박사학위청구논문

2023학년도

인공지능을 활용한 방위사업 보호방안 연구

- 산업보안 및 기술보호 중점으로 -

A study for the protection measure of defense acquisition program using artificial intelligence

- Regarding industrial security and technology protection -

광운대학교 대학원

방위사업학과

정 웅 규

인공지능을 활용한 방위사업 보호방안 연구

- 산업보안 및 기술보호 중점으로 -

A study for the protection measure of defense acquisition program using artificial intelligence

- Regarding industrial security and technology protection -

광운대학교 대학원

방위사업학과

정 웅 규

인공지능을 활용한 방위사업 보호방안 연구

- 산업보안 및 기술보호 중점으로 -

A study for the protection measure of defense acquisition program using artificial intelligence

- Regarding industrial security and technology protection -

김 도 영 지도교수

이 논문을 경영학 박사학위논문으로 제출함

2023년 6월 일

광운대학교 대학원

방위사업학과

정 웅 규

정웅규의 경영학 박사 학위논문을 인준함

심사위원장 _____ 인

심사위원 _____ 인

심사위원 _____ 인

심사위원 _____ 인

심사위원 _____ 인

광운대학교 대학원

2023년 6월 일

감사의 글

논문을 작성하다 창밖을 보며 지난 7년간의 박사학위과정을 생각해 봅니다. 혼자서 '박사 졸업을 목표로 하고 노력해야지'라는 마음가짐은 항상 있었지만 쉽지가 않았습니다. 일과 학업을 동시에 진행하면서 힘들고 지친 적도 있었지만, 주변의 도움으로 어려운 시기를 극복하고 이겨낼 수 있었습니다. 좋은 성과를 이룰 수 있게 기여해주신 모든 분들께 진심으로 감사의 말씀을 드리고 싶습니다.

먼저, 부족한 논문을 지도해주시고 항상 여유로운 미소로 격려 해주신 김도영 지도교수님께 깊은 감사를 드립니다. 교수님의 지도제자가 될 수 있었던 것부터 저에게는 큰 행운이었습니다. 지도제자로 흔쾌히 승낙해주신 점부터 졸업까지 꼼꼼히 보살펴주신 점에 대해 잊지 못할 은혜입니다.

또한, 바쁘신 와중에도 꼼꼼하게 논문을 보완하도록 도와주시고 졸업을 할 수 있게 조력해주신 정형원 교수님, 최진주 교수님, 강구민 교수님, 이재환 박사님께도 깊은 감사의 말씀을 올립니다. 교수님 및 박사님 덕분에 논문이 한층 발전하는 것을 볼 수 있었습니다. 그리고 인생 및 군 생활의 선배로서 가치 있는 대학원 생활을 함께해주신 방위사업학과 19기 원우님들께도 감사의 인사를 전합니다. 함께한 원우님들이 없었다면 이 자리까지 올 수 없었을 것입니다.

논문 작성간 많은 도움을 주신 김도우・엄유진・이가은 박사님께도 머리 숙여 감사드립니다. 꼼꼼한 교정을 통해 성공적인 논문이 될 수 있었던 공신입니다.

마지막으로 논문이 완성되기까지 육아와 집안일을 도맡으며 적극적으로 도와준 사랑하는 아내 진아에게도 감사와 사랑을 전합니다. 제 아내는 저보다 먼저 동국대 박사를 졸업하여 직접적인 조력자로 저를 도와주었습니다. 바쁜 일정에도 불구하고 즐겁고 이쁘게 성장해준 아들 이도에게도 고마움을 전합니다. 이외에도 직・간접적으로 관여해주신 모든분에게 감사드립니다.

국문 요약

인공지능을 활용한 방위사업 보호방안 연구
- 산업보안 및 기술보호 중점으로 -

세계적으로 국가별 주권강화를 위한 군비경쟁은 지속되고 있다. 4차 산업혁명 시대가 도래하면서 인공지능 등 진화된 기술을 방위사업에 적용하여 새로운 무기체계를 개발하고 있다. 이에 따라 국가간의 해킹 및 침해기술을 이용하여 선진국의 기술을 불법적으로 획득하려는 행위도 증가하고 있는 추세다. 그리고, 축척되는 데이터 급증과 이를 효율적으로 활용하기 위한 인공지능 기술 도입의 필요성은 높아지고 있다.

특히, 방위사업 분야에 축척되어 있는 데이터와 상호 전송간에 발생할 수 있는 데이터의 유출은 국가차원의 손해가 크며, 국가안보에도 위협이 될 수 있는 요소가 된다. 이것은 방위사업에서도 산업보안 및 기술보호가 중요해지고 있음을 의미한다.

이와 관련한 선행연구 분석결과 무기체계에 인공지능 적용을 통해 군비 증강에 대한 연구는 다수 있으나, 이를 뒷받침할 수 있는 방위사업 기술보호와 관련된 논문은 찾아보기 어려웠다. 그 결과, 인공지능을 활용한 방위사업 기술보호에 대한 연구 보완이 필요하다는 것을 알 수 있었다.

본 연구는 대한민국이 직면하고 있는 세계적 정세와 국내·외 인공지능 기술에 대해 분석하고 기존 방위사업에서 운용되는 보안관리체계가 향후 인공지능 기반의 방위사업이 적용되었을 경우 어떻게 발전해야하는지 방향성에 대해 연구해보았다.

4차 산업 혁명의 기반은 빅데이터와 인공지능이다. 빅데이터는 인공지능이 운용되는 원천이자 자원이고 인공지능은 빅데이터를 자동으로 분석 및 판단하는 기술이다. 4차 산업혁명은 인공지능으로 빅데이터를 처리하여 원하는 판단 결과를 얻고 이를 방위사업에 적용하여 국방에서 필요하는 무기체계를 생산하고 국방 획득체계의 효율을 높이는 분야로도 활용할 수

있다. 예를 들어, 3차 산업혁명 단계에서 방위사업 종사자가 자신의 업무를 위한 정보에 대해 검색과 저장, 처리를 수행했다면, 4차 산업혁명에서는 인공지능이 제공하는 판단 내용을 참고하여 결심을 하거나, 일부는 판단을 인공지능이 대체하도록 될 것이다. 이렇게 4차 산업혁명으로 인공지능이 국방분야 전반에 활용될 것으로 예상됨에 따라 발생할 수 있는 문제점과 인공지능의 보안취약점에 대해 중요성이 높아지고 있다.

보안취약에 따른 사고를 예방하기 위해서는 현재 적용중인 국방보안시스템이 인공지능 기술이 도입되었을 경우 발생할 수 있는 문제점을 분석해보면 사람에 의한 보안 취약점, 딥페이크, 스팸 및 피싱, 퍼징 등을 통한 사이버 상의 약점이 대표적이었으며, 이를 고려하여 인공지능 기반의 방위사업에 적합한 기술보호 방안을 모색하고 적용할 수 있는 방안이 필요할 것으로 판단되었다. 인공지능 기술이 각 분야에 도입되면 취약점을 이용한 내·외부 침해 시도도 빈번히 발생할 것으로 예상된다. 현재까지 인공지능이 도입되어 운용되는 무기체계가 없기 때문에 연구 과정에 있는 내용 외에 인공지능을 활용한 실제 침해공격이 발생한 사례는 거의 보고되고 있지 않다. 그래서 해외에서 발생하는 침해공격과 사례 등을 바탕으로 분석하였다. 현재에도 방위사업청과 방위사업체에 대한 침해공격은 지속적으로 증가하고 있으며 침해공격 기술은 고도화 되고 있다. 취약점을 보완하는 기술이나 방법도 가시적으로 국내에서 진전되고 있지 않기 때문에 해외 사례를 참고하였다.

현재까지 발생한 문제점과 예상되는 인공지능 기반 방위사업 취약점 분석을 바탕으로 기술보호 방안을 연구한 결과 개인·기업의 보안인증제도, 교육프로그램, 시스템 및 사이버 보호방안에 대해 연구하여 대안을 찾아볼 수 있었으며, 세부적으로 (가칭) ‘인공지능 방위사업 보안전문가’ 자격증, (가칭) ‘국방 인공지능 보안담당자 교육’ 프로그램, ‘프라이빗 블록체인’, ‘양자암호’, ‘인공지능 보안관제체계’에 적용 방안을 제시하였다. 특히, 인공지능은 사람이 실시간으로 관제하는 능력보다 패턴인식을 빠르고 정확하게 식별할 수 있다. 정상적인 알고리즘의 패턴과 비교하여 비정상적인 패턴이 식별되면 즉각적인 방어로 해킹과 기술유출을 보호할 수 있다.

본 연구내용은 인공지능 개발 단계에서부터 보안취약점을 대비할 수 있는 부분에 강점이 있다. 이외에도 다양한 단계에서 보안취약점이 발생 할 수 밖에 없을 것으로 예상된다. 인공지능 기술을 활용한 보안강화 대책 연구가 활발히 진행되길 바란다.

방위사업, 인공지능, 산업보안, 기술보호, 양자암호, 블록체인, 보안대책

ABSTRACT

A study for the protection measure of defense acquisition program using artificial intelligence

- Regarding industrial security and technology protection -

Jung, Ung Kyu

Dept. of defense acquisition program

The Graduate School

Kwangwoon University

The arms race to strengthen national sovereignty continues around the world. As the era of the 4th industrial revolution has arrived, new weapon systems are being developed by applying advanced technologies such as artificial intelligence to defense projects. Accordingly, the act of illegally obtaining technology from developed countries by using hacking and infringing technologies between countries is also on the rise. In addition, the need to introduce artificial intelligence technology to efficiently utilize the rapidly accumulating data is increasing.

In particular, data leakage that can occur between data accumulated in the defense business field and mutual transmission causes great damage at the national level and is a factor that can pose a threat to national security. This means that industrial security and technology protection are becoming more important in the defense industry.

As a result of the analysis of previous studies related to this, there are many studies on arms augmentation through the application of artificial intelligence to weapon systems, but it was difficult to find papers related to defense technology protection that can

support this. As a result, it was found that it is necessary to supplement research on defense business technology protection using artificial intelligence.

This study analyzed the global situation facing Korea and domestic and foreign artificial intelligence technologies, and studied the direction of how the security management system operated in the existing defense business should develop if the future AI-based defense business is applied. .

The basis of the 4th industrial revolution is big data and artificial intelligence. Big data is the source and resource for which artificial intelligence operates, and artificial intelligence is a technology that automatically analyzes and judges big data. The 4th Industrial Revolution can process big data with artificial intelligence to obtain desired judgment results and apply it to defense projects to produce weapon systems necessary for national defense and to improve the efficiency of defense acquisition systems. For example, in the 3rd industrial revolution stage, if defense workers searched, stored, and processed information for their work, in the 4th industrial revolution, decisions were made by referring to the judgment provided by artificial intelligence, Some will be replaced by artificial intelligence for judgment. As artificial intelligence is expected to be used throughout the defense sector due to the 4th industrial revolution, the importance of problems that may arise and security vulnerabilities of artificial intelligence is increasing.

In order to prevent accidents due to security vulnerabilities, analysis of problems that may occur when artificial intelligence technology is introduced into the currently applied national defense security system reveals cyber security vulnerabilities caused by humans, deepfakes, spam and phishing, fuzzing, etc. Weaknesses were representative, and considering them, we proposed ways to seek and apply technology protection measures suitable for AI-based defense projects. When artificial intelligence technology is introduced in each field, internal and external infringement attempts using vulnerabilities are expected to occur frequently. Since there is no weapon system in which artificial intelligence has been introduced and operated so far, there have been few reports of actual infringement attacks using artificial intelligence other than those in the research process. Therefore, it was analyzed based on intrusion attacks and cases that occurred

abroad. Infringement attacks on the domestic Defense Acquisition Acquisition Program Administration and defense companies are continuously increasing and the technology is being advanced. In addition, foreign cases were referred to as technologies or methods to compensate for vulnerabilities were not visibly progressing in Korea.

As a result of research on technology protection measures based on the analysis of the problems that have occurred so far and the vulnerabilities of the expected artificial intelligence-based defense business, it is possible to find alternatives by studying security certification systems, educational programs, systems, and cyber protection measures for individuals and companies. In detail, (tentative name) 'artificial intelligence defense business security expert', (tentative name) 'defense artificial intelligence security officer training', 'private block chain', quantum cryptography, and proposals for application to 'artificial intelligence security control system' did In particular, artificial intelligence can identify patterns faster and more accurately than functions controlled by humans in real time. If an abnormal pattern is identified compared to the pattern of a normal algorithm, hacking and technology leakage can be protected with immediate defense.

The strength of this study is that it can prepare for security vulnerabilities from the AI development stage. In addition, many security vulnerabilities are expected to occur in the future. It is hoped that research on security reinforcement measures using artificial intelligence technology will be actively conducted.

---

sustinability of defense acquisition, artificial intelligence, industrial security, technology protection, quantum cryptography, blockchain, security measures

차 례

감사의 글 ····· i
국문 요약 ····· ii
영문 요약 ····· iv
차례 ····· vii
그림 차례 ····· viii
표 차례 ····· ix
제1장 서 론 ····· 1
1.1. 연구의 필요성과 목적 ····· 1
1.2. 연구의 방법과 범위 ····· 7
제2장 선행연구와 이론적 배경 ····· 10
2.1. 선행연구 ····· 10
2.2. 이론적 배경 ····· 12
2.3. 방위사업의 국가적 가치 ····· 20
2.3.1. 인공지능을 활용한 방위사업 현황 ····· 20
2.3.2. 대한민국 방위사업의 세계적 수준과 가치 ····· 33
2.4. 소 결 ····· 36
제3장 방위사업 보안 현황과 취약점 ····· 38
3.1. 현 방위사업 보안체계와 기술유출 ····· 37
3.2. 인공지능 기반 방위사업 보안취약점 ····· 45
3.3. 소 결 ····· 50
제4장 인공지능을 활용한 기술보호 및 보안강화 방안 ····· 51
4.1. 미국의 방위사업 보안 및 기술보호 강화 ····· 51
4.2. 방위사업 인공지능 보안 인증제도 ····· 56
4.3. 보안교육 프로그램 ····· 72
4.4. 방위사업 시스템 및 사이버 보안 ····· 77
4.5. 인공지능 활용 산업보안 및 기술보호 방안 검증 ····· 87
4.5.1. 1차 델파이 조사 결과 ····· 90
4.5.2. 2차 델파이 조사 결과 ····· 97
4.5.3. 인공지능 활용 방위사업 발전 요소 조사 결과 ····· 104
4.5.4. AHP 기법을 활용한 우선순위 도출 결과 ····· 106
4.6. 소 결 ····· 107
제5장 결 론 ····· 109
참고 문헌 ····· 112

그 림 차 례

그림 1. 방위사업보안과 산업보안의 상관 관계 · · · · · · · · · · · · · · · 14
그림 2. 4차 산업혁명의 발전 · 15
그림 3. 무기체계 획득 절차도 · 18
그림 4. 국방 인공지능 기능 발전단계 · · · · · · · · · · · · · · · · · · 24
그림 5. 대한민국 방산 수출 현황 · 34
그림 6. 대한민국 국방과학 기술 수준 · · · · · · · · · · · · · · · · · · 35
그림 7. 딥페이크를 활용한 사기 · 46
그림 8. 딥페이크를 이용해 재현한 이미지 · · · · · · · · · · · · · · · · 48
그림 9. 인공지능 관련 업체 및 자격·교육과정 · · · · · · · · · · · · · 57
그림 10. 인공지능 관련 국내 교육프로그램 · · · · · · · · · · · · · · · 75
그림 11. 인공지능기반 보안관제체계도 · · · · · · · · · · · · · · · · · 83
그림 12. 딥러닝에 사용되는 알고리즘 · · · · · · · · · · · · · · · · · · 84
그림 13. 인공지능 적대적 훈련 방법 · · · · · · · · · · · · · · · · · · 86

표 차 례

표 1. 연구 모형 · 9
표 2. 인공지능과 방위사업 관련 연구 · 10
표 3. 인공지능과 방위사업 관련 연구 요약 · · · · · · · · · · · · · · · · · · 12
표 4. 인공지능을 활용한 방위사업 분야 · · · · · · · · · · · · · · · · · · · 21
표 5. 인공지능 데이터의 분류와 회귀 · 22
표 6. 인공지능을 활용한 방위사업 국내 개발 현황 · · · · · · · · · · · · · · 26
표 7. 대한민국의 미국 대비 인공지능 수준 · · · · · · · · · · · · · · · · · · 27
표 8. 미군의 인공지능 기술 적용안 · 32
표 9. 방위사업 보안관리체계 · 37
표 10. 방산업체 보안요건 · 40
표 11. 방위사업 기술유출 유형 · 42
표 12. 2015년부터 2022년까지 기술 유출 현황 · · · · · · · · · · · · · · · · 43
표 13. 2015년부터 2022년까지 기술유출 관련자 현황 · · · · · · · · · · · · 43
표 14. 언론에 공개된 방위사업 기술유출 현황 · · · · · · · · · · · · · · · · 44
표 15 인공지능에 대한 보안 위협 종류 · · · · · · · · · · · · · · · · · · · 52
표 16. 선진국 업체들의 인공지능 보안 강화 추진 분야 · · · · · · · · · · · 54
표 17. 미국에서 운용중인 인공지능 자격증 · · · · · · · · · · · · · · · · · · 58
표 18. 미국의 보안인증 공인자격제도 · 59
표 19. 미국의 보안분야 자격제도 · 60
표 20. ISP 및 CPP 자격 인증 · 62
표 21. 국내 보안 관련 자격증 · 63
표 22. (가칭) 인공지능 방위사업 보안전문가(안) · · · · · · · · · · · · · · · 64

표 23. CMMC 등급별 내용 및 심사 주관 · · · · · · · · · · · · · · · · · · · 66
표 24. CMMC 등급별 내용 · 67
표 25. 방산기술보호 점검분야별 점검지표 · · · · · · · · · · · · · · · · · 68
표 26. CMMC와 통합실태조사 비교시 부족한 항목 · · · · · · · · · · · · · 70
표 27. 인공지능 유형별 교육대상과 역할 · · · · · · · · · · · · · · · · · · 73
표 28. 인공지능 역량 구분 · 74
표 29. (가칭) '국방 인공지능 보안 담당자' 교육 프로그램(안) · · · · · · · 76
표 30. 블록체인의 주요 특징 · 79
표 31. 양자암호의 주요 특징 · 81
표 32. 델파이 조사 패널 현황(20명) · 88
표 33. 1차 델파이 조사 결과 <인공지능 적용> · · · · · · · · · · · · · · · 91
표 34. 1차 델파이 조사 결과 <방위사업 기술유출 원인> · · · · · · · · · · 92
표 35. 1차 델파이 조사 결과 <산업보안 및 기술보호 취약점> · · · · · · · 93
표 36. 1차 델파이 조사 결과 <방위사업 시스템 및 사이버 보안> · · · · · 94
표 37. 1차 델파이 조사 결과 <방위사업 보안 인증제도> · · · · · · · · · · 95
표 38. 1차 델파이 조사 결과 <보안교육 프로그램> · · · · · · · · · · · · · 96
표 39. 1차 델파이 조사 삭제 및 추가 항목 · · · · · · · · · · · · · · · · · 97
표 40. 2차 델파이 조사 결과 <인공지능 적용> · · · · · · · · · · · · · · · 98
표 41. 2차 델파이 조사 결과 <방위사업 기술유출 원인> · · · · · · · · · · 99
표 42. 2차 델파이 조사 결과 <방위사업 기술유출 취약점> · · · · · · · · · 100
표 43. 2차 델파이 조사 결과 <방위사업 시스템 및 사이버 보안> · · · · · 101
표 44. 2차 델파이 조사 결과 <방위사업 보안 인증제도> · · · · · · · · · · 102
표 45. 2차 델파이 조사 결과 <보안교육 프로그램> · · · · · · · · · · · · · 103
표 46. 인공지능 활용 방위사업 발전 요소 조사 결과 · · · · · · · · · · · · 104
표 47. AHP분석을 통한 중분류 우선순위 도출 결과 · · · · · · · · · · · · 106

Ⅰ. 서론

1.1. 연구의 필요성과 목적

최근 국제적인 군비경쟁 속에서 각 국가는 자국의 입지를 강화하기 위해 지속 노력하고 있다. 세계속에서 주도권을 강화하기 위해 인공지능을 포함한 첨단 기술 개발을 통해 무기체계를 개발하고 상대가 대응하기 어려운 무기체계를 연구하는 등 방위사업 활성화를 위해 노력하는 모습을 주변국의 사례에서 쉽게 살펴 볼 수 있다. 우크라이나와 러시아의 전쟁, 중국과 대만의 전쟁 분위기 고조, 일본 등 주변 국가의 군비경쟁으로 4차 산업혁명 기술을 활용한 첨단무기의 출현, 북한의 지속적인 미사일 및 무인기 도발 등 복합적인 상황이 우리나라에 영향을 주고 있다.

러시아는 우크라이나 무력 침공 이전부터 사람들과 밀접하게 연결되어 있는 스마트폰・영상매체・컴퓨터 등의 취약점을 활용하여 개인정보를 수집하고 해당 국가에서 건설하고자 하는 이상적인 모습을 전송하여 사람들을 현혹 시키는 활동을 수행하는 등 사이버전, 여론전, 심리전, 기만전을 펼치고 있다. 이를 이해하기 쉬운 말로 하면, 물리적인 전쟁만이 아니라 보이지 않는 부분에서 함께 전쟁을 수행하는 하이브리드 전쟁이 진행중인 것이다. 이는 사람들의 심리를 서서히 동화시켜 나가는 행동을 의미한다. 예로, 스마트폰을 통해 러시아가 추구하는 모습을 인식하게 만들고, 러시아 국가의 통치를 받았을 때 발생하는 이점들을 다양한 사물인터넷 기기를 통해 사람들의 인지영역에 스며들며 서서히 신뢰하도록 하는 것이다.

또한, 러시아는 분산서비스거부[1] 공격을 포함한 전격적인 사이버 공격을 통해 우크라이나 지휘 통제체계를 마비시켜 초기 전장 주도권을 장악하고자 했다. 아울러 서방 우주정보 감시체계를 무력화하기 위한 위성위치확인시스템 재밍(GPS

1) 공격자가 한 지점에서 서비스 거부 공격을 수행하는 형태를 넘어 광범위한 네트워크를 이용하여 다수의 공격 지점에서 동시에 한곳을 공격하도록 하는 형태의 서비스 거부 공격

jamming)[2]과 수푸핑(Spoofing)[3] 등을 병행함으로써 수일 내 우크라이나 수도인 '키이우(Kyiv)'를 함락시켜 제2의 크림반도와 같은 합병을 도모했다.

상대가 대응하기 어려운 무기체계를 활용한 관련 사례는 우리나라와 가장 가까이 있는 북한에서 찾아볼 수 있다. 2022년 북한은 무인기 5대를 서울까지 이동시키는 과감한 도발을 시행하였다. 당시 육·공군은 헬기와 전투기를 이용하여 북한의 무인기를 격추시키기 위해 노력하였지만 1대의 무인기도 격추하지 못했다. 결국 우리나라의 대공망은 3m이하 크기의 무인기에 무방비가 된 상황이었다. 당시 각종 언론과 미디어에서는 군에 대해 많은 비판이 있었고 책임자를 처벌하자는 여론이 조성되고 있었다. 우리나라가 보유하고 있는 감시 및 타격 무기체계의 한계점을 인식하고, 이를 이용한 북한의 도발로 평가되고 있다.

3m 크기의 무인기는 1km 거리에서 보면 1cm 내외의 작은 크기로 보인다. 그리고 북한의 무인기가 맞는지 판단하기 위해서는 획득된 사진을 확대하여 사람의 분석과 판단이 들어가야 한다. 레이더에서 식별이 되고 그것을 확대하여 적기 여부를 판단하기 위해서는 많은 시간이 소요되는 것이 현실이다. 그리고 무인기는 대기의 영향을 많이 받는다. 그렇기에 공중에서 무인기를 격추하기 위해서는 바람의 방향과 속도를 계산하여 무인기 운동 방향을 계산한 다음 예측 사격을 해야 한다. 그렇기 때문에 사람의 예측만으로 사격한다면 격추하기 굉장히 어려울 수 밖에 없으며 상당한 시간이 소요될 수 밖에 없다.

주변국 및 적성국[4]들의 사이버·물리적 공격은 목적 달성을 위해 수시로 자행하고 있으며, 전시와 평시를 막론하고 전 세계적으로 빈번히 발생하고 있다. 미국 등

---

2) 위성 위치 확인 시스템(GPS)이 사용하는 주파수로 전파 방해(jamming, 재밍) 신호를 발사하여 GPS 수신을 방해하는 행위. 연속파(continuous wave) 형태나 펄스 형태의 재밍 신호를 방사함으로써 특정 주파수나 전파의 사용을 방해하는 교란 형태와 허위 정보를 전송하여 잘못된 위치나 시각 정보를 제공하는 방법 등이 있다.(한국정보통신기술협회)

3) 공격자가 네트워크, 웹사이트 등의 데이터 위변조를 통해 정상 시스템인 것처럼 위장하여 일반 사용자를 속이는 해킹 기법(IT 용어사전)

4) 적국 또는 가상 적국으로, 전쟁법규의 범위 안에서 군사적인 행위를 가해올 수 있는 국가(군사용어사전)

선진국들은 사이버·물리적 공격에 대응하기 위해 기존의 지상, 해상, 공중에서 펼쳐지는 전쟁을 우주와 사이버 공간까지 확대하는 다차원 전장에서의 무기체계 역량 강화를 강조하고 있다.

수년전부터 주변국은 방위사업과 관련된 공·사 업체를 대상으로 국내를 포함 각 국가를 대상으로 여러 차례 침해공격을 수행하였다. 우리가 개발한 무기체계 설계도면 유출을 유도하거나, 내부 인원들을 활용하여 타 국가에 불법 판매를 유도하는 사례들을 찾아 볼 수 있었다.

최근에는 사이버 해킹과 랜섬웨어(Ransomware)[5]와 같은 사이버 공격 등을 병행하여 침해공격 국가가 추구하는 방향으로 해당 국가들이 움직일 수 밖에 없도록 유도하고 있다. 이와 관련된 통계를 살펴보면 대한민국 방위사업청을 기준으로 해킹 시도가 2020년에는 3천여건, 2021년에는 4천3백여건, 2022년에는 5천여건으로 늘어나는 추세이다.[6] 무기체계에 대한 해킹 및 기술 유출은 상당한 국가적 경제적 손실을 가져올 뿐만 아니라, 유출된 설계도면으로 양산된 무기체계가 적성국의 소유물이 되어 도리어 대한민국을 겨냥할 수 있는 위험이 충분히 발생할 수 있으며 시대적 흐름에 따라 공격방법도 다양·고도화되고 있다.

제 3차 산업혁명 이후 더욱 치밀해지고 통합적으로 진화한 디지털 기술을 기초로 제 4차 산업혁명은 사회와 세계 경제, 문화의 변화를 주도하고 있다. 제 4차 산업혁명 시대는 고도화되어 있는 센서 및 네트워크 등을 통해 활용하는 모든 사물이 연결되는 초연결성의 특성을 가지고 있다. 각종 기기와 시스템을 연결하고 스마트하게 운용하는데 그치지 않고 재생가능 에너지, 나노기술, 퀀텀 컴퓨팅[7] 등 다양한 분야에서 운용되어 초지능성의 특징을 지닌 미래 사회로 발전하고 있다. 제

---

5) 랜섬웨어는 '몸값'(Ransom)과 '소프트웨어'(Software)의 합성어다. 시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 만든 뒤, 이를 인질로 금전을 요구하는 악성 프로그램을 의미(한국인터넷진흥원)

6) 매년 급증하는 방산업체 대상 해킹 공격… 사이버보안 필요성 극대화(IT BIZ NEWS), 22.11.04

7) 원자의 집합을 기억 소자로 간주하여 원자의 양자 역학적 효과를 기반으로 방대한 용량과 초병렬 계산이 동시에 가능한 컴퓨터.

4차 산업혁명 시대에는 사물인터넷(IOT), 빅데이터(Big Data), 클라우드(Cloud), 모바일(Mobile) 등의 신기술을 중심으로 기존의 전통적인 산업과 ICT[8]가 융합되어 새로운 가치를 지닌 서비스와 제품을 제공하는 산업이 융합되는 환경으로 변화하고 있다. 산업융합 환경에서는 혁신적인 일상이 일어나고 있으며, 산업 간의 경계가 허물어지고 새로운 사업 모델이 생겨나는 혁신이 활성화 되고 있다.

산업융합 환경에서는 산업의 융합으로 인한 파괴적 혁신이 일상화 되며 산업간의 경계가 해제되고 새로운 사업 모델이 출현하는 융합 혁신이 활성화 되고 있다. 의료산업, 금융산업, 물류산업 등 다양한 산업과 ICT가 융합되어 드론과 로봇이 네트워크에 연결되어 인간과 기계가 협력하는 높은 효율의 물류 시스템인 '스마트 물류', 일상의 소비생활 패턴 정보가 금융 네트워크에 연결되어 소비자 중심의 금융생활을 넘어 로봇 금융 전문가가 조언해주는 '스마트 금융', 환자와 의료진의 연결, 생체신호와 스마트폰과 같이 일상생활에서 활용하는 기계가 사용자와 연결되어 인공지능 판단에 의한 처방과 진료를 통해 치료하는 '스마트 헬스케어'와 같은 다양한 산업융합 사례가 보이고 있다. 산업융합 환경의 제품(Product)은 기존에 활용하고 있는 물품에서 ICT 기능을 내재화하여 새로운 형태와 기능을 가진 제품을 생산하고 생산 공정의 전반에는 ICT 기반 도구를 활용함으로써 기 운용하던 공정의 변화를 통해 실시간 생산성 향상 등 효율적인 성과를 거두고 있다.[9]

발전하는 산업융합 환경 속에서 발견되는 새로운 가치 및 자산을 보호하고 국가나 조직의 안정과 발전을 저해하는 사이버・물리적 일부 요소로 보안(Security)은 필수적인 요소가 될 수 밖에 없다. 제 4차 산업혁명 시대의 4대 주요 기술로 강조되는 것은 ICBM(사물인터넷・클라우드・빅데이터・모바일)이다. 그리고 보안 개념을 추가하여 ICBMS로 명시되기도 한다. 특히, ICT가 접목된 산업융합 환경에서

8) 정보 기술(Information Technology, IT과 통신 기술(Communication Technology, CT)의 합성어로 정보기기의 하드웨어 및 이들 기기의 운영 및 정보 관리에 필요한 소프트웨어 기술과 이들 기술을 이용하여 정보를 수집, 생산, 가공, 보존, 전달, 활용하는 모든 방법을 의미

9) 우광제, "융합보안전문가의 핵심과업 및 직무역량", 중앙대학교, (2015.)

는 생산 공정상에 침해공격으로 인한 내부정보 유출 발생이나, 사물인터넷 제품들과 같이 ICT 기능이 내재되어 있는 제품에 대해 불순분자의 침입 등 네트워크를 통한 외부 침해공격이 발생하는 등 기존 전통적인 산업에 비해 새로운 보안 위험이 나타나고 있는 것이 현실이다.

보안위험에 대한 기술적인 취약점을 이용하여 발생하는 정보유출, 사기, 물리적 절도, 저작권 침해 등 물리적 및 관리적 취약점이 동시에 발생하는 융복합적인 보안위험이 나타나는 양상이다. 발전하는 환경 속에서 융복합적으로 발생하는 보안 침해공격에 대응하기 위해서는 기술적 보안 대책이나 물리적, 관리적 보안 대책 중 하나에만 치우친 단편적인 보안 방안은 한계점이 드러날 수 밖에 없다. 관리적 역량을 가지고 물리적, 기술적 침해행위에 대해 융복합적으로 대응하며 다각도로 보안침해공격 대응이 필요한 시대가 다가오고 있다.

4차 산업혁명 시대에는 방위사업도 발전하고 있다. 위에서 언급한 사회의 발전과 함께 인공지능 등을 활용한 방위사업 발전도 진행중이다. 2022년 육군사관학교에서 '인공지능 강군으로 변혁을 위한 인공지능 학습데이터 증강방안에 대한 연구' 제하로 연구 발표를 하였다. 해당 내용에는 군사용 위성인 SAR를 이용하여 적 장비에 대한 수천장의 이미지를 수집하고 이를 데이터화 하여 향후 피아식별 판단이 필요한 적 영상 정보의 분석을 통해 기존에 구축해놓은 적 장비 수천장 이미지와 비교하여 적 장비 성질 판단 후 군 결정권자에게 제공하는 미래지향적 기술을 보여주었다. SAR를 통해 입수된 사진은 고배율로 확대되기 때문에 사람이 판단하기에는 다소 어려운 면이 있다. 물론 해상도가 월등히 우수하여 사람의 인지능력으로도 구분할 수 있다면 가장 좋은 방법이지만, 우주에서부터 확대하는 사물의 사진을 고 해상도로 보기에는 아직 기술력이 부족하다. 그러나 인공지능은 해상도가 낮은 이미지를 수천장 수만장의 사진과 비교하여 표적의 성질을 분석하여 정확도가 높은 정보를 제공해 줄 수 있다.

인공지능 기술은 사진상 1cm 이내 크기의 무인기를 보고 적기 여부를 판단하는

데 이용할 수 있다. 수많은 데이터들을 활용하여 북한 무인기의 뒷부분만 보아도 형태와 종류를 판단할 수 있다는 것이다. 신속한 무인기의 성질을 판단을 통해 성능과 바람의 방향 및 속도를 계산하여 실시간으로 사격할 수 있는 시스템이 도입되어야 할 수 밖에 없는 환경이다. 인공지능 기술은 시간이 흐를수록 대한민국 방위사업에서 가치가 높은 분야로 발전할 수 밖에 없다.

방위사업에 적용될 인공지능 핵심기술이 유출되면 국가에 미치는 피해는 매우 클 것으로 예상된다. 그렇기 때문에 보안관리체계 보완 대책도 강구되어야 한다. 기술유출과 해킹 공격 피해 최소화를 위해서는 시대적 흐름에 맞는 보안관리체계를 구축하는 것이 필요하다. 예를 들어, 사이버 무기체계를 포함한 방위사업 보안산업 역량을 갖추어야 한다. 국내 민간 보안산업은 최근 2018년도부터 연간 평균 12.3% 성장하여 2020년 3조 9000억원의 시장을 만들고 있다. 반면, 방위사업 보안 관련 예산은 2020년 283억원 규모로 국내 전체 보안산업과 비교하면 0.7% 수준에 불과하다. 특히, 2021년 방위사업청이 진행하였던 무기체계 개발과 관련하여 방위력개선사업 약 11조 9000억원(162개 사업)중에서 보안분야 사업예산은 거의 찾아보기 어려운 것이 현실이다.[10)]

예산과 더불어 우리나라는 내부적으로 '인구절벽'이라는 문제점이 대두되고 있다. 이로 인해 인력에 의한 보안은 한계점이 발생할 수 밖에 없다. 그래서 기술유출 및 해킹을 예방하기 위해서는 사물인터넷 기반의 무인화가 필요하며 이를 해결할 수 있는 방안으로 인공지능이 대두되고 있다. 현재 방위사업은 인구절벽에 대비하여 인공지능 도입을 통한 무인 전력 확충의 중요성을 강조하고 있다. 대한민국의 남성 중 군에서 근무할 수 있는 가용 나이대의 인구[11)]에서 군에서 활용할 수 있는 인원은 2022년 25.7만명이다. 그러나 2038년이 되는 시기에는 인구가 2022년 대비 37%가 감소한 16.1만명만 가능한 인구절벽의 문제가 다가오고 있다. 그렇다

10) 국방백서, "방위력개선 분야 국방예산 편성", (2022.)
11) 20세 남자인구기준(행정안전부)

면 2022년 기준 군의 구성원 비율처럼 간부 20.2만명, 병 29.8만명을 유지할 수 있는지도 생각해볼 문제이다. 군무원과 중견간부의 자리를 늘려 군의 현재 구성을 유지하는 방법도 있지만 국가 경제를 위해 일할 수 있는 인구는 충분한지 생각해 보아야 한다. 군에서 많은 인구를 활용하면 나라의 경제는 발전할 수 없다. 그렇기에 결국 군이 선택할 수 있는 길은 인공지능을 활용한 유·무인복합체계 밖에 없다는 결론을 도출할 수 있으며, 방위사업도 운용자 및 정비요원의 최소화 설계의 방향으로 변화할 수 밖에 없다는 것을 의미한다.

결론적으로 국외·내부적인 문제들로 인해 인공지능을 방위사업에 적용하는 것은 불가피한 상황이며 이를 완성하기 위한 방안은 빠르게 발전하고 있다. 반면, 기술보호에 대한 보안 대책은 시대 흐름에 맞추어 발전하지 못하고 있는 상황이다. 첨단화·고도화된 인공지능 적용 방위사업 기술을 개발되었을 경우 철저한 보호가 필요함에도 불구하고 기술보호 대책의 부족으로 독자적인 기술이 타국에 유출되어 가치의 저하 또는 상실 될 수 있는 것이다. 방위사업 분야에서 인공지능 적용이 추진되는 있는 시점에서 이와 관련된 기술 보호 대책도 인공지능을 활용하여 보호할 수 있는 방안 연구가 필요하며, 본 연구를 통해 방향성을 제시하고자 한다.

1.2. 연구의 방법과 범위

본 연구는 '인공지능을 활용한 방위사업 보호방향 연구'를 위해 국방에서의 인공지능 개발 현황과 방위사업 보안취약점에 대해 분석하여 인공지능을 방위사업에 적용함으로써 향후 우리가 발전시킬 산업보안 및 기술보호 요소에 대해 도출한다. 그리고, 향후 인공지능 적용에 따른 향후 문제점을 예상해보고 보완 및 개선할 수 있는 방안을 모색하는 것이 본 연구의 목적이라 할 수 있다.

문헌연구와 연구자의 실무경험을 통해 방위사업에 적용할 수 있는 보완대책을 모색해보고, 도출된 결과를 이와 관련된 전문가들의 경험과 직관을 설문조사로 수

렴하여 일치여부를 확인하고 개방형 질문을 통해 전문가 집단의 창의적인 의견을 수렴하여 평가 항목을 도출하는 델파이 기법을 활용하고자 한다. 또한, 평가 항목을 바탕으로 중분류 상대 비교를 통해 가중치 및 우선순위를 도출하는 계층적 의사 결정 방법을 연구방법론으로 채택하여 작성하였다.

델파이 기법은 1950년대 미국의 랜드 연구소에서 개발된 것으로 집단적 판단을 종합하여 결론을 도출하는 방법이다. 이는 정확한 지식이 없는 어떤 문제에 대해 전문가로부터 자문하고 종합할 때 사용된다. 델파이 기법은 '개인의 의견보다 전문가 집단의 의견이 정확도가 높을 것이다'는 것을 바탕으로 시작되었다. 델파이 기법은 전문가 집단이 동일한 문제를 2회 이상 동일한 과정을 거쳐 견해를 제시하는 것으로 이 과정에서 다른 전문가의 의견을 다함께 공유하게 되어 문제에 대해 다시 생각할 수 있다. 이는 익명으로 진행되므로 권위자 발언, 다수의 횡포에 의한 영향 등의 문제를 제거할 수 있는 패널식 연구 방법이다. 델파이 기법은 연구 주제에 대해 해당 분야의 전문가로 패널을 구성하기 때문에 전문가를 선정하는 것은 중요하다. 델파이 조사에 참여하는 전문가의 수는 정해진 것은 없으나, 전문가의 수가 많을수록 신뢰도가 높을 수 밖에 없다. 그래서 최소한 10명 이상의 전문가를 선정한다. 대다수 델파이 기법을 활용한 연구를 살펴보면 1명에서 35명의 전문가를 활용한 것을 볼 수 있었다. 본 연구는 20명의 전문가를 선정하였으며, 세 단계로 구분하여 연구 목적을 달성하도록 노력하였다.

첫째, 계획 수집 단계로 문헌자료 및 선행연구 분석을 통해 연구에 필요한 요소들의 개념을 정의하고, 이론적 근거 내용을 확보하는데 노력하였다. 관련된 문헌으로는 학위논문, 정기 간행물, 국외논문 등을 포함하여 방산업체 보안 관리 실태, 언론 기사, 방위사업 보안관리체계 등을 분석하였다.

둘째, 문헌연구 내용을 바탕으로 델파이 기법을 통해 전문가들이 가진 직관을 통해 인공지능을 활용한 방위사업 기술보호에 대한 정성적 분석으로 내용을 검증하고 1차, 2차 델파이 조사에서 적합성 여부와 항목별 내용 타당도 비율 분석을

통해 신뢰도 분석을 실시하여, 항목을 보완하였다. 델파이 기법에서 전문가들의 의견 일치도에 대한 규칙은 없으나, 라운드별 평균값 및 합의도, 표준편차, 수렴도 감소 등을 기준으로 판단할 수 있었다.

셋째, 델파이 기법을 통해 도출된 내용을 계층적 의사 결정 방법(AHP)을 통해 평가 중분류 항목의 가중치를 도출하고 우선순위를 부여하였다.

<표 1> 연구 모형

델파이 조사 목표 (20명) 대상 조건 설정	**업무 관련자, 학위 보유자, 방산업무 종사자 등**
	군 및 국가기관 방위사업 보안 업무 관계자(팀장급 이상) 석사 이상 또는 전문적 식견을 가진 인원 방산업체 보안분야에서 5년 이상 종사자
↓	
델파이 조사(1차)	**방위사업 산업현장 수요 파악**
	인공지능의 적용분야와 적용 분야 각종 방위사업 기술유출 원인 및 취약점 시스템 및 사이버 보안 강화방안, 인증제도, 교육프로그램
↓	
델파이 조사(2차)	**델파이 1차 조사 이후 항목 검증 및 추가·삭제**
	1차 델파이 조사 결과 바탕으로 추가 및 삭제 내용 검증 1차 델파이 조사 결과 내용 검증 인공지능 활용 방위사업 발전 요소 도출
↓	
AHP 조사	**발전요소 가중치 및 우선순위 도출**
	가중치 및 우선순위 산출 범위 설정 : 중분류 중분류간 상대적 중요도
↓	
결과 분석	**인공지능을 활용한 산업보안 및 기술 유출 방지 대책 분석**
	방위사업 인공지능 적용시 보안 강화 우선순위 평가 인공지능 활용 방위사업 산업보안 및 기술보호 중요도 평가

Ⅱ. 선행연구와 이론적 배경

2.1. 선행연구

인공지능이 이슈가 되기 시작한 시점은 2016년으로 알파고가 이세돌에게 바둑을 승리하던 시기였다. 이후 민간업체로부터 연구가 활발히 진행되었고, 공공분야의 성격이 강한 방위사업 분야는 다소 관심이 부족하였다. 그리고 방위사업분야에 대한 세미나도 특정 종사자 대상으로 개최되기 때문에 다소 관심이 부족하였다. 인공지능 기술에 대한 관심이 높아지기 시작한 것은 인구절벽 대책 필요성이 강조되던 2018년이었다. 인구절벽으로 무기체계의 무인화가 필요했으며, 이에 대한 대책이 인공지능이었다.

인공지능을 활용한 방위사업 보호방안에 대한 선행연구를 찾아본 결과 2018년부터 연구 사례가 증가한 것을 볼 수 있었으며, 방위사업에 인공지능 기술 적용과 민간분야에서 인공지능에 대한 보안이 필요하다는 내용의 논문은 다수를 찾아볼 수 있었다.

<표 2> 인공지능과 방위사업 관련 연구

구 분	2015년	2016년	2017년	2018년	2019년	2020년	2021년	2022년
계	2건	2건	6건	10건	11건	12건	15건	18건
학위 논문	1건	1건	2건	1건	2건	2건	3건	4건
학술 논문	1건	1건	4건	9건	9건	10건	12건	14건

자료 : RISS, 2023.5.19.

반면, 연구자가 연구하려는 인공지능을 활용한 방위사업 보호방안과 직접적으로 연관있는 논문은 1건 내외를 확인할 수 있었고 그 외에는 단순히 참고할 수 있는 수준의 논문이었다.

윤정현은 4차 산업혁명이 촉발한 지능화의 흐름은 미래 안보환경의 패러다임 전환 중 현대전은 전장의 정밀화, 무인화, 자동화, 네트워크화의 양상으로 변화하고 있으며 로봇 간의 전투, 사이버 공간 중심의 전쟁, 무인 시스템의 확대 등은 다차원적이고 자동화된 전투방식이 지배적인 미래전의 흐름으로 부상할 것임을 시사하였다.[12)]

김명주는 인공지능이 제품이나 서비스로 구현되기까지의 전체 단계에 해당하는 데이터 구축, 학습, 테스트 및 상용화 단계에서 발생할 수 있는 보안 공격 기술 동향에 대하여 살펴보고 인공지능 기술을 활용한 다양한 사이버 위협 동향에 대해 현 시점에서의 인공지능 기반 사이버 위협 대응 방안을 제시하였다.[13)]

김세용은 인공지능은 빅데이터를 다양한 기계학습 방법론을 적용하여 군집화하거나 분류하여 예측하는 기술로 인공지능의 사용을 위해서는 데이터의 위·변조를 방지하는 기술이 반드시 필요하기에. 데이터의 위·변조 방지는 해수함수로 암호화된 데이터를 연결된 컴퓨터에 분산 저장 블록체인 기술이 필요하다고 제시하였다.[14)]

12) 윤정현, 국방 분야 인공지능 기술 도입의 주요 쟁점과 활용 제고 방안, 과학기술정책연구원, (2021.)
13) 김명주, 인공지능(AI) 기술 발달에 따른 사이버 위협과 이에 대한 대응 방안, 한국통신학회, (2022.)
14) 김세용, 국방분야 인공지능 블록체인 융합방안 연구, 인터넷정보학회논문지, (2020.)

<표 3> 인공지능과 방위사업 관련 연구 요약

구 분	저자	연구 내용
인공지능 적용	박용병 (2021)	• 딥러닝의 근간이 되는 인공지능, 머신러닝과의 관계를 이해하고 더 나아가 딥러닝 역사 및 배경에 대해 연구
	윤성준 (2021)	• 인공지능 기반의 드론봇 통합관제체계 구축을 개발하기 위한 결정요인을 연구하여 제시
	정두산 (2021)	• 한국의 국방 인공지능 생태계 구축을 위해 국방부 중심의 국방 인공지능 발전업무 총괄 등 방안을 제시
보안분야	정원후 (2019)	• 국내 산업보안 관련 법률들의 내용을 비교, 산업보안기본법의 필요성을 검토하고, 제정 시 입법방향을 검토
	김화영 (2019)	• 산업보안 전문자격 중 약 10년이 경과하는 산업보안관리사 자격을 중심으로 활성화 방안을 도출
	박상호 (2019)	• 산업보안 전문인력의 범위를 명확히 식별하고 산업보안 전문인력 직업군 도출과 각 세부 직업별 기본직무 도출
방위사업 보안	고희재 (2021)	• 방위산업 보안관리체계 전체를 분석하여 개발한 최초의 「방위산업 보안수준 평가 지표」로 향후, 방위산업 보안정책 발전 방향을 제시
	우광제 (2015)	• 방위산업의 핵심기술 유출을 방지하고 기술인력 및 시설을 보호하기 위해서, 방위산업보안을 융합보안 방안을 제시

자료 : RISS, 2023.5.19.

연구자의 논문주제는 2022년 기준 연구사례가 적은 것으로 확인하였다. 따라서, 방위사업에 인공지능이 적용되는 현 시점에서 방위사업보안이 강화되어야 하기에 연구의 필요성이 있으며, 가치가 있을것으로 판단하였다.

2.2. 이론적 배경

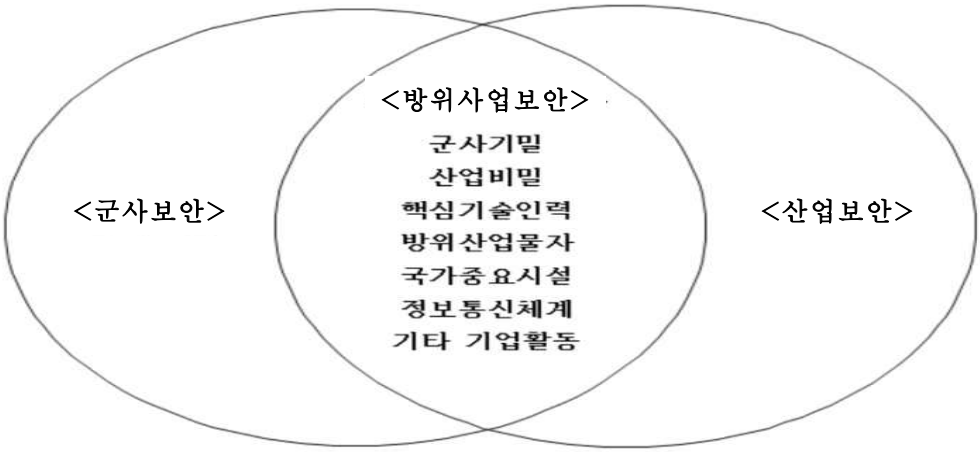
방위사업은 국가의 안전보장과 직결되기 때문에 다른 일반산업과 다르게 더 높은 수준의 보안을 요구하고 있다. 일반산업은 업체의 이익과 연계되는 산업비밀 보호 위주의 보안활동이 이루어지는 반면, 방위사업은 일반산업 대비 다양하고 복합적인 보안요소를 포함하고 있다. 방위사업과 관련된 업체들은 군에서 소요 제기

한 물자와 기술을 연구개발하고 생산하는 과정에서 군사비밀을 활용하고 보관하게 되며 관련 군사비밀도 첨단 과학기술의 집합체인 산업기술 일부로 구성되어 활용된다. 이러한 측면에서 방위사업보안은 군사보안과 일반산업보안의 융합체로 볼 수 있다. 방위사업체에 종사하는 인원들은 군에서 활용하던 군사비밀을 다루고 설계도면을 만들며 방위사업물자 생산에 참여한다. 특히, 핵심기술 개발에 참여하는 연구원들은 핵심 군사비밀과 산업기술을 다루기 때문에 연구원들에 의한 군사비밀 유출 방지 및 외부세력으로부터 협박 및 이직 권유 등으로부터 보호가 필요하다. 즉, 비밀에 의한 문서뿐만 아니라 인원보안도 필요하게 되는 것이다.

주요 방위사업체와 관련된 시설은 국가 안보와 직접적으로 연관되는 무기와 장비 및 시설을 보유하기 때문에 통합방위지침(대통령훈령 제28호)에 의거 국가중요시설로 지정되어 보호를 받는다. 일반 방위사업체들도 방위산업보안업무훈령에 따라 시설 및 장비에 대한 보안대책이 강구되어 보호받고 있다. 계약 및 생산으로부터 판매·수출에 이르기까지 방위사업체의 활동은 국방부훈령인 방위산업보안업무훈령을 준수하여 운영되고 있으며, 국정원 및 방첩사 등으로부터 일부 관여를 받고 있다. 그리고 각종 정보통신 시설과 기술도 일반 업체와 달리 민감한 내용에 대해서는 암호장비 등을 통해 암호화되어 전송되고 있다. 또한 방위산업물자의 연구개발 과정에서 생산된 핵심기술과 관련된 내용도 정보통신매체에 보관되고 있기 때문에 서버 관리의 중요성이 증가되고 있다.

방위사업체들은 방위산업보안업무훈령에 따라 표준화된 정보보호시스템과 자체 보호 시스템을 구축하고 내부 네트워크 및 인터넷망 등에 대한 보안대책을 강구하고 운용하고 있다. 방위사업은 이외에도 방위산업물자의 수출입, 수송, 하도급 등 모든 분야에 있어서 보안대책이 명시되어 있으며, 국방부의 통제하에 이루어진다.

일반산업과 다른점에 대해 종합적으로 살펴보면 군사기밀, 산업비밀, 방위산업물자, 핵심기술인력, 정보통신체계, 국가중요시설 등 다양한 보안요소를 포함하고 있는 것이다. 따라서 방위산업보안은 군사보안과 산업보안의 복합체로 볼 수 있다.



[그림 1] 방위사업보안과 산업보안의 상관 관계

자료 : 우광제, “융합보안 관점에서 방위산업보안 개념 정립과 연구동향 분석”, 융합보안논문지, (2015)

인공지능은 2016년 前 바둑기사 이세돌과 인공지능 알파고의 바둑 대전과 동시에 전 세계적으로 인공지능에 대한 관심이 주목되었다. 당시 진행된 바둑대전은 ‘인간과 기계의 싸움’으로 불리며 1대 4의 전적으로 알파고가 승리하였다.

알파고의 승리는 승자라는 의미에서 끝나지 않았다. ‘인공지능이 인간을 뛰어 넘을 수 있다’는 것을 보여주는 사례가 되었고, 각 국가에서는 인공지능 개발의 중요성을 인식시켜 주었다. 우리의 산업발달은 1차 산업혁명부터 4차례의 단계로 살펴볼 수 있다. 18세기 1차 산업혁명은 증기기관을 기반으로 각종 기계 구동을 통한 제조업이 발달 하였으며, 19세기 2차 산업혁명은 전기에너지 기반을 통한 대량 생산 체제가 구비되었다. 20세기 3차 산업혁명에서는 컴퓨터와 인터넷 기반의 지식정보 혁명이 발전하였으며, 21세기 4차 산업혁명에는 지능과 정보가 융합된 지능정보기술이 산업에 적용되는 것을 의미한다.

[그림 2] 4차 산업혁명의 발전

자료 : 과학기술정보통신부, https://www.msit.go.kr/index.do, (2023.3.12.)

4차 산업혁명에서 핵심적인 기술은 인공지능이다. 일반적으로 인공지능을 '인간의 학습능력과 추론능력, 지각능력, 자연언어의 이해능력 등을 컴퓨터 프로그램으로 실현한 기술로 정의하고 있으며, 각 학계에서도 많은 연구가 진행되고 있다. 연구된 일부 논문에서는 다음과 같이 정의하고 있다.

사전적 의미로는 기억・지각・연상・추론・이해・학습 등 인간의 지성을 필요로 하는 행위를 기계・컴퓨터를 통해 실현하는 기술이며 약한 인공지능[15]과 강한 인공지능[16]으로 구분할 수 있다. 일부 학자들은 아래와 같이 정의하고 있다.

Russell과 Norving(1995)의 정의에 따르면 인공지능은 인간 같이 사고하고, 인간 같이 행동하며, 합리적으로 사고하고 그의 결과에 따라 합리적으로 행동하는 4가지 특징을 가지며 결과적으로 '합리적 에이전트(agent)'라고 정의하고 있으며,[17]

임경숙(2019)에 의하면 인간이 가지고 있는 학습능력, 추론능력, 인지능력 등을 기계가 구현하는 것이며, 인공지능이 탑재된 로봇 또는 인공지능을 요소로 이용하는 시스템을 포함한다는 개념으로 정의하고 있다.[18]

15) 약한 인공지능(WeaK AI) : 특정한 분야의 주어진 과업을 인간의 지시에 따라 수행
16) 강한 인공지능(Strong AI) : 어떤 문제를 스스로 학습・판단・해결 할 수 있는 인간수준의 인공지능
17) Russell Stuart, Peter Norving, "Artificial Intelligence : A modern approach", 1995.

김성룡(2011)에 의하면 인간의 고유 능력이라 할 수 있는 학습, 탐색, 지각, 추론, 등의 능력들을 사람이 만들어낸 컴퓨터의 기술로 풀어낸 것으로 정의하고 있다. 이와 같이 인공지능에 대한 개념과 정의는 유사하게 해석하고 있으며, 그 중 가장 공통적으로 언급되고 있는 사항은 '인간과 유사하다'는 점이다.[19]

기존 선행연구들을 살펴보면 인공지능은 인간이 가지고 있는 추론・학습・인지능력 등을 가지고 있는 사물로 서로 의미하고 있다. 또한, 인공지능의 기능이 운용되기 위해서는 수많은 데이터가 필요하며 이를 '빅데이터'라고 한다. 그리고 이러한 데이터들이 수집되기 위해서는 초연결 통신 시스템을 통해 자료수집 및 공유가 될 수 있어야 하며, 이를 판단하기 위한 각종 하드웨어 및 알고리즘이 필요하다는 요지이다.

이를 종합하여 본 연구자는 빅데이터를 바탕으로 이루어진 '초지능성', 초고속으로 연결된 인터넷으로 수많은 사물이 연결된 '초연결성'을 바탕으로 인간과 유사한 기억・학습・연상・지각・이해・추론 등을 발휘하는 기능으로 정의하고자 한다.

다음은 방위사업에 대해 살펴보고자 한다. 대한민국 방위사업의 역사를 1945년 일본의 억압기에서 해당된 이후 미군원에 의존하였으나, 1968년 김신조 사건[20], 1969년 닉슨독트린[21] 그리고 1970년대 초 미군철수가 가시화되자 자주적 국방력 확보의 필요성이 제기되었다. 이후 전력을 증강하기 위해 미국의 제도를 적용하여 1972년부터 소요기획제도를 도입하였으며, 국방획득관리제도도 소요기획제도와 더불어 1972년부터 도입되어 운용되고 있다. 그리고 1972년에 국방기획관리제도가 최초 도입되면서 다소 미비한 점은 있었지만 전력증강과 관련된 조직 및 제도를 비로소 구축하게 되었다.

이와 같이 제도가 도입된 이후 1972년부터 무기체계 획득사업이 착수되어 1차

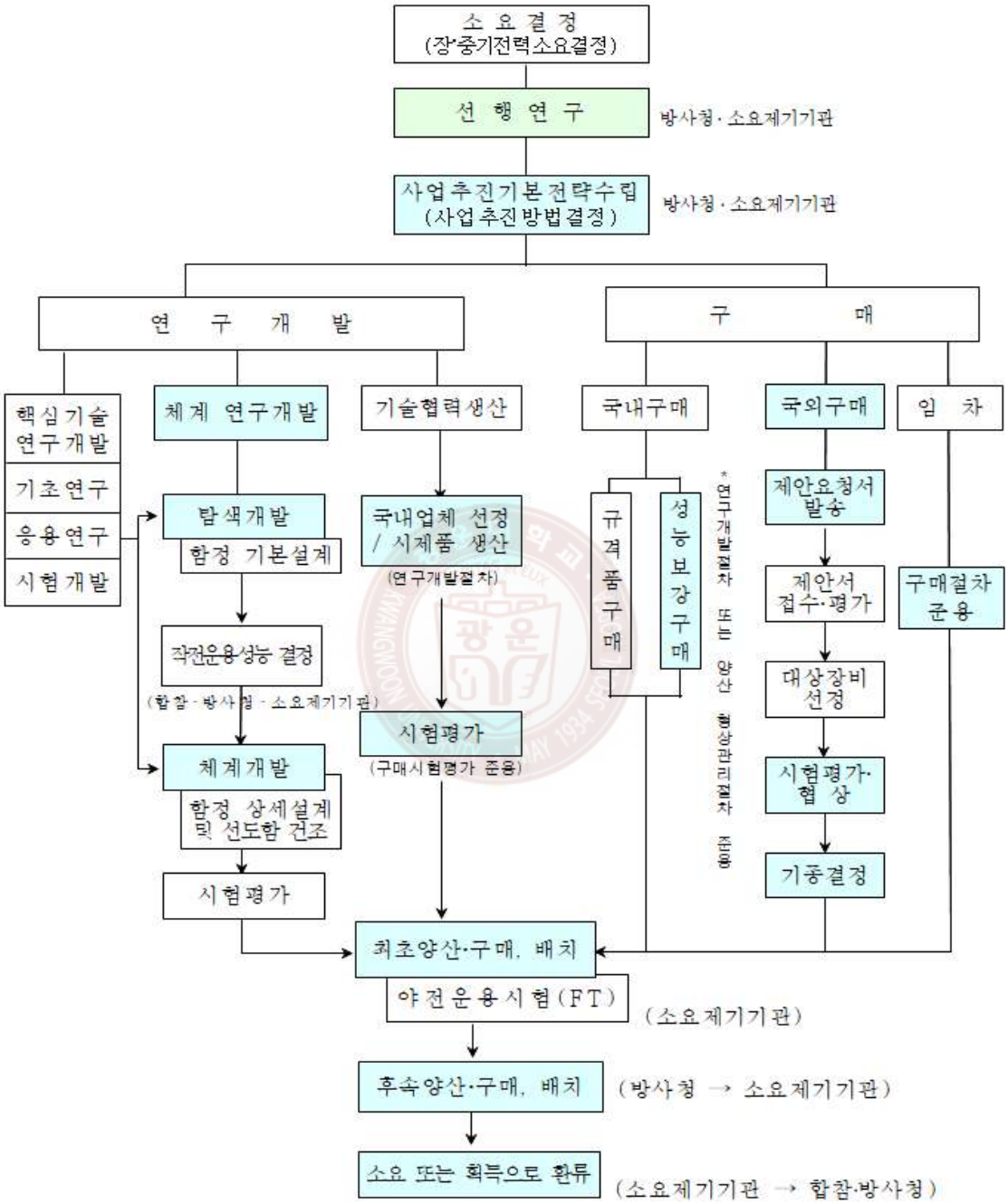
---

18) 임경숙, "인공지능에 관한 법적 규율방안 : 인공지능 알고리즘과 빅데이터의 법적규율을 중심으로", 2019
19) 김성룡, "법적 논증과 관련한 인공지능 연구의 현황, IT와 법 연구", 2011.
20) 1968년 북한으로부터 침투한 김신조 일당이 청와대 테러 기습시도 사건
21) 1969년 닉슨독트린의 주요 내용으로 '방위의 1차적 책임은 자국이 져야 한다'는 내용

율곡사업[22], 전력증강사업, 전력정비사업, 방위력개선사업, 획득사업, 전력투자사업, 방위사업 등의 명칭으로 변경되면서 추진되어 오고 있다. 방위사업을 시작한 이후 자주 국방력 확보와 국내개발 우선정책을 지속적으로 추진한 결과 국내에서 개발한 우수한 장비가 야전에 배치되어 운용되고 있으며, K-9자주포 및 함정 등 일부 무기체계는 다른 나라에 수출하여 국위를 선양하고 있는 등 1970년대 초의 미 군 원장비에 전적으로 의존하여 무기 및 장비를 운용하였던 것에 비하면 비약적인 발전을 이루었다. 1980년대에는 대한민국 군이 최초로 국내 개발한 K1전차를 도입하였으며, 이후로는 K2 전차 및 K9 자주포 등 국내 개발 무기체계가 계속해서 개발되었다. 현재 대한민국 군은 국내 개발 무기체계와 미국 등 해외 기술을 접목한 무기체계를 보유하고 있으며, 미국과의 동맹을 유지하며 군사적 자위력을 유지하고 있다.

현재의 대한민국 방위사업의 무기체계 획득 절차는 각 군, 합참, 국방부, 방사청, 업체별까지 해당 기능 업무를 처리하는 순서로 이루어지며, 그 과정은 아래 [그림 3]와 같다.

22) 1974년부터 모금된 방위성금과 1975년 7월부터 방위세로 마련된 재원으로 군의 전력증강 및 현대화하는 사업으로 1990년까지 추진되어 왔음. 이후 일부 비리문제로 전력정비사업으로 명칭이 변경되었음.



[그림 3] 무기체계 획득 절차도

자료: 국방부, “국방전력발전업무훈령 제2539호”, p.191, (2021.)

방위사업의 정의에 대해서는 다양한 분야에서 해석이 존재한다 OECD(경제협력개발기구)에서는 방위사업을 '국방 목적으로 과학 기술 및 산업과 관련된 모든 작업과 제품을 제조, 유지 보수 및 개발하는 일련의 활동'이라고 정의하고 있고, 일본 방위산업협회(JADI)에서는 방위사업을 '국방의 요구에 따른 방위용품, 시스템 및 장비의 개발, 설계, 생산, 유지보수 및 공급 등을 수행하는 산업 활동'으로 정의하고 있으며 미국 국방부는 방위사업을 '전투 능력 유지 및 증진을 위해 무기체계와 관련된 모든 제품과 서비스를 제공하는 활동'으로 정의하고 있다.

이외에도 국가의 안보를 유지하고 강화하기 위한 핵심 산업 분야 중 하나로, 국가의 안보와 관련된 군사력 강화와 관련된 제반 사업을 의미하며, 국가의 안보를 보장하고, 국가의 경제적, 정치적 안정과 개발에 큰 기여하는 부분이며, 국가의 안보와 관련된 군사력 강화와 관련된 제반 사업으로, 국방력 확보와 전쟁 등의 위기상황에서 국가를 보호하기 위해 수행되는 제반 활동을 포괄하는 개념으로 보고 있다.

사전적 의미에서 볼 때 '방위'라는 단어와 '사업'의 복합어라고 할 수 있으며 사업은 어떠한 일을 목적과 계획을 가지고 지속적으로 경영하는 일이고 방위는 '적의 공격이나 침략으로부터 막아서 지킨다'는 의미를 지니고 있다. 즉, 방위사업은 '적의 공격이나 침략으로부터 방어하기 위해 군이 필요로 하는 것을 획득하거나, 운용할 수 있는 여건을 지속 경영하는 것'으로 정의할 수 있다. 이를 군사적 분야의 해석으로 살펴보면 '국가의 안전보장 및 국민의 생명과 재산을 보호하기 위한 목적으로 군사력 건설에 필요한 무기체계 및 해당 무기체계를 운영하기 위한 전력지원체계(장비, 용역, 물자) 등의 획득과 개발 생산하는 것으로 의미하고 있다.

방위사업은 방위사업법에서 방위력개선 방위산업육성 및 군수품조달까지 포함하는 개념으로 명시되어 있다[23]. 방위력개선은 전차, 전투기, 함정, 유도무기 등을 연

23) 방위사업법 제 1조, 자주국방의 기반을 마련하기 위한 방위력개선·방위산업육성 및 군수품 조달 등 방위사업의 수행에 관하여 필요한 사항을 규정함을 목적으로 한다.

구개발 또는 구매하여 배치하는 활동으로서 방위사업의 가장 중요한 기본임무이고, 군수품조달은 방위력개선을 수행하기 위한 필수적 수반되는 임무를 의미한다.

방위산업육성은 방위력개선사업을 달성하기 위한 기초로 반드시 달성하여야 하는 임무이다. 방위사업은 방위력개선과 이를 지원하는 군수품조달·방위산업육성의 개념을 전반적으로 포함하는 광의의 개념으로 의미하고 있다.

2.3. 방위사업의 국가적 가치

2.3.1. 인공지능을 활용한 방위사업 현황

대한민국 국방부는 2018년도부터 미국과의 동맹 관계와 북한의 군사적 위협으로 인해 방위사업에 대한 관심이 높아지고 있으며, 이에 따라 인공지능을 활용한 방위사업에 대한 관심도 높아지고 있다. 미래의 전장환경 변화와 인구절벽 현상에 따른 병력 감소 현상에 대응하기 위해 무기체계에 대한 인공지능 적용과, 첨단 기술을 활용한 무인화, 인공지능을 활용한 각종 시범사업을 진행하는 등 본격적인 노력이 추진되고 있다.

C4I·정보·화력·기동·방호·작전지속지원 분야로 나누어 과학기술을 융합할 수 있는 부분을 모색하고 있으며, 관련 핵심 기술들의 정보화 구축에 역량을 집중하고 있다. 전력 소요창출과 기술 개발을 통한 무기체계 및 전력지원체계, 운영유지 등 전 분야에서 인공지능을 적용하고 활용할 수 있는 분야를 찾고 있으며, 이를 정리하면 아래 <표 4>과 같다.

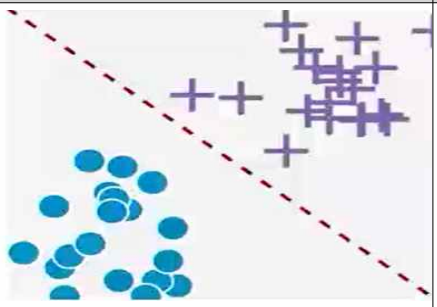
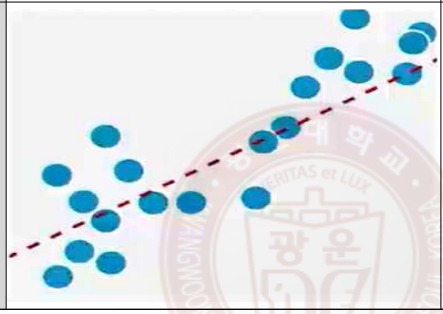
< 표 4> 인공지능을 활용한 주요 방위사업 분야

분 야	주요 내용
C 4 I	• 인공지능기반의 실시간 M&S, 지능정보센터, 초연결 네트워크, 지능형 지휘결심 지원체계 등
정 보	• 사이버 및 전자전 공격/방호 시스템, 지능성 군사정보관리체계 등
화 력	• 지능형 지능탄 및 표적탐지레이더, 사격 지휘통제체계 등
기 동	• 인공지능 기반 자율 및 군집형 기동체계, 지능형 워리어 플랫폼 등
방 호	• 사이버전 수행 기술, 지휘시설 및 무기체계의 방호, 과학화 경계시스템 등
작 전 지 속 지 원	• KCTC와 연계한 인공지능 기반의 지휘결심지원체계, 인공지능 기반의 훈련 시뮬레이터 / 탄약 저장관리체계, 물자보충 및 정비수요 예측 시스템 / 지능형 안전관리 정보체계 / 원격치료 시스템, 지능형 합성 전장훈련체계 등

자료 : 정보통신기획평가원, “주간기술동향 1888호”, (2019.3.)

인공지능의 기본적인 원리에 대해 살펴보면 데이터들을 활용하여 특정한 모델을 통해 결과값을 도출하고 이를 분류와 회귀로 구분하여 결과값을 도출한다. 통상 2차 함수를 통해 결과를 도출하는데 Y=Wx+B의 형태를 띈다. 데이터들은 각종 상황에 따라 X와 Y값을 나타내며 인공지능은 이 데이터들을 이용하여 최적의 값 W와 B값을 찾아낸다. 단순히 수개의 데이터가 아닌 수천 또는 수만개의 데이터들을 통해 W와 B값을 도출해낸다면 주어진 데이터들을 통한 가장 정확한 값에 가까운 결과값을 도출할 수 있으며 아래 <표 5>과 같다.

<표 5> 인공지능 데이터의 분류와 회귀

구 분	형 상	내 용
분류 (Classification)		데이터를 모델링하여 특정 구역으로 분류할 수 있는 기능 (범주를 예측)
회귀 (Regression)		데이터를 모델리하여 향후 수치를 예측할 수 있는 기능 (수치를 예측)

자료 : 국방부, “인공지능 교육자료”, (2022.)

이를 국방에 적용할 수 있는 대표적인 사례가 앞서 예를 들었던 북한의 무인기이다. 헬기 및 방공무기의 위치에서 적 무인기를 보았을 때 적 무인기의 뒷모습 및 아래모습에 대한 데이터들이 있다면 인공지능을 통해 분류하고 예상 이동경로를 인공지능 회귀방법을 통해 예측한다면 가장 근사치에 가까운 예상 이동 경로상 사격으로 격추하는 방식이 될 수 있다. 무인기의 무력화 확률을 높이려면 그물이나 EMP 탄을 인공지능으로 계산한 예상 경로에 사격하는 방법도 연구해볼 수 있다. 인공지능의 원리는 다양한 분야에 활용할 수 있다. 정확한 값을 도출하는 것은 아니지만 다양한 상황에서 데이터를 바탕으로 가장 근사치를 내는 원리, 군에 다양한 데이터가 있다면 이를 바탕으로 가장 정확도가 높은 값을 운용자에게 제공할

수 있는 것이다.

예를 들어 'K-Detector'는 인공지능을 활용하여 군사용 무인기나 로봇 등의 이동 경로를 감시하고, 위험을 예측하는 기술이다. 이를 통해 대한민국 군은 무인체계의 작전수행 능력을 향상시키고, 위험한 상황에서 군인의 생명을 보호할 수 있다.

'K-Monitor'는 인공지능을 활용하여 군사용 CCTV 영상을 분석하여 위험 상황을 탐지하는 기술이다. K-Monitor는 기존에 학습된 알고리즘 분류 모델에서 이상 행동, 적대적인 움직임, 미리 정해진 장소에서의 이상 징후 등을 감지하여 대한민국 군에게 경고를 보내고, 이에 따른 대응책을 마련할 수 있도록 돕는다.

이와 같은 인공지능 기술은 군과 방위사업에서 많은 관심을 받고 있으며, 전투력 강화와 방위사업 기술 발전에 기여를 할 것으로 예상되고 있다.

첫째로, 인공지능은 전투력 강화와 국민의 안전을 강화할 수 있는 기술 중 하나이다. 대한민국은 북한과의 군사적 긴장 상황에 놓여 있으며, 그에 대한 대응 방안으로 인공지능 기술을 도입하고 있다. 인공지능 기술을 활용하여 무인기나 로봇 등을 개발해 전투 상황에서 최소의 희생으로 인간의 안전을 보호하고, 더욱 정확하고 빠르게 정보 수집 및 분석을 수행할 수 있다.

둘째로, 인공지능은 대한민국의 방위사업 발전에도 큰 역할을 할 것으로 기대된다. 대한민국은 방위사업 발전을 적극적으로 추진하고 있으며, 인공지능 기술을 접목시켜 높은 부가가치를 창출할 수 있다. 인공지능 기술은 군사용뿐만 아니라 국가의 경제적 측면에서도 중요한 역할을 할 수 있는 기술이다.

셋째로, 인공지능은 대한민국의 보안을 강화할 수 있는 기술 중 하나이다. 현재 침해공격이 대한민국의 국가 안보에 큰 위협으로 작용하고 있다. 이에 대응하기 위해 인공지능 기술을 활용하여 보안 위협을 감지하고 분석하는 것이 필요하다. 즉, 인공지능 기술을 통해 보안 시스템을 강화하고, 새로운 보안 위협에 대응할 수 있는 능력을 구비가 중요하다.

마지막으로, 대한민국은 인공지능 기술을 활용한 군사훈련을 추진하고 있다. 인

공지능 기술을 활용하여 VR 및 AR 등 가상현실을 통한 군사훈련을 진행하면 기존의 군사훈련보다 현실적인 상황에 대한 대처능력에 빠르게 적응할 수 있도록 훈련이 가능할 것으로 보고 있다.

이외에도, KAIST와 한화시스템 등 연구기관과 방산업체에서도 협업하여 국방인공지능 융합연구센터를 개소하여, 대형급 무인 잠수정 항법 알고리즘, 인공지능 기반 지휘결심지원체계, 인공지능 기반 지능형 물체 인식 및 추적 기술 개발, 인공지능 기반 항공기 훈련 시스템 등의 4개 과제를 선정하고, 상호교류 및 교육, 인공지능 과제 발굴·연구, 기술자문, 등을 추진중에 있다. 그리고 인공지능이 적용되는 과정을 3단계로 나누어 정립하였으며, 방위사업에서 인공지능 적용분야 청사진을 그려 추진하고 있다.

[그림 4] 국방 인공지능 기능 발전단계

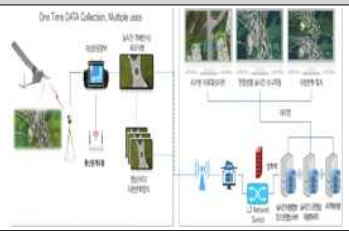
자료: 국방기술진흥연구소, “미래국방 2030 기술전략”, p.8, (2022)

육군은 2019년초 초지능성·초연결성으로 상징되는 인공지능 시대의 군사혁신을 위한 목적으로 ‘인공지능 연구발전처’를 창설하였으며, 인공지능 관련 연구 등 컨트롤타워 역할과, 빅데이터 구축, R&D역량 확보, 인공지능 기반의 군사혁신을 위

한 동력 마련을 목표로, 발전 비전 및 운영 개념을 정립하고 업체 및 연구소와 연계한 각종 시범사업 계획 및 전력화 등을 위해 노력 중에 있다. 최근에는 인공지능 지휘 결심 지원 체계[24]와 드론봇, 인공지능 과학화 경계시스템 등에 중점을 두어 개발을 진행하고 있으며, 이에 맞추어 국방 예산 편성 등의 노력을 기울이고 있다. 군사적 측면에서 감시정찰, 지휘통제, 유·무인복합, 사이버 및 기타 체계로 구분하여 개발중에 있으며, 현재까지 개발되고 있는 인공지능 기술 방위사업 현황을 특성별로 살펴보면 아래 <표 6>과 같다.

24) 전장 정보와 수집된 전술 데이터 결과를 제공해 지휘관의 작전 지휘를 돕는다

<표 6> 인공지능을 활용한 방위사업 국내 개발 현황

구 분	체계명	형상	개발 기관	주요 특성
감시 정찰	소형드론용 영상분석 장비		육군 교육 사령부	- AI 영상분석, 표적추적 - 표적정보 실시간 공유 - 다중 드론 통제/모니터링 - 지형정보 처리(3D 지도 형성)
지휘 통제	다출처영상 융합체계		국방 과학 연구소	- 주요 핵심표적에 대한 징후감시와 전략표적 타격작전 수행시 정확한 표적 영상정보를 제공 - 다출처에서 운용되는 영상센서별 탑재한 정찰자산으로부터 수집되는 영상을 융합
유·무인 복합	무인수상정		KRISO & 한화 시스템	- 군집 수색이 가능한 자율 무인잠수정과 무인항해를 위한 감시정찰 체계가 탑재되는 12m급 함정 - 무인잠수정의 군집운용을 통해 해상 수색이 가능 군집 임무 수행 및 실시간 모니터링 관제시스템 제공
사이버 및 기타	워리어 플랫폼		육군	- 전투력을 최고도로 발휘하기 위해 전투복·장구류·개인화기 등 개인 전투장비와 물자를 통합 - 치명성, 지휘통제, 생존성, 임무지속성, 기동성 5대 기본능력 또는 상황인식/공유, 치명성·생존성 향상의 3대 기능으로 분류

자료: 국방기술진흥연구소, “미래국방 2030 기술전략”, p.50-p.70 (2022)

인공지능의 기술 수준에 대해 살펴보면 대한민국은 미국 대비 약 2.5년 뒤처지고 있는 것으로 평가받고 있다.

<표 7> 대한민국의 미국 대비 인공지능 수준

구 분		기술수준		기술격차	
학습지능	머신러닝	100	69	0	2.6년
신뢰지능	설명가능한 인공지능	100	82	0	1.3년
	견고한 인공지능	100	67.5	0	4.3년
	공정한 인공지능	100	82.7	0	1.9년
고성능 인공지능 H/W	모델 경량화	100	84	0	1.5년
	서버용 H/W	100	60	0	5년
	모바일 / Edge H/W	100	85	0	1.5년
전장인식	영상인식	100	95	0	0.5년
	음성인식	100	100	0	0년
	언어인식	100	86	0	1.3년
	감정인식	100	60	0	7년
자율판단	전장환경 및 상황인지	100	70	0	3년
	국방추폰 및 지식표현	100	80	0	2.5년
지휘결심	임무계획	100	70	0	3년
	임무할당	100	70	0	3년
임무수행	행동지능	100	80	0	2년
	유·무인 협업제어	100	75	0	2.5년
종합적 판단		100	77.4	0	2.5년

자료: 국방기술진흥연구소, “미래국방 2030 기술전략”, p.13, (2022)

미국은 마이크로소프트 및 구글과 같은 업체에서 인공지능에 대한 연구를 대한민국보다 빠르게 진행하였으며, 2023년 마이크로소프트에서는 ‘CHAT GPT’라는

인공지능 기반의 채팅로봇을 만들어 선보였다. 이 로봇은 43TB의 빅데이터를 활용하여 정보를 필요로하는 사람에게 정확도가 높은 데이터를 채팅형식으로 제공하는 기능을 가지고 있다. 대한민국은 인공지능 개발 초기 단계에 있지만 산・학・연과 연계하여 연구・개발하는 등 지속 발전을 위해 노력하고 있다.

미국은 인공지능을 미래전 대비 3차 상쇄전략 구현의 핵심수단으로 보고, 국방 인공지능거버넌스 구축 및 기술개발에 투자를 확대 중이다. 국방부 지능정보화정책관 아래 인공지능업무 총괄 조직인 합동 인공지능센터(JAIC)를 설립하여, 전투수행・자원관리・정보능력 강화 등 전반에 걸쳐 인공지능 프로젝트를 수행중이다.

미국방성은 중국과 러시아의 인공지능 개발에 속도를 내고 있는 것과 관련하여, 군사부문을 모두 망라하는 인공지능 시스템의 사용 가속화 필요성에 대해 인식하고 있다. 또한, 인공지능은 다양한 방위사업 활동을 통해 상당한 이익을 제공할 수 있으며, 물류, 유지, 보수, 기지, 군인의 건강 및 신체관리, 인명 구조, 전시 의료지원, 중단기적 인력 관리, 통신, 사이버 방호 및 정보 분석・비교와 같은 치명적이지 않은 활동에 인공지능을 활용하여 미군을 더욱 안전하게 만들기 위해 노력하고 있다. 그리고 새로운 기능들을 갖춘 인공지능 장비들이 개발되고 운영될 수 있기에 국방에서의 인간 가치, 국가 안보 이익 및 국제 및 국내 의무에 부합하는 자치무기에 대한 정부 차원의 정책을 추진하기 위해 적극적이고 지속적인 정부 간 협의를 진행하고 있다.[25)]

미육군 훈련교리사령부(USTRADOC[26)])에서는 작전부대 지휘관, 민간 방산업체, 공공 연구기관 및 민간 연구기관에서 인공지능 전문가를 포함한 약 115명이 참가한 세미나 자리에서 인공지능과 관련된 미래전 개념을 정립을 위한 시간을 통해 다음과 같은 공감대를 형성하였다.

첫째, 미래 전장에서의 승패 여부는 인공지능이 좌우할 것이다. 미래전 전장이

25) 백악관, “인공지능의 미래를 위한 준비”, p.17-p.19, (2016.10.)
26) United States Army Training and Doctrine Command

지상, 해양과 공중에서 우주, 전자기 스펙트럼과 사이버 공간으로 변화하고 이를 통제하는 것은 형태가 있는 물리적 점유가 아닌, 정보의 충족도에 의해 결정되는 유기적 공간으로 바뀔 것이며, 이는 인공지능만이 유리한 위치를 선점할 수 있을 것으로 전망했다. 특히 이미지 인식(image recognition)과 데이터 처리는 인공지능의 관건이며, 이는 모두 전사가 아닌, 기계가 할 것으로 전망했다.

둘째, 미래전에서는 기계가 전사를 지배할 것이다. 이는 현재 연구개발되고 있는 머신러닝으로 전장에서의 인간과 기계간 관계(machine-human relationship)를 재정립이 필요하며, 여기에 인공지능이 접목되면, 전사가 없는 자율화, 자동화 및 무인화가 전장을 완전히 지배할 것이다. 즉 과거 전사가 전장을 완전히 통제하던 양상에서 기계가 전사에 앞서 전장을 압도하는 양상이다.

셋째, 방어보다 공격이다. 군사 전문가들은 이를 미래전장에서 방어(defense)는 없으며, 오직 공격(offensive)만을 위한 전술-작전-전략이 작용될 것이라고 평가하였다. 이는 평시에는 기계가 움직이지 않다가 인공지능과 머신러닝 등의 알고리즘이 적 표적으로 인식하는 순간 무차별적 공격을 하는 양상으로, 군사과학 기술적 신냉전(Military Technology Cold War) 이라고 정의하기도 한다. 과거 90초 걸리던 소규모 전장에서의 전술 속도가 미래전에서는 0.000075초에 가능한 초행동 현상이 나타날 것이라고 전망하였다. 위와 같이 미래 전투에 대한 양상을 언급하였으며, 이와 같은 상황에 대응하기 위해 미 육군은 인공지능 개념을 발전시키고 있다.[27)]

미국은 인공지능을 활용한 무기체계를 지속 개발하고 연구중에 있으며 일부 장비는 가시적으로 선보이고 있다. 현재까지 미 국방성에서 개발되고 있는 장비로는 스스로 사물을 판단할 수 있는 로봇, 집단 공격 드론, 머신러닝을 활용한 감시정찰 장비, 정교한 3D 프린트 형상 설계, 사물인터넷간 안정적인 통신 기술 게이트웨이원[28)] 등을 선보이고 있다.

---

27) 영국 제인스국방주간지, p.3-p.6, (2019.12.16.)
28) 방대한 양의 정보통신을 안전하게 송수신 할 수 있는 군사용 사물인터넷

최근에는 미 공군에서 '애리조나주 유마성능평가시험장에서 XQ-58A 발키리 무인 스텔스 전투기와 F-22 랩터, F-35A 라이트닝Ⅱ 유인 스텔스 전투기의 시험편대비행을 마쳤다'[29]고 밝혔다. 스텔스 전투기나 폭격기가 인공지능을 탑재한 무인 스텔스 전투기와 전장정보를 실시간 공유한다면 기존의 드론(UAV)과는 차원이 다른 활용성을 갖출 수 있다. 심지어 무인 스텔스 전투기로만 적을 정밀 타격할 수도 있다.

미국 방위고등연구계획국(DARPA)은 존스홉킨스대 응용물리연구소(APL)에서 전투기 조종사와 인공지능 조종사간 모의 공중전을 벌였다. 시험에 참가한 전투기 조종사는 F-16 전투기만 2000시간 넘게 조종한 베테랑이었다. 모의 공중전 결과는 5 대 0으로 인간의 참패였다. 전투기 조종사는 단 한 발의 기총도 맞추지 못하고 격추당했다. 인공지능을 탑재한 무인 스텔스기가 우수했던 비결은 마치 이세돌 기사와 대국에서 이긴 구글의 '알파고'와 비슷한 학습이었다. 인공지능 조종사는 40억 번 이상의 모의 공중전을 학습한 것으로 알려졌다. 게다가 인간 조종사는 안전을 최우선으로 고려하고 경험을 바탕으로 전투하는 반면, 인공지능 조종사는 안전을 문제 삼지 않는 데다 나노초(10억 분의 1초) 만에 판단하는 탓에 이길 수 밖에 없었다. 테슬라모터스 창업주 엘런 머스크 등은 "이제 인간 전투기 조종사는 사라질 것"이라는 전망을 내놓기도 했다.

일부 미국 군사전문가들은 인공지능 탑재 무인 스텔스 전투기가 유인 스텔스 전투기를 엄호하면서 적진에 먼저 들어가 정찰하거나 레이더기지·대공포 제거 등의 임무는 충분히 수행할 것이라고 평가하고 있다.

무기체계에 자율성을 부여한다면 표적의 식별, 누적된 데이터들의 분석을 통한 피·아 식별을 통해 군사 작전의 정밀도를 높이는 활동을 통해 군인들의 생존성을 보장하고 주기적으로 교체가 필요한 수리부속을 예측하여 공급하는 역할도 가능하다.

29) 『daily news』, "AI 탑재 무인 스텔스 전투기, 유인 스텔스 전투기와 편대비행", (2020.12.17.)

미국 무기체계를 연구하는 DARPA[30]에서는 초기에 전입한 해군들이 전문적인 기술을 배우는 시간을 최소화할 목적으로 전문가와 초보자 사이에서 상호 교류하는 인공지능 개발을 위해 노력중이다. 이는 전문가들이 탑재한 각종 노하우를 초급자가 교육받을 수 있고 시험을 통해 취약 분야를 분석하여 해당 분야에 대한 집중 훈련을 통해 교육기간을 줄이겠다는 의도이다. 실제 초기 테스트 과정중에서 인공지능을 통해 교육받은 일부 인원들이 7~10년의 경력을 가진 전문가를 능가하는 결과를 보여주었다. 인공지능 기술을 심화하여 무인화 무기체계가 스스로 판단하여 행동할 수 있는 장비 등 개발을 위해 끊임없는 노력을 하고 있다.[31] 또한, 사회 제도적으로도 자율 또는 기타의 무기체계가 구별이 될 수 있고 비례의 원칙을 포함하여 국제 인도법에 부합하는 방안도 병행하여 지금도 연구하고 있다.

합동 인공지능센터에서는 군사용 인공지능개발을 위해 프로젝트를 기획하여 무기 및 전력지원체계에 기술적 구현 가능성을 신속하게 시범적용하고 있다. 또한 중・러에 대비하여 2030년까지 250~300명의 전투병과 수천대의 로봇으로 구성된 새로운 전투단을 만들 계획이다. 미군의 인공지능 기술을 적용한 주요 수준을 정리하면 아래 <표 8>와 같다.

30) Defense Advanced Research Projects Agency(고등연구 계획국) : 미 국방성을 위한 기초 및 응용 연구개발 프로젝트를 관리・감독한다.
31) 주간해외 군사정보 21-3호, 21-4호

<표 8> 미군의 인공지능 기술 적용안

구 분	내 용
지휘통제	▪ 합동 전영역 지휘통제체계(JDAC[32]) 성능개선 ▪ 인간과 인공지능 전투차량간 이해증진 프로그램 개발 ▪ 자율체계 연결성 획기적으로 향상시키는 SW기술 개발
정 보	▪ 유·무인겸용 항공기 '파이어버드'에 인공지능기반 센서 탑재 ▪ 군집드론 동작 제어용 머신러닝 알고리즘 개발 ▪ 인공지능 기반 접이식 휴대용 자율 드론 X2 출시
기 동	▪ 전투차량에 인공지능기술을 도입하여 자율 주행과 자동표적 선정 기능 개발 추진 ▪ 자율 기동간 장애물 탐지 및 제거 능력 탑재 연구
화 력	▪ 잠재적 위협을 인식하고 표적데이터(표적좌표)를 제공하는 인공지능 알고리즘(프로메테우스) 개발 ▪ 차세대 소총에 인공지능을 포함한 최첨단 사격통제기술 적용
방 호	▪ 대드론방어체계 '타이탄'에 인공지능 소프트웨어 도입 ▪ 인공지능 기반의 사이버 공격 대응체계 구축 및 보완 ▪ 적 기만공격에 대비한 방호 프로그램 개발
지속지원	▪ 1000파운드(450Kg) 무게를 72시간 동안 최대 60마일 이동이 가능한 분대 다목적 장비운용 차량 개발 ▪ 로봇 군견 '비전60' 활용 첨단전장관리체계 연구

자료 : 미국방성, "인공지능 활용 계획안", (2019)

중국은 인공지능을 강군건설의 핵심요소로 인식하고 미국에 대한 상대적인 열세 극복을 위해 대규모 예산 투자로 미래 지능화전을 준비하고 있다. 2030년까지 인공지능 핵심산업에 1조 위안(약 180조원), 관련된 산업에 10조(약 1,800조원) 위안 규모의 시장육성을 목표로 국가 인공지능 기술발전에 집중하는 계획을 세웠다. 2019년에는 인공지능 특허건수(22%)는 미국(15%)보다 우월하였으며, 미국과는 1~2년 격차의 기술 수준을 보이고 있다. 지능형 지휘통제 등 군사분야 전반에 인공지능적용을 위해 지상분야에서는 자율기동, 무인수송 체계, 무인정찰를 연구하고

32) JADC2(Joint All Domain command and Control) 미군의 각 군별 운용되고 있는 정보 수집센서와 전술통제망을 단일화하기 위한 지휘통제 네트워크

있으며, 공중분야에서는 집단자폭드론, 자율·군집비행 등의 개발을 추진중에 있다.

러시아는 2030년까지 군대의 1/3을 원격통제 및 자율화된 로봇으로 대체할 계획이며, 2025년 인공지능 기반으로 독자적 전투단위로 로봇군 창설을 준비하고 있다. 미래 무기체계에 인공지능 도입 촉진을 위해 2021년 러시아 국방부 내 인공지능 발전 전담부서를 신설하였고, 인공지능 로봇 연구 혁신단지 조성을 통해 약 1,000여개 기업 유치 등 기술개발 역량 통합을 위해 노력중에 있다. 미국과는 1년 격차의 기술수준을 보이고 있으며, 국가차원의 지원으로 상당수준의 기술을 발전시키는 등 기술력을 축적하고 있다. 인공지능을 적용한 미사일, 무인전투차량 등을 개발중에 있으며, 해킹기술은 이미 확보한 것으로 예상하고 있다. 또한 이번 우크라이나전에 살상용 자율드론을 투입하여 효과를 시험하였다.

일본은 고령화·저성장의 국가적 난제를 극복하기 위한 국가 경제·사회 혁신의 발판을 인공지능 기술 경쟁력 확보로 판단하고 있으며 인공지능 기술혁신에 집중하고 있다. 국내·외 높은 기술을 보유하고 있는 인공지능 전문가 결집을 위해 '혁신지능통합연구센터'를 설립하고 2018년에 195억엔(약 2,000억원)을 투자하여 오픈소스 인공지능 연구개발 플랫폼을 구축하였다. 미국과는 1.5년 격차의 기술수준을 보이고 있으며, 국방 인공지능에서는 높은 수준의 기술을 보유한 로봇분야에 지능화를 적용하는 연구가 진행되고 있다. 높은 수준의 로봇, 정밀기술을 바탕으로 인공지능 전투기 개발, 드론수송, 지능형 로봇, 인공지능 인사관리, 문서관리체계 등의 개발을 진행하고 있다.

2.3.2. 대한민국 방위사업의 세계적 수준과 가치

방산수출 활성화를 위한 범정부 차원의 노력은 2010년도부터 꾸준히 이루어졌다. 당시 약 30억 달러 수준이던 방산수출 수주실적이 2021년에는 약 72.5억 달러

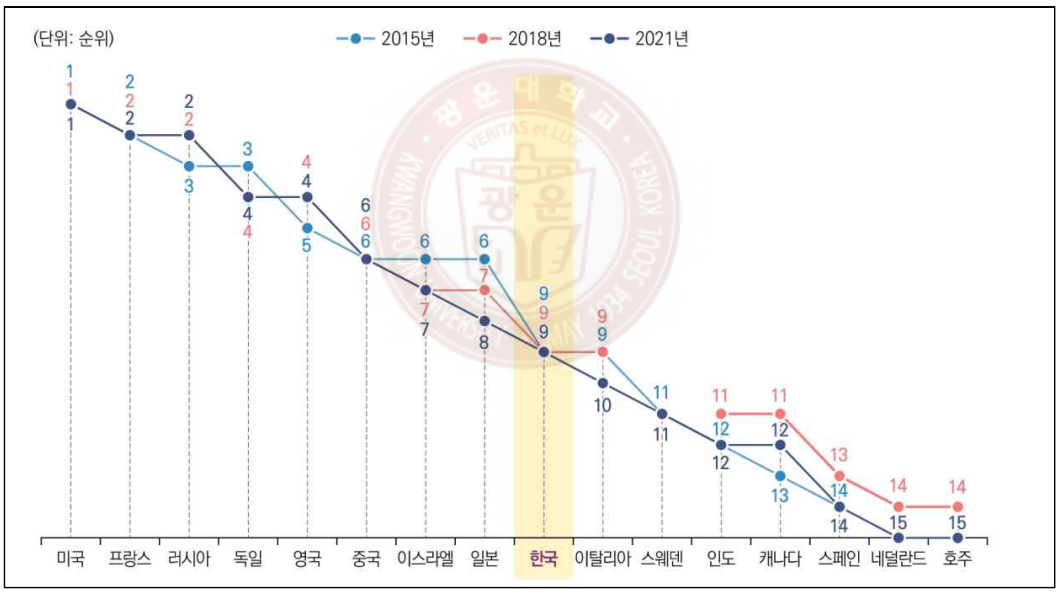
로 대폭 증가하였으며, 2022년에는 최근 5년 평균의 5배 수준인 173억 달러를 달성하여 13만 개의 일자리 창출효과 및 46조 원의 생산유발효과를 거두었다. 수출 대상 지역은 아시아, 중동, 북미, 유럽, 오세아니아, 아프리카 등으로 확대되었고, 품목도 탄약·총포 위주에서 육·해·공군을 아우르는 다양한 무기체계와 유도무기 등 첨단무기체계까지 저변을 넓혀가고 있다. 특히, 2022년에는 정밀 유도미사일, 다기능레이더, 교전통제소, 발사대가 결합된 첨단 복합무기체계인 '천궁-Ⅱ' 중거리 요격체계를 UAE에 최초로 수출하였고, 폴란드에 우리 군의 대표 무기체계인 K2전차, K9자주포, FA-50, 천무를 대규모로 수출하고 협력사업을 진행하는 등 우리 무기체계의 우수성과 높은 기술력을 대내·외적으로 널리 알렸다.

대한민국은 2021년 방위사업 수출 수주액이 약 70억 달러에 달하면서 과거 대비 처음으로 수출 수주액이 수입액을 초과하는 기록을 세웠다. 2022년에는 전년 대비 두배를 초과하는 170억 달러라는 역사에 남을 만한 방산 수출을 기록했다. 2017년부터 2022년까지 수출 금액을 정리하면 아래 그림과 같다.

[그림 5] 대한민국 방산 수출 현황

자료: 국방부, “국방백서”, p.67, (2022)

한국의 방위사업은 무기체계를 자체 생산하는 수준을 넘어 세계시장에서 활발하게 수출할 정도로 역량이 크게 확대되었다. 또한, 2017~2021년 세계 수출시장 점유율의 2.8%를 차지하는 등 세계에서 8번째로 수출을 많이 하고 있으며, 한국의 국방 연구개발 예산은 과기정통부, 산업통상자원부에 이어 3번째로 큰 규모로, 2022년 국방 연구개발 예산은 1조원 수준으로 확대되었다. 그 결과 국방과학기술은 세계 9위를 기록하고 있다.



[그림 6] 대한민국 국방과학 기술 수준

자료: 국방기술진흥연구소, “국가별 국방과학기술 수준조사서”, p.78, (2022)

한국의 국방과학 기술 수준을 분야별로 세계적 순위를 살펴보면 지휘통제 분야에서 국방개혁 2.0을 통해 빅데이터, 인공지능 등 첨단 ICT를 활용한 무기체계 지능화를 시도하며 순위가 6위까지 상승하였으며, 인공지능, 클라우드 등 소프트웨어

에 대한 국가적인 투자를 기반으로 국방 소프트웨어 분야 역시 순위가 2단계 상승하여 9위를 기록하였다. 통신 기술은 민간분야에서 5G를 상용화하고 6G의 개발에 착수하는 등 세계 선진국 수준을 보유하고 있으며, 인공지능, 클라우드, 빅데이터 등 소프트웨어 기술도 민간에서 우수한 기술을 보유하고 있기 때문에 이를 국방에 활용할 수 있다면 더 높은 기술수준의 향상이 예상되고 있다. 레이더 분야는 수준조사 결과 12위로 순위를 유지하고 있으나, 최근 KF-21용 AESA 레이더를 개발하였고 많은 핵심기술 연구개발을 추진하고 있어 방위사업의 우수 국가로 자리매김하고 있다.

2.4. 소 결

2장에서는 인공지능과 방위사업의 정의에 대해 이해하고 방위사업과 일반산업의 차이점에 대해 살펴보았으며, 현재의 방위사업에서 인공지능이 개발되고 있는 분야와 수준, 대한민국 방위사업이 세계적 어느수준으로 평가 받고 있는지 분석해보았다. 인공지능과 방위사업이 연계된 선행연구는 일반적인 다른 산업분야에서의 보안과 관련된 연구에 비해 찾아보기 어려웠다. 이는 방위사업보안을 산업보안의 일부로 이해하는 경향이 있기 때문이다. 그래서 연구자의 실무경험과 기존에 활용할 수 있는 논문들을 최대한 활용하였다.

일반산업과 방위사업 보안의 가장 큰 차이점은 군에서 보유하고 있는 군사비밀을 활용하기 때문에 안보상 불순분자에게 유출이 되면 국가 차원의 피해가 발생하기 때문에 국가중요시설 요건, 암호화 장비 활용 등 보안상 준수해야할 사항들이 많다. 이와 함께 인공지능을 방위사업에 적용하기 위해 어느 수준까지 개발되었는지 살펴보고 이와 관련된 기술들이 보호받을 가치가 높다는 것을 인식하여 방위사업에서의 기술보호 방안이 중요한 공감대 형성을 하고자하였다.

우리나라는 방위사업 기술 수준이 세계 9위라는 점과 2022년 기준 170억 달러의

수출을 기록하는 등 수출 역량도 우수하기 때문에 세계적인 안보와 타 국가의 무기체계 수준에 대해 미칠 수 있는 영향력도 높게 판단할 수 있다. 그렇기 때문에 인공지능이 탑재된 무기체계가 개발되었을 경우 이와 관련된 무기체계를 타국에 수출하는 것에 대비하여 적절한 인공지능 보안관리체계가 함께 구비되어야 하며 이를 통해 우수 방산수출국가 이미지를 유지하는 노력을 해야한다.

해당 장에서는 방위사업에서 인공지능이 방위사업에서 발전하고 있는 현황 분석을 통해 인공지능을 활용한 방위사업 기술보호 중요성에 대해 공감대를 형성하고 C4I, 정보, 화력, 기동, 방호, 작전지속지원 분야에서 활발하게 연구되고 있는 만큼 인공지능 방위사업 기술보호 방안도 함께 연구 필요성에 대해 부각하고자 했다.

Ⅲ. 방위사업 보안 현황과 취약점

3.1 현 방위사업 보안체계와 기술유출

보안이란 국가, 기관, 소속단체별, 기술발전, 시대변화 등에 따라 다양한 목적과 용도에 맞추어 사용되고 있다. 업무 분야에 따라 군사보안, 산업보안, 국가보안, 방위산업보안 등 다양하게 사용되고 있다.

산업보안 개념에 대해 기존 연구자료를 살펴보면 이창무(2017)는 '산업보안이란 단어는 산업과 보안이 합쳐져 만들어진 용어로 명확하게 개념이 정립되지 않았다'고 정리하면서 개념화에 중요성을 언급하고 있다. 방위산업보안도 방위산업과 보안이 합쳐져서 만들어 졌진 용어로 볼 수 있으며, 그 개념은 명확하게 정의되지는 않았으나, 연구자에 따라 다양 해석되고 있다.

보안총론(2011)에서는 '방산 및 방산관련업체의 비밀, 인원, 시설 및 정보통신망 등을 불순분자와 인가되지 않은자로부터 보호하기 위한 활동이나 대책'이라고 정의했으며, 류연승(2018)은 '방위산업보안은 불순분자로부터 생산・공급하는 방산물자 비밀을 보호하고 업체가 군이 필요한 시기에 공급할 수 있도록 지원하는 제반 활동'으로 정의했다. 또한, 우광제(2015)는 '군사보안과 산업보안이 복합된 것으로 방위산업의 보안 요소를 통합하는 융합보안'이라고 정리했으며, 고희재(2019)는 '방산물자를 생산하는 방산업체가 외부 위협으로부터 유・무형의 자산을 보호하는 활동으로 보호 자산, 비용, 위협, 기간 등 분야'로 개념을 정리하였다.

방위사업보안에 대한 개념은 명확하게 정립된 것을 찾아보기 어려우며, 위에서 살펴본 것처럼 연구자의 연구 목적에 따라 다양하게 해석될 수 있음을 알 수 있다. 본 연구에서는 위 연구자들의 의견을 종합하여 볼때 방위사업보안을 '내・외부의 위협으로부터 방산업체 유・무형 자산을 보호하는 활동'으로 정의하여 사용하

고자 한다.

방위사업 보안관리체계는 1973년부터 2015년까지 ‘군사기밀보호법’, ‘방위사업법’을 근거로 국방부에서 정립한 ‘방위산업보안업무시행규칙’을 바탕으로 보안업무를 수행해 왔었다. 2015년 이후부터는 ‘방위산업기술 보호법’을 근거하여 방위사업청에서 ‘방위산업기술보호지침’을 정립하여 방산업체는 두 개의 보안관리체계를 적용받고 있다.

<표 9> 방위사업 보안관리체계

구 분	군사기밀 보호법	방위사업법	방산기술 보호법
제정 년도	1972년	1973년	2015년
적용 대상	비밀취급 업체	방산업체	기술취급 업체
보호 대상	군사기밀	인원, 시설, 장비, 기술	방위산업기술
			방위산업기술
규 정	방위산업보안업무훈령(1977년)		방위산업기술 보호지침(2018년)

자료 : 고희재, “방위산업 보안수준 평가 지표 개발 연구”, 중앙대학교, (2021.)

방산업체는 ‘방위사업법’ 제35조를 근거로 방산물자를 생산하는 업체로서 대통령령에서 정한 시설 및 보안요건을 갖추어 산업통상자원부장관으로부터 지정받은 업체를 의미하고 있으며, 아래 <표 10>과 같이 방위사업법시행령 제44조(보안요건 및 측정 등)항목의 요구 보안요건과 ‘군사기밀 보호법’에서 요구 군사기밀 보호조치 내용을 준수해야한다.

<표 10> 방산업체 보안요건

구 분	내 용
보안 요건	1. 방산시설이 충분히 보호될 수 있는 지역 및 시설에 관한 보안대책 2. 방산업체에 종사하는 인원에 관한 보안대책 3. 비밀문서의 취급 및 보관·관리에 관한 보안대책 4. 방산물자 및 원자재에 관한 보안대책 5. 장비 및 설비의 보호대책 6. 통신시설 및 통신수단에 대한 보안대책 7. 각종 자료의 정보처리과정 및 정보처리 결과 자료의 보호대책 8. 보안사고에 대비한 관계정보기관과의 유기적인 통신수단 9. 그 밖에 보안유지를 위하여 방위사업청장이 필요하다고 인정하는 보안대책

자료 : 고희재, “방위산업 보안수준 평가 지표 개발 연구”, 중앙대학교, (2021.)

‘방위산업보안업무훈령’은 ‘방위사업법’을 근거로 정립된 국방부 훈령이며, 방산업체로 지정받기 위한 보안요건, ‘군사기밀 보호법’ 및 ‘보안업무규정시행규칙’상 군사기밀을 보호하기 위한 내용을 담고 있다. 구성을 살펴보면, 총칙, 문서·인원·시설·기업·정보통신 보안, 보안조사, 기타보안 순으로 구성되어 있다. 방위산업보안업무훈령은 각 보안 분야별로 방산업체 직원들이 업체 내부에서 준수해야 하는 사항을 기술하고 있으며, 보안규정 위반자는 별지에서 명시된 규정에 따라 처벌함으로써 군사기밀 등 방위산업정보가 대외로 유출되지 않도록 유지하는데 목적이 있다.

방위산업기술에 대한 정의는 방위산업기술 보호법 제2조에 명확히 나와 있다. 방위산업기술이란 방위산업과 관련한 국방과학기술 중 국가안보 등을 위해 보호되어야 하는 기술로서 방위사업청장이 지정하고 고시한 것으로 정의하고 있다. 그리고 유출에 의미에 대해서 살펴보면, 사전적 정의는 귀중한 물품이나 정보 따위가 불법적으로 나라나 조직의 밖으로 나가 버리거나, 내보내는 것으로 의미하고 있다.

따라서 방산기술의 법률적 정의와 유출의 사전적 정의를 종합해보면 방위사업 기술유출이란 방위사업기술을 불법적으로 나라나 조직의 밖으로 나가 버리거나 내보내는 것을 의미한다고 볼 수 있다.

방위사업의 보안체계는 기술유출과 밀접한 연관이 있다. 통상 보안유지를 실패하면 기술유출로 연결이 되는 것이 대부분이다. 예를 들면 개인정보에 대한 보안유지를 실패하면 이를 빌미로 접근하여 방위산업 기술 등을 요구할 수 있다. 일부 사례를 살펴 보면 아래와 같다.

2019년 대한민국 국방부는 444명의 항공우주전문가들의 개인정보가 해킹 공격으로 유출되었다고 발표하였다. 이후 전문가들은 적성국 또는 주변국으로의 이직 권유, 금전을 댓가로 한 기술 요구 등을 받았다. 이러한 정보가 유출되는 것은 대한민국 방위사업에도 큰 타격을 줄 수 있다.

2019년 대한민국 해군이 운영하는 정보통신망에서 해킹 공격으로 인해 약 10,000명의 해군 장병의 개인정보가 유출된 사례가 있었다. 이러한 개인정보 유출은 대한민국 해군 인적사항이 대외로 유출되어 보이싱 피싱 전화 등을 받았던 사례로 군의 정보를 유출 등 부정적인 영향을 초래할 수 있다.

보안이 부실하면 방위사업기술은 상대가 의도하는 대로 이용될 수 밖에 없다. 방위사업 기술유출의 유형은 방위사업청에서 국내·외 기술유출 사고사례를 바탕으로 방위사업기술 유출·침해사고 대응 매뉴얼을 통해 살펴볼 수 있다. 기술유출의 유형은 아래 표와 같이 사람에 의한 기술유출, 기업합병, 기술이전시 기술 유출, 정보시스템 사용부주의에 의한 기술유출 등이 있으며, 정리하면 아래 <표 11>과 같다.

<표 11> 방위사업 기술유출 유형

구 분	내 용
사람에 의한 기술유출	▪ 퇴사자가 경쟁업체에 기술 유출 ▪ 외국인 직원이 기술유출 ▪ 핵심 기술인력이 해외로 이직 또는 해외 창업
정보통신시스템 사용 부주의에 의한 기술유출	▪ 이메일, 팩스 무선공유기, P2P 등의 사용 부주의로 기술유출 ▪ 노트북, USB 등을 외부에서 분실
불법 수출에 의한 기술유출	▪ 국가의 수출 승인 없이 방산물자 및 방위산업기술을 수출
기업합병, 기술이전시 기술 유출	▪ 정부 승인 또는 허가 없이 합병 또는 기술이전 ▪ 계약 협상 단계에서 기술자료를 공유했으나, 계약이 파기되어 기술유출
보안성 검토 미흡에 의한 기술유출	▪ 저장장치, 운용장비 정비시 보안성 검토가 미흡하여 기술자료 유출 ▪ 외부로 공개되는 자료의 보안성 검토가 미흡하여 기술 공개
기 타	▪ 군 기관 등 사칭하여 기술자료 요청 ▪ 도청을 통한 기술 유출 ▪ 부도, 폐업시 기술유출

자료 : 방위사업청, “국방기술유출 매뉴얼”, p.17, (2022.)

방위사업 기술유출은 내부사정을 세부적으로 잘 알고 있는 전·현직 인력에 의한 기술유출이 다수를 차지하고 있다. 방위산업의 발전이 고도화됨에 따라 국가안보와 직결되는 주요 기술이 유출되는 경향을 보이고 있다. 그리고 안보에 영향을 준다는 이유로 공개를 하지 않는 부분이 많다.

대표적인 사례로 보면, 방산 관련 A업체 임직원들의 USB를 통한 기술유출, 한국형 구축함 기밀유출 등이 언론 등을 통해 공개되었지만, 방위사업 기술유출과 관련된 통계는 국가안보에 영향을 미칠 수 있다는 이유로 공개하지 않고 있어 일부 기관에서 공개한 기술유출 통계를 바탕으로 분석하였다.

첫째 산업기술보호지원센터에서 발표한 기술유출 현황을 분석하면 2015년부터

2022년까지 최근 7년 동안 기술유출은 약 101여건이 발생하였으며, 기술유출의 대다수는 보안 관리가 대기업에 비해 상대적으로 부족한 중소기업에서 약 81여건으로 집중적으로 발생하였다. 또한 이 가운데 국내 유출은 79여건, 국외 유출은 21여건이 발생하였다. 결과를 분석해보면 기술유출 관련 사례는 감소 없이 꾸준히 발생하고 있으며, 특히 보안이 취약한 중소기업에서 대부분 발생하고 있어 대책이 필요하다는 것을 알 수 있다. 최근 2015년부터 2022년까지 기술유출 현황을 정리하면 <표 12>과 같다.

<표 12> 2015년부터 2022년까지 기술 유출 현황

구 분	계	중소기업	대기업	국책연구기관
건 수	101	81	19	1

자료 : 산업기술보호지원센터, “방산기술 유출 현황”, (2022.)

둘째 기술유출 관련자 현황을 분석해보고자 한다. 중소벤처기업부에서 발간한 중소기업기술보호수준 실태조사 내용을 살펴보면, 기술정보를 외부로 유출시킨 주 대상자는 전·현직 직원, 용역업체, 외국인, 협력업체, 경쟁업체 등으로 나타난다. 특히 내부자인 전·현직 직원에 의한 유출이 전체의 80% 이상으로 조사되어 내부자에 의한 유출이 많이 발생한다는 것을 확인할 수 있었으며, 최근에는 퇴직자에 의한 기술유출이 상승하고 있어 관련 대책 마련이 필요한 것을 알 수 있다. 기술유출 관련자 현황에 대해 정리하면 <표 13>과 같다.

<표 13> 2015년부터 2022년까지 기술유출 관련자 현황

구 분	전 직원	현 직원	협력업체	경쟁기업	용역업체	고용외국인	외국인
비 율	69.3	14.8	8.0	6.8	2.3	1.1	4.5

자료 : 산업기술보호지원센터, “방산기술 유출 현황”, (2022.)

언론을 통해 공개된 방위사업 기술유출 사고를 살펴보면 18건을 확인할 수 있다. 이를 세부적으로 분석해 보면 매년 발생하는 것을 볼 수 있으며, 내부자에 의한 유출이 10건(55%)이고 해킹에 의한 방위사업 기술유출 사고는 4건(22%)이다. 이를 표로 정리해보면 <표 14>와 같다

<표 14> 언론에 공개된 방위사업 기술유출 현황

구 분	뉴스 제목	주체
2006년	1,700억원 신형 레이더 기술 해외 유출	전·현직
2007년	승진 조건으로 방산기술 유출한 일당 적발	전 직
2008년	대우조선 매각자분 선정 취소, 투자 방산기술 유출 우려	인수합병
	흑표 기술 터키 이전, 수출이냐 유출이냐	수 출
2009년	흑표, K1A1 전차 포신기술 유출	현 직
2010년	미얀마에 포탄기술 유출	전·현직
2012년	GPS 교란기술 북 정찰총국에 넘긴 듯	전 직
2013년	러시아로 기술유출 '방산업체 연구원 구속'	현 직
	세종대왕함 개발 방산업체 해킹	해 킹
2014년	단안경 야간 투시경 설계도 해외유출 포착, 방산업체 수사	현 직
	일감 따내려 국산 잠수함 기밀 독일에 유출	현 직
2015년	차기 무인기 개발 방산업체 기밀유출 의혹	외국인
	산업스파이 북 무기 거래국에 포탄기술 빼돌려	전 직
	KF-X 핵심장비 레이더 개발 방산업체 해킹 당해	해 킹
2016년	북 정찰총국, 독도함 만든 한진중공업 해킹	해 킹
	북한, SK 및 대한항공 전산망 해킹 방산자료 유출	해 킹
2017년	금호타이어, 중국업체 매각 반대, 기술유출만	인수합병
2020년	차기 구축함 기밀 빼돌린 현대중공업	현 직

자료 : 고희재, "방위산업 보안수준 평가 지표 개발 연구", 중앙대학교, (2021.)

이외에도 2010년 9월 K사 대표 임씨와 직원 오씨는 정부의 허가 없이 미얀마 국방사업소로부터 금전의 혜택을 받고 105mm 곡사포 고폭탄 등 6종의 포탄 생산 설비 및 기술을 760억원에 수출하는 계약을 체결 후 미얀마 현지에 포탄 제조 설비를 만든 후 포탄 제작이 가능하도록 도면과 공정도 등 전략물자와 기술을 제공한 혐의로 검찰에 구속되었다.

2014년 000사 대표 이씨는 경쟁업체인 OO사 직원 김OO, 이OO이 이직하면서 광학용 군사장비 설계도를 유출하게 지시한 후 제품 제작 목적으로 해외 업체들에게 부품을 주문하는 과정에서 설계도를 이메일 등으로 전송하는 등 불법 행위 혐의로 검찰에 구속되었다.

000중공업은 해군 최대 수송함을 건조하는 회사로 운영중이었다. 북 정찰총국 소속 해커로부터 해군 함정 건조를 위한 설계도 등 각종 기밀자료를 보관중인 업무망 컴퓨터를 해킹 당하여 기술이 유출되었다.

방위사업 기술의 유출 문제는 대부분 사람과 사람, 해킹에 의한 유출 등이 많으며, 사람과 사람에서는 금전과 관련이 있었다. 개인의 이득을 얻기 위해 국가의 안보가 위험해질 수 있고, 국가적으로 고부가 가치가 높은 것을 포기해야 할 수 밖에 없는 상황이 도래할 수 있다. 현재까지의 보안 취약점은 물리적인 행위와 사이버 해킹이 주를 이루었다고 볼 수 있다. 이러한 취약점은 앞으로도 지속 발생할 것으로 예상된다.[33)]

3.2. 인공지능 기반 방위사업 보안취약점

인공지능 기반에 따른 보안취약점은 현재 보고되고 있지 않다. 인공지능을 도입하여 활용하는 곳이 극소수이기 때문이다. 이에 따라 외국의 사례를 찾아보고 인공지능을 활용함에 따른 발생할 수 있는 보안 취약점을 분석하고 전망해 보았다.

33) 고희재, “방위산업 보안수준 평가 지표 개발 연구”, 중앙대학교, (2021)

2018년에 영국에서 일어난 사례로 TOO사의 서버에 DDoS 공격을 당했다. 375만 명의 웹사이트 사용자가 사용자 데이터베이스에서 신용 카드 및 은행 정보를 도난당했다. 이후 해당 정보를 활용하여 2019년에 불순분자가 인공지능을 사용하여 전화 통화 중 CEO의 목소리를 흉내 내어 에너지 회사를 속이고 £200,000을 절취하는 사건이 발생하였다.(KJ Hayward et al., 2021). 이것은 허위 정보를 전파하기 위해 제작된 인공지능 조작 딥페이크 기술을 활용한 것이다.

2023년 트럼프 전 대통령이 경찰에 체포되는 가짜 사진이 트위터 등을 통해 확산하고 있다고 보도되었다. 이는 인공지능 기술을 사용해 만들어진 가짜 사진으로 트럼프가 전 대통령이 자신을 체포하려는 경찰에 강하게 저항하거나 경찰을 피해 도망치는 모습을 담고 있다. 이 또한 미국 대선에 영향을 주기위한 딥페이크 기술이다.

[그림 7] 딥페이크를 활용한 사기

자료: 국방기술진흥연구소, “국가별 국방과학기술 수준조사서”, p.78, (2022)

딥페이크 기술은 신체인증을 악용한 우회 공격을 의미한다. '딥페이크(Deepfake)'란 인공지능 기술 딥러닝(deep learning)과 '가짜'를 의미하는 페이크(fake)의 합성어를 의미한다. 인공지능 기술을 이용하여 생성한 진위 여부에 대한 판단이 매우 힘든 가짜 이미지나 영상을 의미한다. 딥페이크는 2017년 미국 온라인 커뮤니티 Reddit의 회원이 기존 영상에 유명인 얼굴을 합성하여 가짜 콘텐츠를 게재한 데서 유래되었다. 딥페이크는 인공지능 기술 측면에서 볼 때, 딥러닝 기반의 신경망 모델 중에서 새로운 이미지를 만들어내는 생성망 모델을 기반으로 동작한다. 특히 생성망 모델 중에서 '오토인코더'[34] 모델 또는 '생성적 적대 신경망 GAN(Generative Adversarial Network)'[35]이라고 불리는 모델을 주로 사용한다.

2014년에 등장한 GAN은 인공지능 모델을 생성모델과 분류모델로 구분하며, 각 모델의 학습을 반복하는 과정을 거친다. 이 과정에서 생성모델과 분류모델은 서로를 적대적 경쟁자로 인식하며 학습한다. 이에 따라 생성모델은 실제와 유사한 데이터를 생성할 수 있고, 분류모델은 데이터의 진위여부를 구별할 수 없게 된다. 이 과정을 반복 학습함에 따라 원본과의 구분이 어려운 결과물을 생성한다. 최근에는 인공지능이 사람의 피부 및 머리카락까지 육안으로 구분하기 불가능할 정도로 실제와 동일한 이미지를 생성하고 있다.

34) 비지도학습 방식으로 훈련된 인공 신경망으로, 먼저 데이터에 인코딩 된 표현을 학습한 다음, 학습 된 인코딩 표현에서 입력 데이터를 생성하는 것을 목표로 한다. 따라서, 오토인코더의 출력은 입력에 대한 예측이다.

35) 생성자와 식별자가 서로 경쟁(Adversarial)하며 데이터를 생성(Generative)하는 모델(Network)을 의미

[그림 8] 딥페이크를 이용해 재현한 이미지

자료: 정보와 통신, “인공지능 기술 발달에 따른 사이버 위협과 이에 대한 대응 방안”, (2022.)

위 그림은 딥페이크 기술을 이용하여 기존 영상 속의 특정 인물의 얼굴 위에 다른 인물의 얼굴을 합성한 결과를 보여준다. 원본 대조가 불가능한 경우 재현된 결과임을 판단하지 못할 위험성이 매우 커진다. 미국 UC버클리대와 영국 랭커스터대 공동연구팀은 실제 얼굴과 인공지능이 합성한 얼굴을 구별하는 실험을 진행하였다. 실험 결과, 사람들은 진짜와 가짜를 좀처럼 구별하지 못했으면 어떤 경우는 오히려 가짜를 진짜보다 더 신뢰하기도 했다.

SNS 이용자가 갈수록 증가하면서 개인정보 유출 사고가 잦아지고 피해사례도 증가하고 있다. 이에 따라 지문 인식, 안면 인식, 홍채 인식 등의 생체인식기술을 보안강화를 위해 추가로 도입하여 사용하는 추세이다. 그런데 딥페이크 기술은 이러한 추세에 편승하여 개인 SNS나 유튜브 등에서 특정인의 목소리, 이미지 등을 수집하여 인공지능에게 학습을 시켜서 특정인의 생체인식정보를 모방할 수도 있다. 이러한 공격기법은 방위사업의 생체 인증 관련 취약점을 악용할 수 있다.

가짜뉴스, 신종 금융사기 등을 활용한 사건이 방위사업에서도 발생할 수 있는 상황이다. 비즈니스 이메일, 화상 회의 등에서 특정 대상을 사칭 후 금전을 탈취해 가는 침해기술이 예상되고 있다. 방위사업체 개인정보 관리, 재무부서 등 기업의

주요 정보에 대한 접근이 가능한 직무를 지원하는 과정에서, 딥페이크 기술을 이용하여 거짓 신분으로 방위사업에 관여하여, 기업의 주요 핵심 정보에 접근하는 방식을 사용할 수 있다. 최근 인공지능 면접 등 온라인 취업 절차가 증가함에 따라 딥페이크를 이용한 불순분자들의 거짓 취업도 가능할 것으로 보인다. 미국 FBI 정보에 의하면, 기존에 유출된 개인정보를 기반으로 인공지능 딥페이크 기술을 활용하여 특정인을 대리하여 면접을 응시하는 경우가 증가하고 있음을 알 수 있다.

스팸 및 피싱 메일에 취약해질 수 있다. 인공지능 학습 방법의 머신러닝은 스팸 메일의 반복되는 패턴을 인식하여 이를 차단하는 기술로 활용되고 있다. 그러나 머신러닝의 스팸 필터가 특정 메일을 차단하는 기준과 스팸 지수 등 추가적인 정보를 생성할 경우, 불순분자는 이러한 정보들을 집약하여 분석함으로써 스팸 필터를 피할 수 있는 메일을 작성할 수 있게 된다. 불순분자가 이메일을 반복하여 전송함으로써 메일 서버 안의 머신러닝 스팸 필터 모델이 작동하는 기준을 파악할 수 있어서 이처럼 분석된 정보를 기반으로 머신러닝 스팸 필터 우회가 가능한 내용의 이메일을 작성할 수 있게 된다. 심지어 이러한 우회용 이메일의 내용을 작성할 때 아예 인공지능을 활용할 수도 있다. 일단 스팸 필터에 의하여 차단되지 않는 피싱용 이메일을 작성한 후, 방위사업체 PC 내의 회사 내 직원들의 사진과 프로필 등 활용하여 인공지능을 통해 직원인것처럼 생성하여 사용자가 적대적인 이메일을 신뢰하여 열람할 수 있도록 충분히 생성할 수 있다.

인공지능 퍼징(AI fuzzing)에 취약할 수 있다. 퍼징(fuzzing)이란 소프트웨어의 취약성을 발견하기 위한 테스트 방법의 하나이다. 불순분자가 아닌 일반 사용자가 사용할 경우, 퍼징은 고의로 예외를 발생시킴으로써 방위사업체에서 활용하고 있는 윈도우와 같은 소프트웨어의 동작을 분석할 목적으로 사용할 수 있다. 이 과정에서 입력으로 사용하기 위한 무작위 데이터 생성 과정에 인공지능이 사용된다. 예외 발생 가능성이 큰 문자열의 우선순위를 부여함으로써 체계화된 방식으로 입력 값 생성이 가능하다. 그런데 일반 사용자가 아닌 불순분자가 이를 활용할 경우,

인공지능에 의해 자동화된 시스템의 네트워크 취약점 획득, 잠재적인 공격 및 취약점 탐색 등에 활용할 수 있게 된다. 전통적인 퍼징 기법은 취약점의 효율적 발견에 이용되어 왔으며 특히 인공지능을 이용한 퍼징의 경우 무수한 반복작업 등 그 효율성이 높아지므로, 이를 불순분자가 역으로 이용할 경우 방위사업체 전체 운영체제를 통제할 수 있는 위험성이 매우 높은 해킹 도구로 다시 평가되면서 보안 측면에서 큰 우려를 낳고 있다.

3.3. 소 결

방위사업보안에 대해 명확하게 정의된 것이 없다. 그렇기 때문에 과거 연구자들의 연구결과를 종합하여 결론을 내어보면 내·외부 위협으로부터 방위사업체 유무형 자산을 보호하는 활동으로 해석할 수 있다.

방위사업 보안관리체계는 군사기밀 보호법, 방위사업법, 방산기술 보호법의 3가지 법에 의하여 보호 및 관리되고 있다. 그럼에도 불구하고 방위사업에서 기술유출은 지속 발생하고 있는 상황이다. 유형별로 보면, 사람에 의한 기술유출이 가장 많았고, 정보통신시스템 사용 부주의, 불법 수출, 기업합병, 기술이전, 보안성 검토 등에 의한 기술유출이 있었다. 2015년부터 2022년까지 방위사업 분야에서 기술유출 현황을 살펴보면 약 100여건이 발생하였으며, 가장 많은 사례인 사람에 의한 기술유출에서 인원별로 분석해보면 전·현직 직원에 의한 기술유출이 대부분이었고, 이는 국가의 안보와 방위사업체의 경제적 피해를 발생시켰다.

인공지능이 방위사업에 접목되어 보안 취약점이 발생한 사례는 2022년까지 공개된 국내 사례는 없다. 이는 가시적으로 적용하고 있는 인공지능 산물들이 없기 때문이다. 관련된 내용을 분석하기 위해 외국의 인공지능 적용에 따른 보안 취약점을 살펴보면 딥페이크, 스팸 및 피싱, 퍼징에 의한 보안취약점이 대부분이었다.

딥페이는 특정 사람의 사진과 목소리 등을 똑같이 묘사하여 사람들을 속이는 방

법으로 향후 생체인증과 같은 시스템을 무력화 시킬 수 있다. 스팸 및 퍼징은 스팸메일을 필터링하는 방안을 인공지능이 찾아내어 표적으로 하는 대상자에게 스팸메일로 인식하지 못하는 악성코드 메일을 전송하여 대상자의 컴퓨터를 장악하여 본인이 원하는 정보를 빼낼 수 있다. 퍼징은 컴퓨터 환경의 취약점을 찾아내는 명령어를 반복적으로 전송하여 운영체제의 취약점을 찾아내는 것이다. 인공지능 도입에 따른 보안 취약점은 대부분 사람 및 사이버와 관련된 보안취약점으로 향후 대한민국 방위사업에 인공지능이 적용되는 시점에서 보안취약점 해소를 위해 발전이 필요할 것으로 예상된다.

Ⅳ. 인공지능을 활용한 기술보호 및 보안강화 방안

4.1. 미국의 방위사업 보안 및 기술보호 강화

인공지능 기술의 발전으로 인해 방위사업 시장은 지속적인 변화를 겪고 있다. 인공지능 기술은 방위사업 분야에서 중요한 역할을 담당하며, 군사적인 목적뿐만 아니라 국내·외 시장에서도 높은 인기를 얻고 있다. 방위사업에서 인공지능 기술은 센서와 빅데이터와 융합하여 활용되어 군사적인 정보를 수집하고 분석하면, 군사작전에서의 전략적인 의사결정과 정확한 정보 전달이 가능해진다. 또한, 인공지능 기술을 활용하여 방위사업 제품의 생산성을 높일 수 있다. 인공지능을 활용하여 생산 공정을 인공지능화하면, 생산 공정의 효율성과 생산성을 높일 수 있다.

이는 빠른 시간에 대량생산이 가능해짐으로써 생산시간 및 비용을 절감하는데 큰 도움이 되는 것이다. 인공지능 기술을 활용하여 방위사업 제품의 성능을 과거와 다르게 빠르게 제품의 성능 분석 및 평가가 정확하게 이루어질 수 있으며, 이

를 통해 제품의 성능 개선이 가능하다. 이러한 기술을 지속 이용하기 위해서는 보안 취약점을 관리하여 기술을 보호해야 하는 과제가 남는다. 미국의 대책을 살펴보자.

미국에서는 해킹 및 기술유출에서 방위사업을 보호하기 위해 다양한 방법을 시행하고 있다. 이를 위해 미국 국방부는 정보보호 및 사이버보안 강화에 대한 전략을 수립하고, 이를 기반으로 다양한 대응책을 실행하고 있다. 보안 강화측면에서 미국 국방부에서는 시스템 보안 강화에 최우선적으로 노력하고 있다. 보안 전문가들이 취약점을 찾아내고 이를 해결하며, 인공지능을 활용하여 보안 취약점과 위협에 대한 모니터링과 경고 시스템을 구축하고 있다. 인공지능에 대한 주요 취약점으로 정리한 내용은 아래 표와 같다.

<표 15> 인공지능에 대한 보안 위협 종류

구 분	내 용
개인정보 유출	• 인공지능 기술이 들어간 기기들에서 수집된 데이터를 사용자 동의 없이 유출하여 사용
보이스피싱	• 목소리를 모방하는 합성기술로 사칭 및 해킹
적대적 스티커	• 이미지 인식 모델에 인식시키는 '노이즈'를 추가함으로써 이미지의 피사체를 오인시키는 공격 방법. 이런 오작동 문제를 자율주행 자동차에 악용하여 사고를 일으키는 문제
스피어 피싱	• 공격자가 사전에 공격 목표와 관련된 정보를 수집하여 공격하는 형태
인공지능 시스템의 블랙박스 모델 추출	• 블랙박스 모델 내부의 매개변수를 추출하여 악의적으로 사용자가 기본기술에 접근 가능
정교하고 자동화된 스웜 공격	• 취약점 및 액세스 포인트, 장치를 공격하는 스웜 공격 방식은 해커의 명령만 받는 봇넷과 달리 자가 학습이 가능하고, 서로 정보를 교환하여 다수의 피해자를 공격

자료 : 박용병, "인공지능 딥러닝 소개와 보안 동향", (2021.)

미국 방위사업 측면에서는 취약점을 보완하고 예방 강화를 위해 각 분야별로 연구하고 있다. 먼저 기술 보호측면에서 미국 국방부에서는 기술 보호에 매우 높은 우선순위를 두고 있으며, 정보 보호를 위해 보안 강화 및 양자암호화·블록체인 기술을 적용하고 있으며, 유출 및 탈취될 수 있는 기술들은 분리 보관 등 특별한 대책을 취하고 있다. 특히, 사이버 보안 전문가를 활용하여 방위사업의 정보 보호를 강화하고 있다. 이들 전문가들은 인공지능의 알고리즘을 통해 취약점을 찾아내고, 이를 해결하며, 시스템을 모니터링하여 보안 위협을 탐지하는 등 다양한 보안 업무를 수행하고 있다. 방위사업에서 주 적용하는 기술보호방안으로는 다음과 같다.

첫째, 평소의 시스템 흐름과 달리 특이한 현상이 식별되면 반응하는 인공지능 기술을 활용하여 보안 위협을 탐지하고 대응하는 시스템을 구축하고 있다. 인공지능을 활용하여 비정상적인 네트워크 트래픽이나 사용자 활동을 식별하여 이상·악성 행위를 탐지하고 예측하는 기술을 보유하고 있다. 시스템을 사용하면 대량의 보안 로그 및 이벤트 데이터가 남을 수 밖에 없다. 이를 분석하고 모니터링하여 인공지능에 학습된 자료와 다를 경우 이를 경고하고 차단하는 것이다.

둘째, 악성 웹사이트, 스팸 이메일, 사이버 위협 및 공격에 대한 정보를 수집하고 분석하여 시스템에 접근하는 침해공격에 대해 사전에 차단하고 있다. 침해공격에 대한 정보를 국가 기관 및 해외 자료를 통해 인공지능에 학습시켜 특정 IP를 차단하고 사용자에게 경고하고 있다. 그리고 이를 자동화하여 보안인력의 업무 효율성을 높이고 있다.

셋째, 법적 조치측면에서 미국 국방부에서는 인공지능을 활용한 방위사업 기술보호에 대해 법적 근거 마련을 추진하고 있으며, 해킹 및 기술유출을 방지하고 대응하고 있다. 법적인 조치는 방위사업의 정보 보호를 위한 중요한 수단 중 하나로, 기밀 정보를 유출하는 행위에 대해 엄격한 처벌을 명시함으로써, 기술유출에 대한 심각성을 국민들에게 인식시키고 있다.

지능형 사이버 공격에는 지능형으로 대응하는 것이 효과적이기에 머신러닝과 같은 알고리즘을 바탕으로 인공지능 방어가 필수적이라 볼 수 있다. 민간의 인공지능 기술이 미국 방위사업에서 가지고 있는 기술보다 우수하기 때문에 적극적으로 민간 기술을 받아들이고 있다. 민간업체들의 인공지능 보안 강화를 위한 활동들은 아래 표와 같다.

<표 16> 선진국 업체들의 인공지능 보안 강화 추진 분야

구 분	내 용
와트릭스	• 체형과 걷는 방법을 분석 및 비교하여 사람을 인식할 수 있는 '보행인식' 기술을 개발, 이 시스템은 모든 시민들의 행동을 기반으로 식별할 수 있으며 고유 번호를 부여하여 개인별 정보로 활용
구 글	• 하루에 1억개 이상의 스팸 메일을 차단 하기 위해 머신 러닝 오픈소스 프레임 워크 텐서 플로를 활용한 방안 마련 • 악성코드가 숨겨져 있는 이메일, 이미지를 기반으로 한 메시지, 새로운 도메인으로부터 발송된 악성 메시지, 스팸이지만 정상 트래픽과 구분이 가지 않는 경우도 탐지 가능
IBM	• 랜섬웨어와 같은 개인에게 금전을 요구 하는 악성 해커들로부터 피해를 예방하고 사이버 범죄로부터 사고를 예방할 수 있는 클라우드 기반의 지능형 플랫폼 'X-Force Exchange'를 개발
시만텍	• 인공지능과 머신러닝을 적용한 공격패턴 분석 기술 '시만텍 표적 공격 애널리틱스 (Symantec Targeted Attack Analytics)'를 개발
아마존	• 정상적인 패턴과 다른 모든 이벤트 식별하는 머신러닝 으로 AWS 계정을 보호하는 '아마존 가드듀티'를 개발,
파수닷컴	• 머신러닝 기술을 기존에 개발된 보안 기술 시큐어코딩 솔루션 '스페로우'에 적용, 개발 단계부터 소스코드의 보안 취약점을 정확하고 빠르게 제거하여 보안취약점 해결

자료 : 정보통신기획평가원, "주간기술동향 1888호", (2019)

구글은 오픈소스 인공지능 기술을 이용한 악성코드 분석하여 위협탐지 및 예방, 취약점을 분석하는 연구가 진행되고 있다. 인공지능의 기술은 대부분 민간에서 군으로 도입되는 Spin-on 형태가 대부분이다. 그렇기 때문에 방위사업 분야에 적용되는 인공지능 활용 분야도 대부분 민간기술로부터 응용하는 형태로 운영되고 있

다. 그렇기에 군 내부보다 빠르게 발전하는 민간 보안기술에 대해 민감하게 접목할 수 있는 방안을 모색하고 있다. 군에서 운용되는 장비들은 인명 위험성에 큰 영향을 가하기 때문에 보안 강화 대책은 더욱 중요할 것이다.

미국 방위사업은 민간의 기술인 블록체인 기술을 군사적 용도로 도입하여 보안을 강화하고 있다. 이는 미국뿐만 아니라 러시아, 중국 등에서도 연구를 수행하고 있다. 미국에서는 사이버 보안을 위해 블록체인 연구를 추진하는 '군사비 지출 법안'을 승인하여 DARPA에서 해킹이 블가능한 블록체인 기반의 시스템을 연구 중에 있다. 이후 미국은 지휘통제 시스템과 무기 공급 등 군수 조달 분야에도 접목시키기 위해 노력중에 있다. 러시아는 국방기술 진흥원 예하에 '블록체인 연구소'를 설립하여 사이버 공격 탐지 등 중요 데이터베이스를 보호할 수 있는 방안을 연구중에 있다. 중국에서는 군사훈련 성과 평가, 기밀 정보 보호, 물류감시 등에 블록체인 기술을 접목하는 연구를 추진중에 있다.

미래 인공지능 사회에서 보안분야는 거스를 수 없는 대책으로 다가오고 있다. 블록체인 기술을 도입하여 정보 위변조에 의한 시스템 조작 및 인사 정보 작전 관련 데이터베이스를 보호하여 무결성 및 기밀성을 보호하는 것이다. 블록체인에 연계할 수 있는 군내 특정 사용자들을 그룹핑하여 실시간 자료가 공유될 수 있도록 하여 해킹 및 데이터베이스 오염으로부터 보호하는 대책을 적용하는 방향으로 나아가고 있다.

4.2. 방위사업 보안 인증제도

인공지능을 활용한 방위사업 보안 인증제도를 살펴보고자 한다. 통상 개인이 갖출 수 있는 자격과, 업체가 방위사업체 자격을 갖추기 위한 기본적인 인증으로 나눌 수 있다. 먼저 개인이 인증할 수 있는 자격증을 살펴보고자 한다. 일반적으로 인공지능의 보안에 대해 이해하기 위해서는 인공지능에 대한 이해부터 필요하다. 그리고 이러한 능력을 갖추고 전문가가 되기 위해서는 각종 과정교육과 인증할 수 있는 자격증이 필요하다. 2023년 초 국내에 인공지능과 관련된 자격증은 'K'회사에서 시행중인 자격증 AICE(AI Certification for Everyone)이다. 이는 국가에서 인증되지 않은 민간자격으로 2022년 기준 국가에서 공인한 인공지능 자격증은 없는 상황이다. KAIST 등 대학교에서 인공지능에 대한 교육체계를 정립하기 위해 노력중에 있으나, 자격증과 같은 인증제도는 아직 정립되지 않았다. 즉, 방위사업에 적용할 수 있는 인공지능 보안 인증제도는 찾기 어려운 상황이다.

미국의 인증제도에 대해 살펴보고자 한다. 미국의 인공지능 열풍은 2016년부터 시작되었다. 국가보다 먼저 업체들이 먼저 인공지능 개발을 위해 노력하고, 직원들의 이해도를 높이기 위해 각종 인증제도를 진행하고 있다. 미국도 대한민국과 동일하게 국가에서 공인한 인공지능 자격증은 없다. 다만, 각 주요업체에서 자격인증을 만들었으며 미국 방위사업에서도 이를 활용하기 위해 방안을 모색중이다. 세계 최대 클라우드 서비스 기업인 미국 AWS(Amazon Web Service)는 인공지능 자체 자격증을 12개를 만들어 운영하고 있다. 이는 기초, 준전문가, 전문가(인프라) 등 수준별로 자격증을 나누고 '빅데이터', '머신러닝' 등 세부 분야에도 별도 추가 자격을 인증하고 있다. 또한, 2016년 직원들을 교육하기 위해 '머신러닝 대학'을 설립하여 체계적인 교육의 시초를 만들었으며, 2020년도에는 일반인들에게도 모든 과정을 공개하고 있다. 미국의 주요 기업의 인공지능 관련 인증과정은 아래 [그림 9]와

같다.

기업	자격·과정명	특이사항
aws 아마존웹서비스	AWS인증	기술 수준·전문 분야별로 자격 세분화
구글	TDC	자격 보유자 전용 플랫폼 지원
NVIDIA. 엔비디아	젯슨AI	학습용·교수용 자격 별도 운영
IBM	AI 엔터프라이즈 워크플로 인증	초급자·전문자용으로 구분

[그림 9] 인공지능 관련 업체 및 자격・교육과정

자료: 한경신문, “AI 활용 능력′ 검증할 수단 없는 한국…아마존은 자체 시험만 12개”, https://www.hankyung.com/economy/article/2022100209481, (2022,10.22)

구글은 인공지능 개발자 공인 인증 프로그램인 TDC(Tensorflow Developer Certificate) 자격증 제도를 운용하고 있다. 인공지능 툴 텐서플로를 기반으로 머신러닝 모델 개발, 컴퓨터 비전, 자연어 처리 등을 다루는 과정이다. 자격만 주는 것이 아니라 교육생들을 관리까지 하고 있다. TDC 자격을 가진 인원들은 서로 정보를 교류하고 구글회사 채용시 가산점을 받을 수 있도록 지원하는 자체 네트워크를 가지고 있다.

엔비디아는 자체 교육프로그램 딥러닝 인스티튜트(DU)를 통해 인공지능 자격증 ‘젯슨 인공지능’을 운영한다. IBM도 자체 인공지능 전문 자격증 프로그램을 가동하고 있다. 초보부터 교육을 받을 수 있는 인공지능 초급인증 과정, 실력 향상을 원하는 인공지능 개발자・데이터 사이언티스트 등을 위한 전문 자격 과정도 두고 있다. 이와 같은 기업이 자격증의 문화를 일반인까지 확대한 것은 실무형 프로젝트를 바로 실행할 수 있는 인재들을 만든다는 것이다. 각 기업에서 운용하고 있는 인공지능 자격증을 정리하면 아래 표와 같다.

< 표 17> 미국에서 운용중인 인공지능 자격증

구 분	자격증 명칭	내 용
아마존	AWS 인증	• 인공지능을 사용하여 솔루션을 설계 및 구현할 수 있는 능력을 검증
마이크로소프트	Azure AI Engineer Associate	• Azure 환경에서 인공지능 설계, 구현, 모니터링 및 유지 관리하는 능력을 검증
IBM	인공지능 엔터프라이즈	• IBM Watson을 사용하여 인공지능 솔루션을 설계, 구현 및 관리하는 능력을 검증
	Big data Engineer Certified	• 빅데이터 분석 및 보안 기술을 검증
엔비디아	젯슨 AI	• 딥러닝 기술을 사용하여 인공지능 설계, 개발 및 최적화하는 능력을 검증
구글	TDC	• 구글 클라우드 환경에서 인공지능 솔루션을 설계, 구현, 모니터링 및 유지 관리하는 능력을 검증

자료 : “구글, 국내・외 인공지능 능력시험”, http://kocw-n.xcache.kinxcdn.com/data/document/2021 /keris/kangsinok0712/02.pdf, (2023.4.25.)

여기서 공통적인 부분을 살펴보면 각 회사에 제작한 클라우드를 활용하고 있고 이를 기반으로 인공지능 인재들을 양성하고 있으며, 자격증을 발급하고 있다. 해당 회사에서 자격을 인증받거나 교육받은 인재들을 채용하면서 인공지능에 대한 전문성을 높이고 있다. 그리고 IBM에서는 ‘Big data Engineer Certified’ 이름으로 인공지능 보안과 관련된 자격증을 만들어 운용하고 있으며. 방대해진 데이터의 양과 무결성 보호를 위해 중요도가 높아지고 있다. 해당 자격증은 데이터 보안 전문가들이 빅 데이터 분석 및 보안기술을 이해하고 활용 관련된 지식을 담고 있다.

미국에서는 보안 자격 인증 차원에서 인공지능과 간접적으로 활용할 수 있는 공인 자격증을 운용중에 있다. 대한민국에서 운용중인 보안 관련 자격증보다 다양하고 보다 세분화되어 있으며, 자격검정도 엄격하게 운용되고 있다.

< 표 18> 미국의 보안인증 공인자격제도

	자격증명
미국	CISA(Certified Information System Security Auditor) 공인정보시스템감리사
	CISM(Certified Information Security Manager) 공인정보보안관리사
	CISSP(Certified Information System Security Professional) 공인정보시스템보안 전문가
	PSP(Physical Security Professional) 물리보안전문가
	ISP(Industrial Security Professional) 산업보안전문가
	CPP(Certified Protection Professional) 공인보안전문가
	APP(Associate Protection Professional) 보조보안전문가

자료 : 김화영, “산업보안 전문자격 활성화 방안 연구”, 중앙대학교, (2019)

미국 정보보호 분야의 전문가급 자격증은 CISA(공인정보시스템감리사), CISM(공인정보보안관리사), CISSP(공인정보시스템보안 전문가)이 있으며, 모두 해당 경력 5년 이상자에 한해서만 응시 가능하다.

물리적 보안분야와 관련된 자격제도로는 PSP(물리보안전문가)가 있다. 이들 자격제도들은 공통적으로 학력, 취득 자격증, 경력 등을 기준하여 응시자격이 제한되어 있으며, 아래 <표 19>와 같다.

< 표 19> 미국의 보안분야 자격제도

구분	CISA	CISM	CISSP	PSP
주최	ISACA	ISACA	(ISC)^2	ASIS
내용	• 정보시스템 감사·통제 및 보안실무를 응용 능력 및 정보기술 환경별 요구지식을 보유	• 보안관리와 컨설팅 서비스를 제공할 목적으로 정보보안 관리자 및 관리책임자의 경험 및 지식을 증명	• 정보보호 분야 전반의 일정 수준 이상의 자격을 갖추었음을 공인하는 자격	• 물리적 보안전문가 (취약점의 위험분석을 식별, 적절한 정책 수립)
자격	• 5년 이상 경력	• 5년 이상 경력	• 5년 이상 경력	• (학사학위자) 해당분야 경력 4년 • (APP보유 및 학사학위자) 해당분야 경력 3년 • (APP 보유자) 해당분야 경력 5년 • 해당분야 경력 6년
검정과목	• 정보시스템 감사 20% • 정보기술 거버넌스 및 관리 감사 18% • 정보 시스템 획득 개발 및 구현감사 11% • 정보시스템 운영 및 관리 서비스 관리 감사 24% • 정보자산보호 감사 27%	• 정보보안 거버넌스 23% • 정보위험관리 29% • 정보보안 프로그램 구축 및 관리 28% • 정보보안 사고관리 20%	• 보안 및 위험관리 15% • 자산보안 10% • 보안구조 및 공학 14% • 신원 및 접근관리 12% • 보안측정 및 테스트 13% • 보안운영 12% • SW개발보안 10%	• 물리적 보안 측정 33% • 물리적 보안시스템의 활용, 설계, 통합35% • 보안조치의 시행 32%

자료 : 김화영, “산업보안 전문자격 활성화 방안 연구”, 중앙대학교, (2019)

CPP(공인보안전문가)와 ISP(산업보안전문가)는 현재 국내 산업보안관리사처럼 산업보안 전반을 아우르는 자격제도이다. 이는 방위사업 보안 인증과 관련이 있다.

ISP를 관리하는 NCMS(The society of industrial security professonals)는 1964년 미국 산업계의 비밀 관리 담당자 및 정부 관계자들이 직업으로서의 비밀 관리자의 전문적 역량 발전을 위해 만든 비영리 보안 전문가 단체로서, 교육, 전문성 향상, 인적 교류를 목적으로 하고 있다. 2022년 기준 미국 및 해외에 약 7,000여명의 회원을 보유하고 있고 회원들은 국무부, FBI 등 관련 비밀을 다루는 연방정부 기관,

정부기관 직원, 이들과 협업하는 민간 계약자 직위에서 역할을 수행하고 있으며, 비밀 관리, 컴퓨터 보안, 정보보안, 인적보안, 시설보안, 작업보안, 기술보안 등의 분야에서 전문성 향상 지원 국가정책 워킹그룹에 참여하고 있다. 그리고 국가 방첩 및 정보기관의 발전을 위해 지속 지원하고 있다. NCMS에서 관리중인 ISP는 미국 국가 산업보안 프로그램(NISP)의 매뉴얼(NISPOM)에 기반한 시험으로, 정부 및 산업분야 보안을 다루는 담당자들이 전문적인 훈련 수료 및 자격에 대해 공식적으로 인정할 수 있는 대책을 마련하고 보안 업무종사자들의 자부심 고양과 전문교육을 제공할 목적으로 만들어졌다. ISP는 2013년 미국 국가 표준연구소(ANSI)에서 인증을 받았으며, 비밀을 다루는 국가기관과 계약하여 일하고자 하는 기업체 등에 수요가 있다

ISP가 국가적 비밀보호와 관련된 자격증이라 한다면, CPP는 기업 및 단체의 자산을 보호하는 국내에서 운용중인 산업보안관리사와 가까운 자격증으로 볼 수 있다. ISP와 CPP 모두 학력 및 경력의 응시자격 제한이 있으며, 경력에 중점을 두고 있다. 검정과목에서 국내 산업보안관리사 자격증과 달리 물리보안 및 정보보안보다 행정 및 관리, 문서보안, 경영원리, 정보, 분류, 인적보안(인사보안), 수사, 등이 별도 과목으로 구성되어 있음을 아래 <표 20>와 같다.

< 표 20> ISP 및 CPP 자격 인증

구분	ISP	CPP
관리	NCMS	ASIS
내용	• 정부 기밀 보호 기관의 보안 담당자 혹은 이와 동등한 업무를 수행하는 기관의 보안 담당자로 운영보안, 통신보안, 방첩 등 정부의 보안 요구 사항을 충족시켜주는 역할 수행	• 기업이나 단체의 영업비밀은 물론 유·무형 재산을 보호 및 관리 및 감독하는 보안전문가
검정자격	• 5년 이상 해당분야 경력 • 추천장(현 근무처 상사)	• (학사 학위 이상자) 해당분야 경력 7년 • (APP 보유한 학사학위 이상자) 해당분야 경력 5년 • 해당분야 경력 9년 • (APP 보유자) 해당분야 경력 7년
검정과목	• 보안행정 및 관리, 문서보안, 정보시스템 보호, 물리적 보안, 인적보안, 국제보안, 중요정보 분류, 보안교육, 감사 및 자가 측정 등	• 보안원리와 실무 10%, 경영원리와 실무 10%, 수사 10%, 인사보안 12%, 물리보안 25%, 정보보안 9%, 위기관리 10%

자료 : 김화영, “산업보안 전문자격 활성화 방안 연구”, 중앙대학교, (2019)

국내 보안관련 자격증은 정보보안기사, 산업보안관리사, 국방보안관리사가 있다. 해당 자격증은 국가에서 공인한 자격증으로 자격기준 및 검증 내용은 아래 <표 21>과 같다.

<표 21> 국내 보안 관련 자격증

구분	정보보안기사	산업보안관리사	국방보안관리사
관리	과학기술정보통신부	한국산업기술보호협회	국군방첩사령부
내용	• 정보보안의 이론과 실무능력을 갖추고 시스템과 응용서버, 네트워크 장비 및 보안 장비에 대한 전문가 양성	• 산업현장의 기술유출을 방지하기 위해 인력관리, 설비, 구역, 정보, 문서 등을 내·외부 위해요소로부터 침해받지 않도록 예방 관리하는 전문가	• 군 및 방위산업체 군사자료와 인원, 시설, 보호구역, 정보통신망 및 시스템은 비인가자로부터 보호하는 제반활동을 수행하는 전문가
검정자격	• 산업기사 자격증 취득 및 유사 직무분야 실무경력 1년 이상 • 유사 직무분야 실무경력 4년 이상 • 동일 및 유사 분야 외국자격 소지자	• 응시 자격 없음	• 국방보안관리 직무에서 1년 이상 실무경력과 군 복무 7년 이상한자 • 국방보안관리사 기본교육 이수자
검정과목	• 시스템 보안 - 운영체제, 클라이언트 및 서버보안 등 • 네트워크보안 • 어플리케이션 보안 • 정보보안 일반 • 정보보안 관리 및 법규	• 관리적 보안 • 물리적 보안 • 기술적 보안 • 보안사고 대응 • 보안지식 경영	• 국방보안경영 관리 • 국방정보기반체계 운용 및 관리 • 국방물리보안 구축 및 운용 • 국방비밀관리 • 국방보안수준평가 및 환류

자료 : 과학기술정보통신부, 한국산업기술보호협회, 국방일보 홈페이지, (2023.4.24.)

정보보안기사 자격증을 살펴보면 범위가 광범위하게 설정되어 있다. 이는 국가기관 및 업체 전반야에서 활용할 수 있는 자격을 부여하는 것으로 운영체제, 서버, 스마트폰, 시설 및 인력 위주의 보안에 중점이 맞추어진 것을 볼 수 있다. 산업보안관리사는 민간업체의 보안 담당자 수행 역할 위주로 구성되어 있으며, 데이터 및 네트워크 보호, 보안사고 대응 및 후속조치 분야에 초점이 맞추어져 있다. 국방보안관리사는 국방에서 운용중인 비밀 및 서버에 중요시하고 있어, 방위사업체 등에는 활용하기 좋으나, 일반 민간분야에 활용하기는 어려운 점이 있다.

국내에서 운용중인 자격증을 종합적으로 살펴보면 인공지능 기반의 방위사업 보안 전문가를 양성하기 위한 자격증으로 운용된다고 보기는 어렵다. 위 3가지 자격증을 융합하고 인공지능과 관련된 자격 내용을 추가하여 국가에서 공인할 수 있는 자격증의 필요성이 중요할 것으로 예상된다. (가칭) '인공지능 방위사업 보안전문가'로 하여 자격증을 신설하여 지속적인 인재 양성이 필요하다. 본 연구자가 생각한 내용, 검정자격, 검정과목은 아래 <표 22>와 같다.

<표 22> (가칭) 인공지능 방위사업 보안전문가(안)

구분	인공지능 방위사업 보안전문가
관리	국방부
내 용	• 인공지능이 적용된 방위사업 보안시스템에 대한 이해를 통해 서버·데이터 및 시설·인원에 대한 보안관리를 수행하고 정책 및 제도를 발전시킬 수 있는 전문자격 부여
검정자격	• 인공지능 분야 자격 1년 이상 또는 방위사업 종사자 1년 이상 • 유사 직무분야 실무경력 2년 이상 • 동일 및 유사 분야 외국자격 소지자
검정과목	• 인공지능 기반 방위사업 보안 개념 이해 - 인공지능의 역할, 방위사업보안 위협 및 공격, 방위사업보안 요구사항, 보안 모델 및 방법, 국방보안훈령, 방산기술보호법 • 머신러닝 및 딥러닝 보안 - 머신러닝 및 딥러닝의 개념과 원리, 모델 구성 및 훈련, 적대적 공격 및 방어, 데이터 보안 • 자연어 처리 보안 - 자연어 개념과 원리, 자연어 처리 모델의 보안 이슈 및 방어, 자연어 처리 데이터 보안 • 데이터 보안 - 데이터 보호 및 데이터 기밀성·무결성 유지(블록체인), 데이터 품질 및 관리 • 인공지능 보안 프레임 워크 - 서버 및 시설 보안(양자암호), 인원 관리, 방위사업 비밀 관리, 인공지능 보안관제 체계 등

(가칭) '인공지능 방위사업 보안전문가' 자격증은 민간에 개방하여 운용하는 것이 중요하다. 민간이 인공지능 기술 발전이 국방분야보다 빠르고 다양한 침해공격

을 경험하여 대응방안을 만들기 때문이다. 이를 국방에 적용할 수 있도록 민간에도 개방해야 한다. 자격증의 검정자격은 2년 이상의 유사실무를 가지고 있다면 응시 가능할 수 있도록 제시하였다. 이는 외부 불순분자가 악의적인 목적으로 자격증을 취득하여 방위사업 보안에 종사하였을 경우 국가 경제적 및 안보에 영향을 미치는 것을 고려하여 검증할 수 있는 기간이 필요하다고 판단하였다. 그리고 자격증의 진입 장벽이 높으면 국방분야 인공지능 보안에 대한 관심도가 떨어질 수 밖에 없기 때문에 미국의 5년 기준과 비교시 다소 낮게 설정하였다. 검정과목에 대해서는 방위사업에 특성을 이해해야 방위사업 보안에 설계를 할 수 있기에 '인공지능 기반 방위사업 보안 개념 이해'를 설정하였고 그 외에는 인공지능에 대한 공격사례 동향 등에 대해 이해하고 이를 대응할 수 있는 방안을 설정하였다. 그리고 향후 데이터를 보호할 수 있는 블록체인과 양자암호에 대해 기본적인 이해를 통해 데이터를 관리할 수 있도록 설정하였다.

인공지능과 관련하여 국가에서 공인한 자격이 없는 상황에서 미국의 각 업체는 자사의 클라우드 프로그램에 맞추어 교육을 진행하고 자격을 부여하고 있다. 현재 인공지능 보안 인증에 대해 준비가 필요한 것이 국내의 상황이다. 국내 업체 'K'회사는 자사의 프로그램을 활용하여 인공지능을 교육하고 자격증을 부여하고 있다.

이와 유사하게 국방부에서도 인공지능 활성화를 위해 '국방 지능화 센터'라는 이름으로 빅데이터 기반의 클라우드 구축을 진행중에 있다. 국방 지능화 센터에서 활용할 클라우드 프로그램의 특성에 맞도록 '(가칭) 인공지능 방위사업 보안전문가' 관련 자격증을 만들고 인재를 양성하도록 노력해야한다.

다음은 방위사업체의 인증제도에 대해 알아보고자 한다. 미국은 무기 등 전략물자를 미국 국방부에 납품시 사이버보안인증제도(CMMC)[36] 제도를 모든 국가에 적용할 예정이다. 미국의 CMMC는 방산업체의 보안관리 인증 제도로 3단계로 구성되어 각 부분을 검증하여 방위사업체의 등급을 부여하고 있다. 이는 미국 무기체

36) CyberSecurity Maturity Model Certification

계를 수출하는 국가와 상호 보호가 되어야 수출이 가능하도록 계획하고 있다.

미국의 CMMC에 대해 살펴보면 미국 국방부의 계약업체가 보유한 민감한 정보를 사이버 위협으로 부터 보호하기 위해 개발한 보안 성숙도 모델 인증 프레임워크이다. 미국의 국가정보체계는 Top Secret, Secret, Confidential로 분류·관리하는 국가안보 관련 기밀정보(Classified Information)와 기밀은 아니지만 보호가 필요한 통제 필요한 정보(Controlled Unclassified Information) 및 일반정보(Unclassified Information)로 구성되어 있다. 여기서 계약업체의 CMMC 수준을 3개 등급으로 구분하여 인증을 부여하는데 연방계약정보만을 취급하는 경우에는 1등급 자체심사가 요구되며, 통제 필요정보까지 취급하는 경우에는 2등급 또는 3등급 수준의 인증이 요구된다. 1등급의 모든 기업과 2등급 대상 중 일부 기업은 자체 심사를 통해 규정 준수에 대한 입증이 가능하고 제 3자 심사원의 전문적이고 윤리적인 감독을 강화하여 신뢰할 수 있는 평가가 되도록 하였다. 또한, 특별한 상황에서 기업의 마일스톤에 따른 실행계획을 통해 제한적으로 인증 획득 가능토록 하고 CMMC 인증도 제한적인 면제를 허용하고 있으나, 2025년까지 미국뿐만 아니라 미국에 전략물자를 수출하는 모든 업체에 적용할 예정이다

<표 23> CMMC 등급별 내용 및 심사 주관

등 급	내 용	심사
3등급 (전문)	110+개 항목 NIST SP 800-171,172 기반	3년 주기 정부주도 심사
2등급 (고급)	110+개 항목 NIST SP 800-171,172 연계	3년 주기 제 3차 심사
1등급 (기본)	17개 항목	연단위 자체 심사

자료 : 김동선, “미국 CMMC 제도 대응을 위한 통합실태조사 제도 개선 연구”, 한국방위산업학회, (2022.)

CMMC 1등급은 연방계약정보 보호에 중점을 두고 연방조달규정 조항에 명시된 기본적 보호 요구사항에 해당하는 항목로 구성이 되고, 2등급은 통제 필요정보 보호에 중점을 두고 국립표준기술연구소의 특별간행물 800-171에 지정된 110개의 요구사항으로 구성된다. 3등급은 국립표준기술연구소의 특별간행물 800-172 요구사항의 일부에 기반으로 정립중에 있다. CMMC는 14개 영역으로 구성 되어 있으며 2등급의 경우 아래 표와 같이 전체 110개의 항목을 가지고 있다.

< 표 24> CMMC 등급별 내용

영역	약 어	개 수
접근통제	AC	22
인식 및 교육훈련	AT	3
감사 및 책임추적	AU	9
구성관리	CM	9
신원확인 및 인증	IA	11
사고 대응	IR	3
유지관리	MA	6
미디어 보호	MP	9
인원보안	PS	2
물리적 보안	PE	6
위험평가	RA	3
보안평가	CA	4
시스템 및 통신보호	SC	16
시스템 및 정보 무결성	SI	7

자료 : 김동선, “미국 CMMC 제도 대응을 위한 통합실태조사 제도 개선 연구”, 한국방위산업학회, (2022.)

우리나라도 방위사업체의 통합실태조사를 통해 기술을 보호하고 방위사업체 적격여부를 판단하는 통합실태조사를 진행하고 있다. 통합실태조사는 6개 분야 237

개 점검 항목으로 구성되어 점검하고 있으며 세부내용은 아래 <표 25>와 같다.

<표 25> 방산기술보호 점검분야별 점검지표

구분	방위사업청				국정원	방첩사
	기술의 식별 및 관리	인력통제	시설보호	연구개발 및 수출 기술이전·협력업체	정보보호	군사기밀 관리
점검 지표	기술보호 내규	내규(인원)	내규(시설)	내규(연구)	내규 (정보보호)	군사기밀 취급 및 관리
	연간계획 ·성과분석	신원조사	기술보호 구역	연구개발 보호정책 및 관리	정보보호 시스템	군사기밀 보호구역
	기술보호 책임자	보직이동 및 퇴직시 대책	외부인·외국인 기술보호 구역통제	기술보호 활동이행	외부망 차단 체계 구비	군사기밀 전산자료 관리
	기술보호 교육	상주 및 상시 출입 및 외부인 관리	정보통신 장비사용 구 통제	수출 및 국내 이전시 보호체계	정보시스템 및 저장 매체관리	암호장비 및 보안자재 관리
	심의회 구성·운영	상주·상시 출입 외국인 관리	보호구역 방문 외부인·외국인 통계	합작·제휴·매매시 기술보호	자료별 접근 범위 제한	군사기밀 송수신
	기술유출 침해대응	기술취급 외부인 및 외국인 관리		협력업체 기술보호	보안관제 운용	군사기밀 보안사고
	자가진단	해외출장자 관리			사이버 위협대응	
	실태조사 후속조치				긴급사태대비	
	기술식별 및 등재					
	기술취급 및 관리					
	공개·제공시 절차준수					

자료 : 김동선, “미국 CMMC 제도 대응을 위한 통합실태조사 제도 개선 연구”, 한국방위산업학회, (2022.)

방위사업청은 기술·인력·시설·연구개발(이하 기술관리) 분야에 대해, 국정원은 정보보호 분야에 대해, 방첩사는 군사기밀 분야에 대해 실태조사 업무를 수행하도록 방위산업기술보호지침에 명시하였다. 이에 따라 방위사업청에서 통합실태조사를 계획하고 조사 결과를 종합하여 방산업체 및 유관기관에 통보한다. 정기적으로 실시하는 통합실태조사는 2022년 기준 85개 방산업체 및 국과연, 기품원 등 정부출연기관에 대해 국내 및 해외사무소를 포함하여 약 160여 개의 사업장을 매년 약 10개월간 실시하고 있다. 업체 규모나 기술보유 수준에 따라 A·B·C 그룹으로 수준별 분류하여 실태조사를 진행하고 있으며 조사기간은 사업장 당 3~5일 정도 소요되고 있다. 현재 조사관 인력부족으로 방산 협력업체까지는 통합실태조사 범위에 미치지 못해 민간에 위탁하여 실시하고 있는 실정이다.

2023년 초 진행중인 통합실태조사는 미국의 CMMC와 연계하여 개선되고 방산업체도 미국의 방식과 유사한 방안으로 인증체계를 갖추어야 한다. 미국의 CMMC와 비교시 대한민국이 진행하고 있는 통합실태조사와 비교시 아래 표와 같이 점검되지 않는 항목들은 아래 <표 26>과 같다.

< 표 26> CMMC와 통합실태조사 비교시 부족한 항목

항 목(19개)	종류	인공지능 보완 가능 여부
로그온 시도 실패	기술	○
개인정보보호 및 보안사항 안내	관리	○
세션 잠금	기술	○
세션 종료	기술	○
무선 접근 인가	기술	○
무선 접근 보호	기술	○
모바일의 통제필요정보 암호화	기술	○
감사 실패 경고	기술	○
신뢰된 시간 출처	기술	○
사용자 설치 소프트웨어	관리・기술	
ID 재사용	관리・기술	○
비밀번호 재사용	기술	○
유지관리 수행	관리	○
시스템 유지관리 통계	관리	○
보안 공학	관리	
연결 종료	기술	○
모바일 코드	기술	○
인터넷 전화	기술	
통신 진본성	기술	○

자료 : 김동선, “미국 CMMC 제도 대응을 위한 통합실태조사 제도 개선 연구”, 한국방위산업학회, (2022.)

위 항목을 통해 미국 CMMC와 비교해보면 사이버분야에서 차이가 나는 것을 알 수 있다. 통합실태조사는 기술(기밀)보호 및 정보보호 측면에, CMMC는 사이버 보안 측면에 초점이 맞춰져 있어 관점의 차이로 서로 지향하는 바가 조금은 차이가 있다. 통합실태조사에서는 인력통제·시설통제·정보보호 분야 뿐만 아니라 기술식별·연구개발·군사기밀 등 광범위하게 세분화되어 있어 CMMC를 포함하고 있는

반면, CMMC는 항목수는 적으나 정보보안 영역을 깊이 있게 다루고 있어 서로 미흡·부족함을 비교하는 것은 무의미하다고 본다. 하지만, 우리나라가 방산수출과 기술적 우위를 점하고 있는 미국을 대응하기 위해서 CMMC 제도와 맞추어 보안 인증제도를 발전시켜야 하는 것은 사실이다.

미국 CMMC와 비교시 부족한 부분은 대부분 사이버 보안분야이다. 이는 인공지능을 활용한 보안관제체계를 이용하여 총 19개 항목중 16개 항목은 해결이 가능한 것으로 분석된다. 기존에 수행하던 시스템의 알고리즘을 학습한 후 이와 다른 알고리즘 발생 감지를 통해 경고하고 차단할 수 있는 것이다. 미국의 방위사업 제도가 발전하고 있는 시점에서 국내의 방위사업체 인증제도도 개선이 필요한 시점으로 판단된다. 인공지능을 활용한 보안인증체계를 정립하여 사이버분야를 강화하고 취급하는 정보의 등급에 따라 국내 방위사업체를 미국과 동일하게 3등급으로 구분하는 것이 필요할 것으로 예상된다.

전반적인 인증제도를 살펴보면 인공지능을 활용한 방위사업 보안 관련 자격증을 신설하여 방위사업으로 적용될 인공지능에 대한 개인별 인증자격을 신설을 통해 인재를 발굴하고 관리해야한다. 그리고 방산기술보호법 및 제반 훈령 등에 대한 교육과 방위사업체 대상 실시하는 통합실태조사에 대한 개선을 통해 미국과의 활발한 교류 대응도 필요하다. 2022년 방위산업이 급격히 발전함에 따라 방산기술보호에 대한 중요성이 강조되고 있고, 이를 수행하기 위한 방산인력의 전문성 고도화가 요구되기 때문에 개인 및 업체 대상 인증제도는 발전이 필요하다. 이러한 인증제도 도입은 방산보안 인력에 대해 전반적인 전문성 향상뿐만 아니라 방산인력에게 자긍심과 자존감을 고취할 수 있어 실질적인 기술유출 예방효과를 달성할 수 있을것으로 판단한다. ‘국방 지능화 센터’가 개설이 되면 빅데이터를 기반으로한 인공지능 운용은 더욱 활성화될 것으로 예상된다.

4.3. 보안교육 프로그램

미국에서도 인공지능 방위사업 분야에서 기존 및 신규 인원에 대해 인공지능 관련 교육 필요성이 대두되고 있었다. 본격적인 교육 프로그램에 대해 살펴보면 미 의회는 2020년 국방수권법에서 미 국방부에 인공지능 교육전략 수립과 이행을 요구하였다. 미 국방부는 동년 9월 2020 국방 인공지능 교육전략(2020 Department of Defense Artificial Intelligence Education Strategy)'을 수립하고 교육 프로그램을 추진하기 시작했다. 국방 인공지능 교육 내용에는 전반적인 교육 프로그램과 일정, 자원투입 등의 계획수립(planning) 단계와 우선적인 시범사업, 그리고 결과 분석을 포함한 전면적 확대 추진(scaling)의 단계별 계획과 4대 교육 대상군을 선정하여 이들에게 우선 훈련하는 추진전략을 세우고 있다.

4대 핵심 교육 대상군을 살펴보면 ① 조직 내 인공지능 적용을 촉진시키고 광범위한 변화를 추진할 수 있는 중견 리더 대상 ② 인공지능 기술의 군사적 적용에 직접적 관여하는 영역의 전문가로 구성된 획득사업의 통합사업관리팀(IPT) ③ 분야별 인공지능의 적용 툴과 방안을 모색할 수 있는 소프트웨어 공학자, 사이버, IT 및 디지털 인력 대상, ④ 조직에 인공지능 역량을 배치하고 통합할 수 있는 인력으로 구분하고 있다. 또한, 교육과 함께 이들에 대한 자격 부여 및 관리가 이루어져야 한다는 점을 강조하고 있다. 국방 인공지능 교육전략에는 4대 핵심 교육 대상군을 포함하여 전체 국방부 인력을 아래 표와 같이 6가지 유형으로 구분하고, 유형별로 교육대상과 인공지능 분야에서 역할을 설명하고 있다.

< 표 27> 인공지능 유형별 교육대상과 역할

유 형	교육대상	내 용
선도	정책담당	정책과 교리 등을 결정하고 인공지능 비전과 계획을 수립
	지휘관	
	기관·조직 리더	
추진	획득관리자	적절한 인공지능 개발도구와 능력을 개발하여 전 분야에 적용할 수 있는 역할
	소요관리자	
	생산관리자	
	기술관리자	
개발	인공지능 연구원	현재와 미래의 소요를 충족하는 인공지능 도구 개발
	인공지능 엔지니어	
	시험평가 엔지니어	
	데이터 과학자	
	데이터 엔지니어	
적용	기술자	인공지능을 적용하고 사용자에게 전술단의 지원 제공
촉진	생산기업 소유주	사용자에 적합한 인공지능 도구가 개발되고 활용되도록 사용자를 대변
	국방혁신단	
	기타 기술전문가	
활용	작전	인공지능을 수단으로 최종 사용하는 인원으로 요구에 대한 조언 제공
	정보	
	군수 및 운영유지	
	의무 지원	

자료 : DoD, 2020 DoD Artificial Intelligence Education Strategy, p.7-p.8, (2020.9.)

교육과정 설계는 아래 표와 같이 인공지능 기본개념부터 인공지능 가능화까지 총 8가지의 인공지능 역량으로 구분하고, 요구되는 수준에 도달할 수 있도록 미국방부는 2020년부터 기획부터 시범사업을 거쳐 시행중에 있다.

< 표 28> 인공지능 역량 구분

구 분	과목 및 내용			
인공지능 역량 유형	기본개념	인공지능 기회 및 리스크	데이터 시각화 데이터 관리	책임성있는 인공지능
기 능	인공지능 이해 인공지능 적용 인공지능 개념 발전	리스크 식별 트렌드 식별	데이터 관리 데이터 시각화 데이터 준비	합법적, 윤리적 운영
인공지능 역량 유형	인프라, 코딩 및 소프트웨어 개발	데이터과학 수학, 통계학,	인공지능 배치	인공지능 가능화
기 능	프로그래밍 스크립팅 소프트웨어 엔지니어링 클라우드 운영 컴퓨팅 인공지능 테스팅 인공지능 프레임 워크	분석 수행	산출물 개발관리 인공지능 배치 감독 인공지능 전략 선도	사용자 중심 설계 지재권 관리

자료 : DoD, 2020 DoD Artificial Intelligence Education Strategy, p.8, (2020.9.)

국방 인공지능 교육 추진은 미 국방부의 인공지능 교육 전략(DoD AI Education Strategy)을 참고하여 우리나라도 국방부와 과학기술정보통신부가 협업하여 2022년부터 인공지능 교육 프로그램을 만들어 자체 시행하고 있다.

[그림 10] 인공지능 관련 국내 교육 프로그램

자료: 국방부, “국방부-과학기술정보통신부, 과학기술 강군 육성안”, (2022.5.27.)

국내의 국방 인공지능 교육은 정책담당자, 소요기획 및 관리 담당자, 체계개발 및 운용담당자로 3분류로 나누어 교육 프로그램을 운용하고 있다. 교육의 내용은 대부분 분야별 인공지능 적용에 중점을 두어 구성되어 있으나, 보안 전문가에 대한 교육은 없어 보안전문가 양성 방안은 강구되지 않는 것으로 볼 수 있다. 이는 군 차원에서 인공지능 보안 추진을 주체적으로 이끌어 나갈 전문인력을 지속적이고 체계적으로 양성할 수 있는 교육과정이 부재한 것이다. 국방부의 자체 예산편성을 통해 맞춤형 교육과정 개발이 필요하다.

본 연구자가 연구간 필요하다고 판단되는 보안 담당 직무지식을 바탕으로 생각한 교육프로그램은 (가칭) ‘국방 인공지능 보안 담당자 교육’ 명칭으로 보안전문가들이 인공지능 보안 교육을 받을 수 있도록 대상을 인공지능 교육과 함께 여건을 만들어야 하며, 본 연구자가 제안하는 인공지능 보안 교육 프로그램은 아래 <표 28>과 같다.

< 표 29> (가칭) '국방 인공지능 보안 담당자' 교육 프로그램(안)

구 분	내 용
이 론	방위사업 인공지능 침해공격 동향 및 트렌드(딥페이크 원리 등) 방산기술보호법, 국방보안업무훈령 프라이빗 블록체인, 양자암호학, 인공지능과 보안관제 인공지능 프라이버시 보호 인공지능 기초 및 알고리즘의 이해
실 습	인공지능 기반 생체인증 우회·스팸 및 퍼징 구별법 머신러닝·딥러닝·자연어 설계 및 처리 인공지능 사이버 위협 및 탐지 대응방법 국방 데이터 활용처리 실습(알고리즘 설계 등) 빅데이터 분석 및 서버 관리

인공지능을 활용한 침해공격 동향 및 트렌드는 시간이 지날수록 발전하기 때문에 최신 침해공격에 대해 학습이 필요하다. 그리고 기존에 수행하던 대응 방법에서 발전시켜 피해를 최소화할 필요가 있다. 이와 같은 대응수단은 지능화된 인공지능으로 처리하는 것이 가장 효율적으로 예상되고 있다. 그렇기에 이론적인 면에서는 최신 트렌드를 지속적으로 학습하고 대응방안을 찾아 인공지능에 학습을 시켜야 한다. 또한 빅데이터의 서버 내에 보관되어 있는 고가치의 정보들에 대한 무결성을 보존하기 위해서는 특정 인원들만 공유 가능한 '프라이빗 블록체인'에 대해서 이해하고 적용할 수 있어야 한다. 그리고 기존에 사람이 수행하던 보안분야의 반복적이고 침해 감시와 같은 업무들은 인공지능의 알고리즘 패턴을 통해 대체할 수 있다는 점을 볼 때 교육이 필요한 것이다.

인공지능으로 대체할 수 있는 소요들을 도출하고, 해당 과제들을 인공지능 알고리즘 설계를 통해 적용해야한다. 과거 인공지능의 실패 사례를 살펴보면 '이루다'라는 인공지능 기반 채팅봇이 채팅을 통해 입수된 개인정보를 타인에게 노출하는 경우가 많았다. 인공지능에 대한 알고리즘 설계시 개인정보에 해당되는 내용에 대해 구분하고 노출하지 않도록 학습하는 알고리즘도 동시에 필요할 것이다. 실습면

에서는 이론적 측면에서 배운 것에 대해 전반적으로 실습할 수 있는 내용들로 구성하였다.

본 연구자가 설계한 (가칭) '국방 인공지능 보안 담당자' 교육 프로그램(안)은 개인의 안으로서 방위사업 보안 전문가들에 대한 인공지능 교육이 부재한 것에 대해 필요성이 높을것으로 판단되는 요소들을 종합하여 작성한 내용이다. 인공지능에 대한 활용성은 중요시되고 있으나, 이를 활용하기 위한 보안 전문가 양성도 동시에 진행되어야 하나, 프로그램이 부재한 상황으로 대책이 필요할 것으로 판단된다. 또한, '인공지능 방위사업 보안전문가'를 양성하기 위한 교육프로그램 과정을 민간으로까지 확대하여 추진함으로써 미래 국방 인공지능 보안분야 발전을 이끌어 나갈 전문인력들을 점진적으로 확보해 나가는 방향으로 추진해야 할 것이다.

4.4. 방위사업 시스템 및 사이버 보안

미국의 사례와 같이 인공지능을 활용한 보안을 강화할 수 있는 대책이 필요하다. 그리고 빅데이터를 축적하는 것도 중요하다. 현재 국방망은 외부 인터넷망과 접속이 되지 않도록 망분리가 되어있다. 그렇기에 민간에서 축적되는 데이터의 속도와 맞추어 발전하기가 어려운 상황이다. 외부에서 축적되는 데이터는 각종 사물인터넷, 사람들이 생산해내는 정보 등 광범위한 정보들이 있으나, 이를 활용하기가 어려운 것이다.

정보보안의 3대 원칙은 무결성, 기밀성, 가용성이다. 3가지 모두 중요하기에 준수가 되어야한다. 준수하는 가운데 3가지의 비율을 조화롭게 구성하면서 방위사업도 함께 발전할 수 있는 방안을 찾아야 한다. 원초적인 망분리와 같은 개념에서 발전하여 외부 데이터까지 활용하면서 보안을 지킬 수 있는 플랫폼 형식의 데이터 보안이 중요해질 것으로 예상된다. 그 중 하나의 방법이 '프라이빗 블록체인(Private Blockchain)'이다. 인공지능은 데이터를 기반으로 운영되기 때문에 데이터

의 무결성이 중요하다. 블록체인은 비트코인이 이슈가 되면서 보안상 취약부분을 보완할 수 있는 기술로 거론되고 있다. 개념적인 해석으로는 온라인 거래에서 은행처럼 보증을 해주는 기관을 수천명의 유저들이 동일한 정보를 공유하여 하나의 컴퓨터가 해킹 또는 오염이 되었을 경우 이를 대변해주는 기능인 것이다. 예를 들어 악의적인 인원이 블록체인을 기반으로 한 비트코인을 특정 사용처에 사용 후 다른 사용처에도 중복 사용했을 경우에는 문제가 될 수 있다. 그러나, 블록체인은 유효한 거래내역이 시간 순서대로 연결되고 연결된 거래내역이 수정・폐기되지 않도록 모든 사용자에게 거래내역을 공유하는 것이다. 그렇기에 수천대의 전체 컴퓨터를 해킹하지 않고서는 해당 자료의 무결성 및 기밀성이 유지되는 것이다.

블록체인을 기반으로 데이터 저장·관리 인공지능을 활용하여 서비스 품질 및 안전성 제고를 결정지을 수 있다. 기존의 블록체인은 대상자의 범위가 광범위하다고 한다면 '프라이빗 블록체인'은 탈중앙화된 블록체인 데이터가 한정된 관계자에게만 공유되고, 참여자들이 함께 데이터를 검증하여 저장·관리하는 것이다. 방위사업에서 사용할 인공지능에 '프라이빗 블록체인'을 적용하면 해커의 침해공격도 사전에 탐지할 수 있고, 특정 블록에 침입을 했을 경우라도 다른 블록으로 피해가 확산되지 않도록 차단하는 기능을 구현할 수 있다.

일반적인 블록체인은 기밀성 보장측면에서 다소 낮은편이나, '프라이빗 블록체인'을 통해 기밀성 유지를 보완하는 것이다. 또한, 인공지능과 '프라이빗 블록체인' 융합의 공통점은 데이터보호, 신뢰성, IT 인프라의 절약과 비용 효율성, 보안 보장, 유연한 인공지능 구현 등을 들 수 있다. 인공지능은 대부분 데이터에 의존하고 있으며 이러한 데이터를 활용하여 머신러닝(또는 딥러닝)으로 스스로 발전하는 만큼 방위사업분야 인공지능 적용에서도 민감하고 비밀스러운 데이터 관리를 위해 보호된 분산형 인공지능 시스템을 구축하여 활용하여야 한다.

< 표 30> 블록체인의 주요 특징

특 징	내 용
탈중앙성	• 블록체인 네트워크에 참여하는 자들은 동등한 권리를 가지며 필요한 의사결정은 합의에 의해 도출되므로 제 3의 신뢰기관을 대체 가능
분산성	• 데이터는 똑같이 복제되어 참여자에게 분산되므로 투명하게 공개되며, 모든 복제본이 손상되지 않는 한 데이터는 보존되므로 가용성 보장 가능
불변성	• 암호화 기술을 활용하여 데이터를 시간 순서대로 연결하므로, 데이터가 수정되거나 변조되지 않도록 보장함.

자료 : 국방보안연구소, “국방보안연구 ISSUE”, (2022)

두 번째는 양자암호이다. 양자암호는 더 이상 나눌 수 없는 물리량의 최소 단위를 ‘양자(Quantum)’라고 한다. 해당 특성을 이용해 송신자와 수신자만 해독할 수 있는 암호키(Key)를 만들어 통신하는 기술이다. 초연결로 구성될 미래 방위사업에는 통신망을 통해 운용될 유·무인복합체계에 필요한 데이터, 바이오 및 생체 인증정보 등을 주고받게 될 것이다. 이러한 데이터는 방위사업의 보안과 관련되고, 개인정보를 담고 있어 보안이 중요할 수 밖에 없을 것이다. 현재 통신망은 디지털 신호 체계인 ‘0’과 ‘1’을 구분해 데이터를 주고받고 있다. 보안을 위해 암호키를 사용하고 있지만, 반대로 복호화 할 수 있는 암호키만 알면 해당 정보에 접근할 수 있다는 것이다. 즉, 특정 두 무기체계가 데이터를 주고받으며 임무 수행중 불순분자가 몰래 데이터를 가로챈 후 복제본으로 바꾸어도 변경 여부를 인식하기 어려운 것이다. 반면, 양자는 ‘0’이나 ‘1’이라는 특성이 결정되어 있지 않다. 정보를 송신하는 곳과 수신하는 곳이 각각 양자암호키 분배기를 가지고 있기에 매번 다른 암호키를 이용해 ‘0’과 ‘1’을 결정한다. 중간에 누군가 복제본을 변경하여 전송한다면 암호키가 이미 결정된 상태를 보고 노출되었다는 것을 바로 확인할 수 있는 것이다. 그렇기에 즉각적인 대응이 가능하여 데이터의 변형 등 침해공격이 불가능하다. 다

가올 인공지능 시대에는 모든 사물이 무선으로 연결되는 초연결성 바탕의 네트워크에서 보안은 매우 중요해질 것이다. 각종 센서와 수만 가지의 무기체계가 통신망에 연결되어 실시간 전장상황을 공유하고 통제하기 용이할 수 있지만, 해킹이나 도청이 발생하면 군의 역량에 미칠 파장은 매우 크다고 볼 수 있다.

복잡해지고 다양해지는 보안 이슈에 대응하고 침해공격에 대응하기 위해 양자암호 기술에 대한 관심이 증가하고 있으며, 양자컴퓨팅 기술의 발전으로 기존암호체계에서 양자암호 체계로 표준화해야한다는 필요성도 제기되고 있다. 양자암호는 3가지의 특징을 가지고 있다.

중첩의 원리로 여러 상태가 확률적으로 하나의 양자에 동시에 존재하고 측정하기 전까지 양자상태를 알 수 없는 특성이다. 예를 들어, 고양이가 방사선이 발생하는 상자에 넣어놓고 1시간후에 사망의 여부가 알 수 없듯이 열어보기 전에는 두가지 상태가 공존하는 것이다.

불확정성의 원리는 서로 다른 물리량이 동시에 정확하게 측정이 불가능한 특성이다. 여러 상태를 동시에 가지고 있고 이를 열어보았을 때 상태를 볼 수 있기 때문에 열어보기 전에는 확정지을 수 없다는 것이다. 위에서 언급한 고양이를 예로 들어 상자안의 고양이를 1시간 후 열어보기 전까지 고양이의 상태를 알 수 없다는 것이다.

다음은 복제 불가의 원칙이다. 양자암호는 위에서 언급한 바와 같이 여러 상태가 동시에 존재하고 열어보기 전까지는 상태를 알 수 없기에 복제도 불가능할 수 밖에 없다. 이를 정리하면 아래 <표 31>과 같다.

< 표 31> 양자암호의 주요 특징

특 징	내 용
중첩의 원리	• 서로 구별이 가능한 두가지 상태가 동시 존재할 수 있는 것, 복호화 전의 암호와 복호화 후 의 암호가 동시에 존재
불확정성의 원리	• 중첩이 되어 잇는 양자는 복호화하는 순간 형태가 결정되기 때문에 기존에 결정되어 있지 않은 상태에서 외부의 영향이 있을 경우 형태가 변형
복제불가의 법칙	• 중첩의 원리 및 불확정성의 원리로 인해 측정이 불가하고 위치와 운동량을 완벽하게 같이 만들 수 없어 복제가 불가

자료 : 한국물리학회, “양자정보기술”, https://wiki.quist.or.kr, (2023.4.24.)

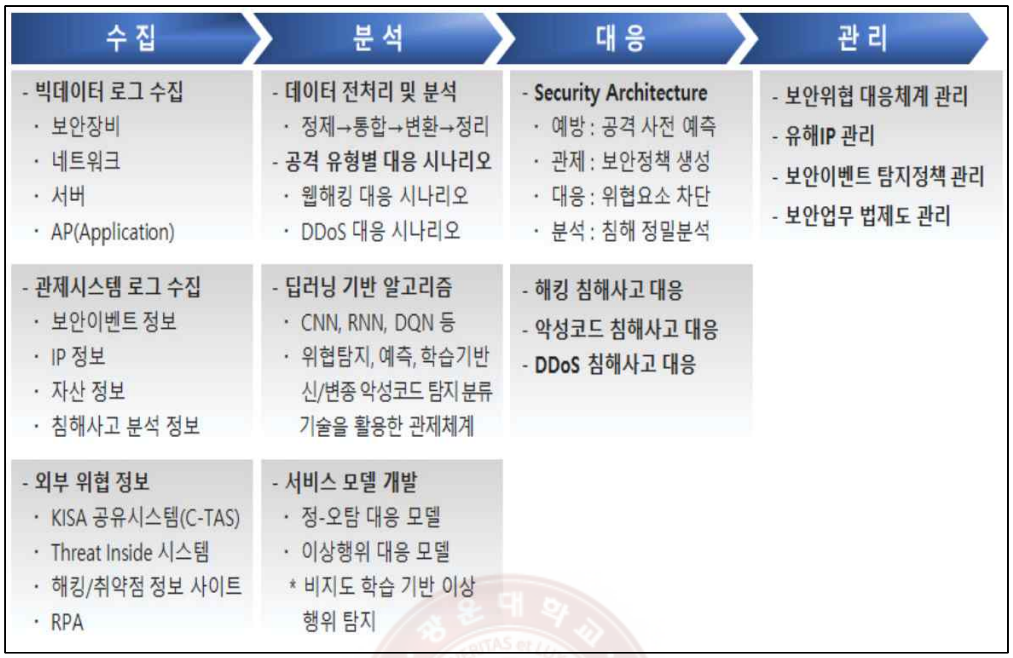
인공지능 기반의 방위사업은 무기체계에 대한 데이터들을 수집하기 위해 사물인터넷과 같이 상호 연결되어 임무를 수행하게 될 것이다. 불순분자들은 초연결성을 바탕으로 각각의 무기체계가 연결되어 있는 통신 침해공격을 통해 정보를 유출하도록 노력할 것이다. 양자암호는 빛 입자인 광자를 이용하는 방식으로 암호화와 복호화 과정에서 암호키로 양자를 활용하며 양자의 특성을 가진다. 따라서 암호키를 전송할때 외부로부터 탈취를 시도하더라도 양자의 상태가 변하는 특징을 가지고 있고, 복호화 전까지 지속 변하기 때문에 기존 운용하고 있는 통신 시스템의 취약점을 극복할 수 있는 기술이다.

초연결 바탕의 인공지능 방위사업에서 양자의 중첩 특성을 이용한 통신은 필수적으로 발전시킬 수 밖에 없는 기술이다. 침해공격을 받았을 경우에도 중첩현상이 붕괴하여 정보 탈취가 어렵기 때문이다. 현재 미군은 양자암호통신을 이용하여 무선통신체계 기술을 접목한 연구를 진행 중이다.

셋째는 인공지능 보안관제체계이다. 수많은 초연결 기반의 무기체계의 연결이 시작되면 허용된 범위의 장비간의 개방성, 확장성, 유연성을 제공하기 위해 분산화 코어 네트워크 구조, 소프트웨어 기반 기술적 변화는 새로운 침해공격 경로를 제

공할 수밖에 없어 플랫폼에서의 보안관제는 필수가 될 것이다. 각 무기체계로부터 수집된 데이터는 국방 지능화센터의 클라우드에 저장이 되기 때문에 플랫폼을 거쳐 클라우드에 접근하기 위한 침해공격이 지능화되고 고도화 될것이며, 머신러닝 등 인공지능 기술을 활용한 침해공격이 다양해질 것으로 예상되고 있다. 그렇기 때문에 대응 또한, 머신러닝과 인공지능 기술을 활용하여 침해공격의 발생환경, 유형, 빈도 등을 분석하여 실시간으로 침해공격 발생을 예측하고, 예방과 지능적인 공격에 대한 선제적 대응이 필요하며, 보안 빅데이터를 인공지능이 학습하도록 하여 기존 알고리즘과 다른 패턴의 징후를 감시하고 차단하는 대응 연구가 필요하다.

보안관제시스템을 인공지능화 하여 단계별(수집・분석・대응・관리) 절차를 보완하고 딥러닝 기반의 알고리즘 분석기술과 대응 보안 기술을 만들어 기존에 보안관제 인력이 수동으로 수행하였던 업무들을 인공지능 기반 보안관제에 자동화하여 기존에 발생하였던 공격과 새로운 침해공격에 대해 보다 효율적이고 정확하게 침해사고 대응이 가능할 수 있다.



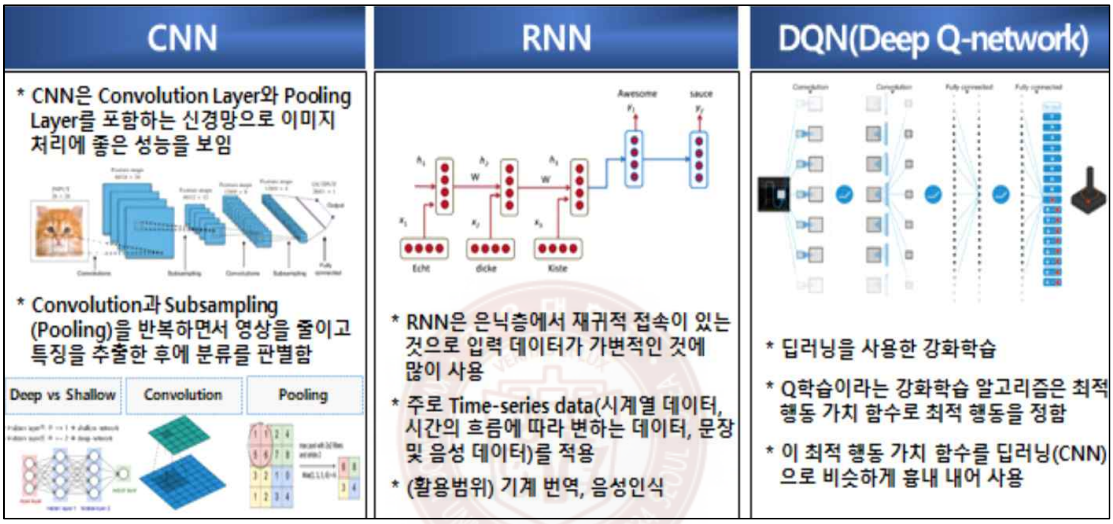
[그림 11] 인공지능기반 보안관제체계도

자료: 한국콘텐츠학회, “인공지능기반 보안관제 구축 및 대응 방안”, (2021)

수집분야에서 빅데이터 기반과 관제시스템, 외부위협정보를 활용하여 수집한다. 빅데이터 시스템에서는 보안장비 등으로부터 로그를 활용하여 정상적 로그와 비정상적 로그로 분류한다. 그리고 정형화된 데이터는 인공지능이 학습할 수 있도록 정상적인 알고리즘과 다른 것을 식별할 수 있는 여건을 만든다. 관제시스템을 통해서는 이벤트 로그, 경보정보를 분석하여 IP의 송·수신지를 분석하여 비정상 IP일 경우 차단하는 것이다. 그리고 해당 IP는 데이터로 관리하여 지속 대응한다. 외부 위협정보수집은 사이버 공격 대응에 국가에서 분석하여 가지고 있는 데이터를 활용하는 것이다.

분석분야에서는 수집된 데이터를 분석 및 처리에 적합한 형식으로 데이터를 조작하고 같은 파일의 데이터는 결합하거나 통합하여 인공지능이 학습할 수 있는 여건을 마련한다. 준비된 데이터를 활용하여 기존에 알려진 침해공격의 패턴은 사람

의 판단 기준을 인공지능에 학습시켜주고, 알려지지 않은 침해공격은 기존의 정상 상태를 인공지능에 학습시켜 이상상태를 식별할 수 있는 기능을 만들어준다. 그리고 정확도를 높여주기 위한 심층학습이 필요하다. 이때 활용할 수 있는 것이 CNN 모델과 RNN모델, DQN모델 등의 알고리즘이다.



[그림 12] 딥러닝에 사용되는 알고리즘

자료: 한국콘텐츠학회, “인공지능 기반 보안관제 구축 및 대응 방안”, (2021)

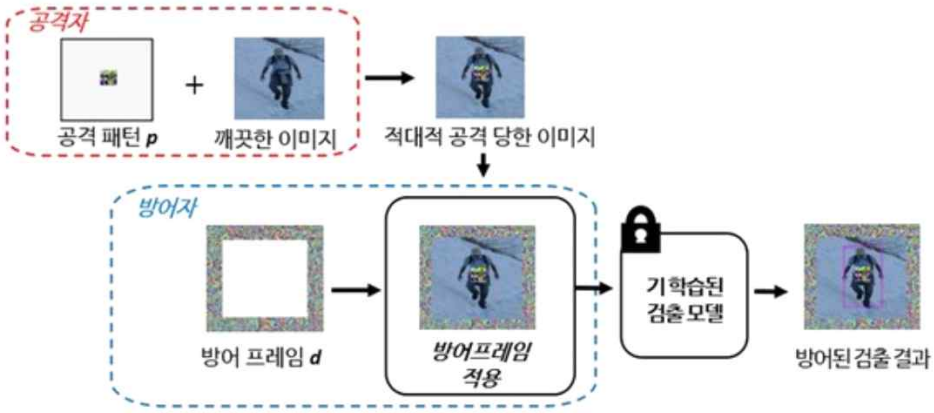
위의 알고리즘을 통해 보안기능 강화와 확산, 탐지 및 분석 체계를 위한 지속적 접근 노력, 클라우드 기반의 위협 데이터 분석, 단위 기술 중심의 악성코드 대응, 인공지능 플랫폼 기반 침해공격 예측 및 IP 추적 등의 자동분석이 가능하다.

대응분야에서는 예방・관제・대응・분석의 유기적인 순환구조와 신규위협에 대해 인공지능의 비정상 행위 식별로 알려지지 않은 침해공격에 대한 대응이 필요하다. 예방은 서비스 및 시스템 보안정책 보안 대응 수준을 유지 강화하고 신규 위협정보 수집체계 기반의 공격을 사전에 예측하고 분석하도록 하며, 관제는 보안대응 시스템 보안 수준을 강화하고 접근통제 강화를 통해 사고예방 기능을 강화한

후 보안 정책 생성 및 권한을 변경하는 것이다. 대응은 이상행위 탐지와 잠재적 위협을 탐지하고 사이버 위협 우선순위를 부여하여 대응하는 것이며, 분석은 외부 위협 정보를 활용하여 침해 정밀분석을 수행하고 보안정책 적용 자동화와 긴급보안 정책을 조언해주는 것이다. 인공지능 기반 침해공격 대응체계는 지속적이고 전반적인 모니터링이 수반되어야하고, 침해공격의 징후를 끊임없이 분석하는 것이 필요하다. 최근 해커들은 컴퓨터에 악성코드를 잠재적으로 심어놓고 장기간에 걸쳐 지능적으로 활용하는 침해공격을 수행하고 있다. 사용자가 컴퓨터를 사용하는 동안 해커는 악성코드를 활용하여 본인이 확인하고 싶은 내용들을 열어보는 것이다. 이를 인공지능 알고리즘을 통해 이상 징후를 식별하고 탐지하여 대응하는 것이다.

관리분야에서는 보안위협 대응 체계와 유해 IP관리, 보안이벤트 탐지 정책 관리, 보안업무 법제도 관리 등을 통해 소프트웨어를 지속 업데이트하고 오탐율 및 미탐율을 줄이는 노력하는 등 침해공격에 대해 대응할 수 있는 능력을 발전시키는 것이다. 보안의 가장 중요한 것은 침해발생의 조기 전파, 사고 대응시간 단축, 경보의 정확성, 새로운 위협과 취약점 파악이다.

넷째는 사이버 보안 강화이다. 적대적 공격에 대한 방어 기법이 있다. 이는 특정 인공지능 모델에 대하여 발생 가능한 모든 적대적 사례를 학습 데이터에 포함하여 훈련을 진행하는 경우를 적대적 훈련(Adversarial training)이라고 부른다. 적대적 훈련은 학습 단계에서 예상 가능한 해킹 데이터를 입력함으로써 모델의 저항성을 향상하는 방어 방법이다. 즉, 인공지능 모델의 결과값 분석을 통해 모델 및 학습 데이터를 추론하는 방식의 모든 공격에 대한 차단을 목적으로, 결과값 노출을 방지하거나 결과값 자체에 대한 분석을 방지함으로써 공격을 차단하는 기법이다.



[그림 13] 인공지능 적대적 훈련 방법

자료: 인공지능 신문,“적대적 공격 막은 방어프레임 개발...KAIST, 인공지능 방어 성능 강화”, (2022.11.15.)

이 기법에 대한 연구 이외에 적대적 공격 적용 여부를 탐지한 후 이를 차단하는 방법도 있다. 또한, 불순분자가 인공지능 모델에 반복적인 쿼리[37]를 진행한다는 점을 방지하기 위하여, 특정 사용자에 의한 쿼리 횟수를 제한하는 방법도 가능한 대안이다. 학습 데이터에 포함된 기밀정보나 개인정보 그리고 민감정보가 노출되지 않도록 암호화 등 비식별 처리 방식을 적용한 학습방법도 연구가 필요하다. 다음은 멤버십 추론 공격 방어이다. 멤버십 추론 공격에 대한 방어가 가능한 MemGuard에 대한 방안으로 격자를 사용하는 모델에 대한 정보가 없기 때문에 직접 자신의 모델을 속이도록 공격 모델을 생성한 후 예측된 값에 노이즈를 추가함으로써 최적의 노이즈를 찾는다. 이는 안전성과 유용성을 모두 보장 가능한 방어 기법이다.

다음은 딥페이크 생체인증 우회이다. 생체인증 우회를 막기 위해서는 안면인식 기술이 적용된 인증 시스템을 사용하기도 한다. 이는 머신러닝을 이용하여 영상

37) 정보 수집에 대한 요청에 쓰이는 컴퓨터 언어

속의 사람이 실제 사람인지 아니면 인공지능과 같은 소프트웨어를 사용하여 생성된 이미지인지를 탐지한다. 딥페이크로 생성된 영상은 원본과는 다른 특징을 갖기 때문에 이 점을 이용하여 진위 여부를 판단할 수 있다.

다음은 설명 가능한 인공지능(XAI) 개발이다. 인공지능은 시스템에서 발생하고 있는 모든 행위와 트래픽, 로그를 실시간 혹은 실시간에 가깝게 분석할 수 있다. 그리고 모든 이벤트의 상관관계를 분석할 수 있다. 인공지능은 사람이 보기 어려운 것을 볼 수 있기 때문에 탐지가 되지 않는 확률을 줄여나갈 수 있으며, 알고리즘에 대한 학습 기간이 많을수록 올바른 탐지 확률도 올라간다. 그러나 인공지능은 이러한 분석 과정을 알려주지 않기 때문에 인공지능의 탐지가 정확한지 판단하기가 어렵다. 오염된 데이터를 대량으로 발생시켜 인공지능이 잘못 학습하게 하는 공격도 가능하다.

이를 대응하기 위하여 '설명 가능한 인공지능(XAI)' 연구가 여러 곳에서 진행 중에 있다. 인공지능 기술의 투명성과 신뢰성에 대한 중요도는 계속해서 증가할 것으로 보이며 이처럼 인간이 이해할 수 있도록 설명을 제공해주는 기술인 '설명 가능한 인공지능(XAI)'이 필요할 것으로 예상된다.

인공지능을 방위사업에 도입함에 따라 보안취약점을 보완할 수 있는 대책들이 있다. 인공지능의 특징을 이해를 바탕으로, 블록체인, 양자암호, 인공지능 보안관제 체계, 사이버 보안 강화 등의 대안이 필요할 것으로 판단된다.

4.5. 인공지능 활용 산업보안 및 기술보호 방안 검증

델파이 기법 적용을 위한 조사 대상은 군 및 국가기관 방위사업 보안 업무 관계자와 석사 이상 또는 그와 준하는 전문적 식견을 가진자, 방산업체 보안분야에서 5년 이상 종사한 인원들을 대상으로 정하였으며, 해당 전문가가 많지 않은 점을 고려하여 20명을 목표로 하였다. 설문조사의 배경 및 목적을 설명하고 동의를 거

쳐 델파이 조사 대상자 20명을 구성하였다.

이 중 재직자는 20명으로 국내 주요 방위사업 보안분야에서 종사하고 있으며, 보안관리자 16명이 포함되었다. 20명의 전문가들의 경력은 최소 5년에서 최대 30년까지였으며, 평균 경력은 13년 이었다. 보안학 박사는 3명이 있었으며, 보안분야 전공자가 14명(70%), 관련 자격증 소지자가 13(65%)명이었다.

<표 32> 델파이 조사 패널 현황(20명)

응답자 ID	소 속	보안업무 경력	공인 자격증	학위
1	육군	15-20년	무	·
2	육군	15-20년	유	석사
3	육군	15-20년	무	석사
4	육군	20-25년	유	석사
5	육군	20-25년	무	석사
6	육군	10-15년	무	·
7	육군	10-15년	유	석사
8	육군	5-10년	무	·
9	정부기관	5-10년	유	석사
10	정부기관	5-10년	무	석사
11	정부기관	5-10년	유	·
12	정부기관	10-15년	유	박사
13	정부기관	10-15년	유	박사
14	정부기관	10-15년	무	석사
15	정부기관	10-15년	유	석사
16	방위사업체	10-15년	유	석사
17	방위사업체	10-15년	유	박사
18	방위사업체	20-25년	유	·
19	방위사업체	20-25년	유	석사
20	방위사업체	5-10년	유	·

첫 번째 델파이 조사에서는 20명 중 18명이 응답(회수율 90%)하였으며 현재 운영중인 인공지능 적용 분야, 방위사업 기술유출 원인, 인공지능 적용시 산업보안 및 기술보호 취약점, 방위사업 시스템 및 사이버 보안, 방위사업 보안 인증제도, 보안교육 프로그램 의견을 수집하였다. 이후 델파이 조사 결과를 바탕으로 전문가의 삭제 및 추가 의견을 고려하여 항목을 수정하였다.

두 번째 델파이 조사에서 첫 번째 조사 방위사업체의 낮은 보안 수준 항목을 삭제하고 자부심 및 명예심 고취 제도 부족을 추가하여 전문가들과 공유하고 5점 리커트 척도로 2차 조사하였다. 두 번째 조사 회수율은 16명(80%)이였다. 이후 중분류 과목별 배점은 계층별 분석 기법(AHP) 조사를 통해 중요도를 산출하여 적용하였다. AHP 조사는 중분류 단위만 진행하였으며, 산업보안 및 방위사업 기술보호에 대한 전문적 식견을 가지고 있어야 하므로 2회의 델파이 조사 평균 경력은 14년을 기준으로 하여 그 이상의 보안 경력자 중 보안 관련 석사 이상자 또는 자격증 소지자로 한정하여 5명을 조사 대상으로 추출하였다.

AHP 조사는 두 개의 등급별로 각각 중분류 과목간의 상대적 중요도를 설문하였다. AHP 조사방식을 적용하여 두 중분류의 중요도가 동일할 경우에는 1점, 그렇지 않을 경우에는 본인이 생각하는 수준의 중요한 과목 쪽에 2-9점에서 선택하도록 하였다. 엑셀을 통해 가중치를 도출한 후 C.I(일관성 지수)를 분석하였으며, 이를 통해 결과 수용 여부를 판단하였다. 연구결과는 수집된 의견 통합, 정리하여 기본적인 운영 방향에 대해서 제시하는 수준의 연구를 진행하였다.

4.5.1. 1차 델파이 조사 결과

1차 델파이 조사에서는 평가 항목 평가항목 84개(대분류 6개, 중분류 12개, 평가항목 47개)를 대상으로 5점 리커트 척도를 활용하여 폐쇄형 질문과 전문가 의견을 수렴할 수 있는 개방형 항목을 추가하여 평가 항목별 적합성을 평가하는 방법으로 진행하였다. 설문은 전문가 총 20명에게 서면 및 구글 설문지를 배포하여 95%에 해당하는 19명이 응답했다. 제 1차 델파이 조사에서는 평균값이 3.0미만(5점 척도 평균값) 이거나, 내용 타당도 비율(CVR : Content Validity Ratio)이 0.42 미만인 평가 항목은 정확도가 낮다고 판단하여 삭제하였다. Cronbach's a값은 0.6 이상일 경우 신뢰도가 있는 것으로 분석했다.

<인공지능 적용>의 설문조사 결과 아래 표와 같이 11개 평가 항목 모두 평균값이 3.0 이상이며 내용 타당도 비율(CVR)도 .42 이상인 것으로 확인되어 11개 항목 모두 제 2차 델파이 조사 항목으로 결정하였다. 설문조사 결과 <인공지능 적용>의 평가 항목 중 무기체계 감시·정찰 분야의 평균값이 4.622로 가장 높게 나타났다. 중분류에서는 무기체계 평균값이 4.339로 전력지원체계 보다 높게 나타난 것을 확인하였다. 모든 평가 항목이 내용 타당도 비율(CVR)은 .599~1의 범위로 타당한 것으로 분석되었으며, 감시·정찰 분야는 1로 가장 높게 나타났다. Cronbach's a값은 .84로 신뢰도에 문제가 없는 것으로 분석되었다.

< 표 33> 1차 델파이 조사 결과 <인공지능 적용>

중분류	주요 평가항목	평균	표준편차	CVR	합의도	신뢰도	결과
무기체계	지휘통제・통신	4.207	.675	.724	.75		○
	감시・정찰	4.622	.494	.599	.8		○
	기 동	4.172	.539	.862	.87		○
	함 정	4.276	.702	.724	.75		○
	항 공	4.448	.736	.724	.75		○
	화 력	4.310	.604	.862	.75		○
	방 호	4.345	.669	.793	.75	.84	○
	소 계	4.339	.631	.741	.77		・
전력지원체계	전투지원	4.345	.614	.862.	.75		○
	의무지원	4.207	.726	.655	.75		○
	교육훈련	4.446	.587	.712	.8		○
	국방정보시스템	4.233	.643	.744	.75		○
	소 계	4.307	.642	.743	.76		・

<방위사업 기술유출 원인>의 설문조사 결과 아래 표와 같이 1개 항목을 제외한 6개 평가 항목 모두 평균값은 3.0 이상, 내용 타당도 비율(CVR) 값도 .42 이상인 것으로 분석되었다. '방위사업체의 낮은 보안 수준'은 타당도가 .39로 기준값에 미치지 못하여 삭제하였다. 그 외 6개 항목은 제 2차 델파이 조사 항목으로 결정하였다. 전문가 1명이 '자부심 및 명예심 고취 제도 부족'의 의견을 주어 검토한 결과 의견을 수용하는 것으로 결정했다. 설문조사 결과 평가 항목 중 산업보안 및 기술유출에 대한 전문적인 자격인증제도 부실의 평균값이 4.448로 가장 높게 나타났다. 중분류에서는 개인적 요인이 평균값 4.326로 높게 확인되었다. 내용 타당도 비율(CVR)은 삭제 항목을 제외하고 모든 평가 항목이 .439~.862의 범위로 타당한 것으로 분석되었으며, Cronbach's a값은 .82로 신뢰도에 문제가 없는 것으로 분석되었다

< 표 34> 1차 델파이 조사 결과 <방위사업 기술유출 원인>

중분류	주요 평가항목	평균	표준편차	CVR	합의도	신뢰도	결과
제도적 요인	방위사업에 종사하는 군인의 정년 미보장	4.276	.736	.724	.75	0.82	○
	방위사업 관련 국가기관의 낮은 보수	4.121	.604	.862	.75		○
	방위사업체의 낮은 보안 수준	3.334	.669	.393	.56		○
	방위사업 관계자의 교육 부족	4.276	.631	.684	.77		○
	산업보안 및 기술유출에 대한 전문적인 자격인증제도 부실	4.448	.614	.862.	.75		○
	소 계	4.091	.650	.705	.716		·
개인적 요인	개발자 및 연구자들의 윤리의식 부족	4.207	.726	.655	.75		○
	개인의 물질적 욕심	4.446	.778	.439	.5		○
	소 계	4.326	.752	.547	.625		·

<산업보안 및 기술보호 취약점>의 설문조사 결과 아래 표와 같이 5개 항목의 평균값이 3.0이며, 내용 타당도 비율(CVR)이 .42 이상인 것으로 확인되었다. 설문조사 결과 'IOT 및 사물인터넷 등 초연결로 구성된 서버 보안'의 평균값이 4.621로 높게 나타났다. 중분류에서는 '시스템 측면'의 평균값이 4.414로 '사이버 측면' 보다 .242 더 높았다. 내용 타당도 분야에서는 데이터 모두 .479~.931의 범위로 모두 타당하며, 이중 'IOT 및 사물인터넷 등 초연결로 구성된 서버 보안'이 가장 높았다. Cronbach's a값은 .86으로 신뢰도에는 문제가 없는 것으로 분석했다.

< 표 35> 1차 델파이 조사 결과 <산업보안 및 기술보호 취약점>

중분류	주요 평가항목	평균	표준편차	CVR	합의도	신뢰도	결과
시스템 측면	빅데이터 무결성 유지	4.207	.774	.724	.75	.86	○
	IOT 및 사물인터넷 등 초연결로 구성된 서버 보안	4.621	.562	.931	.87		○
	소 계	4.414	.668	.827	.81		·
사이버 측면	딥페이크를 활용한 신체인증 악용	3.966	.778	.479	.5		○
	스팸 및 피싱	4.276	.631	.684	.77		○
	퍼 징	4.276	.649	.793	.75		○
	소 계	4.172	.686	.652	.673		·

<방위사업 시스템 및 사이버 보안>의 설문조사 결과 아래 표와 같이 7개 평가 항목 모두 평균값이 3.0 이상이며, 내용 타당도 비율(CVR) 값이 .42 이상인 것으로 확인되어 5개 항목 모두 제 2차 델파이 조사 항목으로 결정하였다. 설문조사 결과 평가 항목 중 블록체인 기반의 데이터 보호의 평균값이 4.450로 가장 높게 나타났다. 중분류에서는 시스템 보안강화 평균값 4.391로 높게 나타났다. 내용 타당도 비율(CVR)은 .684~.862의 범위로 모든 평가 항목이 타당한 것으로 분석되었으며, Cronbach's a값은 .82로 신뢰도에 문제가 없는 것으로 분석되었다.

< 표 36> 1차 델파이 조사 결과 <방위사업 시스템 및 사이버 보안>

중분류	주요 평가항목	평균	표준편차	CVR	합의도	신뢰도	결과
시스템 보안강화	블록체인 기반의 데이터 보호	4.450	.587	.712	.8	.82	○
	양자암호를 통한 전송 보호	4.277	.631	.684	.77		○
	인공지능을 활용한 보안관제체계 개발	4.446	.587	.712	.8		○
	소 계	4.391	.601	.702	.79		·
사이버 보안강화	적대적 훈련 학습	4.446	.736	.724	.75		○
	멤버쉽 추론 공격 방어	4.310	.604	.862	.75		○
	딥페이크 생체 인증 우회	4.345	.669	.793	.75		○
	설명 가능한 인공지능 개발	4.276	.631	.684	.77		○
	소 계	4.344	.66	.765	.755		·

<방위사업 보안 인증제도>의 설문조사 결과 아래 표와 같이 8개 평가 항목 모두 평균값이 3.0 이상이며, 내용 타당도 비율(CVR) 값이 .42 이상인 것으로 확인되어 8개 항목 모두 제 2차 델파이 조사 항목으로 판단하였다. 설문조사 결과 평가 항목 중 머신러닝 및 딥러닝 보안의 평균값이 4.510로 가장 높게 나타났다. 중분류에서는 개인자격 인증이 평균값 4.382로 방위사업체 자격인증보다 높게 나타났다. 모든 평가 항목의 타당도비율(CVR)은 .684~.862의 범위로 타당한 것으로 분석되었으며, Cronbach's a값은 .88로 신뢰도에 문제가 없는 것으로 분석되었다.

< 표 37> 1차 델파이 조사 결과 <방위사업 보안 인증제도>

중분류	주요 평가항목	평균	표준편차	CVR	합의도	신뢰도	결과
개인자격 인증	인공지능 기반 방위사업 보안 개념 이해	4.448	.736	.724	.75	.88	○
	머신러닝 및 딥러닝 보안	4.510	.704	.862	.75		○
	자연어 처리 보안	4.446	.736	.724	.75		○
	데이터 보안	4.277	.631	.684	.77		○
	인공지능 보안 프레임 워크	4.233	.643	.744	.75		○
	소 계	4.382	.69	.747	.754		·
방위 사업체 자격인증	통합실태조사 등급화(1~3)	4.345	.669	.793	.75		○
	인공지능을 활용한 사이버 보안 강화	4.339	.631	.741	.77		○
	방산종사자 전문성 평가	4.277	.631	.684	.77		○
	소 계	4.320	.643	.739	.763		·

<보안교육 프로그램>의 설문조사 결과 아래 표와 같이 8개 평가 항목 모두 평균값이 3.0 이상이며, 내용 타당도 비율(CVR) 값이 .42 이상인 것으로 확인되어 7개 항목 모두 제 2차 델파이 조사 항목으로 판단하였다. 설문조사 결과 평가 항목 중 '머신러닝·딥러닝·자연어 설계 및 처리'에 대한 평균값이 4.476으로 가장 높게 나타났다. 중분류에서는 실습과목이 4.287로 이론과목 보다 높게 나타났다. 모든 평가 항목이 내용 타당도 비율(CVR)에서 .655~.862의 범위로 타당한 것으로 분석되었으며, Cronbach's a값은 .80로 신뢰도에 문제가 없는 것으로 분석되었다

< 표 38> 1차 델파이 조사 결과 <보안교육 프로그램>

중분류	주요 평가항목	평균	표준편차	CVR	합의도	신뢰도	결과
이론과목	방위사업 인공지능 침해 공격 동향 및 트렌드	4.210	.604	.862	.75		○
	블록체인, 양자암호, 인공지능과 보안관제	4.239	.631	.741	.77		○
	개인정보 보호	4.245	.614	.862.	.75		○
	인공지능 알고리즘 이해	4.232	.618	.823	.75		○
	소 계	4.231	.616	.822	.755		·
실습과목	생체인증 우회·스팸 및 퍼징 구별법	4.246	.587	.712	.8	.80	○
	머신러닝·딥러닝·자연어 설계 및 처리	4.476	.631	.684	.77		○
	인공지능 사이버 위협 및 탐지 대응 방법	4.276	.649	.793	.75		○
	국방 데이터 활용처리 실습(인공지능 설계)	4.233	.643	.744	.75		○
	빅데이터 분석 및 서버 관리	4.207	.726	.655	.75		○
	소 계	4.287	.647	.717	.764		·

제1차 델파이 조사 결과를 요약하면 총 47개 평가 항목 중 평균값 및 내용 타당도 비율(CVR)이 기준값 .42에 미치지 못하는 1개 항목이 삭제되었고 전문가 의견을 분석하여 1개 의견은 추가하였다. 최종적으로 대분류 6개, 중분류 12개, 평가항목 47개가 2차 델파이 조사 항목으로 결정되었다. 제 1차 델파이 조사 결과 삭제 및 추가된 평가 항목은 아래와 같다. 1차 델파이 조사 평균 값은 3.314~4.622이었으며, 내용 타당도 비율은 1건을 제외하고 .439~.931로 타당도에는 문제가 없는 것으로 분석되었다.

< 표 39> 1차 델파이 조사 삭제 및 추가 항목

구 분	주요 평가항목
삭제 항목	• 방위사업 기술유출 원인 : 제도적 요인 - 방위사업체의 낮은 보안 수준
추가항목	• 방위사업 기술유출 원인 : 제도적 요인 - 자부심 및 명예심 고취 제도 부족

4.5.2. 2차 델파이 조사 결과

2차 델파이 조사에서는 제1차 델파이 조사로 판단된 총 47개 평가 항목을 20명의 전문가들에게 서면 및 이메일, 구글 설문지로 배포하여 약 90%에 해당하는 18명이 응답했다. 제 2차 델파이 조사에서는 평균값이 3.0 미만 또는 내용 타당도 비율(CVR)이 .42 미만인 평가 항목은 없었다. 그리고 Cronbach a값은 0.6 이상일 경우 신뢰도가 있는 것으로 분석했다.

<인공지능 적용>의 설문조사 결과는 아래 표와 같이 11개 평가 항목은 평균값이 3.0이며, 내용 타당도 비율(CVR)이 .42 이상인 것으로 확인되었다. 평가 항목 중 '감시・정찰'분야가 4.734로 가장 높았다. 중분류에서는 '무기체계' 평균값이 4.459로 전력지원체계 4.438보다 높게 나타났다. 모든 항목이 내용 타당도 비율(CVR)의 값이 .620～.888의 범위로 타당한 항목들로 구성된 것으로 나타났다. Crobach's a값은 .86으로 신뢰도에 문제가 없는 것으로 분석되었다. 이는 1차 델파이 조사와 유사하게 나타났다.

< 표 40> 2차 델파이 조사 결과 <인공지능 적용>

중분류	주요 평가항목	평균	표준편차	CVR	합의도	신뢰도	결과
무기체계	지휘통제・통신	4.512	.741	.734	.76	.86	○
	감시・정찰	4.734	.748	.620	.94		○
	기 동	4.376	.575	.888	.88		○
	함 정	4.316	.712	.734	.85		○
	항 공	4.512	.754	.731	.77		○
	화 력	4.333	.712	.767	.79		○
	방 호	4.432	.712	.814	.78		○
	소 계	4.459	.707	.755	.824		・
전력지원체계	전투지원	4.435	.634	.882	.77		○
	의무지원	4.456	.554	.712	.78		○
	교육훈련	4.531	.627	.743	.84		○
	국방정보시스템	4.332	.667	.754	.77		○
	소계	4.438	.620	.772	.79		・

<방위사업 기술유출 원인>의 설문조사 결과 아래 표와 같이 7개 평가 항목 모두 평균값이 3.0 이상이며, 내용 타당도 비율(CVR) 값이 .42 이상인 것으로 확인되었다. 평가 항목 중 '산업보안 및 기술유출에 대한 전문적인 자격인증제도 부실'이 4.511로 가장 높았다. 중분류에서는 '개인적요인' 평균값이 4.390으로 '제도적 요인'보다 .058 높게 나타났다. 모든 항목이 내용 타당도 비율(CVR)의 값이 .612~.888의 범위로 타당한 항목들로 구성된 것으로 나타났다. Crobach's a값은 .78으로 신뢰도에 문제가 없는 것으로 분석되었다. 이는 1차 델파이 조사와 유사하게 나타났다.

< 표 41> 2차 델파이 조사 결과 <방위사업 기술유출 원인>

중분류	주요 평가항목	평균	표준편차	CVR	합의도	신뢰도	결과
제도적 요인	방위사업에 종사하는 군인의 정년 미보장	4.314	.744	.732	.76	.78	○
	방위사업 관련 국가기관의 낮은 보수	4.311	.634	.882	.75		○
	자부심 및 명예심 고취 제도 부족	4.213	.689	.803	.76		○
	방위사업 관계자의 교육 부족	4.312	.655	.712	.78		○
	산업보안 및 기술유출에 대한 전문적인 자격인증제도 부실	4.511	.624	.888.	.78		○
	소 계	4.332	.669	.803	.766		·
개인적 요인	개발자 및 연구자들의 윤리의식 부족	4.327	.743	.661	.78		○
	개인의 물질적 욕심	4.454	.790	.612	.77		○
	소 계	4.390	.766	.636	.775		·

<방위사업 기술유출 취약점>의 설문조사 결과 아래 표와 같이 5개 평가 항목 모두 평균값이 3.0 이상이며, 내용 타당도 비율(CVR) 값이 .42 이상인 것으로 확인되었다. 평가 항목 중 'IOT 및 사물인터넷 등 초연결로 구성된 서버 보안'이 4.513으로 가장 높았다. 중분류에서는 '시스템 측면' 평균값이 4.412로 '사이버 측면'보다 .002 높게 나타났다. 모든 항목이 내용 타당도 비율(CVR)의 .479~.877의 범위로 타당한 항목들로 구성된 것으로 나타났다. Crobach's a값은 .84으로 신뢰도에 문제가 없는 것으로 분석되었다. 이는 1차 델파이 조사와 유사하게 나타났다.

< 표 42> 2차 델파이 조사 결과 <방위사업 기술유출 취약점>

중분류	주요 평가항목	평균	표준편차	CVR	합의도	신뢰도	결과
시스템 측면	빅데이터 무결성 유지	4.311	.655	.691	.78	.84	○
	IOT 및 사물인터넷 등 초연결로 구성된 서버 보안	4.515	.612	.731	.82		○
	소 계	4.413	.633	.711	.8		·
사이버 측면	딥페이크를 활용한 신체인증 악용	4.511	.754	.731	.78		○
	스팸 및 피싱	3.333	.612	.877	.76		' ○
	퍼 징	3.966	.778	.479	.5		' ○
	소 계	4.414	.683	.804	.77		·

<방위사업 시스템 및 사이버 보안>의 설문조사 결과 아래 표와 같이 7개 평가 항목 모두 평균값이 3.0 이상이며, 내용 타당도 비율(CVR) 값이 .42 이상인 것으로 확인되었다. 평가 항목 중 '블록체인 기반의 데이터 보호'가 4.513으로 가장 높았다. 중분류에서는 '시스템 보안강화' 평균값이 4.367로 '사이버 보안강화'보다 .0018 높게 나타났다. 모든 항목이 내용 타당도 비율(CVR)의 .684~.887의 범위로 타당한 항목의 구성으로 나타났다. Crobach's a값은 .88으로 신뢰도에 문제가 없는 것으로 분석되었다. 이는 1차 델파이 조사와 유사하게 나타났다.

<표 43> 2차 델파이 조사 결과 <방위사업 시스템 및 사이버 보안>

중분류	주요 평가항목	평균	표준편차	CVR	합의도	신뢰도	결과
시스템 보안강화	블록체인 기반의 데이터 보호	4.513	.754	.733	.77	.88	○
	양자암호를 통한 전송 보호	4.312	.633	.887	.78		○
	인공지능을 활용한 보안관제체계 개발	4.277	.631	.684	.77		○
	소 계	4.367	.672	.768	.773		·
사이버 보안강화	적대적 훈련 학습	4.421	.682	.812	.78		○
	멤버쉽 추론 공격 방어	4.354	.661	.764	.78		○
	딥페이크 생체 인증 우회	4.277	.631	.684	.77		○
	설명 가능한 인공지능 개발	4.345	.669	.793	.75		○
	소 계	4.349	.660	.763	.77		·

<방위사업 보안 인증제도>의 설문조사 결과 아래 표와 같이 8개 평가 항목 모두 평균값이 3.0 이상이며, 내용 타당도 비율(CVR) 값은 .42 이상인 것으로 확인되었다. 평가 항목 중 '머신러닝 및 딥러닝 보안'이 4.545으로 가장 높았다. 중분류에서는 '개인인증자격' 평균값이 4.389로 '방위사업체 자격인증'보다 .0064 높게 나타났다. 내용 타당도 비율(CVR)에서는 모든 항목이 .676~.877의 범위로 타당한 항목들로 구성된 것으로 나타났다. Crobach's a값은 .82으로 신뢰도에 문제가 없는 것으로 분석되었다. 이는 1차 델파이 조사와 유사하게 나타났다.

< 표 44> 2차 델파이 조사 결과 <방위사업 보안 인증제도>

중분류	주요 평가항목	평균	표준편차	CVR	합의도	신뢰도	결과
개인자격 인증	인공지능 기반 방위사업 보안 개념 이해	4.334	.612	.877	.76	.82	○
	머신러닝 및 딥러닝 보안	4.543	.641	.766	.78		○
	자연어 처리 보안	4.366	.621	.877	.76		○
	데이터 보안	4.350	.626	.86	.76		○
	인공지능 보안 프레임 워크	4.354	.661	.764	.78		○
	소 계	4.389	.632	.828	.768		·
방위사업체 자격인증	통합실태조사 등급화(1~3)	4.456	.591	.733	.84		○
	인공지능을 활용한 사이버 보안 강화	4.255	.665	.766	.77		○
	방산종사자 전문성 평가	4.265	.744	.676	.76		○
	소 계	4.325	.666	.725	.79		·

<보안교육 프로그램>의 설문조사 결과 아래 표와 같이 9개 평가 항목 모두 평균값이 3.0 이상이며, 내용 타당도 비율(CVR) 값은 .42 이상인 것으로 확인되었다. 평가 항목 중 '머신러닝·딥러닝·자연어 설계 및 처리'가 4.545으로 가장 높았다. 중분류에서는 '실습과목' 평균값이 4.417으로 '이론과목'보다 .0317 높게 나타났다. 모든 항목이 내용 타당도 비율(CVR)의 .733~.887의 범위이며 타당한 항목으로 구성된 것으로 나타났다. Crobach's a값은 .82으로 신뢰도에 문제가 없는 것으로 분석되었다. 이는 1차 델파이 조사와 유사하게 나타났다.

< 표 45> 2차 델파이 조사 결과 <보안교육 프로그램>

중분류	주요 평가항목	평균	표준편차	CVR	합의도	신뢰도	결과
이론과목	방위사업 인공지능 침해 공격 동향 및 트렌드	4.312	.633	.887	.78	.82	○
	블록체인, 양자암호, 인공지능과 보안관제	4.344	.651	.762	.78		○
	개인정보 보호	4.411	.754	.731	.78		○
	인공지능 알고리즘 이해	3.333	.612	.877	.76		○
	소 계	4.1	.662	.814	.775		·
실습과목	생체인증 우회·스팸 및 퍼징 구별법	4.456	.591	.733	.84		○
	머신러닝·딥러닝·자연어 설계 및 처리	4.546	.641	.766	.78		○
	인공지능 사이버 위협 및 탐지 대응 방법	4.312	.633	.887	.78		○
	국방 데이터 활용처리 실습(인공지능 설계)	4.421	.682	.812	.78		○
	빅데이터 분석 및 서버 관리	4.354	.661	.764	.78		○
	소 계	4.417	.641	.792	.792		·

제 2차 델파이 조사 결과를 요약하면 타당도 비율(CVR)과 합의도, 신뢰도가 모두 기준으로 적합하였으며 대분류 6개, 중분류 12개, 평가항목 47개로 분석되었다. 1차 델파이 조사 평균 값은 3.333~4.546이었으며, 내용 타당도 비율은 1건을 제외하고 .526~.84로 타당도에는 문제가 없는 것으로 분석되었다. 이는 1차 델파이 조사와 유사하게 나타났다.

4.5.3. 인공지능 활용 방위사업 발전 요소 조사 결과

<표 46> 인공지능 활용 방위사업 발전 요소 조사 결과

대분류	중분류	주요 평가항목	중요도(%)
인공지능 적용 분야	무기체계	지휘통제・통신	90.2
		감시・정찰	94.7
		기동	87.5
		함정	86.3
		항공	90.2
		화력	86.7
		방호	88.6
	전력지원체계	전투지원	88.7
		의무지원	89.1
		교육훈련	90.6
		국방정보시스템	86.6
방위사업 기술유출 원인	제도적 요인	방위사업에 종사하는 군인의 정년 미보장	86.3
		방위사업 관련 국가기관의 낮은 보수	86.2
		자부심 및 명예심 고취 제도 부족	84.3
		방위사업 관계자의 교육 부족	86.2
		산업보안 및 기술유출에 대한 전문적인 자격인증제도 부실	90.2
	개인적 요인	개발자 및 연구자들의 윤리의식 부족	86.5
		개인의 물질적 욕심	89.1
방위사업 기술유출 취약점	시스템 측면	빅데이터 무결성 유지	86.2
		IOT 및 사물인터넷 등 초연결로 구성된 서버 보안	90.3
	사이버 측면	딥페이크를 활용한 신체인증 악용	90.2
		스팸 및 피싱	66.7
		퍼징(Fuzzing)	79.3

<표 46> 인공지능 활용 방위사업 발전 요소 조사 결과(계속)

대분류	중분류	주요 평가항목	중요도(%)
방위사업 시스템 및 사이버 보안	시스템 보안강화	블록체인 기반의 데이터 보호	90.3
		양자암호를 통한 전송 보호	86.2
		인공지능을 활용한 보안관제체계 개발	85.5
	사이버 보안강화	적대적 훈련 학습	88.4
		멤버쉽 추론 공격 방어	87.1
		딥페이크 생체 인증 우회	85.5
		설명 가능한 인공지능 개발	86.9
방위사업 보안 인증제도	개인자격 인증	인공지능 기반 방위사업 보안 개념 이해	86.7
		머신러닝 및 딥러닝 보안	90.9
		자연어 처리 보안	87.3
		데이터 보안	87.0
		인공지능 보안 프레임 워크	87.1
	방위사업체 자격인증	통합실태조사 등급화(1~3)	89.1
		인공지능을 활용한 사이버 보안 강화	85.1
		방산종사자 전문성 평가	85.3
보안교육 프로그램	이론과목	방위사업 인공지능 침해 공격 동향 및 트렌드	86.2
		블록체인, 양자암호, 인공지능과 보안관제	86.9
		개인정보 보호	88.2
		인공지능 알고리즘 이해	66.7
	실습과목	생체인증 우회・스팸 및 퍼징 구별법	89.1
		머신러닝・딥러닝・자연어 설계 및 처리	90.9
		인공지능 사이버 위협 및 탐지 대응 방법	86.2
		국방 데이터 활용처리 실습(인공지능 설계)	88.4
		빅데이터 분석 및 서버 관리	87.1

4.5.4. AHP 기법을 활용한 우선순위 도출 결과

본 연구는 인공지능을 활용한 방위사업 보호방안 요소를 도출하는데 목적이 있다. 도출된 내용 중에서 우선순위를 판단하여 국방에 우선 적용할 요소들을 살펴본다. 델파이 기법을 통해 문헌연구로 도출된 평가항목들을 검증하고 추가 및 삭제하였다. 이를 바탕으로 우선순위를 도출하기 위해 계층적 의사결정 방법(AHP)을 적용하였다.

AHP(Analytic Hierarchy Process) 기법은 설문 문항이 3가지 이상일 경우 논리적 오류가 발생할 수 있기 때문에 이를 최소화하기 위해 서로 쌍대비교가 가능한 중분류에 대해서만 가중치와 우선순위를 도출하였다. AHP 전문가 조사는 중분류 12개 항목을 9점까지 리커트 척도를 활용하여 쌍대 비교하는 방법으로 진행했다. 설문은 1·2차 델파이 조사에 응답한 전문가 중에서 14년 이상의 경력자 5명으로부터 응답을 받았으며 설문을 분석하여 중분류 항목별 가중치와 우선순위를 도출하였다. 중분류 항목에 대한 가중치와 우선순위는 아래 표와 같다.

<표 47> AHP분석을 통한 중분류 우선순위 도출 결과

대분류	중분류	가중치	우선순위
인공지능 적용분야	무기체계	0.332	1
	전력지원체계	0.154	2
방위사업 기술유출 원인	제도적 요인	0.263	2
	개인적 요인	0.392	1
방위사업 기술유출 취약점	시스템 측면	0.432	1
	사이버 측면	0.254	2
방위사업 시스템 및 사이버 보안	시스템 보안강화	0.413	1
	사이버 보안강화	0.335	2
방위사업 보안 인증제도	개인 자격 인증	0.451	1
	방위사업체 자격 인증	0.392	2
보안교육 프로그램	이론과목	0.221	2
	실습과목	0.263	1

4.6. 소 결

4장에서는 미국의 인공지능을 활용한 방위사업 보안 및 기술보호 강화 방안에 대해 살펴보고 국내에 필요한 방위사업 보안 인증제도와, 보안교육 프로그램, 시스템 및 사이버상 보안 강화 방안에 대해 제시하였다. 그리고 본 연구자가 제시한 내용을 바탕으로 전문가 20명을 통해 델파이 기법을 활용하여 검증하였으며, 전문가들의 의견을 수렴하여 일부 내용을 수정・보완하였다. 이후에는 AHP 분석기법을 통해 각 중분류 항목을 대상으로 쌍대비교를 통해 중요도를 분석하였다.

미국 국방부는 인공지능을 활용한 방위사업 발전을 위해 시제품을 만들어 보완하는 단계에 있으며, 보안 전문가가 인공지능의 알고리즘을 검증하며 지속 발전하는 과정에 있다. 데이터 전송시에는 양자암호화 및 블록체인 기술을 적용하고 있으며, 인공지능을 활용한 방위사업 기술보호 기틀을 만들기 위해 법적근거를 마련하는 절차가 진행중이다. 또한, 인공지능의 기술은 국방부보다 민간에서 발전이 빠르기 때문에 민간의 기술을 적극적으로 벤치마킹하여 발전하고 있다. 우리나라도 인공지능을 활용한 방위사업 기술보호 노력이 필요하다.

첫째, 자격인증제도 마련이 필요하다. 국내에는 인공지능 보안 전문가에 대한 자격증이 없다. 다만, 보안과 인공지능 분야가 각각 나누어진 자격증이 있어 이를 융합하여 (가칭) '인공지능 방위사업 보안전문가' 명칭의 자격증 신설이 필요할 것으로 예상되며 방산업체 지정 또한, 가능 여부를 판단하는 것이 아니라, 미국의 제도와 맞추어 3개 등급으로 방위사업체 지정 등급을 나누는 노력이 필요할 것으로 예상된다.

둘째, 방위사업 보안교육 프로그램이 부재하기 때문에 전문성 있는 인재양성이 제한될 것으로 예상되어 (가칭) '국방 인공지능 보안 담당자' 교육 과정을 신설해야한다. 이론과 실습으로 나누어 최신 침해공격 동향을 분석하고 대한민국에 적용되는 방산기술보호법, 국방보안업무훈령에 연계되어 교육할 수 있는 프로그램이

존재해야 한다.

셋째, 방위사업 시스템 및 사이버 보안을 위해 블록체인, 양자암호, 인공지능 보안관제체계가 필요하다. 블록체인은 미국에서도 적용하는 방안으로 데이터의 무결성을 강화할 수 있는 방안중에 하나이다. 특정 인원 일부만 서로 공유하여 특정 시스템의 침해공격으로 인해 데이터 오염시 다른 시스템이 이를 대체할 수 있고 변경 여부 등에 대해 검증을 할 수 있다. 양자암호는 데이터 전송시 암호키가 열어보기 전까지 결정되지 않은 특성을 이용한 방안으로, 데이터 전송시 중간자에 의한 침해공격을 예방할 수 있는 장점이 있다. 마지막으로 인공지능 보안관제체계는 인공지능의 알고리즘 학습을 이용한 방안으로 정상적인 알고리즘 이외에 패턴이 감지되었을 경우 이를 차단하고 사용자에게 경고해주는 것이다. 인공지능을 활용한 방위사업은 시대적 흐름에서 필수적일 수 밖에 없다. 그렇기 기술보호 요소가 뒷받침되어 지속 발전될 수 있도록 지원해야한다.

위에서 연구한 내용들을 바탕으로 국가기관 및 방위사업체 직원 20명 대상으로 1차, 2차 델파이 기법을 통해 검증한 결과 본 연구자가 제시한 방위사업 기술보호 방안과 유사한 일치도를 보였다. 대한민국 방위사업에서 인공지능 적용을 위해서는 본 연구에서 제시한 개인 및 기업인증체계, 보안교육 프로그램, 시스템 및 사이버 보안 방안이 강구되어야 할 것으로 예상된다.

Ⅴ. 결 론

본 연구는 향후 인공지능을 활용한 방위사업 환경에서 산업보호 및 기술보호를 위한 요소에 대해 연구한 결과이다. 먼저 문헌연구를 통해 도출한 연구자의 결과를 전문가 20명을 대상으로 1차, 2차델파이조사, AHP 분석을 통해 연구 내용의 가치에 대해 검증하였다.

2022년 기준 방위사업에서 기술유출이 발생하고 있는 매개체는 사람과 사람에 의한 사고가 가장 많았으며, 향후 인공지능을 활용한 방위사업 환경에서 방위사업 종사자가 기본적으로 갖추어야 할 산업보안 및 기술유출에 대한 전문적인 지식 부족 등 자격인증제도의 부실로 인한 기술유출이 발생할 것으로 확인하였다.

인공지능을 적용한 방위사업 환경에서 기술유출을 예방하기 위해서는 IOT 및 사물인터넷 등이 연결된 서버 보안이 중요한 것으로 나타났으며, 방위사업 시스템 및 사이버 보안 분야을 위해 구비해야할 방안으로는 블록체인 기반의 데이터 보호, 개인자격인증에서는 머신러닝 및 딥러닝에 대한 보안 능력이 중요한 것으로 의견이 모아졌으며, 보안교육 프로그램에서는 머신러닝 및 딥러닝・자연어에 대한 설계 및 처리에 대한 교육이 중요한 요소가 될 것으로 확인하였다.

종합적으로 정리해보면 인공지능을 활용한 방위사업에서 기술보호를 위해서는 다양한 대책이 필요하다.

첫째, 기술보호를 위한 전문 인력 양성이 필요하다. 빅데이터, 클라우드, VR/AR, 사물인터넷 등 인공지능과 관련된 기술 및 인력은 시장의 성장과 기술의 발전에 따라 수요가 빠르게 성장하고 있다. 민간을 포함하여 전체적으로 분석해보면 2018년~2022년간 4년 동안 인공지능 분야에서 약 3.2만명의 인력이 부족할 것으로 예상하고 있으며, 석・박사급 고급인력 부족이 60% 이상을 차지하여 기술 고도화 분야에서 차이가 심화될 것으로 예상된다.[38] 전문인력을 양성할 수 있는 전문적인

38) 소프트웨어정책연구소(2018)

자격인증제도와 교육 프로그램을 정착하여 군 특성에 맞는 인재를 꾸준히 양성 할 수 있는 환경조성이 필요할 것으로 보인다.

민간에서는 인공지능을 활용한 발전과 보안 대응이 군보다 빠르게 진행될 것으로 예상된다. 그렇기에 민간에 있는 인적자원을 활용하기 위한 노력도 중요하다. 민간 인력을 군에 활용하기 위해서는 군이 외부에 일부데이터를 공개하고 제공하는 것이 필요한데 이는 제한적일 수 밖에 없다. 선진국의 일부 인공지능과 관련된 기업에서는 인터넷에 인공지능 관련 각종 코드 및 학습에 데이터가 온라인에 개방되어 있다. 그렇기에 다양한 계층과 인원들이 접근하여 지식을 쌓고 기업에 특화된 인재를 자연스럽게 영입하여 활용하는 체제가 마련되어 있다. 이와 같이 방위사업도 인공지능 지능화센터를 만들어 클라우드 기반을 준비하는 과정에서 국방 클라우드에 맞는 인재를 양성하는 것이 중요하다. 국방 데이터를 공유 할 수 있는 적절한 경계점을 찾는 문제가 향후 쟁점이 될 수 있을 것으로 예상된다.

둘째, 무결성을 유지할 수 있는 보안관리체계가 강화되어야 한다. 방위사업의 생산물인 무기체계는 안보의 각 현장에서 운용중에 있으며, 무기체계 운용간 발생하는 각종 데이터를 수집할 수 있는 시스템은 미흡한 실정이다. 실례로 국내 차량 생산 대기업에서는 각 차량에 유심칩을 심어 차량 운행에 대한 정보를 실시간으로 받아 데이터를 축적하고 있다. 국방에서도 초연결성을 구현하기 위해서 5G 통신망과 연결해야하며, 이를 뒷받침할 수 있는 기기의 무결성 확보가 중요하다. 데이터는 무선으로 각 서버에 보내질 것이고 중간 매개체 서버 및 최종 매개체 서버에 왜곡 없는 데이터가 저장되지 위해서는 보안이 중요할 수 밖에 없다. 데이터 왜곡을 방지하기 위해서는 양자암호 기술이 도입되어야 하며, 서버의 무결성 유지를 위해서는 프라이빗 블록체인 기술이 적용되어야 한다.

셋째, 인공지능 기술은 보안체계의 취약성과 이상 행동을 식별하여 방위사업의 침해 공격을 감지할 수 있는 인공지능 보안관제체계 도입이 필요하다. 현재 식별되는 침해공격 발생시 91%는 경고를 생성하지 않고 있으며, 방위사업체는 침해를

식별하는 데 평균 200여일, 침해를 억제하는 데 70여일이 소요된다고 한다.[39] 인공지능 보안관제체계는 이벤트를 신속하게 분석하여 보안관리자가 판단하는 위험과 재정손실에 보조를 맞출 수 있도록 지원할 수 있다. 침해공격을 하기 위한 악성코드 삽입 등 여건을 만들이 위한 패턴 알고리즘을 사전에 학습하고 일반적인 행동 패턴과 다른 잠재적인 침해공격 시기를 예측하는 시스템도 만들 수 있다.

향후 2025년에는 인공지능 산업이 2,000조원에 이르는 시장으로 확대되고 인공지능으로 인한 7,000조 원에 이르는 파급 효과가 발생할 것으로 예상하고 있다. 인공지능 산업이 활성화 될수록 보안 대책은 따라올 수 밖에 없으며, 국방부에서 주도하고 있는 국방혁신 4.0에도 인공지능 기술이 핵심으로 확인할 수 있다. 앞으로 방위사업 분야에서 인공지능을 활용한 보안대책은 방위사업에서 피할 수 없는 과제일 수 밖에 없다.

이에 대해 국방부 및 방위사업 관련 업체들의 보안 그룹, 개인 차원의 적극적인 대비가 중요할 수 밖에 없다. 중·장기 관점에서 양질의 데이터 확보, 관련 법·제도 정비, 연구개발 투자를 통해 국방분야 인공지능을 활용한 보안 연구를 유도해야 할 것으로 생각된다. 또한, 민·관·군 협력 및 인공지능 연구기관 부서의 신설·확대를 통해 전문인력을 양성하는 한편, 국방부는 인공지능 보안 기술 확보를 위해 집중 지원하고 방위사업 분야에 인공지능 보안 투자를 적극 유도해야할 것이다.

본 연구는 방위사업에 인공지능 도입에 따른 취약요소 및 보완방안 위주로 분석하였으나, 세부적으로 기술적인 면까지는 연구하지 못하였다. 향후에는 무기체계 및 전력지원체계의 최초 소요제기부터 생산시까지 각각 부분별 인공지능 도입에 따른 보안 취약점을 분석하고 대책을 마련할 수 있는 연구를 통해 본 연구와 더불어 국방혁신 4.0 추진에 기초 연구자료가 되길 기원한다.

39) 산업기술보호지원센터, “방위산업 침해공격 유형과 식별”, (2021)

Ⅵ. 참고문헌

1. 국내 문헌

[1] .국방기술진흥연구소, “미래국방 2030 기술전략”, p.24-p.25, 2022.

[2] 국방기술진흥연구소, “국가별 국방과학기술 수준조사서”, p.17-p.19, 2022.

[3] 국방부, “국방백서”, p.12-p.21, 2022.

[4] 국방부, “국방전력발전업무훈령(제2539호)”, p.13-p.45, 2021.

[5] 국방부, “인공지능 교육자료”, p.2-p.5, 2022.

[6] 국방보안연구소, 국방보안연구 ISSUE, p.3-p.6, 2021.

[7] 고희재, “방위산업 보안수준 평가 지표 개발 연구”, p.12-p.99, 중앙대학교, 2021.

[8] 김동선, “미국 CMMC 제도 대응을 위한 통합실태조사 제도 개선 연구”, p.2-p.7, 한국방위산업학회, 2022.

[9] 김명주, “인공지능 기술 발달에 따른 사이버 위협과 이에 대한 대응 방안”, p.16-p.19, 한국통신학회, 2022.

[10] 김무석, “산업보안을 위한 행정조사에 관한 연구”, p.22-p.56, 성균관대학교, 2022.

[11] 김세용, ‘국방분야 인공지능과 블록체인 융합방안 연구’, 한국인터넷정보학회, 2020.

[12] 강구민, 이재철, 김창범, “산업보안조사에 있어 디지털포렌식 조사의 임의성에 관한 연구”, p.13-p.15, 성균관대학교, 2021.

[13] 김화영, “산업보안 전문자격 활성화 방안 연구”, p.33-p.72, 중앙대학교, 2019.

[14] 박상호, “빅데이터를 활용한 산업보안 전문인력 요구직무 분석”, p.21-p.81, 중앙대학교, 2019.

[15] 박용병, “인공지능 딥러닝 소개와 보안 동향”, p.11-p.53, 공주대학교, 2022.

[16] 방위사업청, “국방기술유출 매뉴얼”, p.2-p.6, 2022

[17] 법체처, “방위산업기술보호법”, p.1-p.2, 2021.

[18] 변태진, “과학교육과 인공지능”, p.1-p.44 광주교육대학교, 2022.
[19] 산업기술보호지원센터, “방위산업 침해공격 유형과 식별”, p.1-p.18, 2021.
[20] 소프트웨어정책연구소, “연구보고서”, p.1-p.6, 2018.
[21] 서대호, “1년 안에 AI빅데이터 전문가가 되는 법”, p.1-p.8, 2020.
[22] 우광제, “융합보안전문가의 핵심과업 및 직무역량”, p.2-p.23, 중앙대학교, 2015.
[23] 우광제, “융합보안 관점에서 방위산업보안 개념 정립과 연구동향 분석”, p.3-p.14, 융합보안논문지, 2015.
[24] 윤성준, “국방 드론봇 통합관제체계 개발을 위한 결정요인 연구”, p.3-p.12, 광운대학교, 2021.
[25] 윤정현, “국방 분야 인공지능 기술 도입의 주요 쟁점과 활용 제고 방안”, 과학기술정책연구원, 2021
[26] 이선희, “방위사업개론”, p.3-p.22, 방위사업청, 2008.
[27] 임동선, “산업현장 수요중심의 산업보안 전문자격제도 연구”, p.12-p.14, 중앙대학교, 2020.
[28] 오동환, “미래전과 네트워크 환경 변화에 따른 보안대책”, p.3-p.8, 한국융합보안학회, 2021.
[29] 장원준, ‘주요 무기체계 방산수출 최근 동향과 향후 과제’, p.4-p.6, 산업연구원, 2022.
[30] 조영모, “개념기반 인공지능 융합교육프로그램 개발”, p.3-p.12, 성균관대학교, 2023.
[31] 정보와 통신, “인공지능 기술 발달에 따른 사이버 위협과 이에 대한 대응 방안”, p.8-p12, 2022.
[32] 정두산, “국방인공지능(AI) 생태계구축방향연구”, p.2-p.11, 국방연구, 2021.
[33] 정보통신기획평가원, “주간기술동향 1888호”, p.2-p.3, 2019.
[34] 정성배, “산업보안 관리활동이 기업의 보안성과와 업무효율성에 미치는 영향”, 용인대학교, p.4-p.8, 2015.
[35] 정원후, “산업보안기본법 입법 필요성 및 입법방향에 관한 연구”, p.5-p.7, 중앙대학교, 2019.
[36] 최기일, ‘미래 국방을 대비한 인공지능 기반의 방위산업 발전방향 연구’, p.6-p.22, 한국방위산업학회, 2021.
[37] 한국콘텐츠학회, “인공지능기반 보안관제 구축 및 대응 방안”, p.2-p.9, 2021.
[38] 홍준희, “인공지능기반 보안관제 구축 및 대응 방안”, p.5-p.11, 2021.

2. 국외 문헌

[1] Attaullah, H. M., Khan, R. A., & Mughal, S. “Cyber security forIndustrial Control System - A Survey. iKSP Journal of Emerging Trends in Basic and Applied Sciences“, p.4-p.15, 2021.

[2] Dhaliwal, A. “Reinventing Logistics: Use of AI & Robotics”, p.11-p.12, Technologies. BUSINESS RESEARCH AND INNOVATION, 2021.

[3] DoD, “DoD Artificial Intelligence Education Strategy”, p.3-p.6, 2020.

[4] Hutter, Reinhard, and Marcus Hutter, “Chances and Risks of Artificial Intelligence－A Concept of Developing and Exploiting Machine Intelligence for Future Societies. Applied System Innovation”, p.8-p.10, 2021.

[5] IBM Corporation, “IBM Cost of data report 2021”, p.2-p.3, 2021.

[6] Kshetri, N. “Economics of Artificial Intelligence in Cybersecurity. IT Professional“, p.6-p.8, 2021.

[7] Russell Stuart Peter Norving, “Artificial Intelligence : A modern approach”, p.4-p.6, 1995.

[8] U.S. Department of Defense, "Artificial Intelligence Utilization Plan", p.2-p.5, 2020.

[9] White House, “preparing for the future of artificial intelligence”, p.9-p.16, 2016.

3. 기 타

[1] 구글, “국내・외 인공지능 능력시험”, (https://certlys82.tistory.com/entry/%EA%B5%AD%EB%82%B4-%EC%9D%B8%EA%B3%B5%EC%A7%80%EB%8A%A5-%EB%8A%A5%EB%A0%A5%EC%8B%9C%ED%97%98-AICEAIFB, 검색일 2023.3.2.)

[2] 국방부 보도자료, “국방부-과학기술정보통신부, 과학기술 강군 육성 및 디지털 인재양성에 박차를 가하다”, (https://www.korea.kr/news/pressReleaseView.do?newsId=156509105, 검색일 2023.1.10.)

[3] 국방일보, “수출 170억 달러 기록 견인한 무기들”, (https://kookbang.dema.mil.kr/newsWeb/20230111/1/ATCE_CTGR_0020010016/view.do, 검색일 2023.1.10.)

[4] 보안뉴스, “SW 보안을 넘어 HW 중심의 보안 체계 전환 필요”, (https://blog.naver .com/cwoon3825/222436162734, 검색일 2023.1.2.)

[5] 오피니언, “맞춤형 양성이 필요한 사이버보안 인력”, (https://www.asiatime.co.kr/article/20210525500061, 검색일 2023.1.5.)

[6] 인공지능 신문, “딥러닝, 적대적 공격 막은 방어프레임 개발...KAIST, 인공지능 방어 성능 강화”, (https://www.aitimes.kr/news/articleView.html?idxno=26512, 검색일 2023. 3.2.)

[7] 인공지능 신문, “인공지능이 사이버 보안을 강화할 수 있는 3가지 방법은”, (https://www.aitimes.kr/news/articleView.html?idxno=24170, 검색일 2023.1.3.)

[8] 한경신문, “AI 활용 능력′ 검증할 수단 없는 한국…아마존은 자체 시험만 12개”, (https://www.hankyung.com/economy/article/2022100209481, 검색일 2023.1.7.)

[9] 한국물리학회, 양자정보기술,(https://wiki.quist.or.kr, 검색일 2023. 4.24.)

[10] AI타임즈, “인공지능 시대, 새로운 사이버 보안의 과제”, (https://www.aitimes.com/news/articleView.html?idxno=139180, 검색일 2023.3.14.)

[11] newdaily , “인공지능이 인간과 싸운다. 미 AI조종사 무인스텔스 전투 테스트”, (https://www.newdaily.co.kr/site/data/html/2020/12/17/2020121700200.html, 검색일 2023.2.13.)