https://doi.org/10.33778/kcsa.2021.21.1.149

사이버 작전 군대부호 표준화에 관한 연구★

이 종 관*, 이 민 우**, 김 종 화***, 김 종 화****, 이 재 연****, 오 행 록*****

요 약

본 논문은 사이버 작전 상황을 직관적으로 이해하기 위한 사이버 군대부호를 제안한다. 현재 사용하고 있는 군대부호들은 사이버 작전을 고려하지 않고 물리적 작전만을 고려하여 표준화되었다. 미군의 합동군대부호 표준인 MIL-STD-2525D에서는 일부 사이버 작전을 위한 부호들이 포함되어 있으나 영문자 3자로 구성된 아이콘만이 표준화되어 있다. 따라서 사이버 작전을 효과적으로 표현하는데 한계가 있다. 이러한 이유로 본 논문은 현존하는 군대부호 생성 규칙에 부합하는 사이버 작전을 위한 군대 부호를 제안한다. 단지 군대부호만을 제시하는 것에 그치지 않고 제안하는 부호의 효용성을 증명하기 위해 제안하는 부호를 사용하여 다양한 사이버 상황을 표현한 예제도 함께 제시한다. 본 논문에서 제안한 부호들이 모든 사이버 상황을 표현할 수는 없으나, 제안한 부호들을 기반으로 더 많은 부호들이 향후 표준화될 수 있을 것으로 기대한다.

A Study on Military Symbology Standardization for Cyber Operations

Jongkwan Lee*, Minwoo Lee**, Jonghwa Kim***,

Jongkwa Kim****, Jaeyeon Lee****, Haengrok Oh*****

ABSTRACT

In this paper, we propose military symbols for cyber operations to understand the situation in cyberspace intuitively. Currently, standardized military symbols are mainly for kinetic operations, and they do not consider cyber operations. Although, MIL-STD-2525D includes some symbols for cyber operations, only icons that are composed of three letters are standardized. So there is a limit to effectively expressing cyber operations. That is why we propose military symbols for cyber operations compatible with existing military symbol building rules. In addition to merely presenting the symbols, we present examples of expressing various cyber situations using the proposed symbols. It proves the usefulness of the proposed symbol. The small number of symbols proposed in this paper will not be able to represent all cyber situations. However, based on the proposed symbols, it is expected that more symbols will be standardized in the future to more clearly express the cyber situation.

Key words : Military Symbol, Cyberspace, Cyber Operations, Common Operational Picture

접수일(2021년 02월 24일), 게재확정일(2021년 03월 26일)

★ 본 논문은 국방과학연구소의 '멀티레이어드 사이버작전 상황도 구축 기술' 과제의 일환으로 수행되었음.

* 육군사관학교 컴퓨터과학과 (주저자, 교신저자)
** 아주대학교 국방디지털융합학화 (공동저자)
*** 육군사관학교 사이버전연구센터 (공동저자)
**** 한화시스템(주) (공동저자)
***** 국방과학연구소 (공동저자)

1. 서 론

일반적으로 군사작전이 수행되는 경우 지휘관, 참모 등의 전투원들은 충분한 수면을 취하지 못한다. 작전이 장기화되면 극심한 스트레스와 수면부족으로 올바른 상황판단과 의사결정이 점점 어려워질 수밖에 없다. 수면부족은 인지력, 상황판단력에 지대한 영향을 미치는 것으로 알려져 있다[1-2]. 또한 군사작전 목표를 효과적으로 달성하기 위해서는 하위 제대의 전투원에서부터 상위 제대의 지휘관까지 상황에 대한 인식이 일치해야 한다. 극한의 전장 상황에서 효과적으로 작전을 수행하기 위해 각 군별 또는 전장기능별로 C4I체계를 구축하고 상황도 구성을 위해 군대부호를 정의하여 사용하고 있다[3-4].

군대부호는 부대, 장비, 시설, 작전활동 등을 표현하기 위한 표준화된 기호들의 집합으로 군사작전의 상황을 가시화하고 이를 신속하게 공유하기 위한 대표적인 의사소통 수단이다. 대표적인 군대부호로 NATO 표준인 APP-6[5]와 미군 표준인 MIL-STD-2525[6]가 있다. 위 표준들은 합동작전 및 연합작전시 상호운용성을 증진시키는데 큰 역할을 한다. 두 표준은 서로를 참조하며 발전하는 경향이 있으며 생성규칙 및 부호의 모양과 의미들이 서로 유사하다. 한국군은 미군의 표준을 기반으로 자체 군대부호 표준을 정의하고 있으며 많은 부분에서 미군의 표준과 동일하다[3].

한편, 미국은 사이버공간을 육, 해, 공, 우주에 이은 제5의 전장으로 규정하고, 사이버전도 기존의 지상, 해양, 공중, 우주에서와 같은 군사작전으로 대응할 것을 선언하였다. 사이버공간은 인간과 기계간의 정보의 흐름을 나타낸다. 사이버 공간에서의 정보흐름은 다른 전장 공간에서 물리적인 영향력으로 발현된다. 즉, 사이버 공간에서의 활동이 타전장과 무관하지 않으며, 군사작전은 물리적 공간과 사이버 공간을 넘나들며 수행된다. 따라서 전투원은 사이버 공간에서 일어나고 있는 작전상황을 이해해야만 한다. 그런데 사이버 작전을 표현하기 위한 군대부호 표준이 미흡하다. 미군은 MIL-STD-2525D에서 사이버공간에 대한 표준 군대부호를 일부 정의하고 있지만 내용이 구체적이지 않아 활용성이 크게 떨어진다. 따라서 사이버 군대부호를 정의하기 위한 연구가 미국을 중심으로 진행되고 있으며, 한국군도 사이버작전 상황도의 개발을 추진하고 있다[7-10].

본 논문에서 한국군 환경에 부합하는 사이버 작전 상황도 운용을 위해 필요한 사이버 군대부호 중 전술기호의 표현방법을 제안한다. 본 연구결과는 인터넷에 공개되어 있는 미군의 군대부호 표준인 MIL-STD-2525D 기반으로 수행되었으며 한국군의 표준은 미군의 표준을 따르고 있기 때문에 본 연구결과가 한국군의 표준에도 적용될 수 있다.

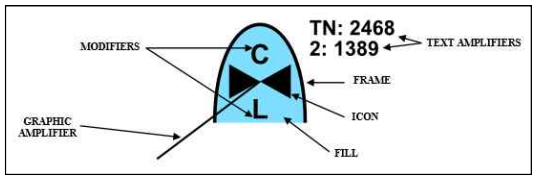
본 논문은 다음과 같이 구성되어 있다. 2장에서는 MIL-STD-2525D에 대해 살펴본다. 3장에서는 이를 바탕으로 사이버 전술기호의 표현 방법을 제안하며 4장에서는 제안한 방법을 활용한 사이버 전술기호의 활용 예를 시나리오 기반으로 살펴본다. 마지막으로 5장에서 결론과 향후 연구에 대해서 논한다.

2. MIL-STD-2525D

본 절에서는 미군의 군대부호 표준 중 가장 최근에 발표된 MIL-STD-2525D에서 제시된 전술기호의 구성 요소와 표현 방법을 살펴본다.

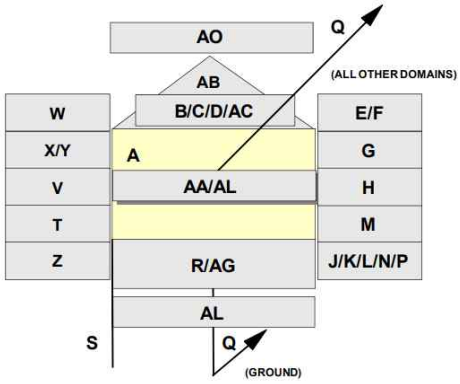
MIL-STD-2525D는 사이버공간을 포함한 11개 분야[1]에 대한 군대부호를 정의하고 있다[4]. 아이콘 기반의 기호로 프레임(frame), 채움(fill), 아이콘(icon), 수정자(modifier), 확장자(amplifier) 등의 요소들로 구성된다. (그림 1)은 아이콘 기반의 부호를 구성하는 요소들의 예를 나타낸다.

1) 우주, 공중, 지상, 수상, 수중, 사이버공간, 전술수단, 안정화 작전 및 민간 지원, 신호정보, 기상, 해양 등



(그림 1) 아이콘 기반 전술기호의 구성요소

프레임은 부호의 외형으로 가상의 팔각형(octagon)이 프레임 안에 존재한다고 가정한다. 팔각형은 가로 또는 세로로 3개의 섹터로 구분된다. 아이콘은 부호의 가장 가운데에 위치하며 부대, 장비, 시설, 활동 또는 작전 등을 표현하는 함축적 그림모양 또는 영숫자(alphanumeric)이다. 아이콘은 가상의 팔각형에서 가운데 섹터에 위치하거나(main icon), 팔각형의 가운데 섹터를 초과하지만 팔각형의 외곽선을 초과하지 않는 범위 내에 위치하거나(full octagon icon), 팔각형의 외곽선을 초과한다(full frame icon).



(그림 2) 확장자의 필드 위치

수정자는 아이콘과 연계되어 표현되는 그림모양 또는 영숫자로 부가적인 정보를 제공하며 메인 섹터를 제외한 섹터에 위치한다. 확장자는 부호에 대한 다양한 부가적인 정보를 제공하며 프레임 바깥에 위치한다. 확장자를 표기하기 위한 필드는 총 41개가 정의되어 있다. (그림 2)는 확장자가 표기되는 필드의 위치를 나타낸다. 각 필드에 포함되는 확장자의 의미는 표준서[6]를 참고한다. 모든 확장자가 모든 부호에 적용되는 것은 아니다. 그리고 상황도에 도시되는 부호의 가독성을 위해 필수적인 일부 확장자만 사용되며, 하나의 필드에 다수 확장자가 표시될 수 있는 경우에는 가장 중요한 확장자만 표기한다. 채움은 프레임의 내부영역을 의미하며 색상으로 피아관계(identity)[2]를 나타낸다.

MIL-STD-2525D은 사이버 부호에 대해 부록 L에서 다루고 있다. 사이버 부호 생성절차와 아이콘들이 일부 정의되어 있다. 하지만 사이버 부호에 대한 수정자가 정의되어 있지 않다. 또한 아이콘을 이용하여 봇넷 구성요소, 네트워크 장비, 피해현황, 객체의 상태 등의 표현이 가능하나 모든 아이콘이 영문자 3개의 약어 형태로 표현되어 있어 직관적인 이해가 어렵고 활용도가 떨어진다.

3. 제안하는 사이버 전술기호

본 장에서는 사이버 전술기호의 구체적인 표현 방법을 제안한다. 이를 위해 사이버 전술기호를 정의할 때 고려해야할 사항들을 우선 살펴보고, 사이버 전술기호로 표현해야하는 대상을 선정한다. 그리고 선정된 대상별로 사이버 전술기호로 표현하는 방법을 구체적으로 설명한다.

3.1 사이버 전술기호 정의시 고려사항

사이버 전술기호 정의시 다음과 같은 사항들이 고려되어야 한다.

첫째, 사이버 공간은 물리적 공간과 달리 물리계층, 논리 계층, 소셜 계층 등 3개의 계층으로 구성된다. 물리계층은 사이버 공간을 형성하기 위해 사용되는 물리적 객체들을 표현하는 계층이다. 물리계층에서는 각 객체가 배치된 위치 정보가 중요하다. 적의 사정거리 또는 감시거리 이내에 위치했는지 여부에 따라 위협의 정도가 달라지기 때문이다.

논리계층은 네트워크 노드들 사이에 존재하는 논리적 연결들을 나타낸다. 노드들은 네트워크에

2) 아군, 적군, 중립, 미식별 등

연결된 모든 장치들을 의미한다. 따라서 노드들은 컴퓨터, 핸드폰 등 네트워크 통신 기능이 있는 모든 디지털 장치를 포함한다.

소셜 계층은 인간 및 인지(cognitive) 측면으로 구성되며 페르소나와 사이버 페르소나를 포함한다. 페르소나는 네트워크에 존재하는 사람들을 의미한다. 즉, 네트워크에 접속하여 사이버 공간에서 활동하는 사람들이다. 사이버 페르소나는 사이버 공간에서의 개인 ID, 이메일 주소, IP 주소, 휴대전화 번호 등을 의미한다. 한 개인은 여러 개의 사이버 페르소나를 가질 수 있으며 하나의 사이버 페르소나를 여러 사용자가 공유할 수도 있다.

물리적 공간에는 중요하게 고려되지 않는 논리 계층과 소셜 계층의 구성요소들을 표현하기 위한 객체들을 선정해야 한다. 물리적 작전에서는 중요한 정보가 아닌 객체가 사이버 작전에서는 중요한 요소일 수 있기 때문이다. 사이버 전술기호의 세부적인 대상에 대한 논의는 다음 장에서 다룬다.

둘째, 사이버 공간에서는 적과의 상대적 거리 또는 위치정보는 큰 의미가 없을 수 있다. 사이버 공간에서는 물리적 공간에서와 같은 거리 개념이 존재하지 않는다. 물리적으로 아무리 멀리 이격되어 있는 적이라도 사이버 공간에서는 근거리에 있는 적과 동일한 위협이 될 수 있다. 한편, 적의 시스템으로 부터 아군의 시스템에 도달하기 까지 거쳐야 하는 라우터 개수 또는 정보보호체계의 개수가 거리 개념으로 생각될 수 있다.

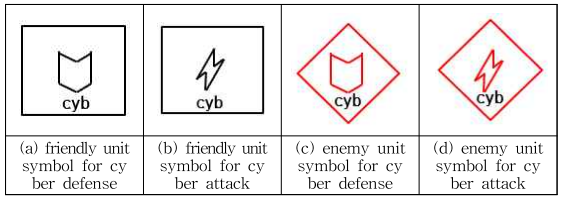
셋째, 사이버 전술기호의 생성 절차 및 표현 방법이 물리적 작전에서의 전술기호와 유사해야 한다. 물리적 작전에서의 전술기호는 오랜 시간동안 발전해왔고 전투원들은 이미 해당 전술기호들에 익숙해져 있다. 또한 물리적 작전과 사이버 작전이 통합되어 수행되는 경우 사이버 전술기호와 물리적 작전의 전술기호들이 하나의 상황도에 함께 도시될 것이다. 만약 사이버 전술기호의 생성절차와 표현방법이 물리적 작전의 전술기호와 다르다면 이를 다시 익히기 위한 불필요한 노력이 소요되고 많은 혼란과 불편을 초래할 것이다. 따라서 사이버 전술기호의 표현방법은 기존 표준에서 정의된 방법과 유사해야 한다.

3.2 사이버 전술기호의 대상

사이버 전술기호로 표현해야 하는 대상은 사이버 부대, 장비(네트워크 장비, 서버, 정보보호체계 등), 시설 뿐 아니라 사이버 공간, 특정 인원(아군, 적군, 용역업체 민간인), 사이버 페르소나 등을 포함해야 한다. 사이버 공간, 사이버 활동, 임무, 책임 등은 전술도식으로 표현하며 본 연구에서는 사이버 전술기호와 사이버 공간을 표현하는 전술도식만을 다룬다.

3.3 사이버 부대, 장비, 시설의 표현 방법

사이버 작전을 위해 운용되는 사이버 부대, 장비, 시설들은 모두 물리적 공간에 위치한다. 또한 물리적 공간에서의 활동이 사이버 공간에 영향을 미치고 반대로 사이버 공간에서의 활동이 물리적 공간에 영향을 미친다. 예를 들어, C4I체계 서버가 적의 해킹에 의해 메일전송이 불가능해졌다면 물리적 공간에서의 지휘통신 능력이 훼손된다. 따라서 사이버 작전을 위해 물리적 공간에서 운용되는 객체들은 물리적 공간에서 정의하고 있는 전술부호를 이용하여 충분히 표현이 가능하다.



(a) friendly unit symbol for cy ber defense	(b) friendly unit symbol for cy ber attack	(c) enemy unit symbol for cy ber defense	(d) enemy unit symbol for cy ber attack

(그림 3) 사이버 부대를 표현하는 전술기호의 예

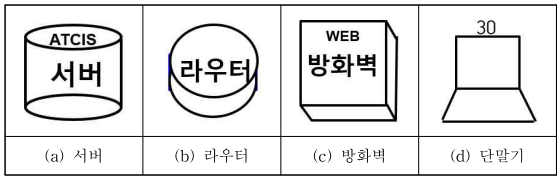
현재 사이버 부대의 편성은 크게 공격팀과 방어팀으로 구분된다. 따라서 사이버 부대의 전술기호는 표준에 제시된 방법을 준용하되 사이버 부대의 임무를 명확하게 표현하기 위해 사이버 부대의 아이콘 두 종류를 추가한다. 방패 모양의 아이콘은 방어임무를 수행하는 사이버 부대를 의미하며, 번개 모양의 아이콘은 공격임무를 수행하는 사이버 부대를 의미한다. 또한 사이버 부대임을 명시

적으로 표현하기 위해 아이콘 하단에 'cyb'라는 문자 수정자를 추가한다. (그림 3)은 사이버 공격부대, 방어부대를 표현하는 전술기호를 나타낸다. 확장자의 세부 내용은 <표 1>을 참조한다.

한편 네트워크 장비, 서버, 정보보호체계 등의 표현을 위해 새롭게 프레임을 정의하되 IT 업계에서 통상적으로 사용되는 도형을 간략화 하여 사용한다. 아이콘은 메인섹터에 서버, 라우터, 방화벽 등의 문자로 정의하고 수정자에 아이콘의 세부정보를 기입한다. 시설에 대한 표현은 표준의 방법을 그대로 적용한다. (그림 4)는 장비를 표현하는 사이버 전술기호의 예를 나타낸다. (그림 4)에

<표 1> 사이버 확장자의 필드별 의미

필드	제 목	설 명
A	아이콘	사이버 전술부호를 대표하는 기본 부호를 표현한다.
B	부대단위	사이버 부대의 규모를 표기한다.
C	장비수량	장비의 총 수량을 숫자로 표기한다. 또는 부분수량과 전체수량을 '/'로 구분하여 표기한다.
D	TF 식별	TF부대 여부를 표기한다.
E	외형 수식	사이버 전술부호임을 CY 문자로 표기한다. 피아구분, 훈련여부를 J, K, X 문자로 표기한다.
F	부대 증감	사이버 부대의 증감을 표기한다. '+': 증가, '-': 감소, '±' : 증감
G	조치 내용	사이버 부대, 시설, 장비의 피해현황에 대한 조치내용을 기입한다.
H	부가 정보	사이버 부대, 시설, 장비의 피해현황 등의 부가적인 정보를 기입한다.
J	평가 등급	표현하는 정보에 대한 신뢰성과 신빙성을 문자와 숫자로 표기한다. 신뢰성: A, B, C, D, E, F 신빙성: 1, 2, 3, 4, 5, 6
K	전투력	사이버 부대, 장비, 시설의 능력을 숫자로 표기한다.
M	상급부대	상급 부대명을 기입한다.
N	적군 표시	적 장비임을 '적' 또는 'ENY'로 표기한다.
Q	이동방향	사이버부대, 장비 및 시설에 대한 이동 또는 예상 이동 방향을 표기한다.
R	이동 수단	장비의 이동수단을 표기한다.
S	지휘소 표시/ 실제위치 표시	지휘소를 나타내거나 또는 실제 위치로부터 떨어진 객체를 표시한다.
T	고유명칭	사이버부대, 장비, 시설의 고유 식별자를 표기한다. 사이버 장비의 경우 IP주소, 포트번호 등이 될 수 있다.
V	장비명, 종류	장비명 또는 종류를 표기한다.
W	활동시각	날짜와 시각을 '년월일, 시:분:초'형식으로 표기한다.
Y	위치	부대, 장비 및 시설의 위치를 표기한다.
Z	속도	이동 속도 표시가 필요한 사이버부대, 장비 및 시설의 속도를 표기한다.
AA	지휘통제소	지휘소에 해당하는 부대는 지휘소명을 표기한다.
AB	가장/가상 식별부호	가장/가상 식별부호를 표기한다.

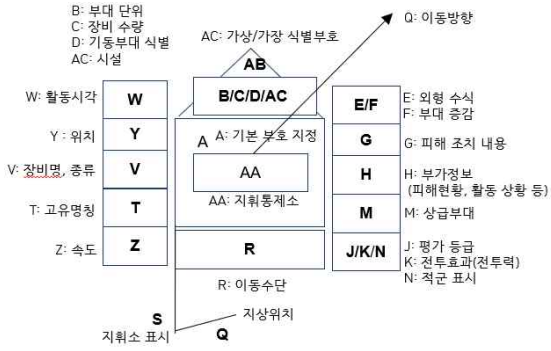


(a) 서버 (b) 라우터 (c) 방화벽 (d) 단말기

(그림 4) 사이버 장비를 나타내는 전술기호의 예

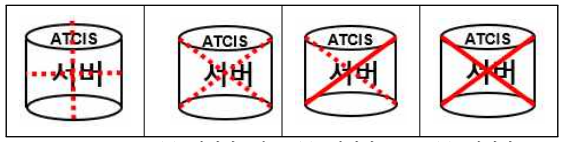
서 (d)의 전술기호 윗부분의 숫자는 수량을 나타낸다. 만약 명시적으로 숫자가 없는 경우는 1로 간주한다.

기타 부가적인 정보를 제공하는 확장자는 표준에서 제시하는 방법을 준용하되 사이버 공간에서 필요한 필드들만 선별하고 필드의 내용을 추가적으로 정의하여 사용한다. 예를 들어 필드 T에 장비의 IP 정보를 기입하고, 필드 G와 H에는 각각 사이버 피해조치내용과 사이버 피해현황 또는 활동상황을 기입한다. (그림 5)는 사이버 객체 표현을 위한 수정된 확장자를 나타낸다. 세부적인 확장자의 내용은 <표 1>을 참조한다.



(그림 5) 사이버 전술기호에 대한 확장자 필드

한편 취약점이 식별된 장비에는 붉은 점선을 '+' 모양으로 추가하고 사이버 공격을 당했지만 정상적으로 동작하는 장비에는 붉은 점선을 'X' 모양으로 추가한다. 만약 사이버 공격으로 인해 정상동작이 불가능해졌다면 붉은 색의 'X' 모양으로 표현하되 좌측 상단에서 우측 하단으로 이어지는 선분은 점선으로 그렇지 않은 선분은 실선으로 표기한다. 그리고 사이버 공격으로 인해 복구가 불가능한 상태로 파괴된 경우에는 붉은 실선의 'X' 모양을 추가한다. (그림 6)은 장비의 상태를 표현하는 예를 나타낸다.

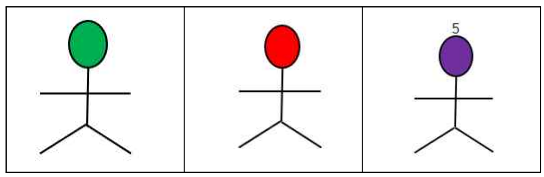


(a) 취약점 존재 (b) 사이버공격이 있었으나 정상동작 (c) 사이버 공격으로 정상동작불가 (d) 사이버 공격으로 물리적으로 파괴

(그림 6) 장비의 상태를 나타내는 전술기호의 예

3.4 사이버 인물의 표현 방법

물리적 공간에서는 일반적으로 한 개인이 발휘할 수 있는 물리적 영향력이 제한적이다. 따라서 부대가 아닌 각개 전투원은 전체 작전수행 과정에서 주요 관심 대상이 아니다. 하지만 사이버 공간에서는 한 개인이 전체 사이버 공간을 장악할 수 있을 정도로 막대한 영향력을 발휘할 수 있다. 또한 내부 네트워크 공간에서 활동하는 용역업체 직원들은 사이버 공격의 취약점이 될 수 있다. 따라서 사이버 주요 인물을 표현하는 것이 필요하다. 하지만 현재 표준에는 특정 인원을 표현하는 방법이 제시되어 있지 않기 때문에 추가적인 표현 방법이 필요하다. (그림 7)은 사이버 인물에 대한 아이콘을 나타낸다. 머리의 색상을 통해 피아식별을 하는데 녹색, 빨간색, 보라색은 각각 아군, 적군 그리고 민간인을 나타낸다. 그리고 머리 위의 숫자는 인원수를 의미하며 명시적인 숫자 표시가 없으면 1명으로 간주한다. 세부적인 확장자의 내용은 <표 1>을 참조한다.



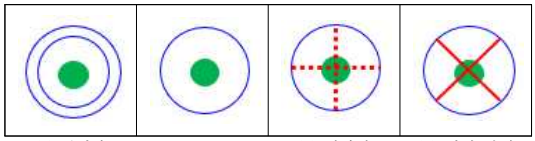
(a) 아군 인원 1명 (b) 적군 인원 1명 (c) 민간인 5명

(그림 7) 사이버 공간에서 인원을 나타내는 전술기호의 예

3.5 사이버 페르소나의 표현 방법

사이버 페르소나는 사이버 공간에서 활동 주체를 구분하는 가상의 객체라 할 수 있다. 계정 정보를 제외한 기타 사이버 페르소나는 사이버 인물 부호의 확장자 필드 H에 부가정보로 표현한다.

한편, 계정은 사이버 공간에서 정보의 접근, 처리 등에 관해 특정 개인에게 할당된 권한으로 계정의 유출, 탈취는 큰 사이버 위협을 야기한다. 특히 관리자 계정인 경우 그 문제는 더욱 심각해진다. 따라서 사이버 공간의 상황을 이해하기 위해 계정의 관리상태, 취약성 등을 확인하는 것이 필요하다. 하지만 현재 표준에서는 사이버 계정을 표현하기 위한 적절한 방법이 제시되어 있지 않기 때문에 이를 표현하기 위해 프레임을 사용하지 않는 아이콘을 (그림 8)과 같이 정의한다. 계정은 크게 관리자 계정과 일반계정으로 구분한다. 일반계정은 큰 원안에 작은 원이 중앙에 위치한 형태이다. 작은 원의 색상은 피아식별을 나타낸다. 그리고 관리자 계정은 큰 원이 하나 더 추가된 형태이다. 한편 취약점이 있는 계정은 큰 원 안에 '+' 모양으로 붉은 점선을 추가하고, 침해된 계정은 'X' 모양으로 붉은 실선을 추가한다. 세부적인 확장자의 내용은 <표 1>을 참조한다.

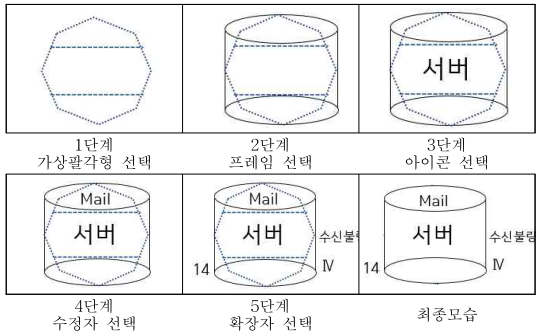


(그림 8) 계정을 나타내는 전술기호의 예

3.6 사이버 전술기호 생성 절차

사이버 전술기호의 생성절차는 표준에서 제시한 방법과 동일하다. 먼저 가상의 팔각형에 프레임을 선택하고, 아이콘, 수정자, 확장자를 조합한다. (그림 9)는 사이버 전술기호의 생성 절차의 예를 도식적으로 나타낸다.

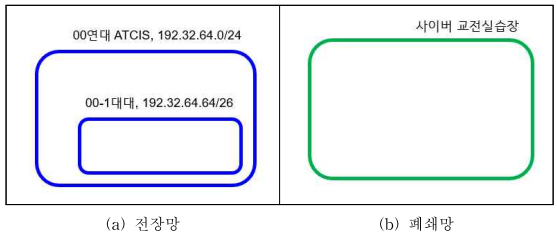
3.7 사이버 공간의 표현



(그림 9) 사이버 전술기호 생성 절차

사이버 공간은 둥근 사각형으로 표현하며 사각형 안에는 해당 공간을 구성하는 객체들을 사이버 전술기호 형태로 배치한다. 사이버 공간 안에 하위 공간을 추가로 표현해야 하는 경우에는 사각형 안에 사각형을 추가적으로 도시한다. 사각형의 크기는 도시되는 상황도의 크기와 포함되는 전술기호에 따라 융통성있게 설정한다. 왜냐하면 사이버 공간은 물리적인 공간과 달리 상대적인 크기 개념이 명확하지 않고 공간의 크기가 사이버 작전 상황을 이해하는데 필수적인 요소는 아니기 때문이다.

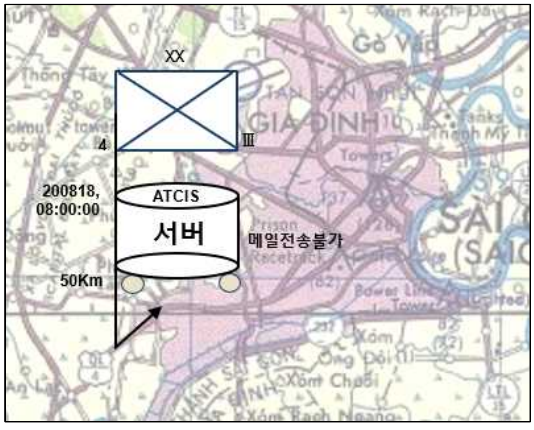
한편, 사이버작전 측면을 고려했을 때 사이버 공간은 크게 인터넷, 국방망, 전장망, 폐쇄망으로 구분할 수 있다. 이들 공간의 유형은 1차적으로 사각형의 색상으로 구분한다. 노란색, 검은색, 파란색 그리고 초록색은 각각 인터넷, 국방망, 전장망, 폐쇄망을 의미한다. 그리고 사이버 공간의 이름 또는 IP 대역을 사각형의 우측 상단에 표기한다. (그림 10)은 사이버 공간을 전술도식으로 표현한 예를 나타낸다.



(그림 10) 사이버 공간에 대한 전술기호의 예

4. 제안한 사이버 전술기호를 활용한 사이버 상황 표현 예제

본 장에서는 앞서 정의한 사이버 전술기호들을 이용하여 사이버 상황을 어떻게 표현할 수 있는지 예제를 통해 살펴본다. 사이버 상황은 군사지도 위에 사이버 전술기호를 배치하여 물리적 작전상황과 함께 표현될 수도 있고, 사이버 공간만을 위한 별도의 상황도에 독립적으로 표현될 수도 있다. 사이버 객체의 물리적 위치보다는 데이터 흐름을 가시화하는 것이 중요하다면 별도의 사이버 상황도가 필요하다.

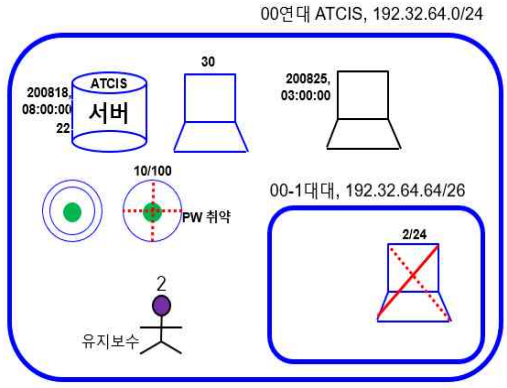


(그림 11) 지도에 도시된 사이버 전술기호의 예

(그림 11)은 지도 위에서 사이버 전술기호를 도시한 예이다. 일반적으로 ATCIS[3] 서버는 지휘소와 동일한 지점에 위치한다. 따라서 지휘소를 나타내는 기존 전술기호와 함께 도시하는 것이 가능하며 사이버 전술기호에 포함되어야 할 확장자의 수를 감소시킬 수 있어 가독성을 개선할 수 있다. 예를 들어 (그림 11)에서 지휘소 전술기호에 소속과 상급부대가 명시되어 있기 때문에 ATCIS 서버를 나타내는 전술기호에 추가적으로 소속과 상급부대 등을 표기할 필요가 없다. (그림 11)의 사이버 전술기호가 의미하는 것은 다음과 같다.

"3군단 4사단 소속의 차량화된 ATCIS 서버가 20년 8월 18일 08시부터 메일전송이 불가능한 상태이고 현재 지도에 표기된 지점에 위치해 있으며 3시 방향으로 50km의 속도로 지휘소와 함께 이동중에 있다."

지도 위에 사이버 전술기호가 사용되기 때문에 현재 위치, 이동방향 등의 표기가 용이하다.



(그림 12) 지도가 아닌 별도 상황도에 도시된 사이버 전술기호의 예

(그림 12)는 지도가 아닌 별도 상황도에 사이버 공간을 정의하고 사이버 전술기호를 추가하여 사이버 상황을 표현한 것이다. 사이버 공간을 나타내는 둥근 사각형 안에 서버, 단말기, 계정, 사이버 인물을 나타내는 사이버 전술기호들이 있다.

(그림 12)에서 선들이 파란색이기 때문에 네트워크가 전장망임을 직관적으로 알 수 있다. 그런데 서버, 단말기 등의 장비들 간의 물리적인 선로 연결은 명시적으로 표시되지 않았다. 이는 동일한 사이버 공간(즉, 둥근 사각형) 안에 존재한다는 것은 상호 연결되어 있어 네트워킹이 가능하다는 것을 암묵적으로 의미하기 때문이다. 또한 물리적인 선로 연결도는 전술적 상황판단보다 기술적 상황판단시에 필요하기 때문에 선로 연결은 표현하지 않는다.

서버를 나타내는 전술기호는 192.32.64.22 주소를 사용하는 ATCIS 서버이며 20년 8월 18일 08시 이후 정상적으로 운용되고 있음을 나타낸다.

3) 지상전술C4I체계(ATCIS: Army Tactical Comm and Information System)

단말기를 나타내는 전술기호는 총 3개가 있다. 제일 외곽 둥근 사각형에 포함되어 있는 파란색 단말기 모양의 전술기호는 00 연대 소속의 ATCIS 단말기로 30대가 정상 운용 중임을 나타낸다. 반면 내부에 둥근 사각형에 포함되어 있는 단말기 모양의 전술기호는 00-1대대 소속의 ATCIS 단말기 24대 중 2대가 사이버 공격으로 인해 정상적으로 동작하지 않고 있다는 것을 의미한다. 한편 검은색 단말기 모양의 전술기호(즉, 국방망용 단말기)가 있는데 이는 20년 8월 25일 03시에 국방망 단말기가 전장망에 잘못 연결되어 현재 망혼용이 발생하고 있음을 나타낸다.

계정을 나타내는 전술기호들은 해당 네트워크에 관리자 계정 1개와 일반 사용자 계정 100개가 있으며 일반 계정 중 10개의 비밀번호가 취약하다는 것을 나타낸다. 한편, 사이버 인물을 나타내는 전술기호는 유지보수업체 직원 2명이 전장망 접근이 가능함을 나타낸다.

(그림 12)를 통해 살펴본 바와 같이 단순한 기호들의 조합을 통해 사이버 공간에서의 다양한 상황을 직관적으로 이해할 수 있음을 알 수 있다. 또한 제안하는 방법은 MIL-STD-2525D 표준에서 제시하고 있는 부호 생성 절차와 규칙을 준용하고 있기 때문에 MIL-STD-2525D 표준에 익숙한 이들은 짧은 시간의 학습을 통해 쉽게 사이버 전술기호를 이해할 수 있을 것으로 판단된다.

5. 결론 및 향후 연구

본 논문에서는 제5의 전장으로 인식되는 사이버 공간에서의 상황을 신속하게 인식하고 공유하기 위한 사이버 전술기호들을 정의하고 생성 절차 및 방법을 제안하였다. 또한 제안한 전술기호들을 이용하여 사이버 상황을 표현한 예시들을 통해 제안한 방법의 유용성과 활용 가능성을 살펴보았다. 제안한 방법은 MIL-STD-2525D 표준에서 제시한 전술기호 생성방법과 절차를 준용하고 있어 기존 군대부호에 익숙한 이들이라면 추가적인 많은 노력 없이 사이버 전술기호를 이해하고 활용할 수 있을 것으로 판단된다.

하지만 본 연구는 군대부호 중 사이버 전술기호와 사이버 공간을 표현하기 위한 일부 사이버 전술도식에 국한되어 있다. 사이버 활동, 임무, 책임 등을 표현하기 위한 사이버 전술도식에 대한 연구가 추가적으로 필요하다. 향후 본 연구 결과를 바탕으로 사이버 전술도식에 대한 연구를 수행하여 전술기호와 전술도식을 이용하여 사이버 작전상황을 보다 완전하게 표현할 수 있는 표준을 만들어갈 예정이다.

참고문헌

[1] Harrison, Yvonne, and James A. Horne, "Sleep loss and temporal memory," The Quarterly Journal of Experimental Psychology: Section A 53.1, pp. 271-279, 2000.

[2] Pilcher, June J., and Allen I. Huffcutt. "Effects of sleep deprivation on performance: a meta-analysis," Sleep, Vol. 19, No. 4, pp. 318-326, 1996.

[3] No-Hyeok Park, "A Study on Development Trend of Joint Military Symbology," 2019 KIMST Annual Conference Proceedings, pp. 1445-1446, 2019.

[4] Sungho Kong, "A Study on the connetion between war-fighting symbology of combat system and tactical data link," 2019 KIMST Annual Conference Proceedings, pp. 616-617, 2019.

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

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

[7] Fugate, Sunny J., and Robert S. Gutzwiller. "Rethinking Cyberspace Symbology," NATO IST-HFM-154, Cyber Symbology Specialists' Meeting, USA, 2016.

[8] M. Varga, C. Winkelholz and S. Träber-Burdin, "An Exploration of Cyber Symbology," 2019 IEEE Symposium on Visualization for Cyber Security (VizSec), pp. 1-5, 2019.

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

[10] Koohyung Kwon, et. al., "A Study of Cyber Operation COP based on Multi-layered Visualization," Journal of Information and Security, Vol. 20, No. 4, 2020.10.

〔저자소개〕

이 종 관 (Jongkwan Lee)
2000년 2월 육군사관학교 전자공학과 학사
2004년 2월 한국과학기술원 전자공학 석사
2014년 2월 아주대학교 NCW 박사
2017년 12월~현재 육군사관학교 컴퓨터과학과 조교수
email : jklee64@kma.ac.kr

이 민 우 (Minwoo Lee)
1998년 2월 한국항공대학교 학사
2013년 2월 아주대학교 NCW 박사
2019년 3월~현재 아주대학교 국방디지털융합학과 대우부교수
email : iminu@ajou.ac.kr

김 종 화 (Jong-hwa Kim)
2010년 아주대 NCW학과 박사수료
현 재 육군사관학교 사이버전연구센터 연구실장
email : joakim_kma@mnd.go.kr

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

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

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