석사학위논문

사이버 공격이 군사작전에 미치는 영향 분석을 위한 시뮬레이션 모델 개발

2014년

한성대학교 국방과학대학원

국방M&S학과

국방M&S학전공

신 동 호

석 사 학 위 논 문
지도교수 김종만

사이버 공격이 군사작전에 미치는 영향 분석을 위한 시뮬레이션 모델 개발

The development of a simulation model for analyzing the impact of cyber attacks on military operations

2013년 12월 일

한성대학교 국방과학대학원
국방M&S학과
국방M&S학전공
신 동 호

석 사 학 위 논 문
지도교수 김종만

사이버 공격이 군사작전에 미치는 영향 분석을 위한 시뮬레이션 모델 개발

The development of a simulation model for analyzing the impact of cyber attacks on military operations

위 논문을 국방M&S학 석사학위 논문으로 제출함

2013년 12월 일

한성대학교 국방과학대학원
국 방 M & S 학 과
국방M&S학전공
신 동 호

신동호의 국방M&S학 석사학위논문을 인준함

2013년 12월 일

심사위원장 _____ 인

심 사 위 원 _____ 인

심 사 위 원 _____ 인

국 문 초 록

사이버 공격이 군사작전에 미치는 영향 분석을 위한 시뮬레이션 모델 개발

한성대학교 국방과학대학원
국방 M&S 학과
국방 M&S학 전공
신 동 호

컴퓨터와 정보기술이 전장 환경에 융합된 현대 국방 네트워크 중심전 환경에서는 사이버 공격에 의한 IT 시스템의 피해 손실은 군사 작전의 성공 여부에 큰 영향을 준다. 적군에 의한 사이버 공격 하에서 군사 작전 성공 여부를 과학적으로 판단하기 위해서는 네트워크 중심전 기반기술인 C4ISR+PGM (Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance+Precision Guided Munitions) 체계를 구성하는 컴퓨터 시스템 및 네트워크의 손실 또는 성능 저하로 인한 군사정보의 유출, 변조, 전달 지연이 얼마나 아군 군사 능력에 영향을 주는지를 이해해야 한다.

본 논문에서는 사이버 공격이 군사작전에 미치는 영향을 분석하기 위한 모델 개발에 필요한 체계화된 모델링 절차 및 요구사항을 정립하고 상용 시뮬레이션 소프트웨어를 이용하여 사이버 공격 영향 평가 모델을 구현하였다.

사이버 공격 영향 평가 모델은 타격순환체계를 통한 시한성 긴급 표적 처리 과정을 시뮬레이션하는 군사작전 프로세스 모델, C4ISR 체계를 구성하는 IT 시스템의 성능을 시뮬레이션하는 표준 IT 시스템 프로세스 모델 및 사이버 공격 모델이 상호작용을 하도록 설계되어, 모델 사용자는 정의된 범주의

사이버 공격으로 인한 IT 시스템의 성능 저하 및 중단이 전체 군사 작전에 미치는 효과도를 과학적으로 분석 할 수 있다.

모델 설계 방법론은 UML에 기반한 4+1 뷰모델을 적용하여 제안된 모델에 대한 이해와 구현을 명확하게 하였다. Use Case 다이어그램, 절차 다이어그램 및 클래스 다이어그램을 통하여 사용자의 요구조건에 따른 모델 객체와 객체 간의 상호작용, 모델링 환경에서 시스템의 동작을 이해하기 위한 메시지 순서 및 시스템 구조를 나타내는 시스템 변수를 표현하였다.

모델 구현은 개발의 편의성, 모델링 요구사항에 따른 적합성, 모델 데이터 관리를 위한 데이터베이스 설계 지원을 고려하여 이산사건 시뮬레이션을 지원하는 상용 소프트웨어를 이용하여 구현하였다. 구현된 모델은 개별 블록으로 구성되어 모델의 수정과 기능 업그레이드가 용이하고 계층 모델 표현을 통하여 모델 사용자에게 편의성을 제공하였다.

사이버 영향 평가 모델을 이용한 시뮬레이션 결과 분석을 통해서는 사이버 공격이 군사작전의 결과에 어떻게 영향을 주는지를 검증하고 개발된 모델의 활용 방안을 제시하였다.

【주요어】 사이버공격, 군사작전, 4+1 뷰모델, 모델링, 시뮬레이션

목 차

【 표 목 차 】

【 그 림 목 차 】

제 1 장 서 론

컴퓨터와 정보기술(IT: Information Technology)이 전장 환경에 융합된 현대 국방 네트워크 중심전(NCW: Network Centric Warfare) 환경에서는 사이버 공격에 의한 IT 시스템의 피해 손실은 군사 작전의 성공여부에 큰 영향을 준다. 따라서, 적군에 의한 사이버 공격 하에서 군사 작전 성공 여부를 과학적으로 판단하기 위해서는 NCW 기반기술인 C4ISR+PGM(Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance +Precision Guided Munitions) 체계를 구성하는 컴퓨터 시스템 및 네트워크의 손실 또는 성능 저하로 인한 군사정보의 유출, 변조, 전달 지연이 얼마나 아군 군사 능력에 영향을 주는지를 이해해야 한다. 그러나, 현재까지 사이버 공격에 의한 작전 효과도 측정 연구는 초기 단계로 사이버 공격과 군사작전의 관계를 효과적으로 분석할 수 있는 방법과 모델을 제시 하지 못하고 있다. 본 논문에서는 이러한 제한사항을 해결하기 위한 군사작전과 연계한 사이버 공격에 대한 모델링 방법론을 제안하고 시뮬레이션을 통해 사이버전 (Cyber Warfare) 상황인식에 대한 분석을 실시하였다.

제 1 절 연구의 배경 및 목적

현대의 진보된 정보기술이 국방 분야에 융합되어 전장 환경은 NCW로 변화하고 있다. NCW는 전투원과 군 전투세력의 행동에 관한 것이며, 정보시대의 네트워크 중심적인 사고방식을 군 작전 및 전투 분야에 적용하여 그 효율성을 극대화한 전투 양상이라 할 수 있다. 또한 NCW는 지리적으로 분산된 세력을 통합 운용하고 지식능력을 보유하며, 전투공간의 구성요소 간 효과적인 연결을 통해 정보공유를 극대화시켜 주는 개념이라 할 수 있다. NCW의 목적은 C4ISR 네트워크를 통해 센서와 전투원간의 통합적인 연결성을 구현하여 전투공간 내의 모든 전투원들에게 정보공유 능력을 제공하고, 전투공간에 대한 공통의 상황인식과 자기 동기화, 즉 독립적인 의사결정 능력을 제공함으로써

군사작전에서 정보우위가 가능함은 물론, 전투력의 상승효과를 유발하기 위한 것이다.[1)]

현대전 환경인 NCW에서는 군사작전 시 컴퓨터 시스템과 네트워크의 활용도 및 의존도가 과거의 개별 플랫폼(Platform) 기반의 작전 환경보다 절대적이다. 이에 따라 사이버 공격으로 인한 컴퓨터 시스템 및 네트워크의 피해는 군사작전 성공 여부에 영향을 미치는 중요한 요소이다.

사이버 공격은 군사적 우위를 위한 비대칭 전략의 중요한 수단으로 활용되고 있으며, 사이버 공격의 주 대상은 C4ISR+PGM 체계이다. C4ISR+PGM 체계 자체가 표적이 될 수 있으며, 구성하고 있는 네트워크와 시스템 자원, 그 속에서 소통되는 군사정보 및 데이터가 주요 표적이 된다. 또한, 국방정보통신체계와 연결되어 있는 국가 기간망도 사이버 공격 표적이 될 수 있다.[2)] 따라서, 컴퓨터 시스템과 네트워크의 활용을 전제로 하는 NCW 환경에서 사이버 공격이 군사작전에 미치는 영향을 정확하게 이해하기 위해서는, 군사작전을 지원하는 IT 시스템과 군사임무를 관련지어 모델을 개발 분석하여야 한다.

기존의 군사작전 분석모델은 사이버 공격의 영향을 전혀 고려하지 않고 모델을 개발하여 시뮬레이션을 하거나, 네트워크 시뮬레이터의 결과를 데이터베이스화하여 모델의 입력 요소로 활용하는 수준이었다. 최근에는 분산 시뮬레이션 환경 하에서 전투 모델과 네트워크 시뮬레이션 모델을 상호 연동하여 분석하려는 연구가 진행되고 있으나, 현재의 연동기술은 사이버 환경에 대한 특성을 충분히 고려하지 않고 개발되어 사이버 도메인에서 일어나는 활동 및 결과에 대한 연동 지원이 제한적이며, 모델 개발 요구 조건과 모델링 충실도(Fidelity) 차이로 상호 연동이 어려워 사이버 공격의 효과를 반영한 현실적인 결과를 얻기가 어려웠다.

본 논문에서는 사이버 공격이 증가하는 현대전의 상황에서 군사작전 성공을 위한 사이버 상황인식(Situation Awareness) 연구에 활용될 수 있도록 군사작전 효과 척도에 영향을 주는 IT 시스템을 식별하고, 해당 IT 시스템의 가용성과 군사작전 효과도 관계를 시뮬레이션을 통해 분석할 수 있는 이산사건(Discrete-Event) 모델링 개발 방법론을 정립하고 제안한다.

---

1) 윤희병, 『NCW서비스와 기술』, 서울 : 홍릉과학출판사, 2012. p.6
2) 엄정호외 2명, 『사이버전개론』, 서울 : 홍릉과학출판사, 2012, p.4

제 2 절 연구 범위 및 구성

기존의 방법론으로는 컴퓨터와 IT 시스템 활용이 군사작전 과정에 통합된 NCW 환경 하에서 군사작전이 진행될 때 사이버 공격이 군사작전에 미치는 영향을 분석하기가 어렵다. 예를 들면, 시한성 긴급표적(TST: Time Sensitive Target) 처리를 위한 군사 작전이 진행 중일 때, 부대 IT 관리자는 사이버 공격에 의해 데이터베이스 서버의 일부 타격 정보가 변조되어 저장되었음을 발견하였고, 전술 데이터 체계를 구성하는 네트워크 라우터에 대한 DoS(Denial of Service) 공격으로 시한성 긴급표적(TST)의 위치 정보 전달이 지연된다면 작전사령관은 제한된 정보를 바탕으로 작전을 진행하거나 중단할지를 판단해야 한다.

본 논문에서는 적의 사이버 공격이 성공하여 진행 중임을 가정하고 사이버 공격이 군사작전에 미치는 영향을 분석할 수 있는 시뮬레이션 모델을 〈그림 1-1〉과 같은 과정을 통해 개발하였다.

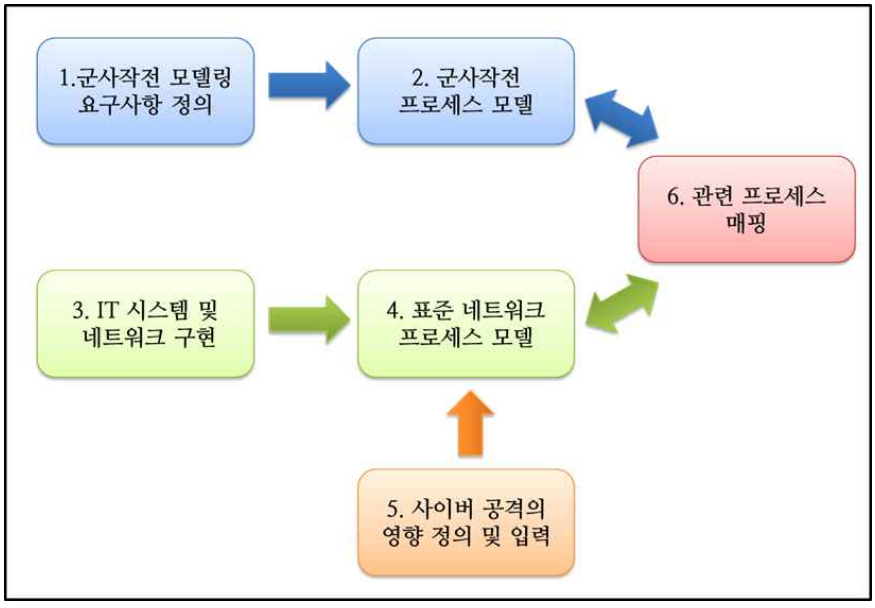
첫 번째, 모델 개발 방법론에 대한 사전연구를 통하여 군사 작전의 모델링 절차 및 요구사항을 정의하고, 군사작전 시나리오에 따른 프로세스 모델(Process model)을 구현한다.

두 번째, IT 시스템 및 네트워크를 기능 및 규모에 따라 미리 정의된 표준 네트워크 프로세스 모델을 개발한다.

세 번째, 사이버 공격으로 인한 IT 시스템 및 네트워크에 대한 영향을 정의하고 이산사건 모델링 방법론을 기반으로 사이버 공격에 대한 모델을 구현한다.

네 번째, IT 시스템과 군사작전의 연관성에 따라 군사작전 프로세스 모델과 네트워크 프로세스 모델을 매핑(Mapping)하여 최종 사이버 영향 평가 모델을 개발한다.

본 논문에서 제시한 사이버 영향 평가 모델을 구성하는 군사 작전에 대한 프로세스 모델링은 군사 시나리오에 대한 전체적인 효과도 분석을 위하여 국방 M&S(Modeling and Simulation) 계층 구조의 전구급 및 임무급 모델 수준에서 이루어지며, 사이버공격의 효과도 분석을 위한 IT 시스템의 모델링은 시스템 성능을 반영한 교전급 및 공학급 모델의 해상도 수준에서 구현한다.



〈그림 1-1〉 본 논문의 모델링 접근 방법

본 연구의 논문은 구성은 다음과 같다.

1장은 서론으로 연구의 배경 및 목적, 연구 범위와 구성에 대하여 기술하였다.

2장에서는 사이버 영향 평가 모델 개발의 이론적 배경으로 사이버전에 대한 개념 및 사이버 공격 영향 평가 방법론, 시뮬레이션 모델링 및 기존 사이버 공격 모델링 관련 연구에 대하여 설명하였다.

3장에서는 모델 개발을 위한 모델링 일반 사항으로 모델 개발 절차, 시뮬레이션 시나리오 및 모델링 요구조건에 대하여 기술하고, 모델 구조 표현을 위한 UML(Unified Modeling Language)과 4+1 뷰모델(View Model)을 설명하고 모델 구조(Architecture)를 Use Case 다이어그램, 절차(Sequence) 다이어그램 및 클래스(Class) 다이어그램을 통해 설계하였다.

4장에서는 이산모델링 및 시뮬레이션 환경을 제공하는 ExtendSim 소프트웨어에 대한 개요와 모듈을 설명하고, 본 논문에서 제안한 사이버 공격 영향 평가 모델(Cyber attack Impact Assessment Model)을 구현 검증하고 시뮬레이션 결과를 분석하였다.

5장에서는 본 논문의 활용 방안을 제시하고 결론을 맺었다.

제 2 장 이론적 배경

제 1 절 사이버전 (Cyber Warfare)

과거의 전통적인 전쟁이 실제 무기체계를 이용하여 현실세계에서 일어난다면, 사이버전은 인터넷을 비롯한 사이버 공간에서 일어나는 전쟁을 말한다. 즉, 사이버 전은 컴퓨터 네트워크를 통해 디지털화된 정보가 유통되는 가상적인 공간에서 다양한 사이버 공격수단을 사용하여 적의 정보 체계를 교란, 거부, 통제 및 파괴하는 등의 공격과 이를 방어하는 활동으로 정의 할 수 있다.[3)]

군사작전에서 정보전(Information Warfare)이 가치가 있는 모든 정보를 획득 방어하기 위한 모든 공격 및 방어에 관련된 군사작전을 포함한다면, 사이버전은 정보전이 사이버환경에서 수행되는 걸로 이해 할 수 있다.

사이버전을 명확히 정의하기 위해 중요한 세 가지의 개념을 정리하면 다음과 같다.

첫 번째, 사이버전에서 활동의 핵심은 정보이다.

두 번째, 사이버전의 목적은 아군의 무기체계를 보호하면서 적군의 물리적 무기체계 능력에 영향을 주는 것이다.

세 번째, 성공적인 사이버 공격이 의사 결정에 미치는 영향을 과학적으로 분석하여 이해하는 것은 중요하다.[4)]

1. 사이버 공간 (Cyber Space)

사이버전의 배경인 사이버공간(Cyber Space)은 네트워크로 연결된 시스템 및 물리적 기반시설(Infrastructure)을 통해 데이터가 저장, 수정 및 교류되는 개념적인 환경으로 정의된다. 사이버공간은 컴퓨터, 컴퓨터 시스템, 네트워크 및 해당 컴퓨터 프로그램, 컴퓨터 자료, 자료내용, 트래픽 자료 및 이용자에 의해 생성되고, 구성되어진 물리적인 영역과 비물리적 영역을 모두 포함한다.

---

3) 이태규, 『군사용어사전』, 서울 : 일월서각, 2012

4) Larry W. Fortson, 「Towards the Development of a Deffensive Cyber Damage and Mission Impact Methodology」, Ohio, Air Force IOT, 2007

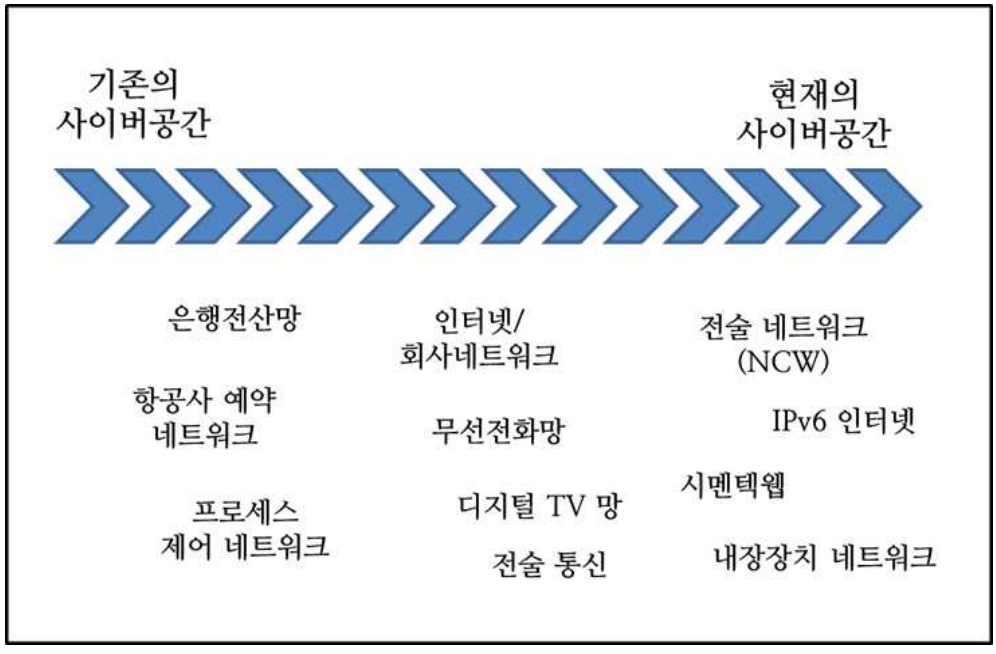
사이버 공간은 [표 2-1]과 같이 상호 의존적인 3개의 계층으로 구분할 수 있다.

첫 번째, 인간 계층으로 컴퓨터 및 컴퓨터 통신을 사용하는 사용자로 구성된다.

두 번째, 논리적 계층으로 정보, 사이버공간의 자산, 악성코드(Malware) 등을 나타내는 소프트웨어 및 비트(bits)로 구성된다.

세 번째, 물리적 계층으로 하드웨어, 이동통신 기반시설, 고정 기반시설 등 네트워크 컴포넌트로 구성된다.

사이버 공간의 개념은 〈그림2-1〉과 같이 사이버 관련 기술의 발전에 따라 기존의 일반적인 네트워크에서 전술 네트워크(Tactical Network)와 같은 새로운 IT기술과 개념을 포함하여 진화하고 있다.



〈그림 2-1〉 사이버 공간 개념의 발전[5)]

5) Chris Scott, 「Cyber Warfare: A Perspective on Cyber Threats and Technology in the Network-Centric Warfare Battlespace」, MIT, 2008

[표 2-1] 사이버 공간 계층 구조[6)]

계층	활동의 형태와 목적	내용 (예시)	현재의 경향 (예시)
인간 계층			
사용자	컴퓨터 시스템에 대한 인간의 사용	독서, 무역, 투자에 관한 정보, 정보의 교환, 친구와의 연락을 유지, 시민, 정부 기관 담당자 사이의 연락, 범죄, 사이버 전쟁	사용자 커뮤니티 현상의 증가(WEB2)와 이동통신 및 통합장치(스마트폰)의 사용, 정교한 인터넷 이용의 시작(WEB3)
논리적 계층: 소프트웨어적 활동			
Graphic User Interface (GUI)	사용자 언어로부터 컴퓨터 언어로의 번역 (디지털 정보) 및 그 반대의 번역	문자, 사진 비디오, 오디오, 버튼의 페이지	인터페이스에서 표현되는 응용 프로그램의 유형 증가, 그래픽 표현, 3D의 전환
어플리케이션 소프트웨어	사용자 인터페이스, 네트워크 관리 소프트웨어로부터의 처리	프로그래밍 언어 (알고리즘)에서의 설명 및 순서도	어플리케이션 증가, 하드웨어와 사용자 인터페이스간의 소프트웨어 계층 증가
시스템 운영체계	소프트웨어 실행 및 컴퓨터 언어에서 기계어로의 변환	관련 계층과 관련 있는 프로그래밍 언어 정보	
물리적 계층			
하드웨어	기계적 작업을 하는 전자 물리 기반체계	전자칩, 전자카드 등, 전기적 충격	전자 부품에 대한 정보, 소형화, 이동성, 플래시 메모리 증가
통신 및 에너지 시스템 (전자 기반 체계)	전자분야의 전산화에 대한 존재와 활동을 위한 조건을 제공	케이블, RF 신호 및 조명 및 전자파 등 기반체계 및 유지	통신 시스템의 확장 및 성장
하드웨어 및 소프트웨어 캐리어	사이버 공간 유지를 위한 추가 조건 제공		스마트폰 휴대의 증가, 컴퓨터 내장 설치, 통합된 프로세서. 사이버 공간과 현실 세계를 연결

6) Shmuel Even, David Siman-Tov, 『Cyber Warfare: Concepts and Strategic Trends』, Institure for National Security Studies, 2012

2. 사이버 공격 (Cyber Attack)

사이버 공격은 컴퓨터와 네트워크를 기반으로 시스템과 전자장비 등으로 구성된 사이버 공간에서 악성코드, 웜, 바이러스, 논리폭탄[7], EMP (Electromagnetic Pulse Effect: 전자기펄스효과) 폭탄 등의 사이버 무기체계를 이용하여 공격대상 시스템을 마비, 파괴하거나 저장된 정보를 변경, 유출 등의 사고를 유발하는 행위를 말한다.[8] 현대전장 환경에서 사이버 공격에 대한 이해는 군사작전을 성공적으로 수행하기 위한 필수 조건이다.

사이버 공간에서 이루어지는 사이버 공격의 방어가 어려운 이유를 분석해 보면 다음과 같다.

첫 번째, 사이버 공간은 인터넷 및 내부 LAN을 포함한 대부분의 네트워크에서 쉽게 접근이 가능하므로, 사이버 공격에 대한 추적이 어렵다.

두 번째, 적대국 및 해킹그룹에 대한 능력 파악이 이루어지지 않아, 이에 대한 대비 부족으로 사이버 공격 억제력이 낮은 수준이다.

세 번째, 사이버 보안은 특정한 제품으로 해결되는 것이 아니라, 보안 규정과 같은 절차 (process)에 의해 영향을 받는다.[9] 그러나, 국내 사이버 환경은 대부분 민간 관리 하에 있어, 국가적인 사이버 절차 정립 및 적용이 어렵다.

네 번째, 사이버 공격은 비대칭 전략의 일종이다. 방어적 측면에서는 다양한 가능성에 대비해야 하지만, 공격자는 한가지의 취약점만 파악하면 공격이 가능해진다.

다섯 번째, 사이버 공격을 위한 도구 및 기술은 비약적으로 발전하고 있으며, 인터넷 등으로 빠르게 전파된다.

여섯 번째, 기존의 무기체계는 네트워크로 연결되는 현대 전장 환경을 고려하지 않고 설계 제작되어 사이버 공격에 대한 대비가 없다.

일곱 번째, 사이버 공격을 위해서는 많은 비용이 들지 않는다. 기존 무기체계는 개발과 운영에 많은 비용과 시간이 소요되지만 사이버 공격을 위해서는 최소한의 비용으로도 국가적 큰 피해를 줄 수 있는 공격이 가능하다.

---

7) 보통의 프로그램에 오류를 발생시키는 프로그램 루틴을 무단으로 삽입하여, 특정한 조건의 발생이나 특정한 데이터의 입력을 기폭제로 컴퓨터에 부정한 행위를 실행시키는 것. (IT용어사전, 한국정보통신기술협회)

8) 엄정호외 2명, op.cit., p.31

9) Bruce Schneier, 『Risk of Networked System』, 2013, p1

사이버 공간별 사이버 공격의 피해는 [표 2-2]와 같이 분류할 수 있다.

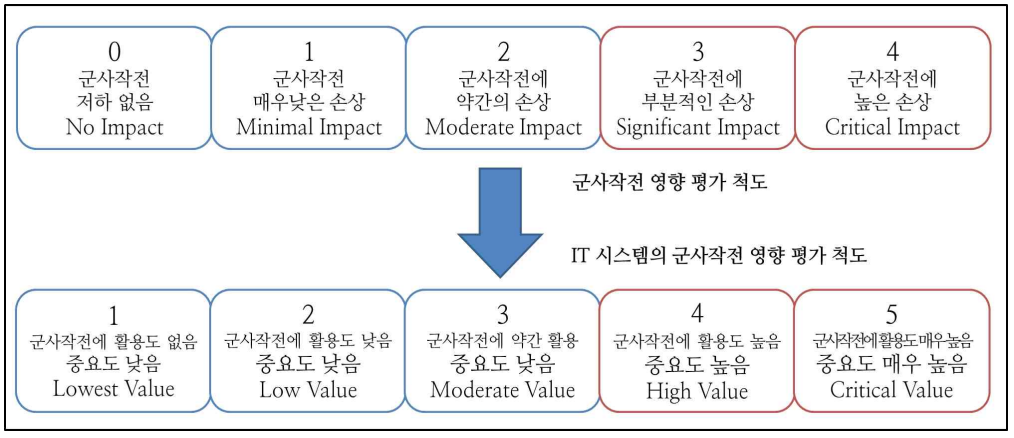
[표 2-2] 사이버 공간별 사이버 공격 피해 분류[10)]

	사이버 공격	
사이버 공간	정치/외교	· 외교정보 유출, 변경, 삭제 등 잘못된 정보 제공으로 인한 외교 정책 방향 변경 · 정당의 홈페이지 변조 및 서비스 중단으로 이미지 훼손 · 정치가의 신상정보 조작 및 유언비어 살포로 정치역량 약화
	국방	· C4ISR 체계로부터 군사정보의 유출, 변경, 파괴로 인한 군사작전 실패 · 전자우편 폭탄, 논리 폭탄 등으로 인한 C4ISR 체계 마비 · 무선전파 차단, 교란으로 각종 작전 및 훈련 차질 · EMP 폭탄, HERF GUN 등으로 국방정보통신체계 마비
	산업/경제	· 국가적으로 중요한 산업정보 유출로 국가 경쟁력 약화 · 웜, 바이러스 등에 의한 산업유통체계 마비로 생산성 저하 · 악의적 내용이 내포된 전자우편 폭탄으로 노사갈등 유도 · 홈페이지 서비스 중단, 생산시스템 오작동으로 기업이미지 훼손
	사회/문화	· 포털 검색사이트 등에 서비스 거부공격, 웜, 바이러스 유포로 중요정보 교류 장애 · 교통, 재난정보 등의 악의적 차단이나 송수신 장애에 의한 경보 미전파로 불안감 조성 · 정보 무단배포 등의 불법적인 행위로 인한 국가 이미지 훼손 · 불법적인 해킹 프로그램 공유로 사이버 범죄 증가

10) 엄정호외 2명, op.cit., p.33

3. 사이버 공격 영향 평가

사이버 공격이 실제 군사작전의 성공여부에 영향을 준다는 점에서는 별다른 이견이 없으나, 이를 시뮬레이션하기 위한 모델링은 별도의 방법론 정의가 필요하다. 기존 군사용 분석 모델과 별도의 사이버 공격 모델을 연동하려고 하여도, 현재의 연동기술은 사이버공격에 대한 특성 및 정보를 반영하지 않고 있기 때문에 별도로 사이버 공격의 영향은 해당 모델에서 사용자 정의로 개발하여야 한다. 사이버 공격이 군사작전의 임무에 미치는 영향을 모델 개발에 반영하기 위하여 기존의 군사작전 영향 평가 척도를 활용하여 사이버 자산의 의존도에 따른 중요도를 반영하여 〈그림2-2〉와 같이 구분한다.



〈그림 2-2〉 IT시스템의 영향에 따른 중요도 척도 구분[11)]

레벨 1에서 3에 속한 IT 시스템은 군사작전에서 활용도가 매우 낮거나 없어서 사이버 공격에 의하여 기능이 손상되어도 군사작전의 성공여부에 크게 영향이 주지 않는 사이버 자산이다. 레벨 4에 속한 IT 시스템은 군사정보의 흐름에 중요한 역할을 하는 사이버 자산으로 사이버 공격에 의해 기능의 손상이나 감소는 실질적인 정보처리 능력에 감소를 초래하지만, 전체 군사작전의 성공여부의 결정적 영향은 미치지 않는다. 레벨 5에 속한 IT 시스템은 군사작전 과정에서 핵심적인 지원을 하는 사이버 자산으로 사이버 공격에 의한 손상이나 능력의 감소는 군사작전을 지원하는 정보처리에 실패를 가져온다.

11) Larry W. Fortson, 「Towards the Development of a Deffensive Cyber Damage and Mission Impact Methodology」, Ohio, Air Force IOT, 2007, p183

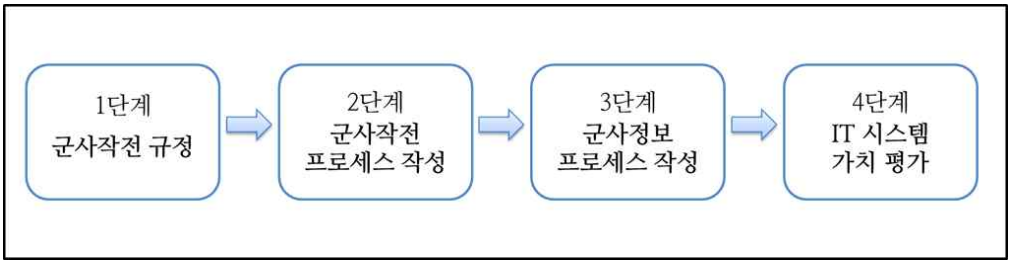
IT 시스템의 중요도를 평가하는 과정은 〈그림 2-3〉과 같다.

첫 번째, 군사작전의 목표를 규정한다.

두 번째, 군사작전의 목표를 달성하기 위한 계획을 수립하고, 수행 프로세스에 대한 우선순위를 결정하여 문서화를 한다.

세 번째, 수행 프로세스를 분석하여 군사정보 프로세스를 규정하고 우선순위 결정 및 문서화를 한다.

네 번째, IT 시스템을 정보 프로세스의 기여도에 따라 분석하여 평가하고 가치에 따라 분류한다.



〈그림 2-3〉 IT시스템의 가치평가 단계

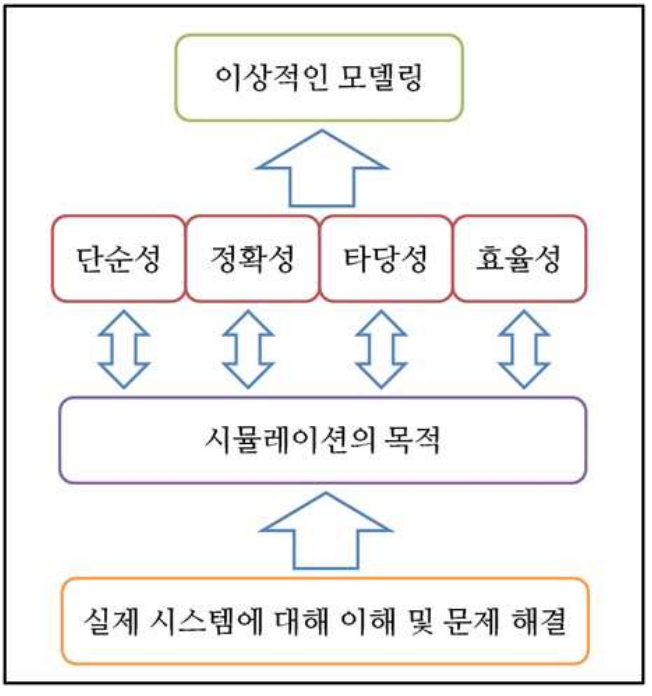
제 2 절 시뮬레이션 모델링

시스템을 주어진 목표를 달성하기 위해 구성된 하드웨어 또는 소프트웨어, 자연 또는 인공적인 모든 자원과 요소를 포함하는 모임으로 정의한다면, 시뮬레이션은 실세계의 시스템을 이해하기 위한 효과적인 컴퓨팅 기술이다. 즉, 시뮬레이션은 복잡한 실제 시스템을 이해하고 예측할 수 있도록 단순화한 개념적 프레임워크인 모델을 컴퓨터로 실행하여 실험을 실시하는 것이다.

1. 시뮬레이션 모델링 개념

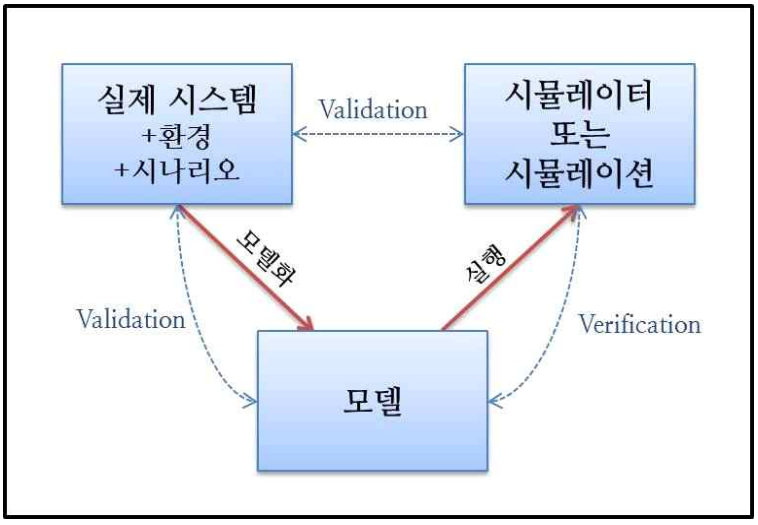
이상적인 모델링을 위해서는 단순성, 정확성, 타당성 및 효율성을 고려하여야 한다. 모델의 단순성을 위해서 의도한 목적을 위한 최소의 필수 요소만을 고려하여야 하며, 반복되고 명확하지 않은 요소는 배제하여야 한다. 효과적인 단순화는 모델에 대한 확인(Validation)을 쉽게 하고, 시뮬레이션 효율성을

높여준다. 정확도는 실제 시스템과 이를 나타내는 모델과의 물리적 및 기능적으로 얼마나 유사한가를 나타내는 척도이다. 모델의 정확도를 높이기 위해서는 개발 비용이 증가하고, 모델 확인의 어려움으로 인한 오차 발생의 가능성이 증가하므로 시뮬레이션의 목적에 맞는 적정한 정확도 수준을 유지해야한다. 모델의 타당성은 모델 검증의 결과로 모델이 주어진 목적을 위해 실제 시스템을 충분히 정밀하고 정확히 표현할 수 있는 지를 나타낸다. 마지막으로 효율성을 위해서는 최소한의 비용과 시간으로 분석의도를 충족하는 정확한 결과를 낼 수 있도록 모델링하여야 한다. 〈그림 2-4〉는 이상적인 모델 구현을 위한 고려사항을 도식화하여 나타낸다.



〈그림 2-4〉 이상적인 모델을 위한 고려사항

시뮬레이션은 〈그림 2-5〉와 같이 세 단계의 기본 절차로 구분한다.

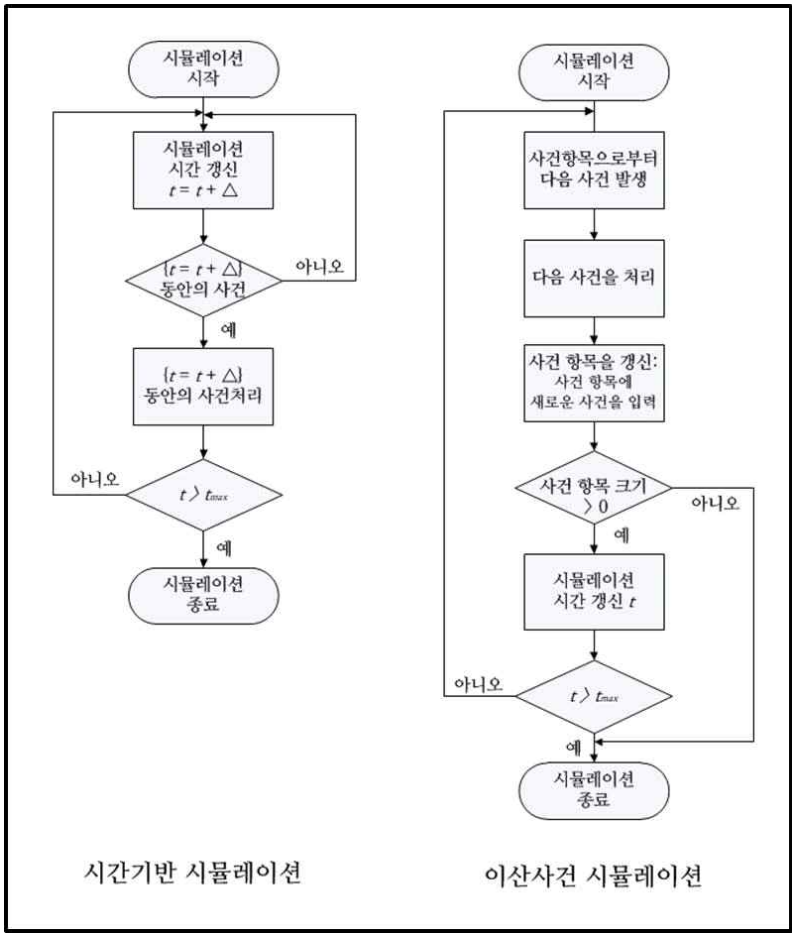


〈그림 2-5〉 일반적인 시뮬레이션 과정[12)]

2. 시간기반 모델링과 이산사건 모델링

사이버 공격을 시뮬레이션하기 위한 방법으로는 시간기반 시뮬레이션과 이산사건 시뮬레이션이 모두 사용 될 수 있다. 이산사건 시뮬레이션은 상태(State)의 변화를 이산사건의 집합으로 나타낼 수 있는 디지털 컴퓨터 상에서의 모델링에 대한 행위이다. 이산사건 시뮬레이션에서 상태의 변화는 사건(Event)이 발생함을 의미하며, 개체(Entity)의 상태는 연속적인 사건 사이에서 일정하게 유지된다. 따라서, 모델에서 사건이 발생하지 않는 시간동안에는 시뮬레이션을 할 필요가 없으므로, 시뮬레이션 시간은 계획된 다음 사건이 발생하는 순간까지 진행된다. 시간기반 시뮬레이션에서는 시간슬롯(Time Slot)의 반복 과정을 통하여 시간의 흐름에 따라 시뮬레이션이 진행된다. 시뮬레이션 시간은 사건 발생과 상관없이 진행되며 반복되는 시간슬롯 간에서 사건은 발생한다. 시간기반(Time-based) 시뮬레이션과 비교하면 〈그림 2-6〉과 같다.

12) Pascal Cantot, Dominique Luzeaux, 『Simulation and Modeling of Systems of Systems』, John Wiley & Sons, 2011



〈그림 2-6〉 시간기반 시뮬레이션과 이산사건 시뮬레이션 비교[13)]

사이버 공격에 대한 이산사건 시뮬레이션을 실행하기 위해서는 필요한 기본 요소는 다음과 같다.

첫 번째, 초기 입력변수로 확률변수(Random Variable)를 생성하는 확률변수 생성기가 필요하다.

두 번째, 시뮬레이션을 진행할 수 있도록 시뮬레이션 시간이 변경되어야 한다.

세 번째, 사건이 우선순위에 의해 실행되도록 사건의 순서가 정해져야 한다.

네 번째, 일반적인 방법인 시뮬레이션 시간과 같은 시뮬레이션 종료 조건이 있어야 한다.

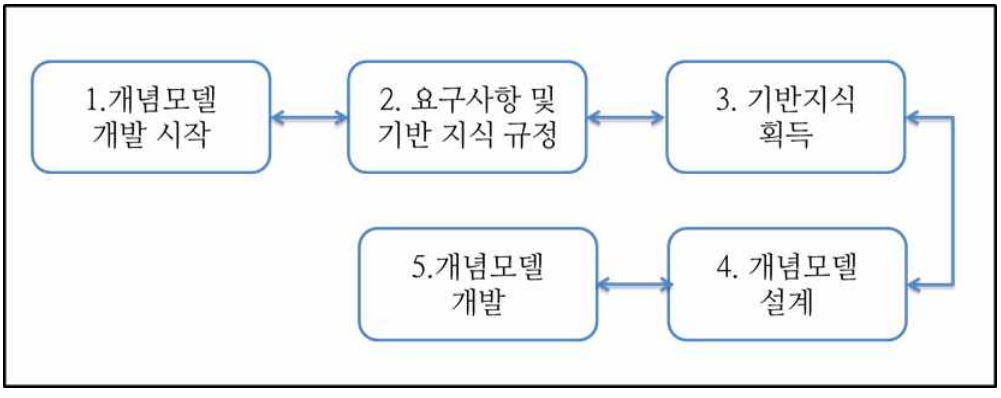
13) Zheng Lu, 『Unlocking the Power of OPNET Modeler』, Cambridge University Press, 2012, p7,p8

3. 개념 (Conceptual) 모델링

개념모델링은 시뮬레이션 모델 개발 단계에서 중요한 과정이므로 정확히 규정하여야 한다. 개념모델은 시뮬레이션 모델 개발 단계에서 실세계와 시뮬레이션의 중간적 단계의 산출물로 시뮬레이션 및 그 구성요소에 관한 시뮬레이션 개발자의 모델링 요구조건을 나타내는 수단이자 정보의 집합이다.

개념 모델에서의 정보는 시뮬레이션을 위해 모델링되는 객체, 행위, 태스크, 프로세스 및 상호작용과 시뮬레이션 요구 조건을 만족하기 위한 수단을 모델링하기 위한 가정 사항, 알고리즘, 특성, 관계 및 자료로 구성되어 있다.

시뮬레이션 요구사항은 실제 모델링 구현에 핵심 요소이므로 개념모델은 시뮬레이션의 요구사항을 정확히 반영하도록 개발되어야 한다. 모델개발의 요구사항에 따른 실세계의 모든 모델링 필수 요소를 정확히 식별하고 개념모델에 구체적으로 반영하여야만 최종 시뮬레이션 모델의 결과는 요구사항을 만족할 수 있다. 개념모델의 개발 과정은 〈그림 2-7〉과 같다.

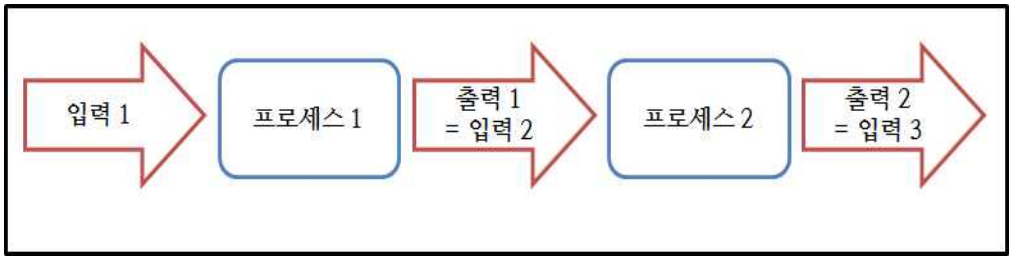


〈그림 2-7〉 개념모델 개발 단계

4. 프로세스 (Process) 모델링

프로세스는 정해진 목표 달성을 실현하기 위해 순서화된 업무 단계의 집합이다. 프로세스 모델링은 모델의 목적에 중요한 역할을 하면서 인간 또는 시스템에 의해 구현 가능한 개별 프로세스 요소들로 연결되는 실제로 진행되거나 제안된 프로세스의 추상적인 설명으로 규정한다. 프로세스 모델은 〈그림 2-8〉과

같이 명확히 규정된 입력과 출력 값을 가지며 현재 또는 미래의 의도된 프로세스의 상태를 묘사하고 프로세스 간에 상호 관계를 갖는다. 프로세스 모델을 통해서 다른 관점에서 수행하고자 하는 목표, 업무를 수행하는 주체, 업무의 수행 시기와 장소, 업무의 수행방법을 이해 할 수 있다.



〈그림 2-8〉 프로세스 모델의 실행 관계

프로세스 모델은 [표 2-3]과 같이 모델링의 상세도에 따라 다양한 레벨을 갖게 되고, 상위레벨은 하위레벨로 나누어 질 수 있다. 프로세스 모델링은 상위레벨의 프로세스에 대한 규정에서 시작하여 하위 업무 단계로 세분화하여 개발한다.

[표 2-3] 프로세스 모델 레벨 분류

레벨(level)	프로세스	설명
레벨1	최상위 프로세스	모델링 과정에서 최종 결과 산출을 위하여 모델링 대상에 대한 핵심적인 프로세스를 상호 기능적 관점에서 개발한 프로세스
레벨2	주요 프로세스	단일 최상위 프로세스 내에서 상세화된 흐름을 표현
레벨3	하위 프로세스	주요 프로세스를 구성하기 위한 개별 활동을 상세하게 표현
레벨4	활동(Activity)	단일 작업 기능에 의해 수행되는 일의 단위로, 단일 또는 다수의 태스크로 구성
레벨5	태스크(Task)	단일 활동을 완수하기 위한 최하위 업무단계

제 3 절 기존 사이버 공격 모델링 관련 연구

실제 전장 환경 이전에 안전하고 경제적인 방법으로 실험 및 훈련을 지원하는 국방 시뮬레이션에서 전통적인 분야인 육상, 해상 및 항공 도메인에 대해서는 오랜 기간 개념 및 기술 연구를 통해 분석 실험을 위한 많은 국방 시뮬레이션 모델이 개발되었다. 최근에는 사이버 공격에 대한 공개된 자료의 부족과 사이버 공간의 복잡성 및 급속한 보안 분야의 기술 발전으로 효과적인 시뮬레이션 모델 개발의 어려움에도 불구하고 대규모 사이버 공격에 의한 국가적 피해 사례로 인한 사이버 보안의 중요성이 증가하여 민간과 공공부문에서 사이버 공격의 모델링 및 시뮬레이션에 대한 연구가 활발히 진행되고 있다.

1. 학술적 연구

사이버 공격 모델링에 대한 민간 부분 및 학술연구는 상당한 연구가 진행되었다. 대부분은 사용자의 개입 없이 자동적으로 실행되는 구성(Constructive) 시뮬레이션으로 사이버 공격에 대한 일반적인 이해를 제공하나 결과의 정확도는 사용된 모델의 해상도에 따라 다를 수 있다. 또한, 대부분의 모델들이 실제 일어나는 사건과 관련하여 입력 파라미터와 사이버 공격 프로세스를 규정하기 어렵기 때문에 제한적인 확인(Validation) 만을 제공한다.

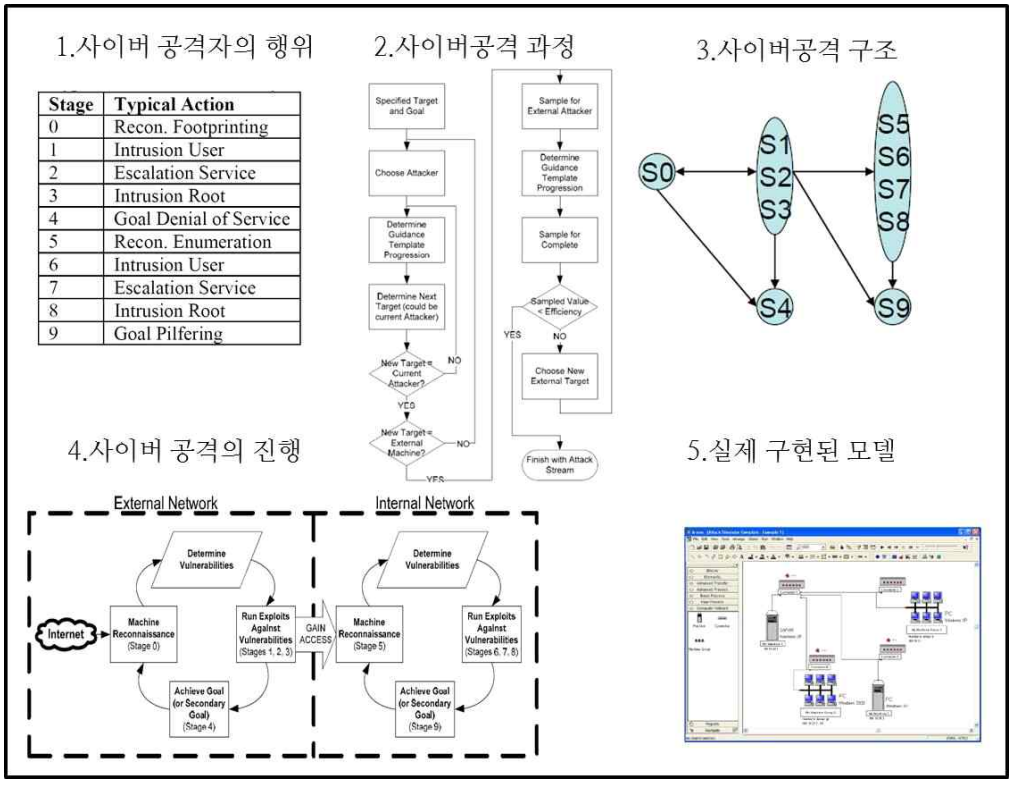
가) Kuhl의 사이버 공격 모델링[14)]

Kuhl은 RTI(Rochester Institute of Technology)에서 개발한 상용 구성 시뮬레이션 도구인 ARENA를 통한 사이버 공격 시뮬레이션 모델을 제안하였다. 사이버 공격은 모델 내에서 사용자 인터페이스를 통해 자동적으로 발생하거나, 설정된 XML(eXtensible Markup Language) 파일을 통하여 발생시킨다. 모델에서의 사이버 공격은 구체적인 사이버 공격 형태와 네트워크상의 공격 목표를 갖는다. 시뮬레이션은 DoS(Denial of Service) 공격과 같은 다양한 사이버 공격 형태 및 목표 컴퓨터에 백도어(Backdoor) 설치를 지원한다. 사이버 공격은 최종 목표 컴퓨터에 접속 권한을 획득하기 위해 사이버 공격자가

14) Michael E. Kuhl, 「Cyber attack modeling and simulation for network security analysis」, 2007 Winter Simulation Conference, 2007

다수의 공격을 시도하는 과정을 포함한다. 모델에서는 사이버 공격의 형태와 목표뿐만 아니라 사이버 공격자의 효율성, 기밀성 및 기술에 관하여 정규화된 수치를 포함하여 확률적으로 사이버 공격의 성공을 결정한다. 시뮬레이션 과정은 사용자가 컴퓨터 네트워크를 구성하고, 사이버 공격 형태, 공격 목표 컴퓨터, 침입탐지시스템(IDS: Intrusion Detection System) 센서의 유형을 수동적으로 선택하여 사이버 공격을 시작하거나, 설정된 XML 파일에 의해 자동적으로 실시한다. 시뮬레이션 결과로 네트워크상에서 발생된 사이버 공격 리스트와 IDS 센서에 의한 경고 리스트를 통계적으로 출력하여 제한적이지만 분석가가 목표 네트워크 구조를 분석하는데 사용할 수 있도록 한다.

〈그림 2-9〉는 Kuhl의 사이버 공격 모델링의 과정을 나타낸다.

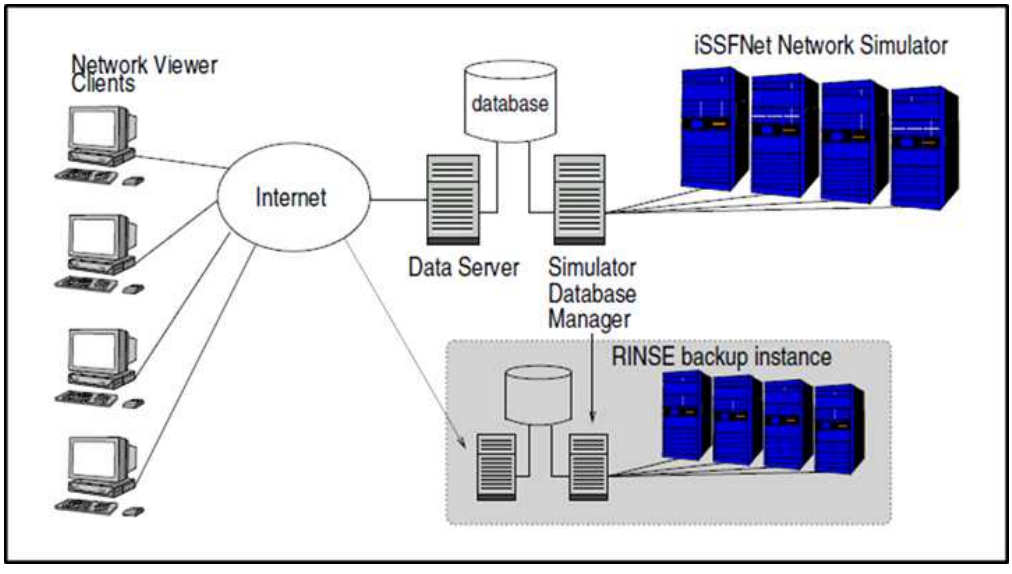


〈그림 2-9〉 Kuhl의 사이버 공격 모델링

나) RINSE[15)]

RINSE(Real-Time Immersive Network Simulation Environment)는 Illinois 대학 연구팀에 의해 개발된 실기동(Live) 시뮬레이션으로 대규모의 독립적인 사용자에 의해 관리되는 다수의 LAN(Local Area Network)으로 이루어진 대규모 WAN(Wide Area Network)을 지원하기 위한 목적으로 개발되었다. 시뮬레이터는 물리적으로 다른 컴퓨터에서 시뮬레이션 연습에 참가하는 LAN 관리자의 역할의 몇몇 사용자를 갖는 폐쇄형 네트워크로 구성된다. 사용자는 시뮬레이션 도구에 의하여 발생한 사이버 공격에 대항하여 각자가 관리하는 네트워크의 방어 임무를 갖는다. 컴퓨터 명령창을 통해서 사용자는 공격, 방어, 네트워크 진단 도구 및 장치 관리에 관한 명령을 내리거나 시뮬레이션 자료를 입력한다. 이러한 시뮬레이션의 핵심은 높은 트래픽을 유발하는 외부 사이버 공격에 대한 훈련과 교육에 있다.

RINSE 시스템 아키텍처는 〈그림 2-10〉과 같다.



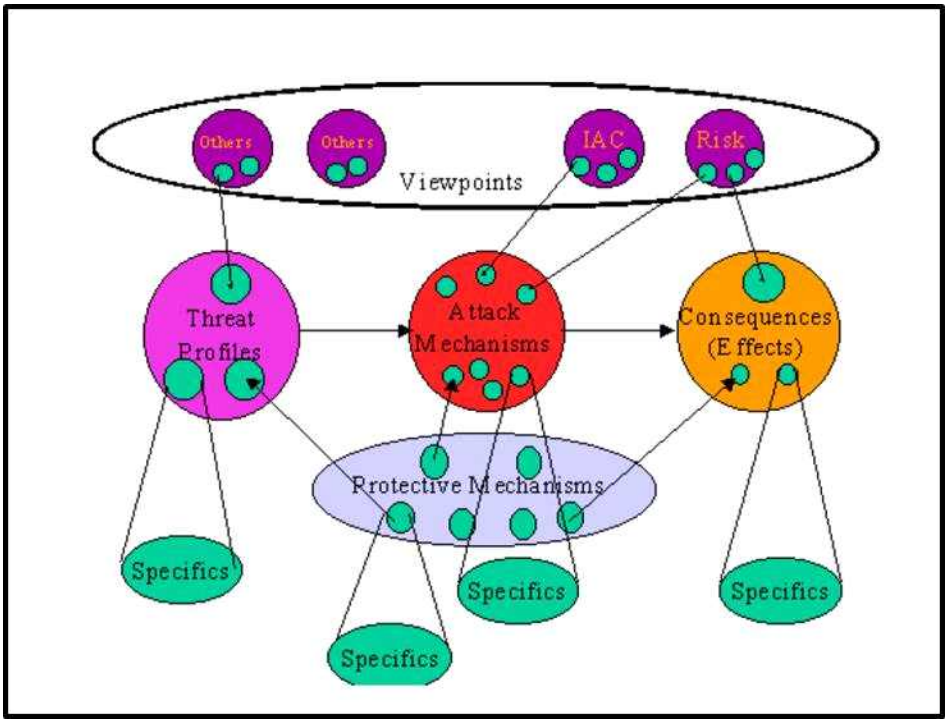
〈그림 2-10〉 RINSE 아키텍처

15) Michael Liljenstam, 「RINSE: the Real-time Immersive Network Simulation Environment for Network Security Exercises」,The 19th Workshop on Principles of Advanced and Distributed Simulation, 2005

다) Cohen의 연구[16)]

Cohen은 사이버 공격자와 방어자의 기술을 중요한 시뮬레이션 파라미터로 활용하여 다양한 공격 시나리오를 시뮬레이션 하였다. Cohen의 모델에서 관심 있는 결과는 사이버 공격과 결과에 대한 시뮬레이션 되는 시간으로 37 개의 위협 형태, 94 개의 공격 분류 및 대략 140 개의 방어 방법을 데이터베이스화하여 약 15,000가지의 조합을 제안하였다. 원인과 결과 사이의 지연시간을 이용하여 단순한 방법으로 사이버 공격에 대한 시뮬레이션을 제공하는 장점이 있다.

사용된 시간과 장비의 가격에 관하여 사이버 공격자와 방어자의 비용을 평가하여 시뮬레이션 결과의 의미를 높였다. 〈그림 2-11〉은 Cohen의 사이버 공격과 방어의 원인 결과 모델의 개념도를 나타낸다.



〈그림 2-11〉 사이버 공격과 방어의 원인 결과 모델

16) Fred Cohen 「Simulating Cyber Attacks, Defences and Consequences」, Sandia National Laboratories, 1999

라) 상용소프트웨어를 활용한 사이버 공격 모델

통신 네트워크, 장치, 프로토콜 및 어플리케이션 분석을 위해 다양한 상용 소프트웨어(COTS: Commercial off-the-shelf)가 개발되었다. QualNet 및 OPNET 등과 같은 상용소프트웨어가 제공하는 네트워크 기술과 사용자 인터페이스 환경은 사이버 공격 시뮬레이션의 효과적인 도구가 될 수 있다.

2. 군사부문 연구

군사부문은 네트워크 중심 운용을 보장하기 위하여 국가 기간망에 대한 사이버 공격을 대비하고 훈련 및 비상계획을 수립하기 위한 사이버 공격 시뮬레이션에 많은 관심을 가지고 진행하고 있다. 군사부문의 연구결과 및 방법론은 중요도에 따라 보안 목적을 위해 전혀 공개되지 않거나 간략한 개요만이 공개된다.

가) SIMTEX (Simulator Training Exercise Network)

SIMTEX는 미국 공군이 훈련을 목적으로 다양한 컴퓨터 네트워크 공격을 시뮬레이션하기 위하여 개발된 기반체계이다. 시뮬레이터는 미 공군의 3개 계층의 네트워크 아키텍처를 모방하여, 다수의 시뮬레이터를 연결하여 내부 네트워크를 구성하고 시뮬레이션된 인터넷 환경을 제공하여 가상의 사이버 적을 대상으로 훈련 할 수 있게 하였다.

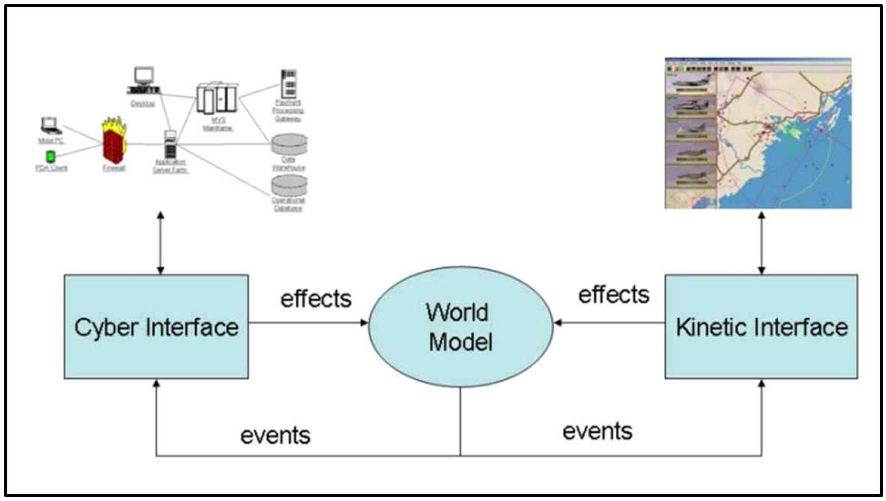
나) CAAJED (Cyber and Air Joint Effects Demonstration)[17]

SIMTEX가 컴퓨터 네트워크 레벨에서 공격의 기술적인 면을 시뮬레이션 한다면, CAAJED는 상위 레벨의 관점에서 사이버 공격이 전쟁 상황에 미치는 영향에 중점을 둔다. CAAJED는 인간 대 인간, 인간 대 컴퓨터 또는 컴퓨터 대 컴퓨터 간의 워게임 플레이를 지원한다. 사이버 공격은 컴퓨터에 의하여 자동적으로 발생하지 않고 운용자에 의해 수동으로 실행된다. 사이버 공격이 네트워크 서비스에 영향을 주면, 워게임(Wargame) 운용자는 항공기지, SAM(Surface-to-Air Missile), 레이더 및 개별 항공기 등 관련된 자산의

17) Raphael S. Mudge 「CYBER AND AIR JOINT EFFECTS DEMONSTRATION (CAAJED) 」,USA DTIC, 2007

기능을 비활성화하거나 저하시키도록 지시한다. 워게임에서의 자산은 사이버 공격에 의해 활성화, 비활성화 또는 효과도면에서 기능이 저하된다. 시뮬레이터 사용자는 사이버 공격을 지시하는 운용자의 존재를 알 수 없으나, 사이버 공격에 의한 영향은 항상 관찰할 수 있다. 시뮬레이션은 개념 확인이라는 측면에서 제한적으로 진행되어지나, 워게임에 사이버 공격 요소를 반영할 수 있다는 점에서 의미가 있다.

CAAJED 시스템 아키텍처는 〈그림 2-12〉와 같다.



〈그림 2-12〉 CAAJED 아키텍처

다) Cyber Storm I, II, III 및 IV

Cyber Storm I, II, III 및 IV는 미국 국토 안보부 사이버 부서에서 계획되어 2006년, 2008년, 2010년 및 2012년에 각각 수행된 라이브 시뮬레이션 훈련이다. Cyber Storm은 100명이 넘는 산업, 군사 및 정부 관계자가 참가하여 시뮬레이션된 사이버 이벤트에 대한 국제적 대비, 대응, 조정 및 복구 메커니즘을 점검하기 위해 실시되었다. 결과적으로, 시뮬레이션은 사이버 보안에 대한 관심과 국제적으로 다른 조직 기관 간에 사이버 공격을 대비하여 협조할 수 있는지에 대한 이해를 제공하였다. Cyber Storm에서 실제적인 사이버 공격에 대한 구체적인 모델링 방법론은 소개되지는 않았지만, 시뮬레이션 결과로 분석된 사이버 공격의 효과와 잠재적인 사이버 위협에 대한 국제적 민간, 군사 및 정부 기관간의 대응 방법에 대한 연구가 이루어진 점에서 의미가 있다.

제 3 장 사이버 공격 영향 평가 모델 설계

제 1 절 모델링 일반사항

1. 모델 개발 절차

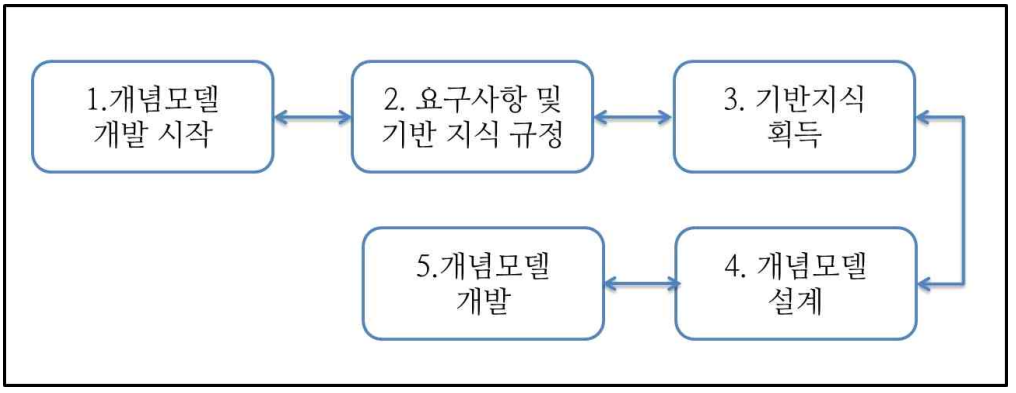
모델링 개발 절차에 대해서는 다양한 방법론이 존재하나 일반적인 모델링 개발 절차는 [표 3-1]에 제시된 기존의 시뮬레이션 모델링 절차의 예와 같이 서로 유사하다.

[표 3-1] 모델링 절차 방법론[18)]

모델링 개발 절차			
단계	J. Banks et al.	Law et al.	Imagine That Inc.
1	문제 정립	문제 정립 및 연구 계획	문제 정립
2	목표 및 전체 프로젝트 계획 정립	자료 수집	정보의 흐름 기술
3	모델 개념화	개념 모델 설계	모델 작성 및 테스트
4	데이터 수집	확인	데이터 획득
5	모델 변환	컴퓨터상에서 모델구현	모델 실행
6	검증	검증	검증
7	확인	실험 설계	확인
8	실험 설계	실제 실행	결과 분석
9	실제 실행 및 분석	통계적 분석	실험 시행
10	추가 실행	결과 해석	문서화
11	문서화 및 보고		의사결정 사항 구현
12	구현		

18) Magnus Felde, 「Analyzing Security Decisions with Discrete Event Simulation」,Gjovik University, 2010

모든 방법론은 실제 시스템에 대해 알고자 하는 문제 정립(Problem Formulation) 단계로부터 시작하며, 각각의 단계는 일회성으로 끝나지 않고, 연구 목적을 달성할 때까지 다음단계에서 이전단계로 반복적인 모델 검증 및 확인 단계를 거친다. 기존의 시뮬레이션 모델링 절차에 대한 연구를 참조하여 본 연구에서는 모델 개발 접근 방법을 〈그림 3-1〉과 같이 제시한다.



〈그림 3-1〉 모델 개발 절차

1단계는 문제를 식별하고 정립한다. 기존의 시스템에 대한 문제를 파악하고 제안할 시스템에 대한 요구사항을 작성하기 위한 실제 시스템에 대한 문제 또는 일부 관심 분야에 대한 범위를 정한다. 모델의 최종 사용자와 협의하여 간략한 시스템 구성사항을 식별하고 최종 시스템 성과 측정을 위한 정량적 성공 기준을 정한다.

2단계는 실제 시스템 자료를 수집하고 처리한다. 즉, 모델링에 필요한 시스템 사양, 입력요소 및 현재 시스템 성능에 대한 자료를 수집하고 시스템이 갖는 통계적 임의성(Randomness)을 파악하여 통계적 입력 변수에 적당한 확률 분포를 선택하고 확률 파라미터를 예측한다.

3단계는 모델을 개발하고 구현한다. 개념모델인 도식적인 시스템의 다이어그램 또는 프로세스를 시뮬레이션 프로그램 언어로 구현하여 컴퓨터상에서 실현 가능한 모델을 개발한다.

4단계는 모델을 확인 및 검증한다. 시뮬레이션 모델이 의도한대로 동작하는지 확인하기 위하여 알려진 환경에서 모델의 결과와 실제시스템의 결과를

비교하고, 통계적 추론 테스트와 해당분야 전문가에 의한 검토를 받는다. 모델의 확인 및 검증 과정은 모델 교정을 위해 이루어지는 반복적인 과정이다.

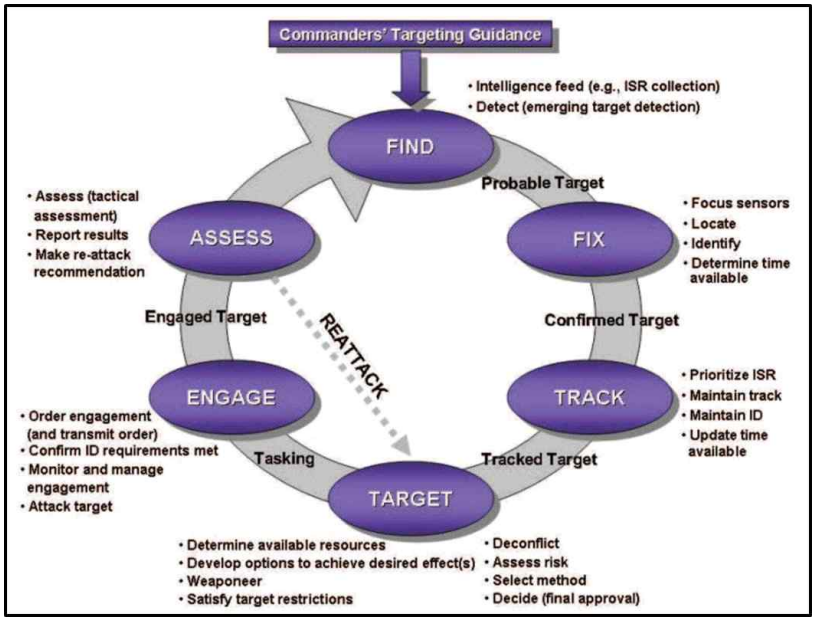
5단계는 시뮬레이션을 실행하고 결과를 분석한다. 시뮬레이션의 결과에는 확률적 편차가 존재하므로 관찰된 결과의 차이가 모델 구현상의 오차에 의한 문제인지 단순한 확률적 분포에 의한 차이인지를 확인 및 검증하기 위한 통계적 분석이 필요하다.

6단계는 모델에 대한 문서화를 한다. 모델링의 목적, 가정상황 및 입력 변수에 대하여 문서화하여 재사용성을 높인다.

2. 시뮬레이션 시나리오

시뮬레이션 시나리오는 모델 설계에 기본이 되는 기능 명세서를 작성하고 모델 개발의 요구사항을 결정하는 분석 대상을 선정하는데 필요한 기본요소이다. 시뮬레이션 시나리오는 모델링의 목적을 정확하고 효과적으로 측정할 수 있도록 구체적이면서도 구현이 가능하도록 작성하여야 한다.

타격순환체계는 〈그림 3-2〉와 같이 타격 목표 처리를 위해 반드시 거쳐야 하는 일련의 이벤트 과정이다. 일반적인 타격순환체계는 F2T2EA로 언급되는 탐지(Find), 확인(Fix), 추적(Track), 조준(Target), 교전(Engage) 및 평가(Assess) 과정을 거친다.

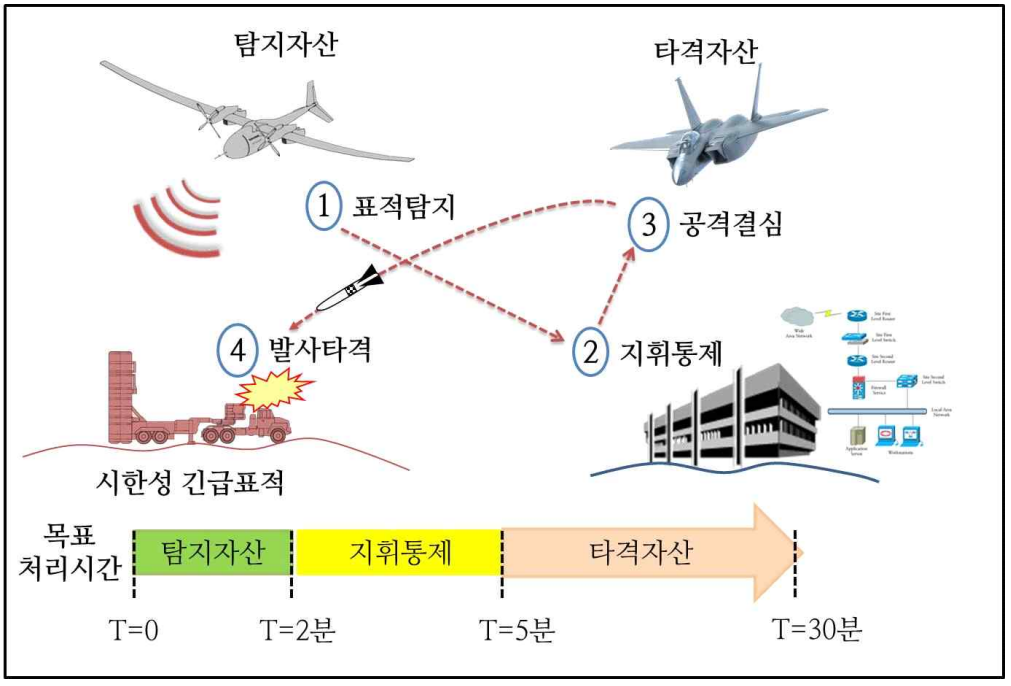


〈그림 3-2〉 시한성 긴급표적(TST) 표적 타격 단계[19]

이러한 탐지, 확인, 추적, 조준, 교전 및 평가의 6 단계는 탐지 자산(Sensors)에서 탐지한 표적 정보를 지휘통제(C2: Command and Control) 시스템에 전달하고 지휘통제 시스템에서는 이를 확인하고 평가하여 타격체계(Shooters)에 교전 명령을 전달하여 타격하는 과정으로 볼 수 있다.

19) Edward H.S. Lo, et al. 「Improving the Kill Chain for Prosecution of Time Sensitive Targets」,InTechOpen, 2010

본 논문에서는 〈그림 3-3〉과 같이 일반화되고 단순화한 타격순환체계(Kill Chain)를 통한 시한성 긴급표적(TST) 처리 과정과 C4ISR 체계를 구성하는 IT 시스템을 대상으로 하는 사이버 공격에 대한 시나리오를 작성하여 모델링 요구사항 및 효과도 분석 지수를 결정하였다.



〈그림 3-3〉 군사작전 시나리오 및 목표 처리시간

본 논문에서 모델 개발을 위한 군사작전 시나리오의 가정 사항은 다음과 같다.

첫 번째, 군사적 데이터의 제한으로 정확한 데이터에 의존하지 않는 해상도의 모델을 개발한다.

두 번째, 입력요소는 공개된 자료를 기반으로 추정하여 입력한다.

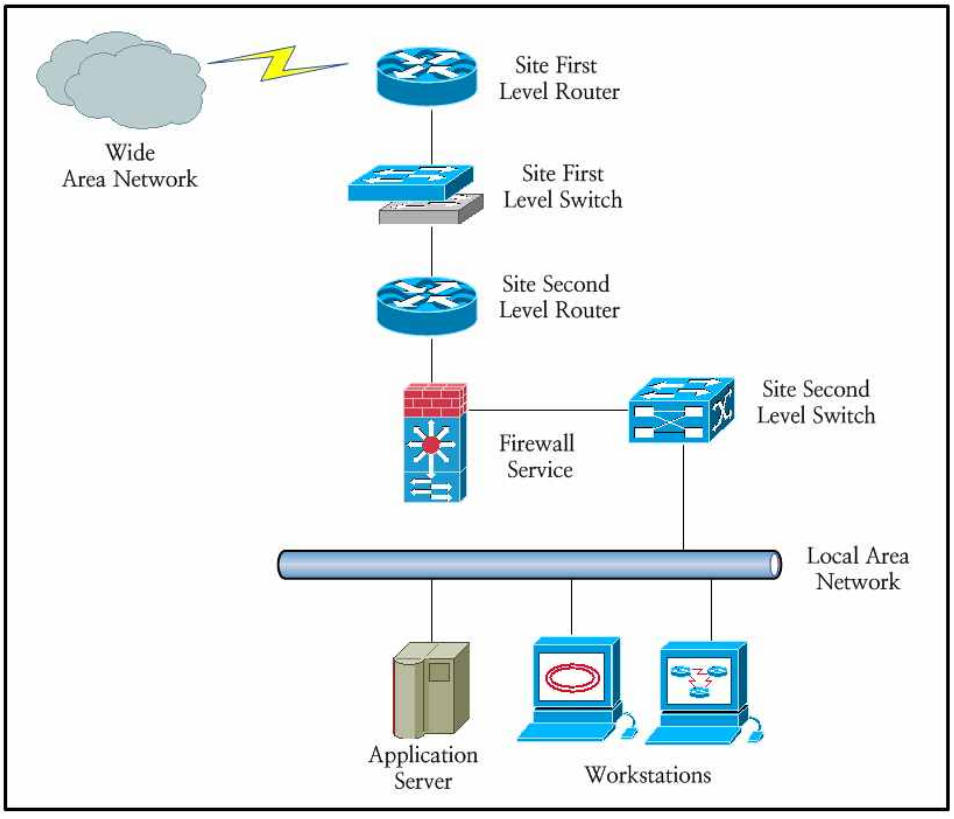
세 번째, 작전 참여자에 의한 의사 결정 요소는 고려하지 않는다.

네 번째, 모델의 명확성을 위해 실제 군사작전의 과정을 단순화하여 모델링 한다.

다섯 번째, 실험 설계를 위한 시나리오 입력 파라미터는 개발된 모델의 효과도를 검증하고, 시뮬레이션 결과의 실험적 분석과 모델의 활용방안을 제시하기 위하여 임의로 입력 파라미터를 달리하여 작성한다.

타격순환체계(Kill Chain) 과정을 통한 군사작전의 성공은 IT 시스템에 의한 신속한 정보의 전달과 처리에 의존한다. 지휘통제체계를 구성하는 IT 표준 시스템은 〈그림 3-4〉와 같이 방화벽, 라우터, 스위치, 워크스테이션, 어플리케이션 서버 및 소프트웨어로 구성되어 있다. 군사정보는 네트워크 장치인 방화벽, 라우터 및 스위치를 통해 워크스테이션 및 어플리케이션 서버에 전달된다.

개별 IT 시스템은 확률변수에 의해 다양한 크기의 트래픽을 유발하여 전체 프로세스에 지연효과를 발생시킨다.



〈그림 3-4〉 표준 IT 시스템 구성도

사이버 공격에 대한 시나리오는 Musman의 논문을 참조하여 사이버 공격의 영향에 대한 범주를 [표 3-2]와 같이 구분하였다. 사이버 공격으로 인한 영향을 시스템의 서비스 능력에 대해서는 성능저하와 중단으로 구분하였으며, 시스템의 데이터에 대하여는 변조, 가공, 감청 및 무단 사용으로 구분하였다. 사이버 공격의 발생 빈도와 지속 시간은 분석자의 입력 값에 의해 결정된다.

[표 3-2] 사이버 공격 범주에 따른 영향[20]

공격범주	프로세스에 미치는 영향	정보에 미치는 영향
성능저하	정해진 배수만큼 프로세스 속도 저하	정보 전달 속도 감소 활동에 의해 생산된 정보의 품질과 정확도가 감소
중단	일정기간 동안 프로세스가 동작하지 않고 사건이 복구될 때까지 재시작하지 않음	일정기간 동안 정보를 사용할 수 없음
변조	프로세스 특성이 프로세스의 결과/출력에 영향을 줄 수 있게 변경됨	정보가 변조되어, 변조된 정보를 사용하는 프로세스가 실패하거나 잘못된 결과를 출력
가공	허위 임무가 시스템에 입력되어, 실제 임무에 간섭을 일으킴	허위 정보가 시스템에 입력됨
감청	프로세스가 공격자에 의해 감청되어짐	정보가 공격자에 의해 포착됨
무단사용	프로세스 상에서 미래 영향에 대한 가능성이 증가하거나, 예기치 않은 출력 발생	정보에 대한 미래 영향에 대한 가능성 증가

20) Scott Musman 「Computing the Impact of Cyber Attacks on Complex Missions 」,USA, MITRE, 2011

3. 모델링 요구조건

시뮬레이션 모델 개발 이전 단계인 실제 시스템에 대한 정확한 개념 모델링 및 프로세스 모델링을 위한 요구사항 정립은 시뮬레이션을 통한 문제 해결을 위해 중요한 과정으로 모델링의 수준을 결정하여 모델개발 시간과 비용에 영향을 준다. 올바른 모델 요구사항을 위해서는 모델링의 제한사항을 이해하고 개발 기간과 비용을 고려하여 합리적인 해상도 수준에서 제시하여야 한다.

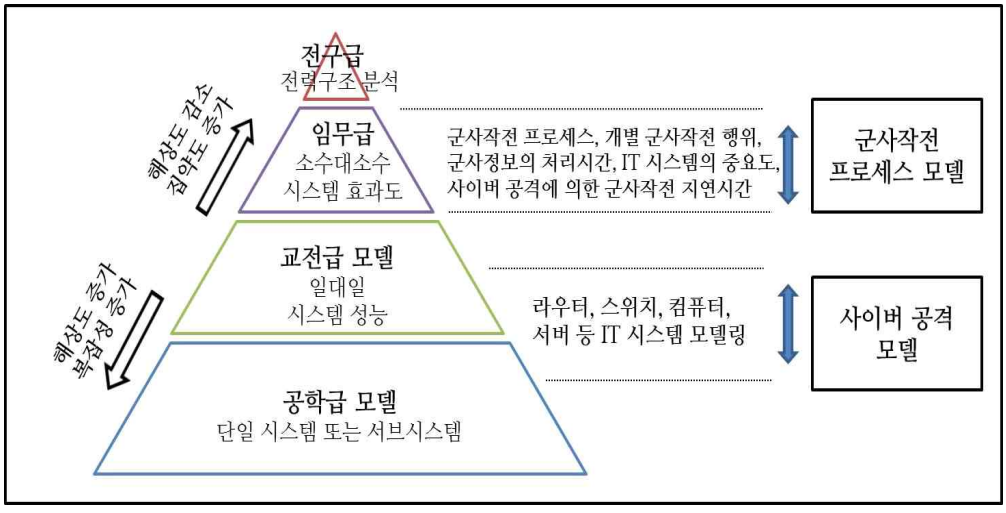
본 논문에서 모델 개발을 위해 고려한 시뮬레이션 결과에 따른 효과도(MOE) 분석지수는 다음과 같다.

첫 번째, 현재 군사작전 절차에 소요되는 시간과 목표시간을 판단 기준으로 하는 예상 군사작전 성공률은 얼마인가?

두 번째, 사이버 공격의 지속 시간에 따른 군사작전의 성공률의 변화는 얼마인가?

세 번째, 현재 사이버 공격의 진행으로 군사 정보의 전달이 지연되는 상황이 발생했다면, 군사작전의 성공률을 높이기 위해 작전 사령관이 IT 시스템 복구를 기다리거나 군사 정보 없이 최종 타격 명령을 내려야 하는 최대 시간은 얼마인가?

이러한 분석지수에 대한 결과를 도출하기 위한 모델의 해상도와 국방 M&S (Modeling and Simulation)의 계층구조와의 관계는 〈그림 3-5〉와 같다.



〈그림 3-5〉 M&S 계층구조와 모델 요구사항의 해상도

모델 해상도를 고려한 사이버 공격이 군사작전에 미치는 영향 분석을 위한 모델링 요구사항은 다음과 같다.

- 개별 군사작전 프로세스 처리시간에 대한 확률적 입력
- 군사작전 프로세스에서 정보처리 시간의 확률적 결과 출력
- 정의된 성공 기준에 따른 군사작전의 성공 여부에 대한 평가기준의 지원
- 군사작전 전체 전개시간에 대한 확률적 계산에 의한 결과 출력
- 정의된 범주에 따른 사이버 공격의 랜덤(Random) 발생
- 사이버 공격 범주에 따른 정보처리 프로세스 시간 평가
- 사이버 공격 범주에 따른 군사작전 프로세스 처리 시간 및 성공 여부 평가
- 개별 군사작전의 IT 시스템 의존도에 따른 중요도 평가 지원
- 사이버 공격에 의한 IT 시스템의 기능 감소 평가 지원
- 사이버 공격 지속 시간에 의한 군사작전 영향 평가 지원
- 사이버 공격의 영향에 의한 IT 시스템의 기능 변화가 개별 군사작전 임무에 미치는 영향 평가
- 사이버 공격의 영향에 의한 IT 시스템의 기능 변화가 전체 군사작전에 미치는 영향 평가
- IT 시스템의 개별 정보 처리 시간에 대한 확률적 입력 및 결과 출력

모델링 요구사항을 모델 구성 요소별로 구분하면 [표 3-3]과 같다.

[표 3-3] 모델링 요구사항 요소

구분	모델링 요구사항
입력 요소	- 범주에 따른 사이버 공격의 발생 확률 - 사이버 공격의 지속 시간 - 개별 IT 시스템의 정보 처리 시간 - 개별 임무의 프로세스 시간
출력 요소	- 전체 IT 시스템의 정보 처리 시간 - 전체 군사작전 프로세스 시간
분석 요소	- 전체 군사작전 성공 여부 평가 - IT 시스템의 중요도 평가 - 사이버공격에 의한 군사작전 성공 여부 평가

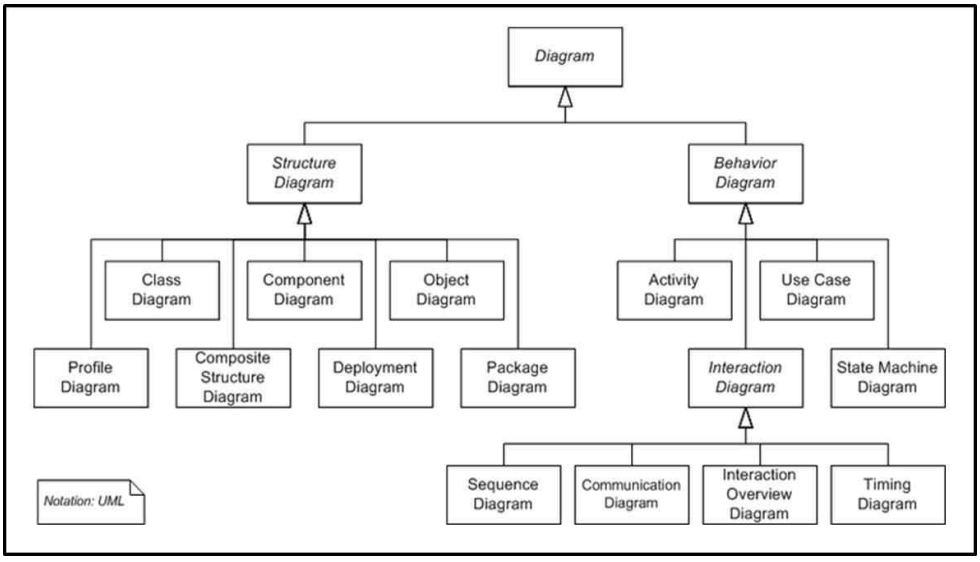
제 2 절 모델 표현

1. UML (Unified Modeling Language)

UML은 국제 표준화 기구인 OMG(Object Management Group)에서 객체 지향적 분석 및 설계 방법론을 통합하여 1997년에 표준화한 모델링 표기법으로 소프트웨어 시스템에 대한 시각화, 명세화, 구축설계 및 문서화에 대한 방법을 규정하여 다양한 관점에서 소프트웨어 아키텍처를 정의할 수 있도록 지원한다.

UML을 통한 모델 개발의 장점은 시스템 컴포넌트를 모델링함으로써 모델 산출물에 대한 재사용성을 높일 수 있으며 자동화된 레이아웃 및 시각화 도구를 이용하여 개발 시간을 단축할 수 있다. 또한 시스템에 대한 논리적이고 이해가 쉬운 표현법을 제공하여 시스템에 대한 개발자간의 이해와 의사소통을 쉽게 하여 복잡한 시스템을 관리 할 수 있게 한다.

UML 2.4.1은 다이어그램을 상위레벨에서 〈그림 3-6〉과 같이 구조적 다이어그램과 행위 다이어그램으로 구분한다.



〈그림 3-6〉 UML 다이어그램의 분류[21)]

21) Norman Daoust, 『UML Requirements Modeling For Business Analysis』, Technicals Publications, 2012

2. 4+1 뷰모델 (View Model)

Kruchten에 의해 제안된 4+1 뷰모델은 복잡한 시스템에 대한 아키텍처(Architecture)를 설명하기 위해 동시에 여러 관점에서 전체 시스템을 관련된 부분으로 나누어 표현하는 방법론이다[22]. 4+1 뷰모델은 구조뷰(Structural View), 행위뷰(Behavioral View), 구현뷰(Implementation View), 환경뷰(Environment View) 및 다른 뷰의 기준이 되는 Use Case뷰로 구성된다.

각각의 뷰는 시스템 사용자, 개발자 및 프로젝터 관리자와 같은 다양한 이해 당사자의 관점에서 시스템을 설명하며, 시스템을 표현하려는 목적에 따라 특정한 UML(Unified Modeling Language)과 연관되어 있다.

구조뷰는 클래스(Class)와 객체(Object)를 강조하며 시스템을 구성하는 부분과 그에 대한 상호관계를 추상적으로 나타내어 시스템이 최종 사용자에 제공해야 할 서비스를 표현한다. 구조뷰를 나타내는 UML 다이어그램은 클래스 다이어그램, 객체(Object) 다이어그램 및 복합구조(Composite Structure) 다이어그램이 있으며 패키지 다이어그램을 포함하기도 한다.

행위뷰는 시스템의 프로세스를 표현하며 프로세스 간의 모든 통신 및 상호작용을 표현하며 시스템 내에서 어떠한 일이 일어날 필요가 있는지를 조사한다. 행위뷰는 시스템의 처리능력을 표현하며 시스템이 다중의 스레드(Thread) 또는 프로세스(Process)를 가지고 있을 때 유용하다. 행위뷰를 표현하는 UML 다이어그램은 절차(Sequence) 다이어그램, 통신(Communication) 다이어그램, 상태(State) 다이어그램, 활동(Activity) 다이어그램, 상호작용(Interaction Overview) 다이어그램 및 시간(Timing) 다이어그램이 있다.

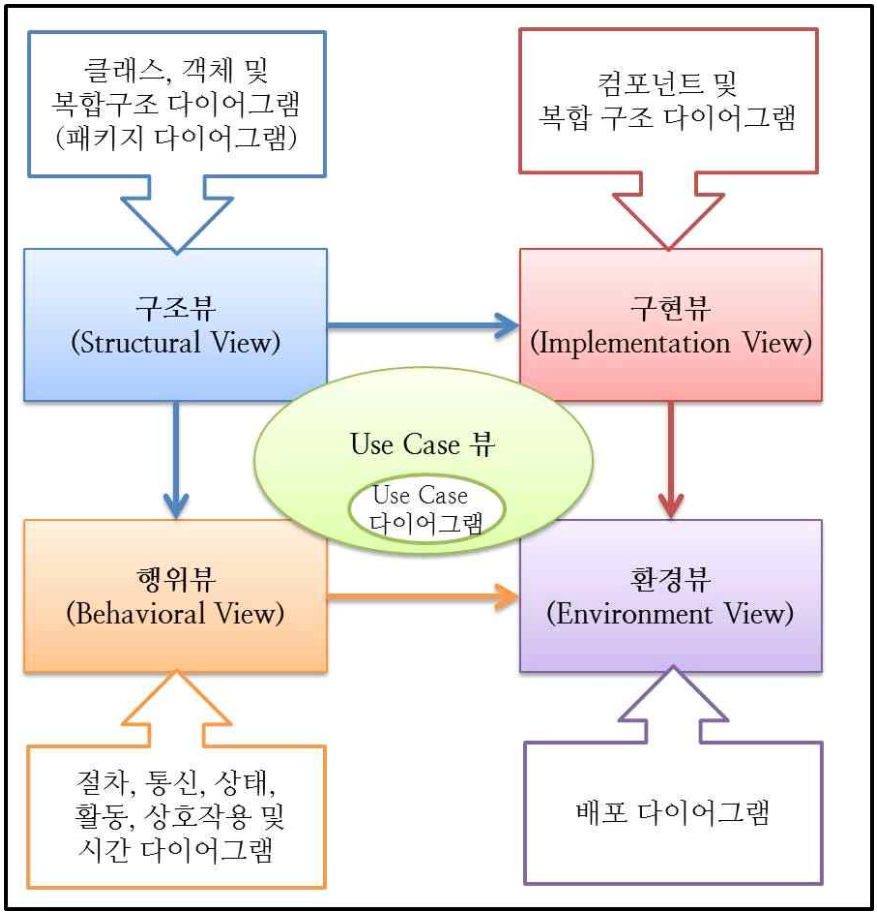
구현뷰는 시스템의 패키지(Package), 서브시스템(Sub-System), 클래스라이브러리(Class Library)를 포함하는 모듈(Module) 또는 컴포넌트(Component)를 표현하여 시스템 배포의 형상관리에 사용된다. 구현뷰는 시스템의 빌딩 블록(Building Block)을 표시하며 시스템 레이어(Layer)를 관리하는데 유용하다. 개발뷰를 나타내는 UML 다이어그램은 컴포넌트 다이어그램과 패키지 다이어그램이 있다.

---

22) Philippe Kruchten, 「Architectural Blueprints—The “4+1” View Model of Software Architecture」,IEEE, 1995

환경뷰는 시스템의 하드웨어 실행 환경을 모델화한다. 소프트웨어 산출물을 해당 하드웨어에 대한 분산, 인도 및 설치를 표현한다. 물리적뷰를 표현하는 UML 다이어그램은 배포(Deployment) 다이어그램이 있다.

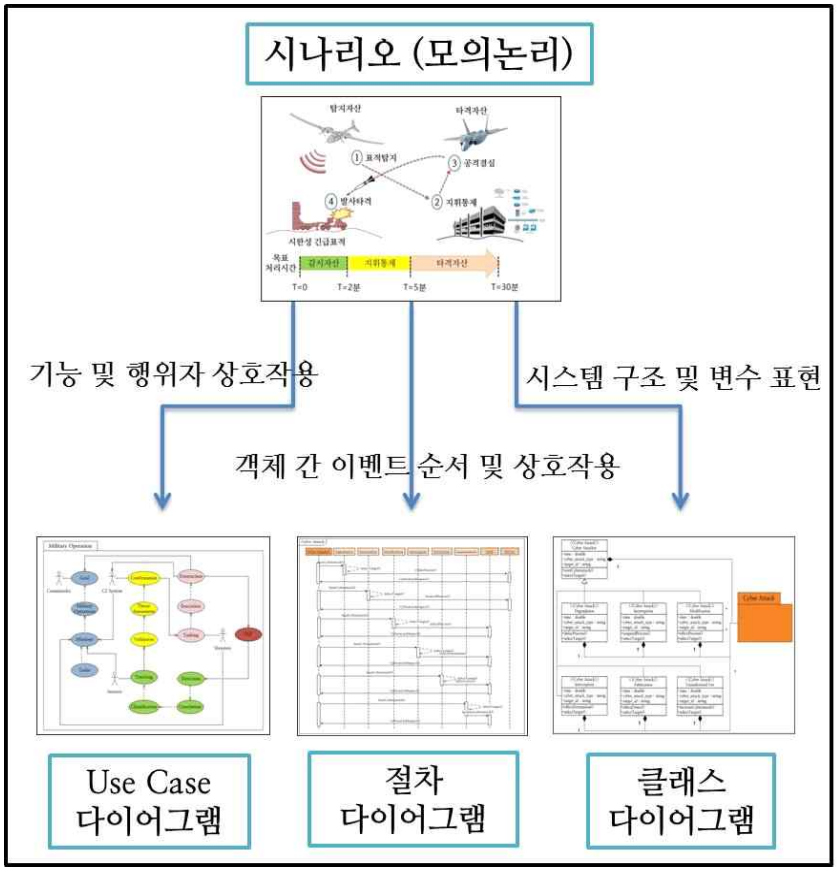
마지막으로 Use Case뷰는 가장 중요한 구조적 뷰로 시스템의 기능 및 행동을 나타내며 시스템 아키텍처를 구체화하는 요인들을 명세화하여 사용자의 목적과 시나리오를 파악하게 한다. Use Case뷰는 시스템에 대한 외부관점에서의 이해를 제공하여 다른 4가지 뷰에 대한 구조와 기능을 규정하고 설명하는데 유용하다. Use Case뷰를 표현하는 UML 다이어그램은 Use Case 다이어그램이 있다. 4+1 뷰모델과 지원 UML 다이어그램을 정리하여 제시하면 〈그림 3-7〉과 같다.



〈그림 3-7〉 4+1 뷰모델과 지원 UML 다이어그램

제 3 절 모델 구조 (Model Architecture)

개념모델의 목적은 최상의 객체와 객체간의 속성에 대하여 상위레벨에서 관계를 규정하는 것이다. 개념모델을 표현하기 위해 4+1 뷰모델 방법론을 지원하는 UML(Unified Modeling Language) 다이어그램을 활용하였다. 〈그림 3-8〉은 모델 구조 설계를 위한 시나리오와 UML 관계를 나타낸다.



〈그림 3-8〉 모델 구조 설계와 UML 관계

Use Case 다이어그램에서는 시스템 기능 및 행위자의 상호작용을 표현하고, 절차 다이어그램에서는 시스템 기능 구현을 위한 객체간의 이벤트 순서 및 상호작용을 표시한다. 마지막으로 클래스 다이어그램을 활용하여 모델링하려는 시스템의 클래스 구조 및 변수를 표현한다.

1. Use Case 다이어그램

Use Case 다이어그램은 사용자의 시스템에 대한 요구조건을 이해하기 위한 것으로 시스템의 구현을 배제하고 시스템 자체의 행위 및 외부와의 상호작용의 관점에서 작성한다. [표 3-4]는 실험 설계를 위한 시나리오를 구성하는 Use Case 요소를 나타낸다.

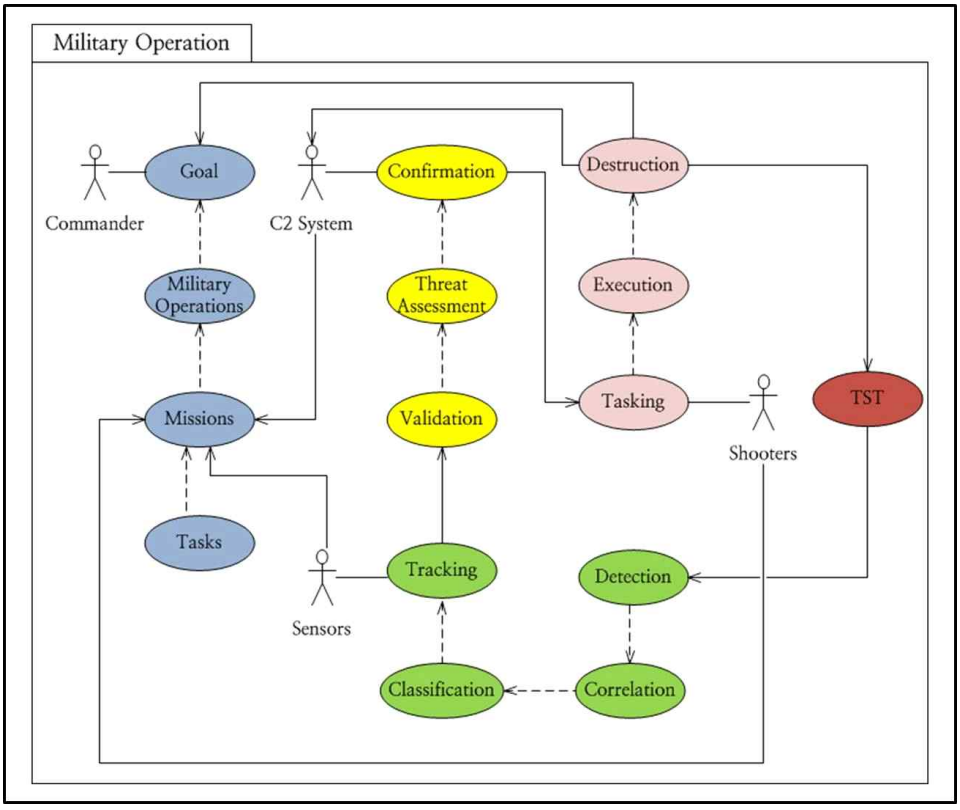
Use Case 요소에서 군사작전에 대한 행위자는 군사작전을 지휘하는 작전사령관, 지휘통제 시스템(C2 System), 탐지자산(Sensors) 및 타격자산(Shooters)으로 구분한다. 작전사령관은 군사작전의 최종목표 실현을 위하여 군사작전 및 군사임무와 연관관계를 가지고 상호 작용을 한다. 작전사령관의 군사작전 완수를 지원하기 위한 지휘통제체계와 통신체계가 합쳐진 지휘통제 시스템은 내부적으로 타격 목표에 대한 평가 판단, 위협평가 및 타격명령의 행위를 수행한다. 탐지자산은 타격목표에 대한 탐지, 상관 알고리즘에 따른 트랙정보를 생성하고, 타격 목표 분류 및 추적 정보를 지휘통제 시스템에 전달하기 위한 행위를 실시한다. 타격자산은 지휘통제 시스템에서 전달 받은 정보를 바탕으로 타격자산의 할당 및 교전 절차를 실행하여 타격 목표의 파괴 여부를 확인하는 행위를 수행한다.

[표 3-4] 군사작전 시나리오에 대한 Use Case 요소

Actor	Use Case	
작전사령관  Commander	목표  	군사작전을 통해 이루려고 지향하는 대상 또는 목적
	군사작전  	전략과 작전목표를 달성하기 위한 계획에 따른 전투 행동
	군사임무  	개인, 조직 또는 부대에 부여된 군사작전을 구성하는 과업 또는 명령
	군사업무  	예하부대에 할당된 군사임무를 달성하기 위한 개별 업무

지휘통제  C2 System	평가 Validation	피아식별장치를 통해 탐지 정보를 평가 판단
	위협평가 Threat Assessment	추적 정보간의 우선순위를 비교하고 최우선 위협을 할당
	타격명령 Confirmation	탐지확률과 위협평가를 고려하여 타격체계에 교전 순위를 전달
탐지자산  Sensors	탐지 Detection	레이더 또는 탐지 시스템을 통해 타격목표를 탐지하고 추적기(Tracker)에 정보를 보냄
	상관 Correlation	상관 알고리즘에 의한 탐지 정보를 종합하여 탐지 확률에 따른 트랙정보 생성
	분류 Classification	탐지된 정보를 클래스 라이브러리와 비교하여 목표를 식별 분류하여 지휘통제(C2) 시스템에 전달
	추적 Tracking	추적(Track) 정보에 따른 우선순위(Priority)에 따라 지휘 통제 시스템에 정보를 전달
타격자산  Shooters	할당 Tasking	교전을 위해 최적의 타격체계(교전무기)를 할당하고 역탐지 (Counter-Measure)를 작동
	실행 Execution	타격체계 무기(미사일)를 발사하고 교전 절차를 시작
	파괴 Destruction	미사일 요격 정보 및 폭발 신호를 수신

시나리오에서의 행위자(Actor)는 사람 또는 시스템이며 개별 행위는 다른 행위와 독립적이거나 종속되어 있다. 개별 행위자와 행위에 대한 관계를 군사작전의 범주에서 Use Case 다이어그램으로 나타내면 〈그림 3-9〉와 같다.



〈그림 3-9〉 군사작전 시나리오에 대한 Use Case 다이어그램

군사작전 시나리오에 대한 Use Case 다이어그램은 작전사령관이 시한성 긴급표적(TST) 타격을 목표로 하는 군사작전을 계획하고 실행하기 위한 Use Case 요소의 상호 관계를 나타낸다. 군사작전은 군사업무로 이루어진 군사임무에 의해 전개되고, 타격목표에 대한 정보는 탐지자산에 의하여 탐지, 판독, 분류 및 추적 과정을 통해 지휘통제 체계에 전달한다. 지휘통제 체계에서는 획득된 정보를 확인하고 위협분석을 통해 타격자산에 타격명령을 내린다. 타격자산은 할당된 타격수단을 이용하여 실제 타격을 실시하며 타격목표에 대한 파괴 여부를 확인하는 행위를 수행한다.

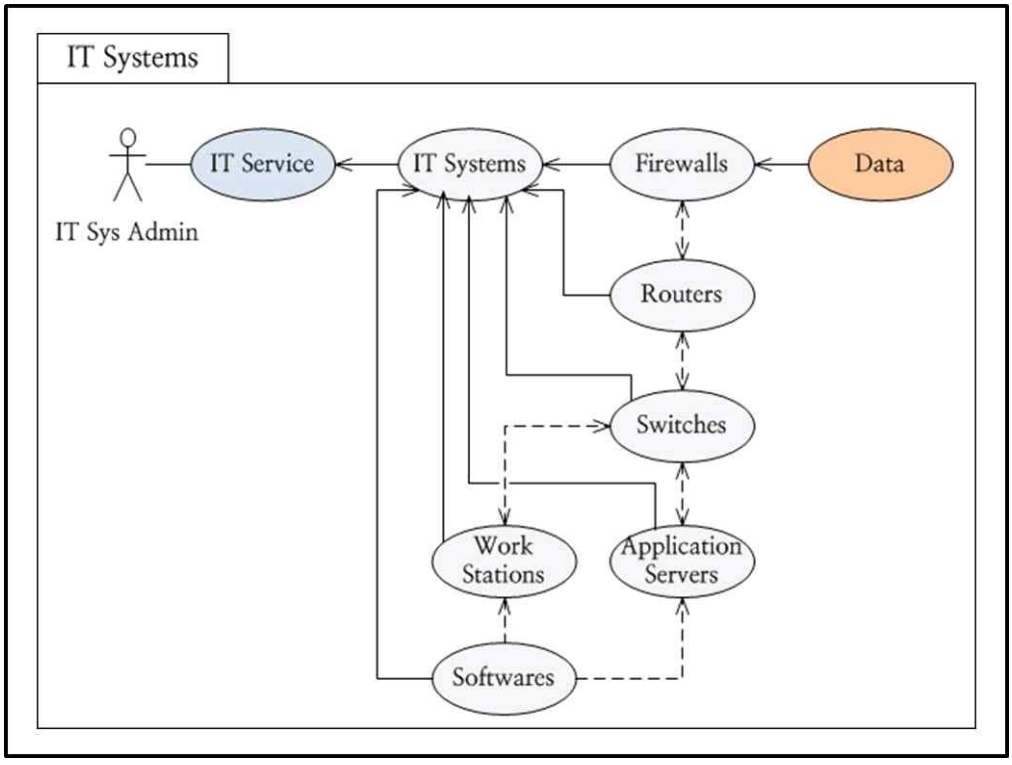
시나리오에서 군사작전을 지원하는 IT 시스템을 일반화하여 행위자와 행위를 나타내면 [표 3-5]와 같다. IT 시스템을 구성하는 하드웨어 및 소프트웨어는 Use Case의 개별요소로 상호 행위를 통해 IT 관리자에게 IT 서비스를 제공한다.

군사작전을 지원하는 표준 IT 시스템은 방화벽, 라우터 및 스위치로 구성되는 네트워크 장비와 어플리케이션 소프트웨어를 실행하기 위한 워크스테이션 및 어플리케이션 서버로 구성되어 있다.

[표 3-5] IT 시스템에 대한 Use Case 요소

Actor	Use Case	
IT 관리자  IT Sys Admin	IT 서비스 	군사 정보 및 작전 절차의 생성, 관리, 최적화 또는 접속을 위해 IT 시스템 및 기술을 제공
	IT 시스템 	군사 정보를 수집, 처리, 생성 및 전달을 위해 사용되는 모든 하드웨어 및 소프트웨어
	소프트웨어 	컴퓨터 프로그램과 그와 관련된 모든 문서를 포함
	워크스테이션 	PC를 포함한 특수한 분야에 사용하기 위해 만들어진 고성능 컴퓨터
	어플리케이션서버 	네트워크 환경에서 응용프로그램을 통해 군사작전을 지원하는 서버
	스위치 	네트워크 내에서 개별 IT 시스템을 연결하는 장비
	라우터 	네트워크 간의 적절한 통신 경로를 선택하여 IT 시스템에 정보를 전달해 주는 장치
	방화벽 	네트워크 환경에서 불법적인 접속을 차단하고 허가된 트래픽만 전달하는 시스템

IT 시스템에 대한 행위자와 행위에 대한 관계를 Use Case 다이어그램으로 나타내면 〈그림 3-10〉과 같다.

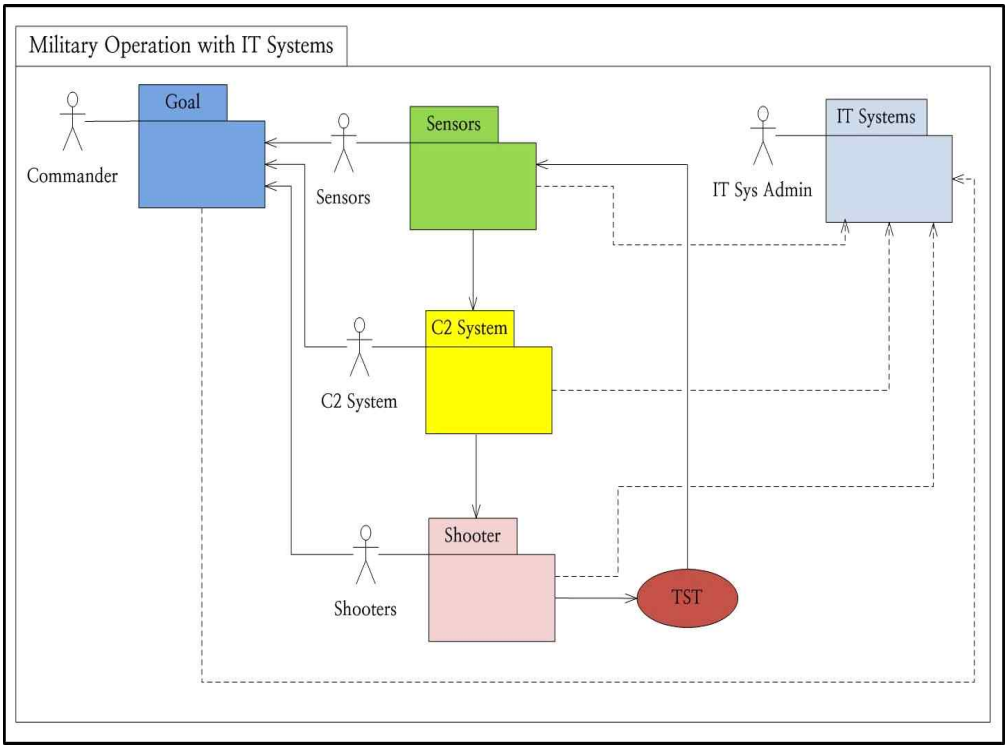


〈그림 3-10〉 IT 시스템에 대한 Use Case 다이어그램

군사 작전을 지원하는 표준 IT 시스템에 대한 Use Case 다이어그램은 군사 정보가 방화벽, 라우터, 스위치를 통한 전달과정을 거쳐 어플리케이션 서버 또는 워크스테이션에서 처리되는 과정과 시스템 사용자의 소프트웨어 접속 행위를 나타내는 Use Case 요소의 상호 관계를 나타낸다.

Use Case 다이어그램에서 IT 시스템은 군사작전을 수행하기 위해 필요한 군사 정보를 생성, 수집, 처리 및 전달하기 위해 사용되는 모든 하드웨어 및 소프트웨어를 포함한다. IT 시스템은 군사작전 수행에 필요한 군사정보 및 군사작전 절차의 생성, 최적화 및 관리를 지원하는 IT 서비스를 제공하기 때문에 IT 시스템 가용여부는 군사작전 성공의 중요한 요소이다.

군사작전과 IT 시스템의 상호 관계에 대한 요소를 상위 계층구조로 나타내면 〈그림 3-11〉과 같다. 개별 Use Case 요소는 유사한 기능에 대하여 행위자 별로 그룹화를 통해 최상위 단계로 패키지화하여 전체 시스템에 대한 이해를 쉽게 하고 이후 컴포넌트 단위 구현을 쉽게 한다. 개별 무기체계의 내부 군사정보 처리 및 외부 시스템으로의 전달 프로세스를 위한 상호 행위는 IT 시스템이 제공하는 IT 서비스에 의존하여 지원되기 때문에 최종 군사작전의 성공여부는 IT 시스템이 제공하는 서비스 가용성 및 중요도 척도에 따라서 결정된다.



〈그림 3-11〉 IT 시스템을 포함한 군사작전의 Use Case 다이어그램

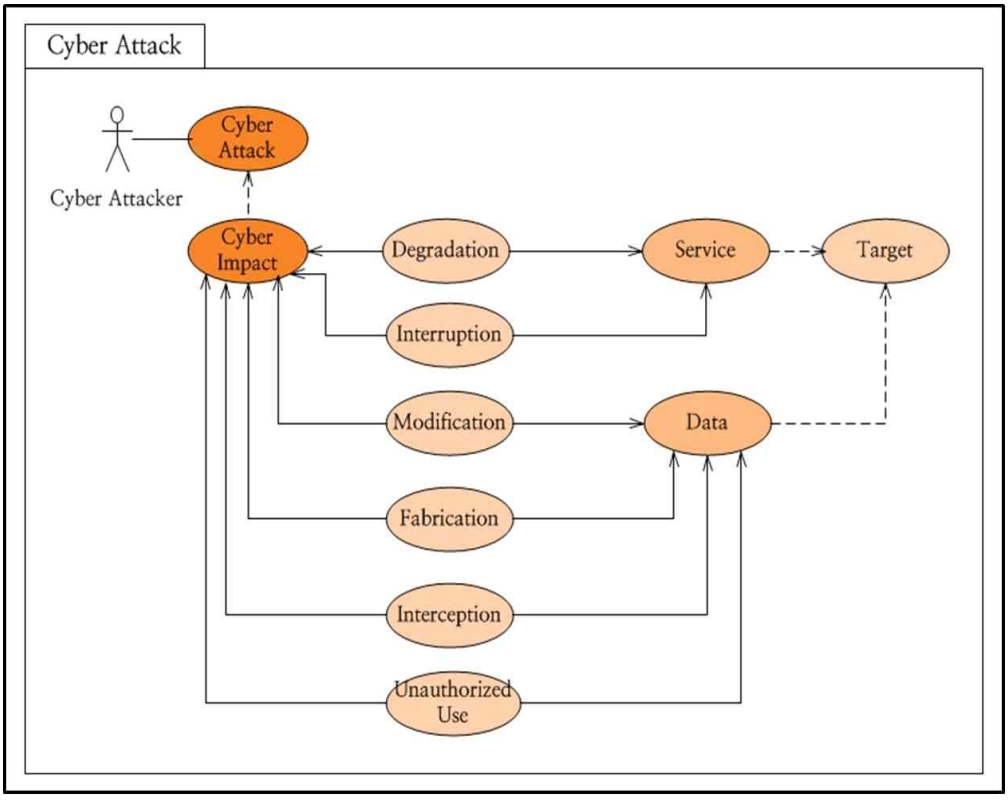
IT 시스템을 포함한 군사작전의 Use Case 다이어그램으로 표현된 시스템 행위자간의 상호관계에서 알 수 있듯이 IT 시스템에 의한 군사정보의 개별 처리 시간은 군사작전에서 중요한 성공 척도인 전체 군사 작전 소요 시간을 식별하기 위한 중요한 입력요소 및 분석요소가 된다.

사이버 공격에 대한 Use Case 요소는 [표 3-6]과 같이 나타낼 수 있다.

[표 3-6] 사이버 공격에 대한 Use Case 요소

Actor	Use Case	
사이버공격자  Cyber Attacker	사이버공격 	IT 시스템에 불법 접속하여 군사작전에 손상을 입히려는 행동
	사이버영향 	사이버 공격으로 유발되는 군사작전 결과의 변화
	성능저하 	사이버 공격으로 유발되는 IT 시스템의 정보 처리 속도의 지연
	중단 	사이버 공격으로 유발되는 정보 처리 기능 중단
	변조 	사이버 공격으로 유발되는 군사작전 정보의 변조
	가공 	사이버 공격의 영향으로 가공된 군사작전 정보가 전파
	감청 	사이버 공격자에게 아군의 군사 작건 정보가 유출
	무단사용 	사이버 공격자가 아군 IT 시스템의 접속 권한을 불법적으로 획득 사용
	서비스 	사이버 공격의 대상이 되는 IT 시스템을 통해 제공되는 군사작전 지원업무
	데이터 	사이버 공격의 대상이 되는 군사작전에 필요한 모든 정보

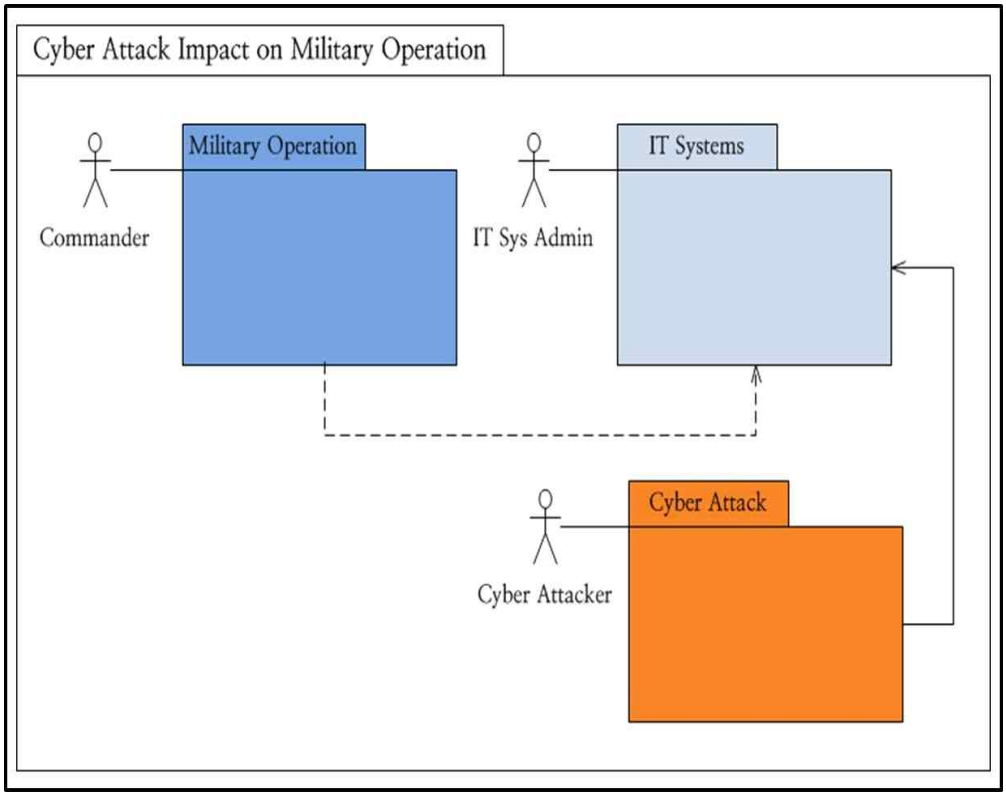
사이버 공격자는 사이버 공격을 통하여 IT 시스템의 서비스와 정보에 사이버 공격의 영향을 주고자 한다. 사이버 공격자, 사이버 공격 및 영향에 대한 Use Case 다이어그램은 〈그림 3-12〉와 같다.



〈그림 3-12〉 사이버 공격에 대한 Use Case 다이어그램

사이버 공격자는 Use Case 다이어그램의 행위자가 되며, IT 시스템에 대한 사이버 공격을 통하여 군사작전 결과에 영향을 준다. 사이버 공격의 결과인 사이버 공격 영향은 IT 시스템이 제공하는 서비스에 영향을 주어 군사정보 처리 속도를 지연시키거나 처리 중단을 초래하여 군사작전에 영향을 주는 행위와 군사작전에서 우위를 점하기 위하여 군사정보에 대한 변조, 가공 및 감청을 시도하는 행위로 구분할 수 있다. Use Case 다이어그램에서 서비스는 사이버 공격의 대상이 되는 IT 시스템을 통해 제공되는 모든 군사작전 지원 업무를 포함하고, 데이터는 군사작전에 필요한 모든 군사정보를 포함한다.

최종적으로 군사작전 시나리오는 군사작전, IT 시스템 및 사이버 공격의 상위 계층으로 패키지화하여 표현 할 수 있으며 작전 사령관, IT 관리자 및 사이버 공격자에 대한 행위 상호 관계는 〈그림 3-13〉과 같이 Use Case 다이어그램으로 나타낼 수 있다.

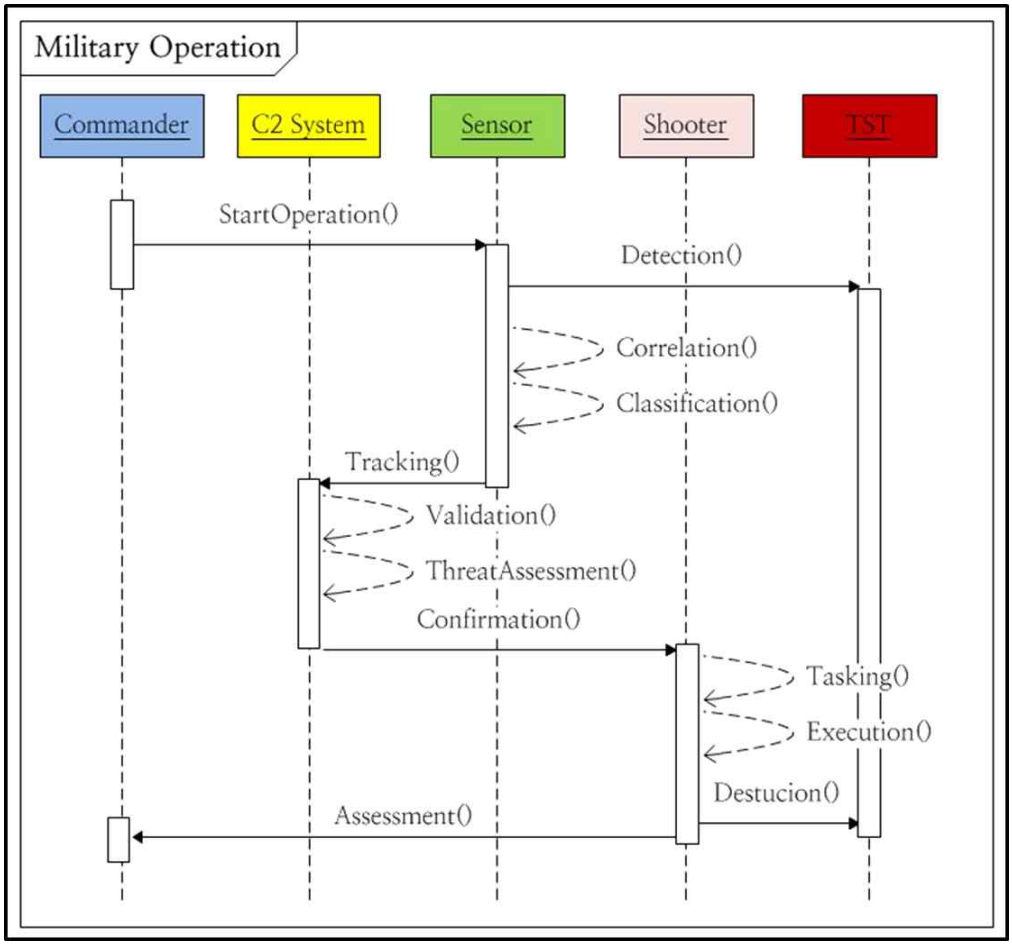


〈그림 3-13〉 사이버 공격의 영향을 포함한 Use Case 다이어그램

사이버 공격의 영향을 포함한 Use Case 다이어그램은 군사작전을 수행하기 위한 모든 시스템의 행위자와 기능을 가시적으로 표시하여 모델 개발에 대한 기반을 제공한다. Use Case 다이어그램은 모델 사용자의 관점에서 전체 모델을 구성하는 개별모델 간의 관계를 명시하여, 개별 시스템 간의 적절한 행위 범위를 이해할 수 있으며, 명확한 모델 요구 사항을 정의하고 사용자 매뉴얼을 작성하기 위한 기본 자료로 사용될 수 있다.

2. 절차(Sequence) 다이어그램

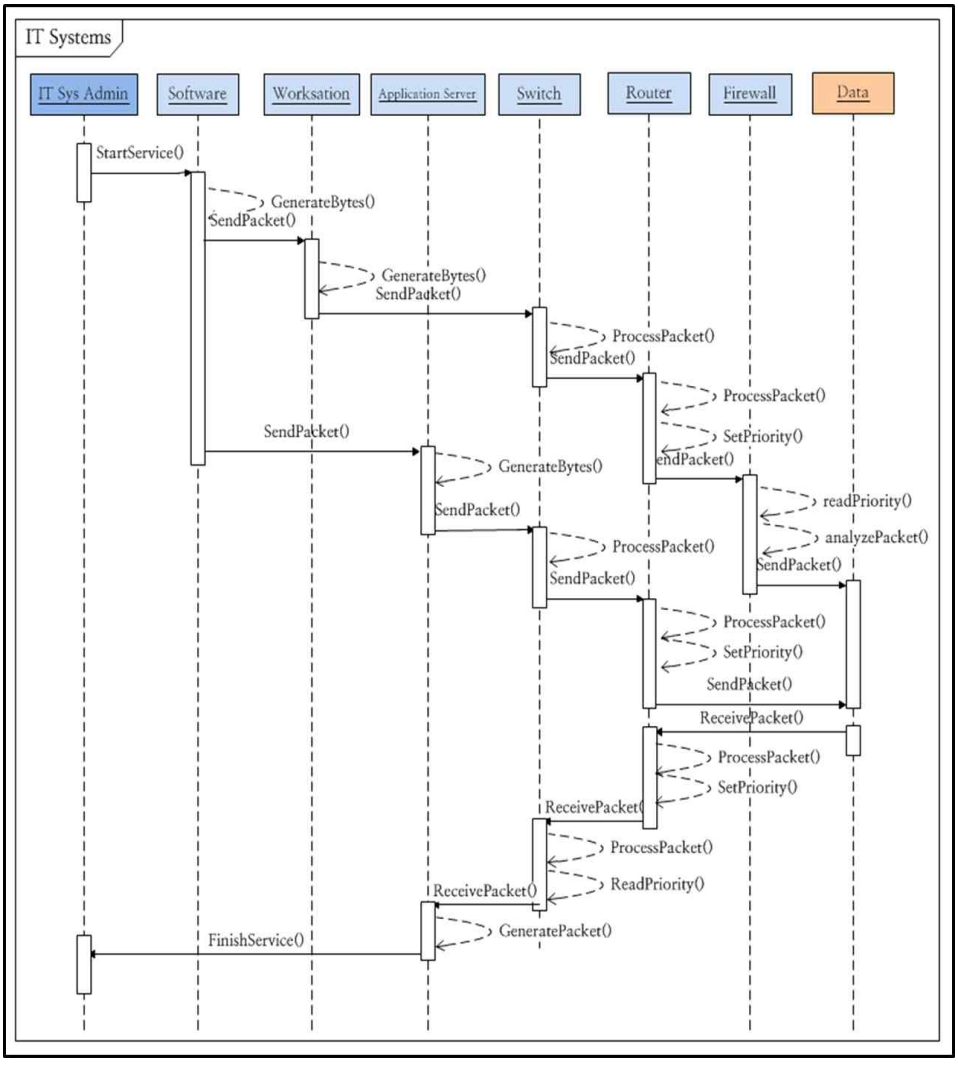
UML 절차 다이어그램은 동적인 모델링 환경에서 시스템의 동작을 이해하기 위해 객체들이 어떻게 상호작용 하는지를 메시지 순서에 초점을 맞추어 보여주는 다이어그램이다.



〈그림 3-14〉 군사작전 시나리오에 대한 절차 다이어그램

군사작전 시나리오에 대한 절차 다이어그램은 〈그림 3-14〉와 같이 지휘통제 시스템을 포함하는 타격 순환체계에 의한 시한성 긴급표적 처리 과정을 구성하는 개별 이벤트가 시간의 흐름에 따라 어떻게 상호작용하는 지를 표현한다. 절차 다이어그램은 사용자 관점의 Use Case 다이어그램과는 달리 정의된 개별 행위를 개발자의 관점에서 표현한다.

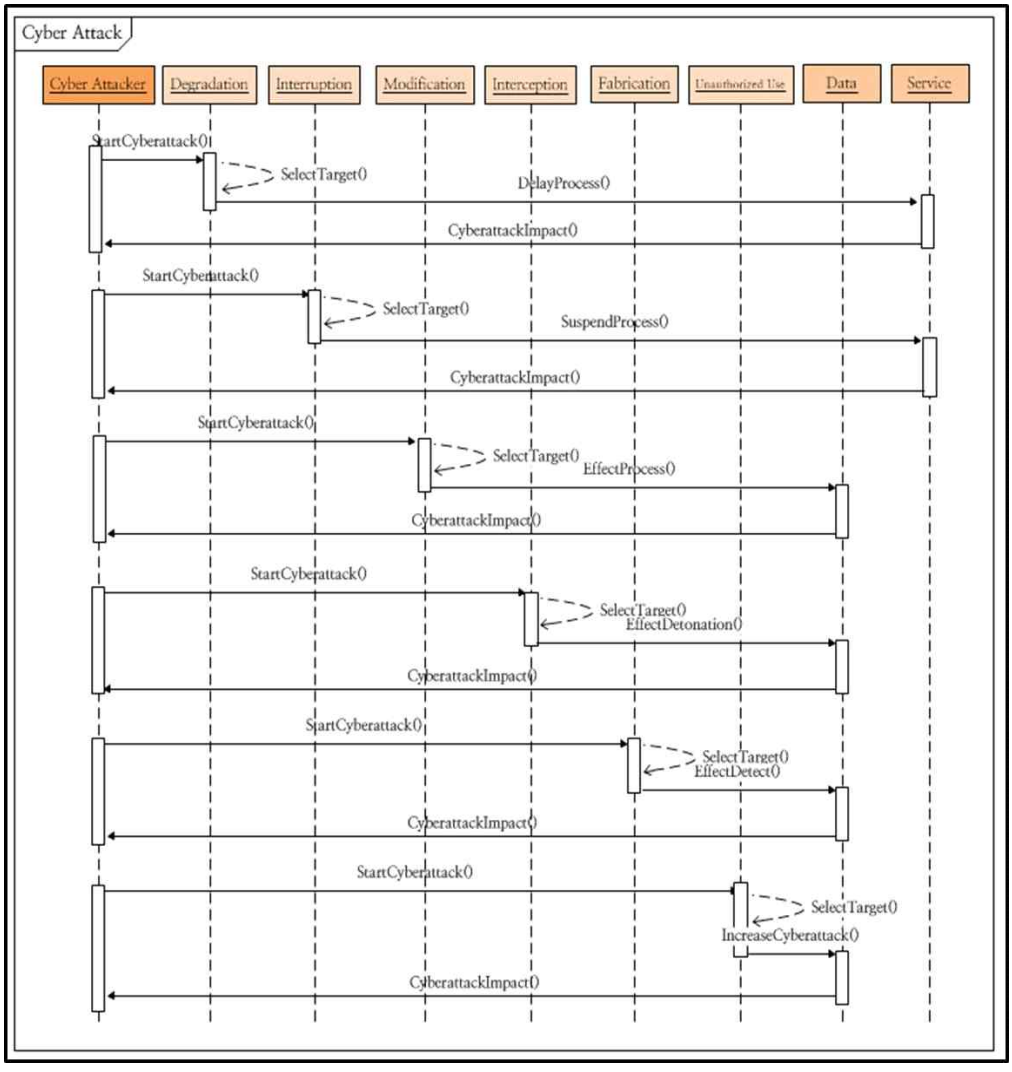
IT 시스템의 내부 프로세스는 군사 정보의 흐름에 따라 복잡하게 진행된다. 〈그림 3-15〉는 LAN 환경에서의 데이터가 생성 되고 처리되는 과정을 메시지 흐름에 따라 도식화한 절차 다이어그램이다.



〈그림 3-15〉 IT 시스템에 대한 절차 다이어그램

IT 시스템에 대한 절차 다이어그램은 관리자가 서비스 시작을 소프트웨어를 통해 요청하면 워크스테이션 및 어플리케이션 서버는 처리할 데이터를 처리하거나 생성하여 네트워크 장비에 전송하고, 네트워크 장비는 설정된 데이터의 우선순위에 따라 패킷을 분석하고 해당 시스템에 정보를 전달하는 과정을 도식화한다.

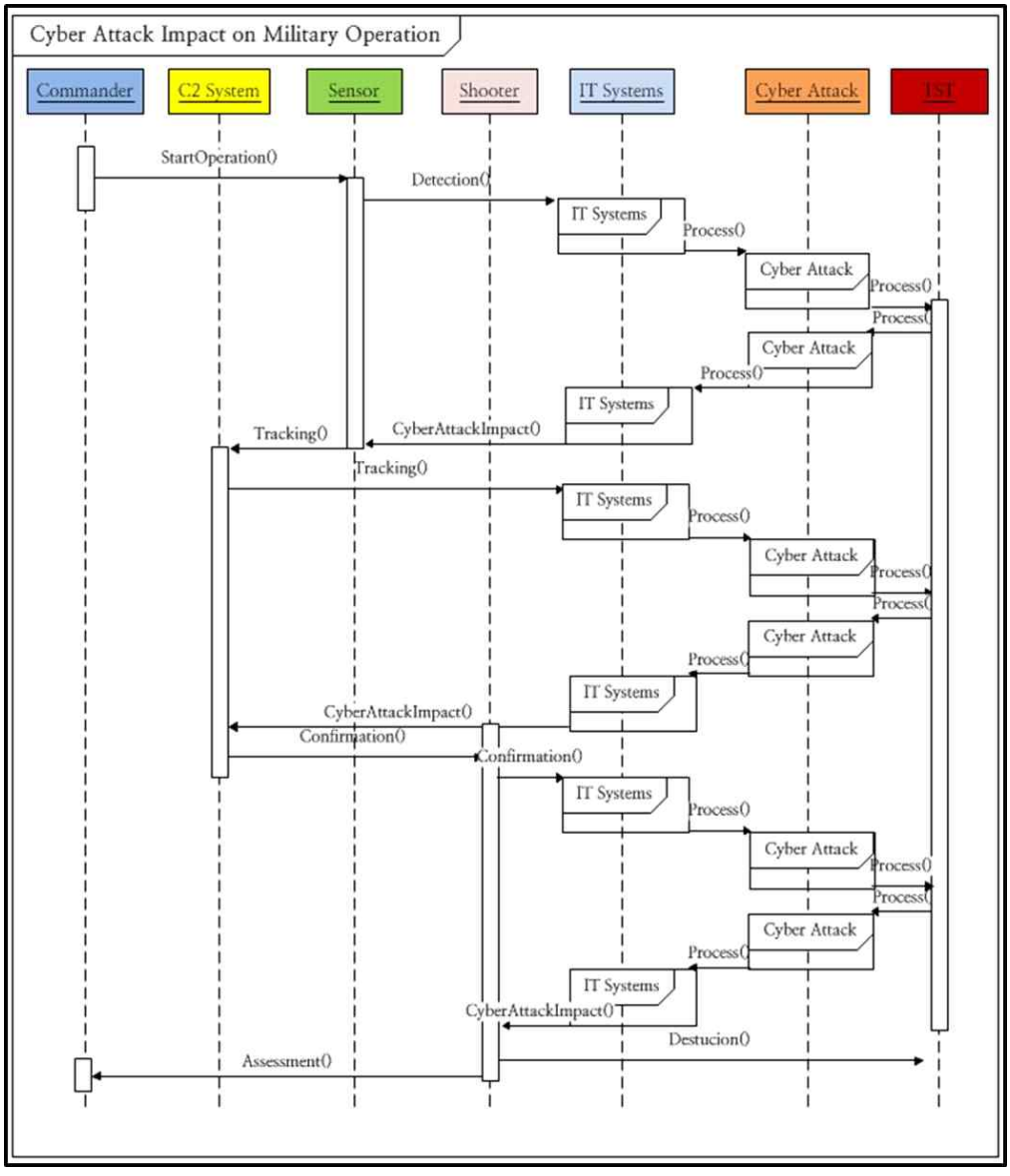
사이버 공격의 개별 범주는 〈그림 3-16〉과 같이 주어진 확률분포에 따라 확률적으로 발생하며 군사정보 또는 IT 시스템에 영향을 미친다.



〈그림 3-16〉 사이버 공격에 대한 절차 다이어그램

사이버 공격에 대한 절차 다이어그램은 사이버 공격자가 IT 시스템에 대한 사이버 공격을 통하여 서비스에 대한 성능저하 및 중단을 초래하여 전체 프로세스 시간을 증가시키는 절차와 군사정보에 대한 변조, 가공 및 감청에 의하여 사실과 다른 위조된 정보를 전파시키고 아군 군사정보를 유출시켜 전체 군사작전 프로세스에 영향을 주는 절차를 도식화하여 나타낸다.

〈그림 3-17〉은 사이버 공격의 영향을 포함하는 절차 다이어그램을 나타낸다. 군사작전 시나리오에서 IT 시스템에 대한 사이버 공격으로 인한 서비스의 지연 또는 중단은 최종 목표인 시한성 긴급표적(TST) 타격의 성공 여부에 중요한 영향을 미친다.

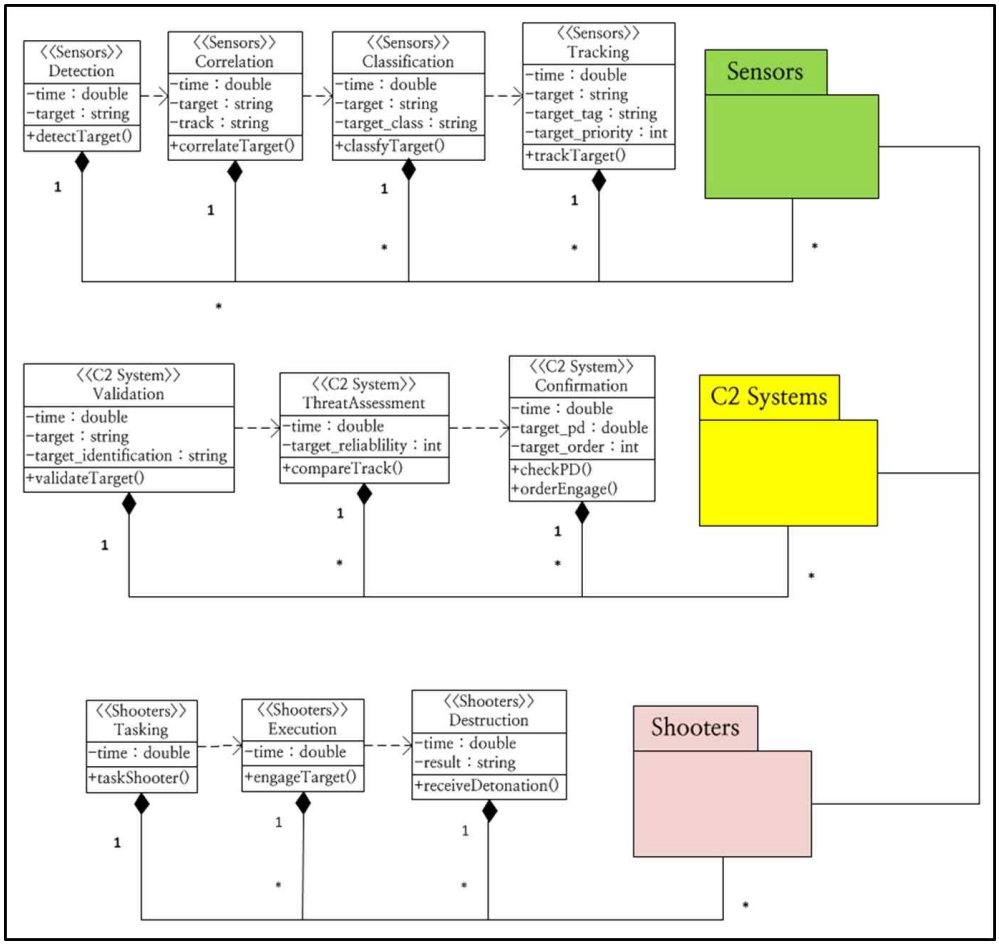


〈그림 3-17〉 사이버 공격의 영향을 포함한 절차 다이어그램

3. 클래스(Class) 다이어그램

객체지향(Object-oriented)의 개념에서 클래스는 동일한 성질을 상속받는 객체의 집합이다. 객체는 현실세계를 이해하고 설명하기 위해 복잡한 현실세계를 모델링의 목적에 부합하도록 추상화하고 단순화한 절차, 방법 기능 또는 정보를 모두 포함하는 개념이다. 클래스 다이어그램은 객체지향 방법론을 기반으로 시스템에 대한 속성이나 정보를 가시적으로 표현한 것이다.

시나리오에 대한 Use Case 다이어그램의 개별 자산 간의 행위에서 군사작전의 시스템적인 요소만을 클래스 다이어그램으로 표현하면 〈그림 3-18〉과 같다.



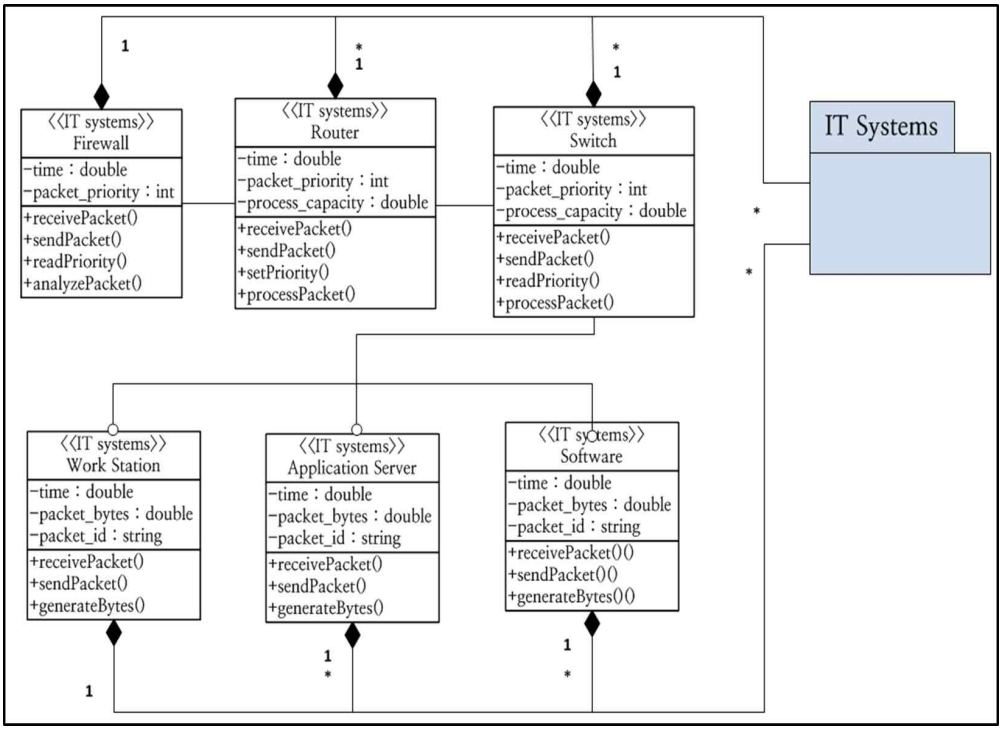
〈그림 3-18〉 군사작전 시나리오에 대한 클래스 다이어그램

군사작전 시나리오에 대한 클래스 다이어그램에서 해당 스테레오타입에 대한 클래스, 속성 및 오퍼레이션 설명은 [표 3-7]과 같다.

[표 3-7] 시나리오 군사작전에 대한 속성과 오퍼레이션

스테레오타입	클래스	속성(Attributes)	오퍼레이션	설명
Sensors	Detection	time: double target: String	detectTarget()	타격목표 탐지
	Correlation	time: double target: string track: string	correlateTarget()	트랙정보 생성
	Classification	time: double target: string target_class: string	classfyTarget()	목표 식별 및 보고
	Tracking	time: double target: string target_tag: string target_priority: int	trackTarget()	추적 정보 관리 및 보고
C2 System	Validation	time: double target: string target_identification: string	validateTarget()	탐지 정보에 대한 평가
	Threat Assessment	time: double target_reliability: int	compareTarget()	최우선 목표 선정
	Confirmation	time: double target_pd: double target_order: int	checkPD() orderEngage()	타격체계에 교전 순위 전달
Shooter	Tasking	time: double	taskShooter()	타격체계 할당
	Execution	time: double	engageTarget()	교전절차 시작
	Destruction	time: double result: string	receiveDetonation()	교전성공 확인

IT 시스템을 구성하는 개별 IT 자산의 특성과 서비스 정보를 클래스 다이어그램으로 표현하면 〈그림 3-19〉와 같다.



〈그림 3-19〉 IT 시스템의 클래스 다이어그램

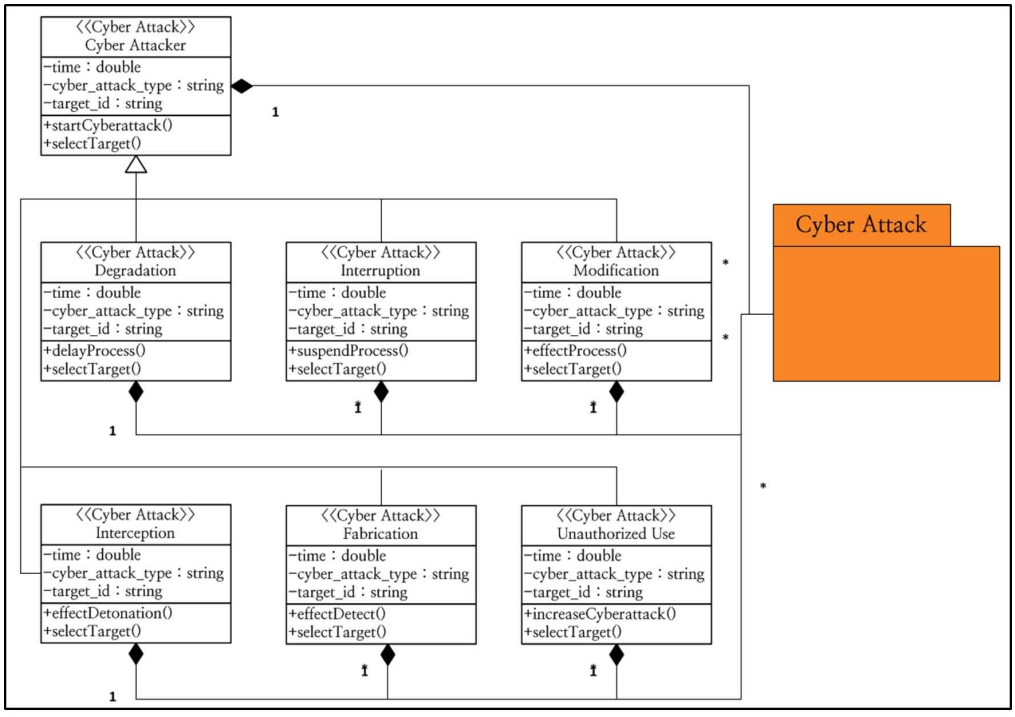
클래스 다이어그램은 개발하려는 모델에서 사용자와 통신하여 사용되는 개체 및 정보 구조를 기술한다. 클래스는 지정된 구조 또는 동작 특징을 공유하는 개체로 클래스 상속을 통해 일반화 될 수 있다. 속성은 클래스의 상태 또는 특성을 나타내며 클래스 외부에서 가져오거나 변경될 수 있다. 개별 클래스는 연관관계에 따라 서로 연결되어 있으며 인터페이스를 통하여 행위의 일부를 가시화하여 나타낸다. IT 시스템에 대한 클래스 다이어그램에는 방화벽, 라우터, 스위치, 워크스테이션, 어플리케이션 및 소프트웨어와 같이 IT 시스템을 구성하는 개별 개체에 부여된 역할에 따라 수행하는 작업을 하는 함수가 정의되어 있다. 개별 클래스 내부에는 모델 구현에 사용되는 데이터 형식이 정의되어 시스템에 사용되고 구성 요소 간에 전달되는 변수 속성에 대한 설명이 제공된다.

IT 시스템에 대한 클래스 다이어그램에서 스테레오타입에 대한 클래스, 속성 및 오퍼레이션 설명은 [표 3-8]과 같다.

[표 3-8] IT 시스템에 대한 속성과 오퍼레이션

스테레오타입	클래스	속성(Attributes)	오퍼레이션	설명
IT Systems	Firewall	time: double packet_priority: int	receivePacket() sendPacket() readPriority() analyzePacket()	패킷 수신 패킷 전송 패킷 판독 패킷 분석
	Router	time: double packet_priority: int process_capacity: double	receivePacket() sendPacket() setPriority() processPacket()	패킷 수신 패킷 전송 우선순위 설정 패킷 처리
	Switch	time: double packet_priority: int process_capacity: double	receivePacket() sendPacket() readPriority() processPacket()	패킷 수신 패킷 전송 우선순위 판독 패킷 처리
	Workstation	time: double packet_bytes: double packet_id: string	receivePacket() sendPacket() generateBytes()	패킷 수신 패킷 전송 바이트 발생
	Application Server	time: double packet_bytes: double packet_id: string	receivePacket() sendPacket() generateBytes()	패킷 수신 패킷 전송 바이트 발생
	Software	time: double packet_bytes: double packet_id: string	receivePacket() sendPacket() generateBytes()	패킷 수신 패킷 전송 바이트 발생

사이버 공격으로 인한 시스템 효과에 대한 특성과 결과 정보를 클래스 다이어그램으로 표현하면 〈그림 3-20〉과 같다.



〈그림 3-20〉 사이버 공격에 대한 클래스 다이어그램

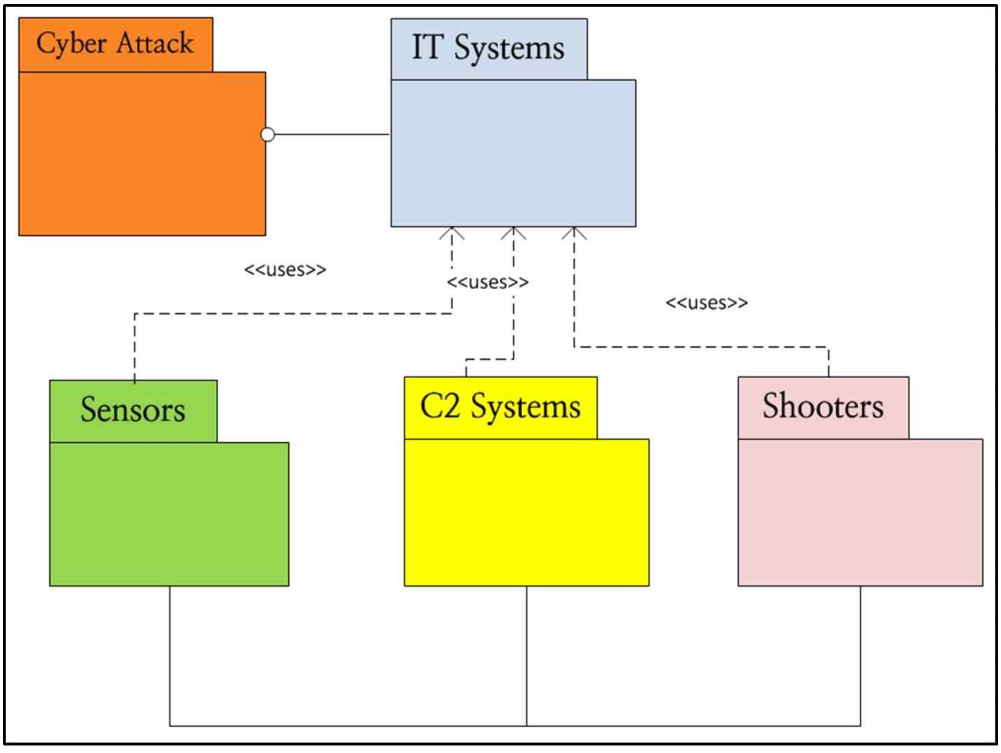
사이버 공격에 대한 모델 구현을 위한 클래스 다이어그램에서는 사이버 공격에 대한 범주를 클래스로 정의하고 함수를 통해 오퍼레이션을 정의한다. 속성은 클래스의 구조를 표현하여 모델 구현에 필요한 데이터베이스 정보를 제공한다. 개별 클래스를 연결한 실선을 통하여 클래스 간에 존재하는 관계를 표현한다. 클래스 다이어그램에서 화살표는 일반화 및 특수화의 관계를 나타내는 상속관계를 표현하며, 실선은 두 클래스의 관련성을 나타내는 연관관계를 표현한다. 전체와 부분의 관계를 나타내는 집합연관 관계의 경우에는 마름모 형태를 가진 실선으로 표기한다. 사이버 공격의 결과를 도출하기 위해 정의된 함수의 기능은 의존관계 또는 연관관계에 있는 외부 클래스에 참조되어 전체 프로세스의 처리 결과에 영향을 준다.

사이버 공격에 대한 클래스 다이어그램에서 스테레오타입에 대한 클래스, 속성 및 오퍼레이션 설명은 [표 3-9]와 같다.

[표 3-9] 사이버 공격에 대한 속성과 오퍼레이션

스테레오타입	클래스	속성(Attributes)	오퍼레이션	설명
Cyber Attack	Cyber Attacker	time: double cyber_attack_type: string target_id: string	selectTarget() startCyberattack()	공격 목표 선택 공격 시작
	Degradation	time: double cyber_attack_type: string target_id: string	selectTarget() delayProcess()	공격 목표 선택 프로세스 지연
	Interruption	time: double cyber_attack_type: string target_id: string	selectTarget() suspendProcess()	공격 목표 선택 프로세스 중단
	Modification	time: double cyber_attack_type: string target_id: string	selectTarget() effectProcess()	공격 목표 선택 전체 프로세스 영향
	Interception	time: double cyber_attack_type: string target_id: string	selectTarget() effectDetonation()	공격 목표 선택 교전 프로세스 영향
	Fabrication	time: double cyber_attack_type: string target_id: string	selectTarget() effectDetect()	공격 목표 선택 탐지 프로세스 영향
	Unauthorized Use	time: double cyber_attack_type: string target_id: string	selectTarget() increaseCyberattack()	공격 목표 선택 공격 발생률 증가

마지막으로 시나리오 군사작전에서 사이버 공격으로 인한 IT 시스템 성능 변화에 대한 전체 효과도 평가를 위한 클래스 다이어그램은 〈그림 3-21〉과 같이 패키지화하여 표현할 수 있다.



〈그림 3-21〉 사이버 공격의 영향을 포함한 클래스 다이어그램

UML에 기반을 둔 4+1 뷰(View) 모델을 적용하면 개발할 모델의 아키텍처를 다양한 관점에서 정의할 수 있다. 뷰는 이해당사자에 따라 구현하려는 시스템을 바라보는 관점으로 정의된다. Use Case 다이어그램은 모델에 대한 요구 기능을 사용자의 관점에서 가시적으로 표현하여 개발자가 모델을 개발하기 위한 기반을 제공한다. 구조뷰의 관점은 사용자에게 서비스를 제공하기 위한 시스템의 구조와 상호관계를 나타내기 위해 사용된다. 행위뷰의 관점을 통해서는 합리적인 개발 범위를 설정하고, 모델을 구성하는 내부 시스템의 동작 내용을 사전에 정의한다. 구현뷰의 관점은 최종 개발 모델의 형식을 정의하여 모델의 배포 및 형상 관리를 할 수 있도록 지원한다. 최종적으로 환경뷰의 관점을 통하여 모델의 설치 및 운용환경을 제시한다.

제 4 장 사이버 공격 영향 평가 모델 구현

제 1 절 시뮬레이션 소프트웨어

운영시스템에 대한 시뮬레이션 모델은 대부분의 경우에 처음부터 프로그래밍 언어를 통해 개발되기 보다는 모델링에 특화된 시뮬레이션 소프트웨어를 활용하여 개발된다. 시뮬레이션 소프트웨어는 정확하고 신뢰할 수 있는 모델을 개발할 수 있도록 다양한 도구와 환경을 제공한다.[23)]

본 논문에서는 일반적인 모델 구현을 위하여 개발의 편의성, 모델링 요구사항에 따른 적합성, 결과 분석을 위한 그래픽 도구 지원, 모델 데이터 관리를 위한 데이터베이스 설계 지원, 프로그래밍을 통한 사용자 정의 및 이산사건 모델링 환경 지원 여부를 고려하여 ExtendSim을 모델링 소프트웨어로 선택하여 활용하였다.

1. ExtendSim 개요

ExtendSim은 연속(Continuous), 이산사건(Discrete Event) 및 이산비율(Discrete Rate) 프로세스 모델링을 모두 지원하는 Imagine That 사에서 1988년에 개발한 시뮬레이션 프로그램이다.[24)]

ExtendSim에서 모델은 라이브러리(Library) 기반의 아이콘 블록(Icon Block)과 C++의 기능을 강화한 ModL 프로그래밍 언어를 통해 구현된다. ExtendSim 라이브러리는 사건(Event)의 대기(Queue), 동작(Activity), 경로(Routing), 배칭(Batching), 특성(Properties) 및 리소스(Resources)를 처리하는 아이템(Item) 블록과 연산(Math), 입력, 출력 및 통계의 값을 처리하는 벨류(Value) 블록을 제공한다. 벨류 블록은 아이템의 속성을 변경하거나 시뮬레이션 과정에서 모델의 동작을 변화시키는 역할을 한다. 개별 블록은 전체 프로세스에서 단일 프로세스의 연산 및 동작을 정의하고, 개별 블록을 연결하여 전체 프로세스를 구현한다. 블록 다이얼로그(Dialog)를 통해 자료를 입력하거나 결과에 대한 출력을 지원하고

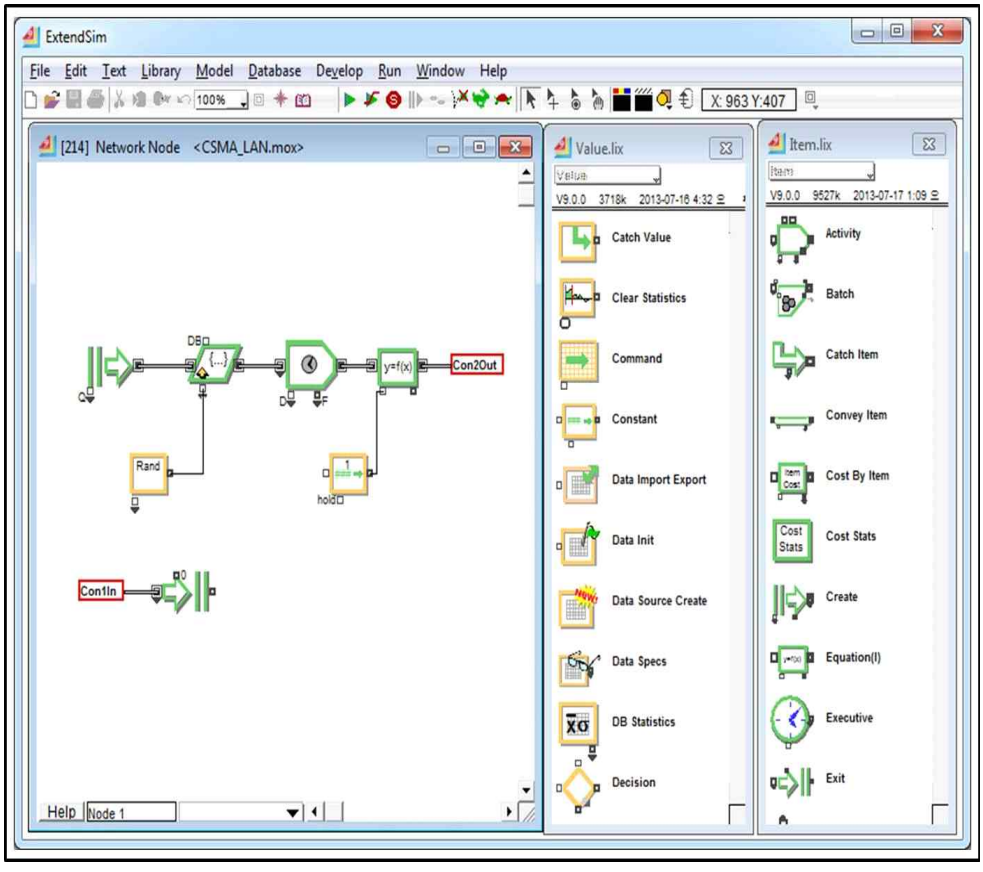
23) Stewart Robinson, 『The Practice of Model Development and Use』, John Wiley & Sons, Ltd, 2004, P13

24) 『ExtendSim User Guide Release 9』, ImageThat, 2013

ModL 언어를 활용하여 블록의 기능을 강화하거나 새로운 사용자 정의 블록을 생성할 수 있다. ExtendSim에 제공하는 프로그래밍 언어인 ModL을 활용하면 단일 블록에서 다수의 프로세스를 처리하거나 데이터에 대한 연산을 수행할 수 있어 복잡한 모델 개발에 활용될 수 있다.

ExtendSim 모델에서 다수의 블록은 하나의 블록으로 통합되어 단일 계층(Hierarchical) 블록으로 나타낼 수 있다. 계층 블록을 활용하면 복잡한 모델을 기능별로 단순하게 표현하여 사용자 및 개발자에게 모델 구성과 기능별 동작의 이해를 쉽게 한다.

〈그림 4-1〉은 ExtendSim의 실행 화면으로 실제 모델 개발을 작업 화면과 모델 개발에서 개별 개체로 사용되는 아이템 라이브러리를 나타낸다.



〈그림 4-1〉 ExtendSim 개발 화면

2. ExtendSim 블록 모듈

본 논문에서 사용된 대표적인 아이템 블록의 설명은 [표 4-1]과 같다. 개별 아이콘 블록을 연결하여 요구기능을 수행하는 모델을 구성한다.

[표 4-1] ExtendSim 아이템 블록

명칭	아이콘	기능
Create Item		일정한 시간 간격이나 확률적으로 아이템을 발생하는 블록
Exit		모델의 실행을 종료하는 블록
Workstation		Queue 블록과 Activity 블록으로 구성되어 아이템을 대기시키고 조건에 따라 실행하는 블록
Queue Equation		동작을 일정 조건에 따라 일시 정지시키는 블록
Select Item Out		입력 아이템 중에 조건에 맞는 아이템을 선택하거나 병합하여 전송시키는 블록
Select Item In		입력 아이템을 여러 블록으로 전송시키는 블록
Set		입력 아이템에 속성을 입력하는 블록
Get		아이템의 지정된 속성을 입력받는 블록
Equation(I)		ModL 언어를 통해 아이템을 처리하거나 다른 블록의 기능을 실행하는 블록
Information		아이템에 대한 정보를 보고하는 블록
Catch Item		Throw 블록으로부터 아이템을 전송받는 블록
Throw Item		아이템 속성에 따라 직접적인 연결 없이 다른 블록으로 전송하는 블록
Resource Pool		아이템을 활용할 수 있도록 저장하는 블록

Create Item 블록을 통해 아이템을 발생 시키며 Read 및 Write 블록을 활용하여 결과를 모델 내부 데이터베이스에 저장한다. Random Number 블록은 다양한 확률분포를 선택하여 입력할 수 있게 지원한다. 실행횟수 및 시간 단위와 같은 시뮬레이션 환경은 Simulation Variable 블록을 이용하여 설정한다. Equation 블록을 활용하면 프로그래밍을 통해 아이템에 대한 연산을 수행하거나, 모델 데이터베이스를 관리할 수 있다. Queue Equation 블록은 아이템의 진행을 일정 조건에 따라 일시 정지 시키는 기능을 수행하여 프로세스의 지연이나 처리시간을 표현하기 위해 사용될 수 있다.

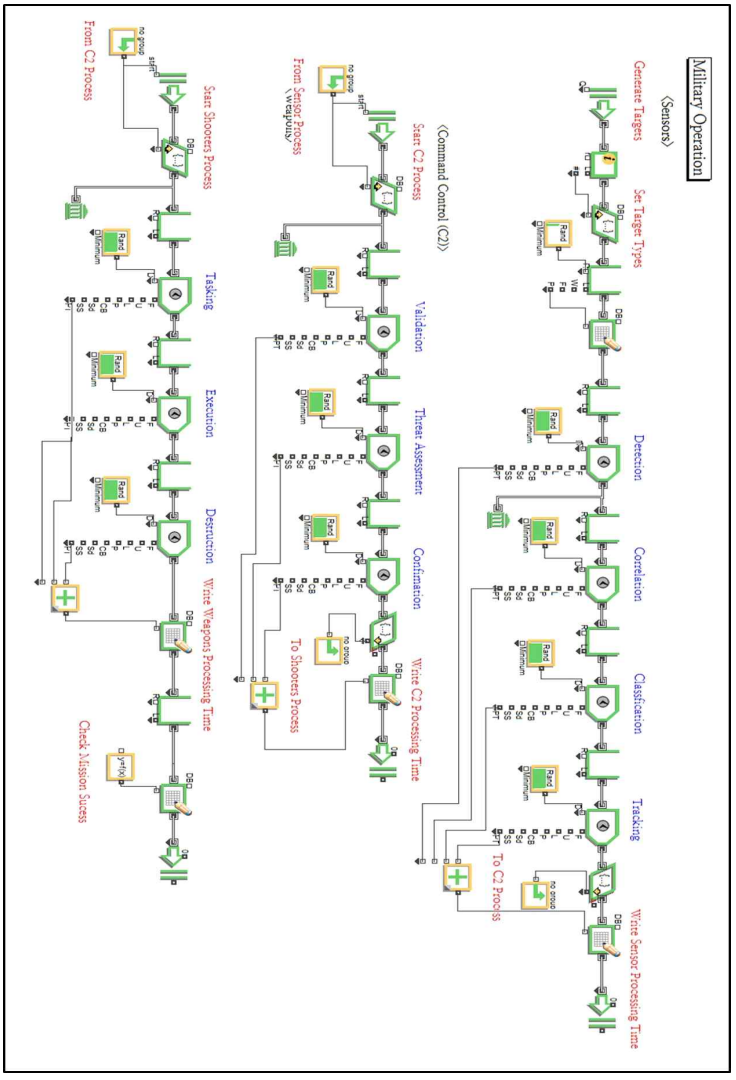
본 논문에서 사용된 대표적인 벨류 블록의 설명은 [표 4-2]와 같다.

[표 4-2] ExtendSim 벨류 블록

명칭	아이콘	기능
Random Number		정의된 확률함수에 따른 값을 발생시키는 블록
Simulation Variable		시뮬레이션과 관련된 변수를 출력하는 블록
Read		데이터를 내부 데이터베이스로부터 읽어오는 블록
Write		데이터를 내부 데이터베이스에 기록하는 블록
Equation		방정식 또는 수학 공식을 통해 값을 계산하는 블록
Lookup Table		아이템의 상태를 표시하는 블록
Data Import Export		모델 데이터베이스로부터 지정된 보고서를 출력하는 블록
Constant		상수 값을 입력시키는 블록

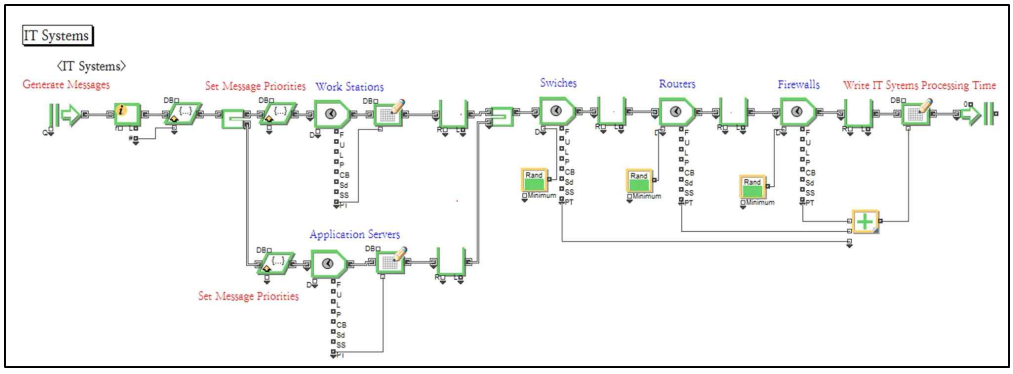
제 2 절 시뮬레이션 모델

군사작전에 대한 시뮬레이션 모델은 〈그림 4-2〉와 같이 구현된다. 각 블록은 4+1 모델 표현을 통해 설계된 기능을 구현한다. 모델에서 탐지자산을 통해 탐지된 타격 목표를 처리하는데 소요되는 최종 시간은 평균과 표준편차 시간을 입력 파라미터로 하는 로그정규분포에 따른 개별 프로세스 지연시간의 합계에 의해 계산된다.



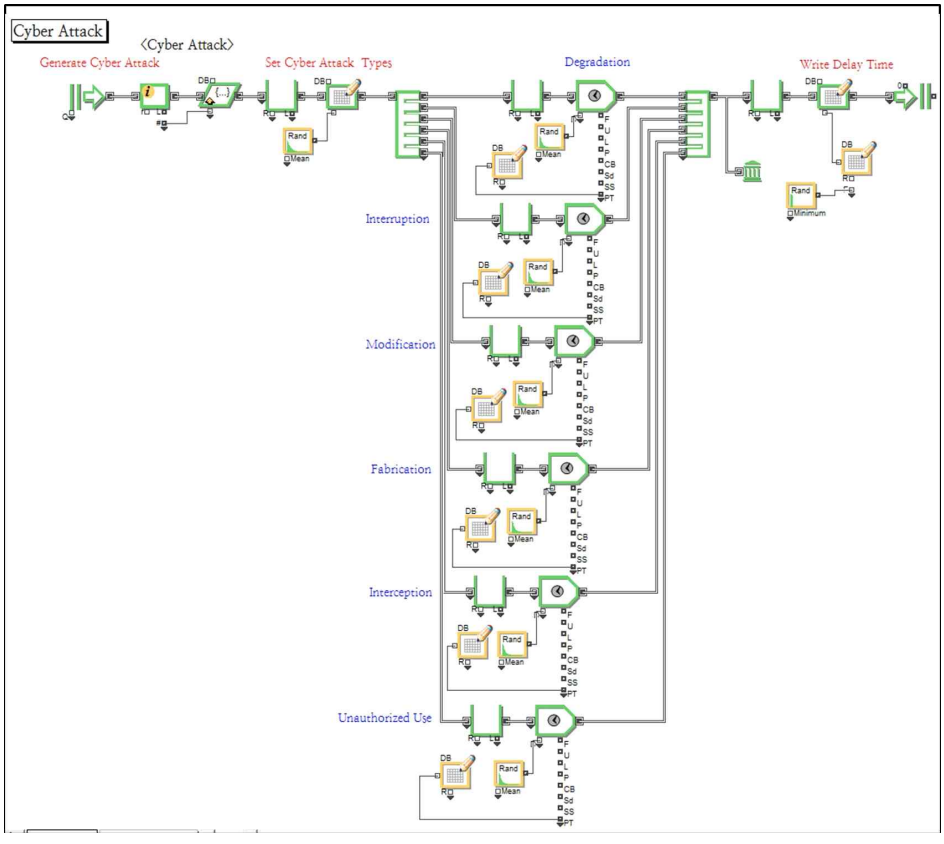
〈그림 4-2〉 군사작전에 대한 ExtendSim 모델

IT 시스템에 대한 시뮬레이션 모델은 설계된 아키텍처를 기반으로 〈그림 4-3〉과 같이 구현된다.



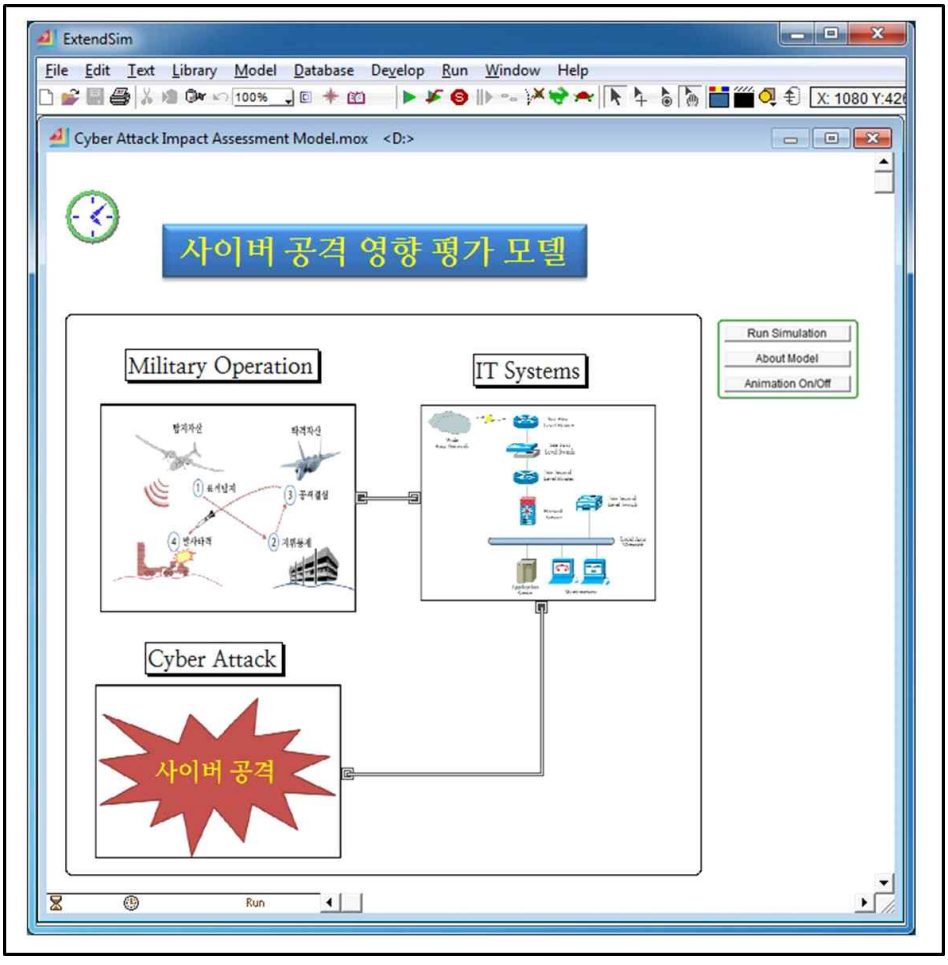
〈그림 4-3〉 IT 시스템에 대한 ExtendSim 모델

사이버 공격에 대한 시뮬레이션 모델은 〈그림 4-4〉와 같이 구현된다.



〈그림 4-4〉 사이버 공격에 대한 ExtendSim 모델

최종적으로 계층화 모델(Hierarchical Model) 표현 방법을 이용한 사이버 공격이 군사작전에 미치는 영향 분석을 위한 모델은 〈그림 4-5〉와 같이 구현된다. 사이버 공격 영향 평가 모델은 군사작전에 대한 프로세스모델, 표준 IT 시스템 구현 모델 및 사이버 공격 모델로 구성되어 있다. 사이버 공격 모델에서 확률분포에 의해 발생한 사이버 공격은 IT 시스템의 성능에 영향을 주어 전체 군사 작전 프로세스 시간을 지연시킨다.



〈그림 4-5〉 사이버 공격에 대한 영향 평가 모델

계층화 모델을 활용하면 모델 구성의 복잡성이 감소되어 사용자는 모델구성을 쉽게 이해할 수 있고, 개발자는 컴포넌트화한 표현을 통해 모델 성능의 개선과 문제해결을 쉽게 할 수 있다.

제 3 절 시뮬레이션 결과 분석

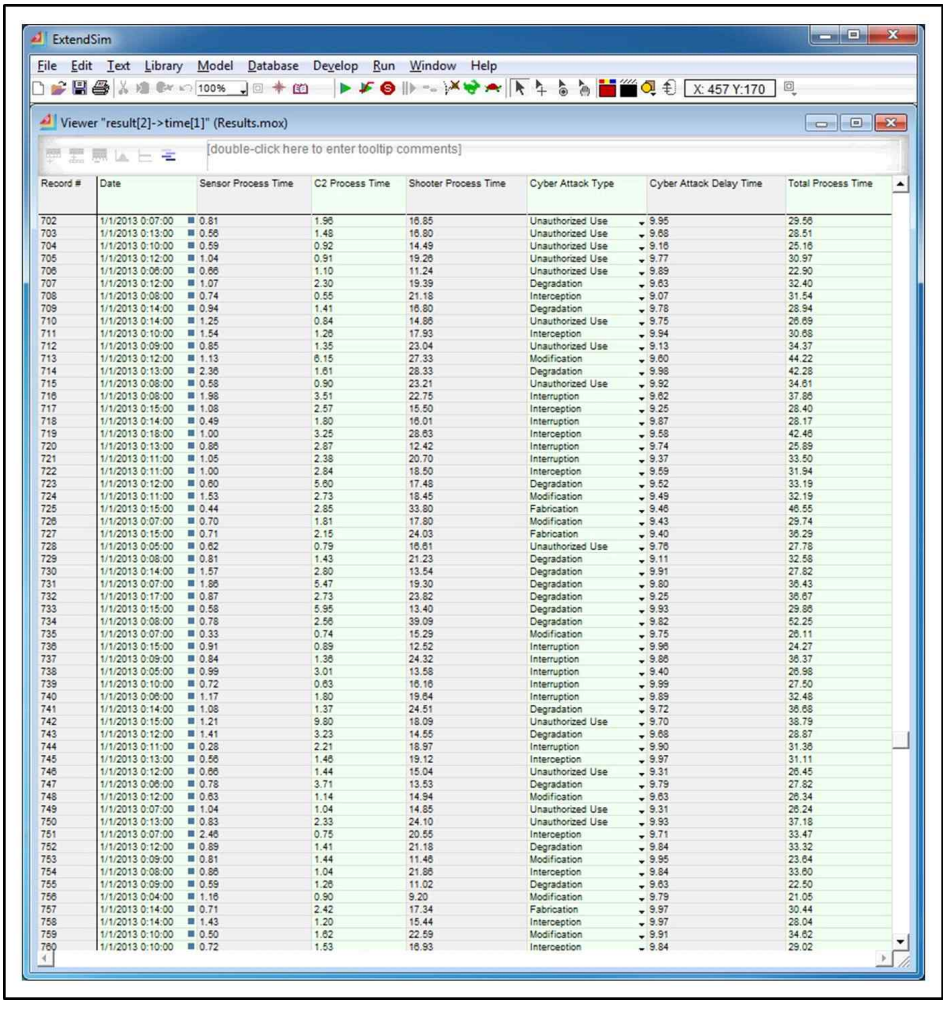
본 논문에서 제안한 모델을 이용한 시뮬레이션을 위해 사용된 군사작전 시나리오의 입력 파라미터는 [표 4-3]과 같다. 실험은 모델 요구 조건에서 식별된 분석지수를 측정 할 수 있도록 군사정보의 처리시간과 사이버 공격의 지속시간에 대한 입력 값을 변경시키면서 실험을 실시하였다.

[표 4-3] 시나리오 시뮬레이션 구성

구분	내용	입력 파라미터 (단위: 분)						목표 처리 시간
		시나리오1		시나리오2		시나리오3		
		평균	표준 편차	평균	표준 편차	평균	표준 편차	
탐지자산 (Sensors)	탐지 (Detection)	0.2	0.2	0.4	0.2	0.7	0.2	2분
	상관 (Correlation)	0.2	0.2	0.4	0.2	0.7	0.2	
	분류 (Classification)	0.3	0.3	0.6	0.3	0.8	0.3	
	추적 (Tasking)	0.3	0.3	0.6	0.3	0.8	0.3	
지휘통제 (C2 System)	평가 (Validation)	1.0	1.0	1.5	1.0	2.0	1.0	3분
	위협평가 (Threat Assessment)	0.5	0.5	0.7	0.5	1.0	0.5	
	타격명령 (Confirmation)	0.5	0.5	0.8	0.5	1.0	0.5	
타격자산 (Shooters)	할당 (Tasking)	8.0	4.0	10.0	4.0	12.0	4.0	25분
	실행 (Execution)	8.0	4.0	10.0	4.0	11.0	4.0	
	파괴 (Destruction)	4.0	2.0	5.0	2.0	7.0	2.0	
실험계획	• 사이버 공격이 발생 하지 않을 시 전체 군사작전 프로세스 시간 측정 • 사이버 공격이 지속 시간을 1분 단위로 증가시키며 전체 군사작전 프로세스 시간에 따른 성공률을 측정 (성공 기준: 30분) - 실험 반복 횟수 1000회 • 군사작전 프로세스는 확률변수를 로그정규분포 사용 • 사이버 공격 지속시간의 확률변수는 삼각분포 사용 • 입력 파라미터는 공개된 데이터 및 예측 데이터를 사용							

기본 시나리오1의 입력 파라미터는 공개된 자료를 참조하여 타격순환체계를 통한 시한성 긴급표적 처리 과정의 전체 목표 시간을 30분으로 가정하고 작성하였다. 추가 시나리오 2와 3은 모델 입력 파라미터에 따른 시뮬레이션 결과 변화의 실험적 차이점 분석을 위하여 전체 목표 시간을 7분 간격으로 증가시켜 작성하였다. 기본 시나리오와 추가 시나리오의 결과 분석을 통하여 모델의 성능을 검증하고 활용방안을 제시한다.

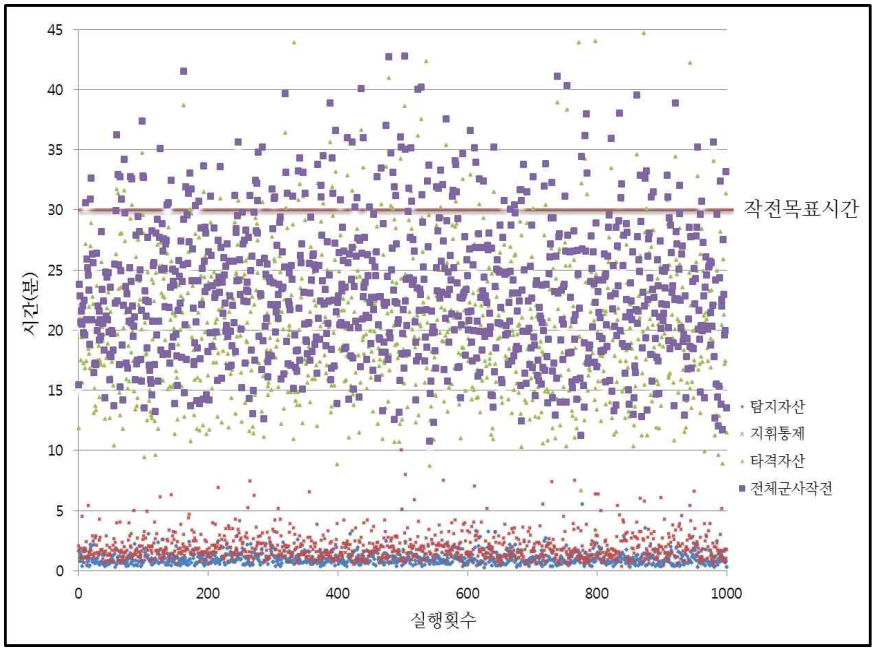
확률적으로 발생한 사이버 공격 형태를 포함한 시나리오에 따른 시뮬레이션 결과는 모델 내부에 설계된 데이터베이스에 〈그림 4-6〉과 같이 저장되어 분석에 활용될 수 있다.



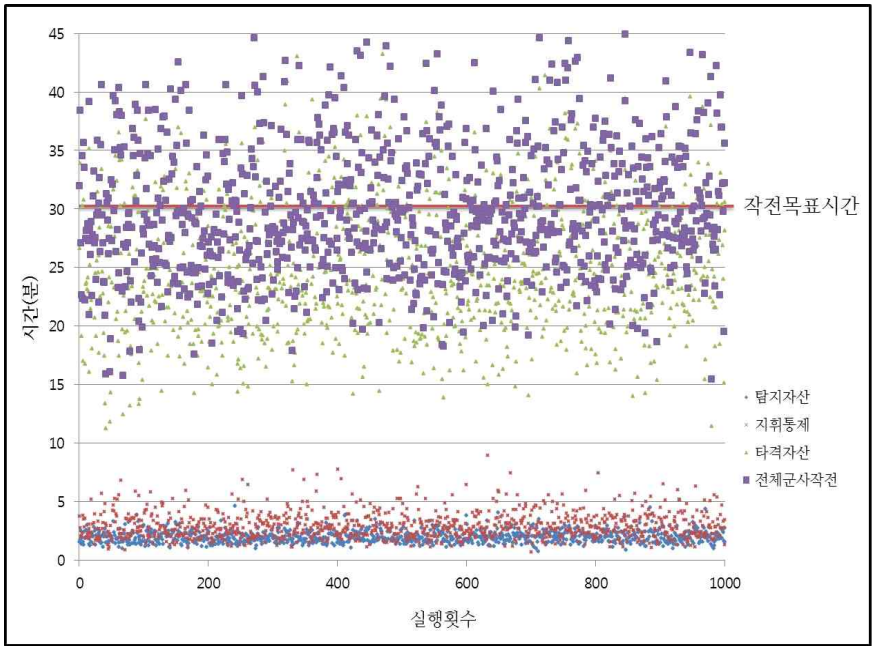
Record #	Date	Sensor Process Time	C2 Process Time	Shooter Process Time	Cyber Attack Type	Cyber Attack Delay Time	Total Process Time
702	1/1/2013 0:07:00	0.81	1.96	16.85	Unauthorized Use	9.95	29.56
703	1/1/2013 0:13:00	0.56	1.48	16.80	Unauthorized Use	9.68	28.51
704	1/1/2013 0:10:00	0.59	0.92	14.49	Unauthorized Use	9.16	25.16
705	1/1/2013 0:12:00	1.04	0.91	19.26	Unauthorized Use	9.77	30.97
706	1/1/2013 0:06:00	0.66	1.10	11.24	Unauthorized Use	9.89	22.90
707	1/1/2013 0:12:00	1.07	2.30	19.39	Degradation	9.63	32.40
708	1/1/2013 0:08:00	0.74	0.55	21.18	Interception	9.07	31.54
709	1/1/2013 0:14:00	0.94	1.41	16.80	Degradation	9.78	28.94
710	1/1/2013 0:14:00	1.25	0.84	14.86	Unauthorized Use	9.75	26.69
711	1/1/2013 0:10:00	1.54	1.26	17.93	Interception	9.94	30.68
712	1/1/2013 0:09:00	0.85	1.35	23.04	Unauthorized Use	9.13	34.37
713	1/1/2013 0:12:00	1.13	6.15	27.33	Modification	9.60	44.22
714	1/1/2013 0:13:00	2.36	1.61	28.33	Degradation	9.98	42.28
715	1/1/2013 0:08:00	0.58	0.90	23.21	Unauthorized Use	9.92	34.61
716	1/1/2013 0:08:00	1.98	3.51	22.75	Interruption	9.62	37.86
717	1/1/2013 0:15:00	1.08	2.57	15.50	Interception	9.25	28.40
718	1/1/2013 0:14:00	0.49	1.80	16.01	Interruption	9.87	28.17
719	1/1/2013 0:18:00	1.00	3.25	28.63	Interception	9.58	42.46
720	1/1/2013 0:13:00	0.86	2.87	12.42	Interruption	9.74	25.89
721	1/1/2013 0:11:00	1.05	2.38	20.70	Interruption	9.37	33.50
722	1/1/2013 0:11:00	1.00	2.84	18.50	Interception	9.59	31.94
723	1/1/2013 0:12:00	0.60	5.60	17.48	Degradation	9.52	33.19
724	1/1/2013 0:11:00	1.53	2.73	18.45	Modification	9.49	32.19
725	1/1/2013 0:15:00	0.44	2.85	33.80	Fabrication	9.46	46.55
726	1/1/2013 0:07:00	0.70	1.81	17.80	Modification	9.43	29.74
727	1/1/2013 0:15:00	0.71	2.15	24.03	Fabrication	9.40	36.29
728	1/1/2013 0:05:00	0.62	0.79	16.61	Unauthorized Use	9.76	27.78
729	1/1/2013 0:08:00	0.81	1.43	21.23	Degradation	9.11	32.58
730	1/1/2013 0:14:00	1.57	2.80	13.54	Degradation	9.91	27.82
731	1/1/2013 0:07:00	1.86	5.47	19.30	Degradation	9.80	36.43
732	1/1/2013 0:17:00	0.87	2.73	23.82	Degradation	9.25	36.67
733	1/1/2013 0:15:00	0.58	5.95	13.40	Degradation	9.93	29.86
734	1/1/2013 0:08:00	0.78	2.56	39.09	Degradation	9.82	52.25
735	1/1/2013 0:07:00	0.33	0.74	15.29	Modification	9.75	26.11
736	1/1/2013 0:15:00	0.91	0.89	12.52	Interruption	9.96	24.27
737	1/1/2013 0:09:00	0.84	1.36	24.32	Interruption	9.86	36.37
738	1/1/2013 0:05:00	0.99	3.01	13.58	Interruption	9.40	26.98
739	1/1/2013 0:10:00	0.72	0.63	16.16	Interruption	9.99	27.50
740	1/1/2013 0:06:00	1.17	1.80	19.64	Interruption	9.89	32.48
741	1/1/2013 0:14:00	1.08	1.37	24.51	Degradation	9.72	36.68
742	1/1/2013 0:15:00	1.21	9.80	18.09	Unauthorized Use	9.70	38.79
743	1/1/2013 0:12:00	1.41	3.23	14.55	Degradation	9.68	28.87
744	1/1/2013 0:11:00	0.28	2.21	18.97	Interruption	9.90	31.36
745	1/1/2013 0:13:00	0.56	1.46	19.12	Interception	9.97	31.11
746	1/1/2013 0:12:00	0.66	1.44	15.04	Unauthorized Use	9.31	26.45
747	1/1/2013 0:06:00	0.78	3.71	13.53	Degradation	9.79	27.82
748	1/1/2013 0:12:00	0.63	1.14	14.94	Modification	9.63	26.34
749	1/1/2013 0:07:00	1.04	1.04	14.85	Unauthorized Use	9.31	26.24
750	1/1/2013 0:13:00	0.83	2.33	24.10	Unauthorized Use	9.93	37.18
751	1/1/2013 0:07:00	2.46	0.75	20.55	Interception	9.71	33.47
752	1/1/2013 0:12:00	0.89	1.41	21.18	Degradation	9.84	33.32
753	1/1/2013 0:09:00	0.81	1.44	11.46	Modification	9.95	23.64
754	1/1/2013 0:08:00	0.86	1.04	21.86	Interception	9.84	33.60
755	1/1/2013 0:09:00	0.59	1.26	11.02	Degradation	9.63	22.50
756	1/1/2013 0:04:00	1.16	0.90	9.20	Modification	9.79	21.05
757	1/1/2013 0:14:00	0.71	2.42	17.34	Fabrication	9.97	30.44
758	1/1/2013 0:14:00	1.43	1.20	15.44	Interception	9.97	28.04
759	1/1/2013 0:10:00	0.50	1.62	22.59	Modification	9.91	34.62
760	1/1/2013 0:10:00	0.72	1.53	16.93	Interception	9.84	29.02

〈그림 4-6〉 사이버 영향 평가 모델 시뮬레이션 결과 화면

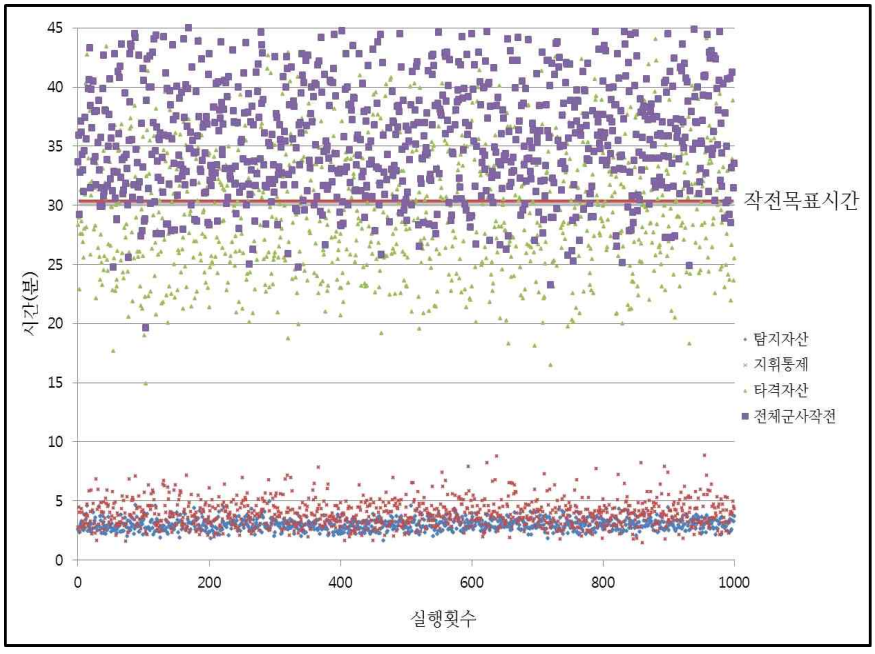
사이버 공격의 영향을 고려하지 않은 개별 시나리오의 입력 파라미터에 따른 시뮬레이션 결과는 〈그림 4-7〉, 〈그림 4-8〉 및 〈그림 4-9〉와 같다.



〈그림 4-7〉 시나리오1에 대한 군사작전 시뮬레이션 결과



〈그림 4-8〉 시나리오2에 대한 군사작전 시뮬레이션 결과



〈그림 4-9〉 시나리오3에 대한 군사작전 시뮬레이션 결과

사이버 공격의 영향이 없을 경우에 타격순환체계에 따른 시한성 긴급표적 처리를 위한 평균 소요시간은 각각 평균 23.4분, 29.9분 및 36.8분이었다.

타격순환체계의 목표시간인 30분을 군사작전의 성공기준으로 가정하면 시뮬레이션 시나리오에 대한 군사작전 성공률은 85.7%, 57.6% 및 10.4%로 판단할 수 있다.

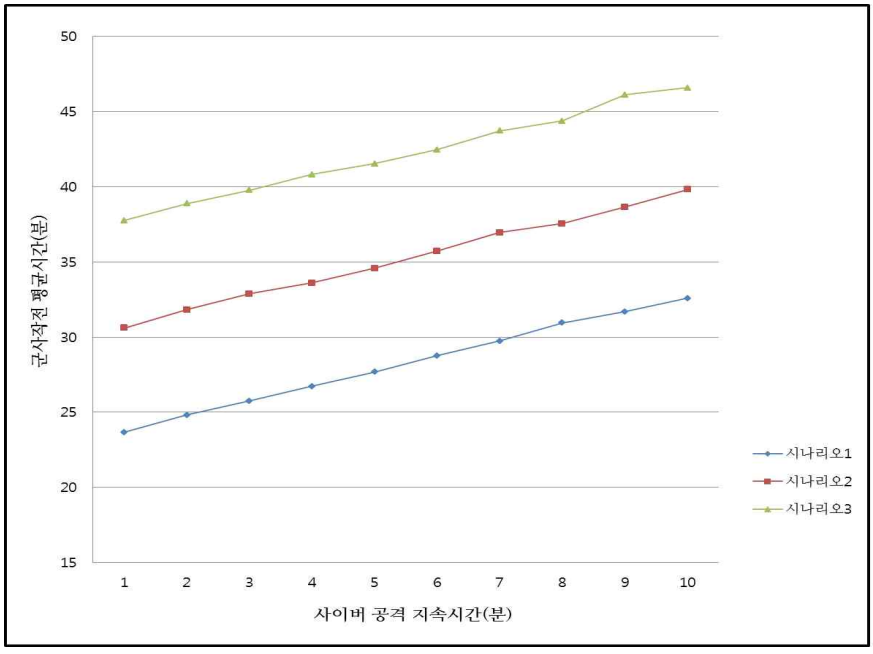
개별 시나리오에 대하여 실시한 시뮬레이션 실행 결과는 [표 4-4]와 같다.

[표 4-4] 군사작전 시뮬레이션 결과

	시나리오 1	시나리오 2	시나리오 3
최소 소요 시간	10.7	15.4	19.6
최대 소요 시간	52.1	57.8	64.1
중앙값	22.8	28.9	36.1
평균값	23.4	29.9	36.8
성공률 (30분 기준)	85.7	57.6	10.4

시뮬레이션 결과에서 알 수 있듯이 타격순환체계에 따른 시한성 긴급표적 처리에 대한 군사작전의 성공 여부는 정보의 전달 및 처리 속도에 크게 의존한다.

사이버 공격 발생 후 IT 시스템의 속도 저하에 따른 개별 군사작전 시나리오에 대한 지연시간은 〈그림 4-10〉과 같다. 제안한 모델을 통한 실험을 통하여 전체 군사작전 시간은 사이버 공격의 지속시간이 증가함에 따라 선형적으로 증가하는 것을 알 수 있다.

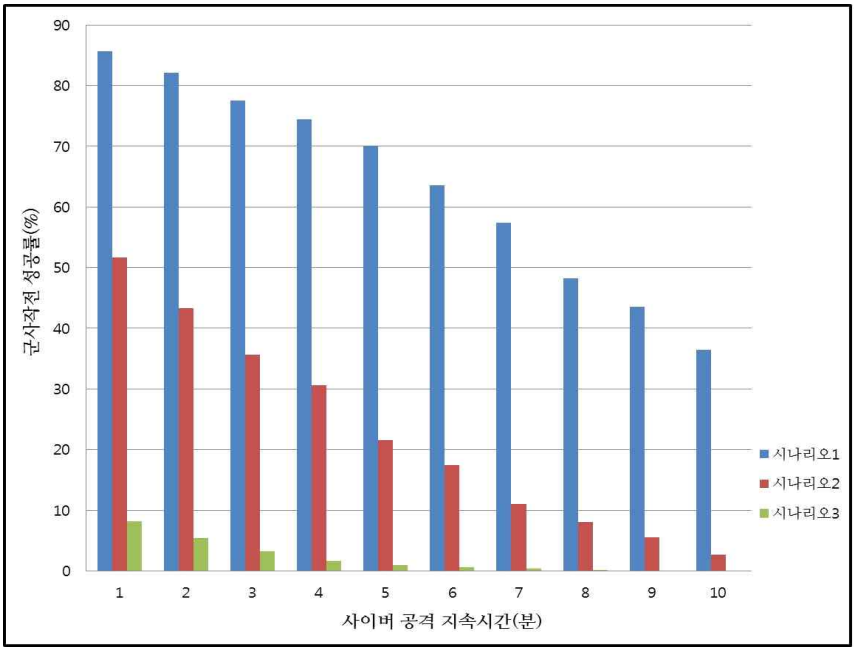


〈그림 4-10〉 사이버 공격 지속시간에 따른 군사작전의 지연시간

기본 시나리오 1에 대하여 사이버 공격 지속시간에 따른 군사작전 성공률을 분석하면 군사작전을 50% 이상으로 성공시키기 위해서는 7.5분 안에 사이버 공격에 대응하여 IT 시스템을 복구하여야 한다. 또한 10분 안에 사이버 공격에 대응하지 않으면 군사작전의 성공률은 50% 이상 감소하는 것을 알 수 있다.

작전사령관은 군사작전 목표 성공률을 고려하여 특정 시간 안에 사이버 공격에 의한 영향으로 성능이 저하된 IT 시스템의 복구가 되지 않는다면 제한된 군사정보만을 이용하여 군사작전을 계속 수행 할지를 결정하여야 한다.

〈그림 4-11〉은 모든 시나리오에 대하여 시뮬레이션 결과로 얻어진 사이버 공격의 지속시간에 따른 군사작전 성공률의 변화를 나타낸다.



〈그림 4-11〉 사이버 공격 지속시간에 따른 군사작전 성공률

본 논문의 시뮬레이션 결과는 어떠한 확률분포를 사용하는지에 따라 달라질 수 있다. 개별 프로세스 처리에 대한 시간 결과를 얻기 위해서는 로그정규분포(Lognormal Distribution)를 선택하였고 사이버 공격의 발생과 지연시간은 각각 프아송분포(Poisson's Distribution)와 삼각분포(Triangular Distribution)를 적용하였다. 모델 사용자는 분석 요구 수준에 맞게 확률분포, 입력 파라미터 및 성공기준을 달리하여 시뮬레이션을 실시하면 최적의 분석결과를 얻을 수 있다.

제안된 모델은 기능별 프로세스 모델을 컴포넌트 방식으로 구현하여 최소한의 수정으로 특정 군사작전에 대한 사이버 공격의 영향을 분석하기 위한 모델로 용이하게 업그레이드할 수 있다.

이와 같이 모델 사용자는 본 논문에서 제안한 사이버 공격 영향 평가 모델을 활용하여 입력 파라미터에 따른 사이버 공격이 군사작전에 미치는 영향을 다양한 효과도 측면에서 분석 할 수 있다.

제 5 장 결 론

본 논문에서는 사이버 공격이 군사작전에 미치는 영향을 분석하기 위한 모델 개발에 필요한 체계화된 모델링 절차 및 요구사항을 정립하고 상용 시뮬레이션 소프트웨어를 이용하여 사이버 공격 영향 평가 모델을 구현하였다.

사이버 공격 영향 평가 모델은 타격순환체계를 통한 시한성 긴급 표적 처리 과정을 시뮬레이션 하는 군사작전 프로세스 모델, C4ISR 체계를 구성하는 IT 시스템의 성능을 시뮬레이션 하는 표준 IT 시스템 프로세스 모델 및 사이버 공격 모델이 상호작용을 하도록 설계되어, 모델 사용자는 정의된 범주의 사이버 공격으로 인한 IT 시스템의 성능 저하 및 중단이 전체 군사 작전이 미치는 효과도를 과학적으로 분석 할 수 있다.

모델 설계 방법론은 UML에 기반한 4+1 뷰모델을 적용하여 제안된 모델에 대한 이해와 구현을 명확하게 하였다. Use Case 다이어그램, 절차 다이어그램 및 클래스 다이어그램을 통하여 사용자의 요구조건에 따른 모델 객체와 객체간의 상호작용, 모델링 환경에서 시스템의 동작을 이해하기 위한 메시지 순서 및 시스템 구조를 나타내는 시스템 변수를 표현하였다.

모델 구현은 개발의 편의성, 모델링 요구사항에 따른 적합성, 모델 데이터 관리를 위한 데이터베이스 설계 지원을 고려하여 이산사건 시뮬레이션을 지원하는 상용 소프트웨어를 이용하여 구현하였다. 구현된 모델은 개별 블록으로 구성되어 모델의 수정과 기능 업그레이드가 용이하고 계층 모델 표현을 통하여 모델 사용자에게 편의성을 제공하였다.

사이버 영향 평가 모델을 이용한 시뮬레이션 결과 분석을 통해서는 사이버 공격이 군사작전의 결과에 어떻게 영향을 주는지를 검증하고 개발된 모델의 활용 방안을 제시하였다.

본 논문의 목적은 전통적인 군사작전 도메인과 사이버 도메인을 연결하여 사이버 공격에 따른 군사작전의 효과도를 분석할 수 있는 모델을 개발하는 것이다. 사이버 공격 효과를 포함한 군사 작전에 대한 시뮬레이션 모델 개발은 새로운 연구 분야로 사이버 도메인의 광범위함, 복잡성, 실시간 효과도 측정의 기술적 어려움으로 인해 명확한 결과를 얻기가 어려운 분야이다.

군사작전과 연계한 사이버 공격의 영향 분석을 위한 모델 개발에 대한 문제를 해결하기 위해서는 사이버 도메인에 대한 심화된 개념연구를 통하여 사이버전에 대한 모의논리를 발전시키고, 군사작전 참여자의 의사결정 요소를 고려하여 복잡하고 다양한 사이버 공격의 영향을 분석할 수 있도록 분석지수에 따른 효과적인 모델 개발 방법론에 대한 지속적인 연구가 필요하다.

결론적으로는 본 논문을 통하여 제시된 사이버 공격의 효과도 분석을 위한 체계적인 모델링 방법론은 기존 군사작전 분석 모델 및 새로운 분석 모델 개발에 사이버 공격의 영향 분석 기능을 추가하기 위한 기반 연구가 될 것이다.

【참고문헌】

1. 국내문헌

윤희병, 『NCW서비스와 기술』, 서울 : 홍릉과학출판사, 2012, p.6

엄정호외 2인, 『사이버전개론』, 서울 : 홍릉과학출판사, 2012, p.4

정태명, 『사이버 공격과 보안 기술』, 서울 : 홍릉과학출판사, 2009

남길현, 원동호, 『정보시스템 보안론』, 서울 : 그린, 2011

최상영, 『국방 모델링 및 시뮬레이션 총론』, 서울 : 북코리아, 2010

이종호, 『모델링 및 시뮬레이션』, 서울 : 21세기군사연구소, 2008

조완수, 『UML 객체지향 분석 설계』, 서울 : 홍릉과학출판사, 2000

전병선, 『UML 분석 설계 활용』, 서울 : 와우북스, 2011

민성기, 『시스템 엔지니어링』, 서울 : 시스템체계공학원, 2012

서보환외 2인, 『소프트웨어 개발 방법론』, 서울 : 웅보출판사, 2004

양회석외 3인, 『Practical Software Engineering』, 서울 : 이한미디어, 2013

전건욱, 『시스템 신뢰도』, 서울 : 두남출판사, 2012

이태규, 『군사용어사전』, 서울 : 일월서각, 2012

지식경제부, 『국가 정보 보호 백서』, 서울 : 지식경제부, 2012

이철호, 「군 정보체계 통합 연동에 따른 보안정책수립 방안」, 국사학술용역 연구과제, 2011, p11

2. 국외문헌

Zheng Lu, et al. 『Unlocking the Power of OPNET Modeler』, Cambridge University Press, 2012

Andy Oppel, 『Data Modeling』, McGraw-Hill, 2009

Steve Winterfeld, Jason Andress, 『The Basics of Cyber Warfare』, Syngress, 2012

Hussein Al-Bahadili, 『Simulation in Computer Network Design and Modeling』, IGI Global, 2012

Pascal Cantot, Dominique Luzeaux, 『Simulation and Modeling of Systems ofs』, John Wiley & Sons, 2011

Alexandre Barreto, Paulo Costa and Edgar Yano, 「A Semantic Approach to Evaluate the Impact of Cyber Actions to the Physical Domain 」, STID2012, 2012

Scott Musman, Aaron Temin, Mike Tanner, Dick Fox, Brian Pridemore, 「Evaluating the Impact of Cyber Attacks on Missions」,MITRE Corp, 2010

Cyril Onwubiko, Thomas Owens, 『Simuational Awareness in Computer Network Defense』, IGI Global, 2012

ImageThat 『ExtendSim User Guide Release 9』, ImageThat, 2013

Sakari Ahvenainen,「Backgrounds and Principles of Network-Centric Warfare」,US Army War College, 2003

Michael R. Grimaila, Larry W. Fortson, 「Towards an Information Asset-Based Defensive Cyber Damage Assessment Process」, Ohio, IEEE CISDA 2007, 2007

Scott Musman, et al.「Computing the Impact of Cyber Attacks on Complex Missions」,VA, MITRE Corp, 2011

Larry W. Fortson, 「Towards the Development of a Deffensive Cyber Damage and Mission Impact Methodology」, Ohio, Air Force IOT, 2007

Shmuel Even, David Siman-Tov, 『Cyber Warfare: Concepts and Strategic Trends』, Institure for National Security Studies, 2012

Bruce Schneier, 『Risk of Networked System』, 2013, p1

Chris Scott, 「Cyber Warfare: A Perspective on Cyber Threats and Technology in the Network-Centric Warfare Battlespace」, MIT, 2008

Dale K. Pace 「Conceptual Model Development for C4ISR Simulations」, USA, The 5th ICCRTS,2012

Stewart Robinson, 『The Practice of Model Development and Use』, John Wiley & Sons, Ltd, 2004

Sylvain P. Leblanc, 「An Overview of Cyber Attack and Computer Network Operations Simulation」, Society for Computer Simulation International, 2011

Michael E. Kuhl, 「CYBER ATTACK MODELING AND SIMULATION FOR NETWORK SECURITY ANALYSIS」, 2007 Winter Simulation Conference, 2007

Michael Liljenstam, 「RINSE: the Real-time Immersive Network Simulation Environment for Network Security Exercises」,19th Workshop on Principles of Advanced and Distributed Simulation, 2005

Fred Cohen, 「Simulating Cyber Attacks, Defences and Consequences」, Sandia National Laboratories, 1999

Raphael S. Mudge, 「CYBER AND AIR JOINT EFFECTS DEMONSTRATION (CAAJED) 」,USA DTIC, 2007

Scott Musman, 「Computing the Impact of Cyber Attacks on Complex Missions 」,USA, MITRE, 2011

Antita D'Amico, Laurin Buchanan 「MISSION IMPACT OF CYBER EVENTS: SCENARIOS AND ONTOLOGY TO EXPRESS THE RELATIONSHIPS BETWEEN CYBER ASSETS, MISSIONS, AND USERS 」,USA, The 5th International Conference on Information Warfare and Security, 2009

Magnus Felde, 「Analyzing Security Decisions with Discrete Event Simulation」,Gjovik University, 2010

Philippe Kruchten, 「Architectural Blueprints—The "4+1" View Model of Software Architecture」,IEEE, 1995

Norman Daoust, 『UML Requirements Modeling For Business Analysis』, Technicals Publications, 2012

Edward H.S. Lo, et al. 「Improving the Kill Chain for Procecution of Time Sensitive Targets」,InTechOpen, 2010

Opher Etzion, et al. 「Military Scenario Use Case」,EDA Symposium, 2006

ABSTRACT

The development of a simulation model for analyzing the impact of cyber attacks on military operations

Sihn, Tongho
Major in National Defense Modeling & Simulation
Dept. of National Defense Modeling & Simulation
Graduate School of National Defence Science
Hansung University

In the current Defense Network Centric Warfare environment where computers and information technology are integrated to the battlefield, the loss and damage of IT systems caused by a cyber attack can result in military operations failure. It must be understood whether this affects military capabilities by interception, modification and delay of military information caused by performance degradation of computer systems and networks which support C4ISR+PGM(Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance +Precision Guided Munitions) under cyber attack by enemy forces in order to determine analytically whether the military operations can be accomplished.

This paper defines the systematic modeling process and requirements to develop a simulation model for analyzing the impact of cyber attacks on military operations and implements a Cyber Attack Impact Assessment Model using commercial modeling software.

The Cyber Attack Impact Assessment Model consists of a Military Operations Process Model for simulating the kill chain for prosecution of time sensitive targets and Standard IT Systems Process Model for simulating IT systems supporting C4ISR system and Cyber Attacks Model so it is designed to interact with each model to make model users analyze and measure the effectiveness of degradation and interruption of IT systems scientifically due to predefined cyber attacks on overall Military operations.

This paper represents the proposed model by adapting a 4+1 View model based on UML as a modeling design methodology to help a model user understand and implement the model clearly. It utilizes Use Case Diagram, Sequence Diagram and Class Diagram to create visual models to represent interactions of model objects based on user requirements and the sequences of messages exchanged between the objects to understand behavior in the modeling environments and the classes of system to describe the structure of systems.

This paper implements the proposed model using commercial modeling software which provides ease of development, suitability with modeling requirements and support of database design to manage the data model. The implemented model in this paper consists of individual functional blocks help model users modify and upgrade new functionalities of the model easily and provides a hierarchical model representation for the convenience of model users.

Finally this paper validates how to assess a cyber attack impact results on military operations through the analysis of simulation outcomes using the Cyber Attack Impact Assessment Model and presents a method for utilizing the proposed model.

【Keyword】Cyber Attack, Military Operations, 4+1 View Model, Modeling, Simulation