J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

사이버공간 내 상황인식을 위한 사이버 공통 작전 상황도 연구☆

A study on the cyber common operation picture for situational awareness in cyberspace

김 국 진[1,2] 윤 재 필[1] 윤 석 준[3] 강 지 원[1,3] 김 경 신[4] 신 동 규[1,2,3*]
Kook-jin Kim Jae-pil Youn Suk-joon Yoon Ji-won Kang Kyung-shin Kim Dong-kyoo Shin

요 약

사이버공격은 사이버공간에서 눈 깜짝할 사이에 일어나며, 그 피해는 전 세계에 점차 늘어나고 있다. 따라서, 사이버공간 3계층에 속하는 다양한 자산들을 여러 가지 시각에서 파악할 수 있는 사이버 공통작전상황도의 개발이 필요하다. 이는 군에서 사용하는 전장 정보 파악에 대한 방안을 적용하면 최적의 사이버공간 내 상황인식을 할 수 있다. 따라서 본 연구에서는 사이버 공통작전상황도에 필요한 가시화 화면들을 식별하고 기준(응답속도, 사용자 인터페이스, 객체 기호, 객체 크기)들을 조사한다. 그 후 식별 및 조사한 사항들을 적용하여 프레임워크를 설계하고 그에 따라 가시화 화면들을 구현한다. 최종적으로 가시화 화면이 조사한 기준 중 사진으로는 알아볼 수 없는 응답속도에 대한 실험을 진행한다. 결과적으로 구현된 가시화 화면들은 모두 응답속도 기준에 부합했다. 이와 같은 연구는 지휘관이나 보안 담당자들이 사이버공격을 대비하기 위한 사이버 공통작전상황도를 구축하는데 도움이 된다.

☞ 주제어 : 사이버보안, 사이버 지휘통제, 사이버공간, 사이버 작전, 사이버 상황인식, 사이버 공통작전상황도

ABSTRACT

Cyber-attacks occur in the blink of an eye in cyberspace, and the damage is increasing all over the world. Therefore, it is necessary to develop a cyber common operational picture that can grasp the various assets belonging to the 3rd layer of cyberspace from various perspectives. By applying the method for grasping battlefield information used by the military, it is possible to achieve optimal cyberspace situational awareness. Therefore, in this study, the visualization screens necessary for the cyber common operational picture are identified and the criteria (response speed, user interface, object symbol, object size) are investigated. After that, the framework is designed by applying the identified and investigated items, and the visualization screens are implemented accordingly. Finally, among the criteria investigated by the visualization screen, an experiment is conducted on the response speed that cannot be recognized by a photograph. As a result, all the implemented visualization screens met the standard for response speed. Such research helps commanders and security officers to build a cyber common operational picture to prepare for cyber-attacks.

☞ keyword : Cybersecurity, Cyber Command & Control, Cyberspace, Cyber Operation, Cyber Situational Awareness, Cyber Common Operational Picture

1. 서 론

인터넷의 급속한 성장과 함께 사이버공간 내에서 사이버공격이 날로 증가함에 따라 사이버보안의 중요성이 증대되고 있다 [1,2]. 국방 분야에서도 이러한 중요성을 인지하여 美, 국방부(The United States Department of Defense)는 사이버공간을 육지, 바다, 공중, 우주에 이어 제5 전장으로 지정했다 [3]. 그리고 사이버공간 내에서 진행되는 작전을 계획, 실행 및 평가하기 위한 교리를 배포했다 [4].

사이버공격은 평시 상황뿐만 아니라 전시상황에서도 마찬가지로 활발히 진행되고 있다. 현재까지 진행되고 있는 우크라이나와 러시아전을 살펴보면, 재래식 전력뿐만 아니라 사이버공격을 동원하는 복합전술인 하이브리드전

1 Department of Computer Engineering, Sejong University, Seoul, 05006, Korea.
2 Department of Convergence Engineering for Intelligent Drones, Sejong University, Seoul, 05006, Korea.
3 Department of Cyber Warfare Research Center, Sejong University, Seoul, 05006, Korea.
4 Advanced Defense Science & Technology Research Institute of Agency for Defense Development, Daejeon, 34186, Korea.
* Corresponding author (shindk@sejong.ac.kr)
[Received 25 August 2022, Reviewed 17 September 2022(R2 6 October 2022), Accepted 14 October 2022]
☆ 본 연구는 2020년 국방과학연구소에서 주관하는 미래도전국방기술 연구개발사업(9129156)의 지원을 받아 수행되었습니다.

(Hybrid Warfare)을 전쟁 시작부터 지금까지 꾸준하게 시행하고 있었다 [5-7]. 우크라이나에 대한 사이버공격은 전투 첫 3일 동안 196%나 급증했으며, 러시아는 4% 증가했다 [8].

이러한 사이버공격에 대비하기 위해서는 사이버 상황을 신속하게 인지하는 것이 필요하다. 그러기 위해서는 통상 지휘관이나 보안 담당자들이 사이버 상황인식에 사용할 수 있는 사이버 공통작전상황도(CyCOP: Cyber Common Operational Picture)가 필요하다. 효과적인 CyCOP을 개발하기 위해서는 첫 번째로는 사이버공간 내 데이터 또는 실제 데이터를 여러 관점에서 분석할 수 있는 화면들이 필요하다. 두 번째로는 데이터가 오고 가는 사이버공간의 상황을 순식간에 파악해야 하므로 빠른 응답시간과 높은 인지도를 갖춰야 한다.

본 연구는 사이버 상황인식을 위한 CyCOP Framework 설계 연구이다. 이를 위한 목표로는 위의 설명과 같이 사이버 공격에 대비하는 것이다. 그에 따라 본 연구는 5개의 장으로 구성되며, 2장부터 5장까지의 요약은 아래와 같다. 2장에서 공개된 군 교범에 명시된 작전계획과 사이버 상황인식에서 CyCOP의 필요성을 도출한다. 그리고 CyCOP을 구성하기 위한 화면들을 식별하고 인터페이스를 구성을 위해 응답속도, 객체 아이콘 등의 연구 들을 조사한다. 3장에서는 2장에서 조사한 공개된 군의 교범이나 여러 연구자료 들에서 시사점을 도출한다. 그리고 도출된 시사점을 바탕으로 CyCOP 프레임워크(Framework)를 설계 및 구현한다. 4장에서는 구현한 CyCOP 화면들의 응답시간에 대한 실험을 진행한다. 마지막으로 5장에서는 본 논문에 대한 결론을 도출한다.

2. 관련 연구

2.1 사이버 작전 및 사이버 상황인식 정의

2.1.1 사이버 작전 정의

사이버공간은 인터넷, 네트워크 등을 포함한 정보 시스템 인프라가 상호 의존적으로 구성된 정보 환경 내의 글로벌 도메인이다 [9]. 사이버 작전은 사이버공간 내에서 목표를 달성하는 행위이다 [4]. 그리고 사이버 작전을 수행하는 공간은 3개의 네트워크 계층으로 분류되며, 각 계층에 대한 설명과 요소는 아래와 같이 기술된다 [4,10,11].

1) 물리적 네트워크 계층: 지리적 구성요소와 물리적 네트워크 구성요소(라우터, 서버, 컴퓨터 등)를 포함하는 계층.
2) 논리적 네트워크 계층: 네트워크 노드 사이에 존재하는 논리적 연결로 구성된 논리 네트워크 구성요소(APP(Application), OS(Operational System) 등)를 포함하는 계층.
3) 인적 네트워크 계층: 사이버공간 내에서 작업을 계획하고 실행하는 행위자 또는 사용자의 정보(이름, 나이, E-mail, SNS 계정 등)를 포함하는 계층.

JOPP(Joint Operational Planning Process)는 모든 수준의 계획과 군사 작전의 전체 범위에 걸친 임무를 지원하는 기술이다 [12]. 또한 임무 완수를 위한 부대의 행동을 시간, 공간, 목적에 따라 동기화하는 기획부터 지휘까지의 과정이다. 하지만 이는 사이버공간이 고려되지 않은 절차이다. 이에 따라 JP(Joint Publication) 3-12 [4]는 JOPP에서 사이버공간 작전계획 고려사항을 적용하는 방안을 제시했으며, 이는 그림 1과 같이 JCOPP(Joint Cyberspace Operational Planning Process)로 정리된다.

(Figure 1) Joint Cyberspace Operational Planning Process based on Joint Publication 3-12

2.1.2 사이버 상황인식 정의

상황인식은 군사 분야에서 가장 활성화되어 있는 연구이다. 이는 환경에 있는 개체에 대한 인식, 의미에 대한 이해, 가까운 미래 상태에 대한 예측이다 [13-15]. 이러한 상황인식을 사이버공간 내에서도 수행하기 위해 여러 가지 연구가 수행되었다. P. Barford et al. [16]는 사이버 상황인식을 아래와 같은 7가지 측면으로 설명했다.

1) 현재 상황을 알고 있어야 한다: 침입 탐지를 넘어선 공격 식별 및 인식할 수 있어야 한다.
2) 공격의 영향에 주의하라: 현재, 미래에 대한 영향 평가를 수행해야 한다.
3) 상황이 어떻게 전개되는지 인식하라: 상황 추적은 이 측면의 주요 구성요소이다.
4) 위협 행위자의 행동에 주의하라: 상황 자체보다 상황 내 공격자 또는 위협 행위자의 행동에 중점을 둔다.
5) 현재 상황이 왜 그리고 어떻게 발생했는지 인식하라: 인과관계 분석 및 포렌식이 포함된다.
6) 수집된 상황인식 정보 항목 및 파생된 지식 결정의 품질을 인식한다: 구체적인 인식의 일부로 볼 수 있다.
7) 현재 상황의 그럴듯한 미래를 평가한다: 위협이 미래에 취할 수 있는 경로 및 행동을 예측한다.

U. Franke 등 [17]은 사이버공간에서 발생하는 모든 종류의 의심스러운 활동에 대한 인식이 포함되며, 전체 상황에 대한 추가 통찰력을 제공하는 것이 사이버 상황인식이라고 정의했다.

O. Jacq 등 [18]은 데이터의 수집, 융합 및 시각화를 통해 사건, 사건의 기원, 결과 및 미래의 예측을 인식하여 의사결정자를 돕는 것이 사이버 상황인식이라고 정의했다.

위의 연구[13-18]를 종합하면 사이버 상황인식은 위협 행위자의 행동을 중심으로 현재 상황을 자세히 인식하고 미래 상황을 예측하는 것으로 정의된다.

2.2 사이버 공통작전상황도(CyCOP)

군사 분야에서 COP(Common Operational Picture)은 일반적인 상황을 인식하고, 변화하는 상황에 대한 데이터를 업데이트하고, 내부 및 외부시스템과 데이터를 교환하고, 정보를 수집한다. 이러한 COP은 사용자가 데이터 시각화 화면을 보고 상황인식을 쉽게 할 수 있다면 효과적인 명령 및 제어 시스템이라고 할 수 있다 [19-24].

CyCOP은 지휘관의 사이버 상황인식을 위한 가시화 도구이며 정보를 제시할 때 전략적, 운영적, 전술적/기술적 수준을 고려한다 [25]. 기존의 COP과 메뉴, 기호, 입력 방법 등 사용 방법에 쉽게 적응할 수 있는 수준의 연관성을 포용해야 한다. 또한 내부적으로 사이버공간을 이용하는 기존의 무기체계 또는 지휘통제(C2: Command & Control) 체계를 충분히 지원할 수 있어야 한다 [26-35].

2.2.1 사이버 전장정보분석

美, ATP(Army Techniques Publication) 2-01.3 IPB(Intelligence Preparation of the Battlefield) [36]는 작전에 미치는 영향을 결정하기 위해 관심 지역의 적, 지형, 날씨 및 시민 고려사항의 임무 변수를 분석하는 체계적인 절차가 기술되어 있다. 절차의 목적은 적의 의도를 파악하는 것이다. 각 절차마다 가시화해야 할 투명도 및 템플릿 예제를 제공하고 있으며, 사이버공간에서의 전장정보분석 절차는 아래와 같다.

1) 작전환경 (OE: Operation Environment): 작전지역 내에서 사이버공간의 3계층(JP 3-12 [4]) 구성요소 및 위협의 현재 물리적 위치를 그래픽으로 가시화한다. 사이버공간 3계층 식별사항은 표 1과 같다.

(Table 1) Identification items for each layer in cyberspace

사이버공간 계층	식별사항
물리 네트워크	사이버 C2 시스템, 사이버 네트워크 교두보 노드, 네트워크 장치 (PC, 서버, 라우터 등), 내·외부망 접점 노드, IDS/IPS 등
논리 네트워크	웹사이트, 취약점, 자원 URL 경로, 메신저, repository 주소, S/W(Software), OS, One Time Password APP 등
인적 네트워크	ATP(Advanced Persistent Threats) 그룹, 문서, 사진, 비디오, 개인키, 공개키, 비밀번호 등

2) 작전에 미치는 환경적 영향 설명: 수정된 종합 장애물 투명도(MCOO: Modified Combined Obstacle Overlay)는 사이버공간 3계층을 반영하여 가시화한다. 이는 인터넷을 사용할 수 있는 외부망과 인터넷을 사용하지 않는 내부망(폐쇄망)으로 구분된다. 그리고 외부망과 내부망을 잇는 접점(방화벽) 등을 고려하여 가시화한다.
3) 위협평가: 위협 특성 최신화, 위협 모델 생성, 광범위한 위협 대응 방책 개발, 고가치표적의 식별이 되어야한다.

또한 사이버공격 구조 및 공격자의 과거 패턴 분석 시, 위협에 대한 상황을 이해하는데 도움이 되어야한다. 그리고 위협이 선호하는 내부 이동 공격 기법, 위협 요소에 사용되는 모든 멀웨어(Malware)를 볼 수 있어야 하며, 위협이 작전 또는 지점을 수행할 수 있는 능력에 중요 자산(고가치표적)을 식별해야 한다.

4) 위협 대응 방책 결정: 위협 대응 방책 선택 시, 예상되는 조치(경로) 등을 그래픽으로 표시해야 한다. 그리고 MCOO를 중첩하여 환경적 영향을 통합하고 특정 대응 방책을 실행하는 위협을 표현해야 한다.

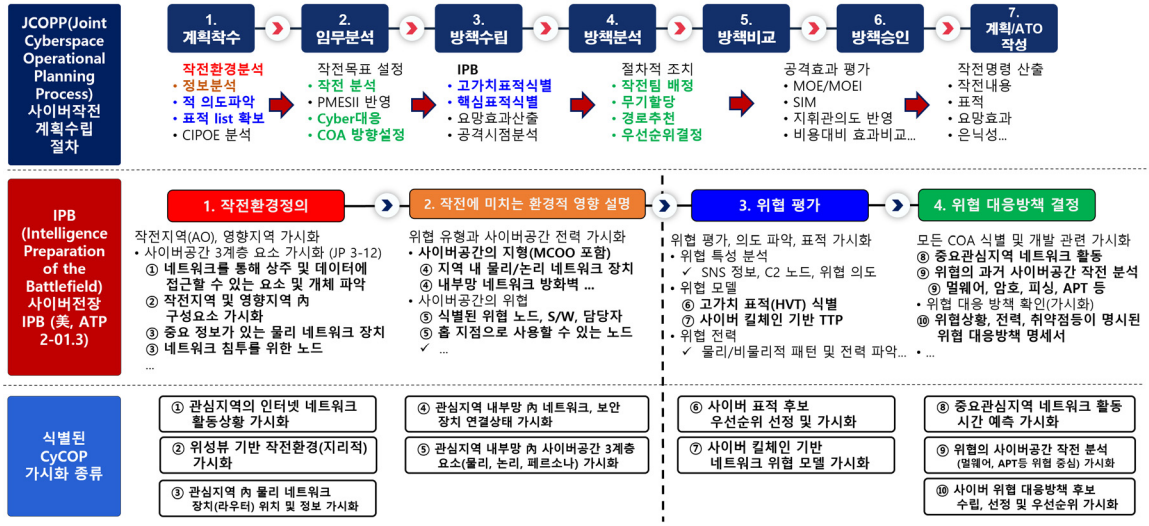
2.2.2 CyCOP 가시화 종류 식별

2.1.1에서 조사한 JCOPP와 2.2.1에서 조사한 ATP 2-01.3 IPB를 기반으로 CyCOP을 구성할 때 필요한 가시화 종류를 그림 2와 같이 식별한다. JCOPP 1단계 계획착수부터 5단계 방책 비교 일부까지 ATP 2-01.3에 포함된다. JCOPP의 붉은색 글씨는 IPB 1단계에 해당되며, 주황색 글씨는 IPB 2단계에 해당된다. 이와 같은 방법으로 IPB 4단계까지 식별된다. CyCOP 가시화 종류는 IPB의 각 단계에서 각 요소 및 정의에 따라 식별했다. 그림에서는 IPB 단계 상세 설명에서 ①이라고 표시된 항목은 식별된 CyCOP 가시화 종류에서 ①에 해당된다. 이와 같은 요령으로 ⑩까지의 가시화 종류를 식별했다.

표 2는 그림 2에서 확인된 10가지 유형의 가시화 중 어떤 시각화가 조사된 CyCOP 연구들 [25-35]에서 구현되었는지 요약한 결과이다. 표 2를 보면 대다수의 연구들은 지리적 가시화(②)와 내부망 네트워크 연결상태(④)만을 가시화하고 있음을 알 수 있다. 하지만 이 경우 IPB 3단계인 '위협 평가'에서 고가치표적을 식별할 수 있는 정보가 부족하다. 따라서 본 연구에서는 IPB 1, 2단계의 가시화 화면들(①~⑤)를 구현하여, 추후 IPB 3단계에서 고가치 표적을 식별할 수 있도록 정보를 구체적으로 표현할 것이다.

2.3 사이버 공통작전상황도(CyCOP) 인터페이스

빠르게 이뤄지는 사이버공격을 신속하게 대비·대응하기 위해서는 사이버 상황인식이 빨라야 한다. 그러기 위해서 CyCOP은 빠른 시스템 응답시간이 필요하고 누구나 쉽고 빠르게 알아볼 수 있어야 한다. 본 장에서는 4가지 항목에 대하여 조사한다. 첫 번째로, 사용자가 빠르다고 인지하는 시스템 응답시간에 관한 연구 및 메뉴얼들을 조사한다. 두 번째로, CyCOP 가시화 화면 사용자 인터페이스(UI: User Interface)에 대하여 조사한다. 세 번째로, 사용자가 CyCOP 가시화 화면을 볼 때, 명확히 이해할 수 있도록 하는 객체 기호에 대하여 조사한다. 네 번째로, CyCOP 가시화 화면 내에서 표기되는 객체 크기에 대하여 조사한다.



(Figure 2) Identification of types of CyCOP visualization based on JCOPP and ATP 2-01.3 IPB

(Table 2) Visualization implementation status in CyCOP studies

연구	구현된 가시화 번호
M. Esteve 등 [25]	②
T. Pahi 등 [26]	가시화 컨셉/방법론만 제시됨
S. Noel 등 [27]	②, ④
R. S. Gutzwiller 등 [28]	가시화 컨셉/방법론만 제시됨
S. Jajodia 등 [29]	④
M. Jenkins 등 [30]	②, ④
S. Llopis 등 [31]	②, ③, ④
L. Jiang 등 [32]	여러 가시화 연구에 대한 리뷰만 작성되어 있음
H. Doucette [33]	가시화 컨셉/방법론만 제시됨
C. Dillabaugh 등 [34]	②, ④
L. Beaudoin 등 [35]	가시화 컨셉/방법론만 제시됨

2.3.1 응답시간 관련 연구

美, MIL-STD(Military Standard)-1472H [37]에서는 응답시간이 일어날 수 있는 항목별로 그에 대한 정의와 시간들을 표 3과 같이 제시하고 있다. 또한, 실시간 시스템의 최대 시스템 응답시간은 표 3의 값을 초과하지 않아야 한다고 제시하고 있다.

(Table 3) Acceptable system response time

시스템 설명	응답시간 정의	시간(초)
키보드, 스크롤휠, 광학 휠, 마우스 클릭	키보드, 마우스 동작 후 모니터에 반응이 나타날 때까지 시간 (예: 클릭)	0.1
키보드 타이핑	타이핑 후 모니터에 형상이 나타날 때까지 시간	0.2
페이지 넘기기	페이지 넘긴후 처음 몇줄이 보일때까지 시간	1.0
페이지 스크롤	텍스트가 스크롤 될 때까지 시간	0.5
XY entry	필드 선택 후 시각으로 확인하기까지 시간	0.2
Pointing	포인트 값을 입력 후 모니터에 시현 될 때까지 시간	0.2
Sketching	점 입력 후 선으로 시현 될 때까지 시간	0.2
Local update	로컬 데이터베이스를 사용하여 영상으로 변화하는데 걸리는 시간	0.5
Host update	쉽게 액세스할 수 있는 형태의 호스트 데이터 위치 변경(예: 기존 이미지 축척변경)	2.0
File update	이미지를 업데이트하려면 호스트 파일에 액세스해야 함	10
조회(단순)	명령에서 일반적으로 사용되는 메시지 표시까지 시간	2.0
조회(복잡)	통상 반응은 그래픽 형식, 복잡한 계산이 종종 요구됨.	10
오류피드백	입력 초기에서 오류 메시지가 나타날 때까지	0.2

Kim 등 [38]은 스마트폰 관련 분야의 응답시간 연구에서 일반적으로 사용자들이 조작 후 느끼는 응답시간에 대해 0.1~0.2초 내에 시스템이 응답하면 순간적(Instantaneous)이라고 느끼며, 응답시간이 0.5~1초면 즉각적(Immediate), 2~5초면 진행중(Continuous), 7~10초면 끊김(Captive)으로 느낀다고 제시했다. 표 4는 사람의 응답시간에 대한 연구와 지침에서 제시하는 사용자 조작 후 적절한 시스템의 최소 응답시간에 대한 지침을 요약하여 정리한 것이다. 이 연구에서 주목해야 할 내용은 일반적으로 사용자들이 응답시간이 5초까지는 시스템이 정상적으로 작동중이라 생각하고 진행 과정에 관심을 갖게 되지만 응답시간이 7초 이상이면 시스템이 정상적인 작동을 하지 않는다고 생각한다는 점이다. 따라서 사용자들에게 최소 시스템이 정상적으로 작동되고 있다는 신뢰를 주기 위해서는 응답시간이 5초 이내여야 한다고 제시하고 있다.

B. Shneiderman [39]은 대부분의 사용자가 짧은 응답시간을 선호하고 응답시간이 15초 이상 걸리면 집중이 분산된다고 제시했다. 또한 시간 정의에 따른 적절한 반응시간을 표 5와 같이 제시하고 있다.

앞서 살펴본 3가지 연구들 [37-39]은 실행에 따라 응답속도를 제시하고 있는데, 이를 다시 연산과 데이터처리의 난이도에 따라 분류하여 종합해보면 단순 응답시간(2초 이하)과 복잡 응답시간(2초 이상) 2가지로 아래와 같이 정의할 수 있다.

(Table 4) Guidelines for Appropriate Response Times

시스템 설명	적절한 응답시간(초)
스위치/버튼의 눌림 표시	0.1
키보드 입력 후 문자 표시	0.1-0.2
터치된 문자의 표시	0.2
시스템 액세스에 대한 초기 반응	1-3
기능의 실행 - 간단한 것 - 복잡한 것 - S/W의 로딩을 수반할 때	 2 5 15-60
입력 확인, 입력 오류 통지	2-4

(Table 5) Guidelines for Response Times

시스템 설명	응답시간(초)
타이핑, 커서움직임, 마우스 선택	0.05 ~ 0.15
간단하고 자주쓰는 실행	1
일반적인 실행	2 ~ 4
복잡한 실행	8 ~ 12

표 6에서는 위 연구들[37-39]이 제시하고 있는 실행항목 12개 항목 중 단순 실행으로 분류할 수 있는 10개 항목의 응답시간이 2초 이내 수준이며 복잡한 조회 등의 연산이나 데이터처리가 필요한 실행항목은 응답시간을 10초 수준으로 제시하고 있다. 표 안의 시간은 모두 초 단위로 표기했다.

- 단순 응답시간의 정의

▪ 입력장치 조작에 따라 시연되는 입력반응 대략 0.5초 이내에 응답 - 키보드 입력 후 문자 표시, 커서 움직임, 마우스 선택, 스위치/버튼의 눌림 표시, 스크롤휠, 광학휠, 마우스 클릭, 페이지 스캔, XY entry, Pointing, Sketching, Local update, 오류피드백 등 ▪ 입력장치의 조작 후 다소 용량이 있는 파일을 실행할 때는 1초 이내의 응답 - 페이지 넘기기, 간단하고 자주 쓰는 실행 등 ▪ 단순하고 반복적인 기능 실행은 응답속도 2초 - 지역 내 호스트로부터 단순 조회, 간단한 기능 실행, Host update 등

- 복잡 응답시간의 정의

▪ 단순하지만 연산 및 부대 지역 외 데이터 호출이 필요한 실행 - 일반적인 실행, 시스템 액세스에 대한 초기 반응, 입력 확인, 입력 오류 통지 등 - 위협정보 또는 지도 구성요소 등 다양한 데이터 호출 ▪ 복잡한 연산 및 데이터처리 등 복잡한 실행 - 시스템의 시작 또는 종료와 같이 복잡한 순차/기능 실행, S/W의 로딩을 수반할 때 - 원격 서버 데이터의 호출, File update, 복잡한 조회 등

(Table 6) Response time by related works

단순/복잡 응답시간	시스템 설명	MIL-STD-1472H [37]	Kim 등 [38]	B.Shneiderman [39]	공통
단순	키보드, 스크롤휠,광학휠, 마우스 클릭	0.1	0.1	0.05-0.15	0.1
	키보드 프린트	0.2	0.1-0.2	0.05-0.15	0.2>
	XY entry	0.2			
	Pointing	0.2			
	Sketching	0.2			
	오류피드백	0.2	2-4		2>
	페이지 스캔	0.5			
	Local update	0.5			
	페이지 넘기기	1.0			
	Host update	2.0			
복잡	조회(단순)	2.0	2.0	2-4	2.0
	조회(복잡)	10	5.0	8-12	10
	File update	10			

2.3.2 CyCOP 가시화 화면 UI 관련 연구

UI는 사용자와 시스템, S/W 등이 의사소통을 할 수 있도록 만들어진 물리적, 가상적 매개체를 뜻한다. 이러한 UI는 사용자가 사이버 상황인식을 해야 하는 CyCOP에서도 아주 중요한 사항이다.

M. Esteve 등 [25]는 좌측과 하단에 작은 화면들(Ri)를 배치하고 중앙에는 Map/Main display를 표현하고 우측에는 scorecard/Logger를 볼 수 있도록 하는 UI를 제시했다. Map/Main display에서는 지형 혹은 사이버공간 도메인을 표시할 수 있다. scorecard/Logger에서는 사용자가 시스템과 상호작용할 수 있는 추가 제어 기능 및 로그를 제공한다. Ri에서는 그래프, 차트 등 즉석에서 생성된 데이터 표현을 나타낸다.

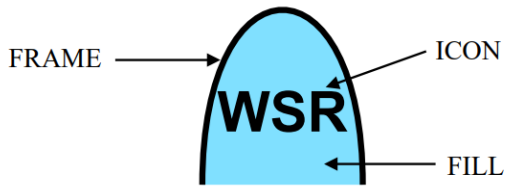
C. Dillabaugh 등 [34]은 CyCOP을 시나리오 시뮬레이션 기반으로 구현했다. 그에 따라 UI 상단과 좌측에 아래와 같은 화면기능들을 배치했다.

1) Scenario Controls: 사용자가 시나리오 시작/일시 정지/속도 조절을 할 수 있는 Widget.
2) Active Persona Widget: 현재 활성 페르소나를 설정할 수 있다. 이는 현재 시나리오 내에서 CyCOP 시나리오를 사용하고 있는 가상의 개인이다.
3) Layers Widget: 사용자가 화면 내 표시되는 Layer를 제어할 수 있다.
4) Ticket Widget: 활성 페르소나에 대한 스티커를 표시한다. Ticket은 현재 사용자에게 할당된 작업 또는 정보이다. Ticket Widget을 사용하면 활성 페르소나가 현재 할당된 모든 Ticket을 볼 수 있다.

조사한 UI 관련 연구들 [25,34]은 각 CyCOP에서 표현하고자 하는 특성에 따라 다르게 설계되었다. M. Esteve 등 [25]의 연구에서는 UI에 Ri라는 영역을 여러 개 배치해서 Map/Main display에서 선택한 객체를 그래프, 차트 등으로 객체의 상세 분석 정보를 확인하기 위한 의도가 부각되었다. C. Dillabaugh 등 [34]의 연구에서는 UI 상단과 좌측에 시나리오 관련 창들을 배치하여, 시나리오를 시계열과 같이 분석하려는 의도가 부각되었다. 위의 연구들과 같이 본 연구에서도 CyCOP 가시화 화면에서 표현하려는 의도나 주요 데이터에 따라 UI를 조금씩은 다르게 구성할 것이다.

2.3.3 화면에 표현되는 객체 기호 관련 연구

CyCOP 가시화 화면에 도시되는 객체는 모든 실무자에게 공통의 표준을 적용하여 명확히 이해시키는 것이 중요하다. E. D. McCroskey 등 [40]은 사이버공간을 논리적으로 표현하고 객체들을 육각형으로 표현했다. 객체들을 구분하기 위해 안에 여러 기호나 문자를 넣었다. 또한, 각 객체들의 행위를 선등을 사용하여 공격, 추출, 수리 등을 표현한다. 이는 사이버공간을 작전을 수행하는 공간만으로 한정하고 그에 따른 사이버공격 및 방어방책을 그래픽(Graphic)으로 표현할 때 적절한 표현 방법이다.



(Figure 3) Cyberspace symbol components

美, MIL-STD-2525D [41]에서는 사이버공간 도메인 내 객체들을 그림 3과 같이 표시할 것을 제안하고 있다.

Frame은 객체의 상태를 나타내는 기하학적 테두리이며, 아이콘(Icon)은 객체의 그래픽 표현을 제공하는 기호의 가장 안쪽 부분이다. 사이버공간 객체의 아이콘은 표 7과 같은 형식으로 작성된다. 마지막으로 Fill은 Frame 내부 영역이며, 색상은 표준 인식과 관련된 지표를 제공한다. 색상은 적대적 - 빨간색, 우호적 - 파란색, 중립적 - 초록색, 알려지지 않음 - 노란색으로 설정한다. 이와 같은 표현은 사이버공간뿐만 아니라 실제 지도상에서 표현할 수 있는 범용성이 큰 표현 방법이다. 본 연구에서는 그림 6에서 도출한 CyCOP 가시화들을 구성하기 위해 美, MIL-STD-2525D [41]의 기호 표현 기준을 준수할 것이다.

(Table 7) Some of the cyberspace icons

정의	아이콘
ROUTER Type: Entity Type Entity: DEVICE TYPE Symbol Set Code: 60 Code: 140200	RTR
FIREWALL Type: Entity Type Entity: DEVICE TYPE Symbol Set Code: 60 Code: 140900	FWL
...	...

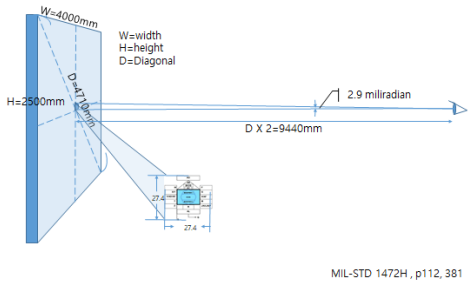
2.3.4 화면 내 표현 객체 크기에 관한 연구

美, MIL-STD-1472H [37]에서는 Wall Screen에서 CyCOP 지도 화면을 가시화할 때 기준으로 화면 크기 및 객체 크기 비율을 계산했다. 이는 표 8과 같이 화면 크기와 하나의 객체에 대한 시야각으로 객체의 크기를 정의했다.

(Table 8) Distance based on wall screen size

요인	최적	선호한계	허용한계
화면 대각선에 대한 시청 거리의 비율	4.0	3.0-6.0	2.0-10
중심선에서 벗어난 각도	0°	0-20°	0-30°
이미지 휘도	35cd/m² 1/	27-48cd/m² 1/	17-70cd/m² 1/
화면 전체의 휘도 변화	1.0	1.5	3.0
관찰 위치에 따른 휘도 변화	1.0	2.0	4.0
이미지의 가장 밝은 부분에 대한 주변광의 비율	0	0.002-0.01	0.1 최대 2/
NOTES: 1) 정지 투영의 경우 더 높은 값이 사용될 수 있다. 2) 회색조 또는 색상이 포함되지 않은 프레젠테이션(예: 선, 그림, 표)의 경우 0.2를 사용할 수 있다.			

먼저 화면 크기에 따른 사용자의 눈으로부터 화면까지 최대 예상 가시거리를 계산하면 시야각에 따른 객체의 크기를 정할 수 있다. 이때, 객체는 부가적인 글씨와 제목 등을 모두 포함한 크기이다. 예를 들어 2.5m x 4m 화면의 CyCOP을 구성할 경우 (1680x1050 또는 1900x1200 해상도에 해당) 대각선의 길이는 4.72m이므로 최적 거리는 18.9m로 결정되고 허용한계 거리는 최소 9,44m가 된다. 만일 최소거리인 9.44m로 설계했을 경우, 사용자가 인식할 수 있는 객체의 크기는 2.9 miliradian인 27.4mm 크기로 계산된다. (1miliradian = 1radian /1000)할 수 있다. 2장의 관심사는 최대 수용 객체 수이므로 수직으로 채울 수 있는 객체의 개수는 2500mm/27.4mm=91개(최대)로 그림 4와 같이 계산된다.



(Figure 4) Minimum viewing angle according to line of sight

화면의 해상도가 아래와 같은 형상이라고 가정할 때 Wall screen으로 자료를 보내는 사용자 모니터 또한 최소 객체 크기에 대해 계산할 수 있다. Wall screen의 객체를 나타내기 위해 본 연구에서 CyCOP을 구현할 때 사용하는 모니터의 해상도인 1900x1200으로 계산한다. 그에 따라 Wall screen으로 보낼 수 있는 최소 크기 객체 = 1200 pixel ÷ 91 = 13으로 최소 13 pixel 이상의 객체 크기로 구현해야 한다. 실제 Wall screen에서는 2.9 miliradian 시야각으로 Wall screen에 나타나게 되고 객체 하나의 크기는 2400/91=26(mm), 4000/91=44(mm)으로 나타나게 된다. 만일, 화면 전체를 객체 부호로 채운다면 이론상으로 8,281개의 부호를 겹치지 않고 넣을 수 있다.

3. CyCOP 프레임워크 설계 및 구현

CyCOP은 사이버공간 내 상황인식을 위한 그래픽 가시화 도구이다. 사이버공간을 외부 네트워크 정보와 내부 네트워크 정보로 구분하여 데이터를 수집하고 이를 가공하여 가시화를 해야한다. 그에 따라 CyCOP 프레임워크를 그림 5와 같이 설계했다.

3.1 외부/내부 네트워크 정보 수집

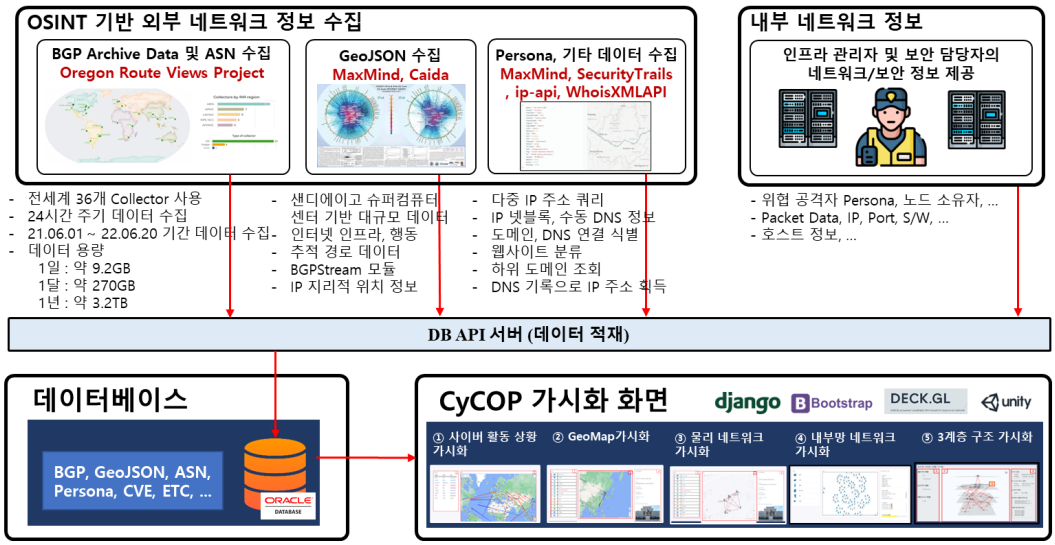
OSINT(Open Source Intelligence)는 공개된 출처에서 얻은 정보를 말한다. 즉, 그림 5의 상단의 항목은 공개된 출처의 정보를 기반으로 외부 네트워크 정보를 수집한다는 뜻이다. 외부 네트워크 정보는 BGP(Boarder Gateway Protocol)정보, Geo(Geographic)JSON, Persona 및 기타 데이터를 수집한다.

BGP는 서로 다른 자율 시스템(AS: Autonomous System)의 라우터 간에 라우팅 정보를 교환하는데 사용되는 외부 게이트웨이 프로토콜이다. 이러한 BGP 정보를 Oragon 대학교는 2시간 주기로 University of Oregon Route Views Archive Project [42]에 업로드하고 있다. 본 연구에서는 이러한 데이터를 24시간 주기로 2021.06.01.-2022.06.20.까지의 데이터를 수집했다. 데이터의 용량은 1일 약 9.2GB(GigaByte), 1달 약 260GB, 1년은 약 3.2TB (TeraByte)이다.

GeoJSON은 지리적정보를 갖는 점을 기반으로 체계적으로 지형을 표현하기 위해 설계된 개방형 공개 표준 형식이다 [43]. BGP 정보에는 상세한 지리적 정보가 없는데, 이를 MaxMind [44], Caida [45]에서 제공하는 정보를 활용하여 지리적 정보를 획득하고 이를 GeoJSON으로 변환한다.

Persona, 기타 데이터 수집에는 MaxMind, SecurityTrails [46], ip-api [47], WhoisXMLAPI [48]를 사용한다. 앞서 수집한 IP, 지리적 정보들을 활용하여 사이버공간 3계층에 포함된 정보들을 찾고 중복되지 않는 항목들을 모두 수집한다.

내부 네트워크 정보는 인프라 관리자 및 보안 담당자에게 요청하여 네트워크 장비, S/W, 방화벽, IP, Port 등의 정보를 수집한다.

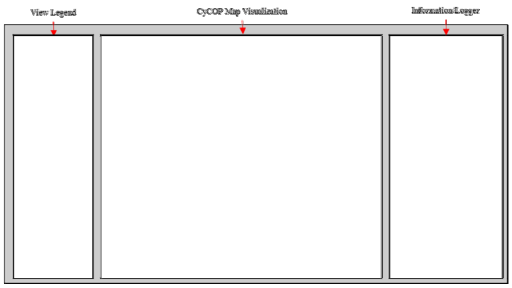


(Figure 5) CyCOP Framework Structure

3.2 CyCOP 가시화

2장에서 도출한 반응속도, UI, 객체 기호, 객체 크기를 준수하여 CyCOP 인터페이스를 설계한다. 반응속도를 준수하기 위해 가시화 출력 시, 파일들을 최소한으로 호출한다. UI는 그림 6과 같이 설계했다. 하지만 2.3.2에서 시사한 바와 같이 CyCOP 가시화 화면들의 의도나 주로 사용하는 데이터의 종류에 따라 조금씩은 UI의 형태가 달라진다. 객체 기호는 美, MIL-STD-2525D [41]의 기준을 준수한다. 객체 크기는 2.3.4에서 시사한 바와 같이 13 pixcel의 크기로 설계 및 구현한다. 이를 기반으로 CyCOP을 구현하는데 사용한 하드웨어 및 소프트웨어 정보는 표 9와 같다.

군사적인 관점에서 IPB 1, 2단계의 경우는 사이버공격에 대한 대비 단계이다. IPB 3, 4단계의 경우는 '정보'와 '작전'의 영역으로 이는 사이버공격에 대한 대응 단계다. 본 연구의 목표는 사이버공격에 대비하는 것이기 때문에 그림 6의 CyCOP 가시화 종류 중 IPB 1, 2단계에 해당하는 ①~⑤까지의 가시화를 설계 및 구현한다. 그림 6의 CyCOP 가시화 ①~⑤까지의 가시화 화면과 가시화에 사용되는 데이터는 그림 7과 같다.

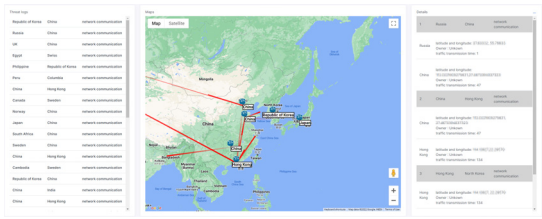


(Figure 6) CyCOP UI Structure

(Table 9) CyCOP Implementation Environment Hardware and Software

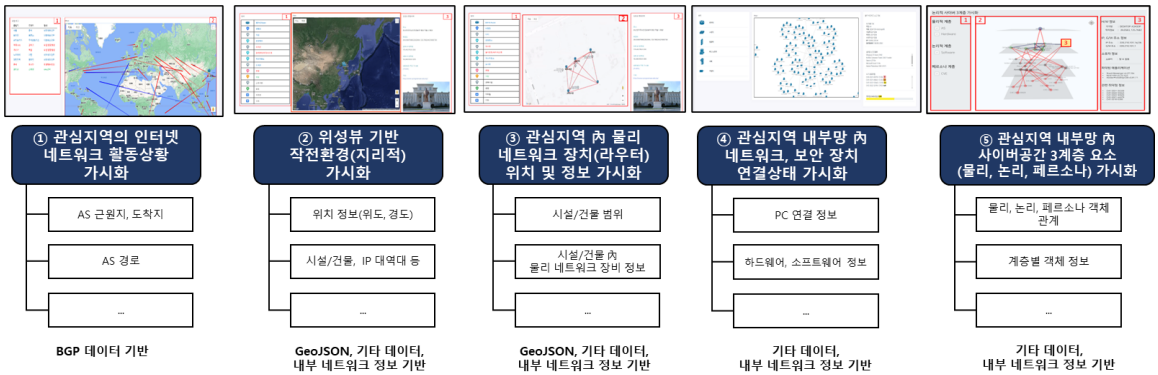
구분	사용 하드웨어 및 소프트웨어
운영체제	Windows 10 Pro
프로세서	AMD Ryzen 7 3700X 8-Core Processor 3.59 GHz
메모리	64GB
사용 언어, 소프트웨어 및 툴	Python 3.9, django 4.1, deck.gl 8.4, Unity 2022.1.13., bootstrap 5.2.0, oracle 21c, Google Maps Platform

①번 가시화는 BGP 데이터에서 AS 근원지, 도착지, 경로 등의 정보를 사용한다. 그림 8과 같이 해당 정보를 가시화와 연결시켜, 관심 지역 내에서의 인터넷 네트워크 활동 상황을 동적으로 볼 수 있다. 좌측 인터페이스에서는 패킷의 출발지와 도착지를 볼 수 있다. 우측 인터페이스에서는 패킷이 특정 지역에서 특정 지역을 경유하여 특정 도착지로 가는지 확인할 수 있다.



(Figure 8) ① Visualization: Visualization of Internet network activity in the area of interest

②번 가시화는 Google Maps [49]와 같은 지도 서비스 API를 사용하여, 위성뷰 기반 지도를 그림 9와 같이 가시화한다. 그 위에 GeoJSON, 기타 데이터, 내부 네트워크 정보



(Figure 7) CyCOP visualization screen and data by visualization

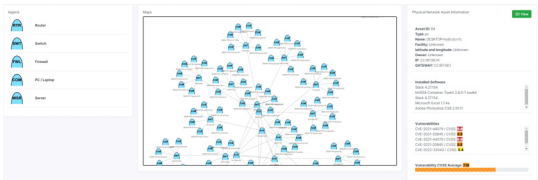
등의 지리적 정보와 위치/시설/건물 등의 정보를 혼합하여 가시화한다. 좌측 인터페이스는 아이콘들의 범례를 표현하고 중앙 인터페이스는 위성뷰 기반 지도를 표현한다.

(Figure 9) ② Visualization: Satellite view-based geographic visualization

③번 가시화는 ②번 가시화에서 특정 시설 등의 물리적 네트워크 현황을 그림 10과 같이 상세히 가시화한다. 물리적 네트워크 자산 중에서 라우터를 중점적으로 가시화하며, 라우터의 정보들과 라우터들이 어떻게 연결되어 있는지 확인한다. 사용되는 데이터로는 GeoJSON, 기타 데이터, 내부 네트워크 정보 등이 있다. 좌측 인터페이스는 아이콘들의 범례를 나타내고, 우측 인터페이스는 중앙 인터페이스에서 선택한 시설의 상세 정보를 표현한다.

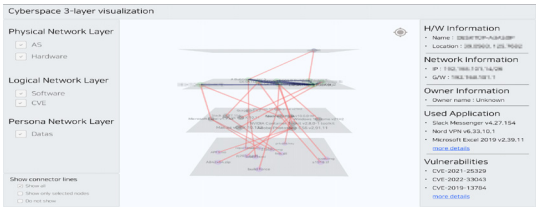
(Figure 10) ③ Visualization: Visualization of physical network device location and information within the facility

④번 가시화는 ③번 가시화에서 선택된 시설 등의 내부 네트워크를 파악하는 가시화다. 정확한 위치를 제대로 파악할 수 없는 PC, Server, Switch, 방화벽 등의 물리적 네트워크 자산들을 논리적 그래프로 가시화하고 이들의 연결관계 등을 그림 11과 같이 파악한다. 좌측 인터페이스는 아이콘들의 범례를 표현하며, 중앙 인터페이스에서는 각 객체들의 연결상태를 표현한다. 우측 인터페이스에서는 물리적 네트워크 자산에 설치되어 있는 S/W, 취약점이나 IP, MAC 주소 등의 정보를 표현한다. 취약점의 경우는 CVSS(common vulnerability scoring system) 점수를 사용하여 나타낸다 [50]. 사용되는 데이터로는 Persona, 기타 데이터, 내부 네트워크 정보 등이 있다.



(Figure 11) ④ Visualization: Visualization of internal network of facilities

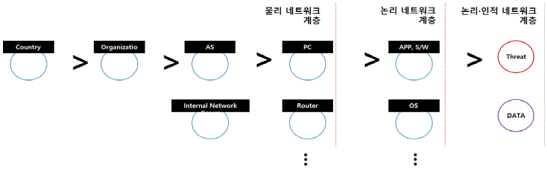
⑤번 가시화는 그림 12와 같이 내부망 네트워크를 사이버공간 3계층으로 표현하여 네트워크 자산 간의 관계를 상세하게 파악하는 가시화이다. 각 계층별 자산들이 어떻게 상호연결성을 가지고 있으며, 다른 계층과는 어떤 관계를 가지고 있는지 파악할 수 있다. 각 계층 간 관계는 그림 13과 같은 기준으로 표시된다. 좌측 인터페이스는 각 계층별 요소를 가시화할지 여부를 선택할 수 있다. 우측 인터페이스는 중앙 인터페이스에 선택한 객체의 하드웨어(H/W) 정보, IP, G/W, 소유자, 사용하는 애플리케이션 및 소프트웨어, 취약점 등을 표현한다.



(Figure 12) ⑤ Visualization: Cyberspace 3-layer visualization

4. CyCOP 응답속도 실험

3장에서 설계한 프레임워크는 2장에서 조사한 UI, 객체 기호, 객체 크기를 준수하여 그림 8-12와 같이 구현되었다. 하지만 응답속도에 대한 것은 그림으로 확인할 수 없기에 실험으로 증명한다. 기준으로 구현한 CyCOP 가시화 화면들에 대한 응답속도를 실험한다.

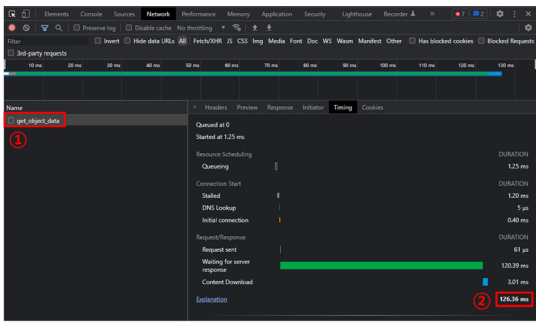


(Figure 13) Diagram of Object Relationships Between Network Layers

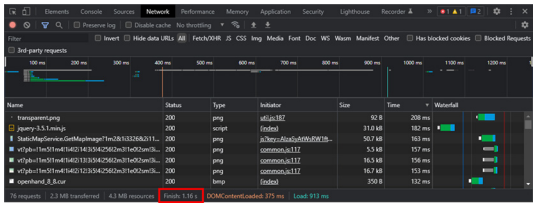
실험 항목은 표 5의 항목에서 추출했다. 단순 응답시간의 항목들은 웹으로 제작된 환경에서는 측정이 어려워 제외하였다. 단, 사람들이 응답속도에 가장 민감하게 반응하는 객체의 상세 정보조회와 화면 출력에 대한 실험인 복잡 응답시간에 해당하는 항목들을 선정했다. 그중 File Update는 본 연구에서 구현한 가시화에 없는 기능이므로 제외했다.

각 가시화 화면에 있는 모든 객체들은 클릭할 때 화면 우측 인터페이스에 객체에 대한 상세 설명이 표시된다. 조회(단순)은 가시화 화면에서 객체를 클릭했을 때부터 우측 인터페이스에서 객체의 상세 설명 나타나기까지의 시간을 측정했다. 이는 그림 14의 1번 사각형과 같이 객체 정보를 서버에 요청한다. 그리고 2번 사각형과 같이 CyCOP 가시화 화면(Client)으로 객체 정보를 받는 시간(응답시간)을 브라우저 개발자도구의 Network 탭에서 측정했다. 조회(복잡)은 여러 외/내부 데이터를 사용하는 가시화 화면을 호출한다. 이를 측정하기 위해 그림 15의 붉은 상자의 시간을 측정했다. 이는 가시화 화면을 출력하기 위한 자산들이 모두 호출되는 데까지 걸리는 시간을 의미한다. 객관적인 평가를 위해 조회(단순)과 조회(복잡)을 측정할 때는 브라우저의 캐시를 모두 지우고 10번씩 호출한 후 그에 대한 평균을 표 10과 같이 도출했다.

표 10의 각 응답시간은 초 단위로 소수점 둘째 자리까지 표기했다. 표 10에서 볼 수 있듯이 모든 가시화 화면들은 표 6의 항목들의 응답속도를 모두 준수했다. 조회(단순)은 모든 가시화들이 약 0.1초 정도로 빠른 응답속도를 보였다. 조회(복잡)의 경우는 ④번 가시화가 가장 빠른 응답속도를 보였으며, ①번 가시화가 가장 느린 응답속도를 보였다. 이는 ④번 가시화는 리소스가 큰 이미지를 호출하지 않았기 때문에, 가장 빠른 속도를 보인 것이다. ①번 가시화의 경우는 여러 패킷에 대한 정보 호출과 Google Map API를 최초로 호출하는 화면이기 때문에, 가장 느린 속도를 보였다.



(Figure 14) Measure query (simple) response time in browser developer tools network tab



(Figure 15) Measure query (complex) response time in browser developer tools network tab

(Table 10) Response time for each CyCOP visualizations

시스템 설명	①	②	③	④	⑤
조회(단순)	0.12	0.11	0.11	0.10	0.14
조회(복잡)	1.50	0.94	0.92	0.63	1.38

5. 결 론

본 연구의 목적은 사이버공간 내 상황인식을 위한 CyCOP 프레임워크를 설계 및 구현하는 것이다. JP 3-12 기반으로 작성한 JCOPP와 ATP 2-01.3 IPB 문서를 분석하여 CyCOP에서 가시화 해야되는 화면들을 식별했다. 그리고 CyCOP을 설계 및 구현하기 위한 인터페이스(응답시간, UI, 객체 기호, 객체 크기) 관련 연구들을 조사를 했다. 조사한 사항들을 바탕으로 CyCOP 프레임워크를 설계하고 구현한 각 가시화 화면들에 대한 설명을 작성했다. 마지막으로 가시화 화면들의 응답시간을 측정하여 구현된 CyCOP이 조회(단순), 조회(복잡) 기준에 충분히 부합하는 것을 증명했다.

본 연구에서 제안한 CyCOP 프레임워크를 적용하여 CyCOP을 개발한다면, 보안 담당자들과 군의 지휘관들은 사이버공격에 대비할 수 있는 능력을 갖출 수 있을 것이다. 향후 연구에서는 ATP 2-01.3 IPB 단계 중 3, 4단계에 해당하는 가시화 ⑥~⑩까지 구현할 것이다. 그에 따라 CyCOP의 최종 모습은 사이버공격에 대비뿐만이 아닌 대응까지 할 수 있는 능력을 가질 것이다.

참고문헌(Reference)

[1] R. Adlakha, S. Sharma, A. Rawat and K. Sharma, "Cyber Security Goal's, Issue's, Categorization & Data Breaches," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing

(COMITCon), pp. 397-402, 2019.
http://dx.doi.org/10.1109/COMITCon.2019.8862245.

[2] K. Cabaj, Z. Kotulski, B. Księżopolski et al., "Cybersecurity: trends, issues, and challenges," EURASIP Journal on Information Security, pp. 1-3, 2018.

[3] S. dageet, "Quadrennial defense review report," Department of Defense., Virginia, USA, Feb. 2010.

[4] The Joint Staff, "Joint Publication (JP) 3-12, Cyberspace Operation," Washington, DC, USA, June 2018.

[5] O. Zaporozhets and O. Syvak, "In the Line of Russian Aggression: Ukraine, hybrid warfare, and cybersecurity defense," Routledge Companion to Global Cyber-Security Strategy, Thames, Oxfordshire, England, UK: Routledge, pp. 185-190, 2021.

[6] O. Analytica, "Ukraine-linked cyber threats remain serious," Emerald Expert Briefings oxan-es, April. 2022, http://dx.doi.org/10.1108/OXAN-ES268913.

[7] M. Husák, M. Laštovička, and T. Plesník, "Handling Internet Activism during the Russian Invasion of Ukraine: A Campus Network Perspective," Digital Threats: Research and Practice, April. 2022. http://dx.doi.org/10.1145/3534566.

[8] "Cyber Attack Trends In The Midst Of Warfare – The numbers behind the first days of the conflict," Check Point Software Technologies Ltd., Israel, Feb. 2022. [Online]. Available: https://blog.checkpoint.com/2022/02/27/196-increase-in-cyber-attacks-on-ukraines-government-and-military-sector/

[9] P. D. Gallagher, et al. "Guide for Conducting Risk Assessments," NIST Special Publication 800-30, Washington, DC, September 2012.

[10] Department of the army, "FM 3-12 Cyberspace and Electromagnetic Warfare," Washington, DC, USA, August 2021.

[11] Ducheine Paul and Jelle Van Haaster, "Fighting Power Targeting and Cyber Operations," Cyber Conflict (CyCon 2014)2014 6th International Conference, pp. 303-327, 2014.
https://doi.org/10.1109/CYCON.2014.6916410

[12] P. W. Poteete, "Implementing the DoD joint operation planning process for private industry enterprise security," NAVAL POSTGRADUATE SCHOOL MONTEREY CA DEPT OF INFORMATION SCIENCES, Sep. 2011. https://calhoun.nps.edu/handle/10945/5518

[13] A. Munir, A. Aved, and E. Blasch, "Situational Awareness: Techniques, Challenges, and Prospects," AI, vol. 3, no. 1, pp. 55–77, Jan. 2022. http://dx.doi.org/10.3390/ai3010005.

[14] Mica R Endsley, "Toward a theory of situation awareness in dynamic systems", Human factors, vol. 37, no. 1, pp. 32-64, 1995.
https://doi.org/10.1518/001872095779049543

[15] M. R. Endsley, "Design and evaluation for situation awareness enhancement," Proc. Human Factors Ergonom. Soc. Annu. Meeting, vol. 32, no. 2, pp. 97-101, 1988.
https://doi.org/10.1177/154193128803200221

[16] P. Barford et al., "Cyber SA: Situational Awareness for Cyber Defense," in Cyber Situational Awareness. Advances in Information Security, Boston, MA, USA:Springer, vol. 46, pp. 3-4, 2010.

[17] U. Franke and J. Brynielsson, "Cyber situational awareness—A systematic review of the literature," Comput. Secur., vol. 46, pp. 18-31, Oct. 2014.

[18] O. Jacq, D. Brosset, Y. Kermarrec and J. Simonin, "Cyber attacks real time detection: towards a Cyber Situational Awareness for naval systems," 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), pp. 1-2, 2019.
http://dx.doi.org/10.1109/CyberSA.2019.8899351.

[19] R. Mittu and F. Segaria, "Common operational picture (COP) and common tactical picture (CTP) management via a consistent networked information stream," Proc. Command Control Res. Technol. Symp., pp. 3-7, 2000.

[20] Daniel T. Keuhlen, Oliver L. Bryant, and Kenneth K. Young, "The common operational picture in joint vision 2020: a less layered cake", NATIONAL DEFENSE UNIV NORFOLK VA JOINT AND COMBINED WARFIGHTING SCHOOL, 2002.
https://apps.dtic.mil/sti/citations/ADA421610

[21] Dr David. Baar, and Garth. Shoemaker, "Pliable Display Technology for the Common Operational Picture," IDELIX Software Inc, 2004.

[22] J. Copeland, Emergency response: Unity of effort through a common operational picture, U.S. Army War College, Carlisle, PA, Strategy Research Project, Mar 2008.

[23] Erin E. Wreski, and Erik A. Lavoie, "A concept of operations for an unclassified common operational picture in support of maritime domain awareness," Naval Postgraduate School Monterey United States, 2017.

[24] R. Mittu, and F. Segaria, "Common operational picture (cop) and common tactical picture (ctp) management via a consistent networked information stream (cnis)," NAVAL RESEARCH LAB, Washington, DC, USA, 2000.

[25] M. Esteve at el., "Cyber Common Operational Picture: A Tool for Cyber Hybrid Situational Awareness Improvement," North Atlantic Treaty Organization (NATO) Science and Technology Organization (STO), Technical Report STO-MP-IST-148, Washington, DC, USA, 2016.

[26] T. Pahi, et al. "Preparation, Modelling, and Visualisation of Cyber Common Operating Pictures for National Cyber Security Centres," Journal of Information Warfare, vol. 16, no. 4, pp. 26 – 40, 2017.

[27] S. Noel, S. Purdy, A. O'Rourke, et al. "Graph analytics and visualization for cyber situational understanding," The Journal of Defense Modeling and Simulation, Oct. 2021. http://dx.doi.org/10.1177/15485129211051385.

[28] R. S. Gutzwiller, S. M. Hunt and D. S. Lange, "A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts," 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), pp. 14-20, 2016. http://dx.doi.org/10.1109/COGSIMA.2016.7497780.

[29] S. Jajodia, S. Noel, P. Kalapa, M. Albanese and J. Williams, "Cauldron mission-centric cyber situational awareness with defense in depth," 2011 - MILCOM 2011 Military Communications Conference, 2011, pp. 1339-1344, 2011. http://dx.doi.org/10.1109/MILCOM.2011.6127490.

[30] M. Jenkins, M. G. Catto and M. Les Bird, "Increased Space Situational Awareness through Augmented Reality Enhanced Common Operating Pictures", The Advanced Maui Optical and Space Surveillance Technologies Conference, 2018.

[31] S. Llopis et al., "A comparative analysis of visualisation techniques to achieve cyber situational awareness in the military," 2018 International Conference on Military Communications and Information Systems (ICMCIS), pp. 1-7, 2018. http://dx.doi.org/10.1109/ICMCIS.2018.8398693.

[32] L. Jiang, A. Jayatilaka, M. Nasim, M. Grobler, M. Zahedi and M. A. Babar, "Systematic Literature Review on Cyber Situational Awareness Visualizations," in IEEE Access, vol. 10, pp. 57525-57554, 2022. http://dx.doi.org/10.1109/ACCESS.2022.3178195.

[33] H. Doucette, "Identifying Requirements for a Cyber Common Operating Picture (CyCOP): Information Collection," Defence Research and Development Canada, Ottawa, Canada, March 2020.

[34] C. Dillabaugh et al., "CyberCOP: Cyber Situational Awareness Demonstration Tool," Defence Research and Development Canada, Ottawa, Canada, Feb. 2020.

[35] L. Beaudoin et al., "Coalition Network Defence Common Operational Picture," FRAUNHOFER SOCIETY WACHTBERG (GERMANY) FRAUNHOFER INST FOR COMMUNICATION INFORMATION PROCESSING AND ERGONOMICS, Wachtberg, Germany, Nov. 2010.

[36] Headquarters, Department of the Army, "Army Techniques Publication (ATP) 2-01.3, Intelligence Preparation of the Battlefield," Washington, DC, USA, Jan. 2021.

[37] Department of Defense, United States of America, "Military-Standard (MIL-STD)-1472H, DESIGN CRITERIA STANDARD, HUMAN ENGINEERING," Washington, DC, USA, Jan. 2019.

[38] Kim. H, H. Song, and S. Park, "Proper response times and design factors influencing user satisfaction with diverse touch tap operations for the smartphone," Archives of Design Research, vol.27, no.2, pp.95-105, 2014. https://doi.org/10.15187/adr.2014.05.110.2.95

[39] B. Shneiderman, "Response time and display rate in human performance with computers," ACM Computing Surveys (CSUR), vol. 16, no. 3, pp. 265 – 285, 1984.

[40] E. D. McCroskey and C. A. Mock, "Operational Graphics for Cyberspace", Joint Force Quarterly(JFQ), Issue 85, 2nd Quarter, pp.42-49, 2017.
[41] Department of Defense, United States of America, "Military-Standard (MIL-STD)-2525D, INTERFACE STANDARD, JOINT MILITARY SYMBOLOGY," Washington, DC, USA, Nov. 2008.
[42] University of Oregon Route Views Archive Project, 2022. http://archive.routeviews.org/
[43] H. Butler, M. Daly, A. Doyle, S. Gillies, S. Hagen and T. Schaub, The GeoJSON Format, 2016.
[44] Maxmind, 2022. https://www.maxmind.com/en/home
[45] Caida, 2022. https://www.caida.org/
[46] SecurityTrails, 2022. https://securitytrails.com/
[47] ip-api, 2022. https://ip-api.com/
[48] WhoisXMLAPI, 2022. https://www.whoisxmlapi.com/
[49] Google Maps, 2022. https://www.google.com/maps
[50] K. Scarfone and P. Mell, "An analysis of CVSS version 2 vulnerability scoring," 2009 3rd International Symposium on Empirical Software Engineering and Measurement, pp. 516-525, 2009. http://dx.doi.org/10.1109/ESEM.2009.5314220

◐ 저 자 소 개 ◑

김 국 진(Kook-jin Kim)
2017년 서울호서전문학교 정보보호학과(학사)
2019년 (주)엠투소프트 전자문서사업부 주임
2019년~현재 세종대학교 대학원 컴퓨터공학과(석박사통합과정)
관심분야 : 사이버전, 사이버 지휘통제, 정보보호, 인공지능, etc.
E-mail : kjkim@sju.ac.kr

윤 재 필(Jae-pil Youn)
2008년 육군3사관학교 전산정보처리학(학사)
2017년 아주대학교 정보통신대학원 사이버보안전공(석사)
2019년~현재 세종대학교 대학원 컴퓨터공학과(박사과정)
2021년~현재 육군사이버작전센터 사이버작전연습장교
관심분야 : 국방정보시스템, 사이버보안, etc.
E-mail : jpyoun@sju.ac.kr

윤 석 준(Suk-joon Yoon)
1980년 공군사관학교 항공공학과(학사)
1991년 국방대학교 무기체계공학(석사)
1996년 독일지휘관참모대학 군사학(석사)
2016년 합동군사대 교리부 연구교수
2020년~현재 세종대학교 사이버전연구소 교수
관심분야 : 사이버전, 사이버보안, 사이버 지휘통제, 사이버작전, etc.
E-mail : ysjoony@sejong.ac.kr

◐ 저 자 소 개 ◑

강 지 원(Ji-won Kang)
1988년 금오공과대학교 전자공학과(학사)
1997년 연세대학교 대학원 컴퓨터과학과(석사)
2012년 경기대학교 대학원 정보보호학과(박사)
2017년~현재 세종대학교 컴퓨터공학과 교수
관심분야 : 사이버전, 사이버보안, 사이버 지휘통제, 사이버작전, etc.
E-mail : jwkang@sejong.ac.kr

김 경 신(Kyung-shin Kim)
1986년 금오공과대학교 전자공학과(학사)
1993년 연세대학교 대학원 전자공학과(석사)
2007년 경희대학교 대학원 컴퓨터공학과(박사)
2019년~현재 국방과학연구소 국방첨단기술연구원 융복합기술부 수석연구원
관심분야 : 머신러닝, 멀웨어 탐지, 사이버보안, etc.
E-mail : updatekim@add.re.kr

신 동 규(Dong-kyoo Shin)
1986년 서울대학교 컴퓨터과학과(학사)
1992년 Illinois Institute of Technology 대학원 컴퓨터과학과(석사)
1997년 Texas A&M University 대학원 컴퓨터과학과(박사)
1998년~현재 세종대학교 컴퓨터공학과 교수
관심분야 : 사이버전, 사이버보안, 사이버 지휘통제, 인공지능, 정보보호, etc.
E-mail : shindk@sejong.ac.kr