https://doi.org/10.33778/kcsa.2022.22.2.027

4차 산업혁명 시대의 선제적 위협 대응 모델 연구★

최 향 창*

요 약

4차 산업혁명 시대에는 산업혁신이라는 목표를 달성하기 위해 기존 산업의 생산성을 높일 수 있는 디지털 전환이 더욱 중요해지고 있다. 디지털 전환에는 디지털 뉴딜과 스마트 국방 등이 있으며, 이들은 인공지능과 빅데이터 분석기술, 사물인터넷을 이용한다. 이러한 변화는 사이버공간을 지속해서 확장함으로써 국가의 국방, 사회, 보건 등의 산업화 영역을 더 지능적인 새로운 서비스들로 혁신하고 있다. 하지만 이로 인해 업무 생산성, 효율성, 편리성, 산업 안전성 등은 강화되겠지만, 디지털 전환영역의 확대로 사이버공격에 따른 위험성 또한 지속해서 증가할 것이다. 본 고의 목표는 이러한 위협에 선제적으로 대응하기 위해 미래의 변화로 나타날 수 있는 위협시나리오를 고찰하고, 이를 해결할 근본적인 대안 중의 하나인 미래의 복합안보 상황에서 요구되는 4차 산업혁명 시대의 선제적 위협 대응 모델을 제안한다. 본고는 향후 미래 사회에서 사이버 위협에 능동적으로 대응할 사이버안보 전략과 기술 개발의 선행 연구로 활용할 수 있을 것이다.

A Study on the Model for Preemptive Intrusion Response in the era of the Fourth Industrial Revolution

Hyang-Chang Choi*

ABSTRACT

In the era of the Fourth Industrial Revolution, digital transformation to increase the effectiveness of industry is becoming more important to achieving the goal of industrial innovation. The digital new deal and smart defense are required for digital transformation and utilize artificial intelligence, big data analysis technology, and the Internet of Things. These changes can innovate the industrial fields of national defense, society, and health with new intelligent services by continuously expanding cyberspace. As a result, work productivity, efficiency, convenience, and industrial safety will be strengthened. However, the threat of cyber-attack will also continue to increase due to expansion of the new domain of digital transformation. This paper presents the risk scenarios of cyber-attack threats in the Fourth Industrial Revolution. Further, we propose a preemptive intrusion response model to bolster the complex security environment of the future, which is one of the fundamental alternatives to solving problems relating to cyber-attack. The proposed model can be used as prior research on cyber security strategy and technology development for preemptive response to cyber threats in the future society.

Key words : Fourth Industrial Revolution, Incident Response Models, Cyber Security threats, Cyber threat intelligence, Cyber Security Models

접수일(2022년 5월 31일), 수정일(1차: 2022년 6월 20일), 게재확정일(2022년 6월 29일)

★ 이 논문은 2019년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2019S1A5C2A03082827)

* 대전대학교 안보군사연구원 선임연구원(주저자)

1. 서 론

최근 몇 년간 COVID19의 팬데믹(Pandemic)의 영향으로 디지털 세상으로의 영역 전환은 가속화 되었다[1]. 이러한 디지털 기술의 영역 전환의 가속화로 4차 산업화의 핵심 기술들이 공장, 도시, 금융의 서비스들과 융합되는 등 편리하고 윤택한 삶을 임무(Mission)로 하는 정보통신(Information Technology) 기반의 산업 생태계의 태생을 더욱 가속화하고 있다[1, 2, 3].

디지털 기반의 생태계는 정보통신 기술 기반의 세상으로 AI(Artificial Intelligence)와 상황인식(Context Awareness) 기술과 IoT 센서와 관련된 기술 등 4차 산업화 기술들이 상호 복합적으로 결합 되어 현재와는 비교가 되지 않을 정도로 생산성을 극대화하고, 삶에서 생성되는 데이터를 기반으로 지식을 처리하고 생성해내는 능력이 강화되어, 현재의 기술로는 해결할 수 없는 난제들을 해소할 수 있도록 하는 삶을 태생시키는 것을 목표로 한다[37, 38].

최근의 정보통신 기술이 4차 산업혁명 기술의 극대화를 이루지는 못했지만 근 몇 년 동안 사람을 대신할 수 있는 지능을 갖는 생산물인 로봇과 서비스들이 생성되고 있다. 예를 들면 운전자를 대신할 수 있는 자율 주행차(Self-driving Car), 사용자의 이동 편의성을 지금보다 더 개선하는 스마트 이동(Automated Driving & Smart Mobility), 다양한 산업기반 시설들이 갖추어진 공장 자동화(Smart Factory)와 스마트 계약(Smart Contract) 기능이 있는 핀테크(FinTech) 서비스[4, 5] 등이 이것이다. 이렇듯 정보통신 기반 기술들이 세상을 더욱 편리하게 하고 삶의 가치를 증대시키고 있지만, 디지털화가 가속화되고 있는 만큼 새로운 디지털 환경을 이용한 공격도 사회적으로 중대한 위협이 되고 있다[11, 30, 38]. 최근 가트너(Gartner)의 예측에 따르면 2025년에는 사이버 공격자가 인명피해를 일으킬 물리적인 공격력을 갖게 될 것이라고 시사했다[11, 36]. 이러한 사이버 위협들은 정보통신 기술 중심의 4차 산업화 사회가 가속화되면 될수록 우리의 삶에 높은 영향력을 끼치게 되리라는 것을 암시한다. 경제발전을 위해서라면 산업의 생산성을 극대화하는 4차 산업화를 추구하는 것은 당연하겠지만, 이로 인해 직면할 수 있는 위협을 예측하고 대비하는 능력을 갖추는 것이 4차산업의 전환 시기인 지금의 시대에 무엇보다 중요하다.

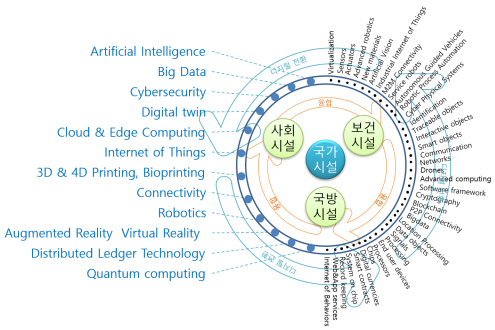
따라서, 본 논문의 구성은 다음과 같다. 2장에서는 4차 산업화 사회에서 어떠한 복합적인 위협이 나타날 수 있을지 안내하기 위해 그간의 다양한 선행 연구를 조사하여 보인다. 3장에서는 이들이 제시한 취약점과 위협 기술의 개념에 근간하여 4차 산업혁명 기술들이 국방, 사회, 보건시설들과 융합됨으로써 나타날 수도 있는 4차 산업화 사회의 복합안보 상황에서의 단위 위협시나리오를 만드는 방법을 개념적 실례로써 안내한다. 이후 4장에서는 4차 산업혁명 시대에 핵심 기술인 IoT(Internet of Things) 기반의 기술들에서 발생할 수 있는 사이버 위협 들을 어떻게 사전에 인지하고 대응할 수 있는지 선행 연구로 활용할 수 있는 모델을 제안하고, 컨텍스트 브로커(Context Broker)와 적응형 보안(Adaptive Security)기술 기반의 구축방안도 보인다.

2. 관련 연구

2.1 4차 산업혁명 관련 기술과 미래 서비스

4차 산업혁명의 기술들은 모두 디지털 관련 기술이기 때문에 3차 산업화 기술들을 디지털 전환[6] 시킴을 의미한다[29]. 다시 말하면, 4차 산업혁명 기술은 인공지능(Artificai Intelligence), 빅데이터(Big Data), 클라우드와 엣지 컴퓨팅(Cloud & Edge Computing), 사물인터넷(Internet of Things), 로보틱스(Robotics), 증강현실 & 가상현실(Argmented Reality & Virtual Reality), 분산원장 기술(Distributed Ledger Technology), 양자 컴퓨팅(Quantum computing) 기술[17, 18]들이 사회 환경에 융합되어 동작하는 사회이다.

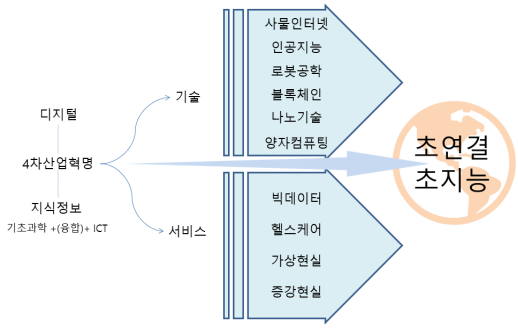
국가시설인 사회시설, 보건시설, 국방시설이 (그림 1)과 같은 4차산업 핵심 기술들과 융합하여 디지털 전



(그림 1) 4차 산업혁명의 핵심 기술 기반의 디지털 기술 융합 및 전환

환되면서 세상이 어떻게 변화될지 예측하는 노력은 중요하다. 이러한 미래 사회의 핵심 서비스를 실현하기 위해 요구되는 기초과학과 주요 ICT(Information and Communications Technology) 기반 기술들인 가상화(Virtualization), 센서(Sensors), 액츄에이터(Actuators), 고급 로봇공학(Advanced Robotics), 인공 비전(Artificial Vision), 행위 인터넷(Internet of Behaviors) 기술들의 융합으로 초연결, 초지능이 중심이 되는 지식 정보화 사회가 태생 될 수도 있다. 이 지식 정보화 사회는 국가의 기본 기능을 조력하기 위해 사회의 다양한 빅데이터(Bigdata), 헬스케어(Healthcare), 가상현실, 증강현실 등으로 스마트 수식어가 붙는 국가 전자정부, 도시, 공장, 홈 등을 견고히 하거나 이들을 위한 새로운 서비스들을 지속해서 출현시킬 것이다.

예를 들면 최근의 정보통신 기술은 자동화를 위해 사람의 인지능력을 모사하여 구현할 수 있는 인공지능 기술 등 다양한 연구를 수행하고 있다. 또한 최근 IoT 기술[15, 16] 등 4차 산업화 기술들로 사람의 시각, 청각, 미각, 후각, 촉각을 자료화할 수 있는 기반 기술들이 연구되고 있으며, 이것이 실용화되어 인간의 다섯 가지 감각의 범위에서 수집되는 데이터가 더욱 폭넓어지고 있다. 이러한 변화는 IoT 기술들로 4차 산업화 혁명 기술이 바꾸는 세상에 더 가까이 다가갈 수 있도록 하는 동력이 될 수도 있다. 즉 이러한 기술들이 사람의 인지적인 능력을 온전히 보강하도록 지속해서 발전되면 컴퓨팅 기술에 의해 수집되고 처리되는 데이터가 사회현상 등 현 세상을 디지털 세상으로 단순 예측을 넘어서 스마트하게 관리할 수 있는 수준의 국가 전자정부, 스마트 도시, 스마트 공장, 스마트 홈 등이 디지털 트윈(Digital Twin) 기반의 분석 기능이 제공되는 형태로 전환돼 있을 수 있다. 즉 디지털 트윈을 통해 사회현상을 시뮬레이션하여 위협을 초계 적으로 발견하여 제거하거나 삶의 질을 향상할 수 있는 새로운 가치를 추구하는 혁신적인 시도를 기획할 수 있는 시대가 도래될 것이다. 또한 이를 기반으로 사회적 질적 향상을 이끌 수 있도록 하는 실 세상의 구현물로 미래 사회를 위한 (그림 2)와 같은 초연결, 초지능 기반의 서비스들이 동시다발적이며 지속해서 출현 되어질 것이다.



(그림 2) 4차 산업혁명의 주요 기술 및 서비스

2.2 디지털 전환에 따른 주요 위협

최근 디지털 전환 영역에서 사이버 위협들이 빈번하게 발생하고 있다. 예를 들면 사회시설인 미국 최대송유관인 콜로니얼 파이프라인의 전산망이 사이버공격을 받았다[20]. 이 공격으로 미국의 최대송유관은 6일 동안이나 가동을 중단해야만 했다. 이외에도 2015년도에는 우크라이나 에너지 시설인 발전소에 대한 사이버테러로 대규모 정전사태가 발생하였다[7, 12]. 또한 2021년경에 미국 플로리다주의 정수 제어 시스템을 원격지에서 조정하여 수돗물을 음용하는 플로리다주의 시민들에게 악영향을 미칠 수 있는 공격도 있었다[21]. 이 사이버 공격은 미수에 그친 사건으로 피해를 초래하지는 않았지만, 사이버 위협이 국민의 건강까지 위협하는 등 그 양상이 다양해지고 있음을 시사한다. 이 사이버공격은 공격자가 정수 시스템에 무단으로 접근하고 제어권을 획득하여, 정수에 요구되는 수

산화나트륨 적정 투입 비율을 100배 이상 증가시켰던 공격이다. 다행하게도 공격 시점에 정수 시스템을 관리했던 운영자에게 공격이 발견되었으며, 이 운영자는 위협을 발견한 즉시 수산화나트륨의 투입 비율을 정상 수준으로 낮추고 사이버 공격을 받은 사실에 대해 신속하게 공지했다. 만약 이 위협이 신속하게 감지되지 못했다면 플로리다주의 시민의 건강에 심각한 위협을 끼칠 수도 있는 상황으로 전개될 수도 있었을 것이다. 또한 국내에서는 스마트 월패드(Wallpad)에 의한 사생활 침해[23]가 발생했다. 의료시설 부분에서는 2018년 워너크라이 랜섬웨어에 의한 영국 국민 건강서비스 피해[19]와 2020년에 미국과 영국에서 UHS(Universal Health Services)가 랜섬웨어 공격을 받아 관련된 의료서비스가 마비된 사태도 발생했다[30]. 이외에도 국내외 다양한 곳에서 테러가 정보통신 기술 기반으로 자행[8, 9]되는 등 정보통신 기술과 관련되거나 정보통신 기술 기반의 사이버 위협들이 지속적으로 국가안보에 위협이되고 있다.

가트너 보고에 의하면 2025년이면 사이버 공격자가 산업제어 시설을 제어 하는 등 사이버공격이 물리적인 시설을 파괴할 수 있는 공격으로 발전될 것이라고 시사하였다[11]. 예를 들어 자율주행 자동차는 연결 기반의 서비스를 제공한다. 이 디지털화된 자율주행 기능이 외부의 공격자에게 자동으로 제어될 수 있으면, 이것은 그 자체로 물리적인 파괴력을 갖는 공격무기와 다를 바가 없다. 만약에 자율주행 기능을 가지는 자동차에 운전자와 탑승자의 신원이 식별될 수 있고, 이 신원을 중심으로 식별되고 제어될 수 있는 디지털 장비들이 연결되어 있을 때, 악의적인 공격자가 운전자의 제어 권한보다 더 높은 권한을 획득하게 된다면, 이것은 운전자와 탑승자의 안전에 위협이 될 수 있다. 만약 정보통신으로 제어될 수 있는 군사용 무기가 사이버안전을 담보할 수 없다면, 이것은 아군과 적군의 정보통신 보안기술 수준에 따라서 아군의 공격무기가 사이버공격을 받아 한순간에 적군의 공격무기가 될 수 있는 위협이 있음을 시사한다[38]. 예를 들면 전투 기능이 있는 무인기 같은 경우에 공급망 공격을 받아 이 무인기가 운영체제나 관련된 제어응용에 대한 업데이트가 오용되어 공격자가 통신 프로토콜을 추출하고, 암호화 키를 유출하고, 통신 명령체계를 오용할 수 있어서 원격에서 제어할 수 있는 상황이라면 이것은 그 자체가 위협일 것이다.

2.3 4차 산업혁명 관련 위협 보안기술 연구

IoT 시스템 자체에 장애를 일으키거나 그 자체를 공격에 대응하는 연구에는 머신러닝 접근방식을 이용한 IoT 센서에 대한 공격 이상 감지 연구 등이 있다[24]. 이것은 로지스틱 회귀(Logistic Regression), 서포트 벡터 머신(Support Vector Machine), 의사결정 트리(Decision Tree), 랜덤포레스트(Random Forest), 인공신경망(Artificial Neural Network) 등 다양한 머신러닝(Machine Learning) 모델의 성능을 비교하여 IoT 시스템에 대한 이상징후를 가장 정확하게 예측하는 기술이 무엇인지 찾는 연구를 수행했다. 이 연구에서는 랜덤포레스트 방식이 가장 우수하다고 평가했다[24].

또한 소프트웨어 정의 네트워크와 퍼지 신경망을 이용하여 사물인터넷(Internet of Things)에 대한 공격 탐지를 수행한 연구들도 있다[25]. 이 연구에서는 소프트웨어 정의 네트워크(Software-Defined Network)를 이용한 IoT 공격 탐지를 제안한 것으로 SDN 컨트롤러가 분산 서비스 거부, 부채널 및 악성코드 징후 등에 대한 트래픽의 이상 흐름을 탐지하기 위한 연구를 수행했다. 이외에도 IoT 클라우드에서 공격 탐지에 대한 다중 측면 기반으로 접근하는 방식으로 네트워크 공격을 탐지하기 위한 연구가 있다. 이 연구는 클라우드 인프라 내에서 수행되는 방식으로 에이다브스트 분류기(Adaboost Classifire), 랜덤포레스트(Random Forest), 멀리노미얼엔비(MultinomialNB) 등과 같은 기계학습 방법을 이용하여 훈련모델을 구성한다. 이 공격 탐지 방식은 세션 기반, 호스트 및 트래픽 공간 등 다중영역을 기반으로 위협을 관찰하여 품질을 개선하는 노력을 수행하였다[26].

앞의 연구가 IoT 그 자체의 위협을 탐지하기 위한 연구였다면 산업제어 시스템에 대한 침입 탐

지를 위해 기계학습을 이용한 연구도 있다. 이는 산업제어시설 그 자체가 외부로부터 공격을 받고 있음에 집중한다. 여기서는 기계학습 알고리즘에 기반을 두어 스마트 시티나 공장에서 기계학습을 사용하여 공격을 탐지하기 위한 연구를 수행했다[27]. 또한 산업용 제어 시스템에 대한 잠재적인 공격을 탐지하기 위한 침입 탐지 시스템을 검토하고, 다양한 산업제어 시설에 대한 각 프로세스에 대한 제어 체계를 자동으로 학습할 수 있는 연구를 수행한 연구 사례[28]들도 있다.

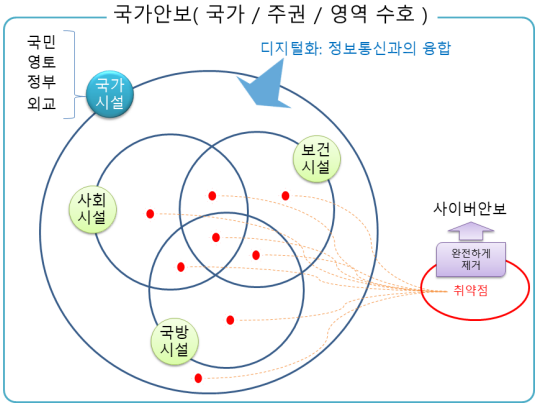
3. 4차 산업혁명 시대의 사이버 위협

3.1 국가시설의 사이버안보 관련 영역

4차 산업혁명 기술에 의한 디지털 전환으로 사이버 위협에 영향을 받을 수 있는 영역은 국가안보 영역이다. 왜냐하면 국가안보란 국가의 안녕과 주권 보장, 국가 영역을 안전하게 수호하는 것이며 이를 위해 국가는 국민과 영토, 정부, 외교와 관련된 다양한 시설들을 유지하는데 이 시설들의 대부분은 정보통신 기술과 연관되어 있다.

여기서 이 시설들은 국가의 중심인 국민이 사회에 참여하여 그들의 생활을 영위하는 데 필요하도록 갖추어진 다양한 시설들이기 때문에, 국가시설들을 통칭하여 국가의 사회 구성원의 시설을 의미하는 사회시설로 표현할 수 있다. 왜냐하면 사회란 동일한 정치와 문화를 갖는 동일한 공간을 이르기 때문에, 국가 사회에 참여하는 주체는 국민이고 이들 국민이 국가에 속하는 다양한 활동들을 사회활동으로 통칭할 수 있다[34]. 부연하면 사회기반시설은 사회기반시설에 대한 민간투자법 등에서도 정의[31]하고 있는데, 사회기반시설은 사회의 각종 생산활동의 기반이 되는 시설이나 국민 생활의 편익을 증진하게 시키는 시설을 의미한다. 이 시설들은 경제 활동의 기반이 되는 산업시설, 사회서비스 제공을 위해 필요한 시설, 국가 또는 지방자치단체 업무수행을 위하여 필요한 공용 시설들이다. 이러한 의미에서 보건시설도 사회적 시설의 범주 안에 포함될 수 있다.

본고는 (그림 3)과 같이 사회활동을 영위하는 시설에서 보건시설과 국방시설을 따로 분리하여 보건시설과 국방시설이 아닌 이외에 산업기반 시설들을 사회시설로 한정하여 정의한다. 예를 들어 금융이나 교육이나, 공장 등은 사회시설 범주 안에 포함한다. 금융이나 교육, 공장 등을 새로운 영역으로 분할하여 정의할 수도 있겠으나 최근 4차 산업화의 핵심 기술인 디지털 기술로의 전환으로 국민의 생명과 삶의 안위에 영향을 줄 가능성이 큰 위협들인 보건시설과 국방시설을 구분하여 정의한다.



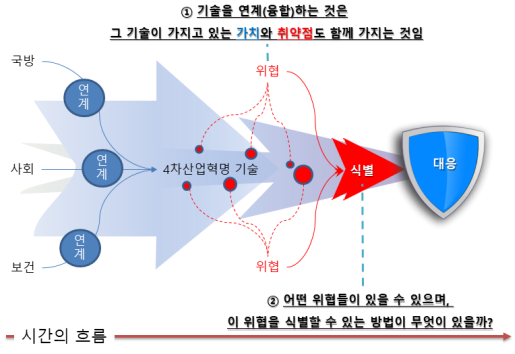
(그림 3) 국가안보의 사회, 보건, 국방시설영역에서 사이버안보 취약점 형태

결국 국가의 국민을 위한 사회시설이기 때문에 서비스의 편의를 위해 이들 간에는 연관 관계가 있을 수 있으며, 국민 개인이 갖는 역할 범위 중심으로 사회, 보건, 국방시설 등 다수의 기능이 단일하게 하나로도 묶일 수 있다. 예를 들면 금융 서비스에 대한 신용평가[4]를 위해서 건강보험 등 보건시설에 정보를 이용할 수 있으며, 국방시설에 접근하기 전에 이용자의 신분을 확인하기 위해 현재 접근하려는 주체에 대한 정확성을 식별하기 위해 접근자의 위치정보를 기반으로 국방시설 이외에 다른 시설을 이용하고 있는지 추적해야 할 필요가 있을 수도 있다. 이러한 부분 이외에도 사회시설과 보건시설, 국방시설들 사이에서는 복지 등을 위해서 다양한 서비스가 상호 간에 연관처리를 위해 연결 접점이 만들어질 수 있다. 예를 들어 국방시설과 보건시설이 연계될 수 있는 서비스 중 하나는 주요 임무 실행에 대한 현시점에 최적의 주체를 선택하기 위해서 최근의 보건 기록을 통한 건강정보와 금융 기반 신용정보, 교통정보 등 사회 기반 정보로 신변 변화 등 특이 징후를 감별하기 위한 서비스가 요구

될 수 있다. 이경우는 주요 임무에 대한 실행이 개인의 사생활보다 우선시 되는 경우로 한정된다. 따라서 이러한 경우에 국방시설 서비스와 보건시설 서비스 간에 상호 정보 데이터를 교환하기 위해 정보통신 기반 기술로 상호 간에 연결 접점이 생길 수도 있다. 이러한 서비스는 디지털 중심의 사회에서 사이버 위협의 공격이 날로 고도화될 수 있으므로 이러한 상황에서 안전함을 보장하기 위해서 개인을 식별하는 보안 강도가 현재보다는 더 강화될 수 있어서 나타날 수 있는 변화들이다. 또한 다양한 산업 기반 시설이 지속적으로 자동화에 의존할 수 있는 상황으로 전개될 수 있음에 기인한다.

3.2 4차 산업혁명 시대의 사이버 영역의 취약점, 공격, 방어대책

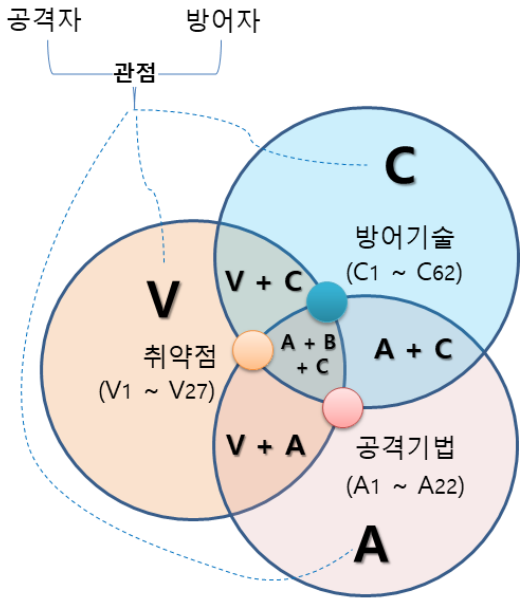
4차 산업혁명 시대는 4차 산업화의 기술들인 디지털 기술로 확장되었을 때 4차산업의 기술들이 갖는 장점인 정보통신 기술의 연결성, 편리성 등 핵심 가치를 갖는 동시에 취약점도 함께 가지게 된다. 따라서 4차 산업화 기술들로 융합되어 새롭게 확장되어 나타나는 서비스들에는 정보통신 기술의 다양한 취약점으로 인한 피해[32, 10]들이 나타날 수 있기에 4차산업으로 전환으로 어떤 위협들이 있을 수 있으며, 이 위협을 탐지하기 위해 각 위협을 식별하여 대응하는 방법에 관한 선행적인 연구와 기반 기술들이 요구된다.



(그림 4) 4차 산업혁명 시대의 사이버 위협 식별과 대응에 대한 함의

예를 들면 '22년 4월 폰투온(Pwn2Own) 해킹대회에서도 네델란드 출신의 해킹기술 연구원이 4차 산업화 기술의 범주로 포함할 수 있는 세계 전력망과 가스관들을 제어하는 소프트웨어의 해킹 시연에 성공하였다[10]. 이러한 상황이 단순 해킹 시연이 아니고 실제 상황이라면 이로 인한 피해는 막대했을 것이다. 이렇듯 4차 산업화가 다양한 사이버 위협 들을 발생시킬 수도 있기에 (그림 4)와 같이 4차 산업혁명 기술로 연계될 때 어떤 위협들이 있을 수 있는지 인식하는 것이 중요하며, 이러한 위협을 식별하여 대응하는 방법에 관한 연구가 필요하다.

이를 위해 산업제어 시스템인 C3I(Command, Control, Communication and Intelligence) 시스템에서 취약점, 공격, 방어대책 연구[32]를 참고한다. 이 연구에서는 취약점의 유형을 모두 27개, 공격기법을 22개, 방어대책인 방어 기술을 62개로 축약했다. 본고는 이 논문에서 정리한 V, C, A의 개념적 정의를 그대로 사용한다. 단, 4차 산업혁명의 보안 시나리오와 선제적 위협 대응 모델 제안을 위해서 (그림 5)와 같은 개념을 포함하여 제안한다.



(그림 5) 공격자와 방어자 관점에서 공격벡터 정의

(그림 5)에서 취약점은 V(Vulnerabilities), 공격기법은 A(Attacks), 방어 기술은 C(Countermeasures)로 표기한다. 이 기술들을 습득하고 활용하는 공격

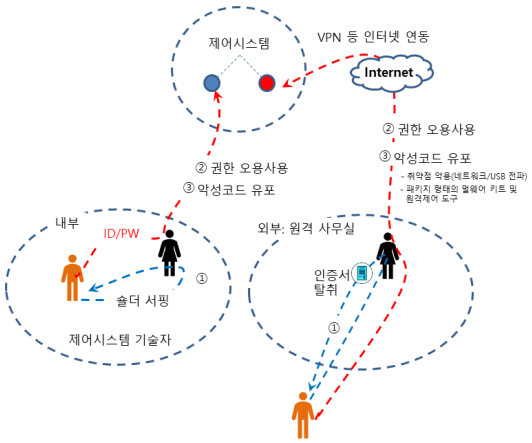
자와 방어자 관점이 존재한다. 공격자 관점에서 V는 공격자가 공격을 수행하기 위해 대상 시스템, 네트워크와 관련된 응용에 대한 취약점을 획득하였음을 의미한다. 또한 A는 공격자가 가지고 있는 공격기법을 의미하며, C는 공격기법을 수행하기 위해 보안장비에서 탐지되거나 방어되지 않도록 우회할 수 있는 방어기술들이 이용될 수 있음을 의미한다.

C는 공격자로서 공격자가 공격하는 데 있어서, 방해 요인에 대한 면밀한 분석을 위해 요구되는 방어 기술에 대한 상세한 기술들을 통칭한다. 다른 측면으로는 방어자 관점이 있다. 방어자 관점에서 V는 대상 시스템이나 네트워크나 관련된 응용에서의 취약점을 의미하며 이 취약점들은 긴급하게 조치하거나 보안 장비로 위협사항이 발생하여도 피해가 발생하지 않도록 안전조치를 수행해야 할 사항이다. 또한 A는 방어자 관점에서 이미 알고 있는 공격기법으로 시스템, 네트워크, 엔드포인트(Endpoint) 보안장비에서 실시간 안전하게 대응할 수 있도록 준비해야 할 공격 기법이다 [33]. 이외에도 알려진 공격법임에도 불구하고, 방어대책이 마련될 수 없는 상황이라면 공격자 관점에서 이러한 공격행위가 발생하면 방어자 관점에서 공격단계의 흐름에 따라 단계적으로 피해를 최소화할 수 있는 전략도 준비될 필요가 있다. 끝으로 C는 공격자를 방어하기 위해 방어자가 이용할 수 있는 기술들이다.

3.3 복합안보 위협 시나리오

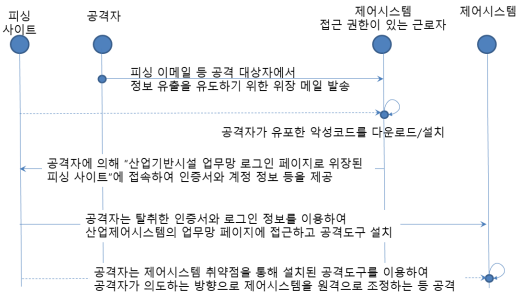
3.2에서 정의한 V에 대한 A 기술을 이용하여 4차 산업화 기술로 융합된 서비스들에 다양한 사이버 공격 위협들이 발생될 수 있다. 이러한 공격 들에서 복합안보 상황이란 공격에 따른 피해 위협들이 중첩되어 있어 복합적으로 안보를 수행할 상황임을 의미한다. 이 상황은 위협에 대한 공격을 받아 피해가 발생했음에도 보안관리자와 보안시스템이 관련된 위협을 탐지하지 못한 상황일 수 있다.

(그림 6)과 (그림 7)은 복합안보 위협 중에 단위 위협으로 산업기반 제어 시스템에 어떻게 침투할 수 있는지 보인다. (그림 6)은 산업기반시설 관련 인증정보 탈취를 위한 사이버공격에 대한 주요한 두 가지 유형을 나타낸다. (그림 6)에서 내부 영역에 해당하는 것은 산업 제어 시스템에 접근할 수 있는 경우가 내부망을 통해 접근할 수 있는 경우인 내부 공격자에 의한 접근이다. 이는 내부망에서 내부자 중에 제어 시스템 접근 등의 이용 권한이 있는 담당자에게 공격자가 의도적으로 접근하여 어깨너머로 ID와 패스워드를 탈취하고, 이렇게 탈취한 ID와 패스워드를 무단으로 사용하여 산업기반시설에 접근함으로써 발생할 수 있는 위협 경로이다. 또 다른 유형은 (그림 6)은 내부망이 아닌 외부의 인터넷망을 통해 접근하는 경우로 내부자가 아닌 외부자에 의한 접근으로 외부의 원격 사무실 등을 통해 내부의 제어 시스템에 접근하는 것이다. 이것은 원격 사무실 등 외부 인터넷망에서 VPN을 통해 제어 시스템과 연결될 수 있도록 하여 업무망에 접근하려는 사용자를 노리는 공격이다.



(그림 6) 산업기반시설 관련 인증정보 탈취를 위한 사이버 공격 주요 유형

이 공격은 제어 시스템에 접근할 수 있는 인증서와 비밀번호를 탈취하기 위해서 원격 사무실 등 외부 인터넷망 접근을 위해 사용하는 개별 PC에 무단으로 침투하여 제어권을 획득하기 위해 (그림 7)과 같은 단계로 공격을 수행한다. 따라서 (그림 7)에서 도시된 바와 같이 시스템에 접근할 수 있도록 권한을 획득하는 데에는 최신의 신변종 악성코드 등이 이용될 수 있다. 공격자는 내부 업무망보다 상대적으로 취약할 수 있는 보안 환경일 수밖에 없는 외부의 원격 사무실 등으로부터 VPN 접근을 하는 사용자의 행위에 악의적으로 개입하여 제어시스템에 침투할 수 있는 시나리오이다.



(그림 7) 산업기반 시설 관련 사이버공격 흐름

또한 공격자는 제어 시스템에 접근하기 위해서 온라인으로 연결된 망뿐만 아니라 USB 등으로 악성코드가 전파될 수 있는 기술들도 이용될 수 있다. 이외에도 산업 제어시설의 물리적인 공간에 침투하고 물리적인 시스템에 스파이 칩과 같은 기능을 할 수 있는 형태의 네트워크 장치 등의 미디어를 설치하여 외부의 원격지에서 오용 사용하는 시도 등의 위협사례들도 존재할 수 있다.

4차 산업화로 전환된 환경에서는 이러한 공격들이 복합적으로 나타날 수 있는데 이들 유형의 단위 위협은 다음과 같다.

단위 위협 ①: 공격자가 댐 수문 조절을 공격자가 의도하여 강우량이 급속하게 늘어나는 시즌에 홍수나 강우량이 극히 적은 시즌에 가뭄을 발생시킬 수 있도록 조정 되어질 수 있다.

이 산업제어 시스템에 대한 모니터링 기능은 평시와 다를 바 없이 정상적으로 수문 조절이 운영되고 있는 것처럼 모니터링되는 데이터가 의도적으로 조작되어 질 수 있다.

단위 위협 ②: 교통정보 시스템은 의도적인 교통 교란 상황을 일으켜서 자동차 간 추돌을 의도적으로 일으킬 환경을 만들어 내고, 이에 더하여 자율주행 기능의 자동차이면서 원격 제어 시스템에 운영 SW가 업데이트되는 자율주행 자동차의 공급망이 탈취되어 자율주행 시스템의 주요 소프트웨어가 의도적으로 조작되어 정상적인 자율주행 기능이 아닌 공격자에 의해 의도된 위협을 가할 수 있는 상황들이 전개될 수 있다. 또한 이들 행위가 예측할 수 없는 단위 사고처럼 위장되어 불특정하게 발생하여 위협으로 간주하지 않을 수 있도록 위협이 간헐적으로 발생할 수 있다.

단위 위협 ③: 블록체인 기반의 개인 지불 결재 시스템에 대한 응용 기능에 대한 취약점이 발견되어, 이 취약점을 이용하여 전자지갑의 고유 기능이 악성코드에 의해 탈취되어 개인 신원정보가 도용되고, 금융기능이 탈취되는 상황 등도 여러 영역에 흩어져 있는 소규모 특정인들에게 피해 사실을 인지할 수 없도록 조작된 피해가 연일 계속될 수 있다. 이 위협의 핵심은 지갑 소유자가 거래 내역 외에는 잔고가 전혀 이상 없는 것처럼 보이게 조작될 수 있다. 이러한 상황이 가능할 수 있는 해킹기법 상황은 지갑 소유자에게 해커가 의도적으로 전환한 가상의 지갑을 보여주고, 백그라운드 프로세스(Background Process)로 동작하는 해커의 명령·제어(Command and Control)에 의해 오용 조작되고 있는 실제의 지갑이 있을 수 있다. 보이는 잔고는 해커에 의해 의도적으로 조작된 것이며, 실재의 잔고 보다 큰 거래가 아닌 동안에는 전자지갑 소유자는 피해 사실을 인지할 수 없도록 공격자들은 공격행위를 은닉할 수 있다.

단위 위협 ④: 국방망의 AI 기반의 아군 편대가 순식간에 적군의 편대로 탈바꿈될 수도 있다. 이러한 위협시나리오는 운영체제와 보안 업데이트, 관련 서비스에 대한 응용 소프트웨어들의 업데이트를 위한 패치 관리 시스템 등 응용취약점 제거를 관장하는 공급망을 공격자의 의도대로 소프트웨어가 업데이트됨으로써 운영 제어권이 넘어갈 수 있을 수도 있음을 의미한다. 이러한 상황은 최악의 상황으로 관련된 운영체제와 응용에 대한 전 공급망 영역에 대한 관리 권한을 탈취할 수 있고, 공격행위가 은닉되면서 원격으로 명령으로 전달하여 조정할 수 있으며, 공격이 성공할 수 있는 취약점들을 가지고 있는 경우여야만 가능하다. 또한 이러한 위협과 관련된 피해 상황이 발생하기 이전에는 전혀 위협을 감지할 수 없는 상황일 수 있다. 공격자는 평시에는 온전하게 정상 동작하도록 하면서도, 공격자의 의도대로 피해를 일으킬 수 있는 상황이 만들어질 수도 있다.

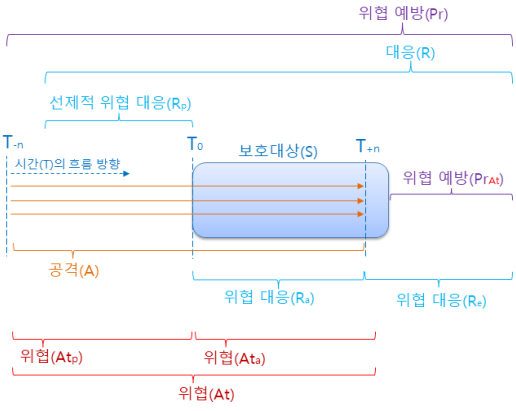
앞에서 정의한 단위 위협 ①에서 ④까지의 단위 위

협시나리오들은 고도의 해킹기법과, 관련 운영체제(Operating System)와 제어 시스템(Control System) 응용에 대한 심각한 결함을 갖는 취약점을 기반으로 공격자의 기능으로 위변조할 수 있는 고도의 전술과 기법이 선행되어야만 관련 피해가 나타날 수 있다. 즉, 공급망이 내부의 보안체계에 탐지되지 않으면서 오용 조정될 수 있는 환경에 노출될 수 있어야 하며, 또한 각 인증 체계, 인가 체계가 공격자에 의해 무력화될 수 있는 다양한 선제 조건들이 요구된다. 예를 들면 소프트웨어 관리 공급망에 취약한 결함이 발생하여 운영체제 등 제어 시스템이나 관련 서비스 소프트웨어를 개발하는 개발사와 이들의 업데이트를 네트워크 의존적으로 수행하는 체계가 신뢰 될 수 없는 상황이 만들어질 경우에 발생할 수 있는 최악의 위협 상황이다. 최근 솔라윈즈(SolarWinds) 공급망 위협사례를 보안전문가들이 두려워하는 이유 중 하나가 바로 이것이다[22].

4. 선제적 위협 대응

4.1 선제적 위협 대응 모델

4차 산업혁명 시대의 선제적 위협 대응 모델을 보이기 전에 사이버공격에 따른 선제적 위협 대응은 (그림 8)과 같이 정의될 수 있다.



(그림 8) 사이버 위협 방어에서 선제적 위협 대응

선제적 위협 대응이란 (그림 8)에서 공격(A)이 보호대상(S)에 영향을 미치기 이전에 방어를 취하는 것을 선제적 위협 대응(Rp)으로 볼 수 있다. 위협 예방(Pr)은 선제적 위협 대응(Rp)을 포함한 대응(R) 영역보다 넓은 범위를 갖는다. 특정 공격 즉 공격(A)과 공격이 발생한 시간(t)를 고려한 사후 대응적인 측면에서 재발 방지를 의미하는 위협예방(PrAt)은 최근 산업기반시설 등 디지털화로 인해 사이버공격에 악용[13]될 수 있는 다양한 취약점이 지속적으로 출현하고 있어서 복합안보 위협 대응에서 집중해야 할 영역이다.

위협(At)은 보호 대상(S)에 접근하는 등 직접적인 영향을 주기 이전의 위협(Atp)과 공격 대상인 보호대상에 직접적인 영향을 줄 수 있는 위협(Ata)이 있다. 대응은 앞서 언급한 선제적 위협 대응(Rp)과 보호대상에 접근할 때 IPS(Intrusion Prevention System)와 IDS(Intrusion Detection System)에 의한 실질적인 방어 영역인 위협대응(Ra)과 실시간 위협을 감지하여 초동대응 단계로 최대한 신속하게 위협에 대한 방어체계를 세우는 것을 의미하는 것이 위협대응(Re) 이다.

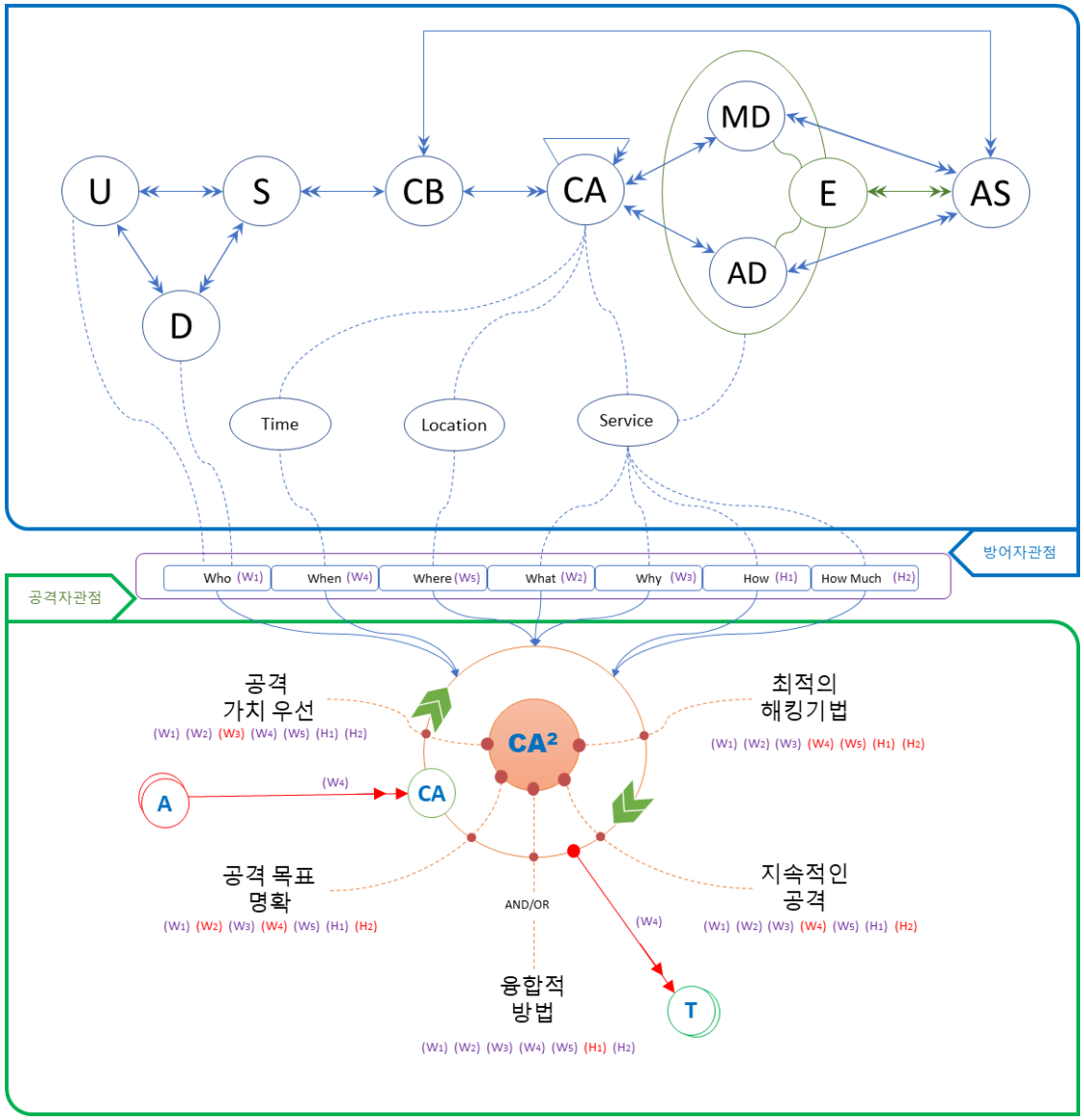
제안하는 4차 산업혁명 시대에 선제적 위협 대응 모델은 (그림 9)와 같다. (그림 9)의 각 구성요소는 <표 1>과 같다.

<표 1> 선제적 위협 대응 모델 구성요소

구성 요소	정의
U (Users)	U는 미래의 4차산업의 미래화된 삶을 살아가는 사용자들의 집합이다. U = {u1, u2, u3, ⋯ ⋯, uN} ※ N은 각 사용자를 고유하게 식별할 수 있는 1부터 순차적으로 증가하는 정수이며 D에서도 동일한 의미로 이용된다.
D (Devices)	D는 U가 이용하는 하드웨어나 소프트웨어 장치들로써 구성된 생산품들이다. 예를 들어 휴대폰, 자동차의 자율주행 장치, 산업제어 시스템의 로봇, 식당의 주문형 로봇, 스마트폰 등도 이들에 해당된다. 또한 클라우드 기반으로 장치들이 SW일 수도 있다. 스마트폰 등의 일반적인 장치외에 디지털 기술 기반으로 특정인을 식별할 수 있는 RFID 등의 뱃지 등을 착용하고 있을 경우에도 이들 식별자들의 행위를 감시하기 위해

	센서가 동작할 수 있다. 또한 최근 가상화되고 있는 메타버스 환경에서도 가상 세계의 메타와 소프트웨어 세계를 포함하는 현 세상의 유니버스를 통합할 수 있게 하도록 D가 U의 UI(User Interface)와 상호작용해서 움직이는 메타버스의 아바타를 관찰하기 위해 이용되는 소프트웨어 유형의 디바이스도 있을 수 있다. D = {d1, d2, u3, ⋯ ⋯, dN}
S (Sensors)	S는 실생활에 모든 부분에서 각 센서의 기능을 수행하여 U, D를 관찰하여 데이터를 생성하고 CB에 전달하는 센서들의 집합이다.
CB (Context Broker)	이기종의 다양한 S에서 보내져 오는 데이터를 일괄로 수집하고 각 데이터가 요구되는 곳에 보내는 브로커 역할을 수행한다. 제안된 모델에서 CB는 동일 프로토콜 내에 있는 도메인 간에 유효하다. 경우에 따라서 이들 간에는 포함관계와 계층적인 구조도 있을 수 있으나, 본 고는 동종의 프로토콜을 이용하는 관계된 구성 요소간 도메인 간에 계층관계가 존재하지 않고 상호 연관 처리가 가능한 범주의 단일 도메인 영역으로 한정하여 제안한다.
CA (Context Aware)	CA는 발생시간(Time = {t1, t2, t3, ⋯ ⋯, tn}), 발생한 위치에 관한정보(Location = {l1, l2, l3, ⋯ ⋯, lk}), 센서가 센싱(Sensing)을 요청한 서비스 수행 주체(Service = {s1, s2, s3, ⋯ ⋯, sj})에 대한 식별정보 쌍으로 생성된다. 여기서 n, k, j는 각각 다른 식별 공간을 가지는 정수이며, 이 정수는 개별의 발생시간, 위치정보, 서비스를 고유하게 식별하기 위한 식별 번호이다. 관리의 용이성을 위해 CA는 Tn × Lk × Sj 쌍으로 표현되며 발생시간, 발생한 위치에 관한 정보, 센서가 센싱을 요청한 서비스 수행 주체들의 식별자 간에는 계층적인 포함관계를 가질 수 있다.
MD (Misuse Detection)	MD 방식은 이미 알려진 위협을 규칙 기반으로 탐지하는 모델에서 각 구간별로 위협의 규칙을 정의하고, 일치할 때에 경보를 보내 위협을 탐지 및 차단하는 형태로 동작한다. MD는 사이버 공격 행위로 이미 알려진 위협들인 단위 위협의 집합으로 정의된다. 이 기능은 공격으로 알려진 단위 행위들로 시나리오 공격을 이루는 단위 공격 유형들로 (그림 5)의 A1부터 A22인 각 개별 단위 요소들로 이루어진다. MD = {A1, A2, A3, ⋯ ⋯, A22} 이들 A1은 동일유형 범주에 속하는 공격으로 공격의 주체, 공격에 이용된 상세코드 등 세부의 공격 기법이 달라지면 서로 다른 공격이 될 수 있다. 따라서 공격 A1은 다음과 같이 나타내질 수 있다. A1 = {A1(1), A1(2), A1(3) ⋯ ⋯, A1(i)} 이외 A2에서 A22도 각 단위 공격 유형들로 A1처럼 서로 다른 공격 유형별로 서로 다른 서브 셋을 가지고 있다.
AD (Anomaly Detection)	AD는 정상행위 이외의 행위를 탐지할 수 있는 경우를 의미하는 경우로 정상행위에 어긋날 수 있는 사기 탐지 등의 유형일 수 있는 것에 대한 집합이다.
AS (Adaptive Security)	AS는 적응형 보안기술 기반의 모듈이며 CB에서 MD와는 전혀 관련되지 않고 AD 영역에서 불분명한 이상치를 분석모듈(Analyzer)이 받아서 이를 탐지할 수 있는 적절한 MD 또는 AD 기반의 정책 규칙으로 정의하는 기능인 E를 수행한다.
E (Effect)	AS가 보내져 오는 MD 또는 AD 기반의 정책을 ODRL[14] 기반으로 규칙으로 정의하는 기능을 수행한다.

(그림 9)에서 상단을 의미하는 방어자 관점과 하단을 의미하는 공격자 관점으로 기능이 나뉜다. 방어자 관점은 사이버 위협을 정의하기 위해 요구되는 각 구성 요소의 구조를 보인다. U와 D의 관계는 1:N관계



(그림 9) 공격자 관점 방어자 관점 기반의 4차 산업혁명 시대의 선제적 위협 대응 모델

로서 U는 하나 이상의 D를 가질 수 있다. S는 다양한 U와 다수의 D를 다양하게 관찰할 수 있도록 요구되는 센서들로 하나 이상의 센서들을 가진다. 센서들은 통합되고 일관된 CB에 연결된다. CB는 대응 모델이 수용할 수 있는 영역이다. 이 CB는 시간(Time), 위치(Location), 서비스(Service)의 한정 자로 운영되는 하나 이상의 CA에게 연결된다. 이 CA는 시간, 위치, 서비스들로 각 영역 공간에 포함관계로 이들 포함관계에 의해서 계층관계를 가진다. CA는 MD와 AD와 N:N 관계인 하나 이상의 CA는 하나 이상의 MD와 하나 이상의 AD와 상호 연관을 갖는다. MD와 AD는 E에 의해 새로운 기능이 추가되거나 삭제되거나 조정되는 등 조작되는데 이를 수행하는 주체는 AS이다. AS는 하나 이상의 MD와 하나 이상의 SA와 연결성을 갖는 AS가 있다. AS는 AD에서의 정상행위를 제외한 이상 행위의 부분을 (그림 9)와 같이 적응적으로

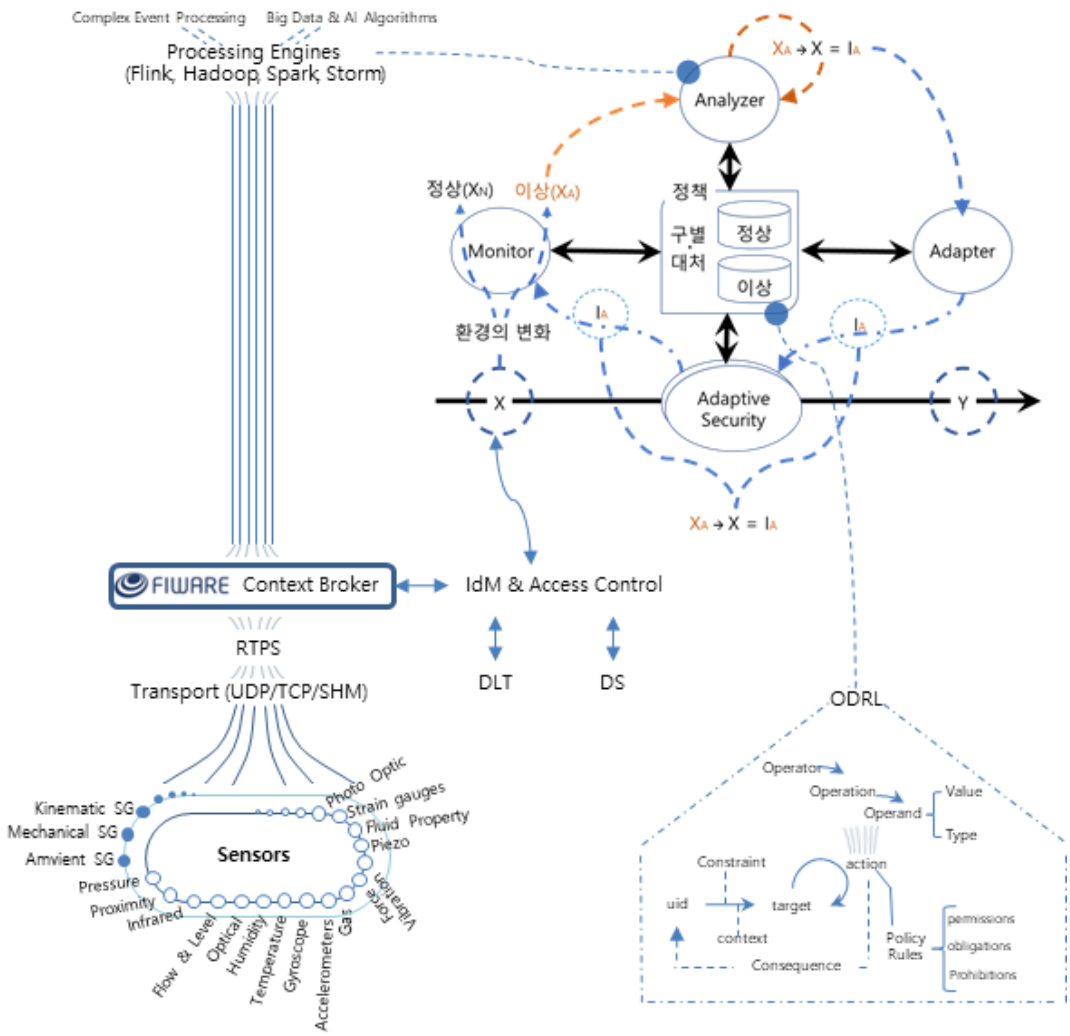
분석한다. 이때 이상 행위 부분이 공격인지, 아니면 정상 행위를 의미하는 사전에 정의된 ODRL(Open Digital Rights Language)[14]에 기반하여 위협을 판단할 수 있는 MD와 AD를 E로 업데이트하는 모델이다. 이 ODRL의 각 정책은 하단의 공격자 관점에서의 위협시나리오를 기반으로 발생할 수 있는 행위에 대해 이들 행위가 정상행위인지 관리 감독할 수 있는 방어자 관점의 모델에서 정상행위와 공격행위를 판단할 수 있도록 생성된 정책이다. 현재 모델은 현 상황에서 위협을 감별할 수 있는 정책 생성에는 전문가가 개입하여 ODRL[14]을 정의하도록 설계되었다.

공격자 관점은 (그림 9)에서 하단으로 현재의 공격(CA2: Current Attack Activity)은 공격자(A: Attackers)가 공격 목표 대상(T: Attack Target)에 현 공격 시점에 대한 상황인지(CA: Context Aware)를 기반으로 공격 가치 우선(핵심 인자: W3), 공격 목표 명확화(핵심 인자: W2, V4, H2), 최적의 해킹기법(핵심 인자: W4, W5, H1, H2), 지속적인 공격(핵심 인자: W4, H2)이 유·무형의 융합적 방법(핵심 인자: H1)으로 혼합(AND/OR)된 형태로 나타난다. 최근 공격자는 날로 고도화 지능화 되었는데 이들 공격은 공격자 관점의 각 요소에 의해 정의될 수 있다.

4.2 선제적 위협 대응 모델 구축방안

4차 산업혁명 시대의 선제적 위협 대응을 위해 FIWARE 컨텍스트 브로커(Context Broker)[14, 35]를 활용하여 (그림 10)과 같은 구성적 환경으로 제안된다. (그림 10)에서의 다양한 센서들(Sensors)로부터 UDP(User Datagram Protocol), TCP(Transmission Control Protocol), SHM(Shared Memory)으로 센싱된 데이터를 받을 때 산업 자동화를 위해 RTPS(Real Time Publish Subscribe)가 이용된다. RTPS를 통해 FIWARE 컨텍스트 브로커에 전달된 센서로부터 센싱된 데이터는 분산형 빅데이터 분석을 위한 오픈 플랫폼(Fink, Hadoop, Spark, Storm)에서 센서로부터 올라온 센싱 데이터에 대한 복잡한 이벤트 처리(Complex Event Processing)를 위해 빅데이터와 AI 알고리즘(Big Data & AI Algorithms) 등이 이용된다. 신원 관리와 접근 통제(IdM & Access Control)는 사용자가 허가받은 접근 권한 동안만 FIWARE 컨텍스트 브로커에 접근하여 센싱된 데이터를 가져올 수 있도록 통제한다. 이때 센싱된 데이터는 선제적인 위협 대응을 위해서 새로운 변화된 영역을 지속적으로 추출하고 대응하여야 한다. 본고는 적응형 보안기법을 활용하여 센싱된 데이터로부터 전달된 데이터에서 (그림 9)의 CA동안 유효한지 정상행위와 이상 행위를 구분하는 역할을 수행한다. 정상(X_N)은 정책 범위 내에서 처리가 가능한 경우를 의미하지만 이상(X_A)은 기존까지 알려진 유형이 아니기 때문에 처리할 수 없는 영역으로 처리할 수 있는 규칙에 대한 정의가 필요한 부분이다. 간단히 예를 들면 사무공간이 있을 때 A가 오후 2시에 사무공간의 특정 영역인 B 공간에 특정 서비스를 수행하는 센서에 감지가 되었을 때 이렇게 생성된 이벤트가 정당한 경우는 정상 이벤트로 분류되며, 미리 정의되지 않아 처리될 수 없는 이벤트는 이상(X_A)으로 분류한다. 모든 경우의 수를 모두 고려하여 미리 정의할 수 있도록 하는 것은 IoT 기반의 미래 상황인 4차산업 복합안보 상황에서는 더 어려울 수 있다. 최근 우리는 다양한 센싱 정보를 처리하는 데 있어서 센서로부터 데이터를 온전히 처리하지는 못하고 있다. 이러한 경우에는 선제적으로 특정의 센싱된 상황에 대처할 수 없게 되는 것이기 때문에 이로 인해 예기치 못한 위협이 발생하면 이를 탐지하거나 차단할 수 없다. 본고는 이러한 문제를 막기 위해 4차산업 복합안보 상황에서 선제적인 위협 대응이 될 수 있도록 최종단의 센서로부터 센싱되어 생성되는 데이터를 적응형 기법으로 처리될 수 있는 환경을 제공한다. 현실 세상은 다양하고 사용자가 4차산업 복합안보 상황에서 다양한 행위들이 센싱될 것이며 이 센싱된 상황이 (그림 9)의 CA동안 허가받은 정상인 경우일 수도 있다.

예를 들어 3.2에서 언급한 4차 산업혁명 시대의 복합안보 위협시나리오에서 단위 위협시나리오 ①번으로 정의한 공격자가 댐수문 조절을 공격자가 의도하여 강우량이 급속하게 늘어나는 시즌에 홍수 피해를 의도적으로 일으키고, 강우량이 극히 적은 시즌에는 가뭄을 발생시킬 수 있도록 조정될 수 있다. 이러한 산업제어 시스템을 침투하는 기본 경로는 3.2절에서 언급한 (그림 6)과 (그림 7)이 이용될 수 있다. 댐에 강우량을 조정하기 위해서 수력발전장치의 유량 측정



(그림 10) FIWARE Context Broker와 ODRL을 활용한 적응형 모델 구축방안

센서, 고온 음파 방사 센서, 고온 가속도계, 압전 저항 압력 트랜스미터 등 다양한 센서들이 이용될 수 있다. 이들 센서는 유량과 유속을 측정하여 댐의 강우량을 조정하는 데 이용된다. 공격자는 제어 시스템을 조정해서 센서로부터 받은 센싱된 데이터 결괏값을 위조하여 댐을 오용 조정하여 수문을 올려서 물을 방출하여 홍수나 가뭄을 일으킬 수 있다. 이러한 상황에서 제어 시스템에서 진행된 결과와 센서에서 반환되는 측정치가 서로 다른 이상치가 존재함으로써 (그림 9)와 (그림 10)에서 보인 선제적 위협 대응 모델은 (그림 9)의 CB(FIWARE Context Broker)의 (그림 10)의 분석자(Analyzer)에서 경보를 반환하며 어댑터(Adapter)가 수문 관리자에게 통보하는 등 응급조치를 수행한다. 이 어댑터는 정책이 신규로 생성되고 업데이트되어, 다음부터는 센서의 행위가 이상치로 분기되지 않고 이 정책에 의해서 관리자에게 제어 시스템이 공격받아 오동작하고 있음을 통보하고 차단 대응 등의 응급조치를 수행하는 등 정상적인 행위 단계로 처리를 수행한다. 앞의 사례는 (그림 10)의 ODRL 정책으로 포함되어 있지 않았을 때 이상치로 구분될 수 있음을 보인 사례이며, 이러한 신규 사례들이 지속 누적되어 정책 기반의 선제적인 위협 처리가 가능할 수 있

도록 유도하는, 센서 기반 센싱에 대한 가시성을 적응형으로 강화하는 모델이다.

5. 결 론

본고는 현재의 사이버 위협 상황과 미래의 상황인 4차 산업혁명 기술을 기반으로 미래에서 발생할 수 있는 복합안보 위협을 연구하였다. 이를 위해 복합안보 상황에서 발생 가능 한 시나리오와 4차 산업혁명 시대의 IoT 기술을 기반으로 위협에 대한 가시성을 보조하여 위협에 대응하는 선제적 위협 대응 모델과 모델 구현을 위해 FIWARE Context Broker를 활용할 방안도 제시했다.

이들은 온전한 것은 아니지만, 이러한 노력 들은 앞으로도 다양하게 이뤄져야 할 것이며 이들의 노력은 미래의 위협을 쉽게 인식하게 할 것이다. 따라서 본 연구는 미래의 위협에 대해 선제적으로 대응하는데 필요한 선행연구자료로도 이용될 수 있을 것이다.

본고의 향후 연구로 사회시설, 보건시설, 국방시설에 대한 구체적인 활용 가능한 사례연구를 통해 가시적인 구현물이 나올 수 있도록 보강하여 4차 산업혁명 시대의 선제적 위협 대응 모델을 초월하는 차세대 위협 대응 모델로 발전시킬 예정이다. 이를 위해서는 (그림 9)의 CB로부터 IoT 센서들로부터 오는 데이터에서 비정상 행위를 구분하는 영역을 인공지능 기술을 이용하도록 발전시킬 예정이다. 예를 들면 (그림 9)의 S가 (그림 9)의 CB로 보내오는 각 센싱 된 데이터를 (그림 9)의 CA별로 자동으로 분류하는데 순환신경망(Recurrent Neural Network) 기반의 학습과 각 영역에 대한 분류를 위해 (그림 9)의 CB가 보내는 각 센싱된 데이터를 이미지화 하여 이들간의 상관관계에서 그간의 센싱된 데이터에서 위협을 CNN(Convolutional Neural Network)으로 학습시키는 등 이 위협의 특성과 연관 관계를 추출하는데 CNN을 이용하고, 이들에서 새로운 규칙을 모델링하고 생성하는데 GAN(Generative Adversarial Network)이 활용되는 방식으로 제안하는 연구를 수행할 예정이다.

또한 IoT 데이터에서 이상 행위를 구분하기 위해서는 정상행위에 대한 데이터가 충분하게 있어야 하며, 향후 적대적 AI 기술 등으로 공격받을 때를 대비해 충분한 데이터 확보와 설명 가능한 AI(Explainable Artificial Intelligence)로 전환 발전시키는 연구도 추가로 요구된다.

요약하면 COVID 19 등으로 가속화된 온라인 비대면 등 디지털 사회적 변화를 반영하고 더 정교화된 환경정의를 통해 디지털 트윈 등에 기반을 둔 미래사회를 예측하고, 향후 도래할 4차 산업혁명 시대인 디지털 환경의 초 극대화로 발생할 수 있는 초국경의 환경에서의 복합적 안보 위협사례를 예측하고, 각 상황에서 발생할 수 있는 이벤트들을 사람의 눈과 귀를 대신할 수 있는 IoT 센싱 기술들을 이용하여 각 처리에 대한 가시성을 확보하기 위한 제반 노력 등을 하는 등 4차산업 시대의 도래로 발생할 수 있는 사이버 위협에 선제적이고 적극적으로 대비할 필요가 있다.

참고문헌

[1] Pedoro Soto-Acosta, “COVID-19 Pandemic: Shifting Digital Transformation to a High-Speed Gear,” Information Systems Management, vol. 37, no. 4, pp. 260-266, 2020.

[2] Sandra Grabowska, “SMART FACTORIES IN THE AGE OF INDUSTRY 4.0 ,” Management Systems in Production Engineering, vol. 28, no. 2, pp. 90-96, 2020.

[3] Gabrielli do Livramento Goncalves, Walter Leal Filho, Samara da Silva Neiva et al., “The Impacts of the Fourth Industrial Revolution on Smart and Sustainable Cities,” Sustainability, 2021.

[4] Erik Feyen, Jon Frost, Leonardo Gambacorta et al., “Fintech and the digital transformation of financial services: implications for market structure and public policy,” Bank for International Settlements, pp. 1000-1004, 2021.

[5] Machkour, Badr, and Ahmed Abriane. , “Industry 4.0 and its Implications for the

Financial Sector," Elservier B.V., pp. 496-502, 2020.
[6] V Fremont, "The Digital Transformation of the Manufacturing Industry," Vincent Fremont, Oct. 2021.
[7] Rafat Mahmood1 and Michael Jetter, "Communications Technology and Terrorism," Journal of Conflict Resolution, pp. 127-166, 2020.
[8] "United Nations Security Council Counter-Terrorism Committee Executive Directorate: Information and Communications Technologies," UN Security Council, 2021.
[9] Robert Graham, "How Terrorists Use Encryption," CTS(Comating Terrorism Center at West Point), vol. 37, no. 4, pp. 20-25, Jun. 2016.
[10] Patrick Howell O'Neillarchive page, "These hackers showed just how easy it is to target critical infrastructure," 2022, https://www.technologyreview.com/2022/04/21/1050815/hackers-target-critical-infrastructure-pwn2own/
[11] Stamford, "Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans," Gartner, 2021.
[12] Robert M. Lee, Michalel J. Assante, Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," Electricity Information Sharing and Analysis Center, 2016.
[13] Andre Kudelski, "The dark side of the Fourth Industrial Revolution," World Economic Forum, 2016.
[14] Andres Munoz-Arcentales, Sonsoles Lopez-Pernas, Alejandro Pozo, Alvaro Alonso, Joaquin Salvachua and Gabriel Huecas, "Data Usage and Access Control in Industrial Data Spaces: Implementation Using FIWARE," Sustainability, 2020.
[15] Goiuri Peralta, Raul G. Cid-Fuentes, Josu Bilbao and Pedro M. Crespo, "Network Coding-Based Next-Generation IoT for Industry 4.0," Intechopen, 2017.
[16] Mohd Javaid, Abid Haleem, Ravi PratapSingh, Shanay Rab, Rajiv Suman, "Significance of sensors for industry 4.0: Roles, capabilities, and applications," ScienceDirect, 2021.
[17] Vidar, "Google's Quantum Computer Is About 158 Million Times Faster Than the World's Fastest Supercomputer," Published in Predict, 2021.
[18] Michal Krelina, "Quantum Technology for Military Applications," arXiv:2103.12548v2, 2021.
[19] Amyas Morse, "Investigation: WannaCry cyber attack and the NHS," National Audit Office, 2017.
[20] Kenneth B Medlock, "The Colonial Pipeline Outage: An Important Lesson For US Energy Security," Forbes, 2021.
[21] Andy Greenberg, "A Hacker Tried to Poison a Florida City's Water Supply, Officials Say," WIRED, 2021.
[22] Saheed Oladimeji, Sean Michael Kerner, "SolarWinds hack explained: Everything you need to know," TechTarget, 2021.
[23] "우리 집 거실 훤히 '월패드 해킹'...똑똑한 아파트일수록 불안 커진다," 한국일보, 2021, https://www.hankookilbo.com/News/Read/A2021120915500002964
[24] Mahmudul Hasan, Milon Islam, Ishrak Islam Zarif, Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," Internet of Things, 2019.

[25] Fahiba Farhin; Ishrat Sultana; Nahida Islam; M Shamim Kaiser; Md. Sazzadur Rahman; Mufti Mahmud, "Attack Detection in Internet of Things using Software Defined Network and Fuzzy Neural Network," 2020 Joint 9th International Conference on Informatics, 2021.

[26] Vasily Desnitsky, Andrey Chechulin, Igor Kotenko, "Multi-Aspect Based Approach to Attack Detection in IoT Clouds," PubMed Central, 2022.

[27] Gauthama Raman M. R., Chuadhry Mujeeb Ahmed & Aditya Mathur "Machine learning for intrusion detection in industrial control systems: challenges and lessons from experimental evaluation," Cybersecurity. springeropen, 2021

[28] Mohamad Kaouk; Jean-Marie Flaus; Marie-Laure Potet; Roland Groz, "A Review of Intrusion Detection Systems for Industrial Control Systems," 2019 6th International Conference on Control, Decision and Information Technologies (CoDIT), 2019.

[29] Bernard Marr, "The Top 10 Technology Trends Of The 4th Industrial Revolution," Forbes, 2020.

[30] Sean Lyngaas, "Universal Health Services reports $67 million in losses after apparent ransomware attack," Sophos Endpoint Cybersecurity, 2021.

[31] "사회기반시설에 대한 민간투자법,"기획재정부, 2021.

[32] Hussain Ahmad, Isuru Dharmadasa, Faheem Ullah, M. Ali Babar, "A Review on C3I Systems' Security: Vulnerabilities, Attacks, and Countermeasures," Cornell University, 2021.

[33] "The Critical Importance of Endpoint Management and Security," TBConsulting, 2020.

[34] "Wikipedia," 2022, https://en.wikipedia.org/wiki/ Society

[35] "FIWARE," FIWARE Foundation, 2021, https://www.fiware.org/

[36] "Gartner's 8 Cybersecurity Predictions for 2023-2025,",2022, https://krontech.com/gartners-8-cybersecurity-predictions-for-2023-2025.

[37] Dominic Endicott, John Sviokla, "Facing up to a four-generation society,"strategy&, 2022, https://www.strategy-business.com/aricle/Facing-Up-to-a-Four-Generation-Society

[38] Klaus Schwab, "The Fourth Industrial Revolution: what it means, how to respond," WORLD ECONOMIC FORUM, 2016, https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

[39] Matthew J. Kalas, "Drones Aren't Just Hackers' Targets - They're Hackers' Weapons," Locke Lord, 2020, https://www.lockelord.com/newsandevents/publications/2020/07/drones-arent-just-hackers-targets.

[저자소개]

최 향 창 (Hyang-Chang Choi)
2005년 8월 전남대학교 정보보호 졸업 (박사)
2009년 2월 전남대학교 시스템 보안 연구센터 근무
2011년 2월 호남신학대학교 전산 초빙교수
2021년 8월 국가정보자원관리원 근무
2021년 9월 ~ 현재 대전대학교 안보군사연구원 근무
email : hc.choi@dju.kr