INSS
전략보고
November 2022. No.196

www.inss.re.kr
INSTITUTE FOR NATIONAL SECURITY STRATEGY

정보심리전의 진화 양상과 대응 방안

윤정현 부연구위원
yjh5791@inss.re.kr

국가안보전략연구원

국문 초록

오늘날 정보심리전은 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. 본 연구는 정보심리전 및 이와 연계된 다양한 개념들을 고찰하고, 향후 전망과 위협 양상을 전망하며, 한국적 상황에 제기하는 시사점을 도출하고자 하였다. 정보심리전과 인지전의 진화 양상은 한반도 안보환경에도 새로운 도전을 제기할 것이다. 이에 맞서 동맹 및 우호국과의 공조는 정부의 정치적 정당성과 권위, 민주주의 제도와 사회질서를 유지하는데 필수불가결한 요소라 할 수 있다. 따라서, 진화된 정보심리전 위협에 대비하기 위한 국제 소통 강화, 한미 정보자원 우위를 위한 논의 확장, 민간·비정부 행위자들과의 연구기반·정보협력 확대 등 다층적 수준에서 다양한 행위주체들과의 협력방안을 고민해야 할 것이다.

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

목차

Ⅰ. 문제 제기

- 오늘날 정보심리전은 군사적 효용 뿐만 아니라 정치적 정당성 확보, 국제적인 지원과 우호적 전쟁여론 조성 측면에서 결정적인 요소로 변모하고 있음
  - 오늘날의 정보심리전은 디지털 정보 네트워크의 초국가적 인프라를 토대로 작전 공간의 범위가 과거에 비해 광범위하게 확장되어 그 전략적 중요성 또한 증가
    ※ 정보와 내러티브의 신속한 발신, 정보소통 채널에의 접근성, 핵심 작전수행 주체의 다양성 측면에서 과거와 비교할 수 없을 만큼 기능과 영향력이 강화, 확대되는 추세[1)]
  - 나아가 민간과 공공, 전쟁 행위와 범죄, 작전 영역과 비작전 영역의 경계가 불분명해지면서 사이버 공간 속 다양한 행위자가 평시와 전시의 정보심리전을 수행 가능한 환경으로 변모[2)]

- 하이브리드전 시대의 정보심리전이 갖는 파급력은 사이버 공간과 물리적 공간, 전시와 평시를 구분하지 않고 증대
  - 정치적 정당성과 원활한 사회적 기능 유지를 위해 평시의 정보심리전 공격에 대한 대비태세는 전시의 사이버-물리전의 복합적인 국면에서도 유리한 전황 확보를 위한 중요한 영향력을 발휘
  - 타국의 공세적인 프로파간다에 의해 중대한 선거가 영향을 받는 사례를 경험한 서방 진영에서는 최근 허위조작정보 유포활동을 평시 주권에 대한 침해와 민주주의 제도에 대한 공격으로 인식하기 시작
    ※ 2014년 러시아의 크림반도 합병 과정, 소셜미디어 플랫폼을 통해 전개된 서방세계의 주요 선거에 대한 정보심리전의 막대한 영향력을 목도
    ※ 최근 중국 또한, 세계 각지에서 일대일로 사업과 공공외교를 통한 다양한 영향공작을 전개하였으며,[3)] 홍콩과 대만의 선거에 개입한 정황이 분석된 바 있음

1) 송태은, "2022년 러시아-우크라이나 전쟁의 정보심리전: 내러티브·플랫폼·세 모으기 경쟁", 『국제정치논총』, 제62집 3호, (2022), p. 222.
2) Dwayne Winseck, "Information Operations 'Blowback': Communication, Propaganda and Surveillance in the Global War on Terrorism." International Communication Gazette (December 1, 2008).
3) 송태은, "미래전으로서의 정보전·심리전·인지전의 도전과 대응" 미래전과 항공우주산업(미발간 발표자료), (2021).

- 특히, 인공지능과 뇌과학의 발달로 주요국들은 인간의 마음과 사고의 공간인 '인지 영역'을 미래의 전장으로 간주하고 정보심리전을 통해 이를 공략하려는 시도
  - 디지털 초연결 사회(hyper-connected society)의 등장은 일상 공간과 작전 공간, 민간 영역과 공적 영역 및 평시와 전시의 경계를 모호하게 함
  - 이 같은 디지털 전환이 고도화된 사회시스템은 정보심리전이 파괴력을 배가시키는데 최적의 조건을 제공[4)]
  - 나아가 정보전심리전의 부상은 심화되고 있는 미중 패권경쟁이 기술, 경제, 군사영역을 넘어 가치와 이념을 둘러싼 진영 간 체제 우월성의 경쟁구도로까지 이어지는 원동력으로 작용

- 이러한 정보심리전의 진화에 대비해 한국 역시 직면 가능한 새로운 형태의 대결방식과 위협 양상에 대해 전략적 고민이 필요한 상황
  - 특히, 러시아-우크라이나 간 전쟁에 나타난 정보·심리전의 진화 양상은 지정학적 불확실성과 정전 상태의 긴장구도를 상시적으로 안고 있는 한반도 안보환경에도 시사하는 바가 큼
  - 정보심리전의 진화는 전면전 이전 단계에서 선행하는 포괄적 의미의 전술적 도구로 활용 가능성이 높은 만큼, '평시-긴장고조-무력충돌'로 이어지는 전주기적 관점에서의 고찰이 필요
  - 또한, 정보심리전 참여 주체의 확장에 맞추어 민간과 비국가행위자 등 다양한 행위자들의 역량을 결집하고 활용할 수 있는 협력 방식과 소통 채널에 대한 실천 방안을 시급히 고민해야 하는 상황

4) Ibid., p. 2.

Ⅱ. 정보심리전의 개념과 진화 양상

가. 각 연관 개념의 정의와 유래

- 정보전(information warfare)과 심리전(psychological warfare)
  - 정보전은 정보콘텐츠의 흐름을 통제하기 위한 일련의 공격과 방어로서, 정보전과 인지전은 정보콘텐츠가 인간의 뇌로 이어지는 흐름의 선후관계에 따라 구분됨
  - 심리전은 상대방이 특정 사건이나 정보를 관찰 및 인지하고 이를 통해 인식·생각·감정을 형성하는 과정에 개입·조작·통제하여 궁극적으로 상대방의 생각과 감정 및 행동에 영향을 미치려는 시도를 의미
    ※ 러시아의 경우, 안보, 전쟁 등을 다룰 때는 "사이버"라는 용어 대신 "정보전쟁"을 사용하며, 이를 다시 다시 정보-기술전쟁(информационно-технологическая война)과 정보-심리전쟁(информационно-психологическая война)으로 세분화, 전자는 해킹, 랜섬웨어 공격 등과 같은 사이버-기술전을, 후자는 선전, 선동, 프로파간다, 가짜뉴스, 여론조작 등의 사이버-심리전 또는 인지전을 의미함[5]

- 사이버전(cyber warfare)과 전자전(electronic warfare)
  - 사이버전은 국가 및 국가에 준하는 정치집단, 또는 이들을 지지하는 개인이 정치적 의지를 달성하기 위해 상대방의 디지털 인프라에서 IT기술을 기반으로 컴퓨터 시스템을 교란하거나 첩보, 파괴, 선전, 조작 또는 금전 탈취 등을 통해 정상적 활동을 불가능하게 만드는 활동[6]
  - 반면, 전자전(electronic warfare)는 대기 중을 오가는 무형의 전파를 차단, 방해, 개입함으로써 물리적 피해를 야기하려는 시도와 관련된 공격과 방어로, 전파의 물리적 개입·침해·탈취와 관련이 있음

5) М. М. Кучерявый, "Роль информационной составляющей в системе политики обеспечения национальной безопасности Российской Федерации." Известия Российского государственного педагогического университета им. А.И. Герцена. 2014. № 164, pp. 155-163; Сергей Николаевич Черных and Наталья Александровна Зуева, "Информационная война: традиционные методы, новые тенденции." *Context and Reflection: Philosophy of the World and Human Being*, 6(6A) (2017), pp. 191-199.
6) NATO. "Cyberwar: does it exist?" (June 13, 2019); 박동휘, 『사이버전의 모든 것』, (서울: 플래닛 미디어), p. 56.

- 사이버 심리전은 사이버상에서 인간 사용자들의 생각과 정서, 심리에 영향을 미치는 일련의 공격과 그에 대한 방어로, 악성 정보가 무기화
- 특히, 대중과 정책결정자 사이의 정보격차 해소를 왜곡하는 해외 여론공작의 수행을 통해 행위자와 국가의 위협인식 형성을 포함하는 대외정책결정과정의 왜곡을 목표로 함

[그림 1] 사이버 심리전에 의한 대외정책결정 과정의 변동 메커니즘

*출처: 이원진(2022), p. 160을 토대로 재구성.

- 제6의 미래 전장으로서 인지전(cognitive warfare)
  - 인간의 인식을 조작하여 인간의 결심과 행동을 바꾸려는 행위 및 이와 관련된 모든 노력을 포함하는 개념으로, 정보의 소비, 해석, 인식(perception)을 포함하는 정신적 과정을 의미[7]
    ※ 인지 영역은 개인, 집단, 대중들의 상호 연결된 믿음, 가치, 문화 등에 영향을 미치는 정보환경을 활용함으로써 군사적 기동(maneuver)이 완수되는 인식과 이성을 구성
  - 인지전은 기존의 정보전, 선전전과 심리전에서 한층 진화한 개념으로, 기존의 심리전과 프로파간다, 정보전 수준을 뛰어넘어 오늘날 전쟁의 궁극적 전략목표인 '마음과 생각의 장악(win one's hearts and minds)'을 위해 인지조작과 프로파간다, 반응통제(reflexive control), 사회공학 등의 다양한 부문을 포괄하는 복합 활용술(art)이라 할 수 있음[8]
    ※ 인지전이 부상한 배경에는 인간의 정보 습득-의사결정-행동 메커니즘에 대한 광범위한 데이터의 축적뿐만 아니라 인공지능을 통한 분석 역량이 극대화됨으로써 이를 각 분야에 적용, 활용할 수 있게 되었기 때문

7) 윤민우, "우크라이나 전쟁과 사이버 인지전", 2022 하계학술대회, (서울, 한국국제정치학회, 2022년 6월 30일), pp. 57-104.
8) Leonid Savin, "NATO developed new methods of cognitive warfare" Nournews, (November 14, 2021)

- 온·오프라인의 물리적 행동과 정보콘텐츠가 인간의 의식 영역으로 들어가 인간의 뇌에 의해 해석되어지는 과정과 이후의 인간 행동까지가 인지전의 공략 대상이라 할 수 있음
  ※ 정보전(information warfare)과 달리 인지전은 정보콘텐츠 흐름 자체의 통제보다는 인간의 뇌가 수용·해석하는 것과 밀접하게 관련

• 하이브리드전(hybrid warfare)
- 하이브리드전은 키네틱전과 비키네틱전이 융합된 개념으로, 키네틱전은 육·해·공·우주 등 물리적 공간에서 실제 물리적 폭력이 행사되는 전쟁이고, 비케네틱전은 인지전, 정보전, 전자전, 사이버전 등 실제 물리적 폭력이 동반되지 않는 전쟁을 의미

나. 주요 초점 및 범위

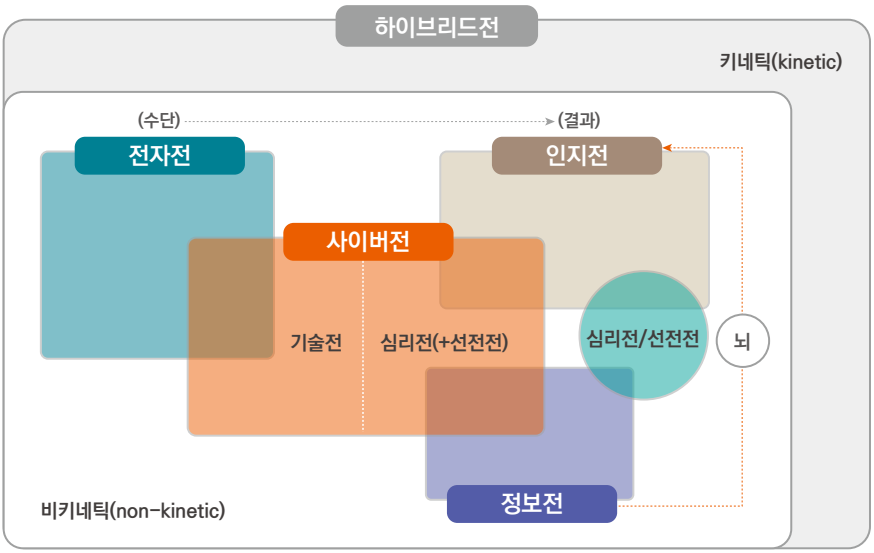
• 정보심리전의 주요 초점 및 범위
- 정보전은 사이버 공간 및 오프라인 공간의 방송, 통신, 신문, 도서, 영화, 공연 등 모든 정보콘텐츠를 대상으로 함
- 심리전은 관찰을 통해 정보를 수용하는 인간 행위자의 인식·생각·감정 자체에 초점을 두는 반면, 선전전(propaganda warfare)은 이들에 영향을 미치는 수단과 과정에 주목[9)]

• 인지전의 주요 초점 및 범위
- 인지전은 최근 주로 사이버 공간에서 전개되는 경향을 보이지만 사이버 공간에 한정되지 않고 오프라인 공간까지를 포함
  ※ 오프라인 공간: 전통적 지상파 및 케이블(종편) 방송, 신문, 저널, 책 등 출판물, 교육기관의 강의, 영화·다큐멘터리, 음악·미술 전시회 및 스포츠 경기대회, 문화센터·시민강좌 등 일반인 대상 강연, 기타 친목회 등을 포함
  ※ 인지전에서는 인간의 뇌가 주요 전장으로 뇌 작용에 대한 신경생리학적 개입과 같은 뇌과학의 무기화, 이민·난민 등 인구구성 변화를 통한 영향력 공작(influence operation), 광범위한 문화전쟁을 포함한 사회공학적(social engineering) 공작까지 포함

9) Bernal et al., "Cognitive Warfare: An Attack on Truth and Thought." (2021), https://www.stratagem.no/cognitive-warfare-and-the-use-of-force/ (검색일: 2022.10.7.)

- 인지전은 국내/해외와 같은 공간적 구분, 전쟁·평화의 시기적 구분이 혼재되어 있으며, 군사/비군사 및 정부/민간의 부문이 융합되어 있음

[그림 2] 정보심리전 및 주요 연관 개념들의 적용 영역 및 관계도



*출처: 윤민우(2022), 김소연 외(2021), Bernal et al.(2021), Helmus, et al.(2018), Lewis(2018)를 토대로 저자 작성.

다. 현대전에서의 정보심리전의 진화 양상

- 정보전과 심리전, 선전전이 복합된 '인지전'으로 진화 중
  - 최근 학계에서는 정보심리전의 새로운 전장으로서 뇌에 주목하며 사람들의 인식(perception)을 바꾸거나 영향을 미치기 위한 인지전의 중요성을 강조하기 시작
  - 특히, 미국, 영국, NATO 등을 중심으로 '인간의 생각(human mind)'메커니즘을 결정하는 인지 부분이 주요 영역이라고 규정하였으며, 육·해·공·우주·사이버에 이어 6번째 전쟁 영역으로 추가[10)]

10) Leonid Savin, "NATO developed new methods of cognitive warfare", (November 14, 2021).

- 주요국들은 하이브리드전 시대의 군사적 효용을 극대화시키기 위한 수단으로서 사이버전략과 정보·심리전 역량을 강조하고 있음
  - 디지털 전환 시대의 사이버공간 확대는 각종 정보 시스템 및 무기체계가 유기적으로 운용되는 사이버 공간의 전략적 가치를 높이고 보호해야할 공격표면의 증가로 이어지는 중[11)]
  - 사이버 공간에서의 활동을 '정보 대립'의 관점에서 국제적 영향력 투사를 위한 전략 투쟁의 형태로 인식[12)]
    ※ 정보 대립(information confrontation)은 사이버전과 심리전의 전통 강국인 러시아의 전략사상가들이 분쟁 국면에서 정보의 역할을 정의하기 위해 사용한 개념으로, 정보통신의 기술적 차원과 인식과 감정의 차원까지 포괄[13)]
  - 물리적 공간과 사이버 공간이 혼재된 현대전의 입체적인 전장에서 전략적·전술적 주도권을 점하기 위해서는 정보 우위의 확보가 필수적이며 이는 작전형태, 임무부대, 민간협력, 지식기반 측면의 협력적 전환을 전제
    ※ 사이버안보전략 및 사이버 군사전략의 적극적 공세적 작전형태로의 전환, 정보수집 분석, 융합, 운용기동력 등 군 현행작전과 연계된 사이버작전, 네트워크 방어에 민간, 언어학자 등 학제간 전문가와 협조 등이 요구됨[14)]
  - 비정규 조직으로의 사이버전의 주체 확장 또한 주요한 양상으로, SNS를 이용한 'IT기반 사이버 의용군(cyber volunteer army)'의 역할이 주목받고 있으며, 사이버공격 뿐만 아니라 허위정보의 차단과 역습, 국제여론 조성 등 현대 정보전과 심리전의 주된 수행자로 참여[15)]
    ※ 기존 사이버 공격의 핵심 표적이 군사전략 지점, 언론·미디어, 인프라 등이었다면 최근에는 오픈소스와 데이터가 광범위하게 유통되는 ICT 공급망이 주요 표적[16)]

11) Molander, Roger C. Andrew Riddile and Peter A. Wilson. "Strategic Information Warfare: A New Face of War." *RAND Report*, (1996).
12) Kurt Wagner, "Why Social Media Acted So Fast After Russia's Ukraine Invasion." Bloomberg(March 3, 2022).
13) 송태은, "러시아-우크라이나 전쟁의 정보·심리전: 평가와 함의"『IFANS 주요국제문제분석』, 제12호, (2022), p. 1.
14) 송태은. "디지털 시대 하이브리드 위협 수단으로서의 사이버 심리전의 목표와 전술,"『세계지역연구논총』 제39집 1호 (2021). pp. 28-64.
15) Yves-Marie Doublet, "Disinformation and electoral campaigns." *Council of Europe*, (2019); Christina Nemr and William Gangware, *Weapons of Mass Distraction: Foreign State- Sponsored Disinformation in the Digital Age*, (Washington D.C.: Park Advisors, 2019).
16) https://www.ciokorea.com/news/238609

• 현대전의 주요 작전수단으로서 정보작전 및 심리작전의 효과
  - '정보심리전(information & psychological warfare)'은 정보의 우위를 통해 여론을 주도하고, 적국의 의사결정 혼선과 저항의지를 무력화시킴으로써 전황을 유리한 국면으로 이끌기 위한 중요한 전쟁 수단[17]
  - '정보작전(information operation)'은 잠재된 적의 올바른 의사결정 시스템을 좌절시키기 위해 다른 종류의 작전과 통합된 방식으로 수행하면서 동시에 아군의 의사결정은 보호하는 정보 관련 군사 활동을 의미
    ※ 정보작전(IO)에는 진짜정보와 허위정보, 조작정보 상황에 대한 오독과 왜곡, 기만, 정보의 과부하를 유발하는 형태로 상대의 올바른 의사결정을 방해하는 전술로, 자원 투입대비 효과가 큰 이점을 가지나, 효과적인 수행을 위해서는 온라인 플랫폼 등 주요 네트워크와 인프라에 대한 접근이 확보되어야 함[18]
  - '심리작전(psychological operation)'은 적의 사기나 전투 및 저항의지를 꺾고 아군 및 동맹의 결의와 사기를 강화시키기 위한 활동을 총칭
    ※ 상대의 허위조작정보 공격이나 선전 프레임에 맞서 자국의 정치적 정당성과 권위, 민주주의 제도와 사회질서를 유지하는데 유용한 수단으로 작용[19]
    ※ 심리작전은 평시와 비상시, 전시 모든 상황에서 이루어질 수 있으며 그 자체로는 비무력적 활동이지만, 폭력적 상황에서는 군사적 파괴력을 배가시켜주는 수단으로 작용할 수 있음

• 어떠한 내러티브를 신속하고 광범위하게 전달할 수 있느냐는 디지털 시대 정보심리전의 승패를 가루는 중요한 변수[20]
  - 이번 러시아-우크라이나 전쟁에서 보듯이 이 같은 정보심리전의 주요 국면에서 동맹 및 우호국과의 공조는 전세 변화에 결정적으로 기여
  - 따라서 전장 정보의 신속한 획득과 발신하는 메시지의 설득력, 메시지를 확산시킬 소통채널의 확보, 작전 수행 주체의 결집 역량이 중요

17) 송태은(2022), p. 1.
18) U.S. Department of Defense. "Information Operations", (November 2014).
19) https://www.rand.org/topics/psychological-warfare.html.
20) 윤정현. "러시아-우크라이나 전쟁 장기화와 정보·심리전의 진화 양상"『이슈브리프』, (2022), 제383호.

Ⅲ. 러시아-우크라이나 전쟁에 나타난 정보심리전의 양상과 의미

가. 전시(戰時) 정보심리전의 파급력

- 2022년 러시아-우크라이나 전쟁은 비무력적 군사활동인 정보심리전이 전쟁 직전 단계, 그리고 전시(wartime)에서 효과적인 공격 수단으로 작용하는 양상을 보여준 사례
  - 러시아의 정보심리전은 게라시모프(Valery Gerasimov)가 주창한 수행단계로 구분되며 '정치적 취약점 공략-대리자 운용-정권약화 및 개입'단계로 구성, 2014년 크림병합 시에는 성공적으로 수행된 바 있음[21)]
    ※ 1단계(정치적 취약점 공격): 러시아 첩보기관인 GRU의 지원을 받는 APT 28, 고스트라이터(Ghostwriter), 세컨더리 인펙션(Secondary Infektion) 등에 의한 언론조작 등 정보작전과 심리전, 그리고 부분적인 사이버 공격을 감행
    ※ 2단계(대리자 운용(proxy sanctum)): 점령지 내의 반군 조직과 소속이 불확실한 '리틀 그린맨' 조직을 활용하여 소요, 테러 및 주요 기반시설을 장악함으로써 우크라이나 내 극도의 사회정치 불안을 유발
    ※ 3단계(정권약화 및 개입): 우크라이나군의 통신 네트워크, 정부기관과 은행의 웹사이트를 차단한 후 대규모 군사훈련 및 침공 실시

[표 1] 2022년 러시아의 우크라이나 침공 전후에 나타난 정보심리전

단계	러시아 정보·심리전의 메시지	의도
2014년~2022년 러시아 우크라이나 침공 전	1) 우크라이나 정부는 미국의 꼭두각시 정부이다. 2) NATO의 동진이 이번 전쟁의 근본적인 원인이다.	침공 명분 합리화, 현지인 저항 억압, 국제사회의 동조 유발 의도

21) 송승종, "러시아 하이브리드 전쟁의 이론과 실제"『한국 군사학 논집』, Vol. 73, No. 1, (2017), pp. 63-94.

2022년 러시아 우크라이나 침공 초기	1) 젤렌스키가 이미 우크라이나에서 탈출했다. 2) 우크라이나는 먼저 러시아를 도발했다.	러시아가 우크라이나를 군사적으로 압도하고 있거나 서방이 우크라이나 지원을 주저하는 인상을 주어 우크라이나의 대항의지 좌절시키려는 의도
2022년 러시아 우크라이나 침공의 본격적인 정보·심리전	1) 네오 나치주의자들이 민간인들을 인간 방패막이로 삼고 있다. 2) 우크라이나가 핵폭탄을 개발 중이라는 증거를 발견했다.	우크라이나 정부 중상모략 및 우크라이나인에 대한 혐오유발 통해 우크라이나인에 대한 학살과 인권유린을 정당화하려는 의도

*출처: 송태은(2022). "러시아-우크라이나 전쟁의 정보심리전: 평가와 함의." IFANS Focus.

- 반면, 전쟁 이전부터 서방-우크라이나 간에는 긴밀한 사이버전 대응 및 정보공유를 위한 공조체계가 가동 중
  - 2014년 러시아의 크림병합 직후부터 우크라이나와 NATO는 국가사이버 위협 대응역량 강화를 위해 NATO와의 긴밀한 공조체계를 구축
    ※ 2014년 NATO-우크라이나 사이버 방어 신탁기금(Cyber Defence Trust Fund)이 설립되고, 2016년 포괄적 지원 패키지가 승인되었으며, 양자 간 사이버 대응협력체로서 컴퓨터 보안 사고 대응팀 (CSIRT1) 설립(2016)
    ※ 또한, 우크라이나 정보원(Security Service of Ukraine)의 사이버 보안 탐지 및 대응역량 강화를 위해 사이버안보 상황 센터와 연구소가 창설되었으며(2018.1), NATO로부터 정보 인프라 보호에 필요한 장비와 소프트웨어, 사이버 대응 훈련 매뉴얼, 교육훈련 방식 등을 지원받음
  - 이번 전쟁의 대표적인 특징은 전황에 대한 민간-비정규 전쟁집단의 정보공유가 전세 변화에 영향을 미치는 중요한 요소로 부상
  - 특히, 우크라이나 침공 과정에서 러시아의 정보심리전은 전세를 유리하게 바꿀만큼 충분히 기여하지 못했으며, 오히려 서방과 우크라이나 측의 담론 프레이밍과 반격 내러티브가 전세에 유리하게 기능
    ※ 서방과 우크라이나는 압도적인 정보역량과 소셜미디어 플랫폼을 바탕으로 유리한 콘텐츠를 지속 확산시킴으로써, 러시아發 정보에 대한 신뢰성 공격과 크렘린을 '무능한 거짓말쟁이' 이미지로 고착화시킴[22]

22) 송태은(2022), p. 2.

- 특히, 글로벌 IT기업과 초국가적 해커 및 민간조직들이 러시아 관영매체의 콘텐츠를 차단하고 우크라이나 관점의 담론 확산을 지원함으로써 국제사회의 광범위한 지지와 군사적 지원을 확보하고 장기간의 항전을 지속할 수 있는 동력 제공
- 즉, 2014년 당시 정보심리전이 러시아 승리의 원동력이었다면, 이번 2022년 침공에서는 △우크라이나에 국제여론전에 패하고, △역으로 우크라이나 국민의 항전의식 또한 고취

나. 정보심리전 행위 주체의 다변화

• 우크라이나 측 비정규 집단·민간의 사이버 공간內 협력·대리전 효과
- 국제 핵티비스트인 어나니머스 그룹과 우크라이나 정부가 SNS로 전 세계에서 모집한 IT 의용군인 IT Army of Ukraine은 크렘린궁과 러시아 정부, 은행의 웹사이트들을 마비시켰으며, 러시아 방송채널을 해킹, 전쟁 반대 영상 송출
  ※ 특히, 전쟁 개시 다음 날 어나니머스 그룹은 러시아 정부에 "사이버 전쟁"을 선포, 러시아의 오일·가스 업체(Aerogas), 에너지 업체(Petrovsky Fort) 등에서 빼돌린 400GB의 이메일을 고발 전문 사이트인 디도시크렛(DDoSecrets)에 공개
  ※ 벨라루스의 반정부 핵티비스트 그룹인 사이버 파르티잔(Cyber Partisans)은 전쟁 발발 전 러시아군의 이동을 방해하기 위해 벨라루스 철도의 데이터베이스를 암호화
- 일론 머스크는 우크라이나 정부의 요청에 위성인터넷 서비스인 스타링크를 제공, 러시아의 지속적인 공격에도 불구하고 우크라이나는 인터넷 서비스를 유지할 수 있었음
  ※ 소형 인공위성 운영 기업인 미국의 맥사테크놀로지(Maxar Technologies Inc.), 플래닛랩스(Planet Labs), 카펠라스페이스(Capella Space) 등은 러시아군 정보 영상을 실시간으로 중계, 가짜뉴스와 프로파간다가 넘쳐나는 심리전에서 우크라이나와 서방이 주도권을 쥘 수 있도록 풍부한 전장 정보를 제공
- 국제 핵티비스트의 자율적인 사이버공격에 상당부분 의존하였으나, 정규 조직 못지않은 이들의 사이버공격 역량을 효과적으로 활용

다. 정보심리전 공격의 진화에 따른 효과적 방어의 중요성 증가
- 수행 목표 측면에서 물리적 충돌시 대규모 충돌과 확전을 야기함에 따라 전시의 판단이 모호한 회색지대에 대한 침투로 혼란을 유도하고 효과적인 정치·군사적 목표를 달성하려 시도

- 고도화되고 있는 정보심리전 환경은 향후에도 국가 뿐만 아니라 국제 배후 조직과 연계한 은밀한 공격행위들이 지속될 것임을 시사
- 공세적인 사이버 심리전 공격에 효과적으로 대응하기 위한 대칭적인 역공세 심리전, 혼란에서 사회적 안정을 신속하게 찾아가는 회복력(resilience) 기반 시스템 구축의 필요성 예상
- 정규전에 대비한 상시전투태세(Fight Tonight) 뿐만 아니라 비물리적 상황에서의 사이버전, 정보심리전의 공세에 즉각적으로 대응하기 위한 정보 자원 공유 등

  ※ 이를 위해 특히 원활한 정보공유체계(소통채널 예비인프라 운용 등)의 강건성 확보, 극단적 위기대응 시나리오 매뉴얼 수립 등이 요구될 것

Ⅳ. 한국적 시사점과 대응 방안

가. 국내 정보심리전 운용의 쟁점

- 현재 국내에서는 사이버 심리전의 기반이 되는 안보 목적의 정보 수집 활용이 제약되어있으며, 기관 간 정보공유와 상호협력의 범위와 절차, 내용 역시 구체성이 취약한 상황
  - 최근의 러시아 우크라이나 전쟁, NATO군의 인지전 작전의 확장 등에 따라 국내에서도 정보심리전 또는 인지전에 대한 관심과 논의가 진행 중이나, 본격적인 전략개념 발전과 실행단계에 이르지는 못한 상황
  - 반면, 러시아, 미국 등은 민간의 대학, 협회, 기업, 싱크탱크, 온라인 커뮤니티, 시민사회단체 등을 전면에 내세우고 이들이 자발적, 주도적으로 임무를 수행하는 형태로 운영 중

    ※ 애국적 핵티비스트, 해커집단, 민간시민사회단체, 민간보안회사 등 민간 행위자들이 직접 임무를 수행하며, 이들과 정부의 관계는 deniability 원칙에 따라 표면적인 식별이 불가

나. 한반도 정보심리전의 위협 전망과 취약점

• 최근 북한에 대한 정보심리전 측면에서의 위협과 취약점
  - 북한은 정보전을 유용한 비대칭무기로 인식하여 사이버전, 전자전, 심리전 등의 능력을 집중적으로 배양해왔으며, 오랜 경색국면이나 위기시 이 같은 비물리적 공격을 적극적으로 감행할 가능성
  - 그간 북한은 평시에도 미사일 발사, 핵실험 뒤 위협적 선전을 통해 우리사회 내부 분열과 무력감 확산을 노린 '와해전략(distuption strategy)'을 토대로 심리적 투쟁을 전개해왔음[23)]
  - 이에 대한 대응책으로 한·미는 북한의 주요 도발시마다 입수한 대북 정보를 실시간으로 상세히 공개하며, 양국의 강고한 공조체계와 정보우위를 갖고 있음을 확인, 압박하는 전략을 구사해왔음
  - 반면, 지난 6월 4일 대륙간탄도미사일(ICBM) 추정 미사일 발사 후부터는 미사일 발사 소식 관련 보도를 의도적으로 생략한 채 '침묵 모드'를 이어가며, '정보 암묵지의 위협'을 새롭게 제기
    ※ 과거에는 미사일 도발 이튿날 관영 매체를 통해 구체적 제원과 김정은 국무위원장의 참관 여부, 대남·대미 메시지까지 '패키지'로 공개하는 것이 관행
  - 즉, 북한은 전술핵 탑재가 가능한 발사체 실험에 이어, 핵 사용 교리까지 바꾸며 큰 틀에서 핵 선제 타격 가능성을 열어둔 상태이나, 정확한 의도와 목표는 오히려 감춤으로써, '침묵의 교란술'을 통해 한미 공조의 무력화와 불안감을 증폭시키는 전략을 구사하고 있음
    ※ 비대칭 핵전력의 과시와 대비되는 한국 정부의 무력함을 유도하는 심리전을 통해 정부에 대한 불신과 한반도 비핵화 의지 및 한미동맹의 결속을 좌절시키려는 의도
  - 이 같은 장기간의 침묵 모드에서 갑작스런 대규모 도발 시, 주체가 불명확하고 치안과 국방의 경계가 모호한 회색지대를 중심으로 물리-심리 간의 쌍방향 공세를 감행할 수 있으며, 대응시간 지연에 따른 피해 확산과 사회적 혼란이 예상됨

• 중국발, 러시아발 사이버·정보심리전 위협 가능성
  - 최근 미국이 주도하는 공급망 재편에 따른 중국 배제, 우크라이나 침공에 대한 러시아 제재 등에 동참하고 있는 한국으로서는 이들과도 불가피한 긴장관계를 갖고 있으며, 은밀한 사이버 공격이나 정보심리전의 공격 보복 위험성을 내재

23) 부형욱, "우크라이나 전쟁으로 본 하이브리드전" 2022 한국국제정치학회 하계학술대회, (서울, 한국국제정치학회 자료집), (2022), p. 146.

다. 정책적 고려사항

- 진화된 정보심리전 위협에 대비하기 위한 국제공조와 소통 강화
  - 정보심리전이 고도화되는 사이버전의 진화 양상은 한반도 환경에도 전시 뿐만 아니라 평시에도 국가 배후 및 해킹조직과의 연계한 허위조작 및 왜곡정보 유포 등의 공격행위들이 지속될 것임을 시사
  - 군사교리 내 정보심리전 개념 확장 재정의 및 적용 임무와 범위를 구체화하고, 특히, 위기상황, 전시의 사회적 혼란을 틈타 난민, 테러 등 민감 이슈에서의 조작정보 등에 효과적으로 대응하기 위한 전략커뮤니케이션 채널이 필요
  - NATO와도 정보심리전에 공조할 수 있는 전략 시나리오 훈련의 촉진, 위협대응 모델을 개발·공유할 필요
  - 특히, 허위조작정보 문제 등 민주주의를 위협하는 행위들에 대한 적극적인 참여를 통해 국제협력 이니셔티브 및 다자주의 공조에 지속적으로 동참함으로써, 보편적인 이슈에 기여할 수 있는 책임있는 국가로의 역할을 수행할 필요
    ※ 한국은 지난 2019년 9월 유엔총회 내 '정보와 민주주의 파트너십(International Partnership for Information and Democracy)'에 동아시아 국가 최초로 서명한 바 있으며, 민주주의와 언론의 자유 증진 및 디지털 정보와 소통 규범 형성을 위한 국제협력에 이미 동참하고 있는 상황[24)]

- 한미 정보자원 우위를 위한 전략적 기반논의 확장
  - 주로 전술적 수준에 머물러 있는 정보협력과 정보심리전 대응 수준을 보다 상위의 전략적 수준 및 실행 기반 구축 측면에서도 논의할 필요
  - 이를 위해서는 우리의 대미 정보 우위를 어느 수준까지 제공할 수 있는지를 세심히 검토하고, 한미 통합국방협의체(KIDD: Korea-U.S. Integrated Defense Dialogue) 등을 통해 정보협력 수준을 논의할 필요
    ※ MIMS-C: AI와 최신 ICT기술을 적용해 기존 한미 군사정보처리 장비의 정보공유·분석능력 향상을 목표로 2024년 12월까지 전력화 계획

24) 송태은(2020), p. 33.

- 정규전에 대비한 상시전투태세(Fight Tonight) 뿐만 아니라 비물리적 상황에서의 사이버전, 정보심리전의 공세에 즉각적으로 대응하기 위한 정보 자원 공유, 활용 준비태세 확립 방안 논의 필요
  ※ 현재 미국은 정보심리전, 인지전에 대한 연합작전 등의 중요성을 인식, 한국에 대중국 및 대북한 정보심리전 대응체계와 공조에 적극적인 상황
  ※ 효과적인 공조를 위해서는 정보심리전·인지전 개념에 대한 이해와 긴밀한 한미동맹을 축으로 대북, 대중국 인지전 핵심 내러티브 개발과 인지전 전략 개발, 작전능력 함양 등, 실제 수행역량 등이 갖춰져야 함

• 민간·비정부 행위자들과의 연구기반·정보협력 확대
  - 향후 정보심리전의 수단은 더욱 발전된 AI의 분석능력과 첨단 정보커뮤니케이션 기술을 토대로 물리전과 맞물려 국가안보에 치명적인 타격을 가할 수 있는 효과적인 수단으로 진화할 것으로 전망됨
  - 전쟁의 수행주체인 군, 이를 뒷받침하는 국민, 나아가 국제사회에 누구의 내러티브를 신속하고 광범위하게 전달할 수 있느냐는 정보심리전의 진화 국면에서 승패를 결정짓는 중요한 변수
  - 고도화된 정보심리전에 대한 신속한 분석·대응 공조가 이루어질 수 있도록 민간·비정부 행위자들의 역량을 활용할 수 있는 협력 채널을 구축
  - 향후 정보심리, 인지전의 핵심 기반이 되는 데이터 분석력과 보안을 위한 '데이터 비식별화', '동형암호(암호화된 상태로 데이터 분석·연산이 가능한 암호)' 등 활용역량 강화를 위한 기반 조성
  - 평시 IT 기업과 정부 간의 사이버 위협 대응 협력을 위한 빈번한 정보교류, 상호지원 및 인력 파견, 공동연구와 국제협력 공동 진출 등이 획기적으로 활성화될 필요가 있음

• 한국적 안보적 특수상황에 부합하는 후속연구의 필요성
  - 한반도 안보상황에서 그간 초점을 두었던 정규전·사이버전의 대응방안 뿐만 아니라 정보심리전, 인지전의 복합적 위협상황의 대비 필요
  - 특히, 실천적 차원에서 한·미간 정보운용성의 개발과 협조는 더욱 중요하며, 포괄적 전략 파트너십에 부합하는 미래전 관점의 정보심리전 및 인지전 대응훈련의 확대 필요
  - 정규전에 대비한 상시전투태세(Fight Tonight) 뿐만 아니라 비물리적 상황에서의 사이버전, 정보심리전의 공세에 즉각적으로 대응하기 위한 정보 자원 공유, 활용 준비태세 확립 방안 연구가 요구됨

참고문헌

김소연·김성표·박범준·정운섭·추헌우·윤정·김진용. 2021. “Cyber electronic Warfare Technologies and Development Directions,” *The Journal of Korean Institute of Electromagnetic Engineering and Science*, 제32권, 제2호, pp. 119-126.

박동휘. 2022.『사이버전의 모든 것』, 서울: 플래닛 미디어.

부형욱. 2022. “우크라이나 전쟁으로 본 하이브리드전” 2022 한국국제정치하계학술대회 (서울, 한국국제정치학회, 2022년 6월 30일), pp. 135-148.

송승종. 2017. “러시아 하이브리드 전쟁의 이론과 실제”『한국 군사학 논집』, Vol. 73, No. 1, (2017), pp. 63-94.

송태은. 2020. “하이브리드 위협에 대한 최근 유럽의 대응,”『IFANS 주요국제문제분석』, 2020-31,

_____. 2021. “디지털 시대 하이브리드 위협 수단으로서의 사이버 심리전의 목표와 전술,”『세계지역연구논총』 제39집 1호.

_____. 2022. “러시아-우크라이나 전쟁의 정보·심리전: 평가와 함의”『IFANS 주요국제문제분석』, 2022년 제12호, (2022년 5월 10일).

_____. 2022. “2022년 러시아-우크라이나 전쟁의 정보심리전: 내러티브·플랫폼·세 모으기 경쟁”, 『국제정치논총』, 제62집 3호.

_____. 2022. “미래전으로서의 정보전·심리전·인지전의 도전과 대응”『미래전과 항공우주산업(미발간 발표자료)』, (2021년 10월 31일).

윤민우. 2022. “우크라이나 전쟁과 사이버 인지전”, 2022 한국국제정치하계학술대회 (서울, 한국국제정치학회, 2022년 6월 30일), pp. 57-104.

윤정현. 2022. “러시아-우크라이나 전쟁 장기화와 정보·심리전의 진화 양상”『이슈브리프』, 제383호.

이수진. 2022. “미래 합동 전장에서의 전력 승수: 공세적 통합 사이버 작전”, 제3차 세종사이버안보포럼, (서울, 세종연구소, 2022년 3월 30일).

이원진. 2022. “사이버 심리전에 의한 대외정책결정과정 변동성의 구조화와 대응 전략 연구”, 2022 한국국제정치하계학술대회 (서울, 한국국제정치학회, 2022년 6월 30일), pp. 157-172.

Bernal et al., 2021. “Cognitive Warfare: An Attack on Truth and Thought.” https://www.stratagem.no/cognitive-warfare-and-the-use-of-force/ (검색일: 2022.10.7.)

Doublet, Yves-Marie. 2019. “Disinformation and electoral campaigns.” *Council of Europe*.

Helmus, Todd C., Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman, 2018. "Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe," RAND, Santa Monica, California, pp. 7-8.

Lewis, James Andrew. 2018. "Cognitive effect and state conflict in cyberspace," *CSIS Report*, September 26, (2018).

Molander, Roger C., Andrew Riddile and Peter A. Wilson. 1996. "Strategic Information Warfare: A New Face of War." *RAND Report*.

NATO. 2019. "Cyberwar: does it exist?" (June 13, 2019).

NATO. 2020. "NATO Standardization Office participates in JMRC-hosted multinational exercise Combined Resolve XIII." (February 17, 2020).

Nemr, Christina and William Gangware. 2019. *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age*, (Washington D.C.: Park Advisors, 2019).

Savin, Leonid. "NATO developed new methods of cognitive warfare", (November 14, 2021).

U.S. Department of Defense. "Information Operations", (November 2014).

Wagner, Kurt 2022. "Why Social Media Acted So Fast After Russia's Ukraine Invasion." *Bloomberg*, (March 3, 2022).

Winseck, Dwayne. 2008. "Information Operations 'Blowback': Communication, Propaganda and Surveillance in the Global War on Terrorism." International Communication Gazette, (December 1, 2008).

Кучерявый, М. М. 2017. "Роль информационной составляющей в системе политики обеспечения национальной безопасности Российской Федерации." Известия Российского государственного педагогического университета им. А.И. Герцена. 2014. № 164, pp. 155-163; Сергей Николаевич Черных and Наталья Александровна Зуева, "Информационная война: традиционные методы, новые тенденции." *Context and Reflection: Philosophy of the World and Human Being*, Vol. 6, No. 6A (2017), pp. 191-199.

https://www.ciokorea.com/news/238609

https://www.rand.org/topics/psychological-warfare.html.

Abstract

Evolution of Information & Psychological Warfare and response strategy

Junghyun Yoon
(Institute for National Security Strategy)

Today, information psychological warfare is a means to lead the public opinion and to lead the battlefield to a favorable phase by neutralizing the enemy's decision-making confusion and resistance will. In particular, the Russian-Ukrainian war in 2022 is an example of how information and psychological warfare, a non-military activity of wartime in an advanced digital information communication environment, acts as an effective means of attack and defense in all-out war. In fact, the Ukrainian discourse framing and counterattack narrative against the Russian attack played a decisive role in securing the initial premises. In addition, it became an opportunity to clearly show the aspect of digital platform being weaponized in cyberspace information and psychological warfare in earnest.

The purpose of this study is to examine various concepts related to information psychological warfare, to predict future prospects and threats, and to draw implications for the Korean situation. The evolution of information psychological warfare and cognitive warfare will pose a new challenge to the security environment on the Korean peninsula, and cooperation with allies and friendly countries is an indispensable factor in maintaining the

Abstract

political legitimacy and authority of the government, democratic institutions and social order. Therefore, it is necessary to consider ways to cooperate with various actors on a multi-layered level, such as strengthening international communication to prepare for evolving information psychological warfare threats, expanding discussions for superiority of information resources between Korea and the US, and expanding research base and information cooperation with private and non-government actors.

Keywords: information warfare, psychological warfare, cognitive warfare, Russo-Ukraine war, hybrid warfare

INSS 전략보고

November 2022. No.196

※ 본지에 실린 내용은 집필자 개인의 견해이며, 국가안보전략연구원의 공식입장이 아닙니다.

국가안보전략연구원

06295 서울시 강남구 언주로 120 인스토피아 빌딩
02-6191-1000 02-6191-1111 www.inss.re.kr