석사학위논문

한국군 사이버 심리전 운용방안에 관한 연구

2024년

한성대학교 국방과학대학원

국 방 경 영 학 과

국 방 경 영 전 공

윤 용 재

석 사 학 위 논 문
지도교수 최원상

한국군 사이버 심리전 운용방안에 관한 연구

A Study on the Cyber Psychological Warfare in ROK Armed Forces

2023년 12월 일

한성대학교 국방과학대학원

국 방 경 영 학 과

국 방 경 영 전 공

윤 용 재

석 사 학 위 논 문
지도교수 최원상

한국군 사이버 심리전 운용방안에 관한 연구

A Study on the Cyber Psychological Operation Warfare in ROK Armed Forces

위 논문을 국방경영학 석사학위 논문으로 제출함

2023년 12월 일

한성대학교 국방과학대학원

국 방 경 영 학 과

국 방 경 영 전 공

윤 용 재

윤용재의 국방경영학 석사학위 논문을 인준함

2023년 12월 일

심사위원장 박 동 순(인)

심 사 위 원 최 원 상(인)

심 사 위 원 김 종 배(인)

국 문 초 록

한국군 사이버 심리전 운용방안에 관한 연구

한성대학교 국방과학대학원
국 방 경 영 학 과
국 방 경 영 전 공
윤 용 재

본 논문은 국가안보에서 사이버 공간의 중요성이 확대되는 국내·외 안보환경(국내 및 우크라이나 전쟁 등에의 사이버 심리전 위협 증대) 북한의 사이버 심리전의 위협과의 연관성을 중심으로 한국군의 사이버 심리전 발전 방향을 제시하는데 목적을 두고 있다. 본 논문의 핵심내용은 “사이버 안보의 비중이 확대되고 그중에서도 사이버 심리전이 전쟁의 주도권과 향방을 결정짓는 핵심 요소로 작용하는 추세와 전망 속에서 한국군은 어떻게 대비하고 준비해야 하는가?”이다. 발전 방향을 제시하기 위해 본 논문은 미래전에서의 사이버 안보(심리전)의 중요성과 러시아의 사이버 심리전 전술을 고찰하고 북한의 사이버 위협을 분석하였다.

본 논문은 미래전에서의 사이버 안보의 확장 및 다변화에 대해 고찰하고 사이버 심리전의 개념과 특성, 전술 그리고 법적인 근거에 대해 살펴보고 북한의 사이버 심리전 위협에 대비하기 위한 한국군의 사이버 심리전 운용방안에 관해 연구하였다.

사이버전은 전자전, 정보전, 인지전 등의 여러 비물리적 전쟁과도 중첩되어 있으며, 물리적 전쟁과도 긴밀히 연관되어 있다. 또한, 외교전쟁, 문화전쟁과 같은 여러 안보 이슈들과도 관련되어 있어 사이버전은 개념의

확장과 다변화 속에서 이해해야 한다. 또한, 여러 전쟁형태가 융합된 미래 하이브리드(Hybrid) 전쟁에서의 사이버 공간의 비중은 더욱 확대될 것임을 알 수 있었다.

사이버 심리전은 전통적인 심리전의 단순한 확장이 아닌 명확한 특징을 가지고 있다. 러시아와 같은 권위주의 국가들에 사이버 심리전은 공격과 방어에 있어서 비대칭전의 이점을 취할 수 있는 매력적인 수단으로 지속 확대될 것이다. 그러나 미국, 유럽, 한국과 같은 민주주의 국가들이 사이버 심리전을 수행하기 위해서는 법적 근거와 정치적 영역에 포섭되지 않아야 하는 등의 제한사항이 있음을 알 수 있었다.

북한도 사이버 환경과 정치·사회 환경의 비대칭성을 이용하여 국제사회와 한국을 대상으로 사이버 공격(사이버 기술 및 심리전 공격)을 지속하고 있다. 또한, 중국과의 관계, 경제난 심화 등의 여러 제한사항이 있음에도 한국 사회의 개방성과 내부갈등, 사이버 심리전의 간접성과 은닉성 등의 이점을 이용하여 사이버전 전력과 전략을 강화 및 진화시키고 있음을 알 수 있었다.

결론적으로 한국은 북한의 사이버 심리전의 위협에 대비하여 조직과 임무개편, 사이버 심리전 전략 수립, 우수한 유·무형 인터넷 인프라를 활용한 민·관·군 통합 사이버 심리전을 운용체계 정립 등을 위해 노력해야 한다. 나아가 러시아, 중국 등 권위주의 국가들의 사이버 심리전에 대항하고 대응능력을 향상하기 위해 미국과 일본, 유럽 등 우방 국가와 집단 방위체계를 구축해야 한다.

끝으로 본 연구는 한국의 정치적 환경과 사이버 심리전의 특성 때문에 구체적인 북한의 사이버 심리전 위협을 증명하는데 제약이 많았다. 그리고 러시아-우크라이나 전쟁, 이스라엘과 하마스와의 전쟁에서의 사이버 심리전 전략과 전술을 구체적으로 반영하기 어려웠다. 향후 사이버 심리전의 전훈 분석과 함께 인지전속에서의 사이버 심리전에 대한 지속해서 연구가 이루어져야 할 것이다.

【주요어】 사이버 안보, 사이버 위협, 심리전, 사이버 심리전, 인지전

목 차

표 목 차

그 림 목 차

제 1 장 서 론

제 1 절 문제 제기 및 연구목적

2010년대에 들어서면서 한국은 사회 전반에 초고속 인터넷이 급속하게 구축되고 다양한 네트워크 체계가 구축, 초연결되면서 사이버 공간의 중요성과 사이버 분야에 관한 관심이 높아졌다. 한국은 2020년 유엔 전자정부 평가에서 '전자정부 발전'에서 2위, '온라인 참여'지수에서는 공동 1위(한국, 미국, 에스토니아)에 랭크[1]되는 등 지식정보화시대 사이버 강국으로 비약적인 발전을 이뤄내고 있다. 이와 같은 정보기반체계의 극적인 발전은 안보 및 군사 측면에서의 다양한 기회와 강점을 제공해주고 있지만, 그 이면에는 지식 정보화, 네트워크화에 따른 또 다른 위협과 약점의 증대 그리고 위험의 다원화 및 다양화로 전략적, 작전적 환경이 더욱 복잡해지고 있는 것도 사실이다. 더욱이 한국의 비약적으로 발전된 정보화 시대의 역기능으로서 사이버 공간에서의 해킹과 바이러스 등의 침해 및 공격으로 인한 피해는 각국의 사이버 공간으로 확산되어 가공할 정도의 규모로 커지고 있어, 범국가적, 범세계적 이슈로 확장되고 있다. 특히 한반도 전구는 분단상황이라는 특수한 안보환경으로 인해 사이버 공간의 확장과 더불어 국가주요시설 등 핵심노드 확장, 사이버 심리전에 의한 국민 안보의식 약화 등 관련 위협이 대폭 증가하고 있다.

더욱 중요한 것은 이러한 사이버 위협이 국가안보와 군에 대한 직접적인 위협으로 대두되었다는 현실이다. 이와 더불어 최근 북한의 위협은 과거 재래식 방법에 의한 침투 및 국지적인 도발 위주에서 사이버 기술공격을 통한 사이버 테러, 사이버 심리 공격을 통한 한국 정부나 국민의 내부 분열 조장 등과 같이 무형적이지만 파괴적인 위협으로부터 테러, 생화학무기 등까지 다원화 및 다양화되고 있다. 이와 같은 위협은 불특정 대상으

1) 대한민국 행정안전부, "2020 UN 전자정부 평가'발표! 전자정부발전지수 2위, 온라인참여지수 1위," 『대한민국 행정안전부』, 2020년 7월 11일; https://blog.naver.com/mopaspr/222027870611 (검색일: 2022년 7월 2일).

로 범위가 무한정 확대되고 주체가 불분명하며 은밀한 양상으로 전개되기 때문에 위협의 불확실성이 심화하고 있다.

특히 북한의 사이버 심리전은 과거 친북 사이트 중심의 선전물 게시와 같은 수동적 형태에서 SNS, 전용 앱은 물론 한국 사람으로 위장한 토론글 게시 등 공격적 형태로 바뀌고 있다.[2] 그러나 한국의 대응은 사회 내부 이념 논쟁과 갈등을 유발할 위험 때문에 사이버 기술공격에만 초점이 맞춰져 있어 북한의 사이버 심리전에 대한 대응이 공론화되지 못하고 있는 것이 사실이다. 이는 최근 북한의 위협 변화와 비대칭 능력의 강화에 따라 국가 및 군사 전략적 수준의 적극적 대응과 발전 방향을 모색해야만 하는 시점이 이미 도래해 있다는 것을 말하고 있다. 또한, 전 세계적으로 이슈가 되고 있는 가짜뉴스(fake news) 및 허위조작정보(disinformation)[3] 또한, 한국의 안보 불안을 초래하고 경제손실을 유발하는 등 심각한 위협으로 대두되고 있다. 특히 북한 관련 가짜뉴스는 북한이 이를 활용해 역공작을 펼칠 수 있다는 점에서 새로운 유형의 위협으로 부상하고 있다.[4]

지금까지 논의된 바와 같이 최근의 전략적 안보환경 변화와 북한의 위협 양상을 고려해 볼 때, 관련 범정부 및 범군(軍) 차원의 총체적인(Holistic) 관점에서 국가와 군의 사이버 공간 및 사이버 심리전 위협에 대한 대비와 대응을 위한 체제발전의 모색이 시급한 실정에 있다. 이러한 측면에서 본고는 사이버 심리전의 개념과 특성을 정의하고, 그 중 거듭할수록 국가안보에 위협이 되는 북한의 대남 사이버 심리전에 대응하기 위한 합리적인 사이버 심리전 수행방안을 모색하는 데에 목적이 있다.

---

2) 이상진·위강섭, “북한의 사이버 심리전 징후 분석에 관한 연구,” 『디지털포렌식연구』, 제10권 1호,(2016), p. 39.

3) 가짜뉴스라는 용어는 규제 관련 논의 및 정교하고 치밀한 논의를 필요로 하는 학술 담론에서 폐기되는 것이 바람직하다, 가짜뉴스라는 용어는 허위조작정보가 발생시키는 복잡한 문제들을 모두 아울러 지칭하기에 부적합하고 정치적으로 악용되어 오해를 낳고 있기도 하다. 김민정, “가짜뉴스(fake news)에서 허위조작정보(disinformation)로”, 『미디어와 인격권』, 2019년 제 5권 제 2호(2019년), p. 24.

4) 경남대 극동문제연구소는 2020년 5월 11일 ‘북한 관련 허위정보 실태와 대응’이라는 제목의 보고서를 발표했다. 보고서는 최근 김정은 북한 국무위원장 건강 이상설 관련 가짜뉴스 유통 과정과 이에 따른 안보·경제적 손실을 분석하였는바, 북한 관련 가짜뉴스는 남북 긴장을 고조시키고 한반도 평화를 흔드는 등 불필요한 분단비용을 소모하게 하고 軍이 만일의 사태를 대비해 장기간 대응태세를 유지할 경우 피로감이 쌓여 오히려 안보 공백을 유발할 수 있다고 분석했다.

제 2 절 선행연구 고찰 및 연구방법

본 논문의 주제와 정확히 부합하는 한국의 사이버 심리전 발전 방향을 제시한 선행연구는 이기중(2008), 이상호(2011), 배달형(2015) 등이다. 사이버전에 관한 대부분의 연구들은 사이버전이라고 기술되어 있으나 하나 사이버 기술전(해킹, DDoS 공격 등)을 중심으로 한 연구들이어서 사이버 심리전에 관한 연구는 상대적으로 적다.

이기중(2008)은 북한의 사이버 심리전 사이트들에 대한 차단 등 최대한의 기술적 규제를 지속해야 하고 공세적 운용으로 제한적이지만 해외 거주 북한 유학생 등을 대상으로 하는 심리전 사이트 운영이 필요하다고 주장하였다. 또한, 잠재적 위협이 발생 가능한 지역에 대한 사이버 심리전을 전개하여 군사작전에 유리한 환경을 조성하여 분쟁 발생 시에는 국익을 실현하기 위한 사이버 심리전을 전개해야 함을 제기하였다. 다소 오래전의 연구임에도 불구하고 본 연구와 같이 북한의 사이버 심리전 위험성을 분석하였고, 나아가 한국의 국익과 관련된 세계의 분쟁을 대비한 사이버 심리전의 필요성 등 발전 방향에 대해 제시하였다. 그러나 사이버 심리전을 수행하기 위해 갖춰야 할 능력과 전제 조건에 관한 연구는 다소 아쉬웠다.[5)]

이상호(2011)는 본 연구와 같이 북한의 사이버 심리전 강화 배경과 능력 및 위협을 고찰하였다. 북한의 사이버 심리전 위협에 대응하기 위해서는 언론·미디어와 협력을 강화하고 위기 시에는 제한적으로 인터넷을 통제하며 국가 및 개인정보보호를 강화하고 국가 사이버 안전 총괄 기구를 통합을 제시하였다.[6)] 한국 사회의 인터넷 의존도를 고려 시 위기라 할지라도 인터넷을 통제하는 것은 너무나 큰 희생을 감수해야 하므로 현실성이 떨어진다는 아쉬움이 있지만 언론과의 소통, 정보보호, 조직 통합 및 개편에 대한 필요성에 대한 부분은 연구에 많은 참고가 되었다.

---

5) 이기중, "효율적인 국방 사이버 심리전 수행방안," 『정보·보안 논문지』, 제8권 제1호(2008), pp. 112-114.

6) 이상호, "북한의 사이버 심리전의 실체와 대응방향," 『대전대학교 한국정치외교사 논총』,(2011), pp. 279-286.

비교적 최근 연구인 배달형(2015)은 본 연구자와 유사하게 4세대전쟁과 비대칭 위협 측면에서 사이버전 및 사이버 심리전의 양상과 중요성을 제기하였다. 또한, 한국군의 사이버전 및 사이버 심리전의 포괄적 발전 방향성을 정립하였다. 발전과제로 ① 국가 및 군사전략 수준의 정책과 전쟁 및 위기에 대비한 사이버 거버넌스 정립, ② 전쟁과 위기 대비 사이버전 능력의 군사작전 수행에의 통합체계 마련, ③ 통합적 국방 사이버 심리전 체계 및 절차 발전 방향을 제시[7]하여 본 연구에 많은 부분을 활용하였다. 다만 사이버 심리전보다는 사이버 기술전을 포함한 사이버전으로 대응 방향에 집중되어 있어 아쉬웠다.

공통적으로 자료 작성 시기와 공개된 정보의 부정확성 등으로 북한의 사이버 심리전 능력과 위협에 대해 연구자마다 상이하였다. 사이버 테러, 사이버 공격, 사이버 심리전 등 사이버전에 대한 정확한 개념 정립이 없어 사이버전에 대한 정확한 대한 이해에 제한되었다. 또한, 기존의 전통적인 키네틱전과 비키네틱전[8]의 다른 유형인 인지전, 정보전, 전자전 등과 사이버전(사이버 심리전)이 어떠한 차이와 연관성을 가지고 있는지에 대한 명확한 정리가 부족하였다. 끝으로 사이버 심리전에 전술에 관한 구체적인 연구가 불충분하였다.

이에 본고는 앞서 비교적 최근 연구자료인 송태은(2021, 2020), 윤민우·김은영(2023) 등을 적극 참고하여 사이버전에 대한 이해, 미래전에서의 역할, 사이버 심리전 전술과 유럽 및 NATO의 대응 등을 연구하였다. 송태은(2021, 2020)은 여러 연구자료에서 하이브리드 위협 수단으로서의 사이버 심리전의 목표와 전술을 분석하였다. 또한, 미국과 유럽이 권위주의 국가들의 하이브리드 위협에 대응하기 위해 다양한 대응체제와 조직을 구축하고 협업과 공조를 위해 노력한 것을 한국과 역내 국가들이 벤치마킹해야 함을 제기하였다. 윤민우·김은영(2023)은 사이버 안보의 확장과

---

7) 배달형, "4세대전쟁 및 비대칭 위협 관점의 사이버전 및 사이버 심리전 발전방향," 『전략연구』, 제22권 1호(2015), pp. 141-172.

8) 키네틱전(kinetic warfare)은 물리적인 폭력이 동원되는 전쟁양식이며, 비키넥틱전(non-kinetic warfare)은 물리적 폭력수단을 우회할 수 있는 형태의 전쟁양식이다. 윤민우·김은영, 『모든 전쟁: 인지전, 정보전, 사이버전, 그리고 미래전쟁애 대한 전략이야기』(서울: 박영사, 2023), pp. 93-94.

다변화 현상, 미래전의 발전 추이와 사이버 안보의 비중 확대, 인지전의 전략과 전술에 대해 심도 깊은 연구결과를 제시하였다.

또한, 본고는 선행연구에서 제시한 전략 수립, 조직의 개편, 민·관과의 협조 및 공조에 추가하여 법적 근거 마련, 사이버 집단 방위체계 구축 및 협력 강화 등 추가적인 발전 방향도 제시하였다.

본고는 경험적 사회과학의 방법론에 기초하여 문헌 조사 방법을 적용하였다. 국방부 및 합참, 육군의 교리에 대해서는 군사보안 규정에 저촉되지 않는 범위 내에서 참고하였으며, 국방대학교, 한국국방연구원(KIDA), 국내·외 민간 연구기관의 학술세미나 및 연구 논문, 서적, 학술지, 그리고 기사 등을 광범위하게 참고하였다. 특히, 러시아와 우크라이나 전쟁에서의 사이버 심리전, 이스라엘-하마스 전쟁 간 사이버 심리전은 심도 깊은 아직 전쟁이 진행 중인 제한사항으로 심도 깊은 연구보다는 단편적인 전문가들의 분석(인터넷 언론사 투고) 등을 활용하였다.

본 논문의 구성은 총 5장으로 구성되어 제1장 서론에서는 연구배경 및 목적을 통해 한국군의 사이버 운용방안 정립의 필요성을 제기하였다. 제2장에서 사이버 안보와 사이버 심리전 이해와 법적 근거, 제3장에서는 북한의 사이버 심리전 능력과 위협, 제4장에서는 한국군의 사이버 심리전 운용 발전방안을 도출하였으며, 제5장 결론으로 마무리하였다.

제 2 장 사이버 안보 및 심리전에 대한 이해

제 1 절 사이버 안보 개념의 확장과 다변화

빠르게 변화하는 안보환경 속에서 사이버 안보의 개념과 정의 또한 변화하고 있으며 다변화하고 있다. 사이버 안보는 통상적인 의미에서 해킹과 분산서비스거부(DDoS; Distributed Denial of Service, 이하 디도스) 공격[9], 랜섬웨어(ransomware)[10] 공격 등의 사이버 기술공격 위협을 지칭했다. 하지만 점차 온라인에서의 가짜뉴스나 오정보, 여론조작 등의 정보 콘텐츠와 관련된 문제들도 주요 위협으로 부각되고 있다. 또한, 드론과 무인자동차, 로봇, 그리고 사물인터넷(IoT; Internet of Things) 등 인공지능(AI; Artificial Intelligence) 기반의 여러 무인 디바이스들이 인터넷을 통해 서로 연결되어 사이버 안보는 이와 같은 새로 등장하는 각종 무인 디바이스들과 관련된 위협의 문제로까지지 확장되고 있다.

사이버 안보는 사이버를 구성하는 모든 부문에 대한 안보를 모두 합친 개념이다. 사이버는 ① 인터넷 기반시설과 관련 장비·부품들, ② 인터넷에 연결된 유·무인 디바이스들, ③ 다비이스들을 운영하는 운영체계(OS)와 온라인 플랫폼, 그리고 AI 등의 프로그램, ④ 가상의 네트워크 체계와 규칙들, ⑤ 인터넷 공간에서 유통되는 정보 콘텐츠들, ⑥ 인터넷 공간의 정보와 인터페이스하는 인간의 의식(perception), ⑦ 콘텐츠(contents)[11]

---

9) 감염된 대량의 숙주 컴퓨터를 이용해 특정 시스템을 마비시키는 사이버 공격. 공격자는 다양한 방법으로 일반 컴퓨터의 봇을 감염시켜 공격대상의 시스템에 다량의 패킷이 무차별로 보내지도록 조정한다. 이로 인해 공격대상 시스템은 성능이 저하되거나 마비된다. 한국정보통신기술협회 정보통신용어사전 참조; http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=041650-3(검색일: 2023년 12월 1일).

10) 컴퓨터 사용자의 파일들을 암호화하여 금전을 요구하는 악성코드. 한국정보통신기술협회 정보통신용어사전 참조; http://terms.tta.or.kr/dictionary/dictionaryView.do?word_ seq=053701-5 (검색일: 2023년 12월 1일).

11) 인터넷이나 컴퓨터 통신 등을 통하여 제공되는 각종 정보나 그 내용물. 유·무선 전기 통신망에서 사용하기 위하여 문자·부호·음성·음향·이미지·영상 등을 디지털 방식으로 제작해 처리·유통하는 각종 정보 또는 그 내용물을 통틀어 이른다. 정보통신용어사전 참

또는 디바이스들을 연결하는 무선통신 등으로 구성되어 있다. 여기서 ①과 ②는 하드웨어, ③과 ④ 그리고 ⑤는 소프트웨어로 정의할 수 있다. ⑥은 인간의 뇌의 인지, 심리, 정서의 영역이다. ⑦은 대기(air)를 통해 연결되는 무형의 전파 또는 정보 패킷(Packet)이다.[12]

<표 2-1> 사이버 구성부문과 위협 형태

구 분	성 질	사이버전 위협	중첩
① 인터넷 기반시설과 관련 장비·부품들	하드웨어	사이버-기술전	키네틱전
② 인터넷에 연결된 유·무인 디바이스들	하드웨어	사이버-기술전, 사이버-심리전	전자전
③ 다비이스들을 운영하는 운영체계(OS)와 온라인 플랫폼, 그리고 AI 등의 프로그램	소프트웨어	사이버-기술전, 사이버-심리전	
④ 가상의 네트워크 체계와 규칙들	소프트웨어	사이버-기술전	
⑤ 인터넷 공간에서 유통되는 정보 콘텐츠들	소프트웨어	사이버-심리전	정보전
⑥ 인터넷 공간의 정보와 인터페이스 하는 인간의 의식(perception)	인지·심리 영역	사이버-심리전	인지전
⑦ 콘텐츠 또는 디바이스들을 연결하는 무선통신 등	무형 전파, 정보패킷(Packet)	사이버-기술전	전자전

* 출처 : 윤민우·김은영, 『모든 전쟁: 인지전, 정보전, 사이버전, 그리고 미래전쟁에 대한 전략이야기』(서울: 박영사, 2023), pp. 264-272. 내용을 요약하여 작성

먼저 ①에는 인터넷데이터센터(IDC; Internet Data Center), 통신기지국, 통신장비, 정보통신망, 케이블, 위성 등 물리적인 시설, 설비, 장비, 부품 등이 해당한다. 이 부문에서의 사이버전은 해킹과 악성 바이러스 유포 등의 사이버 기술전이며 시설·설비·정보통신망에 대해서는 지·해·공·우주

조; https://stdict.korean.go.kr/search/searchView.do(검색일: 2023년 12월 1일).

12) 윤민우·김은영, 『모든 전쟁: 인지전, 정보전, 사이버전, 그리고 미래전쟁에 대한 전략이야기』(서울: 박영사, 2023), pp. 265-266.

공간에서의 키네킥전과도 긴밀히 중첩되어 있다.

②에는 인터넷 기반시설과 결합되어 다양한 목적으로 사용되는 여러 디바이스들이. PC와 랩탑, 스마트폰과 스마트워치 등이 해당된다. 최근에는 무인자동차, 드론, 지능형 CCTV, 무인 잠수정 등 디바이스의 수와 종류는 폭발적으로 증대되고 있다. 이 부문에서 사이버전은 사이버 기술전과 사이버 심리전이 함께 나타난다. 사이버 기술전은 해킹, 디도스, 악성 바이러스 공격을 통한 디바이스 오작동, 탈취, 파괴 등으로 구현되는데 이때 전자전과 연계된다. 전자파 송출 또는 차단·방해를 통한 디바이스 탈취, 파괴, 오작동을 일으킬 수 있다. 사이버 심리전은 각종 디바이스들이 좀비 PC 형태로 가짜뉴스, 여론조작, 선전·선동, 극단주의 추종자 채용 등에 동원됨으로써 이루어진다. 이처럼 기계적인 방식으로 여론조작에 이용되는 좀비 PC[13]들을 '트롤봇(trollbot)'으로 부르기도 하며 국내에서는 드루킹 사건의 '킹크랩'으로 잘 알려져 있다.

셋째, ③에는 컴퓨터와 데이터베이스시스템, 스마트폰을 운영하는 소프트웨어(MS 프로그램과 MacOS, 안드로이드, iOS 등), 온라인 플랫폼(구글, 유튜브, 네이버, 다양한 SNS 서비스)이 해당한다. 또한, AI도 사람의 지능을 모방하는 소프트웨어이자 프로그램이기 때문에 여기에 해당한다. 이와 같은 소프트웨어와 프로그램은 사이버 기술전의 핵심 전장이다. 프로그램 침해와 탈취, 교란 등으로 인터넷 설비들과 각종 디바이스들의 오작동, 정지 등을 통해 경제적, 심리적, 사회적 피해를 유발하고 경우에 따라서는 미국과 이스라엘의 스턱스넷 공격처럼 물리적 피해까지 유도할 수 있다. 그리고 사이버 심리전과도 연관이 있다. 온라인 플랫폼은 가짜뉴스 유포와 댓글 조작, 여론선동과 프로파간다(Propaganda)[14]의 주요 수단이

13) 해커의 원격 조종에 의해 스팸을 발송하거나 DoS나 DDoS 공격을 수행하도록 설정된 컴퓨터나 서버. 봇(bot)이라 불리는 해킹 프로그램에 감염된 컴퓨터는 다른 사람에 의해 원격 조종될 수 있게 된다. 봇(bot)은 주로 채팅룸과 파일 공유 프로그램을 통해 PC를 감염시키는데, 봇(bot)에 감염된 PC는 직접적인 피해 증상이 나타나지 않아 사용자가 눈치채지 못하는 사이 스팸 메일 및 불법 프로그램을 유포하고, 정보를 유출하는 행위에 이용되게 된다. 한국정보통신기술협회 정보통신용어사전 참조; http://terms.tta. or.kr/dictionary/dictionaryView.do?word_seq=062073-2(검색일: 2023년 12월 7일).

14) 라틴어의 Propa-gatus에서 유래된 용어로 식물을 번성케 하기 위하여 접목을 붙인다는 뜻이 있으며 책임과 존경의 의미가 내포되어 있다. 사전적 의미는 어떤 것의 존재나 효능 또는 주장 따위를 남에게 설명하여 동의를 구하는 일이나 활동으로 주로 사상이나 교의

자 무대이다. 또한, 사이버 기술 및 심리 공격이 통합적으로 나타나기도 한다. 해킹을 통해 민감한 정보를 탈취하고 이를 뉴욕타임스(New York Times)와 같은 주요 미디어나 위키리크스(Wiki Leaks)와 같은 폭로 전문 채널을 통해 유포하여 여론을 선동하고 이를 다시 트롤봇과 인간 댓글부대를 이용하여 확산시키는 방법이다. 향후 인공지능의 발전으로 이와 같은 사이버 기술-사이버 심리 융합전은 더욱 정교해지고, 빨라지고 파괴적으로 될 것이다.

넷째, ④는 인터넷을 구성하는 기반설비와 디바이스들 그리고 무형의 프로그램들을 연결해서 인터넷이라는 가상현실을 구축하는 가상의 네트워크 체계와 규칙들이다. 도메인 네임 시스템(DNS; Domain Name System)과 IP 등과 관련된 각종[15] 규칙과 체계들, 가상 사설 통신망(VPN; Virtual Private Network)[16]과 클라우드 서비스와 관련된 가상의 인프라들 등이 이에 해당한다. 이와 같은 가상의 네트워크 체계와 규칙들은 사이버-기술전의 무대이며 공격-방어의 대상이. 또한, 사이버 국제 규범 질서 구축과 관련된 외교전(Diplomatic warfare)의 대상이자 공격-방어의 대상이다. 서방 국가들의 "자유롭게 개방된 하나의 글로벌 네트워크 공동체" 주장들과 러시아-중국의 "각국이 배타적으로 가상 네트워크 체계와 규칙들, 프로토콜을 통제하자는 국가 주권별로 분할된 디지털 베스트팔렌 체제" 주장들이 국제기구나 국제회의에서 충돌하고 있는 것은 이와 같은 맥락에서 이해될 수 있다.[17]

다섯째, ⑤는 인터넷 공간에서 생산, 소비, 유통되는 콘텐츠들을 모두

따위의 선전을 이른다. 『표준국어대사전』(2023).

15) CP/IP 애플리케이션에서, 'chollian.dacom.co.kr'와 같은 주 컴퓨터의 도메인 네임(domain name)을 '164.124.101.2'와 같은 IP 주소(Internet Protocol address)로 변환하고 라우팅 정보를 제공하는 분산형 데이터베이스 시스템. 한국정보통신기술협회 정보통신용어사전 참조; http://terms.tta.or.kr/dictionary/dictionaryView. do?word_seq= 041788-2(검색일: 2023년 12월 7일).

16) 공중망 상에 사설망을 구축하여 마치 사설 구내망 또는 전용망 같이 이용하는 통신망. 한국정보통신기술협회 정보통신용어사전 참조; http://terms.tta.or.kr/dictionary/dictionaryView. do?word_seq=059703-1(검색일: 2023년 12월 7일).

17) 윤민우, "미래 사이버 안보 경쟁과 중러 협력," 김상배 엮음, 『사이버 안보의 국가전략 2.0』(서울: 사회평론 아카데미, 2019), pp. 50-51.

포함한다. 여기에는 영상과 텍스트, 그래픽 정보가 모두 포함된다. 또한 미디어 보도나 논문, 보고서, 웹사이트의 정보들뿐만 아니라, 댓글, 해시태그, SNS상에서의 텍스트와 그래픽 등 다양한 유형이 모두 포함된다. 온라인비디오게임 역시 콘텐츠의 일종이다. 콘텐츠와 관련된 위협은 사이버 심리전에 해당한다. 하지만 최근 들어 콘텐츠를 찾는 데이터마이닝(Data mining)[18]과 AI 알고리즘, 머신러닝-딥러닝 등이 중요해지면서 사이버 기술전이 정보 콘텐츠 부문에서도 중요해졌다. 이 부문에서의 사이버전은 정보전(information warfare)과 중첩된다. 정보전은 정보의 흐름을 장악하고 통제하는 것과 관련된 전쟁이다.[19] 하지만 사이버 심리전은 정보의 흐름이 인간 사용자에게 미치는 영향까지 포함하는 개념이다. 정보전과 사이버 심리전이 중첩되지만 차별되는 부문은 사이버 심리전의 경우 온라인상에서의 콘텐츠에 한정되어 있지만, 정보전의 콘텐츠는 온라인뿐만 아니라 방송·통신·신문 등의 전통적 미디어의 정보들, 도서, 논문, 강의, 설교 등 다양한 오프라인에서 유통되는 정보를 모두 포함한다.

여섯째, ⑥은 인터넷 공간의 콘텐츠가 인간의 의식(perception) 영역으로 들어가 뇌에 의해 해석된 결과물, 그리고 이후의 인간 행동까지를 포함한다. 사이버 심리전과 인지전이 중첩되는 지점이면서 사실상 많은 부분이 인지전의 영역에 해당한다. 여기서는 콘텐츠뿐만 아니라 해당 콘텐츠를 소비하는 인간의 심리적, 성격적 특성들, 그리고 콘텐츠를 관찰하고 판단-결심-행동으로 이어지게 하는 뇌의 정보처리작용, 인간의 인지대본(script) 또는 습관까지가 모두 전쟁의 무대 또는 공격-방어의 대상이 된다. 최근 들어 뇌과학과 심리-설득지식의 급격한 발전으로 뇌파 조작, 기억 조작 등에 대한 기술적 개입의 개연성이 커지고 있다. 특히 AI는 이 부분에서도 게임체인저가 될 수 있다.

마지막으로 ⑦은 기반시설, 디바이스들, 콘텐츠들을 연결하는 무형의 정보통신과 전파 등이며 이와 관련한 위협은 사이버 기술전인데 전자전과

---

18) 대용량 데이터에서 의미 있는 통계적 패턴이나 규칙, 관계를 찾아내 분석하여 유용하고 활용할 수 있는 정보를 추출하는 기술. 한국정보통신기술협회 정보통신용어사전 참조; http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=040402-16(검색일: 2023년 12월 7일).

19) Bemal et al., "Cognative Wafare: An Attack on Truth and Thought", p. 19.

중첩된다. 전자전의 영역에는 무선통신과 라디오 통신, 적외선 유도 등이 포함된다. 이러한 전자전은 사이버 기술전 부문의 Wifi 데이터 송수신과 각종 기반시설, 디바이스, VPN 등에 개입을 통해 사이버 기술전과 중첩된다. 따라서 사이버 전자전(Cyber Electronic Warfare)은 사이버전과 전자전이 결합한 융합전쟁의 개념이다.[20] 예를 들면, 전자전과 사이버전의 대상 위협이 중첩되는 주파수 스펙트럼은 통신대역으로 식별되고 있으며, 해당 대역에서 '원거리 고출력 전자파 탐지·송출'로 대표되는 전자전 능력과 '정보(메시지) 조작·교란'으로 대표되는 사이버전 능력이 융합되고 있다. 따라서 두 기술이 시너지 효과를 발휘할 수 있는 사이버 전자전 기술로 발전시켜야 할 필요가 있다.[21]

요약하면, 사이버전은 사이버 기술전과 사이버 심리전로 구분될 수 이있다. 사이버전은 다른 비키네틱 전쟁양상인 전자전과 정보전, 심리전, 인지전 등의 여러 유사하게 중첩되면서도 구별되기 때문에 다른 전쟁 유형들과의 관계 속에서 이해되어야 한다. 또한 여러 유형의 비키네틱 전쟁들은 물리적 섬멸 및 파괴가 이루어지는 키네틱 전쟁과도 긴밀히 연관되어 있으며 외교전쟁, 국제규범전쟁, 경제전쟁, 문화전쟁과 같은 여러 다른 비군사적 안보이슈들과도 관련되어 있다. 따라서 사이버 안보 개념에 대한 이해는 이와 같은 개념의 확장과 다변화 속에서 이해해야 한다.

제 2 절 미래전의 발전추이와 사이버 안보의 비중

미래전은 아래의 그림과 같이 키네틱전과 사이버전, 전자전, 정보전, 그리고 인지전이 같이 중첩되고 융합된 방식, 즉 하이브리드 전쟁[22]이 진

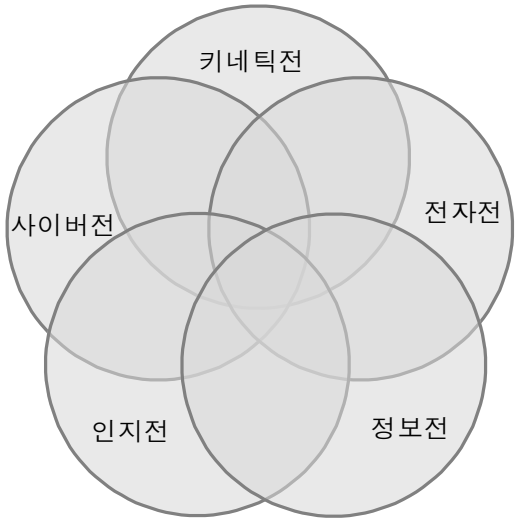
20) 김소연 외, "사이버전자전 기술 및 발전방향," 『한국전자파학회논문지』. 32(2), 2021, pp. 119-126.

21) Ibid, p. 123.

22) 송태은, "하이브리드 위협에 대한 최근 유럽의 대응," 『IFANS 주요국제문제분석』, 2020-31(2020), pp. 6-7.

행될 것으로 추정된다. 대체로 다른 전쟁형태와 중첩되지 않는 순순한 단일형태의 전쟁은 드물 것이며, 경우에 따라서는 모든 전쟁형태가 결합된 형태로도 전쟁이 전개될 것이다.

<그림 2-1> 전쟁형태들의 관계[23]



키네틱전은 지상-해상-공중-우주 공간에서 물리적 폭력의 충돌이며 핵전쟁까지 포함한다. 여기에 테러전이나 분란전, 또는 소규모 저강도 전쟁 역시 포함된다. 키네틱전은 키네틱 폭력이 사용되어 물리적 공간에서 살상과 파괴가 발생하는 모든 형태의 폭력적 충돌을 의미한다. 키네틱전을 제외한 나머지 네 가지 형태의 전쟁은 모두 비키네틱 전쟁에 해당한다. 이들 전쟁형태는 직접적인 물리적 살상·파괴가 발생하지 않는다는 점이다. 물론 이는 상대적인 개념이며 물리적 공간에서의 살상수단 또는 유·무인 전투체계를 통해 간접적인 방식으로 키네틱 살상-파괴 효과를 물리적 공간에서 구현할 수 있다. 예를 들면, 특정 개인에 대한 극단화의 인지조작을 통해 자발적인 폭력 공격을 유도하거나 적 드론 운영체계를 해킹하거나 탈취하여 적을 공격하도록 유도하는 것이다.

사이버전은 앞서 기술한 대로 사이버 기술전과 사이버 심리전을 합친

23) 윤민우·김은영, 『모든 전쟁: 인지전, 정보전, 사이버전, 그리고 미래전쟁에 대한 전략이야기』(서울: 박영사, 2023), p. 273.

개념이다. 전자전은 무형의 대기 중을 오가는 전파의 차단, 방해, 개입 등을 통해 물리적 피해를 일으키려는 것과 관련된 공격-방어이다. 이는 WiFi 등과 같이 사이버전과 관련이 있을 수도 있지만, 라디오, 방송 등 전통적인 무선통신과 관련이 있을 수도 있다. 정보전은 콘텐츠의 흐름을 통제하기 위한 일련의 공격-방어이다. 이는 사이버 공간의 콘텐츠를 포함하지만 오프라인상에서의 다양한 콘텐츠를 포함한다.

'인지전'이란 정보와 기타 수단을 활용하여 인간의 인지 능력·과정을 공격함으로써 표적이 되는 개인·집단의 인식과 사고방식을 변화시키고, 궁극적으로 그들의 의사결정과 행동을 변화시키는 전쟁[24]이다. 인간은 콘텐츠를 받아들이고 해석하는데, 받아들이는 과정을 인지(cognition) 과정으로 인지의 결과물을 인식(perception)을 정의할 수 있다. 인지전은 인간의 인지-인식이 이루어지는 뇌 영역이 전쟁 무대이며 인간의 인식을 조작함으로써 인간이 결심과 행동을 바꾸려는 것이 핵심적인 전략목표다. 따라서 여기에는 심리전 요소뿐만 아니라, 인간의 뇌 작용에 대한 신경생리학적 개입, 이민·난민 등의 인구구성 변화를 통한 영향력 확산, 광범위한 역사문화전쟁까지 넓게 인지전의 영역에 포함된다. 따라서 인지전은 사이버 공간상에서의 심리전을 포함할 뿐만 아니라 오프라인에서의 강의, 교육, 방송, 영화, 게임, 도서, 발표, 집회·시위, 테러·폭격 등 폭력적 공격, 군사적 기동, 핵미사일 실험, 뇌파 조작[25], 인구이동의 무기와 등을 포함한 일체의 내러티브(narrative) 전달을 담고 있는 영향력 투사를 모두 포함한다.[26]

미래전은 키네틱과 비키네틱 수단이 동시에 융합적으로 동원되는 하이브리드 전쟁으로 발전하고 있다. 적에게 나의 의지를 관철시키는 데는 키네틱 폭력뿐만 아니라 상대방의 의지를 직접 개입·왜곡·조작함으로서도 가능하다. 미래전은 키네틱 결전뿐만 아니라 선거 개입, 여론조작, 프로파간다, 극단주의 또는 테러리즘 유포·확산을 통한 정치 및 사회 혼란과 정부

24) 육군 교육사, 『미래 작전환경분석서』(서울: 육군교육사령부, 2022).

25) 전황수, "뇌-컴퓨터 인터페이스(SCI) 기술 및 개발 동향," 『전자통신동향분석』, 26(5), 2011, pp. 124-126.

26) Bemal et al., "Cognitive Warfare: An Attack on Truth and Thought," pp. 6-10.

전복, 사보타지, 사이버 기술공격을 통한 사회 혼란과 공포, 경제적·외교적 압박, 전자전을 통한 정보통신 네트워크의 블랙아웃, 정보전을 통한 시스템 마비 등 다양한 형태로 전개될 수 있다.[27]

미래전의 또 다른 트랜드는 인간-기계 결합 살상체계(kill-chain)의 등장이다. 인간 지휘관들은 점점 더 AI와 같은 지능형 기계들에게 전투지휘와 통제를 위임할 것이다.[28] 전투현장에서는 유인전투체계와 무인전투체계가 결합된 방식으로 운용될 것이다. 또한, 미래전은 공격능력의 분산, 취약성의 분산, 그리고 방어의 분산을 특성으로 한다. 국가의 정규군과 정보기관, 다른 정부 부문들, 그리고 비국가 행위자들을 포함한 다양한 인간-기계 공격자들의 이질적이고 비대칭적인 공격역량이 분산되어 전쟁이 수행될 것이다. 취약성은 국가의 전쟁지휘부와 민간인, 정보통신기반시설과 사이버 공간에서의 여론 등 매우 다양하고 분산되어 산재할 것이다. 이처럼 공격자와 공격능력이 다양하고 취약성이 다양하고 분산되어 있기 때문에 방어 역시 분산되어 운용되어야 할 필요가 있다. 따라서 공격-방어의 분산이 미래전의 특징으로 두드러질 것이다.

이와 같은 미래전의 특성들과 발전 추이 때문에 미래전은 지휘통제와 전투행동의 집중-분산을 동시에 달성해야 하는 도전에 직면해 있다. 미래전은 일원화된 중앙집중식 합동참모시스템의 지휘·통제·명령 체계로 감당하기에는 너무 이질적이고 비대칭적이며 복잡하고 전쟁의 국면변화와 전개 속도가 빠르다. 다영역 전쟁인 미래전에서는 각각의 전투 국면과 현장에서 즉각적인 감시-결심-대응의 전투 수행체계가 갖추어져야 한다. 따라서 각 전쟁영역에서 벌어지는 개별 전투현장의 개별 전투 집단의 자기주도(self-initiative) 전투수행 권한과 능력이 강화될 필요가 있다. 이는 지휘통제-전투 행동의 분산을 의미한다. 또한, 동시에 이와 같은 다영역에 분산된 자기 주도 전투 집단은 인간 지휘 컨트럴타워에 의해 전체 전쟁을 관통하는 핵심 내러티브와 전략목표의 방향성에 맞추어 조율될 필요

27) 윤민우·김은영, 『모든 전쟁: 인지전, 정보전, 사이버전, 그리고 미래전쟁에 대한 전략이야기』(서울: 박영사, 2023), p. 262.

28) Christan Brose, The Kill Chain: Defending America in the future of High-Tech warfare,(New York: Hachette Book, 2020), pp. 128-129.

가 있다. 이와 같은 실시간적인 집중-분산 구현에 있어서 AI와 사이버 공간을 통한 전투현장과 전쟁지휘부와의 초연결성 구축, 정보처리능력과 속도의 강화, 그리고 AI의 알고리즘과 딥러닝을 통한 지휘부와 유·무인 전투지휘체계에 대한 쌍방향 동시 지원 등이 대안으로 제기되고 있다.

이와 같은 미래전 발전 추이와 사이버 안보는 밀접히 관련되어 있으며, 그 비중과 관련성 역시 매우 크다. 이는 다음과 같은 이유들 때문이다. 첫째, 사이버전은 다른 유형의 키네틱 전쟁과 비키네틱 전쟁형태와 밀접히 관련되어 있다. 예를 들면, 키네틱 전쟁에서 물리적 전투력의 투사는 사이버 공격 때문에 영향을 받을 수 있다. 또한, 사이버전 능력은 힘의 증대 효과를 가져와 기존 키네틱 전투력을 극대화할 수 있다. 또한, 사이버 공간의 콘텐츠와 플랫폼들, 그리고 AI와 메타버스(Metaverse)[29], 뇌파 조작과 관련된 기술들은 인지전의 주요한 수단이자 무대로 활용된다. 대부분의 오프라인 콘텐츠들이 온라인으로 이동하고 있는 추이를 감안할 때, 점차 인지전의 무대는 사이버 공간이 되고 있다. 전자전 역시 사이버전이 결합되면서 전자전의 파괴력과 효용성이 증대했다.[30]

둘째, 인간-기계 결합 살상체계를 구동하기 위해서는 하드웨어와 소프트웨어를 포함하는 사이버 인프라 확보가 핵심적이다. 유·무인 전투차량, 유·무인 전투함정 및 잠수함, 유·무인 항공기 등과 개인용 모바일 디바이스, 컴퓨터 등으로 연결된 유인전투원, 로봇 등은 인터넷을 통해 서로 결박된다. 따라서 사이버 위협으로부터 이들 유·무인 전투체계를 구동하는 운영프로그램의 안정성이 확보되어야 한다. 또한, 이와 같은 인간-기계 결합 살상체계의 안정적 결박과 통합운용을 지원하기 위한 위성과 케이블, 고출력 WiFi 송·수신기기, 대용량 정보의 소통·처리·저장 시스템 등을 포함한 정보통신 네트워크의 안정적 운용환경구축, 그리고 이를 지원하기 의한 전력(에너지)의 원활한 확보와 공급 등이 고려되어야 한다.

셋째, "인간 지휘부-AI-전투단위"를 결박하고 운용하는데 사이버 공

29) 현실에서 가능한 사회, 경제, 교육, 문화, 과학기술 활동을 아바타(avatar)를 통하여 할 수 있도록 지원하는 가상의 3차원 공간 플랫폼. 한국정보통신기술협회 정보통신용어사전 참조; http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=048870-4(검색일: 2023년 12월 7일).

30) 김소연 외, "사이버전자전 기술 및 발전방향," 『한국전자파학회논문지』. 32(2), 2021, p. 123.

간은 핵심연결 통로이다. 작전계획을 발전시키고 임무 명령을 하달하는 인간 지휘부와 지상군부대, 탱크, 전투함정, 항공 스트라이커 그룹, 드론, 미사일, 위성 등 전투 임무를 수행하는 개별 유·무인 전투단위들, 그리고 임무 수행을 위한 단위요청과 가용한 능력기반 킬체인을 구성하는 AI 기반 기계 보조 통제의 3축 간의 연결은 사이버 또는 사이버-전자 수단을 통해 이루어진다. 이처럼 사이버 공간 또는 사이버 수단은 다양한 측면에서 미래전 수행의 중심적 위치에 있다.[31]

제 3 절 심리전과 사이버 심리전의 개념과 특성

1) 심리전의 개념과 특성

심리전(Psychological Warfare)라는 용어는 1920년 영국의 군사평론가이자 역사가인 풀러(J. F. C. Fuller)의 "세계대전에서 탱크의 역할"이라는 논문에서 최초로 사용되었다. 풀러에 따르면 심리전(a purely psychological warfare)이란 타인 또는 타민족의 의지를 왜곡하는 것으로서 인간 이성의 부패, 지성의 훼손, 도덕과 영적 생활의 붕괴를 유도하는 방법이다(Fuller, 1920, p. 320). 이후 1948년 미국의 심리학자 라인버거(Paul M. A. Lineberger)는 심리전에 대한 광의의 개념은 "정치적, 경제적 또는 군사적인 모든 조치의 효과를 촉진하기 위하여 심리학을 전쟁 수행에 적용한 것"이며 협의의 개념은 "군사적 수단과 함께 선전을 이용하는 전쟁"이라고 하였다[32]. 즉, 전쟁(war)의 구체적인 양상, 형태로서 군사활동(전, warfare)으로서 정의하였다.

하지만 현대사회에서는 심리전의 사용 주체가 국가나 군대뿐만 아니라 일반 기업체나 스포츠, 인간 개개인의 관계까지 널리 활용되고 있으므로

31) 남두현 외, "4차산업혁명 시대의 모자이크 전쟁: 미군의 군사혁신 방향과 한국군에 주는 함의," 『국방연구』. 제63권 제3호, 2020, pp. 161-163.

32) Paul M. A. Linebarger, Psychological Warfare (Washington, D. C: Combat Forces Press, 1954), p. 25.

전쟁의 형태로 한정하지 않고 현대사회에서 사용되는 정치·경제·사회·군사적인 제반 심리적 활동으로 이해해야 한다. 따라서 심리전의 개념은 인간 개인의 심리라든지 집단 심리의 자극과 반응 관계의 원리에 기초를 두고 있으며 대적 관계뿐만 아니라 대내 관계까지 포함해서 이해되어야 한다. 즉 심리전은 전시, 평시를 막론하고 적이나 자국민, 국제사회에 국가목적을 달성하기 위하여 국가정책 및 전략을 수행하는 데 유리한 감정과 태도, 행위를 조성하기 위하여 사용되는 계획적인 정치, 경제, 사회, 문화 등 군사적인 제반의 심리전 활동이라고 정의할 수 있다.

그런데 평시에도 수행되는 심리전은 반드시 군사 활동을 동반하는 것이 아니므로 상당히 복잡한 성격을 갖는다. 심리전은 적국보다 정보의 우위를 점하는 정보전(information warfare)의 성격과 적국 대중의 여론에 개입하려는 정치전(political warfare)의 성격도 갖는다. 심리전이 정보커뮤니케이션기술(information & communication technology, ICT)을 이용한 정보활동을 넘어 경쟁국의 여론을 관리하거나 개입하는 활동도 펼치므로 미국이나 영국은 2000년대 초부터 보다 포괄적인 '전략커뮤니케이션(strategic communication, SC)'의 개념으로 심리전을 다루기 시작했다.

'전략커뮤니케이션'이란 '해외의 핵심 청중을 이해하고 이들에게 개입하여 국익과 국가정책 및 목적을 이루는데 유리한 조건을 구축하기 위한 국가 활동'이다. 즉 전략커뮤니케이션은 해외대중에게 자국이 전달하려는 정보를 알리고 이들의 생각이나 태도, 행동에 영향을 끼치려는 국가 커뮤니케이션 활동이다. 국가의 전략커뮤니케이션 활동에는 프로파간다(propaganda) 활동, 군사작전으로서의 '심리작전(psychological operations, PSYOP)'과 비군사적 외교활동인 '공공외교(public diplomacy)' 및 '공공문제(public affairs) 관리'까지 포함한다.[33] 보다 공식적이고 전문적 맥락에서 '심리전' 용어는 '전략커뮤니케이션' 용어로서 사용되며, '군사활동으로서의 심리전'을 특정적으로 일컬을 경우 심리전은 군 조직의 '작전(operations)'으로서 수행되

33) Kirk Hallahan, Derina Holtzhausen, Betteke van Ruler, Dejan Verčič & Krishnamurthy Sriramesh, "Defining Strategic Communication." International Journal of Strategic Communication 1-1(2007), pp.3-35; James P. Farwell, Persuasion and Power: The Art of Strategic Communication. Georgetown University Press, 2012), pp. 1-53.

므로 '심리작전' 혹은 간단히 'PSYOP'으로 불린다.

19세기 인쇄술과 근대의 다양한 미디어의 발명으로 세계 대중의 읽고 쓰는 능력이 증대하면서 국가가 주도하는 프로파간다 활동은 국가의 메시지를 국내외 대중에게 전달하는 효과적인 도구가 되었다. 양차 대전기 국가 프로파간다 활동은 라디오, 신문, 텔레비전 등 다양한 미디어를 통해 군인을 징집하고 대중의 단합된 전쟁 여론을 구축하는 과정과 긴밀하게 맞물려 왕성하게 수행되었다. 전쟁 중 참전국 대중의 적대국에 대한 증오는 프로파간다가 효과적으로 작동하는데 유용한 '감정' 변수이다. 증오의 대상이 명확하고 대상에 대한 고정관념(stereotype)이 강화될 때 프로파간다 메시지는 설득력을 발휘한다. 그러므로 불확실성이 고조되는 전쟁 기간의 프로파간다는 적대국의 야만성과 폭력성을 과장하고 국가가 겪는 여러 어려움의 원인을 적국에 전가하는 방식으로 국가의 전쟁 수행을 대중이 지지하게 하는 역할을 했다.[34]

학자에 따라서 프로파간다의 정의가 조금씩 다른 것은 주로 양차 세계대전기 두드러졌던 프로파간다의 역할에 기인하는 경우가 많다. 예컨대 테일러(Philip Taylor)는 프로파간다를 '발신자의 이익에 봉사하도록 설계된 메시지나 이념을 커뮤니케이션을 통해 전달하는 것'으로 정의하였다. 그리고 전시(wartime) 프로파간다는 아군으로 하여금 '싸우도록' 설득하는 것이고 '심리전(psychological warfare)'은 적이 아군과 '싸우지 않도록' 설득하는 것이라고 프로파간다와 심리전을 구분했다.[35] 하지만 현대 전쟁 연구에서 '프로파간다'와 심리전의 군사용어인 'PSYOP'은 자국 대중이 아닌 오로지 타국 전투원과 대중만을 상대로 하는 국가 활동으로 언급된다. 미국 국방성의 PSYOP 부대는 해외대중이나 타국 전투원만을 목표 청중으로 삼고 있음을 적시하고 있고 1948년 美 의회의 스미스-먼트법(the Smith-Mundt Act)에 의해 PSYOP의 목표 청중에서 국내 청중을 제외시켰다. 미국과 영국 등 서구 민주주의 선진국에서 PSYOP은 철저하게

34) David Welch, Propaganda, Power and Persuasion: From World War I To Wikileaks (London & New York: I.B. Tauris, 2015), pp. 37-61.

35) Philip M. Taylor, Munitions of the Mind: War Propaganda from the Ancient World to the Nuclear Age (Wellingborough: Patrick Stephens Ltd, 1990), p. 13.

해외청중만을 대상으로 한다.

제2차 세계대전 종식 후 美 의회에서는 전시에 전개한 해외방송을 통한 프로파간다 활동을 지속하는 것에 대한 회의론이 있었다. 하지만 냉전기에도 수행된 소련의 정교한 프로파간다 활동으로 인해 美 의회는 평시에도 프로파간다 활동이 필요하고 정당함을 인정했다. 자유 진영과 공산 진영이 치열한 '이념전쟁(war of ideas)'을 치른 1950년대부터 1980년대까지 국가 프로파간다 활동은 양 진영의 군사, 정치, 경제체제 및 과학기술과 문화 전반의 우월함을 상대 진영에 선전하는 것이었다. 그런데 데탕트(détente)를 거쳐 탈냉전에 이르러 미국 학계는 프로파간다의 부정적 이미지를 상쇄하고 해외청중에 대한 국가의 설득전략을 새롭게 정의하기 위해 '공공외교'의 개념을 정립했다. 미국 학계는 양차 대전과 냉전기 체제경쟁과 이데올로기 대립에서 비롯된 프로파간다 활동으로부터 공공외교를 차별시킴으로써 미국 정부가 추구하는 외교정책과 국제정치 질서를 합리화하고 미국이 내세우는 세계적 아젠다(agenda)에 명분을 제공하는 역할을 했던 것이다.[36]

공공외교와 프로파간다는 국가가 해외여론에 대해 적극적으로 영향을 끼치려 한다는 점에서 유사해 보인다. 하지만 공공외교는 메시지의 '신뢰성(credibility)'을 통해 세계 대중의 '마음과 생각을 얻어(winning hearts and minds)' 설득하는 반면, 프로파간다는 기만 혹은 허위일 필요는 없으나 '진실'일 필요도 없다. 프로파간다의 주요 목적은 메시지를 유포하는 주체의 의도와 이익을 '효과적'으로 전달하는 것이므로 거짓이나 악의적 메시지도 프로파간다의 내용이 될 수 있다.[37] 즉 프로파간다는 왜곡된 정보와 정확한 정보를 구분하지 않는다. 따라서 정확한 정보의 확산 활동은 '백색선전(white propaganda)', 출처와 정확도가 애매한 경우 '회색선전

---

36) 1965년 美 터프츠 대학(Tufts University)의 머로우 센터(Edward R. Murrow Center of Public Diplomacy)는 공공외교를 "외교정책의 구축과 실행과 관련한 대중의 태도에 영향을 주는 활동"으로 정의했다. Nicholas J. Cull, "Public Diplomacy before Gullion: The Evolution of a Phase" In Nancy Snow and Philip M. Taylor (eds.), Routledge Handbook of Public Diplomacy (New York & London: Routledge, 2009), p. 19.

37) Richard A. Nelson, A Chronology and Glossary of Propaganda in the United States. (Westport, CT: Greenwood Press, 1996), pp. 232, 338.

(gray propaganda)', 거짓정보의 유포는 '흑색선전(black propaganda)'으로 불린다.

자국 메시지의 신뢰성을 가장 중시하는 미국 국방성은 프로파간다를 '메시지 발신자의 이익을 위해 특정 그룹의 의견, 감정, 태도, 행동에 직·간접적으로 영향을 주도록 고안된, 메시지 수신자에게 편향된(biased) 인식을 심어 호도하는(misleading) 것을 목표로 하는 적대적 커뮤니케이션'으로 정의하고 있다.[38] 이렇게 미국 정부가 프로파간다를 부정적으로 정의함으로 동일한 국가 심리전 활동이라도 '프로파간다'는 적군이 수행하는 것이고 아군이 전개하는 심리전 활동은 '심리작전(PSYOP)'으로 일컫는다. 이러한 명칭의 차이는 기본적으로 '적군은 거짓말을 말하고 아군은 진실을 말하는 것'으로 간주하는 것이다.[39] 이를테면, A국가 군의 입장에서 적국인 B국가 군의 PSYOP은 프로파간다 활동이다. 그러므로 미국, 영국 등 서구 민주주의 국가는 국가 전략커뮤니케이션에서 프로파간다 활동을 제외한다.

PSYOP과 공공외교를 포괄하는 전략커뮤니케이션의 역할은 자국에 대한 신뢰성(credibility)과 정당성(legitimacy)은 증진 시키고 적의 신뢰성과 정당성은 약화시켜 해외청중이 자국이 추구하는 정책을 지지하게 하고 경쟁국이나 적국도 자국이 원하는 행동을 취하게 하는 것이다.[40] 결국 전략커뮤니케이션의 시각에서 PSYOP은 군사영역에서 소프트파워를 발휘하는 활동이다. 같은 맥락에서 나이(Joseph Nye)는 오늘날의 분쟁에서는 "누구의 군대가 이기는가보다 누구의 이야기가 이기는가가 중요하다(it is not whose army wins, but whose story wins)"라고 언급한 바 있다.[41] 그러므로 전략커뮤니케이션의 시각으로 볼 때 9·11 테러 이후 미국은 이

38) Joint Publication 3-13.2. "Psychological Operations." US Department of Defense (January 7, 2010). www.fas.org/irp/doddir/dod/jp3-13-2.pdf(검색일: 2016.12.4.).

39) James P. Farwell, Persuasion and Power: The Art of Strategic Communication. Georgetown University Press, 2012, pp. 25-26.

40) U.S. Department of Defense, "Strategic Communication: Joint Integrating Concept." Washington D.C. (2009), pp. 7-8.

41) Joseph S. Nye, "The Information Revolution and Soft Power." Current History 113-759, 2014), pp. 19-22

슬람권에 미국의 전략적 내러티브를 전달하는 데에 완전히 실패한 것으로 평가된다.[42] 아프가니스탄전과 이라크전 이후 반미감정이 9·11 테러 전보다 세계적으로 더 고조되고 확산되었기 때문이다.

정치학에서의 여론연구, 심리학, 군사학, 경영학, 사회학 등 다양한 학문영역에도 적용되고 있는 전략커뮤니케이션(SC)라는 개념이 군사안보 분야에서 과거보다 중요해진 것은 군사안보와 외교의 전략적 환경이 근본적으로 달라졌다는 세계 각국 정부의 인식과 연결되어 있다. 초연결된 인터넷과 소셜미디어의 대중화로 인해 전 세계적으로 확산·유통되고 있는 정보의 양과 유통속도가 비약적으로 증대함에 따라 각종 군사안보 사안들은 국내·외의 정치적 쟁점이 되기 쉽고 상호 경쟁 및 충돌하는 군사안보 분야의 정보가 쉽게 확산되면서 각국의 전략적 입지를 제한할 수도 있다. 여론이 쉽게 활성화될 수 있는 이러한 정보환경에서는 심리전의 전략적 가치와 효과가 높아지므로 국가도 상당히 복합적인 커뮤니케이션 전략을 구사하게 된다. 이를테면 PSYOP은 특정 지역이나 청중을 대상으로 단기간에 특정 이슈를 다루면서 기밀 유지를 중시하지만, 공공외교는 지역 전체 혹은 한 국가 전체를 대상으로 보다 장기적으로 긍정적인 국가 관계 형성과 타국 대중과 열린 소통을 추구한다.[43]

한편, 한국의 합동교리에서도 '심리전' 또는 '심리작전' 용어를 '군사정보지원작전(MISO; Military Information Support Operation)'으로 변경[44] 하면서 국가정책 및 군사작전의 목표달성을 위하여 선정된 정보를 조직적이고 계획적으로 표적 대상에게 전달하여 주최 측이 의도하는 방향으로 상대 국가, 단체와 개인의 견해, 감정, 태도, 행동의 변화를 유도하는 작전'이라고 정의하였다.[45] 또한, 군사정보지원작전을 운용, 표적 대상, 출

---

42) David Betz, "Failure to communicate: Producing the war in Afghanistan" In D. Richards and G. Mills (eds.), Victory Among the People: Lessons from Countering Insurgency and Stabilizing Fragile States (London, 2011), p. 140.

43) Farwell(2012), p. 52

44) 합동참모본부. (2022), 합동교범 3-14『합동군사정보지원작전』. p. 1-1. "전쟁의 한 형태이면서 포괄적 의미로 사용했던 심리전(Psychological Warfare)의 용어와 전·평시 지속적인 운용의 필요에 따라 사용했던 심리작전(Psychological Operations) 용어 대신 군사정보지원작전(MISO, Military Information Support Operations)이라는 용어를 사용"

45) 합동참모본부. (2022). 합동교범 3-14 『합동군사정보지원작전』. p. 1-1.

처, 매체에 따라 아래 <표 2-2>와 같이 12개로 분류하였는데 미국의 PSYOP처럼 적국이나 해외 우방국이나 중립국만을 목표로 삼고 있음을 적시하고 있다.

<표 2-2> 한국군 군사정보지원작전 분류[46]

구 분	내 용
목적	● 전략적 군사정보지원작전 ● 작전적 군사정보지원작전 ● 전술적 군사정보지원작전
표적 대상	● 대적 군사정보지원작전 ● 대외 군사정보지원작전
출 처	● 백색 군사정보지원작전 * 출처 분명(제시) ● 흑색 군사정보지원작전 * 출처 모방 또는 도용 ● 회색 군사정보지원작전 * 출처 불분명
매 체	● 인쇄매체 : 신문, 전단, 화보, 유인물 등 ● 방송매체 : TV, 라디오, 확성기 등 ● 정보통신매체 : 인터넷, 스마트폰, 전화, 팩스 등 ● 기타 매체 : 시간, 인간접촉, 시청각 매체 등

2) 사이버 심리전의 개념과 특성

앞에서 살펴보았듯 사이버전은 사이버 기술전과 사이버 심리전을 합친 개념이다. 사이버 기술전은 컴퓨터 네트워크의 하드웨어와 소프트웨어에 대한 기술적 방식의 공격-방어를 의미한다. 이를 위해 악성 소프트웨어가(malicious software) 무기로 이용된다. 사이버 심리전은 사이버상의 인간 사용자들의 생각과 정서, 심리에 영향을 미치려는 것과 관련된 일련의 공격-방어이다. 이를 위해 악성 정보(malicious information)가 무기로 이용된다.[47]

허태회(2010, p. 31)는 사이버 심리전이 정보전의 한 형태로 가상의

46) 합동참모본부. (2022). 『합동교범 3-14 『합동군사정보지원작전』. pp. 1-12.

47) 윤민우·김은영, 『모든 전쟁: 인지전, 정보전, 사이버전, 그리고 미래전쟁에 대한 전략이야기』(서울: 박영사, 2023), p. 24.

사이버 공간에서 심리전 목표를 달성하기 위해 수행되는 첨단 심리전의 형태로 정의하였다. 또한, 사이버 심리전은 전통적으로 오프라인에서 수행되던 심리전의 전장을 사이버 공간이라는 시간과 공간의 제약을 받지 않은 새로운 전장으로 확장시켰다고 평가하였다. 하지만 사이버 심리전은 전통적인 심리전과 달리 방법과 수단이 사이버 공간에 종속되어 있다. 사이버 기술발전 속도는 사이버 심리전의 발전도 가속화시킬 수 있으며, 이에 대한 대응도 사이버 기술을 기반으로 수행해야 효율적이다. 이처럼 사이버 심리전은 '사이버 공간'에서 이뤄지는 '심리전 활동'으로 관점에 따라 '심리작전'과 '사이버 작전'의 범주 모두에 포함될 수 있는데, 이에 대한 논의도 지속되고 있다.

사이버 심리전의 효과는 국가 정보통신기반의 발달과 사이버 심리전 대상의 정보통신기술 의존도를 통해 극대화된다. 사이버 심리전은 2000년대 인터넷의 보급과 함께 본격적으로 확대되었다. 자유민주주의 국가에서는 법에 근거하지 않은 인터넷 통제를 할 수 없으며, 누구나 인터넷을 이용한 여러 가지 수단[48]으로 자유롭게 개인의 의견을 제한 없이 피력하고, 다른 이의 의견 또한 전파할 수 있다. 정보통신기술의 발달에 따라 정보의 생산과 유통의 제약은 크게 줄어들고 있다. 따라서 잘못된 정보일지라도 정부의 규제를 받지 않고 개인에게 얼마든지 전파될 수 있다. 누구나 유튜브 등을 통한 방송/영상매체 전달 수단으로 허위조작정보(disinformation)'[49]을 생산하여 유포할 수 있다. 어느새 대중에게 일반명사로 인식되고 있는 '팩트체크(Fact check)'란 말은 이러한 허위조작정보에 대한 불안감과 불신이 가져온 사회적 현상일 것이다.

사이버 심리전은 기존의 전통적 심리전의 단순한 확장으로만 볼 수 없는 아래 <표 2-3>와 같은 명확한 특징을 가지고 있다.

---

48) 개인방송(유튜브, 아프리카TV 등), SNS(Social Networking Service), 댓글 달기, 블로그(Blog) 등.

49) 해외 주요국가에선, 가짜뉴스, 즉 '페이크 뉴스(fake news)'란 단어의 의미가 불분명하기 때문에 허위조작정보, 즉 '디스인포메이션(disinformation)'이라는 개념으로 대응하고 있음. 한국 정부도 '허위조작정보'라는 개념을 정립하여 다양한 해결책 마련에 노력 중임. '허위조작정보'는 악의적 의도를 가지고 명백한 사실관계를 조작한 정보라는 뜻임(한상혁 방송통신위원장,'19년 10월 청와대 국민청원 답변).

<표 2-3> 전통적 심리전 대비 사이버 심리전의 특징

구 분	전통적 심리전	사이버 심리전
효과 피드백	제 한 (일방형적 정보이동)	가 능 (양방형적 정보이동)
경제적· 시간적 비용	상대적으로 높음	상대적으로 매우 낮음
제약 요소	많 음 (물리적 공간 필수)	없 음 (물리적 공간 불필요)
주체에 대한 법적 제재	용 이	극히 제한 (주체 은닉·위장 용이)
심리전에 대한 대응	적극적 대응 가능	극히 제한 (추적·증거확보 제한)

우선, 전통적인 심리전의 특징부터 살펴보면, 첫째, 효과에 대한 피해평가를 위한 피드백을 받기 어렵다. 전통적인 심리전 수단은 전단 살포나 확성기, 라디오 방송 등 발신자에서 수신자까지의 정보이동이 일방향적이어서 수신자의 피해 여부와 범위, 효과를 분석 및 피드백하여 방법과 수단을 보완할 수 없다. 둘째, 전통적 심리전은 그 수단을 제작하는데 경제적, 시간적 비용이 반드시 발생한다. 전단지 제작, 인력 동원, 전파수단 구축에 들어간 비용은 이를 통해 얻게 되는 효과가 명확하지 않기 때문에 투입의 가치를 따져보기 힘들다. 셋째, 물리적인 공간을 활용하기 때문에 이에 따른 수 많은 제약이 따를 수밖에 없다. 넷째, 행위자가 비교적 명확하기에 제네바 협약 등 전쟁 관련 국제법에 대한 규제법 적용이 용이하다. 마지막으로 심리전 대상 상대 국가는 심리전에 대한 적극적인 대응이 가능하다. 이는 한국의 탈북단체들의 전단 살포에 대한 북한의 대응을 보면 명확하다.

이에 반해 사이버 심리전의 특징은 우선, 인터넷 댓글, 접속자 및 트래픽 분석을 통해 정보이동이 양방향적이어서 피해평가를 위한 즉시적인 피드백을 받을 수 있다. 정보가 특정 개인에게 미치는 심리적 영향력 정도는 “좋아요” 추천과 “팔로워”나 “구독자”의 수, 미디어 보도에 대한 댓글이나 온라인 커뮤니티에서의 논쟁, 그리고 즉석 온라인 여론조사 등으로 거의

실시간으로 파악이 가능해졌다. 더욱이 AI 알고리즘을 통해 유튜브나 뉴스, 쇼핑 등 디지털 정보를 이용하는 이용자들의 성향과 선호도 등을 거의 실시간으로 파악할 수 있어 심리전 효과의 실시간 피드백은 더욱 쉬워지고, 정교해지고 빨라졌다. 둘째, 사이버 심리전을 위한 수단이 다양[50]하고 보편적이라서 시간적, 경제적 비용 부담이 상대적으로 적다. 셋째, 사이버 공간을 이용하기 때문에 공간적 제약이 없다. 넷째, 사이버 심리전의 주체는 행위에 대한 부인이 용이하기 때문에 법적 규제가 거의 불가능하다. 마지막으로, 사이버 심리전에 대한 상대국의 추적과 증거확보가 어렵기 때문에 사전 대응, 방어, 보복, 반격이 곤란하다.

또한, 사이버 심리전은 AI 기술과 접목되어 더욱 고도화되고 지능화되고 있다. AI는 '딥러닝(deep learning)'을 통해 내러티브를 이해하고 스토리텔링 기술을 구현하며 다양한 심리 전술을 펼칠 수 있다. 예컨대 '정치봇(political bots)'으로 불리는 AI 알고리즘인 소셜봇은 온라인 공간에서 특정 정보를 집중적으로 확산시켜 특정 이슈만이 언급되게 하여 소위 '반향실효과(echo chamber effect), 필터버블(filter bubble)'효과와 다양한 '봇 효과(bot effect)'를 부추기고 강화시킬 수 있다. 소셜봇은 인지심리학이나 커뮤니케이션학에서 발전시킨, 설득효과가 입증된 고도의 심리적 기제가 적용된 내러티브를 사용하며, 그러한 정보를 봇부대(bot army)를 통해 실시간으로, 대규모로 확산시킬 수 있다.[51] 최근 AI의 정보조작기술 중 가장 고도화된 '딥페이크(deep fake)' 기술은 AI 알고리즘을 이용하여 동영상 원본에 등장하는 사람을 다른 사람으로 편집하여 마치 영상 속 인물이 실존하는 것처럼 조작할 수 있다. 이러한 딥페이크는 진위 여부를 식별하기 가장 어려운 종류의 허위조작정보를 제작하는 데 사용된다.[52] 결과적으로 첨단 AI 기술이 사이버 심리전에 적용되면서 비인간 행위자를

---

50) 정보생성을 위한 인적자원만 확보하면, 정보전달을 위한 경로인 인터넷을 통해 SNS, 블로그, 댓글 등으로 신속하고 지역과 관계없이 불특정 다수나 특정 그룹에 제한 없이 정보를 전파할 수 있다.

51) 송태은, "디지털 허위조작정보의 확산 동향과 미국과 유럽의 대응," 『IFAN 주요국제문제분석』, 2020-13, 국립외교원 외교안보연구소(2020a), pp. 20-21.

52) 송태은, "디지털 시대 하이브리드 위협 수단으로서 사이버 심리전의 목표와 전술 : 미국과 유럽의 대응을 중심으로," 『세계지역연구논총』, 39(1)(2021), p. 86.

통해서도 자동화된 디지털 프로파간다를 활동을 수행할 수 있게 되었다.

<표 2-4> 편향된 커뮤니케이션 효과와 심리전의 설득기재

반향실 효과(echo chamber effect)[53]	봇 효과(bot effect)
유사한 관점·생각을 가진 사람끼리 반복 소통하여 편향된 사고가 고착화되어 동의하는 의견만 수용하는 현상	정치적으로 편향된 정보와 메시지를 대규모로 확산시켜 여론이 특정 방향으로 유도되게 하는 현상
필터버블 효과(filter bubble effect)	트롤링(trolling)
사용자에게 AI 알고리즘에 의한 맞춤형 정보만 제공하여 사용자가 마치 거품에 가둬진 것 같은 현상[54]	타인의 강한 감정적 반응을 유발하기 위해 적대감이나 화를 부추기거나 혹은 거짓 비난의 글을 온라인 공간에 의도적으로 게시하는 행위
정보의 양(volume)에 의한 효과	진실착각효과(the illusory truth effect)
● 서로 다른 정보원이 제공하는 정보가 일치하거나 서로 다른 논쟁이 동일한 결론에 이를 경우 사람들은 정보의 질(quality)보다 동일한 결론에 이른 정보의 양(volume)을 더 중시	동일한 거짓 메시지에 반복 노출될 경우 사람들은 그러한 메시지를 신뢰함. 즉, 처음 접한 출처가 불분명한 정보라도 시간이 경과 하면서 정보 자체만을 기억하여 사실로 착각하는 경향을 보임.
	비전통적 설득전략
● 정보가 풍부한 환경에서는 다수가 인정하는 정보를 전문가의 의견보다 더욱 신뢰	거짓으로 밝혀진 정보를 재사용하거나 또 다른 거짓 정보를 수정된 정보로 제공하는 등의 전략

* 출처 : 송태은(2020a), pp. 21, 24

이러한 사이버 심리전의 특징은 향후 사이버 심리전의 범위와 능력이 제한 없이 확장될 수도 있다는 점과 정보화 환경이 발달된 국가일수록 상대적으로 사이버 심리전에 대한 취약성을 내포하고 있음을 암시한다. 사이버 공간을 활용하는 기술의 발전은 전장 영역을 확장 시켰고, 사이버 공간에 대한 우세확보가 전쟁 승패의 중요한 요소가 될 것이다. 따라서 정보통신기술이 발달 될수록 사이버 심리전이 더욱 증가할 것이며, 이는 전·평시와 군사·비군사 등 시간과 분야를 가리지 않을 것이기 때문에 사이버 심리전에 관한 역량의 확보는 필수적이라고 할 수 있다.(Eom et al. 2012, p. 298).

53) kathleen H. Jamieson and Joseph N. Cappella, Echo, chamber: Rush Limbaug and the conservative media establishment(Oxford University Press. 2008), pp. 75-78.

54) Eli Pariser, The Filiter Bubble (New York: The Penguin Press, 2011), p. 2.

제 4 절 사이버 심리전 사례와 전술

1) 사이버 심리전의 등장과 주요 사례

최초의 사이버 심리전 사례는 코소보 사태(1999)에서 찾아볼 수 있다. 코소보사태는 세르비아 대통령이 코소보 지역을 세르비아에 합병시키려고 하자, 코소보는 이에 반발하여 무력으로 시위하였고, 1998년 세르비아군과 코소보 해방군 간의 무력충돌로 인해 미국과 NATO 공군까지 참여하는 국제전으로 확대된 사건이다. 세르비아 정부는 코소보 해방군에 대한 대규모의 소탕 작전을 펼치며 비무장한 알바니아인들까지 대량으로 학살하였고 이에 NATO는 세르비아를 공습하면서 사이버 심리전이 전개되었다. 세르비아는 사이버 공간을 통해 국제사회에 NATO 공습의 부당함과 오폭에 의한 민간인 피해 사실을 적극적으로 전파하였고, 이에 미국과 NATO는 공습의 정당성과 세르비아의 민간학살에 대한 사실을 알림으로써 유고연방과 국제사회에 대한 우호적인 여론을 조성하고자 하였다.

또한, 이슬람 무장단체들은 서방 국가들에 비해 자금력이 열세인 상황을 사이버 심리전 전개를 통해 극복하고자 한다. 전 세계를 대상으로 인터넷을 통한 체제선전 및 조직원 선발, 그리고 사상 교육을 통한 외로운 늑대형 테러를 유발하고 있다. 알카에다 조직의 알 자르카위는 인터넷을 통한 사이버 심리전의 중요성을 깨닫고 2004년 이라크 저항세력의 훈련 및 종교적 장면, 서방세력 인질들의 참수 장면 등을 담은 동영상을 유포하였다.[55] 이는 수 많은 이슈와 함께 중동지역의 결속과 반미정서를 조성하였으며, '트프와트 알 시남'이라는 인터넷 뉴스를 제작하여 지하드 종교의 정당성을 전파하는 등 전문가 못지 않은 홍보 효과를 이루었다.

이후에도 아래 <표 2-5>에서 보는 것처럼 2000년대 들어 발생한 대부분의 분쟁과 전쟁에서 키네틱 폭력과 함께 사이버 공격(사이버 기술공격, 사이버 심리전 공격)을 병행하거나 단독으로 사이버 공격을 감행하였다.

---

55) YTN뉴스, "알케에다 지도자 알 자르카위 사망," 2006년 6월 8일; https:// n.news. naver. com/mnews/article/052/0000119397?sid=115(검색일: 2023년 5월 16일).

<표 2-5> 2000년대 사이버전 중심의 하이브리드전 사례[56]

2006년 7월 이스라엘-레바논 전쟁	• 헤즈볼라는 이스라엘에 대한 미사일 공격 전 육군 시스템을 해킹하여 군 무선 통신에 침투하고 미국 웹서버 업체들을 하이재킹하여 이스라엘의 인터넷망 공격. • 이스라엘 군인들의 휴대폰 통화를 도청하여 군사정보를 수집[57], 가짜 시체와 폭격 장면을 연출하는 등 사이버 심리전 전개.
2007년 4월 러시아의 에스토니아 사이버 공격	• 러시아는 에스토니아의 대통령궁, 의회, 정부기관, 금융기관, 언론기관, 이동통신 네트워크 등에 대해 3주간 지속적으로 디도스 공격하여 에스토니아 국가 시스템 전체 마비.
2008년 6월 러시아-조지아 5일 전쟁	• 러시아는 정규전 외에 바이러스에 감염된 컴퓨터 네트워크인 봇네트(botnets)를 이용하여 사흘간 '메일 폭탄(Mail bombing)', '디도스 공격'으로 에스토니아 전산망 무력화 • 사이버 범죄조직 '러시아비즈니스네트워크(RBN)'를 이용한 디도스 공격은(정부기관, 언론사 등 대상) 평균 2시간 15분, 최장 6시간 동안 이루어짐
2012년 11월 가자-이스라엘 분쟁	• 이스라엘군은 트위터를 통해 선전포고 후 페이스북, 트위터, 인스타그램, 유튜브를 활용하여 가자지구 공습에 대한 우호적 여론을 조성.[58] • 하마스 해커들은 이스라엘 장교 소유 휴대전화 5천여 대 해킹, 협박 메시지 발신
2013년 11월 이스라엘-하마스 교전	• 하마스는 이스라엘에 대해 1,400회 로켓공격과 4천 4백만 회의 사이버 공격 감행. 이스라엘은 하마스와 이슬람 지하드의 라디오 방송을 강탈하여 테러리스트를 돕지 말라는 심리전 수행.[59] • 이스라엘 방위군과 하마스 무장세력 간 트위터 상 설전
2014년 3월 러시아의 크림반도 합병	• 우크라이나의 친러 정권이 붕괴한 이후 우크라이나 동부 돈바스 지역에서 친러시아 반군과 정부군 간 무력분쟁 발생. • 2014년 3월, 2천 명의 러시아군은 소속부대나 계급, 명찰이 식별되지 않는 국적이 불분명한 군복을 착용하고 우크라이나 침공. 러시아군은 우크라이나 군과 교전 없이 우크라이나의 군사기지, 의회, 대법원, 공항을 점령함. • 러시아 연방보안국(FSB)과 군사정보국(GRU)은 우크라이나에 대한 정보활동과 여론공작 등 사이버 심리전 전개

56) 송태은, "하이브리드 위협에 대한 최근 유럽의 대응," 『IFANS 주요국제문제분석』, 2020-31(2020), p. 12.

57) 요제프 요페, "레바논 전쟁의 승자는 누구인가?," 『중앙일보』(인터넷판), 2006년 9월 7일; https:// www. joongang.co.kr/article/2441652(검색일: 2023년 11월 10일).

58) 김수빈, "나흘 만에 4천 4백만 회 공격, 보다 치열해진 사이버전," 『한겨레』 (인터넷판),

한편, 한국에서도 2015년 이슬람 무장단체 IS에 김모 군이 가담하는 사건이 발생하였다. 김 군은 2014년 트위터를 통해 IS 가입방법을 알게 되었고 터키지역 간부를 통해 구체적인 계획을 세우고 2015년 터키를 경로로 IS에 가담하게 되었다.[60] 또한, 2019년에는 박모 씨가 군 복무 중 IS에 가입할 계획을 세우고 심지어 테러 준비까지 한 혐의로 체포된 사건도 있었다.

이 사건들이 시사하는 바는 언어와 문화가 다르고 지리적으로 떨어져 있어도 인터넷을 통한 사이버 심리전이 충분히 영향을 끼칠 수 있다는 점이다. 또한, 대상을 한정하지 않고 정부의 규제와 감시를 피해서 얼마든지 일반인에게 영향을 끼칠 수 있다. 이는 사이버전이 시간과 장소에 구애받지 않으면서도 공격 주체를 은폐하면서 언제든지 선제적으로 취할 수 있으며, 공격대상이 되는 사회의 국가 시스템을 마비시킬 수 있음을 인식하였기 때문이다. 특히 사이버 심리전은 상대국(집단)의 내부갈등을 표면적으로 분출시키고 연대를 와해시키려는 일종의 티핑포인트(tipping point) 역할을 수행할 수 있다.

2) 비정규전, 비대칭전으로서의 러시아 사이버 심리전 사례

서구 민주주의 국가들이 본격적으로 사이버 심리전에 대해 경각심을 가지고 본격적으로 대비하기 시작하게 된 것은 서구사회의 선거 시기에 러시아에 의해 발생한 사이버 심리전이었다. 러시아는 2016년 미국 대선과 영국의 브렉시트 국민투표, 2017년 독일 총선과 프랑스 대선, 스페인의 카탈루냐 독립투표, 2018년의 이탈리아 총선, 2019년 유럽의회 선거(EU Parliamentary Election), 미국 중간 선거, 2020년 미국 대선 시기에 서구권 소셜미디어 플랫폼에 AI 프로그램인 가짜계정 봇(bots)을 이용한

2013년 1월 1일; http://defence21.hani.co.kr/34508(검색일: 2023년 1월 21일).

59) 위의 기사.

60) KBS뉴스, "외교부, 'IS 가담 김모군 사망 추정...확인은 안돼,' 2015년 11월 17일; https://n.news.naver.com/mnews/article/056/0010249390(검색일; 2023년 4월 1일).

허위조작정보를 대규모로 유포하여 공격하였다.

<표 2-6> 러시아 사이버 심리전에 의한 가짜뉴스 사례[61]

피해국	공격대상 정치 일정	러시아가 배후로 밝혀졌거나 의심되고 있는 가짜뉴스 내용
미국	2016년 12월 대선	● 피자게이트(Pizza gate) 사건: 2016년 12월 4일 힐러리 클린턴 후보가 워싱턴 D.C. 피자 가게에서 아동 성매매 조직을 운영함. 이 가짜뉴스를 믿은 한 남성이 피자 가게에 총격을 가함 ● 프란치스코 교황은 클린턴과 트럼프 후보를 지지한 일이 없었으나 트럼프에 대한 지지를 선언했다는 가짜뉴스가 대선 직전 3개월간 페이스북에서 96만 건 공유. ● 오바마 대통령이 불법체류자들에게 선거권을 부여, 투표하게 함. ● 힐러리 클린턴 선거비용의 20%를 테러리스트들이 제공하고 있으며, 힐러리는 건강에 심각한 문제가 있어 집권 시 부유층의 비선 실세가 국정을 운영할 것임
프랑스	2017년 4월, 5월 대선	● 러시아 언론 Sputnik와 Russia Today는 마크롱이 동성애자이고 해외에 비밀계좌를 보유하고 있다고 보도. 이들 매체는 마크롱 대선 캠프의 취재를 금지당했고 결선 투표를 앞두고 프랑스 검찰은 러시아의 가짜뉴스 유포에 대한 수사 착수
영국	2017년 6월, Brexit 국민투표	● 약 15만 개의 러시아어 트위터 계정들이 투표 전날과 당일에 Brexit와 관련한 글을 집중적으로 게시. ● 가짜 트위터 계정들이 무슬림 증오를 유발시키는 사진을 유포하고 The Sun 紙 등의 주요 언론도 이러한 사진을 인용하여 보도. 이에 노동당과 테레사 총리는 가짜뉴스 관련 러시아에 경고
독일	2017년 9월 연방하원 총선거	● 2016년 12월 20일, 베를린 크리스마스시장 테러 발생 10일 후인 12월 31일 독일 도르트문트에서 이슬람 이민자 1,000명이 경찰 및 시민을 공격하고 가장 오래된 독일의 교회를 방화하기 위해 폭죽을 터뜨림. ● 2017년 초, 러시아 소녀가 베를린에서 시리아 난민에게 성폭행을 당하고 살해됨. 당시 러시아 외무장관 세르게이 라브로프와 독일 외무장관 프랑크발터 슈타인마이어가 사건의 진위를 모르는 상태에서 언쟁을 벌임. ● 메르켈 총리와 셀피(selfie)를 찍어 유명해진 시리아 난민 출신 청년인 아나스 모다마니가 노숙자 옷에 불을 붙이려 함. ● 메르켈 총리가 동독 비밀경찰 출신 혹은 히틀러의 딸임.

61) 송태은, “미국과 중국의 공공외교와 국제평판,” 하영선·김상배 편, 『신흥무대의 미중 경쟁: 정보세계정치학의 시각』(파주: 한울아카데미, 2018), pp. 173-174.

피해국	공격대상 정치 일정	러시아가 배후로 밝혀졌거나 의심되고 있는 가짜뉴스 내용
스페인	2017년 10월 카탈루냐 독립 국민투표	● 스페인 경찰이 독립투표를 저지하다 한 여성의 손가락을 부러뜨림. 경찰이 독립지지자들에게 폭행당해 심장마비로 사망함. 6살 소년이 경찰의 폭력으로 인해 몸이 마비되었음. ● 2012년 마드리드 광부들의 파업 사진이 카탈루냐 독립투표에 참여했다가 경찰에 의해 부상 당한 사진으로 조작 및 유포됨. 스페인 정부가 투표저지를 위해 카탈루냐에 탱크를 보냈다는 조작된 동영상이 유포됨. ● 마리아노 라조이 총리는 허위정보를 확산시킨 가짜 트위터 계정의 50%는 러시아에, 30%가 베네수엘라에 근거지를 두고 있다고 주장.

이러한 시기는 공격대상 국가의 국내 여론이 활성화되는 정치적 시점, 즉 국가정책에 대한 각종 논쟁적인 정보와 충돌하는 의견이 난무할 수 있는 선거 또는 국민투표 캠페인 기간이었다. 정기적으로 반복되는 민주주의 국가들의 선거나 투표 기간은 심리전 공격 주체가 언제든지 '게릴라전(guerilla warfare)'을 펼칠 수 있는 '비정규전'의 성격을 갖는다. 즉 정부와 정당들, 정치인 및 대중들의 모든 관심과 막대한 에너지가 국내 선거에 집중될 수밖에 없는 일정 기간은 심리전 방어자(defender)가 상당히 취약한(vulnerable) 환경이다. 반대로 심리전 공격자(attacker)에게는 상대 국가의 약한 틈을 치고 들어갈 수 있는 최상의 조건이 된다. 또한, 선거기간이 아니더라도 장차 선거에서 논쟁적인 이슈가 될 만한 민감한 사회적 문제 즉 인종, 이민, 종교, 총기 소지 관련 이슈 등은 언제든지 그러한 이슈를 둘러싸고 사회갈등이 심화될 수 있기 때문에 비정규전으로서 사이버 심리전이 활용할 만한 효과적인 내러티브의 소재가 될 수 있다.

이러한 평시 심리전은 단순히 여론의 양극화만을 노린다기보다는 사회갈등의 증폭과 심화, 집단적인 대중들의 불만 폭발을 유도하여 국가기관이나 민주주의 제도에 대한 대중들의 신뢰와 기대가 무너지고 국가의 권위와 정당성이 치명적으로 훼손되는 것을 목표로 한다. 그러므로 극단적이고 자극적이며 고도의 설득전략(persuasion strategy)이 동원된 내러티브를 사용한다. 공격자가 목표로 겨냥하기 쉬운 대상은 이미 여론분열과 사회갈등이 잠재되어 있거나 본격적으로 표출되는 사회이므로 양극화된

여론 환경에 처한 일반 대중들은 심리전 목적으로 유포되는 허위정보를 분별하기가 쉽지 않다.

권위주의 국가의 사이버 심리전이 민주주의 국가에 대해 갖는 두 번째 강점은 '비대칭전'의 이점을 취할 수 있다는 점이다. 개방된 민주주의 사회의 정치 커뮤니케이션(political communication)에 개입하여 여론을 교란하는 일은 공격자의 입장에서는 상대적으로 적은 노력과 비용으로 선제공격의 우위를 언제든지 점할 수 있음을 의미한다. 더군다나 권위주의 국가는 자국의 정치과정은 국외에 개방시키지 않고 국가가 온라인상에서의 정보이동을 차단할 수 있기 때문에 이들 국가가 심리전 방어자가 될 때 갖는 사이버 네트워크에 대한 통제력은 민주주의 국가에 비해 압도적으로 크다. 비대칭전이 본래 약자가 선호하는 전략인 것을 고려한다면 사이버 심리전에서 권위주의 레짐이 민주주의 레짐에 대해 갖는 권력은 약자의 권력이 아닐 수 있다. 방어자 입장에서는 공격자의 악의적인 정보가 일회적이어도 그러한 정보가 사실이 아닌 허위라는 것을 국내·외의 청중에게 다시 알리는 일이 더 복잡하고 어렵기 때문이다.

게다가 사이버 심리전은 전통적인 심리전에 비해 방어자 입장에서 대응이 더 어려운 여러 가지 조건을 가지고 있다. 양차 대전기나 냉전기와 시기가 겹치는 매스미디어 시대의 심리전에서는 공격자가 수신자(방어자)의 피드백이 없는 '일방향적인 입장 전달의 형태'로 메시지를 전파했다. 또한, 매스미디어 시대에는 심리전의 방어자인 정부와 언론은 정보전달 채널을 중앙집권적으로 통제하는 방식으로 정보의 문지기(gate keeper) 역할을 수행하여 외부로부터 유입되는 공격적인 메시지를 쉽게 차단할 수 있었다. 이러한 매스미디어 환경에서는 일방적인 메시지 전달이라도 더 많은 미디어 채널을 확보한 국가(행위자)가 더 유리하였다. 즉 거대 예산을 동원하여 전 세계적으로 수많은 미디어 채널을 가동할 수 있는 미국은 소련으로부터의 프로파간다 메시지를 얼마든지 상쇄시킬 수 있었다.

하지만 지금의 인터넷과 소셜미디어 시대에서는 타국으로부터의 심리전에 대해 정부가 공격자의 프로파간다 메시지에 대해 국내 청중에게 역선전(counter propaganda)을 수행해야 하고 이미 악의적인 메시지에 노출

된 국내 청중들이 악의적 메시지를 다시 유포하지 않도록 조치를 취해야 하는 등 청중들에 대한 적극적인 관여(engagement) 절차를 수행해야 한다. 또한, 정부는 국내·외 청중들이 타국으로부터의 사이버 심리전 징후를 정부에 적극적으로 알리는 등의 자발적인 협조가 필요하다. 결국, 사이버 심리전의 방어자는 자국 청중들과 지속해서 상호 소통해야 하는 비용을 부담해야 하고 국내 청중의 '참여'와 '협업'을 통해 가짜정보의 허위를 밝혀낼 수밖에 없다. 요컨대 사이버 심리전의 방어자는 집단지성(collective intelligence)을 동원하면서까지 허위정보를 일일이 격파하거나 인공지능 알고리즘 기술을 통해 사이버 공간에서의 악의적 정보를 찾아내는 등 상당히 복잡한 대책을 강구해야 한다. 따라서 이러한 환경에서 심리전 공격자는 더 빈번하게 선제공격을 취할 유인을 갖게 된다. 그야말로 심리전은 지속적인 공격을 통해 방어자를 지치게 만드는 '소모전(war of attrition)'의 효과도 노릴 수 있는 것이다.

3) 러시아의 사이버 심리전 목표와 전략

러시아는 「2000년 정보안보독트린(2000 Information Security Doctrine)」에서 정보전의 정보공격(informational attacks) 형태를 기술적 공격과 심리적 공격으로 구분하였다. 이 두 가지 모두 PSYOP 활동으로서 적국 대중에 '침투하고(infiltrate)', '혼란케 하며(disorganize)', 적국의 국가기능을 '중단시키거나(disrupt)' 종국적으로는 '파괴하는 것(destroy)'을 목표로 하고 있음을 명시하고 있다. 이 문건에서 명시하고 있는 '심리적 전복(psychological subversion)'은 적국을 '속이고(deceiving)', 정책결정자들에 대한 '신뢰를 무너뜨리며(discrediting)', 대중과 군의 '방향성을 상실케 하고(disorienting)', '사기를 꺾는(demoralize)' 것을 목표로 한다. 러시아는 이러한 사이버 전술을 통해 EU와 NATO의 '유대(cohesion)'와 '통합성(integrity)'을 와해시키고 궁극적으로는 러시아에 유리한 새로운 유럽의 정치 질서를 구축하려 한다.[62]

62) Rugge, Fabio. "Mind Hacking: Information Warfare in the Cyber Age." ISPI Analysis No.

이러한 목표에 따라 러시아는 서유럽뿐만 아니라 폴란드나 슬로바키아와 같은 동유럽의 신생 민주주의 국가 대중의 정치적, 경제적 좌절감과 불만을 자극하고 EU와 NATO에 대해 반감을 갖도록 유도하고 있다. 슬로바키아에 대해서는 슬라브 민족으로서 러시아와 공통된 정체성을 호소하고, 더딘 민주화로 인해 슬로바키아와 폴란드가 EU 공동체의 진정한 일원으로 받아들여지기 힘들다는 것을 강조하는 등 여론을 분열시키는 전술을 사용하고 있다.[63] 또한 러시아는 서구 유럽에 대한 동유럽 대중의 증오심을 유발하기 위해 자국을 악마화하는 서방을 악마화하기도 한다. 예컨대 2016년 2월 러시아의 주요 언론은 리투아니아의 NATO 소속 독일 병사가 리투아니아의 15세 소녀를 강간했다는 가짜뉴스를 보도하기도 했다. 궁극적으로 러시아는 서방의 자유주의 질서가 와해 되었으므로 앞으로의 세계가 러시아를 필두로 하여 전통과 보수적 가치, 진정한 자유를 수호하는 유라시아 세력으로 대체되어야 한다고 주장한다.

게라시모프 독트린(Gerasimov doctrine) 혹은 새 세대 전쟁(New Generation War)으로 불리는 러시아의 2014년 군사독트린은 군사력으로 대변되는 하드파워 전력과 경제전(economic warfare), 에너지 갈취(energy blackmail), 파이프라인 외교(pipeline diplomacy) 등 일련의 경제 전술과 외교 전술을 모두 아우를 수 있는 전술로서 '정보전(information warfare)'을 명시했다. 이 군사 독트린에서 정보전은 모든 종류의 군사 활동과 비군사적 활동, 정부 행위자와 비정부 행위자의 활동을 하나로 묶어내는 '시스템 통합자(system integrator)'로 제시되고 있다. 즉, 러시아에 있어서 사이버 심리전은 평시와 전시, 국내와 해외, 그리고 다양한 미디어를 통해 동원할 수 있는, 적국을 억압할 가장 효율적인 수단으로 인식되고 있다. 또한, 러시아에 있어서 평시 사이버 심리전은 서방과의 갈등이 군사 위기 혹은 전쟁으로 고조되는 것을 막을 수 있는, 서방에 대한 사전 경고 수단으로도 인식되고 있다.[64]

319, 2018. p. 4.

63) Christopher Walker & Jessica Ludwig, "Introduction: From 'Soft Power' to 'Sharp Power': Rising Authoritarian Influence in the Democratic World." In Sharp Power, Rising Authoritarian Influence. International Forum for Democratic Studies (Washington D.C.: National Endowment for Democracy, 2017), pp. 16-19.

러시아의 서방에 대한 사이버 심리전은 서구 민주주의의 개방된 정치 시스템을 이용하고 있지만, 러시아는 자국의 사이버 공간을 철저하게 닫힌 시스템으로서 방어하고 있다. 러시아의 「2016년 정보안보독트린(2016 Information Security Doctrine)」은 외부로부터의 사이버 위협과 영향으로부터 러시아 시민을 보호할 것과 러시아의 정보 자유(information freedom)를 위해 사이버 전력과 사이버 무기를 통제할 국가 시스템을 확립할 것을 강조했다.[65] 러시아는 이미 2000년 이전부터 사이버 주권을 강조해왔고 이러한 관점은 더욱 강화되고 있으며 러시아에 있어서 서방과 동유럽에 대한 사이버 심리전 개시와 자국 사이버 주권의 강화는 러시아가 세계질서에서 다시 지배적 위치를 확보할 수 있는 주요한 수단으로 인식되고 있다.

러시아는 공공외교를 정부가 위계적으로 주도하는 프로파간다 활동의 일환으로 인식하기 때문에 민간과 비정부 행위자의 공공외교 참여에 대한 구체적 구상을 결여하고 있다.[66] 결국 서유럽과 동유럽, 남미, 중동 모든 지역에서 하락한 자국 평판과 공공외교 실패를 만회할 방법으로 러시아가 추구한 전술은 서구의 선진 민주주의 사회도 엘리트의 부패와 경제난 등 러시아가 갖는 문제를 동일하게 갖고 있음을 드러냄으로써 서구 민주주의 제도의 정당성과 우월함을 부정하는 방식인 것이다. 따라서 러시아의 사이버 심리전은 서구사회에 혼란과 두려움을 유발하고 국가기관, 정치제도, 정치인들에 대한 불신을 조장하는 것을 목표로 삼고 있다.

특히 2008년 조지아 침공에 이어 2014년 크림반도 합병과 우크라이나 침공 등 동유럽에서 공격적인 군사행동을 감행한 러시아는 이후 국제사회로부터 제재를 받게 되자 동유럽과 서유럽 여론이 미국과 EU, NATO에 대해 회의적으로 되도록 좌절감과 반감을 유발하는 심리전을 적극적으로 전개하고 있다. 러시아는 조지아와 우크라이나에 대해서도 이들 국가의 민주주의 혁명인 2003년 장미혁명과 2004년 오렌지혁명을 비판하고 자유

64) Rugge(2018), p.4; Defense Intelligence Agency(2017), pp. 37-41.

65) Defense Intelligence Agency(2017), p. 40.

66) 두진호, "러시아 군사공공외교의 특징과 함의," 『국방정책연구』, 제30권 제2호(2014), pp. 53-54.

주의 세계질서의 거버넌스 모델도 함께 비판하는 심리전을 펼쳤다.[67]

최근의 미국 대선을 기점으로 하여 러시아의 사이버 심리전은 2016년부터 본격화되었지만 사실상 국가적 차원에서의 러시아 심리전의 역사는 매우 길다. 냉전기 KGB 예산의 상당 부분을 심리전 공작에 투입했던 만큼 러시아는 세계 최고의 전술을 갖춘 다양한 비밀공작 활동을 보유하고 있다. 러시아의 간첩 조직들은 미국을 비롯한 서방의 대학가에서 이들 국가의 정책 방향을 분석하고 비밀작전 수행을 위해 주요 인물을 정보원으로서 포섭하며 민감한 군사시설 및 연구물에 접근하는 활동을 전개해왔다. 특히 서구 학계의 투명성과 공정한 절차를 통해 지원되는 장학금 체계나 구직과정은 러시아가 활용할 수 있는 유용한 조건이 되어 왔다.[68] 그러므로 러시아의 사이버 심리전은 과거 소련이 다양한 채널을 통해 전개했던 정보활동의 연장선으로 이해될 수 있다. 다만 현재의 사이버 심리전은 러시아보다 우월한 하드파워와 소프트파워를 보유한 미국을 포함한 서구 민주주의 국가들에 대해 러시아가 비정규전, 비대칭전으로서의 비폭력적 전술을 구사할 수 있게 하며, 만약의 군사충돌이나 하이브리드전에서 역전을 노릴 수 있는 전술로 기능한다고 볼 수 있다.

4) 러시아의 컴퓨터 프로파간다와 마인드해킹 설득기제

'컴퓨터 프로파간다(computational propaganda)'란 정치적 프로파간다 활동을 위해 인공지능의 커뮤니케이션 도구와 기술을 사용하는 것을 말한다. 2016년 미국 대선과 2017년 서유럽 선거기간에 수행된 러시아의 가짜뉴스 공격은 인공지능의 알고리즘 기술이 동원된 컴퓨터 프로파간다 활

67) Vivian S. Walker, "Crafting Resilient State Narratives in Post Truth Environments: Ukraine & Georgia," In Shawn Powers & Markos Kounalakis (eds.), Can Public Diplomacy Survive the Internet? Bots, Echo Chambers, and Disinformation(US Advisory Commission on Public Diplomacy(2017), pp.83-88. https://www.state.gov/documents/ organization/271028.pdf(검색일: 2022.10.1.).

68) Daniel Golden, Spy Schools: How the CIA, FBI, and Foreign Intelligence Secretly Exploit American's Universities (New York: Henry Holt and Co., 2017).

동이었다. 러시아는 소셜미디어 가짜계정의 '봇 부대(bot army)'를 이용하여 거대 규모의 서구 온라인 청중에게 허위정보를 신속하게 유포할 수 있었다.[69] 2018년 4월 7일 시리아 아사드 정권의 반군에 대한 화학무기 사용으로 미국, 영국, 프랑스 연합군이 시리아를 공습했을 때 이에 반발한 러시아가 취했던 첫 번째 군사행동은 사이버 심리전이었고 이때 동원된 것이 인공지능 봇 기술인 '로보-트롤링(robotrolling)' 이었다.

인공지능 알고리즘 기술이 빈번하게 사용되는 사이버 심리전은 일반적인 커뮤니케이션 공간에서 이루어지므로 가짜뉴스의 대다수 수신자인 일반 대중은 특정 메시지가 정치적 목적에 의해 의도적으로 생산되고 확산된다는 사실과 인공지능 봇이 그러한 메시지를 유포시킨다는 사실을 인지하기가 어렵다. 지금의 인공지능은 내러티브에 대한 이해가 필요한 스토리텔링 능력을 '딥러닝(deep learning)'을 통해 갖추고 있고, 대화형 프로그램을 수행하는 '소셜봇(social bot, social networking bot)'은 사람과 쌍방향 커뮤니케이션이 가능하기 때문이다. 사이버 심리전 공격과 일상적인 커뮤니케이션 간의 경계가 모호한 상황에서 공격자가 의도한 메시지나 담론의 설득 전술은 수신자의 메시지 수용에 있어서 결정적인 영향력을 발휘하게 된다.

러시아의 심리전에서 위력을 발휘한 소셜봇은 선거 여론에 영향을 끼칠 목적으로 만들어진 '정치봇(political bot)'이었다. 러시아의 정치봇 활동에 이용된 다양한 설득 기제는 현대 민주주의 국가가 수행하는 심리전의 설득방식과는 차별되는 전술을 펼쳤다. 일반적으로 심리전에서 효과적인 설득방식은 메시지의 신뢰성을 높이기 위해 '진실'과 '일관성(consistency)'을 강조하는 데 반해, 러시아는 이러한 전통적 사고에 반하여 메시지의 진실과 일관성을 철저히 부인하는 심리전을 전개했다. 흥미로운 것은 러시아의 심리전 전략이 인지심리학(cognitive psychology)이나 커뮤니케이션학에서 논하는 다양한 설득 원리를 철저하게 적용하고 있다는 점이다.[70]

---

69) 송태은, "미국과 중국의 공공외교와 국제평판," 하영선·김상배 편, 『신흥무대의 미중 경쟁: 정보세계정치학의 시각』(파주: 한울아카데미, 2018), p. 166.

70) Matt Chessen, "Understanding the Psychology Behind Computational Propaganda." In Shawn Powers & Markos Kounalakis (eds.), Can Public Diplomacy Survive the Internet? Bots, Echo Chambers, and Disinformation(US Advisory Commission on

러시아의 설득전략은 전문가들이 '인지적 해킹(cognitive hacking)' 혹은 '정신적 해킹(mind-hacking)'으로 일컬을 정도로 상당히 정교하게 고안되어 있다.[71]예컨대 서로 다른 정보원을 갖는 여러 미디어가 서로 다른 논지로 어떤 특정 이슈를 다루더라도 결국 모두 같은 결론에 이르거나, 여러 미디어가 같거나 유사한 정보를 보도할 경우 이렇게 제공된 정보는 더 설득력을 갖는다. 한편 관심이 낮거나 다수가 인정하는 정보의 경우 사람들은 대개 정보의 질과 출처가 불확실해도 그러한 정보를 신뢰하는 경향을 보인다. '진실착각효과(the illusory truth effect)'로 불리는 이러한 심리적 경향은 정치봇의 프로파간다 전략에 활용되고 있다. 즉 소셜미디어의 정치봇은 팔로워(followers) 수 혹은 '좋아요(likes)'를 생성시키는 알고리즘으로 여론을 왜곡할 수 있는 것이다. 또한, 사람들은 자신이 속한 그룹이나 자신과 공통점이 많은 그룹이 인정하는 정보를 더 신뢰하고, 정보의 양이 적은 경우에는 전문가를 신뢰하지만, 정보의 양이 크면 반드시 전문가의 의견을 따르지는 않는다.[72]

정치봇은 개방된 온라인 공론장에서 '반향실 효과 혹은 메아리방 효과(echo chamber effect)' 현상을 부추기고 강화시킬 수 있다. 반향실 효과는 서로 비슷한 관점과 생각을 가진 사람들 사이에서 커뮤니케이션이 반복되면서 편향된 사고가 고착화되고 개인이 선호하고 동의하는 의견만을 수용하는 현상이다. 정치봇은 소셜미디어 공간에서 특정 메시지와 정보만을 지속적으로 제공, 확산시켜 대중이 특정 이슈에만 주목하게 유도하여 여론의 양극화를 더욱 악화시킬 수 있다.[73] 더욱이 서유럽의 선진 민주주의 사회뿐 아니라 조지아나 우크라이나와 같은 동유럽의 신생 민주주의 국가도 러시아가 펼치는 사이버 심리전의 대상이 된 것은 신생 민주주의의 시민사회는 온라인 공론장에서의 자유로운 의견교환과 토론을 통해 새

Public Diplomacy(2017), pp. 19-20. https://www.state.gov/documents/organization/271028.pdf(검색일: 2022년 10월 1일).

71) Fabio Rugge, "Mind Hacking: Information Warfare in the Cyber Age." ISPI Analysis No. 319 (January 2018).

72) Paul & Matthews(2016), pp. 2-3.

73) Rugge(2018), p. 4.

로운 사회적 합의에 이르는 경험을 충분히 갖지 못하여 가짜뉴스의 공격에 쉽게 영향을 받기 때문이다.

제 5 절 현행법상 사이버 심리전의 법적 근거

1) 국내법

사이버 심리전은 '사이버'라는 공간에서 수행되는 '전쟁의 수행방식(warfare)'이므로 당연히 국내법을 따라야 한다. 우선, 한국의 헌법 제5조 제1항은 침략전쟁을 부인한다. 따라서 평시에도 이뤄지는 사이버 심리전의 특성상 대북 사이버 심리전 수행은 그 수준에 따라 이를 위반할 소지가 있을 수 있다.[74]

반면 전시 사이버전은 헌법 제73조와 60조에 따라 대통령의 선전포고 및 국회의 동의를 받을 경우 수행할 수 있다. 하지만 헌법의 전쟁 수행에 대한 통제 절차를 사이버 심리전에 적용하기에는 다소 무리가 있다. 사이버 전쟁을 위해 계엄을 선포하는 경우 국민의 기본권에 대한 심각한 제한이 발생할 수 있기 때문이다.[75] 따라서 평시에 수행하는 사이버 심리전은 국군조직법(법률 제10821호)에 의해 근거한다고 볼 수 있다. 국군조직법 제9조 제2항에 의거하여 작전부대는 합동참모의장의 작전지휘를 받고 그 범위는 대통령령으로 정할 수 있다. 구체적으로 사이버 작전을 수행하는 사이버작전사령부는 사이버작전사령부령 제2조[76]에 의거하여 사이버 작전과 관련된 임무를 계획하고 수행할 수 있다. 이와 같은 국내법에 근거한 사이버 심리전은 우선, 헌법에서 명시한 국군의 정치적 중립성 의무를 바

74) 침략전쟁은 위법한 전쟁에 속한다. 적법한 전쟁은 국제법상 허용되어 있는 전쟁을 말하며, 자위를 위해 수행하는 전쟁이다. 그러나 양자의 구별, 즉 침략전쟁과 정전의 차이는 기본적인 것이지 만 오늘날 이 양자의 구별은 거의 불가능해졌다. 즉, 침략이냐 아니냐는 개별국의 주관에 의해 판단될 수밖에 없다.

75) 오일석·김소정, "사이버 공격에 대한 전쟁법 적용의 한계와 효율적 대응방안," 『인하대학교 법한연구소 법학연구』, 제17집 제2호(2014), p. 138.

76) 사이버작전사령부령(대통령령 제29561호, 2019년 2월 26일 전부개정) 제2조(임무) 1항 사이버작전의 계획 및 시행, 7항 그 밖에 사이버작전과 관련된 사항.

탕으로 정치적 영역에 포섭되지 않아야 한다. 그리고 스스로 그러한 접근을 배척하고 공개하며, 견제할 수 있어야 할 것이다.

2) 국제법

사이버전은 이전에 없던 새로운 형태의 전쟁이다. 사이버 공간은 국경의 초월하고, 사이버 공격의 주체와 피·아 식별이 거의 불가능하며, 대치하고 있는 전선도 모호하다. 또한, 관련 기술의 발전속도는 가공할 정도로 가속화되고 있으며, 민·관·군의 영역 구분은 더욱 모호해지고 있다. 또한, 사이버전에 대한 개념 정의도 명확하지 않을 뿐만 아니라 이에 대해 기존의 무력분쟁법이나 국제인도법을 적용하는데 국제적 합의도 아직은 부족하다. 사이버전에 대한 국가들의 이해수준과 능력이 천차만별이기 때문에 국제 규범의 정립도 쉽지는 않다. 하지만 국제사회는 날이 갈수록 점증하고 있는 사이버 공격을 규제 밖에 방치할 수 없었기에 국제 규범 적용에 많은 노력을 기울여 왔다.(이민효, 2017, p. 11).

그 결과 2013년 사이버 전쟁에서 적용되는 국제법을 담은 지침서인 탈린메뉴얼(Tallinn Manual)[77]이 발간되었고, 그에 따르면 사이버 공간은 현존 국제법에 적용된다고 규정하였다. 제1장 제2절은 사이버 작전에 대한 국제공법상 규칙의 적용을 다루며, “국가는 자국의 주권 영역 내의 사이버 기반시설 및 사이버 활동에 대하여 통제권을 행사할 수 있다.”라고 기술한다. 이는 자국의 사이버 영역에서 사이버 심리전 활동에 대한 수행 근거로 해석할 수 있다. 대외 사이버 심리전의 근거는 조금 다르다. 특정 국가가 UN 헌장 제51조[78]에 따른 ‘무력공격’의 피해자가 되는 경우, 국가는 제2(4)조[79]에도 불구하고 ‘무력사용’이 허용된다고 한다. 즉, 타국의

77) 2013년 3월 북대서양조약기구(NATO : North Atlantic Treaty Organization)가 사이버테러에 관한 조항들을 성문화한 최초의 사이버 교전 수칙. 이후 내용이 더욱 확장됨에 따라 2017년 2월에 탈린 매뉴얼 2.0이 발간.

78) UN 헌장 제51조는 다음과 같다. “Nothing in the present Charter shall impair the inherent righto individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.”

불법적 무력사용에 대해 자위권 발동을 보장하고 있다. 탈린메뉴얼 제2장 규칙11에서는 “사이버작전은 그 규모와 효과가 비(非)사이버작전에 의한 무력사용의 수준에 준할 때 무력사용이 되며, 사이버 작전 또는 사이버 작전에 의한 위협은 그 위협행위의 실행이 불법적인 무력사용을 구성하는 경우 불법적 무력에 의한 위협으로 간주된다.”고 기술한다. 사이버 심리전이 ‘무력공격’을 형성하는지 여부는 그 규모와 효과에 따라 결정된다(규칙 13). 따라서 대외 사이버 심리전의 수준이 ‘무력공격’에 준하지 않는다면 전쟁법 위반에 대한 소지는 미미하다. 또한 북한의 대남 사이버 심리전의 효과가 ‘무력공격’으로 인정받는다면 UN헌장에 따라 한국도 그에 준하는 무력공격이나 대북 사이버 심리전의 수행근거를 획득하게 된다.

제 6 절 소결론

사이버 안보는 ‘사이버’를 구성하는 7개 부문[80]들에 대한 안보를 모두 합친 개념이다. 각 부문들은 하드웨어, 소프트웨어, 인지 및 심리 영역, 전파, 정보패킷 등의 성질로 이루어져 있으며 이러한 성질들은 사이버-기술전, 사이버-심리전 위협과 연관되어 있다. 또한 각각의 부문들은 키네틱전, 다른 비키네틱전(전자전, 정보전, 심리전, 인지전)과 중첩되어 있고 외교전쟁, 문화전쟁과 같은 비군사적인 안보이슈들과도 연관되어 있기 때문에 개념의 확장과 다변화 속에서 이해해야 한다.

한편 미래전은 러시아-우크라이나 전쟁처럼 키네틱전과 비키넥틱전이

79) UN 헌장 제2(4)조는 다음과 같다. “[all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of anystate, or in any other manner inconsistent with the Purposes of the United Nations.” 동규정의 기초과정에서 원래 ‘영토보전이나 정치적 독립’에 관한 언급은 없었다. 그러나 ‘어떠한 기타방식’이 포함되어 동규정의 무력사용 금지는 원칙적으로 제한을 받지 않는 것으로 이해된다.

80) ① 인터넷 기반시설과 관련 장비·부품들, ② 인터넷에 연결된 유·무인 디바이스들, ③ 다비이스들을 운영하는 운영체계(OS)와 온라인 플랫폼, 그리고 AI등의 프로그램, ④ 가상의 네트워크 체계와 규칙들, ⑤ 인터넷 공간에서 유통되는 정보 콘텐츠들, ⑥ 인터넷 공간의 정보와 인터페이스하는 인간의 의식(perception), ⑦ 정보콘텐츠 또는 디바이스들을 연결하는 무선통신.

중첩되고 융합된 하이브리드 전쟁으로 진행될 것이며 군사적 영역 뿐만 아니라 비군사영역도 포함한 다영역에서 동시에 전개될 것이다. 이와 같은 미래전 추이와 사이버 안보는 밀접히 관련되어 있으며, 그 비중과 관련성 역시 매우 크다. 사이버전은 키네틱 전쟁과 다른 유형의 비키네틱 전쟁의 다른 수단이자 전제 조건이 될 수도 있고 기폭제가 될 수도 있으며 동시에 반대의 영향을 받을 수 있다. 따라서 사이버 공간 또는 사이버 수단은 미래전 수행에 있어 중심적인 위치에 있다.

심리전은 전시 및 평시를 막론하고 자국민, 상대국가(적), 국제사회에 대해 국가의 목적을 달성하기 위한 국가정책 및 전략을 수행함에 있어 유리한 감정과 태도, 행위를 조성하기 위하여 사용되는 계획적인 정치, 경제, 사회, 문화 등 군사적인 제반의 심리전 활동이라고 정의할 수 있다.
사이버 심리전을 단순하게 정의하면 사이버 공간에서 이루어지는 '심리전 활동'이라 할 수 있다. 하지만 이는 사이버 심리전이 심리전에 종속되거나 사이버 심리전이 단순한 심리전 확장이라는 개념은 아니다. 사이버 심리전은 기존 심리전과는 대별되는 명확한 특징을 가진다. 먼저 심리전 효과의 피드백이 쉽고, 정교하며 빠르다. 또한, 수단이 다양하고 보편적이기 때문에 상대적으로 시간적, 경제적 비용 부담이 적다. 그리고 공간적 제약이 없으며 사이버 심리전 주체는 부인이 용이하여 법적 규제가 거의 불가능하고 주체에 대한 추적과 증거확보가 어려워서 사전 대응, 방어, 보복, 반격이 곤란하다.

이러한 사이버 심리전의 특징은 향후 사이버 심리전의 범위와 능력이 제한 없이 확장됨과 동시에 정보화 환경이 발달되고 인터넷 개방성이 보장된 자유민주주의 국가들이 상대적으로 사이버 심리전에 대한 취약함을 내포한다. 향후에도 정보통신기술이 발달로 사이버 심리전이 더욱 증가할 것이며, 이는 전·평시와 군사·비군사 등 시간과 분야를 가리지 않을 것이다.

사이버 심리전의 최초 사례는 코소보 사태(1999)이며 이슬람 무장단체들 또한 사이버 심리전을 통해 서방 국가들에 비해 자금력이 열세인 상황을 극복하고자 하였다. 하지만 서구 민주주의 국가들이 본격적으로 사

이버 심리전에 대해 경각심을 가지고 본격적으로 대비하기 시작하게 된 것은 러시아가 2016년 이후 거의 모든 서구사회의 선거 시기에 서구권 소셜미디어 플랫폼에 AI 알고리즘 프로그램 가짜계정 봇(bots)을 활용한 디지털 허위조작정보를 대규모 유포하는 사이버 심리전 때문이었다.

러시아는 권위주의 국가가 갖는 강점(자국의 사이버 주권 강화 등)을 무기로 자유민주주의 국가들의 상대적 약점(민주주의 국가의 개방된 정치체제 및 인터넷 정책 등)과 사이버 심리전에서 방자가 감수해야 하는 취약성을 적극적으로 활용하여 사이버 심리전을 전개하였다, 러시아는 사이버 심리전을 평시는 물론 전시, 국내와 해외, 그리고 다양한 미디어를 통해 동원할 수 있는, 적국을 억압하는데 가장 효율적인 수단으로 인식하고 있으며, 러시아의 사이버 심리전의 목표는 EU와 NATO의 '유대(cohesion)'와 '통합성(integrity)'을 와해시키고 궁극적으로는 러시아에 유리한 새로운 유럽의 정치 질서를 구축이며, 궁극적으로는 러시아가 세계 질서에서 다시 지배적 위치를 확보하는 것이다. 이러한 목표를 달성하기 위해 러시아는 대량의 거짓 정보를 다양한 채널을 통해서 신속하고, 지속·반복적으로 유포하며 메시지 또한 객관적 현실과 일관성에 개의치 않는 전략을 사용한다. 또한, 인공지능의 커뮤니케이션 도구와 기술의 산물인 정치봇(Political bot)과 정교하게 고안된 마인드 해킹 설득 기제를 결합시켜 상대 국가들의 여론의 양극화를 더욱 악화시키는 효과를 달성하였다.

사이버 심리전은 침략전쟁을 부인하고 대통령의 선전포고 및 국회의 동의 절차를 받아야 하는 헌법을 위반한다는 논란의 소지가 있을 수 있다. 하지만 사이버 심리전에 전통적인 키네틱 전쟁과 동일한 기준을 적용하는 것은 무리가 있으며, 따라서 평시에 수행하는 사이버 심리전은 국군조직법에 근거해 수행할 수 있다. 다만 사이버 심리전의 성격상 군의 정치적 중립성 의무를 훼손하지 않도록 정치적 영역으로부터 벗어날 수 있도록 제도적인 장치가 마련되어야 하며 군 스스로 정치적 접근을 경계하여야 한다.

또한, 탈린메뉴얼에 의하면 각 국가는 주권 영역 내의 사이버 기반시설 및 사이버 활동에 대해서 통제권을 행사할 수 있음을 기술하고 있는데 이

는 자국의 사이버 영역에서의 사이버 심리전에 대한 수행근거로 해석할 수 있다. 대외 사이버 심리전은 그 수준이 '무력공격'에 준하지 않는다면 전쟁법 위반에 대한 소지는 미미하며, 북한을 포함한 적대국가의 한국에 대한 사이버 심리전의 효과가 '무력공격'으로 인정받는다면 UN 헌장에 따라 한국도 그에 준하는 무력공격이나 사이버 심리전의 수행근거를 획득할 수 있다.

제 3 장 북한의 사이버 심리전 능력과 위협

제 1 절 남북한 사이버 환경 및 비대칭성

북한은 사회주의 경제의 태생적 모순과 비효율성의 가중, 국제사회의 경제적 제재와 자연재해에 의한 장기적인 경제 침체 및 내부 불안 심화, 미국의 초강대국화와 굳건한 한미동맹으로 한국과의 국력 격차가 심화되고 있다. 북한은 이러한 전략적 불균형 심화의 돌파구로 비대칭 전력의 증강에 심혈을 기울이고 있다.

한국 정보당국은 북한이 김정은 시대 들어서 비대칭 전력 강화의 일환으로 사이버 전력을 급속도로 강화하고 있으며, 사이버 공격 수준에서는 학자나 보고서마다 견해가 조금씩 다르지만, 미국, 중국, 러시아, 이란에 이어 세계 5위 수준에 도달한 것으로 평가하고 있다.[81] 사이버 심리전에 국한해서는 러시아, 중국, 베네수엘라, 인도, 사우디아라비아, 이란, 이집트, 미얀마, 파키스탄이 세계 최고 수준의 사이버 심리전 부대를 운영하는 것으로 알려져 있다.[82] 하지만 북한의 사이버전 수행 인력은 한국 국방부가 2022년 12월에 발행한 국방백서에 따르면 6,800여 명 정도로 추산된다.[83] 또한, 북한은 단기간 내에 외국군의 한국지원이 제한, 도시의 발달과 수도권이 MDL에 근접하여 있는 등의 한반도의 지정학적 위치로 인한 취약점을 인식하고 있다. 그리고 다양한 이익집단의 출현 및 개인주의로 인한 한국사회의 안보의식 약화와 ICT 의존도 심화 등의 전략적 취약점을 간파 및 인식하고 있다. 따라서 북한은 이를 극적으로 활용할 수 있는 핵무기 / 다종의 미사일 개발, GPS 교란, 화학 및 생물무기 배치, 제2전선

81) 유동열, “우크라이나 전쟁으로 드러난 사이버전의 위력,”『미래한국』, 2023년 3월 13일; http://www.futurekorea. co.kr/news/articleView.html?idxno=146808(검색일: 2023년 11월 5일).

82) Samantha Bradshaw and Philip N. Howard, “Global Disinformation Order: 2019 Global Inventory of Organized Social Media Manipulation” The Computational Propaganda Project(2019) p.5.; http//demtech.oii.ox.ac.uk/wp-content /uploads/sites/93/2019/09/CyberTroop-Report19.pdf(검색일: 2022년 12월 14일).

83) 대한민국 국방부,『2022 국방백서』(서울: 국방부, 2022), p. 25.

형성 / 후방교란 전력 증강뿐만 아니라 사이버 기술공격, 사이버 심리전 등의 비대칭 전력 증강에 집중적으로 노력하고 있다. 실제로 김정은은 사이버전을 핵·미사일과 함께 3대 전쟁수단으로 규정하면서 핵·미사일과 함께 북한군의 무자비한 타격 능력을 담보하는 '만능의 보검'이라고 강조한 바 있다.(2013년 11월 남재준 당시 국정원장이 국회 정보위원회에 북한의 사이버전 실태를 보고)[84] 이는 '한국 안보상 취약점 이용'을 기본 전략개념으로, 북한이 보유한 특이한 수단이나 특이한 방법(사이버 수단, 속도, 모호성을 기초한 기습 등)을 이용한 비대칭적 전략 및 작전적 운용을 강조하고 있다고 판단할 수 있다.[85]

비대칭 전력에 있어 북한이 특히 심혈을 기울이는 것은 사이버전이다. 북한 사이버 위협들의 특징은 다음과 같이 열거할 수 있다.[86] 우선 한반도 전구에서 사이버 위협의 상시성과 전방위성이다. 한국은 정보기술과 인터넷 강국으로서 정보기반시설에 고도로 의존하고 있어 사이버 위협은 상시적으로 존재하고 있고, 발달된 사이버 공간은 피·아와 전·평시 구분이 모호하며, 위협의 근원이 군과 민을 가리지 않을 뿐만 아니라 범위도 전 세계적으로 연결되어 있다. 또한, 분쟁의 주체 역시 개인, 군, 국가에 이르기까지 다양해질 수 있고, 위협행위 역시 비폭력적, 폭력적 수단이 배합되어 즉시적으로 발생하고 있으며, 그에 대한 합법성 역시 모호하여 전방위적으로 위협을 받을 수 있다는 것이다. 둘째, 정보기술의 혁신적인 발전으로 정보의 질과 양이 폭발적으로 증대되고, 사이버 기술과 무기체계가 신속하고 광범위하게 확산되고 있을 뿐만 아니라, 기술의 발전이 아주 짧은 기간 내에 이루어지기 때문에 한국과 한국군에 주는 북한의 사이버 위협은 매우 역동적이고 동태적이라는 것이다. 셋째, 북한의 사이버 위협 유형이 매우 다양하게 확산되어 체계에 대한 침해 및 해킹과 여러 통신체계 마비를 위한 전자공격, 물적 정보체계 및 기반 구조에 대한 물리적 타격,

84) 정영교, "김정은 손에 '2조' 쥐어줬다…전방위 공격하는 北 '만능 보검'," 『중앙일보』, 2021년 12월 26일; https://www.joongang.co.kr/article/25035443(검색일: 2023년 11월 25일).

85) 배달형, "4세대전쟁 및 비대칭 위협 관점의 사이버전 및 사이버 심리전 발전방향," 『전략연구』, 22권 1호 (2015), pp. 141-172.

86) 문장렬, "평시 및 위기시의 사이버전 대비전략과 전력기획." 『안보연구 시리즈』, 제11집 12호(2010), pp. 72-74.

소프트웨어적인 타격, 사이버 심리전 확대 등 사이버 위협 영역이 지속 확대되고 있다.

<표 3-1> 북한 사이버 위협의 특징

구 분	내 용
상시성, 전방위성	● 한국은 정보기반시설에 고도로 의존하고 있어 위협은 상시적으로 존재 ● 피·아와 전·평시 구분이 모호, 위협대상도 군과 민을 가리지 않고 범위도 전 세계적으로 연결 ● 비폭력적, 폭력적 수단이 배합되어 즉시적으로 발생, ● 합법성이 모호하여 전방위적으로 위협 발생
역동성, 동태성	● 정보의 질과 양이 폭발적으로 증대, 사이버 기술과 무기체계가 신속하고 광범위하게 확산 ● 혁신적이고 빠른 정보통신기술의 발전
다양성	● 사이버 기술 공격(침해, 해킹), 전자공격 및 물리적 타격, 사이버 심리전 등 위협 영역이 지속 확대

북한의 사이버 위협에 대한 효율적이고 장기적인 대응책은 남북한의 사이버 환경과 사이버전 수행능력에 대한 정확한 평가에서부터 출발해야 한다. 남북한의 사이버 현황을 분석해보면 첫째, 한국의 사이버 환경은 민간(산업계)과 정부·공공 영역이 분리돼 있지만, 북한은 그렇지 않다. 북한의 경우에는 사이버 공간을 소유하고 운영하는 주체가 국가 즉 정부이기 때문에 모든 사이버 환경은 철저히 중앙집권적인 계획과 통제하에 있다. 이는 정책의 효율성에 큰 차이를 발생시킨다. 한국은 일관성 있는 사이버 안보 정책의 수립을 위해 민간과 공공 영역이 협력해야 하므로 시간이 걸리고 비용이 들어간다. 이런 상황은 위기 때 신속한 대응을 하는 데 걸림돌이 될 수 있다. 그러나 북한은 어떤 위기에서도 신속히 대응할 수 있을 뿐 아니라 협력과 대화를 위한 비용도 들지 않는다. 이런 사이버 환경의 차이는 사이버전 수행의 비대칭성을 만드는 원인이 된다. 이러한 사이버 환경의 차이는 비대칭적 취약성(asymmetric vulnerabilities)을 발생시켜 공격 유혹을 강하게 유발한다는 점에 주목해야 한다. 비대칭적 사이버 환경은 2014년 4월 호주전략정책연구원(Australian Strategic Policy Institute,

ASPI)이 발표한 보고서의 사이버 성숙도(cybermaturity)라는 지표에 잘 나타나 있다.(<표 3-2> 참조) 보고서는 사이버 성숙도라는 지표를 산출하기 위해 1) 거버넌스, 2) 군(military), 3) 디지털 경제 및 사업, 4) 사회적 참여를 수치화하여 평가하였다. 흥미로운 것은 남북한은 '디지털 경제 및 사업 분야'와 '사회적 참여'의 하부 요소인 '인터넷 연결도'에서 차이가 크다. 이처럼 경제적 측면을 비롯해 여러 면에서 차이가 큰데도 사이버 공간에서의 군(military) 역할에는 양측의 차이가 전혀 없다는 점은 정책 대안을 마련하는 데 반드시 주목해야 할 대목이다.[87]

<표 3-2> 사이버 성숙도[88]

구분	거버넌스				군	디지털 경제 및 사업		사회적 참여		총점
	조직 구조	입법	국제적 참여	사이버 안보 지원 서비스	사이버 공간에서 군의 역할	정보-비지니스 대화	디지털 경제	대중 인지도	인터넷 연결도	가중치를 둔 총점
한국	7	6	7	8	7	8	8	9	9	75.5
북한	3	1	2	0	7	1	2	1	1	20.7

북한은 디지털 경제 발전에는 관심이 없으며 내부 민심의 이탈을 막기 위해 외부와의 인터넷 연결을 차단하고 자유로운 정보의 유입을 계획적으로 막고 있으면서도 군사적 목적으로는 사이버 공간을 적극 활용하고 있다. 북한은 이러한 현저한 남북한의 비대칭성을 중요한 대남 공격 포인트로 활용하리라 예측할 수 있다. 사이버전으로 남북한의 상호 갈등이 고조될수록 사이버 공간에서 한국의 피해는 기하급수적으로 증가하지만, 북한의 피해는 제한적일 수밖에 없다. 남북의 공격과 방어가 사이버 공간에만 벌어진다면 북한 입장에서는 사이버 공간이 잃을 것이 없는 승리의 공간인 것이다. 사이버 공간은 평시 전략적 자산이지만 방치하면 전시에는 엄청난 취약점이 될 것이며, 북한은 목적 달성을 위해 작전을 펼치고 협박하

87) 신창훈, "북한의 사이버공격과 위협에 대한 우리의 대응—2014년 11월 소니(SONY)사건의 교훈," 『ISSU BRIEF』,(2015).

88) ASPI, Cyber Maturity in the Asia-Pacific Region 2014 (April 2014)

기 쉬운 공간으로 간주하여 집요하게 한국을 공격해 올 것이다.

셋째, 디지털 경제 규모와 인터넷 연결의 차이로 만들어진 비대칭적 취약점은 한국의 사이버전 능력을 현저하게 떨어뜨리는 요인이 되고 있다. 남북 간의 사이버전 능력을 비교하는 자료를 찾기 곤란하지만 단순한 지표를 활용해 주요국 간을 비교하는 공개 자료는 있다. 이중 가장 단순하고 흥미로운 클라크와 네이크(Clarke&Knake)의 비교표를 제시하면 <표 3-3>과 같다.[89]

<표 3-3> 주요국가 사이버전 능력

구 분	사이버 공격	사이버 의존성	사이버 방어	총점
미국	8	2	1	11
러시아	8	5	4	16
중국	7	4	6	15
이란	4	5	3	12
북한	2	9	7	18

<표 3-3>에서는 사이버 의존성이 낮을수록 점수가 높게 표시되는데 이는 사이버전 능력이 강하다는 의미다. 이들은 사이버전 수행능력을 공격, 의존성, 방어라는 세 범주만으로 평가하였기 때문에 비교적 단순한 평가라는 비판을 받는다. 그러나 사이버 의존성이 낮은 북한이 오히려 사이버전 능력은 높게 평가되기 때문에 북한은 전 세계 유력 저널리스트들이 관심을 끄는 대상이 됐다. 사이버 의존성을 과대평가하는 측면은 있지만, 이 문제는 사이버 전략을 구축하는데 있어 반드시 고려해야 할 중요한 요소임을 보여준다.

사이버 공격은 물리적 테러와 달리 형체를 갖고 있지 않아 흔적도 남기지 아니하는 은밀성과 아울러 접속 매체 등에 대한 감염을 확산시키면서(감염성),[90] 일정한 조건이 충족되기를 기다려 계획된 공격을 개시하는 잠복성[91] 등의 특징이 있다. 이외에도 시간적·공간적 제약을 받지 아니하

89) Richard A. Clarke & Robert K. Knake, Cyber War (2012), p. 148.

90) 신영웅 외, "국가사이버보안 피해금액 분석과 대안: 3·20 사이버 침해사건을 중심으로," 『국가정보연구』, 제6권 제1호(2013), p. 135.

는 특성 등으로 인하여 정보화 수준이 높은 지역(한국)과 그러하지 아니한 지역(북한) 간의 비대칭성, 사이버 공격과 물리적 피해의 발생 간에 시간적, 공간적 비대칭성과 징후의 탐지와 대응의 비대칭성 등 국가 총력적인 첩보의 수집과 개인의 PC를 비롯한 사회통신망에 대한 실시간 모니터링이 없는 상황에서는 한국은 북한의 비대칭 전략의 공격대상이 될 수밖에 없을 것이다.

제 2 절 북한의 사이버전 수행능력과 제한사항

1) 북한의 사이버전 교리

북한의 사이버전 교리는 외부로 공개된 자료가 없으므로 이를 정확히 파악하기는 쉽지 않다. 따라서 사이버전 교리의 군사적 특성을 파악하기 위해서는 먼저 중국과 러시아의 사이버전 교리를 살펴볼 필요가 있다. 북한의 사이버전 기술은 중국 및 러시아에 크게 의존하고 있기 때문이다. 첫째, 중국의 사이버전 교리는 2050년까지 적의 정보 기반시설(information infrastructure)을 붕괴시킬 수 있는 능력을 확보하여 전 세계적 범위에서 '전자적 우위(electronic dominance)'를 달성하는 것을 목표로 하고 있으며, 이를 위해 재래식 전쟁을 개시하기 전에 적의 금융 시스템, 민간 또는 군사통신 시스템을 파괴하는 전략을 채택하고 있다.[92] 둘째, 러시아는 대량살상무기를 이용한 재래식 군사 활동의 효과를 증폭시키기 위한 수단으로 사이버전을 활용한다는 교리를 채택하고 있다.[93] 그러나 북한의 사이버전 교리는 북한이 보유한 사이버전 기술에 의해서가 아니라 북한이 처

---

91) 2010년 7월 7일 발생했던 디도스 공격의 경우 2009년 7·7 디도스 당시 삭제되지 않고 살아남은 악성코드에 의한 것이라고 한다. 2015년 1월 23일; http://www.nkvision.com/read.php?num=495(검색일; 2023. 11. 1).

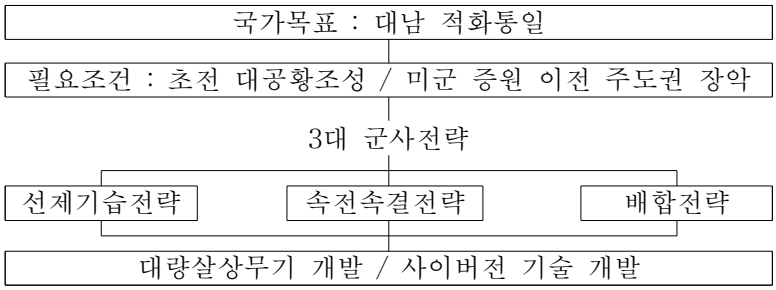
92) Ward Carroll, "China's Cyber Forces,"; http://defensetech.org/2008/05/08/chinas-cyberforces /(검색일: 2023년 9월 9일).

93) Ward Caroll, "Russia's Cyber Forces,"; http://defensetech.org/2008/05/27/russias-cyberforces/(검색일: 2023년 9월 9일).

한 상황에 따라 결정될 가능성이 크다. 이에 따라 북한의 정치·경제·사회적 요인이 북한의 사이버전 수행목표 형성에 미칠 영향을 파악해보았다.

첫째, 북한의 사이버전 교리는 국가목표를 달성하기 위한 목적 지향적 지침이 되어야 하므로 정치적 맥락 속에서 파악해야 한다.[94] 북한은 조선로동당 규약 서문에 “조선로동당의 당면목적은 공화국북반부에서 사회주의강성국가를 건설하며 전국적범위에서 민족해방민주주의 혁명의 과업을 수행하는데 있으며 최종목적은 온 사회를 김일성-김정일주의화하여 인민대중의 자주성을 완전히 실현하는데 있다.”고 규정하고 있다.[95] 북한은 이러한 목표를 달성하고 장기적 전쟁 수행능력 제한을 극복하기 위해 다음과 같이 세 가지 군사전략을 추진하고 있다.

<그림 3-1> 북한의 국가목표와 대남군사전략[96]



북한은 이러한 3대 군사전략을 실현하기 위해 대량살상무기(WMD; Weapons od Mass-Destruction)와 사이버전 능력 강화를 추진하고 있다. 한국에 비해 재래식 전력이 열세인 상황에서 한국 사회 공황을 조성하고 전쟁능력을 약화시키기 위해서는 한국이 효율적으로 대응할 수 없는 비대칭 전력이 필요하기 때문이다. 특히 사이버전 기술을 활용한 공격(사이버 기술공격과 심리전 공격)은 한국 사회의 분열을 유도하고 혼란을 일으킬 수 가장 경제적이고 효과적인 수단임을 인지하고 있는 것이다. 컴퓨터 공

94) 황진환 외, 『신국가안보론』(서울: 박영사, 2014), p. 24.

95) 박성규·길병옥, 『현대 북한의 이해』(대전: 충남대학교출판문화원, 2020), p. 320.

96) 김인수 외, 『정예강군 육성을 위한 북한 바로알기』(서울: 양서각, 2023), p. 181.

학 교수 출신의 탈북자인 김흥광은 사이버전이 북한에게 다음과 같은 군사적 이점을 제공한다고 설명한다.[97] 첫째, 사이버전은 적은 비용으로 군사적 도발을 가능하게 한다. 공격자가 분명하게 드러나는 통상적인 군사도발은 정치적 비난과 책임을 피할 수 없기 때문이다. 둘째, 사이버전은 포병 및 항공전력을 이용한 도발보다 실용적이다. 통상적인 군사도발을 위한 준비 활동은 인공위성이나 기타 감시체계에 의해 신속하게 포착될 수 있기 때문이다. 셋째, 사이버전은 간첩 활동 및 심리전 수행을 위한 토대를 제공한다. 이에 따라 북한은 사이버전 기술을 이용한 군사적 도발을 지속할 것으로 보인다.

둘째, 북한의 경제정책 역시 사이버전 교리에 영향을 미칠 수 있다. 김정일은 "우리에게 간절한 문제는 현대적 과학기술에 튼튼히 의거 경제 강국, 과학기술 대국을 세우는 것"[98]이라고 강조하였으며, 이를 위해 북한은 IT 산업을 핵심으로 경제 활성화를 추구하는 '단번 도약' 전략을 추진해 오고 있다. 김정은도 1980년 제6차 당대회 개최 후 36년 만인 2016년에 제7차 당대회를 개최하고 '사회주의 강국'에 앞서 '과학기술강국'을 건설할 것을 선차적 목표로 선언[99]한 바 있다. 북한이 IT 산업을 중시하는 이유는 군사강국 건설뿐만 아니라 경제구조의 개선을 위해서 반드시 필요하기 때문이다.[100] 그러나 경제적으로 낙후한 북한에서 단기간 내에 IT 산업 육성을 통한 성과를 기대하기는 힘들다. 따라서 북한은 대규모 자본투자 없이 기술 개발이 가능한 소프트웨어를 외화벌이를 위한 수단으로 활용할 수 있다. 김정은이 외화벌이 사업에 나선 "군대가 너무 돈에 맛을 들였다"고 질책했다는 사실 역시 군사과학기술이 경제적 목적으로 전용될 가능성을 보여 준다.[101] 또한, 국내 인터넷 게임 이용자가 북한 해커들에게 해킹

97) HP Security Research, "Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape," HP Security Briefing Episode 16 (August, 2014), p. 26.

98) 『로동신문』, 2002년 1월 23일.

99) 변상정, "김정은 시대 북한의 과학기술정책: '휘황찬 설계'와 불균형적 발전," 『국가안보전략연구원 연구보고서』, 2022-10, p. 17.

100) 김재호, 『김정일 강성대국 건설전략』(평양출판사, 2000), pp. 31-37.

101) 정성장, "'돈줄' 틀어쥐기 위해 군부 군기 잡기 나섰다," 『시사저널』(인터넷판), 1206호, 2012년 11월 29일; http://www. sisapress.com/news/articleView.html?idxno=59345(검

프로그램 개발을 의뢰하거나, 국내 도박꾼이 북한 정찰총국 소속 공작원에게 북한산 해킹 프로그램을 구입하는 사건이 잇따라 발생하고 있는 현실이 이를 뒷받침한다.[102]

셋째, 북한은 정치적으로는 주체사상을 통치이념으로 한 수령중심의 일당 지배체계이며, 경제적으로는 중앙집권적 계획경제, 사회적으로는 집단주의 원칙에 의해 구축되고 수령을 어버이로 하는 '사회주의 대가정 체제'다.[103] 따라서 북한이 안정적으로 유지되기 위해서는 폭력을 통한 강압과 정권의 정당성 강화를 위한 선전·선동이 병행되어야 한다. 폭력의 남용만으로는 체제에 대한 주민들의 자발적 복종을 얻어내기 어렵기 때문이다. 이로 인해 북한에서는 1960년대부터 주체사상을 통치 이데올로기로 제시하여 김일성에 대한 개인 우상화를 진행하였고, 통치자에 대한 우상화 시도는 현재까지 그대로 이어지고 있다. 이에 따라 북한의 학교 교육은 정치사상 교육을 강조한다. 이러한 북한의 정치문화를 고려할 때, 사이버전 기술은 체제선전을 위한 수단으로 활용될 가능성이 크다.

<표 3-4> 북한의 사이버전 수행목표

구 분	북한 체제 특성	사이버전 수행목표
정치적 요인	3대 군사전략	한국 사회 혼란 조성 군사작전 방해, 국가기능 마비
경제적 요인	IT산업 중심의 단번도약 전략	외화벌이
사회적 요인	선전·선동 중시의 정치문화	체제선전

이와 같은 북한 체제의 특성과 군사과학기술의 상호 작용을 고려할 때, 북한의 사이버전 수행목표는 <표 3-4>에 제시한 바와 같이 한국의 사회혼란 조성, 군사작전 방해 및 국가기능 마비, 외화벌이, 체제선전 등으로 요약할 수 있다.[104]

색일: 2023년 10월 4일).

102) YTN, 2010년 5월 6일; 『연합뉴스』, 2014년 9월 10일.

103) 국립통일교육원, 『2023 북한이해』,(서울: 통일교육원, 2023), pp. 15-22.

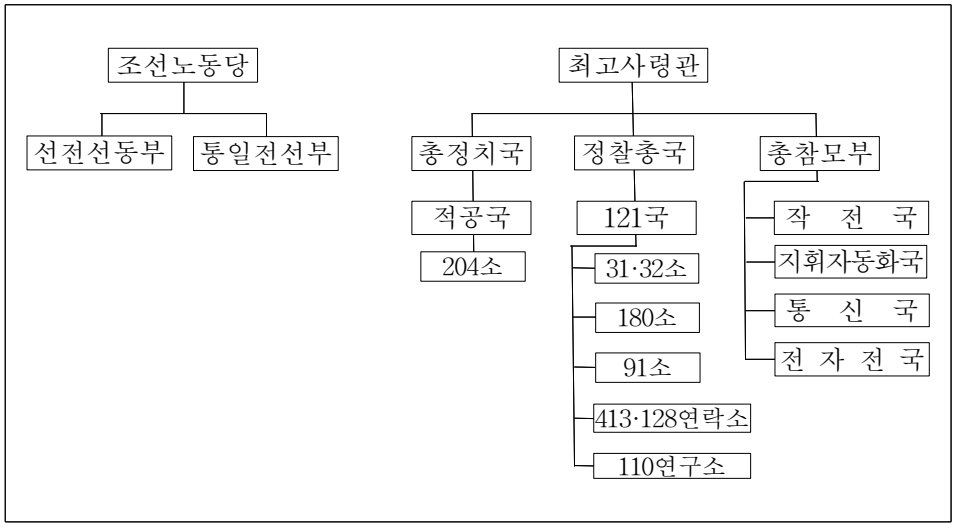
104) 임종인 외, "북한의 사이버전력 현황과 한국의 국가적 대응전략," 『국방정책연구』, 제29권 4

2) 북한의 사이버 조직체계

북한은 노동당이 다른 기관보다 우위에 있는 이른바 당 주도의 권력 구조를 갖추고 있다. 북한 노둥당은 노동당 규약과 당적 원칙에 따라 군을 통제하는 지위를 가지며 그 중심에는 당중앙군사위원회가 있다. 북한은 2021년 1월, 당 규약 개정을 통해서 당중앙군사위원회는 당대회와 당대회 사이의 당의 최고군사지도기관으로 새롭게 규정하였다.[105] 김정은은 당 총비서이자 당중앙군사위원 회원장으로서 중앙군사위원회를 통해 군을 지도하고, 군의 기본적인 의사결정을 직접 하고 있다. 또한, 김정은은 국무위원회 위원장임과 동시에 최고사령관으로서 군을 정점에서 지도 및 지휘하는 등 무력 일체를 장악하고 군정권과 군령권을 행사하고 있다.

이러한 북한 체제의 특성은 북한의 사이버전 조직체계에도 영향을 미친다. 북한의 사이버전 조직체계에 관한 연구는 연구자에 따라 차이가 있지만 비교적 최근 자료들을 종합하여 아래 <그림 3-2> 및 <표 3-5>에서 제시하였다.

<그림 3-2> 북한의 사이버전 지휘체계



호(2013), p. 15.

105) 국립통일교육원, 『2023 북한이해』,(서울: 통일교육원, 2023), pp. 68-69.

<표 3-5> 북한의 사이버전 조직별 주요 임무

구 분		주요 임무
당	통일전선부	·120여 개 친북사이트 운영, 트위터/페이스북 등 SNS 공작 ·대남 사이버 심리전 전담, 여론조작 댓글팀 운영 ·남남갈등, 사회 교란 시도
	선전선동부	·인터넷 선전을 총괄하는 조직을 신설('23. 3월)
총정치국	적공국 204소	·한국군 대상 사이버 심리전 전개 ·역정보, 허위정보유출(인터넷 심리전 전담)
정찰총국	121국	·사이버전지도국으로도 지칭 ·사이버전 수행 총괄 조직으로서, 1998년 결성
	31·32소	·한국 사회일반 사이버 심리전 수행
	91소	·한국 주요 네트워크(폐쇄망) 공격(해커부대) ·대량살상무기 개발을 위한 기밀정보 탈취 (미국의 핵 관련 명령, 통제, 의사소통체계 교란)
	180소	·사이버 외화벌이 수행
	413 및 128 연락소	·한국 및 해외정보 수집, 해킹 ·전담 요원 해외파견, 사이버 테러 수행
	110연구소 (35·98·114소)	·사이버 전략, 전법, 수단 연구 ·한국 및 해외 주요국가 대상 해킹 및 사이버 테러
	해외정보국 자료조사실	·한국 전략정보 수집, 해킹 전담 ·사이버 전담 요원 해외 주재
총참모부	작전국	·기획, 전략 개발 및 운영 ·사이버 작전 수행 간 전략적 결심 수행
	지휘자동화국	·한국군 통신 교란 등 전자전 수행 · 31소 : 악성 코드 개발 · 32소 : 군사용 소프트웨어 개발 · 56소 : 지휘통제용 소프트웨어 개발
	전자전국	·레이더 및 GPS 교란 / 사이버 작전 지원

첫째, 노동당 비서국의 통일전선부는 대남사업의 핵심부서로 대남 심리전 및 통일전선 공작사업을 담당한다. 특히 통일전선부는 2012년 대남간첩공작 임무를 담당하는 내각 소속의 문화교류국(과거 225국)을 흡수하여 '구국전선' 또는 '우리민족끼리'와 같은 웹사이트를 통해 북한 체제를 홍보하고 한국 사회 내에서 종북 세력을 확대하는 사이버 심리전을 담당하고 있다. 둘째, 북한의 노동당 규약은 "총청치국은 인민군 당 위원회의 집행

부서로서 당중앙위원회 부서와 같은 권능을 가지고 사업을 한다."[106]고 규정하고 있다. 총정치국 산하의 적군와해공작부(적공부)는 적군의 전투의지를 무력화시키기 위한 선전, 선동, 전단 살포, 유인, 기만 활동 등 사이버 심리전을 전담한다.[107] 김정은은 "적공일꾼들은 비가 오나 눈이 오나 사회주의 제도 옹위의 전초선을 믿음직하게 지켜가고 있다."고 격려하며 사이버 심리전의 중요성을 강조한 바 있다.[108] 셋째, 국방위원회 직속의 정찰총국은 북한의 해외 공작 활동을 총괄하는 기관이다. 정찰총국에는 사이버전 수행을 총괄하는 사이버전지도국으로 불리는 121국이 편성되어 있으며 예하에는 한국 사회 일반에 대한 사이버 심리전을 수행하는 31·32소, 한국 주요 네트워크 해커부대인 91소, 사이버상에서 불법으로 외화벌이를 담당하는 180소, 사이버 전략 및 전법 기술은 연구하고 사이버 테러를 수행하는 110 연구소 등 사이버전 조직이 집중 편성되어 있다. 넷째, 총참모부 직속의 지휘자동화국은 해킹 및 통신 프로그램 개발을 담당한다. 또한, 북한 사이버전 지휘체계를 분석해보면 사이버 심리전과 관련된 기능이 중복적으로 편성되어 있다는 사실을 확인할 수 있다.

3) 북한의 사이버전 수행능력

1990년대 이후 대부분 국가에서 인터넷 이용자가 폭발적으로 늘어나고, 국가 기반시설의 전산화가 이루어지면서 사이버전을 수행하기 위한 사이버 공간이 확대되었다. 이러한 현상을 잘 포착한 북한은 미래 전쟁에서 사이버전이 차지하는 중요성이 높아질 것이라고 예상하고, 사이버 전력을 강화하고 있다. 북한 노동신문은 "최첨단 과학기술 수단의 하나인 컴

106) 『조선노동당 규약(2010.9.28.)』, 49조.

107) 연합뉴스는 임종인의 연구를 토대로 적공국은 총참모부 직속으로 파악하고 있다. 『연합뉴스』, 2013년 4월 10일 참고. 그러나 북한 원전에 따르면 적공국은 총정치국의 지휘를 받는다. 「조선로동당 중앙군사위원회지시 제002호' 전시사업세칙을 내옴에 대하여」(2004년 4월 3일); 「조선로동당중앙위원회, 조선로동당군사위원회, 조선민주주의인민공화국 국방위원회, 조선인민군 최고사령부 공동명령 제002호」(2012년 9월, 보강된 전시사업세칙) 참고. 김성민, "무시무시한 조직..북한 '적공국'을 아십니까," 『조선 pub』, 2013년 11월 13일 재인용.

108) 『노동신문』, 2013년 11월 12일.

퓨터가 자본주의 나라에서 사람들에게 불안과 공포를 주는 파괴 무기가 되고 있다."며[109] 사이버 위협을 강조하고 있다. 북한의 사이버전에 대한 관심은 1980년대부터 시작되었다. 특히 북한은 2003년 미군이 주도한 '사막의 폭풍작전' 이후 첨단 정보기술의 중요성을 인식하고, 사이버전 관련 기술을 본격적으로 개발하기 시작했으며, 사이버전 관련 기술 도입을 위해 중국, 러시아, 이란과 긴밀하게 협력하고 있다. 중국은 사이버전 기술 교육 외에도 서버, 라우터 등 하드웨어 제공을 통해 북한의 사이버전을 지원하고 있으며, 북한의 사이버전 부대인 정찰총국의 121국이 션양(瀋陽)에서 임무를 수행할 수 있도록 협력하고 있다. 러시아는 프룬제 군사학교 출신 교수 25명을 파견하여 사이버 전문가 양성 교육을 지원하였고,[110] 전자파(EMP) 공격 기술과 인터넷 통제를 위한 기술 정보를 북한에 제공한 것으로 알려져 있다.[111] 이란은 2012년 북한과 기술교류협정을 체결하였으며, IT 기술 공유를 위한 학생 교환, 합동연구 등을 진행하고 있다.[112]

이러한 기술 도입을 토대로 북한의 사이버 공격은 점차 진화하는 모습을 보이고 있다. 사이버 공격의 유형은 이를 구현하기 위한 기술 수준에 따라 바이러스(virus)로부터 지능형 지속가능 위협(Advanced Persistent Threat, APT)[113]으로 구분할 수 있다. 컴퓨터 바이러스와 웜(worms)은 다른 파일을 감염시키거나 변경하기 위하여 자기 자신을 복제하여 다른 컴퓨터에 전염시키는 프로그램을 말하고, 트로이 목마(trojans)는 감염된 PC를 원격 조정할 수 있어 분산서비스 거부 공격(Distributed Denial of Service, DDoS)을 가능하게 한다. 말웨어(Malware)는 시스템의 오작동 또는 마비 등을 목적으로 제작된 악성 소프트웨어(malicious software)를

109) 『노동신문』, 2003년 4월 12일.

110) 윤규식, "북한의 사이버전 능력과 위협 전망," 『군사논단』, 제68호(2011), pp. 76-78.

111) 『연합뉴스』, 2013년 10월 9일.

112) 이에 대해서는 HP Security Research, "Profiling an Enigma: The Mystery of NorthKorea's Cyber Threat Landscape," HP Security Briefing Episode 16(August, 2014), pp. 42-44.

113) 특수한 목적을 가진 하나의 표적에 대해 다양한 기술을 이용해 지속적으로 정보를 수집하고 취약점을 파악하여 이를 바탕으로 피해를 주는 공격 기법. 한국정보통신기술협회 정보통신용어사전 참조; https://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=035578-2 (검색일; 2023년 12월 4일).

말하고, 봇넷(botnets)은 말웨어에 감염되어 인터넷으로 연결되어 있는 PC를 말한다. 마지막으로 가장 높은 수준의 기술을 필요로 하는 APT 공격은 정부 또는 특정 기업의 정보를 취득할 목적으로 일련의 범죄 집단에 의해 이루어지는 지속적인 해킹 공격을 말한다. 북한은 바이러스, 인터넷 웜, 해킹, 디도스, 우회 공격 및 역추적 방지기술, 해킹통신 암호화, 흔적 삭제 등 발전된 소프트웨어를 보유하였으며, 하드웨어 측면에서도 GPS 전파 교란이 가능한 EMP(Electromagnetic Pulse) 무기 등을 개발하고 있다.[114]

2020년 국방부에 따르면 2019년 군 전산망에 대한 해킹 시도는 9,533건으로 2018년 3,986건에 비해 약 2.4배로 늘어났다.[115] 그러나 최근 들어 북한의 사이버 공격 양상은 복합적인 형태로 전개되고 있다. 2009년 7월 7일에는 청와대, 백악관, 주요 포털 사이트를 대상으로 하여 DDoS 공격이 시행되었다. 하지만 DDoS 공격은 심각한 위협으로 간주하지 않는다.[116] 실제로 북한의 공격에 따른 피해는 홈페이지 접속이 일시 제한되고, 웜에 감염된 PC 중 일부에서 하드디스크가 파괴되는 정도에 불과했다.[117] 따라서 7·7 DDoS 공격의 주된 목적은 향후 추가적인 공격을 위해 필요한 봇넷의 규모를 알아보기 위한 것이라는 주장이 제기되기도 하였다.[118] 반면 2013년 3월 20일에 발생한 APT 공격은 KBS 등 방송사와 농협 등 금융사의 내부 시스템 파괴를 목적으로 했다는 점에서 심각한 위협이 되었다. 2011년 4월 12일에는 은밀하게 악성 코드를 심어 놓은 PC를 통해 농협 전산망에 접근하여 서버를 파괴하는 공격이 발생하였다. 북한의 사이버 공격의 양상을 볼 때, 북한은 최고 기술 수준의 사이버 공격을 실행할 수 있는 다양한 전술을 개발하는 데 성공했을 것으로 보인다.

---

114) 북한은 러시아로부터 GPS 전파교란 장비를 수입하여, 최근 3년 동안 세 차례에 걸친 GPS 전파교란을 실시하였고, 그 결과 항공기 1,137대, 함정 4척, 선박 225척, 어선 36척 등 총 1,402대에 피해를 발생시킨 것으로 나타났다. 『연합뉴스』, 2014년 12월 24일.

115) 조명아, "황희, 중국 경유 한국군 전산망 해킹 공격…3년 새 10배 증가", MBC뉴스, 2020.10.10, https://imnews.imbc.com/news/2020/politics/article/5936609_32626.html

116) 리처드 블라크·로버트 네이크, 이선미 역, 『해커 공화국』(서울: 에이콘, 2013), p. 43.

117) 『연합뉴스』, 2009년 7월 9일.

118) 리처드 블라크·로버트 네이크, 이선미 역, 『해커 공화국』(서울: 에이콘, 2013), p. 62.

그러나 이러한 기술적 성과에도 불구하고 북한의 사이버전 수행을 제한하는 다양한 요인들이 존재한다. 따라서 북한 사이버전은 이러한 환경에 대응하면서 최적의 효과를 발휘할 수 있는 방향으로 발전할 것이다.

대표적인 것이 모바일 인터넷 해킹이다. 캐나다 사이버보안업체 '블랙베리 사일런스'는 2019년 연례 보고서에서 북한은 모바일 인터넷 분야 해킹에서 전 세계에서 북한이 가장 위협적 존재로 활동할 것으로 예측하였다.[119] 실제로 2014년 북한의 해킹 시도로 국내 스마트폰 2만여 대가 악성 앱에 감염되었으며, 2016년에는 정부 외교·안보 주요 인사의 스마트폰 중 약 20%가 악성 코드에 감염되었는데 문자메시지를 보내 악성 코드를 침투시킨 것으로 추정하고 있다. 또한, 한국은 최고 수준의 사이버 인프라뿐만 아니라 스마트폰에 대한 개인 의존도 또한 높다. 2023년 7월 기준으로 한국 성인의 스마트폰 사용률은 97%[120]이며 5G 기술발전으로 정보통신 기반의 생활은 정착화 추세에 있다. 이러한 모바일 인터넷 분야에서의 남북한의 비대칭성을 고려 시 북한은 분명 한국 국민의 스마트폰에 대한 사이버 기술공격과 스마트폰을 활용한 사이버 심리전을 강화할 것이다.

과거 북한에 의한 사이버 테러와 해외 사이버전 사례, 그리고 북한의 사이버전 조직을 고려 시 향후 북한에 의한 사이버전 양상을 아래 <표 3-6>와 같이 판단해 볼 수 있다.

<표 3-6> 북한의 사이버전 사례

구 분	내 용	비 고
사이버 심리전	• 북한 체제선전, 반정부·반미·반제국주의 선동 • 허위정보 및 역정보 유출을 통한 공작 시도	광우병, 천안함, 사드 이슈관련 괴담
사이버 기술전	• 한국 공공기관, 한국군 해킹, 정보수집 • 사회 공공망 공격 및 마비(금융기관, 방송사 등) • 교통시스템 공격 : 지하철, 항공기 GPS 교란 등 • 국가기반체계 공격 : 통신망, 전력망 등	2013년 APT 공격, 2014년 한수원 해킹, 2015년 서울메트로 해킹, 2016년 국방망 해킹, 2017년 워너크라이 사태

119) 조상진, "북한 해킹조직, 모바일 사이버 공격 활발,"『VOA』, 2019년 10월 26일; https://www. voakorea. com/a/5139849.html(검색일: 2023년 9월 7일).

120) 한국갤럽, "2012-2023 스마트폰 사용률 & 브랜드, 스마트워치, 무선이어폰에 대한 조사," 2023년 7월 18일; https://www.gallup.co.kr/gallupdb/reportContent.asp?seqNo=1405(검색일: 2023년 9월 7일).

북한은 향후 한국 국민을 대상으로 사이버 심리전을 감행하여 친북 심리전 전개와 반정부 및 반미 심리전을 지속할 것이다. 그리고 사이버 공격을 위한 정보수집을 할 것이며, 필요시에는 한국 사회의 공공 정보통신망에 대한 사이버 기술공격으로 사회 혼란을 조성하고 국가 기간망 및 군 지휘통제망에 대한 공격을 시도하여 무력화하고 여건이 조성되면 전면전을 감행할 것이다.

4) 사이버전 능력 제한요인과 사이버 심리전 위협

북한의 사이버전 수행을 제한하는 요인은 북한을 둘러싼 정치, 경제, 사회, 군사적 환경 속에서 찾아볼 수 있다. 첫째, 중국에 대한 북한의 의존성은 북한의 사이버전 수행을 제한하는 정치적 요인이다. 인터넷 기반 시설이 부족한 북한은 사이버 전사들의 실제 훈련과 작전을 중국의 주요 도시에서 진행하고 있다. 중국을 경유한 북한의 사이버 공격은 익명성으로 인해 이에 대한 책임을 회피할 수 있다는 장점이 있다. 그러나 최근 자국 이익을 중심으로 재편되고 있는 북·중 관계를 고려하면 중국은 국제사회의 비난을 자초하면서 북한의 사이버전을 지원하지 않을 것으로 보인다. 따라서 북한의 사이버 공격이 미국 또는 한국과의 관계를 악화시키거나 GPS 교란공격과 같이 불특정 다수 국가에 피해를 발생시키는 결과를 초래한다면 중국은 자국 영토 내에서 이루어지는 북한의 사이버 공격을 묵인하지 않을 수도 있다. 한국 정부가 북한의 GPS 전파교란 공격에 대해 중국과 방지책을 논의한 사실이 이러한 전망을 뒷받침한다.[121]

둘째, 경제적으로 낙후한 북한에는 사이버 인프라가 거의 구축되지 않았다고 보아도 과언이 아니다. 인프라의 미비는 사이버 방어에 유리하기 때문에 북한의 사이버 전투력을 높게 평가하는 이유로 제시되기도 한다. 그러나 북한의 경제난은 사이버전 능력을 크게 제한할 수 있는 요인이다.

121) Daily NK, “北 GPS공격 장기화되면 직접피해 발생할 것,” 『Daily NK』, 2012년 5월 18일; https://www.dailynk.com/北-GPS공격-장기화되면-직접피해-발생할-것(감색일; 2023년 11월 18일).

클라우제비츠(Karl V. Clausewitz)는 보편적 정신 교양 수준이 높은 국민이 군사적 경향을 강하게 지닐 때 수준 높은 군사적 천재가 태어난다고 설명한다.[122] 대부분의 북한 주민들은 정권의 안정을 유지하기 위해 외부 사회와 차단된 채 살아간다. 따라서 북한에서는 사이버 공간에 대한 국민의 보편적 이해가 형성될 수 없고, 사이버전을 주도할 군사적 천재도 태어날 수 없다. 세계 최고 수준의 사이버 공격능력을 보유한 것으로 평가되는 중국에는 4억 5천 7백만 명 규모의 네티즌이 있으며, 이들 중 일부는 해커로 활동하면서 중국의 국익 또는 개인의 이익을 위한 사이버 공격에 자발적으로 가담하고 있다.[123]

셋째, 정부 주도의 북한 사이버전 교육체계는 사이버전의 효율적 수행을 저해할 수 있는 사회적 요인이다. 북한에서는 1995년 시·군·구역마다 영재학교를 설치하여 선발된 우수 학생들을 프로그래밍과 컴퓨터 하드웨어를 교육하는 금성중학교 컴퓨터 영재반에 진학시키고, 졸업 후에는 평양의 지휘자동화대학에 진학시켜 네트워크 시스템 해킹 기술을 집중적으로 가르치는 것으로 알려졌다.[124] 외국 기술을 모방·추월을 목표로 하는 정부 주도의 기술발전 전략은 단기적으로 상당한 실력을 갖춘 사이버 전사를 양성하는데 효율적일 수 있으나, 민간영역에서 신속하게 변화하는 다양한 기술발전의 추세를 따라잡을 수 없다. 따라서 북한의 사이버 전사들은 혁신적인 기술을 개발하기보다는 기존 기술을 습득·운용하는데 치중할 가능성이 크기 때문에 북한은 사이버전 기술 경쟁에서 수세적 위치에 처하게 될 가능성이 크다. 북한이 사이버전 기술 도입을 위해 긴밀하게 협력하고 있는 중국의 사이버 방어능력이 현격히 떨어진다는 점 역시 북한 사이버전 수행능력의 한계로 작용할 수 있다. 중국은 세계적인 수준의 사이버전 능력을 갖추었지만, 다른 한편으로는 세계 최대의 해킹 피해국으로 알려져 있다.

넷째, 사이버 방어능력 향상을 위한 한국의 지속적인 노력은 북한의 사

122) 클라우제비츠, 강창구 역, 『전쟁론 上』(서울: 병학사, 1991), p. 74.

123) Desmond Ball, “China’s Cyber Warfare Capabilities,” pp. 93-94.

124) 리처드 블라크·로버트 네이크, 이선미 역, 『해커 공화국』(서울: 에이콘, 2013), p. 60.

이버전 능력을 약화시키는 군사적 요인이 될 수 있다. 한국 국방부는 2009년 DDoS 공격을 계기로 효율적인 사이버전 수행을 위해 2010년 국군사이버사령부를 창설하였고, 이후 2018년 8월에는 '사이버작전사령부'로 변경하면서 합참의 작전통제를 받는 합동부대로 변경하였다. 또한, 2014년부터 한미 국방 사이버정책실무협의회를 개최하여 사이버 정책·전략·교리·인력·교육훈련 분야에서 다양한 협력을 강화하고 있다.[125] 북한의 전략문화 역시 북한의 사이버전 능력을 제한할 수 있다. 북한의 전략문화는 구소련 군사교리의 영향으로 조직운영의 융통성이 떨어지는 문제를 안고 있다. 특히 중간급 장교들에게 권한을 부여하지 않기 때문에 이들은 스스로 판단하고 결심할 수 있는 자율성을 갖고 있지 못한 것으로 평가받고 있다.[126] 따라서 강력한 통제를 원칙으로 하는 북한군의 조직문화는 정보화 시대에 요구되는 수평적 협력문화를 만들어내지 못할 것으로 보인다.

북한의 사이버 심리전은 이러한 제약을 상대적으로 적게 받으면서 한국 사회를 위협할 수 있다. 2014년 2월 24~25일 평양에서 조선노동당 전국사상일군대회(제8차)가 10년 만에 열렸으며, 이 행사 폐막일에 김정은이 직접 참석하여 '혁명적인 사상공세로 최후 승리를 앞당겨 나가자'는 제목의 연설을 했다. 이날 연설에는 선전선동사업에서 의미 있는 내용이 많이 언급되었지만, 주목할 만한 부분은 "인터네트(인터넷)를 우리 사상·문화의 선전마당으로 만들기 위한 결정적 대책을 마련하라"고 강조한 대목이다. 사이버 기술전보다 사이버 심리전이 상대적으로 시간적, 경제적, 공간적 제약을 덜 받기 때문에 지속적인 시도가 가능하며, 이는 사이버 심리전의 효용 가치가 커질 수밖에 없는 점을 강조한 것이다.

이러한 결정의 구체적인 이유는 다음과 같이 유추할 수 있다. 첫째, 북한은 사이버전 기술시스템을 도입, 검증·시험, 공고화하는 과정에서 조선노동당과 국방위원회의 대남공작기구들에 사이버 심리전 임무를 중복 편성하고 있다. 이는 북한의 사이버전 수행체계에서 사이버 심리전이 매우 중요한 위치를 차지하고 있으며 역량이 충분하다는 것을 의미한다. 둘째,

125) 위의 책, p. 54.

126) Axel Berkofsky, "North Korea's Military-What Do They Have, What Do They Want?" ISPI Analysis, No. 161(March 2013), pp. 4-5.

익명성이 보장되는 사이버 공간의 특성에도 불구하고, 북한이 사이버 공격의 배후에 있다는 사실이 밝혀지게 된다면 북한에 대한 국민적 경각심이 한층 높아지는 계기가 될 수 있다. 그러나 상대 국가의 국가기반시설에 직접적인 타격을 가하지 않는 사이버 심리전의 경우 사이버 공격과 달리 공격 행위자와 이를 방조한 국가에 대한 국제사회의 제재와 비난을 기대하기도 어렵다. 셋째, 북한의 사이버 심리전은 한국 정권의 정당성을 직접적인 공격 목표로 삼고 한국 사회 내에서 정치적 혼란을 유발할 수 있다. 이를 위해 북한은 SNS, 블로그, 인터넷 카페 등을 통해 왜곡된 정보 또는 루머를 손쉽게 확산시킬 수 있다.

또한, 다른 민주주의 국가보다 한국의 사회갈등지수는 높은 편이다. 한국행정학회가 주요 37개국을 대상으로 사회갈등지수를 분석한 결과, 한국은 2005년, 2010년, 2015년 계속 6위를 차지했다. 한국보다 갈등지수가 더 높은 국가는 심각한 인종차별을 겪었던 남아공, 종교분쟁을 겪은 터키 등이다. [127] 한국 내부의 갈등요소를 표적으로 한 북한의 사이버 심리전은 내부갈등을 심화시킬 수 있는 기폭제가 될 것을 북한도 이미 인식, 학습하고 있을 것이다. 마지막으로 인터넷 통제의 필요성에 대한 일반 국민의 동의를 얻기 힘들기 때문에 북한의 심리전 활동을 차단하기가 쉽지 않은 현실이다.

게다가 북한은 2022년 러시아-우크라이나 전쟁에서 러시아가 보여준 핵무기의 심리전 활용에 주목하고 있을 것이다. 러시아는 우크라이나 전쟁 간 고비가 있을 때마다 핵무기를 언급하여 전 세계를 상대로 사이버 심리전을 전개하였다. 2022년 3월 27일 푸틴은 “핵전력을 특별 준비태세로 전화할 것”과 핵 운용부대에 “특별 근무태세 돌입”을 지시하였다. 그리고 다음 날에는 크렘린궁 대변인이 “국가 존립에 실존적 위협이 있으면 세계는 핵 재앙의 급물살을 타게 될 것”이라고 경고하였다. 또한, 직후인 5월 4일에는 러시아 국영방송이 핵 타격 시뮬레이션을 공개하였는데 여기에는 런던 202초, 파리 200초, 베를린은 10초면 타격 가능함이 포함되어

127) 조용석, “3대개혁 번번이 발목…사회적 갈등 관리 필요성↑,” 『이데일리』, 2023년 7월 19일; https://www.edaily.co.kr/news/read?newsId=01134886635676160&mediaCodeNo=257&OutLnkChk=Y(검색일: 2023년 10월 12일).

있었다. 이후에도 푸틴은 2023년 10월 5일 신형 핵 추진 대륙간순항미사일 '부레베스트닉'의 시험 성공과 차세대 핵무기인 대륙간탄도미사일 '사르마트 시스템'의 완성도 주장하면서 핵실험금지조약 비준도 철회할 수 있다며 30년 만에 핵실험 재개 경고메시지까지 국제사회에 전달하였다. 이러한 러시아의 심리전은 실제로 어느 정도 효과를 보이고 있다. 극한의 상황을 피해야 한다는 국제사회의 인식이 퍼지고 있고 전쟁피로감 등장, 프랑스와 독일을 중심으로 협상을 증대하려는 움직임이 있으며, 미국 또한 강경한 입장에서 다소 물러서는 모습을 보이고 있다.[128] 더군다나 2023년 10월 시작된 하마스와 이스라엘의 전쟁은 국제사회의 전쟁에 대한 우려와 피로감을 더욱 증가시키고 있다. 북한의 경우 핵실험 및 탄도미사일 실험을 하지 않더라도 김정은의 현지 지도 화면을 통해 핵전력 일부를 노출해 한국의 비핵화 노력의 평가절하와 한국 정부의 무능을 강조하는 사이버 심리전이 가능하다. 이는 한국 정치권과 사회 여론 공간에서의 큰 갈등을 격화시킬 것이다. 이러한 북한의 사이버 심리전은 위기를 고조시키기 위한 도발적 행동과 결합할 때에는 또 다른 양상으로 전개될 것이고 한반도에서의 대규모 군사작전을 벌이기 위해서는 상당 기간 선제적으로 심리전을 전개할 것이다.

제 3 절 소결론

북한은 사회주의 한계와 독재정치의 패착으로 시간이 갈수록 벌어지는 한국의 국력과 국방력의 격차를 해소하기 위해 비대칭 전력을 강화하고 있으며 그 중 사이버 전력은 불법적인 경제적 수입까지 창출할 수 있는 매력적인 수단이기에 전력의 증가에 심혈을 기울여 왔다. 그 결과 북한의 사이버 공격능력은 양적, 질적으로 전 세계에서 최상위수준으로 평가받고 있다. 특히 한국 사이버 환경의 높은 개방성과 의존성은 북한이 사이버전

128) 부형욱, "우크라이나에서의 하이브리드전과 우리 안보에의 함의,"『동북아안보정세분석』, 한국국방연구원(2022), p. 34.

능력을 강화시키는 유인책으로 작용하였다. 게다가 분단의 환경이 가져온 한국 사회 내부의 이념 갈등과 경제적 갈등 등은 북한이 평시부터 사이버 심리전을 수행하기에 최적의 환경을 제공하였다.

북한의 사이버전 수행목표는 한국의 사회 혼란 조성, 외화벌이, 체제선정, 군사작전 방해 및 국가기능 마비이며, 사이버 공간의 광역성, 익명성, 비가시성을 최대한 활용하여 한국 및 동맹국들을 대상으로 사이버전을 수행하고 있다. 북한의 사이버전 조직은 노동당과 국방위원회가 각각 사이버전 조직을 편성하고 있어 중국의 체제(공산당 총괄)와는 다소 상의하고 사이버 심리전과 관련된 기능이 중복적으로 편성되어 있다는 특징이 있다. 이는 사이버 심리전이 사이버 기술공격(테러)과 비교하면 북·중 관계, 낮은 사이버 인프라, 국가 주도의 사이버 교육체계, 한국의 방어능력 향상 등의 제약을 상대적으로 적게 받기 때문임을 인식하고 있기 때문이다.

인터넷의 발전과 개방성을 보장하는 자유민주주의 국가에서는 이제 개인 의견이 SNS 여론형성에 영향을 미치는 것이 아니라 SNS가 개인의 견을 지배하는 구조가 되었다. SNS 여론은 정치에 그대로 반영되고 있다. 대표적인 경우가 킹크랩(댓글 조작 프로그램) 사건이다. 한국 대법원은 2021년 7월 21일 인터넷 댓글이 주권재민의 정치 원칙을 훼손하였다고 판결하였는데 이는 댓글 우선순위가 유권자의 정치적 선택에 상당한 부분 영향을 미친다는 점을 인정하였기 때문이다. 북한은 2016년 이후 러시아가 유럽, 미국 등 서구사회의 선거에 개입하려 했던 사례처럼 한국의 선거 시기에 여론을 조작해 친북 정권을 만들려 할 것이다. 또한, 핵을 투발할 수 있는 탄도미사일, 전략 순항미사일, 핵 어뢰, 핵 잠수함 등의 비대칭 전략무기들과 함께 사이버 심리전을 전개하여 한국 정부의 대북정책 실패와 무용성을 강조하여 정부에 대한 신뢰를 무너뜨리고 사회갈등을 증폭시킬 것이다. 또한, 정치적 판단에 따라 2022년 12월 26일 무인기 침투와 같은 재래식 전력을 활용한 도발적 행동과 결합한 사이버 심리전을 전개하여 위기를 고조시킬 것이며, 전면전을 전제로 한 사이버 심리전을 위해 전략을 발전시키고 수단을 확장하기 위해 준비하고 있을 것이다.

제 4 장 한국군 사이버 심리전 운용방안

제 1 절 사이버 심리전 운용 전략 수립

이상호(2014, p. 32)는 북한의 사이버 심리전에 대한 대응을 위해 전시 또는 위기 시 인터넷 통제 또는 폐쇄가 효과적인 대안이라고 제시하였다. 적의 사이버 심리전 수행수단이 되는 국내 인터넷망을 제한하거나 폐쇄하여 적의 위협 자체를 막고자 하는 것이다. 하지만 물리적으로 전시 기간이 짧고 전·평시 구분이 없는 사이버전의 특성상 인터넷 통제로 얻을 수 있는 국가안보의 이익보다는 손실이 더 클 수밖에 없다. 금융, 주식, 유통에서의 혼란으로 인한 경제적인 손실과 생활의 혼란으로 인한 국민의 심리적 불안, 언론 통제로 인한 대외적인 국가 이미지 추락 등이 그것이다. 또한, 외부로부터의 댓글을 통한 사이버 심리전 공격에 대해 동일한 댓글로써 대응할 수 있다는 과거 사이버 심리전 방어 전략은 국민에게 불신을 받고 불안을 조성함과 동시에 더 큰 사회적 혼란을 일으켰다. 댓글작성 기준의 모호성은 정치적 목적으로 악용될 수밖에 없다. 따라서 방어에 중점을 둔 명확한 사이버 심리전 전략이 필요하다.

방어에 중점을 둔 전략은 크게 세 가지로 나눌 수 있다. 바로 예방, 식별, 대응이다. 여기에서 예방이란 적의 사이버 심리전 자체를 예방(완전한 예방은 불가능)하고 적의 사이버 심리전에 대한 오염을 예방한다는 의미이다. 식별은 북한의 사이버 심리전 징후를 신속하고 정확하게 파악하는 역량을 말하며, 대응은 식별된 북한의 사이버 심리전을 최단 시간 내 차단하고 사이버 심리전으로 인한 피해를 최소화할 수 있는 역량을 말한다. 즉, 북한의 사이버 심리전이 국민이나 장병들에게 영향을 주지 못하도록 예방하고 능동적으로 식별하고, 이후 신속한 대응으로 추가 피해에 대한 확산을 방지한다는 개념이다.

예방 분야에서는 적의 사이버 심리전 오염을 예방하기 위한 장병들에 대한 대적관 확립 교육 등 정신교육을 강화하고 전·평시 가장 직접적이고 치명적인 심리전 오염 통로인 스마트폰에 대한 위협을 고려하여 장병 휴

대폰 할용 전략을 수립하는 것이며, 사이버 기술공격과 사이버 심리 공격 수단으로 활용되는 개인(장병)정보 보호를 위한 조직과 제도를 강화하는 것이다.

식별 분야에서는 우선, 국가사이버안보센터 및 사이버작전사령부에서 사이버 전 영역에 대한 관제를 수행하면서 모든 가용한 정보자산을 활용하여 적의 심리전 징후와 활동을 수집한다. IP, 접근경로, 특정 정치기사에 대한 비정상적이고 조직적인 추천 수 증가(조작으로 인한 개연성), 전달 및 전파 속도 등의 정황증거를 수집한다. 위 정보를 모두 종합하여 해당 행위가 가지는 영향력과 파급력을 분석하고 사이버 심리전 여부를 최종 판단한다. 아울러 작전술 및 전술 제대에서도 대사이버공간정보활동을 강화하여 아군의 정보체계에 대한 해킹 시도와 사이버 심리전 징후에 대해 정황증거를 수집하여 보고하는 체계를 갖춰야 한다.

대응단계에서는 우선, 사회적 파급력이 강력하고 즉각적인 대응이 필요한 사안에 대해서는 정부 주도의 명확한 사실관계 검증과 언론을 통한 공표가 필요하다. 천안함 민군합동조사단 조사위원이었던 조광현 예비역 대령은 2018년 동아일보 인터뷰에서 “천안함 논쟁은 편향동화(偏向同化)와 집단극화(集團極化)의 정점을 보여주는 듯하다. 북한 잠수정이 어뢰를 발사하는 것을 본 사람이 없는 이상, 이 논쟁은 진실과 상관없이 꽤 오랫동안 지속되고 과학적 논쟁을 넘어 정치적 공방으로 정부에 대한 불신과 남남갈등을 부추긴다.”라고 하였다.[129] 천안함이라는 초계함 1척의 해군전력과 46명의 소중한 장병의 희생보다 사건 배후에 대한 불신으로 벌어진 국가적 소모가 더 크다는 것은 그만큼 사이버 심리전이 가지는 영향력을 보여준다. 하지만 천안함 사건의 배후에 대한 정부 발표에 대한 불신은 여론조사결과 다국적 민군합동조사 이후 낮아진 바 있다.[130] 이처럼 정부의 적시적·적극적인 대응은 사이버 심리전의 효과를 반감시킬 수 있다. 특히, 북한의 사이버 심리전 동향에 대한 빅데이터를 수집하여 패턴을 분석한다

129) 조성식, “천안함 좌초라면서 왜 암초는 제시하지 못하나,” 『동아일보』, 2018년 4월 15일; https://www.donga.com/news/article/all/20180415/89616355/1(검색일: 2023년 9월 25일).

130) 심인보, “천안함 5년, 1번 어뢰.. 부실조사로 얼룩진 ‘결정적 증거’,” 『뉴스타파』, 2015년 3월 25일; https://www.newstapa.org/article/lfrkN(검색일: 2023년 9월 25일).

면 향후 발생할 사이버 심리전에서 더욱 유연하데 대응할 수 있음은 물론 선제 대응도 가능할 것이다.

마지막으로 평상시에는 방어적 작전을 수행하되, 의명 공세적인 작전 수행을 위한 능력과 개념도 지속 발전시켜야 한다. 위기 시와 전시에 해당 능력을 적시에 대외(상대국) 또는 대내에 투사할 수 있도록 준비하여야 한다. 반면 그러한 행위가 대내를 대상으로 수행할 경우에는 방어와 공세라는 작전의 성격을 불문하고 윤리적, 법적 문제들을 반드시 고려하여야 한다. 작전의 결과가 누구나 볼 수 있는 형태로서 나타나기 때문에 민간인 구별의 방법이 온전한 형태로 존재할 수 없기 때문이다. 따라서 보호의 대상인 국민이 작전의 결과에 영향을 받을 수 있다는 점을 고려하여 작전 수행의 구체적인 전략을 수립하여야 한다.(Baker, 2010, pp. 17−18)

제 2 절 조직과 임무 정비

한국군은 2009년 7월 7일 시작된 북한의 7·7 디도스(DDoS) 공격을 계기로 사이버전 관련 임무를 위해 2010년 1월 11일에 국군사이버사령부를 창설하였다. 하지만 2012년 대선 당시 불법 정치 댓글작성 등으로 논란을 일으켜 2018년 8월 기존 사이버사의 사이버 심리전 기능을 완전히 폐지하고 명칭도 '군 사이버사령부'에서 '사이버작전사령부'로 변경되었으며, 2019년 2월부터는 국방부 직할부대로 유지하면서도 합참의 작전통제를 받는 합동부대로 변경되었다. 합참이 수행하는 다른 군사작전과의 연계성 측면에서는 합동부대로서의 사이버작전사령부가 보다 더 유리해졌다고 평가할 수 있으나 북한의 사이버 심리전 위협의 치명성과 확대, 러시아−우크라이나 전쟁의 사이버 심리전 양상을 고려했을 때 사이버 심리전 기능을 예전과 같이 부활시켜야 한다.

신원식 한국 국방부 장관은 2023년 11월 16일 국방부가 주최하고 사이버작전사령부가 주관하는 '2023 화이트햇 콘퍼런스(White Hat Conference)[131]'에서 "북한은 전 세계를 대상으로 무기 개발과 우주 관련 첨단기술

131) 국방부가 주최하고 사이버작전사령부가 주관하여 사이버 분야 우수 인재 발굴과 국방 사

을 해킹하고 있다. 개인정보를 유출해 사이버 첩보 활동을 벌이거나 가상자산을 탈취해 핵·미사일 개발에 활용하기도 한다. 사이버 전투역량은 국가안보의 핵심이며, 산·학·연과 함께 첨단 사이버 기술을 개발하고 지능형 방어체계와 공세적 대응체계를 구축할 것"이라고 밝혔다.[132] 북한의 사이버전 위협을 직시하고 기존의 과학기술전문사관, 사이버전문사관 등 사이버 전문인력들의 군의 이탈 현상[133] 들을 고려한 긍정적인 정책이나 여기에도 사이버 심리전 위협이나 전략, 역량 강화를 위한 메시지는 없다. 현재의 사이버작전사령부도 외부의 사이버 기술전에 제한되어 있다. 앞서 기술한 것처럼 북한은 중국과의 관계, 경제적 낙후, 한국의 사이버 방어능력 발전 등의 제한사항과 사이버 심리전의 경제성과 효율성, 파급 효과, 방어의 어려움, 한국 사회의 취약성 등을 고려 시 향후 사이버 기술전보다는 공격적인 사이버 심리전에 더욱 집중할 것인데 아직 한국군의 대비는 미비한 실정이다.

사이버 심리전 기능을 부활시키더라도 그 임무는 정치적 환경과 군의 중립성 등을 고려 시 평시에는 사이버 심리전의 관제와 위협분석 등 방어적 사이버 심리전에 집중할 필요가 있다. 이는 과거 댓글 조작으로 인한 국민적 정서와 신뢰의 문제를 해결하는 동시에 필수 불가결한 작전의 공백을 줄이는 방안이기 때문이다. 사이버 심리전의 공세적 수행은 비밀로서 공개되어서는 안 되고, 비밀누출 시 작전 수행에 제한뿐 아니라 국제사회에서의 신뢰 또한 크게 하락할 수밖에 없다. 하지만 사이버 심리전의 관제와 위협분석은 정보를 공유, 공개함으로써 실익을 얻을 수 있기에 정보유출로부터 상대적으로 자유롭다. 또한, 위협에 대한 분석과 판단절차는 국가기관 감사 또는 국회의 국정감사를 통해 견제받을 수 있다.

방어의 관념에서는 적의 사이버 심리전을 신속히 탐지하기 위한 사이버 인프라와 사이버 전문인력이 중요한데 사이버 인프라는 이미 사이버작

이버 안보 역량 강화를 위해 2013년부터 매년 시행 중인 정례 콘퍼런스.

132) 조재형, "신원식 국방장관, 산·학·연과 사이버기술 개발…공세적 대응체계 구축," 『아주경제』, 2023년 11월 16일; https://www.ajunews.com/view/20231116161010926(검색일: 2023년 11월 18일).

133) 허고운, "'4명 중 1명 임관 포기'… 軍 '과학기술전문사관' 뜯어 고친다," 『news1』, 2023년 11월 17일; https://www.news1.kr/articles/5233791(검색일 : 2023년 11월 19일).

전사령부에 구축된 관제 시스템 등을 활용한다면 단기간에 확보 가능할 것이다. 그러나 문제는 전문인력이다. 현재 한국군의 사이버 전문인력은 사이버 기술전에 특화된 인력들이다. 2014 도입한 과학기술전문사관은 국방부가 과기부와 협업하여 이공계 대학의 우수 학생을 후보생으로 선발해 대학 재학 중 2년간 국방과학교육, 국방과학연구과제 수행 등 양성 과정을 거치게 한 뒤 대학 졸업과 함께 소위로 임관해 국방과학연구소(ADD) 등 국방 연구개발 기관에서 3년간 복무하게 하는 제도다. 또한, 국방부가 고려대와 협업하여 임관시키는 사이버전문사관 또한 해킹과 전자정보전 등 사이버 기술전을 위한 전문인력들이다. 물론 사이버 심리전 방어를 위한 관제 기술은 사이버 방호 기술에서 출발한다. 하지만 징후를 식별하고 의도를 분석하고 대응 개념을 설정하며 민·관·군 협력을 수행하는 일은 사이버 기술전을 초월하는 것으로서 별도의 전문인력 양성이 필요하다. 물론 합동부대의 특성상 합참을 중심으로 한 제 기능의 통합을 바탕으로 정책 기획 및 계획, 정보 획득 및 분석, 징후 식별, 대응 개념 개발 등을 이룰 수는 있을 것이다. 하지만 전·평시 구분이 없고 키네틱과 비키네틱 수단과 동시에 융합되어 동원되는 하이브리드 전쟁의 특성을 고려한다면 어느 정도의 사이버 심리전을 위한 전문 조직과 인력은 필수적이다.

또한, 위기 시와 전시에 공세적 사이버 심리전에 대한 필요성도 인식하여 이에 대한 개념과 능력을 발전시켜야 할 것이다. 사이버 심리 공격에서는 전통적 심리전과 같이 전문적인 선전물 제작능력이 중요하다. 그러나 전통적인 심리전 콘텐츠 제작능력을 보유하고 있는 국군심리전단은 사이버 전장의 기술적 기반이 축적되지 않았기에 사이버 심리전을 수행하기에는 제약이 따른다. 이에 따라 국군심리전단의 일부 조직을 사이버작전사령부로 통합시키거나 심리전단에 사이버 심리전을 수행할 수 있도록 개편하여 능력을 갖추는 것도 고려해 볼 수 있다.

사이버 공간의 특성상 사이버 심리전은 군 영역에 국한되지 않고 광범위하게 발생한다. 따라서 국가 사이버 영역의 관제는 군 뿐만 아니라 민간 영역에서도 수행하고 있다. 국가사이버안전관리규정[134]에 의하면 사이버

134) 대통령훈령 제316호, 2013년 9월 2일 일부개정. 법제처 국가법령정보센터 홈페이지 참조; https://www.law.go.kr/%ED%96%89%EC%A0%95%EA%B7%9C%EC%B9%99/%

공격에 대한 국가 차원의 종합적이고 체계적인 대응을 위하여 국가정보원장 소속에 '국가사이버안보센터'를 둔다. 그리고 국가 차원의 사이버 위협에 대한 종합판단, 상황 관제, 위협요인 분석 및 합동조사 등을 위해 국가사이버안보센터에 '국가사이버위기관리단'을 운영한다. 따라서 해당 규정에 사이버 심리전에 대한 정보수집·분석·전파 등 사이버 심리전 관련 임무를 추가하여 민·관·군이 동시에 상황을 인식하고 분야별 대응을 할 수 있도록 해야 할 것이다. 만약 사이버 심리전이 국가적 혼란을 일으킬 만큼 규모가 크다면 국가 차원에서 사이버 심리전을 수행할 수 있는 컨트롤 타워를 만들어 적시 대응할 수 있어야 한다. 국방 분야에서는 민·관·군이 공유한 상황 정보를 토대로 작전 수행의 영향성을 판단하고 군 차원의 대응방안을 수립·시행할 수 있을 것이다. 즉, 민간과 국가기관의 사이버 심리전 관제 임무를 과학기술정보통신부 및 국가정보원이 주관하고, 각 영역에 대한 관제 정보 종합 관리를 국가사이버안전관리규정에 따라 국가사이버안보센터에서 수행해야 한다. 또한, 필요시에는 민·관·군 상시 협력조직을 설립하여 상호보완 및 합동 대응하여 작전영역 간 효율성을 높여야 한다.

한편 작전술 및 전술 제대에서는 사이버 심리전 예방을 위한 조직 보강 및 임무 정비에 집중할 필요가 있다. 개인정보보호 능력을 강화하는 것이다. 개인정보보호위원회에 따르면 지난 2019년 공공분야 홈페이지에서 개인정보 노출을 탐지 및 삭제한 건수는 875건이며, 민간부문에서는 1만 2,615건에 이른다.[135] 또한, 정부와 군 주요 인사 개인정보를 수집하기 위한 시도도 지속되고 있다.[136] 개인정보는 내부인의 관리 소홀이나 금전 취득을 위한 판매 목적으로 누출되거나 범죄조직의 해킹으로 누출(북한에 의해 재탈취 가능)되거나. 북한의 해킹에 의해서도 누출된다. 이렇게 노출

EA%B5%AD%EA%B0%80%EC%82%AC%EC%9D%B4%EB%B2%84%EC%95%88%EC%A0%84%EA%B4%80%EB%A6%AC%EA%B7%9C%EC%A0%95(검색일; 2023년 12월 2일).

135) 엄호식, "보안·ICT 분야 키워드로 미리 살펴본 2021 국감 ①개인정보·기업보안," 『보안뉴스』, 2019년 9월 29일; https://www.boannews.com/media/view.asp?idx=101103&kind=(검색일: 2023년 11월 1일).

136) 중앙일보 사설, "북한 해킹에 번번이 당하는 IT 강국 한국," 『중앙일보』(인터넷판), 2022년 10월 26일; https://www. joongang.co.kr/article/25128635(검색일: 2023년 11월 18일).

된 개인정보들은 범죄에 이용되기도 하고 사이버 기술공격과 사이버 심리전에도 활용된다. 특히 앞으로 더욱 인간의 삶이 IT를 중심으로 통합되는 정보융합·컨버전스 사회에 살게 될 것이기 때문에 개인정보보호의 중요성은 더욱 중요해질 것이다. 따라서 단순히 IT의 문제로만 생각하고 해커 검거와 같은 관련 기술과 장비 개선 등의 논의들에서 벗어나 국가 정보보호 및 국가 정보망 방어를 위해서는 보다 고차원적이고 종합적인 관리가 필요하다. 개인 정보보호 강화를 위한 보다 구체적이고도 확실한 정책 집행이 필요하다. 한국군도 막대한 양의 개인정보보호를 위해 군 정보통신망 보호와 함께 제대별 개인정보보호 책임관을 임명하는 등의 규정과 제도를 갖추고는 있지만, 인력 및 인식 부족으로 군사정보 보호 활동(군사보안)에 제한되어 있어 관련 규정 및 조직 보강이 필요하다.

제 3 절 주요 언론 공조 및 법령·규정의 정비

국내 최대 포털 사이트인 '네이버'는 2018년 지방 선거를 앞두고 댓글을 이용한 여론 왜곡을 막기 위해, 선거 관련 기사의 댓글 정책을 변경하였다.[137] 이는 독자들이 정치 관련 여론을 주로 기사 제목과 댓글의 추천수를 통해 인지하기 때문이다. 네이버는 정치 관련 기사의 '순공감수' 정렬 기준을 제공하지 않음으로써 정보 왜곡으로 인한 편향적 인지를 방지하였다. 또한, 더 나아가 2018년 10월에는 정치기사에 한해 댓글 관리를 해당 기사의 언론사에 맡김으로써 여론조작의 책임에서 멀어지고자 했다. 드루킹의 댓글 조작 사건을 통해 댓글 공감수 조작이 여론 왜곡을 일으킬 수 있다는 사실을 역설해 볼 수 있듯이, 네이버의 새로운 댓글 관리 정책은 바로 이러한 점에 착안한 영리한 정책일 것이다. 네이버뿐 아니라 주요 언론사와 포털 사이트의 정치기사 관련 공감수 정렬 기준을 제공하지 않는 등 유연한 협의가 이루어진다면 방어적 대내 사이버 심리전의 방어에

137) 주영재, "네이버, 선거기간 정치기사 댓글 직접 노출 않는다,"『경향신문』(인터넷판), 2018년 5월 16일; https://www.khan.co.kr/economy/industry-trade/article/201805162305015 (검색일: 2023년 11월 18일).

도 큰 효과가 있을 것이다. 또한, 조직적인 댓글작성 방지를 위한 필터 연구도 필요하다. 인터넷 기사 등 댓글의 수는 사람이 하나씩 판단하여 걸러낼 수 있는 범주를 벗어난다. 이러한 여론조작을 사후에 밝혀내는 것은 이미 이슈화되어 사회적 파장을 일으킨 이후라면 큰 의미가 없다. 따라서 여론조작 댓글을 사전에 판단하여 방지하는 필터 개발이 필요하다(정연태 외 6명, 2018, p. 3). 조작 댓글에 대한 특징을 빅데이터로 수집·분석하여 대중을 선동하는 댓글의 특성을 판단하고, 이를 자동화 필터링하거나, 댓글마다 조작 댓글 확률을 표시해 준다면, 대중의 정상적 인지를 도와줄 것이다. 장기적으로는 댓글 정책의 효과와 부작용을 면밀히 분석하여 정책 수립의 법적 근거를 마련하여야 한다. 우선, 사이버작전사령부령 등에 해당 임무를 명시하여 법적 근거를 명확히 해야 한다. 동시에 행정규칙(국방부 훈령, 사령부 작전예규 등)에 구체적인 임무 내용을 포함하여 재·개정해야 할 것이다. 또한, 외교적으로 사이버 심리전의 주체가 북한이나 다른 국가일 경우 해당 증거를 수집하여 국제사회의 지지 확보 및 향후 자위권 수행의 명분으로 활용해야 할 것이다.

또한, 장병들에 대한 적 사이버 심리전 오염될 수 있는 가장 위험하고 직접적인 통로인 휴대폰 사용에 관한 법령 정비가 필요하다. 휴대폰은 인터넷 기반으로 실시간 정보확산이 가장 용이한 수단이다. 2022년 러시아-우크라이나 전쟁에서 양국은 자국 장병의 사기 진작 및 적국 장병의 사기 저하, 자국민 항전의식 결집 등의 전략적 목적을 위해 사이버 심리전을 적극적으로 수행하였는데 휴대폰이 주요한 수단으로 활용되고 있다. 러시아는 SNS를 통한 허위정보 유포 등으로 우크라이나 국론 분열을 위한 사이버 심리전(사이버 기술공격 병행)을 전개하였으며, 우크라이나는 SNS(트위터) 기반으로 전쟁의 부당성을 지속 강조하며 자국민 장병의 전의 고양과 국민의 항전 의지 결집을 위해 다양한 정보를 실시간으로 공개하고, 대통령 등 지휘부 활동을 노출하는 등의 전략을 구사하였다. 2023. 5. 24. 기준 젤린스키 대통령의 트위터 팔로워 수는 730만 명으로 이를 적극적으로 활용하고 있다. 이처럼 양국의 치열한 사이버 심리전의 핵심 수단으로 활용되고 있는 것이다. 이는 한국군에게 위기 및 전시 장병들의 휴대

폰을 어떻게 관리하고 활용할 것인가에 대한 시사하고 있다.

한국군은 2020년 7월 1일부로 병사들의 휴대폰 사용을 전면 허용한 뒤 최근에는 병 휴대전화 소지 시간을 확대를 추진하고 있다.[138] 하지만 전시상황에서의 개인 휴대전화 관리 규정 및 지침은 미흡한 실정이다. 평시 규정 중 일부는 전시에도 적용 가능하나, 전시 상황을 고려한 구체적인 대책과 관리방안 미흡하다. 장병들은 휴대폰을 통해 실시간 인터넷 및 SNS 접속하거나 외부로부터 메시지를 수신하는데 이로 인해 전투 집중력이 저하되고 아군의 민감정보 노출(군사자료, 작전 상황 등)될 수 있다. 또한 적의 사이버 심리전 공격에 표적이 될 수 있으며 허위정보로 인한 판단력이 저하되고 전의가 상실될 수 있다. 분실시에는 아군 및 개인의 정보가 유출되어 후속 사이버 공격 수단으로 활용될 수도 있다. 물론 전·평시 휴대폰의 긍정적인 역할도 있다. 이번 러시아-우크라이나 전쟁에서 휴대폰은 장병들의 심리적 안정을 위한 외부와의 소통, 정보(표적 정보, 전쟁범죄 증거 수집, 전투현장 영상 등)를 수집하는데도 기여하고 있기 때문이다. 따라서 이러한 순기능과 역기능을 모두 고려한 '전·평시 장병 휴대폰 활용 전략'을 수립해야 한다.

이를 위해서는 여러 가지 요소를 고려해야 한다. 북한의 폐쇄된 인터넷 환경 및 정보통신체계를 고려한다면 한국이 북한군의 휴대폰을 활용한 사이버 심리전이 극히 제한된다. 물론 우크라이나가 일부러 휴대폰을 유기하여 러시아군이 사용하게 함으로써 표적정보를 획득한 것처럼 한국의 휴대폰을 활용한 심리전을 펼칠 수도 있겠지만 현존하는 북한과 사이버 심리전 능력과 의도, 위협의 확장을 고려해 볼 때 북한의 사이버 심리전에 대응하는 것에 집중할 필요가 있다. 또한, 전시 상황은 개인 휴대전화 사용 위규 행위에 대한 체계적인 관리가 제한되며, 위험의 치명성 고려 시 사후 조치의 효과성이 떨어지기 때문에. 전시 상황의 추가적인 위협 및 특성을 고려한 규정 및 운용관리 방안 보완이 필요하다. 전시 부대 및 임무 특성에 따른 작전적 효용을 고려하여 예외적 상황이 도래할 수 있으므로 지휘관 판단을 위한 결정기준(고려요소) 검토도 필요하다.

---

138) 권구찬, "아침 점호서 21시까지…병사 휴대폰 사용 확대," 『서울경제1』, 2023년 5월 11일; https://www. sedaily.com/NewsView/29PJCKGHFN(검색일: 2023년 11월10일).

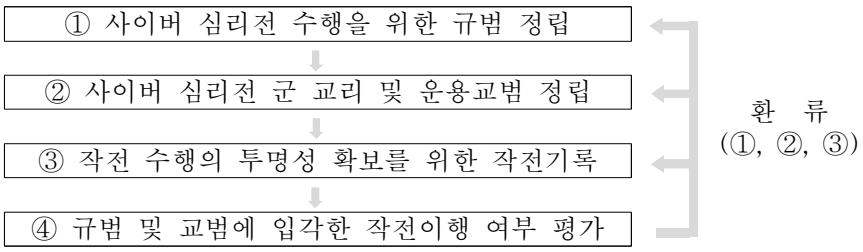
특히 동원병력의 개인 휴대전화 반입 절차 등 관리방안, 예비군 대상 교육도 부재하다. 동원병력은 개인 휴대전화 사용과 관련한 미통제 상황에서 소집되므로 전시 상황에서 심리적 동요가 더욱 심화할 수 있으며, 개인 휴대전화와 관련된 영향 또한 상대적으로 크게 나타날 수 있다. 영국 국방정보국은 2023년 1~5월 러시아군의 탈영자 재판이 1,052건으로 집계된 것으로 조사하였는데 이는 2022년 전체 탈영 재판 건수를 초과한 숫자인데 이는 병력 동원 후 예비군 증가에 따른 영향을 분석하고 있다.

따라서 전·평시 장병 휴대폰의 순기능과 역기능을 종합적으로 고려하여 전략을 수립하고 이를 훈령 형식 등 명시적 규정을 정립해야 하며, 취약성에 대해서는 평시부터 교육을 강화하여야 한다. 이와 더불어 모바일 기기의 장점을 고려하여 한국의 작전환경에 적용 가능한 군사작전 시 임무수행 전용 스마트 기기 및 관련 기술 개발 노력 지속도 병행해야 한다.

제 4 절 사이버 심리전 운용체계 정립

앞에서 설명한 사이버 심리전 수행을 위한 조직과 수행전략, 법적 근거가 마련되었다면 이를 합법적이고 효율적이면서 지속 가능한 운용체계를 정립해야 한다. 사이버 심리전 운용체계는 다음 그림과 같은 수행주기를 가져야 한다.

<그림 4-1> 사이버 심리전 운용체계



우선, 사이버 심리전 수행을 위한 법률, 도덕, 관습과 같은 규범에 대

해 정립을 통해 행위에 대한 법적 근거를 확보해야 한다. 임무 수행 인원의 직무수행 위법 논란을 최소화해야 하며 이를 통해 더욱 적극적인 작전 운용을 해야 한다. 법적 근거를 토대로 군 교리와 하위 교범 및 메뉴얼에 대한 적시적인 수정이 수행되어야 하고, 이를 통해 실제 임무 수행과 교리 간의 괴리가 없어야 한다. 또한, 모든 작전의 수행 과정과 내역이 투명하게 기록되어야 한다. 이를 바탕으로 규범과 교리에 어긋남이 없는지 주기적인 평가를 해야 하고 평가결과는 다시 운용체계 정립을 위해 환류되어야 할 것이다.

마지막으로 이러한 사이버 심리전 운용체계는 전략적 수준에서 국가안보목표, 국방목표에 부합되어야 하며, 작전적 수준에서는 군사목표 및 군사작전과 연계되어야 할 것이다. 어디까지나 사이버 심리전의 목적은 항상 적을 향해야 하며 한국 사회에 대한 사이버 심리전 행위를 사전 차단하거나 그 피해를 최소화하고 필요한 경우 적의 작전 수행 의지를 무력화할 수도 있어야 한다는 명확한 방향성을 보유하여야 한다.(Cheng, 2013, p. 5.).

제 5 절 사이버 집단방위체제 구축 및 협력 강화

한국의 사이버 방위(cyber defense)는 미국 일본 등 우방국와 함께 집단방위(collective defense)체제로 발전시키는 것이 타당하다. 앞서 러시아의 유럽 및 미국에 대한 사이버 심리전 사례와 전술, 위협에 대해 살펴보았지만, 중국 역시 2020년 미국 대선에서 트럼프의 패배를 위해 트럼프를 미치광이로까지 묘사하는 선동에 관여되었다. 그리고 COVID-9로 인해 중국이 비난을 받자 오히려 미국의 생물학 무기 실험실에서 COVID-9가 유출되었다는 허위정보를 퍼뜨리고 소셜미디어의 트롤을 이용하여 허위여론을 형성하여 미국 국민에게 혼란을 초래하려는 시도가 있었다.[139] 또한, 명확히 밝혀진 바 없으나 소수의 언론 보도에 따르면, 지난 박근혜

139) Homeland Security. 2021. Homeland Threat Assessment October 2020. p. 20.

대통령 탄핵 시도에서도 중국이 한국 내의 여론조작에 관여했다는 주장이 제기된다.[140] 특히, 미·중 전략경쟁으로 인해 서구권 민주주의와 러시아와 중국을 중심으로 한 권위주의 레짐 진영 간 경제와 안보 영역의 긴장과 갈등이 확대되고 심화되는 현재의 국제정치 정세를 감안하면 중국의 對한국 영향력 공작, 허위조작정보 등을 이용한 프로파간다 위협은 증가할 것이며, 러시아의 서구사회에 대한 사이버 심리전 효과를 지켜본 북한 또한 사이버전 역량을 강화하고 보다 적극적으로 한국에 대한 사이버 심리전을 강화할 것이기 때문이다.

NATO와 EU는 러시아의 사이버 심리전의 심각한 위험성을 자각하고 집단사이버 방위체계를 구축하고 정기적인 모의훈련을 통해 대응 능력을 숙달하고 있다. NATO는 2018년 브뤼셀 정상회담(Brussels Summit)에서 사이버 심리전을 포함한 사이버 공격에 대응할 조직이자 NATO의 강화된 명령체계 일부로서 'NATO사이버공간작전센터(NATO Cyberspace Operations Centre, COC)'를 'NATO연합변혁사령부(Allied Command Transformation, NATO's ACT)' 산하 'NATO센터(NATO Centres of Excellence, NATO COEs)'에 설치할 것을 결정했다. 이러한 새로운 조직을 통해 NATO는 24시간 동맹국의 도움 요청에 응할 수 있는 'NATO 사이버신속대응팀(NATO Cyber Rapid Reaction teams)'도 운영하고 있다.[141] 또한, NATO는 2000년대 초부터 사이버전을 대비하는 다양한 연례 군사훈련을 수행해왔다. NATO가 새롭게 마련한 방위태세와 군사훈련 대부분은 평시와 전시를 구분하지 않는 사이버 심리전을 비롯한 다양한 사이버 공격 및 하이브리드전 상황을 상정한 군사적 대응 및 시민사회 보호에 집중되어 있다. 2016년부터 NATO의 '위기관리훈련(Crisis Management Exercise, CMX)'은 사이버 테러, 소셜미디어를 통한 허위조작정보의 유포 및 해킹, 테러 등이 복합적으로 일어날 수 있는 하이브리드 위협에 민간과 군이 함께 대응하는

140) 나혜윤, "<동아일보>간부 "중국 정부, 박근혜 탄핵하려 중국 유학생 6만명 동원" 중국 반발 등 후폭풍 우려, 민주당 "가짜뉴스로 朴대통령 비호,"『Views & News』, 2017년 1월 31일; http://www.viewsnnews.com/article?q=141360(검색일: 2023년 10월 26일).

141) NATO COEs는 NATO의 지휘체계에 속하지 않으나 'NATO명령협정(NATO Command Arrangements)'을 지원하는 기능을 수행하며 각각의 전문성과 기능을 갖춘 여러 기관의 네트워크 형태의 다국적 조직임.

훈련을 하기 시작했으며,[142] NATO의 '사이버방어협력센터(Cooperative Cyber Defence Centre of Excellence, CCDCOE)'는 이미 2010년부터 사이버 방위훈련인 '라키드쉴드훈련(Excercise Locked Shields)'을 주도하고 있다.

2008년부터 사이버 공격 상황에서 NATO내 다양한 조직 간 공조와 전략적 의사결정을 모의 연습하기 위해 수행하고 있는 NATO의 연례 사이버 방위 주력훈련(flagship exercise)인 '사이버연대(Cyber Coalition)'에는 EU도 매년 참여하고 있다. 사이버연대 훈련은 NATO연합변혁사령부(ACT) 주도로 수행되며, NATO COC가 사이버전의 기술적, 절차적 모의훈련을 주도해오고 있다. 이러한 모의훈련을 통해 미국과 EU 회원국들은 사이버전과 관련 주요정보를 공유하고 상황을 함께 판단하며 사이버 작전을 조정, 협력하며 군사작전을 함께 수행하는 능력을 향상시키고 있다. 2017년에는 특별히 사이버 심리전을 포함하여 하이브리드전 상황을 염두에 둔 모의훈련을 수행했으며, 2019년의 훈련은 급속도로 발전하는 디지털 기술환경의 새로운 도전에 대응하고자 AI 기술을 이용한 다양한 시뮬레이션 실험을 수행하고 있다. 그러한 시뮬레이션 훈련에는 AI가 사람 대신 적의 행동을 분석하고 공격 및 이상 징후를 감지하여 대응시간을 확보하는 실험, 적의 행위와 의도 간의 복잡한 인과관계를 파악하거나 사이버 공간에서 발생하는 다양한 수준의 위험을 파악하고 적절한 의사결정 및 대응 행위를 취하는 목적의 머신러닝(machine learning)을 통한 다양한 알고리즘을 개발이 포함되었다.

EU 차원에서도 2016년부터 하이브리드 위협에 대응하는 일련의 제도적 이니셔티브와 절차를 적극적으로 마련하고 NATO와의 공조를 통해 대응책을 도모하기 시작했다. 2016년 2월 EU와 NATO는 'EU 사이버 방위 정책 프레임워크(EU Cyber Defence Policy Framework)'에 근거하여 '사이버 방위 기술협정(Technical Arrangement on Cyber Defence)'을 맺고 사이버 공격과 관련된 정보공유, 군사훈련, 연구 등의 분야에서 긴밀한 협력을 도모하기로 천명했다.[143] 또한, EU 집행위원회는 'EU정보정세센터

142) NATO, "Crisis Management Exercise 2019" Press Release (May 3, 2019); https://www.nato.int/cps/en/natohq/news_165844.htm(검색일: 2023년 2월 9일).

143) NATO, "NATO and the European Union enhance cyber defence cooperation"(February

(EU Intelligence and Situation Centre, EU INTCEN)'에 'EU하이브리드 퓨전반(EU Hybrid Fusion Cell)'을 설립하여 특히 사이버전에 대비한 하이브리드 위협 대응체제를 갖춰나갔다. 이 조직들은 사이버 심리전 공격을 모니터링하고 관련한 주요정보를 취합하고 분석하며 EU 정책결정자들에게 구체적인 정책을 제안하는 기능을 담당하고 있다.[144]

하이브리드 위협 상황을 전제한 유럽의 다양한 모의 군사훈련도 EU와 NATO 간 긴밀한 공조를 통해 진행되고 있다. 'EU HEX-ML 18 (Hybrid Exercise - Multi Layer 18)'와 'NATO-EU 페이스훈련(NATO-EU Parallel and Coordinated Exercise, PACE)'와 같은 모의훈련은 모두 사이버전과 허위조작정보 유포를 통한 심리전 공격 및 범죄·밀수·테러와 관련된 복잡한 하이브리드 위기 상황이 일어나는 시나리오를 가정하고 정보교환 및 효과적인 위기 대응을 연습한다. 이 두 훈련에는 EU위기대응반(EU Crisis Response Cell)도 참여하며 NATO국제군간부(NATO International Military Staff)들과 EU군간부(EU Military Staff) 간 교육교류도 활발하게 이루어지고 있다.[145]

EU 집행위원회가 2019년 5월에 발간한 하이브리드 위협 대응에 대한 보고서 "유럽의 보호: 하이브리드 위협 대응 진척사항(A Europe that protects: good progress on tackling hybrid threats)"는 2016년 브뤼셀 공동성명에서 천명했던 22개 분야 실행계획에 대한 성과를 담았다. 이 보고서에서 주목할 것은 사이버전 및 비전통 안보와 관련된 항목에서 많은 조치가 취해진 것으로, 보고서는 허위조작정보에 대응하여 신속하게 사실을 전달하고 대중의 경각심을 높이는 전략커뮤니케이션을 강화한 것과, 사이버 안보(cyber security)와 사이버 방위(cyber defense) 강화를 위해 사이버전 공격국에 대해 EU가 제재를 취할 수 있는 유럽 최초의 제재 레

10, 2016); https://www.nato.int/cps/en/natohq/news_127836.htm(검색일: 2023년 3월 4일).

144) European Commission, "Joint Framework on countering hybrid threats"(April 6, 2016); https://eucyberdirect.eu/content_knowledge_hu/joint-framework-on-countering-hybrid-threats(검색일: 2023년 11월 1일).

145) NATO & EU, "Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on December 6, 2016 December 5, 2017."; https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/190617-4th-Joint-progress-report-EU-NATO-eng.pdf(검색일: 2023년 11월 1일).

짐(sanctions regime)을 구축했음을 강조했다. 또한, 이 보고서는 생화학, 방사능 및 핵 시설에 대한 공격을 억지할 제재조치를 마련한 것과 에너지 원과 에너지 수송로 등 에너지 네트워크를 다변화시키는 등 에너지 부문에서의 회복력을 증진시키고 주요 인프라 기반을 보호하는 조치를 마련했음을 밝혔다. 이 밖에도 이 보고서는 운송수단, 우주, 공중보건과 식량안보, 극단주의와 테러리즘 등 비전통 안보와 관련된 사안에서 앞으로 유럽이 취할 조치와 실행계획을 구체적으로 소개했다.[146]

물론, 상술한 공동의 대응체제 정비와 조직마련에도 불구하고 하이브리드 위협에 효과적으로 대응하는 데에 있어서 현재의 미국과 유럽의 방위태세는 아직도 많은 문제를 풀어야 한다. 첫째, 현대 대다수 강대국이 관심을 갖는 최첨단 기술에 의한 미래전 위협에 대한 대비는 복잡한 전술을 구사하는 하이브리드 위협에 효과적으로 대응하기가 쉽지 않다. 둘째, 하이브리드전은 과거 비정규전과 달리 고도로 발전된 군사기술과 정보통신기술이 결합하여 사이버전이나 사이버 정보심리전을 동반하는 등 지속해서 진화하며 새로운 형태의 위협을 구사한다. 셋째, 선진국들이 군사혁신에 의한 최첨단 기술로써 단일하게 전투방식을 일원화하는 것은 하이브리드전의 공격 주체의 입장에서는 그러한 조건을 악용할 유인을 갖게 한다. 즉 하이브리드 위협을 구사하는 데에 있어서 공격 주체는 새로운 형태의 공격 형태를 지속해서 발굴할 동기를 갖게 된다. 결과적으로 하이브리드 위협은 전쟁의 모든 스펙트럼을 망라하는 모든 수준에서의, 모든 형태의 분쟁에 대한 대비태세를 요구하므로 각국 군은 그러한 모든 위협에 대응할 인력, 자원, 기술을 갖추어야 한다. 하지만 그러한 대응태세를 갖추는 것은 비용이 많이 들고 군이 적응해야 하는 긴 시간을 요구하므로 앞으로 NATO와 EU는 이 같은 문제를 지속해서 다루며 대응태세를 개선해나갈 것으로 보인다.[147]

---

146) European Commission, “A Europe that protects: good progress on tackling hybrid threats” (May 19, 2019)https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2788; “A Europe that Protects: Countering Hybrid Threats (June 2018); https://www.dsn.gob.es /sites/dsn/ files/ hybrid_ threats _en_final.pdf(검색일: 2023년 10월 5일).

147) Hoffman, Frank G, “Ewamining Complex Forms of Conflict: Gray Zone and Hybrid Challenges,” PRISM, the Journal of Complex Operations 7-4. Washington, D.C.:

이처럼 미국과 유럽이 사이버전 중심의 하이브리드 위협 대응에 있어서 전략커뮤니케이션 체제의 구축과 긴밀한 정보 공유 및 위기상황에 대한 공동의 인식, 다양한 교류 및 연구 활동 지속 등은 한국 및 역내 주요국들이 향후 어떻게 공조하고 협력을 확대해 나갈지 고찰하고 논의하는 데에 있어서 유용한 사례가 될 것이다. 또한, 최근 한국과 전통안보 및 신안보 영역에서 다양한 의제를 통해 교류와 협력을 확대하고 있는 미국과 유럽(EU, NATO)의 하이브리드전 모의 군사훈련 및 다양한 협의체에서의 한국의 참여는 지속되어야 한다. 더불어 한국은 지금보다 다양한 국내 기관과 민간단체, 그리고 전문가들이 EU 및 NATO의 하이브리드 위협 대응과 관련된 훈련, 협의체 등에 동참하고 아이디어를 공유하며 기여와 협력을 증진할 방안을 국가적, 지역적 차원에서 마련하고 장려할 필요가 있다

제 6 절 소결론

한국의 평시 사이버 심리전은 정치적 목적을 위해 악용되지 않도록 방어(예방, 식별, 대응)에 중점을 둔 사이버 전략을 수립해야 한다. 예방이란 적의 사이버 심리전에 대한 오염을 예방한다는 의미이며 식별은 북한의 사이버 심리전 징후를 신속히 파악하는 역량을 말하고 마지막으로 대응은 식별된 북한의 사이버 심리전을 차단하고 적의 사이버 심리전으로 인한 피해를 최소화할 수 있는 역량을 말한다. 즉, 적의 사이버 심리전이 국민과 장병들에게 노출되거나 영향을 주지 못하도록 적극적으로 식별하고, 이후 신속한 대응으로 추가 피해에 대한 확산을 방지한다는 개념이다.

예방 분야에서는 장병들에 대한 대적관 확립 등 정신교육을 강화하고 전·평시 휴대폰이 가장 직접적이고 치명적인 심리전 오염 통로임을 고려하여 장병 휴대폰 활용 전략을 수립하는 것이며, 사이버 기술공격과 사이버 심리 공격 수단으로 활용되는 개인(장병)정보 보호를 위한 조직과 제도를 강화해야 한다. 식별 분야에서는 우선, 국가사이버안보센터 및 사이

National Defense University, 2018.

버작전사령부에서 사이버 전 영역에 대한 관제를 수행하면서 모든 정보자산을 활용하여 적의 심리전 징후와 활동을 수집하고 종합하여 해당 행위가 가지는 영향력과 파급력을 분석하고 사이버 심리전 여부를 최종 판단한다. 아울러 작전술 및 전술 제대에서도 대사이버공간정보활동을 강화하여 아군의 정보체계에 대한 해킹 시도와 사이버 심리전 징후에 대해 정황증거를 수집하여 보고하는 체계를 갖춰야 한다. 대응단계에서는 우선, 사회적 파급력이 강력하고 즉각적인 대응이 필요한 사안에 대해서는 정부 주도의 명확한 사실관계 검증과 언론을 통한 공표가 필요하다. 적시적이고 적극적인 대응은 사이버 심리전의 효과를 반감시킬 수 있다. 특히, 북한의 사이버 심리전에 동향에 대한 빅데이터를 수집하여 패턴을 분석한다면 향후 발생할 사이버 심리전에서 보다 유연하고 선제적인 대응도 가능할 것이다. 마지막으로 평시에는 방어적 작전을 주로 수행하되, 공세적 작전 수행을 위한 능력과 개념도 지속 발전시켜야 한다.

한편, 사이버작전사령부의 사이버 심리전 기능을 부활시켜 평시에는 사이버 심리전의 관제와 위협분석 등 방어적 사이버 심리전에 집중하되 위기 시와 전시의 공세적 사이버 심리전에 대한 필요성도 인식하여 이에 대한 개념과 능력까지 발전시켜야 한다. 또한, 한국군의 사이버 전문인력은 사이버 기술전 분야뿐만 아니라 사이버 심리전 수행(징후 식별, 의도 분석, 대응 개념 설정, 민·관·군 협력 등)을 위한 별도의 전문인력 양성도 필요하며 사이버 공간에서의 민간영역의 확장과 영향력 확대를 고려하여 주요 언론과의 공조를 강화하고 법적 근거를 마련하여 지속 가능한 운용체계를 정립해야 한다.

전략 수립, 능력 및 운용체계를 구비와 동시에 사이버 심리전에서도 집단방위체제를 구축하고 협력을 강화해 나가야 한다. 중국과 러시아 등 권위주의 국가들의 사이버 심리전을 포함한 하이브리드 위협에 대응하기 위한 미국과 유럽의 활발한 협력과 훈련에 적극 동참하고 공조체계를 구축해야 한다. 더불어 더 다양한 국내 기관 및 민간단체와 전문가들이 우방국과의 교류, 훈련 및 협의체에 동참하게 하는 방안을 마련하고 장려하는 것이 한국이 가진 우수한 사이버 인프라를 활용하는 것임을 인식해야 한다.

제 5 장 결 론

제 1 절 정책적 제언

사이버 심리전은 전·평시가 없다. 현재 평시의 북한의 사이버 심리전은 한국사회의 갈등을 부추기고 북한의 핵, 미사일을 비롯한 비대칭무기들을 활용한 무력시위, 무인기 침투와 같은 국지적인 도발과 통합하여 공포심을 확대하고, 한국군의 대응능력을 흠집 내 대군 불신을 부추기고 한국군의 사기를 저하시키고 국론을 분열시키는 이른바 와해(disruption)에 중점을 둘 것이다. 더군다나 한국의 경우 북한의 사이버 심리전은 회색지대 분쟁과 결합한 하이브리드전으로 지금도 일어나고 있다고 봐도 된다. 강도와 시기의 차이일 뿐이다. 국제관계와 국내정치를 고려하여 반복적이고 상습적으로 강도와 방법을 선택하여 하이브리드전을 전개하고 있다.

사이버 공격(기술, 심리)의 모든 분야에서 북한이 비교 우위에 있다. 이는 북한이 사이버전 수행에 있어 한국의 환경이 매우 유리하기 때문일 것이다. 같은 전력으로 싸우는 공성전으로 비유했을 때 대한민국이라는 성은 외부로 향하는 문과 다리가 성벽 외곽에 곳곳에 걸쳐 있지만, 북한이라는 성은 출입문조차 봉쇄한 철옹성에 비유될 수 있다. 전장의 환경이 비대칭적이기에 공략하기 위한 전략도 다를 수밖에 없다. 사이버 환경의 비대칭성에 따라 북한과의 사이버 심리전은 한국의 사이버 공간에서 주로 전개될 수밖에 없다. 우선, 북한과의 사이버 심리전은 평시에도 수행되어 한국 사회를 서서히 패닉과 붕괴로 이르게 할 수 있으므로 철저한 예방과 식별, 대응에 중점을 두어야 할 것이다. 하지만 국가안보의 필요와 목적에 따라 공세적인 심리전 수행 개념과 능력도 발전시켜야 한다.

한국은 과거 사이버 심리전 영향력을 명확하게 인식하고 여러 조직을 창설, 보강하였다. 하지만 사이버 심리전 개념에 대한 명확한 이해, 이를 바탕으로 한 목표와 수행에 대한 구체적인 가이드라인이 모호하여 이른바

‘정치 댓글’ 사건으로 큰 홍역을 치렀다. 그리고 이로 인해 한국군의 사이버 심리전 관련 조직과 기능은 크게 위축되었다. 본 연구에서는 사이버 심리전의 개념과 다양한 사례, 미래전에서의 역할과 중요성을 고찰하였고, 사이버 심리전 수행 관련 법적 근거를 통해 합법적인 사이버 심리전 수행 방안에 대해 알아보았다.

한편, 사이버 심리전이 정치적으로 악용될 수 있다고 하여 그 조직과 기능을 함부로 축소하거나 없애서는 안 된다. 북한의 사이버 심리전 지금도 여전히 진행되고 있으며 더욱 진화하고 있기 때문이다. 민주주의 국가에서는 대중의 인식이 정치에 미치는 영향력은 상당하다. 만약 북한이 한국 대중의 인식변화를 의도대로 변화시킬 수 있다면 국가안보의 중심이 흔들릴 수밖에 없다. 따라서 한국은 사이버 심리전의 한계를 명확히 인식하고, 이를 극복하여 합법적·효율적 사이버 심리전 수행방안을 마련해야 한다.

본 연구는 한국군의 사이버 심리전을 수행방안을 제시하였다. 우선, 방어에 중점을 둔 사이버 심리전 운용 전략을 수립해야 한다. 먼저 장병들의 사이버 심리전 오염을 예방하기 위해 대적관 확립 교육을 강화하고 가장 치명적인 오염 통로인 휴대폰에 대한 전·평시 활용 전략을 수립해야 한다. 식별 분야에서는 국가사이버안보센터 및 사이버작전사령부에서 기존의 사이버 기술공격뿐만 아니라 사이버 심리 공격까지 관제하고, 작전술 및 전술 제대에서도 대사이버공간정보 활동을 수행해야 한다. 사이버 심리전에 대한 대응은 국가사이버안보센터를 중심으로 적시적이고 적극적으로 대응하여 심리전 효과를 반감시키고 빅데이터를 축적함으로써 선제적인 대응도 가능하도록 준비해야 한다. 아울러 위기 및 전시 공세적인 사이버 심리전을 수행할 수 있는 능력과 개념도 지속 발전시켜야 한다.

조직적인 측면에서는 민간영역을 중심으로 국가 사이버 영역 전체를 아우르고 있는 국가사이버안보센터를 컨트롤타워(Control Tower)로 민·관·군 작전 수행 조직과 기능을 다시 보강해야 한다. 국가 사이버 심리전 위협에 대한 국가사이버위기관리단 운영을 통해 공동의 상황인식을 토대로 분야별 조치를 취해야 한다. 특히, 사이버 기술공격뿐만 아니라 심리전 공

격에 대한 관제를 위해서는 조직을 보강하고 전문인력도 양성하여야 한다. 작전술 및 전술 제대 또한 대사이버공간정보 활동이 가능하도록 대정보 부대(서) 등 관련 조직을 보강하여야 한다. 아울러 사이버 기술 및 심리 공격에 활용되는 개인정보보호를 조직 보강과 함께 인식전환, 구체적이고 확실한 정책 집행이 필요하다.

셋째, 주요 언론과의 공조를 강화하고 사이버 심리전의 합법적 수행근거를 확보하기 위해 규범을 정립해야 한다. 언론과의 유연한 협력을 통해 조작 댓글을 필터링, 조작확률 표시 기술 등을 개발하고 시행한다면 심리전을 관제 및 방어에 큰 도움이 될 것이다. 또한, 적시적이고 즉각적인 대응의 효과도 배가될 것이다. 또한, 국가사이버안보센터 및 사이버작전사령부의 사이버 심리전 임무 수행을 위해서는 국가사이버안보전략에 사이버 심리전 위협 및 대응을 포함하고 국가사이버안전관리규정, 사이버작전사령부령, 사이버작전사령부령 등의 법령 및 행정규칙들을 개정하여 반드시 합법적인 수행근거를 마련해야 한다. 아울러 한국군 장병들 휴대폰 사용 전략과 함께 훈령 등 명시적인 규정 정립도 병행되어야 한다.

넷째, 이러한 법적 근거를 바탕으로 합법적이고 효율적인 사이버 심리작전 수행을 위한 운용체계를 정립해야 한다. 사이버 심리전 운용체계는 규범 정립, 교리 및 운용 교범 정립, 작전기록, 평가 순의 수행주기를 가진다. 이러한 수행주기는 지속해서 환류됨으로써 작전의 합법성과 합목적성(국가목표, 국방목표, 군사목표 달성)을 유지하고 작전 효과를 향상 시켜야 한다.

마지막으로 중국과 러시아 등 권위주의 국가들의 사이버 심리전을 포함한 하이브리드 위협에 대응하기 위해서는 사이버 심리전에서도 미국, 일본 등 우방국과의 집단방위체제를 구축하고 협력을 강화해 나가야 한다. 특히 최근 러시아의 사이버 심리전 및 인지전(하이브리드전)에 대응하기 위한 미국과 유럽(EU, NATO)간의 활발한 교류, 훈련 및 협의체에 적극적으로 동참하고 아이디어를 공유하며 기여와 협력을 증진할 방안을 국가적 지역적 차원에서 마련하고 장려할 필요가 있다.

제 2 절 연구의 한계

본 연구는 현재와 미래전에서의 사이버 심리전 중요성에 대해 강조하고, 합법적이고 현실적인 수행방안을 제시하였다. 현재 한국의 정치·사회적 인식과 안보환경을 고려한 사이버 심리전의 한계와 이를 극복하기 위해 필요한 대책과 방안을 제시한 점에서 큰 의미가 있다. 하지만 사이버 심리전의 수행과 관련된 조직과 운영에 대한 사항은 국내·외를 막론하고 공개된 자료가 부족하였기 때문에 자료 수집에 한계가 있었다. 또한, 사이버 심리전의 특성상 북한의 사이버 심리전 공격 사례와 결과에 대해 구체적으로 담지 못한 것은 한계로 남는다. 향후 연구에서 구체적이고 객관적으로 증명된 사례 연구를 통해 더욱 세부적이고 다차원적인 발전방안이 도출된다면 의미 있는 연구가 될 것이다. 특히 2022년 러시아-우크라이나 전쟁에서의 러시아의 사이버 심리전은 2008년 조지아 침공, 2014년 크림반도 합병 당시 보다 그 효과가 미비하였는데 이는 사이버 공간에서의 비국가 행위자들의 역할 증가, 우크라이나의 학습효과에 의한 효과적 대응(러시아의 메신저 신뢰성 훼손 등) 때문이었다. 이러한 사례를 더욱 깊게 연구한다면 한국군의 사이버 심리전 운용 및 대응체계 구축에 큰 도움일 될 것이다. 아울러 23년 10월 7일 하마스의 기습적인 로켓 및 침투 공격을 시작된 이스라엘과 하마스의 전쟁에서도 사이버 심리전은 치열하게 이루어지고 있다. 전쟁 초기 이스라엘과 하마스 양측 모두 전쟁의 정당성 확보와 상대방의 흠집 내고 국제사회(또는 이슬람 국가들)의 지지를 획득하기 위해 이스라엘은 하마스의 민간인 납치와 학살에 대한 증거 영상을 수집하여 공개하고 있고 하마스는 이스라엘군은 가자지구 봉쇄와 공격에 대한 자극적 영상(민간인 희생 영상)들을 촬영, 편집하여 주요 언론은 물론이고 SNS, 유튜브 등 사이버 공간에서 전 세계인들에게 공개하고 있다. 또한, SNS상에서는 진실을 알 수 없는 많은 뉴스와 동영상들이 확산되고 있다. 전쟁의 추이와 함께 양측의 사이버 심리전에 관해서도 연구가 필요하다.

마지막으로 최근 미국 및 NATO는 물론 한국군 또한 인지전에 대한

논의와 연구가 활발하게 이어 나가고 있다. 본 연구에서는 인지전과 사이버 심리전과의 관계와 차별성에 대해서만 간략하게 고찰하였다. 하지만 인지전은 결국 사이버 심리전, 전통적인 심리전보다 진화한 개념이기에 사이버 심리전을 수행하기 위한 국가와 군의 운용체계 또한 인지전을 전제로 도출해야 하는 것이 타당하기에 향후 인지전 수행에 대한 깊이 있는 연구가 필요하다.

참고 문헌

1. 국내 문헌

김두현. “북한의 사이버전 위협분석과 대응방안 고찰.”『IIBC』. 2014.

김민정. “가짜뉴스(fake news)에서 허위조작정보(disinformation)로.”『미디어와 인격권』. 제5권 제2호, 2019.

김소연 외. “사이버전자전 기술 및 발전방향.”『한국전자파학회논문지』. 32(2), 2021.

김인수 외,『정예강군 육성을 위한 북한 바로알기』. 서울: 양서각, 2023.

김재호,『김정일 강성대국 건설전략』. 평양출판사, 2000.

남두현 외, “4차산업혁명 시대의 모자이크 전쟁: 미군의 군사혁신 방향과 한국군에 주는 함의.”『국방연구』. 제63권 제3호, 2020.

『노동신문』, 2003년 4월 12일.

『노동신문』, 2013년 11월 12일.

대한민국 국방부,『2022 국방백서』. 서울: 국방부, 2022.

두진호. “러시아 군사공공외교의 특징과 함의.”『국방정책연구』. 제30권 제2호, 2014.

리처드 블라크·로버트 네이크, 이선미 역,『해커 공화국』. 서울: 에이콘, 2013.

문장렬. “평시 및 위기시의 사이버전 대비전략과 전력기획.”『안보연구 시리즈』. 제11집 12호. 2010.

박성규·길병옥,『현대 북한의 이해』. 대전: 충남대학교출판문화원, 2013.

배달형. “한반도 사이버전 위협과 정책적 대응방향”,『전략연구』. 2011.

_____. “4세대전쟁 및 비대칭 위협 관점의 사이버전 및 사이버 심리전 발전방향.”『한국전략문제연구소 전략연구』. 제 22집, 2015.

부형욱, “우크라이나에서의 하이브리드전과 우리 안보에의 함의”,『동북아안보정세분석』. 한국국방연구원. 2022.

송태은. “디지털 시대 하이브리드 위협 수단으로서 사이버 심리전의 목표와 전술 : 미국과 유럽의 대응을 중심으로.”『세계지역연구논총』. 39(1), 2021.

_____. “디지털 허위조작정보의 확산 동향과 미국과 유럽의 대응.”『IFAN

주요국제문제 분석』. 2020-13, 2020.

_____. “하이브리드 위협에 대한 최근 유럽의 대응.” 『IFANS 주요국제문제 분석』. 2020-31, 2020.

_____. “미국과 중국의 공공외교와 국제평판.” 하영선·김상배 편. 『신흥무대의 미중 경쟁: 정보세계정치학의 시각』. 파주: 한울아카데미, 2018.

신범식·이규철. 『러시아의 사이버 안보』. 서울: 사회평론아카데미, 2021.

신영웅 외, “국가사이버보안 피해금액 분석과 대안: 3·20 사이버 침해사건을 중심으로.” 『국가정보연구』. 제6권 제1호, 2013.

신창훈, “북한의 사이버공격과 위협에 대한 우리의 대응-2014년 11월 소니(SONY)사건의 교훈”, 『ISSU BRIEF』. 2015.

염돈재. “대사이버전 정보활동 추진방향.” 성균관대학교 국가전략대학원 석사학위 논문, 2013.

육군 교육사. 『미래 작전환경분석서』. 서울: 육군교육사령부, 2022.

윤민우·김은영. 『모든전쟁: 인지전, 정보전, 사이버전, 그리고 미래전쟁에 대한 전략이야기』. 서울: 박영사, 2023.

오일석·김소정. “사이버 공격에 대한 전쟁법 적용의 한계와 효율적 대응방안.” 『인하대학교 법학연구소 법학연구』. 제17집 제2호, 2014.

윤규식, “북한의 사이버전 능력과 위협 전망.” 『군사논단』. 제68호. 2011.

윤민우. “미러 사이버 안보 경쟁과 중러 협력.” 김상배 엮음. 『사이버 안보의 국가전략 2.0』. 서울: 사회평론아카데미, 2019.

이관세 외. 『북한 관련 허위정보 실태와 대응』. 서울: 경남대 극동문제연구소, 2020.

이기중. “효율적인 국방사이버 심리전 수행방안.” 『정보·보안 논문지』. 제8권 제1호, 2008.

이민효. “사이버전에 적용될 국제법에 관한 Tallinn Manual 고찰” 『인도법논총』. 제 37집, 2017.

이상진·위강섭, “북한의 사이버 심리전 징후 분석에 관한 연구.” 『디지털포렌식연구』. 제10권 1호, 2016.

이상호. “북한의 사이버 심리전의 실체와 대응방향.” 『대전대학교 한국정치외교사논총』. 2011.

이재형·윤상필·권헌영. “합리적인 사이버심리전 설계를 위한 개념연구와 운용

전략.”『국방정책연구』. 제126권 4호. 2020.

임종인 외, “북한의 사이버전력 현황과 한국의 국가적 대응전략.”『국방정책연구』. 제29권 4호. 2013.

전황수. “뇌-컴퓨터 인터페이스(SCI) 기술 및 개발 동향.”『전자통신동향분석』. 26(5), 2011.

정연태 등 6명. “사이버 여론 조작 방지를 위한 필터.”『한국정보기술학회』. 2018.

클라우제비츠, 강창구 역,『전쟁론 上』. 서울: 병학사, 1991.

통일교육원,『2023 북한이해』. 서울: 통일교육원, 2023.

황진환 외,『신국가안보론』. 서울: 박영사, 2014.

합동참모본부.『합동군사정보지원작전』. 서울: 합동참모본부, 2022.

합동참모본부.『합동·연합작전 군사용어 사전』. 서울: 합동참모본부, 2020.

허태희. “커뮤니케이션 융합시대의 국가안보: 전망과 과제.”『한국국제정치학회 학술대회 발표논문집』. 2010.

2. 국외문헌

Axel Berkofsky, “North Korea’s Military-What Do They Have, What Do They Want?” *ISPI Analysis*, No. 161, 2013.

Baker. P. O. (2010). “*Psychological Operations within the Cyberspace Domain*.” Air War College of Air University.

Bemal et al., “*Cognitive Warfare: An Attack on Truth and Thought*.”

Cheng, D. (2013). “Winning without Fighting: The Chinese Psychological Warfare Challenge.” *Backgrounder*, No. 2821. The Heritage Foundation.

Christan Brose, *The Kill Chain: Defending America in the future of High-Tech warfare*. New York: Hachette Book, 2020.

Christopher Walker & Jessica Ludwig, “*Introduction: From ‘Soft Power’ to ‘Sharp Power’: Rising Authoritarian Influence in the Democratic World*.” In Sharp Power, Rising Authoritarian Influence. International Forum for Democratic Studies (Washington D.C.: National Endowment for Democracy, 2017)

Daniel Golden, *Spy Schools: How the CIA, FBI, and Foreign Intelligence Secretly Exploit American's Universities*. New York: Henry Holt and Co., 2017.

David Betz, "*Failure to communicate: Producing the war in Afghanistan*." In D. Richards and G. Mills (eds.), Victory Among the People: Lessons from Countering Insurgency and Stabilizing Fragile States (London, 2011)

David Welch, *Propaganda, Power and Persuasion: From World War I To Wikileaks*. London & New York: I.B. Tauris, 2015.

Eli Pariser, *The Filiter Bubble*. New York: The Penguin Press, 2011.

Eomm, J. H., Kim, N. U., Kim, S. H., Chung, T. M (2012). "Cyber Military Strategy for Cyberspace Superiority in Cyber Warfare." *IEEE 2012 International Conference on Cyber Security*. Cyber Warfare and Digital Forensic.

Fabio Rugge, "Mind Hacking: Information Warfare in the Cyber Age." *ISPI Analysis* No. 319, 2018.

Farwell, James P. *Persuasion and Power: The Art of Strategic Communication*. Georgetown University Press, 2012

Hoffman, Frank G, "Ewamining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *PRISM, the Journal of Complex Operations* 7-4. Washington, D.C.: National Defense University, 2018.

Homeland Security, "*Homeland Threat Assessment October 2020*". 2021.

HP Security Research, "Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape," *HP Security Briefing* Episode 16, 2014.

J.F.C. Fuller, Tanks in the Great War 1914-1918. New York: E. P. Dutton and Company, 1920. James P. Farwell, Persuasion and Power: *The Art of Strategic Communication*. Georgetown University Press. 2012.

Joseph S. Nye, "The Information Revolution and Soft Power." *Current History* 113-759, 2014.

Joseph W. Alba & Howard Marmorstein, "Information Utility and the Multiple Source Effect," *Journal of Consumer Research* 14-1. 1987., Paul & Matthews, 2016.

Kathleen H. Jamieson and Joseph N. Cappella, Echo, chamber: *Rush Limbaug and the conservative media establishment*. Oxford University Press, 2008.

Kirk Hallahan, Derina Holtzhausen, Betteke van Ruler, Dejan Verčič & Krishnamurthy Sriramesh, "Defining Strategic Communication." *International Journal of Strategic Communication* 1-1, 2007.

Michad Aschmann, Joey Jansen van Buuren, Louise Leenen, "*CyberArmies : The Unseen Military in tfe Grid*." The Proceedings of the 10th International Conference on Cyber Warfare and Security, 2015.

Nicholas J. Cull, "*Public Diplomacy before Gullion: The Evolution of a Phase*" In Nancy Snow and Philip M. Taylor (eds.), Routledge Handbook of Public Diplomacy, 2009.

Paul M. A. Linebarger, *Psycholgical Warfare*. Combat Forces Press, 1954.

Philip M. Taylor, Munitions of the Mind: *War Propaganda from the Ancient World to the Nuclear Age*. Wellingborough: Patrick Stephens Ltd, 1990.

Richard A. Clarke & Robert K. Knake, *Cyber War*. 2012.

Richard A. Nelson, *A Chronology and Glossary of Propaganda in the United States*. Westport, CT: Greenwood Press, 1996.

Rugge, Fabio. "Mind Hacking: Information Warfare in the Cyber Age." *ISPI Analysis* No. 319, 2018.

Stephen G. Harkins & Richard E. Petty, "The Effects of Frequency Knowledge on Consumer Decision Making." *Journal of Personality and Social Psychology* 52-2, 1987.

U.S. Department of Defense, *Strategic Communication: Joint Integrating Concept*: Washington D.C., 2009.

3. 인터넷

국립국어원『표준국어대사전』(2023), https://stdict.korean.go.kr/main/main.do

권구찬, “아침 점호서 21시까지…병사 휴대폰 사용 확대”, 서울경제, 2023.5.11, https://www.sedaily.com/NewsView/29PJCKGHFN

김수빈, “나흘 만에 4천 4백만 회 공격, 보다 치열해진 사이버전”, 한겨레, 2013.1.1, http://defence21.hani.co.kr/34508

나혜윤, “<동아일보>간부 “중국정보, 박근혜 탄핵하려 중국 유학생 6만명 동원” 중국 반발 등 후폭풍 우려, 민주당 “가짜뉴스로 朴대통령 비호”, Views & News, 2017.1.31, http://www.viewsnnews.com/article?q=141360

대한민국 행정안전부, “2020 UN 전자정부 평가'발표! 전자정부발전지수 2위, 온라인참여지수 1위,” 대한민국 행정안전부 홈페이지, 2020.7.11, https://blog.naver.com/mopaspr/222027870611

Daily NK, “北 GPS공격 장기화되면 직접피해 발생할 것,” Daily NK, 2012.5.18., https://www.dailynk.com/北-GPS공격-장기화되면-직접피해-발생할-것

박건형, “중, 뇌파 조종해 적군 무력화 노린다”, 조선일보, 2021.12.18, https://www.chosun.com/international/2021/12/18/I74SBQDTSNFLRB6ULXK3GDOXWU/?utm_source=naver&utm_medium=referral&utm_campaign=naver-news

사이버작전사령부령(대통령령 제29561호, 2019년 2월 26일 전부개정)

심인보, “천안함 5년, 1번어뢰.. 부실조사로 얼룩진 ‘결정적 증거’”, 뉴스타파, 2015.3.25, https://www.newstapa.org/article/lfrkN

엄호식, “보안·ICT 분야 키워드로 미리 살펴본 2021 국감 ①개인정보·기업보안”, 보안뉴스, 2019.9.29., https://www.boannews.com/media/view.asp?idx=101103&kind=

연합뉴스, “북한, GPS 전파 교란 도발… 속내는?”, 2016.4.2, https://www.yna.co.kr/view/MYH20160402008100038

요제프 요페, “레바논 전쟁의 승자는 누구인가?”, 중앙일보, 2006.9.7, https:// www.joongang.co.kr/article/2441652

유동열, “우크라이나 전쟁으로 드러난 사이버전의 위력”, 미래한국, 2023.3.13,

http://www.futurekorea.co.kr/news/articleView.html?idxno =146808

한국정보통신기술협회 정보통신용어사전, http://word.tta.or.kr/main.do

YTN뉴스, “알케에다 지도자 알 자르카위 사망”. 2006.6.8, https://n.news.naver.com/mnews/article/052/0000119397?sid=115

전경웅, “김정일 “남조선 땅만 밟으면 무조건 이겨!”, 뉴데일리, 2013.11.9, https://www.newdaily.co.kr/site/data/html/2013/11/09/2013110900046.html

정락인, “북한 ‘해커부대’의 위험한 거래”, 시사저널1779호, 2011.8.23, http://www.sisajournal. com/news/articleView.html?idxno=132864

정성장, “‘돈줄’ 틀어쥐기 위해 군부 군기 잡기 나섰다”, 시사저널 1206호, 2012.11.29, http://www.sisapress.com/news/articleView.html?idxno=59345

정영교, “김정은 손에 '2조' 쥐어줬다…전방위 공격하는 北 '만능 보검'”, 중앙일보, 2021.12.26, https://www.joongang.co.kr/article/25035443

정혜인, “개인정보 유출로 이어지는 ‘해킹’...전 세계 역대 해킹 사건들”, 시선뉴스,2023.7.31, http://www.sisunnews.co.kr/news/articleView.html?idxno=187374

조명아, “황희, 중국 경유 한국군 전산망 해킹 공격…3년 새 10배 증가”, MBC뉴스, 2020.10.10, https://imnews.imbc.com/news /2020/politics/article/5936609_ 32626.html

조상진, “북한 해킹조직, 모바일 사이버 공격 활발”, VOA, 2019.10.26, https://www. voakorea. com/a/5139849.html

조성식, “천안함 좌초라면서 왜 암초는 제시하지 못하나”, 동아일보, 2018.4.15,https://www.donga.com/news/article/all/20180415/89616355/1

조용석, “3대개혁 번번이 발목…사회적 갈등 관리 필요성↑”, 이데일리, 2023.7.19, https://www.edaily.co.kr/news/read?newsId=01134886635676160&mediaCodeNo=257&OutLnkChk=Y

조재형, “신원식 국방장관, 산·학·연과 사이버기술 개발…공세적 대응체계 구축”, 아주경제,2023.11.16.https://www.ajunews.com/view/20231116161010926

주영재, “네이버, 선거기간 정치 기사 댓글 직접 노출 않는다”, 경향신문, 2018.5.16, https://www.khan.co.kr/economy/industry-trade/article/201805162305015

최현수, “북한, 국내 안보라인 수십명 스마트폰 해킹"..2차 피해 우려”, BBS뉴스,2016.3.8, http://news.bbsi.co.kr/news/articleView.html?idxno=732168

KBS뉴스, “외교부, ‘IS 가담 김모군 사망 추정...확인은 안돼’, 2015.11.17, https:// n.news.naver.com/mnews/article/056/0010249390

한국갤럽, “2012-2023 스마트폰 사용률 & 브랜드, 스마트워치, 무선이어폰에 대한 조사”, 2023.7.18, https://www.gallup.co.kr/gallupdb/reportContent.asp?seqNo=1405

허고운, “'4명 중 1명 임관 포기'… 軍 '과학기술전문사관' 뜯어 고친다”, news1, 2023.11.17. https://www.news1.kr/articles/5233791

Joint Publication 3-13.2. “Psychological Operations.” US Department of Defense (January 7, 2010), www.fas.org/irp/doddir/dod /jp3-13-2.pdf

Vivian S. Walker, “Crafting Resilient State Narratives in Post Truth Environments: Ukraine & Georgia,” In Shawn Powers & Markos Kounalakis (eds.), Can Public Diplomacy Survive the Internet? Bots, Echo Chambers, and Disinformation(US Advisory Commission on Public Diplomacy(2017), https://www.state.gov/documents/organization/271028.pdf

Christopher Paul & Miriam Matthews, “The Russian” Firehose of Falsehood “Propaganda Model: Why it Might Work and Options to Counter It.” Perspective(RAND corporation, 2016). https://www.rand.org/pubs/perspectives/ PE198.html

Matt Chessen, “Understanding the Psychology Behind Computational Propaganda.” In Shawn Powers & Markos Kounalakis (eds.), Can Public Diplomacy Survive the Internet? Bots, Echo Chambers, and Disinformation(US Advisory Commission on Public Diplomacy(2017), https://www.state.gov/documents /organization/271028.pdf

Samantha Bradshaw and Philip N. Howard, “Global Disinformation Order: 2019 Global Inventory of Organized Social Media Manipulation” The Computational Propaganda Project(2019), http//demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

European Commission, “A Europe that protects: good progress on tackling hybrid threats”(May 19, 2019), https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2788; “A Europe that Protects:

Countering Hybrid Threats (June 2018), https://www.dsn.gob.es /sites/dsn/ files/hybrid_ threats_en_final.pdf

Vivian S. Walker, "Crafting Resilient State Narratives in Post Truth Environments: Ukraine & Georgia," In Shawn Powers & Markos Kounalakis (eds.), Can Public Diplomacy Survive the Internet? Bots, Echo Chambers, and Disinformation(US Advisory Commission on PublicDiplomacy(2017), https://www.state.gov/documents/organization/271028.pdf

European Commission, "Joint Framework on countering hybrid threats" (April 2016), https://eucyberdirect.eu/content_knowledge_hu/joint-framework-on-countering-hybrid-threats

NATO & EU, "Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on December 6, 2016 December 5, 2017." https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/190617-4th-Joint-progress-report-EU-NATO-eng.pdf

NATO, "Crisis Management Exercise 2019" Press Release (May 3, 2019), https://www.nato.int/cps/en/natohq/news_165844.htm

NATO, "NATO and the European Union enhance cyber defence cooperation" (February 10, 2016), https://www.nato.int/ cps/en/natohq/news_127836.html

Paul, Christopher and Miriam Matthews. "The Russian "Firehose of Falsehood" Propaganda Model: Why it Might Work and Options to Counter It" Perspective. RAND corporation(2016), https://www.rand.org/pubs/perspectives/ PE198.html.

Ward Caroll, "Russia's Cyber Forces," http://defensetech.org/2008/05/27/ russias -cyberforces

ABSTRACT

A Study on the Cyber Psychological Warfare in ROK Armed Forces

Yoon, Yong-Jae

Major in Defense Management

Dept. of Defense Science

Graduate School of National Defense Science

Hansung University

This paper aims to suggest the direction of the South Korean military's cyber psychological warfare development, focusing on the connection between the domestic and foreign security environment, where the importance of cyberspace is expanding in national security, and the threat of North Korea's cyber psychological warfare. The core content of this paper is how the Korean military should prepare for the growing proportion of cybersecurity, especially in the trend and prospect of cyber psychological warfare acting as a key factor in determining the leadership and direction of the war.

In order to suggest the direction of development, this paper analyzed the importance of cybersecurity(psychological warfare) in future warfare, Russia's cyber psychological warfare tactics, and North Korea's cyber

threats. In addition, the expansion of cybersecurity in future warfare, the concept and characteristics of cyber psychological warfare, and the legal basis were examined, and the Korean military's management of cyber psychological warfare was studied.

Cyber warfare overlaps with many non-kinetic warfares, such as electronic warfare, information warfare, and cognitive warfare, and is also closely related to kinetic warfare. It should also be understood in the expansion and diversification of the concept of cyber warfare because cyber warfare is also related to various security issues, such as diplomatic and cultural wars. In addition, it was found that the proportion of cyberspace in the future hybrid warfare in which several war types were fused will be further expanded.

Cyber psychological warfare is not just an extension of traditional psychological warfare, but has a clear feature. Authoritarian countries, such as Russia, will continue to expand cyber psychological warfare, recognizing it as an attractive means of taking asymmetric benefits in attack and defense. On the other hand, it was found that democracies such as the United States, Europe, and Korea have limitations such as not being included in the legal basis and political sphere in order to carry out cyber psychological warfare. North Korea is also continuing cyberattacks against the international community and South Korea by taking advantage of the asymmetry of the cyber, political, and social environment. In addition, despite various limitations such as relations with China and deepening economic difficulties, it was found that the cyber warfare forces and strategy were being strengthened and evolved by taking advantage of the openness and internal conflict of Korean society, and the indirectness and concealment of cyber psychological warfare.

In conclusion, South Korea should strive to reorganize its organization and mission, establish cyber psychological warfare strategies, and establish

an operation system for integrated civil, government, and military cyber psychological warfare using excellent Internet infrastructure in preparation for the threat of North Korea's cyber psychological warfare. Furthermore, a collective defense system should be established with allies such as the United States, Japan, and Europe to counter cyber psychological warfare and improve response capabilities of authoritarian countries such as Russia and China.

Finally, due to the political environment and the characteristics of cyber psychological warfare in Korea, this study had many limitations in proving the specific threat of North Korea's cyber psychological warfare. And it was difficult to specifically reflect the strategies and tactics of cyber psychological warfare in the Russia-Ukraine war and the wars with Israel and Hamas. In the future, along with the analysis of the training of cyber psychological warfare, research on cyber psychological warfare in cognitive warfare should be continued.

【Key words】 cyber security, cyber threats, psychological warfare, cyber psychological warfare, cognitive warfare