변화하는 디지털 전장: 인공지능 적용의 확대

차용준[1,2], 조한얼[1,3], 이상철[1], 장효석[1,2], 백승호[1,2], 강경일[4,+], 김찬수[1,2,+,*]

1 한국과학기술연구원 인공지능·정보·추론 (AI/R) 연구실

2 과학기술연합대학원대학교 AI-로봇

3 세종대학교

4 합동참모본부

* Correspondence should be addressed to eau@ust.ac.kr.

Evolving Digital Battlefields: Expanded Applications of AI

Yongjun Cha[1,2], Haneol Cho[1,3], Sangchul Lee[1], Hyoseok Jang[1,2], Seungho Baek[1,2], Kyung-il Kang[4,+], Chansoo Kim[1,2,+,*]

1 AI·Information·Reasoning (AI/R) Laboratory, Korea Institute of Science and Tech. (KIST)

2 The Department of AI-Robotics, University of Science and Technology (UST)

3 Sejong University

4 Joint Chiefs of Staff

+ Equally contributed.

요 약

러시아-우크라이나 전쟁과 이스라엘-이란 분쟁의 사례 연구를 통해 AI가 디지털 전장의 역학 관계와 군사 작전의 전략적 접근 방식에 어떤 영향을 미치고 있는지를 고찰한다. AI가 정보 환경을 재편하고 대중의 서사를 조작하는 데 활용되는 방식과 이와 관련된 윤리적, 우려, 특히 감시 증가 및 잠재적 민간이 피해 등의 도전 과제를 제시한다. 두 주요 사례에서 보듯, AI가 확대 적용되는 현대 디지털 전장에서 AI는 단순한 지원 도구를 넘어 전략적 게임 체인저로 부상했다. 미사일과 군수품뿐만 아니라 데이터, 알고리즘, 서사를 통한 전투가 점점 더 중요해지고 있음도 드러난다.

Ⅰ. 서 론

인공지능(AI)의 비약적인 발전은 현대 전장의 양상을 근본적으로 변화시키고 있다. 과거 전장에서의 정보 수집과 분석, 그리고 의사결정 과정은 인간 중심으로 이루어졌으며 방대한 데이터의 처리에는 한계가 따랐고, 복잡한 전술적 판단을 신속하게 내리기 어려웠다.

그러나 AI의 등장은 이러한 제약을 극복하게 하였고, 전장의 자동화와 디지털화를 가능하게 만들었다. 러시아 - 우크라이나 전쟁과 이스라엘 - 이란 분쟁은 AI가 실제 군사 작전에서 어떤 방식으로 활용되고 있는지를 잘 보여주는 대표적인 사례들이다. 이 둘은 AI가 단순한 지원 도구를 넘어 현대전에서 전략적 게임 체인저로 작용하고 있음을 보여준다 [1-3].

Ⅱ. 본론

1. AI와 러시아-우크라이나 전쟁

러시아 - 우크라이나 전쟁은 AI가 ISR(정보·감시·정찰), C2(지휘통제), 사이버전 전반에 걸쳐 어떻게 활용될 수 있는지를 보여주는 결정적 사례이다. 전통적 전쟁에서 정보 수집과 분석은 수작업 중심으로 이루어져 대량의 데이터를 신속히 처리하기 어려웠고, 지휘관의 판단 역시 시간 지연에 크게 영향을 받았다. 그러나 이 전쟁에서 우크라이나는 AI 기반 데이터 융합 및 분석 시스템을 적극적으로 활용함으로써 이러한 한계를 극복하였다.

우크라이나는 위성 이미지, 드론 촬영 영상, 그리고 소셜미디어와 같은 비전통적 데이터까지 통합하여 전장의 디지털 트윈을 구축하였다 [1, 3]. 이러한 체계는 실시간으로 적의 위치와 움직임을 추적할 수 있도록 하여, 기존의 전장 상황 인식보다 훨씬 신속하고 정밀한 목표 식별을 가능하게 했다. 더 나아가 AI 기반 정찰·공격 드론은 아군의 인명 손실을 최소화하면서도 정밀 타격과 감시 임무를 수행하며 전술적 우위를 제공했다 [3].

대표적으로, 우크라이나가 자체적으로 개발·운용 중인 'Delta 상황인식 시스템'은 클라우드 기반의 디지털 전장 관리 플랫폼으로, 상업위성 이미지, UAV(무인항공기) 영상, 군사 통신 자료, 공개 출처 정보(OSINT, Open Source Intelligence)까지 통합한다 [8]. 이러한 클라우드 인프라는 대규모 데이터를 실시간 저장·처리·공유하며, 위성·드론·통신 등 이종 센서 데이터를 결합하고 지휘부와 전선 간 저지연(low-latency) 협업을 지원한다 [16, 17, 22]. 이어서 AI는 이 자료를 전처리·분석해 적의 위치와 위협 수준을 시각화하고, 지휘관은 이를 바탕으로 최종 결정을 내린다 [2, 9].

무인기와 자폭형 드론에는 AI 기반 부분 자율 기능이 적용되어 통신 두절이나 GPS 교란 상황에서도 항법 유지, 회피 기동, 목표 재획득이 가능하다. 이를 통해 인명 손실을 줄이고 정밀 타격과 전술적 유연성을 확보했지만, 자율성은 아직 원격조종·자동화 단계에 머물고 교전 결정은 인간

이 맡고 있다 [9].

러시아는 Lancet 자폭형 드론(loitering munition)을 전쟁에서 실전 배치하였다. Lancet은 정찰과 공격 임무를 동시에 수행할 수 있으며, 우크라이나군의 포병 및 방공 자산을 타격하는 데 널리 활용되었다. 특히 Lancet은 영상 인식 및 표적 추적 알고리즘을 통해 목표를 탐지하고 타격한다 [11].

AI 기반 영상 인식·추적 알고리즘은 컴퓨터 비전과 딥러닝을 활용해 목표물을 실시간 탐지·추적한다. CNN과 객체 탐지 네트워크(YOLO, Faster R-CNN)는 군사 장비나 차량을 인식·분류하고 [12, 13], 추적 단계에서는 칼만 필터, DeepSORT, Siamese 네트워크 등이 적용되어 이동 목표를 안정적으로 추적한다 [14, 15]. 이러한 기술은 GPS 교란 상황에서도 표적 재식별과 회피 후 재공격을 가능케 하며, Lancet과 같은 드론 무기의 정밀성과 자율성을 뒷받침한다.

AI 기반 사이버 전도 향후 발발할 가능성이 있다. 러시아 - 우크라이나 전쟁에서 AI가 직접 활용된 사이버 공격이 수행되었다는 명확한 증거는 현재까지 확인되지 않았다. 실제로 보고된 사이버 작전은 주로 와이퍼 악성코드(HermeticWiper, CaddyWiper, Industroyer2 등), 분산 서비스 거부(DDoS), 피싱 캠페인 등이다 [31].

우크라이나의 사이버 방어는 전통적인 시그니처 기반 탐지를 넘어, 서방 보안 기업들이 제공한 AI/머신러닝 기반 보안 솔루션을 적극 활용한 것이 특징적이다. Microsoft는 Defender와 Sentinel에 탑재된 ML 기반 탐지 시스템을 통해 HermeticWiper, CaddyWiper 등 러시아의 파괴적 악성코드를 조기에 식별하고 차단했다 [32].

향후 사이버 영역에서도 AI는 중요한 역할을 수행할 수 있다. AI는 악성코드 탐지, 공격 패턴 분류, 위협 예측, 자동 대응 등에 활용되어 방어적 역량을 강화한다 [3]. 이러한 기술은 전장을 물리적 공간에 한정하지 않고, 사이버 공간을 병행하는 다차원적 전장으로 확장시켰다.

악성코드 탐지에는 머신러닝과 딥러닝 기법이 활용된다. SVM·랜덤 포레스트는 코드의 정적·행위 특징을 학습해 새로운 악성코드를 식별하고, CNN과 RNN/LSTM은 실행 파일이나 로그 데이터를 분석해 악성 행위를 탐지한다 [18]. 또한 이상 탐지와 클러스터링(k-means, DBSCAN) 기법은 정상·비정상 트래픽을 구분해 다단계 공격을 조기에 식별하는 데 기여한다 [19].

2. 이스라엘-이란 분쟁과 AI

이스라엘 - 이란 분쟁은 AI가 물리적 전장뿐만 아니라 정보전과 인지전(cognitive warfare)의 차원에서 얼마나 강력한 영향을 미치는지를 보여주는 중요한 사례이다. 과거의 정보전은 주로 전통적인 심리전 기법과 언론 조작에 의존했지만, 이번 분쟁에서는 생성형 AI가 핵심적인 역할을 하였다.

2024 - 2025년의 분쟁에서는 고도로 정교한 AI 생성 이미지와 영상이 대규모로 생산되었고, 파괴된 기반시설이나 격추된 항공기, 대규모 시위 장면과 같은 허위 시각자료가 실제처럼 묘사되었다 [4, 8].

이스라엘 - 이란 분쟁에서 군사 여론 분석에는 NLP가 활용되며, 최근 Transformer 기반 언어모델(BERT, GPT 등)이 등장해 분석의 정확성과 속도를 높였다 [10, 20, 21]. 이스라엘은 가자지구 작전에서 다국어 AI 챗봇으로 현지 여론을 실시간 모니터링 했으며, 동시에 생성형 AI는 합성 이미지·영상·음성을 생산·확산시켜 사실과 허구의 경계를 흐렸다.

이스라엘은 AI 기반 오디오 분석 도구를 사용하여 폭음이나 공습의 위치를 추적하였다. 안면인식 시스템은 부상으로 얼굴이 손상되거나 가려진 인물까지 식별할 수 있도록 개발되었다. 이러한 기술은 실제로 하마스 지휘관의 위치를 특정하는 데 활용되었으며, 이는 터널 복합체에 대한 공습으로 이어졌다 [7].

반면 이란은 가짜 뉴스 앵커를 활용한 딥페이크 방송으로 국제 정보 환경을 교란하였다 [6]. 딥페이크 기술의 핵심은 생성적 적대 신경망(GANs)으로, 가짜 데이터를 만드는 '생성자'와 이를 구별하는 '판별자'가 경쟁하며 학습해 실제와 거의 구분되지 않는 결과물을 만들어낸다 [23].

오토인코더(Autoencoders)는 입력 데이터를 압축·복원해 얼굴 교환에 활용되며, 원본 인물의 표정과 움직임을 유지한 채 다른 얼굴을 합성할 수 있다. 이러한 딥페이크 기술은 영화나 교육 분야에 활용되는 등 긍정적 가능성을 지니지만, 동시에 정치적 허위 영상, 가짜 뉴스, 사생활 침해 등 악용 위험도 크다 [24].

3. 두 분쟁을 통해 본 전쟁 패러다임의 변환

러시아 - 우크라이나 전쟁은 AI가 단순한 보조 기술에서 벗어나 물리적 전장의 효율성과 속도를 좌우하는 핵심 요소로 부상한 전환점이었다. 전쟁 이전에는 완전 자율 무기와 대규모 드론 스웜 운용이 실현될 것이라는 기대가 있었으나, 실제로는 항법·비행·목표 식별 수준에서만 자율성이 구현되었고 살상 여부는 여전히 인간이 통제하였다 [27].

또한 전역 단위 자동화를 가능하게 할 것이라 예상되었던 대규모 드론 스웜은 소규모 실험 수준에 머물렀으며, 네트워크 안정성과 명중률의 한계가 드러났다. 그 대신 Delta 상황인식 시스템을 통해 드론, 위성, 센서 데이터를 실시간으로 융합하여 수백여 개의 목표를 관리할 수 있었고, FPV·자살 드론과 같은 저비용 무기가 고가 장비를 무력화하는 사례가 확산되었다. 이처럼 전쟁 전 예상과 달리 실제로는 저비용·고효율 기술과 실시간 정보 융합 체계가 부상하면서, AI는 전장의 정보 우위와 작전 주도권을 결정하는 핵심 기술로 자리매김하게 되었다 [27, 28].

이스라엘 - 이란 분쟁에서는 AI의 역할이 물리적 전투를 넘어 정보전과 인지전의 중심으로 확장되었다. 전쟁 이전까지는 AI가 주로 정찰과 타격의 정밀성을 높이는 물리적 전투 지원 도구로 여겨졌으나, 실제로는 정보 환경과 여론을 통제하는 도구로 적극 활용되었다 [26, 29].

이스라엘은 가자지구 작전에서 다국어 AI 챗봇을 활용하여 현지 여론을 실시간 분석하였고, 동시에 생성형 AI는 합성 이미지와 영상, 음성을 대량 생산하여 소셜미디어를 통해 빠르게 확산시켰다. 이처럼 AI는 전쟁의 초점을 무기와 병력에서 여론과 인식으로 이동시켰으며, 전장의 범위를 물리적 충돌에서 정보와 서사 통제까지 확장시켰다. 이는 AI가 단순한 물리적 전투의 보조 기술을 넘어 국제 안보 전략의 핵심 변수로 부상했음을 보여준다 [30].

Ⅲ. 결론

러시아 - 우크라이나 전쟁과 이스라엘 - 이란 분쟁은 AI가 단순한 정찰·보조 기술을 넘어 전쟁의 성격 자체를 바꾸는 전략적 자산으로 부상했음을 잘 보여준다. 우크라이나 사례에서는 드론·위성 데이터를 실시간으로 통합하는 상황 인식 체계와 저비용 드론 전술이 전장의 물리적 양상을 변화시켰고, 이스라엘 - 이란 분쟁에서는 생성형 AI와 딥페이크 기술이 정보전과 심리전의 핵심 도구로 활용되면서 전쟁의 무게 중심이 물리적 충돌에서 여론과 인식의 장으로 확장되었다.

그러나 AI의 부상은 동시에 심각한 도전 과제도 드러냈다. 완전 자율 무기의 부재 속에서 'AI 제안 - 인간 결심' 구조가 유지되고 있으나, 잘못된 식별로 인한 민간인 피해, 허위 정보와 딥페이크 확산에 따른 사회적 신뢰 훼손, 자율 무기 사용의 법적 책임 공백 등은 여전히 해결되지 않은 문제들이다. 이는 AI 군사 활용이 기술의 문제가 아니라 국제 규범과 제도

적 장치 마련의 과제임을 보여준다. 앞으로의 국제 안보 질서는 AI의 발전과 이를 관리하는 규범적 틀에 의해 크게 좌우될 것이다.

ACKNOWLEDGMENT

This research was funded by the grant Nos. 2023-00262155; 2024-00339583; 2024-00460980; and 2025-02304717 (IITP) funded by the Korea government (the Ministry of Science and ICT).

참 고 문 헌

[1] International Centre for Defence and Security (ICDS). Russia's War in Ukraine: Artificial Intelligence in Defence of Ukraine, 2024.

[2] Tsur, M.; Morag, M. Navigating the AI frontier: Insights from the Ukraine conflict for NATO's governance role in military AI. 873 Defense & Security Analysis 2024.

[3] Ratti, P. From Ukraine to Gaza: Artificial intelligence in war. Critique internationale 2024, 243, 39 - 55.

[4] European Digital Media Observatory (EDMO). The First AI War: How the Iran-Israel Conflict Became a Battlefield for Generative 876 Misinformation, 2024.

[5] Nickel, D. AI slop spreads in Israel-Iran war. POLITICO 2025.

[6] Radware. Hybrid Warfare Unfolded: Cyberattacks, Hacktivism and Disinformation in the 2025 Israel-Iran War, 2025.

[7] Timesof Israel. Israel using AI to pinpoint Hamas leaders, find hostages in Gaza tunnels - report. The Times of Israel 2024.

[8] CSIS, "Does Ukraine Already Have a Functional CJADC2 Technology?" Center for Strategic and International Studies, February 21, 2024, https://www.csis.org/analysis/does-ukraine-already-have-functional-cjadc2-technology?

[9] NATO Allied Command Transformation, "The DELTA System and CWIX," NATO Allied Command Transformation, July 11, 2023, https://www.act.nato.int/article/delta-system-cwix/.

[10] Apurv Gupta, Suthikshn Channarayapatna Kumar, and Odelu Ojjela, "Sentiment Analysis for Defence Ecosystem and Armed Forces?" presented at the European Conference on Cyber Warfare and Security, June 2025, https://www.researchgate.net/publication/393048207_Sentiment_Analysis_for_Defence_Ecosystem_and_Armed_Forces.

[11] Nafuye, I. (2024). Weaponizing Artificial Intelligence in the Russia-Ukraine War.

[12] Redmon, J., & Farhadi, A. (2018). YOLOv3: An Incremental Improvement. arXiv:1804.02767.

[13] Ren, S., He, K., Girshick, R., & Sun, J. (2015). Faster R-CNN. NeurIPS.

[14] Bewley, A., Ge, Z., Ott, L., Ramos, F., & Upcroft, B. (2016). Simple online and realtime tracking. IEEE ICIP.

[15] Bertinetto, L., Valmadre, J., Henriques, J. F., Vedaldi, A., & Torr, P. (2016). Fully-convolutional siamese networks for object tracking. ECCV.

[16] Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. NIST Special Publication 800-145.

[17] Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1(1), 7 - 18.

[18] Saxe, J., & Berlin, K. (2015). Deep neural network based malware detection using two dimensional binary program features. MALWARE.

[19] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Comm. Surveys & Tutorials.

[20] Goldberg, Y. (2017). Neural Network Methods for Natural Language Processing. Synthesis Lectures on Human Language Technologies.

[21] Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2019). BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. NAACL-HLT.

[22] Systematic. "The Silver Lining of Military Cloud Computing: Benefits and Solutions." Systematic, 27 July 2023, systematic.com/us/industries/defense/news-knowledge/blog/the-silver-lining-to-military-cloud-computing/.

[23] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2014). Generative Adversarial Nets. In Advances in neural information processing systems (pp. 2672-2680).

[24] Verdoliva, L. (2020). Deepfake video detection methods: A survey. IEEE Journal of Selected Topics in Signal Processing, 14(5), 1083-1094.

[25] International Centre for Defence and Security. (2025). Russia's War in Ukraine: Artificial Intelligence in Defence of Ukraine. https://icds.ee/en/russias-war-in-ukraine-artificial-intelligence-in-defence-of-ukraine/

[26] European Digital Media Observatory. (2025, July 14). The First AI War? How the Iran-Israel Conflict Became a Battlefield for Generative Misinformation. https://edmo.eu/publications/the-first-ai-war-how-the-iran-israel-conflict-became-a-battlefield-for-generative-misinformation/.

[27] Bondar, Kateryna, and Samuel Bendett. "The Russia-Ukraine Drone War: Innovation on the Frontlines and Beyond." Center for Strategic and International Studies, 28 May 2025, www.csis.org/analysis/russia-ukraine-drone-war-innovation-frontlines-and-beyond.

[28] Hunder, Max. "Ukraine Rolls out Dozens of AI Systems to Help Its Drones Hit Targets." Reuters, 31 Oct. 2024, www.reuters.com/world/europe/ukraine-rolls-out-dozens-ai-systems-help-its-drones-hit-targets-2024-10-31/.

[29] The Times of Israel Staff. "Israel Using AI to Pinpoint Hamas Leaders, Find Hostages in Gaza Tunnels – Report." The Times of Israel, n.d., www.timesofisrael.com/israel-using-ai-to-pinpoint-hamas-leaders-find-hostages-in-gaza-tunnels-report/.

[30] European Digital Media Observatory. "The First AI War: How the Iran-Israel Conflict Became a Battlefield for Generative Misinformation." European Digital Media Observatory, 25 Apr. 2024, edmo.eu/publications/the-first-ai-war-how-the-iran-israel-conflict-became-a-battlefield-for-generative-misinformation/.

[31] Microsoft. (2024). Microsoft Digital Defense Report 2024. Retrieved from

https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024

[32] Smith, B. (2022, June 22). Defending Ukraine: early lessons from the cyber war. Microsoft On the Issues. https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/