https://doi.org/10.33778/kcsa.2021.21.4.041

모자이크전 수행 개념을 적용한 능동형 상황 탄력적 사이버 방어작전★

엄 정 호*

요 약

최근 4차 산업혁명기술로 인해 전쟁의 양상까지 진화하고 있다. 그 중에서도 인공지능 기술이 첨단 무기체계와 의사결정시스템에 적용됨에 따라 전쟁 수행 방식을 변모시키고 있다. 미국의 방위고등연구계획국에서 제시한 모자이크전은 사물인터넷, 클라우드 컴퓨팅, 빅데이터, 모바일, 인공지능 기술을 접목시킴으로써 군사적전을 소모중심에서 결심중심으로 전환하고 네트워크화된 전장 상황에 따라 분산 배치된 전력을 적절히 재조합하여 신속하게 전쟁을 수행하는 방식이다. 즉, 획일화된 전투 프로세스에 의해 군사작전을 수행하는 것이 아니라 상황에 따라 분산체계를 통해 다양한 전력을 운용한다는 것이다. 사이버전에서도 인공지능이 사이버공격 기술에 적용됨에 따라 기존의 사이버 킬 체인과 같은 절차적 대응 방식으로는 한계가 있다. 그래서 본 논문에서는 공격 상황에 따라 대응 시스템을 운용할 수 있는 능동형 상황 탄력적 사이버작전을 효과적으로 수행하기 위해서 모자이크전의 수행 방식을 적용하고자 한다.

Active and Context-Resilient Cyber Defense Operation applying the Concept of Performing Mosaic Warfare

Jung-Ho Eom*

ABSTRACT

Recently, the aspect of war is evolving due to the 4th industrial revolution technology. Among them, AI technology is changing the way of war as it is applied to advanced weapon systems and decision-making systems. Mosaic Warfare, presented by the U.S. DARPA, is shifting military warfare from attrition-centric warfare to decision-centric warfare by combining Internet of Things, cloud computing, big data, mobile, and artificial intelligence technologies. In addition, it is a method to perform operations quickly so that the most offensive effect can be achieved by appropriately combining the distributed and deployed forces according to the battlefield context. In other words, military operations are not carried out through a uniform combat process, but various forces are operated through a distributed system depending on the battlefield context. In cyber warfare, as artificial intelligence is applied to cyber attack technology, there is a limit to responding with the same procedural response method as the existing cyber kill chain. Therefore, in this paper, the execution method of mosaic warfare is applied to perform context-resilient cyber operations that can operate a response system according to the attack and cyberspace context.

Key words : Mosaic Warfare, Cyber Defensive Operation, Cyber Maneuver, Security System, Cyber Attack

접수일(2021년 09월 26일), 게재확정일(2021년 10월 16일)

* 대전대학교 군사학과&안보융합학과 교수

★ 이 논문은 2020년 대한민국 교육부와 한국연구재단의 인문사회분야 중견연구자지원사업의 지원을 받아 수행된 연구임(NRF-2020S1A5A2A01044520).

1. 서 론

2021년 8월에 개최된 제2회 AI Security Day 세미나에서 인공지능 기술이 지능형 CCTV, 자율주행 차량, 웹서비스 등에서도 사용되고 있지만, 사이버 공격자가 AI 기술을 사이버공격 알고리즘에 적용하여 지능형 사이버공격을 감행하고 있다고 밝혔다. 또한, 인공지능 기술을 적용한 퍼즈 테스트를 통해 시스템의 문제점을 식별하고 제로데이 취약점도 발굴한다고 밝혔다[1]. 인공지능을 접목한 사이버공격 기술은 인공지능의 학습능력을 활용하여 악성 문서와 메일을 작성하고 배포할 수 있으며, 취약점을 찾아 공격 성공률이 높은 공격기법을 추천하기도 한다[2]. 앞으로 인공지능 기술 성숙도가 높아질수록 더욱 더 사이버공격 알고리즘에 적용될 것이며, 사용도도 증가할 것으로 예상된다. 이러한 인공지능 기술을 접목한 지능형 사이버공격을 대비하기 위해서는 기존의 사이버공격 대응 전략으로는 한계가 있다. 물론, 사이버 대응 기술에도 인공지능 기술이 접목되어 현재보다는 보다 정확하고 신속하게 대응할 수도 있다. 하지만, 사이버전에서 사이버작전을 운용함에 있어서 기존의 절차 중심적이고 인간 통제적인 방식을 적용한다면, 지능형 사이버공격을 보다 신속하고 효과적으로 차단하고 탐지하기가 힘들 것이다.

4차 산업혁명기술은 국방분야에서도 많은 변화를 주고 있다. 빅데이터와 인공지능 기술로 인해서 탐지-결심-타격까지 신속하게 진행되고 첨단무기체계로 타격의 정확도를 향상시키고 있다. 최근에는 4차 산업혁명기술의 핵심인 인공지능과 자율시스템과 같은 새로운 기술을 활용하여 적이 효과적으로 대응할 수 없도록 임무 중인 전력을 재조합하거나 임무 전환하여 전장환경 변화에 신속하게 적응하고 전투력을 확장시키는 새로운 전투 패러다임이 나타났다. 이는 인공지능의 기반의 시스템이 인간의 의사결정을 돕고 전력을 통제하여 첨단 무기체계로 적을 타격함으로써 아군에게는 전장 적응력과 전투 확장력을 제공하며, 적에게는 복잡성과 불확실성을 제공하는 전투 수행개념인 모자이크전이다[3].

본 논문에서는 지능형 사이버공격을 효과적으로 대응하기 위해서 모자이크전의 전투 수행 개념을 사이버 방어작전에 적용한 능동형 상황 탄력적 사이버 방어작전 개념을 제안한다. 2장에서는 사이버작전 개념을 살펴보고 3장에서는 능동형 상황 탄력적 사이버 방어작전에 적용 가능한 모자이크전의 전투 수행 개념을 설명한다. 4장에서는 모자이크전 전투 수행 개념이 적용된 능동형 상황 탄력적 사이버 방어작전 개념을 제안하고 5장에서 결론을 맺는다.

2. 사이버작전

2.1 사이버작전의 개념과 특징

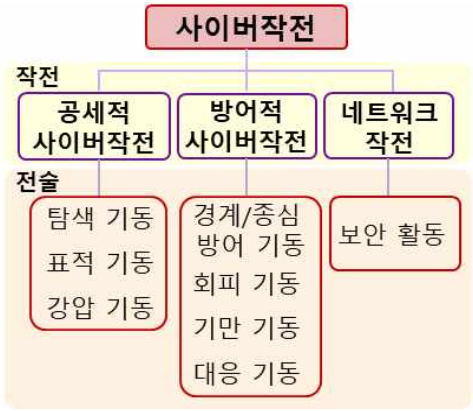
여러 문헌에서 정의한 사이버작전 개념은 '사이버작전은 사이버전장 내에서 또는 사이버전장을 통해서 군사적 목적을 달성하기 위해서 사이버공간에서 다양한 전력을 운용함으로써 아군의 사이버전장 우세권을 확보하는 것'으로 정리할 수 있다[4-7].

사이버작전의 특징도 다양한 연구문헌과 지침서를 요약 정리하면 다음과 같다[6-9]. 첫째, 적보다 상대적으로 군사력이 약할 경우에 사이버작전을 통해서 적의 군사작전을 지연시키거나 방해할 수 있는 비대칭성을 갖는다. 둘째, 4차 산업혁명기술과 군사과학기술의 진보로 인해서 사이버공격과 방어에 사용되는 모든 기술과 전술이 끊임없이 변화하고 진화한다. 셋째, 사이버 무기체계를 적은 비용으로 신속하게 여러 지역에 배치할 수 있으며, 다양한 사이버 무기체계를 동시에 공격할 수 있는 병렬과 분산의 특성을 갖는다. 넷째, 물리적 피해나 인명손실을 최소화하면서 적의 군사작전을 지연시키거나 중지시킴으로써 아군의 군사작전의 우세권을 확보할 수 있게 한다. 다섯째, 사이버작전은 은밀하고 순식간에 이루어지기 때문에 지휘관의 신속한 결심과 행동이 요구된다. 마지막으로 국지적인 사이버작전을 통해서 하나의 네트워크로 연결되어있는 정치, 군사, 경제, 사회, 군사 등의 다양한 안보분야에 위협을 가하거나 자국의 안보체계를 보호할 수도 있다.

2.2 사이버작전의 종류

미 육군성의 '사이버작전과 전자전[4]'에서는 사이버작전의 종류를 공세적 사이버공간 작전, 방어적 사

이버공간 작전, 그리고 네트워크 작전으로 구분하고 있다. S. D. Applegate의 'The principle of maneuver in cyber operations[8]' 논문에서는 사이버 기동을 공세적 기동과 방어적 기동으로 구분하였다. 공세적 기동에는 탐색 기동, 표적 기동 및 강압 기동, 방어적 기동에는 경계/종심 방어 기동, 회피 기동, 기만 기동과 대응 기동 세분화하였다. 엄정호의 '제4차 산업혁명시대의 사이버전 개론[7]'에는 위의 참고문헌을 참고해서 사이버작전을 분류하였는바, 본 논문에서는 이를 기반으로 새롭게 수정된 내용을 포함하여 아래 그림과 같이 분류한다.



(그림 1) 사이버작전의 종류

공세적 사이버작전은 지휘관의 목적을 지원하기 위해서 사이버공간 내에서 또는 통해서 사이버 전력을 활용하여 작전을 전개하는 것이다. 세부 전술로는 사이버 전투에 필요한 적대국의 시스템과 네트워크의 구성 정보와 소통되는 데이터를 수집 및 분석하는 탐색 기동, 아군의 사이버작전 우세권을 확보하기 위한 사이버전장에서 주요 자산을 파괴하고 핵심 데이터를 유출하는 표적 기동, 적대국의 작전 프로세스를 방해하거나 의사결정을 지연시키는 강압 기동이 있다.

방어적 사이버작전은 아군의 네트워크와 데이터, 그리고 주요 시스템을 보호하기 위한 사이버 역량을 유지하고 방어 활동을 수행하는 것이다. 세부 전술로는 내부로 침입하는 악성코드를 차단하고 핵심 시스템이나 데이터에 도달하지 못하도록 하는 경계 및 종심 방어 기동, 적에게 표적이 된 시스템이나 데이터를 표적화하지 못하도록 변경 및 이동시키는 회피 기동, 허니팟이나 허니넷으로 적의 공격을 유도하는 기만 기동, 적의 공격으로 인한 피해만큼 보복하는 대응 기동이 있다. 마지막으로 네트워크 작전은 아군의 네트워크와 데이터의 기밀성, 가용성과 무결성을 보장하기 위하여 사이버공간을 보호, 구성, 운영 및 유지하는 활동이다. 세부 전술로는 컴퓨터, 네트워크 및 플랫폼을 포함한 데이터에 대한 무단 접근, 악용 및 손상을 방지하고 가용성, 무결성, 기밀성, 인증을 보장하기 위한 사이버 보안 활동이 있다.

2.3 사이버작전의 절차

본 논문에서는 공세적 사이버작전이 아닌 방어적 사이버작전 측면에서 사이버작전 절차를 살펴본다. 이를 통해서 본 연구에서 제안하고자 하는 능동형 상황 탄력적 사이버 방어작전 수행 개념이 보다 유연성이 있고 상황 중심의 대응 작전임을 알 수 있다.

우선 록히드 마틴에서 제시한 사이버 킬 체인(Cyber Kill Chain)을 대응하는 방어 절차[10]와 김성중의 '사이버전 수행절차 운영 개념에 관한 연구[11]에서 제시한 사이버전 프레임워크를 설명한다. 록히드 마틴사의 사이버 킬 체인에 따른 대응 절차는 아래 표와 같이 6단계로 탐지, 거부 교란, 약화, 기만, 파괴 단계로 구성된다.

<표 1> 사이버 킬 체인 대응 절차

단계	기 능
탐지	공격 행위 탐지
거부	접근 차단 및 자원 사용 거부
교란	공격을 위한 정보 이동 방해
약화	공격 행위 효과(율)성 감소
기만	정보 조작 및 오판 유도
파괴	공격 도구의 기능 손상 및 복원 불능

사이버전 프레임워크는 아래 표와 같이 4단계로 사이버 정보감시정찰, 사이버 지휘통제, 사이버방어, 사이버 전투피해평가로 구성되며, 상호 유기적으로 연결되어 있다.

<표 2> 사이버전 프레임워크

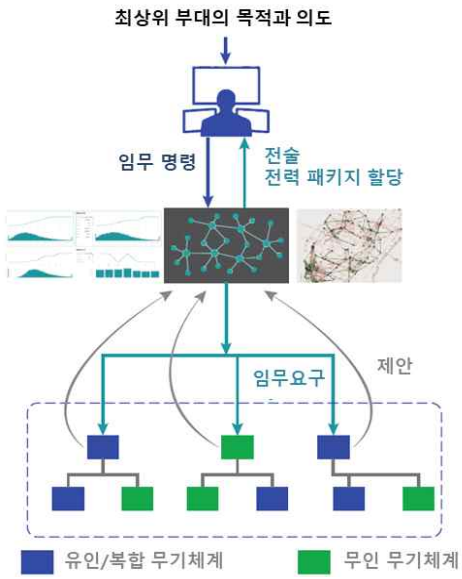
단계	기 능
정보감시 정찰	사이버공간 감시/정찰을 통해서 공격 징후 정보 수집
지휘통제	수집된 사이버정보를 기반으로 각 부대를 지원하기 위한 의사결정
방어	사이버 위협 탐지 및 대응 활동
전투피해 평가	공격으로 인한 자산의 손상, 임무 중지, 복원 등에 소요되는 피해 평가 활동

3. 모자이크전

3.1 모자이크전의 개념

미래전은 4차 산업혁명의 신기술과 첨단 군사과학기술로 인해서 끊임없이 변화하고 진화하게 될 것이다. 특히 인공지능 기술이 군사과학기술에 접목되면서 전쟁의 패러다임까지도 변화시키고 있다. 새로운 정보통신기술이 기존의 무기체계에 적용되면서 지능화된 무기체계로 진화하고 정밀성과 파괴력을 향상시키며, 전투 프로세스에 인간의 개입을 최소화시키고 있다. 지능화되고 자율성을 갖게 된 무기체계로 인해서 표적이 식별되면 분산된 무기체계를 재조합하여 가장 효과적인 작전 수행을 가능케 한다. 이러한 전쟁 수행 개념을 모자이크전(Mosaic Warfare)라고 한다[12].

모자이크전은 인간의 지휘와 AI 및 자율 시스템을 활용한 기계 통제 시스템 간의 결합을 통해 분산 배치되어 있는 유·무인 복합체계, 다영역 C2 노드 등의 전력을 가장 효과적으로 운영하기 위해서 보다 신속하게 재구성함으로써 상대방에게 불확실성과 복잡성을 강요하여 적의 의사결정체계를 무력화할 수 있는 새로운 전투 패러다임을 의미한다. 인공지능 기술에 의하여 전장 상황과 임무에 따라 요구되는 능력과 이러한 능력을 충족시킬 수 있는 분산된 전력들을 조합하여 적이 아군의 전력 운영을 예측할 수 없게 한다. 또한, 감시정찰-지휘통제-타격 체계를 분산하여 준독립적으로 운용함으로써 중앙 지휘통제체계를 보호하고 분산되어 재조합된 감시정찰-지휘통제-타격 체계가 파괴될지라도 전쟁 지속능력을 갖게 할 수 있다[3,13-15]. 다음 그림은 모자이크 전쟁의 수행 개념을 보여준다[13].



(그림 2) 모자이크전 개념

모자이크전의 핵심은 의사결정 중심 및 상황 중심 C3 체계이다. 의사결정 중심 체계는 인공지능과 자율시스템을 활용하여 표적이 식별될 때 효과적으로 작전이 가능한 전력을 분산된 전력 내에서 재조합하여 운용함으로써 적의 의사결정체계를 무력화하는 것이다. 상황 중심의 지휘통제 및 통신(C3: Command and Control, Communication) 체계는 기존의 C3에 인공지능 기술을 접목시켜서 인간 결정의 오류를 최소화하고 전력을 재조합하여 적시 적소에 할당할 수 있도록 의사 결정하는 것이다. 모자이크전은 인공지능 접목된 지능형 의사결정 시스템이 지휘관의 의사결정을 돕고 분산된 전력을 재조합하고 임무를 할당하는 통제 역할을 수행한다[3,14].

3.2 모자이크전의 특징

기존의 전력으로 모자이크전 수행 개념을 적용시킬 경우에 아래와 같은 이점을 제공한다[13].

첫째, 기능이 낮은 무기체계는 다중 임무를 갖고 있는 무기체계만큼 고도로 통합하지 않아도 되기 때문

에 새로운 기능의 무기체계를 통합할 수 있는 플랫폼이나 부대의 변화가 크지 않다.

둘째, 전통적인 단일 플랫폼 및 부대 편성에 비해 다양한 방식으로 전력을 운용할 수 있기 때문에 지휘관 선택의 폭이 넓어진다.

셋째, 전력 운용에 있어서 분산된 다양한 전력을 재조합하고 임무를 할당하기 때문에 적에게 아군의 전력 운용을 노출시키지 않고 불안감을 더해준다.

넷째, 전력 운용에 있어서 다양한 형태와 방식으로 운용할 수 있기 때문에 효율성이 증가한다.

다섯째, 효과적인 작전을 위해서 분산된 전력을 표적 맞춤형으로 운용 가능하기 때문에 불필요한 전력의 낭비를 줄이면서 더 많은 단위 전력으로 편성하여 운영할 수 있다.

마지막으로, 무인 시스템은 수많은 동시 임무 수행, 전력 운용 및 임무 할당 조정, 정밀 공격 임무 등이 가능하기 때문에 고 위험의 임무나 공격과 방어 임무의 동시 수행 등 다양한 임무에 할당할 수 있다. 이는 지휘관의 전력 운용 폭을 높여주기도 한다.

4. 능동형 상황 탄력적 사이버 방어작전

모자이크전의 핵심은 인공지능 기술과 자율 시스템을 활용하여 인간의 개입을 최소화하고 지능형 기계통제로 분산된 전력들을 재조합하여 임무를 할당하여 보다 빠르게 전투 프로세스를 진행시키는 것이다. 다양한 표적에 대해서 효과적으로 분산된 전력을 운용할 수 있게 하며 표적 맞춤형으로 전력을 운용함으로써 정확도와 파괴력이 향상되고 적으로 인해서 아군의 전력 운용을 예측하지 못하게 함으로써 불안감과 복잡성을 일으키게 하는 것이다.

최근 사이버공격도 지능형 공격 방식으로 변화되고 있는데, 이를 대응하기 위해서는 인간의 개입을 최소화시키고 자동화된 대응 시스템을 활용하여 사이버전장과 공격 상황에 맞게 대응해야 한다. 특히, 대규모 네트워크를 형성하고 있는 국방망을 보호하기 위해서는 능동적으로 방어 시스템을 사이버전장과 공격 상황에 따라 탄력적으로 운용하는 사이버 방어작전을 전개해야 한다.

4.1 요구사항

지능형 사이버공격을 효과적으로 대응하기 위해서는 능동형 상황 탄력적 사이버 방어작전은 다음과 같은 조건을 충족시켜야 한다.

첫째, 사이버 방어작전에서 지휘관은 모자이크전의 지휘관의 역할과 마찬가지로 최초 지휘와 임무 하달 그리고 최종 결심에만 관여하도록 한다. 인간의 선택과 결정은 인공지능에 비해 상대적으로 오류가 많고 시간도 오래 걸린다. 기존의 사이버공격도 매우 짧은 시간에 이루어지는데, 지능형 사이버공격의 경우는 인공지능 기술을 활용하여 공격경로와 방식 등을 결정하고 보안 시스템도 우회하거나 공격할 수 있기 때문에 인간이 모든 방어과정에 개입한다면, 방어작전은 실패할 확률이 높다.

둘째, 기존의 사이버 방어 및 대응 절차 중심의 작전은 지양한다. 지능형 사이버공격은 인공지능이 탑재되어 아군의 정보통신체계의 시스템과 네트워크, 심지어 보안 시스템 현황 정보까지 알고 있을 가능성이 높다. 그래서 동시에 여러 표적을 공격하거나 몇 만개의 공격 에이전트들을 하나의 표적을 대상으로 분산 공격할 수 있기 때문에 공격 방식이나 형태도 예측할 수 없다. 이러한 공격 방식에 절차 중심적인 방어작전은 효과가 미비할 것이다.

셋째, 모자이크전의 분산된 전력을 재조합해서 운영하듯이 능동형 상황 탄력적 사이버 방어작전도 사이버전장과 공격 상황에 따라 보안 시스템을 운영해야 한다. 공격 징후가 탐지된 이후에 모든 보안 체계를 가동하는 것이 아니라 사이버전장의 환경과 공격 상황에 따라 적시 적소의 보안 시스템을 가동해야 한다. 모든 체계를 가동할 경우에 동일한 기능이 충돌하여 성능이 저하될 수 있으며, 공격 경로를 미리 예측하여 경로에 따라 보안 시스템을 가동할 경우에는 탐지를 못하는 경우가 발생할 것이다.

마지막으로, 하나의 보안 시스템이 악성코드에 감염되면, 다른 보안 시스템이 바로 대응 가동할 수 있어야 한다. 지능형 사이버공격은 보안 시스템을 우회하기도 하지만, 보안 시스템을 공격하는 경우도 있다. 그렇기 때문에 공격으로 인해 보안 시스템 작동이 중지되면 다른 보안 시스템이 신속하게 대체하여 작동해야 한다.

4.2 능동형 상황 탄력적 사이버 방어작전의 수행 개념

본 연구에서 제안하는 능동형 상황 탄력적 사이버 방어작전 수행 개념은 모자이크전의 수행 방식을 적용하여 설계하였다. 사이버작전 사령관의 개입을 최소화하고 인공지능 기반의 운영시스템이 지휘관의 결심을 보조하고 사이버작전에 따라 선택되어 가동하는 보안 시스템을 통제한다. 단, 사이버 킬 스위치(Cyber Kill Switch) 기동은 지휘관에게 추천만 하고 직접 기계가 통제하지 않는다. 능동형 상황 탄력적 사이버 방어작전의 수행 개념은 아래 그림과 같으며, '지능형 사이버공격 대비 상황 탄력적 및 실행 중심의 사이버 대응 메커니즘[16]'을 참고하였다.

(그림 3) 능동형 상황 탄력적 사이버 방어작전의 수행 개념

최상위부대의 지휘관은 전략 및 목적을 달성하기 위하여 인공지능 기반 운영 시스템을 통해서 임무 명령을 하달한다.

인공지능 기반 운영 시스템은 지휘관의 전략과 목적을 가장 효과적으로 달성할 수 있는 사이버 기동을 선택하고 관련 도메인들을 식별한다. 그리고 나서 도메인 내에서 설치되어 있는 보안 체계를 확인한다. 그리고 사이버전장 환경과 사이버공격 상황에 따라 지능형 사이버공격에 대응할 보안 체계를 구성한다. 최종적으로 인공지능 기반 운영 시스템은 최상위 부대 지휘관에게 효과적인 방어를 위한 사이버 기동의 우선순위를 추천하면, 최종 결정은 지휘관이 한다.

사이버 기동은 2장에서의 사이버작전 종류 중에서 방어적 사이버작전으로 구성되어 있다. 사이버 기동은 사이버전장 환경과 지능형 사이버공격의 수준에 따라 하나의 사이버 기동을 실행할 수도 있고 여러 개의 사이버 기동을 동시에 실행할 수도 있다. 여기서 사이버 킬 스위치 기동은 어떤 사이버 기동을 실행하더라도 지능형 사이버공격에 대응할 수 없다고 판단될 경우에 인공지능 기반 운영 시스템이 이 상황을 지휘관에게 제공하면, 지휘관이 최종적으로 사이버 킬 스위치 기동을 결정한다. 사이버 킬 스위치 기동은 도메인별로 연결된 모든 시스템의 전원을 내리거나 대규모의 공격일 경우에는 모든 도메인의 전원을 동시에 차단하는 행위를 의미한다.

도메인은 세분화된 사이버전장으로 육군, 해군, 공군 C4I 체계별 또는 운영하는 국방망의 임무별로 구분할 수도 있으며, 상황에 따라서 구분할 수 있다.

지능형 보안 체계는 현재 운용 중인 지능형 보안 시스템이나 프로그램으로 기능별로 사이버 기동에 적합한 시스템과 프로그램이 인공지능 기반 운영 시스템에 의해서 추천되어 작동하게 된다.

4.3 능동형 상황 탄력적 사이버 방어작전의 수행 기능

능동형 상황 탄력적 사이버 방어작전은 공격 진행에 따라 다음과 같이 기능을 실행한다.

우선, 인공지능 기반 운영 시스템이 사이버공격에 대한 징후 정보를 입수하면, 최상위 부대 지휘관에게 해당 사항을 전달하고 그에 따른 임무 명령을 받는다. 인공지능 기반 운영 시스템은 임무 명령에 따라 사이버기동 중에 국방망 내·외 경계에서 방어할 수 있는 경계방어 기동과 적의 공격을 유인할 수 있는 기만 기동, 조사나 역추적할 수 있는 대응 기동을 선택한다. 그리고 공격 경로로 예측되거나 가장 중요한 도메인을 선정하고 그 도메인에서 운영하는 지능형 보안 시스템이나 프로그램을 사이버 기동에 따라 집중 가동할 수 있도록 준비시키고 지휘관에게 사이버 방어작전 수행 방식을 추천한다.

두 번째는 지능형 사이버공격을 경계방어에서 실패하고 국방망 내부로 침입했을 경우에 인공지능 기반 운영 시스템은 중요 데이터나 정보 보호를 위한 회피기동, 주요 시스템까지 침입하지 못하도록 하는 종심방어기동, 역추적을 위한 대응 기동을 선택하고 현재 사이버공격이 진행되는 도메인과 인접한 도메인의 지능형 보안체계 중에서 지능형 침입탐지 시스템, 통합보안관리시스템, 자가 치유 시스템, 권한 접근 관리 시스템, 포렌식 시스템 등을 집중 가동할 수 있도록 지휘관에게 추천한다.

마지막으로 지능형 사이버공격의 징후를 탐지하고 내부 침입도 확인했음에도 불구하고 공격의 의도와 경로도 파악하지 못하고 사이버 기동을 모두 가동할지도라도 사이버공격이 계속 진행된다면, 사이버 킬 스위치 기동을 추천한다. 사이버 킬 스위치 기동은 지휘관의 승인과 동시에 해당하는 모든 시스템의 전원을 차단하기 때문에 아군의 시스템에도 피해가 발생할 수 있으나, 사이버 공격으로 인한 피해보다는 적기 때문에 방어작전에서 최후의 기동으로 활용한다.

5. 결 론

인공지능 기술이 접목된 지능형 사이버공격은 현재의 대응 전략으로는 효과적으로 차단하기 쉽지 않다. 특히, 표적 시스템에 대한 정보까지도 인공지능을 활용해서 수집하고 있는 상황에서는 정확한 데이터를 기반으로 다양한 방식으로 공격을 실행하기 때문에 현재의 대응 방식으로는 예방과 차단이 쉽지 않다.

최근에 국방분야에도 4차 산업혁명기술과 군사과학기술이 접목되면서 전쟁의 패러다임을 변화시키고 있다. 모자이크전의 수행 개념은 지휘관이 전투 프로세스에 관여하는 것을 최소화하고 전력 운용을 인공지능 기반의 통제 시스템을 통해서 중앙 통제가 아닌 분산된 전력을 군사작전을 성공시킬 수 있도록 재조합하여 운용할 수 있도록 하는 것이다. 또한, 지휘관이 정확한 판단을 내릴 수 있도록 인공지능 기반의 기계통제 시스템으로부터 상세한 정보를 제공받는다. 그래서 본 연구에서는 공격 목적을 달성하기 위해서 분산 운영 중인 전력 상황을 파악하고 표적을 효과적으로 공격할 수 있는 전력을 선별·재조합시켜 보다 신속하고 정확하게 공격할 수 있는 모자이크전의 수행 개념을 사이버 방어작전에 적용함으로써 지능형 사이버공격을 핵심 시스템까지 침입하지 못하도록 유연하게 대응할 수 있는 능동형 상황 탄력적 사이버 방어작전을 제시하였다.

능동형 상황 탄력적 사이버 방어작전은 모자이크전 수행 개념과 유사하게 인공지능 기반의 운영 시스템이 지휘관으로 임무 명령을 받으면 그에 따라 사이버 기동을 선택하고 사이버공격이 예상되거나 발생한 도메인에 설치된 지능형 보안체계 중에 사이버 기동에 부합되는 보안 시스템을 집중 가동 준비시키고 지휘관에 몇 개의 사이버 기동을 추천한다. 제안한 사이버 방어작전은 지능형 사이버공격 상황과 수준에 따라 사이버 기동에 맞는 보안 시스템을 운영할 수 있으며, 동시에 수 개의 사이버 기동을 전개할 수도 있는 장점이 있다.

참고문헌

[1] https://www.boannews.com/media/view.asp?idx= 100307, “해커는 이미 사이버 공격에 AI 활용중... 보안 역시 AI로 강화해야” (검색일: 2021.09.01.).

[2] https://www.datanet.co.kr/news/articleView.html? idx-no =156120, “[2021 사이버 보안 전망④] AI 활용하는 공격”, (검색일: 2021.09.01.).

[3] 장진오, 정재영, “미래전을 대비한 한국군 발전방향 제언: 미국의 모자이크전 수행개념 고찰을 통하여”, 해양안보, 1(1), pp.215-240, 2020.

[4] “CYBERSPACE OPERATIONS AND ELECTROMAGNETIC WARFARE”, Department of The Army, 2021.

[5] “Strategic Cyberspace Operations Guide”, The U.S. Army War College, 2021.

[6] Patrick D. Allen, “Cyber Maneuver and Schemes of Maneuver”, THE CYBER DEFENSE REVIEW, FALL, pp.79-96, 2020.

[7] 엄정호, 김남욱, 정태명, “제4차 산업혁명시대의 사이버전 개론”, 도서출판 홍릉, 2020.

[8] S. D. Applegate, "The principle of maneuver in cyber operations", 2012 4th International Conference on Cyber Conflict (CYCON 2012), pp.1-13, 2012.

[9] 이상운, 박용석, “사이버작전에 대한 공통상황

인식 함양을 위한 군 사이버작전 교육체계 연구 및 방향성 제안정책 제안", 융합보안논문지, 19(4), pp.13-22, 2019.

[10] "Seven Ways to Apply the Cyber Kill Chain® with a Threat Intelligence Platform", A White Paper Presented by Lockheed Martin Corporation, 2015,

[11] 김성중, 유지훈, 오행록, 신동일, 신동규, "사이버전 수행절차 운영개념에 관한 연구", 한국인터넷정보학회, 21(2), pp.73-80, 2020.

[12] "2020 세계 주요 군사동향 6부: 미래전 준비와 차세대 전력 건설", 한국군사문제연구원 연구총서 2021-1, pp.153-197, 2021.

[13] Bryan Clark, Dan Patt, and Harrison Schramm. "Mosaic Warfare", Center for Strategic and Budgetary Assessments, 2020.

[14] 남두현, 임태호, 이대중, 조상근, "4차 산업혁명 시대의 모자이크 전쟁", 국방연구, 63(3), pp.141-170, 2020.

[15] 박지훈, 윤웅직, "모자이크전, 개념과 시사점", 국방논단, 20(35), pp.1-10, 2020.

[16] 김남욱, 엄정호, "지능형 사이버공격 대비 상황 탄력적 및 실행 중심의 사이버 대응 메커니즘", 디지털산업정보학회 논문지, 16(3), pp.69-80, 2020.

[저 자 소 개]

엄 정 호 (Jung-Ho Eom)
1994년 2월 공군사관학교 항공공학과 학사
2003년 2월 성균관대학교 전기전자 및 컴퓨터공학과 석사
2008년 2월 성균관대학교 컴퓨터공학과 박사
2011년 3월~현재 대전대학교 군사학과&안보융합학과 교수
email : eomhun@gmail.com