Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 10 pp. 682-689, 2023

https://doi.org/10.5762/KAIS.2023.24.10.682
ISSN 1975-4701 / eISSN 2288-4688

방위산업 디지털 전환에 따른 보안위협 분석 및 대응방안

류지선*, 박정호
국방기술품질원

Analysis and Countermeasures of Security Threats to Digital Transformation in Defense Industry

Jiseon Yu*, Jeongho Park
Defense Agency for Technology and Quality

요 약 4차 산업혁명으로의 시대적 흐름과 디지털 트윈, 빅데이터, AI 등 기술이 진보하면서 초연결 시대가 도래하였다. 이에 국방분야에서도 사물과 사람이 커뮤니케이션 할 수 있도록 디지털 전환이 빠르게 진행 중이다. 이와 같은 산업 환경의 변화 속에서 불법적으로 정보를 취득하고자 하는 해커 입장에서는 공격 표면이 늘어나 공격에 활용할 수 있는 출입구가 더욱 많아진 것이다. 방산업체는 오래 전부터 해킹 공격의 먹잇감이 되어 왔다. 따라서 초연결 시대로 전환하는 기점 속에서 무기체계를 개발하고 양산하는 방위산업 환경의 변화를 예측하고 이에 따른 공격표면과 보안위협에 대한 선제적인 분석이 필요한 상황이다. 본 논문에서는 방위산업 분야에 영향을 줄 수 있는 핵심 기술을 디지털 트윈, 빅데이터, AI로 판단하고 방위산업 디지털 전환 환경의 보안 위협을 공급망, 내부자, 네트워크로 구분하여 분석하였다. 그리고 관리적 관점에서 신기술 도입 간 보안 내재화, 업체 자체 공격표면 관리 지침 수립, 기술 발전을 반영한 방위산업 규정 개정과 같은 대응 방안을 제안한다.

Abstract The technological advances in Digital twins, Big Data, and Artificial Intelligence have developed into the Hyper-Connected Society era. Accordingly, the battlefield environment and defense industry are being converted into a network-based environment. On the other hand, digital transformation has widened the scope of supply chain management, increased the security threats of insiders, and increased the exposure of vulnerabilities in the network. In particular, because the defense industry has been a target of hackers, it is necessary to analyze security threats in advance. As the attack surface increases, security threats are on the rise. This paper proposes countermeasures to security internalization, attack surface management guidelines, and defense industry regulations to identify attack surfaces that may occur in the digital transition environment to distinguish and control security threats.

Keywords : Digital Twin, Bigdata, AI, Security, Threat, Defense, Digital Transition Environment

1. 서론

네트워크로 사람과 사람을 잇고 사물과 사물을 이어 커뮤니케이션 할 수 있는 초연결 시대로 발전하면서 전장환경을 포함한 방위산업 전반에도 네트워크 기반 환경으로 변화하고 있다. 규모가 큰 항공 및 함정 무기체계 사업에서는 이미 체계 관리를 위해 부품 정보나 고장 이력 등 지금까지 쌓아왔던 빅데이터를 기반으로 AI 기술을 활용해 제품의 수명을 예측하거나 고장 관리 등에 활용 중이며 디지털 트윈 기술을 적용하여 실제 체계와 가상 소프트웨어를 이어 센서 신호를 실시간으로 수집하면서 이를 활용해 위험 분석이나 원격으로 장치를 조작하

*Corresponding Author : Jiseon Yu(DTaQ)
email: gsun2@dtaq.re.kr
Received August 29, 2023 Revised September 11, 2023
Accepted October 6, 2023 Published October 31, 2023

는데 활용하고 있다. 이처럼 모든 것이 연결된 산업 환경의 변화 속에서 불법적으로 정보를 취득하고자 하는 공격자 입장에서는 공격 표면(attack surface)이 늘어나 공격에 활용할 수 있는 출입구가 더욱 많아진 것이다.

민간 제조환경에서는 이미 디지털 전환이 상당 부분 진행되어 각종 센서로부터 제품의 상태 정보 등을 실시간으로 축적하여 축적된 데이터 기반으로 정보를 분석하여 제품의 고장을 예측한다거나 신기술 개발에 활용하고 있다. 여기서 센서로부터 받은 제품의 정보들은 유출이 되어도 경쟁업체가 아니면 유의미한 정보로 활용할 수 없지만 방위산업에서는 아주 작은 데이터 유출이 쌓이고 나아가 우리군 전력을 가늠할 수 있는 정보가 되어 국가안보를 위협할 수 있기 때문에 사전에 보안 위협을 분석하고 대응 방안 마련이 필요하다. 실제로 지난 5년간 방위사업청, 국방과학연구소 등 방위산업 관련 기관 해킹 시도가 무려 3만 2천 건이 발생했을 만큼 오래전부터 방위산업 분야는 해커의 공격 대상이 되어 왔으며 실제 일부 기밀 정보가 유출되는 피해를 입기도 했다[1,2]. 이러한 상황에서 공격 표면이 늘어나는 것은 매우 위험한 상황이지만 기술의 발전과 인구 감소의 가속화, 전세계적인 탄소 중립 추진에 대한 흐름으로 현재 산업 전 분야에서 디지털 전환은 피할 수 없는 숙제가 되었다.

본 논문에서는 방위산업 분야에 도입되는 디지털 전환 환경에서 발생할 수 있는 공격표면을 식별하고 여기서 발생할 수 있는 보안위협을 분석하여 관리적 관점의 대응 방안을 제안한다.

2. 이론적 배경

2.1 방위산업 디지털 전환 핵심 기술

2.1.1 디지털 트윈

디지털 트윈(Digital Twin)이란 가상공간에 실물과 똑같은 물체(쌍둥이)를 만들고 모의시험(시뮬레이션)을 통해 성능과 같은 궁금증을 검증하거나 실물의 상태를 가시화할 수 있는 기술을 말한다. 즉, 디지털 트윈은 물리적 자산이나 프로세스를 디지털로 복제(Modeling)한 것으로, 물리적 자산으로부터 생산되는 데이터와 상시 연계되어 있는 살아 있는 시스템이다[3]. 디지털 트윈은 인터넷으로 연결된 환경을 통해 실제 물리체계에서 일어나지 않은 일을 미리 모의시험을 할 수 있어 다양한 분야에 적용될 수 있다. 제조분야, 도시공간, 발전소 등은 물론이며 방위산업 분야에서도 데이터를 기반으로 한 의사결정이 가능한 체계 또는 새로운 비즈니스 모델 개발에 접목 될 수 있다. 이는 다양한 산업 사회문제를 해결할 기술로 자리 잡을 것으로 전망된다[4]. 디지털 트윈의 보안 위협으로는 디지털 트윈은 '사악한 디지털 트윈(evil digital twin)이라는 말이 있을 정도로 랜섬웨어나 피싱 등 악의적 공격에 활용될 가능성이 높아 일부 보안전문가 사이에서는 우려가 큰 상황이다[5].

2.1.2 빅데이터

가트너에서는 2012년에 빅데이터를 '향상된 시사점(Insight)과 더 나은 의사 결정을 위해 사용되는 비용 효율이 높고, 혁신적이며, 대용량, 고속 및 다양성의 특성을 가진 정보 자산'이라고 정의하였으며[6], McKinsey는 데이터베이스의 규모에 초점을 맞추어, '일반적인 데이터베이스 SW가 저장, 관리, 분석할 수 있는 범위를 초과하는 규모의 데이터'라고 정의하였다. 또한, IDC는 데이터베이스가 아닌 업무수행에 초점을 맞추어, '다양한 종류의 대규모 데이터로 부터 저렴한 비용으로 가치를 추출하고 데이터의 초고속 수집, 발굴, 분석을 지원하도록 고안된 차세대 기술 및 아키텍처'로 빅데이터를 개념화 하였다[7]. 이를 종합하면 빅데이터의 정의는 데이터의 규모가 방대하고(Volume), 데이터의 종류가 다양하며(Variety), 데이터 처리 및 분석을 적시에 해결해야 하는(Velocity) 특성을 가지고 있는데, 최근에는 여기에 데이터의 품질에 영향을 받는 진실성(Veracity)과 데이터가 갖는 실제 가치를 의미하는 가치(Value)까지 개념이 확장되었다. 여기서 말하는 빅데이터는 일반적으로 데이터베이스로 저장, 관리, 분석할 수 있는 한계를 넘어서며, 기업정보, 웹, 이미지/동영상, SNS, 센서 스트림 등 정형/비정형 데이터를 모두 포함하고, 분석과 예측에 있어서 실시간 처리 등 적시성을 요구한다고 정의할 수 있다[7]. 빅데이터와 관련된 보안 문제는 정보를 독점적으로 수집해 강력한 권력을 구축한 뒤 정보를 통한 권력을 기반으로 사회를 통제하는 '빅브라더(big brother)' 이다. 최근 대부분 기업에서는 사용자에게 딱 맞는 맞춤형 서비스를 제공한다는 취지로 사용자의 소비 패턴을 분석하여 취향에 맞는 제품이나 서비스를 추천하는 각종 서비스를 속속 내놓고 있다. 뿐만 아니라 공공분야에서도 국가에서 보유한 다양한 데이터를 공공데이터로 제공하고 있고 금융 분야에서는 통합 신용관리를 할 수 있는 마이데이터 서비스를 제공하고 있다. 이처럼 우리 일상 속에서 그저 스마트폰의 한 앱을 다운받아 쓰고 신용카드를 썼을 뿐인데 개인의 취향이나 위치, 생활 패턴 등이

고스란히 드러나게 되는 것이다.

2.1.3 AI

인공지능은 1956년 미국 Dartmouth대학교에서 개최된 워크숍에서 처음 사용한 용어이다. 이는 인간의 추론능력 및 인지능력을 컴퓨터로 구현하는 과학기술로서 ①상황을 인지하고, ②이성적·논리적으로 판단·행동하며, ③감성적·창의적 기능을 수행하는 능력까지 포함하는 것이다[8]. 인공지능은 인간의 언어, 음성, 시각, 감성 등의 인지능력, 학습능력, 추론능력 과 같은 지적 능력을 구현하는 기술분야이다. 한편, 인공지능은 '인공지능 시스템'으로 인간의 목적에 따라, 인간에 의해 설계된 시스템을 기반으로, 주어진 데이터를 내부적으로 분석하여 외부 환경에 영향을 주는 행위를 수반한다[9]. 인공지능을 가능하게 하는 기술로는 머신러닝(machine learning)과 딥러닝(deep learning)이 있다. 머신러닝은 경험적 데이터를 기반으로 학습을 하고 예측을 수행하고 스스로의 성능을 향상시키는 시스템과 이를 위한 알고리즘을 연구하고 구축하는 기술이다. 머신러닝은 기본적으로 알고리즘을 이용해 데이터를 분석하고, 분석을 통해 학습하며, 학습한 내용을 기반으로 판단이나 예측을 한다. 딥러닝은 인간의 뇌 신경회로를 모방한 신경 회로망을 다층적으로 구성하여 다양한 데이터를 통해 마치 사람처럼 생각하고 배울 수 있도록 하는 기술이다[10].

2.1.4 스마트팩토리

통신기술의 발달은 제조업 분야와 ICT(Information & Communication Technology)의 융합을 기반으로 4차 산업혁명을 가속화 시켰다. 이에 따라, 제조설비와 생산 전 과정이 네트워크와 연결되어 생산 프로세스를 개선하고, 시장의 동향 파악 및 분석과 설비의 관리를 효율적으로 할 수 있는 스마트팩토리가 등장하였다. 한국산업표준 'KS X 9001'에서는 스마트팩토리를 제품의 기획, 설계, 생산, 유통, 판매 등 전통적인 제조산업의 전 과정에 AI, 빅데이터, 클라우드 등의 ICT 기술로 통합하여, 최소한의 제조공정 비용과 시간으로 고객 맞춤형 제품 생산을 지향하는 공장으로 정의하고 있다[11]. 스마트팩토리의 보안 취약점은 기존의 제조공장에서 겪은 물리적 공격, 고장/오작동과 같은 분야를 벗어난 통신분야와 연관된 해킹, 악성코드 감염, 사이버공격, 랜섬웨어 등 사이버 상에서의 위협에 노출되었고 실제로 큰 피해를 불러일으켰다. 이에 대해 아래 네 가지 종류의 보안 요구사항이 존재한다. ① 네트워크 보안 : 네트워크 분리/접근통제, DDoS 방지, 원격접근통제, 무선 보안, ② 침입/악성코드 탐지 : 침입 차단/방지/탐지, Anti-Virus, 패치관리, ③ 중요 정보 보호 : 암호화/DB보안, 인증 및 권한관리, 문서·이메일 보안, ④ 생산설비 보안 : 기기/상호인증과 같은 보안 요구사항이 있다. 이를 수행한다면 생산성 향상, 에너지 절감, 인간 중심의 작업환경 구현, 개인 맞춤형 제조, 융합 등 새로운 제조환경에서 능동적인 대응이 가능할 것으로 보인다[12].

2.2 방위산업 디지털 전환

국방분야에서는 국방혁신 4.0을 추진하며 4차 산업혁명 과학기술 기반 첨단전력 확보를 통한 AI 과학기술강군을 육성하고 있다. 기술발전 추세에 따라 유·무인 복합전투체계를 단계적으로 구축하는 것을 목표로 하고 있으며 우주, 사이버, 전자기 영역에 대한 작전 수행 능력을 강화를 꾀하고 있다. 따라서 AI 기반 고성능 무기체계와 전력지원체계 개발 및 운용을 위해 국방데이터 구축 및 관리, 초고속 및 초연결 네트워크 구축으로 국방 AI 기술을 확보 하는데 노력하고 있다[13]. 이에 방위산업에서는 디지털트윈 기술을 활용해 스마트 공장을 구현하고 자율운항을 위한 기술 연구가 활발히 진행 중이다[14].

군은 빅데이터 기술을 활용해 업무처리·관리 및 분석 중심의 군수 분야 혁신을 꾀하고 있다. ①업무처리 혁신은 군수통합정보체계와 군수시설에 대한 관리체계를 말한다. 전력화 중인 군수통합정보체계는 소요, 조달, 수불, 저장, 처리 등 일상적인 업무처리 중심으로 정형화된 군수 데이터를 중심으로 활용하는 정보체계로 정비공장, 물류창고, 탄약고, 유류고 등 군수시설의 관리에 데이터를 활용하고자 한다. ②관리 및 분석 분야에서는 총 수명주기를 관리하기 위함이다. 최근 전력화된 주요 무기체계는 기계식에서 SW를 적용한 전자식 장비로 변화되고 있고, 가동률 향상과 같은 목표 달성을 위해 다양한 군수 데이터를 활용하여 진단과 예측을 하고자 한다. 특히나 센서를 적용하여 얻어지는 데이터를 저장, 관리, 분석하기 위한 노력을 하고 있다. 미군은 2000년 이후 주요 전투 장비에 센서 데이터를 부착하여 전투 장비의 상태를 기반으로 한 정비를 시행 중이며 호주군은 차기 장갑차 구매를 위한 경쟁 입찰 시 센서 데이터 부착을 요구한 것이 이와 같은 맥락이라고 볼 수 있다[15].

AI·데이터 기반 핵심업무 고도화로 효율적이고 신뢰가능한 국방을 구현하고자 한다. 그 방안으로는 국방 지능화 추진 로드맵('20)에 따른 핵심업무 AI 융합 확산과 전군 공통 AI 서비스를 개발·지원하는 지능형 플랫폼(대

규모 국방 데이터를 빠르게 분석·처리하고 의료, 군수, 행정 등 공통 서비스 개발·지원을 목적으로 하는) 구축 그리고 국방 데이터의 표준화 및 축적·공유를 위한 지능 데이터센터 구축이 있다. 이를 통해 지휘체계를 지원하는 지능(협업·결심 등) 개발 가속화를 하고자 한다. 나아가 ①위협정보 탐지 및 침해사고 대응(신고 접수 → 분류 → 검증 → 조치) 전반에 AI 기술 적용을 통한 지능형 기술 기반의 사이버 침해사고 탐지·분석·대응체계 구축 ② 다양한 기기·네트워크의 취약점 자동분석, 암호 안전성 검증 등 AI 기반 정보보호 기술개발 ③민간의 정보보호 AI 머신의 종합적 검증 및 컨설팅 제공을 위한 '정보보호 AI 학습지원 센터' 구축을 통한 정보보호 지능화 혁신을 꾀하고 있다[16].

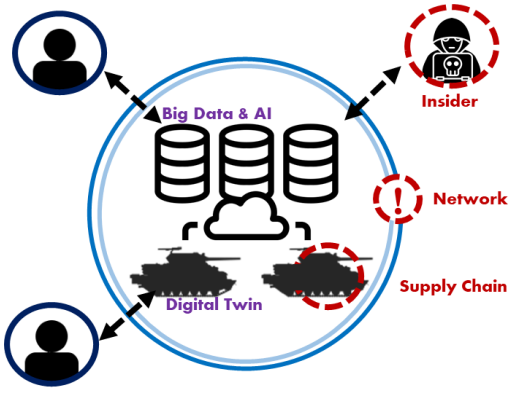

Fig. 1. The technologies and the threats in defense industry

3. 방위산업 디지털 전환 보안위협 분석

방위산업체가 아닌 일반 제조업체 역시 같은 위협이 존재하고 더 다양한 위협이 존재하겠지만 특히 방산업체는 국가 안보와 관련되어 보안에 더욱 엄격하다. 방산업체는 오래전부터 해커의 공격대상이 되어왔다. 지난 5년간 방사청, 국방과학연구소 등 방산관련 기관 해킹 시도가 3만 2천 건이 있었고[1], 실제 일부 기밀정보가 유출되는 피해를 입기도 했다[2]. 공격에 사용된 다양한 위협요소 중에서 본 논문에서는 크게 공급망, 내부자, 네트워크, 데이터 측면으로 구분하여 위협을 분석하였다. 특히 공급망은 무기체계와 같이 대규모 체계는 서브 시스템들이 통합되는 형태로 개발되고 아주 작게는 부품 단위로도 개발 또는 공급업체가 다르기 때문에 주요한 위협 요소로 분류하였다. 내부자와 같은 경우도 유관업무를 수행하는 기관과 담당자는 보안측정, 신원조사 등 보안 절차에 의한 검증을 거치지만 사실상 가장 제어 및 통제가 어려운 위협원인과 동시에 신뢰할 수 있는 인가자가 되어 내부자 역시 주요 위협이 될 수 있다. 또한 네트워크 위협을 분석한 이유는 디지털 전환의 흐름에 따라 무기체계를 제조하는 환경 뿐만 아니라 획득 프로세스 전반에 따라 네트워크 환경이 확대되고 있으므로 주요 위협으로 구분하여 이를 분석하였으며 이를 그림으로 표현한 것이 Fig. 1이다.

3.1 공급망

제품과 서비스의 설계, 개발, 제조, 운용, 보수, 폐기 단계의 프로세스에서 업무를 외부로 위탁하여 공급하는 형태를 공급망이라 한다. 무기체계 규모에 따라 많게는 수만 개의 부품이 탑재된다. 이 중에 체계개발 업체에서 자체 생산하는 부품이 있는 반면 서브 시스템은 협력 업체에서 개발하기도 하고 부품을 수입하는 등 다양한 경로로 획득한 시스템이 하나로 통합되어 무기체계를 이룬다. 따라서 신뢰할 수 있는 공급망 확보는 필수적이며 조직 중심의 보안관리 체계를 갖추고 설계부터 납품까지 안전한 공급망을 유지하는 것은 방위산업에서 매우 중요하다. 또한 방산분야 디지털 전환이 본격적으로 진행되면 무기체계에 탑재되는 각종 물리 센서들과 똑같은 가상의 체계를 개발하여 센서로부터 부품의 상태 정보 등의 데이터를 실시간으로 수집하고 수집된 데이터를 활용하여 적절한 AI 기술을 적용하여 부품의 수명분석 등에 활용될 것이다. 그렇기 때문에 무기체계 획득과 관련된 방위산업 공급망의 보안수준을 주기적으로 진단하고 실태를 확인하는 것은 매우 중요하다.

실제 2016년 크립토와이어(kryptowire)가 BLU프로덕트 저가형 안드로이드 휴대폰 펌웨어에서 72시간 간격으로 중국 서버로 사용자 정보를 전송하는 백도어를 발견한 사례가 있었는데 이는 설계 단계의 공급망 공격사례로 볼 수 있다[17]. 남 일이라고 생각했던 이런 사례가 우리나라에서도 최근 확인 되었는데, 공공기관에 도입된 중국산 기상관측장비에서 무선으로 도청, 감청이나 해킹이 가능한 백도어 프로그램을 발견하였다[18]. 실제 이런 사례가 방산에서 발생하는 경우 협력업체의 납품 과정 전체를 전부 들여다 볼 수 없기 때문에 납품받은 부품에서 이와 같이 설계 단계에서 심어진 백도어 프로그램을 발견하는 것은 매우 어렵다.

따라서 공급망 보안이 취약한 경우에는 위 사례처럼

부품 자체에 백도어 프로그램을 삽입하는 백도어 공격뿐만 아니라 하드웨어 부품의 신호를 수집하고 이를 분석하여 주요 정보를 탈취하는 부채널 공격의 대상이 될 수도 있기 때문에 무기체계의 공급망에 해당되는 방산업체 자체적으로 조직 관점의 보안 지침을 수립하고 관련 보안 규정을 준수하기 위해 노력해야 한다.

3.2 내부자

보안사고 대부분은 개인의 부주의에 의해 발생한다. 가령 획기적인 보안 기술을 사용하여 보안시스템을 마련했다 하더라도 인가된 사용자가 자신도 모르는 사이에 혹은 자신의 의지하에 공격을 수행하는 주체가 된다면 그 보안기술은 아무런 쓸모가 없어진다. 지난 해 현역 장교가 비트코인을 받고 군사기밀을 넘긴 사례가 있었다[19]. 정보에 접근할 수 있는 인가된 사용자였던 군 장교는 시계처럼 생긴 불법 장비를 반입한 채 각종 보안 인증을 거쳐 원하는정보에 접근할 수 있었을 것이다. 올해 4월에도 미군이 전 세계에서 수집한 350여 건의 비밀을 온라인 비밀채팅방에 공개한 사례 등 내부자 위협은 국방분야의 큰 숙제가 되었다[20]. 보통 시스템 해킹은 최상위 권한을 탈취하는 것을 목표로 수행되는데 이처럼 인가된 사용자가 공격자가 되는 내부자 위협의 경우에는 고도의 기술을 쓰지 않고도 원하는 정보를 탈취할 수 있는 다루기 어려운 문제가 된다.

방산에서 디지털 전환으로 현재보다 더 큰 디지털 환경이 구성되면 이 환경을 구축하기 까지 관련 업무를 수행하는 내외부 직원이 늘어나 필수불가결하게도 디지털 전환을 위한 환경이 모든 유관업무 수행자들에게 공개되어 더 많은 내부자가 발생하여 모두가 위협원이 되는 셈이다. 물론 국방보안업무훈령이나 기타 보안 관련 지침에 따라 해당 업무를 수행하는 업체의 보안측정과 구성원을 대상으로 신원조사를 수행하고 또한 주기적인 보안교육 등을 실시해야 하는 규정을 충분히 준수하였음에도 불구하고 앞선 사례와 같이 인가된 사용자가 공격자가 되는 내부자 공격을 막기에는 분명한 한계가 존재한다.

3.3 네트워크

네트워크는 디지털 전환에 있어 보호해야 할 자산으로 연결되는 통로이자 동시에 공격자의 먹잇감이 되는 공격 표면으로 노출되기 때문에 보안이 매우 중요하다. 국가기반시설이나 국방 등에서는 업무망을 외부 인터넷망을 물리적으로 분리하는 망분리를 구성하여 외부의 침입과 내부정보의 유출을 막는다. 그러나 실제 관리를 위해 이 분리된 망을 잇는 DMZ 구간이 존재하여 이 구간이 공격을 당하면 바로 업무망에 피해를 입힐 수 있다.

실제 이론적으로는 이러한 망분리로 외부의 침입이 불가능하다고 하나 2010년 6월 이란 원자력발전소에서는 원심 분리기 1천여 대가 마비되어 사이버무기로 보는 시선이 있을 정도로 큰 파장을 일으킨 스턱스넷(stuxnet)이라 불리는 초유의 사태가 있었다. 우리도 이미 2021년 3월 한국전력공사 통신망이 해킹을 당해 검침 모델 1만여대 가량 통신이 두절된 바 있다. 뿐만 아니라 한국원자력연구원과 방산업체인 한국항공우주산업, 대우조선해양에서 해킹으로 인한 정보 유출 사건이 있었다. 우리나라의 사례가 앞선 스턱스넷과 완전히 같은 방식으로 발생했다고 할 순 없지만 일반적으로 망분리를 수행하는 국가주요기관이 해킹 피해를 입었다는 점에서 유사 사례로 판단하였다.

4. 대응 방안

초연결 시대로의 디지털 전환에서 보안 공격 대상은 날로 늘어나고 해킹 기술 또한 발전하고 있는 상황 속에서 방위산업에서 디지털 전환으로 발생할 수 있는 위협을 3장에서 크게 셋으로 구분하여 분석 하였지만 보안은 단순히 각 위협에 대응하는 한 가지 방법으로 해결할 수 없기 때문에 기술적, 물리적, 관리적 모든 부분을 고려한 보안 대책을 수립해야 한다. 본 장에서는 앞서 식별한 위협에 대한 대응 방안을 관리적 측면을 중심으로 제안하며 이를 전체적으로 시각화하여 나타낸 것이 Fig. 2 이다.

4.1 신기술 도입 간 보안 내재화

보안 내재화란 요구사항 분석 및 설계 단계부터 제품의 보안성, 신뢰성, 안전성 등의 요소를 종합적으로 고려해 복잡도를 감소시키고 제품의 신뢰성을 달성하는 것을 말한다[21]. 우리군은 유무인 복합전투체계를 단계적으로 구축하며 AI 기반 핵심 첨단전력 확보에 노력하며 우주, 사이버 등 첨단 전력체계 발전을 도모하고 있다. 이와 같이 신기술의 등장에 따라 첨단과학기술 기반 체계에 대한 군의 소요가 증가 하는 것이다. 군의 소요에 따라 방산업체들은 관련 기술을 구현하여 실제 무기체계로 개발하게 되는데 현재는 보안보다 성능에 초점이 맞추어 획득 프로세스가 진행되고 있는데 보안 내재화를 수행하

Fig. 2. Countermeasures for security threats

여 무기체계나 국방 정보시스템에 보안을 위한 어떤 기술을 활용할 것인지 단계 내내 지속적인 검토가 필요하다. 국방분야에서는 현재 한국형 사이버보안제도를 개발하여 소요단계부터 폐기단계까지 보안 내재화 달성을 위한 보안 위험 관리 수행 계획에 있다[22].

이밖에도 최근 공공 데이터나 흩어진 데이터를 하나로 모아 더 큰 가치를 창출하고자 하는 움직임이 일고 있다. 국방에서도 같은 움직임이 이미 진행되어 왔고 시간이 지날수록 데이터가 축적되어 처리해야 하는 양이 기하급수적으로 늘어나기 때문에 확장성을 고려하여 대용량의 데이터를 안전하게 저장하고 처리할 수 있도록 시스템 구축이나 무기체계 개발 초기 단계부터 보안 내재화를 통해 보안성을 확보해 나가야 한다.

4.2 공격표면 관리 지침 수립

사이버보안은 대부분 방어적 관점으로 위험을 관리 해왔다. 그러나 현재는 공격자 관점으로 시스템을 관찰의 필요성에 따라 공격표면관리(이하 ASM, Attack Surface Management)에 많은 기업이 관심을 가지고 이를 도입하는 추세이다. ASM은 자산을 식별하고 분류 및 분석을 통해 취약성을 결정하고 공격 가능성에 따라 우선순위를 지정한 뒤, 우선 순위에 따라 위험을 관리하고 지속적으로 모니터링한다[23]. 일반적으로 자산을 식별하여 위협을 분류하고 위험을 관리하는 절차와 같은데 ASM은 악의적 내부자 또는 부적절한 사용자에게 피싱 사기 예방 교육을 진행하는 등 조직의 물리적, 소셜 엔지니어링 공격 표면 취약성도 함께 해결할 수 있다는 점에서 차이가 있다. 이와 같이 ASM 수행으로 조직 자체의 보안을 자체적으로 엄격하게 관리하면서 내부자 역시 위협원으로 구분하여 지속적으로 관리할 수 있다. 특히 방산에 도입이 필요한 이유는 방위산업은 현재 디지털 전환의 기로에 있기 때문에 전반적인 시스템 구축 시점에서부터 공격표면을 관리하여 더욱 세밀한 분석이 가능하다. 다만 무기체계 획득 프로세스에 따라 공격표면분석 결과와 같은 기술자료들을 관리하는 주체가 달라지고 체계 운용 환경이 달라질 수 있기 때문에 이에 따른 대응방안과 기존 기술자료의 이관 방안 등에 대한 고민이 필요하다.

4.3 기술 발전을 반영한 방위산업 규정 개정

국방분야는 특히 국가 안보에 직결되는 사항이기 때문에 보안이 매우 중요하여 자료를 반출하는 등 자료 취급에 민감한 사항들은 발생 가능한 위협을 최소화하기 위해 다소 불편하더라도 고전적인 방식을 고수하고 있다. 그러나 첨단 기술의 등장과 디지털 전환의 흐름으로 국방혁신 4.0을 추진하며 첨단과학기술 기반 AI 과학기술 강군 육성을 목표로 하는 등 국방분야에서도 시대의 변화에 대응하며 상당 부분의 변화가 진행되고 있다. 이 국방혁신 4.0의 일환으로 국방AI센터 및 데이터분석센터 신설을 통해 국방R&D 체계 구축을 준비하고 있는데 이에 발맞춰 방위산업 관련 규정 역시 산업 환경 변화에 따른 개정이 필요하다.

4.4 고려사항 및 한계점

무기체계 획득 프로세스에서 방위산업은 소요단계부터 폐기까지 전 단계에 직·간접적으로 모든 범위에 걸쳐있다. 무기체계는 정부주도 사업으로 개발중에는 방위사업청에서 사업을 관리하고 전력화 이후 군에게 인도되어 소요 부대에서 운용하게 된다. 이처럼 무기체계 획득 프로세스는 방산업체 뿐만 아니라 직접 체계를 사용할 소요군, 개발 과정에서 보안대책 및 보안측정을 수행하는 방첩사령부, 무기체계 연구개발 사업을 관리하는 방위사업청 등 많은 관련 기관들이 존재하는데 앞서 제안한 보안 내재화, 공격표면 관리 지침, 관련 규정 개정 등을 달성하기 위해서는 이러한 전 기관의 공감과 노력이 필요한 것이 첫 번째이다. 그러나 보안 내재화나 공격표면 관리 지침이 규정에 반영되면 연구개발기관에서는 이에 필요한 개발 기한 연장과 사업비 증액을 요구할 것이며 사업관리기관과 기술지원기관에서는 불가피하게 무기체계 획득 프로세스에서 수행하고 검토해야 할 항목과 절차가 늘어나 일부에서는 과다한 행정 소요라는 인식이 생길 수 있는 문제점이 있기 때문에 디지털 전환에 대한 보안성 확보를 위한 관련 기관들의 공감과 모두의 노력이 필요하다.

5. 결론

본 논문에서는 초연결 시대의 방위산업 디지털 전환의 보안 위협을 공급망, 내부자, 네트워크로 나누어 분석하였고 이에 대한 대응 방안으로 관리적 관점의 보안 내재화, 공격표면 관리 지침 수립, 규정 개정을 제안하였다. 이 대응방안을 실현하기 위해 국방부나 방위사업청 등 정부기관에서 규정 제·개정을 선도하겠지만 이에 직접적으로 영향을 받는 곳은 일반 방산업체가 될 것이기 때문에 사전에 규정 개정에 따른 개발 프로세스 절차 등의 변화에 충분히 대응할 수 있도록 방산업체의 의견을 적극 수렴하여 민·관·군이 함께 디지털 전환에 대응해야 한다. 그리고 방위산업에 첨단 기술 도입 뿐만 아니라 보안성까지 놓치지 않고 확보해야 하기 위해 디지털 전환으로 발생할 수 있는 산업 환경의 변화를 사전에 점검하고 분석하여 중대 정보가 유출되지 않도록 준비해야 한다. 현재는 기술을 도입하는 시점이므로 앞서 제안한 방안들을 선제적으로 도입할 수 있는 최적의 시기이다. 다만 디지털 전환에 매몰되어 반드시 필요한 절차를 간소화하거나 또는 불필요한 행정 소요가 발생하지 않도록 주의해야 한다. 그리고 방위산업 관련 정보는 국가 안보에 직결되는 사항인 만큼 모두가 보안에 경각심을 가지고 국방 및 방산에 편의성을 확보하면서 보안성을 확보할 수 있는 방안 마련을 위한 지속적인 연구가 필요하다.

References

[1] [Internet]. KOIT [cited 2022 Oct 5], Available From: https://www.koit.co.kr/news/articleView.html?idxno=103913

[2] [Internet]. boannews [cited 2021 Oct 6], Available From: https://www.boannews.com/media/view.asp?idx=101298

[3] H. S. Sakong, 「KRIHS Policy Brief」, 6page, KRISH, 2018, "Digital Twin Space(DTS) Construction Strategy Leading the 4th Industrial Revolution.

[4] Policy Research Team, Gartner Announces Top 10 Strategic Technology Trends for 2018, Weekly Trends in IoT Industry, Korea Intelligent IoT Association, 2017.

[5] [Internet]. ITWORLD [cited 2023 May 15], Available From: https://www.itworld.co.kr/news/290599

[6] Gartner, The Importance of 'Big Data' : A Definition, 2012.

[7] C. W. Ahn, S. G. Hwang "Big Data Technologies and Main Issues", Communications of the Korean Institute of Information Scientists and Engineer, Vol.30, No.6, pp10-17, 2012.

[8] S. Y. Cho, "Artificial Intelligence(AI) and Ethics", AI and Human society, Vol.1 No.2, 2020.

[9] E. S. Heo, Y. H. Lee, J. W. Shim, "Why Ethics is: A Landscape of Modern AI Ethics Debate, Its Features and Limitations", Human·Environment·Future, Vol.No.24, 2020.

[10] K. N. Cho, "The development of artificial intelligence and the changing world of artificial intelligence", The Magazine of the IEEK, Vol.48 No.10, pp789-800, 2021.

[11] Korean Agency for Technology and Standards, "Smart factory - Section one: Basic Concept and Structure", KS X 9001-1:2016, 2016.

[12] S. J. Kang, J. M. Oh, S. Y. Oh, Smart Factory Security in the era of ICT convergence security, Journal of Korea Technology Innovation Society, Vol.2019. No.5, 2019.

[13] Ministry of National Defense, Defense innovation 4.0(2023)

[14] [Internet]. Yonhapnews [cited 2022 Apr 19], Available From: https://www.yna.co.kr/view/AKR20220419099900003

[15] S. R. Choi, Y. Kim, J. H. Lim, The Meeting of Defense Forces and Big Data. Prepare for a leap toward 「Optimum, Prediction focus」, Defense and Technology, ISSN 1227-1705, No.497, pp72-83, 2020.

[16] related government department, "National Strategy for Artificial Intelligence", 2019.

[17] [Internet]. AhnLab [cited 2016 Nov 7], Available From: https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=25726

[18] [Internet]. KBS [cited 2023 Aug 21], Available From: https://news.kbs.co.kr/news/view.do?ncd=7754114

[19] [Internet]. KBS [cited 2022 Apr 28], Available From: https://news.kbs.co.kr/news/view.do?ncd=5451391

[20] [Internet]. BBS News [cited 2023 Apr 12], Available From: https://www.bbc.com/korean/articles/c3gre1l3320o

[21] [Internet]. SAMSUNG DISPLAY [cited 2017 Oct 16], Available From: https://news.samsungdisplay.com/11513

[22] Yongseok Lee, Jeong Min Choi.(2020). Research for Application the RMF to the Korean Military. The Journal of Korean Institute of Communications and Information Sciences,45(12),2132-2139. DOI: http://doi.org/10.7840/kics.2020.45.12.2132

[23] [Internet]. IBM [cited 2023 May 15], Available From: https://www.ibm.com/kr-ko/topics/attack-surface-management

류 지 선(Jiseon Yu) [정회원]

- 2018년 8월 : 고려대학교 정보보호대학원 정보보호학과 (정보보호학석사)
- 2018년 12월 ~ 현재 : 국방기술품질원 연구원

〈관심분야〉
무기체계 소프트웨어, 소프트웨어 보안

박 정 호(Jung-Ho Park) [정회원]

- 2017년 2월 : 금오공과대학교 산업공학부 (산업공학석사)
- 2019년 5월 ~ 2022년 6월 : 국방기술진흥연구소 연구원
- 2022년 7월 ~ 현재 : 국방기술품질원 연구원

〈관심분야〉
국방, 사이버 보안, 무기체계 소프트웨어