https://doi.org/10.33778/kcsa.2023.23.4.071

공세적 사이버 작전을 위한 사이버 킬체인 모델 연구

조 성 배*, 김 완 주**, 임 재 성***

요 약

사이버공간은 지상, 해상, 공중, 우주에 이어 다섯 번째 새로운 전쟁 공간으로 자리매김하였고, 군사작전 측면에서도 사이버공간이 핵심적인 공격과 방어 목표가 되고 있다. 세계 각국은 이러한 사이버공간에 대한 공세적 사이버 작전 수행 의지를 보인다. 본 논문에서는 기존의 방어적 전략인 사이버 킬체인 모델에 합동 항공임무명령서(ATO)의 임무수행주기와 합동표적처리 절차를 융합한 공세적 개념의 사이버 킬체인 모델을 제안한다. 제안한 모델은 사이버 작전의 합동성 측면에서 물리 작전과 사이버 작전의 통합을 통해 전략적 차원의 국가 사이버 작전 역량 개선에 기여할 것으로 기대한다.

Research on Cyber Kill Chain Models for Offensive Cyber Operations

Seong Bae Jo*, Wan Ju Kim**, Jae Sung Lim***

ABSTRACT

Cyberspace has emerged as the fifth domain of warfare, alongside land, sea, air, and space. It has become a crucial focus for offensive and defensive military operations. Governments worldwide have demonstrated their intent to engage in offensive cyber operations within this domain. This paper proposes an innovative offensive cyber kill chain model that integrates the existing defensive strategy, the cyber kill chain model, with the joint air tasking order (ATO) mission execution cycle and joint target processing procedure. By combining physical and cyber operations within a joint framework, this model aims to enhance national cyber operations capabilities at a strategic level. The integration of these elements seeks to address the evolving challenges in cyberspace and contribute to more effective jointness in conducting cyber operations.

Key words : cyber warfare, cyber killchain, cyber operation, offensive cyber operation, cyber attack, cyber defense

접수일(2023년 9월 15일), 게재확정일(2023년 10월 15일)

* 아주대학교/국방디지털융합학과(주저자)
** 아주대학교/국방디지털융합학과(공동저자)
*** 아주대학교/국방디지털융합학과(교신저자)

1. 서 론

대한민국은 현재 유일하게 북한과 군사적으로 대치하는 상태에 있으며 북한은 대한민국에 대해 수시로 무력도발을 감행하고 있다. 특히 북한은 사이버 전력을 전략적 무기로서 국가적 목표 달성을 위한 핵심 전력으로 인식하고 있으며, 3·20 전산 대란(2013), 한수원 해킹 사건(2014), 국방망 해킹 사건(2016) 등 현재까지도 지속해서 민·관·군을 가리지 않는 사이버 공격을 감행하고 있다. 이에 우리 정부도 사이버사령부를 창설하고 NCSC[1], KISA[2] 등 유관기관들이 협력하여 국가 사이버 안보에 많은 노력을 기울이고 있지만 사이버 방어에만 치중하는 소극적인 모습을 보이는 것도 사실이다.

물론 사이버전의 특성상 비국가 행위자가 사이버 공격을 수행할 위험성과 공격자 식별 및 사실관계 확인이 어려운 등 제한되는 여러 특징이 있지만, 미국을 비롯한 여러 강대국은 이미 방어의 한계를 인식하여 사이버 공격을 억지하기 위해 능동적 방어 및 공세적 사이버 작전에 대한 전략을 수립하고 노력을 기울이고 있으며, 이미 미국은 2008년부터 이스라엘과 함께 이란의 핵 시설 內 원심분리기를 파괴하는 매우 복잡한 수준의 Stuxnet 작전을 수행할 능력이 있었고, 2014년·2015년에 북한의 탄도미사일 발사를 저지하기 위해 사이버 수단을 사용했다는 연구가 있었다.[1]

이처럼 공세적 사이버 작전은 전략적/작전적 측면에서 적의 사이버 위협뿐만 아니라 적의 핵·미사일 등의 위협으로부터 비물리적 수단이 선제적 억지 전략에 활용될 수 있음을 보여주었으며, 이에 한국군도 기존의 방어적인 개념으로부터 사이버 공격에 대한 보복 공격까지 포함하는 '능동대응' 전략 및 물리전과의 연계를 고려한 합동작전 측면의 공세적 사이버 작전 수행 능력을 키워나가야 한다.

본 연구에서는 연구 과정에서의 군사보안 문제를 최소화하기 위해 연구에 활용된 모든 군사작전 교리와 교범은 공개된 미군 합동교리·교범을 사용하였다. 또한, 기존에 연구된 사이버 킬체인 모델의 제한점을 식별하고 미 합동교리에 명시되어 있는 합동임무수행주기와 기존의 사이버 킬체인 모델을 융합한 공세적-능동방어 킬체인 모델을 사이버 작전에 적용하여 전략적 차원에서 국가의 사이버 보안 역량 개선에 기여하고자 한다.

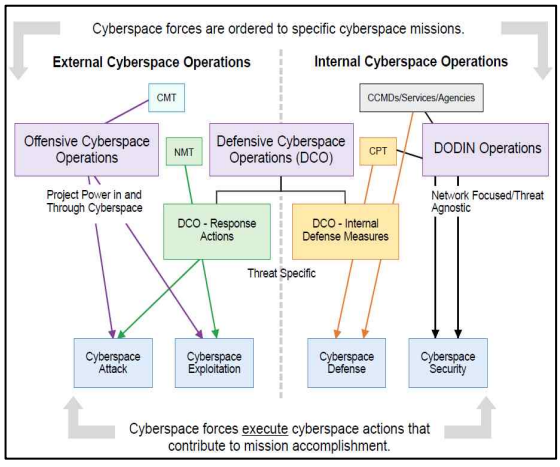
1) 국가사이버안전센터(NCSC: National Cyber Security Center)
2) 한국인터넷진흥원(KISA: Korea Internet & Security Agency)

2. 관련 연구

2.1 미 합동 사이버작전 교리·교범

미군은 합동작전을 수행하는 미군의 활동과 업무를 통제하기 위해 미 합동교범 'JP 3-12 Cyberspace Operations'을 발간했다. 사이버공간작전(CO)의 정의는 사이버공간에서 혹은 사이버공간을 통해 주요 목표를 달성하기 위해 사이버 공간의 다양한 기능을 운용하는 것이며, 해당 교리는 사이버공간에서 수행되는 군사작전에 중점을 두고 있다.

사이버작전의 원활한 계획과 수행을 위해 사이버공간을 물리네트워크영역, 논리네트워크영역, 사이버페르소나 영역의 3개 계층으로 구분하며, 작전형태에 따라 사이버공간을 청색공간, 회색공간, 적색공간으로 구분하고 있다.



(그림 1) 사이버 임무 및 기능

사이버작전의 임무와 기능은 (그림 1)과 같이 공세적 사이버작전(OCO), 방어적 사이버작전(DCO), 국방네트워크(DODIN) 작전의 3개 임무로 구성되며 성공적인 사이버 작전을 위해서는 해당 사이버 작전들이 잘 연계되고 통합되어야 한다.[2]

2.2 사이버 킬체인 모델

사이버 보안 공격 및 방어 접근 방식을 모델링하기 위한 다양한 기술이 제안되었고, 대표적으로 록히드 마틴社의 킬체인 모델은 일련의 사이버 공격 과정을 거치며, 사이버 공격 과정에서 방어자가 한 단계만 차단해도 공격자가 다음 단계로 진행할 수 없다는 점에 착안하여, 사이버 킬체인이라는 용어로 명명하고, 정찰(Reconnaissance), 무기화(Weaponization), 유포(Delivery), 악용(Exploitation), 설치(Installation), 명령 및 제어(Command&Control), 그리고 목적 달성(Action On Objective)으로 이루어진 7단계 사이버 킬체인 모델을 소개하였다.[3]

김영환 등[4]은 현행작전에서 능동적 억제전략의 핵심인 킬체인과 사이버 영역에 킬체인의 개념을 적용한 Cyber Intrusion Kill Chain을 분석하고 적용의 제한점을 식별하여 기존 물리적 킬체인 F2T2EA(Find, Fix, Track, Target, Engage, Assess)의 운용 절차를 바탕으로 기존의 킬체인을 활용한 사이버 작전 전략 수립을 통해 기술 중심적 접근 방식을 탈피하고 방어 위주의 대응에 초점을 둔 기존의 사이버 킬체인을 현행작전과 통합된 사이버 작전 개념 수립이 가능토록 전략 개념을 발전시키는데 의의가 있다.

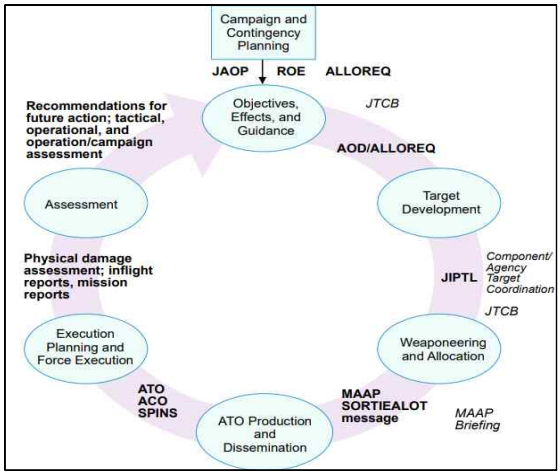
유재원 등[5]은 공격 원점 타격을 위한 킬체인 전략으로 현실 세계의 킬체인과 동일하게 감시정찰(Sensor)-결심(Decusion)-타격체계(Strike)와 이를 연동할 수 있는 연동체계(System of Systems)를 제안하였다. 위 방식 또한 기술 중심적 접근 방식을 탈피하고 현실 세계의 킬체인과 통합하여 연동체계를 바탕으로 공격 의도를 가진 대상에 대해 선제공격을 통한 억지 전략을 수립하는 데 의의가 있지만, 합동 사이버작전 측면에서 현행교리와 한국군 임무 특성을 반영하지 못한 한계점이 보인다.

앞선 선행 연구들은 기존의 사이버 킬체인 모델에서 식별된 문제점들을 해결하기 위해 기존 물리 작전 기반 모델을 결합하여 방어적 전략인 사이버 킬체인 모델에서 탈피하여 공세적 사이버 전략의 킬체인 모델을 제시하였지만 제시된 킬체인 개념은 현재 지침이 되는 미 합동교리[3] 사이버 작전(CO)의 공세적 사이버 공간작전(OCO)과 방어적 사이버 공간작전 대응조치(DCO-RA)에 적용하기에는 교리상 부여받은 임무의 특성이 맞지 않는 한계가 있다. 또한 합동 사이버 작전 측면에서 적의 위협징후를 포착시 신속한 대응과 지속적인 방어 능력을 갖추고 적시에 공세적 사이버 작전 수행을 위한 빠른 지휘 결심 및 4D 작전 개념[3] 하 선제타격을 위한 ATO 임무 수행주기에 상응하는 새로운 개념의 사이버작전 킬체인이 필요하다.

2.3 합동 항공임무명령서(ATO) 임무 수행주기

합동 군사작전에서 항공임무명령서(ATO: Air Tasking Order)는 항공작전을 수행하기 위해 합동군사령관의 지침에 따라 구성군 및 예하 부대에게 과업을 배포하고 지휘통제 기구가 세부적인 수준의 임무와 과업을 부여하는 방법론으로, 타 구성군은 즉각적이고 신뢰성이 높은 항공임무명령서에 의거하여 작전을 기획하고 시행한다.[6]

ATO의 작성과 시행 및 평가를 위한 6단계의 임무수행 주기를 항공임무수행주기 ATO(Air Tasking Cycle)이라고 하며, 미 합동교범 3-30 'joint Air Operations'에서는 합동 항공임무수행주기 절차를 (그림 2)와 같이 6단계로 구분한다.[7]



(그림 2) ATO 임무수행주기(Air Tasking Cycle)

1단계는 항공작전지침서(AOD: Air Operations Directive)를 작성하는 단계이며, 이 단계에서는 목표(Objective) 및 효과(Effects)와 연관된 합동군사령관의 지침(Guidance)을 통해 표적우선순위와 합동군사령관의

3) "핵·화생 탄두를 포함한 북한 미사일 위협을 탐지, 교란, 파괴 방어하기 위한 미사일 대응작전개념

항공전력배당 우선순위를 판단한다.

2단계 표적 개발(Target Development)은 1단계에서 작성된 AOD를 기반으로 각 구성군의 표적 데이터베이스에 타 기관의 분석가들이 작성한 모든 표적추천목록(NTL)을 통합한 후 항공임무를 위한 표적개발, 표적 탄착점 선정, 관련 자료의 제출에 집중한다. 추천된 표적과 전술적 과업을 연계하여 ATO에 포함시키며, 이러한 과정을 통해 작성되고 합동군사령관이 승인한 결과물이 합동통합우선순위표적목록(JIPTL: Joint Integrated Prioritized Target List)이다.

3단계 무기추천 및 할당(Weaponeering and Allocation) 단계에서는 2단계에서 선정된 표적에 대해 어떤 무기와 전력으로 공격할 것인지를 결정하고 예상되는 결과를 정량화하기 위해 추천된 각 표적별로 요망효과(물리적/비물리적)를 달성할 수 있는 모든 가용수단(항공, 해상, 지상, 우주, 사이버 등)을 반영한 종합공중공격계획(MAAP: Master Air Attack Plan)을 작성한다. 4단계 ATO 생산 및 배포(ATO Production and Dissemination) 단계에서는 3단계(무기추천 및 할당)까지의 세부 내용을 포함하여 해당 일자의 일일 ATO 및 특별지시를 작성하고 전술제대에 배포한다.

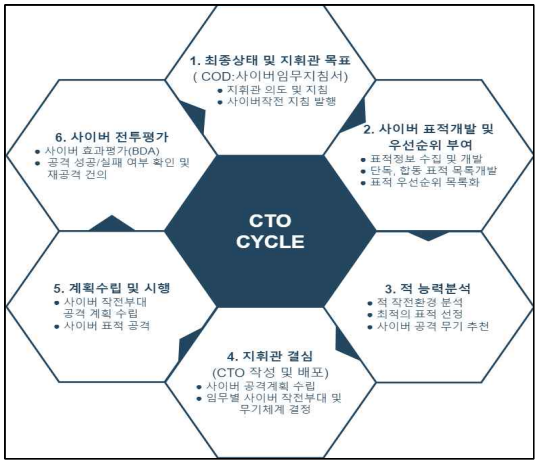
5단계 시행 계획 수립 및 전력 시행(Execution Planning and Force Execution)에서는 ATO 세부시행 계획을 수립하고 합동항공작전을 위한 전력의 운용을 지시하여 해당 일자에 시행한다. 마지막으로 6단계인 평가(Assessment)단계에서는 ATO 시행 결과를 모든 합동 제대해서 평가하며 해당 평가는 합동전력 운용으로 얻어지는 전체적인 효과를 측정하는 지속적인 과정으로 다음 ATO 임무수행 주기에 반영한다.

3. 사이버 킬체인 모델 제안

이번 장에서는 기존의 방어적 전략인 사이버 킬체인 모델에 항공임무명령서(ATO)의 임무수행주기와 합동표적처리 절차를 융합한 사이버임무명령서(CTO)를 제안한다. 또한 미 합동교범의 공세적 사이버작전(OCO)에 기반한 공세적 킬체인과 방어적 사이버작전 능동 대응(DCO-RA)에 기반한 능동방어 킬체인을 제안한다.

3.1 사이버임무명령서(CTO)

본 논문에서 제안하는 사이버 킬체인 모델은 합동작전 측면에서 지휘관의 목표에 맞추어 세부 표적 선정 및 피해평가 기능을 수행할 수 있는 항공임무명령서(ATO) 임무 수행주기와 합동 표적 처리 절차의 물리적 방법론을 적용하여 방어작전에서부터 공세적 작전까지 전략·전술·작전 별로 임무를 수행할 수 있는 킬체인 모델을 제안한다. 킬체인 모델은 (그림 3)과 같은 항공임무명령서의 절차를 사이버 작전에 적용하여 사이버 작전을 수행하기 위한 사이버임무명령서(CTO : Cyber Tasking Order)를 발행하며, 적의 물리적 도발 및 사이버 위협 징후가 식별시 위기/전시 작전계획과 지휘관의 명령을 바탕으로 적시에 공세적 사이버 작전을 수행하여 선제적으로 적의 위협으로부터 대응하며, 단독 및 합동작전에 기여한다.



(그림 3) CTO 임무수행주기(Cyber Tasking Cycle)

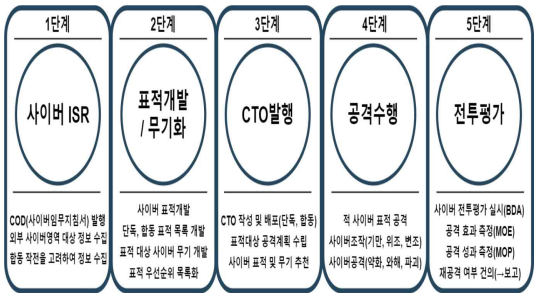
본 논문에서 제안하는 공세적 킬체인 모델은 합동작전 측면에서 지휘관의 목표에 맞추어 세부 표적 선정 및 피해평가 기능을 수행할 수 있는 항공임무명령서(ATO) 임무 수행주기와 합동 표적 처리 절차의 물리적 방법론을 적용하여 방어작전에서부터 공세적 작전까지 전략·전술·작전 별로 임무를 수행할 수 있는 킬체인 모델을 제안한다. 킬체인 모델은 위와 같은 항공임무명령서의 절차를 사이버 작전에 적용하여 사이버 작전을 수행하기 위한 사이버임무명령서(CTO : Cyber Tasking Order)를 발행하며, 적의 물리적 도발 및 사이버 위협 징후 식별시 위기/전시 작전계획과 지휘관의 명령을 바탕으로 적시에 공세적 사이버 작

전을 수행하여 선제적으로 적의 위협으로부터 대응하며, 단독 및 합동작전에 기여한다.

사이버임무명령서(CTO)의 전반적인 흐름은 (그림 3)과 같다. CTO Cycle의 단계는 1. 최종상태 및 지휘관 목표(사이버임무지침서, COD : Cyber Operations Directive) 발행), 2. 사이버 표적개발 및 우선순위 부여(사이버 표적 추천), 3. 적 능력분석 및 사이버 무기 추천, 4. 사이버임무명령서 생산/전파(공격 계획 및 사이버 공격 시나리오 전파) 5. 사이버 공격 시행 (Action), 6. 사이버 전투평가(Cyber BDA(효과측정(MOE), 성과측정(MOP))으로 이루어진다.

3.2 공세적 사이버 킬체인

적의 사이버 위협에 선제적으로 대응하고 합동작전에 기여할 수 있는 공세적 사이버 킬체인 전략의 운용 절차는 기존 록히드 마틴社의 Cyber kill Chain 운용 절차를 바탕으로 제안하는 사이버임무명령서(CTO) 단계를 추가하고 간소화하여 (그림 4)와 같이 정의하였다.



(그림 4) 공세적 사이버 작전 킬체인

공세적 사이버 작전 킬체인 모델 1단계 Cyber ISR (정보·감시·정찰)은 전/평시 구분 없이 군의 작전적 목표에 부합하는 사이버 정찰 활동을 사이버공간 內 회색 영역[4] 및 적색 영역[5]에서 수행하며, 사이버공간의 물리 계층, 논리 계층, 페르소나 정보를 수집하는 활동을 수행한다. 2단계 표적개발 무기화 단계에서는 1단계에서 수집된 정보를 바탕으로 표적정보를 생성하며 공격에 앞서 사이버 무기를 개발하는 준비단계에 해당한다. 3단계는 단독 및 합동작전을 위한 사이버 공격의 최종상태 및 지휘관의 목표 달성을 위한 사이버임무명령서(CTO)가 발행되는 단계이며, 상세 개념은 앞서 설명하였다. 4단계 공격 수행 단계에서는 앞서 3단계에서 정해진 최종상태 및 목표 달성을 위해 적의 사이버공간에 대한 공세적 작전이 수행되는 단계이며, 5단계 사이버 전투 평가 단계에서는 수행된 사이버 작전 결과를 평가하는 단계로 이 단계에서는 공격의 성공 여부와 그 효과를 분석하여, 필요한 경우 추가적인 조치와 수정사항을 결정하고 최종 보고서를 상위 지휘부에 제출하고, 지휘부에서는 다음 CTO 사이클에 반영할 개선사항이나 변경사항 등을 결정한다.

3.3 능동방어 사이버 킬체인

또한 능동적 억제 구현을 위한 방어적 사이버 작전의 능동방어 킬체인 모델은 록히드 마틴 社의 Cyber kill Chain 방어 절차인 탐지, 거부, 교란, 약화, 기만, 파괴의 절차에 군사적 전략을 운용할 수 있는 사이버임무명령서(CTO) 단계를 추가하여 (그림 5)와 같이 정의하였다.

(그림 5) 능동방어 사이버 작전 킬체인

능동방어 사이버 작전 킬체인 모델은 방어적 사이버 작전의 한 종류로서 아군의 사이버 영역에 대한 적대행위, 위협에 대한 확신, 피해 예상 정도를 판단하여 능동적으로 대응하는 활동이며, 물리력을 이용해 적 시스템을 선제적으로 무력화하는 공세적 활동도 포함한다. 1단계에서는 [6]청색 영역의 사이버 위협을 탐지하고 사이버 위협을 선제적으로 조치할 수 있는 위협정찰 활동을 수행한다. 2단계에서는 1단계에서 식별된 위협에 대해 기만/약화/교란 활동을 수행하며 공

4) 청색과 적색 사이버공간에 해당하지 않는 모든 영역
5) 적대세력이 통제하거나 소유한 영역

6) 아군이 사이버공간 우세를 장악하거나 통제할 수 있는 사이버공간

격을 수행한 적에 대한 역추적 및 침해조사, 위협 행위자 판단 등을 실행한다. 3단계에서는 적의 사이버 위협에 대해 자위권 차원의 선제적으로 조치를 위한 사이버임무명령서(CTO)가 발행된다. 4단계에서는 3단계 사이버임무명령서(CTO)의 작전목표에 따라 적의 원점을 추적하여 선제적으로 적의 시스템을 무력화 하는 능동대응 작전을 수행하며, 5단계에서는 앞서 제안한 공세적 킬체인 모델과 동일하게 능동대응 작전에 대한 성공 여부와 그 효과를 분석하여, 필요한 경우 추가적인 조치와 수정사항을 결정하고 최종 보고서를 상위 지휘부에 제출하고, 지휘부에서는 다음 CTO 사이클에 반영할 개선사항이나 변경사항 등을 결정한다.

4. 시나리오 기반 사이버 킬체인 적용

이번 장에서는 실제 사이버 작전 상황에 대한 사이버 킬체인 모델의 적용 가능성을 확인하기 위해 2022년 2월 24일부터 현재까지 진행되고 있는 우크라이나-러시아 전쟁 사례를 활용하였고, 전쟁 초기 합동성 측면에서 전략적, 작전적으로 사용된 사이버 공격을 제안하는 모델에 적용하였다.[8] 다만, 우크라이나-러시아 양국이 사이버 공격의 피해 상황을 구체적으로 공개하지 않기 때문에 각국 보안업체와 언론에서 발표한 공개정보를 중심으로 시나리오를 구성하였다.[9]

4.1 사이버 공격 사례

우크라이나-러시아 전쟁은 2022년 2월 24일 러시아가 우크라이나 영토를 침공하면서 시작되었으며, 전면적인 공격을 시작하기 직전인 2월 23일 우크라이나 정부, 금융, 국방, 항공, IT 웹사이트 대상으로 DDoS 공격 및 시스템을 파괴하는 와이퍼(Wiper) 등의 악성코드를 이용한 공격을 감행하였고,[10] 지속해서 군사적 목적을 달성하기 위해 우크라이나 대상 사이버 공격을 감행하였다.[11]

이에 우크라이나는 러시아의 사이버 공격에 대한 대응으로 러시아의 침공 개시 후 사이버 반격을 수행하였으며, 실제 사이버 공격 수행 주체는 국제 민간해킹 단체인 어나니머스를 중심으로 러시아 및 벨라루스의 언론 및 기반시설 등 서비스를 마비시키고 반전 여론을 조성하는 사이버 심리전이 전개되었으며, 물리전 수행에 활용되거나 영향을 초래할 수 있는 전장(battle-field) 밀접형 정보탈취 및 기반시설(철도망)공격 등을 공격하는 능동대응 작전을 수행하였다.[12]

4.2 공세적 사이버 킬체인 적용

본 논문에서 제안하는 공세적 사이버 킬체인 모델은 (그림 4)에서 보듯이 5단계의 절차로 이루어지며 해당 킬체인 모델에 공격 시나리오를 적용하면 다음과 같다.

러시아의 사이버 작전 부대는 우크라이나를 침공하기 전 군사적 목적을 달성하기 위해 사이버 임무 지침서(COD(최종 상태 및 지휘관 목표))를 발행하였고, 최종 상태는 우크라이나 중앙 정부, 금융, 국방, 항공 등 주요 기반시설 시스템에 파괴형 악성코드를 이용하여 기능을 마비시키는 것이고, 지휘관의 목표는 침공 개시 전 24시간 동안 우크라이나 주요 기반시설을 사용 불능 상태로 만들어 사회의 혼란을 야기하고 합동성 측면에서 다른 전장 영역에서의 공격과 통합하여 전략적 목적을 달성하는 것을 목표로 한다.

이를 위해서 1단계 Cyber ISR(정보·감시·정찰)을 수행하였으며, 이 단계에서는 우크라이나의 주요 기반시설 시스템 네트워크를 탐색하기 위해 사이버공간 회색 영역과 적색 영역에서 활동하며 대상 네트워크의 물리 계층, 논리 계층 그리고 사용자와 관련된 정보(페르소나)를 수집하였다. 이러한 활동은 적색 영역에 진입하는 것을 포함하여 신중하게 계획 및 실행되었다. 2단계 표적개발 및 무기화 단계에서는 첫 번째 단계에서 수집된 정보를 바탕으로 표적 정보를 생성하고, '위스퍼 게이트(Whisper Gate)', '허메틱 와이퍼(Hermetic Wiper)' 등 시스템 파괴형 사이버 무기를 개발하였고, 임무명령서 발급 시점에 맞추어 해당 공격 도구를 선택하여 이용할 준비를 하였다. 3단계 CTO발행(결심) 단계에서는 임무지침서(COD)에서 명시된 최종 상태와 지휘관의 목표 달성을 위해 사이버임무명령서(CTO)를 발행하였고, 해당 임무명령서 대한 자세한 내용은 <표 1>을 참고한다.

4단계 공격수행 단계는 세 번째 단계에서 발급

된 CTO를 실제로 실행하는 단계로 설정된 최종 상태 및 목표 달성을 위해 실제로 멸망 작전을 시작하였다. 즉, 와이퍼 악성코드의 배포와 실행을 통해 우크라이나 우크라이나의 중요 정보 기반시설 시스템에 대한 파괴적인 공격을 실행하였으며, 데이터를 훼손하고 시스템을 불능화하였다. 마지막으로 수행되는 5단계 사이버 전투 평가는 4단계 공격 수행에 대한 사이버 작전 결과를 평가하는 단계이며, 여기서는 공격 성공 여부와 그 효과를 분석하고, 필요한 경우 추가적인 조치나 수정사항을 결정한다. 와이핑 작전의 평가결과는 최종 보고서로 작성하여 러시아 상위 지휘부에 제출되었으며, 이를 통해 다음 CTO 사이클에 반영할 개선사항이나 변경사항 등을 고려하여 재공격 여부를 결정하였다.

멸망 작전에 관한 사이버 효과 평가(Cyber BDA)는 효과 측정(MOE), 성과 측정(MOP)으로 나뉘며, 효과 측정(MOE)은 대상 네트워크가 24시간 동안 사용 불능 상태를 유지했는지 확인하고, 성과 측정(MOP)은 공격이 성공적으로 이루어졌고, 예상대로 와이퍼 악성코드가 작동하였는지 확인하였다.

<표 1> 사이버 임무 명령서(CTO)

항목	설명
CTO 번호	2022-2-23-RU-UA01
CTO 발행일	2022년 2월 23일
작전명	멸망 작전
작전개요 (Operations Overview)	"와이퍼" 악성코드를 이용하여 우크라이나의 중요 정보 기반시설 시스템에 대한 파괴적인 공격을 실행, 네트워크가 최소한 24시간 동안 사용 불능 상태 요망
사이버 표적개발 및 우선순위 부여 (Cyber Target Development and Prioritization)	표적은 우크라이나 중요 기반시설 시스템 및 네트워크이며 이는 국가 관리 및 안보에 필수적인 역할을 수행하므로, 이를 공격하는 것은 우크라이나에 큰 영향을 줄 것으로 예상됨
공격 계획 (Attack Planning)	와이퍼 악성코드를 배치하여 시작하며 MITRE ATT&CK 기술(T1059 - Command and Scripting Interpreter)과 전략(T1190 - Exploit Public-Facing Application)을 사용하여 시스템에 침입하고 데이터를 파괴하거나 변경함으로써 시스템을 사용 불능 상태로 만드는 기능을 실행
공격 실행 및 시간 테이블 (Execution and Timing)	공격은 즉시 시작되며, 와이퍼 악성코드가 배치 및 실행되어야 하며, 목적 달성을 확인하기 위한 첫 번째 체크 포인트는 악성코드 배치 후 6시간이다.
기타 지원 요소	예상되는 적 방어 능력(백신 프로그램, IDS/IPS 등), 예상 위협(우크라이나의 반응), 그리고 추가적인 정보(예: 대상 네트워크의 구조나 사용 중인 소프트웨어)

4.3 능동방어 사이버 킬체인 적용

본 논문에서 제안하는 능동방어 사이버 킬체인 모델은 (그림 5)에서 보듯이 5단계의 절차로 이루어지며 해당 킬체인 모델에 공격 시나리오를 적용하면 다음과 같다.

우크라이나는 러시아와의 군사적 긴장감이 고조되는 상황에서 자국의 사이버공간을 효과적으로 보호하기 위해 사이버 임무 지침서(COD(최종 상태 및 지휘관 목표))를 발행하였고, 최종 상태 및 지휘관의 목표는 우크라이나의 중앙 정부, 금융, 국방, 항공 등 주요 기반시설을 보호하고 러시아의 사이버 공격을 성공적으로 차단하고 국가 안전과 안정을 유지하는 것을 목표로 한다.

이를 위해서 1단계 탐지/거부 단계에서는 SIEM 등을 활용한 보안관제를 비롯하여, 침입 탐지/방지 시스템(IDS/IPS) 등을 통해 청색 영역 내 적의 공격을 탐지 및 차단하고, 회색 영역 위협정찰을 통해 러시아와

친 러시아 해커조직의 공격 패턴과 전략을 분석한다.

이 단계에서 각국의 과거 사이버 공격 기록 및 사용되는 악성코드 도구, 가능한 공격 경로 등에 대한 정보를 수집하고 분석하였다. 2단계 기만, 약화, 교란 단계에서는 1단계에서 수집된 정보를 바탕으로 자국의 사이버공간을 보호하는 데 필요한 조치를 취하며, 특정 IP주소 및 도메인에 대한 접근 제어, 시스템 설정 변경, 패치 적용, 허니팟 체계 운영 등을 통해 잠재적인 공격자들로부터 네트워크를 효과적으로 보호하고 적을 교란시켰다. 하지만 우크라이나의 이러한 노력에도 불구하고 러시아는 우크라이나를 대상으로 사이버 공격을 감행하여 2022년 2월 23일 우크라이나 주요 시설에 대한 멸멸 시스템을 무력화시켰고, 러시아는 바로 다음 날인 2022년 2월 24일 물리전과 통합된 전면전을 개시하였다.

이에 우크라이나는 지휘부는 식별된 적 사이버위협에 따른 자위권 차원의 선제적 조치를 위한 3단계사이버임무명령서(CTO)를 발행하였고, 해당 임무명령서에 대한 자세한 내용은 <표 2>를 참고한다.
우크라이나는 4단계 능동대응 단계에서 3단계 사이버임무명령서(CTO)의 작전목표에 따라 적의 원점을 추적하여 선제적으로 적의 시스템을 무력화하는 능동대응 작전을 수행하였으며, 우크라이나의 사이버 작전부대와 민간 해커 그룹은 러시아 및 벨라루스의 시스템에 대한 선제적인 능동대응 공격을 수행하여 러시아의 언론 및 기반시설 등 서비스를 마비시키고 반전여론을 조성하는 사이버 심리전을 전개하며 물리전 수행에 활용되거나 영향을 초래할 수 있는 전장(battle-field) 밀접형 정보탈취 및 기반시설(철도망)을 공격하였다. 5단계에서는 앞서 제안한 공세적 킬체인 모델과 동일하게 능동대응 작전에 대한 성공 여부와 공격 및 방어에 대한 효과를 분석하여, 필요한 경우 추가적인 조치와 수정사항을 결정하고 작전 결과에 대한 최종 보고서를 우크라이나 상위 지휘부에 제출하고, 지휘부에서는 다음 CTO 사이클에 반영할 개선사항이나 변경사항 등을 결정하였다.

우크라이나의 평화 작전에 관한 사이버 효과 평가(Cyber BDA)는 효과 측정(MOE), 성과 측정(MOP)으로 나뉘며, 효과 측정(MOE)은 우크라이나의 사이버 공격과 방어에 대한 성공률을 평가하여 러시아의 사이버 공격으로부터 국가 기반시설 및 주요 정보시스템을 성공적으로 보호하였는지 확인하고, 능동대응조치를 통해 악성코드 침입, DDoS 공격 등을 얼마나 효과적으로 차단하고, 네트워크의 안정성 회복 정도를 확인하여 사이버 공격 이후 네트워크의 안정성을 얼마나 빠르게 회복하였는지 평가하고 서비스 중단 시간 및 복구 시간 등을 측정하여 회복력을 평가한다. 성과 측정(MOP)은 공격이 성공적으로 이루어졌는지 작전계획 수립과 이행 절차를 검토하여 목표 달성에 얼마나 잘 준비되었고, 체계적으로 실행되었는지 확인하고 작전계획의 유효성과, 작전 담당자들 간의 협력 및 커뮤니케이션 등을 평가한다.

<표 2> 사이버 임무 명령서(CTO)

항목	설명
CTO 번호	2022-2-24-UA-RU01
CTO 발행일	2022년 2월 24일
작전명	평화 작전
작전개요 (Operations Overview)	러시아에 대한 능동방어 작전을 수행하여 우크라이나의 국가안보와 정보시스템을 선제적으로 보호하고, 러시아의 사이버 공격을 차단 및 무력화
사이버 표적개발 및 우선순위 부여 (Cyber Target Development and Prioritization)	표적은 러시아의 주요 기반시설과 우크라이나를 공격한 사이버 공격 단체이다. 해당 표적들은 우크라이나에 대한 위협을 가지고 있으며, 국가안보에 큰 영향을 줄 수 있는 요소이다.
공격 계획 (Attack Planning)	개발된 사이버 무기체계 및 MITRE ATT&CK 기술과 전략을 사용하여 러시아의 주요 기반시설에 침입, 데이터 파괴, 네트워크 마비 등 다양한 방법으로 타격하여 러시아와 적 사이버 조직을

	무력화시킨다.
공격 실행 및 시간 테이블 (Execution and Timing)	공격은 즉각적으로 시작되며, 각 단계별로 계속 진행 체크 포인트는 각 단계별로 설정되어 해당 단계가 성공적으로 완료되었음을 확인한다.
기타 지원 요소	예상되는 적 방어 능력(백신 프로그램, IDS/IPS 등), 예상 위협(러시아의 반응), 그리고 추가적인 정보(예: 대상 네트워크의 구조나 사용 중인 소프트웨어) 등은 상황 분석과 함께 고려되어야 한다.

5. 결 론

본 논문에서는 공세적 사이버 작전을 위한 사이버 킬체인 모델을 미 합동교범 'JP 3-12 Cyberspace Operations'의 사이버 작전(CO)의 공세적 사이버 작전(OCO)과 방어적 사이버 작전 대응조치(DCO-RA)를 기반으로 기존 록히드 마틴社의 Cyber Kill Chain 모델에 합동 항공임무명령서(ATO) 임무수행주기와 합동 표적처리 절차의 물리적 방법론을 융합한 공세적 개념의 사이버 킬체인 모델을 제안하였다.

본 논문에서 제안한 사이버 킬체인 모델은 즉각적인 공격이 기반되어야 하므로 보다 신속한 대응을 가능케 하고, 사이클 반복성으로 인한 지속적인 공격과 방어 능력을 강화하여 국가 사이버 작전 역량 개선에 기여하는데 그 의의가 있다.

특히 해당 모델을 통해 현행 군 사이버 작전이 합동성 측면에서 물리 작전과 사이버 작전의 통합으로 이어져 전략적/작전적 차원에서 국가의 사이버 보안 역량 개선에 기여하고 향후 한국군의 사이버 작전의 활용성이 높아질 것이라고 기대한다. 하지만 제안한 사이버 킬체인 모델은 다양한 사이버 공격사례를 기반으로 각 단계에 속한 공격 전술(tactic) 또는 각 공격 전술에 속한 기술(technique)에 대한 연구가 더 진행되어야 할 필요성이 있다.

따라서 향후 연구에서는 다양한 사이버전 사례를 통해 제안한 사이버 킬체인 모델과 MITRE 社의 ATT&CK Matrix[12]를 기반으로 하여 주요 공격기술 및 절차의 연계를 가시화하고 실제 사이버전 사례를 기반으로 사이버 공격/방어 시나리오를 활용하여 정교하게 사이버 킬체인 모델을 구성하고 각 공격 단계에 대한 전체적인 공격기술을 분류하여 다양한 위협 벡터를 다루는 한국군 사이버 작전 특성에 맞게 실전적 사이버 작전을 수행할 방안이 연구되어야 하며, 향후 한국군의 적법한 사이버 작전 수행을 위한 정책·전략적·법적 기반이 마련되어야 한다.

참고문헌

[1] International Institute for Strategic Studies, "Cyber capabilities and national power - A net assessment," IISS, 2021. [Online]. Available: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---a-net-assessment___.pdf. (accessed Aug. 4, 2021).

[2] JP 3-12, Cyberspace Operations, 8 June 2018.

[3] Martin L. Cyber kill chain. URL: http://cyber. lockheedmartin.com/hubfs/Gaining the Advantage Cyber Kill Chain. pdf. 2014.

[4] Y. H. Kim and S. Lee, "Cyber Kill Chain Strategy for Offensive and Integrated Cyber Operations," vol. 13, no. 5, pp. 325 - 340, 2016.

[5] J. Yoo and D. Park, "Cyber kill chain strategy for hitting attacker origin," vol. 21, no. 11, pp. 2199 - 2205, 2017.

[6] U.S. Joint Chiefs of Staff, DOD Dictionaty of Military and Associated Terms, November 2021.

[7] JP 3-30, Joint Air Operations, 25 July 2019, VR 17 Sept 2021.

[8] 김대건, 차장현, 이종덕, and 백승수, "우크라

이나-러시아 전쟁에 나타난 사이버전 양상 분석을 통한 사이버전 용병술 체계 정립 필요성 고찰," vol. 78, no. 2, pp. 1 - 21, 2022.

[9] 이형동, 윤준희, 이덕규, and 신용태, "러시아-우크라이나 전쟁에서의 사이버공격 사례 분석을 통한한국의 대응 방안에 관한 연구," vol. 11, no. 10, p. 10, 2022.

[10] T. H. TeamSymantec, T. H. Team, Symantec, About the AuthorThreat Hunter TeamSymantecThe Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, and A. the Author, "Ukraine: Disk-wiping attacks precede Russian invasion," Symantec Enterprise Blogs, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia (accessed Jul. 7, 2023).

[11] "A year of wiper attacks in Ukraine," Award-winning news, views, and insight from the ESET security community, https://www.welivesecurity.com/2023/02/24/year-wiper-attacks-ukraine/ (accessed Oct. 12, 2023).

[12] S. Ikeda, "'Anonymous' hacker collective declares Cyber War against Russian government over Ukraine invasion," CPO Magazine, https://www.cpomagazine.com/cyber-security/anonymous-hacker-collective-declares-cyber-war-against-russian-government-over-ukraine-invasion/ (accessed Sep. 4, 2023).

[13] "Mitre ATT&CK®," MITRE ATT& CK®, https://attack.mitre.org/ (accessed Oct. 1, 2022).

〔저자소개〕

조 성 배 (Seong-Bae Jo)
2017년 2월 중원대학교 학사
2020년 3월 ~ 현재 아주대학교 국방디지털융합학과 석사과정
email : babufree@ajou.ac.kr

김 완 주 (Wan-ju Kim)
1998년 2월 서울과학기술대학교 학사
2008년 1월 국방대학교 석사
2017년 2월 아주대학교 박사
2017년 3월 ~ 현재 아주대학교 국방디지털융합학과 겸임교수
email : sizipus1@ajou.ac.kr

임 재 성 (Jae-sung Lim)
1983년 2월 아주대학교 학사
1985년 2월 KAIST 석사
1994년 8월 KAIST 박사
1998년 3월 ~ 현재 아주대학교 국방디지털융합학과 교수
email : jaslim@ajou.ac.kr