특집 05

적성국의 사이버 공격에 대응하는 위성통신 및 무선통신 시스템의 보안 강화 전략

정진우 · 윤상범 (LIG 넥스원)

목 차

1. 서 론

사이버 안보의 중요성은 현대 사회에서 더욱 강조되어야 할 필수 요소다. 특히, 북한과 같은 적성국에 의한 사이버 공격은 전 세계적으로 심각한 위협으로 부상하고 있다. 북한은 2015년부터 금융기관에 대한 사이버 공격을 세계적으로 수행해 왔으며, 이는 베트남의 티엔퐁 은행에 대한 공격과 같은 사례에서 명확히 드러난다[1]. 또한, 유엔 전문가들은 최소 17개국에서 북한이 불법적인 자금 조달을 위해 사이버 공격을 시도한 적이 있다고 보고하고 있다[2].

특히, 북한은 최근 남한의 조선소를 대상으로 한 집중적인 사이버 공격을 감행, 이를 통해 남한의 국가 안보에 직접적인 위협을 가한 바가 있다[3]. 이러한 사이버 공격은 단순히 정보 탈취에 그치지 않고 군사적, 경제적 파급효과를 목표로 하고 있다. 북한의 사이버 공격 능력은 많은 이들에게 과소평가 되고 있으나, 이는 물리적인 피해뿐만 아니라 국가의 핵심 인프라를 위협하는 수준에 이르렀다[4].

더불어, 북한은 사이버 공격을 통해 약 20억 달러를 조달하여 대량살상무기 프로그램에 자금을 지원하는 등, 사이버 영역에서의 범죄 활동을 통해 국가적 차원의 이익을 추구하고 있다[5-6]. 이처럼 북한의 사이버 공격은 단순한 해킹 활동을 넘어서 국가 안보에 중대한 위협을 제기하며, 위성통신 및 무선통신 시스템의 보안 강화가 절실하게 요구되는 배경이 된다.

2. 위성통신과 무선통신의 기술적 구조 및 운용 방식 개요

위성통신 시스템은 지상의 기지국과 우주에 위치한 인공위성을 활용하여 데이터를 전송하는 복잡한 기술 체계이다. 이 시스템은 전 세계적인 커버리지를 제공하며, 글로벌 포지셔닝 시스템(GPS), 통신, 기상 관측 등 다양한 목적으로 활용된다. 위성통신은 특히 광범위한 지역 커버리지가 필요한 해양, 항공, 군사 및 재난 관리 분야에서

중요한 역할을 수행한다. 이 시스템은 지리적으로 접근이 어려운 지역에서도 통신 서비스를 제공할 수 있어, 원격 지역의 연결성과 응급 상황에서의 통신 능력을 향상시킨다.

무선통신 네트워크는 전파를 통해 정보를 전송하는 현대적인 통신 방식으로, 이는 고도화되고 지능화된 기술을 기반으로 한다. 이러한 네트워크는 휴대폰, 무선 인터넷, 위성통신 등 다양한 형태의 통신에 사용되며, 일상생활에서 중요한 역할을 담당한다. 무선 네트워크 기술은 계속 발전하고 있으며, 5G와 같은 최신 기술은 더 빠른 데이터 전송 속도, 낮은 지연 시간, 그리고 높은 네트워크 효율성을 제공한다. 이러한 기술은 스마트 시티, 자율주행 차량, 원격 의료와 같은 미래 기술의 발전에도 중요한 기반을 제공한다[7]. 다음의 <표 1>은 위성통신과 무선통신의 기본적인 공통점과 차이점, 그리고 각각의 장단점을 요약한 것이다. 위성통신은 주로 원거리 통신과 광역 커버리지를 제공하는 반면, 무선통신은 주로 근거리 및 지역적 커버리지를 제공한다. 또한, 위성통신은 지형에 구애받지 않는 광범위한 서비스를 제공하는 반면, 무선통신은 설치 및 유지보수의 편의성과 빠른 데이터 전송 속도를 제공한다. 그러나 위성통신은 신호 지연, 보안성 문제, 고비용과 같은 단점이 있으며, 무선통신은 간섭, 제한된 대역폭, 지리적 제한 등의 단점을 가지고 있다.

2.1 현재 시스템의 취약점과 과거 사례

위성통신은 외부 신호 교란에 취약할 수 있으며, 과거 우크라이나 사태에서 GPS 신호와 상업용 위성통신이 교란된 사례가 있었다[8]. 또한 무선통신 네트워크의 취약점으로는 해킹, 데이터 유출, 네트워크 침입 등이 있으며, 이는 사이버 공격 기법의 진화와 연관이 깊다[9]. 미국 GPS 시스템이 사이버 공격을 받은 사례는 이러한 시스템들의 취약성을 잘 보여준다[10]. 2023년 기준으로 위성통신 시스템과 무선통신 시스템의 취약점에 대한 사이버 공격 사례를 살펴보면 다음과 같다.

2.1.1 위성통신 시스템에 대한 사이버 공격 사례

위성 해킹은 실제로 발생 가능한 사이버 위협이다. 위성 시스템은 국방, 외교, 안보 분야의 핵심 자산이 되었기 때문에 전 세계 여러 국가들이 위성 전용 보안 정책과 기술을 개발하고 있다. 위성 시스템에 대한 사이버 공격은 주파수 대역에 간섭 신호를 방사하는 주파수 재밍, 민감한 데이터 도청, 비인가자의 위성 신호 도용, 데이터 불법 변경 또는 허위 데이터 전송, 탈취한 신호 재전송 등의 형태로 발생할 수 있다. 실제로, 러시아 군용 통신 위성과 위성통신 업체 비아샛이 악성 소프트웨어를 이용한 해킹을 당한 사례가 있었다. 이와 함께 위성 항법 시스템 탈취로 테슬라의 레벨2 자율주

〈표 1〉 위성통신과 무선통신의 특징

구분	위성통신	무선통신
공통점	정보 전송에 전파 사용	정보 전송에 전파 사용
차이점	우주에 위치한 위성을 이용 대부분 장거리, 광역 커버리지	지상 기반 장비 이용 주로 근거리, 지역적 커버리지
장점	광범위한 지역 커버리지 지형에 구애받지 않음	설치와 유지보수가 상대적으로 간단 빠른 데이터 전송 속도, 안정적 연결
단점	신호 지연, 보안성 문제, 전파 간섭 문제 고비용, 불안정한 데이터 전송 속도	간섭, 제한된 대역폭, 보안 문제 지리적 제한 (신호 범위 내에서만 사용 가능)

행 차량 오동작을 유도하는 시도도 있었다[11].

2.1.2 무선통신 시스템에 대한 사이버 공격 사례

최근 랜섬웨어, 가상화폐, 국가 안보는 사이버 보안의 주요 키워드로 부각되었다. 랜섬웨어 그룹의 활동은 개인, 기업, 국가 안보, 글로벌 경제시장에 영향을 미쳤으며, 러시아와 미국 및 서방 국가 간의 이해충돌은 사이버 보안에 새로운 도전을 제시했다. 러시아의 우크라이나 침공은 물리적 충돌과 사이버 공격이 결합된 하이브리드 전쟁의 사례로, 다양한 분야에서의 사이버 공격 효과가 나타났다[12]. 서비스형 랜섬웨어(RaaS)의 출현은 사이버 범죄의 전문화와 조직화를 촉진했으며, 공공, 금융, 제조, 교육, 국방 등 다양한 산업에 대한 공격이 확대되었다. 공급망 공격의 증가 추세는 Microsoft Exchange Server 취약점, Solarwinds 해킹, Kaseya 사례 등을 통해 공급망 보안의 중요성을 강조했다. 이러한 사이버 공격 사례들은 위성통신 및 무선통신 시스템의 취약점을 이용하며, 국가 안보, 사회기반시설, 경제적 안정성에 직접적인 영향을 미치고 있다. 이는 지속적인 대응과 보안 강화의 필요성을 시사한다. 다음의 <표 2>는 위성 통신 및 무선통신을 대상으로 하는 다양한 사이버 공격 유형과 이러한 공격에 대처하기 위한 보안 대책들을 요약하여 보여준다.

<표 2>에서 보는 바와 같이 위성 통신과 무선통신이 공통적으로 직면할 수 있는 사이버 공격 유형들에 대해서 각 통신 방식에 특화된 대응을 해야 한다. 두 시스템 모두 공통적인 위협에 직면할 수 있으나, 위성 통신의 경우 우주 환경과 같은 특별한 요소들을 고려해야 하고, 무선통신은 더 다양한 형태의 네트워크 침입과 인프라 공격에 노출될 수 있다. 따라서, 각각의 시스템에 적합한 보안 대책을 수립하는 것이 중요하다.

2.2 적성국의 사이버공격 유형 및 가능한 시나리오

적성국은 위성통신과 무선통신 시스템을 대상으로 한 다양한 형태의 사이버 공격을 시도할 수 있으며, 이는 국가 안보에 직접적인 위협이 될 수 있다. 이러한 공격에는 신호 교란, 데이터 해킹, 서비스 거부 공격(DoS) 등이 포함될 수 있다. 예를 들어, 북한의 정찰총국이나 라자루스와 같은 조직은 사이버전을 통해 타국의 통신 시스템에 침입하고, 이를 통해 정보를 유출하거나 군사적 목적으로 신호를 방해하는 등의 활동을 할 수 있다.

〈표 2〉 위성 통신에 대한 사이버 공격 유형과 그에 대한 대응 방안

사이버 공격 유형	일반적 대응방안	위성 통신 대응방안	무선통신 대응방안
신호 방해 (Jamming)	간섭 회피 기술 사용	주파수 이동 (Frequency Hopping)	신호 강도 강화
스푸핑 (Spoofing)	암호화된 신호 사용	위성 위치 인증 메커니즘	강력한 인증 프로토콜 적용
트래픽 분석 (Traffic Analysis)	트래픽 패턴 마스킹	랜덤 트래픽 생성	네트워크 트래픽 암호화
네트워크 침입 (Network Intrusion)	침입 탐지 및 방지 시스템 (IDS/IPS)	추가적인 물리적 보안 조치	다중 계층 보안 (Multi-Layer Security)
서비스 거부 공격 (DoS/DDoS)	분산 서비스 거부 (DDoS) 대응 전략 구축	대역폭 확장 및 관리	탄력적 네트워크 인프라 구축
물리적 공격 및 파괴 (Physical Attack)	물리적 보안 강화 및 감시 체계 구축	위성 장비의 강화된 보호 설계	무선통신 장비의 보안 강화

국가 간의 갈등 상황에서는 통신 시스템을 통한 정보 유출이나 군사적 목적을 위한 신호 방해가 더욱 증가할 가능성이 높다[13]. 위성통신과 무선통신의 중단은 국가의 중요한 인프라 및 서비스에 심각한 영향을 미치며, 이는 국가 안보를 심각하게 위협할 수 있다. 이러한 위협에 대응하기 위해서는 탈린 메뉴얼과 같은 국제적인 사이버전 법률 및 규범을 참고하여 효과적인 대응 전략을 수립하고 실행하는 것이 중요하다. 따라서, 위성통신 및 무선통신 시스템의 보안을 강화하는 것은 국가 안보를 보장하는데 필수적이다[14-15]. 이를 위해서는 지속적인 보안 평가, 기술적 대응 전략의 개발 및 업데이트, 그리고 국제 협력을 통한 정보 공유와 공동 대응이 필요하다. 이러한 조치들은 사이버 위협을 효과적으로 관리하고, 국가 안보를 보호하는 데 있어 중요한 역할을 한다. 다음의 <표 3>은 적성국이 위성통신 및 무선통신 시스템을 대상으로 수행할 수 있는 다양한 사이버공격 유형과 시나리오를 나타낸다. 이러한 공격에는 신호 교란, 데이터 해킹, 서비스 거부 공격(DoS) 등이 포함되며, 이들은 국가 안보와 중요 인프라에 직접적인 영향을 미친다[16-18]. 국가 간 갈등이나 군사적 목적을 위한 신호 방해의 가능성은 통신 시스템의 보안 취약점을 드러내며, 이에 대한 적절한 대응과 보안 강화 조치가 필수적이다.

3. 고도화된 사이버 위협과 탐지 기술

사이버공격 탐지는 현대의 사이버 보안 분야에서 매우 중요한 위치를 차지하고 있다. 최신 기술과 방법론의 발전은 사이버 위협에 대응하는 데 필수적인 요소로 자리 잡았다.

3.1 최신 사이버공격 탐지 기술 및 방법론

위성통신과 무선통신 분야에서는 네트워크 트래픽 분석과 행위 기반 탐지를 통해 사이버 보안을 강화하고 있다. 이들 기술은 네트워크 유입 트래픽을 분석해 해킹을 탐지하고 대응하며, 빅데이터, 딥러닝, 인공지능을 결합해 정교한 보안 체계를 구축하고 있다. 또한, SUN 무선 센서 네트워크와 원거리 무선통신을 활용한 스마트 시티 기술 개발에 기여하고 있다. <표 4>에서는 이러한 사이버공격 탐지 기술을 요약하고 있다. <표 4>에서 보는 바와 같이 위성통신과 무선통신 분야에서 사용되는 주요 사이버공격 탐지 기술은 고급 네트워크 모니터링, 이상 징후 탐지 시스템, 그리고 인공지능 및 머신 러닝을 기반으로 한 탐지 알고리즘

〈표 3〉 적성국의 사이버공격 유형 및 시나리오

사이버공격 유형	설명	영향 및 중요성
신호 교란	통신 신호를 방해하여 정상적인 운영을 저해하는 공격.	국가 안보와 관련된 중요한 통신이 방해 받을 수 있음.
데이터 해킹	정보를 불법적으로 접근하거나 조작하는 공격.	정보 유출로 인한 보안 위협이 증가함.
서비스 거부 공격 (DoS)	대량의 트래픽을 발생시켜 정상적인 서비스 제공을 방해하는 공격.	필수적인 서비스와 인프라에 심각한 영향을 미칠 수 있음.
정보 유출	적성국이 통신 시스템을 통해 중요한 정보를 빼내는 행위.	국가의 기밀 정보가 외부로 유출되는 위험 존재.
군사적 목적의 신호 방해	국가 간 갈등 상황에서 특정 목적을 위해 통신 시스템의 신호를 방해하는 행위.	군사 작전의 효율성 저하 및 안보 위협 증가.
위성통신 및 무선통신 보안 강화	위성통신 및 무선통신 시스템의 보안을 강화하는 조치.	국가 안보를 보장하고 중요 인프라를 보호하는데 필수적임.

〈표 4〉 위성통신과 무선통신 분야의 사이버공격 탐지 기술

분야	기술적 적용	목적 및 기능
위성통신	트래픽 분석, AI 기술 적용	이상 징후 수집 및 분석, 해킹 침해 탐지 및 대응
무선통신	빅데이터, 딥러닝 기술 적용	보안 체계 강화, 실시간 모니터링, 스마트 시티 기술 개발 지원

을 포함한다. 이 기술들은 무단 접근, 데이터 유출, 및 기타 사이버 위협을 식별하고 대응하는데 중요한 역할을 한다.

3.2 암호화, 인증, 네트워크 모니터링 방법론

사이버 보안에서 암호화, 인증, 네트워크 모니터링은 중요한 역할을 한다. 암호화는 민감한 정보를 변조하기 어려운 형태로 바꾸어 데이터 기밀성을 유지한다. 예를 들어, 공개 키 암호화는 메시지를 안전하게 전송하는 데 사용되며, 금융 거래부터 전자 메일 보안에 이르기까지 다양한 분야에서 활용된다. 인증은 사용자의 신원을 확인하고 액세스 권한을 부여하는 과정이다. 다단계 인증은 해킹과 같은 무단 액세스를 방지하는 데 효과적이며, 금융 서비스와 기업 네트워크에서 널리 사용된다. 네트워크 모니터링은 활동을 감시하고 분석하여 보안 위협을 식별한다. 이상 징후 탐지 시스템은 비정상적인 활동을 조기에 감지한다. 이 방법론들은 상호 보완적으로 작용하여 포괄적인 보안 체계를 구축하는 데 기여한다.

3.3 인공지능 및 머신러닝을 활용한 사이버 위협 분석 사례

인공지능(AI)과 머신러닝(ML)은 사이버 보안 분야에서 중요한 역할을 하고 있다. 이 기술들은 대규모 데이터 분석, 복잡한 패턴 인식, 예측 모델링을 통해 보안 위협 탐지와 대응을 개선한다. 머신러닝 알고리즘은 기존의 사이버 공격 패턴을 학습하여 새로운 공격 유형을 예측하고, 네트워크 트래픽 분석을 통해 비정상적인 데이터 흐름을 감지한다. 이는 기업이나 금융기관의 데이터 보호에 중요하다. AI와 ML은 또한 피싱 공격 식별 및 차단에도 활용된다. 예를 들어, Palo Alto Networks와 같은 보안 솔루션 제공업체들은 AI와 ML을 활용하여 사이버 위협을 효과적으로 탐지하고 대응한다. 이 기술들은 또한 사이버 보안 분야에서의 자동화와 효율성 증대에 기여하며, 전문가들이 더 중요한 과제에 집중할 수 있게 한다.

이와 같은 고도화된 사이버 위협 탐지 기술은 지속적인 발전과 혁신을 통해 사이버 공간의 안전을 확보하는 데 중요한 역할을 하고 있다. 이러한 기술들의 발전은 사이버 보안의 미래를 밝히는 중요한 열쇠가 될 것이다.

4. 사이버 보안 강화 전술 및 기술적 대응 전략

위성통신 및 무선통신 시스템의 보안 강화는 사이버 안보의 핵심 요소로, 전술적 및 기술적 대응 전략의 개발이 필수적이다. 이러한 전략은 광범위한 위협에 대응하고, 효과적인 보안 체계를 구축하기 위한 핵심적인 부분이다.

4.1 전술적 접근

위성통신 및 무선통신 시스템의 보안 강화를 위한 전술적 접근 방법은 다양한 위협으로부터 통신 인프라를 보호하는 데 중점을 둔다. 이러한 접근 방식에는 몇 가지 중요한 요소가 포함된다.

4.1.1 위험 평가 및 감시

첫 단계는 위협과 취약점을 정확하게 파악하는 것이다. 이를 통해 특정 위험에 대한 대비책을 마련할 수 있으며, 시스템이 어떤 공격에 취약한지를 파악할 수 있다. 다음의 <표 5>은 위험 평가 및 감시 과정에서 중요한 단계들을 정리해 놓은 것으로, 각 단계에서 필요한 활동과 목표를 설명하고 있다. 이 표는 위험을 체계적으로 식별, 평가, 감시하고 이에 대응하는 과정을 단계별로 구체화하여 보여준다.

4.1.2 데이터 암호화

위성통신 및 무선통신에서 데이터 암호화는 보안을 강화하는 핵심적인 요소이다. 암호화는 제3자로부터 데이터 도청을 방지하고, 데이터 무결성을 유지하여 변조를 방지한다. 이렇게 함으로써 통신 네트워크의 안정성과 신뢰성을 확보할 수 있다. 따라서 위성통신 및 무선통신 분야에서는 데이터 암호화 기술의 중요성이 더욱 부각된다.

4.1.3 네트워크 접근 제어

네트워크 보안의 중요성을 강조하고 있다. 엄격한 인증 및 권한 부여 절차는 무단 접근을 예방하며, 더 높은 수준의 네트워크 보안을 제공한다. 이러한 절차는 사용자와 장치가 신뢰할 수 있는지 확인하고, 필요한 권한만 부여하여 데이터 및 시스템의 안전성을 유지한다. 이는 방어 산업과 같이 민감한 분야에서 특히 중요한데, 정보 유출 및 해킹으로부터 보호하기 위해 필수적이다.

4.1.4 지속적인 모니터링 및 대응

보안 시스템의 효과를 지속적으로 모니터링하는 것은 중요하다. 이를 통해 시스템의 작동 상태를 실시간으로 파악하여, 어떠한 문제가 발생하더라도 빠른 조치를 취할 수 있다. 또한, 위협이 발견되었을 때 신속하게 대응함으로써 중요한 정보나 시스템을 보호할 수 있다. 이러한 신속한 대응은 잠재적인 보안 사고의 효과적인 예방과 조기 탐지를 가능하게 한다. 따라서 보안 시스템을 효과적으로 관리하고 감시하는 것은 모든 조직에게 필수적인 요소이다.

4.1.5 보안 업데이트 및 유지보수

위성통신 및 무선통신 시스템의 정기적인 업데이트는 매우 중요하다. 이것은 현대 전자전에서 핵심적인 역할을 한다. 첫째, 보안 패치와 소프트웨어 업데이트를 통해 시스템의 취약성을 최소화할 수 있다. 이는 위협에 대한 강력한 방어를 제공한다. 둘째, 새로운 기술과 표준을 통합하여 효율성을 향상시킬 수 있다. 이것은 통신 시스템의 성능을 향상시키며 새로운 기회를 창출한다. 따라서 시스템의 정기적인 업데이트는 보안과 성능 개선을 위해 필수적이다.

〈표 5〉 위험 평가 및 감시의 중요 단계

단계	설명
위협 식별	현재 및 잠재적 위협 파악 (해킹, 물리적 침입, 소프트웨어 취약점 등 포함)
취약점 분석	시스템의 취약한 부분 찾기 (소프트웨어, 하드웨어, 프로세스, 인적 요소 검토)
위험 평가	위협과 취약점을 바탕으로 위험 수준 결정 (위협 가능성과 영향 평가)
모니터링 및 경보 시스템	지속적인 감시 및 경보 메커니즘 구축 (비정상 활동과 잠재적 위협 감지)
지속적인 개선	보안 환경 변화에 따른 위험 평가 및 감시 방법의 지속적인 개선

4.2 기술적 솔루션

4.2.1 암호화 기술의 발전

암호화 기술은 현대 정보 보안에서 중요한 역할을 한다. 이 기술은 데이터의 기밀성을 보호하여 무단 접근으로부터 보호하고, 데이터의 무결성을 유지하여 변경 또는 변조로부터 방지한다[19]. 특히, 퀀텀 컴퓨팅의 발전으로 인해 고전적인 암호화 방법들이 취약해질 우려가 있으므로, 현대 암호화 기술은 퀀텀 컴퓨팅에 대응할 수 있는 수준으로 발전해야 한다. 이는 미래의 정보 보안을 위해 매우 중요한 과제 중 하나이다.

4.2.2 효과적인 네트워크 모니터링 시스템 구축

실시간 네트워크 모니터링과 데이터 분석은 정보 보안을 강화하기 위한 필수적인 단계이다. 이를 통해 비정상적인 트래픽 패턴을 식별하고 대응함으로써, 잠재적인 위협을 미리 탐지할 수 있다. 또한, 이러한 접근 방식은 네트워크 활동에 대한 투명성을 제공하며, 보안 사고의 효과를 최소화하는 데 도움이 된다. 더불어, 이러한 실시간 감시와 분석은 조직의 데이터 자산을 보호하고 비인가된 액세스를 방지하는데 중요한 역할을 한다. 따라서 네트워크 보안에 있어서 이러한 접근 방식은 반드시 필요한 단계이다.

4.2.3 무선통신 시스템의 안전한 아키텍처 설계

무선통신 시스템의 아키텍처는 공격에 대한 내성을 가질 수 있도록 설계되어야 한다. 이는 통신망의 분산화, 중요 데이터의 분산 저장, 장애 허용 시스템 설계 등을 포함할 수 있다.

4.3 다층적 방어 전략 및 장기적 보안 체계 구축

다층적 방어 전략은 다양한 보안 계층을 통합하여 전체 보안 체계를 강화하는 방법으로, 단일 솔루션에만 의존하지 않는다. 이 전략은 공격자가 방어를 우회하거나 해체하기 어렵게 만들기 위해 지속적인 위협 평가, 기술 업데이트, 인원 교육 및 정책 개정을 포함한다. 네트워크, 애플리케이션, 물리적 보안을 통합하고, 방화벽, 침입 탐지 시스템, 암호화 등 다양한 보안 요소를 운용해야 한다. 이와 더불어, 정부, 산업, 학계 간의 협력은 정책 개발과 기술 표준 설정에서 중요하다. 국제적 협력 및 표준화를 통한 지속 가능한 보안 체계 구축은 위성통신 및 무선통신 시스템의 보안을 강화하고 사이버 위협에 대응하는 데 필수적이며, 국가 안보에 중요한 역할을 한다[19]. 대한민국 합동참모본부에서 사이버 경보 체계를 인포콘(Infocon)에서 CP콘(Cyber Protection Condition)으로 변경하고, 국가정보원의 NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) 가입은 대한민국이 사이버 공간에서의 적성국의 공격에 대응하기 위한 정부 차원의 국제 공조 및 세계적인 공동 대응 노력을 강화하는 중요한 전략적 움직임이다.

5. 정책 제안 및 미래 전망

정부와 관련 산업 간의 협력은 사이버 보안을 강화하기 위한 기반을 제공한다. 이를 위해, 정부는 다부처 간 협력 체계를 강화하여 사이버 보안 문제에 통합적으로 대응해야 한다. 이를 통해 정보 공유, 정책 조정 및 자원 배분의 효율성을 높일 수 있으며, 더욱 강력한 보안 체계를 구축할 수 있다[20]. 또한, 정부와 산업계는 보다 넓은 관점에서 협력하여 사이버 보안 인식을 높이고 관련

교육 프로그램을 확대해야 한다. 이는 사용자의 보안 행동을 개선하고 전반적인 보안 문화를 조성하는 데 중요한 역할을 한다.

미래 사이버 보안 환경을 예측하고 대응 전략을 수립하는 것은 매우 중요하다. 미래의 사이버 위협을 예측하고 분석하는 연구를 강화하여 미래 사이버 보안 환경을 이해하고 적절한 대응 전략을 마련해야 한다[21]. 또한, 끊임없이 변화하는 사이버 보안 환경에 적응하기 위해 유연한 사이버 보안 기술의 개발이 필요하다. 이는 인공지능과 머신러닝을 활용한 자동화된 위협 탐지 및 대응 시스템 개발을 포함하며, 보다 효과적인 사이버 보안 대책을 구축하는 데 기여할 수 있다[23].

기술 혁신은 사이버 보안을 변화시키고 있으며, 이에 맞춘 정책의 개발이 필요하다. 기술 발전과 정책의 조화는 사이버 보안의 지속 가능성을 보장하는 핵심 요소이다[24]. 또한, 장기적인 관점에서 전략을 수립하여 글로벌 사건이 사이버 보안 환경에 미치는 영향을 고려해야 한다. 이를 통해 미래의 다양한 도전에 대비하는 강력하고 유연한 보안 체계를 마련하는 것이 중요하다.

정부와 산업계의 협력, 미래 사이버 보안 환경의 예측 및 대응 전략, 그리고 기술 혁신과 정책의 조화는 사이버 보안의 미래를 위한 중요한 축이다. 이러한 요소들은 통합적인 접근을 통해 사이버 보안의 지속 가능성을 보장하고, 국가 안보를 강화하는 데 기여할 것이다.

6. 결 론

위성통신과 무선통신 시스템의 보안 강화는 적성국의 사이버 공격에 대응하는 데 필수적이다. 이를 위해 첫째, 인공지능과 머신 러닝을 활용한 첨단 사이버 보안 기술 개발과 신속한 대응 메커니즘 구축이 중요하다. 둘째, 글로벌 사이버 보안 협력과 정보 공유를 통한 국제적 위협 인식과 협력 체계 구축이 필요하다. 셋째, 정부, 산업계, 학계 간 협력을 강화하고 사이버 보안 인력 양성 및 교육에 주력해야 한다. 마지막으로, 지속적인 보안 평가와 시스템 업그레이드를 통해 취약점을 식별하고 해결하는 것이 중요하다. 이러한 전략적 접근을 통해 시스템 보안을 강화하고 사이버 공격에 대응할 수 있다.

참 고 문 헌

[1] K. C. Woo and C. Polito, "The Evolution of North Korean Cyber Threats," The Asan Institute for Policy Studies, Feb. 20, 2019.

[2] E. M. Lederer, "UN probing 35 North Korean cyberattacks in 17 countries," AP News, The Associated Press, Aug. 13, 2019.

[3] S. M. Oh, "N. Korea intensifying cyber attacks against S. Korean shipbuilders: spy agency," Yonhap News Agency, Oct. 4, 2023.

[4] M. H. Jung, "Experts warn of North Korea's evolving cyberattack capabilities," _The Korea Times_, Aug. 30, 2022.

[5] "North Korea Cyber Threat Overview and Advisories," Cybersecurity & Infrastructure Security Agency (CISA), Dec. 3, 2023.

[6] M. Nichols, "North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report," Reuters, Aug. 5, 2019.

[7] S. Joo, S.-Y. Kim, and I.-G. Lee, "차세대 무선통신 네트워크 기술 동향 및 보안 이슈 분석," Review of KIISC, Korea Science, Jun. 30, 2021.

[8] S. Park, "[우주산업 리포트]인공위성 겨냥한 사이버 공격이 현실화되고 있다," DongA Science, Mar. 25, 2022.

[9] H.S. Yoon, M.W. Yun, Joshua Freilich, Steven Chermak, Robert G. Morris, and I. S. Kim, "Cyberterrorism : Trends and Reponses," Korean Institute of Criminology and Justice, Dec., 2012.
[10] Ministry of National Defense, "해군지휘통제체계 성능 고도화 및 발전방안," Republic of Korea Navy Education Command, School of Information and Communications, Dec. 2012.
[11] H. Song, "위성 해킹, 이미 시작됐다. 핵심 보안 기술 조속히 확보해야," Newsis, Dec. 3, 2023.
[12] "2023년 사이버 보안위협 및 대응기술 전망," Security & Intelligence, Igloo Corporation, 2023.
[13] Y. K. Jin, Y. J. Kim, J. S. Lee, and C. S. Choi, "디지털 안심국가 실현을 위한 중장기 로드맵," DUDUIT Co., Ltd., KISA, Dec. 8, 2021.
[14] "인공위성과 사이버 안보," SPACE ISSUE No. 20, 항공우주연구원 미래전략본부, May 8, 2015.
[15] G. Y. Moon, “Attacks on Satellite Communication Systems Are Actually Happening,” Boannews, Aug. 10, 2018.
[16] Y. Jung-Ho, K. Yoon-Sun, O. Jin-Young, L. Joo-Ho, "Methods and Devices for Signal Transmission and Reception in a Satellite Communication System," KR20210133109A, filed Nov. 24, 2020, and published Nov. 5, 2021.
[17] P. Kim, J. Yoo, and W. Byun, "Research Trends in Global Wireless Communication Technology Based on the LEO Satellite Communication Network," in Electronics and Telecommunications Trends, vol. 35, no. 5, pp. 83-91, Oct. 01, 2020.
[18] G. Shibuya, "위성통신을 이용한 효율적 원격감시시스템," 계장 (A025), vol. 46, no. 15, pp. 54-58, 2003.
[19] A. Scrase and K. C. Koo, "Cybersecurity for Consumer IoT Standardisation and De-identifications solutions," ETSI and TTA Webinar, Nov. 10, 2021.
[20] D. Kim, I. Choi, E. Lee, H. Cho, and W. Jang, "2030 Future Society Change and Cyber Threat Forecast Study," Nexintelligence Inc., KISA, Dec. 2021
[21] D. Lee, "Cybersecurity Technology and Standardization Trends in the Pandemic Era," in Convergence Research Review, Nov. 2022.
[22] C. Park and H. Yim, "10 Emerging Technologies in the Era of Data Security," KISTEP Brief, 2023.
[23] J. S. Lee, S. M. Choi, C. M. Ahn, and Y. Yoo, "Trends and Implications of Cybersecurity Policies in Major Countries," Electronics and Telecommunications Trends, 2023.
[24] A. Kim, '[2023 AI Security Monitoring Report] A Major Counterattack on Security Threats with ChatGPT, the Hot AI Technology,' Boannews, Jun. 30, 2023.

저 자 약 력

정 진 우

이메일 : jinwoo.jeong@lignex1.com

- 1999년 한양대학교 전자통신공학과 (공학사)
- 2001년 한양대학교 전자통신공학과 (공학석사)
- 2016년 한양대학교 전자통신공학과 (공학박사)
- 2001년~2007년 LG전자 디지털미디어연구소 선임연구원
- 2016년~2017년 한양대학교 신호정보특화연구센터 연구교수
- 2017년~2022년 국방정보본부 OOO사령부 OO팀장
- 2023년~현재 LIG넥스원 사이버전자전개발단 수석연구원
- 관심분야 : 신호정보, 사이버전자전, 안티드론 시스템, 위성통신, 무선통신

윤 상 범

이메일 : sangbom.yun@lignex1.com

- 1999년 고려대학교 제어계측공학과 (공학사)
- 2002년 고려대학교 전기공학과 (공학석사)
- 2002년~현재 LIG넥스원 사이버전자전개발단 수석연구원
- 관심분야 : 신호정보, 사이버전자전, 안티드론 시스템, 위성통신, 무선통신