https://doi.org/10.33778/kcsa.2023.23.3.021

# 전력시스템 대상 지능형 사이버공격 동향 분석★

홍 순 민*, 엄 정 호**, 이 재 경***


## 요 약

21세기 정보통신기술의 발달은 주요기반시설의 제어시스템에 초연결성과 초지능성을 갖게 하여 운용 효율성을 높였으나, 보안 취약점을 증가시켜 해킹 위협에 노출되고 있다. 그중에서도 일상생활에 필수적으로 사용하는 전력을 공급하는 전력시스템은 국가 중요기반체계로서 사이버공격의 주요 표적이 되고 있다. 최근에는 전력시스템을 보호하기 위해서 다양한 보안체계를 개발하고 실전형 사이버공방훈련을 통해서 전력시스템의 안정성을 유지하고자 한다. 하지만, 사이버공격이 인공지능과 빅데이터 등의 첨단 ICT 기술과 접목되면서 기존의 보안체계로 지능화되고 있는 사이버공격을 방어하기가 쉽지 않게 되었다. 이러한 지능화되는 사이버공격을 방어하기 위해서는 지능형 사이버공격의 유형과 양상을 사전에 파악하고 있어야 한다. 본 연구에서는 첨단 ICT 기술과 접목된 사이버공격의 진화에 대해서 분석하였다.


# Trend Analysis of Intelligent Cyber Attacks on Power Systems

Soon-Min Hong*, Jung-ho Eom**, Jae-Kyung Lee***


## ABSTRACT

The development of information and communication technology in the 21st century has increased operational efficiency by providing hyper-connectivity and hyper-intelligence in the control systems of major infrastructure, but is also increasing security vulnerabilities, exposing it to hacking threats. Among them, the electric power system that supplies electric power essential for daily life has become a major target of cyber-attacks as a national critical infrastructure system. Recently, in order to protect these power systems, various security systems have been developed and the stability of the power systems has been maintained through practical cyber battle training. However, as cyber-attacks are combined with advanced ICT technologies such as artificial intelligence and big data, it is not easy to defend cyber-attacks that are becoming more intelligent with existing security systems. In order to defend against such intelligent cyber-attacks, it is necessary to know the types and aspects of intelligent cyber-attacks in advance. In this study, we analyzed the evolution of cyber attacks combined with advanced ICT technology.


**Key words : Cyber Attack, Power Infrastructure, 4th Industrial Revolution, Cyber Security**

접수일(2023년 08월 28일), 수정일(2023년 09월 08일), 게재확정일(2023년 09월 21일)

★ 이 논문은 2022년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2022S1A5C2A03093531).

★ 이 논문은 2023년도 융합보안학회 하계학술대회에서 수상한 논문을 수정·보완한 논문임.

* 대전대학교 안보융합학과(주저자)

** 대전대학교 안보융합학과&군사학과 교수(공동저자)

*** 대전대학교 군사학과 박사과정(교신저자)

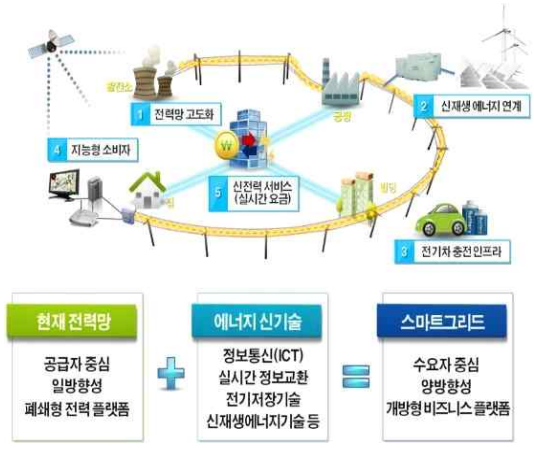
## 1. 서 론

제4차 산업혁명 시대의 정보통신기술이 급진적으로 발달함에 따라 주요기반시설의 환경에 적용되어 보다 지능적이고 초연결적인 환경으로 변모하고 있다. 특히 지능형 전력망은 첨단 정보통신기술을 활용하여 전력망을 지능화, 고도화된 전력서비스를 제공하고, 에너지효율을 극대화하는 제어시스템을 도입하였다. 국내 한국전력공사도 지능형 전력망 구축을 위해서 꾸준히 연구 개발을 하고 있다. 하지만, 코로나 팬데믹 이후 주요기반시설에 대한 사이버공격이 지속되고 있는 가운데 일상생활에 필수적으로 쓰이는 전기를 생산 및 공급하는 전력망에 대한 사이버공격도 발생하고 있는 전력망에 대한 사이버공격은 정전뿐만 아니라 이로 인한 공장 가동 중단, 생필품 생산 지연 등으로 경제적 피해로도 이어질 수 있다. 이는 일상 삶에 필수적인 전기 에너지와 관련된 전력망에 대한 사이버공격은 국가 측면에서 매우 중대한 위협으로 여겨지고 있다. 또한 최근에 추진하고 있는 '지능형 전력망(Smart Grid)'은 기존 폐쇄적인 전력망보다 개방적이기 때문에 보안 취약점이 증가할 것이며, 사이버공격에 빈번하게 노출될 것으로 보인다.

따라서 본 논문에서는 향후 전력망에 대한 사이버공격을 대비하는 측면에서 미래 지능형 사이버공격 양상을 예측하고자 한다. 최근 국내·외 전력망 및 전력기반시설에 대한 사이버공격 사례를 기반으로 공격기법과 양상을 분석한 후에 4차 산업혁명 기술의 핵심 정보통신기술인 인공지능, 빅데이터 등이 적용된 지능형 사이버공격 양상을 제안한다.

## 2. 전력시스템의 구조 및 특징

신재생에너지 확대 정책과 4차 산업혁명 신기술 패러다임에 대응하기 위해 국내·외 전력시스템은 기존 폐쇄적이고 단일적인 전력망과 더불어 개방적이면서 ICT 기술 융합으로 다양한 정보 교환이 가능한 지능형 전력망으로 구축하고 있다. (그림 1)은 지능형 전력망 구축 전략을 보여준다.




(그림 1) 지능형 전력망 구축 전략[1]

지능형 전력망은 기존 전력망에서 전기 생산, 공급을 담당하는 제어시스템을 통합하고 상호 연결하여 스마트 전력시스템으로 구축하고자 한다[1]. 그러기 위해서는 아래의 3가지 시스템을 갖춰야 한다.

- 지능형 검침 인프라 (AMI: Advanced Metering Infrastructure) : 지능형 전력망의 핵심 기술로써 스마트미터, HAN 통신망, MDMS 데이터관리시스템과 WAN 운영시스템으로 구성되어 있다. 스마트미터를 기반으로 주기적으로 전력 사용량을 측정, 수집하여 분석하는 시스템으로 AMI 네트워크를 통해 하드웨어 정보, 데이터 관리 및 수집, 통신설비 상태, 소비자 동향 수집 및 제어, 보안정책 관리 등을 포함한다[2,3].

- 에너지 관리 시스템 (EMS: Energy Management System) : AMI 네트워크에서 수신한 데이터를 기반으로 에너지효율을 향상하기 위해서 전력을 생산 및 공급, 사용을 최적화하도록 IT기술을 통해 관리한다[4].

- 에너지 저장 시스템 (ESS: Energy Storage System) : 생산된 전기를 저장장치에 저장했다가 전력이 필요할 때 공급하여 실시간으로 전력을 사용하는데 효율적으로 사용할 수 있다. 전력저장원, 전력변환장치(PCS), 관리시스템(EMS)로 구성되어 있다. 에너지를 저장하고 공급하는 과정에서 ESS는 EMS와 네트워크 통신 및 데이터 처리 프로세스 연계가 필수적이다. EMS를 통해 실시간으로 변하는 주파수에 즉각적인 반응을 하여 충전과 방전을 유지하며 ESS 제어

저장방식은 물리적 방식으로 저장한다[5].

# 3. 국내·외 전력시스템 대상 사이버공격 사례

지능형 전력망은 다양한 IoT 센서들과 유·무선 네트워크로 연결되고 특정 상황에서는 휴대용 무선 장비를 통해서 외부에서 통제를 가능하도록 구축하고 있기에, 보안 취약점이 점점 증가하게 된다. 특히, 제어시스템 대상으로 네트워크 마비, 데이터 변조 등의 해킹이 발생할 경우, 원활한 전력을 제공하지 못하게 될 것이다. 이번 장에서는 국내·외에서 발생한 전력망 대상 사이버공격 사례를 분석한다.

## 3.1 국내 전력망 사이버공격 사례

국내 전력망 대상 사이버공격은 국정원의 사이버안보센터에서 밝힌 내용을 참고하였다. 코로나 팬데믹 이후 스마트미터 AMI LTE 모뎀을 임의로 조작, 교체하여 고객들의 개인정보를 유출한 사건이 21년도 국내에서 있었으며[6], 국내 주요 원자력발전소 직원에게 피싱메일 유포, 비인가 홈페이지 접속 유도, 원격근무 취약점을 이용한 사이버공격 등이 발생했다[7].

<표 1> 국내 전력망 대상 사이버공격 사례[7]

| 날짜 | 공격 사례 |
|---|---|
| 21.03 | 한전이 사용하는 고압 AMI LTE 모뎀 1만2308대 악성코드 미라이봇네 공격으로 통신 차단 |
| 21.06 | 한국 원자력발전소 내 피싱메일, 비인가 홈페이지 접속 유도, 원격근무시스템 VPN 취약점을 악용하여 대규모 해킹 시도 |

국내 사례를 분석해 볼 때, 외부에서 내부로 연결되어있는 네트워크 접점을 통해서 네트워크를 마비시키고 내부망으로 악성코드를 침투시키기 위해서 내부자의 메일을 이용하였다. 국내 전력 제어시스템은 폐쇄망 형태로 운영하기 때문에 내부망으로 침투하기에는 반드시 내부 직원 PC를 이용한 해킹 방법을 사용하고 있다.

## 3.2 국외 전력망 사이버공격 사례

국외 전력망 대상 사이버공격 사례는 미국 CSIS ‘중대 사이버 사고보고서’[8]을 참고하여 <표 2>와 같이 요약 정리하였다.

<표 2> 국외 전력망 대상 사이버공격 사례[8]

| 날짜 | 국가 | 공격 사례 |
|---|---|---|
| 20.05 | 독일 | 러시아 해킹그룹이 독일의 에너지 전력공급망 네트워크를 손상 |
| 21.05 | 노르웨이 | 노르웨이 에너지 기술회사 VDUE에 대한 랜섬웨어 공격 |
| 21.12 | 호주 | 러시아 해킹그룹이 호주 CS 에너지 회사에 랜섬웨어 공격 |
| 22.04 | 우크라이나 | 러시아 해킹그룹이 악성코드를 사용하여 전력 공급 및 변전소 사이버공격 시도, 발전소 원격 모니터링 중단 |
| 22.07 | 리투아니아 | 국영 에너지 공급업체 해킹 |
| 22.08 | 이탈리아 | 해커가 이탈리아 에너지 공급망 네트워크 침입 |
| 22.08 | 독일 | 독일 전력 반도체 부품 기업 세미크론 랜섬웨어 공격으로 2TB 내부 데이터 유출 |
| 22.10 | 인도 | 인도 전력회사 일부 IT 시스템이 랜섬웨어 및 APT 공격으로 마비 |

위의 <표 2>를 보면, 주로 사용되는 사이버공격 방식은 피싱메일, 랜섬웨어, APT 공격 등이다. 최근에 국가 중요기반시설의 제어시스템을 대상으로 발생하는 사이버공격 기법에는 랜섬웨어와 APT 공격을 활용하고 있다. 이러한 공격 방식은 기존의 사이버보안 체계를 우회하거나 보안관리자가 인지하지 못한 상황에서 내부망으로 침투한다. 특히, 랜섬웨어에 감염된 시스템은 암호화되기 때문에, 시스템에 저장된 모든 데이터가 암호화되어 복호화하기 전까지 사용하지 못한다. 또한 공격자에게 복호화 비용을 지불하더라도 완벽하게 복호화가 되지 않기 때문에, 빠른 시일 내 정상적인 시스템으로 복구 불가능하다. 최근에는 랜섬웨어와 APT 방식이 결합한 형태의 공격 방식이 사용되고 있어서 전력망 보호를 위해서 이러한 공격에 대한 대비책을 마련해야 한다. 미국은 국가 중요기

반체계에 대한 사이버공격에 대해서는 통합억지 개념으로 다루고 있어서 국내에서도 이러한 보안 전략도 고려할 만하다[9].

## 4. 전력시스템 대상 사이버공격 기법

### 4.1 사이버공격 유형

전력시스템은 내부망과 외부망을 분리해서 운영하는 경우가 많기에, 본 연구에서도 사이버공격 유형을 각 내부망과 외부망 대상으로 한, 공격 유형으로 기술한다. <표 3>은 외부망 대상 사이버공격 유형을 '국내·외 지능형 전력망에 대한 사이버공격 사례'에서 발췌 및 요약한 것이다[10]. AMI, ESS, EMS 제어시스템을 대상으로 발생할 수 있는 사이버공격 유형이다.

<표 3> 외부망 대상 사이버공격 유형[10]

| 유형 | 피해 |
|---|---|
| 방해 공격 | 정보 충돌을 송수신하기 위해 하나 이상의 노드 차단 |
| 스푸핑 공격 | 다른 노드를 오해 유도 |
| 주입 공격 | 잘못된 데이터 주입<br>합법적인 프로세스 및 운영 손상 |
| 플러딩 공격 | 노드 오작동/네트워크 가용성 손실 |
| 중간자 공격 | 중요한 정보에 대한 무단 액세스 |
| 소셜 엔지니어링 공격 | 사용자의 개인정보 침해 시스템의 일시적 또는 영구적 손상 |
| 도청 공격 | 개인정보 손실 |
| 침입 공격 | 네트워크에서 사용이 가능한 리소스를 잘못 사용하도록 유도 |
| 브루트 포스 공격 | 사용자의 시스템 또는 계정에 무단 액세스 권한 획득 |
| 시간 동기화 공격 | 위치 추정 및 결함 감지와 같은 손상 이벤트 성능 저하 |
| 트래픽 분석 공격 | 노드 간 통신 패턴에 대한 정보를 얻기 위해 메시지 스니핑 |
| 신분 위장 공격 | 시스템에 대한 무단 액세스 권한 획득 |
| 버퍼 오버플로 공격 | 시스템 충돌 또는 리소스 소모 |
| 티어드롭 공격 | 통제시스템 운영체제 중단 |
| 스머프 공격 | 네트워크 포화 상태 유도 |
| 꼭두각시 공격 | AMI 네트워크에서 가짜 데이터 전송 |
| HMI POP 기능 공격 | 무단 액세스 허용 |

내부망 대상 사이버공격은 IT 인프라가 갖는 고유의 보안 취약점을 이용하거나 인가된 사용자의 내부 시스템을 이용하는 등의 방법을 이용한다. 내부망 위협은 데이터 처리 구간에서의 식별 및 인증 정보 탈취를 통해 내부정보를 유출할 수도 있고 내부자와 공모해서 발생할 수도 있다. 즉, 시스템/통신 점검을 위한 외부 직원이 랜섬웨어나 APT 공격 프로그램이 저장된 PC나 USB를 내부망에 연결한다면, 가장 심각한 피해를 볼 수 있다. 또 다른 공격 유형으로는 외부 인터넷망과의 연결 지점(접점) 사이의 취약점을 이용하거나 내부망 환경에서 전자기, 음향, 광학, 진동 등의 기술들을 활용하여 데이터를 유출하는 에어 갭 공격 등이 있다. 아래 표는 내부망 대상으로 발생할 수 있는 사이버공격 유형을 보여준다.

<표 4> 내부망 대상 사이버공격 유형[11]

| 유형 | 피해 |
|---|---|
| USB 사용 | 내부자의 USB 내 악성코드를 주입하거나 악성코드가 주입된 USB를 내부자가 본인 PC에 꽂아 내부 시스템으로 침투시키는 공격 |
| USB RF 전송 | USB 기기를 RF 전송기로 변환하여 물리적으로 USB를 꽂지 않고 멀웨어를 통해 침투 가능 |
| CPU 전자기기 신호 | CPU 전자기 신호를 이용하여 키 스트로크 정보 탈취 |
| 초음파 통신 | 초음파를 사용하여 두 개 이상 망분리 시스템 사이 통신 채널 구축을 통해 통신 방해 |
| 에어 갭 공격 | 외부 인터넷망과의 접점 사이의 취약점을 이용하거나 에어 갭 환경 내에서 전자기, 음향, 광학, 진동 등의 다양한 기술을 활용하여 데이터를 유출하는 방식 |
| 공급망 공격 | 전력시스템을 공급하는 IT업체의 서버나 개발자 PC에 악성코드를 침투시킨 후에 전력시스템을 교체하거나 소프트웨어를 업그레이드할 때 심어둔 악성코드가 내부망으로 침투하게 하는 공격 |

내부망 대상 사이버공격 유형은 AMI 시스템에 연결된 전력망이 물리적으로 망 분리가 되어 있어도 공

격에 활용할 수 있다. 스마트미터에 설치된 CPU 전자기기 신호를 탈취하여 양방향 통신을 불가능하게 만들거나 인위적으로 외부 통신 모델을 교체하는 경우는 논리적 공격뿐만이 아닌 물리적 공격이 동시에 가능하다는 점에서 매우 취약하다고 할 수 있다. 에어갭 공격이나 초음파 통신 같은 경우는 실제 전력망 ESS 물리적 배터리 저장 설비에서 나타나는 전류 흐름, 하드웨어 온도변화, 진동 등을 파악할 수도 있으며, 배터리의 저장용량을 줄이거나 방전을 유도하는 공격도 가능하다고 밝혔다[12]. 전력망은 내부망 자체에 대한 보안뿐만 아니라 내부망이라고 할지라도 원격 통제를 위해서 외부망과 연결되는 접점이 있기에 외부에서 침입하는 사이버공격에 대한 보안 체계를 갖추어야 한다.

### 4.2 사이버공격 절차

<표 3>과 <표 4>의 공격 유형을 기반으로 전력기반시설을 해킹하기 위한 사이버공격을 진행할 때 <표 5>의 사이버공격 절차를 활용한다. 이는 '스마트그리드에 대한 공격 주기'에서 요약 정리한 사이버공격 절차로 정찰-스캐닝-침투-액세스 유지 단계로 진행된다[12].

<표 5> 사이버공격 절차[12]

| 절차 | 공격 특징 |
|---|---|
| 정찰 | - 트래픽 분석, 사회공학 분석 |
| 스캐닝 | - IP, 포트, 서비스, 취약점 스캔 |
| 침투 | - 악성코드(PC바이러스, 웜, 트로이목마) 감염<br>- 서비스 거부(DOS) 공격<br>- MITM(main-in-the-middle)공격<br>- HMI(Human Machine Interface)팝업<br>- 무결성 위반 및 개인정보 침해<br>- 재생 공격 및 방해 채널 |
| 액세스 유지 | - 백도어<br>- 액세스 권한 허가 및 유지 |

각 단계에 대한 공격 절차는 다음과 같다.

- 정찰 단계 : 시스템 검색을 통해서 활성화 여부를 확인한다거나 사회 공학적 방법을 통해서 전력시스템에 대한 정보를 획득하는 것이다. 예를 들면, 전력기반체계에 대한 통신설비에 연결하여 암호 또는 PIN 번호와 같은 자격 증명 및 기밀 정보를 얻는 단계이다.

- 스캐닝 단계 : 다양한 스캔 기법을 통해서 네트워크에서 공격에 필요하거나 수신이 가능한 모든 장치와 호스트를 식별하는 단계이다. 지능형 전력망 각 구조는 연계되어 있기에 어느 하나의 시스템에 공격이 노출되면 모든 시스템이 스캐닝 될 수 있다. 또한, 공격 경로를 찾기 위해서 취약점 분석 도구를 활용하여 취약점을 식별한다.

- 침투 단계 : 스캐닝 단계에서 획득한 취약점을 이용하여 취약점을 이용할 수 있는 가장 적합한 공격 기법을 선택하여 공격 대상 시스템에 침투하는 단계이다. 예를 들면, 악성코드 감염, 디도스 공격, APT 공격, 랜섬웨어 공격 등 다양한 공격을 시도할 수 있다. 또한, ESS에 인가되지 않은 제어 명령을 전송하거나 AMI에 오정보를 삽입할 수 있다.

- 액세스 유지 단계 : 첫 번째 사이버공격을 시도하여 성공하였다면, 재차 공격하기 위해서 접근 경로를 유지하고 있어야 한다. 그래서 백도어를 설치하여 차후 공격을 시도할 때 활용한다.

## 5. 전력시스템 대상 지능형 사이버공격 전망

지능형 사이버공격은 새로운 공격 기법일 수도 있지만, 대부분이 기존 사이버공격 유형의 기능을 확장하고 성능을 향상하는 것이다. 즉, 4장에서 기술한 사이버공격 유형과 절차에 인공지능과 빅데이터 기술을 접목하면, 공격 성공률을 높일 수 있다. 예를 들면, 브루트 포스 공격 기법에 빅데이터 기술을 적용하면 효율적이고 빠르게 시스템에 대한 정보를 획득할 수 있으며, 사이버공격 마스터 에이전트에 인공지능 기술을 적용한다면, 사이버공격 중에 가장 성공률이 높은 유형을 선택하고 경로를 찾아내어 공격을 시도하게 할 것이다. 아울러 몇 가지의 사이버공격을 융합시켜서 최적의 공격 기법을 제작할 수도 있다.

사이버공격 절차에도 정찰과 스캐닝 단계에 빅데이터 기법을 적용하여 가장 신속하게 공격 대상의 정보와 공격 경로를 찾아낸다거나 침투 단계에서 악성코드를 정상 코드처럼 위장시킨다거나 가장 최적의 공

격 기법을 선택하게 할 수도 있다. 이렇게 지능형 사이버공격은 기존의 사이버공격 유형과 절차에 첨단 ICT 기술을 접목하여 보안 취약점과 공격 대상을 보다 신속하고 정확하게 찾아내고 최적의 공격 기법과 경로를 식별하여 보안시스템을 우회하여 공격 목적을 달성하는 것이다.

그리고 지능화되는 전력기반체계의 제어시스템은 운용 측면에서 효율성은 높아지겠지만, 오히려 증가하는 보안 취약점으로 인해서 점점 더 교묘해지고 은밀해지는 지능형 사이버공격에 취약하게 될 것이다[13]. 이 밖에도 앞으로 전력시스템에 대한 지능화된 사이버공격은 다음과 같은 양상으로 나타날 수 있다.

첫째, 여러 사이버공격 유형이 여러 개 혼합한 형태로 나타날 것이다. 예를 들면, 표적형 공격인 APT의 데이터 유출과 랜섬웨어 공격의 암호화를 결합하여 데이터를 유출한 후에 공격 대상 시스템을 암호화시키는 것이다. 또한, 논리적 사이버공격과 물리적인 에어 갭 공격이 융합한 형태로도 동시에 발생할 수도 있다.

둘째, 인공지능 기술 기반의 변종 악성코드 공격이다. 전력시스템은 외부로부터 오는 악성코드를 차단하는 방화벽이나 침입방지시스템이 설치되어 있다. 이를 우회하기 위해서 인공지능 기술을 활용하여 정상적인 데이터처럼 전력망에 악성코드를 침투한 후에 시스템을 감염시킨다. 그리고, 침투 후에는 인공지능 기술을 활용하여 악성코드를 데이터 유출용으로 변형하여 2차 공격을 감행할 수도 있다.

셋째, 지속적으로 공급망 공격을 시도할 것이다. 논리적 망분리 또는 물리적 망분리로 구축된 전력시스템일 경우에는 외부에서 내부로 침입하는 것은 쉽지 않다. 그렇기에 전력망 시스템에 사용하는 프로그램 제조사의 서버나 개발자 PC를 해킹한 후에 악성코드가 감염된 PC가 내부망과 연결되어 내부 시스템에 프로그램이 설치되거나 업데이트할 때 악성코드가 삽입하는 공격을 할 것이다. 악성코드에 감염된 시스템은 오류가 발생하거나 주요 데이터가 유출될 수도 있다.

넷째, 클라우드 컴퓨팅, 안드로이드 운영체제 등 개방형 시스템 환경의 취약점을 이용하여 사전 오픈소스 SW에 악성코드, 랜섬웨어 등을 심어놓고 원하는 시기에 사이버공격이 실행되도록 설정할 수도 있다. 전국에 지역별로 분산된 재생에너지 발전소, 외부에 설치된 ESS 전력저장시스템 등에 동시다발적으로 지능형 사이버공격을 시도하여, 보안시스템이나 관리자가 대응하지 못하도록 할 수도 있다. 이러한 동시다발적 사이버공격의 통제는 인공지능을 활용하여 진행된다.

다섯째, 최근 기후변화 위기로 인해 구축된 재생에너지 기반 전력시스템의 구조적 취약점을 활용한 사이버공격 경로의 다변화가 예상된다. 재생에너지 풍력 및 태양광 발전소뿐만 아니라 기존 화력, 원자력발전소에서 공급하는 전력서비스의 데이터 공유를 위한 많은 장비들이 디지털로 연결돼 있어 공격이 가능한 취약점이 증가하여 보안 위협에 대한 위험 요소가 매우 많다. 인공지능이 접목된 취약점 분석 도구를 활용하여 가장 취약한 시스템을 식별하고 최적화된 공격 기법을 활용하여 단계적으로 공격한 후, 최종 공격 대상 시스템까지 침투하여 공격 목적을 달성할 수 있다.

여섯째, 드론 및 소형 로봇 등에 스마트 전파 교란기를 탑재하여, 전력시스템간 통신을 방해할 수 있다. 스마트 전파 교란기를 탑재한 드론을 전력시스템 통신 구간으로 이동시켜서 전파 교란을 시도할 경우, 통신 마비를 발생시킬 수 있다. 또한, 소형 로봇에 EMP 폭탄을 탑재하여 공격 대상 전력시스템으로 이동시킨 후에 폭발시키면, 물리적인 피해뿐만 아니라 시스템이 마비되는 논리적 파괴뿐만 아니라 시스템에 충격을 가해 물리적인 파괴도 유도할 수 있다.

마지막으로, 현재 및 미래에 사이버 공간에서의 최고 잠재적인 위협인 내부자를 이용하는 내부자 위협이다. 특히, 소속 직원은 시스템에 접근할 수 있는 권한이 주어졌기에 내부자에 의한 데이터 유출은 해킹보다 더 큰 피해를 줄 수 있다. 예를 들어, 내부자의 이동 동선에, 악성코드에 감염된 USB를 놓아두고 내부자가 습득하게 한 후 PC에 꽂게 한다. 이때, 꽂자마자 악성코드가 내부망으로 침투하게 되면, 보안시스템이나 프로그램에 탐지될 수 있다. 그래서 일정 시간이 지나거나, 신호가 있을 때 침투하게 한다. 또한, 전력시스템을 유지 보수하는 회사의 직원일 경우, 정기적으로 전력망 내부 시스템에 접근할 수 있기에 악성코드를 숨겨둔 유지보수용 노트북이 내부 시스템에 접속될 때 전력 전체 시스템에 악영향을 주는 악성코드

에 감염될 수도 있다.

## 6. 결 론

본 연구는 국내·외 지능형 전력망에 나타난 사이버 공격을 기반으로 미래에 발생할 수 있는 지능형 사이버공격 동향을 전망하였다. 실제로 전력 공급을 관리하는 시스템에 대한 사이버공격은 국내·외 사례가 유사하며 세계 각국 전력기반시설에 대한 사이버공격은 매년 끊임없이 나타나고 있다.

제4차 산업혁명시대의 전력망의 초연결성과 효율성을 위한 발전은 사이버공격이라는 역효과도 동반하고 있다. 첨단 정보통신기술을 활용하여 초연결성과 초지능성 환경으로 제어시스템의 보안 취약점이 증가하고 이를 이용한 사이버공격이 점점 증가하고 그 방법도 교묘해지는 추세이다. 논리적인 침투 및 정보 탈취, 시스템 마비 등을 넘어 전자기 교란, 물리적 피해 발생을 동반한 하이브리드 공격은 핵심 기반시설을 무력화하여 국가의 존립까지 위협할 수 있는 최악의 상황으로 확대될 수도 있다. 따라서 국가의 핵심 기반시설인, 전력기반체계에 대한 사이버보안은 정책적, 체계적, 기술적인 모든 관점에서 대응 방안을 수립해야 한다. 특히 관련 시스템을 대상으로 더욱 지능화될 사이버공격을 예측하고 분석함으로써 앞으로 산업제어시스템 보안 계획을 수립하고 보안시스템을 운영할 때 최적화된 보안기술을 적용할 수 있을 것이다.

## 참고문헌


[1] 이창훈 "스마트그리드 기술동향 및 향후전망", 한국통신학회 vol.38. no.9. August. 2021. pp 71-77.

[2] 정준홍, 서충기 "AMI 시스템의 효과적인 계량정보 수집방법" 한국통신학회 vol.43. no.8, August. 2018. pp 1311-1320.

[3] 최재덕, 서정택., "스마트그리드 보호를 위한 AMI 망 분리 및 인증 프레임워크" 한국 정보보호학회논문지 vol.22, no.3, June. 2012. pp. 525-536.

[4] 유성민, 김남균, 김윤기 "스마트그리드 보안기술 동향 분석 및 대응방안" 한국정보기술학회 vol.31. no.5. April. 2014. pp 8-14.

[5] 이대성 "지능형 전력망의 안전성과 신뢰성 확보를 위한 보안위협과 정책분석" 한국정보통신학회 vol.25. no.10, October. 2021. pp 1381-1390.

[6] 국정원 국가사이버안보센터 국가정보보호백서 2021.

[7] 국정원 국가사이버안보센터 국가정보보호백서 2022.

[8] Center For Strategic and International Studies, "Significant Cyber Incidents Since 2006", May. 2023.

[13] Hyang. chang. Choi., "A Study on the Model for Preemptive Intrusion Response in the era of the Fourth Industrial Revolution" Journal of convergence security, vol.22(2), June. 2022, pp. 27-42.

[9] Daewook. Kang., Sangjung. Lee., Jaesik. Kang., Youngju. Park., Jongpil. Lee., Taejin. Kim., Dongwook. Yoo. "Cyber Physical Security Technology Trend in Power Conversion System" Korea Electrotechnogy Research Institute, vol.30(5), October. 2020, pp. 7-11.

[10] Tala. Talaei. Khoei., Hadjar. Ould. Slimane., Naima. Kaabouch., "Cyber-Security of Smart Grids: Attacks, Detection, Countermeasure Techniques, and Future Directions." Scientific Research, Communications and Network, vol.14(4), November 2022, pp.119-170.

[11] 유재현 외2명 "사이버 공격대응을 위한 최신 망분리 공격 동향 연구" 한국통신학화 학술대회 논문집, 2001. pp. 899-900.

[12] Z. Elmrabet, H. Elghazi1, N. Kaabouch2, H. Elghaz., "Cyber-security in smart grid: Survey and challenges", International Journal of Computers & Electrical Engineering, Vol. 67, April 2018, pp.469-482.

[13] Hyang. chang. Choi., "A Study on the Model for Preemptive Intrusion Response in the era of the Fourth Industrial Revolution" Journal of convergence security, vol.22(2), June. 2022, pp. 27-42.

## [저 자 소 개]

홍 순 민 (Soon-Min Hong)
2016년 3월 대전대학교 정치외교학 전공 학사
2023년 3월 ~ 현재 대전대학교 안보융합학과 석사과정 재학

email : hrs8457@naver.com

엄 정 호 (Jung-Ho Eom)
1994년 3월 공군사관학교 항공공학과 학사
2003년 2월 성균관대학교 전기전자 및 컴퓨터공학과 석사
2008년 2월 성균관대학교 컴퓨터공학과 박사
2010년 9월~2011년 2월 : 성균관대학교 정보통신공학부 연구교수
2011년 3월~현재 대전대학교 군사학과&안보융합학과 교수
email : eomhun@gmail.com

이 재 경 (Jae-Kyung Lee)
1994년 3월 공군사관학교 경영학 학사
2006년 12월 국방대학교 국방대학원 전산정보학 석사
2016년 3월 프랑스 국립고등항공우주학교 위성 엔지니어링 석사과정 수료
2020년 3월~현재 대전대학교 군사학과 박사과정 재학
1994년 3월 ~ 현재 대한민국 공군 현역 장교
email : jakeyleekr@naver.com