ISSUE BRIEF

이슈브리프 844호
(2026. 5.21)

# 이란전에 나타난 사이버전의 진화적 양상과 시사점

제844호

윤정현 yjh5791@inss.re.kr

국가안보전략연구원
Institute for National Security Strategy

INSS
www.inss.re.kr

# 국문초록

2026년 이란전은 사이버전의 위상과 작동 방식이 새로운 전환점에 도달했음을 보여주고 있다. 2022년 개전 당시의 러시아-우크라이나 전쟁이 '하이브리드전(Hybrid Warfare) 시대를 열었다면, 이번 이란전은 사이버전이 물리전·정보전·심리전 전반에 상시적으로 결합됨은 물론, 전술적 차원을 넘어 전략적 파급력을 갖는 복합 전쟁 수행 환경으로 진화하고 있음을 보여주기 때문이다. 특히 이번 전쟁에서 주목할 점은 사이버전이 단순한 시스템 파괴나 기술적 교란을 넘어, 압도적인 군사력 열세를 보완하기 위해 민간 플랫폼을 활용한 비대칭 전략 수단으로 자리매김했다는 점이다. 이란은 미국·이스라엘과의 정면 군사 경쟁에서 한계를 보완하기 위해 Telegram, WhatsApp 등을 활용한 위협 메시지와 정보 유출, 생성형 AI 기반 허위 전장 콘텐츠 확산 등을 병행한 것이 대표적이다. 이번 이란전은 향후 사이버안보 전략이 전통적인 정보망 보호와 기술적 방어에 머물러서는 안된다는 점을 보여준다. 플랫폼·통신·클라우드·산업 네트워크 의존도가 높은 한국은 이 같은 사이버전의 진화에 대응하기 위해 △국가 핵심 인프라 보호에 초점을 둔 사이버안보 전략, △핵티비스트·민간 플랫폼이 결합된 회색지대 사이버전에 대한 대비, △AI 기반 정보전 확산에 대응하는 신뢰성과 책임성 강화노력이 필요하다. 이는 우리의 사이버안보 전략이 전·평시와 공공·민간의 구분을 넘어 사회 전체의 상시적 안정성과 신뢰성을 관리하는 방향으로 확대되어야 함을 의미한다.

**주제어 : 사이버안보, 이란전, 사이버전, 핵티비스트, AI 정보전**

2026년 미국-이스라엘 대 이란 전쟁은 사이버전이 전쟁 전반에 상시적으로 결합되는 보다 정교한 복합 전쟁 수행 환경으로 진화하고 있음을 보여주고 있다. 지난 2022년 러시아-우크라이나 전쟁 초기, 사이버전이 전력망 마비, 정부 기관 네트워크 공격, 와이퍼 악성코드 배포 등 국가 핵심 인프라를 직접 무력화하는 방식이 중심을 이루었다면, 이번 이란전에서는 사회적 불안과 공포, 정치적 피로감을 증폭시키는 AI 기반 정보 심리전, 인지전의 양상이 더욱 선명하게 나타나고 있다. 또한, 국가 중심에서 핵티비스트·플랫폼 결합형 생태계로의 변화 역시 감지되고 있다. 이번 전쟁에서는 친이란 성향 핵티비스트 그룹들이 활발하게 활동하였으며, 민간 플랫폼과 상용 서비스가 작전 수행의 핵심 기반으로 활용되고 있다. 이는 국가가 직접 수행하는 전통적 사이버전 개념을 넘어, 국가·대리세력·온라인 커뮤니티·민간 플랫폼이 결합된 분산형 사이버전 수행 구조가 강화되고 있음을 보여준다.

더 나아가, 압도적 군사력 격차를 상쇄하기 위한 효과적 비대칭 수단으로서 사이버전의 중요성이 더욱 증대되고 있다. SNS 기반 심리전과 여론전 등은 상대 사회 내부의 불안과 피로를 누적시키기 위한 비대칭 전략의 성격을 선명히 보여준다. 이는 현대 사이버전이 단순한 기술적 공격을 넘어 상대국 사회 전체의 심리적 안정성과 신뢰체계를 흔드는 장기적 압박 수단으로 기능하고 있음을 암시하는 것이다. 이 같은 변화의 양상들은 우리에게도 미래 사이버전 환경에 부합하는 국가 사이버안보 전략의 보완·재편 필요성 역시 제기하고 있다.

## 2026년 이란전에 나타난 사이버전의 주요 특징

이번 이란전에서 나타난 첫 번째 특징은 군사작전과 더 긴밀히 연결되는 사이버 첩보 활동 및 실시간 표적화 양상이다. 러시아-우크라이나 전쟁 초기 사이버전이 정부 기관 네트워크 마비, 와이퍼 악성코드 배포, 통신 장애 유발 등 전쟁 개시 이전 또는 초기 단계에서 상대

지휘체계와 기반시설을 혼란시키는 전초전 성격이 강했다면, 이번 이란전에서는 사이버 공간에서 수집된 정보가 실제 군사작전과 긴밀하게 연계되는 양상이 두드러지게 나타나고 있다. 특히 민간 디지털 인프라와 상용 플랫폼, CCTV 교통시스템·모바일 애플리케이션·소셜미디어 등 일상적 네트워크 환경이 정보수집 및 표적화 과정에 적극 활용되었다는 점은 주목할 필요가 있다.[1] 실제로 개전과 시작된 미국과 이스라엘의 이란 지도부 암살에는 표적 식별에서 이동 경로 추적, 우선 공격대상 타격까지 채 60초가 되지 않는 시간 안에 작전이 이루어진 것으로 보고되었다.[2] 즉, 사이버 공간을 활용한 첩보활동이 실시간으로 핵심적인 군사작전과 결합되고 있는 것이다.

두 번째 특징은 빈번하게 나타나는 중요 인프라와 산업제어시스템을 겨냥한 비대칭 공격이라 할 수 있다. 특히 이번 이란전에서는 상대국의 정치적 불안과 압박을 가하기 위한 교란형 공격들이 두드러지게 감행되었다. 특히 미국 및 이스라엘과의 정면 군사 경쟁에서 열세에 있는 이란 정부 및 일부 친이란 조직들은 수자원 시설, 에너지 설비, 산업 자동화 시스템 등 인터넷에 노출된 제어·운용 장비를 주요 공격 대상으로 설정하였다. 특히 친이란 성향 핵티비스트 조직들은 미국 및 이스라엘 연계 수자원·에너지 시설을 대상으로 인터넷에 노출된 공장·발전소·정수 처리시설 등의 기계 설비에 대한 자동 제어장비(Programmable Logic Controlle, PLC)에 대한 반복적 접근을 시도한 것으로 보고되었다.[3]

세 번째 특징은 AI 기반 정보전과 SNS 영향력 공작의 고도화 양상이다. 특히 AI 기반 정보전과 SNS 영향력 공작이 보다 적극적이고 정교한

1) Palo Alto Networks Unit 42 (April 17, 2026),
2) Greg Miller, “Israel targets Iran′s leaders with lethal expertise using new AI platform,” *The Washington Post*, (March 30, 2026); Alec Dent, “How Israel tracks and targets Iran′s leaders,” The Washington Post, (March 30, 2026).
3) CCCS, “Cyber Threat Bulletin: Iranian Cyber Threat Response to US/Israel Strikes,” (May 2026); CISA, “Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest,” (2026).

방식으로 전개되었다는 점을 들 수 있다. 러시아-우크라이나 전쟁에서도 딥페이크 영상과 허위정보 유포 등 정보전 양상이 나타난 바 있으나, 당시에는 상대적으로 국가기관·언론·공식 선전 채널 중심의 여론전 성격이 강했다. 반면 이번 이란전에서는 생성형 AI와 소셜미디어 플랫폼이 결합되며, 보다 분산적이고 실시간적인 형태의 인지전 양상이 두드러지게 나타나고 있다.

특히 사이버전의 중심이 단순 시스템 공격에서 사회적 인식과 정보 신뢰성을 균열시키는 방향으로 확대되고 있다는 점에서 주목할 필요가 있다. 생성형 AI 기반 콘텐츠와 자극적 메시지는 플랫폼 알고리즘을 통해 단시간 내 대규모로 확산될 수 있으며, 사실 검증 이전에 사회적 반응과 정치적 논쟁을 유발하는 특징을 가진다. 실제로 쇼폼 영상과 밈(Meme) 형태의 콘텐츠가 Telegram·X 및 TikTok 등을 중심으로 빠르게 확산되면서 정보의 사실 여부보다 감정적 반응과 공유 속도가 더욱 중요해지고 있는 양상을 보여주었다.[4] 이는 현대 사이버전이 단순한 네트워크 공격을 넘어, 사회 구성원들의 심리적 안정성과 일상적 신뢰 환경 자체를 공격 대상으로 삼고 있음을 시사하고 있다. 이를 종합하면, 지난 2022년과 비교하여 2026년의 이란전은 사이버전의 진화적 측면에서 다음과 같은 특징을 보여주고 있다.

4) The Guardian, “Iran Social Media Strategy Pivots to Information War Amid Attacks,” (March 22, 2026); Politics Today, “The US-Iran War: Cognitive Warfare and the Use of AI-Integrated Systems,” (May 2026).

<표 1> 러시아-우크라이나 전쟁과 2026년 이란전의 사이버전 비교

| 구분 | 2022 러시아-우크라이나 전쟁 | 2026년 미국-이스라엘·이란 전쟁 |
|---|---|---|
| 사이버전의 역할 | 개전 초기 교란 및 전초전 성격 | 전쟁 전반에 상시 결합된 작전 환경 |
| 주요 공격 목표 | 정부망·전력망·통신망 | 사회 인식·민간 플랫폼·산업제어망 |
| 주요 공격 방식 | 개전초기 심리전·영향력 공작 와이퍼·DDoS·네트워크 마비 | 심리전·영향력 공작·지속 교란 |
| 정보전 특징 | 국가기관·공식 선전 중심 | 생성형 AI·SNS 기반 분산형 인지전 |
| 전략적 목적 | 군사작전 지원 및 기반시설 무력화 | 사회적 피로감 및 불확실성 제기 |
| 주요 특징 | 하이브리드전의 전초전 | 하이브리드전의 전초전 + 비대칭·사회침투형 사이버전 |

출처: 저자 작성

## 이란전에 나타난 사이버안보 전략의 새로운 전환 과제

이번 이란전이 주는 첫 번째 함의는 사이버안보 전략이 기존 정보망 보호 중심에서 국가 핵심 인프라와 사회 운영 환경 전반의 안정성 확보를 중시하는 방향으로 확대되고 있다는 점이다. 특히 에너지·수자원·통신·산업자동화시스템 등 민간 운영 기반 시설이 실제 전쟁 상황에서 지속적인 사이버 위협에 노출되면서, 핵심 인프라 자체를 국가안보의 핵심 영역으로 인식하는 경향이 더욱 강화되고 있다는 점에 주목할 필요가 있다. 과거 사이버안보 전략이 정부 기관과 군사 네트워크 방어에 상대적으로 집중되었다면, 최근에는 국가 경제와 사회 운영을 지탱하는 민간 기반시설의 회복탄력성 확보가 중요한 전략 과제가 될 수 있음을 시사한다.

이 과정에서 민간 운영 기반 시설과 정부 간 협력체계 강화 필요성이 더욱 부각되고 있다. 이란전에 나타난 사이버 공격 표적을 통해 상당수의 핵심 서비스와 산업 운영 환경이 민간 기업 및 상용 플랫폼 중심으로 운영되고 있다는 점이 재확인되었기 때문이다. 이미 NATO와 EU는 중요 기반 시설 보호와 사이버 회복탄력성(resilience) 강화를 핵심 의제로 설정하였으며, 클라우드·통신·에너지·플랫폼 기업들을 국가 사이버안보 체계의 일부로 통합하려는 움직임이 확대되고 있다. 이는 현대 사이버안보 전략에서 민간 부문의 역할이 점차 확대되고 있음을 보여준다.[5]

두 번째 함의는 국가기관 중심의 전통적 사이버전 개념이 국가·핵티비스트·민간 플랫폼이 결합된 보다 분산적인 수행 구조로 변화하고 있다는 점이다. 이번 전쟁에서는 Handala, CyberAv3ngers 등 친이란 성향 조직들이 활발하게 활동하였으며, Telegram·WhatsApp·X·TikTok 등 글로벌 플랫폼이 정보 확산, 심리전의 핵심 공간으로 활용되었다. 이는 국가가 직접 개입하지 않더라도 우호적 온라인 세력과 비국가 행위자, 상용 플랫폼을 활용하여 전략적 압박 효과를 증폭시킬 수 있는 환경이 확대되고 있음을 의미한다. 특히 이러한 회색 지대형 사이버전 환경에서는 책임 귀속(attribution)과 억지(deterrence)가 더욱 어려워질 수 있다는 점에서 주목할 필요가 있다.

세 번째 함의는 정보의 신뢰성과 사회적 안정성 확보를 위한 플랫폼 기업과의 민관 파트너십의 재정립 필요성이다. 이란전에 나타난 AI 기반 사이버전은 단순한 네트워크 공격을 넘어 사회적 인식과 여론을 흔드는 정보전·인지전의 비중이 높아지고 있기 때문이다. 특히 허위 콘텐츠 생산 비용과 시간이 급격히 감소하면서, 정보의 사실 여부보다 감정적 반응과 확산 속도가 우선되는 양상이 강화되고 있다. 이는 향후 사이버안보 전략의 초점 역시 기술적 보안 뿐만 아니라 정보와

5) NATO CCDCOE, “Cyber Threats and Critical Infrastructure Resilience,” (2026); European Commission, “ProtectEU Strategy,” (2026).

콘텐츠의 신뢰성을 검증하기 위한 기반을 어떻게 마련할 것인가에 두어야 함을 시사한다. Brookings를 비롯한 주요 싱크탱크들은 플랫폼 기업들을 사실상 글로벌 정보 환경의 '준(準)안보 행위자'로 인식하고, 이들과 정부 간 긴밀한 협력체계 구축이 필수적임을 강조한 바 있다.[6] 즉, 사이버안보 전략이 기술적 보안 역량뿐만 아니라 플랫폼 거버넌스와 정보 검증체계 구축까지 포괄하는 방향으로 확대될 필요가 있음을 보여준다.

## 한국의 사이버안보 전략에 주는 시사점

우리 정부 역시 △데이터 중심 정보보호체계 전환, △범정부 차원의 사이버보안 대응체계 구축, △AI 기반 신종 사이버위협 대응 강화 등에 초점을 맞추어 사이버안보 정책을 주요 방향으로 추진 중이다. 특히 민관 협력을 통한 사이버보안 기술 경쟁력 강화와 핵심 기술 국산화, 중소기업 및 지역 산업 대상 정보보호 투자 확대, AI 악용 보이스피싱·스미싱 대응 강화 등은 현 정부가 사이버안보를 단순 기술 문제가 아니라 국민 생활과 신뢰, 사회적 안정성 전반의 문제로 인식하고 있음을 보여준다.

그러나 이번 이란전에서 나타난 사이버전의 진화는 보다 확장된 관점에서 민관 파트너십을 재구성 해야할 필요성을 보여준다. AI 기반 허위 전투 장면 생성, 조작된 피해 이미지, 자동 생성 선전 콘텐츠 등이 대량 확산되며 정보 신뢰성에 대한 공격이 더욱 고도화되었으며, 정치적 개입과 여론 확산 시도 역시 보다 적극적으로 전개되었다. 이는 기존의 정보망 방어와 기업 보안 강화만으로는 대응하기 어려운 새로운 형태의 복합적 사이버 위협이 확대되고 있음을 보여준다. 특히 플랫폼·통신·클라우드·산업 네트워크 의존도가 높은 한국은

6) Brookings Institution, "Platform Governance and the Future of Information Security," (2026); Carnegie Endowment for International Peace, "AI Disinformation and Platform Accountability," (2026).

사회적 불안과 정보 혼란, 핵심 서비스 장애 등이 빠르게 확산될 가능성이 있다는 점에서 더욱 경계할 필요가 있다.

이는 결국 한국의 사이버안보 전략 역시 단순한 정보망 보호 차원을 넘어, 사회 전체의 정보 신뢰성과 심리적 안정성, 플랫폼 환경과 여론 공간까지 함께 관리해야 하는 보다 복합적이고 장기적인 안보 과제를 마주하고 있음을 의미한다. △플랫폼 의존성이 국가안보 취약성으로 전환될 가능성에 대비한 전략적 자율성 확보, △AI 기반 허위정보와 플랫폼 영향력 공작에 대응하기 위한 민관 공동 정보 검증체계 강화, △산업제어시스템에 대한 회복탄력성 중심 설계 전환, △회색 지대형 사이버 위협 대응체계 정교화 등이 대표적이다. 이는 전·평시를 막론하고 우리의 사이버안보 전략이 사회 전체의 정보 신뢰성과 국가 운영 안정성까지 함께 관리하는 방향으로 확대되어야 함을 의미한다.

*//끝//*

**본 내용은 집필자 개인의 견해이며,**
**국가안보전략연구원의 공식입장과는 다를 수 있습니다.**