https://doi.org/10.33778/kcsa.2020.20.4.143

멀티레이어드 시각화를 적용한 사이버작전 상황도 개발에 관한 연구

권 구 형*, 고 장 혁*, 김 선 영**, 김 종 화**, 이 재 연**, 오 행 록***

요 약

제 5의 전장이라고 불리는 사이버 전장은 육·해·공·우주의 기존 물리 전장과 달리, 지형적인 정보를 기반으로 하지 않으며 각 정보간 긴밀한 연관 관계를 갖는 특징을 갖고 있다. 사이버 전장은 물리 전장에 위치한 장비의 네트워크 연결 정보를 기반으로 생성되므로 지형 정보와 완전히 분리되어 있지 않으면서도, 물리적 공간 제약을 넘어서 네트워크 토폴로지 기반의 논리적인 연결 상태와 OS 및 SW의 취약점 등에 의존적인 특징을 가진다. 그러므로 사이버 전장의 상황인식을 위한 정보 분석은 지리적이거나 논리적인 특정 정보 분석으로는 제한적이며, 여러 도메인의 상황을 한 눈에 인식할 수 있는 형태로 정보가 제공되어야 한다. 본 논문에서는 사이버 전장에서의 지휘통제를 위해 반드시 필요한 사이버작전 상황도 개발에 관한 연구를 기술한다. 특히 멀티레이어드 개념을 적용한 시각화 기술을 기반으로 지리정보를 비롯한 사이버 자산, 위협, 임무 등 상호 연관분석이 필요한 여러 계층의 정보를 상황도에서 직관적으로 도시할 수 있는 아키텍쳐를 제안한다. 본 연구를 통해 사이버작전 수행을 위해 필요한 지휘결심 지원 정보들이 도시요소로 표현되어, 복잡하고 이해하기 어려운 사이버 전장에서 지휘관이 신속하고 정확하게 지휘통제를 수행할 수 있도록 지원하는 상황도 구조를 제안한다.

A Study of Cyber Operation COP based on Multi-layered Visualization

Koohyung Kwon*, Jang-hyuk Kauh*, Sonyong Kim**,
Jonghwa Kim**, Jaeyeon Lee**, Haengrok Oh***

ABSTRACT

The cyber battlefield called the fifth battlefield, is not based on geological information unlike the existing traditional battlefiels in the land, sea, air and space, and has a characteristics that all information has tightly coupled correlation to be anlayized. Because the cyber battlefield has created by the network connection of computers located on the physical battlefield, it is not completely seperated from the geolocational information but it has dependency on network topology and software's vulnerabilities. Therefore, the analysis for cyber battlefield should be provided in a form that can recognize information from multiple domains at a glance, rather than a single geographical or logical aspect. In this paper, we describe a study on the development of the cyber operation COP(Common Operational Picture), which is essential for command and control in the cyber warfare. In particular, we propose an architecure for cyber operation COP to intuitively display information based on visualization techniques applying the multi-layering concept from multiple domains that need to be correlated such as cyber assets, threats, and missions. With this proposed cyber operation COP with multi-layered visualization that helps to describe correlated information among cyber factors, we expect the commanders actually perfcrm cyber command and control in the very complex and unclear cyber battlefield.

Key words : cyber operation, multi-layered COP, cyber situational awareness, cyber warfare

접수일(2020년 09월 29일), 수정일(1차: 2020년 10월 19일),
게재확정일(2020년 10월 28일)

* 국방과학연구소
** 한화시스템(주)
*** 국방과학연구소(교신저자)

1. 서 론

사이버작전은 사이버 공간 내 또는 사이버 공간을 통하여 주요 목적을 달성하기 위해 수행하는 작전활동으로, 육·해·공·우주 전장에 추가되는 제5의 전장이다. 물리작전의 목적과 마찬가지로, 사이버작전 역시 지휘관의 목표를 달성하기 위한 임무 수행을 목적으로하는 합동작전에 포함된다. 그러므로 사이버작전 단독으로 수행될 수도 있고, 타 작전과 동기화되어 수행될 수도 있어야 한다. 그러나 사이버작전의 수행 환경은 물리전과는 다른 여러 가지 특징들을 가진다. 사이버 전장은 물리 전장에 위치한 장비의 네트워크 연결 정보를 기반으로 생성되므로 지형 정보와 완전히 분리되어 있지 않으면서도, 물리적 공간 제약을 넘어서 네트워크 토폴로지 기반의 논리적인 연결과, 운영체제 및 소프트웨어의 사이버 정보와 보다 밀접한 연관성을 가진다. 또한 전략 제대에서 전술 제대까지 어디에서 어떤 형태로 발생하여 그 영향성이 어떤 임무 수행에까지 영향을 줄 수 있는지도 명확하지 않다는 광범위적인 특징도 가진다. 그러므로 사이버작전 수행을 위해서는 물리전과의 합동작전을 위한 전장환경 분석 뿐만 아니라, 사이버 전장의 특징을 분석 후 이를 물리전장과 연관하여 분석하는 활동 등 여러 관점에서의 환경분석과 상황인식이 필요하다.

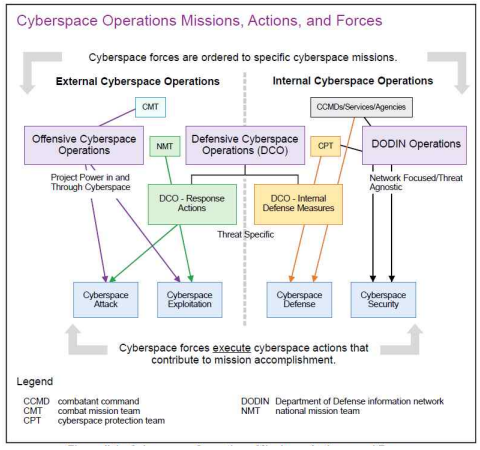
본 논문에서는 사이버작전 수행 및 지휘통제를 위해 반드시 필요한 사이버작전 상황도 개발을 위한 연구를 수행한다. 특히 멀티레이어드 개념을 적용한 시각화 기술을 기반으로 지리정보를 비롯한 사이버 자산, 위협, 임무 등 상호 연관분석이 필요한 여러 도메인의 정보를 상황도에서 직관적으로 도시할 수 있는 아키텍처를 제안한다. 본 연구를 통해 사이버 작전 수행을 위해 필요한 작전요소들이 멀티레이어드 계층의 도시요소로 표현되어, 복잡하고 이해하기 어려운 사이버 전장을 직관적으로 상황도를 통해 시각화하는 방안을 제안한다. 2장에서는 멀티레이어드 개념을 적용한 사이버작전을 위한 상황도에 대한 관련 연구를 분석한다. 3장에서는 본 논문에서 멀티레이어드 사이버작전 상황도를 위해 제안하는 아키텍처를 설명하고, 4장에서는 3장의 구조 기반으로 상황도를 개발하기 위한 연구 내용을 기술한다. 끝으로 결론에서는 본 논문에서 제안하는 상황도 개발을 통해 기대할 수 있는 사이버작전의 수행 목표와 향후 연구 방향을 기술한다.

2. 관련 연구

2.1 사이버 전장 및 작전

사이버 공간은 네트워크 및 컴퓨터가 창출하는 가상공간으로, 무형의 사이버 관련 정보가 교환되고 공유되는 영역이다. 물리전장의 공간은 지리적인 속성 중심으로 정보를 표현할 수 있으나, 사이버전장의 공간은 네트워크 속성을 중심으로, 자산 계층, 위협 계층, 페르소나 계층 등 여러 계층을 기준으로 표현될 수 있다.

미군은 [1]을 통해 물리적 공간과 정보 공간의 일부인 사이버 공간과는 밀접하게 연관되어 있다고 정의하고 있다. 왜냐하면 사이버 공간을 창출하는 요소 장비들이 모두 육·해·공·우주 전장 내에 위치하고 있기 때문이다. 물리적 전장에서 사용되는 장비가 점차 컴퓨팅 환경을 가지는 장비로 진화하고, 각 장비들이 모두 네트워크 내에 연결되어 물리적인 제약없이 연동될 수 있는 네트워크 중심전 환경이 되었기 때문에, 사이버 전장 내의 사이

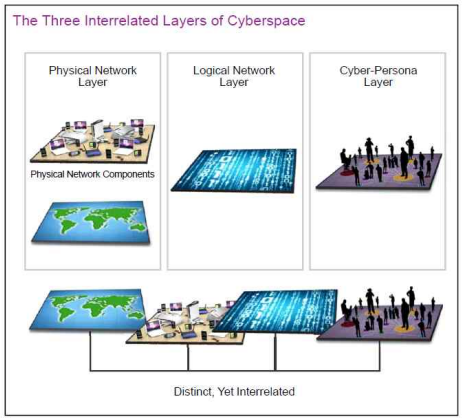


(그림 1) 사이버전장 내 작전 및 임무[1]

버 위협의 중요성이 대두되었기 때문이다. 물리 전장 내 구성 장비가 없이는 사이버 전장도 생성되지 않기 때문에, 사이버전장이 독립전장이 아니라 물리전을 기반으로 한 합동전장 내에 포함된다.

미군은 (그림 1)과 같이 사이버작전을 크게 내부적 사이버작전과 외부적 사이버작전으로 구분하고, 구체적인 작전 형태를 방어적, 공세적, 네트워크 작전으로 정의하였다. 해당 3가지 작전 형태는 사이버공간 공격, 사이버공간 분석, 사이버공간 방어, 사이버공간 보안의 기능으로 구분되며, 해당 부대는 임무 완수에 기여할 수 있도록 위의 기능을 포함한 과업들을 수행한다.

미군 사이버작전 교리는 이런 모호한 사이버공간의 특징을 명확하게 정의하여 사이버작전을 수행하고자, (그림 2)와 같이 3개의 계층-물리적 네트워크, 논리적 네트워크, 그리고 사이버 페르소나 계층-으로 사이버공간을 구성했다[1]. 물리적 네트워크 계층은 하드웨어적인 컴퓨팅 장비, 네트워크 장비, 유무선 네트워크 등 주변 환경으로 구성된다. 일반적으로 서버, 단말, 네트워크 장비 등 실제 형상을 갖고 물리적인 위치를 표현할 수 있는 실물 위주의 정보가 물리적 네트워크 계층에 표현된다. 논리적인 네트워크 계층은 물리적 네트워크 계층의 장비들이 서로 연결된 네트워크를 의미하며, 네트워크를 동작하는 논리적인 프로그래밍 소프트웨어를 포함한다. 실물 장비가 가지고 있는 IP나 port 정보, 타 장비와의 네트워크 형성 정보, 운영체제를 비롯해 응용 프로그램까지 물리



(그림 2) 사이버 공간의 연관 레이어[1]

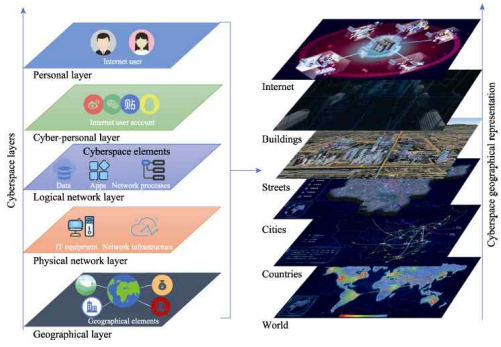
장비에서 운용되는 소프트웨어들에 대한 정보가 모두 논리적인 네트워크 계층에서 표현된다.

사이버 페르소나 계층은 사이버 행위를 수행하는 주체나 집단의 정체를 논리 네트워크에 적용하여 표현하는 계층이다. 개인이나 단체가 사용하는 시스템 계정 정보, email, SNS ID 등이 사이버 페르소나 계층에 표현 가능한 정보이다. 일반 개인도 한 사람이 여러 시스템 계정이나 email ID를 가지고 있기 때문에, 사이버 페르소나와 실제 인간과의 관계는 다대다(N:M) 관계를 형성하게 되어 실존하는 인물 정보보다 방대하고 복잡한 정보가 생성될 수밖에 없다.

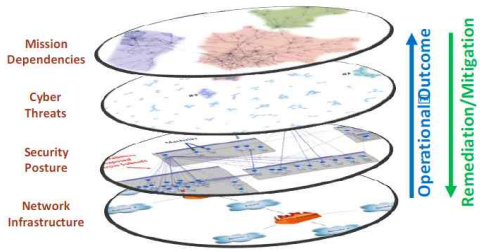
사이버작전은 물리적 계층과 논리적 계층 뿐만 아니라, 여러 계층에 존재하는 복잡한 정보들이 서로 밀접하게 연관되어 있다. 각 계층별로도 정보 분석을 수행해야 하지만, 계층간의 연관분석을 통해서도 추가적인 지휘결심 지원 정보를 획득할 수 있다. 사이버정보 및 첩보는 장비, 연결성, 인물정보 등이 총괄적으로 포함되어 여러 도메인에서 서로 다른 형태로 동시에 나타나기 때문에, 각기 다른 이벤트로 인지될 수 있어, 적의 정확한 의도나 활동을 파악하기 위해서는 반드시 데이터 연관분석을 수행해야 한다.

2.2 멀티레이어드 시각화 개념

사이버 공간은 IP 주소를 사용하여 네트워크로 연결된 장비들의 연결상태를 표현하는 네트워크 맵을 기반으로 표현된다. 네트워크 맵 상의 가상 공간 정보와 실제 장비가 물리적으로 위치한 실제 공간 정보와



(그림 3) 사이버공간의 멀티레이어 표현[2]



(그림 4) CyGraph에서 제안한 사이버 전장 계층[3]

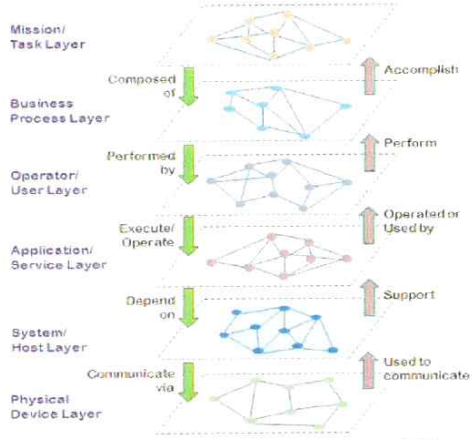
의 연관성은 사이버전장을 이해하는데 반드시 필요하다. 그러나 사이버전장을 단순히 물리 계층과 네트워크 맵 계층으로만 구분한다면, 사이버 위협을 분석하기 위한 연관관계를 맵핑하기에 연관성이 부족하다[2]. [1]에서 정의한 3가지 계층보다 상세하게 [2]에서는, (그림 3)과 같이 사이버 공간을 물리적 계층, 실 네트워크 계층, 논리적 계층, 사이버 페르소나 계층, 사용자 계층의 총 5개의 계층으로 구성하는 시각화 개념을 제안하였다.

MITRE는 사이버 위협으로부터 임무지속성을 향상시키기 위해, Cygraph를 통해 계층별 속성 및 우선순위를 구분하였다[3]. 사이버 복원력을 분석하기 위해, 각 계층별 연관관계 표현은 반드시 필요하며 낮은 레벨은 상위 계층에 영향을 미치고 결국 임무지속성에 영향을 주기 때문이다. (그림 4)과 같이 임무 영향성을 기준으로 사이버 위협 계층을 구분하고, 논리적인 네트워크 토폴로지를 기반으로 실제 네트워크 장비 구성 계층을 위치하였다. CyGraph는 여러 관점별 분석 요구사항에 따라 여러 형태로 데이터 분석 결과를 표현하여, 상황인식, 리스크 분석, 선제적 예방 및 침해대응할 수 있도록 제안하였다[3].

이처럼 사이버공간을 표현하기 위해서는 정보의 연관분석이 용이하도록 다계층 형태로 화면을 제공하는 다양한 연구들이 진행중이다. 본 연구에서도 사이버 임무지속성 및 사이버 복원력 향상을 위해, 사이버전장 상황 내 연관정보 분석을 위한 멀티레이어드 상황도를 제안한다.

2.3 사이버작전 상황도

사이버작전 환경에서의 상황인식은 사이버 공간과 아군 및 적군에 영향을 미치는 모든 환경을



(그림 5) 멀티레이어드 사이버 상황도 개념[5]

인식할 수 있어야 한다. 상황인식의 목적은 현재 상황을 신속하게 인지할 수 있어야 할 뿐만 아니라, 작전 수행을 위해 향후 발생 가능한 상황에 대비할 수 있는 정보를 제공해야 한다. 지휘관은 신속하고 직관적인 상황인식을 위해 도시요소로 구성된 공통작전상황도를 사용해 작전환경을 지속적으로 평가한다.

전장정보관리체계에서의 상황도는 디지털 지도를 배경으로 지휘관의 실시간 전장상황 인식을 위하여 투명도 및 다양한 전술자료를 중첩 전시하는 기능을 수행한다. 가시적인 전장상황을 제공함으로써 작전계획 수립과 상황판단에 필요한 도구로 사용된다. 공통작전상황도(Common Operational Picture, COP)는 가용한 정보의 표현 도구이며, 상황인식은 COP의 정보를 이해하면서 획득된 지식 행위를 의미한다[4]. 지휘통제를 위한 COP은 서로 다른 위치나 환경에 있는 사람들이 공통작전상황도를 통해 동일한 임무와 작전을 인지하고 수행할 수 있도록 정보를 동기화하는 도구로, 국방C4I를 포함한 상황인식 시스템의 중요한 분석도구로 사용되고 있다.

사이버 공통작전상황도는 사이버 공간의 각 영역에 대한 우호적, 중립적, 적대적 환경을 그림으로 표현해야 하며, 이를 위해 사이버센서로부터 수집된 데이터를 융합하고 연관분석하여 표현해야 한다. 사이버 공통작전상황도는 단일의 군사전략

목표 달성을 위해, 지상, 해상, 공중, 우주 작전이 실시되는 지리적 영역을 표현하는 전구작전영역에 사이버 영역을 추가하여 표현함으로써, 모든 전장을 포함해 합동작전을 수행할 수 있도록 지원할 수 있어야 한다.

[5]에서는 사이버전장의 속성별 계층을 6개로 구분하고, 각 계층별 연관성을 (그림 5)와 같이 분석하였다. 최상단에 수행중인 임무 계층을 표현하고, 그 아래에 비즈니스 프로세스 계층, 사용자 계층, 응용 서비스 계층, 시스템 호스트 계층, 물리적인 장비 계층으로 구분하였으며, 각 계층간 연관 속성을 표현함으로써 여러 계층의 속성을 한 화면에서 멀티레이어드로 표현하면 얻을 수 있는 정보의 속성도 연구하였다. 사이버전장의 지휘통제를 위해 이러한 계층별 속성이 분석되기 위해 개발되어야 하는 시스템 컴포넌트를 제안하였고, 최종적으로 사이버 위협 발생시 임무에 어떤 영향을 끼치는지에 대한 연구를 수행하였다.

본 연구에서는 사이버 자산 계층, 사이버 위협 계층, 임무 계층을 중심으로 지휘관이 사이버작전 수행에 필요한 정보를 계층으로 표현하고, 이들간의 연관관계를 한 화면에 3D로 시각화하여, 지휘관이 빠르게 상황을 인식해 적시에 사이버작전을 수행하도록 지원하는 사이버작전 상황도를 제안한다.

3. 멀티레이어드 개념을 적용한 사이버작전 상황도 아키텍처

본 연구에서는 실시간 사이버 상황인식 및 사이버작전 수행 현황을 다차원 뷰로 시각화하는 기술을 적용하여, 사이버작전 수행을 위한 사이버작전 상황도 구조를 제안한다. (그림 6)과 같이 본 연구의 사이버작전 상황도(Multi-layered COP, 이하 MLCOP)는 크게 상황도 도시, 상황도 관리, 임무기능 도시의 3가지 기능을 가진다. 제안하는 상황도는 멀티레이어드 개념을 적용한 사이버전장 분석을 위해 사이버 자산 계층, 사이버 위협 계층, 임무 계층으로 구성하고, 각 계층별로 필요한 도

(그림 6) MLCOP 기능 구성도

시요소를 연구하여 페르소나 계층, 장비 관리자 계층 등 필요한 계층을 추가하여 직관적 시각화를 통해 상황인식을 수행할 수 있도록 지원한다. 특히, 사이버작전을 수행하는 전략적 제대에서부터 전술적 제대에 이르기까지 광범위한 운용자가 사용할 수 있도록, 운용자의 drill-down/roll-up을 통해 도시요소 수준을 다르게 제공하여 제대별 원하는 정보 수준에 맞는 맞춤형 상황도 화면을 제공한다. 상황도를 위한 시각화 DB는 일반적인 상황도 COP에서 사용되는 관계형 DB와, 사이버전장의 정보를 관리할 수 있는 빅데이터 DB를 포함하는 구조로 구성되도록 제안한다.

최근 국방C4I 상황도가 웹 기반의 non-plugin 방식으로 개발되고 있으므로, 본 연구에서도 HTML5 웹 표준[6]을 기반으로 상황도를 개발하고 있다. (그림 7)에서와 같이 데이터베이스를 사용하는 웹 서비스를 기반으로 개발하여, 별도의 클라이언트 SW를 설치하지 않고도 웹브라우저를 통해 상황도를 사용할 수 있도록 사용자 편의성을 제공한다.

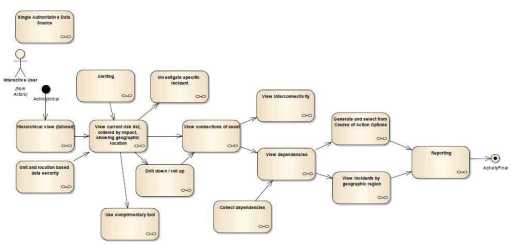
또한, MLCOP은 사이버작전 뿐만 아니라 물리작전과의 연계성을 표현하고 타 체계와의 연계를 위해 국방C4I와의 연동성을 고려하여 개발하고 있다. 일반적인 국방C4I가 지형정보 기반의 물리적 지형에서 수행되고 있으므로, MLCOP의 물리적 지형 도시는 지형정보 기반의 물리뷰를 통해 도시하고, 사이버 지형은 네트워크 토폴로지 기반의 논리뷰를 통해 도시하여, 물리 전장과 사이버 전장을 연결하여 인식할 수 있도록 연관분석 뷰 기능을 제공한다. MLCOP의 물리뷰는 타 국방 전

(그림 7) HTML5 웹 기반 MLCOP 시스템 구조도

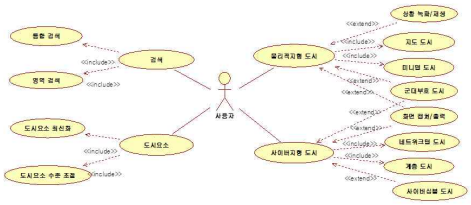
장관리체계와의 연동성 및 합동작전 수행 환경을 고려해, 국방 C4I의 상황도 기능과 동일하거나 유사한 기능을 지원할 수 있도록 개발하고 있다. 국방 C4I의 공통작전상황도와 마찬가지로, 지형 정보 기반으로 현재 군에서 사용하고 있는 MND-STD-2525C 기반 군대 부호를 사용하여 현재 군 작전상황을 표시하고, 작전활동부호를 투명도를 통해 표시할 수 있도록 개발하고 있다.

사이버 지형 기반의 MLCOP 논리뷰는 사이버전을 위해 네트워크 맵 중심으로 개발하고 있다. 네트워크 토폴로지 형태를 기본으로 하되, 군의 제대별 특성에 맞춰 hierarchical layout, force-direct layout[7] 등 다양한 layout 알고리즘을 적용하면서 사이버작전 상황에 적합한 네트워크 토폴로지 레이아웃으로 개발할 예정이다.

본 연구에서는 NATO에서 사이버 상황인식 시스템 개발을 위해 발행한 RFI(Request for Information)를 분석하여[8], 사이버 상황인식 시스템의 시각화 기능이 가져야 하는 기본적인 기능에 대해 분석했다. NATO는 3가지 시나리오를 제시하였는데, (그림 8)과 같이 APT 공격에 대한 대응을 위해 상황인식 시스템이 가져야 하는 기능에 대해 flow diagram으로 표현하고 각 기능에 대한 use case를 기술하였다. 본 연구에서는 [8]에 제



(그림 8) NATO RFI 시나리오 [8]



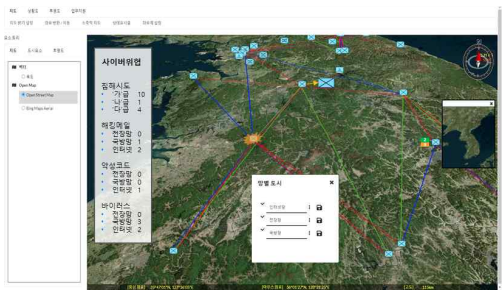
(그림 9) MLCOP use case 예시

시된 use case를 분석하여, MLCOP의 사용자 기능을 도출하고 (그림 9)과 같은 use case로 표현하였다.

4. 사이버작전 상황도 개발

MLCOP 상황도는 크게 물리뷰, 논리뷰로 구성되어, 물리 전장과 사이버 전장을 표현한다. 특히 네트워크 토폴로지를 기반으로 하는 논리뷰에서는 3D 형태로 계층간 연관관계를 한 화면으로 도시하는 기능도 갖추고 있으며, 사이버 전장에 대한 상황인식 뿐만 아니라 시공간 시각적 분석 수행을 위한 분석 기능도 개발될 예정이다.

(그림 10)과 같이 MLCOP의 물리뷰는 기존 국방 C4I 상황도와 최대한 유사한 형태와 기능을 제공하도록 개발하고 있다. 이는 지휘관이 상황도에 대한 이질감을 최대한 적게 느끼면서, 합동작전 수행에 사이버작전이 기여할 수 있도록 기존 상황도 기능을 최대한 준용하고자 하는 목적이다. 군대부호와 투명도 기능은 MND-STD-2525C를 기반으로 하되, 사이버작전 및 상황을 나타내는 심볼을 신규로 개발하거나 MIL-STD-2525D에서 일부 정의된 사이버 심볼을 적용하는 방안을 연구



(그림 10) MLCOP 물리뷰 예시

(그림 11) MLCOP 사이버 상황도 엔진 기능도

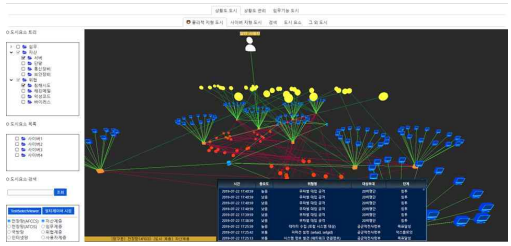
중이다. 또한 군대부호의 notation 내에 사이버 상황을 추가적으로 기술하거나, 현재 물리전장에서 사용중인 심볼을 사이버 전장에 맞게 재해석하는 방안 등 여러 가지 도시요소를 개발하고 있다.

MLCOP은 HTML5 웹 표준을 사용함으로써 국방C4I에서 사용하던 Active-X 또는 플래시 등 별도의 외부 플러그인을 설치하지 않고도, 다양한 2D 및 3D 그래픽 형태를 지원하는 장점을 가진다.

또한 국방C4I 상황도 엔진에 사이버작전 도시요소 기능을 추가한 MLCOP에 최적화된 사이버작전 상황도 엔진을 포함해 개발하고 있다. (그림 11)과 같이 사이버 상황도 기능을 라이브러리 형태의 엔진으로 개발함으로써, 국방C4I와 같이 지형정보단 지도 기반으로 물리적 지형을 도시할 수도 있고, 상황도 내 기능들을 API를 이용하여 개발할 수 있도록 인터페이스를 제공한다. 가시성 분석 또는 지형분석과 같이, 기존 물리상황도 엔진에서는 사용하지만 사이버전장에서는 사용하지 않는 기능은 엔진에서 제외하여, 사이버작전 상황도에 필요한 기능에 최적화된 엔진으로 개발하고 있다.

물리뷰가 국방 C4I와 같이 부대별 위치 정보를 기반으로 표현된다면, (그림 12)와 같이 논리뷰는

(그림 12) MLCOP 논리뷰 예시



(그림 13) MLCOP 계층간 연관분석뷰 예시

네트워크 연결상태를 토폴로지 형태로 표현한 네트워크 맵 기반으로 표현된다. 한국군의 국방 네트워크는 크게 전장망, 국방망, 인터넷망으로 구성되므로, 각 망 별 네트워크 상태를 한 눈에 알아볼 수 있도록 입체도형 형태로 네트워크를 도시하였다. 물리뷰에서와 달리 논리뷰에서는 사이버 자산에 발생한 위협을 상세하게 분석할 수 있고, 공격 그래프 분석 등을 통해 향후 공격이 발생할 가능성이 높은 자산에 선제적인 대응방책을 적용할 수도 있도록 기능을 개발중이다. 논리뷰는 사이버 자산 계층을 기반으로 표현되나, 좌측 분석 메뉴에서 해당하는 도시요소를 선택 및 필터링하여 원하는 상황인식 및 사이버전장 분석을 수행할 수 있다.

논리뷰를 기준으로 여러 계층간 연관관계를 한 화면에 표현하기 위해 본 연구에서는 (그림 13)과 같은 계층별 연관관계를 분석할 수 있는 멀티레이어 계층 도시 기능을 제공한다. 연관관계 분석을 통해 지휘관은 특정 위협을 단편적인 정보로만 인식하지 않고, 여러 정보를 연관분석한 결과를 바탕으로 향후 예측 가능한 정보를 추론하는 전장지식을 획득할 수 있다. MLCOP은 자산, 위협, 임무 계층 등 여러 계층에 대한 연관 분석 결과를 설정 메뉴를 통해 가변적으로 제공함으로써, 사이버작전의 임무 영향성을 용이하게 분석하고, 복잡하고 상호의존도가 높은 사이버보안 관련 정보를 정제해서 분석할 수 있도록 지원할 예정이다.

5. 결론 및 향후 연구

사이버전장의 중요성은 현대전이 네트워크 중심

전으로 발전되면서 더욱 강조되고 있다. 물리전장의 무기체계 장비들이 IP와 같은 논리적 정보로 연결되고, C4I 체계와 연동하여 복합적인 작전을 수행해야 하는 현대전에서, 제 5의 전장인 사이버 전장에서의 우세는 물리작전 및 합동작전 수행에 필수적인 조건이 되었다. 이처럼 사이버전장에서의 우위 달성을 위한 사이버 작전을 수행하기 위해서는, 지휘통제에서 반드시 필요한 공통상황도(COP)가 반드시 필요하다. 사이버전장에서의 작전 활동은 사이버 자산의 정보보호 관제 활동을 포함하여, 지휘관이 사이버 상황을 인식하고 작전을 계획·수행·평가하며, 합동작전과 연계해 타 C4I와 연동할 수 있도록 확장되어야 한다.

본 논문에서는 사이버작전에 특화된 상황도를 연구하고, 사이버작전 수행을 위해 멀티레이어드 개념을 적용한 사이버작전 상황도 구조를 제안하였다. 본 논문을 통해 멀티레이어드 사이버작전 상황도의 SW 아키텍처, 구조, 기능 등에 대해 기술하고, 사이버작전을 위해 여러 계층으로 표현되는 정보들을 한 화면에 표현하기 위해 연관분석 뷰 기능을 포함한 상황도 화면 및 관련 기술을 제안하였다.

향후 연구를 통해 사이버작전의 수행 범위를 고려하여, 전략급, 작전급, 전술급 부대의 사이버작전 및 업무 수행을 고려한 계층적 도시요소 시각화 기능을 개발할 예정이다. 또한 사이버전장을 시간적, 공간적으로 분석하면서 지휘통제를 수행할 수 있도록 시공간 시각적 분석 기능을 추가적으로 개발하여, 복잡하고 연관성이 높은 사이버 정보간의 연관관계를 시각적으로 분석하는 기능을 개발할 예정이다.

참고문헌

[1] DoD Joint Publication 3-12, “Cyber Operations”, June 2018.

[2] Chundong Gao et al., “Theoretical basis and technical methods for cyberspace geography”, Journal of Geographical Sciences, 2020.

[3] S. Noel, D. Bodeau, and R. McQuaid, ‘Big-Data Graph Knowledge Bases for Cyber Resilience,’ in NATOIST-153 Workshop on Cyber Resilience, 2017.

[4] 김의순, “지휘통제능력 향상을 위한 COP(공통작전상황도) 개선방안”, 한국국방연구원 주간국방논단, 2017.

[5] Yi Cheng et al., “Integrated situational awareness for cyber attack detection, analysis, and mitigation”, Proc. SPIE 8385, Sensors and Systems for Space Applications, 2012.

[6] World Wide Web Consortium, http://www.w3.org/TR/2014/REC-html5-20141028/.

[7] Zhongyan Liang et al, “Research on Auto-Drawing Technology of Orthogonal Network Topological Graph with High Degree Nodes”, International Conference on Network, Communication, Computer Engineering (NCCE), 2018.

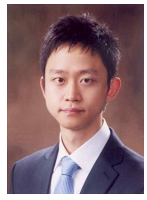
[8] NCI Agency, “CO-14068-MNCD2” RFI, 2015.

〔저자소개〕

권 구 형 (Koohyung Kwon)
2001년 2월 고려대학교 전기전자전파공학 학사
2003년 2월 고려대학교 전파공학과 석사
2006년 7월~ 현재 국방과학연구소 재직
email : koohyung@add.re.kr

김 선 영 (Sonyong Kim)
2019년 2월 고려대학교 전기전자전파공학 학사
2019년 1월 ~ 현재 한화시스템 재직
email : sonyong.kim@hanwha.com

고 장 혁 (Jang-hyuk Kauh)
1996년 2월 광운대학교 컴퓨터과학과 학사
1998년 2월 광운대학교 컴퓨터과학과 석사
2018년 8월 광운대학교 컴퓨터과학과 박사
1998년 3월 ~ 현재 국방과학연구소 재직
email : jhkauh@add.re.kr



김 종 화 (Jonghwa Kim)
2009년 2월 고려대학교 전기전자전파공학 학사
2009년 1월 ~ 현재 한화시스템 재직
email : jonghwa3.kim@hanwha.com

오 행 록 (Haengrok Oh)
1987년 2월 인하대학교 전산학과 학사
1989년 2월 인하대학교 전산학과 석사
2004년 고려대학교 컴퓨터학과 박사 수료
1989년 ~ 현재 국방과학연구소 재직
email : haengrok@add.re.kr

이 재 연 (Jaeyeon Lee)
2002년 2월 가톨릭대학교 정보통신학사
2004년 2월 광주과학기술원 정보통신 석사
2004년 2월 ~ 현재 한화시스템 재직
email : jaeyeon46.lee@hanwha.com