https://doi.org/10.33778/kcsa.2020.20.4.027

빅데이터/클라우드 기반 미래 C4I체계 사이버위협 관리체계 적용 방안 연구★

박 상 준*, 강 정 호**

요 약

최근 4차 산업혁명 기술은 기술발전을 통해 일상생활을 크게 바꾸고 있을 뿐 아니라 국방정책 수립에 있어서도 주요 키워드가 되어 가고 있다. 특히 ICBMS라 불리는 사물인터넷, 클라우드, 빅데이터, 모바일, 사이버보안 기술은 인공지능과 더불어 국방정보화정책의 핵심선도기술로 선정되었다. 4차 산업혁명 기술의 중요성이 증대되는 가운데 현재 KJCCS, ATCIS, KNCCS, AFCCS 등 합참 및 각 군 기능별로 분리 운용되고 있는 C4I체계를 미래전에 대비하는 하나의 체계로 개발하기 위한 연구가 추진되고 있다. 이는 C4I체계를 각 도메인별로 운용함에 따라 정보교환 등 합동작전을 위한 상호 운용성이 저하되는 문제를 해소하기 위함이다. 또한 각종 무기체계들이 초연결 및 초지능화 체계로 개발이 추진되고 있어 이들을 효율적으로 통제하고 안전하게 운용하기 위해 통합C4I체계 구축과 미군의 RMF(Risk Management Framework) 같은 체계의 도입이 필수적이다. 따라서 본 논문에서는 빅데이터/클라우드 기반의 미래 C4I체계의 사이버위협 지능화 탐지 및 사용자 정보 접근권한 관리, 사이버위협의 지능화 관리 및 가시화 방안을 제시한다.

A Study on the Application of the Cyber Threat Management System to the Future C4I System Based on Big Data/Cloud

Sangjun Park*, Jungho Kang**

ABSTRACT

Recently, the fourth industrial revolution technology has not only changed everyday life greatly through technological development, but has also become a major keyword in the establishment of defense policy. In particular, Internet of Things, cloud, big data, mobile and cybersecurity technologies, called ICBMS, were selected as core leading technologies in defense information policy along with artificial intelligence. Amid the growing importance of the fourth industrial revolution technology, research is being carried out to develop the C4I system, which is currently operated separately by the Joint Chiefs of Staff and each military, including the KJCCS, ATCIS, KNCCS and AFCCS, into an integrated system in preparation for future warfare. This is to solve the problem of reduced interoperability for joint operations, such as information exchange, by operating the C4I system for each domain. In addition, systems such as the establishment of an integrated C4I system and the U.S. military's Risk Management Framework (RMF) are essential for efficient control and safe operation of weapons systems as they are being developed into super-connected and super-intelligent systems. Therefore, in this paper, the intelligent cyber threat detection, management of users' access to information, and intelligent management and visualization of cyber threat are presented in the future C4I system based on big data/cloud.

Key words : Bigdata, Cloud, C4I system, Cyber threat, Future warfare

접수일(2020년 8월 18일), 게재확정일(2020년 10월 14일)

★ 본 논문은 육군사관학교 사이버전연구센터의 연구활동비 지원을 받아 연구되었음.

* 육군사관학교 전자공학과

** 합동참모본부, 교신저자

1. 서 론

최근 4차 산업혁명 기술의 발달은 일상생활을 크게 바꾸고 있을 뿐 아니라 국방정책 수립에 있어서도 주요 키워드가 되고 있다. 특히 ICBM으로 불리는 사물인터넷, 클라우드, 빅데이터 및 모바일 기술은 인공지능과 더불어 국방정보화정책 수립의 핵심 기술로 자리매김 하고 있다. 이 기술들은 그동안 합동참모본부와 각 군별로 운용하던 KJCCS, ATCIS, AFCCS, KNCCS 등의 C4I체계를 통합할 수 있는 기술적 기반을 마련해 줌으로써 한국군 C4I체계의 통합을 위한 정책 추진이 가능하게 하고 있다. C4I체계는 센서와 슈터로부터 발생하는 정보를 종합하여 가시화함으로써 지휘관 및 참모들이 정확한 상황판단을 할 수 있도록 해주는 것으로 네트워크중심작전환경 구현을 위해서 필수적인 요소이다[1][2]. 전장에서 발생하는 대부분의 정보가 C4I체계로 집중되기 때문에 빅데이터가 구성되며 이를 가장 효율적으로 운용하기 위해서 클라우드 컴퓨팅을 적용하기에 적합한 체계이다[3].

현재 운용중인 한국군 C4I체계는 합동참모본부와 각 군이 별개로 개발하여 운용하던 중에 상호운용성을 위해서 일부 정보를 연동하는 방식으로 보완되어 왔다. 그러나 앞으로는 미래전에 대비하여 각종 무기체계에 4차 산업혁명 기술이 적용되고 이들이 초연결・초지능 네트워크로 연결될 것으로 예상된다[4][5]. 따라서 미래전에 사용될 C4I체계는 대용량 데이터의 발생, 전송, 처리, 보관 등의 절차를 원활하게 할 수 있어야 할 뿐 아니라 수 많은 데이터를 보호하고 체계의 안전성을 보장하기 위해서 사이버위협에 대응하기 위하여 다양한 요소를 고려한 정책을 수립하고 체계 개발에 적용하여야 한다. 현재의 C4I체계는 한 명의 사용자가 다른 두 개의 C4I체계를 사용할 경우 각 체계별 암호모듈과 사용자 ID, 비밀번호를 별도로 사용하여 인증을 받는다[6]. 이러한 복잡한 인증절차는 더욱 복잡해지는 미래전에서 상호운용성 및 작전의 효율성을 저하시키는 요인으로 작용할 것이다. 또한 IoT와 더불어 드론봇 전투체계 등 다양한 경로에서 발생하는 사이버위협에 대한 대비와 대응의 효율도 저하될 것이다.

본 논문에서는 현재 운용중인 C4I체계의 문제점을 개선하고 빅데이터/클라우드 기반의 미래 C4I체계의 사이버위협을 효율적으로 관리하기 위한 체계 적용 방안을 제안하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 국방분야에서 빅데이터/클라우드 기반의 사이버전 및 사이버보안 기술 연구 등과 관련한 선행연구들을 살펴보고, 3장에서는 미래 전장에서 C4I체계에서 발생할 수 있는 사이버위협 탐지의 자동화 방안과 사용자의 정보 접근권한 부여 방안을, 4장에서는 미래 C4I체계에서 자동 탐지된 사이버위협의 지능화 관리 및 가시화 방안을 제시하고 5장 결론을 통해 요약 및 향후 활용 방향을 제시한다.

2. 관련 연구

최근 4차 산업혁명 기술이 미래전을 대비하기 위한 핵심원천기술로 부상하면서 국방분야에서 AI+ICBM을 활용한 빅데이터, 클라우드 보안 아키텍처 및 사이버전 등에 대한 연구가 활발하게 이루어지고 있다.

먼저 빅데이터를 이용한 선제적 사이버전 강화방안 연구에서는 사이버전의 주요 위협요소를 살펴보고 빅데이터와 기계학습을 이용하여 APT 공격 방법 탐지 등 사이버전에 대응하는 방안을 제시하였다[7]. 빅데이터 분석 기술 기반의 네트워크 정상행위 규정 방법 연구에서는 빅데이터 분석 플랫폼인 Hadoop/Hive를 이용하여 사물인터넷 등으로 인해 폭발적으로 증가하는 네트워크 트래픽과 프로토콜 등에서의 비정형 데이터를 정형화하고 분석하여 정상행위 여부를 분석하고 이를 Arena를 이용하여 검증한 결과 등을 제시하였다[8]. 인공지능과 빅데이터 분석 기반 통합보안관제시스템 구축방안에 관한 연구에서는 인공지능 기술과 빅데이터 분석 기반의 통합보안관제시스템(ESMS) 구축을 위한 제도적, 기술적 요소 6가지를 분석하여 제시하기도 하였다[9].

클라우드 기반 미래 한국군 지휘통제체계 보안 아키텍처 설계에 대한 연구에서는 현재 한국군 C4I체계의 보안 요구사항을 분석하고 클라우드 기반의 미래 C4I체계 운용에 필요한 보안 요구사항, 아키텍처 설계 및 동작 절차 등을 제시하였다[6]. 클라우드 컴퓨팅 적용을 위한 다른 연구에서는 현재의 C4I체계를 클라우드 컴퓨팅 적용의 필요성과 레거시 환경을 클라우드 컴퓨팅 환경으로 이전하기 위한 이전기술 및 방법에 대해 제시하기도 하였다[3].

사이버전 수행절차 운영개념에 관한 연구에서는 사이버전 프레임워크를 사이버 정보감시정찰, 사이버 지휘통제, 사이버방어, 사이버 전투피해평가로 구성하여 이를 운용하는 방안 등을 제시하였으며[10], 현재 운용되는 사이버위협 탐지 및 차단 체계가 최근 증가하고 있는 사이버 공격에 대한 선제적 대응이 어렵기 때문에 이를 기계학습을 통해 자동화하고 이렇게 자동화된 시스템이 실시간으로 사이버 위협 정보를 분석하고 예측할 수 있는 시스템이 제안되기도 하였다[11]. 또한 군사작전의 일환인 사이버작전을 효과적으로 수행하기 위해 빅데이터를 수집 및 활용하는데 필요한 빅데이터의 유형과 빅데이터 거버넌스 이슈를 분석한 빅데이터 거버넌스 모델이 제시되기도 하였다[12]. 이외에도 최근 급격히 증가하고 있는 사이버위협에 대응하기 위하여 인공지능 기술과 빅데이터, 클라우드 컴퓨팅을 적용하기 위한 연구들이 다양하게 진행되고 있다.

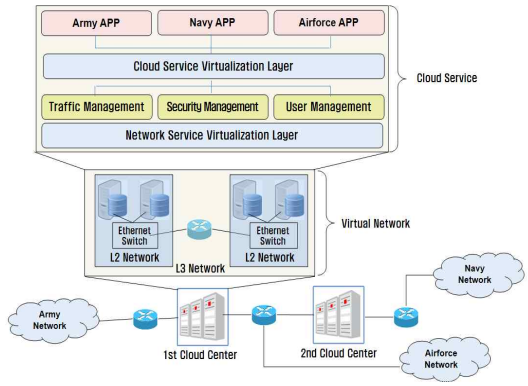
3. 미래 C4I체계의 사이버위협 탐지 자동화 방안

3.1 빅데이터/클라우드 기반 사이버위협 탐지 지능화 방안

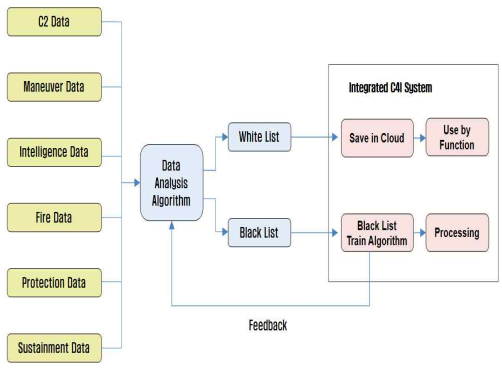
미래 C4I체계에 대한 사이버위협은 정보통신기술이 적용되는 모든 무기체계로부터 발생할 수 있다. 기본적으로 각 제대별 상호 정보공유 및 전장가시화를 위해 C4I체계 단말기 간 정보유통을 한다. 또한 정보를 수집한 센서, 즉 감시정찰체계로부터 정보를 전달받으며, 이 정보를 슈터인 타격체계로 전달한다. 물론 조정통제 등을 이유로 반대의 경로로 정보유통이 되기도 한다. 사실상 모든 경로를 통해 사이버위협이 발생할 수 있는 것이다.

C4I체계에서 유통되는 데이터는 무기체계 및 부대유형에 따라 정형화되어 있는 것이 일반적이다. 그러나 현재의 C4I체계는 합동참모본부 및 각 군이 별도로 운용하고 있어 데이터의 종류, 형태, 패턴 등을 분석하는데 제한이 따른다. 따라서 사이버위협 탐지를 자동화하기 위해 우선 클라우드 컴퓨팅을 도입하여 하나의 통합C4I체계로 구성이 필요하다.

(그림 1)에서처럼 합참 및 각 군의 네트워크를 클라우드 서버로 접속하도록 네트워크를 구성하고 클라우드 서버에서는 네트워크 서비스 추상화 계층을 통해 트래픽, 보안, 사용자 등을 관리하고, 그 상위 계층에 클라우드 서비스 추상화 계층을 거쳐 합참 및 각 군에 해당되는 서비스 애플리케이션에 접속할 수 있도록 한다. 이렇게 클라우드 컴퓨팅을 적용할 때 서버 운용의 안정성을 위하여 서버는 이중화하여 클라우드 1센터와 2센터에서 동시에 운용하고 수시로 동기화하여 무결성을 유지한다. 사이버위협은 보안 매니지먼트에서 유통되는 데이터의 패턴, 형태, 양 등을 통해서 분석하고 학습하여 취약점 점검, 악성코드 분석, 장애예측, 탐지규칙 최적화 등을 자동화한다.



(그림 1) 클라우드 컴퓨팅을 적용한 통합C4I체계 구조



(그림 2) 사이버위협 탐지 흐름도

(그림 2)는 C4I체계에서 유통되는 데이터를 전투수행기능별로 구분하여 사이버위협을 탐지하는 흐름을 보여주고 있다. 전투수행기능인 지휘통제, 기동, 정보, 화력, 방호 및 작전지속지원 데이터들은 클라우드 서버의 보안 매니지먼트의 데이터 분석 알고리즘을 통해 정상 데이터와 이상(異常) 데이터로 구분된다. 정상 데이터는 클라우드에 저장되면서 체계 사용자들에게 제공되고 이상 데이터로 분류된 데이터는 이상 패턴 학습 알고리즘으로 전송되어 학습데이터로 활용한 후에 처리한다. 이상 패턴 학습 알고리즘을 통해 분석되고 학습된 분석 알고리즘을 다시 데이터 분석 알고리즘을 업데이트함으로써 이후 보다 정확한 탐지가 가능하도록 한다.

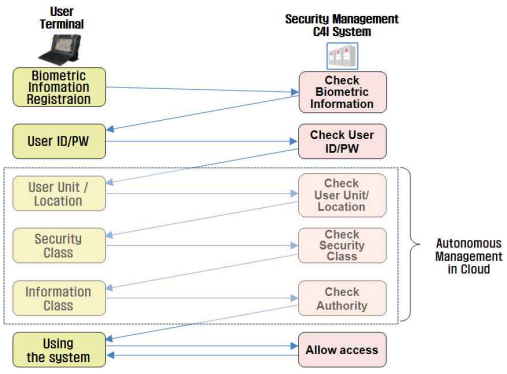
이러한 사이버위협 탐지 지능화를 위해서는 최초의 데이터 분석 알고리즘에 적용할 학습 데이터는 OSINT(Open Source INTelligence)를 통해 상용 네트워크에서 이루어지는 사이버 공격 및 위협의 패턴을 분석하고 탐지할 수 있도록 적용한다. 그리고 각각의 전투수행기능별 데이터를 분류하기 위해서 운용하는 군, 제대 및 무기체계에 따른 고유 ID를 패킷 헤더에 적용함으로써 유통되는 데이터 분석이 정확하게 이루어지도록 적용이 필요하다.

3.2 사용자의 클라우드 접근권한 부여 방안

일반적으로 접근제어를 하는 방법에는 역할 기반 접근제어(Role-Based Access Control), 속성 기반 접근제어(Attribute-Based Access Control), 상황 인식 기반 접근제어(Context-Aware Access Control) 등이 있다[13]. 그러나 군사작전에 사용되는 C4I체계는 상용 네트워크와 다르게 사용자의 교체, 상황 변화 등이 매우 빠르게 일어난다. 전투수행에 따른 전사상자 발생 및 진급 등의 사유로 사용자 정보 변경이 빠를 뿐 아니라 공격작전과 방어작전이 수시로 전환되고 소강상태가 이루어지는 경우도 자주 발생한다. 그럼에도 불구하고 정해진 직책에 따라서 임무와 역할은 고정되어 있기 때문에 조직도와 구성원의 정보가 탈취되었을 경우 접근권한이 쉽게 노출될 가능성이 있다. 반면에 고정된 직책에 따른 고정된 임무와 역할은 클라우드 환경에서의 접근권한 제어를 하기에 용이한 환경이라고 할 수 있다.

(그림 1)과 같은 통합 클라우드 컴퓨팅 환경에서 정보보호를 위해 가장 기본적인 과정이 사용자의 접근권한 부여 방식이라 할 수 있다. 그리고 C4I체계 사용자는 조직 및 직책에 따른 명확한 구분이 가능하므로 역할 기반의 접근제어 방식과 클라우드 컴퓨팅 환경의 상황을 고려한 상황 인식 접근제어 방식을 융합하여 사용자 접근권한을 부여하는 방식을 제안하고자 한다. 상용에서 정보접근권한을 인정해주는 가장 대표적인 공인인증서 사용의무화 정책을 2018년에 폐지하면서 뇌파・심전도・근전도・맥박 등의 생체신호 인증을 통한 신원인증기술에 대한 연구가 활발하게 진행되고 있다[14]. 군은 그 특성상 입대할 때 각종 생체정보를 수집, 저장, 관리 프로세스의 진행이 용이하다. 따라서 군복무를 하는 현역 군인의 생체정보, 해당인원의 계급 및 직책 등의 개인정보 및 User ID, 부대의 조직을 나타내는 User Unit, 부대의 위치 정보를 나타내는 User Location 등과 클라우드 컴퓨팅에 접속하기 위해 필요한 Security Class, 정보에 접근할 수 있는 권한을 주는 Imformation Class 등을 복합적으로 고려하여 동적으로 부여할 수 있어야 한다. 특히 적과 전투 중에 발생하는 체계 사용자의 변경시에는 (그림 3)과 같이 사용자가 체계 단말기에서 생체정보 등록 요청을 하면 클라우드 서버에 저장되어 있던 개인생체정보를 C4I체계 보안매니지먼트에서 일치여부를 확인한다. 이어서 사용자가 사용자의 고유 ID 및

비밀번호를 입력하면 보안매니지먼트에서 이에 대해 일치여부를 확인하고 일치할 경우 단말기의 운용부대, 위치 정보, 사용자의 보안등급 및 정보접근권한 수준 등을 클라우드 내 데이터를 확인하여 자동으로 확인하여 해당하는 클라우드 서비스에 접근할 수 있도록 허용해 준다. 이렇게 생체인식정보와 ID/PW, 부대 위치정보 등을 종합적으로 비교하여 확인할 경우 단말기가 적에게 탈취되었을 경우에도 적에 의한 사이버 위협을 차단 가능성을 향상시킬 수 있다.



(그림 3) 사용자 접근권한 확인 과정

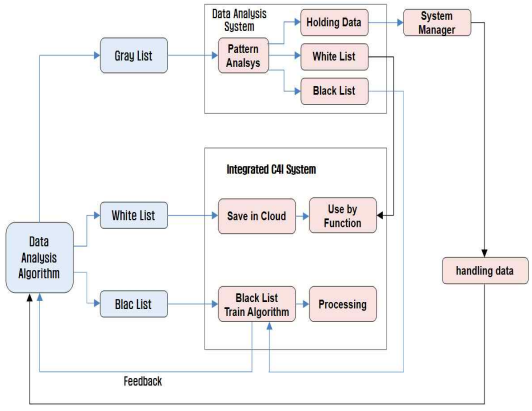
4. 미래 C4I체계를 위한 사이버위협 지능화 관리체계 적용 방안

빅데이터 및 클라우드 컴퓨팅을 적용하여 사이버위협 탐지를 지능화하는 것 못지않게 중요한 부분이 새로운 형태의 사이버위협에 대해 판단하는 것과 체계를 관리하는 체계 관리자에게 가시화해 주는 방법일 것이다. 본 절에서는 사이버위협 지능화 관리체계를 적용하기 위한 방안을 제시한다.

4.1 새로운 패턴의 사이버위협 지능화 관리 방안

AI 기술의 발달은 사이버위협의 형태 또한 자동화・지능화하고 수시로 변화된 형태로 발전시킬 가능성을 높이고 있다[15]. 따라서 사이버위협에 대응하는 방어자의 입장에서도 변화되는 사이버위협에 실시간 대응하기 위해서는 지능화된 관리체계가 필요하다.

먼저 데이터 분석 알고리즘을 통해 탐지된 사이버위협은 체계 관리자에게 알려지기 전에 체계 내에서 자동적으로 구분하고 이를 별도의 저장장치에 저장하거나 백신 등을 이용하여 처리되어야 한다. 즉, 탐지된 사이버위협 요인을 분리하고 삭제하는 등의 행위를 지능화 및 자동화한다는 것이다. 이를 위해서 (그림 2)에서처럼 데이터 분석 알고리즘이 정상 데이터(화이트 리스트)와 이상 데이터(블랙 리스트)를 구분하게 되는데 완전히 새로운 형태의 데이터가 탐지되었을 경우에 충분한 학습이 이루어지기 전이므로 오탐지할 우려가 있다. 따라서 이에 대한 대책이 필요하며 이를 (그림 4)에서 보여주고 있다. 새로운 형태의 데이터가 탐지되었을 경우 판단제한 데이터(그레이 리스트)로 분류하여 데이터 분석 체계에서 별도의 패턴 분석 알고리즘을 통해 기존의 사이버위협 데이터와의 유사성 분석 등을 수행한다. 기존 데이터와 유사성 정도에 따라서 정상 데이터와 이상 데이터, 판단유보 데이터로 분류하고 판단유보 데이터로 분류된 데이터는 체계 관리자가 직접 검토하도록 하여 수동 처리하고 이에 대한 판단 결과를 데이터 분석 알고리즘에 반영하도록 한다. 정상 데이터들은 기능별로 활용하도록 제공하고 이상 데이터로 분류된 데이터는 이상 패턴 학습 알고리즘에서 학습 데이터로 활용 후 처리하는 과정을 거치도록 한다.



(그림 4) 새로운 형태의 사이버위협 지능화 관리

이 밖에 정상 데이터 중에서도 미세하게 변형된 데이터가 있을 수 있다. 이런 경우 시스템이나 체계 관리자가 인지하지 못해서 발생하는 문제를 방지하기 위하여 동일한 경로의 정상 데이터 중 미세한 오류가

수 차례 반복적으로 발생하는 경우 체계 관리자가 인지할 수 있도록 알람처리하고 판단제한 데이터로 처리하도록 하여야 한다.

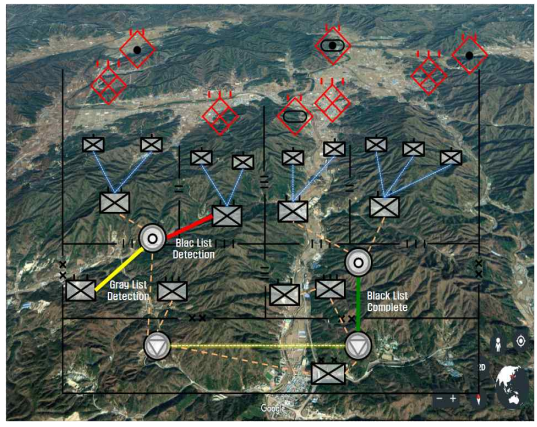
4.2 사이버위협 지능화 관리체계 가시화 방안

탐지된 사이버위협을 지능화·자동화하여 관리하더라도 체계 관리자가 어떤 경로에서 어떤 종류의 사이버위협이 탐지되었는지 모른다면 언젠가 분제가 발생할 수 있다. 따라서 탐지된 사이버위협과 처리 결과를 체계 관리자에게 알려줄 수 있는 가시화 기술이 적용되어야 한다. 탐지된 사이버 위협을 가시화를 하는 내용으로는 <표 1>에서 보는 바와 같이 발생일시, 탐지구간, 탐지유형, 처리유무, 처리내용 등이 주요 요소가 될 것이다. 이 내용을 표의 형태로 가시화하는 것이 가장 쉬운 방법이 될 것이다. 그러나 체계 관리자의 입장에서 사이버위협 발생 여부 등을 위와 같은 표를 통해서 신속하게 확인하는 것은 제한될 수 있다. 이보다 더 시·청각적으로 가시화할 수 있는 방안이 필요하다.

<표 1> 사이버위협 가시화 요소

Date	Section	Type	Status	Details
07132000	17R-2Div	IPT	Complete	Delete
07132125	16R-1BN	Excess Authority	Complete	Cut-Off
07132134	16R-2BN	Gray List	Holding	Holding

C4I체계의 관리자 입장에서 가장 확인하기 쉬운 방법은 전장 지형정보와 부대 네트워크 연결 상태를 보여주는 작전상황도를 동일하게 활용하는 방안으로 (그림 5)에서 보여주고 있다. (그림 5)에서처럼 지형정보를 기반으로 부대 배치를 나타내고 있는 작전상황도와 각 부대 및 노드통신소 간 네트워크 연결상태를 보여주고 있는 네트워크 상황도를 기본으로 구성하고 이상데이터를 탐지 한 경우 알람을 울림과 동시에 해당 경로의 네트워크 연결선을 빨간색으로 변경하도록 함으로서 체계 관리자가 모니터링 및 탐지 내용 등을 확인하도록 한다. 이상데이터 처리가 완료된 경우 연결선은 녹색으로 변경한 후 일정 시간이 지나면 기본 네트워크 연결선으로 변경되도록 한다. 판단제한 데이터를 탐지한 경우에는 알람을 울림과 동시에 네트워크 연결선을 노란색으로 표시함으로써 체계 관리자에게 사이버위협 탐지 체계에 발생한 판단제한 데이터를 처리하기 위한 준비시간을 부여할 수 있어야 한다. 즉, 사이버위협 탐지 지능화를 위한 가시화는 사이버위협 탐지 이벤트가 발생한 경로의 링크 선의 두께, 선색 등의 변경과 함께 텍스트 팝업 및 알람음 등을 사용함으로써 체계 관리자가 신속하게 확인이 가능하도록 하고 이를 확인한 체계 관리자는 세부 내용을 표를 통해서 세부적인 내용을 확인하도록 함으로써 사이버위협 관리의 효율성을 높이는 것이다. 이렇게 사이버위협 탐지 및 관리체계를 가시화할 경우 사이버전 영역에서 지휘관의 신속한 판단을 용이하게 함으로써 작전의 효율성을 향상시킬 수 있을 것이다.



(그림 5) 사이버위협 지능화 관리체계 가시화 방안

5. 결 론

4차 산업혁명 기술은 일상생활의 변화 뿐 아니라 국방분야 또한 크게 바꿀 것으로 예상된다. 특히 미래전은 4차 산업혁명 기술이 고도로 접목된 모든 무기체계들이 네트워크로 연결되고 지능화되는 초연결·초지능 네트워크중심작전환경에서 운용될 것으로 예상된다. 또한 미래전의 영역이 전통적인 군사작전의 영역인 지상, 공중, 해상을 벗어나서 우주와 사이버공간 등으로 확대되고 있으며, 다영역에서 운용되는 다양한

무기체계들이 하나의 네트워크로 연결됨을 의미한다. 이러한 환경에서 운용되는 모든 무기체계들로부터 발생하는 데이터들의 수와 양은 우리의 상상을 뛰어넘을 수 있으며 특정한 무기체계 또는 네트워크 경로 상에서 발생하는 사이버위협 또한 급증할 것으로 예측이 가능하다. 이러한 사이버위협에 실시간 대응하지 못한다면 C4I체계를 활용하여 지휘관 및 참모가 신속한 상황판단과 결심을 할 수 없게 되어 군사작전의 실패를 초래하게 될 것이다.

본 논문에서는 초연결·초지능화되는 미래전의 사이버전에 대응하기 위하여 빅데이터/클라우드 기반의 미래 C4I체계에 발생할 수 있는 사이버위협 탐지, 사용자 접근제어 방법과 탐지된 사이버위협의 지능화 관리 및 가시화 방안에 대해 제안하였다. 이는 인공지능 기술을 활용하여 사이버공격의 패턴이 빠르게 변하고 있기 때문에 이에 대해 보다 효율적으로 대응하기 위한 방안 중의 하나를 제시한 것이다. 이를 토대로 향후 빅데이터/클라우드 컴퓨팅 환경 기반에서 지능화 되어가는 미래 C4I체계에서 사이버위협에 대응함에 있어 군사작전 측면과 기술적 측면이 모두 고려되는 사이버전 기술개발 정책 수립에 활용되어 사이버전 영역에서의 우위를 점할 수 있기를 기대한다.

참고문헌

[1] 박상준, 신규용 외 4명, "증강현실 기반 지휘통제 훈련 시뮬레이터 개발," 융합보안 논문지, 제18권, 제5호, pp. 53-60, 2018.

[2] 박동석, 오동한, 최은호, 임재성, "합동지휘통제 통합망 구조 QoS 모델(안)," 한국군사과학기술학회지, 제23권, 제2호, pp. 106-114, 2020.

[3] 임충수, 전호철 외 3명, "레거시 지휘통제체계의 클라우드 컴퓨팅 환경 이전기술 및 방법에 관한 연구," 한국통신학회논문지, 제45권, 제2호, pp. 428-436, 2020.

[4] 정유현, 김성남, 박기환, 박혜숙, "국방ICT융합기술의 최근 연구동향," 한국통신학회지(정보와통신), 제37권, 제4호, pp. 54-62, 2020.

[5] 이정규, "무기체계 사이버 보안 정책 동향," 정보보호학회지, 제28권, 제6호, pp. 83-87, 2018.

[6] 구자훈, 김영갑, 이상훈, "클라우드 기반 미래 한국군 지휘통제체계 보안 아키텍쳐 설계," 한국통신학회논문지, 제45권, 제2호, pp. 400-408, 2020.

[7] 강정호, "빅 데이터를 이용한 선제적 사이버전 강화 방안 연구," 보안공학연구논문지, 제13권, 제3호, pp. 195-203, 2016.

[8] 김성진, 김강석, "빅데이터 분석 기술(Hadoop/Hive) 기반 네트워크 정상행위 규정 방법," 정보보호학회논문지, 제27권, 제5호, pp. 1117-1127, 2017.

[9] 배재권, "인공지능과 빅데이터 분석 기반 통합보안관제시스템 구축방안에 관한 연구," 로고스경영연구, 제18권, 제1호, pp. 151-166, 2020.

[10] 김성중, 유지훈 외 3명, "사이버전 수행절차 운영개념에 관한 연구," 인터넷정보학회논문지, 제21권, 제2호, pp. 73-80, 2020.

[11] 임창완, 신영섭 외 4명, "실시간 사이버 위협 지능형 분석 및 예측 기술," 정보과학회 컴퓨팅의 실제 논문지, 제25권, 제11호, pp. 565-570, 2019.

[12] 장원구, 이경호, "효과적인 사이버공간 작전수행을 위한 빅데이터 거버넌스 모델," 한국빅데이터학회지, 제4권, 제1호, pp. 39-51, 2019.

[13] 조도은, 김시정, "스마트 홈에서 프라이버시 보호를 위한 사용자 동적 접근제어," *JOURNAL OF PLATFORM TECHNOLOGY*, 제6권, 제3호, pp. 17-22, 2018.

[14] 김재성, "바이오인식 국제표준화 동향," 정보보호학회지, 제29권, 제4호, pp. 29-34, 2019.

[15] Daesung Lee, "차세대 사이버 보안 동향," 한국정보통신학회논문지, 제23권, 제11호, pp. 1478-1481, 2019.

〔저자소개〕

박 상 준 (Sangjun Park)
2000년 2월 육군사관학교 학사
2010년 2월
한국과학기술원 정보통신공학 석사
2020년 3월 ~ 현재 아주대학교 국방디지털융합학과 박사과정
2019년 11월 ~ 현재
육군사관학교 전자공학과 조교수
email : sigpsj13438@naver.com

강 정 호 (Jungho Kang)
2000년 2월 육군사관학교 학사
2006년 3월 서울대학교 전산학 석사
2015년 9월 아주대학교 NCW공학 박사
2014년 ~ 2017년 육군사관학교 컴퓨터과학과 조교수
2019년 ~ 현재 합동참모본부
email : kjh77@snu.ac.kr