https://doi.org/10.21186/IPR.2024.9.4.065

러시아의 하이브리드전을 통해 본 한국의 사이버전 발전방안

이세훈*, 이승훈**

육군대학*, 동아대학교 산업경영공학과 교수**

Developing Cyber Warfare of South Korea through Russia's Hybrid Warfare case

Se Hoon Lee*, Seung hoon Lee**

Republic of Korea Army College*,

Professor, Department of Industrial Management Engineering, Dong-A University**

요 약 최근 국제 분쟁은 무력전과 함께 사이버전, 여론전, 심리전 등이 결합된 하이브리드전 양상으로 전개되고 있다. 하이브리드전은 전시와 평시의 구분 없이 모든 전력을 동원하고 다양한 유형의 전략을 혼합하여 상대 국가의 취약점을 공략하는 예측 불가능한 전쟁 수행방식이다. 이 중 사이버전은 물리적 군사 공격에 앞서 사회 혼란을 조장하고, 적의 전의를 약화시키며, 정치적·군사적 목표를 달성하기 위한 핵심 수단으로 활용되고 있다. 본 논문은 하이브리드전의 주요 수단인 사이버전을 통해 러시아가 물리적 전쟁을 수행하기 전후에 보였던 공격 양상과 침공 사례를 분석함으로써, 유사시 북한의 사이버 공격 양상을 예측하고 한반도 안보 상황에 적합한 사이버전 발전 방안을 모색하는 것을 목적으로 한다. 이를 위해 2007년 에스토니아 사이버 공격, 2008년 조지아 침공, 2014년 크림반도 합병, 2022년 우크라이나 전쟁 등에서 러시아의 사이버전이 실제 전쟁에서 어떻게 수행되었는지 그 수단, 과정, 양상을 비교·검토하여 시사점을 도출하였다. 또한, 북한과 대치하고 있는 우리나라의 현실에 맞는 사이버전 발전방안으로는 미국과의 협력을 통한 글로벌 사이버 방호체계 구축, SNS를 통한 여론전 및 심리전에 대한 대응, 그리고 사이버 전자전에 대비한 국가 차원의 민·관·군 협력 강화 방안을 제시하였다.

주제어 : 하이브리드전, 차세대전, 사이버전, 사이버 공격, 러시아-우크라이나 전쟁

Abstract Recent international conflicts have evolved into hybrid warfare, combining conventional military operations with cyber warfare, public opinion manipulation, and psychological warfare. Hybrid warfare involves the unpredictable use of various forces and strategies that blur the lines between war and peace, targeting the vulnerabilities of adversary nations. Among these, cyber warfare is a key tool used to incite social chaos, weaken the enemy's resolve, and achieve political and military objectives before physical military attacks take place. This paper aims to analyze the cyber warfare tactics employed by Russia before and after its physical military engagements, focusing on key cases such as the 2007 cyberattack on Estonia, the 2008 invasion of Georgia, the 2014 annexation of Crimea, and the 2022 war in Ukraine. By examining the methods, processes, and patterns of Russia's cyber operations in these conflicts, the study seeks to predict potential cyberattack scenarios by North Korea and explore cyber warfare development strategies suitable for the security context of the Korean Peninsula. Based on these analyses, the paper suggests strategies tailored to South Korea's current situation, which involves a continuous standoff with North Korea. Proposed measures include establishing a global cyber defense cooperation framework with the United States, countering public opinion and psychological warfare through social media, and enhancing national-level civil-military cooperation to prepare for cyber-electronic warfare.

Key Words : Hybrid Warfare, New Generation Warfare, Cyber Warfare, Cyber Attack, Russia-Ukraine War

Received 23 Sep 2024, Revised 02 Oct 2024
Accepted 11 Oct 2024
Corresponding Author: Seung hoon Lee
(Dong-A University)
Email: seungh@dau.ac.kr
ISSN: 2466-1139(Print)
ISSN: 2714-013X(Online)

1. 서론

하이브리드전(Hybrid Warfare)은 국가 또는 정치 집단이 재래식 전쟁을 수행하는 능력뿐 아니라 비정규전, 테러리즘, 범죄행위 등의 다양한 수단을 동원하는 방식을 의미한다. 러시아는 2014년 크림반도 합병시 심리전, 정보전, 사이버전 등 다양한 비군사적 방법을 동원하여 정치적 목적을 달성하였으며, 특수부대와 비정규부대 등 다양한 수단들을 활용하여 크림반도 합병이 기정사실화 될 때까지 은밀한 군사작전을 실시하였다. 이처럼, 공식적인 군사개입을 선언하지 않고 다양한 전쟁 수단들이 혼합하여 활용되는 변형적인 러시아의 전쟁 수행방식을 서방에서는 하이브리드 전쟁으로 인식하기 시작하였다.

최근, 우크라이나가 친서방 정책에 따라 북대서양조약기구(NATO : North Atlantic Treaty Organization) 가입을 추진하자 러시아는 이에 반발하여 우크라이나 국경 인근에 최대 15만 명의 군병력을 배치하였으며, 각종 훈련을 가장하여 침공훈련을 실시하였다[1]. 미국을 중심으로 한 NATO 주요 국가들은 전쟁을 준비하는 러시아의 군사적 움직임에 대응하여 우크라이나에 직·간접적인 군사 및 비군사적 지원활동을 실시하였으며, 이러한 상황에서 러시아는 NATO 가입저지와 돈바스 지역의 친러세력 보호라는 '특별군사작전'을 명분으로 2022년 2월 24일 우크라이나 전역에 공격을 개시하였다[2].

러시아-우크라이나 전쟁은 사이버-물리 시스템(CPS : Cyber-Physical Systems)의 융합으로 가속화된 4차 산업혁명 이후 유럽에서 발발한 대규모 전쟁이라는 측면과 함께 재래식 무기에 의한 교전, 드론에 의한 폭격, 경제전, 선전전 등 네트워크와 무인기, 그리고 전통적 군사활동이 결합된 새로운 전쟁의 양상을 보이고 있다[3]. 특히, 전 세계 정보통신기술(ICT : Information and Communications Technology) 발달에 따른 상호의존성 심화는 사이버 공격의 취약성을 증가시켰으며, 사이버 전력을 활용한 사이버전(Cyber Warfare)은 전 세계 이목을 집중시켰다[3]. 이는 사이버 공간을 정보 대립 측면에서 영향력 투사를 위한 전장 및 군사 목적을 달성할 수 있는 영역으로 인식하였으며[4], 이를 선점하는 것이 결국 전쟁의 승기를 잡는 중요한 분기점이 되었다. 이러한 사이버 전장은 사이버 무기인 해킹과 바이러스 도구를 이용한 공격 및 방어가 동시에 존재하는 재래식 대칭 개념을 포함하고 있으며, 공격의 대상이 적 지휘통제수단, 군사시설 및 정보기반체계, 더 넓게는 국가기관과 시설 등 모든 사이버 기반의 인프라를 망라하고 있다[5].

러시아는 우크라이나 침공 이전인 2022년 2월 15일부터 소속 부대들이 훈련을 마치고 원소속 부대로 복귀를 시작할 것이라 밝혔다[6]. 또한, 러시아 매체들은 2022년 2월 17일과 18일 돈바스 지역에서 우크라이나가 먼저 포격하였다고 허위 보도 하는 등 여론전을 펼쳤으며[7], 이러한 가짜 깃발 작전(False Flag Operation)과 함께 러시아는 15일과 23일 우크라이나의 국방부, 주요 부대, 대형 상업은행 등을 대상으로 대규모 분산 서비스거부(DDoS : Distributed Denial of Service) 공격을 실시하였다[8].

러시아는 2020년부터 2021년까지 러시아군 장비 70%의 현대화를 목표로 하는 10개년 국가무장계획(SAP : State Armament Programme)에 따라 각 군 무기의 성능 개량 및 신형 교체, 항공 및 우주 방어, 사이버, 핵 잠수함, 극초음속 미사일 등의 현대화를 추진하였으며[1], '2020 러시아군 정보통신기술 발전 구상', '차세대 전쟁(New-Generation Warfare)' 전략에 따라 하이브리드전 역량을 강화하는 등 지속적인 전투력 향상과 함께 사이버전 능력을 증강해 나갔다[1,9,10].

한편, 2024년 6월 19일 러시아 푸틴 대통령과 북한 김정은 위원장이 평양에서 정상회담을 통해 북러동맹의 복원을 선언하였다. 이를 통해, 러시아와 북한은 강력한 군사동맹을 천명하였으며, 군사 분야뿐 아니라 사이버 공간에서의 협력 또한 강화할 것으로 보인다[11]. 북한은 우리나라를 대상으로 핵심 정보 및 국방 관련 기술 탈취, 자금조달 등을 목적으로 2009년 7월 7일 디도스 공격, 2013년 3월 20일 및 6월 25일 언론사·금융기관 사이버테러, 2016년 주요 정부 인사 스마트폰 해킹, 2019년 11월 가상화폐거래소 해킹을 지속적으로 시도해왔다[12,13].

윤정현(2022)은 최근 미국은 자국이 주도하는 공급망 재편에 중국을 배제하였으며, 우크라이나 침공에 대한 러시아 제재에 동참하고 있는 한국으로서는 이들과 불가피한 긴장관계를 유지하고 있어 은밀한 사이버 공격 또는 정보·심리전의 보복 위험성을 내재하고 있다고 보았다. 특히, 현재 한반도 환경에서는 전시뿐 아니라, 평시에도 해킹조직과 연계된 정보 조작 및 왜곡정보 유포의 사이버 공격이 지속될 것으로 보고, 다자주의 공조에 기반한 위협대응 모델 공유 등 보편적인 이슈에 기여 가능한

책임있는 역할이 중요하다고 보았다[4].

문계성 등(2023)은 북한은 평시 우리가 대북정책을 압박하거나, 남한 내부 사회혼란시 선제적으로 사이버전을 전개하는 동시에 일부 지역에 침투 또는 대량포격을 실시할 것으로 보았다. 그러나, 우리나라는 이러한 북한의 비정규전 능력을 국방백서에 항상 높은 수준으로 분석하면서도 국방부 이외 관련 부처 및 시·군별 실질적인 대비태세는 미흡하다고 보았다[14].

이승열(2023)은 북한의 사이버 능력은 대표적인 비대칭 수단으로 2016년 4차 핵실험 이후 해외 금융기관 해킹 및 랜섬웨어(Ransomware) 공격, 가상자산 탈취 등 자금 확보에 집중하고 있다고 보았다. 그러나, 북한의 사이버 위협 대비 우리 정부의 적절한 제재 및 대응능력 측면에서 문제점이 식별되고 있어 관련 법 제정과 함께 제재 능력, 정보공유, 국제공조의 보완이 필요하다고 보았다[13].

이에, 북한의 비대칭 전력 위협과 함께 중국과 러시아의 군사적·비군사적 위협 가능성에 직면해 있는 현실에서 하이브리드전의 주요 수단인 사이버전을 통해 러시아가 물리적 전쟁을 개시하기 전·후 보였던 공격 양상 및 침공 사례를 분석함으로써, 유사시 북한의 사이버전 양상을 예측하고 한반도 안보 상황에 적합한 사이버전 발전방안을 모색하는데 그 목적이 있다.

이를 위해, 하이브리드전을 사이버전, 여론전, 심리전, 기만전 등을 포함한 개념으로 보았으며[15], 하이브리드전의 가장 중요한 수단을 사이버전으로 보았다. 따라서 최근 러시아가 보여준 하이브리드전을 사이버전으로 범위를 한정하였으며, 관련 사례인 2007년 에스토니아 사이버 공격, 2008년 조지아 침공, 2014년 크림반도 합병, 2022년 우크라이나 전쟁의 주요 배경과 수단, 경과 등을 비교·검토하여 시사점을 도출하였다. 이는 실제 러시아가 무력 침공 이전부터 선제공격의 가장 주요한 수단으로 사이버 공격을 수행한다는 '차세대전(New Generation Warfare)'의 논리에 근거하여 사이버전이 실제 전쟁에서 어떻게 수행되었는지 정책기관의 자료, 관련 기사, 논문 등 각종 문헌을 참고하여 전쟁의 양상을 분석하였으며, 이를 통해 앞으로의 전쟁이 어떠한 방향으로 전개될 것인가에 대한 함의와 함께 대응방안을 모색하였다[16,17].

따라서, 본 연구에서는 사이버-물리 시스템의 융합으로 급변하는 안보·기술 환경변화에 적절히 대응하고, 비대칭 전력의 핵심 수단인 하이브리드전 위협에 효과적으로 대비하기 위해 러시아의 대표적인 사이버전 수행사례를 통해 북한 및 주변 잠재적 사이버 위협에 대한 한국의 사이버전 발전방안을 제시하고자 한다.

2. 선행연구

김경순(2018)은 2014년 러시아는 우크라이나 크림반도를 합병하고 우크라이나 동부 돈바스 지역의 분리·독립을 지원하면서 다양한 비군사적인 정보전, 선전전, 심리전 등을 통해 정치적 목적을 달성하는 모습을 보였으며, 이는 상대적 약점을 노출하지 않고 적을 혼란시키는 간접적이며 난해한 전술인 하이브리드전을 구사하였다고 보았다. 특히, 러시아는 공식적인 군사개입을 선언하지 않고 은폐성을 유지한 채 전쟁과 평화의 중간인 회색지대(Gray Zone) 전략을 통해 혼란과 불확실성을 증가시키는 동시에 첩보와 사이버 공격을 통해 언론과 미디어를 성공적으로 장악하였다고 보았다[18].

홍규덕(2022)은 러시아는 하이브리드전, 회색지대 전략이라는 비대칭적 수단을 통해 에스토니아 사이버 공격, 조지아 전쟁, 시리아 내전 개입 등 자국의 영향력 유지 및 통제력 강화를 위해 오랜 기간 사이버전, 심리전, 영향력 공작 등을 통해 정치적·전략적 목표를 달성하였다고 보았다. 이에, 러시아, 중국, 북한, 이란을 중심으로 한 군사력과 비군사적 조치에 대응하기 위해서는 국제협력 강화는 물론 민·군 관계의 긴밀한 협조체계 구축을 통한 사이버 방호 및 공격 능력 향상이 필요하다고 보았다[19].

박종일(2023)은 우크라이나 전쟁에서 러시아의 주요 사이버 공격을 파괴형·마비형 공격, 사이버 심리전 및 정보수집 공격 등으로 보았으며, 특히, 전면전에서 군사작전과 사이버전의 통합, 민간기업 및 민간인들의 사이버전 참여, 스마트폰의 사이버전 무기화 확대 등의 추세에 비추어 미래 사이버전은 더욱 복잡해지고 다양해질 것으로 보았다. 이에, 우리 군은 미래 군사작전과 연계한 사이버전 수행능력 향상 및 사이버 복원력 구축, 전자기 펄스(EMP : ElectroMagenetic Pulse) 공격에 대비한 방호역량이 중요하다고 보았다[8].

송운수(2023)는 우크라이나 전쟁은 SNS(Social Network Service)를 통한 허위정보 조작 및 심리전 등 새로운 양상의 정보전이 대두되었으며, 특히 사이버 수

단에 의한 군사정보 수집 및 공유, 민간기업의 참여 및 민간위성을 통한 군사정보의 확대는 기존 군사 정보전의 개념보다 확장된 하이브리드-정보전 양상으로 보았다. 또한, 북한이 전면전이 아닌 하이브리드전 성격의 애매모호한 전쟁을 전개할 수 있어 우리나라는 한·미 사이버 동맹 및 사이버 국제안보 협력을 강화하는 동시에 하이브리드전 관련 교리발전이 필요하다고 주장하였다[8].

이처럼, 러시아의 하이브리드전에 관한 연구는 다수 진행되고 있으며, 하이브리드전 시각에서 러시아의 기존 사이버전 수행양상 및 최근 우크라이나 전쟁의 사이버 공격 양상에 관한 연구 또한 다수 진행되어 왔다. 그러나, 2000년대 이후 러시아의 사이버 공격의 발전양상 및 시대별 변화에 초점을 두고 연구를 수행한 사례는 미비하였으며, 주로 다양한 수단을 고려한 복합전 양상에 주안을 두고 연구를 진행하여 왔다. 이에, 러시아가 그동안 사용하였던 사이버 공간에서의 침투 방법 및 수단, 고도화된 기술과 연계한 사이버 공격 양상의 변화 등을 시대별 사례를 중심으로 구체적인 분석이 필요하다고 보았다.

<표 1> 러시아의 하이브리드전에 관한 선행연구

구 분	세 부 내 용
김경순 (2019)	· 사이버 공격을 통한 정보전 및 심리전 등 전쟁의 직접적 책임을 회피하는 전략 구사
홍규덕 (2022)	· 회색지대 전략을 통한 군사력과 경제·정치·정보 또는 기타 비군사적 조치의 통합
박종일 (2023)	· 군사작전과 연계한 파괴형 공격, 마비형 공격, 심리전 등 물리적 전쟁수단과 통합된 사이버전 수행
송운수 (2023)	· SNS를 통한 정보 조작, 심리전, 민간기업 참여 등 다양한 군사·비군사적 방식 전개

3. 러시아의 하이브리드전

하이브리드전은 학술적으로 개념이 정립된 것이 아닌 현상적인 전쟁을 규정하는 용어로써, '모호전(Ambiguous Warfare)', '비선형전(Non-Linear Warfare)', '차세대전(New Generation Warfare)' 등 다양한 명칭으로 불린다[18,20]. 러시아에서는 하이브리드전이란 용어를 사용하지 않고 비선형전 또는 차세대전이라는 명칭으로 새로운 환경과 방식을 정리하고 있으며[21], 최근 미군의 연구자료들을 살펴보면, '러시아 신세대전(RNGW : Russian New Generation Warfare)'으로 명명하고 있다[22].

이처럼, 서방의 하이브리드전에 대한 논리적 전개와 더불어 러시아 역시 현대전의 상황 변화와 새로운 전쟁 양상의 출현에 대해 지속적으로 논의되었으며, 러시아의 총참모장인 게라시모프에 의해 '게라시모프 독트린(Gerasimov Doctrine)'으로 교리화되었다. 그는 2013년 1월 군사과학아카데미 연설에서 현대 군사위협의 특징, 복합적 안보환경, 전투 성격 및 군사력 사용 수단·방식의 변화에 대한 제기와 함께 새로운 정보 기술은 군대와 통제기관 사이에 시간적·공간적·정보적 격차를 크게 줄일 수 있다고 보았다[23]. 2016년에는 현대전쟁에서 정치·경제·정보의 복잡한 배열을 적용하는 것이 중요하다고 역설하였을 뿐 아니라, 군사적 수단의 강력한 뒷받침으로 만들어진 비군사적 수단을 하이브리드 전쟁이라고 정의하였다[23]. 2017년에는 하이브리드전이 평화나 전쟁으로 명확히 분류되지 않는 모호한 회색지대 안에서 수행된다는 이유만으로 기존 전쟁과의 차별성을 강조하였으며, 특히 비군사적인 전쟁은 기술발전을 통해 강력해짐은 물론 매우 위험한 수단임을 주장하였다[18,23].

이러한 게라시모프 독트린은 러시아의 하이브리드 전쟁을 수행하기 위한 군사전략의 변화를 가져왔으며, 이는 전쟁에서 군사력 사용과 더불어 정치·경제·외교 및 다른 비군사적 방식을 활용하여 서방군대의 의사결정을 교란하고 지연하면서 유리한 상황으로 국면을 전환시키는 신개념의 전략과 전술로 발전하였다[8,17,18].

국가안보전략연구원(2022), 이형동 등(2022), 이용석 등(2022)의 연구에 따르면, 2000년대 이후 러시아가 무력전쟁이나 유사한 분쟁에서 사용하였던 사이버 공격의 주요 사례를 에스토니아, 조지아, 크림반도 침공으로 선정하여 분석하였으며, 이를 바탕으로 최근 러시아-우크라이나 전쟁에서 선보인 대규모 사이버 공격과 함께 현대의 전쟁 수행양상을 전쟁의 경과 및 다양한 공격의 수단·방법을 중심으로 살펴보고자 한다.

3.1 에스토니아 사이버 공격

2007년 4월 27일 에스토니아 정부는 제2차 세계대전을 기념하는 소련군 병사의 동상을 수도 탈린에서 외곽 공동묘지로 이전하는 것을 추진하였다. 이 동상은 에스토니아가 러시아에 지배당했다는 불명예의 상징이었으며, 소련의 그림자를 지우는 것을 국가적 목표로 삼았던 정부와 의회는 2007년 3월「소련 상징물 철거법안」을

통과시켰다[17]. 그러나, 에스토니아의 러시아계 주민들은 동상 이전을 격렬히 반대하였으며, 국립도서관에 집결하여 대규모 시위를 벌였다[24].

러시아는 이에 대한 보복으로 에스토니아 정부 및 관계기관, 정당, 공공기관, 대중매체 등의 웹사이트에 약 3주간 대규모 디도스 공격을 감행하였으며, 메일 폭탄 공격 및 논리폭탄과 함께 전자기 펄스 계열의 공격이 병행되는 등 에스토니아의 금융은 마비되고 은행 피해만 100만 달러를 넘겼다[17]. 당시 러시아 해커집단의 이러한 공격은 에스토니아 국가의 기능 대부분을 마비시켰을 뿐 아니라, 공공 및 민간 영역 모두를 공격 대상으로 삼았다는 점에서 광범위한 영역에서 다양한 방법으로 치명적인 피해를 주었다[24]. 이러한 사이버 공격은 22일간 계속되었으며, 에스토니아 주요 58개 사이트의 운영이 중단되는 등 사이버의 침해 코드가 해커의 영역에서 국가 무기체계의 영역으로 전이되는 계기가 되었다[17].

3.2 조지아 침공

2008년 8월 베이징 올림픽 열리던 기간 조지아와 조지아 내 친러 성향의 남오세티야 자치공화국의 분리주의 세력간 무력 충돌이 발생하였다[12]. 이어서 조지아가 반군에 대한 공격을 감행하자 러시아는 8월 8일 남오세티야 소재 러시아인 및 평화유지군 보호를 목적으로 국경에 진입하였으며, '평화강요작전'이라는 명목하 전쟁을 개시하였다[25]. 러시아군은 남오세티야에 전차 등을 동원한 지상부대와 해·공군 병력을 총동원하여 공세를 펼쳤으며, 조지아군을 일시에 제압하고 남오세티야 수도 츠힌빌리에서 조지아군을 축출하는데 성공하였다. 이에, 러시아군은 조지아 수도 트빌리시까지 진격하였으며, 국제사회의 중재로 8월 12일 러시아의 군사행동이 공식적으로 중단되고 8월 16일 종전협정이 체결되었다[12].

물리적인 군사 충돌이 발생하기 전인 7월 19일 조지아 대통령실의 웹사이트는 디도스 공격을 받아 인터넷 포털과 언론이 마비되었으며, 더불어 러시아는 악성 바이러스 공격을 통해 조지아의 외교부, 내무부, 국방부 등 국가의 중추기관을 무력화 시켰다. 조지아 내 인터넷과 언론이 마비되면서 국민들 사이에 극도의 공포감이 확산되었으며, 이와 함께 조지아 측의 의견을 외부 세계에 표출하여 서방의 지원을 요청하는 것 또한 실패하였다[26]. 결국 러시아는 전쟁 초기부터 정보를 차단하고 선전전에 우위를 점하는 한편 러시아 내부에서는 조지아군의 포격으로 민간인 및 러시아 평화유지군 약 1,000명이 희생되었다고 보도하는 등 언론전, 심리전 등을 통해 조지아 침공에 대한 러시아의 개입을 합리화하는데 유리한 입장을 선점하였다. 이처럼, 러시아는 조지아 침공시 정부 사이트를 선제공격하여 국가기능을 일시 무능화시킨 상태에서 물리력을 동원하는 방법으로 군사적, 정치적, 외교적 효과를 거두었다[12].

3.3 크림반도 합병

2013년 11월 21일 친러 성향의 우크라이나 대통령 야누코비치가 약속했던 유럽연합(EU : European Union)과의 협정 체결을 보류하고 러시아와 협력할 것을 선언하자 친서방 야당과 대중들이 우크라이나 수도 마이단 광장을 중심으로 대규모 반정부 시위를 시작하였다[25]. 결국, 2014년 2월 말 시위대가 승리하고 우크라이나 대통령은 러시아로 피신하면서 우크라이나에는 친서방 과도 정부가 들어섰다. 이에, 러시아는 크림반도의 주민투표를 보장하기 위해 우크라이나군을 봉쇄하였으며, 서방을 비롯한 해외 정보기관에 자국의 의도를 노출시키지 않고 지상군과 해군 병력을 비밀리에 증강시켰다[25]. 이와 함께, 2월 26일과 27일 양일간 장갑차로 증강된 보병과 해병대, 공수부대, 특공부대를 동시다발적으로 운용하여 크림반도를 장악하였다[27]. 2월 28일에는 친러 무장세력이 정부와 의회, 주요 공항을 점령하였으며, 러시아는 공식적인 군사개입을 선언하지 않고 은밀한 기습작전으로 큰 저항없이 4월 2일 크림반도를 합병하였다[27].

특히, 러시아의 공수부대와 특공부대는 소속, 계급 등을 감추고 사전에 잠입하여 크림반도 주민에 대한 선전 및 선동전을 실시하였으며, 무선신호를 엄격히 통제하여 NATO의 추적을 피할 수 있었다. 또한, 러시아의 특수부대는 초기에 중요 인프라를 접수하여 우크라이나 주요 기지를 봉쇄하고 통신 및 지원체계를 차단하였으며, 더불어 우크라이나군이 저항하지 않도록 사전에 설득하는 등 정치인, 유력인, 언론인들까지 포섭하였다[18]. 무력침공 이전에는 디도스 공격을 통해 우크라이나의 통신 네트워크와 정부 웹사이트를 마비시켰으며, 러시아에 기반을 둔 해커집단은 우크라이나 중서부 지역의 사회기반시설에 대규모 정전을 유발하는 사이버 공격을 가하였다[26]. 이처럼, 러시아는 크림반도를 합병하는 과정에서 정

치전, 심리전, 여론전, 정보전, 사이버전, 특수부대 투입 등 비군사적인 수단과 비정규군을 활용하여 물리적 전쟁 유리하게 이끌었다.

3.4 우크라이나 전쟁

우크라이나를 침공하기 위한 러시아의 직접적인 움직임은 2021년부터 시작되었다[16]. 러시아군은 우크라이나 국경 지역으로 군사력을 이동시켰으며, 4월에는 병력 10만 명 이상과 40척 이상의 전함을 크림반도 지역으로 보내 대규모 군사훈련을 실시하였다. 이는 우크라이나의 NATO 가입 반대, 서방과 NATO의 동유럽 내에서 군사 활동 중지, 구소련 국가의 NATO 가입 금지, 러시아에 대한 법적인 안전보장 등을 요구한 것이었다[16]. 러시아는 '특별군사작전'을 선포하고 2022년 2월 24일 새벽 지상과 해상은 물론 공중에서 우크라이나 주요 도시 및 군사적 표적에 대한 대규모 미사일 공격을 시작하였다[8]. 군사적 목표는 흑해와 수도 키이우를 연결하는 운하 통로인 드니프로강 하구까지 완전 장악하여 키이우를 함락시키고 친러 괴뢰 정부를 수립하는 것이었다[1,19]. 이를 위해 국경선에 집결중이던 전차, 장갑차, 포병, 방공, 공병 등으로 구성된 120개 대대전술단(BGT : Battalion Tactical Group) 10만 명을 일시에 투입하는 전면적인 침공을 실시하였다[19].

전쟁 직전 러시아는 우크라이나 정부와 군, 은행 웹사이트를 표적으로 수차례 디도스 공격을 실시하였으며, 2월 15일 러시아는 우크라이나 국방부, 문화부, 외교부 웹사이트와 은행 2곳에 대한 접속을 중단시켰다[8]. 2월 23일에는 파괴형 소프트웨어 '폭스블레이드(Foxblade)'를 통해 우크라이나 전역의 19개 정부 및 주요기반시설을 공격하는 등 데이터 삭제를 시도하였다[3]. 이를 위해 러시아는 2021년 3월부터 우크라이나 에너지 및 통신 네트워크에 대한 사전 정보수집을 실시하였으며, 아울러 미국과 우크라이나를 지지하는 국가들을 대상으로도 정보수집 활동을 수행하였다[3,8]. 전쟁 초기 러시아는 미국 위성시스템 비아샛(Viasat)을 교란하고 독일의 5,800개의 풍력 터빈을 마비시켰으며, 유럽 전역에 30,000개 이상의 인터넷 연결을 일시적으로 중단시켰다[8]. 또한, 러시아 군부와 연관된 해커들이 폴란드와 우크라이나의 운송 및 물류 기업들에 랜섬웨어 공격을 가하는 등 우크라이나에 인도적 또는 군사적 지원 공급을 차단하기 위한 위협을 증폭시켰다[28]. 이처럼 러시아는 우크라이나에 대한 유럽과 미국의 군사 지원 및 정보공유, 기타 지원활동 등을 약화시켜 국가 간 갈등을 유발하고 우크라이나의 군대와 국민의 저항의지를 말살하기 위해 전쟁 개시 전부터 사이버전을 적극 활용하였다[3]. 2022년 3월 23일 우크라이나의 주요 기관은 PC 내 모든 주요 정보 및 부팅, 시스템 구성에 필요한 데이터를 한순간에 삭제시키는 더블제로(Double Zero)라는 시스템 파괴형 멀웨어(Malware) 공격을 받았으며[8], 2022년 3월 29일에는 우크라이나의 인터넷 제공 기업이 대규모 디도스 공격을 받아 우크라이나 전역에 인터넷이 중단되기도 하였다. 한편, 지상공격과 동시에 러시아의 해킹집단은 우크라이나 군대와 정부기관과 관련된 정보를 다크웹 및 특수 엑세스 소스에서 판매하기 시작하였으며, 페이스북(Facebook), 트위터(Twitter) 등을 통해 가짜뉴스를 퍼트리는 등 대규모 공세 이외 심리전, 여론전 등 가능한 모든 수단을 동원하였다[17]. 이처럼 러시아는 사이버 공격을 통해 주요기반시설과 전쟁수행체제를 마비시켜 이어지는 화력타격의 효과를 극대화할 뿐 아니라, 우크라이나 국민과 군을 분열시키고 정부의 리더십을 파괴하기 위한 수단으로 전방위적 사이버 공격과 함께 적극적인 심리전 및 여론전을 병행하고 있다[17].

4. 분석 및 시사점

2007년 에스토니아 정부 및 관계기관, 대중매체, 공공기관, 은행 등에 가해진 대규모 디도스 공격은 타 국가를 대상으로 민간 해커집단이 사이버 공격을 벌인 최초의 사례로 이를 통해, 서방 국가들은 사이버 피해에 대응하기 위한 국제법 제정 및 사이버전 교리연구를 본격화하였으며, 기존 해커의 영역에서 국가 무기체계의 영역으로 사이버 침해 코드가 전이되는 계기가 되었다[17,25]. 2008년 조지아 침공은 정규군 무기를 이용한 군사적 공격과 더불어 사이버 공격이 결합된 사례로 러시아는 지·해·공 작전과 함께 광범위한 디도스 공격을 통해 조지아의 정부·금융기관·언론 웹사이트를 마비시켰다[17,25]. 2014년 크림반도 합병시에는 국제적 비난을 회피하고 전략적·군사적 목적을 달성하기 위해 소규모의 제한적인 사이버 작전을 적절히 활용하였으며, 인터넷을 포함한 다양한 사이버 공간을 통해 선전, 선동, 포섭, 언론방송

및 미디어 통제 등 정치·정보·심리전이 결합된 양상을 보였다[22,25]. 2022년 우크라이나 전쟁은 전격적, 공중전, 게릴라전, 시가전, 정밀폭격, 심리전, 유·무인 복합전 등 모든 수단이 동원된 배합전 양상으로 특히, 사이버전은 군사분야 뿐 아니라, 정치·경제·사회 등 다양한 분야로 확대되었다[29]. 주요 전쟁사례를 통해 살펴본 러시아의 사이버전 수행방식의 변화 및 주요 특성은 다음과 같다.

첫째, 사이버 공간에서의 전쟁 주체 및 공격의 대상이 점차 확대되었다. 기존 러시아는 에스토니아 및 조지아 침공, 크림반도 합병시 국가 대 국가 또는 민간 해커들에 의해 주로 상대국 및 적대국의 사회기반시설, 정부 주요 기관을 대상으로 사이버 공격을 수행하였으나, 우크라이나 전쟁에서는 러시아의 군사 정보기관인 총정찰국 GRU, 러시아 정부에 기반한 해커집단뿐 아니라, 자발적으로 참여한 세계 해커들, 민간인 등 사이버 공격의 주체가 더욱 다양화되었다. 이는 누구나 개인 스마트폰 및 인터넷을 이용하여 틱톡(TikTok), 유튜브(YouTube) 등 다양한 콘텐츠에 접근이 가능한 동시에 온라인을 통해 모든 군사적 행동을 전장의 병사들뿐 아니라, 전 세계 모든 인터넷 사용자들이 실시간 확인할 수 있게 되었다[8,30]. 뿐만 아니라, 이제는 사물인터넷·클라우드·빅데이터·모바일 등의 플랫폼으로 확대된 초연결사회의 특성에 기인하여 사이버전의 전장영역이 훨씬 더 다양해졌으며, 공격의 대상 또한 개인과 기업 홈페이지, 정부의 웹사이트, 사회기반시설 및 군 작전까지 우크라이나 지역 내 전방위로 확대되었다[31]. 따라서 개인 안전과 사회안전을 넘어 지역적으로도 기존 적대국만을 대상으로 이루어지던 공격 양상에서 미국을 포함한 NATO 국가, 다국적 기업, 공공기관까지 글로벌 차원으로 위협이 증대되었다[3,26].

둘째, 인공지능(AI : Artificial Intelligence) 기술을 이용한 허위정보 유포 등 사이버 공격이 고도화되었다. 기존에는 주로 디도스, 메일 폭탄, 악성 바이러스 등 해킹을 통해 주요 홈페이지를 마비시키고, 네트워크를 파괴하는 공격이 주를 이루었으나, 우크라이나 전쟁에서는 정부기관의 홈페이지 화면을 변조하는 디페이스(Deface), 특정 인물의 얼굴을 합성하는 딥페이크(Deepfake) 해킹 공격뿐 아니라, 생성형 인공지능(Generative AI)과 대형 언어모델(LLM : Large Language Models)을 활용한 피싱 공격, 악성코드 개발 등 인공지능 및 자동화 기술을 허위정보 생성에 활용하고 있다[32,33,34]. 특히, 러시아는 전쟁 이전에는 금전 목적의 랜섬웨어 공격을 가하였으나, 전쟁 이후 전쟁을 위한 사이버 공격으로 전환하면서 인공지능 기반 언어모델을 활용하여 랜섬웨어의 공격 속도와 범위를 지속적으로 증가시키고 있다[33,34]. 이처럼, 러시아는 우크라이나 전쟁이 장기화되고 서방의 제재가 지속될수록 경제적 문제를 해결하기 위한 수단으로 인공지능 기술을 활용한 랜섬웨어 공격을 통해 훨씬 더 표적화된 전략적인 방식을 선보일 것으로 예상된다[3,35].

셋째, 러시아는 물리적 공격 이전부터 주요 민·관·군을 대상으로 동시다발적 사이버 공격을 감행하였다. 러시아는 군사적 작전을 수행하기 이전부터 선전 및 선동을 통해 군의 전투력과 사기를 저하시키는 등 전쟁에 유리한 여건을 조성하였으며, 이를 위해, 정부와 정보기술(IT), 에너지, 금융기관 그리고 군 관련 주요시설 및 지휘통제시설 등을 표적으로 대대적인 사이버 공격을 실시하였다. 특히, 조지아 침공의 경우 무력 침공 이전부터 조지아 전역에 있는 주요 행정부서, 은행, 언론기관 웹사이트에 러시아 해커들이 사전 침투하여 5일 만에 신속하게 전쟁을 끝낼 수 있었다[12]. 이처럼, 러시아는 외부 세력이 개입할 수 있는 여지를 차단하기 위해 전쟁 이전 사이버전을 통해 지휘 및 정보체계를 와해시키고 공격 여건을 조성한 이후, 속전속결 형태의 군사적 공격을 감행하는 방식을 적절히 활용하고 있다. 우크라이나 전쟁 또한 기존과 마찬가지로 개전과 동시에 키이우를 최단시간내 함락하기 위해 우크라이나와 NATO의 군사시설, 주요기반시설, 공공기관, 민간기업 등 민·관·군 전방위적 표적을 대상으로 사이버 공격을 감행하였다[3].

<표 2> 러시아의 사이버전 주요 사례

구 분	세 부 내 용
에스토니아 사이버 공격	· 정부 및 관계기관, 대중매체, 공공기관, 은행 등 웹사이트에 대규모 디도스 공격
조지아 침공	· 정부, 언론, 금융기관 등 주요 사이트 디도스 및 악성 바이러스 공격
크림반도 합병	· 사이버 공간을 통한 선전, 선동, 포섭 및 디도스 공격을 통한 통신 네트워크 마비
우크라이나 전쟁	· 멀웨어, 디도스, 랜섬웨어, 디페이스, 딥페이크, 위성시스템 교란 등 사이버전·정보전, 네트워크 파괴

5. 한국의 사이버전 발전방안

러시아는 차세대 전쟁 전략을 기반으로 한 사이버 공

간에서의 전투 수행방식을 오랜 기간 발전시켜 왔으며, 전쟁 이전부터 정치적·군사적 목표를 달성하기 위해 다양한 방식의 사이버전 수행능력을 강화해 나갔다. 이에, 에스토니아를 대상으로 한 사이버 공격부터 최근 우크라이나 전쟁에서의 사이버전, 심리전, 정보전이 결합된 하이브리드전을 살펴봄으로써, 북한과 대치한 현재의 우리나라 현실에 적합한 사이버전 발전방안을 다음과 같이 세 가지로 제안하고자 한다.

첫째, 미국과 연계한 글로벌 사이버 방호 협력체계를 강화해 나가야 한다. 최근에는 사이버 공격이나 악성코드 등과 같은 사이버 위협도 인공지능 기술을 활용하여 더욱 복잡하고 다양하게 진화하고 있다. 러시아가 우크라이나 침공 직후 딥페이크 기술을 활용한 질렌스키 대통령의 항복연설, 우크라이나 대통령을 비난하는 우크라이나군 최고사령관 동영상 등은 SNS를 중심으로 빠르게 확산되었다[32]. 특히, 북한은 현재 김일성대학 등 대학·연구소를 중심으로 문서 분석·관리, 안면·음성·지문 인식, 생산용·자율이동 로봇, 인공지능 기반 사이버 능력 분야의 연구를 수행 중인 것으로 알려져 있으며, 이러한 북한의 인공지능 연구는 정찰총국 121국 등 사이버 작전을 수행하는 해킹 관련 조직에서 주도할 가능성이 크다고 분석되었다[37]. 미국은 2000년대 초반 중국, 북한, 이란 등으로부터 사이버 공격을 받게 되면서 국가적으로 사이버안보의 중요성을 인식하였으며, 이와 함께, 국가차원의 사이버안보 정책 및 조직을 정비하여 현재 세계 최고 수준의 사이버 방호능력을 보유하고 있다. 특히, 바이든 행정부는 2025년까지 인공지능 기술이 적용된 디지털 군사 인프라를 구축하기 위해 2021년 '미국 디지털 부대(US Digital Corps)'를 설립하였으며[38], 더불어, 2023년 3월 '국가 사이버안보 전략(National Cybersecurity Strategy)'을 통해 사이버 공간의 안전성 확보, 주요기반시설 및 제어시스템 보안 강화뿐 아니라, 신기술 개발 및 국제협력을 통한 대응 강화에 초점을 두고 있다[39]. 이에, 우리나라는 정보통신기술(ICT) 강국의 이점을 활용하여 적극적인 기술협력 및 미국과의 정보공유체계를 구축함으로써, 다른 국가들과의 협력 또한 확장해 나가는 글로벌 사이버 방호체계를 구축해야 한다. 이를 통해 북한뿐 아니라 러시아, 중국, 이란 등 권위주의 국가들이 인공지능의 정보생산 및 대량 정보 전달 기술을 이용하여 사이버 공간에서 가짜뉴스, 허위정보를 확산하는 행위를 국제적 차원에서 함께 대응해 나가야 한다.

둘째, SNS를 통한 여론전 및 심리전, 정보전에 대한 사전 준비가 필요하다. 북한은 평시 미사일 발사 또는 핵실험 뒤 위협적 선전을 통해 내부 무력감 확산을 노리는 '와해전략(Distuption Strategy)'을 사용하고 있으며, 향후 다양한 방식의 하이브리드전을 수행할 것으로 예상된다[4]. 최근 북한은 정서적 공감을 유도하는 언어적 댓글 무기를 통해 커뮤니티, 인플루언서(Influencer)들의 SNS를 매개로 한 영향공작의 효과를 극대화하고 있으며, 소규모 북한 댓글 부대의 친북단체, 사회적 인플루언서 등의 표적그룹을 기반으로 한 사이버상 여론 왜곡도 얼마든지 가능할 것으로 보인다[40]. 최근 마이크로소프트(Microsoft), 구글(Google) 등 빅테크(Big Tech) 기업들도 러시아의 정치적 선전 차단에 나섰으며, 유럽연합 또한 최근 러시아발 허위정보 확산을 막기 위해 메타(Meta)와 같은 빅테크 플랫폼 기업에 정치광고와 콘텐츠 관리 규정을 엄격히 하는 의무 조치를 부과하였다[36]. 이처럼, 대량 생산된 허위정보는 민주주의에 심대한 해를 끼칠 수 있어 미국 및 유럽 국가들은 이를 사전에 차단하기 위한 관리 감독 노력을 지속하고 있다. 이에, 우리나라 또한 북한의 여론 및 심리전에 대응하여 가짜뉴스를 불식시키고 허위정보를 차단하기 위해서는 정부의 공식적인 정보 및 긴급정보를 공유 또는 전달할 수 있는 소통창구의 역할이 필요하다. 이를 통해 가짜뉴스에 대한 출처를 빠르게 파악하는 동시에 즉각적인 조치를 통해 국민적 혼란을 예방하고 사회적 혼선을 최소화하기 위한 대국민 홍보 및 소통 강화에 노력해야 한다. 또한, 딥페이크를 만들어 허위정보를 조작하거나 플랫폼을 이용하여 가짜뉴스를 유포·확산하는 것을 사전에 탐지 및 조치하기 위해서는 국내 플랫폼 기업들과 연계한 기술적 대응과 더불어 해외 빅테크 기업들과의 상호 기술 및 모니터링 지원, 공동 대응센터 구축 등 정부 차원의 제도 및 정책개선과 함께 국민들을 대상으로 한 미디어 역량 교육 또한 함께 이루어져야 할 것이다[41].

셋째, 사이버전자전에 대한 민·관·군 공동의 협력이 필요하다. 러시아는 우크라이나를 침공하기 직전 항법위성과 상업용 위성의 통신 신호 교란을 목적으로 미국 위성통신 기업 비아샛에 해킹공격을 가하였으며, 이를 통해 군사 지휘를 차단하고 데이터 해킹 및 미디어 기업을 공격한 정황이 포착되었다[42,43]. 또한, 러시아는 우크라

이나 전쟁 발발 이후 우크라이나를 비롯해 동유럽까지 범위를 넓혀 전자전을 강화하였으며, 발트해 연안에서 위성항법장치(GPS : Global Positioning System) 교란을 통해 상공을 지나가는 민항기 및 군용기에 직접적인 위협을 가하였다[44]. 북한은 러시아에서 GPS 전파 방해 장치 재머(Jammer)를 들여와 이를 모방해 GPS 재머를 만들었으며, 현재 북한은 황해남도 연안, 개성 등과 중·동부전선 일대에 GPS 재머를 설치한 것으로 알려져 있다[45,46]. 최근 북한은 서해 지역 GPS 교란 공격을 통해 우리나라의 군용 선박뿐 아니라, 민간 선박 및 항공기 등의 통신 장애를 유발하고 있다[46]. 특히, 선박제어시스템은 사이버 리스크나 네트워크 모니터링을 염두하고 설계되지 않아 사이버 공격에 취약하며[47], 이러한 제어시스템에 대한 사이버전자전 공격은 사이버 및 무선 공간에서뿐 아니라, 물리적 세계에서의 공격 표면을 증가시켜 더 큰 위험을 초래할 수 있다[42]. 이에, 북한의 사이버 공격을 사전 탐지하고 무선 공격을 회피할 수 있는 민간기업의 위성 인터넷 서비스 기술, 이동통신사의 차폐안테나를 이용한 전자파 차폐 기술, 에너지 관련 기관의 신속 복구 및 에너지 운영 기술 등 IT·민간·공공기업과 함께 관련 부처 및 기관은 북한의 사이버 공격에 대비한 대응 훈련을 정례화하고, 공격 대상 및 수단을 고려한 대응 매뉴얼을 구체화해야 한다. 이를 통해, 유사시 선박과 항공기를 관리하는 관계기관, 전파를 감시하고 대응하는 과기정통부 및 관련 부처, 다수의 무기체계를 운용 및 관리하는 군 및 국방부와의 실시간 정보공유 및 협력을 통해 피해를 최소화하고, 국민 생활이 빠른 시간에 정상화될 수 있도록 국가차원의 구체적인 대응체계 마련이 필요할 것으로 사료된다[48,49].

6. 결론

러시아는 2014년 사이버전 전담부대를 창설하였으며, 사이버 공격 능력은 실제 수행사례 등을 고려하면 미국에 버금가는 수준의 역량을 보유한 것으로 알려져 있다[9]. 러시아는 최소 15년 이상 공격적 사이버 기술을 개발 및 사용해 왔으며, 특히 서방의 해저케이블 및 산업제어시스템(ICS : Industrial Control System)을 포함한 중요 인프라에 대한 사이버 공격 역량을 갖추고 있다[3,9]. 특히, 최근 러시아와 북한의 협력은 핵이나 미사일, 재래식 전력뿐 아니라, 러시아의 사이버전 경험을 북한에 전수할 수 있어 우리에게 가장 큰 위협으로 다가오고 있다[48]. 이에, 러시아가 최근 선보였던 사이버전 수행방식 및 주요 특징을 바탕으로 다음과 같이 한국의 사이버전 발전방안을 모색하였다.

첫째, 미국과 연계한 글로벌 사이버 방호 협력체계를 강화해 나가야 한다.

둘째, SNS를 통한 여론전 및 심리전, 정보전에 대한 제도적 또는 정책적 사전 준비가 필요하다.

셋째, 사이버전자전에 대비한 국가차원의 구체적인 대응전략을 마련하고 민·관·군 협력이 요구된다.

이처럼, 사이버-물리 시스템의 융합으로 급변하는 안보·기술 환경변화에 적절히 대응하고, 비대칭 전력의 핵심 수단인 하이브리드전 위협에 효과적으로 대응하기 위해서는 군사분야 뿐 아니라, 민간의 인공지능 및 정보통신 기술, 국제협력을 통한 군사적·비군사적 지원활동을 통해 사이버전 수행능력 향상이 필요한 시점이다.

본 연구의 한계로는 현재 우크라이나와 비교하여 우리나라의 사이버전 수단 및 방호능력에 대한 분석이 구체적으로 이루어지지 않았으며, 본 논문에서 제안한 발전방안들에 대한 제한사항 식별 및 정책적 검토가 선행되어져야 한다. 향후에는 제안한 발전방안을 보완하여 현재 우리나라와 우크라이나의 사이버 방호태세 및 수단, 전략 등을 비교·분석함으로써, 북한의 사이버 위협을 성공적으로 상쇄시키기 위한 한국의 대응전략을 모색하도록 하겠다.

참고문헌

[1] 합동군사대학교(2022), “러시아-우크라이나 전쟁 분석: 군사적(합동성)관점에서의 전훈 분석 및 함의”, 합동군사대학교, 1-439.

[2] 김성일(2023), “우크라이나 사태에서 배우는 북한 미사일 대응 방향”, 국방과 기술, 528, 98-107.

[3] 신범식, 양정윤(2024), “우크라이나 전쟁과 사이버전: 러시아의 사이버 공격 및 NATO의 우크라이나 지원과 영향에 대한 고찰”, 러시아연구, 34(1), 129-165.

[4] 윤정현(2022), “러시아-우크라이나 전쟁 장기화와 정보·심리전의 진화 양상”, 국가안보전략연구원 이슈브리프, 383, 1-9.

[5] 심승배, 안광수, 김정은, 서영희, 양영철(2022), “첨단 과학기술 기반의 국방 디지털 혁신”, 한국국방연구원, 1-101.
[6] 중앙일보(2022.2.15.), “러 국방부 우크라이나 국경에서 일부 병력 철수”. https://www.joongang.co.kr/article/25048424
[7] 동아일보(2022.2.19.), “우크라서 시작된 ‘하이브리드 전쟁’...러시아發 총성없는 공포”. https://www.donga.com/news/article/all/20220219/111904481/1
[8] 현인택, 권태환, 김광진, 김규철, 김진형, 박재완, 박종일, 박주경, 방종관, 송운수, 송승종, 박철균, 안재봉, 양욱, 윤원식, 이홍석, 장태동, 장원준, 장광호, 조현규, 유형곤(2023), “우크라이나 전쟁의 시사점과 한국의 국방혁신”, 로얄컴퍼니, 1-434.
[9] 채재병(2019), “국제 사이버공격 전개 양상 및 주요국 대응전략”, 국가안보전략연구원, 1-110.
[10] 김성진(2018), “러시아 안보정책의 변화”, 슬라브학보, 33(2), 91-127.
[11] 연합뉴스TV(2024.6.21.), “북러 불법 사이버 활동까지…유엔 안보리 공개 압박”. https://www.yonhapnewstv.co.kr/news/MYH20240621005000641?input=1825m
[12] 우평균(2014), “유라시아 분쟁에서의 러시아의 개입: 조지아 전쟁과 우크라이나 사태”, 국제정치연구, 17(2), 73-97.
[13] 이승열(2023), “북한 사이버 공격 전략의 진화: 대북제재 회피를 위한 외화벌이 수단으로서 사이버 전략”, 통일정책연구, 32(1), 323-353.
[14] 문계성, 권찬주, 송애연(2023), “이스라엘-하마스 공격 전술과 북한의 접경지역에 대한 하이브리드전 대비 연구”, 접경지역통일연구, 7(2), 151-178.
[15] 장원준, 송재필(2022), “최근 글로벌 안보환경 변화에 따른 국내 방위산업의 시사점과 향후 과제”, 월간 KIET 산업경제, 282, 46-57.
[16] 문용득, 박동휘(2022), “러시아의 사이버전 전략: 러시아-우크라이나 전쟁초기 전역을 중심으로”, 민족연구, 80, 10-34.
[17] 이용석, 정경두(2022), “러시아 대 우크라이나 사이버 전쟁의 교훈과 시사점”, 국방정책연구, 137, 37-79.
[18] 김경순(2018), “러시아의 하이브리드전(우크라이나 사태를 중심으로)”, 한국군사, 4, 63-95.
[19] 홍규덕(2022), “하이브리드 전쟁의 역설: 우크라이나 전쟁의 교훈”, 전략연구, 29(2), 53-73.
[20] 송승종(2017), “러시아 하이브리드 전쟁의 이론과 실제”, 한국군사학논집, 73(1), 63-94.
[21] 김남철, “강대국들의 하이브리드전과 주요 사례분석”, 한국군사학논총, 11(2), 3-30.
[22] 유남주(2021), “스베친의 전략론에 의한 러시아 하이브리드전 분석”, 국민대학교 석사학위논문.
[23] 최근대, 나호영(2022), “러시아의 우크라이나 침공과 서방의 대응: 하이브리드전의 이론과 적용을 중심으로”, 군사연구, 154, 1-31.
[24] 국방일보(2021.2.9.), “[러시아-에스토니아] ‘소련 지우기’ 청동군인상 이전이 도화선”. https://kookbang.dema.mil.kr/newsWeb/20210118/1/BBSMSTR_000000100135/view.do
[25] 김규철(2022), “우크라이나 전쟁에서 러시아의 정보전 활동”, 슬라브연구, 38(4), 29-60.
[26] 이형동, 윤준희, 이덕규, 신용태(2022), “러시아-우크라이나 전쟁에서의 사이버공격 사례 분석을 통한 한국의 대응 방안에 관한 연구”, 한국정보처리학회, 11(10), 353-362.
[27] 남보람(2021), “러시아의 영토확장 행동에 대한 나토와 미국의 군사적 대응 연구: 2008년 러시아-조지아 전쟁, 2014년 러시아-우크라이나 전쟁을 중심으로, 한국과 국제정치, 37(4), 143-174.
[28] 뉴시스(2022.11.11.), “MS 러 해킹그룹, 우크라·폴란드 물류기업 랜섬웨어 공격”. https://www.newsis.com/view/NISX20221111_0002082167
[29] 월간조선(2024.5.21.), “2025년에도 전쟁은 계속되고 또 일어날 수 있다”. https://monthly.chosun.com/client/mdaily/daily_view.asp?idx=19655&Newsnumb=20240519655
[30] 유기현(2024), “2개의 전쟁, 무엇을 배울 것인가?”, 한국국방연구원 국방논단, 1992, 1-12.
[31] 임영모, 옥도경, 김태호, 이원승, 이현수, 용환승, 오무송(2017), “국방과 소프트웨어 융합 활성화 방안 연구”, 소프트웨어정책연구소, 1-215.
[32] 국방일보(2024.2.13.), “대통령 대국민 연설·군 총사

령관 명령이 가짜?”.
https://kookbang.dema.mil.kr/newsWeb/20240214/1/ATCE_CTGR_0020010001/view.do
[33] ZDNET Korea(2024.5.28.), “러시아가 獨 정치인에게 보낸 이메일 알고보니 ‘해킹’…포티넷 해결책은?”.
https://zdnet.co.kr/view/?no=20240528112613
[34] ZDNET Korea(2024.6.25.), “금전 이익 노리는 랜섬웨어, 더 빠르고 과감해졌다”.
https://zdnet.co.kr/view/?no=20240625121855
[35] 매일경제(2024.8.22.), “고도화되는 사이버 보안 위협, 모든 기업 대비책 마련해야”.
https://www.mk.co.kr/news/business/11098570
[36] 매일경제(2024.2.19.), “지난해 4분기 랜섬웨어 공격 65% 증가...‘핵비티즘·AI’ 신흥 위협으로 부상”.
https://www.mk.co.kr/news/it/10946286
[37] 이경복(2021), “사이버작전과 인공지능, 미 국방 분야의 추진 동향”, 한국국방연구원 국방논단, 1847, 1-12.
[38] 송태은(2022), “바이든 행정부의 인공지능 국가정책: 평가와 함의”, 국립외교원 외교안보연구소, 2021(47), 1-37.
[39] 김소정(2023), “2023 미국 사이버안보 전략 주요내용과 한국에의 시사점”, 국가안보전략연구원 이슈브리프, 423, 1-11.
[40] 변상정, 윤정현(2024), “북한의 사이버 영향공작 진화와 시사점”, 국가안보전략연구원 이슈브리프, 549, 1-8.
[41] 매일경제(2024.3.28.), “가짜뉴스 꼼짝마 연령대별 미디어 읽기 교육지원”.
https://www.mk.co.kr/news/culture/10976812
[42] IT DAILY(2023.5.31.), “사이버 물리 시스템의 안정성 해결을 위한 3단계 초기 로드맵”
http://www.itdaily.kr/news/articleView.html?idxno=214298
[43] 일요서울(2024.6.10.), “우주항공청 ‘발족’ 사이버 안보 대두...북한의 위성교란 대안은?”.
https://www.ilyoseoul.co.kr/news/articleView.html?idxno=488907
[44] 뉴시스(2024.5.30.), “GPS 교란, 전자전 핵심 공격·방어수단…러시아·이스라엘전에도 활용돼”.
https://www.newsis.com/view/?id=NISX20240530_0002754505&cID=13005&pID=13100
[45] 세계일보(2024.5.31.), “북한이 우리 하늘에 뿌렸다... 비행기·첨단무기 GPS 무력화 노리나”.
https://www.segye.com/newsView/20240531510141?OutUrl=naver
[46] 서울경제(2024.5.31.), “北 GPS 교란에 내비 ‘먹통’... 어선들 위치도 몰라 조업 포기”.
https://www.sedaily.com/NewsView/2D9EICRUSA
[47] 한스경제(2023.9.7.), “사이버 공격, 해상도 안심할 수 없어...해사 사이버보안 인재 육성해야”.
https://www.hansbiz.co.kr/news/articleView.html?idxno=663057
[48] 전자신문(2024.7.16.), “[데스크가 만났습니다]임종인 대통령사이버 특보 러북 협력, 가장 큰 위협은 사이버전 노하우 전수”.
https://www.etnews.com/20240716000302
[49] 이데일리(2016.4.6.), “북한 GPS 교란 6년간 막아낸 이동통신 안테나 고깔모자”.
https://www.edaily.co.kr/news/read?newsId=02955286612613496
[50] 김소정(2022), “우크라이나 사이버전 대응사례와 한국의 역량 제고 방안”, 국가안보전략연구원 전략보고, 200, 1-23.

이 세 훈 (Se Hoon Lee)

- 2018년 2월: 연세대학교 정보산업공학과(공학석사)
- 2023년 2월: 광운대학교 방위사업학과(경영학박사)
- 2019년 7월~2022년 8월: 육군3사관학교 국방시스템과학과 교수
- 2022년 8월~2023년 2월: KAIST 인공지능 연구실 정책연수
- 2024년 4월~현재: 육군대학 소령지휘참모과정
- 관심분야: 방위산업, 국방정책
- E-Mail: leeseddung@gmail.com

이 승 훈 (Seung hoon Lee)

- 2021년 2월: 연세대학교 산업공학과(공학박사)
- 2022년 8월: LG 디스플레이
- 2022년 9월~현재: 동아대학교 산업경영공학과 조교수
- 관심분야: 제조, 헬스케어, 국방
- E-Mail: seungh@dau.ac.kr