이션에 큰 잠재력을 제공하며, 군사 작전, 물류 관리, 장비 조달 등 다양한 군사 분야에 블록체인 적용 가능성이 연구되고 있다.

방위산업의 복잡한 공급망과 다자간 위협 정보 공유에서 가장 중요한 '신뢰'와 '투명성' 문제를 해결할 수 있는 근본적인 해법을 제공하는 것이 블록체인 기술이다. 이는 데이터의 무결성과 추적 가능성을 보장하여, 기존의 중앙 집중식 시스템의 취약점을 보완하고 사이버 방첩의 효율성을 극대화할 수 있다. 방위산업 공급망은 수많은 협력업체와 다단계 구조로 이루어져 있어, 데이터의 단편화와 불확실성이 높으며, 각 참여자 간의 신뢰 부족은 정보 공유를 저해하고, 위협 탐지 및 대응의 지연을 초래한다. 블록체인은 모든 참여자가 공유하고 검증할 수 있는 '단일 진실 공급원'을 제공하여 데이터의 정확성과 투명성을 높이며, 데이터가 한 번 기록되면 변경할 수 없어(불변성) 공급망 내 모든 거래 및 정보의 무결성을 보장하고, 문제가 발생했을 때 원인을 정확히 추적할 수 있다. 또한, 암호화 및 탈중앙화 특성을 통해 민감한 위협 정보를 안전하게 공유하면서도, 필요에 따라 프라이버시를 보호하는 메커니즘을 구현할 수 있으며, 스마트 계약 등을 통해 조달 및 물류 프로세스를 자동화하여 효율성을 높이고 인적 오류를 줄일 수 있다. 따라서 블록체인은 방위산업의 공급망 보안을 획기적으로 강화하고, 위협 정보 공유의 신뢰성과 효율성을 높여 사이버 방첩 역량을 한 단계 끌어올릴 수 있는 핵심 기술로, 시범 프로젝트를 통해 적용 가능성을 적극적으로 모색해야 한다.

4.4. 국제 사이버 방첩 공조체계 구축

방위산업의 전략 자산이 글로벌 방산시장과 연동되어 있는 만큼, 사이버 방첩 역시 국제 정보 공조 체계와 연계된 다국적 대응력 확보가 필수적이다. 단순한 정보교류를 넘어 공동 위협 분석, 침투 탐지, 공격자 그룹 식별, 국제 수사 공조 등의 협력 체계가 필요하다.

미국, 이스라엘, 영국 등 주요 우방국과의 정례 협의체 구성을 통해 방산 분야 사이버 위협 관련 실시간 분석과 공동 대응 전략 설계를 논의하고, NATO, INTERPOL 등과의 연계를 통해 공격자 식별과 추적이 가능한 수준으로 협력을 고도화해야 한다. NATO의 JISR(Joint Intelligence, Surveillance and Reconnaissance) 시스템은 정보 및 인텔리전스를 의사 결정자에게 제공하여 상황 인식을 개선하며, 동맹국 간 '알아야 할 필요성(need to know)' 개념을 넘어 '공유할 책임(responsibility to share)' 개념을 지지한다. 유럽연합(EU)은 2024년 12월 사이버 연대법(Cyber Solidarity Act)을 채택하여 국경 간 사고 대응을 위한 법적 프레임워크를 마련하고, 유럽 사이버 비상 메커니즘을 설립하여 대규모 사이버 공격 대응 능력을 강화하고 있다. 또한, 정보 공유 및 분석 센터(ISACs)와 같은 공유 커뮤니티를 통해 산업계 동료, 공급업체, 고객 간의 양방향 위협 인텔리전스 공유가 가능하며, 이는 민간-공공 보안 협력을 가능하게 한다. 이와 같이 위협 인텔리전스 공유는 조직이 잠재적 또는 진행 중인 사이버 위협에 대한 정보를 교환하여 집단 방어를 강화하는 과정이다.

NATO, INTERPOL 등 다자간 협력 네트워크 확장 및 공동 대응 전략 수립도 중요하다. INTERPOL은 'Operation Secure'를 통해 26개국 법 집행 기관과 협력하여 2만 개 이상의 악성 IP 주소 및 도메인을 차단하고, 32명의 용의자를 체포하는 등 사이버 범죄 인프라에 대한 성공적인 작전을 수행했다. 이는 민간 부문 파트너(Group-IB, Kaspersky, Trend Micro)와의 협력을 통해 이루어졌다. Five Eyes(미국, 영국, 캐나다, 호주, 뉴질랜드)는 세계에서 가장 발전된 정보 공유 파트너십 중 하나로, 신호 정보(SIGINT)를 넘어 군사 정보(MILINT), 인적 정보(HUMINT), 지리공간 정보(GEOINT) 등 다양한 정보 공유를 포함한다. 이 외에도 Club de Berne, Maximator, Colombo Security Conclave 등 다양한 다자간 정보 동맹이 존재하며, 이들은 사이버보안 및 방첩 노력을 조율한다. 한국은 2013년 제3차 GCCS(글로벌 사이버 공간 총회)를 개최하고 COC(사이버 행동 강령) 가입을 추진하는 등 국제 사회의 사이버 규범 수립에 적극 참여하고 있다.

방위산업의 사이버안보를 위한 국제 공조는 단순한 국가 간의 정보 공유를 포함하여 공동 위협 분석 및 대응 작전, 그리고 사이버 공간에서의 책임 있는 국가 행동 규범을 형성하는 외교적 노력까지 포괄하는 다층적 접근이 필요하다. 사이버 위협은 국경을 초월하며, 특정 국가나 산업에만 국한되지 않는 글로벌한 특성을 가진다. 방위산업은 글로벌 공급망과 수출 시장을 가지고 있어 국제 공조가 필수적이다. NATO의 '공유할 책임' 개념은 기존의 수동적 정보 공유를 넘어선 능동적이고 광범위한 정보 공유를 지향하며, 이는 위협 탐지 및 대응 속도를 획기적으로 향상 시킬 수 있다. 다자간 협력의 성공 사례인 INTERPOL의 'Operation Secure'는 민간 기업과의 협력을 통해 악성 인프라를 성공적으로 제거한 사례로, 이는 민간 부문의 위협 인텔리전스 역량 활용의 중요성을 보여준다. 또한 북한 등 고위험 국가를 대상으로 한 사이버 억제 외교를 통해 사이버 첩보 행위에 대한 국제적 규탄과 제재를 제도화함으로써, 방첩 작전의 효과를 외교적 · 법적 차원으로 확장해야 한다.

이상에서 제시한 제도적 과제는 기존의 기술 보안 중심 체계에서 벗어나, 사이버 방첩이라는 전략적 관점에서 법과 제도를 재설계하는 패러다임 전환을 지향한다. 단편적인 보안 강화가 아닌, 적의 정보수집 활동을 무력화하는 전략적 사고와 조직, 기술, 법제, 외교가 통합된 전방위 방첩 체계가 구축되어야만 방위산업의 지속 가능한 경쟁력 확보가 가능할 것이다.

5. 결론

글로벌 방위산업시장에서 주목받고 있는 방위산업은 그 성장과 함께 증가하는 사이버 위협이라는 양면성에 직면해 있다. 첨단 무기체계와 핵심 기술을 노리는 사이버 공격은 날로 정교해지고 조

직화 되어 우리의 취약점을 파고들고 있다. 본 연구는 이러한 도전에 대응하기 위해 사이버 방첩 전략의 중요성을 강조하고, 한국의 현행 대응체계를 분석하며, 해외 사례 분석을 통해 제도적 개선 방안을 제시하였다.

최근 연구 결과, 한국 방위산업의 사이버 위협 대응에는 "방어 중심에서 방어+능동 대응의 복합 전략"으로의 패러다임 전환이 필요함을 확인하였다. 기존의 수동적 사이버보안 조치만으로는 지능적 지속 위협(APT)에 효과적으로 대응하기 어려우며, 탐지-기만-차단-격퇴의 전 주기적 능동 방첩 전략이 요구된다.

이를 실현하기 위해 다음과 같은 제도적 혁신이 필요하다: 첫째, 방산 보안과 방첩을 아우르는 통합 거버넌스 체계 구축, 둘째, 정부-기업 간 실시간 정보 공유 체계 활성화, 셋째, 보안 인증제를 통한 산업계 전반의 방어역량 강화, 넷째, 사이버 기만 기술과 위협 정보 분석 등 능동적 대응 역량 배양, 다섯째, 국제 공조 체계 강화. 이러한 과제들의 공통 목표는 국가와 산업, 민 · 관이 경계를 넘어 '방위산업 원팀(One Team)'으로 협력하는 사이버안보 생태계 구축이다.

국정원이 2024 방산 안보 국제컨퍼런스에서 "우리 기업의 든든한 도우미이자 방산 안보 수호하는 지킴이" 역할 수행을 천명하고, 방산기업들이 "세계 4대 방산 수출국 도약을 위한 핵심 기술 보호와 정보 유출 방지" 의지를 다진 것은 이러한 협력의 가능성을 보여준다. 공공부문과 민간 부문의 인식 일치와 협력 강화가 이루어질 때 사이버 방첩 체계의 실효성이 확보될 것이다.

본 연구의 한계로는 사이버 방첩의 전문성과 기술적 복잡성으로 인해 제도적 제언의 구체적 실행 방안에 대한 추가 연구가 필요하다는 점이다. 특히 사이버 기만 기술 도입의 법적 쟁점, 정보 공유 과정의 프라이버시 문제, 국제공조의 현실적 제약 등에 대한 심층 연구가 요구된다. 또한 AI 등 신기술이 공격과 방어에 동시 활용되는 환경 변화에 따른 지속적 전략 보완이 필수적이다.

그럼에도 사이버 공간에서의 방첩 역량 강화는 더 이상 선택이 아닌 필수 사항이다. 방위산업은 국가안보의 중추이자 경제성장의 동력으로서, 첨단기술 유출은 단순한 기업 손실을 넘어 국가 전략의 근간을 흔드는 결과를 초래한다. "기밀을 지키는 자가 승리한다"는 정보전의 원칙은 사이버 시대에도 여전히 유효하다.

방위산업의 지속적 성장을 위해서는 보이지 않는 사이버 전쟁에서의 우위 확보가 전제되어야 한다. 본 연구가 제시한 사이버 방첩 전략과 제도적 과제들이 산 · 학 · 연 · 관의 지속적 협력을 통해 구현된다면, 한국 방위산업은 사이버 공간에서 견고한 방패와 예리한 감시 체계를 동시에 갖추게 될 것이다. 이는 사이버안보가 곧 국가 경쟁력인 시대에 대한민국의 안보와 번영을 지키는 핵심 기반이 될 것이다.

향후 연구에서는 본 연구에서 제시한 제도적 과제들의 구체적 실행 방안과 단계별 로드맵 수립, 그리고 AI 시대에 적합한 차세대 사이버 방첩 기술 개발 방향에 대한 심화 연구가 필요할 것이다. 또한 국제 공조 체계의 실질적 운영 방안과 법적 기반 마련에 대한 후속 연구를 통해 방위산업 사이버 방첩 체계의 완성도를 높여나가야 할 것이다.

참고문헌

[1] 보안뉴스. 라자루스·안다리엘·김수키…北 해커조직 총동원…국내 방산업체 83곳 공격해 10여곳 해킹. https://www.boannews.com/media/view.asp?idx=124567 (검색일 2025. 6.25).

[2] MarketsandMarkets. Military Cybersecurity Market by Offering (Solutions, Services), Security Type (Network, Endpoint, Application, Cloud, Data, Others), Deployment Mode (On-premises, Cloud), Application, and Region - Global Forecast to 2033. 2023.

[3] 류연승. 방산보안 2.0. 정보보호학회지, 제28권 제6호, pp. 6-12. 2018.

[4] 방위사업청, 방위사업청 2023년도 방위산업기술보호 시행계획 수립 [보도자료]. https://www.korea.kr/briefing/pressReleaseView.do?newsId=156543914 (검색일 2025. 6. 25).

[5] 국가정보원. 국정원, 2024 방산안보 국제컨퍼런스 개최 [보도자료]. https://www.nis.go.kr/CM/1_4/view.do?seq=316 (검색일 2025. 6. 25).

[6] Prunckun, H. Counterintelligence theory and practice (2nd ed.). Rowman & Littlefield (2019).

[7] T. Duvenage et al. Cyber counterintelligence: Defending against espionage in the digital age. Intelligence and National Security, Vol. 35, No. 4, pp. 501-517. 2020.

[8] Defense Counterintelligence and Security Agency (DCSA), U.S. Department of Defense. DCSA Strategic Plan 2022-2027, 2022

[9] 박은열. 방산안보 연구의 한계에 관한 고찰: 국가정보학의 정보수집 및 분석, 방첩의 관점에서. 방산안보연구, 제1권 제1호, pp. 1-17. 2025.

[10] Center for Development of Security Excellence (CDSE). Artificial intelligence and counterintelligence considerations job aid. 2025

[11] 정태진. AI 를 이용한 사이버 위협의 해외사례 분석 및 시사점 연구. 융합보안논문지, 제24권 제5호, pp. 123-136. 2024.

[12] 한국인터넷진흥원. 2024 하반기 사이버 위협 동향 보고서. 2025.

[13] 국가안보전략연구원. 김정은시대 북한의 사이버위협과 주요 대응. 2021.

[14] 경찰청. 경찰청 · 방위사업청 등 관계기관 합동 특별점검을 통해 북한의 케이(K)-방산업체 해킹 공격 규명 및 보호조치 실시 [보도자료]. https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1002&q_bbscttSn=20240423132830276&utm_source=chatgpt.com (검색일 2025 6. 25).

[15] 과학기술정보통신부. 2024년 사이버위협 사례 분석 및 2025년 전망 발표: 생성형 인공지능 악용, 디지털 융복합 확산에 따른 사이버위협 증가 [보도자료]. https://www.msit.go.kr/bbs/view.do?sCode=user&nttSeqNo=3185279 (검색일 2025 7. 2).

[16] 뉴시스. '방산 협력사에 해킹 시도' 5년 사이 최대…"보안책 절실". https://www.newsis.com/view/NISX20241015_0002920926 (검색일 2025. 6. 25).

[17] 송경석. 미국 FBI의 방첩정책 연구. 국가정보연구, 제12권 제1호, pp. 103-140. 2019.

[18] 원동훈 등. 美 CMMC 제도와 한국 방산보안 대응방안. 국방과 보안, 제5권 제1호, pp. 68-93. 2023.

[19] Barbour, D. Top 10 CMMC compliance pitfalls and how to avoid them. Kiteworks. https://www.kiteworks.com/cmmc-compliance/top-10-pitfalls/ (검색일 2025. 7. 2).

[20] 전자신문. [창간 35주년 특집]사이버 보안 강국을 가다〈하〉이스라엘, 폭넓은 '보안 생태계' 구축. https://www.etnews.com/20170918000377 (검색일 2025. 6. 25).

[21] Center for Security Studies (CSS), ETH Zurich. Israel's national cybersecurity and cyberdefense posture. 2020.

[22] 앤소니 온체 등. 사이버수사에서 귀속문제 의사결정을 위한 공개출처정보 처리 자동화. 디지털포렌식연구, 제15권 제2호, pp. 86-98. 2021.

[23] 국가안보전략연구원. 영국「국가사이버전략 2022」의 특징과 시사점. 2022.

[24] 양천수, 김중길. 독일의 사이버 보안법: 정책 · 거버넌스 · 법률. 법제연구, 56호, pp. 53-84. 2019.

[25] 박우경, 정호경. 프랑스 사이버안보 법제 — 정보시스템 보호 관련 논의를 중심으로 —. 법학논총, 제36권 제4호, pp. 31-52. 2019.

[26] Rostrum Legal. (n.d.). International law and cyber warfare. https://www.rostrumlegal.com/international-law-and-cyber-warfare (검색일 2025. 7. 14).

[27] 조수영. 개인정보보호법과 EU 의 GDPR 에서의 프라이버시 보호에 관한 연구. 법학논고, 61호, pp. 117-148. 2018.

[28] Airforce Technology. UK urged to set up Counter-Intelligence Unit for defence. (2025, June 6). https://www.airforce-technology.com/news/uk-urged-to-set-up-counter-intelligence-unit-for-defence/ (검색일 2025. 7. 14).