Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 7 pp. 474-481, 2023

https://doi.org/10.5762/KAIS.2023.24.7.474
ISSN 1975-4701 / eISSN 2288-4688

국내 테러 대응체계 및 개선방안에 관한 연구
-사이버테러를 중심으로-

전태식, 김찬우*, 류연승
명지대학교 보안경영공학과

A study on domestic terrorism response system and improvement plan
-Focusing on cyber terrorism-

Tae-Sik Jeon, Chan-Woo Kim*, Yeon-Seung Ryu
Department of Security Management Engineering, Myongji University

요 약 현대 사회에서 심각한 보안 위협으로 인식되고 있으며, 국가 안보와 개인정보 보호에 막대한 영향을 미칠 수 있다. 사이버테러(Cyberterrorism)는 컴퓨터 기술 및 인터넷을 악용하여 사회, 정치, 경제 등을 목적으로 하는 공격 활동으로, 컴퓨터 및 네트워크 시스템을 공격하여 정보의 손상, 삭제, 유출 등을 행하는 범죄 행위를 의미한다. 국내 사이버테러 대응체계를 갖추고 있지만, 계속해서 진화하는 사이버 위협에 대응하기 위해 개선이 필요하다. 본 연구는 국내 사이버테러 대응체계와 개선 방안을 중심으로 연구하였다. 사이버테러의 정의, 특징, 종류, 그리고 국내외 사이버테러 사례를 분석하였다. 또한, 국내외 대응체계의 문제점과 한계를 분석하였다. 이를 바탕으로 국내 사이버테러 대응체계가 일부 성과를 보여주었으나 여전히 개선이 필요한 상황임을 확인하였다. 기관 및 조직 간 협력 강화, 기술적 대응 역량 강화, 전문인력 확보 등의 방안이 필요하다는 결론을 도출하였다. 국내 사이버테러에 대응하기 위한 체계적이고 효과적인 대응 방안을 모색하는 데 기여할 것으로 기대된다.

Abstract Cyberterrorism is recognized as a serious security threat in modern society and can have a huge impact on national security and privacy. Cyberterrorism is an attack activity for social, political, economic, or other purposes using computer technology and the Internet. Although a domestic cyberterrorism response system is in place, it needs improvement to respond to continuously evolving cyber threats. This study focused on the domestic cyberterrorism response system and an improvement plan. The definition, characteristics, types of cyberterrorism, and cases of domestic and foreign cyberterrorism were analyzed. In addition, the problems and limitations of domestic and foreign response systems were analyzed. Based on this, it was confirmed that the domestic cyberterrorism response system showed some achievements, but it still needs improvement. It was concluded that measures such as strengthening cooperation between institutions and organizations, strengthening technical response capabilities, and securing professional manpower are necessary. This study is expected to contribute to finding systematic and effective countermeasures to respond to domestic cyberterrorism.

Keywords : Cyberterrorism, Response System, Strengthening Capacity, Coordination, Professional Agencies

*Corresponding Author : Chan-woo KIm(Myongji Univ.)
email: chan_woo_kim@naver.com
Received May 2, 2023 Revised May 30, 2023
Accepted July 7, 2023 Published July 31, 2023

1. 서론

현재 국내에서는 사이버테러가 계속해서 발생하고 있으며, 이에 대한 대응체계와 방안이 필요하다는 요구가 제기되고 있다. 선행 연구에서는 사이버위협의 예측을 위해 머신런닝과 인공지능 기반의 휘협 인지 시스템을 개발하고, 취약점 분석을 위한 자동화 도구와 사전예방을 위해 새로운 인증 기술 및 암호화 알고리즘이 개발과 적용에 대한 연구가 진행되었으며, 특히 블록체인 기술을 활용한 분산형 보안 시스템에 대한 연구가 주목받았다. 또한 국민 대상으로 사이버안전 교육 및 인식 제고를 위한 국가 차원의 캠페인과 교육 프로그램에 대한 효과성 평가 및 개선 방안에 대한 연구가 이루어졌다[1]. 특히 최근에는 코로나19 대응을 위한 온라인 업무 증가와 함께 사이버공격이 증가하는 등 사이버보안의 중요성이 한층 더 부각 되었다. 따라서 본 연구는 국내에서 발생한 사이버테러 사례를 분석하고, 이를 바탕으로 효과적인 대응체계와 방안에 대한 제언을 제시하여 국내 사이버보안의 수준을 높이고자 한다. 사이버테러는 컴퓨터와 인터넷 등의 정보통신 기술을 이용하여 다양한 형태로 발생할 수 있으며, 이는 국가, 기업, 개인 등 모든 사람들에게 위협을 제공한다[2]. 이러한 사이버테러의 증가로 인해 사이버보안 분야에서는 다양한 대응체계와 방법을 개발하고 있다[3].

기존 연구에서는 사이버테러에 대한 개념, 형태, 대응방안 등에 대해 다양한 분석과 연구가 이루어졌다. 최근에는 머신러닝, 딥러닝, 블록체인 등의 새로운 기술을 활용한 사이버보안 대응 방안에 대한 연구도 활발히 이루어지고 있다. 하지만 국내에서는 사이버테러에 대한 이론적 연구와 분석이 부족한 실정이다[4]. 이러한 상황에서는 국내에서 발생한 사이버테러 사례와 이를 대응하는 체계에 대한 연구가 더욱 필요하며, 이를 토대로 국내 사이버보안 대응체계를 개선해 나가는 것이 중요하다. 현재 국내에서는 국가정보원, 국방부, 경찰청 등에서 사이버테러 대응을 위한 조직 및 시스템을 운영하고 있지만, 여전히 사이버테러가 지속적으로 발생하고 있으며, 대응체계 개선이 요구되고 있다. 따라서 본 연구는 국내에서 발생한 사이버테러 사례와 관련된 보도 자료와 보안 업체의 보고서 등을 수집하여 분석하고, 이를 통해 국내에서 발생한 사이버테러의 유형과 특징, 대응방안 등을 파악하고, 이를 토대로 대응체계와 방안에 대한 제언을 수립할 것이다. 또한, 사이버테러를 중심으로 국내외 테러 대응체계를 분석하고 개선방안을 제시함으로써, 국내 사이버테러 대응체계를 수립하는데 도움이 되고자 한다.

본 논문의 구성으로는 먼저, 사이버테러의 개념과 종류에 대해 알아보고, 국내외 사례 연구를 통해 현재의 사이버테러 현황을 파악할 것이다. 그다음으로 국내외 사이버 대응체계에 대해 살펴보고, 구성 요소와 정부 기관의 역할에 대해 논의할 것이다. 이어서, 현재 대응체계의 한계와 문제점을 파악하고, 개선방안을 제시할 것이다. 또한, 국제 협력을 강화하는 방안에 대해서도 고려할 것이다. 마지막으로, 국내 사이버테러 대응체계 개선을 위한 제언과 시사점을 제시할 예정이다.

2. 이론적 배경

2.1 사이버테러의 종류와 개념

사이버테러는 여러 가지 형태로 나눌 수 있지만, 대표적인 종류로는 다음과 같다.

Table 1. Types of Cyber Terrorism[5]

Specialized Attack Types	Target	Method	Nature
Social Engineering Attacks	Individuals, Organizations	Manipulation, Deception	Human-based, Psychological
Zero-Day Exploits	Software, Systems	Exploitation of Unknown Vulnerabilities	Technical
Ransomware Attacks	Individuals, Organizations	Encryption, Extortion	Financial, Disruptive
Advanced Persistent Threats (APTs)	Governments, Enterprises	Covert Intrusions, Stealth Persistence	Coordinated, Persistent
IoT Security Challenges	Internet of Things (IoT) Devices	Device Exploitation, Network Breaches	Connectivity, Privacy

사이버테러(Cyberterrorism)는 컴퓨터 기술 및 인터넷을 악용하여 사회, 정치, 경제 등을 목적으로 하는 공격 활동으로, 컴퓨터 및 네트워크 시스템을 공격하여 정보의 손상, 삭제, 유출 등을 행하는 범죄 행위를 의미한다[6]. 이러한 공격은 사람들의 생명과 안전, 국가 및 기업의 시설, 서비스, 시스템 등을 위협하고, 대규모 재난을 초래할 수 있으므로 매우 위험한 범죄 행위로 평가된다.

2.1.1 사이버테러의 위험성과 영향력

사이버테러의 위험성은 크게 두 가지 측면에서 나타난다. 첫째, 사이버테러는 국가 안보와 관련된 시설, 시스템, 정보 등을 공격할 수 있으며, 이로 인해 국가의 안전과 안정성에 심각한 위협을 준다. 둘째, 사이버테러는 기업의 경제적 이익과 개인의 프라이버시를 침해할 수 있으며, 이로 인해 개인과 기업의 자유와 권리에 대한 위협을 준다. 사이버테러가 가지는 영향력은 상당히 크다고 할 수 있다. 사이버테러가 발생하면 다음과 같은 영향이 생길 수 있다.

Table 2. The dangers and impact of cyberterrorism[7]

Risks and Impacts	Description
Economic Losses	Financial losses, decreased productivity, business disruption
Information Leakage	Exposure of confidential information, theft of personal information, violation of intellectual property rights
Infrastructure Destruction	Network, system, and service disruptions, targeting transportation, power, communication infrastructure
Political Influence	Fostering conflicts between nations, election interference, spreading disinformation, political turmoil
Social Disruption	Major service disruptions, societal unrest, hate speech, incitement activities
National Security Threats	Attacks on national facilities, military systems, leaking classified information
Cybercrime Linkages	Connections with cybercrime organizations, funding, technology transfers
Internet Trust Erosion	Exposing personal information, undermining user trust, fostering mistrust in cyberspace
Societal and Cultural Impacts	Manipulation of social and cultural influence, propaganda, incitement, political and religious issues
Personal and Organizational Threats	Defamation, targeting individuals and organizations, harassment
Cyber Warfare Potential	Possibility of cyber warfare between nations, threats to international relations and strategic security

2.2 국내 사이버테러 사례분석

2020년 9월 신한은행 서버에 대한 대규모 DDoS 이다. 이 공격은 전 세계적인 봇넷인 Mirai를 이용한 것으로 확인되었으며, 공격 시도가 몰려들면서 해당 은행 웹사이트와 모바일 앱이 접속 불가능한 상황이 지속된 적이 있었다. 이 공격은 국내 은행 업계에서는 최대 규모로 알려져 있으며, 국내 보안 업계에서도 이에 대한 대응에 매진하고 있다[8].

또한 2013년에 발생한 "DarkSeoul" 사이버 공격이다. 이 공격은 웜과 트로이 목마의 조합을 사용하여 한국의 여러 주요 은행과 미디어 조직을 대상으로 했다. 2013년 3월 20일에 여러 한국 은행과 미디어 회사가 컴퓨터 네트워크에 심각한 중단을 경험하면서 시작되었다. 북한과 관련이 있는 것으로 여겨지는 그룹에 의해 조작되었지만 사이버 공격에 대한 귀속은 어려울 수 있으며 지속적인 조사 및 분석의 대상이 될 수 있다. 공격의 첫 번째 단계는 "Jokra"로 알려진 웜의 배포와 관련이 있다. Jokra 웜은 대상 시스템에 감염되어 확산되었으며 주로 금융 및 미디어 부문 내의 서버를 대상으로 한다. 영향을 받는 시스템의 취약점을 악용하여 공격자가 무단 액세스 및 제어 권한을 얻을 수 있도록 했다. 공격의 두 번째 단계에서는 트로이 목마, 특히 "DarkSeoul" 악성코드의 변종을 사용했다. 트로이 목마는 악성 첨부 파일이나 링크가 포함된 스피어 피싱 이메일을 통해 유포되었다. 순진한 사용자가 첨부 파일이나 링크를 클릭하면 트로이 목마가 시스템을 감염시켜 공격자가 무단 액세스 권한을 얻고 추가 악의적인 활동을 수행할 수 있도록 한다. 이 공격은 대상 조직에 상당한 영향을 미치고 광범위한 혼란을 야기했다. 영향을 받은 은행은 장기간 서비스 중단을 경험하여 운영을 방해하고 고객에게 불편을 끼쳤다. 미디어 조직은 또한 방송 및 출판 시스템의 중단에 직면하여 뉴스 및 콘텐츠 전달 능력에 영향을 미쳤다. 또한, 중요 인프라 시스템의 취약성과 사이버 테러가 필수 서비스에 중대한 중단을 일으킬 가능성에 대한 우려를 불러일으켰다[9].

2.3 국외 사이버테러 사례분석

2021년 7월 Kaseya 사의 제로데이 취약점을 이용한 랜섬웨어 공격이다. Kaseya는 IT 관리 솔루션을 제공하는 미국 회사로, 이 공격으로 수많은 고객 기업의 시스템이 감염되어 데이터 유출과 함께 랜섬웨어로 암호화되었다. 이 공격은 러시아 기반 해커 그룹인 REvil이 주도한 것으로 추정되고, 약 7,000개 이상의 기업과 조직이 피해를 입었다[10]. 2021년 2월 마이크로소프트 엑스체인지 취약점을 이용한 중국 기반 해커 그룹인 Hafnium의 사이버 공격이 있다. 이 공격은 미국 정부 기관, 군사 및 국방업계, 학교 등 다양한 조직에 영향을 미쳤으며, 취약점을 이용해 이메일 서버에 대한 액세스 권한을 획득하여 이메일 내용을 열람하거나 탈취하는 등의 피해를 입혔다[11].

2021년 5월 7일에 일어난 미국 연방 정부 기관 및 기

업을 겨냥한 랜섬웨어 공격이다. 이 공격은 미국의 대형 파이프라인 운영 업체인 컬러스가 대상이 되었으며, 이 회사는 동부 지역의 연료 수송을 책임지는 중요한 회사 중 하나였다. 공격은 러시아 기반의 해커 그룹인 다크사이드(DarkSide)가 수행한 것으로 추정되며, 이 그룹은 파이프라인의 컴퓨터 시스템을 잠금 상태로 만들고 비트코인으로 $500만의 금전 보상을 요구했다[12]. 또 다른 사례로는 2021년 7월 2일 발생한 Kaseya 사의 소프트웨어 공급망 공격이 있다. 이 공격은 Kaseya의 소프트웨어를 이용하는 기업들을 대상으로 한 것으로, 이 공격으로 인해 수백 개의 기업이 데이터를 잃었거나 암호화됐다. 이 공격은 러시아 기반의 해커 그룹인 REvil이 수행한 것으로 추정되며, 이 그룹은 $7백만에 해당하는 금전 보상을 요구했다[13].

이러한 사례들은 보안 업계에서도 큰 관심을 받으며, 이를 막기 위한 대책들이 계속해서 연구 및 개발되고 있다. DDoS는 대부분의 기업, 기관들이 예방 및 대응할 수 있는 방법들이 존재한다. 이러한 방법들 중에는 서버, 네트워크의 보안 강화, 재해 복구 계획 수립 등이 있다. 랜섬웨어 공격은 백업과 같은 대비책과 함께 보안 강화가 필요하다. 또한, SQL 인젝션 공격과 같은 경우에는 웹 애플리케이션에서 보안 취약점을 최소화하고, 보안 업체나 전문가들의 조언을 받아 개선해야 한다. 또한, 개인정보 유출과 같은 사례는 보안 정책, 개인정보 보호법 등에 따라 기업, 기관들이 적극적으로 대응해야 한다. 기업이나 기관들은 보안 강화와 함께, 데이터 유출 시 발생하는 문제에 대비하여 신속하고 적극적인 대응 계획을 수립해야 한다. 최근 국내에서 발생한 사이버테러 사례들은 국내 보안 업계와 정부, 기업, 기관들의 보안 강화와 대응 계획 수립에 대한 필요성을 다시 한번 강조하고 있다. 이를 통해 국내 사이버 보안 수준을 높이는 노력이 계속되어야 한다.

2.4 사이버테러 대응 체계 분석

2.4.1 국내외 대응 체계 비교 분석

국내에서 DDoS, 랜섬웨어, 정보도용 등 다양한 형태의 사이버 위협에 대응하기 위해 사이버테러 종합대응체계를 구축했다. 한국 정부는 국가 차원에서 사이버 보안 및 사이버 테러 대응을 관리하는 전담 기관인 한국인터넷진흥원(KISA)을 설립하는 등 사이버 보안을 강화하고 대응 능력을 강화하기 위한 여러 조치를 시행했다[14].

또한 KISA는 사이버보안 사고대응센터(CIRC), 사이버위협분석과, 사이버보안 교육훈련과 등 사이버보안의 다양한 측면을 처리하기 위해 여러 부서를 신설했다. CIRC는 사이버 위협을 모니터링 및 분석하고 보안 사고에 대응할 책임이 있다. 사이버 공격이 발생할 경우 정부기관, 기업 및 대중에게 실시간 정보 및 기술 지원을 제공한다. 사이버 위협 분석 부서는 위협 평가를 수행하고 잠재적인 사이버 위협을 식별하는 일을 담당하며, 사이버 보안 교육 및 훈련 부서는 인식을 높이고 사이버 보안 기술을 향상시키기 위해 개인과 조직에 교육 및 훈련을 제공한다[15]. KISA 외에도 국가정보원, 경찰청, 국방부 등 다른 정부기관도 사이버테러 대응 활동을 하고 있다. 국정원은 사이버 위협과 관련된 정보를 수집·분석하고, 경찰청은 사이버범죄를 수사하고 사이버범죄자를 검거하는 업무를 담당한다. 국방부는 국방체계에 대한 사이버 공격을 방어할 책임이 있다[16].

전반적으로 국내에서는 강력한 사이버 테러 대응 체계를 구축하기 위해 상당한 노력을 기울였다. 그러나 사이버 공격의 복잡성과 정교함의 증가는 국가의 사이버 보안 방어에 지속적인 문제를 제기한다. 정부는 사이버 위협에 효과적으로 대응하기 위해 사이버 보안에 지속적으로 투자하고 국제 파트너와 협력해야 한다[17]. 전 세계 많은 국가들은 날로 증가하는 사이버 공격 위협에 대처하기 위해 사이버 테러 대응 체계를 구축하고 있다. 이러한 시스템에는 일반적으로 사이버 위협을 탐지, 방지 및 대응하기 위해 협력하는 정부 기관, 민간 부문 기관 및 국제 조직의 조합이 포함된다.

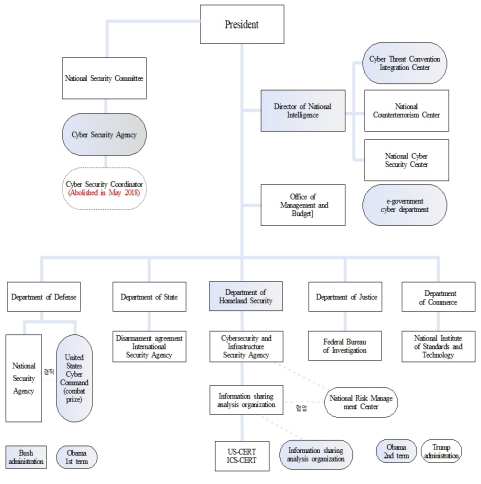

Fig. 1. U.S. cyber terrorism response organization system[18]

먼저 미국은 국가차원의 통합적 사이버안보 실무및 조정기구를 설치하고 있다. 2001년 9.11테러발생 이후「국토안보법(Homeland Security Act)」제정을 통해 신설된 행정부처인 국토안보부(DHS)에 물리적 시설 외에 사이버안보도 국가기반으로서 관리하도록 권한과 책임을 부여하였으며,나아가 대통령 직속의 기구 설치를 통해 범정부차원의 사이버안보 정책을 담당하고 있다[19]. 현재 대통령 직속기구로는 바이든정부 출범 이후「국방수권법(NDAA 2021)」개정을 통해 신설된 국가사이버실(ONCD)이 사이버안보 정책의 부처간 조정 역할을 수행하고 있다[20].

일본은 국가차원의 통합적 사이버안보 대응을 위해 내각에 조정기구를 설치하고 있다. 일본의 경우2014년 이전에는 훈령차원에서 사이버보안 분야는 개별 부처가 각각 주관하되, 부처간 조정 역할은내각의 사이버보안전략본부가 하도록 하였는데, 2014년「사이버보안기본법(サイバーセキュリティ基本法)」제정을 통해 훈령에 근거를 둔 사이버보안조직체계를 법률차원으로 격상시켰다[21].

영국은 개별부처 차원에서 공공 및 민간분야의사이버보안 정책을 수립·운영하고 있다. 즉 내각부(Cabinet Office)가 정보보호정책을 총괄하고 각정부기관의 정보보호 업무를 조정하는 기능을 담당하고 있지만, 업무 범위는 중앙부처 범위에 한정되며, 개별 영역의 사이버보안 정책에 대한 최종적책임은 내무부(Home Office)·외무부(FCO)·국방부(MoD) 등 각각의 부처에 귀속되어 있다[22].

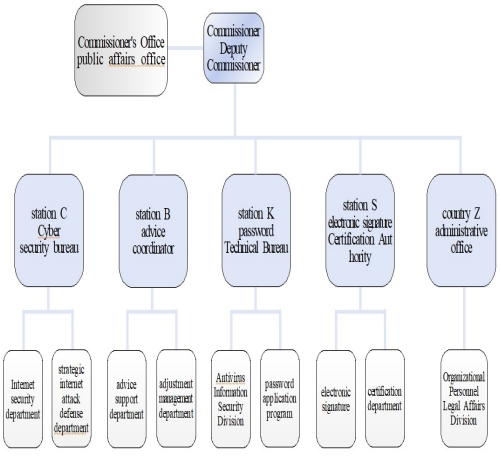

Fig. 2. Organizational structure of the FederalInformation Technology Security Agency in Germany[23]

독일은 국가차원의 통합적 사이버보안정책을 전담하는 별도의 행정기관을 운영하고 있다. 독일은1991년에 제정된 「연방정보기술보안청의 설치에관한 법률(BSI-Errichtungsgesetz)」에 근거하여국가차원에서 사이버보안을 총괄·지원하는 기관으로 연방 내무부 소속으로 연방정보기술보안청(BSI)을 설치하고, 동 기관을 통해 통합적인 사이버보안체계를 운영하고 있다[24].

이와같이 국내외 사이버테러 대응체계를 비교해 보면 몇 가지 유사점과 차이점을 확인할 수 있다. 이 국가들 사이의 주요 유사점 중 하나는 사이버 테러 대응 시스템에 여러 기관 및 단체가 참여한다는 것이다. 5개국 모두 사이버 보안 및 사이버 테러 대응을 전담하는 정부 기관을 설립했으며, 이들 기관 중 많은 기관이 민간 부문 및 국제 기구와 긴밀히 협력하여 정보를 공유하고 사이버 위협에 대한 대응을 조정한다. 또 다른 유사점은 정보 공유 및 협업에 대한 강조이다. 또한, 사이버 위협에 대한 정보 공유와 사이버 공격을 방지하기 위한 모범 사례를 자국 내 및 국제 파트너와 공유하는 것의 중요성을 인식하고 있다.

그러나 이들 국가가 사이버 테러 대응에 접근하는 방식에도 약간의 차이가 있다. 예를 들어 미국은 군사 네트워크에 대한 사이버 공격을 방어하기 위해 전담 군사 사령부인 USCYBERCOM을 설립했으며 다른 국가에서는 이 작업을 민간 기관에 의존한다. 국내에서는 한국인터넷진흥원(KISA)이 사이버 테러 대응 노력을 조정하는 데 중심적인 역할을 하는 고도로 중앙 집중화된 시스템을 가지고 있으며, 유럽 연합은 사이버 범죄 및 사이버 테러리즘과 싸우기 위해 여러 기관이 협력하는 보다 분산된 시스템을 구축했다. 또한, 각 국가가 직면한 위협의 유형과 이에 대응하기 위해 사용하는 전략에도 차이가 있다. 예를 들어, 국내에서는 북한 정부가 후원하는 해커의 중대한 위협에 직면하고 있는 반면, 미국과 유럽 연합은 광범위한 국가 후원 및 비국가 활동가의 위협에 직면해 있다. 또한 일본은 사이버 공격으로부터 중요 인프라를 보호하는 데 특히 중점을 두며 이러한 공격에 대한 대응을 조정하기 위해 사이버 보안을 위한 사고 대비 및 전략 센터(NISC)를 설립했다.

이를 종합해보면, 한국, 미국, 일본, 영국, 독일의 사이버테러 대응체계는 유사하지만 접근방식, 위협의 유형, 대응전략에 있어서도 상당한 차이가 있다. 사이버 공격에 대처하기 위해 사용한다. 그럼에도 불구하고 5개국 모두 사이버 보안 및 사이버 테러 대응에 대한 포괄적이고 협력적이며 선제적인 접근 방식의 중요성을 인식하고

있다.

따라서, 세계 각국은 날로 증가하는 사이버 공격 위협에 대처하기 위해 종합적인 사이버 테러 대응 체계를 구축하기 위한 조치를 취하고 있다. 이러한 시스템은 정부 기관, 민간 부문 기관 및 국제 조직 간의 긴밀한 협력을 포함하며 발생하는 사이버 위협을 신속하게 감지하고 대응하도록 설계되었다.

2.4.2 국내 사이버테러 대응 체계의 문제점

한국은 세계에서 가장 빠른 인터넷 연결과 가장 높은 스마트폰 보급률을 자랑하는 글로벌 디지털 혁명의 최전선에 서 있다. 그러나 이러한 디지털 발전으로 인해 국가는 사이버 테러를 비롯한 증가하는 사이버 위협에 노출된다. 사이버 보안에 대한 막대한 투자에도 불구하고 한국의 사이버 테러 대응 시스템은 여전히 몇 가지 과제에 직면해 있다.

가장 중요한 문제 중 하나는 정부 기관과 민간 기업 간의 조정 및 협력 부족이다[25]. 정부 기관과 민간 기업은 사이버 테러 사건 발생 시 정보 공유를 위한 소통 채널과 지침이 부족한 경우가 많다. 이러한 조정 부족은 효과적인 대응 및 완화에 중요한 정보를 적시에 공유하는 것을 방해한다. 또 다른 문제는 숙련된 사이버 보안 전문가의 부족이다[26]. 한국은 현재 수요를 충족하기 위해 약 27,000명의 전문가가 필요한 사이버 보안 전문가의 상당한 부족에 직면해 있다. 이러한 인력 부족은 스트레스가 많은 환경, 저임금, 부적절한 훈련 및 교육 프로그램으로 인해 사기가 낮고 이직률이 높은 정부 부문에서 특히 심각하다. 또한 사이버테러 대응체계는 사이버테러에 대한 법적인 공백에 직면해 있다[27]. 사이버 보안 및 사이버 범죄와 관련된 다양한 법률이 있지만 사이버 테러를 정의하는 특정 법률은 없다. 이러한 법적 모호성은 민간 기업에 불확실성을 야기할 뿐만 아니라 사이버 테러리스트를 효과적으로 조사하고 기소하는 법 집행 기관의 능력을 제한한다.

또한 사이버 테러 사건에 대한 정부의 대응 능력과 관련된 문제가 있다[28]. 한국 정부의 사이버테러 대응체계는 특히 국가 차원의 사이버테러 비상대응체계가 없는 상황에서 명확한 사고 대응 절차가 미비한 것으로 나타났다.

결론적으로 국내 사이버테러 대응체계는 정부기관과 민간기업 간 조율 및 협업 부족, 숙련된 사이버보안 전문가 부족, 법적 공백, 사이버테러 대응 역량 부족 등 여러 가지 과제에 직면해 있다.

2.5 사이버테러 대응체계 개선방안

국내 사이버테러 대응체계의 문제점 분석을 바탕으로 국내 사이버테러 대응역량 강화를 위한 다음과 같은 방안을 도출할 수 있다.

사이버 테러 대응을 담당하는 다양한 기관의 노력을 통합하고 조정하기 위한 전담 기관을 설립하는 것이 첫 번째 단계이다. 이 기관은 모든 사이버 테러 관련 활동의 중심 연락 창구 역할을 해야 하며 모든 기관이 협력하도록 보장할 책임이 있다. 24시간 대응할 수 있도록 국가사이버테러대응센터를 구축해야 한다. 센터는 최첨단 기술을 갖추고 고도로 훈련된 전문가로 구성되어 모든 사이버 테러 관련 사건을 처리해야 한다. 사이버 테러 대응의 주요 과제 중 하나는 공공 및 민간 부문 전문가의 전문 지식과 지식이 부족하다는 것이다. 사이버테러에 대응하기 위한 개인과 조직의 역량을 향상시키기 위해 더 많은 훈련과 교육 프로그램을 제공해야 한다. 사이버 테러리즘에 대처하기 위해 법적 및 규제 프레임워크를 강화해야 한다. 여기에는 기존 법률 및 규정을 업데이트 및 시행하고 새로운 위협을 해결하기 위한 새로운 규정을 개발하는 것이 포함된다. 사이버 테러는 국제 협력이 필요한 글로벌 이슈이다. 다른 국가 및 국제기구와 긴밀히 협력하여 정보를 공유하고 사이버테러 대응 노력을 조율해야 한다. 또한, 국내 보안 전문인력이 매우 부족한 상태이다. 이를 위해 국가적 차원에서 보안 전문인력을 양성할 수 있도록 많은 지원이 필요하다.

따라서, 현재 사이버테러 대응체계를 재정비하고 개선하기 위해서는 정부, 민간단체, 국제 파트너의 종합적이고 조율된 노력이 필요하다. 제안된 방안은 국내 사이버테러 대응체계 역량을 강화하고 점증하는 사이버테러 위협에 효과적으로 대처하는 데 도움이 될 수 있다.

3. 결론

본 연구는 국내 사이버 테러 대응 체계를 중심으로 한 테러 대응에 관한 연구이다. 사이버 테러의 정의와 분류를 분석하고, 한국의 대응 체계를 평가하고 개선 방안을 제시했다. 그 결과 세계 각국은 날로 증가하는 사이버 공격 위협에 대처하기 위해 종합적인 사이버 테러 대응 체계를 구축하기 위한 조치를 취하고 있었으며, 사이버 시스템은 정부 기관, 민간 부문 기관 및 국제 조직 간의 긴밀한 협력을 포함하며 발생하는 사이버 위협을 신속하게 감지하고 대응하도록 설계되었다는 것을 확인하였다.

국내 사이버 테러 대응 체계를 중심으로 한 테러 대응에 관한 연구 결과를 요약하면, 한국은 사이버 테러 대응을 위해 법률과 정책, 기관 및 조직을 갖추고 있으며, 협력 체계와 정보 공유를 강화하고 있다는 것이다.

또한, 국내 사이버 테러 대응 시스템이 자원과 자금 부족, 여러 기관 간의 조정 부족, 전문인력 부족 등 여러 가지 문제에 직면해 있음을 발견했다. 또한 사이버테러 대응을 위한 법적 틀에 한계가 있고, 이에 대한 국민의 인식도 미흡하다.

이를 해결하기 위해 사이버테러 중앙대응센터 신설, 기관 간 협력 강화, 교육 및 홍보 프로그램을 통한 대국민 인식 제고 등 대응체계 개편 및 업무체계 개선 방안을 제시했으며, 국가적 차원에서 보안 전문인력 양성을 위해 많은 지원이 필요하다. 이를 통해 국내 사이버테러 대응체계 역량을 강화하고 사이버테러 위협에 대한 예방 및 대응능력을 높일 수 있을 것이다.

References

[1] J. Eom, "A Study on the Capability of Cyber Security Education and Training Professional Personnel," Journal of Korea Society of Digital Industry and Information Management, vol. 15, no. 1, pp. 43-51, 2019.
DOI: https://doi.org/10.17662/ksdim.2019.15.1.043

[2] J. Kim and H. Kim, "Intrusion Detection Based on Spatiotemporal Characterization of Cyberattacks," Electronics, vol. 9, no. 3, p. 460, 2020.
DOI: https://doi.org/10.3390/electronics9030460

[3] C. Park and J. Kim, "A Study on the Cybersecurity System of Financial Institutions in Korea," International Journal of Financial Research, vol. 9, no. 2, pp. 105-114, 2018.

[4] S. Kim, "Cyber Terror Response Strategies," Journal of the Korean Society of Electronics Engineers, vol. 59, no. 10, pp. 21-27, 2022.

[5] M. S. Goodman and S. W. Brenner, "The 21st Century Face of Cybercrime: Examining Recent Cyberattack Trends," Crime & Delinquency, vol. 66, no. 3, pp. 332-352, 2020.

[6] J. Arquilla and D. F. Ronfeldt, "The Advent of Netwar (Revisited)," in Networks and Netwars: The Future of Terror, Crime, and Militancy, 2nd ed., 2001, pp. 1-28.

[7] D. E. Denning, "The Looming Specter of Cyber Terrorism: A Call for Global Response," Journal of Counterterrorism & Homeland Security International, vol. 27, no. 2, pp. 30-37, 2021.

[8] Hankyung IT Science. (2020, August 21). "Kakao Bank, K Bank, and Shinhan Bank were attacked by DDoS." Hankyung. Retrieved from https://www.hankyung.com/it/article/2020082095091 (Accessed on July 1, 2023)]

[9] T. Simon and GLOBAL COMMISSION ON INTERNET GOVERNANCE, "CRITICAL INFRASTRUCTURE AND THE INTERNET OF THINGS," Cyber Security in a Volatile World, Centre for International Governance Innovation, 2017, pp. 93-104.

[10] "Kaseya VSA Supply Chain Attack FAQ." Kaseya, 2021, Available From: https://www.kaseya.com/potential-attack-on-kaseya-vsa/ (accessed 25 May 2023)

[11] "Microsoft Exchange Server Vulnerabilities Mitigations – February 2021." Microsoft Security Response Center, 2021, Available From: https://msrc-blog.microsoft.com/2021/03/02/microsoft-exchange-server-vulnerabilities-mitigations-february-2021/ (accessed 25 May 2023)

[12] D. E. Sanger, N. Perlroth, and C. Krauss, "Cyberattack Forces a Shutdown of a Top U.S. Pipeline," The New York Times, May 8, 2021. Available from: https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html (accessed 25 May 2023)

[13] N. Perlroth, "Cyberattack Forces Swedish Supermarkets to Close Nationwide," The New York Times, July 4, 2021. Available from: https://edition.cnn.com/2021/07/06/tech/kaseya-ransomware-attack-businesses-affected/index.html (accessed 25 May 2023)

[14] H. Lee and H. Yoo, "Cybersecurity in South Korea: Policy Overview and Evaluation," Cyber Policy Research, vol. 2, no. 2, pp. 185-202, 2017.

[15] Korea Internet & Security Agency, "Cyber Security Incident Center," Available from: https://www.kisa.or.kr/EN/101 (accessed 25 May 2023))

[16] J. Lee, "Korea's Cyber Security Strategy: A Critical Evaluation," Strategic Studies, vol. 40, no. 5, pp. 684-713, 2017.

[17] Ministry of Foreign Affairs of the Republic of Korea, "Korea cyber security," Available from: https://www.mofa.go.kr/eng/wpge/m_5437/contents.do (accessed 25 May 2023)

[18] S. Kim, "Trump Administration's Cyber Security Strategy: Complex Geopolitical Response to State-sponsored Hacking," International and Regional Studies, vol. 27, no. 4, pp. 1-35, 2018.

[19] Lee Seong-yeop, 「Necessity of National Cyber Security Act and Factors to Consider」, 『Cyber Security and Law』 Edition of Korea Cyber Security Law Policy Association, 2021.

[20] Y. S. Oh, "Prospects of the Biden Government's Cyber Security Policy in 2021," Issue Brief, Vol. 244, 2021.

[21] H. Lee et al., "Comparative law study on information

protection legislation to strengthen cyber security system," Korea Internet & Security Agency, 2015, pp. 177-208.

[22] B.-H. Bae, "Analysis of UK Cyber Security Strategy and Implications: Focusing on National Cyber Security Strategic Plan and Performance," Weekly Technology Trend, no. 1666, 2014.

[23] Y.-T. Jeon, "Current Status of UK Cyber Security System and Policy Response Tasks: From the Perspective of Business Risks of SMEs," Legal Research, vol. 18, no. 3, 2018.

[24] National Assembly Library, "Cyber Terror at a Glance," National Assembly Library, 2013, p. 74.

[25] D. Jeong, "Cyber terrorism concept and countermeasures," Legal studies, vol. 26, no. 1, pp. 345-374, 2023. DOI: https://doi.org/10.22789/IHLR.2023.03.26.1.11

[26] Kwon, Y.-S., & Lee, D.-R. (2021, February 28). A Study on the Cyber Terrorism Countermeasures. Legal Theory & Practice Review. The Korea Society for Legal Theory and Practice. DOI: https://doi.org/10.30833/ltpr.2021.02.9.1.245

[27] D. Kim, "A Study on the Establishment of a Legal System to Respond to Cyber Terrorism," Domestic Doctoral Dissertation, Dong-A University Graduate School, Korea, pp. 116-117, 2020.

[28] Ubi, "Measures to improve the domestic terrorism Response system in response to the increasing threat of terrorism," Master's thesis, Yongin University, Korea, pp. 55-57, 2023.

전 태 식(Tae-sik jeon) [정회원]

- 2015년 2월 : 국방대학교 국방관리대학원 (석사)
- 2022년 2월 ~ 현재 : 명지대학교 일반대학원 보안경영공학과 (박사과정)

〈관심분야〉
테러, 드론, 무기체계, 물리적보안, 시스템 보안

김 찬 우(Chan-woo Klm) [정회원]

- 2021년 8월 : 명지대학교 산업대학원 융합보안안보학과 (석사)
- 2021년 9월 ~ 현재 : 명지대학교 일반대학원 보안경영공학과 (박사과정)
- 2017년 8월 ~ 현재 : JJ 시스템 대표

〈관심분야〉
소프트웨어보안, 데이터보안

류 연 승(Yeon-Seung Ryu) [정회원]

- 1990년 2월 : 서울대학교 계산통계학과 (학사)
- 1992년 2월 : 서울대학교 전산과학과 (석사)
- 1996년 8월 : 서울대학교 전산과학과 (박사)
- 2015년 3월 ~ 현재 : 명지대학교 보안경영공학과 주임교수
- 2017년 1월 ~ 현재 : 방산기술보호 연구회 위원장

〈관심분야〉
시스템 보안, 무기체계 보안, 방산기술 보호