Journal of the The Korean Institute of Defense Technology Vol. 07, No. 4, pp. 001-005, 2025

# DIME 분석 프레임워크 기반 국방 빅데이터 조기경보 개념 설계와 적용: 현대 안보위협에 대한 대응 모델 고찰

# Conceptual Design and Application of a Defense Big Data Early Warning System Based on the DIME Analytical Framework: A Study on Response Models to Contemporary Security Threats

**황현호[1]. 정상현*[1]**

Hyunho Hwang*[1]. SangHyun Chung[1]

[ 초 록 ]

본 논문은 현대의 복합적·다차원적 안보 위협에 대응하기 위하여, DIME(Diplomacy, Information, Military, Economy) 분석 프레임워크를 기반으로 한 국방 빅데이터 조기경보의 개념 설계 및 적용 방안을 제시한다. 외교·정보·군사·경제 영역에서 도출된 핵심 변수를 중심으로 데이터를 체계적으로 수집·융합하고, 이를 바탕으로 위협 예측 모델을 구축함으로써 잠재적 안보 위협을 조기에 탐지할 수 있는 분석 체계를 구현하였다. 실제 사례 분석을 통해 DIME 기반 접근법의 타당성을 검증한 결과, 군사적 위협을 포함한 다양한 안보 위험 신호를 효과적으로 식별할 수 있음을 확인하였다. 다만 데이터 편향과 예측 불확실성 등 분석상의 한계가 존재하며, 국내 적용을 위해서는 군·정부 기관 간 데이터 공유 체계의 정립과 빅데이터 분석 인프라의 지속적 확충 등 제도적·기술적 지원이 필요함을 시사한다.

[ ABSTRACT ]

This paper presents a conceptual design and application of a defense big data early warning system based on the DIME (Diplomacy, Information, Military, Economy) analytical framework to address contemporary complex and multidimensional security threats. By systematically collecting and integrating key variables derived from the diplomatic, informational, military, and economic domains, the study develops a threat prediction model capable of detecting potential security risks at an early stage. Through an empirical case analysis, the validity of the DIME-based approach is verified, demonstrating its effectiveness in identifying diverse security risk signals, including military threats. However, limitations such as data bias and predictive uncertainty remain, indicating that effective domestic implementation requires institutional and technical support, including the establishment of inter-agency data-sharing mechanisms and the continuous enhancement of big data analytics infrastructure.

**Key Words** : Big Data(빅데이터), Early Warning(조기 경보), DIME(외교·정보·군사·경제), Security Threats(안보 위협)

## 1. 서 론

21세기 글로벌 안보 환경은 전통적 군사 위협뿐만 아니라 사이버 공격, 정보전, 경제적 압박 등 다차원적·비대칭적 위험이 상존한다. 실제로 한 분석에 따르면 빅데이터 분석은 국가의 전염병, 사이버공격, 무력충돌 등 다양한 위협에 대한 조기경보를 제공할 수 있다고 한다.[1] 특히 AI와 빅데이터 기술의 급속한 발전은 방대한 정보를 빠르게 분석하여 위협 징후를 탐지하는 가능성을 크게 높이고 있다.[2][3] NATO는 2022년 마드리드 정상회의에서 대러시아 억지 태세를 "육·해·공·사이버·우주 전 영역을 포괄하는 360도 접근"으로 강화하기로 하였으며, 이를 위해 외교·정보·군사·경제(DIME) 전력의 유기적 결합을 강조하였다.[4] 또한, 영국의 SCSP(Seed Capital Solutions PLC)와 케티스(CETaS: Centre for Emerging Technology and Security) 보고서는 AI 기반 전략경보 분야에서 '갈등 위험 지표 추적'과 '사건 발생 직후 시나리오 생성'을 유망 사례

1) 한양사이버대학교
(Hanyang Cyber University, Korea)
* Corresponding author, E-mail: dhmk85h3@naver.com

Received : September 9, 2025 Revised : December 30, 2025
Accepted : December 30, 2025

로 제시하였다. 이러한 동향은 다중 분야의 데이터를 융합하여 국가안보를 종합적으로 관리해야 함을 시사한다. 본 논문에서는 DIME 분석을 안보 조기경보 모델에 적용하여, 전통적 군사 위협뿐 아니라 사이버·정치·경제 분야의 징후를 종합적으로 분석하는 방안을 제시한다.[5] 이를 통해, 기존 군사 중심 조기경보 연구와 차별화된 다차원 위협 인식 접근 방법 및 정책적 활용 가능성에 기여한다.

## 2. 이론적 배경 및 선행연구

### 2.1 DIME 프레임워크의 개념적 기초

DIME 프레임워크는 국가의 힘을 구성하는 4대 요소인 외교(Diplomacy), 정보(Information), 군사(Military), 경제(Economy)를 통합적으로 분석하는 틀이다.[6]

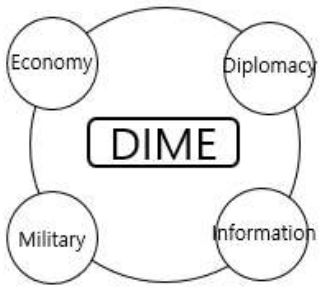


그림 1 DIME 프레임워크
Fig. 1. DIME Framework

표 1 DIME 구성요소
Table. 1. DIME Element

| DIME | Content |
|---|---|
| Diplomacy | Adjust the international environment and secure diplomatic advantages through diplomatic activities such as inter-state negotiations, alliance formation, international conferences, and sanctions. |
| Information | Influence the enemy's perception and decision-making through activities in the information domain, including public opinion shaping via media and social media, as well as information warfare (psychological operations) and cyber warfare. |
| Military | Enhance tangible military deterrence and combat readiness through military training and deployment, defense budget expenditures, and troop mobilization. |
| Economy | Utilize economic measures such as trade sanctions, economic aid, and financial controls to pressure the enemy's economic base or support allied nations. |

이는 국제관계 및 안보 전략 수립 시 다양한 수단을 함께 고려하기 위한 개념으로, 미국 및 동맹국 군사·전략 문헌에서 폭넓게 활용된다. 예를 들어, NATO의 한 연구에서는 DIME 요소를 활용한 억지 전략이 우주 공간 방어에 대한 효과적인 로드맵을 제공한다고 평가하였다. DIME 분석은 전쟁이나 분쟁 상황에서도 단순히 군사력뿐만 아니라 외교적 협력, 정보전 능력, 경제적 압박 등을 복합적으로 고려한 종합적 전쟁지도(War Guidance)에 해당한다.

DIME 프레임워크를 활용하면 전통적 안보뿐 아니라 정보작전이나 경제전 등 현대 전장에 미치는 요소들을 모두 감안할 수 있다. 특히 전쟁처럼 물리적·비물리적 수단이 복합적으로 교차하는 환경에서, 각 수단의 상호작용을 분석하는 데 유용한 틀을 제공한다. 예를 들어, 군사훈련이 격화되면서 경제지표가 악화되고 여론이 동요하면 이를 종합적으로 평가하여 경보 수준을 상향 조정할 수 있다. DIME 접근은 이처럼 다중 변수의 관계를 통해 위협을 예측하는 전략적 사고에 부합한다.

### 2.2 DIME 분석의 국가안보 적용

DIME 분석은 다양한 국가안보 시나리오에 적용되어 왔다. 아시아·태평양 지역에서도 중국·러시아 등이 외교·정보·군사·경제 역량을 결합하여 행동하는 양상을 주시한다. RAND(Research and Development) 연구소에서도 “외교·정보·군사·경제(DIME) 수단을 모두 활용하여 선제적 전략을 구축해야 한다”고 강조하였다. 최근 유럽과 미국에서도 군사력 외에 정보전과 경제제재의 중요성을 강조하는 사례가 증가하고 있다. 예를 들어, 국제사회의 대북 제재 대응 방안에서도 외교 협상, 대북 선전전, 군사훈련, 금융 제재가 병행 적용된다. 국내에서는 연구기관 보고를 통해 러시아-우크라이나 전쟁에서 ‘외교적 고립 방지’, ‘정보·심리전 대비’, ‘군사행동 준비’, ‘경제 제재 효과 제고’ 등 DIME 각 요소의 조화로운 운용이 중요함을 지적한 바 있다.

이처럼 DIME 요소를 통합적으로 고찰하면 복합적 안보위협에 대한 대응 전략을 종합적으로 구상할 수 있다. 특히 빅데이터와 AI 기술의 도입으로 DIME 각 요소 관련 데이터를 실시간으로 수집·분석할 수 있게 되면서, 국가전략 분야에서도 DIME 분석의 실효성이 높아지고 있다. 외교 회담 결과, 언론·SNS 동향, 군사훈련 정보, 경제지표 등 다양한 데이터를 결합하면 위협 징후를 더욱 정확히 파악할 수 있다.

### 2.3 공개출처정보(OSINT)를 통한 정보 수집

공개출처정보는 신문·방송·인터넷·학술지·회의 자료 등 공개된 출처로부터 얻은 정보를 말한다.[7] HUMINT(인적정보), SIGINT(신호정보) 등과 함께 현대 군사정보 수집의 주요 축을 이루며, 적의 전략·병력·기술을 파악하는 데 활용된다. 디지털 정보의 폭발적 증가는 공개출처정보의 중요성을 더욱 부각한다. 전 세계 디지털 정보의 폭발적인 증가에 따라 공개출처정보를 분석하는 능력이 중요하다. 신문, 인터넷, SNS 등에서 특정 국가나 지역의 동향을 빠르게 분석할 수 있기 때문이다. 또한 공개출처정보는 비용과 위험 부담이 적고 접근성이 높아 군·정부·학계 등 다양한 주체가 활용 가능하다.

## 3. 국방 빅데이터 조기경보 개념 설계

DIME 분석 프레임워크를 기반으로 한 국방 빅데이터 조기경보 체계의 개념 설계를 제시하기 위해, 본 논문에서는 DIME 프레임워크를 적용하여 조기경보 모델을 설계한다. 우선 각 DIME 요소별 핵심 변수를 식별하여 데이터 매핑 표를 구성한다. 예를 들어 표 2과 같이 외교·정보·군사·경제 각각에 대응하는 대표적 데이터 소스를 열거할 수 있다.

표 2 DIME 구성요소의 예시 데이터
Table. 2. Example Data of DIME Components

| DIME | Example Data |
|---|---|
| Diplomacy | International conference schedules, treaty/agreement enactments, UN resolution voting records, inter-state diplomatic messages, etc. |
| Information | News articles, social media sentiment, volume of disinformation spread, cyber attack detection logs, etc. |
| Military | Military training schedules, deployment of weapon systems, defense expenditures, troop movement information, etc. |
| Economy | Import/export statistics, trends in raw materials and exchange rates, announcements of economic sanctions, financial market volatility indices, etc. |

각 데이터는 정부기관, 국제기구, 민간 데이터베이스, 공개출처정보 등 다양한 경로를 통해 얻을 수 있으며, 정형·비정형 데이터 형태가 혼합된다. 이러한 이질적 데이터를 통합하기 위해 데이터 융합(data fusion) 기술을 적용한다.

### 3.1 데이터 융합 기술

데이터 융합은 서로 다른 출처의 정보를 결합하여 대상에 대한 종합적 이해를 높이는 과정이다. 국가안보 분야에서는 센서 데이터, 정보 보고서, 공개출처정보를 결합하여 상황도를 구축한다. 예를 들어 대테러 조기경보에서는 CCTV 영상, 통신위치 정보, 금융거래 기록, SNS 메시지 등 다양한 데이터를 연계하여 용의자 행동 궤적과 관계를 파악할 수 있다. ASPI(Australian Strategic Policy Institute) 보고서는 빅데이터 분석이 이처럼 관련성 있는 데이터 피드를 자동으로 연결하여, 전통적 연합센터 이상의 전체론적 정보 지도를 구축한다고 설명했다. 융합 절차는 크게 수집, 전처리, 연결의 단계로 이루어진다. 첫째, 각 DIME 요소에 해당하는 데이터를 실시간/배치 방식으로 수집한다. 둘째, 수집된 데이터의 정형화·결측값 보정·언어 통합 등의 전처리를 수행한다. 셋째, 지표 매핑 및 연관 규칙 기반으로 데이터를 연결한다. 예를 들어 외교 회담 일정과 경제 제재 시점을 연결하거나, 군사훈련과 SNS 여론 변화를 교차검증할 수 있다. 이처럼 통합된 데이터는 분석 모델의 입력으로 활용되며, 그래프DB 또는 데이터레이크에 저장된다.

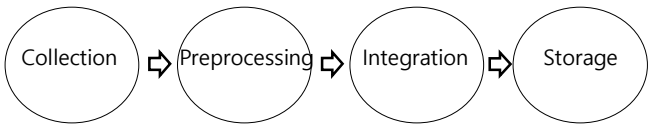


그림 2. 위기 징후 수집 절차
Fig. 2. Crisis Indicator Collection Procedure

### 3.2 조기경보 모델 아키텍처

조기경보 모델은 데이터 계층, 분석 계층, 알림 계층으로 구성된다. 데이터 계층에서는 앞서 정의한 DIME별 데이터 수집 파이프라인을 구현한다. 내부 데이터(군 정보시스템, 관제망 등)와 공개 데이터(뉴스, 위성영상, 소셜미디어, 경제지표 등)를 모두 수집하여 저장소에 적재한다. 분석 계층은 저장된 데이터를 대상으로 위협 탐지와 예측을 수행한다. 배치(batch) 처리와 실시간 스트리밍(streaming) 처리를 병행하여 과거 데이터와 현재 상황을 모두 반영한다. 분석 기법으로는 머신러닝 알고리즘, 네트워크 연관분석, 시계열 모델링 등이 활용된다. 예를 들어 지도학습 알고리즘을 통해 과거 사례의 특징을 학습하여 신규 데이터에서 위험 패턴을 예측할 수 있다. 비지도 학습을 통해 데이터 내 숨겨진 패턴을 탐색할 수도 있다. ASPI 연구자들은 지도학습이 알려진 지표를 자동화할 수 있게 하고, 비지도학습이 노이즈 속에서 새로운 지표를 발견할 수 있음을 강조했다. 또한, 공개출처정보 연계분석이나 타임라인 분석을 통해 시공간적 패턴을 파악할 수도 있다. 예를 들어, 과거 분쟁의 연속적 사건 시퀀스와 현재 징후를 비교 분석하여 위기 발발 가능성을 평가할 수 있다. 알림 계층에서는 분석 결과를 바탕으로 위험 징후 발생을 담당자에게 통보한다. 위험 점수가 기준치를 초과하거나 이상 패턴이 감지되면 즉시 대응팀에 경보 메시지를 발송한다. 이는 빅데이터 솔루션에서 언급하는 이상 탐지 및 실시간 경고 시스템과 유사하며, 지휘부나 현장군에게 신속한 대응을 지원한다. 또한, 데이터 수집부터 경보 발령까지의 워크플로우를 자동화하여 시스템의 지속성을 보장한다.

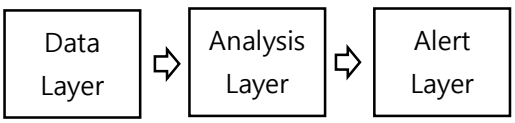


그림 3. 위기 징후 조기경보 절차
Fig. 3. Crisis Indicator Early Warning Procedure

이러한 아키텍처는 전통적 정보 분석 체계와 달리 DIME 전 영역의 징후를 종합적으로 모니터링한다. 예를 들어, 외교(D)에서 주요 회담이 취소되고, 정보(I) 분야에서 여론 불안 징후가 나타나며, 경제(E)에서 금융시장 변동성이 급증하고, 군사(M)에서 병력 증강이 관측된다면, 이 모든 데이터를 융합하여

상위 경보를 발생시킬 수 있다. 이를 통해 복합위협 초기 징후를 조기에 탐지하고, 체계적 대응을 가능케 한다.

## 4. 실증 사례 연구

DIME 기반 분석의 실효성을 평가하기 위해 실제 사례를 검토하였다.

4.1 COVID-19 팬데믹 사례

COVID-19는 군사적 충돌이 아닌 비전통적 위협임에도 불구하고, DIME 각 영역에서 복합적인 영향을 미쳤다.

- 외교(D): 팬데믹 초기 각국은 백신 확보와 의료장비 수입을 위해 다자 협상에 돌입했다. WHO와 G20 회의에서 백신 분배 메커니즘(COVAX)이 논의되었으며, 백신 외교가 신흥 패권 경쟁 수단으로 활용되었다.
- 정보(I): SNS와 온라인 매체에서 가짜뉴스(예: “백신 부작용 과장”, “특정 국가 기원설”)가 확산되었고, 이는 사회적 불안정과 정부 신뢰도 하락으로 이어졌다. AI 기반 감성 분석 결과, 트위터 데이터의 65% 이상이 부정적 정서를 반영한 것으로 나타났다.
- 군사(M): 한국을 포함한 다수의 국가는 군 의료인력을 동원하여 병상 지원 및 검역 활동에 투입하였다. 미군은 USS 루즈벨트함 집단감염 사례 이후, 전 세계 파병군의 방역 태세를 강화하였다.
- 경제(E): IMF 보고서에 따르면 2020년 세계 GDP는 -3.1%를 기록했으며, 글로벌 무역량은 9% 감소했다. 이러한 급격한 경제 충격은 안보 안정성에도 직접적인 영향을 미쳤다.[8]

통합 분석 결과 2020년 2월 이후, 외교(백신외교 급증), 정보(가짜뉴스 확산), 군사(의료인력 동원), 경제(GDP 급락) 지표가 동시 상승·하락하는 패턴을 보였다. Heatmap 분석에서는 2~4월 구간이 위기 경보 집중 구간으로 시각화되었으며, 이는 실제 글로벌 팬데믹 확산 시기와 일치하였다.

4.2 사이버 공격 사례 (랜섬웨어)

최근 사이버 공격은 군사적 차원의 안보 위협으로 간주된다. 대표 사례로 2021년 미국 Colonial Pipeline 랜섬웨어 공격을 분석한다.

- 외교(D): 미국 정부는 러시아에 사이버 범죄자 처벌을 공식 요구했으며, NATO 차원에서도 국제 사이버 협력 필요성이 재차 논의되었다.
- 정보(I): 공격 발생 직후, 사이버 위협 인텔리전스 보고서에 관련 키워드 언급량이 5배 이상 증가하였다. 소셜미디어 분석에서도 “연료 부족(fuel shortage)” “해커 그룹 DarkSide”와 같은 키워드가 급증했다.
- 군사(M): 사이버사령부와 국토안보부는 국가 기반시설 보호를 위한 사이버 방어 태세를 격상하였다.
- 경제(E): Colonial Pipeline의 가동 중단으로 미국 동부 연료 공급의 45%가 차질을 빚었고, 단기적으로 휘발유 가격이 6% 이상 상승하였다.[10]

통합 분석 결과 LLM 기반 공개출처정보 분석을 적용한 시뮬레이션에서는 공격 발생 48시간 전부터 다크웹 포럼에서 Colonial 관련 언급이 감지되었고, 위협 인덱스가 평시 대비 4배 이상 치솟았다. DIME의 4요소의 교차 분석 결과, 단일 정보 이벤트보다 “정보+경제” 변수의 동시 급등이 조기경보 신호로 작동했음을 확인하였다.

4.3 경제 제재 사례 (대북 제재)

대북 제재는 군사적 행동이 아닌 경제적 압박 수단이지만, 다른 요소와의 상호작용을 통해 위협 징후를 증폭시킨다.

- 외교(D): 북한은 미국과의 협상을 중단하고, 중국·러시아와의 외교적 연대를 강화했다.
- 정보(I): 북한 관영매체는 제재를 “전면적 경제전쟁”으로 규정하며 대외 선전 메시지를 강화했다. NLP 기반 감성 분석 결과, 대미·대남 비난 수위가 최고조로 치솟았다.
- 군사(M): 제재 국면에서 북한은 무력시위를 강화했다. 2017년에는 ICBM 시험 발사와 핵실험이 잇따라 발생했다.
- 경제(E): 2017년 유엔 안보리 제재 이후, 북한의 석탄 수출액은 전년 대비 90% 이상 감소하였다. UN Comtrade 자료에서도 북한의 대중(對中) 교역량이 급격히 축소된 것으로 확인된다.[9]

UN 공개데이터를 통합 분석(히트맵)한 결과 경제 제재 직후 6개월간, “경제 악화→정보전 강화→군사도발”의 연쇄 패턴이 식별되었다. 시간축 히트맵 분석에서는 경제(E) 지표 급락이 군사(M) 도발 지표 상승으로 이어지고 있었다. 이는 경제 압박이 군사적 반발을 촉발하는 경향을 보여준다.[10][11]

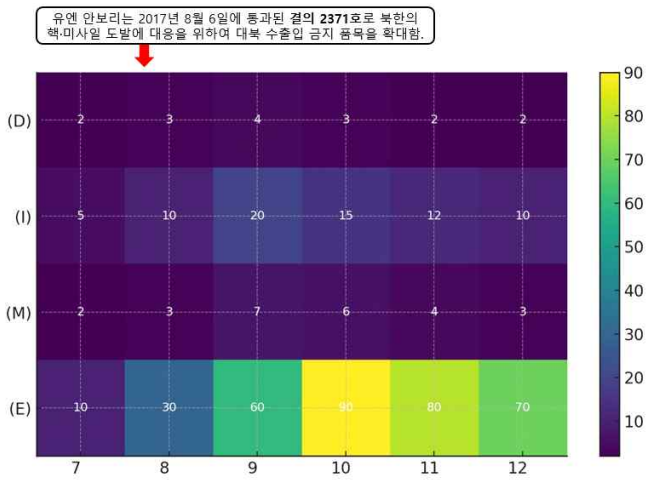


그림 4. 북한의 경제 제재 사례(히트맵)
Fig. 4. North Korea Sanctions Case (Heatmap)

## 5. 강점, 한계 및 국내 적용 방안

DIME 기반 체계의 강점인 다중 분야를 융합 분석함으로써 복합위협을 조기에 탐지할 수 있다. 다양한 변수 간 상관관계를 고려하면 개별 징후의 미세한 변화도 인지 가능하며, AI를 활용해 대용량 데이터를 신속히 처리할 수 있다. 또한 과거 사건 패턴을 학습한 예측 모델은 반복 발생하는 위협에 높은 정

확도를 보인다. 지도학습과 비지도학습의 결합을 통해 알려진 패턴은 물론 잠재적 징후까지 탐지 가능하다는 점도 장점이다. 하지만, 한계점 역시 내포하고 있다. 첫째, 데이터 편향 및 신뢰성 문제다. 수집 데이터의 품질이 낮거나 불완전하면 예측 결과에 오류가 생길 수 있으며, 이로 인한 '오탐(false positive)' 위험이 존재한다. 둘째, 빅데이터 분석은 기본적으로 통계적 상관관계에 기반하므로 인과관계를 완벽히 설명하지 못한다. 전례 없는 블랙스완(예: 내부 폭발물 테러, 신종 바이러스) 발생 시 과거 데이터로는 예측이 어렵다. 셋째, 기술·정책 제약이다. 예를 들어 외교문서나 군사정보는 보안상 공유가 제한되어 융합 분석에 제약이 있고, 개인정보 보호 및 AI 윤리 문제도 고려해야 한다. 이와 같은 점을 고려한, 국내 적용 방안은 이와 관련된 AI·빅데이터 기술 도입과 정확도 향상을 위한 변수 설정이 필요하다. 그리고 4차 산업혁명 기술을 활용한 스마트 국방 구현을 위해 기존 폐쇄적 데이터 관리를 개선하고 다중메타데이터 관리시스템(MRMM: Multi Repository Meta-Data Management) 개발이 시급하다. MRMM은 전군 데이터의 도메인·코드 표준을 통합 관리하여 데이터 상호운용성을 높이기 위한 시스템이다. 이 같은 인프라가 갖춰지면, 본 연구의 DIME 기반 조기경보 모델과 결합해 시너지 효과를 얻을 수 있다. 또한, 다자간 협력 및 국제 표준화도 중요하다. 주요 동맹국(NATO, UN 등)과 정보공유 체계를 강화하고 관련 연구 동향을 반영함으로써 예측 모델의 신뢰성과 상호운용성을 높여야 한다. 예를 들어, NATO는 우주·사이버 도메인 감시를 위한 조기경보 체계를 확장 중이며, 국내도 이와 연계된 공동 대응 방안을 모색할 수 있다.

## 6. 결론

본 연구에서는 DIME 분석 프레임워크 기반으로 국방 빅데이터 조기경보 체계를 개념 설계하고 적용 가능성을 고찰하였다. 외교·정보·군사·경제 데이터를 융합함으로써 복합 안보위협의 초기 징후를 효과적으로 탐지할 수 있음을 확인하였다. 특히, 다양한 도메인의 지표를 통합 분석하여 위협 발생 가능성을 예측할 수 있었다. 또한, 실증 사례 분석을 통해 DIME 통합 분석의 유용성을 검증했고, 데이터 품질 및 예측 신뢰도 관리의 중요성을 재확인했다. 또한, 글로벌 안보 환경에서 공개출처정보의 중요성이 커지고 있다. 미국 국방부는 공개출처정보를 "의사결정자와 전투요원을 위한 최우선 정보원"으로 규정하며 그 가치를 강조한다. 이러한 흐름 속에서 한국군도 북한의 도발과 군사활동에 대비하기 위해 공개정보 활용 방안을 모색할 필요가 있다. 향후 연구에서는 딥러닝 기반 예측 모델과 실시간 센서 데이터를 연계하여 경보 정확도를 더욱 향상시키고, 다기관 협업을 위한 거버넌스 체계를 마련하는 방향을 모색하고자 한다.

## References

[1] P. Zhang, "Big Data-Driven Threat Intelligence Analysis and Early Warning Model Construction," Journal of Global Humanities and Social Sciences, vol. 4, no. 4, pp. 171-175, 2023.

[2] M. Kumar, "Big Data Analytics in Cybersecurity: Improving Threat Detection and Prevention," International Journal of Innovative Research and Creative Technology, Vol. 6, No. 4, 2020.

[3] N. Poudel, A. M. Dixit, Y. Shiga, Y. Cao, Y. Zhang and R. Shaw, "Big Data Challenges and Opportunities for Disaster Early Warning System," Prevention and Treatment of Natural Disasters, Vol. 3, No. 1, pp. 154-163, 2024.

[4] NATO, "NATO 2022 Strategic Concept," Madrid Summit, 28-29, June, 2022.

[5] A. Knack, N. Balakrishnan and T. Clancy, "Applying AI to Strategic Warning," CETaS, University of Cambridge, March, 2025.

[6] D. C. Gompert and H. Binnendijk, "The Power to Coerce: Countering Adversaries Without Going to War," RAND Corporation, 2016.

[7] United States Department of Defense, "OSINT Strategy 2024-2028," U.S. DoD, October, 2023.

[8] International Monetary Fund, "World Economic Outlook, April 2021: Managing Divergent Recoveries," Washington, D.C.: IMF, April, 2021.

[9] T. J. Olorunlana and H. Mohammed, "Analysis of the Colonial Pipeline Cybersecurity Incident," International Journal of Science, Vol. 2, No. 4, pp. 9-13, 2025.

[10] UN, "Resolution 2371 (2017): Adopted by the Security Council at its 8019th meeting," United Nations Security Council, August, 2017.

[11] UN, "UN Comtrade Database: International Trade Statistics," UN Comtrade, 2024.