JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 22, No. 11, pp. 1923-1930, Nov. 2021

Check for updates

사이버작전 상황도 구현을 위한 사이버 심볼 연구동향 및 발전방향

이 종 관[1] · 이 민 우[2*] · 권 구 형[3] · 고 장 혁[3] · 오 행 록[3] · 김 선 형[4]
[1]육군사관학교 컴퓨터과학과 부교수
[2*]아주대학교 국방디지털융합학과 대우부교수
[3]국방과학연구소 연구원
[4]한화시스템(주) 연구원

Research Trends and Future Directions of Cyber Symbology for Common Operational Picture in Cyber Operations

Jongkwan Lee[1] · Minwoo Lee[2*] · Koohyung Kwon[3] · Janghyuk Kauh[3] · Haengrok Oh[3] · Sonyong Kim[4]

[1]Associate Professor, Department of Computer Science, Korea Military Academy, Seoul 01805, Korea
[2*]Adjunct Professor, Department of Military Digital Convergence, Ajou University, Suwon 443-749, Korea
[3]Researcher, Agency for Defense Development, Seoul 05661, Korea
[4]Researcher, Hanwha Systems Co., Ltd, Seongnam 13437, Korea

[요 약]

본 논문은 사이버작전 상황도 구현을 위한 사이버 심볼 연구 동향을 분석하고 한국군 사이버작전 상황을 고려한 사이버 심볼의 발전방향을 제시한다. 사이버 공간에서의 취약점을 이용한 군사적, 경제적 위협이 지속적으로 증대함에 따라 사이버전 역량 강화에 대한 관심이 크게 증대되고 있다. 이에 따라 효과적인 사이버작전 수행을 위한 사이버작전 상황도의 필요성이 최근 제기되고 있다. 그런데 사이버 작전은 물리적 작전과 근본적으로 다른 특성을 갖고 있으므로 물리적 작전을 위해 현재 사용되고 있는 작전 상황도와 군사심볼을 사이버 작전에 그대로 적용하는 것은 제한적이다. 이에 따라 본 논문은 이러한 제한사항을 극복하기 위한 다양한 연구 동향을 분석하고 사이버 심볼의 발전 방향을 제시하였으며, 이는 한국군의 사이버 심볼 표준화 및 사이버작전 상황도의 효과적 구현에 기여할 수 있을 것으로 기대된다.

[Abstract]

We analyze the research trends related to a common operational picture for cyber operations and suggest development direction. As military and economic threats using cyberspace vulnerabilities continue, interest in improving cyber capabilities and preparing for cyber warfare is increasing. Meanwhile, the need for a common operational picture for cyber operations has recently been raised. However, since cyber operations are fundamentally different from kinetic operations, it is limited to using the existing military symbols and common operational picture. We analyze the various research to overcome these limitations and suggest the development direction, including cyber symbol standardization issues. We expect that our research result will contribute to the standardization of cyber symbols of the Korean military and the effective implementation of the cyber operational pictures.

색인어 : 사이버작전, 공통작전상황도, 합동작전, 군사심볼
Keyword : Cyber Operation, Common Operational Picture, Joint Operation, Military Symbol

http://dx.doi.org/10.9728/dcs.2021.22.11.1923

Received 06 October 2021; **Revised** 25 October 2021
Accepted 25 October 2021

***Corresponding Author; Minwoo Lee**

Tel: +2-2197-2855
E-mail: iminu@ajou.ac.kr

Ⅰ. 서 론

북한은 비대칭 전력의 하나로 사이버전 역량을 지속적으로 강화하고 있다. 2011년 정부기관 및 민간업체 등 40개 웹사이트에 가해진 3·4 DDoS(Distributed Denial of Service) 공격, 2013년 주요 언론사 및 금융사의 전산망을 마비시킨 3·20 전산 대란, 2014년 12월 한국수력원자력의 원전 도면 유출사건, 2016년 국방통합데이터센터(DIDC: Defense Integrated Data Center) 해킹에 의한 군사기밀 유출사건 등 북한의 사이버 전력은 우리에게 실질적인 피해를 가져왔다. 최근 북한은 사이버 역량을 외화벌이 수단으로 활용하고 있다. 유엔 안전보장이사회 산하 대북제재위원회 전문가 패널 보고서에 따르면 북한은 2015년부터 2019년 5월까지 최소 17개국의 금융기관과 가상화폐 거래소를 대상으로 35차례의 사이버 공격을 감행하였으며 이를 통해 최대 20억 달러를 탈취했다고 밝혔다. 최근 북한은 사이버 공격을 군사적 목적보다는 경제적 이익 추구에 집중하고 있는 것으로 보인다. 하지만 공격의 목적만 상이하고 이를 구현하기 위한 수단과 방법은 유사하므로 북한의 사이버 역량이 군사적 목적으로 언제든지 전환될 수 있음을 간과해서는 안 된다.

한편, 작전은 독자적으로 수행되는 것이 아니라 팀 단위, 부대 단위로 협업이 필요한 고도로 조직화된 복잡한 과업이다. 따라서 작전에 참여하는 모든 구성원이 같은 상황을 인식하고 이해하는 것은 매우 중요하다. 공통작전상황도(COP: Common Operational Picture)는 복잡한 작전상황을 추상화하여 전투원들이 신속하고 정확하게 작전상황을 이해하고 상호 공유하기 위해 사용되는 가장 중요한 수단이다. 사이버작전에서도 사이버작전을 위한 공통작전상황도의 필요성이 지속적으로 제기되고 있으며, 이를 구현하기 위한 다양한 방법론들이 제시되었다[1-5]. 관련 연구의 방향은 크게 2가지로 구분할 수 있다. 첫 번째는 사이버 공간에서의 사이버 객체와 상황을 표현하기 위한 심볼의 표준화 연구이다. 두 번째는 사이버작전 상황도 구성 및 개발 방안에 관한 연구로 사이버 상황 자체를 표현하는 것뿐 아니라 물리작전과 사이버작전과의 연관 관계를 효과적으로 나타내기 위한 방법론에 관한 연구이다. 사이버 심볼은 사이버작전 상황도의 중요한 구성요소 중 하나이기 때문에 사이버 심볼 표준화 연구와 사이버작전 상황도 개발 방법론 연구는 상호 밀접한 관계가 있다.

사이버작전 상황도 구현을 위하여 사이버 심볼 정의의 연구가 필요하다는 공감대가 형성되어 있다. 하지만 한국군 작전환경을 고려한 사이버 심볼 정의에 대한 구체적인 방법론과 사이버작전 상황도 구현 기술에 관한 연구는 매우 미진한 상태이다[6], [7].

본 논문에서는 사이버작전 상황도 개발과 연계된 사이버 심볼 표준화에 대한 주요 연구동향을 분석하고 이를 토대로 미래 사이버작전 환경을 고려한 사이버작전 상황도의 발전방향을 개념적으로 제시한다. 본 논문의 구성은 다음과 같다. 2장에서 사이버작전 상황도에 대해서 설명하고, 3장에서 사이버 심볼과 관련된 연구동향을 분석한다. 4장에서는 3장에서 분석한 연구동향을 바탕으로 한국군의 사이버작전 상황도 구현을 위한 사이버 심볼의 발전방향을 구체적으로 제시한다. 마지막으로 5장에서 연구결과를 요약하고 결론을 맺는다.

Ⅱ. 사이버작전 상황도 구현을 위한 사이버 심볼

2-1 공통작전상황도와 군사심볼

공통작전상황도는 급변하는 복잡한 전장상황을 추상화하여 표현하고 전자적인 방법으로 공유함으로써 전투원의 상황인식, 전장기능별 전투협조, 지휘관의 의사결정 등을 지원하는 수단이다.

현재 한국군은 각 제대, 전장기능별, 전장 영역별로 다양한 상황도를 개별적으로 작성, 관리하고 있으며, 모든 전장요소들이 통합된 종합상황도는 개별 상황도의 자동 통합이 아닌 수동 통합을 통해 관리하고 있다. 한편, 상황도에 수집된 데이터를 단순히 나열하는 것이 아니라 데이터를 융합, 분석하여 가공된 형태의 데이터를 도시하고, 데이터의 수집도 자동화하는 방향으로 상황도 구현이 발전하고 있다.

육군 군단급 이하 제대의 C4I(Command, Control, Communication, Computer, Intelligence) 체계인 ATCIS(Army Tactical Command Information System) 2차 체계는 피·아 전투력 수준 자동산출, 최적 공격방법 및 부대 추천 등 23개의 분석 기능이 포함되어 있다. 해군은 해군지휘통제체계 성능개량 사업을 통해 KNCCS(Korea Naval Command Control System) 중심으로 해군전술자료처리체계(KNTDS: Korean Naval Tactical Data System), 디지털전문처리체계(DMHS: Digital Message Handling System), 실시간 문자망을 통합하여 ISR(Intelligence, Surveillance, Reconnaissance) 데이터 융합 기능을 보강하였다. 공군은 중앙방공통제소(MCRC: Master Control And Reporting Center)를 중심으로 한국전구의 공중 전술정보를 융합하고 이를 이용하여 한국연동통제소(KICC: Korea Interface Control Cell)에서 공통작전상황도를 생성한다. 미군의 경우 전통적인 공통작전상황도에 연관된 모든 정보를 확인할 수 있도록 발전된 IR-COP(Inter-Related COP)을 개발하여 운영 중이다. 전투원은 가시화된 전장의 전술정보를 이용하여 전장 상황을 이해한다. 따라서 시각적으로 전술정보와 해당 데이터의 속성을 적절히 표현하는 방법의 필요성이 더욱 증가하고 있다.

군사심볼은 이러한 역할을 수행하는 표준화된 기호체계로 오랫동안 발전해 왔다. 대표적으로 미군과 NATO의 군사심볼 체계가 있는데 부호 생성 규칙, 부호 형태와 의미 등이 서로 유사하다[8]-[12]. 한국군은 미군의 군대부호체계를 준용하여 사용하고 있으며, 합동작전 및 연합작전시 상호운용성을 보장하는 데 큰 역할을 하고 있다. 현재의 군사심볼들은

지상, 해상, 공중, 우주 등 비사이버 공간에서의 부대, 장비, 시설, 작전활동 등을 효과적으로 표현할 수 있다. 하지만 물리작전을 표현하기 위한 심볼로 사이버 공간에서의 작전을 표현하는 것은 적절하지 않다. 이는 사이버작전은 물리적 공간이 아닌 사이버 공간에서 수행되고, 사이버작전 수행을 위한 수단과 절차가 물리 작전과 근본적으로 다른 측면이 있기 때문이다. 한편, MIL-STD-2525D 부록 L에서 사이버 군사심볼을 일부 정의하고 있지만 심볼의 수가 매우 적고 부가정보를 기술하는 구체적인 절차가 누락되어 있어 다양한 사이버작전 상황을 표현하는데 제한적이다. 그뿐만 아니라 심볼의 아이콘들이 영문자 3개로 구성된 약어로 정의되어 있어 직관적인 이해가 어렵다. 이러한 문제를 해결하기 위해 사이버작전 상황을 효과적으로 표현하기 위한 여러 시도와 연구가 진행되고 있다.

2-2 사이버 계층과 사이버 심볼

물리 작전의 효과적인 수행을 위해 공통작전상황도가 필수적으로 필요하듯 사이버작전을 위한 별도의 공통작전상황도에 대한 필요성이 지속해서 제기되어 왔다. 하지만 근본적으로 가시적이지 않은 공간을 가시적으로 표현해야 한다는 어려움과 사이버작전 개념과 수행체계에 대한 모호함 때문에 사이버작전 상황도 연구에 대한 큰 진척은 없는 상태이다. 본 절에서는 사이버 계층과 사이버작전 상황도 구현을 위해 필요한 사이버 심볼을 정의할 때 고려해야 하는 사항들을 살펴본다.

1) 사이버 계층

사이버작전 상황도 구현을 위해서는 사이버공간을 특징에 따라 계층적으로 구분하는 것이 효과적이다. 사이버 계층은 관점에 따라 다양하게 구분될 수 있다.

먼저 사이버공간을 작전 관점에서 보는 경우 물리적 네트워크 계층(Physical Network Layer), 논리적 네트워크 계층(Logical Network Layer), 사이버-페르소나 계층(Cyber-Persona Layer)의 3개 계층으로 구분한다. 물리적 네트워크 계층은 정보의 저장, 전송, 처리를 위한 기반시설과 장치들을 지칭한다. 논리적 네트워크 계층은 사이버공간을 통해 접근할 수 있는 자원들을 지칭하며, 네트워크, 소프트웨어가 탑재되어 운영 중인 장치 등을 포함한다. 사이버-페르소나 계층은 사이버공간에 만들어진 추상화된 데이터를 지칭하며, 웹 페이지, 계정, 이메일, 채팅 등을 포함한다. 이러한 관점은 미군의 합참교리 JP 3-12(Cyberspace Operation)에 나타나 있다[13].

사이버 전력의 방어 또는 복원력(resilience) 관점에서 사이버공간을 임무 의존성(Mission Dependencies), 사이버 위협(Cyber Threat), 보안 태세(Security Posture), 네트워크 인프라(Network Infrastructure)의 4개 계층으로 구분한다. 네트워크 인프라 계층은 네트워크 환경의 기술적, 정책적 상태를 보여준다. 보안 태세 계층은 자산의 취약점과 잠재적 공격 경로를 맵핑하여 네트워크 인프라 계층과의 연계성을 보여준다. 사이버 위협 계층은 실제 사이버 공격의 징후, 지표 그리고 보안 태세 계층 사이의 상관성(correlation)을 보여준다. 임무 의존성 계층에서는 조직의 임무와 사이버 자산 사이의 관계를 보여준다[10].

사이버작전에 대한 지휘통제 관점에서 사이버공간을 보는 경우에는 미 합참의 3개 사이버 계층에 지휘통제 계층(Command & Control Layer)과 지리 계층(Geographic Layer)을 추가한다. 지휘통제 계층은 사이버작전에 대한 감독 및 권한을 의미한다. 예를 들어 DDoS 공격을 위한 봇넷(BotNet), C2(Command & Control) 노드, 시스템 관리자 계정 등이 여기에 포함된다. 지리 계층은 전통적인 물리 작전을 의미한다. 이 때문에 지상, 해상, 공중, 우주와 전자기 스펙트럼 영역이 여기에 표시된다. 이와 함께 사이버공간의 물리적 구성요소들의 지리적 위치를 맵핑하여 보여준다[14].

2) 사이버 심볼 정의시 고려사항

사이버작전 상황도를 구현하기 위해서는 사이버 객체를 가시적으로 표현하기 위한 사이버 심볼에 대한 정의가 선행되어야 한다. 사이버 심볼을 정의하는 데 있어 고려해야 할 사항은 아래와 같다.

(1) 어떤 요소들을 사이버 심볼로 표현할 것인가?

물리작전의 군사심볼은 작전에 직·간접적으로 영향을 미치는 부대, 시설, 장비 등의 작전요소와 작전활동, 상태 등을 함축적으로 표현한다. 그런데 사이버작전에서 표현해야 하는 대상은 물리 작전에서 표현해야 하는 대상과 다를 수밖에 없다.

사이버작전은 네트워크 장비들로 형성된 가상의 공간에서 이루어지고 공격 대상과 보호해야하는 대상이 네트워크 장비 등의 물리적인 자산뿐 아니라 데이터 자체, 데이터에 대한 가용성 등이 추가된다. 또한, 사이버작전 활동을 물리 작전에서와 같이 크게 공격과 방어로 구분할 수 있겠지만 세부적인 활동 내용은 물리 작전에서의 활동과 근본적으로 다르다. 그뿐만 아니라 작전활동에 대한 결과도 물리 작전에서와 같이 단순히 무력화, 파괴 등으로 표현하기 애매한 경우가 많다. 결론적으로 사이버작전이 가지는 고유한 특성들로 인해 어떤 요소들을 사이버 심볼로 정의할 것인가에 관한 충분한 연구가 필요하다.

(2) 다수의 사이버 요소들의 관계를 어떻게 표현할 것인가?

사이버 공간에서 사이버 객체들은 독립적으로 운용되기보다는 다른 객체들과 연계되어 운용되는 경우가 대부분이다. 이러한 연계성이 단절되면 정상적인 역할을 수행하지 못하거나 제한적인 임무 수행만 가능하다. 또는 하나의 객체가 기능적으로 비정상일 때 이와 연계된 모든 객체가 영향을 받기도 한다. 따라서 사이버 객체 자체를 표현하는 것뿐 아니라 이들의 관계성을 표현하는 방법이 필요하다.

(3) 사이버 상황을 얼마나 세부적으로 표현해야 하는가?

사이버 상황을 통해 획득하고자 하는 정보의 수준은 제대별, 임무별로 상이하다. 네트워크 작전을 수행하는 전투원은 세부적인 피·아의 네트워크 구성도와 상태에 관심이 있을 것이다. 하지만 합동작전 지휘관은 세부적인 네트워크 구성 보다는 사이버 상황이 물리 공간에 미치는 영향 또는 물리 작전이 사이버 공간에 미치는 영향에 관심이 있을 것이다. 따라서 세부적인 네트워크 구성도 보다는 사이버 상황을 통찰할 수 있는 추상화된 표현이 필요하다. 사이버 상황을 이해하고자 하는 다양한 요구수준을 합리적, 선택적으로 수용할 수 있는 방안이 필요하다.

(4) 다른 영역의 상황도들과 어떻게 연계시킬 것인가?

사이버작전은 합동작전 차원에서 다른 영역의 작전들과 통합적으로 수행될 것이다. 따라서 타 영역의 상황도들과 통합되거나 연계되어 사이버 상황을 표현할 수 있어야 한다. 타 영역의 상황도에 사이버 심볼을 사용하는 것이 가장 쉬운 접근이다. 하지만 타 영역의 상황도는 물리적인 지형정보 위에 작전요소들이 표현되지만, 사이버작전 요소들을 물리적인 지형정보에 표현하는 것이 적절하지 않을 수 있다. 사이버 공간이 지형정보와 맵핑되지 않을 수도 있고, 사이버 심볼을 지형정보와 함께 표기했을 때 정보의 왜곡이 발생할 수도 있다. 물리 공간에서의 거리와 사이버 공간에서의 거리 개념은 다르기 때문이다. 따라서 타 영역의 상황도와 사이버 심볼을 연계하여 표현하는 방안이 필요하다.

(5) 사이버 심볼의 성능을 어떻게 평가하고 갱신할 것인가?

사이버 심볼은 작전 참여자들간의 합의된 약속이라 할 수 있다. 현실적으로 모든 구성원이 합의한 형태의 심볼을 정의하는 것은 불가능하다. 또한, 사이버작전 수행간 새로운 형태의 객체가 필요할 수도 있다. 따라서 많은 관계자의 의견을 수렴하여 필요한 사이버 심볼을 우선 정의하고 이를 지속해서 평가, 갱신, 추가하는 절차가 필요하다. 하지만 너무 잦은 심볼의 변경은 오히려 상호운용성을 저해할 수 있다는 것을 고려해야 한다.

Ⅲ. 사이버심볼 연구동향 분석

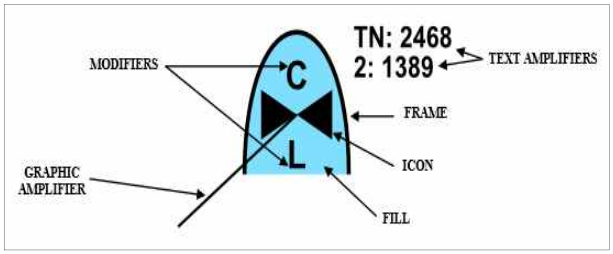

그림 1. 아이콘 기반 심볼의 구성요소[12]
Fig. 1. Icon based symbol components[12]

본 장에서는 미래 사이버작전 환경을 고려한 사이버작전 상황도의 발전 방향을 제시하기 위해 사이버 심볼에 대한 연구내용을 살펴보고 장·단점을 분석한다.

3-1 MIL-STD-2525D

MIL-STD-2525D는 미군의 군사심볼 표준으로 2014년 6월에 공개되었으며 사이버공간을 포함한 11개 분야(우주, 공중, 지상, 수상, 수중, 사이버공간, 전술수단, 안정화 작전 및 민간 지원, 신호정보, 기상, 해양 등)에 대한 심볼을 정의하고 있다[2], [12]. MIL-STD-2525D에서의 심볼 구성요소와 사이버 심볼에 대해 살펴본다.

1) 심볼 구성요소

MIL-STD-2525D에서 정의한 심볼은 아이콘 기반의 기호로 프레임(frame), 아이콘(icon), 수정자(modifier), 확장자(amplifier), 채움(fill) 등으로 구성된다. 그림 1은 아이콘 기반의 부호를 구성하는 요소들의 예를 나타낸다.

프레임은 심볼의 외형을 나타내며 가상의 팔각형(octagon)이 프레임 안에 존재한다고 가정하는데 실제 팔각형은 가시적으로 표현되지 않는다. 팔각형은 가로 또는 세로로 구분된 3개의 섹터로 구성된다. 아이콘은 3개의 섹터 중 가운데 섹터에 위치하는데 부대, 장비, 시설, 활동 또는 작전 등을 표현하는 함축적 그림 모양 또는 영숫자(alphanumeric)로 표현된다. 아이콘은 가상의 팔각형에서 가운데 섹터에 일반적으로 위치하지만, 예외적으로 가운데 섹터를 초과하거나 팔각형의 외곽선을 초과하여 표현되기도 한다.

수정자는 아이콘과 연계된 부가적인 정보를 나타내는데 메인섹터를 제외한 나머지 섹터에 표현된다. 확장자는 심볼에 대한 기타 다양한 부가적인 정보를 나타하며 프레임의 외곽 주변에 위치한다. 채움은 프레임의 내부영역의 색상으로 아군, 적군, 중립, 미식별 등의 피아관계(identity)를 나타낸다.

2) 사이버 심볼

MIL-STD-2525D에는 사이버 심볼들도 포함하고 있다. 사이버 심볼은 기타 심볼과는 달리 수정자를 제외한 아이콘, 프레임, 확장자, 채움 등으로 구성된다. 프레임, 확장자, 채움은 기타 심볼과 동일하게 사용된다. 한편, 사이버 심볼의 아이콘은 모두 영문자 약어이다. 예를 들어, 웹서버, 라우터의 아이콘은 각각 WSR, RTR이다.

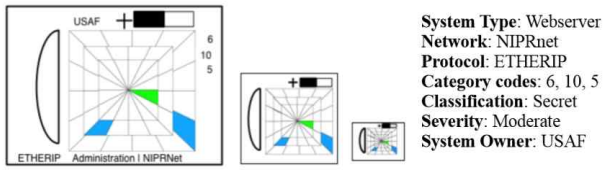

그림 2. 사이버 사고 유형 표현의 예[7]
Fig. 2. Example of cyber accident types[7]

수정자가 별도로 정의되어 있지 않고 아이콘이 영문자 약어이기 때문에 심볼을 통해 충분한 정보를 표현하는 데 한계가 있으며 직관적으로 심볼의 의미를 이해하기 어렵다. 그뿐만 아니라 다양한 사이버 상황을 표현하기에는 심볼의 수가 절대적으로 부족하다. MIL-STD-2525D는 최초로 군사용 사이버 심볼을 정의했다는 의의가 있지만 심볼의 완성도가 높지 않아 사이버작전 상황도에 활용하기에는 부족한 수준이며 추가적인 연구가 필요하다.

3-2 JCD(Joint Cert Database) Storybook 심볼

JCD Storybook 심볼은 정보체계에 대한 상태를 나타내기 위해 고안된 표현법으로 2005년에 소개되었다. 그림 2에서 보는 바와 같이 MIL-STD-2525D에서 정의한 심볼과 유사하게 중심 도형 주변에 시스템 유형, 네트워크, 프로토콜, 기밀 여부, 피해의 심각성, 체계의 소유 조직 등의 부가정보를 표현한다. 그리고 그림 3과 같이 사이버 사고의 유형을 나타내는 숫자코드를 색상과 시계방향의 위치를 이용하여 표현한다. 이러한 표현법의 목적은 JCD 데이터 필드의 방대한 정보를 함축적으로 표현하는 것이다. 도형 내에서의 색상과 위치를 통해 사이버 상황을 유형화한 코드정보를 쉽게 인식할 수 있다. 또한, 도형의 크기가 축소되어 도형 주변의 문자와 숫자가 명확하게 표현되지 않더라도 색상과 위치 정보를 통해 모호한 숫자를 쉽게 유추할 수 있다. 하지만 숫자와 맵핑되는 의미를 암기해야 하는 단점이 있다.

사이버 공격을 이해하고 분류하기 위한 사이버 공격 분류 체계들이 있다. 하지만 사이버 공격은 단일 목적, 단일 수단으로 이루어지지 않고 다수의 목적을 위해 다양한 수단이 동시 다발적으로 사용될 수 있다. 따라서 사이버 공격이 어떻게 수행되었는지를 간단한 심볼을 이용하여 표현하는 것은 쉽지 않다. 그런데 JCD Storybook 심볼은 무엇이 발생했는가에 대한 정보 뿐 아니라 어떻게 발생했는지에 대한 정보도 기본도형(primitive)의 조합을 통해 표현이 가능하다.

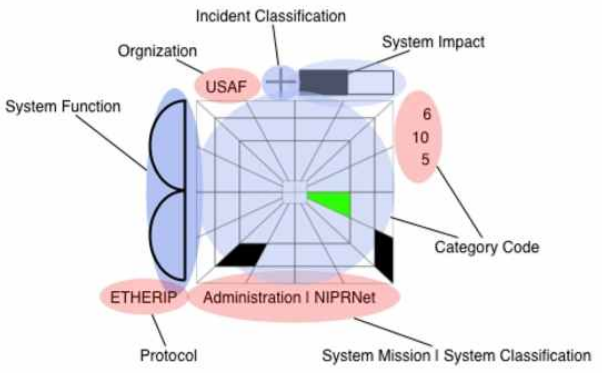

그림 3. JCD 심볼의 구성[7]
Fig. 3. Configuration of JCD symbol[7]

JCD Storybook 심볼은 구조가 간단하고 논리적이며, 기본도형의 조합을 통해 사이버 상황을 효과적으로 표현할 수 있다. 하지만 제시된 심볼들은 MIL-STD-2525와 호환되지 않아 심볼을 익히는데 많은 시간이 소요되는 단점이 있다. 특히 물리 작전에서 사용되는 심볼에 익숙한 전투원이 새로운 유형의 심볼을 추가적으로 익히는 것은 비효율적이다.

3-3 Erick과 Charles의 심볼

Erick과 Charles는 사이버작전의 특성을 고려하여 사이버 공간과 작전 상황을 표현하기 위한 그래픽 요소들을 제안하였다. 저자들은 사이버 요소들을 물리적 작전의 개념과 연계시켰다. 예를 들어, 방화벽, 스캔, 허니팟, 네트워크 등을 각각 물리 작전에서의 장애물, 정찰, 매복지점, 책임지역(Area of Responsibility) 등으로 재해석했다[6],[14],[15].

저자들은 사이버 공간(또는 지형)을 사이버 장비들로 구성된 경계선으로 구분되는 개별 네트워크들로 표현하였다. 실제 네트워크에 포함되는 많은 장비들을 심볼로 표현하지 않고, 사이버작전의 계획, 사이버 상황의 이해와 공유에 필요한 최소한의 장비들만을 포함한다.

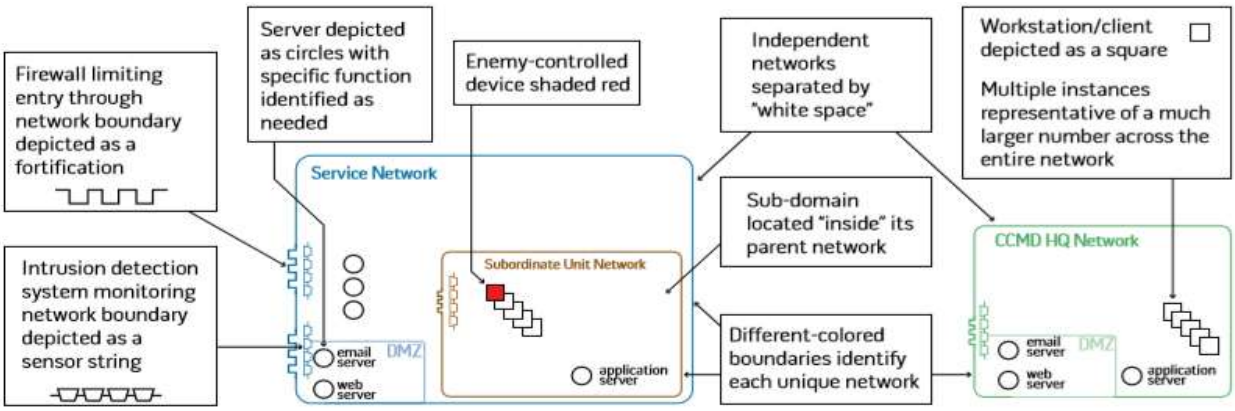

그림 4. Erick과 Charles의 심볼을 이용한 사이버 상황의 표현 예[14]
Fig. 4. Example of cyber situation using symbols of Erick and Charles[14]

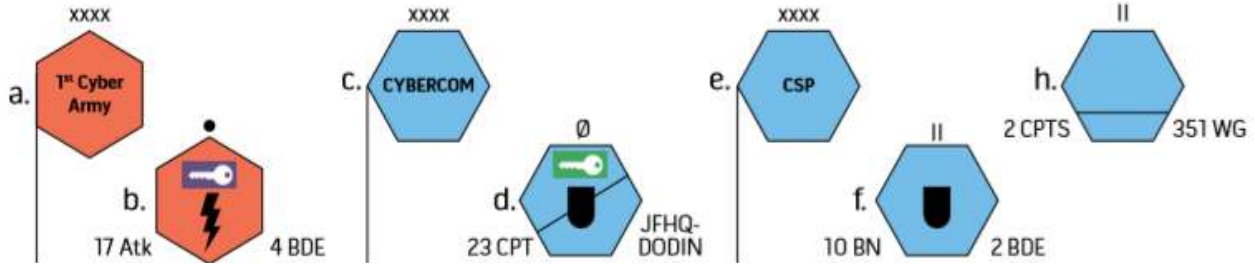

그림 5. Erick과 Charles의 심볼을 이용한 사이버 부대 표현의 예[6]
Fig. 5. Example of cyber units using symbols of Erick and Charles[6]

또한 각 네트워크의 명확한 식별을 위해 네트워크마다 별도의 색상을 사용하고, 네트워크 식별을 위한 부가적인 정보를 제공하기 위해 문자를 사용할 수 있다. 한편, 사이버 공간에서 사이버 장비들의 물리적 거리는 중요하지 않다고 판단한다. 사이버 공간에서의 거리 개념은 데이터를 전송하는데 필요한 홉(hop)으로 측정되어야 한다고 주장한다. 그리고 사이버 공간의 특성을 고려했을 때 사이버 장비들 사이의 거리, 상대적인 위치, 독립 네트워크 등은 중요하지 않지만, 계층적 형태로 포함관계에 있는 네트워크의 관계는 중요하다고 판단한다. 서버와 단말은 각각 사각형과 원으로 표현하고 방화벽과 침입탐지장비는 물리작전에서 사용되는 장애물과 센서 배열 심볼을 차용한다. 그림 4는 사이버 상황을 표현한 예를 나타낸다. 한편 물리작전에서는 존재하지 않는 페르소나 계층의 요소들을 사용자 수준, 체계 수준, 도메인 수준의 접근권한을 색상으로 구분하여 접근권한의 중요도를 신속하게 파악할 수 있게 하였고, 적에게 통제권이 탈취된 사이버 요소들은 붉은색으로 표현한다.

한편, MIL-STD-2525D 표준에는 아이콘 기반으로 부대를 나타내기 위한 프레임을 정의하고 있다. 하지만 사이버작전 전담부대를 표현하는 프레임은 표현되지 않는다. 이에 저자들은 팔각형 도형을 사용하며 사이버 부대를 표현한다. 그림 5는 사이버 부대를 표현하는 예를 나타낸다. 사이버 임무는 JP-3-12에서 분류한 것과 같이 공세적 사이버작전, 방어적 사이버작전, 네트워크 작전으로 구분한다. 공세적 사이버작전(OCO: Offensive Cyberspace Operation)을 수행하는 부대는 심볼에 번개 모양의 아이콘으로 표현하고, 방어적 사이버작전(Defensive Cyberspace Operation)을 수행하는 부대는 방패 모양의 아이콘으로 표현한다. 한편 미 합참에서 분류한 사이버작전 중 네트워크 작전을 수행하는 부대는 MIL-STD-2525D에 정의되어 있는 것과 같이 지원 부대를 나타내는 프레임 내의 가로 직선으로 표현한다.

Ⅳ. 발전방안 및 시사점

앞서 사이버작전 상황도 구현에 필요한 다양한 사이버 심볼 연구결과들을 살펴보았다. 사이버작전이 하나의 독립된 작전영역으로 정착됨에 따라 사이버 상황을 가시적으로 표현하기 위한 연구가 활발히 이루어지고 있다. 사이버 상황을 도시하는 방법은 크게 2가지 부류로 구분할 수 있다.

첫 번째 부류는 물리작전에서 사용하는 방법론을 사이버작전에 접목하는 것이다. 물리작전을 도식화하는 방법은 실제 작전활동을 수행하며 많은 사람들에 의해서 오랜 시간 발전되어 왔으며 NATO, 미군을 중심으로 높은 수준의 표준화가 완료되었다. 또한, 전투원들은 물리작전을 도식화하는 방법에 이미 익숙하므로 사이버작전을 유사한 방법으로 도식화하는 것이 별도의 학습과정을 최소화하는 좋은 방안이 될 수 있다. 하지만 사이버작전 고유의 특성을 반영한 도식 방법은 아니므로 사이버 상황을 표현하는데 비효율적인 측면이 있다.

두 번째 부류는 사이버작전 고유의 특징을 고려하여 새로운 도식 방법을 설계하는 것이다. 설계 단계에서부터 사이버작전을 고려하기 때문에 물리작전을 도식하는 방법으로 표현하기 모호한 부분도 효과적으로 표현할 수 있다는 장점이 있다. 하지만 아직까지 권위 있게 표준화된 방법론은 없는 상태이며 전투원들이 사이버작전을 표현하기 위한 새로운 방법론에 숙달되어야 하고 이 과정에서 적지 않은 저항이 있을 수 있다는 단점이 있다. 특히 작전에 참여하는 모든 인원이 새로운 방법론을 익혀야 신속한 상황공유라는 목적을 달성할 수 있다는 것을 고려했을 때 새로운 방법론이 실질적인 효과를 발휘하기까지는 많은 시간이 소요될 수밖에 없다.

기존 연구결과를 토대로 사이버작전 상황을 효과적으로 표현하기 위한 사이버 심볼 및 사이버작전 상황도의 발전 방향으로 다음과 같이 5가지를 제시한다.

첫째, 다영역 작전을 고려한 사이버작전 상황 표현 연구의 필요성이다. 기존 연구의 두 가지 유형 모두 크게 간과하고 있는 부분은 미래 작전환경이 다영역 작전의 형태로 진화하고 있기 때문에 사이버 상황만을 도시하는 것이 아니라 사이버 상황이 타영역의 작전에 어떠한 영향을 서로 주고받는지를 표현할 수 있어야 한다는 것이다. 다시 말해, 지휘관은 특정영역에서 수행되는 작전만을 지휘하는 것이 아니라 여러 영역에 걸쳐서 발생되는 작전상황을 관리해야 한다. 또한 특정 영역의 작전 활동만을 지휘하는 지휘관이라 하더라도 나의 작전이 타영역에 미치는 영향과 타영역의 상황이 나의 작전에 미칠 수 있는 영향을 종합적으로 고려해야 한다. 따라서 특정 영역의 상황이 아닌 각 작전영역에서의 상황이 통합, 융합된 형태로 제공되어야 한다. 이를 위해서는 물리작전, 사이

버작전에서의 심볼에 대한 도식 방법이 통일될 필요가 있다. 사이버작전의 특성상 하나의 상황도에 물리작전과 사이버작전을 함께 도시할 수 없다면 다수의 상황도를 운용하되 각 상황도 간의 관계성을 가시적으로 표현하여 전투원들이 직관적으로 종합적인 상황을 이해할 수 있도록 해야 한다.

둘째, 상황도를 인지하는 수단의 확대가 필요하다. 현재 연구되고 있는 방안 대부분은 작전상황에 대한 정보를 정지 이미지 형태로 변환하고, 전투원은 시각 기능을 이용해 해당 이미지를 해석함으로써 작전상황을 이해하는 것이다. 물론 인간은 시각 정보를 통해 순간적으로 많은 정보를 습득할 수 있다. 하지만 전장 영역이 점차 확대되고 각 영역간의 관계가 복잡해지고 있어서 작전상황을 그래픽적인 요소들로만 추상화하는 것은 한계가 있다. 따라서 작전상황을 보다 명확하게 표현하기 위해 표준화된 서식, 음향, 애니메이션, 3D 이미지 등의 활용을 고려할 필요가 있다.

셋째, 시간 흐름별 상황변화를 표현하는 방안이 필요하다. 사이버작전은 절차적으로 시행되는 경향이 있다. 예를 들어, 사이버킬체인 모델에 의하면 사이버 공격이 공격대상체계에서 최종적으로 실현되기 위해서는 정찰, 무기화, 유포, 악용, 설치, 명령 및 제어 등이 순차적으로 선행되어야 한다[16]. 사이버 방어 관점에서도 사이버 공격의 단계에 따라 대응 수단과 방법이 달라진다. 따라서 사이버작전 상황의 시간적 흐름 또는 단계를 표현할 수 있어야 한다.

넷째, 다양한 전시체계를 고려한 상황 도시 방안이 필요하다. 개인 전투원은 휴대폰 형태의 전시기를 통해 상황을 공유하지만, 상위 제대로 갈수록 대형 전시체계의 활용이 가능하다. 일반적으로 사이버작전을 통합적으로 지휘하는 제대는 비디오월 형태의 전시기를 사용할 것이다. 즉, 하나의 단일 화면에 전장 상황을 표현할 필요가 없다. 분할된 다수의 화면을 이용하여 상황을 표현하는 방안도 강구해야 한다. 예를 들어, 물리작전은 지형 지도 위에 심볼을 표현하는 것이 효과적인 지만 논리 계층의 사이버작전 상황은 지형 지도 보다는 네트워크 구성도에 표현하는 것이 효과적이다. 하나의 화면에 성격이 다른 두 개 이상의 표현방법을 사용하기보다는 각각의 상황 표현을 별도의 화면에 구성하고 이들의 연관관계를 보조자료 형태로 표현하는 방안도 가능하다. 다시 말해, 활용 가능한 전시체계를 고려한 통합 작전상황 표현이 필요하다.

다섯째, 다양한 인원이 자유롭게 참여할 수 있는 표준화 절차가 제도화되어야 한다. 사이버 심볼을 정의하는 것은 최적의 정답을 찾는 것이 아니라 다수의 합의를 이끌어내는 과정이라고 할 수 있다. 따라서 사용자 의견이 무엇보다 중요하며 사용자 의견이 심볼의 표준화 또는 최신화 과정에서 누락되지 않도록 제도화된 장치 마련이 필요하다.

Ⅴ. 결론 및 향후연구

제5의 전장영역으로 정의되는 사이버 공간에서의 작전활동은 단순히 가상의 공간에서 벌어지는 사이버 전사들만의 전유물이 아니다. 사이버 공간과 지상, 공중, 해상, 우주 등의 물리적 공간은 상호 독립적인 영역이 아닌 상호 의존적인 관계이다. 따라서 작전활동에 참여하는 모든 전투원은 사이버 공간에서의 상황을 공유하고 이해할 필요가 있다. 이러한 필요성을 충족시켜줄 방법이 사이버작전 상황도를 이용하는 것이다. 사이버 상황을 표현하기 위한 기본 요소인 사이버 심볼의 정의와 이들을 활용한 사이버작전 상황도 구성에 대한 연구결과들을 살펴보고, 이를 토대로 향후 사이버작전 가시화를 위한 발전 방향을 개념적으로 다음과 같이 제시하였다.

첫째, 다영역 작전을 고려한 사이버작전 표현 연구가 필요하다. 둘째, 정적인 이미지뿐 아니라 음향, 애니메이션, 3D 이미지 등의 활용방안을 마련해야 한다. 셋째, 현재의 사이버 상황 뿐 아니라 시간 흐름에 따른 단계적 사이버 상황을 표현할 수 있어야 한다. 넷째, 다양한 전시체계를 고려한 상황도 구성 방안을 마련해야 한다. 다섯째, 다수의 인원이 자유롭게 참여할 수 있는 사이버 심볼 표준화 절차를 정립하고 변경 또는 최신화된 심볼들에 대한 내용이 쉽고 빠르게 전달될 수 있는 시스템을 구축하여야 한다.

사이버작전 상황도 구현과 관련된 연구는 높은 필요성에 비해 상대적으로 초기 단계라 할 수 있다. 향후 본 논문에서 분석한 연구동향과 제시된 발전방안을 기초로 한국군 사이버작전환경에 부합하는 사이버 심볼 표준화 및 사이버작전 상황도를 구현할 예정이다.

감사의 글

본 연구는 국방과학연구소의 ‘멀티레이터드 사이버작전 상황도 구축 기술’ 과제의 일환으로 수행되었음.

참고문헌

[1] Jongjin Kang et al., "Display Performance Enhancement for Common Operational Picture", in *Proceedings of Annual Conference on the Korea Institute of Military Science and Technology*, pp. 1073-1074, 2020.

[2] Sungho Kong, "A Study on the connection between warfighting symbology of combat system and tactical data link", in *Proceeding of Fall Conference on KIMST*, pp. 616-617, 2019.

[3] Koohyung Kwon et al., "A Study of Cyber Operation COP based on Multi-layered Visualization", *The Journal of Korea Convergence Security Association*, Vol. 20, No. 4, pp. 616-61, 2020. https://doi.org/10.7741/rjcc.2012.20.4.616

[4] Koo-Hyung Kwon, Jang-Hyuk Kauh and Haengrok Oh, "A Study on the Cyber Common Operational Picture", in *Proceedings of Annual Conference on the Korea Institute of Military Science and Technology*, pp. 1412-1413, 2020.

[5] Jonghwa Kim, Sonyong Kim, Jaeyeon Lee and Haengrok Oh, "A Study of Development for Cyber COP based on HTML5", in *Proceedings of Annual Conference on the Korea Institute of Military Science and Technology*, pp. 1127-1128, 2020

[6] M. Varga, C. Winkelholz and S. Träber-Burdin, "An Exploration of Cyber Symbology", *2019 IEEE Symposium on Visualization for Cyber Security (VizSec)*, Vancouver, BC, Canada, pp. 1-5, 2019. https://doi.org/10.1109/vizsec48167.2019.9161577

[7] S. F. Fugate and R. S. Gutzwiller, "Rethinking cyberspace symbology", *NATO IST-HFM-154, Cyber Symbology Specialists' Meeting*, USA, 2016.

[8] Jongkwan Lee et al. "Study on Military Symbology for Cyber Common Operational Picture", in *Proceedings of Annual Conference on the Korea Institute of Military Science and Technology*, pp. 1113-1114, 2020.

[9] Jaeyeon Lee, Sukdea Yu, Koohyung Kwon and Haengrok Oh, "A Study of Military Symbology for Cyberwarfare Situational Awareness", in *Proceedings of Annual Conference on the Korea Institute of Military Science and Technology*, pp. 1216-1217, 2020.

[10] S. Noel, et. al., "Big-Data Graph Knowledge Bases for Cyber Resilience", *NATO IST-153 Workshop on Cyber Resilience*, 2017.

[11] APP-6(D), "Joint Military Symbology", NATO, 2017.

[12] MIL-STD-2525D, "Joint Military Symbology", *U.S. Department of Defense*, 2014.

[13] Joint Publication 3-12, "Cyber Operations", *U.S. Joint Chiefs of Staff*, 2018.

[14] Gregory Conti and David Raymond, "On Cyber: Towards an Operational Art for Cyber Conflict", Kopidion Press, 2017.

[15] Erick D. McCroskey and Charles A. Mock, "Operational Graphics for Cyberspace", *Joint Force Quarterly(JFQ)*, Issue 85, 2nd Quarter, pp.42-49, 2017.

[16] Jae-won Yoo and Dea-woo Park, "Cyber kill chain strategy for hitting attacker origin", *The Journal of the Korea Institute of Information and Communication Engineering*, Vol. 21, No. 11, pp. 2199-2205, 2017. https://doi.org/10.6109/jkiice.2017.21.11.2199

이종관(Jongkwan Lee)

2000년 : 육군사관학교 전자공학과 (공학사)
2004년 : 한국과학기술원 전자공학과 (공학석사)
2014년 : 아주대학교 NCW공학과 (공학박사)
2021년～현 재: 육군사관학교 컴퓨터과학과 부교수
※관심분야 : 사이버전, 네트워크중심전

이민우(Minwoo Lee)

1998년 : 한국항공대학교 항공통신정보공학과 (공학사)
2013년 : 아주대학교 NCW공학과 (공학박사)
2019년～현 재: 아주대학교 국방디지털융합학과 대우부교수
※관심분야 : 위성통신, 네트워크 보안, 사이버전자전

권구형(Koohyung Kwon)

2001년 : 고려대학교 전기전자전파공학 (공학사)
2003년 : 고려대학교 전파공학과 (공학석사)
2006년～현 재: 국방과학연구소

고장혁(Janghyuk Kauh)

1996년 : 광운대학교 컴퓨터과학과 (공학사)
1998년 : 광운대학교 컴퓨터과학과 (공학석사)
2018년 : 광운대학교 컴퓨터과학과 (공학박사)
1998년～현 재: 국방과학연구소

오행록(Haengrok Oh)

1987년 : 인하대학교 전산학과 (공학사)
1989년 : 인하대학교 전산학과 (공학석사)
2004년 : 고려대학교 컴퓨터학과 (공학박사 수료)
1998년～현 재: 국방과학연구소

김선영(Sonyong Kim)

2019년 : 고려대학교 전기전자전파공학 (공학사)
2019년～현 재: 한화시스템