ISSUE BRIEF

이슈브리프 383호
(2022. 9. 5)

러시아-우크라이나 전쟁 장기화와 정보·심리전의 진화 양상

제383호

윤정현 안보전략연구실

국가안보전략연구원
Institute for National Security Strategy

INSS
www.inss.re.kr

국문초록

오늘날 정보·심리전은 여론을 주도하고, 적국의 의사결정 혼선과 저항의지를 무력화시킴으로써 전황을 유리한 국면으로 이끌어가기 위한 수단이 되고 있다. 특히, 2022년 러시아-우크라이나 전쟁은 고도화된 디지털 정보커뮤니케이션 환경에서 전시의 비무력적 군사활동인 정보·심리전이 전면전에서 효과적인 공격·방어 수단으로 작용하는 양상을 보여준 사례이다. 실제로 러시아의 공격에 맞선 우크라이나 측의 담론 프레이밍과 반격 내러티브는 초기의 전세를 유리하게 확보하는데 결정적으로 작용한 바 있다. 또한, 디지털 플랫폼이 사이버 공간의 정보·심리전에 본격적으로 무기화되는 양상을 극명하게 보여준 계기가 되었다. 러시아-우크라이나 간 전쟁에 나타난 정보·심리전의 진화 양상은 한반도 안보환경에도 시사하는 바가 크다. 전면전 이전 단계에서 포괄적인 형태의 사이버전과 정보심리 공격의 선행 가능성을 보여주는 만큼, '평시-긴장고조-무력충돌'로 이어지는 각 단계에 대한 전주기 대응역량이 필요할 것이다. 특히, 동맹 및 우호국과의 공조는 정부의 정치적 정당성과 권위, 민주주의 제도와 사회질서를 유지하는데 필수불가결한 요소라 할 수 있다. 따라서, 향후 진화된 사이버 공간의 정보·심리전 대응을 위해서는 국제 정보협력 강화에 방점을 두고, 이를 지속할 수 있는 실천 방안을 고민해야 한다. 한·미, 한·NATO와의 긴밀한 정보공유체계 구축, 진화된 인지전에 대비한 민간과의 연구협력 확대는 우선적인 실천과제라 할 수 있을 것이다.

핵심어: 정보·심리전, 인지전, 사이버전, 하이브리드전, 러시아-우크라이나 전쟁

이번 러시아-우크라이나 전쟁에서 보듯이 현대의 하이브리드전에서 전략적·전술적 주도권을 갖기 위해서는 정보의 우위 확보가 필수적이다. 이에 따라 최근 주요 강대국들은 사이버 공간을 정보 대립 측면에서 영향력 투사를 위한 전장으로 인식하고 있으며, 민간·비정규 조직과도 긴밀한 협력을 강화하고 있다. 실제로 러시아의 물리적 침공에 앞선 사이버전 단계에서부터, 우크라이나를 지원한 서방의 민간기업과 SNS 기반의 '사이버 의용군(IT Army)'들은 두드러진 역할을 보여준 바 있다. 이들은 사이버공격 뿐만 아니라 허위정보의 차단과 역습, 국제여론 조성에 이르기까지 사이버전의 주역으로 참여하고 있다. 이러한 맥락에서 러시아-우크라이나 전쟁은 수행 주체, 범위, 방식 등 하이브리드전의 진화 방향을 엿볼 수 있는 중요한 분기점으로 평가되고 있다.

하이브리드전의 주요 전술적 수단으로서 정보·심리전

무엇보다 '정보·심리전(information & psychological warfare)'은 여론을 주도하고, 적국의 의사결정 혼선과 저항 의지를 무력화시킴으로써 전황을 유리한 국면으로 이끌어가기 위한 대결이라 할 수 있다. 특히, 전시의 정보작전과 심리작전은 단순히 선전의 효과를 넘어 전술적 우위를 부여하는 군사적 기능도 수행하고 있어 주목할 필요가 있다. 먼저, '정보작전(information operation)'은 실제 정보와 허위정보, 조작정보 상황에 대한 오독과 왜곡, 기만, 정보의 과부하를 유발하는 형태로 상대의 올바른 의사결정을 방해하는 전술이다. '심리작전(psychological operation)'은 적의 사기나 전투 의지를 꺾고 아군 및 동맹의 결의와 사기를 강화시키기 위한 활동으로, 상대의 허위조작정보 공격이나 선전 프레임에 맞서 자국의 정치적 정당성과 권위, 민주주의 제도와 사회질서를 유지하는데 유용한 수단이라 할 수 있다. 특히, 평시와 비상시, 전시 모든 상황에서 이루어

질 수 있으며 그 자체로는 비무력적 활동일 수 있지만, 폭력적 상황에서는 군사적 파괴력을 배가시켜주는 수단으로 작용하기도 한다. 이들은 모두 자원 투입대비 효과가 큰 수단이지만, 계획된 수행을 위해서는 온라인 플랫폼 등 주요 네트워크와 인프라에 대한 접근이 확보돼야 한다는 전제조건을 안고 있다.[1)]

정보·심리전은 향후 사람들의 인식(perception)체계를 바꾸고, 실제적 행동으로 연결할 수 있도록 과학적 메커니즘을 더욱 정교하게 구현한 '인지전(cognitive warfare)'으로 진화할 것으로 예상된다. 정보콘텐츠의 흐름을 통제하기 위한 공격-방어술인 정보전(information warfare)과 달리, 인지전은 정보콘텐츠를 인간의 뇌가 수용·해석하는 행위와 밀접한 개념이다. 인지전이 부상한 배경에는 인간의 정보 습득-의사결정-행동 메커니즘에 대한 광범위한 데이터의 축적 뿐만 아니라 인공지능을 통한 분석 역량이 극대화됨으로써 이를 각 분야에 적용, 활용할 수 있게 되었기 때문이다. 인지전의 전략적 목표는 적의 담론을 압도할 수 있는 아측의 내러티브(narrative) 역량 확보라 할 수 있다. 즉, 인지전 관점에서는 어느 편의 내러티브가 지적, 정서적, 윤리적 매력과 설득력의 우위를 갖는가에 따라 전쟁의 승패가 결정된다고 보는 것이다.[2)] 주요국들은 사람들의 인지적 반응 통제를 위한 정보기술, 뇌과학 등 사회공학 전반을 포괄하는 복합 전술로서 인지전 역량을 강화하는 중이다. 실제로 미국, 영국, NATO 등에서는 인간의 생각(human mind)을 구현하는 뇌 영역 또한 향후 육·해·공·우주·사이버를 잇는 6번째 전장이 될 것으로 전망한 바 있다.[3)]

---

1) 송태은, "러시아-우크라이나 전쟁의 정보·심리전: 평가와 함의" 『IFANS 주요국제문제분석』, 2022년 제12호, (2022.5.10.), p. 1.
2) 송태은, "사이버 심리전의 프로퍼갠더 전술과 권위주의 레짐의 샤프파워: 러시아의 심리전과 서구 민주주의 대응," 『4차 산업혁명과 신흥군사안보』, (서울: 한울아카데미), p. 174.
3) Leonid Savin, "NATO developed new methods of cognitive warfare", (November 14, 2021).

러시아-우크라이나 전쟁에 나타난 정보·심리전과 협력 사례

2022년 러시아-우크라이나 전쟁은 고도화된 디지털 정보커뮤니케이션 환경에서 전시의 비무력적 군사활동인 정보·심리전이 전면전에서 효과적인 공격·방어 수단으로 작용하는 양상을 보여준 사례이다. 특히, 러시아의 공격에 맞선 우크라이나 측의 담론 프레이밍과 반격 내러티브는 초기의 전세를 유리하게 확보하는데 결정적으로 작용하였다.

우크라이나의 대항 정보·심리전이 러시아를 압도할 수 있었던 배경에는 크림반도 상실 이후 허위조작정보 공격에 체계적으로 대비해 왔던 것이 주효했다고 볼 수 있다. 우크라이나는 2015년 초부터 Ukraine Today와 StopFake와 같은 해외발신에 중점을 둔 미디어 플랫폼과 팩트체크 채널을 구축한 바 있다. 대외적으로도 서방과 민감한 전황 정보 및 러시아 군사정보를 공유할 수 있는 제도적 기반을 마련했으며, 이를 통해 우크라이나 정보부(Ministry of Information)는 전황에 대한 지속적인 보도활동과 유리한 전황 정보를 국내외로 전파할 수 있었다.[4] 이는 실제 전쟁 발발시 우크라이나가 발신하는 정보와 내러티브의 설득력을 높였고, 2022년 전쟁 발발시 전장에서 우크라이나가가 러시아에 비해 정보의 우위를 누릴 수 있도록 하는데 크게 기여했다. 실제로 러시아가 우크라이나를 무력으로 침공하자, 세계 각국에서 비난여론을 쏟아내는 한편, 어나니머스와 같은 국제적인 해킹단체가 러시아 정부와 방송국 등을 공격하면서 맞불을 놓았다. 우크라이나 정부는 텔레그램에 '사이버 의용군'을 모집한다고 공개했으며, 이후 국적을 불문한 많은 자발적 해커들이 참여하였다. 나아가, Facebook, Instagram, Twiter 등 전 세계의 이용자들이 자유롭게 접근가능한 SNS를 기반으로 실시간 전황 정보를 게시하였고, 우크라이나가 제공한 정보를 누구나 자발적으로 공유·확산할 수 있도록 하였다.

4) 송태은(2022.5.10.), p. 2.

다른 한편으로 이번 전쟁은 디지털 플랫폼이 사이버 공간의 정보·심리전에 본격적으로 무기화되는 양상을 극명하게 보여준 계기가 되었다. 우크라이나는 공유한 정보역량을 결집시켜 자국에 유리한 콘텐츠를 효과적으로 확산시킬 수 있었으며, 러시아發 정보에 대한 불신감을 확대하는 한편, 크렘린을 '무능한 거짓말쟁이' 이미지로 고착화시키는데 성공했다. 특히, 이 과정에서 글로벌 IT기업과 초국가적 해커 및 민간조직들은 러시아 관영매체의 콘텐츠를 차단하고 우크라이나 관점의 담론 확산을 지원함으로써, 국제사회의 지원을 유도하고 장기적 항전을 지속할 수 있는 동력을 제공했다고 평가할 수 있다.

한반도 안보 상황에서의 의미와 국제 정보협력의 중요성

러시아-우크라이나 간 전쟁에 나타난 정보·심리전의 진화 양상은 한반도 안보환경에도 시사하는 바가 크다. 전면전 이전 단계에서 포괄적인 형태의 사이버전과 정보심리 공격의 선행 가능성을 보여주는 만큼, '평시-긴장고조-무력충돌'로 이어지는 각 단계에 대한 전주기 대응역량이 필요할 것이다. 특히, 그간 북한은 평시에도 미사일 발사, 핵실험 뒤 위협적 선전을 통해 우리사회 내부 분열과 무력감 확산을 노린 '와해전략(distuption strategy)'을 토대로 심리적 투쟁을 전개해왔으며, 국가배후 및 다양한 해킹조직과의 연계한 허위조작, 왜곡정보 유포 행위들은 위기상황을 고조시켜왔다. 또한, 65개의 친북사이트와 200여개의 국내 인터넷망을 이용하여 사이버 여론전과 프로파간다를 실행했던 것으로 파악되기도 하였다.[5] 그러나 이에 대응하기 위한 우리의 제도적 현실은 디지털정보 수집을 뒷받침하는 세부적인 수단, 방법 및 절차가 법률로 명시되지 않아 적극적인 수집이 제한되어 있다. 이로인해 악의적인 정보·심리전 활동을 실시간으로 탐지하고, 역추적하여 신속히 대응하는데 한계가 있는 실정이다. 또한, 평시-전시 국면에서의 국방 사이버공간과 사이버작전공간의

5) 윤민우, 『폭력의 시대 국가안보의 실존적 변화와 테러리즘』, (서울: 박영사, 2017), p. 251.

개념이 여전히 불일치하며, 사이버 공간의 확장과 재정의가 필요한 상황이다. 나아가 사이버안보 기본법의 임무 확대 공식화와 사이버 작전 책임 범위, 군사교리 내 정보·심리전 개념의 확장 및 적용 임무, 범위를 구체화해야하는 문제가 남아있다. 뿐만 아니라 위기상황, 전시의 사회적 혼란을 틈타 난민, 테러 등 사회적으로도 민감한 이슈에서 조작정보 등에 효과적으로 대응하기 위한 전략커뮤니케이션 측면의 보완도 요구되고 있다.

이 같은 난제는 당장 독자적으로 해결하기 어려우며, 초국가적 정보공유를 위한 채널을 필요로 한다. 러시아-우크라이나 전쟁에서 보듯이, 정보·심리전의 대응에 있어서 동맹 및 우호국과의 공조는 정부의 정치적 정당성과 권위, 민주주의 제도와 사회질서를 유지하는데 필수불가결한 요소이기 때문이다. 즉, 향후 진화된 사이버 공간의 정보·심리전 대응을 위해서는 국제 정보협력 강화에 방점을 두고, 이를 지속할 수 있는 실천방안을 고민해야 한다.

한·미, 한·NATO와의 긴밀한 정보공유체계 구축

우선, 한반도 안보상황에서 한·미간 원활한 정보 공유를 위한 운용성의 개발과 협조는 더욱 중요해지고 있다. 대북 조기경보징후 판단을 위한 확장억제전략협의체 조기 재가동, 한미 연합훈련 확대 가능성 등의 사안이 보다 심층적으로 논의되어야할 것이다. 또한, 포괄적 전략파트너십에 걸맞게 훈련범위를 전통적 군사작전 범위 외연으로 확대할 필요성이 제기된다. 예를 들어, 현재 한미 연합전투력을 배가하기 위해 수립된 연합군사정보처리체계(MIMS-C: AI와 최신 ICT기술을 적용해 기존 한미 군사정보처리 장비의 정보공유·분석능력 향상을 목표로 2024년 12월까지 전력화 계획)와 ICT 협력위원회의 동맹 간 상호 운용성 확보 분야의 논의를 정규전 군사지휘통제 외연으로 확장할 필요가 있다.

또한, 최근 미국 방첩보안센터는 전방위적 위협을 가하는 주요 관심국가(러·중·이란·북한)에 대한 전략계획(2018-2022 NCSC Strategic Plan)을 수립한 바 있다. 그리고 북한처럼 기술 수준은 낮더라도 악의적 의도를 가진 국가행위자를 이데올로기적 해커, 미국과 동맹국의 사이버첩보를 활용하는 내부자 등과 함께 주요 사이버 적대활동의 주체로 규정하였다. 정규전에 대비한 상시전투태세(Fight Tonight) 뿐만 아니라 비물리적 상황에서의 사이버전, 정보·심리전의 공세에 즉각적으로 대응하기 위한 정보 자원 공유, 활용 준비태세 확립 방안 논의가 필요하다고 볼 수 있다.

최근 안보 파트너십의 범위를 확대하고 있는 NATO와도 정보·심리전에 공조할 수 있는 전략 시나리오 훈련, 위협대응 모델을 개발·공유할 필요성 역시 제기되고 있다. NATO는 사이버공격에 대한 동맹국 간 신뢰구축조치 개발 및 적용에 많은 관심을 보여왔다. 한국은 NATO의 사이버방위 정책 형성 논의에는 참여하지 못했으나, 현재 NATO 사이버방위협력센터(CCDCOE)의 기여국(Contributing Partner)으로 가입한 상태이다. 또한, CCDCOE이 주관하는 'Locked Shields 22' 훈련을 참관하는 등, 지역을 넘어 글로벌 사이버안보 협의체에 참여를 약속한 바 있다. 나아가 우리 군은 2023년부터 NATO 회원국 및 파트너국과의 사이버동맹 연례연합훈련에 참가할 예정이며, 2022년 10월에는 美사이버사령부가 주관하고 영국, 캐나다, 호주, 뉴질랜드, 일본, 프랑스 등이 참가하는 '사이버 플래그(Cyber Flag)' 연례 훈련에도 합류할 계획이다. 이 같은 활동들이 우리의 실질적인 사이버전 역량으로 이어지기 위해서는 공격·방어훈련 및 상황보고, 국제법 적용가능성 판단, 미디어 대응 등 발생가능 시나리오상의 모든 단계에 대한 의사결정 및 훈련을 체계화할 필요가 있다.

진화된 인지전에 대비한 민간과의 연구기반·정보협력 확대

인지전은 은밀함과 익명화의 특성을 보이고 있다. 따라서 향후 진화된 인지전에 대비하기 위해서는 데이터 분석력과 보안을 강화해야 한다. 이를 위해 '데이터 비식별화', '동형암호(암호화된 상태로 데이터 분석·연산이 가능한 암호)' 고도화 등, 민간의 축적된 기술을 도입하여 활용성을 제고하는 방법을 모색해야 한다. 이는 평시에도 IT 기업과 정부 간 사이버 위협 대응 협력을 위한 빈번한 기술교류와 상호지원, 인력 파견의 필요성을 시사한다.

특히, 민간의 역량을 적극 활용하기 위해 평시 신뢰할 수 있는 파트너십과 연대를 강화하고 사이버보안의 회복탄력성(resilience) 발휘를 위한 다양한 교류를 정례화할 필요가 있다. 그리고 전략토론과 공동훈련 등 민·관 협력의 기반이 되는 정보·심리전 대응을 위한 표준 프레임워크 개발이 마련되어야 한다. 나아가 정보·심리전 역량을 갖춘 전문인력을 양성하기 위해서는 공학 뿐만 아니라 인문사회적 지식을 제공하는 융합적 교육 프로그램이 필요하다. 이는 인재 양성 주체로서의 교육기관에 대한 지원 강화가 전제되어야 하는 일이다.

//끝//