논문접수 2025.11.16 | ISSN 1738-6144 | Journal of The Korea Association of Defense Industry Studies Vol. 32, No. 3(2025)
논문확정 2025.12.26 | http://journal.kadis.or.kr/ | 한국방위산업학회지 제32권 제3호 | https://doi.org/10.52798/KADIS.2025.32.3.14

사이버 드론 : 자율형 사이버 전력 개념의 제안과 방위산업 전략적 시사점

Cyber Drone : Proposing an Autonomous Cyber Power Concept and Strategic Implications for the Defence Industry

문원식*
Won Sic Mun*

ABSTRACT

This paper analyzes the structural limitations of conventional, human-centered, and reactive cyber operations in the context of increasingly sophisticated cyber threats, including advanced persistent threats (APTs) and supply-chain attacks. To address these limitations, it proposes the concept of a "Cyber Drone" as an autonomous cyber force element that applies the operational logic of physical drones—unmanned operation, persistent reconnaissance, conditional autonomy, and effects-based operations—to the cyber domain.

Cyber Drones are defined not as individual technologies or automated tools, but as distributed force units capable of autonomously performing cycles of reconnaissance, analysis, response, and learning while remaining integrated within a centralized command-and-control framework. Through case analyses of the Stuxnet, NotPetya, and SolarWinds attacks, the paper examines how existing cyber defense architectures—characterized by centralized monitoring and post-incident response—are structurally vulnerable to stealthy and persistent cyber operations, and explores how the Cyber Drone concept may mitigate these vulnerabilities.

The paper further analyzes the legal, ethical, and institutional implications of autonomous cyber power, focusing on attribution, proportionality, accountability, and auditability. It advocates a model of conditional autonomy under human oversight rather than fully autonomous cyber weapons. By framing Cyber Drones as a force element aligned with open architectures, software-defined systems, and service-based operational concepts, the study derives strategic implications for the institutionalization of autonomous cyber power and future defense-industrial development.

초 록

본 연구는 지능형 지속 위협(APT)과 공급망 공격으로 대표되는 고도화된 사이버 위협 환경에서, 기존의 인간 중심·사후 대응형 사이버 작전 체계가 기술적 성능의 문제가 아니라 전력 개념 차원에서 구조적 한계를 지니고 있음을 분석한다. 이러한 한계를 극복하기 위한 대안으로, 본 논문은 '사이버 드론(Cyber Drone)'이라는 자율형 사이버 전력 개념을 제안한다. 사이버 드론은 물리적 드론의 형상을 모방한 기술 개념이 아니라, 무인성, 지속적 정찰, 조건부 자율성, 효과 중심 작전이라는 운용 논리를 사이버 공간에 적용한 전력 단위(force element)로 정의된다.

사이버 드론은 탐색, 분석, 대응, 학습의 기능을 분산·자율적으로 수행하면서 중앙 통제 체계와 결합된 구조를 통해 사이버 공간 전반에 걸친 지속적 작전 수행 가능성을 제시한다. 본 연구는 Stuxnet·NotPetya·SolarWinds 사례 분석을 통해 기존 사이버 방어 체계의 사후 탐지 중심 구조와 중앙집중식 대응 방식이 고도화된 공격에 취약함을 확인하고, 사이버 드론 개념이 이러한 한계를 어떻게 보완할 수 있는지를 개념적으로 검토한다.

아울러 본 논문은 자율형 사이버 전력의 도입과 관련하여 행위 귀속, 비례성, 책임성, 감사 가능성 등 법적·윤리적·제도적 쟁점을 분석하고, 완전 자율이 아닌 인간 통제 하의 조건부 자율성 모델을 제시한다. 나아가 사이버 드론을 개방형 아키텍처와 서비스 기반 전력 운용 개념에 부합하는 전력 요소로 위치시킴으로써, 향후 자율형 사이버 전력의 제도화와 방위산업적 시사점을 도출한다.

Key Words : Cyber Drone(사이버 드론), Autonomous Cyber Power(자율형 사이버 전력), Cyber Operations(사이버 작전), Defense Industry Strategy(방위산업 전략), Autonomous Systems(자율 시스템)

* 지상군연구소 과학화훈련발전센터장(E-mail: K5115857@naver.com)

Ⅰ. 서 론

사이버 공간은 단순한 정보 교환의 장이나 보조적 안보 영역에 머물지 않는다. 오늘날 사이버 공간은 국가, 군, 기업, 범죄 조직 등 다양한 행위자가 상시적으로 경쟁하는 지속적 경쟁 공간의 장으로 인식되고 있다.[1] 이 과정에서 정찰, 침투, 교란, 차단, 회복과 같은 다양한 형태의 사이버 작전이 연속적으로 전개되고 있다. 이러한 변화는 사이버 공간을 하나의 독립된 작전 영역으로 인식하고, 이에 상응하는 새로운 전력 개념을 모색할 필요성을 제기한다.

특히 사이버 위협은 은닉성과 복잡성이 증대되는 양상을 보이고 있다. 특히 사이버 작전은 장기간의 준비와 정찰을 전제로 수행되는 경우가 많으며, 이 과정에서 공격 경로와 행위 주체를 식별하는 것은 구조적으로 어려운 문제로 지적되고 있다.[2] 이러한 환경에서 기존의 인간 중심 분석과 사후 대응에 의존해 온 사이버 운영 방식은 구조적 한계를 드러내고 있다.

기존 사이버 대응 체계는 주로 침해 이후의 탐지와 대응을 중심으로 한 방어적 사고에 기초해 설계되어 왔다는 점이 지적되어 왔다.[3] 침입 탐지와 이상 징후 식별을 중심으로 한 기존 사이버 대응 기능은 일정 수준의 효율성을 제공해 왔으나, 이러한 체계는 사전에 정의된 규칙과 중앙 집중적 통제 구조에 의존하는 경향이 있다. 이로 인해 새로운 공격 방식이나 은닉성이 높은 위협에 대해서는 능동적 대응에 구조적 한계가 존재한다는 점이 지적되어 왔다.[4] 이는 사이버 공간에서도 인간의 직접 개입을 최소화한 상태에서 임무를 수행할 수 있는 새로운 작전 단위의 필요성을 부각시킨다.

이러한 문제의식 속에서 본 연구는 '사이버 드론(Cyber Drone)'이라는 자율형 사이버 전력 개념을 새롭게 제안한다. 사이버 드론은 물리적 드론의 형태를 모방한 것이 아니라, 물리 드론이 지닌 무인성, 지속적 정찰, 자율적 작동, 효과 중심 작전 수행이라는 운용 논리를 사이버 공간의 작전 환경에 맞게 적용한 개념이다. 본 개념은 자동화된 디지털 행위자와 효과 중심 작전 논리에 대한 기존 논의를 이론적 참고 대상으로 삼되, 특정 저자의 개념을 단순히 확장하거나 차용한 것이 아니라, 사이버 작전 환경에 적용 가능한 전력 단위로서 개념적으로 정식화하고자 한다.[5] 사이버 드론은 네트워크, 시스템, 클라우드, 외부 인터넷 등으로 구성된 사이버 공간을 하나의 작전 지형으로 인식하고, 그 안에서 자율적으로 정찰・탐색・분석・대응・학습을 수행하는 무인・자율 작전 유닛으로 이해될 수 있다.

본 연구의 목적은 사이버 드론을 단순한 기술적 도구나 자동화 기능이 아니라, 사이버 공간에서 독립적으로 임무를 수행하는 전력 개념으로 정립하는 데 있다. 이를 위해 본 논문은 사이버 위협 환경의 변화와 자율화 요구를 분석하고, 사이버 드론 개념을 기존 사이버 운영 방식 및 관련 개념과 비교하여 이론적으로 정립하며, 사이버 드론 운용에 수반되는 법적・윤리적・거버넌스 쟁점을 검토한다. 나아가 주요 사이버 작전 사례를 통해 사이버 드론 개념의 적용 가능성을 탐색하고, 방위산업 관점에서의 전략적 시사점을 도출한다.

이에 따라 본 논문은 다음과 같은 연구 질문을 설정한다.

첫째, 사이버 공간의 변화된 위협 환경은 기존 사이버 운영 방식에 어떠한 한계를 드러내고 있는가.

둘째, 사이버 드론은 기존의 사이버 방어 및 자동화 개념과 어떻게 구별되는 새로운 전력 개념으로 정의될 수 있는가.

셋째, 자율형 사이버 전력으로서의 사이버 드론은 법적・윤리적・제도적 측면에서 어떠한 쟁점을 수반하는가.

넷째, 사이버 드론 개념은 방위산업과 사이버 전력화 전략에 어떠한 시사점을 제공하는가.

이러한 연구 질문에 답하기 위해 본 논문은 개념 분석, 비교 정책 분석, 사례 기반 추론을 결합한 질적 연구 방법을 활용한다. 본 연구는 실증적 기술 구현을 목표로 하지 않으며, 사이버 드론이라는 개념이 갖는 이론적 정합성과 정책적・전략적 함의를 분석하는 데 초점을 둔다. 이를 통해 본 연구는 자율형 사이버 전력 논의의 출발점으로서 사이버 드론 개념을 제시하고자 한다.

1) Libicki, Martin C., Cyberdeterrence and Cyberwar, RAND Corporation, 2009, ch.1.

2) Rid, Thomas, Cyber War Will Not Take Place, Oxford University Press, 2013, ch.2.

3) Libicki. 2009.

4) Libicki. 2009. ch.2.

5) Singer, P. W. & Brooking, E. T., LikeWar: The Weaponization of Social Media, Houghton Mifflin Harcourt, 2018.

Ⅱ. 연구 배경 및 관련 연구

2.1 사이버 위협 환경의 변화와 작전 공간으로서의 사이버 공간

사이버 공간은 기술 발전과 함께 그 성격이 변화해 왔으며, 초기의 사이버 위협이 주로 개별 시스템 침해나 정보 탈취와 같은 제한된 형태로 인식되었던 것과 달리, 점차 국가 전략과 연계된 은닉적·지속적 작전 양상으로 이해되고 있다.[6] 특히 지능형 지속 위협(Advanced Persistent Threat, APT)과 자동화된 악성코드의 반복적 확산은, 사이버 공간이 단발성 사건의 무대가 아니라 상시적인 경쟁과 충돌이 이루어지는 작전 공간임을 보여준다.[7]

이러한 변화는 사이버 공간의 작전적 특성을 더욱 부각시킨다. 기존 연구에 따르면, 사이버 작전은 물리적 전장과 달리 공간적 경계가 불분명하고, 공격과 방어의 구분이 모호하며, 행위자의 식별과 귀속에 구조적 어려움이 수반된다는 점이 논의되어 왔다.[8] 또한, 사이버 공간에서는 공격 준비·침투·효과 발생까지의 주기가 매우 짧게 압축되는 경향이 있으며, 이로 인해 인간 중심의 의사결정만으로는 실시간 대응에 구조적 제약이 발생할 수 있음이 지적된다.[9] 이로 인해 사이버 작전은 점차 속도와 자율성을 중심으로 한 전력 운용 방식으로 이동하고 있다.

2.2 기존 사이버 운영 방식의 한계

현재 다수의 국가 및 조직에서 운용 중인 사이버 대응 체계는 전반적으로 방어 중심의 구조를 유지하고 있다. 침입 탐지 시스템(Intrusion Detection System, IDS), 방화벽, 위협 인텔리전스 공유 체계, 그리고 최근 확산된 보안 오케스트레이션·자동화(Security Orchestration, Automation, and Response, SOAR) 도구들은 일정 수준의 자동화를 제공하지만, 이러한 체계의 기본 운용 논리는 여전히 사전에 정의된 규칙과 인간 중심의 의사결정 구조에 기반하는 경향을 보이며, 이에 따른 한계가 지적되고 있다.[10]

기존의 규칙 기반 사이버 대응 구조는 알려진 위협이나 반복적인 공격에 대해서는 일정한 효과를 발휘할 수 있으나, 새로운 공격 기법이나 은닉성이 높은 작전에 대해서는 대응 지연이나 사후 대응에 머무를 수 있다는 한계가 내재되어 있다.[11] 특히 사이버 작전의 준비 단계나 초기 침투 단계에서 능동적으로 개입하기에는 구조적 한계가 존재한다. 이는 기존 사이버 운영 방식이 사후 탐지·대응 중심에서 벗어나지 못하고 있음을 의미한다.

2.3 무인·자율 체계 연구 동향

이러한 한계를 보완하기 위해, 다양한 분야에서 무인·자율 체계에 대한 연구와 운용이 확대되어 왔다. 특히 물리적 전장에서는 무인항공기(UAV)를 중심으로 무인체계가 정찰·감시·타격 임무에 활용되며, 군사 작전에서의 역할이 점차 확대되고 있다.[12] 이들 체계의 공통점은 인간의 직접 개입을 최소화하려는 방향으로 설계되었으며, 사전에 설정된 규칙과 제한된 자율성을 통해 임무 수행의 효율성과 지속성을 제고한다는 데 있다.

사이버 분야에서도 인공지능과 머신러닝을 활용한 자동화 연구가 진행되고 있으나, 다수의 연구는 특정 기능의 고도화에 초점을 맞추고 있다. 예를 들어 이상 탐지 정확도 향상이나 대응 절차의 자동화는 논의되었으나, 사이버 공간 전체를 작전 지형으로 인식하고 임무 단위로 운용되는 자율 체계에 대한 논의는 상대적으로 제한적이다.

2.4 기존 연구의 한계와 '사이버 드론' 개념의 필요성

기존의 사이버 자동화 및 자율화 연구는 기술적 효율성 향상에는 기여하였으나, 사이버 공간에서의 전력 단위와 작전 개념을 재정의하는 데까지는 이르지 못하였다. 대부분의 연구는 방어 체계의 보조 수단 또는 운영 효율화 도

6) Libicki. 2009.
7) Rid. 2013. ch.2.
8) Rid. 2013. ch.2.
9) Libicki. 2009. ch.2.
10) Libicki. 2009. ch.2.
11) Libicki. 2009. ch.2.
12) Singer & Brooking. 2018. ch.1.

구로서 사이버 자동화를 다루고 있으며, 독립적으로 임무를 수행하는 자율 작전 주체로서의 사이버 시스템에 대한 논의는 부족하다.

이러한 한계는 사이버 공간의 변화된 성격과 요구를 충분히 반영하지 못한다. 사이버 공간이 상시적 경쟁의 장으로 변화한 상황에서, 단순한 방어 자동화는 근본적인 해결책이 되기 어렵다. 이에 따라 본 연구는 사이버 공간에서도 물리 드론과 유사한 운용 논리를 갖는 자율형 작전 단위, 즉 '사이버 드론' 개념이 필요하다는 문제의식에서 출발한다.

2.5 소결

본 장에서는 사이버 위협 환경의 변화와 기존 사이버 운영 방식의 한계를 검토하고, 무인·자율 체계 연구 동향을 통해 사이버 공간에서 자율화 요구가 제기되는 배경을 분석하였다. 분석 결과, 기존 사이버 대응은 기술적 자동화 수준이나 개별 기능의 고도화에 주로 초점을 두어 왔으며, 사후 탐지와 중앙집중식 대응 구조에 기반한 기존 전력 개념 자체가 은닉적·지속적 위협에 대해 구조적 한계를 지니고 있음을 확인하였다.

아울러 국내 선행연구는 사이버 작전을 기술적 보안 체계, 정책적 대응, 또는 개별 운용체계 개선의 관점에서 주로 논의해 왔으나, 사이버 공간에서 독립적으로 임무를 수행하는 전력 단위 차원에서 자율형 사이버 전력을 개념화한 연구는 제한적인 것으로 나타났다. 이러한 분석은 사이버 공간에서 단순한 방어 자동화를 넘어, 자율성과 지속성을 전제로 한 새로운 전력 단위에 대한 개념적 전환이 요구됨을 시사한다.

Ⅲ. 사이버 드론 개념 정립

3.1 사이버 공간의 작전 환경 변화

사이버 공간은 단순한 정보 교환의 장이나 물리적 전장을 보조하는 부수적 영역에 머물지 않는다. 기존 연구에 따르면, 오늘날 사이버 공간은 국가·군·기업·범죄 조직 등 다양한 행위자가 상시 경쟁하는 지속적 경쟁 공간으로 인식되고 있으며, 이 과정에서 정찰·침투·교란·차단·회복과 같은 다양한 형태의 작전이 전개되는 양상이 관찰된다.[13]

초기의 사이버 위협이 개별 시스템 침해나 정보 탈취에 국한되었던 것과 달리, 최근의 사이버 작전은 국가 전략과 연계된 지능형·지속형 작전으로 발전해 왔다는 논의가 되어 왔다.[14] 특히 지능형 지속 위협(APT), 공급망 공격, 자동화된 악성코드 확산 등은 사이버 공간이 단발성 사건의 무대가 아니라 상시적인 작전 환경임을 보여준다. 이러한 변화는 사이버 공간을 단순한 방어 대상이 아닌, 능동적으로 관리·운용되어야 할 작전 영역으로 인식할 필요성을 시사한다.

3.2 자율형 사이버 전력 개념의 필요성

기존 사이버 운영 방식은 주로 사후 탐지와 대응 중심으로 설계되어 왔으며, 알려진 위협이나 반복적인 공격에 대해서는 일정 수준의 효과를 보여 왔다는 점이 관찰된다.[15] 그러나 새로운 공격 기법이나 은닉성이 높은 작전에 대해서는 대응이 지연되거나 사후 대응에 머무르는 경향이 나타나며, 특히 사이버 작전의 준비 단계나 초기 침투 단계에서 선제적으로 개입하는 데에는 구조적 제약이 존재한다는 분석이 이루어지고 있다.[16]

이러한 구조적 제약은 기존 사이버 방어 체계만으로는 한계가 있음을 시사하며, 자율성과 지속성을 갖춘 새로운 사이버 전력 개념의 필요성으로 연결된다. 자율형 사이버 전력은 인력 부담을 경감하는 수단을 넘어, 작전의 속도와 연속성을 구조적으로 보장하기 위한 핵심 요소로 인식될 수 있다.

3.3 사이버 드론의 정의

본 연구에서 제안하는 사이버 드론은 물리적 드론의 형

13) Libicki. 2009.
14) Rid. 2013.
15) Libicki. 2009.
16) Libicki. 2009.

태나 플랫폼을 모사한 개념이 아니라, 드론이 지닌 무인성, 지속적 정찰, 자율적으로 수행되는 판단 과정, 임무 중심 운용이라는 작전 논리를 사이버 공간의 작전 환경에 맞게 재구성하여 적용한 자율형 운용 단위를 의미한다. 즉, 사이버 드론은 네트워크, 시스템, 클라우드, 외부 인터넷 환경 등 사이버 공간 전반에서 자율적으로 탐색・분석・대응・학습을 수행하는 무인 운용체계이다.

사이버 드론은 개별 보안 기능이나 단일 자동화 도구가 아니라, 특정 임무를 수행하는 전력 단위로 이해된다. 본 논문에서 '전력 단위'란, 개별 기술이나 기능이 아니라 독립적인 임무 부여와 운용, 그리고 작전 효과 평가가 가능한 최소 전력 구성 요소를 의미한다.

이는 사이버 역량이 물리적 전력을 보조하는 수단에서 벗어나, 사이버 공간에서 자체적으로 작전 효과를 창출할 수 있는 전력으로 확장되는 개념적 전환을 의미한다.

이에 따라 본 논문에서는 사이버 드론의 운용 특성을 지칭함에 있어 '자율형'이라는 용어를 일관되게 사용하며, 이는 인간의 통제와 규범적 제약 하에서 운용되는 조건부 자율성을 전제로 한다.

3.4 사이버 드론의 핵심 특성

사이버 드론의 핵심 특성은 무인성, 자율성, 협업성, 확장성으로 요약될 수 있다. 사이버 드론은 상시적인 인간 개입 없이도 자율적으로 임무를 수행하도록 설계되며, 탐색・분석・대응・학습의 전 과정이 사전에 정의된 규칙과 알고리즘에 따라 자동으로 수행된다. 또한 개별 드론은 독립적으로 작동하면서도 중앙 통제 체계와 연동되어 정보 공유와 임무 조정이 가능하며, 기관망・외부망・클라우드 환경 등 다양한 사이버 공간 계층으로 운용 범위를 유연하게 확장할 수 있다.

이러한 특성은 사이버 드론을 단순한 자동화 기술이 아닌, 지속적이고 능동적인 작전 수행을 전제로 설계된 핵심 전력 요소로 기능하게 한다.

3.5 기존 사이버 운영 개념과의 비교

사이버 드론의 개념적 독창성을 명확히 하기 위해서는 기존 사이버 운영 개념과의 비교가 필요하다. 기존 사이버 방어 체계와 자동화 도구, 그리고 최근 논의되고 있는 자율 방어 개념은 각각 일정한 역할을 수행해 왔으나, 사이버 드론과는 운용 목적과 작전 단위의 성격에서 본질적인 차이가 있다.

기존 방어 체계는 방어 중심의 시스템 단위 운용에 초점을 두었으며, 자동화 도구는 반복 업무의 효율화를 목표로 설계되었다. 자율 방어 개념은 일부 자율성을 도입하였으나, 여전히 방어 범주 내에서 제한적으로 운용되는 경우가 많다. 반면, 사이버 드론은 사이버 공간에서 자율적으로 임무를 수행하는 전력 단위로서, 능동적 정찰과 임무 기반 자율성을 중심 개념으로 한다. 이러한 차이는 〈표 1〉의 비교를 통해 보다 명확히 확인할 수 있다.

〈표 1〉에서 확인할 수 있듯이, 사이버 드론은 기존 사이버 방어 체계나 자동화 도구와 달리 단일 기능이나 시스템 차원의 개선이 아니라, 사이버 공간에서 자율적으로 임무를 수행하는 전력 단위로 개념화된다. 이러한 차별성은 단순히 운용 목적의 변화에 그치지 않고, 사이버 드론이 어떠한 구조로 배치되고, 어떠한 방식으로 운용되는가에 대한 구조적 설명을 요구한다.

즉, 사이버 드론을 하나의 전력 개념으로 이해하기 위해서는 개별 기능 비교를 넘어, 분산된 자율 유닛과 이를 통합 관리하는 체계가 어떻게 결합되어 작전 효과를 창출하는지를 살펴볼 필요가 있다.

〈표 1〉 기존 사이버 운영 개념과 사이버 드론의 비교

구 분	기존 방어 체계	자동화 도구	자율 방어 개념	사이버 드론
운용 목적	방어 중심	운영 효율화	방어 고도화	자율적 임무 수행
작전 단위	시스템	기능/모듈	시스템	전력 단위(자율 유닛)
탐색 방식	수동・반응형	제한적 자동화	부분적 능동	지속적・능동적 정찰
자율성 수준	낮음	제한적	중간	임무 기반 조건부 자율성
협업 운용	제한적	제한적	일부 가능	중앙 통제 하 군집 운용
작전 범위	방어 영역	방어 영역	방어 중심	정찰・분석・대응・학습 전 주기

3.6 사이버 드론의 운영 구조와 운용 메커니즘

사이버 드론은 단일 시스템이 아니라, 분산 배치된 다수의 자율 유닛과 이를 통합 관리하는 중앙 통제 체계로 구성된 전력 구조이다. 개별 사이버 드론은 외부 인터넷 환경, 기관 내부망, 클라우드 환경 등 사이버 공간의 각 계층에 배치되어, 해당 환경의 특성과 위협 양상에 맞는 정찰 및 분석 임무를 수행한다.

각 자율 유닛은 자신이 배치된 환경 내에서 네트워크 트래픽, 시스템 행위, 이상 징후를 상시 감시하며, 사전에 정의된 임무 범위와 운용 규칙, 그리고 학습된 모델에 따라 위협 가능성을 평가한다. 이 과정에서 개별 유닛은 단순한 탐지 기능에 머무르지 않고, 탐색과 분석을 바탕으로 위협을 분류하고 대응 우선순위를 판단하는 최소 작전 단위로 기능한다. 또한 탐지된 정보와 분석 결과는 중앙 통제 체계와 공유되어, 개별 판단이 전체 작전 맥락 속에서 재해석될 수 있도록 설계된다.

중앙 통제 체계는 이러한 분산 유닛들로부터 수집된 정보를 종합·상관 분석하여 전체 작전 상황을 통합적으로 인식한다. 중앙 통제 체계는 개별 사이버 드론의 모든 행위를 실시간으로 직접 통제하지는 않지만, 분산 유닛들의 판단 결과를 조정하거나 임무를 재할당하고, 필요 시 임무 우선순위 조정이나 추가 정찰 지시를 하달함으로써 분산된 사이버 드론의 운용 방향을 조정한다. 이를 통해 사이버 드론 체계는 특정 지점의 이상 징후를 국지적 사건으로 처리하는 데 그치지 않고, 여러 계층에서 발생하는 신호를 하나의 작전 상황으로 통합 인식할 수 있다.

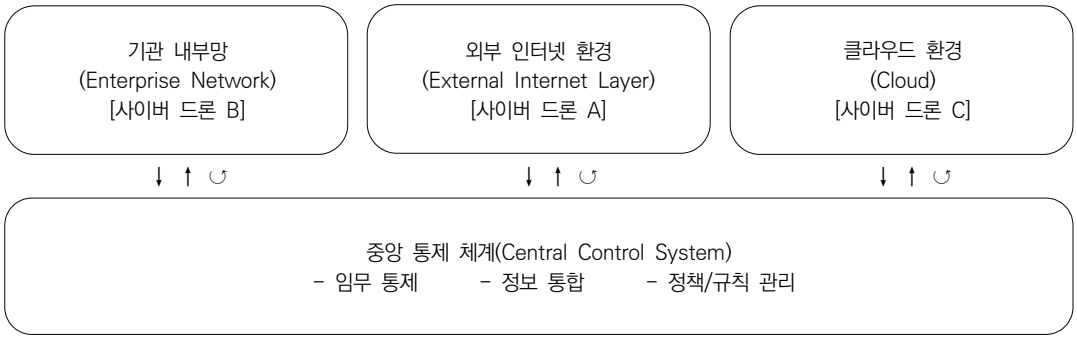
주목할 점은 이와 같은 구조가 완전한 중앙집중형 통제 체계도, 완전한 분산 자율 체계도 아니라는 점이다. 사이버 드론은 평시에는 분산 유닛의 자율성을 최대한 활용하여 상시 정찰과 대응을 수행하되, 임계 상황에서는 중앙 통제 체계를 통해 판단 기준과 작전 방향을 조정하는 조건부 자율 운용 구조를 따른다. 이러한 구조는 인간의 개입을 배제하기보다는, 인간의 개입 지점을 사후 대응 단계가 아니라 사전 설계와 운용 규칙 설정 단계로 이동시킨다는 점에서 기존의 인간 중심 사이버 운영 방식과 구별된다.

사이버 드론의 계층별 배치와 중앙 통제 체계 간의 연동 구조는 〈그림 1〉에 제시되어 있다. 본 그림은 외부 인터넷 환경, 기관 내부망, 클라우드 환경 등 사이버 공간의 각 계층에 분산 배치된 사이버 드론이 중앙 통제 체계와 연동되어 자율적 정찰과 임무 수행을 수행하는 구조를 개념적으로 나타낸 것이다.

3.7 사이버 드론의 단계별 작동 흐름

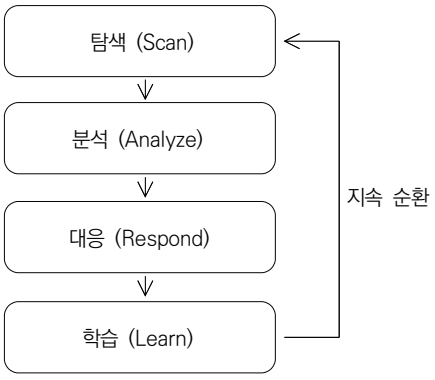
사이버 드론의 운용은 탐색·분석·대응·학습의 네 단계로 구성되며, 이는 단발적 절차가 아닌 순환적 작동 구조를 갖는다. 탐색 단계에서는 네트워크 트래픽과 시스템 행위를 지속적으로 관찰하여 이상 징후를 식별하고, 분석 단계에서는 탐지된 행위의 위험도를 평가한다. 대응 단계에서는 분석 결과에 따라 차단·격리·경보 등의 조치가 자율적으로 수행되며, 학습 단계에서는 대응 결과가 데이터로 축적되어 이후 판단의 정확도를 향상시키는 데 활용된다.

이와 같은 단계별 운용 흐름은 사이버 드론이 사후 대응 중심의 체계를 넘어, 지속적이고 능동적인 작전 수행을



〈그림 1〉 사이버 드론의 계층별 배치 및 통제 구조 개념도

가능하게 하는 핵심 메커니즘이다. 사이버 드론의 단계별 작동 흐름은 〈그림 2〉에 제시되어 있다.



〈그림 2〉 사이버 드론의 단계별 작동 흐름도

본 그림은 사이버 드론이 탐색, 분석, 대응, 학습의 네 단계를 순환적으로 수행함으로써 지속적인 정찰과 적응적 작전 수행이 가능함을 개념적으로 표현한 것이다.

3.8 소결

본 장에서는 사이버 공간의 작전 환경 변화와 자율형 사이버 전력에 대한 논의를 바탕으로 사이버 드론의 개념을 정립하였다. 사이버 드론은 단순한 보안 기술이나 자동화 도구가 아니라, 사이버 공간에서 상시적인 인간 개입 없이 사전에 설계된 규칙과 정책에 따라 임무를 수행하되, 중앙 통제 체계와 결합된 조건부 자율 구조를 갖는 전력 단위로 이해될 수 있다. 특히 운영 구조와 단계별 작동 흐름을 제시함으로써, 사이버 드론이 개념적 제안에 그치지 않고 운용 가능한 자율형 사이버 전력 개념으로 정식화될 수 있음을 논증하였다.

Ⅳ. 사이버 드론 운용의 법·윤리·거버넌스 쟁점

4.1 자율형 사이버 전력 논의의 전제

사이버 드론은 자율적 판단과 임무 수행을 핵심 속성으로 하는 전력 개념이므로, 기술적 효율성뿐 아니라 법적 정당성, 윤리적 수용성, 제도적 통제 가능성이 함께 논의될 필요가 있다. 특히 사이버 공간은 물리적 전장과 달리 행위자의 식별과 행위 귀속이 구조적으로 불확실하며, 작전 효과의 범위가 비가시적으로 확산될 가능성을 지닌다.[17] 이러한 특성은 자율형 사이버 전력의 도입이 기존 법·윤리·제도 체계에 어떠한 도전을 제기하는지를 검토할 필요성을 시사한다.

본 논문에서 '사이버 드론'은 공격 자동화를 지향하는 개념이 아니라, 정찰·식별·분석과 저위험 대응을 중심으로 한 조건부 자율 운용을 전제로 하며, 물리적·전략적 영향을 수반하는 고위험 효과는 인간의 명시적 통제 하에 제한된다.

본 장은 사이버 드론을 무제한적 자동화 수단이 아닌, 규범적 통제 가능성이 전제된 자율형 사이버 전력으로 위치시키기 위해, 주요 쟁점을 국제법·윤리·거버넌스 관점에서 체계적으로 분석한다.

4.2 행위 귀속성과 국제법적 고려

사이버 작전에서 행위 귀속성은 반복적으로 핵심적인 법적 쟁점으로 논의되어 왔다.[18] 국제법 논의에서는 사이버 행위의 국가 귀속 여부를 판단함에 있어, 해당 행위가 국가기관에 의해 수행되었는지, 또는 국가의 지시나 실질적 통제 하에서 이루어졌는지가 주요 쟁점으로 다루어져 왔다.[19] 이러한 원칙과 적용 기준은 Tallinn Manual 2.0에서 체계적으로 정리되어 있으며, 사이버 행위의 귀속 판단이 기술적·법적 불확실성을 내포한다는 점이 논의되어 왔다.

사이버 드론은 자율적 의사결정 구조를 포함한다는 점에서 행위 귀속 문제를 형식적으로 복잡하게 만들 수 있다. 그러나 본 연구에서 제안하는 사이버 드론의 자율성은 완전한 독립성이 아니라, 자율무기체계 일반에 대한 기존

17) Lin, Herbert S., "Attribution of Malicious Cyber Incidents: From Soup to Nuts", Journal of National Security Law & Policy, Vol.7, No.2, 2015.

18) Schmitt, Michael N. (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017.

19) Schmitt(ed.). 2017.

논의에서 강조되어 온 바와 같이, 사전에 정의된 임무 목표, 운용 규칙, 정책적 제한 내에서 작동하는 조건부 자율성에 해당한다. 사이버 드론의 작전 수행은 국가 또는 조직이 설정한 운용 프레임에 종속되며, 국제법상 그 결과에 대한 법적 책임은 원칙적으로 운용 주체에 대한 귀속의 문제로 다루어질 수 있다.[20]

이와 같은 구조는 자율형 사이버 전력이 기존 국제법 체계와 단절되는 것이 아니라, 기존 책임 귀속 원칙 하에서 해석 가능한 범주 내에 위치함을 시사한다.

4.3 비례성・필요성 원칙과 효과 통제

국제인도법과 사이버 작전 규범에서는 비례성과 군사적 필요성이 핵심적인 판단 기준으로 적용된다. 이러한 기준은 사이버 작전 일반에 대해 정립된 원칙으로서, 본 연구에서 제안하는 사이버 드론과 같이 자율적 대응 효과를 수행하는 전력 개념을 평가하는 데 중요한 분석 기준으로 활용될 수 있다.[21] 또한 기존 연구에서는 사이버 작전에서 자동화되거나 통제 범위가 제한된 작전 효과가 발생할 경우, 그 영향이 의도하지 않게 확산되거나 과도한 피해로 이어질 수 있다는 우려가 제기되어 왔다.[22] 사이버 작전의 특성상 효과 범위가 비가시적으로 확산될 수 있다는 점은, 비례성 판단과 효과 통제의 필요성을 더욱 강화한다.

이를 완화하기 위해 사이버 드론은 효과 수행 단계에서 다층적 제한 구조를 갖출 필요가 있다. 예를 들어, 정보 수집이나 정찰 단계에서는 상대적으로 높은 수준의 자율성을 허용하되, 네트워크 차단이나 시스템 격리와 같은 고위험 효과는 사전에 정의된 임계 조건을 충족해야만 수행되도록 제한할 수 있다. 이러한 접근은 자율성과 통제 간의 균형을 유지하는 현실적 제도 설계 방향으로 평가될 수 있다.

4.4 인간 통제 모델과 자율성의 범위

자율형 전력에 대한 국제적 논의에서는 인간의 통제 수준이 반복적으로 핵심 쟁점으로 제기되어 왔으며, 자율무기체계 전반에서 완전 자율형 체계보다는 인간-개입형 통제(Human-in-the-loop) 또는 인간-감독형 통제(Human-on-the-loop) 구조가 바람직한 설계 방향으로 제시되고 있다.[23] 본 연구에서 제안하는 사이버 드론 역시 이러한 논의 틀을 참조하여, 인간의 통제가 유지되는 조건부 자율 구조를 전제로 한다.

인간-개입형 통제는 주요 작전 효과 수행 이전에 인간의 승인 절차를 요구하는 방식이며, 인간-감독형 통제는 자율 운용을 허용하되 인간이 상시 개입할 수 있는 구조를 의미한다. 본 연구는 사이버 드론의 임무 특성과 위험 수준에 따라 이러한 통제 방식을 단계적으로 조합하는 혼합형 통제 모델이 현실적인 대안이 될 수 있음을 제안한다.

4.5 책임성, 투명성 및 감사 가능성

사이버 작전의 제도화 논의에서는 책임성과 감사 가능성이 핵심적인 요소로 반복적으로 제기되어 왔으며, 이는 행위의 귀속과 책임 판단을 가능하게 하는 제도적 기반으로 이해된다.[24] 이러한 규범적 요구를 본 연구에서 제안하는 사이버 드론 운용에 적용할 경우, 탐색・분석・대응・학습의 전 과정에서 생성되는 주요 의사결정 정보를 기록・보관할 수 있는 체계의 구축이 필요하다. 이러한 기록은 사후 작전 평가뿐 아니라 법적・정책적 책임 소재를 명확히 하는 근거로 활용될 수 있으며, 자율형 사이버 전력에 대한 조직 내부 및 외부의 신뢰를 제고하는 요소로 작용할 수 있다.

이와 같은 책임성과 감사 가능성의 제도적 확보는 사이버 드론의 자율성이 국제법과 윤리적 기준 하에서 운용될 수 있는 최소한의 제도적 조건이라는 점에서, 본 장의 논의를 종합하는 핵심 요소라 할 수 있다.

4.6 소결

본 장에서는 자율형 사이버 전력 개념의 도입과 관련하여 행위 귀속, 비례성, 책임성, 감사 가능성 등 주요 법적・

20) Schmitt. 2017.

21) Schmitt(ed.). 2017.

22) Libicki. 2009.

23) UN CCW Group of Governmental Experts on Lethal Autonomous Weapons Systems. Report of the 2019 Session, United Nations, 2019.

24) Schmitt(ed.). 2017.

윤리적 쟁점을 검토하였다. 분석 결과, 사이버 드론과 같은 자율성을 내재한 전력 개념은 기술적 효율성만으로는 정당화될 수 없으며, 인간 통제 하의 조건부 자율성과 제도화된 책임·감사 체계를 전제로 할 때 비로소 제도적 수용 가능성을 확보할 수 있음을 확인하였다. 이는 사이버 드론 개념이 기존 법·윤리·제도 틀과의 정합성 속에서 발전되어야 할 전력 개념임을 시사한다.

Ⅴ. 주요 사이버 작전 사례 분석과 사이버 드론 적용 가능성

5.1 사례 분석의 목적과 접근 방법

본 장의 목적은 대표적인 고도화 사이버 작전 사례를 분석함으로써, 기존 사이버 운영 체계의 구조적 한계를 확인하고, 본 연구에서 제안하는 사이버 드론 개념이 실제 작전 환경에서 어떠한 작전적 차이를 만들어낼 수 있는지를 검토하는 데 있다. 특히 본 연구는 사이버 드론을 무제한적 자율 체계가 아닌, 인간 통제와 규범적 제약 하에서 운용되는 조건부 자율형 사이버 전력으로 개념화한다는 점에서, 기존 기술 중심 논의와 구별된다.

현실적으로 사이버 드론의 실제 운용 사례는 존재하지 않으므로, 본 장에서는 과거에 발생한 사이버 작전을 기준으로, 동일한 조건 하에서 사이버 드론이 운용되었을 경우의 변화를 가정적으로 검토하는 가상 적용 시나리오 방식을 활용한다.

다만 본 장의 사례 분석은 개별 사건의 상세 서술에 목적이 있지 않다. 세 사례는 모두 중앙집중식·사후 대응 중심의 기존 사이버 운영 체계가 은닉성·지속성·신뢰 경로 악용을 특징으로 하는 공격에 구조적으로 취약함을 공통적으로 보여준다. 이에 따라 각 사례에서는 동일한 한계 설명을 반복하기보다, 공격 양상의 차이와 그에 따른 사이버 드론 적용 가능성의 차별적 지점에 분석의 초점을 둔다.

5.2 Stuxnet 사례와 사이버 드론 적용 가능성

Stuxnet 공격은 이란 핵시설을 표적으로 한 고도화된 사이버 작전으로, 악성코드가 물리적 설비에 직접적인 영향을 미친 대표적 사례로 평가된다. 이 공격은 다수의 제로데이 취약점 활용, 내부망 침투, 장기간 은닉이라는 특징을 통해 기존 사이버 방어 체계의 구조적 한계를 드러내는 사례로 논의되어 왔다.[25]

기존 사이버 대응 체계는 Stuxnet 공격의 초기 침투와 내부 확산을 조기에 탐지하지 못하였다. 이는 중앙집중식 모니터링과 정적 규칙 기반 탐지 방식이 은닉성과 지속성을 특징으로 하는 공격에 구조적으로 취약함을 보여준다. 특히 산업 제어 시스템 환경에서는 정상 제어 신호와 악성 행위 간의 구분이 어렵다는 점이 제약 요인으로 작용한 것으로 분석된다.[26] 이러한 양상은 기존 사이버 운영 방식이 사건 발생 이후의 탐지와 대응에 집중되어 있으며, 공격 준비 단계나 은닉 단계에서 선제적으로 개입하기 어렵다는 구조적 한계를 시사한다.

사이버 드론이 운용되었다면, 산업 제어 시스템 환경 내에서 지속적이고 능동적인 정찰 임무를 수행함으로써 정상 제어 신호의 장기적 패턴과 미세한 편차를 반복적으로 학습·분석했을 개연성이 있다. 이를 통해 공격의 은닉 단계에서 이상 징후를 조기에 포착했을 가능성이 제기된다. 또한 사이버 드론은 고위험 효과 수행 이전에 중앙 통제 체계 또는 인간 운영자의 개입을 전제로 하는 조건부 자율 구조를 갖기 때문에, 무분별한 자동 대응이 아닌 비례적·국지적 대응으로 연결될 여지를 제공했을 것으로 평가된다.

5.3 NotPetya 사례와 사이버 드론 적용 가능성

NotPetya 공격은 공급망을 통해 확산된 파괴적 악성코드로, 단기간에 글로벌 기업과 국가 인프라에 막대한 피해를 초래한 대표적 사례로 평가된다.[27] 이 사례는 사이버

25) Langner, Ralph. "Stuxnet: Dissecting a Cyberwarfare Weapon", IEEE Security & Privacy, Vol. 9, No. 3, 2011.

26) Langner. 2011, pp.51-52.

27) Greenberg, Andy, Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers, Doubleday, 2019.

작전의 효과가 단일 표적에 국한되지 않고, 연쇄적으로 확산될 수 있음을 보여준다.

NotPetya 공격은 정상적인 소프트웨어 업데이트 경로를 악용함으로써, 기존 보안 체계가 신뢰하던 채널 자체를 공격 벡터로 활용한 사례로 인용되어 왔다. 기존 연구에 따르면, 다수의 조직은 공격이 확산된 이후에야 이상 징후를 인지하였으며, 대응 역시 조직별로 분절적이고 사후적으로 이루어졌다.[28] 이러한 양상은 중앙집중식 대응 구조와 사후 탐지 중심의 운영 방식이 공급망 기반 공격에 구조적으로 취약함을 보여준다.

사이버 드론이 운용되었다면, 공급망 업데이트 과정에서 발생하는 통신 구조와 행위 패턴을 상시 탐색·분석함으로써 정상 업데이트와 다른 변화를 조기에 식별했을 가능성이 있다. 분산 배치된 사이버 드론은 업데이트 서버, 내부 네트워크, 외부 연결 지점을 연속적으로 관찰하며, 중앙 통제 체계와 연동하여 확산 이전 단계에서 대응 조치를 수행할 여지를 제공했을 것으로 평가된다. 이러한 대응은 사전에 정의된 정책과 인간 통제 하에 수행됨으로써, 자율성과 책임성 간의 균형을 유지할 수 있다.

5.4 SolarWinds 사례와 사이버 드론 적용 가능성

SolarWinds 공격은 정상적인 IT 관리 소프트웨어 업데이트 경로를 악용한 대표적인 공급망 기반 사이버 작전으로, 미국 정부 기관과 다수의 글로벌 기업을 장기간 은닉 상태에서 침해한 사례로 평가된다.[29] 이 공격은 단일 취약점 공격이 아니라, 소프트웨어 개발·배포·운영 전반에 걸친 신뢰 체계를 체계적으로 악용하였다는 점에서 기존 사이버 작전과 구별된다.

SolarWinds 사례에서 기존 사이버 대응 체계는 공격자가 정상적인 업데이트 프로세스에 악성코드를 삽입하는 과정에서 이를 탐지하지 못하였다. 이는 기존 보안 체계가 외부 침입이나 명백한 이상 행위를 중심으로 설계되어 있으며, 신뢰된 내부 공급망과 관리 체계에 대한 지속적 감시에는 구조적 한계가 있음을 시사한다.[30] 특히 공격이 수개월간 은닉 상태로 유지되면서 정보 수집과 측면 이동이 이루어졌음에도, 다수의 피해 조직은 사후적으로 침해 사실을 인지하였다. 이는 중앙집중식 보안 관제와 사후 탐지 중심의 운영 방식이 장기적·저가시성 공격에 취약함을 드러낸 사례로 이해된다.

사이버 드론이 운용되었다면, 소프트웨어 개발·배포·업데이트 전 과정에서 정상 행위의 기준선을 장기적으로 학습·분석함으로써, 신뢰된 경로 내에서 발생하는 미세한 행위 변화 역시 감시 대상에 포함했을 개연성이 있다. 이러한 접근은 공급망 내부에서의 은닉형 공격을 조기에 식별하는 데 기여할 수 있으며, 분산된 탐지 결과를 중앙 통제 체계에서 통합 분석함으로써 전체 작전 상황에 대한 인식을 제고했을 가능성이 있다.

5.5 사례 분석의 시사점

세 사례는 서로 다른 방식으로 전개되었으나, 사이버 작전이 단일 이벤트가 아니라 준비・은닉・확산・효과의 단계적 과정으로 수행된다는 점을 공통적으로 보여준다. 이는 사후 탐지와 대응에 집중된 기존 사이버 운영 방식이 구조적으로 불리함을 의미한다.

사이버 드론 개념은 사이버 공간을 상시 탐색・감시하는 자율 작전 단위를 제공함으로써, 공격의 준비・확산・은닉 단계에서 선제적 개입 가능성을 이론적으로 제시한다. 동시에 인간 통제와 책임성 원칙을 전제로 운용된다는 점에서, 규범적 제약과 작전 효율성 간의 균형을 유지할 수 있는 전력 개념으로 평가될 수 있다.

5.6 소결

본 장의 사례 분석은 사이버 드론이 추상적 개념에 머무르지 않고, 실제 사이버 작전 환경에서 작전적 차이를 만들어낼 수 있는 잠재적 가능성을 지니고 있음을 보여주었다. 특히 조건부 자율성, 인간 통제, 책임성이라는 제도적 전제를 반영할 경우, 사이버 드론은 현실적으로 제도화

28) Greenberg. 2019.

29) FireEye Blog, 2020.

30) U.S. Cybersecurity and Infrastructure Security Agency (CISA), Alert (AA20-352A): Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations, 2020, (검색일: 2025. 12. 16.).

가능성이 검토될 수 있는 자율형 사이버 전력 개념으로 이해될 수 있다.

Ⅵ. 사이버 드론의 방위산업 전략적 시사점

6.1 자율형 사이버 전력과 전력 개념의 확장

사이버 드론은 개별 기술이나 단일 시스템이 아니라, 사이버 전력 개념의 구조적 확장으로 이해될 수 있다. 기존의 사이버 역량이 물리적 전력을 보조하는 방어 수단 또는 특정 작전을 지원하는 기능에 머물렀다면, 본 연구에서 제안하는 사이버 드론은 사이버 공간에서 독립적으로 임무를 수행하는 전력 단위로 개념화된다.

이러한 개념은 사이버 공간을 단순한 지원 영역이 아니라, 육·해·공·우주와 병렬적인 독자적 작전 영역으로 인식하는 최근의 군사 전략 흐름과도 개념적으로 부합한다.[31] 즉, 사이버 드론은 사이버 전력을 기술적 보조 수단이 아닌, 작전 단위 차원의 전력으로 전환시키는 개념적 매개체로 해석될 수 있다.

이와 같은 전력 개념의 변화는 방위산업에도 구조적 영향을 미칠 수 있다. 전통적인 무기체계 중심의 획득·운용 논리에서 벗어나, 작전 환경의 속도와 복잡성에 대응하기 위해 자율성·지속성·확장성을 핵심 가치로 하는 새로운 전력 구성 요소에 대한 요구가 이론적으로 제기되기 때문이다.

6.2 무기체계 중심에서 플랫폼·에코시스템 중심으로의 전환

전통적인 방위산업은 개별 무기체계의 성능과 수량을 중심으로 발전해 왔다. 그러나 사이버 드론은 단일 제품으로 완결되는 체계가 아니라, 플랫폼과 이를 둘러싼 에코시스템의 형태로 발전할 가능성을 내포한다.

사이버 드론 체계는 자율 에이전트, 중앙 통제 시스템, 데이터 분석 및 학습 모듈, 운용 정책과 규칙, 그리고 이를 지원하는 인프라로 구성된다. 이러한 구조는 방위산업이 단발성 납품 중심의 구조에서 벗어나, 지속적 업그레이드와 운용 지원을 포함하는 장기적 산업 모델로 전환될 수 있는 여지를 시사한다.

이는 최근 방위산업 분야에서 강조되고 있는 개방형 아키텍처, 소프트웨어 정의 체계, 서비스 기반 전력 운용 개념과도 정책적·개념적 정합성을 가진다. 이러한 흐름은 전력 체계를 단일 플랫폼이 아니라, 유연하게 결합·확장 가능한 구성 요소의 집합으로 재정의하는 방향으로 제시되고 있다.[32]

6.3 연구개발(R&D)과 전력화 간의 연계 문제

사이버 분야의 연구개발은 기술적 성과에도 불구하고 실제 전력화로 이어지지 못하는 경우가 반복되어 왔다. 이는 연구개발 단계에서의 기술 목표와 실제 작전 운용 요구가 충분히 연계되지 못했기 때문이다.

사이버 드론 개념은 이러한 단절을 완화할 수 있는 이론적 구조를 제공한다. 사이버 드론은 모듈화된 설계와 단계적 기능 확장을 전제로 하여, 초기에는 제한된 정찰 임무를 수행하는 형태로 도입한 뒤 대응·협업·학습 기능이 점진적으로 확장되도록 설계될 수 있다.

이러한 접근은 방위산업에서 요구되는 단계적 획득과 위험 관리 전략과도 부합하며, 연구개발 성과가 실제 전력화로 이전될 수 있는 현실적 경로를 제시한다.

6.4 국내 방위산업 생태계와의 결합 가능성

사이버 드론은 물리적 장비 중심의 방위산업뿐 아니라, 소프트웨어·인공지능·데이터 분석 역량을 보유한 국내 산업 생태계와 결합될 수 있는 구조를 갖는다. 특히 중소·중견 기업과 스타트업이 참여할 수 있는 여지가 크다는 점에서, 방위산업 참여 구조의 다변화 가능성을 시사한다.

또한 사이버 드론은 장비 수출이 아닌, 플랫폼·운용 개

31) U.S. Department of Defense. Summary of the 2018 Department of Defense Cyber Strategy, 2018.

32) U.S. Department of Defense, Modular Open Systems Approach (MOSA) Reference Framework, 2019.

념・서비스를 포함한 패키지형 수출 모델로 확장될 수 있는 잠재력을 지닌다. 이는 방위산업의 수출 구조를 기존의 하드웨어 중심에서 소프트웨어・서비스 중심으로 확장시키는 전략적 의미를 가질 수 있다.

6.5 정책적・제도적 시사점

사이버 드론의 전력화를 위해서는 기술 개발과 더불어 정책・제도적 기반이 필수적이다. 자율형 사이버 전력의 운용 범위, 승인 절차, 책임 구조에 대한 명확한 기준이 마련되지 않을 경우, 기술 발전이 실제 전력화로 이어지기 어렵다.

본 연구는 사이버 드론을 기존 무기체계와 동일한 틀로 관리하기보다는, 자율형 전력이라는 특성을 반영한 별도의 정책 프레임이 검토될 필요가 있음을 시사한다. 이는 향후 국방 사이버 전략과 방위산업 육성 정책을 설계하는 데 있어 중요한 고려 요소가 될 수 있다.

6.6 소결

사이버 드론은 방위산업 관점에서 단순한 기술 트렌드가 아니라, 전력 개념・산업 구조・정책 프레임을 동시에 변화시킬 가능성을 지닌 개념으로 이해될 수 있다. 자율형 사이버 전력으로서의 사이버 드론은 향후 방위산업이 직면하게 될 새로운 기회이자 도전이며, 이에 대한 선제적 논의와 준비가 요구된다.

Ⅶ. 결론 및 향후 연구

7.1 연구 결과의 종합

본 연구는 지능형 지속 위협과 공급망 공격으로 대표되는 고도화・지속화된 사이버 위협 환경에서, 기존의 방어 중심 또는 제한적 자동화 접근이 구조적 한계를 지니고 있음을 분석하였다. Stuxnet・NotPetya・SolarWinds 사례 분석을 통해, 사후 탐지와 중앙집중식 대응에 의존해 온 기존 사이버 운영 방식이 은닉성・지속성・신뢰 경로 악용을 특징으로 하는 공격에 효과적으로 대응하기 어렵다는 점을 확인하였다. 이러한 한계는 개별 기술이나 운용상의 문제가 아니라, 사이버 전력을 구성하고 운용해 온 기존 전력 개념 자체의 제약에서 비롯된다는 점에서 개념적 전환의 필요성을 시사한다.

이에 본 연구는 '사이버 드론'이라는 자율형 사이버 전력 개념을 제안하고, 이를 사이버 공간에서 독립적으로 임무를 수행하는 전력 단위로 개념화하였다. 사이버 드론은 무인성, 지속적 정찰, 조건부 자율성, 효과 중심 작전이라는 운용 논리를 사이버 공간에 적용한 전력 요소로서, 기존의 사이버 방어 체계나 자동화 도구와 구별되는 개념적 작전 단위로 이해될 수 있음을 논증하였다.

7.2 학술적・정책적 기여

본 연구의 학술적 기여는 다음과 같이 정리할 수 있다.

첫째, 사이버 공간에서의 자율형 전력 논의를 기존 보안 기술 또는 자동화 논의에서 확장하여, 작전 단위 수준의 개념적 틀로 제시하였다. 이는 사이버 전력 연구에서 상대적으로 부족했던 전력 개념 논의를 보완하는 시도로 평가될 수 있다.

둘째, 사이버 드론 운용에 수반되는 법적・윤리적・거버넌스 쟁점을 체계적으로 검토함으로써, 자율형 사이버 전력이 국제 규범과 제도적 틀 내에서 논의될 수 있는 조건을 제시하였다. 이는 기술 중심 논의에 치우치기 쉬운 자율화 담론에 규범적 균형을 제공한다.

셋째, 방위산업 관점에서 사이버 드론을 단일 기술이 아닌 플랫폼 및 에코시스템 중심의 전력 개념으로 분석함으로써, 사이버 전력화와 산업 전략 간의 연결 가능성을 이론적으로 제시하였다.

7.3 연구의 한계

본 연구는 개념 제안과 정책적・전략적 분석을 중심으로 수행된 질적 연구로서 몇 가지 한계를 지닌다.

첫째, 사이버 드론의 기술적 구현이나 성능을 실증적으로 검증하지 못하였다. 본 논문은 개념적 타당성과 전략적 의미를 중심으로 논의하였으며, 실제 시스템 구현이나 실

험 결과를 포함하지 않는다.

둘째, 사례 분석은 실제 사이버 드론 운용 사례가 존재하지 않는 현실을 고려하여 가상 적용 시나리오에 기반하였다. 따라서 분석 결과는 가능성과 시사점을 제시하는 수준에 머무르며, 실증적 효과를 단정적으로 제시하지 않는다.

셋째, 국제법 및 정책 분석은 공개 자료와 기존 연구를 중심으로 수행되었으며, 비공개 군사·산업 정보까지 포괄하지는 못하였다.

이러한 한계는 본 연구의 결론을 완결된 해답이 아니라, 후속 연구를 위한 분석적 출발점으로 이해할 필요가 있음을 의미한다.

7.4 향후 연구 방향

향후 연구에서는 다음과 같은 방향에서 사이버 드론 개념을 확장·심화할 필요가 있다.

첫째, 사이버 드론의 기술적 아키텍처와 자율 판단 알고리즘을 구체화하는 연구가 요구된다. 이를 위해 기능 모듈 간 인터페이스 구조, 자율 판단 단계별 의사결정 로직, 중앙 통제 체계와의 연동 메커니즘을 설계 수준에서 정식화하고, 시뮬레이션 기반 실험이나 제한적 테스트베드를 활용하여 운용 효과와 안정성을 검증할 필요가 있다. 이러한 접근은 사이버 드론 개념을 이론적 제안에 그치지 않고 기술적으로 구현 가능한 전력 개념으로 구체화하는 데 기여할 것이다.

둘째, 다수의 사이버 드론이 동시에 운용되는 군집 운용 모델과 중앙 제어 체계의 설계 원리에 대한 분석이 필요하다. 이 연구에서는 분산 자율 유닛 간 정보 공유 방식, 임무 분담과 재할당 메커니즘, 중앙 통제 체계의 개입 수준에 따른 성능 차이를 비교·분석하는 방법론이 활용될 수 있다. 이를 통해 자율성과 통제 간 균형이 실제 운용 환경에서 어떻게 구현될 수 있는지를 평가함으로써, 자율형 사이버 전력의 실질적 전력화 가능성을 보다 체계적으로 검토할 수 있을 것이다.

셋째, 자율형 사이버 전력의 운용과 관련된 국내·국제 법제 및 정책 프레임을 보다 구체적으로 검토하는 후속 연구가 요구된다. 기존 연구에서는 사이버 작전 전반에서의 책임성과 국제법적 쟁점이 지속적으로 제기되어 왔으며, 이러한 논의는 본 연구에서 제안하는 사이버 드론 개념의 제도적 수용성과 국제적 신뢰 형성을 검토하는 데 중요한 분석 틀을 제공한다. 향후 연구에서는 국제인도법, 국가책임 이론, 자율체계 규범 논의를 종합적으로 검토하고, 이를 사이버 드론 운용 시나리오에 적용하는 규범적·정책적 분석이 병행될 필요가 있다.

마지막으로, 방위산업 관점에서는 사이버 드론을 중심으로 한 산업 생태계 구축, 획득 전략, 그리고 플랫폼·운용 개념·서비스를 포함한 수출 모델에 대한 실증적 연구가 향후 중요한 과제가 될 것이다. 이는 사이버 드론이 군사적 전력 개념을 넘어 산업적·경제적 가치로 확장될 수 있는 조건을 구체화하는 데 기여할 것으로 기대된다.

7.5 맺음말

사이버 공간은 이미 국가 경쟁과 안보의 핵심 영역으로 자리 잡았으며, 사이버 작전은 단발적 사건이 아니라 지속적이고 구조화된 경쟁 양상으로 전개되고 있다. 이러한 환경에서 사이버 드론은 단순한 기술적 제안이 아니라, 자율성과 속도가 강조되는 현대 사이버 작전 환경에서 사이버 전력을 어떻게 구성하고 운용할 것인가에 대한 새로운 사고 틀을 제시하는 개념적 시도로 이해될 수 있다.

본 연구는 사이버 드론을 완전한 자동화 수단이 아닌, 중앙 통제 체계와 결합된 조건부 자율 구조 하에서 운용되는 전력 단위로 개념화함으로써, 기존 사이버 방어 체계나 자동화 도구와 구별되는 작전적 의미를 정리하였다. 또한 주요 사례 분석을 통해 현대 사이버 작전에서 은닉성, 지속성, 신뢰 경로 악용이 핵심 특징으로 부상하고 있음을 확인하고, 이러한 변화가 자율형 사이버 전력 개념의 필요성을 구조적으로 뒷받침함을 논증하였다. 본 연구의 논의가 향후 사이버 전력 운용, 관련 제도 정비, 그리고 방위산업 전략을 둘러싼 학술적·정책적 논의의 기초 자료로 활용되기를 기대한다.

참고문헌

1) Greenberg, Andy. Sandworm: *A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, Doubleday, 2019.
2) Libicki, Martin C. *Cyberdeterrence and Cyberwar*, RAND Corporation, 2009.
3) Rid, Thomas. *Cyber War Will Not Take Place*, Oxford University Press, 2013.
4) Schmitt, Michael N.(ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017.
5) Singer, P. W. & Brooking, E. T. *LikeWar: The Weaponization of Social Media*, Houghton Mifflin Harcourt, 2018.
6) Langner, Ralph. "Stuxnet: Dissecting a Cyberwarfare Weapon", *IEEE Security & Privacy*, Vol. 9, No. 3, 2011.
7) Lin, Herbert S. "Attribution of Malicious Cyber Incidents: From Soup to Nuts", *Journal of National Security Law & Policy*, Vol. 7, No. 2, 2015.
8) U.S. Department of Defense. *Summary of the 2018 Department of Defense Cyber Strategy*, Washington, D.C., 2018.
9) U.S. Department of Defense. *Modular Open Systems Approach (MOSA) Reference Framework*, Washington, D.C., 2019.
10) UN CCW Group of Governmental Experts on Lethal Autonomous Weapons Systems. *Report of the 2019 Session*, United Nations, 2019.
11) FireEye. "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims", FireEye Blog, 2020, (검색일: 2025. 12. 16.).
12) U.S. Cybersecurity and Infrastructure Security Agency(CISA). "Alert (AA20-352A): Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations", 2020, (검색일: 2025. 12. 16.).