Center for Future Warfare Studies,
Institute of International Studies at Seoul National University |
국제문제연구소 미래전연구센터 워킹페이퍼 No.71(발간일: 2021.5.18.)

사이버 심리전의 미중경쟁과 한국:

미국과 유럽의 대응과 함의*

송태은 국립외교원 연구교수

목 차

요 약

21세기 디지털 기술의 고도화와 인터넷 네트워크의 지구적 확장은 다양한 군사적 · 비군사적 위협 수단을 복합적으로 사용하는 하이브리드전을 공격 비용이 낮으면서도 공격대상 국가에 치명적인 피해를 입힐 수 있는 사이버 공간으로 이동시키고 있다. 최근 사이버 공격에 동반되거나 혹은 개별적으로 빈발하고 있는 사이버 심리전은 민주주의 사회의 위기를 상시화하고 민주주의 제도의 정상적 기능을 약화시키는 전술을 취하고 있다. 사이버 심리전은 초연결 사회의 공개된 사이버 공론장을 공격하면서 정보와 내러티브를 무기화하고 정치적 우위를 점하려는 전술을 취하며, 인공지능 알고리즘의 스토리텔링 및 대규모 정보확산 기술을 동원하는 디지털 프로퍼갠더로 진화하고 있다. 주로 러시아, 중국, 이란 등 권위주의 레짐의 민주주의 사회에 대한 공격의 형

태를 띠는 경우가 대부분인 국가 發 사이버 심리전은 2016년부터 서구권 선거철 러시아가 소셜 미디어 플랫폼을 통해 확산시킨 허위조작정보가 선거에 영향을 끼치면서 현대전의 주요 위협수단으로 부상하게 되었다. 중국의 사이버 심리전은 대만과 홍콩 등 중국어권에 대해서는 러시아의 심리전 방식을 모방하고 있으나 세계대중에 대해서는 글로벌 리더로서의 이미지와 평판을 증진시키려는 메시지가 지배적이므로 보다 체제선전에 초점이 맞춰져 있다. 미국과 유럽은 사이버 심리전을 주권에 대한 도전으로 간주하고 NATO 차원에서 군사적으로 대응하고 있으며 미 국방부도 최근 허위조작정보 공격에 대한 체계적인 대응태세를 마련하고 있다. 한국도 외부로부터의 사이버 심리전 공격에 대응하는 다양한 모의훈련 및 민관 · 민군 공동연구에 참여하고 협업함으로써 유사한 대응 태세를 준비해나갈 필요가 있다.

**이 글은 『세계지역연구논총』 제39집 1호(2021)에 게재한 저자의 논문 "디지털 시대 하이브리드 위협 수단으로서의 사이버 심리전의 목표와 전술"에 중국에 대한 분석을 추가하여 편집, 수록한 것임. 또한 이 글은 저자의 견해를 바탕으로 집필한 저작으로 외교부의 공식입장과는 무관함.*

1. 들어가며

최근 전투원 간의 직접적인 교전 혹은 가시적인 군사활동이 부재하거나, 전통적인 무력수단과 비전통적 위협 수단을 복합적으로 사용하며 국가 시스템과 정부의 의사결정을 무력화시키려는 '하이브리드 위협(hybrid threats)' 혹은 '하이브리드전(hybrid warfare)'이 빈번하게 발생하고 있다. 대개 소셜미디어 플랫폼(social media platform)에서 대규모의 허위조작정보를 유포(disinformation campaign)시키는 방법이 빈번하게 이용되는 사이버 심리전(psychological warfare)은 하이브리드 위협의 한 형태로서 다른 형태의 위협과 결합될 때 파괴력이 배가될 수 있다. 지상, 해상, 항공, 사이버 공간 등 복합적인 전장을 사용하는 하이브리드 위협은 테러, 생화학 및 핵 위협, 해적행위, 주요 에너지 자원 및 전략자원에 대한 접근 차단, 국가 주요기관이나 기반시설에 대한 사이버 공격이나 해킹 등을 통해 전개되고, 여기에 사이버 심리전이 결합됨으로써 국가 안보와 사회전체의 회복력(resilience)을 심각하게 약화시킬 수 있다.

이러한 사이버 심리전은 대규모의 군사력을 동원하지 않고 공격의도를 은폐하기 위해 공격 주체의 노출을 최소화하면서 전략적 목적을 달성하려는 현대 하이브리드전의 효과적인 위협 수단으로 부상하고 있다. 전통적인 전쟁과 달리 공격주체의 공식적인 선전포고와 전장이 부재하고 군사적 수단과 비군사적 수단이 다전장에서 혼합되어 동시다발로 사용될 수 있는 하이브리드전에서 사이버 심리전은 대중 여론을 쉬운 공격대상으로 삼으며 공격의 유무 자체를 쉽게 은폐할 수 있다. 사이버 심리전은 공격대상으로 삼는 사회 내 이미 존재하는 갈등과 분열을 효과적

으로 활용할 수 있는 가장 애매모호한 형태의 하이브리드 전술이라고 볼 수 있다.

2014년 러시아가 크림반도 합병 당시 전개한 여론전은 우크라이나 대중을 공격목표로 삼았기 때문에 당시 미국과 유럽의 러시아 發 하이브리드 위협 대응에 대한 논의는 사이버 심리전에 초점을 둔 것은 아니었다. 하지만 2016년 영국의 브렉시트(Brexit) 국민투표와 미국 대선을 시작으로 하여 2020년 미 대선에 이르기까지 미국과 유럽의 거의 모든 주요 선거가 외부로부터의 사이버 심리전 공격을 받게 되면서 서구권은 심리전의 하이브리드 위협에 주목하기 시작했다. 최근 중국도 홍콩이나 대만 등 중국어권을 비롯하여 미국과 유럽 대중을 상대로 러시아의 심리전과 비슷한 방식으로 소셜미디어 플랫폼을 이용하여 허위조작정보를 대규모로 유포하는 활동을 전개함에 따라 그동안 러시아의 심리전에 주목해온 미국이 중국의 심리전에도 주목하게 되었다.

2021년 3월 16일 바이든 행정부 출범 이후 새로 신설된 미 하원 군사위원회 산하 정보·특수전 소위원회(House Armed Services Subcommittee on Intelligence and Special Operations)는 "회색지대의 허위조작정보: 기회, 한계, 도전(Disinformation in the Gray Zone: Opportunities, Limitations, and Challenges)"라는 주제 하에 청문회를 개최하고 중국과 러시아의 심리전 활동에 대한 국방부의 보고를 청취했다. 제임스 설리번(James Sullivan) 국방정보국(Defense Intelligence Agency, DIA) 사이버 담당관(Defense Intelligence Officer for Cyber)은 소셜미디어와 인공지능을 이용한 심리전 활동에 있어서 현재 러시아의 심리전 역량이 가장 강력하지만 중국도 인공지능(Artificial Intelligence, AI) 기계학습(machine learning)을 통해 러시아의 심리전 기술력을 추월할 것으로 내다봤다(House Armed Services Committee 2021).

미국과 유럽이 타국 發 사이버 심리전에 대해 예민한 반응을 보이고 있는 것은 이러한 심리전이 서구권의 대중을 직접적인 공격상대로 삼고 있고, 평시에도 사회교란과 민주주의 제도의 약화 등 악의적인 공격을 수시로 전개할 수 있기 때문이다. 러시아, 중국, 이란 등 권위주의 진영이 전개한 사이버 심리전은 서구권 온라인 공론장의 연결성(connectivity)과 개방성(openness)이 갖는 취약성을 이용하여 여론을 왜곡하고 사회분열을 극대화하며 선거과정과 정부의 정당성을 공격하는 등 민주주의 제도의 핵심 기능과 가치를 집중적으로 훼손하려는 시도를 보였던 것이다. 미국과 유럽은 자국의 선거 여론이 허위조작정보의 공격만으로도 심각하게 교란되는 상황을 직접 경험하면서 이러한 공격을 단순히 여론왜곡 시도를 넘어선 서구권의 주권과 민주주의 제도에 대한 직접적인 파괴행위로서 간주하게 되었고, 다양한 조사를 통해 그러한 심리전이 AI 알고리즘 기술이 동원된 디지털 프로퍼갠더 활동임을 발견했다(송태은 2019, 180-190).

이러한 맥락에서 이 글은 최근 세계 정보커뮤니케이션 환경의 변화와 함께 빈발하고 있는 사이버 심리전이 어떤 방식으로 공격대상 국가의 위기를 유발하며 어떤 전술을 사용하고 있는지 살펴본다. Ⅱ장과 Ⅲ장은 사이버 심리전이 하이브리드 위협의 한 수단으로서 어떤 목표를 갖고 어떤 공격 행태 및 전술을 보여주는지 짚어본다. Ⅳ장에서는 최근 중국이 러시아의 방식을 모

방하여 중국어권과 서구권을 대상으로 소셜미디어 공간에서 허위조작정보를 확산시키며 자국의 체제우위를 선전하려 했던 시도들을 살펴본다. V장에서는 사이버 심리전 공격에 대해 가장 먼저 체계적으로 군사적 태세를 마련하고 있는 미국과 유럽이 어떤 방식으로 대응태세를 갖추고 있는지 구제적으로 짚어본다. 마지막으로 VI장은 사이버 심리전 대응을 강화하고 있는 서구권의 대응이 우리에게 주는 함의를 짚어보는 것으로 이 글을 마무리한다.

II. 사이버 심리전의 목표

21세기의 진입 시점에서 빈발하고 있는 사이버전은 초연결 시대의 현대 국가 시스템을 효과적으로 무력화시킬 수 있는 위협 수단이며, 대개 허위조작정보의 유포 형태를 띠는 사이버 심리전은 사이버 공격에 수시로 동반되는 주요한 위협 수단이다. 심리전은 목표청중의 생각, 감정, 행동에 영향을 끼치려는 체계적인 형태의 의도적이고 조직적인 설득 행위로서, 전하려는 메시지를 미디어를 통해 통제된 방식으로 전달하는 프로퍼갠더 활동이다. 특히 전시(wartime) 심리작전(psychological operation)은 적의 사기나 전투 및 저항의지는 꺾고 아군 및 동맹의 결의와 사기는 강화시켜 자국의 위치를 우월하게 만드는 것을 목표로 한다(CIA 1948). 심리전 공격 주체는 특정한 정치적 혹은 이념적 메시지를 전파할 수도 있지만 대안적 어젠더가 부재해도 공격대상이 되는 정부의 정당성과 제도의 권위를 훼손하여 상대적인 정치적 우위(political dominance, political supremacy)를 확보하는 것이 일차적 목표이다.

2006년 이스라엘-레바논 전쟁, 2007년 러시아-에스토니아(Estonia) 분쟁, 2008년 러시아-조지아(Georgia) 분쟁, 2012년 가자-이스라엘 분쟁, 2013년 이스라엘-하마스 교전 및 2014년 러시아-우크라이나 분쟁은 모두 사이버 공격에 사이버 심리전이 동반된 대표적인 하이브리드전 사례이다(Hoffman 2007, 7-8; McCulloh & R. Johnson 2013; Calha 2015). 2014년 우크라이나 침공에서 러시아는 국가안보위원회(KGB)의 후신인 연방보안국(FSB)과 군사정보국(GRU)뿐 아니라 민간기업인 'Internet Research Agency(IRA)'와 같은 '트롤팜(troll farm)'과 같은 비국가 행위자를 동원하여 우크라이나에 대한 정보활동과 여론공작 등 사이버 심리전을 전개했다. 러시아는 2016년부터 서구권 선거를 심리전의 공격 대상으로 삼고 민간 기업과 계약을 맺어 대리공격을 수행했고, 이후에도 비슷한 방식으로 서구권에 대해 사이버 심리전을 전개하며 책임소재를 피해나갔다. 이렇게 사이버 심리전은 일반적인 사이버 공격과 마찬가지로 국가와 계약을 체결하고 정보 · 군사활동을 수행하는 민간기업도 이용되는 등 '전쟁의 외주(outsourcing)'가 가능하다(조한승 2012, 25-26).

사이버 심리전은 공격주체를 은폐하고 책임소재를 불분명하게 만드는 데에 유리하고, 개방된 온라인 공론장과 소셜미디어 플랫폼은 사실상 언제든지 공격을 취할 수 있는 열린 전장

이나 다름없다. 비가시적 영역인 디지털 커뮤니케이션 공간에서 전개되는 사이버 심리전은 공격 주체의 모호성을 극대화시키고 공격을 받은 대상의 즉각적인 복수가 불가능하며 적절한 복수 수단도 부재하다. 2016년 이후 러시아가 동유럽과 서구권에서 구사한 가짜뉴스 유포를 통한 사이버 심리전에 대해 미국과 유럽은 선거 이전 그러한 공격 정황을 인지하고 있었음에도 불구하고 신속한 대응을 취하지 못했다. 사이버 공간의 국가 · 비국가 행위자의 행위를 규제할 국제규범과 레짐이 제대로 형성되어 있지 않은데다가 인명 피해를 발생시키지 않는 사이버 심리전은 무력공격으로 인식되지 않으므로 공격을 받은 대상의 즉각적인 군사적 보복이 어렵기 때문이다 (Carment & Belo 2018).

하이브리드전은 국가 행위자의 정책결정을 지연시키고 국가 시스템을 마비시키며 정치제도의 정상적인 기능을 방해하는 등 전복적인 목표를 추구한다. 이러한 하이브리드전의 목표를 달성하기 위해 사이버 심리전은 사회교란과 분열을 극대화하여 공격자가 정치적 우위를 달성하는 과정을 용이하게 만들어준다. 2014년 크림반도 합병 과정에서 러시아는 군사적, 비군사적 수단을 혼합하여 압도적인 군사력 사용의 필요성을 축소시키고, 전면적인 공격을 통해 상대방을 패배시키기보다 비전통적 · 비대칭적 · 간접적 군사행동으로 정치적 우위를 달성할 수 있었다. 즉 러시아는 심리전을 통해 우크라이나 사회의 혼란과 불안을 유발하고 대리전을 수행하면서 우크라이나 침공의 최종 국면에서 결정적인 군사행동을 전개하는 전략을 취했다(김경순 2018, 64-90).

심리전은 권위주의 레짐의 고유한 전술이 아니다. 프로퍼갠더 활동 자체가 과거 양차대전과 냉전기를 더 거슬러 올라가 중세시대의 카톨릭교회 등 다양한 정치세력이 사용한 전술이기 때문이다. 러시아의 시각에서는 소련의 붕괴와 아랍의 봄, 오렌지 혁명은 서구 민주주의 진영에 의한 전복적인 프로퍼갠더 활동이다. 따라서 러시아 입장에서는 대중에게 끼친 정보의 위협적인 전략을 러시아의 세력권인 우크라이나에서 전개한 것이라고 주장할 수 있다(Korybko 2015, 10-11; 신범식 · 윤민우 2020, 170). 특히 디지털 정보통신기술(Information & Communication Technology, ICT)의 발전과 온라인 네트워크 및 사물인터넷(Internet of Things, IoT)에 의한 초연결 사회(hyper-connected society)의 연결성은 사이버전 수행주체의 시각에서는 공격의 파괴력을 최대화할 수 있는 취약점으로 인식하게 만들었다. 결과적으로 시간과 장소에 구애받지 않고 언제든지 선제공격이 가능한 사이버 심리전은 공격 대상 사회의 상시적 위기를 유발할 수 있는 효과적인 위협 수단이다.

〈표1〉에서 보는 바와 같이 2000년대에 들어 발생한 대부분의 하이브리드 위협은 사이버 공격이나 사이버 심리전이 반드시 동반되었다. 사이버 심리전은 국내외 여론에 영향을 끼치고 사회분열과 갈등을 촉발시키는 '소프트파워(soft power)' 혹은 '샤프파워(sharp power)' 위협이며,[1] 직접적인 군사공격인 탱크, 전투기, 미사일 사용 등 하드킬(hard-kill) 형태의 공격과 대비되

1) 주로 권위주의 레짐이 추구하는 경향이 있는'샤프파워'는 국가가 국내외 청중의 자유로운 표현을 제약

는 소프트킬(soft-kill) 형태의 공격이다. 사이버 공격은 국가 기반시설의 시스템을 정지시키거나 해킹을 통해 정보를 유출·조작함으로써 하드킬 수단에 동반될 경우 공격의 파괴력을 배가시킬 수 있고, 사이버 심리전은 사회 내 잠재되어 있는 갈등이 표면적으로 분출되게 하고 사회전체의 연대를 와해시키는 일종의 '티핑포인트(tipping point)' 역할을 수행할 수 있다.

사이버 심리전 메시지는 국내 소셜미디어 공간에서 표면적으로는 국내 발신과 국외 발신이 구별되지 않고 어떤 개인도 목표청중(target audience)으로 삼을 수 있다. 그러한 메시지에 설득되어 특정한 정치적 의견을 갖게 된 국내청중이 시위와 같은 정치적 행위로 나타나도 그러한 행위가 심리전 메시지에 의해서만 유발된 것인지 인과관계를 밝히기는 어렵다. 그것은, 개인의 정치적 의사와 대중 여론에 영향을 주는 변수는 아주 다양하고 국내에서 생산된 허위조작정보와 해외 發 허위조작정보의 내용이 대개 유사한 경우가 많으며, 메시지 발신 방식도 국가 행위자를 철저히 은폐하므로 국가 간 문제로서 언급되려면 정밀한 조사가 수행되어야하기 때문이다.

〈표1〉 2000년대 사이버전 및 사이버 심리전 사례

2006년 7월 이스라엘-레바논 전쟁	▪ 이스라엘의 레바논에 대한 폭격에 대해 헤즈볼라(Hezbollah)는 이스라엘에 대한 미사일 공격 전 이스라엘 육군 컴퓨터 시스템을 해킹하여 군의 무선 통신에 침투하고 미국 웹서버 업체들을 하이재킹하여 이스라엘의 인터넷망 공격. ▪ 헤즈볼라는 이스라엘 군인들의 휴대폰 통화를 도청하여 군사정보를 수집하고 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(DDos) 공격 수행하여 에스토니아의 금융거래와 행정업무가 일주일 이상 중단되는 등 국가 시스템 전체 마비 및 공포심 유발.
2008년 6월 러시아-조지아 5일 전쟁	▪ 러시아는 조지아에 대해 대규모의 지상군을 투입하는 정규전 외에 바이러스 프로그램에 감염되어 있는 컴퓨터 네트워크인 봇네트(botnets)를 이용하여 사흘 간 '메일폭탄(Mail-bombing)', 디도스 공격'으로 에스토니아 전산망 무력화. ▪ 민간 사이버 범죄조직 '러시아비즈니스네트워크(RBN)'를 이용한 디도스 공격은 조지아 대통령 홈페이지, 국방부, 외교부, 의회 웹사이트에 대해 수행되었고, 이들 정부기관 및 언론사, 포털 등이 평균 2시간 15분, 최장 6시간 동안 공격받음.
2012년 11월 가자-이스라엘 분쟁	▪ 이스라엘 군사령부는 트위터(Tweeter)를 통해 선전포고를 했으며, 페이스북(Facebook), 트위터, 인스타그램(Instagram), 유튜브(Youtube)를 활용하여 가자지구 공습에 대한 우호적 여론을 조성. ▪ 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 회 사이버 공격 수행. 이스라엘은 하마스와 이슬람 지하드(Jihad)의 라디오 방송을 강탈(hijacking)하여 테러리스트를 돕지 말라는 심리전 수행. ▪ 이스라엘 방위군과 하마스 무장세력 간 트위터 상 설전.
2014년 3월 러시아의 크림반도 합병	▪ 우크라이나의 親러 정권이 붕괴한 이후 우크라이나 동부 돈바스 지역(도네츠크주, 루간스크주)에서 親러시아 분리주의 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. ▪ 국가안보위원회(KGB)의 후신인 연방보안국(FSB)과 군사정보국(GRU)은 우크라이나에 대한 정보활동과 여론공작 등 사이버 심리전 전개.
2016년 이후	▪ 2016년 미 대선, 영국 브렉시트 국민투표, 2017년 독일 총선, 프랑스 대선, 스페인 카탈

하고 검열하며 조작된 정보를 확산시키는 등의 방식으로 사회의 혼란을 부추기고 민주주의 정치제도의 정상적인 기능을 방해하는 영향력을 일컬음.

사이버 심리전을 통한 선거개입	루냐 독립투표, 2018년 이탈리아 총선, 2019년 유럽의회선거(EU Parliamentary Election), 2020년 미 중간선거와 대선 등 서구권 소셜미디어 플랫폼에 AI 알고리즘 프로그램 가짜계정 봇(bots)을 이용한 디지털 허위조작정보 대규모 유포.

출처: 송태은(2020b), p.12

Ⅲ. 사이버 심리전의 전술

전쟁의 시작과 종식에 있어서 '정보(information)'는 가장 중요한 변수이다. 전쟁 중 전장(battlefield)에서 직접 대결을 통해 얻게 되는 적에 대한 정보는 협상 테이블에서 얻는 정보와 달리 무력충돌을 통해 전투능력의 상대적 우열이 직접 드러나므로 의도적으로 왜곡되거나 과장될 유인이 큰 협상 테이블에서의 정보와 다르다. 즉 전장에서 분쟁국은 물리적인 대결 전에는 가용하지 않았던 새로운 정보를 획득할 수 있다(Wagner 2000; Fearon 1995). 국가 간 사이버전에서도 상대국에 대한 공격은 곧 자국의 사이버전 전력과 공격 기술의 노출을 의미한다. 사이버 공격을 받은 국가가 상대방의 공격 기술과 방식을 분석할 수 있기 때문이다. 결과적으로 한 번 사용한 공격 기술은 방어자에게 차후 동일한 형태의 공격에 대한 방어 능력을 갖게 하는 등 사이버전에서도 정보의 역할은 핵심적이다.

반면 사이버 심리전에서 정보의 역할은 일반적인 사이버전에서의 정보의 성격과 다르다. 일반적인 사이버 공격은 컴퓨터 네트워크 시스템에 대한 공격인데 반해, 사이버 심리전의 공격대상은 사이버 공간에서 정보를 얻고 커뮤니케이션 행위를 하는 사람들의 '생각'이나 '감정'이다. 공격을 받은 측이 사이버 심리전 메시지를 사후(ex post) 분석하여 거짓정보의 성격을 파악해도 이후 공격을 받은 국가의 대중은 또 다시 그러한 비슷한 거짓정보에 다시 속을 수 있다. 즉 심리전 공격자는 동일한 심리전 전술을 반복해서 사용할 수 있고, 그러한 전술이 알려져도 메시지의 내용은 계속 바뀌므로 전술의 유효성이나 효과가 사라지지 않는다. 요컨대 심리전 공격자의 전투력은 메시지의 '내러티브(narrative)'가 갖는 설득력에 있으므로 동일한 설득기제의 재사용은 무한대로 가능한 것이다. 메시지의 내러티브가 갖는 기만성이 밝혀지고 설득전술이 공개되어도 대중은 여전히 스스로 정보를 분별할 수 있어야 한다. 사이버 심리전은 일반적인 사이버 공격과 달리 정보의 탈취나 유출 등의 피해를 발생시키지 않으므로 개인은 그러한 심리전 메시지의 악의적 의도를 의식하지 못할 가능성이 크다.

전시와 평시에 모두 전개할 수 있는 심리전이 의도하는 내러티브의 전략적 효과는 〈표 2〉에서 나열한 것과 같이 다양하다. 심리전 내러티브는 정책결정자의 정확한 정보분별을 방해하여 속이고, 주의를 분산시키고 왜곡하며, 정보의 과부하를 유발하여 의사결정을 지연시키고, 경계심을 완화시키거나 좌절감을 유발하여 정책결정을 마비시키는 등 다양한 효과를 노릴 수 있다(Errey 2019, 6). 심리전의 공격 대상은 타국 정부의 의사결정자와 대중 모두를 대상으로 하므로

적국 정부가 군사적으로 중요한 사안에 대해 스스로를 의심하게 만들어 의사결정의 실수를 유도하는 전략도 사용될 수 있으며, 공격을 받은 국가의 복수를 막기 위해 대중의 반전(antiwar) 여론을 유도할 수도 있다(McFate 2019, 66). 또한 심리전은 공격대상 사회의 내러티브와 유통되는 정보를 통제하면서 대리 행위자가 급진적, 극단적 행동을 하도록 자극하여 산발적 혹은 대규모의 폭력도 촉발시킬 수 있다.

〈표2〉 정책결정 교란을 위해 심리전 내러티브가 의도하는 효과

전략적 의도	공격자가 의도하는 효과
기만(Deceive)	적국의 잘못된 판단을 유도하여 군대 자산을 재배치하게 만듦.
지연(Delay)	적국의 시의 적절한 의사결정을 지연시킴.
차단(Deny)	중요 사안을 특정 프레임으로 보게 만들어 적의 정확한 정보분별 차단
억지(Deter)	위협이나 장애 극복 가능성에 대한 좌절감 주입
주의분산(Distract)	적국이 공격목표에 집중할 수 없도록 실제 혹은 가상의 위협, 이슈, 장애를 발생시킴
분열(Divide)	적국 정부가 동맹의 이익에 반대되는 행동을 하도록 유도
왜곡(Manipulate)	널리 알려져 있는 정보에 대한 고의적인 공작이나 왜곡
과부하(Overload)	대량의 정보발신
진정(Pacify)	예상되는 위협이나 공격적 활동에 대한 적국의 경계심 완화(예: 공격적 대비태세가 아니라 마치 예정된 통상적인 훈련이 진행되는 것처럼 인식하게끔 유도)
마비(Paralyze)	적국에게 핵심 이익에 대한 위협이 발생한 것 같은 인식을 심어주거나 혹은 적국의 취약성을 이용해 적의 대응 움직임을 부분적 혹은 전체적으로 무력화시킴
압박(Pressure)	적국이 국익에 반하는 행동을 하도록 설득 혹은 위협
자극(Provoke)	공격목표로 삼는 대상에 대해 적국도 공격적 행동을 하도록 유발
정보제시(Suggest)	적국의 법 · 도덕 · 이념에 영향을 끼칠 수 있는 정보 유출
손상(Undermine)	대중의 적국 정부에 대한 신임이 줄어들도록 적국 정부의 정당성 약화

출처: Errey(2019)

민주주의 제도와 시민사회에 대한 대중의 신뢰를 훼손시킬 수 있는, 저비용의 고효율 수단인 심리전은 공격대상 정부의 정당성(legitimacy)과 법적 권위에 대한 현지 주민 혹은 시민의 지지를 제거하기 위한 효과적인 위협 전술이다. 특히 현대의 발전된 정보통신기술은 대규모의 특정 메시지를 실시간으로, 원하는 특정 기간에 유포, 확산시키는 일을 기술과 비용 측면에서 쉽게 만들었으므로 사이버 심리전은 게릴라전처럼 수시로 급작스럽게 수행되고 있고, 정보와 내러티브는 사이버 심리전의 효과적인 무기가 되었다. 사이버 심리전의 가장 큰 파괴력은 피해의 원상복귀가 불가능하다는 데에 있다. 예컨대 선거철 급증하는 사이버 심리전으로 인해 유권자의 투표행위와 선거 결과가 이미 영향을 받은 뒤 그러한 심리전술이 밝혀져도 선거결과에 대한 피해구제는 불가능하다. 또한 선거철과 같이 논쟁적인 정보와 의견이 풍부한 시기에 가짜뉴스에 노출된 대중에 대해 팩트체크(fact check) 정보를 재유포해도 제공된 정확한 정보가 대중에게 제대로 전

달될 가능성과 대중이 이러한 정보를 더 신뢰할 지의 여부는 불확실하다. 팩트체크 정보는 본질적으로 가짜뉴스 메시지가 확산된 이후 만들어지는 반응적인(reactive) 정보이므로 청중확보에 불리하기 때문이다.

사이버 심리전은 현대의 AI 기술의 발전으로 더 지능화되고 있다. 오늘날의 AI는 '딥러닝(deep learning)'을 통해 내러티브를 이해하고 스토리텔링(storytelling) 기술을 구현하며 다양한 심리전술을 펼칠 수 있다. 예컨대 '정치봇(political bot)'으로도 불리는 AI 알고리즘인 소셜봇은 온라인 공간에서 특정 정보를 집중적으로 확산시켜 특정 이슈만이 언급되게 하여 소위 '반향실 효과(echo chamber effect)'(Jamieson & Cappella 2008, 75-78), '필터버블(filter bubble)' 효과(Pariser 2011, 2)를 비롯한 다양한 '봇 효과(bot effect)'를 부추기고 강화시킬 수 있다. 또한 소셜봇은 인지심리학이나 커뮤니케이션학에서 발전시킨, 설득효과가 입증된 고도의 심리적 기제가 적용된 내러티브를 사용하며, 그러한 정보를 봇부대(bot army)를 통해 실시간으로, 대규모로 확산시킬 수 있다(송태은 2020a, 20-21). 최근 AI의 정보조작 기술 중 '딥페이크(deep fake)'는 AI 알고리즘을 이용하여 동영상 원본에 등장하는 사람을 다른 사람의 모습으로 편집하여 마치 영상 속 인물이 실존하는 것처럼 조작하여 진위여부를 식별하기가 가장 어려운 형태의 허위조작 정보를 만들 수 있다.

〈표3〉 소셜미디어 공간의 편향된 커뮤니케이션 효과와 심리전의 설득기제

<table>
<tr><th>반향실 효과(echo chamber effect)</th><th>봇 효과(bot effect)</th></tr>
<tr><td>유사한 관점 · 생각을 가진 사람끼리 반복 소통하여 편향된 사고가 고착화되어 동의하는 의견만 수용하게 되는 현상</td><td>정치적으로 편향된 정보와 메시지를 대규모로 확산시켜 여론이 특정 방향으로 유도되게 하는 현상.</td></tr>
<tr><th>필터버블 효과(filter bubble effect)</th><th>트롤링(trolling)</th></tr>
<tr><td>인터넷 사용자에게 AI 알고리즘에 의한 맞춤형 정보만을 제공하여 사용자가 마치 거품에 가둬진 것 같은 현상. '반향실 효과'는 정보에 대한 인터넷 사용자의 주관적 선택에 의한 것이나, '필터버블'은 사용자의 선택이 덜 개입되어 더 개인화된 세계에 갇히는 효과를 만들 수 있음.</td><td>타인의 강한 감정적 반응을 유발하기 위해 적대감이나 화를 부추기거나 혹은 거짓 비난의 글을 온라인 공간에 의도적으로 게시하는 행위. 인터넷 트롤(troll)은 인터넷 사용자일 수도 있고 AI 알고리즘이 조종하는 봇(bots)일 수도 있음.</td></tr>
<tr><th>정보의 양(volume)에 의한 효과</th><th>진실착각효과(the illusory truth effect)</th></tr>
<tr><td rowspan="2">▪ 서로 다른 정보원(source)이 제공하는 정보가 일치하거나 서로 다른 논쟁이 동일한 결론에 이를 경우 사람들은 정보의 '질(quality)'보다 동일한 결론에 이른 정보의 '양(volume)'을 더 중시함.
▪ 알고리즘은 인기 있는(high ranking) 정보에 과도한 우선권을 주므로 허위정보 확산에 악용될 수 있음.
▪ 정보가 풍부한 환경에서 사람들은 다수가 인정하는 정보를 전문가의 의견보다 더 신뢰하므로 소셜봇은 특정 여론 조성을 위해 팔로워 수나 '좋아요(likes)'를생성하는 알고리즘을 사용함.</td><td>동일한 극단적인 메시지에 반복 노출될 경우, 사람들은 그러한 메시지를 신뢰하고, 처음 접한 정보를 이후에 접한 정보보다 신뢰하는 경향이 있음. 즉 사람들은 처음 접한 출처가 불분명한 정보라도 시간이 경과하면서 정보 자체만을 기억하여 사실로 착각하는 경향을 보임.</td></tr>
<tr><th>비전통적 설득전략</th></tr>
<tr><td>전통적인 설득전략은 메시지의 신뢰성을 높이기 위해 진실과 일관성을 강조하지만 심리전은 효과가 입증된 반대 전략을 취하기도 함. 거짓으로 밝혀진 정보를 재사용하거나 또 다른 거짓 정보를 수정된 정보로서 제공하기도 함.</td></tr>
</table>

출처: 송태은(2020a, 21,24).

결과적으로 첨단 AI 기술이 사이버 심리전에 적용되면서 사이버 심리전의 공격주체는 비인간 행위자(non-human actors)를 통해서도 자동화된 디지털 프로퍼갠더 활동을 급작스럽게 선제공격처럼 수행할 수 있다. 또한 사이버 심리전은 국가 간 군사긴장이 고조되어 무력사용이 발생하기 직전 적국에 대한 '경고(warning)'로서 수행되기도 한다(Hunter & Pernik 2015, 7). 2018년 시리아 아사드(Bashar Assad) 정권이 반군에 대해 화학무기 사용한데 대해 미국, 영국, 프랑스 연합군이 시리아를 공습하자 반발한 러시아가 취한 서방에 대한 적대행위는 서구권 소셜 미디어 공간에 AI 알고리즘 기술인 '로보-트롤링(robotrolling)' 활동을 하루 동안 2,000% 급증시킨 일이었다. 당시 美 국방부는 미국과 유럽의 동맹국에게 러시아 發 심리전 대비를 주의시킨 바 있다(Newsweek 4/14/2018). 이렇게 사이버 심리전은 무력충돌 초기 단계에서 경고신호로서 수행될 수도 있지만, 전시가 아닌 선거철과 같은 평시에도 상시적으로 공격을 은밀하게 구사할 수 있으므로 공격대상 사회를 지속적으로 취약하게 만들 수 있다(Antonovich 2011, 35-43; Heickerö 2010, 20). 반면 이와 같이 디지털 정보커뮤니케이션 공간에 대한 심리전 공격은 개인과 대중의 감정과 생각에 영향을 끼치는 활동이므로 심리전 공격에 대한 적절한 반격과 팃포탯(tit-for-tat)과 같은 상호성(reciprocity)에 입각한 복수 행위는 여전히 쉽지 않다.

Ⅳ. 중국 발 사이버 심리전의 양상

중국의 '영향공작(Influence Operations)'은 2003년부터 인민해방군(People's Liberation Army, PLA)의 '3戰(Three Warfares)' 즉 '심리전(psychological warfare)', '여론전(public opinion warfare)', '법률전(legal warfare)'의 영역으로서 문화기관, 미디어, 비즈니스, 학계, 정책전문가 집단 및 국제기관 등을 대상으로 전개된다. 중국은 심리전을 프로퍼갠더, 기만(deception), 위협 및 강압 등의 성격을 갖는 활동으로 분류하여 국내외 여론에 영향을 끼치려는 여론전과 표면적으로는 구별하고 있으나 사이버 공간을 영향공작을 위한 주요한 플랫폼으로 간주하고 있으므로 두 활동의 성격은 명확하게 분리되지 않는다(U.S. Department of Defense 2020, 130)..

중국이 목표청중으로 삼는 대상은 외국인뿐 아니라 해외에 거주하는 중국인 및 화교를 포함하며, 필요시 이들에 대한 위협도 영향공작의 방법이 된다. 해외 거주 중국인 학자나 학생단체 및 공자학원 등의 교육기관은 해외에서 중국 정부의 내러티브를 확산시키는 프로퍼갠더 혹은 공공외교의 주체가 될 수 있다. 영향공작과 관련된 정책결정은 통일전선공작부(United Front Work Department), 국무원신문판공실(State Council Information Office), 국가안전부(Ministry of

State Security)의 고위급에서 이루어진다. 미 국방부는 의회에 제출한 연례보고서 "2020 중국 군사안보 현황(Military and Security Developments Involving The People's Republic of China 2020)"에서 중국이 미국과 같은 개방된 민주주의 국가를 영향공작에 취약한 공격 대상으로 보고 있다고 기술했다(U.S. Department of Defense 2020, 130).

중국은 미중경쟁 시대 전 세계 대중을 대상으로 자국이 책임감 있고 신뢰할 수 있는 글로벌 리더임을 설득하며 중국이 미국을 대신할 수 있는 대안적 패권이 될 수 있음을 강조하고 있다. 특히 중국은 일대일로 사업이 대거 진출해있는 아프리카와 중동, 동아시아의 개발도상국이나 권위주의 국가에 대해 중국이 미국처럼 민주주의와 인권 등 특정 가치와 사상을 강요하지 않고 각국의 체제를 인정하는 포용적인 강대국임을 각인시키는 체제선전에 보다 중점을 두고 있다. 반면 대만과 홍콩 등 중국어권에서의 중국의 내러티브는 러시아가 동유럽에서 확산시키는 내러티브처럼 좀 더 강압적이고 공격적인 성격을 띤다. 즉 글로벌 리더로서의 포용적 이미지를 내세우며 중국의 국제평판을 증진시키려는 선전보다 러시아가 동유럽에서 펼치는 심리전 메시지처럼 역내에서는 중국의 패권적 입지와 '하나의 중국' 원칙을 주입시키는 등 주변 국가들에 대한 내러티브는 일종의 '길들이기'의 성격을 갖는다.

프리덤하우스는 "2018 인터넷 자유: 디지털 권위주의의 부상(Freedom on the Net 2018: The Rise of Digital Authoritarianism)"과 "2019 인터넷 자유: 소셜미디어의 위기(Freedom on the Net 2019: The Crisis of Social Media)"에서 중국 식 인터넷 검열 모델이 사이버 공간을 점점 권위주의 통치에 유리한 방향으로 만들고 있고, 러시아, 중국, 이란 등 권위주의 레짐들이 소셜미디어를 통해 타국의 선거에 지속적으로 개입하고 있다고 경고해왔다(Freedom House 2018; Freedom House 2019). 프리덤하우스의 보고서 "2020년 세계의 자유(Freedom in the World 2020)"는 중국이 러시아의 심리전 방식을 모방하여 자국에서는 사용이 금지된 다양한 세계적 소셜미디어 플랫폼에 허위조작 정보를 확산시키는 온라인 트롤(troll) 활동을 지원하고 있다고 지적했다. 소셜미디어 플랫폼뿐 아니라 중국은 자국 IT 기업이 진출해있는 타국의 정보 인프라인 디지털 텔레비젼 방송과 모바일 핸드폰의 커뮤니케이션 장치를 통해 다양한 정보활동을 전개하고 있다(Freedom House 2020, 6-7).

한편 중국이 서구권에 대해 체제우위를 내세우는 선전 성격의 여론전은 지속되고 있으나 미국의 대통령 선거와 관련해서는 아직 그러한 심리전이 본격화되지 않은 것으로 보인다. 2016년 대선과 마찬가지로 2020년 미 대선은 러시아와 이란이 전개한 사이버 심리전 공격 대상이 되었다. 美 국가정보위원회(U.S. National Intelligence Council)가 작성한 비밀해체된 보고서 "2020년 미 대선에 대한 해외위협(Foreign Threats to the 2020 US Federal Elections)"는 2020년 미 대선의 투표결과나 투표용지 등과 관련해서 타국 정부의 개입은 없었지만, 러시아와 이란의 온라인 여론에 대한 영향공작이 있었다. 美 대선을 앞두고 9월 마이크로소프트사(Microsoft)도 러시아 군사정보국(GRU) 해커들이 200개 이상의 美 주요 기관 컴퓨터 네트워크와

약 7천개의 이메일 계정에 대한 해킹을 시도했다고 밝힌 바 있으며, 美 국가정보국(DNI) 국장도 미 유권자 정보를 확보한 이란이 美 우파 단체 프라우드 보이스(Proud Boys)를 사칭하여 이메일을 통해 유권자를 위협하는 활동을 벌이고 있음을 언급한 바 있다. 당시 로버트 오브라이언(Robert C. O'Brien) 국가안보보좌관은 중국의 美 대선 개입 프로그램의 존재를 경고했었다. 하지만 국가정보위원회의 보고서는 트럼프 前 미국 대통령이 주장한 바와 달리 중국은 2020년 美 대선에서 심리전을 전개하지 않았으며, 미 대선에 대한 새로운 심리전 공격 주체로서 쿠바와 베네수엘라, 헤즈볼라가 활동한 사실을 확인했다(U.S. National Intelligence Council 2021).

반면 대조적으로 역내 중국어권 국가의 선거에 대해서 중국의 심리전은 활발하게 전개되고 있다. 2004년 조직된 온라인 공간에서 중국 당국의 프로퍼갠더 활동을 활발하게 펼치는 200만 명 규모의 댓글부대 "5마오군(五毛軍, 5 cent army)"은 중국 정부의 주요 정책을 지지하는 내러티브를 확산시키며 친중 여론을 형성하는 활동을 펼치고 있다. 반정부 게시글이나 댓글을 당국에 신고하면 건당 5마오(약 85원)를 수당으로 받았던 데에서 이름이 만들어진 이러한 댓글부대는 매년 평균적으로 4억4천8백만 개의 댓글을 올리고 있다. 美 스탠포드대학 인터넷 옵저버터리(Stanford Internet Observatory) 연구소가 분석한 결과, 2018년 대만의 통일지방선거에서 중국 정부를 옹호하는 댓글 4만3천8개의 99% 이상이 이러한 댓글부대에 의해 작성되었음이 밝혀졌다(Washington Post 2019).

중국은 2018년 11월 대만 통일지방선거에서 차이잉원(蔡英文) 총통과 집권 민진당이 패배하게끔 가짜뉴스를 대거 발신하는 프로퍼갠더 활동을 왕성하게 전개했다. 대만 법무부 조사국은 코로나19 감염병 관련 가짜뉴스의 발신원을 추적 조사한 결과 중국 정부의 해커 조직인 '망군(網軍)'이 2019년 6월부터 7월에 걸쳐 도메인 거래 플랫폼을 통해 대만인 소유 도메인 13개를 구입한 사실을 밝혀냈다. 이러한 활동은 2018년 선거 개입처럼 2020년 1월 대만 총통선거와 입법위원 선거를 앞두고 심리전을 개시하기 위한 사전 작업으로서 중국은 인터넷 도메인 인수 뒤 페이스북과 웨이보(weibo) 및 대만 소셜미디어 가짜계정을 이용하여 친중 후보가 선거에서 이기도록 여론을 조작하는 시도를 보여주었다(동아일보 2020/3/9). 인터넷 옵저버터리(Stanford Internet Observatory) 연구소가 조사한 결과, 소셜미디어의 중국 본토 가짜계정이 대만 총통선거 기간 동안 '하나의 중국', '경제난' 등의 쟁점을 온라인 공간에 확산시켰고 이러한 활동은 2018년 대만 독립을 주장한 민진당의 실패에 기여한 것으로 분석되고 있다(Washington Post 2019).

대만 정부는 2018년 중국의 심리전 공격이 2020년 1월 대만 총통선거에서도 반복될 것을 예상하여 2019년 4월 중국 인터넷 기업이 제공하는 동영상 서비스를 금지하는 방안을 마련했다. 대만에서 서비스를 제공하는 중국 최대 검색 업체 바이두(百度) 산하 아이치이(愛奇藝)는 서비스 제공이 금지되었고 대만 진출을 모색하고 있던 텅쉰 비디오(騰訊視頻)도 금지 대상이 되었다(뉴시스 2019/4/3). 2019년 홍콩 정부의 도주범죄인 및 형사법 관련 법률 지원 개정 법

안이 도입되면서 6월 초부터 촉발된 홍콩 시민들의 '反범죄인 인도법안(송환법)'에 대한 반대 시위도 중국 심리전의 직접적인 공격대상이 되었다(데일리굿뉴스 2019/8/23). 중국은 페이스북과 트위터에서 홍콩의 민주화 시위대를 악마화하는 메시지를 확산시켰고 구글(Google), 레딧(Reddit), 유튜브(YouTube)의 콘텐츠가 노출되는 순위 시스템을 조작하여 그러한 메시지를 전방위로 유포시키는 활동을 펼쳤다(Freedom House 2020, 7).

이러한 홍콩 사태를 지켜 본 대만 유권자들은 일국양제 체제인 홍콩에 대한 중국의 강압적인 태도와 홍콩 시위를 공격하는 중국의 심리전을 크게 경계했고 대만 정부는 선거와 관련된 허위조작정보의 확산에 대비하는 대책부서를 따로 설치하기도 했다. 흥미롭게도 2020년 1월 대만 총통선거에서 중국이 왕성한 심리전을 전개했음에도 불구하고 친중 후보가 패배하고 차이잉원이 승리하자 중국은 차이잉원이 표를 매수하고 인터넷 부대를 동원하여 중국에 대한 공포를 부추기는 가짜뉴스를 확산시켰다고 주장했다(중앙일보 2020/1/12). 이후 외교적 긴장 관계가 지속되고 있는 대만과 중국의 양안관계 속에서 대만을 상대로 하는 중국 發 허위조작정보가 지속적으로 확산되자 차이잉원 대만 총통은 민진당 내 미디어 담당 부서의 업무가 가짜뉴스 문제에 신속하게 대응할 것을 주문한 바 있다(한국경제TV 2020/11/26).

최근 중국의 허위조작정보 유포 활동은 정치적인 성격의 사이버 심리전 성격을 넘어 역내 동아시아 국가의 문화와 역사를 왜곡하고 타국의 고유한 문화자산을 중국의 것으로 둔갑시키는 등 역내 대중을 대상으로 제국주의적인 태도를 드러내고 있다. 중국 관영매체 환구시보는 한국전쟁 70주년 관련 방탄소년단(BTS)의 밴 플리트상(General James A. Van Fleet Award) 수상 소감을 문제 삼았고, 중국의 소셜미디어인 웨이보(weibo)와 위챗(wechat)을 비롯해 트위터에서 가짜뉴스를 확산시키며 오히려 BTS의 팬클럽 아미(Army)의 반발에 직면하기도 했다(조선일보, 2020/12/17). 또한 중국은 한국 연예오락 프로그램의 역사콘텐츠를 거짓정보라고 주장하면서 이러한 프로그램에 등장한 한국 연예인들의 역사와 문화지식에 대해 공격하고 한류에 대한 반감을 드러내고 있다(조선일보, 2020/12/17). 또한 중국은 한국의 김치와 한복 등 고유한 문화가 자국의 문화라고 주장하거나 중국 최대 포털 바이두(Baidu)에 윤동주 시인, 독립운동가 이봉창, 윤봉길의 국적을 중국, 민족을 조선족으로 표기하거나, 한류스타 이영애와 피겨스케이팅 선수 김연아도 조선족으로 표기하는 등 전방위적인 문화 동북공정을 온라인 공간을 통해 전개하고 있다(한국경제 2021.2.21.).

V. 미국과 유럽의 대응과 대비태세

앞서 논의한 바, 사이버 심리전이 2000년대 초반부터 나타났음에도 불구하고 미국과 유럽이 최근에 와서야 군사안보 차원에서 이러한 심리전을 심각하게 인식하며 대응태세를 갖추

게 된 가장 중대한 이유는 허위조작정보 유포 활동을 통해 전개된 심리전이 선거 과정에 직접적인 영향을 끼치며 민주주의 제도의 정상적인 기능을 방해하는 등 주권의 영역에 위협이 되었기 때문이다. 또한 디지털 허위조작정보의 유포활동이 세계적 권위주의 확산에 기여하며 진영 간 갈등에도 영향을 끼치고 있는 것도 서구권의 경각심이 높아진 원인이 되고 있다.

군사적인 차원에서 미국의 기존 전략문화는 '전통적인 국가 간 전쟁'이나 '대전쟁 패러다임(big war paradigm)'에 초점이 맞춰져 있었고 美 국방부의 '단일한 제한적인 형태의 전쟁(a single preclusive form of warfare)'에 대한 과도한 집중은 사이버 심리전과 같은 다차원적이고 다기능적인 하이브리드 위협에 대해 충분히 대비되어 있지 않았다(Mattis 2018). 현재 미국의 정보작전(Information Operations)은 특수작전사령부(U.S. Special Operations Command, SOCOM)에서 수행하고 있고, 2019년 4월 사령부는 정보작전 활동을 더 효과적으로 수행하기 위해 'Joint Web Ops Center'를 설치했다. 육군도 미래사이버작전에 있어서 정보작전을 주요 활동으로 간주하고 있으며, 2020년 7월 육군사이버사령부(Army Cyber Command, ARCYBER)를 이끌고 있는 중장 스테픈 포가티(Lt. Gen. Stephen G. Fogarty)는 육군의 정보공작을 사이버전, 영향공작, 전자전 역량으로 통합시켜 즉각적인 정보전 전투력을 갖추게 하는 계획에 착수했다(Tucker 2021).

바이든 행정부 출범 이후 새로 신설된 美 하원 군사위원회 산하 정보 · 특수전 소위원회에 출석한 제임스 설리번(James Sullivan) 국방정보국(DIA) 사이버 담당관 , 닐 팁턴(Neil Tipton) 국방차관실 직속 수집 · 특수프로그램(Collections and Special Programs) 담당 국방정보국장(Director of Defense Intelligence, DDI)을 비롯하여 크리스토퍼 메이어(Christopher Maier) 미 국방부 특수공작 · 저강도 분쟁 담당 차관보 대행(Acting Assistant Secretary of Defense, Special Operations/Low-intensity Conflict)은 미국이 러시아와 중국 등으로부터의 심리전에 대응할 정보작전을 재편할 필요를 강조하였다. 메이어는 현재 미국이 폭력적인 극단주의 세력에 대응하는 데에 집중되어 있으나 오늘날 정보를 위협의 도구로서 사용하는 세력에 대응하기 위해 SOCOM의 군 인력이 행동과학, 문화, 언어, 디지털 미디어 기술 등 기존의 훈련 내용과는 매우 상이한 훈련 과정을 거치게 되거나 혹은 그러한 기술을 갖춘 인력을 선발할 수 있어야 한다고 강조했다(Tucker 2021)

美 국방부는 국무부 공공외교정책 부서와 미국의 해외 방송을 관장하는 글로벌미디어국(United States Agency for Global Media, USAGM)과의 공조 하에 적성국의 허위조작정보 유포에 대응할 것이며 특수전사령부(SOCOM)의 군사정보지원작전(Military Information Support Operations, MISO)이 이러한 정보공작에 대처할 것이라고 언급했다(Washington Post 2021). 민주당의 루벤 갈레고 소위원장은 2020년 9명의 전 구사령관들이 국가정보국장(DIA)에게 중국과 러시아의 심리전에 대응할 긴급지원을 요청했음을 밝혔다(House Armed Services Committee 2021). 이러한 긴급한 요구에 부응하여 2021년 3월 말 美 특수전 사령관(U.S.

Special Operations Command commander) 리처드 클락 장군(Army GEN Richard D. Clarke)은 美 의원들에게 허위조작정보의 유포를 통한 심리전 대응에 있어 동맹국과 협력할 합동태스크포스를 구성했음을 밝혔다.[2)]

미국과 유럽은 2016년 이후의 서구권의 거의 모든 선거 여론이 러시아의 사이버 심리전에 의해 직접적으로 영향을 받자 NATO와 EU의 공조를 통해 다양한 대응태세를 마련해나가기 시작했다. 미국과 유럽은 사이버 심리전을 개별적으로 구사되는 단독적인 위협의 형태로 보기보다 하이브리드 위협의 한 형태로 간주하기 때문에 하이브리드 위협에 대한 대응의 차원에서 사이버 심리전이 다뤄지고 있다. 먼저 2014년 9월 웨일즈(Wales) NATO 정상회담에서는 하이브리드전에 대한 미국과 유럽의 우려가 처음 공식적으로 언급되어 하이브리드전에 대한 국제사회의 관심을 촉발하는 계기가 되었다. NATO는 하이브리드전을 사이버 공격과 같은 비군사 수단과 군사수단을 혼합하여 위협을 구사하는 '현대전'이며, '군사 · 준군사(paramilitary) · 민간수단이 노골적으로 혹은 은밀하게 사용되는 고도로 통합된 도발'로서 평가했다(NATO 2014).

2014년 NATO 정상회담 선명을 통해 NATO는 하이브리드전이 공격대상 국가의 정책결정을 혼란하게 만들어 정상적인 국정운영을 방해하며 사회를 분열시키는 등 전복적인 목적을 갖는다고 지적하고, 공격국가가 공격의 증거를 은폐하여 NATO의 보복과 군사개입 명분을 상실하게 만드는 전략을 사용한다고 언급했다. 미국과 유럽은 2018년 9월 폴란드 바르샤바(Warsaw)에서 개최된 NATO 군사위원회 컨퍼런스에서 미군유럽사령부와 EU군 최고 사령부의 최고 사령관 커티스 스캐퍼로티(Curtis M. Scaparrotti)는 러시아의 하이브리드전이 서구의 가치와 서구 정부의 신뢰성(credibility)을 훼손하려하고 군사적 충돌 없이 심리전으로써 정치적 목적을 획득하려 한다고 언급했다.

미국과 유럽이 하이브리드전 대응을 본격적으로 공식적으로 논의하기 시작한 2014년 웨일즈 NATO 정상회담을 계기로 NATO는 하이브리드 위협 대응의 NATO와 EU 간 공조에서 가장 시급한 활동으로서 '전략커뮤니케이션(strategic communication)'의 역할에 주목했다. NATO는 2014년 9월 NATO 전략커뮤니케이션센터(NATO Strategic Communication Centre of Excellence)를 라트비아(Latvia)에 설립함으로써 유럽-대서양 역내에 전략커뮤니케이션 체제를 구축하는 일에 가장 먼저 착수했고, 이러한 전략커뮤니케이션 체제는 유럽의 사이버전 모의훈련에서도 핵심 역할을 담당하고 있다.[3)] 당시 유럽은 중동으로부터의 대규모 난민 유입, 이슬람 극단주의에 의한 유럽 내 테러 빈발 및 영국의 EU 탈퇴 가능성 등 역내 안보 불확실성이 증대되고 있었으므로 이 센터 설립의 필요성이 요구되고 있던 터였다.

현재 사이버 심리전을 포함한 사이버전에 대비하는 사이버 방위(cyber defence)는 NATO 회원국에 대한 집단방위(collective defence)의 주요 임무이다. 2016년 7월 NATO는 '사

2) https://www.dvidshub.net/video/788438/senate-committee-reviews-authorization-request-fiscal-year-2022.
3) https://www.nato.int/cps/en/natohq/topics_156338.htm(검색일: 2020.3.4.)

이버 방위협정(Cyber Defence Pledge)'을 통해 사이버 공간을 육 · 해 · 공과 아울러 독립된 제4의 작전영역이며 국제법이 적용되는 공간임을 재차 확인했고, 이러한 인식 하에 사이버전과 하이브리드전 대응에 집중할 수 있는 조직을 다수 설립했다. 먼저 NATO는 2018년 브뤼셀 정상회담(Brussels Summit)에서 사이버 심리전을 포함한 사이버 공격에 대응할 조직이자 NATO의 강화된 명령체계의 일부로서 'NATO사이버공간작전센터(NATO Cyberspace Operations Centre, COC)'를 'NATO연합변혁사령부(Allied Command Transformation, NATO's ACT)' 산하 'NATO 센터(NATO Centres of Excellence, NATO COEs)'에 설치할 것을 결정했다.[4] NATO는 이러한 새로운 조직을 통해 24시간 동맹국의 도움 요청에 응할 수 있는 'NATO 사이버 신속대응팀(NATO Cyber Rapid Reaction teams)'도 운영하고 있다.

NATO는 2000년대 초부터 사이버전을 대비하는 다양한 연례 군사훈련을 수행해왔다. NATO가 새롭게 마련한 방위태세와 군사훈련의 대부분은 평시와 전시를 구분하지 않는 사이버 심리전을 비롯한 다양한 사이버 공격 및 하이브리드전 상황을 상정한 군사적 대응 및 시민사회 보호에 집중되어 있다. 1992년 이래 NATO가 시행해온 '위기관리훈련(Crisis Management Exercise, CMX)'은 2016년부터는 사이버 테러, 소셜미디어를 통한 허위조작정보의 유포 및 해킹, 테러 등이 복합적으로 일어날 수 있는 하이브리드 위협에 민간과 군이 함께 대응하는 훈련을 실시하기 시작했다(NATO 2019). 소위 '페이스(Parallel and Coordinated Exercise, PACE)'로 불리는 EU와 NATO의 합동 모의군사훈련 중 'EU HEX-ML 18 (Hybrid Exercise - Multi Layer 18)'도 사이버전과 허위조작정보 유포를 통한 심리전 공격 및 범죄 · 밀수 · 테러와 관련된 복잡한 하이브리드 위기 상황이 일어나는 시나리오를 가정하고 정보교환 및 효과적인 위기 대응을 연습한다.

NATO의 '사이버방어협력센터(Cooperative Cyber Defence Centre of Excellence, CCDCOE)'는 이미 2010년부터 사이버 방위훈련인 '라키드쉴드훈련(Excercise Locked Shields)'을 주도하고 있다. 라키드쉴드훈련은 최첨단 기술과 시뮬레이션을 통해 대규모의 사이버 공격 하에서 국가의 IT 시스템과 주요 인프라를 방어하는 기술을 향상시키는 훈련을 수행하며, 이러한 훈련에는 각국이 당면할 전략적 의사결정과 법적 · 커뮤니케이션 상황을 포함하고 있다. 2008년부터 사이버 공격 상황에서 NATO 내 다양한 조직 간 공조와 전략적 의사결정을 모의연습하기 위해 수행하고 있는 NATO의 연례 사이버 방위 주력훈련(flagship exercise)인 '사이버연대(Cyber Coalition)'에는 EU도 매년 참여하고 있다.

NATO연합변혁사령부(ACT)가 주도하는 사이버연대 훈련은 사이버전에서의 기술적, 절차적 체계를 구비하기 위한 모의훈련으로서 미국과 유럽은 사이버전 관련 주요 정보를 공유하고 상황을 함께 판단하며 사이버 작전을 조정, 협력하여 군사작전을 수행하는 능력을 향상시키고 있

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

다. 2017년 사이버연대 훈련에는 특별히 사이버 심리전 상황을 염두에 둔 모의훈련이 진행되었으며, 2019년의 훈련은 급속도록 발전하는 디지털 기술환경의 새로운 도전에 대응하고자 AI 기술을 이용한 다양한 시뮬레이션이 이루어졌다. 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 위험에 대해 적절한 의사결정 및 대응 행위를 취하는 알고리즘을 개발하기 위한 프로그램이 포함되었다.

EU도 2016년부터 사이버전 및 하이브리드 위협에 대응하는 일련의 제도적 이니셔티브와 절차를 적극적으로 마련하고 NATO와의 공조를 통해 대응책을 도모하기 시작했다. 2016년 2월 EU와 NATO는 'EU 사이버 방위정책 프레임워크(EU Cyber Defence Policy Framework)'에 근거하여 '사이버 방위 기술협정(Technical Arrangement on Cyber Defence)'을 체결하고 사이버 공격과 관련된 정보공유, 군사훈련, 연구 등의 분야에서 긴밀한 협력을 도모하기로 천명했다(NATO 2016). 또한 EU는 'EU정보정세센터(EU Intelligence and Situation Centre, EU INTCEN)'에 'EU하이브리드퓨전반(EU Hybrid Fusion Cell)'을 설립하여 사이버전에 대비한 대응 체제를 갖춰나갔다. 이 조직들은 사이버 정보심리전 공격을 모니터링하고 관련된 주요 정보를 취합하고 분석하며 EU 정책결정자들에게 구체적인 정책을 제안하는 역할을 담당하고 있다(European Commission 2016).

2016년 12월 6일 EU이사회와 대서양위원회(North Atlantic Council)는 미국과 유럽 8개국 – 영국, 프랑스, 독일, 폴란드, 스웨덴, 핀란드, 라트비아, 리투아니아 - 이 중심이 되어 2017년 10월 2일 핀란드 헬싱키(Helsinki)에 '유럽 하이브리드 위협 대응센터(European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE)'를 설립했다. Hybrid CoE는 유럽의 하이브리드전 대응에 있어서 NATO와 EU간 전략적 토론과 훈련을 촉진하며 하이브리드 위협 대응의 모범사례를 개발하고 연구결과를 역내에 공유하는 역할을 담당한다.[5] 이러한 Hybrid CoE의 설립 과정에서 유럽은 허위조작정보 유포를 통한 사이버 심리전이 하이브리드전의 주요 위협 수단이 되고 있음을 재확인했다(NATO 2019b).

최근 러시아는 2021년 3월부터 우크라이나 국경 지역인 돈바스에 탱크와 군용차량 등 러시아의 약 8만 명의 대규모 병력을 집결시키고 있으며 이 병력 중 대대전술단 1만4천명은 정보전과 포병 화력을 결합시킨 부대로서 드론이나 전술무인기 등 첨단 무기를 사용하고 적의 통신망을 마비시킬 수 있다. 4월 12일 미국과 영국 등 G7 외무장관과 EU는 공식성명을 통해 러시아의 이러한 도발에 우려를 표명했고 미국 유럽사령부(EUCOM)는 현 상황을 임박한 위협으로 보고 경계태세를 최고 수준으로 격상한 상태이다. 2014년 크림반도 합병 과정에서 러시아가 보여준 심리전이 수반된 하이브리드전이 예상되는 상황에서 이번 러시아의 재도발은 상술한 미국과 유럽의 2014년 이후 마련해온 다양한 대비태세가 얼마나 효과적일 수 있는지 시험할 수 있는 첫

5) https://www.hybridcoe.fi/what-is-hybridcoe.

사례가 될 것으로 보인다.

VI. 나오며: 한국에 대한 함의

21세기 디지털 기술의 고도화와 인터넷 네트워크의 전방위 연결 및 지구적 확장은 국가 간 갈등의 새로운 전장을 공격 비용이 낮으면서도 분쟁 상대국에 대해 치명적인 피해를 입힐 수 있는 사이버 공간으로 이동시키고 있다. 특히 현대 AI 기술의 양방향 커뮤니케이션 기능을 비롯하여 다양한 첨단 디지털 정보커뮤니케이션 기술은 사이버 심리전을 과거 전시에 수반되는 부차적 전술의 차원을 넘어 평시와 전시를 가리지 않고 전개되는 적대 국가에 대한 효과적인 위협 수단이 되어가고 있다. 사이버 심리전은 이제 현재 전방위로 확대되는 미 · 중 전략경쟁, 4차 산업혁명의 진전에 따른 강대국들의 미래전 대비, 환경 · 보건 · 에너지 · 대량난민 · 재난 · 테러 · 감염병 등 비전통 안보(non-traditional security) 이슈의 부상과 함께 세계 안보환경을 더욱 복잡하게 만들고 있는 것이다.

과거에도 존재한 심리전은 현대 사회의 초연결성을 취약점으로 이용하면서 개방되어 있는 민주주의 사회의 온라인 공론장을 위험한 전장으로 변화시키고 있다. 러시아와 중국, 이란 등이 전 세계 민주주의 사회의 선거에 개입하며 소셜미디어 플랫폼을 통해 허위조작정보를 유포하는 심리전을 빈번하게 전개하자 미국과 유럽은 세계 어느 지역보다도 대비태세 마련을 서둘렀다. 미국과 유럽은 사이버 심리전이 사이버전에 동반되며 사회교란 및 국가 시스템 마비 등 공격의 파괴력을 배가시킬 수 있으므로 NATO와 EU간 긴밀한 공조를 통해 사이버전에 중점을 둔 대응체제를 마련하고 다양한 모의군사훈련을 개최하고 있으며 민관 및 민군 협력을 장려하는 제도적 이니셔티브를 다양하게 추진해왔다. 미국과 유럽의 이러한 노력은 사이버 심리전을 동반하는 하이브리드 위협에 노출되고 공격받더라도 사회의 회복력을 유지하는 것을 목표로 삼고 있다.

중국은 러시아가 서구권과 동유럽에서 전개한 방식의 사이버 심리전 공격을 특히 동아시아 역내에서 전개하고 있으며, 앞으로 중국이 그러한 전술을 미국과 유럽 등 서구권의 선거철에 전개할 가능성은 농후하다. 한국은 중국이 우리의 문화와 역사에 대한 왜곡된 정보를 유포하는 방식의 간접적인 형태의 정보공격을 경험하고 있다. 특히 미중전략경쟁으로 인해 서구권 민주주의와 러시아와 중국을 중심으로 한 권위주의 진영 간 경제와 안보 영역의 긴장과 갈등이 확대되고 심화되는 현 정세를 감안하면 앞으로 심리전은 진영 간 정치적 우위 확보와 경쟁 세력 간 위기 상시화의 전술적 수단으로 빈번하게 이용될 것으로 보인다.

이러한 맥락에서 미국과 유럽의 사이버 심리전에 대한 다차원의 대응체계와 조직의 구축 및 NATO와 EU, EU 회원국 내의 협업과 공조의 노력은 한국과 동북아시아, 그리고 동아시아와 아시아-태평양 지역의 안보협력에도 시사하는 바가 크다. 특히 개방된 민주주의 국가인 미국

과 EU가 하이브리드 위협 대응에 있어서 가장 먼저 서둘렀던, 전략커뮤니케이션 체제의 구축과 회원국 간 긴밀한 정보 공유 및 위기 상황에 대한 공동의 인식 수렴, 다양한 교류 및 연구활동은 한국과 역내 주요국들이 어떤 협력 의제를 통해 공조하고 협력을 확대할 것인지 고찰하고 논의하는 데에 적용할 만한 유용한 사례가 될 것으로 보인다. 또한 최근 한국이 전통안보 및 신안보 영역에서 미국 및 유럽과 다양한 의제를 통해 교류, 협력하고 하이브리드전 모의 군사훈련 및 다양한 협의체에 참여하며 구체적인 협력 의제를 발굴하는 노력은 지속되고 확대될 필요가 있다. 더불어 한국은 더 다양한 정부 부처와 기관, 민간단체와 전문가들이 미국 및 유럽의 하이브리드 위협 대응과 관련된 교류, 훈련 및 협의체에 동참하고 아이디어를 공유하며 기여와 협력을 증진할 방안을 국가적, 지역적, 세계적 차원에서 마련하고 장려할 이니셔티브를 취할 필요가 있다.

한편 미국과 유럽 등 서구권 민주주의 국가에서 진행된 타국 發 심리전에 대한 군사적 차원에서의 대응이 반드시 대중의 지지를 얻는 것만은 아니다. 국가가 온라인 공론장에서의 반정부 내러티브를 정부 행위자가 검열하며 일일이 대응하는 것은 대중의 입장에서는 표현의 자유에 대한 간섭이나 침해행위로 인식될 수 있기 때문에 민주주의 정부로서는 매우 조심스럽게 접근해야 할 부분이다. 잭 쿠퍼(Zack Cooper)는 상호성에 입각한 중국 發 심리전에 대한 민주주의 국가의 정책이 다음과 같은 사안을 고려해야 함을 역설했다. 먼저 중국과 같은 권위주의 국가에서는 국가의 언론과 개인의 커뮤니케이션 행위에 대한 검열이 일상화되어 있고 정부의 프로퍼갠더 내러티브는 정보조작을 통해서 사회 속에 만연되어 있으므로 중국 발 메시지에 대한 검열과 규제는 자칫 자유로운 정치적 의사표현과 관련한 중국과 민주주의 국가의 차별성을 희석시킬 가능성이 있다. 둘째, 상호성에 입각한 미국의 중국에 대한 대응은 미국의 강점과 중국의 약점에 초점을 두어야 하며, 중국 행위에 대한 '반응적(reactive)' 정책은 중국이 미중경쟁 관계의 성격을 결정하게 만드는 우를 범할 수 있다. 민주주의 사회의 정보공간의 강점은 정보의 자유로운 이동에 있으므로 정보에 대한 제한과 검열이 중국에 대한 대응이 될 경우 민주주의 정보환경의 강점인 개방성과 투명성을 약화시킬 수 있다. 셋째, 중국의 정보심리전은 사실상 중국의 이미지와 평판을 훼손시키고 있으며 미국은 타국이 중국이 아닌 미국을 모범사례로 삼도록 만드는 것이 중요하다(Cooper 2020).

이와 같은 주장은 미국 내 많은 지식층이 공유하는 시각이지만 이러한 원칙에 입각한 접근법과 정공법이 과연 다양성과 포용성을 상실하고 분열하고 있는 현재의 미국과 서구 민주주의 사회에서 효과가 있을 지는 의문스럽다. 더욱 우려스러운 바는 고도로 지능화되고 있는 정보커뮤니케이션 기술과 치밀하게 고안된 설득기제를 이용한 현대의 심리전이 '인지적 해킹(cognitive hacking)'으로 불릴 정도로 개인과 대중의 정보분별을 어렵게 하고 있다는 점이다. 따라서 민주주의 사회의 개인과 대중의 정보분별과 성숙한 시민의식 및 다양한 방식의 가짜뉴스 탐지 및 팩트체크 기술의 발전에 기대고 있는 원칙주의적 접근법은 전술적, 전략적 차원에서 볼 때는 심리전에 대한 다소 안이한 대응을 초래할 수 있다. 우리의 경우도 같은 언어를 사용하는

북한에 의한 심리전의 위협에 항시로 노출되어 있고 현재 중국 발 허위조작정보에 의해 피해를 경험하고 있으므로 미국과 유럽의 대응 사례는 우리도 시급히 논의를 시작할 필요가 있다.

[참고문헌]

김경순. "러시아의 하이브리드전: 우크라이나 사태를 중심으로"『한국군사』4집 (2018).

송태은. "디지털 시대 하이브리드 위협 수단으로서의 사이버 심리전의 목표와 전술: 미국과 유럽의 대응을 중심으로"『세계지역연구논총』제39집 1호(2021).

_____. "사이버 심리전의 프로퍼갠더 전술과 권위주의 레짐의 샤프파워"『국제정치논총』제59집 2호(2019).

_____. "디지털 허위조작정보의 확산 동향과 미국과 유럽의 대응"『IFANS 주요국제문제분석』2020-13. 국립외교원 외교안보연구소(2020a).

_____. "하이브리드 위협에 대한 최근 유럽의 대응."『IFANS 주요국제문제분석』2020-13. 국립외교원 외교안보연구소(2020b).

신범식 · 윤민우, "러시아 사이버안보 전략 실현의 제도와 정책,"『국제정치논총』제60집 2호 (2020).

조한승. "민간군사기업의 전쟁 외주가 전쟁 양상 변화에 미치는 영향"『국방연구』제55권 1호(2012).

Antonovich, Pavel. "Cyberwarfare: Nature and Content." Military Thought 20-3 (2011).

Calha, Julio M. "Hybrid warfare: NATO's new strategic challenge?" General Report, NATO Parliamentary Assembly, Defence and Security Committee(October 10, 2015).

Carment, David and Dami Belo, "War's Future: The Risks and Rewards of Grey-Zone Conflict and Hybrid Warfare" Canadian Global Affairs Institute (October 2018), pp.4-5. https://d3n8a8pro7vhmx.cloudfront.net/cdfai/pages/4059/attachments/original/1539971167/Wars_Future_The_Risks_and_Rewards_of_Grey-Zone_Conflict_and_Hybrid_Warfare.pdf?1539971167(검색일:2020.2.5).

Central Intelligence Agency, "Definition of the term 'psychological warfare'" CIA-RDP84-00022R000400110010-8(1948). https://www.cia.gov/library/readingroom/docs/CIA-RDP84-00022R000400110010-8.pdf(검색일: 2020.6.1.).

Cooper, Zack. "How to respond to China's information warfare," American Enterprise

Institute(October 29, 2020). https://www.aei.org/op-eds/how-to-respond-to-chinas-information-warfare(검색일: 2021.2.21.)

Errey, M. Hammond. "Understanding and Assessing Information Influence and Foreign Interference" Journal of Information Warfare. 18-1(2019).

European Commission, "Joint Framework on countering hybrid threats" (April 6, 2016). https://eucyberdirect.eu/content_knowledge_hu/joint-framework-on-countering-hybrid-threats(검색일: 2020.4.15.)

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: 2020.1.5.)

James D. Fearon, "Rationalist Explanations for War." International Organization 49-3(1995).

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

Freedom House. "Freedom on the Net 2018: The Rise of Digital Authoritarianism" (October 2018). https://freedomhouse.org/sites/default/files/FOTN_2018_Final.pdf(검색일: 2019.7.21.)

Freedom House. "Freedom on the Net 2019: The Crisis of Social Media" https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf(검색일: 2019.3.2.)

Freedom House, "Freedom in the World 2020: A Leaderless Struggle for Democracy" https://freedomhouse.org/sites/default/files/2020-02/FIW_2020_REPORT_BOOKLET_Final.pdf(검색일: 2021.2.7.)

Heickerö, Roland, "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations." Swedish Defence Research Establishment (2010). www.foi.se/ReportFiles/foir_2970.pdf(검색일:2020.6.7.)

House Armed Services Committee, "Subcommittee on Intelligence and Special Operations Hearing: "Disinformation in the Gray Zone: Opportunities, Limitations, and Challenges" (March 16, 2021). https://armedservices.house.gov/2021/3/subcommittee-on-intelligence-and-special-operations-hearing-disinformation-in-the-gray-zone-opportunities-limitations-and-challenges

(검색일: 2021.4.5.)

Kwong, Jessica. "Russian Trolls Increased '2,000 Percent' After Syria Attack, Pentagon Says," Newsweek (April 14, 2018) https://www.newsweek.com/russian-trolls-increased-2000-percent-after-syria-attack-pentagon-says-886248(검색일: 2019.6.10.)

Mattis, James N. "Roll Out Speech for National Defense Strategy." School of Advanced International Studies, Johns Hopkins University, Washington, D.C.(January 19, 2018).

McCulloh, T. & Johnson, R. (2013). "Hybrid Warfare," ISOU Report, 13-4(August 2013).

McFate, Sean. The New Rules of War: Victory in the Age of Durable Disorder. New York, NY: William Morrow, 2019.

NATO, "Wales Summit Declaration." Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. NATO Press Release (September 5 2014).

NATO, "Next Steps in NATO's Transformation: To the Warsaw Summit and Beyond" NATO White Paper(2015).

NATO, "NATO and the European Union enhance cyber defence cooperation" (February 10, 2016). https://www.nato.int/cps/en/natohq/news_127836.htm(검색일: 2020.3.4.)

NATO, "Crisis Management Exercise 2019" Press Release (May 3, 2019a). https://www.nato.int/cps/en/natohq/news_165844.htm(검색일: 2020.2.9.)

NATO, "NATO's response to hybrid threats" (August 8, 2019b). https://www.nato.int/cps/en/natohq/topics_156338.htm(검색일: 2020.4.15.)

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:2020.4.23.)

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

Tucker, Patrick, "Key Official: Defense Information Operations 'Not Evolving Fast Enough'" Defense One (March 17, 2021). https://www.defenseone.com/technology/2021/03/key-official-defense-information-operations-not-evolving-fast-enough/172742(검색일: 2021.3.31.)

Tucker, Patrick, "Putin Authorized Smear Campaign Against Biden, US Intelligence

Concludes" Defense One (March 16, 2021). https://www.defenseone.com/technology/2021/03/putin-authorized-smear-campaign-against-biden-us-intelligence-concludes/172715(검색일: 2021.3.31.)

U.S. National Intelligence Council, "Foreign Threats to the 2020 US Federal Elections" ICA 2020-00078D(Declassified document) (March 10, 2021). https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf(검색일: 2021.4.15.)

U.S. Department of Defense, Military and Security Developments Involving The People's Republic of China 2020, Annual Report to Congress(2020).

Wagner, Harrison. "Bargaining and War," American Journal of Political Science 44-3(2000).

Gertz, Bill, "'Three Warfares': U.S. pummeled by covert disinformation war waged by Russia, China," Washington Post(March 16, 2021). https://www.washingtontimes.com/news/2021/mar/16/us-pummeled-covert-disinformation-war-waged-china-(검색일: 2021.4.1.)

[신문기사]

뉴시스, "대만, 중국발 가짜뉴스 유입 차단 위한 규제 강화 추진" (2019. 4.3). https://newsis.com/view/?id=NISX20190403_0000608795(검색일: 2021.2.1.)

데일리굿뉴스, "中, 홍콩 시위 겨냥해 '가짜뉴스' 공세…'흡수통합' 목적" (2019.8.23.). http://www.goodnews1.com/news/news_view.asp?seq=89972(검색일: 2021.2.1.)

동아일보, "중국, 대만서 도메인 대량 매수…선거 등 여론조작에 악용" (2020.3.9.) https://www.donga.com/news/Inter/article/all/20200309/100077355/1(검색일: 2021.2.1.)

조선일보, "'역사지식 없어' 中매체들 이효리 · 이수근 등 계속 때린다" (2020.12.17.) https://www.chosun.com/international/china/2020/12/17/KJFOTDHP6NHYFJCRQQMU62FDOY(검색일: 2021.3.5.)

중앙일보, "대만 독립" 반기 든 차이잉원…中 "역사의 죄인" 경고 던졌다"(2020.1.12.) https://news.joins.com/article/23679998(검색일: 2021.1.13.)

한국경제TV, "차이잉원 대만총통 '가짜뉴스로 사회혼란…신속 대응해야'" (2020.11.26.) https://www.wowtv.co.kr/NewsCenter/News/Read?articleId=AKR20201126087400009(검색일: 2021.1.13.)

한국경제, "한복 · 김치도 모자라 '조선족 윤동주'…中 도발 어디까지" (2021.2.21.)

https://www.hankyung.com/life/article/202102199538H(검색일: 2021.4.1.)

Washington Post, "There's another expert player warming up to online election interference. We should worry." (September 23, 2019). https://www.washingtonpost.com/opinions/global-opinions/theres-another-expert-player-warming-up-to-online-election-interference-we-should-worry/2019/09/22/76c8c870-d990-11e9-bfb1-849887369476_story.html (검색일: 2021.2.5.)