CENTER FOR FUTURE WARFARE STUDIES
INSTITUTE OF INTERNATIONAL STUDIES
SEOUL NATIONAL UNIVERSITY

서울대학교 국제문제연구소
미래전 연구센터
08826 서울시 관악구 관악로 1
서울대학교 종합교육연구동 220동 517호

Tel. 02-880-6311
Fax. 02-871-4115

Center for Future Warfare Studies,
Institute of International Studies at Seoul National University |
국제문제연구소 미래전연구센터 워킹페이퍼 No.69(발간일: 2021.5.18.)

사이버 · 전자전/안보의 미중경쟁과 한국

이중구 한국국방연구원 북한군사연구실 선임연구원

〈목 차〉

〈개 요〉

이 글에서는 중첩성을 갖는 사이버 · 전자전/안보의 영역에서 미국과 중국이 각각 군사적 교리와 조직체계를 어떻게 발전시켜왔는지를 살펴보고, 사이버·전자전 영역에서 전개되고 있는 미국과 중국의 주요 행위를 미중경쟁의 맥락에서 비교하면서 미중 사이버 · 전자전 경쟁의 전망을 제시해보고자 한다. 오늘날에는 군사행동이 육 · 해 · 공군의 중추적 기동수단과 무기체계를

정보 데이터베이스와 과감히 연결하여 수행되는 형태를 띄게 됨에 따라, 아군의 디지털구조를 보호하고 상대국의 지휘통제체계와 통신체계를 교란 · 무력화하는 과업은 전쟁의 승패를 결정지을 만큼의 중요성을 갖게 되었다. 사이버전/안보와 전자전/안보는 그에 필요한 공격·방어수단에는 차이가 있지만, 공격·방어의 대상이 디지털체계라는 공통점을 가지며, 이점에서 사이버전과 전자전을 통합함으로써 전과를 확대시키는 사이버전자전의 개념이 필요하다는 지적도 제기되어 왔다. 이러한 사이버 · 전자전과 관련하여, 미국은 정보기술의 발전을 전제한 군사교리를 1990년대 후반부터 발전시켜 왔으며, 합동작전의 측면에서 사이버, 전자전 유관부서들의 조율을 중시하고 있다. 2010년 사이버사령부를 전략사령부 예하로 공식적으로 창설한 이래, 전자전의 중요성도 함께 강조하고 있다. 한편, 2000년대 초부터 '망전일체전(INEW)'과 같은 정보화 전쟁 개념을 가시화시켜온 중국은 사이버, 전자전 임무를 총괄하는 조직인 '전략지원부대'를 2016년 창설하여 미국의 위성감시능력과 ISR 등 전자정보전 우위 상쇄를 추구하고 있다. 서로 상대방에 대한 강점을 확대하고 취약성을 줄이려는 노력이 동(同) 영역 내 미중의 향후 행보를 특징지을 것이다.

Ⅰ. 머리말

'사이버전 · 전자전 영역에서의 미중경쟁은 어떻게 전개되고 있으며, 우리는 이 영역에서 펼쳐지는 미중경쟁에 어떻게 대응해가야 할 것인가?' 1990년대 이래 정보통신 기술의 군사적 활용이 증대되면서, 사이버전 및 전자전 능력의 중요성에 대한 인식이 확대되어 왔다. 2009년에 창설된 미국의 사이버사령부와 2016년 발족한 중국의 전략지원부대를 볼 때, 이미 사이버전 공격 및 방어, 전자전 공격 및 방어 능력은 주요국 군사력의 한 축으로 자리잡혔다고 할 수 있다. 사이버 영역에서의 군비경쟁은 이미 시작되었다는 평가도 제시되고 있다(Siroli 2018, 15). 아울러, 전자전은 이미 1940년대부터 태동된 개념이었지만, 전략경쟁 속에서 미국의 군사적 우위를 유지하는 데 있어 그 중요성이 더욱 강조되고 있다. 2021년에는 미 해군의 EA-18G 그라울러 전자전기에 차세대 전자전 체계(NGJ)가 도입되어 전투기들의 중국, 러시아의 현대화된 방공망을 침투해야 하는 임무를 지원할 것으로 전망되고 있는 것이다(〈연합뉴스〉 2016. 10. 6). 한반도도 미국, 중국 등의 사이버·전자전 발전 노력과 무관하지 않다. 중국과 러시아의 군용기가 동해 상공을 비행하는 이유는 한반도 주변 전자정보 수집 목적인 것으로 논의되며, 북한의 미사일 발사를 어렵게 하려는 미국의 '발사의 왼편' 작전은 전형적인 사이버·전자전 활동인 것이다.

군사적 차원에서 사이버 우세의 중요성에 대한 인식이 자리하면서, 사이버전과 전자전을 상호보완적인 요소로 연결짓는 접근방식도 형성되어 왔다. 사이버 활동은 유 · 무선 통신망을 매개로 하며, 이 가운데 무선 통신망은 전자기 스팩트럼(Electromagnetic Spectrum) 영역에 있다. 이 점에서 사이버 우세를 위해 주요한 요소의 하나가 무선 통신망에 대한 보호와 공격이 되기 때

문에, 전자기 스팩트럼 작전은 사이버우세의 유지와 달성에 기여할 수 있는 요소라고 볼 수 있는 것이다. 더욱이 4차 산업혁명과 함께 무선통신의 잠재력과 비중이 확대되고 있기 때문에, 전자전과 사이버전을 연결짓는 전략적 사고는 더욱 뚜렷해져갈 것으로 보인다. 그에 따라, 군사적 사고 속에서도 두 영역을 연결짓는 개념들도 제시되어 왔다(U.S. Army 2014).

이 글에서는 사이버전/안보와 전자전/안보의 개념을 개관하고, 사이버와 전자기 스팩트럼 공간에서 미국과 중국이 추진 중인 전략과 조직 마련 노력을 살펴본 후, 사이버 · 전자기 영역에서 미중 전략경쟁이 어떻게 전개될지에 대해 고찰해보고자 한다. 사이버 영역과 전자전 영역에서 미중이 구축하려는 강점은 향후 전략경쟁의 양상을 전망할 수 있게 하는 단초가 될 수 있을 것이다.

II. 사이버 · 전자전/안보의 개념과 영역

사이버전/안보와 전자전/안보는 각각 의미있는 전투의 영역으로서 서로 영향을 주고 받을 수 있는 특징을 지닌다. 우선, 사이버전, 전자전의 개념을 검토하고, 사이버 · 전자전/안보의 개념을 고찰해볼 것이다. 사이버 · 전자전/안보의 영역도 역시 사이버전과 전자전의 영역을 검토한 바탕에서 생각해볼 수 있다.

1. 사이버 · 전자전/안보의 개념

우선, 사이버전(CW: Cyber Warfare)은 행위자가 사이버공간의 행위를 통해 국가안보 위협에 대응하거나 정치적 이득을 얻는 행위로 이해될 수 있다. 파울로(Shakarian, Shakarian and Ruef 2013: 2)는 사이버전을 “국가안보에 심각한 영향을 미치거나 국가안보에 대한 위협에 대응하여 국가 또는 비국가 행위자가 사이버공간에서 취한 행동에 의한 정책의 연장”으로 정의했다. 미 합참은 “사이버 수단만을 혹은 그 일부를 사용하여 수행되는 무장 분쟁”이라고 규정했다(US Joint Chiefs of Staff, 2010). 이러한 정의는 사이버전의 행위자에는 비국가행위자가 포함될 수 있으나, 사이버전은 본질적으로 국가안보 상의 목적과 사이버공간의 행동으로 구성된다는 의미일 것이다. 또한 사이버전은 국가의 사이버체계를 행동의 대상으로 한다. 국내 학계에서도 사이버전은 “한 나라가 의도적으로 다른 나라의 컴퓨터 시스템 또는 디지털 기간시설에 대하여 사이버 공격을 가함으로써 정치적 이득을 얻거나 보복을 가하는 행위”로 규정되고 있으며(민병원 2015, 3), 한국 국방부에서도 사이버전을 “사이버공간에서 일어나는 새로운 전쟁수단으로서 컴퓨터 시스템 및 데이터 통신망 등을 교란, 마비 및 무력화함으로써 적의 사이버 체계를 파괴하고 아군의 사이버체계를 보호하는 것”으로 정의하고 있다(엄정호, 김남욱, 정태명 2020, 29).

보다 구체적으로, 사이버작전은 공세적 사이버작전(OCO: Offensive Cyber Operations), 방어적 사이버작전(DCO: Defensive Cyber Operations) 그리고 네트워크 작전 혹은 국방부정보망작전(DODIN: Department of Defense Information Operations)으로 구분된다(U.S. Army 2014, 3-1). 공세적 사이버작전이란 다른 나라의 사이버공간을 통해 사이버전력을 투사하는 것이며, 방어적 사이버작전은 국방부정보망을 보호하기 위한 임무로 규정된다. 아울러, 네트워크 작전 혹은 국방부정보망작전은 국방부 정보망을 보장, 설정, 운용, 확장, 관리, 지속시키고 국방부정보망의 기밀성, 가용성, 통합성을 창출하고 보존하기 위한 작전을 의미한다(Joint Chiefs of Staff 2018, xi).

한편, 전자전(EW: Electronic Warfare)은 전자기파 위협에 대응하거나 그를 통해 군사활동에서 이익을 얻는 것을 의미한다. 일반적으로 전자전은 '전자 스펙트럼에 대한 적 이용의 파악, 역이용, 방해를 하기 위한 전자 에너지의 사용과 우군의 전자 스펙트럼 이용을 확보하기 위한 수단을 포함하는 군사행동'으로(장수덕 2000, 1)으로 정의된다. 참고로, 정보통신기술의 발달과 더불어 사이버전의 개념이 본격적으로 형성되었다면, 전자전의 개념은 레이더와 무선통신이 군사활동에 광범위하게 이용되기 시작하면서 태동되었다. 한국전쟁 시기 조기경보레이더 등이 도입되자 미군은 상대방의 전파 이용을 방해하기 위해 전자대항장치(Electronic Counter-measures)를 도입했던 것으로 알려져 있다. 본격적인 전자전 운용 사례로는 1990년대 걸프전 당시 미군이 이라크의 대공무기체계와 통신시설에 전자공격을 가한 후 이들 시설을 공군전력으로 무력화한 경우가 꼽힌다. 다만, 전자전이 전쟁수해에 본격적으로 도입된 것은 사이버전의 기원과 맞물리는데, 최초로 사이버전이 수행되었던 것으로 알려진 걸프전 당시(김상배 2018, 118-119) 미국은 체계적인 형태의 전자전을 수행했었다. 이라크의 지대공 미사일 기지, 방공체계 등에 전자공격을 실시하고 이러한 시설을 파괴하는 데 전자전기를 투입했었던 것이다.

전자전 역시 목적에 따라 전자전 지원(ES: Electronic Support), 전자공격(EA: Electronic Attack), 전자보호(EP: Electronic Protection)로 구분될 수 있다. 이 가운데, 전자전 지원은 상대방의 전자공격 위협을 탐지 및 식별하거나 상대측의 군사력 구조와 위치를 탐지하는 것을 목표로 하며, 전자공격은 상대방의 전자 무기체계를 교란하거나 파괴하는 것을 추구하는 작전영역을 의미하고, 전자보호는 상대방의 전자공격에 대한 대응책을 통해 아측의 전자무기체계를 보호하는 것을 뜻한다(Adamy 2010, 11).

사이버 · 전자전/안보는 사이버 공간의 대상에 영향을 미치기 위한 수단으로 전자전 무기를 주목하는 개념이다. 첨단무기의 등장과 네트워크중심전의 등장 하에 사이버공간에서의 우세는 전쟁의 승패를 결정할 수 있는 요인이 되었고, 이러한 배경에서 전자기 스펙트럼(EMS: Electro Magnetic Spectrum)에 대한 이용을 제어하는 전자전은 사이버공간의 물리적 층위를 통제하는 싸움으로서의 성격도 뚜렷하게 가지게 되었던 것이다. 미 육군 교범도 전자전(EW)가 전자기 스펙트럼을 사용하는 사이버공간 기능에 영향을 준다는 점으로부터 사이버전과 전자전을 단일하고

통합되며 동기화된 방법론을 통해 다루는 '사이버공간&전자전(Cyberspace and Electronic Warfare)' 개념의 필요성을 제기하고 있다(U.S. Army 2014). 다만, 이러한 사이버 · 전자전/안보의 개념은 상대방의 사이버체계에 대한 하드웨어 측면의 전자기 공격만 고려하는 것이 아니라, 아군의 사이버체계에 대한 전자기파 공격을 방어하는 측면을 동시에 고려하고 있다. 즉, 사이버전과 전자전을 통합적으로 다루어야 한다는 접근에서 사이버 · 전자전/안보의 개념이 제시되고 있는 것이라고 볼 수 있다.

2. 사이버 · 전자전/안보의 영역

사이버 영역은 "인터넷, 정보통신 네트워크, 컴퓨터 시스템과 내장형 프로세서 및 제어장치를 포함하는 정보기술 인프라와 내부의 데이터로 구성된 정보환경 내의 지구적 영역"를 의미하는 것으로 규정될 수 있다(U.S. Army 2017, 1-2). 이러한 사이버공간에 대한 이용 능력은 시스템 내의 논리층만이 아니라 – 그러한 기능을 가능하게 하는 하드웨어적인 조건인 – 물리층에 대한 파괴로도 제한될 수 있기 때문에, 사이버전의 영역에는 물리층에 대한 파괴도 포함될 수 있다(김상배 2018, 121).

동시에, 포괄적인 의미에서 사이버전력은 일반적으로 사이버무기로 이해되는 소프트웨어 방식의 무기와 더불어 하드웨어 방식의 무기로 구성된다. 소프트웨어 방식의 사이버무기는 감염 방식에 따라서는 웜(Worm), 바이러스(Virus) 그리고 트로이 목마(Trojan) 등으로 구분되고, 행위 방식에 따라서는 스파이웨어(Spyware), 애드웨어(Adware), 랜섬웨어(Ransomware), 루트킷(Rootkit), 크립토재킹(Cryptojacking), 파일리스 악성코드(Fileless Malware) 등으로 분류될 수 있다. 그리고 전자전 무기의 범주와도 일부 겹칠 수 있는 하드웨어 방식의 무기 범주에는 전자기파 폭탄(EMP bomb), 전자총[HERF(High Energy Radio Frequency) Gun], 전파교란(Jamming), 칩핑(Chipping), 나노머신(Nano Machine), 템피스트(TEMPEST) 등이 있다(엄정호, 김남욱, 정태명 2020, 44-51). 사이버체계에 대한 물리적 파괴 역시 사이버공격의 하나로 이해되고 있으며, 사이버체계를 물리적으로 파괴하는 하드웨어 방식의 무기가 사용되는 경우는 사이버 위협이 국가 간의 분쟁으로까지 고조된 상황임을 함축한다(김상배 2018, 122).

특히, 앞서 각국은 소프트웨어 영역에서 다양한 사이버무기를 개발하는 데 주력해왔다. 대표적인 소프트웨어 무기로는 2010년 이란의 나탄자 핵시설 해킹에 사용된 스턱스넷(Stuxnet)이 있는데, 스턱스넷은 웜이기도 하면서 루트킷으로 분류될 수 있는 프로그램이다. 이 스턱스넷 웜은 발전소와 같은 국가기반시설 운영에 많이 사용되는 지멘스 산업제어시스템을 공격하는 것으로 알려져 있다. 이외에도 Flame, Duku 등도 잘 알려진 사이버 공격 소프트웨어 무기체계이다(장노순 2012, 8; 조성렬 2016, 403). 방어용 소프트웨어 체계로는 사이버 아이언돔, 추적 파괴 멀웨어, Great Firewall, 독자개발 운영체계 및 라우터 등이 있다.

한편, 전자전의 영역은 현대전에 있어 전장의 차원이 사이버공간과 우주공간으로 확대되면서 함께 확장되고 있다. 기존의 전자전은 지상, 해상, 공중 무대의 재래식 전투를 지원하기 위한 전자기 관련 활동을 의미했다면, 현재는 사이버, 우주전장까지 포괄하여 전자기 스펙트럼을 관리하는 활동으로 그 임무영역이 확대되고 있다. 이때, 전자기 스펙트럼은 가능한 주파수의 모든 범위를 포괄하는 개념이다(Joint Chiefs of Staff 2012b, I-1). 오늘날의 전쟁수행체계에서는, 사이버영역을 포함하여 무선으로 데이터를 주고받는 지상, 해상, 공중의 재래식 무기와 우주 센서/무기체계까지 전자기 스펙트럼에 의존하고 있다고 할 수 있다.

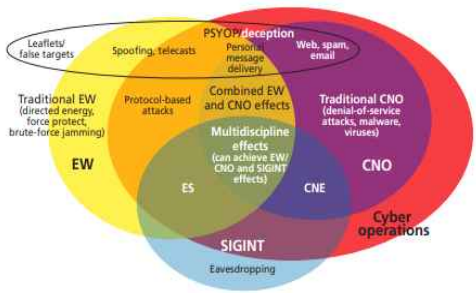
일반적으로, 전자전 무기는 전자공격과 전자보호, 전자지원 등 작전의 목적에 따라 개발, 운용된다. 대표적인 전자공격 기술로는 대방사유도탄[1], 전자기펄스 폭탄, 전자기 재밍[2], 전자기만을 꼽을 수 있으며, 전자방어 기술로는 주파수 변조, 방사통제, 저피탐 기술을 들 수 있다. 전자전 무기체계의 발전 추세에서 특징적인 것은 전자공격 매체가 지향성에너지와 EMP 무기로 확장되고 있다는 점과 더불어(〈사이언즈 타임즈〉, 2010. 12. 3), 첨단무기체계에 대응하는 과정에서 미코닝(Meaconing), 스푸핑(Spoofing) 등으로 GPS 전파교란 기법이 더욱 발전하고 있는 것이다(황선한 2018, 19).

사이버전과 전자전 사이에는 서로 겹쳐지는 사이버 · 전자전의 영역이 존재한다. 전술한 바처럼, 사이버전 영역에서도 전자전 무기체계가 하나의 수단으로 고려되고 있다. 이러한 경향은 앞으로 더욱 확대될 것으로 전망된다. 사이버 영역에서 무선통신의 비중이 증가하면서 전자기 스펙트럼을 효율적으로 사용할 필요가 있다는 점이 고려되고 있는 것이다(FM 3-38 2014, 1-6). 사이버전 영역에서도 전자기 스펙트럼 기술이 사용된 결과, 사이버전 영역이 전자전 영역을 대체적으로 포괄하는 성격을 갖게 될 것이라고 예측할 수 있다. 일부에서는 기능적 측면에서 사이버전 영역이 전자전 영역의 약 60%를, 기술적 측면에서 사이버전 영역이 전자전 영역의 거의 모든 부분을 포함한다고 평가한다(〈그림-1〉, 〈그림-2〉 참조). 기능적 측면에서 지향성 에너지(directed energy)와 무차별 전자재밍 기능 등 전통 전자전 영역을 제외하고는 전자전과 사이버전 영역이 겹쳐져 있고, 기술적 측면에서는 지향성 에너지를 제외하고는 전자전의 나머지 모든 영역이 사이버전의 영역과 중첩된다는 뜻이다.

---

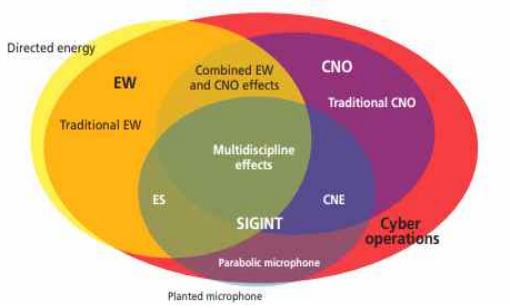
1) 대방사 미사일(Anti-radiation Missile)이란, "적 레이더에서 방사되는 전파신호를 탐지하고, 해당 레이더를 추적하여 파괴하기 위한" 미사일을 의미. 이를 사용하여 적의 레이더 사용을 무력화함으로써 감시 및 방공체계를 와해시킬 수 있음(김문조, 유석봉 2019, 106).

2) 전자기 재밍(Electronic Jamming)이란, "수신자의 전자파 수신을 저하 또는 방해하기 위하여 고의적으로 전자파를 방사 또는 재방사하여 적 장비에 원하지 않는 전자신호의 수신을 강요하는 활동"을 의미함(김문조, 유석봉 2019, 106).



〈그림 1〉 사이버전-전자전-신호정보 간 기능적 측면의 중첩 영역

출처: Porche III et al(2013), p. 51.



〈그림 2〉 사이버전-전자전-신호정보 간 기술적 측면의 중첩 영역

출처: Porche III et al(2013), p. 53.

물론, 사이전과 전자전의 영역 간에는 차이점도 존재하지만, 사이버전과 전자전은 서로를 지원해줄 수 있는 관계에 있다. 사이버전은 전시만이 아니라 평시에도 발생할 수 있는 것으로 컴퓨터와 서버를 표적으로 하지만, 전자전은 군사적 활동과 관련하여 수행되면서 레이더나 그와 관련된 통신시설 및 데이터 링크에 대해 수행된다. 그와 동시에, 사이버작전의 대상인 유무선 통신체계는 전자전 수단에 취약하기 때문에, 공세적 · 방어적 사이버 작전에 전자전 수단이 동원될 수도 있다(Hoehn 2019, 3-4).

또한 4차 산업혁명에 따른 변화는 사이버전과 전자전이 하나의 작전으로 수렴되는 변화를 촉진해갈 것이다. 기술의 발달로 네트워크 자산이 전자전 자산이 되어 가고, 전자전 장비가 동시에 네트워크 자산일 수 있게 되기 때문이다. 무선 네트워크에 무인무기체계들이 연결되어 있기 때문에, 전자기파로 악성코드나 거짓 표적 정보를 전송하여 이들 무기체계의 오작동을 일으키는 방안도 탐색되어 왔다. 실제로도 현대적인 무기체계에 대한 대응에 사이버 · 전자전이 활용되고 있다. 2011년 12월에는 이란이 사이버 · 전자전 장치로 미국측 RQ-170 무인기를 해킹하여 착륙시킨 사건도 발생했다. 2017년 북한에 대한 미국의 '발사 직전 교란(Left of Launch)'도 사이버 · 전자전 수행의 예이다(Sanger 2019, 405-440). 이러한 흐름은 미 육군의 'CEMA(Cyber Electronic Activities)' 개념, 호주 국방부의 '사이버-전자전 연속체(Cyber-EW Continuum)' 개념을 통해서도 드러나고 있다(Cyber and Electronic Warfare Division 2014, 26).

Ⅲ. 미국의 사이버 · 전자전/안보 전략과 조직체계

1. 사이버 · 전자전/안보 전략

탈냉전 이래 미국은 사이버전략을 사이버 방어의 필요성에 주목하여 발전시켜왔다. 1991년 걸프전 직후부터 사이버공간 방호의 전략적 필요성에 주목하여 관련 연구를 개시했고, 9.11 테러 이후에도 국가기반시설 보호의 중요성을 인식했다(신규용 외 2016, 136). 부시행정부 시기부터 국토안보부의 사이버안보 관련 책임을 강조하는 "사이버안보국가전략(The National Strategy to secure Cyberspace)"를 발간했던 것이다(이강규 2011, 4). 뿐만아니라 부시 행정부 말기에는 국가안보 차원의 사이버안보 문제에 대한 대응책을 제시한 "국가 사이버안보 종합계획(Comprehensive National Cybersecurity Initiative)"을 발표하고(김상배 2018, 145-153), 2008년 악성코드에 의한 시스템 교란 사고를 겪었으면서 미국은 오바마행정부 시기에 걸쳐서도 사이버 사령부 설치 등 사이버위협 대응을 강화해갔다(김상배 편 2017, 140). 특히, 오바마 행정부 시기 미국은 사이버안보 전략 수립에 적극적인 태도를 보였고, 2009년 "사이버 정책 검토보고서(Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communication Infrastructure)", 2011년 5월 "사이버 공간에 대한 국제전략(International Strategy For Cyberspace)", 2011년 7월 "사이버 공간에서의 국방부 작전 전략(Department of Defense Strategy for Operating in Cyberspace)"를 각각 공개했다(이강규 2011, 4). 이후 미국은 사이버안보 전략을 공세화해갔고, 이러한 변화는 2015년 "국방부 사이버 전략(the DOD Cyber Strategy)"에 반영되었다.

앞서 트럼프 행정부에서도 안보환경이 급속한 기술적 변화와 전쟁의 변화하는 성격에 영향받고 있다는 점에 주목하면서 사이버공간의 위협에 대응해야 할 필요성을 강조했었다. 2017년 12월에 발표된 "국가안보전략(National Security Strategy)"는 사이버공간이 국가 및 비국가적 행위자들이 미국의 정치, 경제, 안보 이익에 반하는 캠페인을 벌일 수 있는 상황이 조성되었다고 경고하면서, 사이버, 물리, 전자 공격에 대한 미국의 핵심 인프라의 취약성은 적대국이 미국 군사지휘통제, 금융과 재정 활동 및 전력 · 통신망에 장애를 야기할 수 있음을 의미한다고 설명했다(The White House 2017, 12). 이에 따라 미국 정부는 데이터를 보호하는 데 있어 개선된 태세를 갖추어야 한다면서, 핵심부문에[3] 대한 위협 평가, 방어 가능한 정부 네트워크의 구축, 적대적 사이버 행위자에 대한 억제 및 차단, 정보 공유와 감지능력의 개선, 중층적 방어의 배치 등을 추구할 것임을 밝혔다(The White House 2017, 13). 특히, 미국의 2018년 "국가국방전략(National Defense Strategy)"은 공중, 육상, 해상, 우주 및 사이버공간과 같은 모든 영역에서 경쟁구도가 보여지고 있음을 언급하는 동시에(The Department of Defense 2018, 3), 급속한 기술적 진전과

3) 국가안보, 에너지, 전력, 은행, 재정, 보건·안전, 통신, 수송 분야 등

(그에 따른) 전쟁양상의 변화에도 안보환경이 영향받고 있다고 지적했다. 더욱 많은 나라들이 고등 컴퓨팅, 빅데이터 분석, 인공지능, 자율, 로봇, 지향성 에너지, 극초음, 생물공학(biotechonology)과 같은 새로운 기술의 개발을 추구하고 있는 것이 미국 안보환경에도 변화를 가져오고 있다는 의미이다. 그리고 이러한 새로운 환경에 대처하기 위한 전력 현대화 방향의 하나로 사이버 방어 및 복구, 군사작전 전반과 사이버 역량의 통합에 대한 투자를 언급했다(The Department of Defense 2018, 6).

사이버전과 전자전을 통합적으로 바라보는 군사적 사고는 2012년 이후에 구체화되어 왔다. 2011년 국방부 차원의 사이버작전 전략이 제시된 다음에 사이버·전자전의 개념도 다듬어져 온 것이다. 2012년 미 합동전자전 규범(JP 3.13-1)은 컴퓨터네트워크작전과 전자전 간의 상호보완적인 성격과 잠재적인 시너지 효과를 고려할 때 두 영역의 작전이 조율되어 진행되어야 함을 강조했다. 전자전 활동은 의도치 않게 사이버공간의 인프라와 국방부 정보 네트워크에 미칠 수 있는 영향까지 기본적으로 고려해야 한다고 지적하면서, 합동군 사령부의 전자전 담당자(JCEW: Joint Force Commander's EW Staff)나 전자전 조직(EWC: electronic warfare cell)으로부터 전투지휘부, 사이버사령부에까지 순차적으로 조율과 지도가 이루어져야 한다는 점을 제시했다. 또한, 전자전 차원에서 국방 네트워크의 보호도 제공해야 한다는 점도 요구했다. 뿐만아니라 2012년 합동 전자전 스펙트럼 관리 작전(JP 6-01)에서도 전자기 작전 환경에는 지상, 공중, 해상, 우주의 물리적 요소만이 아니라 사이버공간과 같은 정보환경도 포함된다는 점을 명시했다. 나아가, 미 육군은 2014년에 사이버 · 전자전 관련 야전 교범을 미군 최초로 발간했다(FM-3-38). 사이버작전과 전자전, 스펙트럼 관리 작전을 통합한 "사이버전자기 활동(CEMA: Cyber Electronic Activities)"이라는 새로운 개념을 제시하고, 이를 "사이버공간과 전자기 스펙트럼 모두에서 적에 대한 우위를 장악, 유지, 활용하고, 적이 그렇게 하는 것을 거부하고 약화시키며, 아군의 지휘체계를 보호"하는 것으로 규정했다.

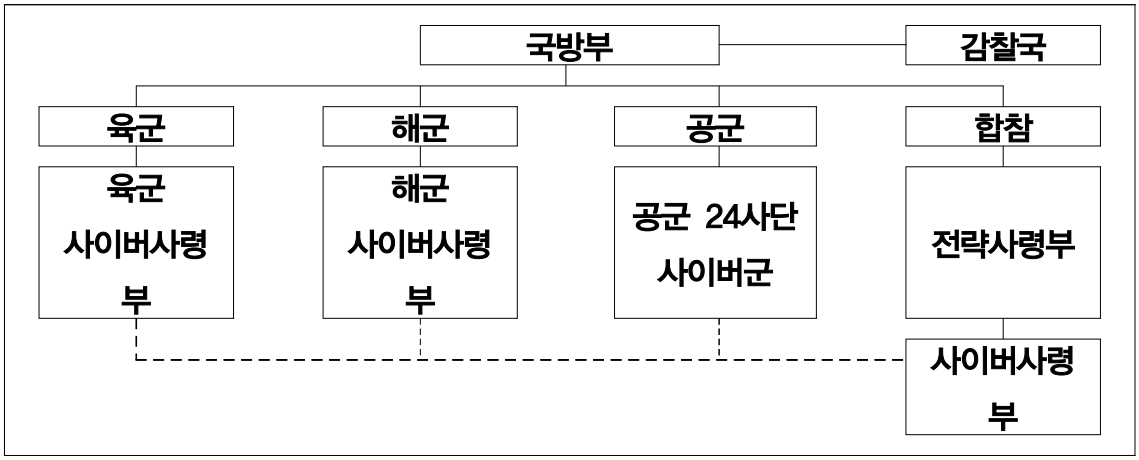
한편, 미국은 다양한 사이버 무기를 보유, 운용하고 있으나, 주로 알려진 것은 사이버공격 등에 사용되는 수단들이다. 스턱스넷(Stuxnet)은 가장 널리 알려진 사이버무기로서 독일 지멘스사의 제어시스템을 감염시킴으로써 국가기반시설의 운영을 마비시키거나 오작동을 유발한다. 이란의 나탄즈 핵시설에 대한 사이버공격에 사용되었었다. 또한 플레임(Flame) 역시 미국과 이스라엘과 함께 개발한 것으로 알려진 정교한 스파이웨어로서, 윈도우 업데이트 방식으로 정보를 빼내는 역할을 수행한다. 그리고 스노든의 폭로로 그 실체가 논란이 되었던 에셜론(Echelon)은 국가안보국(NSA)이 중심적으로 운용하는 것으로 알려져 있는데, 통신내용을 광범위하게 감청할 수 있는 사이버 감시정찰체계이다. 나아가 미국은 2012년 5월 발표한 플랜-X 코드명의 프로젝트를 통해서 재래식 전투를 지원하기 위한 사이버무기 개발을 진행했다. 이를 통해, 전투기의 작전을 지원하기 위해 상대방의 통신망과 레이더를 방해하는 등의 사이버 무기체계를 개발하고, 사이버전에 대비하기 위해 사이버 지도를 제작하고자 하고 있는 것이다(〈연합뉴스〉, 2012. 5. 31).

동시에, 미국은 전자전 지원과 전자공격 차원에서 전자전기 등을 운용하고 있다. 전자전 공격체계 가운데 가장 대표적인 것으로는 보잉사의 EA-18G Growler가 있다. EA-18G Growler는 항공모함 탑재기로도 활용될 수 있으며, 상대방의 레이더를 탐지하고 전파방해(jamming)하는 것을 주된 임무로 한다. EA-18G는 AN/ALQ-99 전자전 교란장치(jammer)와 ALQ-218 윙팁 레이더를 장착하고 있는데, 이는 향후 개발될 차세대 재머(NGJ)로 대체될 전망이다. 또한 전자공격에 관여하는 무기체계로 원격지원 전자교란기인 EC-130H Compass Call도 꼽힐 수 있다. 상대방의 지휘통제 통신을 방해함으로써 지상, 해상, 공중의 작전을 지원한다. 미국은 이를 대체하기 위한 EC-37B Call Re-Host Aircraft도 개발 중인 것으로 알려졌다. 이 외에도 잘 알려진 F-35 합동타격기 역시 전자전 역량(AN/ASQ-239)을 내장하고 있으며(Hoehn 2019, 4-17), 무장감시 무인기인 MQ-1C 그레이이글과 MQ-9 리퍼에도 각각 2013년과 2017년에 전자전 능력이 추가되었다. 또한 대(對) 레이더 미사일인 AGM-88 제압유도탄 등도 전자공격 무기에 해당한다. 덧붙여, 전자전 지원 무기체계로는 대표적으로 RC-135 V/W Rivet Joint 전자정찰기 등이 있다.

2. 사이버 · 전자전/안보 조직체계

미국은 앞서 오바마 행정부에서는 백악관에 사이버안보 관련 보좌관직을 신설한 데 이어, 2010년 5월 전략사령부 예하에 사이버 사령부도 창설했다. 사이버사령부 사령관으로는 4성 장군이 임명되었고, 사이버사령부의 규모도 IT 및 전자전 전문인력 5천명을 포함해 총 4만명에 이르렀다(김상배 편 2017, 151). 사이버사령부는 사이버공간에 대한 일상적 방어체계 구축 · 지원 · 관리를 맡고, 육군 사이버사령부, 제24공군, 함대 사이버사령부, 해병대 사이버사령부로 구성되어 미군 전체에 걸친 사이버전 자원을 단일 지휘계통으로 관리하며, 대내외 협조체계를 구성하고 있다(김상배 편 2017, 151-152). 나아가 사이버사령부는 2017년 8월 통합전투사령부로 격상됨으로써 독자적인 지휘체계도 갖추게 되었다(김상배 2018, 154). 2018년 5월 미국 사이버사령부는 통합전투사령부로 격상됨으로써 전략사령부에서 독립했다는 것이다(차정미 2019. 51).

〈그림-3〉 미군 사이버사령부 조직 체계



출처: 한국인터넷진흥원(2014) 참조.

사이버전 전력과 전구의 전자전 무기가 서로를 지원하며 운용되는, 사이버 · 전자전 수행을 위한 미국의 부대구조는 사이버사령부보다는 각 군 차원에서 발전되고 있는 것으로 보인다. 앞서 사이버 · 전자기 활동(CEMA) 개념을 제시한 미 육군은 사이버작전과 전자전을 통합하기 위하여 5개 조치를 고안했다고 알려졌다. 첫째, 여단에서 구성군까지 CEMA 조직을 신설하여 사이버전과 전자전 작전을 계획, 동기화, 통합하게 하고 전자기 스펙트럼도 관리하게 한다는 것이다. 둘째, 군사정보중대 내에 전자전소대를 새로이 설치하여 육군의 감시능력을 강화한다는 구상이다. 셋째, 전자전중대를 원정 군사정보여단 내에 창설함으로써 정찰대항 임무(counter reconnaissance mission)을 수행하게 할 것이다. 넷째, 신설 다영역(ICEWS: intelligence, cyber, electronic warfare, space) 파견대를 포트 루이스의 다영역 임무부대에 설치함으로써 다영역 작전의 추진방향을 파악하고, 마지막으로 육군 사이버사령부 내에 새로운 사이버전 지원대대를 창설할 계획이다.[4] 실제로 이 구상들 가운데 넷째로 언급된 신설 다영역 부대 설치 방침에 따라, 2019년 초 I2CEWS(Intelligence, Information, Cyber, Electronic Warfare and Space) 대대(제915 사이버전 지원대대)가 루이스-맥코드 합동기지(Joint Base Lewis-McChord)에 창설됨으로써[5] 사이버 · 전자전 수행을 위한 육군의 조직 구상이 현재 이행 중이라는 점을 보여주었다.

4) 출처: https://www.c4isrnet.com/show-reporter/technet-augusta/2018/09/04/here-are-5-army-modernization-efforts-to-keep-pace-in-cyber-and-electronic-warfare/ (검색일: 2020년 5월 28일).

5) 출처: https://www.armytimes.com/news/your-army/2019/03/27/this-new-army-unit-could-help-the-us-win-the-next-cold-war/ (검색일: 2020년 5월 28일).

Ⅳ. 중국의 사이버 · 전자전/안보 전략과 조직체계

1. 사이버 · 전자전/안보 전략과 능력

중국의 군사교리는 개혁개방 이후 인민전쟁에서 국지제한전쟁으로, 걸프전 이래 군사기술의 발달을 감안한 변화를 보여왔다. 1980년대 초 중국의 전통적인 인민전쟁 교리는 "현대적 조건 하 인민전쟁"으로 변화했으며, 1985년에서 1991년 사이에는 국지제한전쟁 교리로, 1990년대 중반에는 고기술제한전쟁(고기술 조건 하의 유한 국부전쟁전략)으로 변천해갔던 것이다(Gurtov and Hwang 1998, 제4장). 특히 1990년대 중반 중국의 교리 변화는 걸프전의 영향에 따라 현대전의 주요 환경은 하이테크 기술의 도입이라는 점이 강조되었는데, 걸프전을 목도한 장쩌민 걸프전에서 보여진 미측의 전자기술 및 정밀폭격에 유의하고, 첨단기술 조건 하 국부전쟁을 준비할 것을 지시했다(성인모 2014, 42). 이후 미국의 반테러전을 전후하여 중국은 정보 및 첨단기술의 영향에 유의하면서 미래전의 주요양상은 정보전이 될 것이라고 판단했고, 중국 지도자들이 정보전 수행을 위한 군사혁신을 요구함에 따라 '정보화 조건 하 국부전쟁전략'이 발전되었다(성인모 2014, 43). 2004년 국방백서에 명시되었던 이 전략은 첨단무기로 해군과 공군을 강화하고 적극적 방어를 수행한다는 것이었는데, 정보화전쟁의 핵심요소로는 적대국의 정보체계를 파괴하고 아측 정보체계를 보호하는 것이 꼽혔다(이창형 출간예정, 70). 이에 따라 인민해방군은 2010년 국방백서를 통해 2020년까지의 목표로 기계화의 기본적 실현 및 정보화의 중대한 발전을 제시했었다(Information of Office of the State Council 2010).

이후에도 중국은 정보화(informationization)의 개념 속에서 사이버 전장의 중요성을 강조해갔다. 2015년의 중국 국방백서는 군사혁신이 새로운 단계로 접어들고 있다고 지적하면서, 무기체계의 장거리화, 정밀화, 지능화, 스텔스화 등이 추진되는 동시에 우주와 사이버전장이 전략경쟁의 핵심적 고지가 되고 있다고 설명했다. 이로부터 강조된 것은 전쟁의 형태가 "정보화로의 진화를 가속"하고 있다는 점이었다(The Information Office of the State Council 2015). 2019년 중국 국방백서 역시 인민해방군이 중국 특색의 군사혁신을 추진해왔지만, 기계화를 아직 달성하지 못한 상태에서 정보화를 개선해야 할 긴급한 임무를 지니고 있다고 언급했다(The State Council Office of the People's Republic of China 2019). 이러한 인식은 중국이 정보화전에 필요한 군사혁신을 장기적으로 추진하는 토대가 되고 있다. 시진핑 시기에는 중국이 대비하는 전쟁이 '정보화 국지전'에서 '정보화전쟁'으로 이동했기 때문에, 전쟁을 특정 지역에 국한하기 어려운 정보화된 전쟁을 수행하기 위한 다양한 작전 방법도 고민되었다. 그 연장선에서 2019년 중국 국방백서는 정보화전쟁에 대한 논의를 심화시켜 '지능화 전쟁' 개념을 제시했다(이창형 출간예정, 73-75).

중국은 2000년대 이래 망전일체전(INEW: Integrated Network Electronic Warfare; 网电

一体)의 개념과 같은, 네트워크[6] 전력과 전자전 전력을 통합적으로 운용하는 방안을 발전시켜 온 것으로 보여진다(Costello and McReynolds 2018, 7). 물론 1980년대 중반에도 '점혈전략'의 일환으로 사이버전에 주목했었으나, 중국은 망전일체전의 개념으로 사이버전과 전자전을 공격과 방어 양 측면에서 결합시켜갔던 것이다(조성렬 2016, 406-407). 중국의 망전일체전은 상대방의 데이터 수신과 처리 능력을 파괴, 방해하는 것을 주요한 목표로 하며(Sharma 2010, 36), 분쟁 초기 단계에 상대방의 정보체계에 대해 사이버전 수단과 전자전 무기를 결합하여 사용하는 것을 특징으로 한다고 알려져 있다. 중국은 기본적으로 정보화 조건 하 유한 국부전쟁 교리에 따라서 지상, 해상, 공중, 전자기 영역에서 동시에 조율된 작전을 수행하는 것을 목표로 하고, 그를 위해 전자기 등 새로운 영역에서 작전 수행 능력을 갖추는 데 초점을 두어왔다(Sharma 2010, 38). 중국의 망전일체전 개념은 사이버작전, 전자전, 우주 통제 및 물리적 타격을 통해 상대방의 C4ISR(Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) 체계에 사각지대를 창출해내어 승리의 기회를 만들어내겠다는 것으로 이해되며, 특히 분쟁 초기에 이러한 망전일체전을 수행함으로써 네트워크 능력에 기반하는 상대방의 군사력을 마비시키고 군사활동의 목적을 달성하는 데 초점을 두는 것으로 추정된다.

중국의 망전일체전은 사이버 전력과 전자전 전력만이 아니라 대우주 전력과 장거리 타격 능력을 동시에 운용해야 한다는 점을 강조한다. 망전일체전에 대한 사고는 소위 중국의 '네트워크 스워밍 전쟁(network swarming warfare)' 논의에도 반영되어 있다. '네트워크 수워밍 전쟁'의 구체적인 내용은 알려져 있지만 중국은 이를 통해 소규모 및 다기능 작전 부대, 전자전, 대우주전, 사이버부대, 장거리 정밀타격 수단을 동시 운용하여야 한다는 사고를 드러내고 있다. 또한 중국은 정보 우세를 달성하기 위해서 우주기반 정보자산을 1차 장악대상으로 상정하고, 우주 기반 정보자산의 영역을 통제해야 한다고 간주한다. 우주 우세가 합동작전의 수행과 전장에서 주도권 유지에 필수적이라고 강조하는 것이다. 이를 위해 우주 공간의 위성만이 아니라 지상의 발사대, 원격측정(telemetry) 기지 등 관련 시설도 공격 및 방어 대상으로 상정하고 있다(Raska 2017 참조).

아울러, 중국의 사이버능력은 2000년대 중반 이래 국제적 관심의 대상이 되어 왔다. 중국발 사이버 정찰활동 혹은 사이버 첩보활동은 제로데이 취약성(zero-day vulnerabilities)에[7] 대한 공격에 초점을 두어왔는데, 미국 국방부는 2013년 이러한 중국발 사이버 해킹에 중국 정부가 관여하고 있다고 판단하고 그러한 입장을 발표한 바 있다.[8] 특히, 체제수호의 차원에서, 중국 정부는 정보안보(information security)의 중요성을 강조하고, 국내 사이버공간에 해외의 정보가 자유롭게 유포되어 국내 체제가 위협받게 되는 가능성을 막기 위해 인터넷 검열 프로그램(Great

6) 중국에서는 '사이버'라는 표현 대신 '네트워크(網絡)'로 표현함(김태호 2018 참조).
7) 보안 취약점이 발견되었으나, 아직 해당 취약점에 대한 패치가 나오지 않은 시점에서의 취약점을 의미함.
8) 『서울신문』, 2013년 5월 7일자, "중국정부가 사이버 해킹 관여…정보수집 목적."

Firewall of China)을 운영 중이다(김상배 외, 199-200). 한편, 공격의 차원에서, 중국의 사이버 공격 프로그램에 해당하는 '만리대포(Great Canon)'는 해당 IP 주소의 트래픽을 가로채 내용을 변경시키는 중간자 공격을 취하는 프로그램으로 알려져 있다. 2015년 공개 개발자 SW 커뮤니티인 깃허브(GitHub)에 대한 대규모 디도스 공격도 만리대포에 의해 이루어진 것으로 알려져 있다.[9] 최근에는 홍콩의 시위대가 자주 방문하는 온라인 포럼인 'LIHKG'를 공격하기 위해 재가동된 것으로 관측되고 있다(Winder 2019 참조).

또한, 중국은 2009년 경에 미국의 우주 기반 C4ISR과 항법 체계를 거부하거나 방해할 수 있는 전자전 체계도 배치한 것으로 알려져 있다(Costello and McReynolds 2018, 8). 중국이 이미 배치하고 있는 전자전기나 전자전 장치도 있으나, 주목되는 것은 전자전 능력을 기술적으로 계속 신장시키고 있다는 점이다. 중국의 전자전기인 J-16D는 미국의 대표적인 전자전기 기종인 EA-18G Growler에 비교되기도 하며, 구체적인 정보는 공개되어 있지 않으나 전파교란이나 대레이더 공격을 수행할 수 있다고 전해진다. 또한, 중국은 Y-9 수송기의 기체를 개조한 신형 전자전기인 GX-11도 개발하고 있다.[10] 이는 조기경보와 정찰, 대잠작전에 투입될 수 있고, 기존의 구형 전자전기인 GX-4를 대체할 것으로 추정된다.[11] 이외에도 중국이 2015년 9월 열병식에서 공개한 바 있는 CH-5 역시 전자전 장비를 탑재해 전자정보 수집 및 전파방해 기능을 수행할 수 있는 것으로 평가된다(〈아주경제〉 2017. 7. 6).

2. 사이버 · 전자전/안보 조직체계

중국이 2015년 12월 31일 창설한 전략지원부대(Strategic Support Force, 中国人民解放军战略支援部队)는 분산되어 있던 사이버전, 전자전, 우주전, 심리전 전력의 조직체계가 통합하여 만들어진 조직이다. 중국은 앞서서도 사이버전 등에 관심을 보였고, 1997년 인민해방군 아래에 해커 관련 조직을 창설했으며, 전문적인 교육과 훈련을 통해 100만명 이상의 유관 인력을 양성한 것으로 알려져 있었다(나영주 2009, 64). 아울러, 중국은 총참모부 3부와 4부가 전자전과 사이버전 수행을 담당하도록 했다. 총참모부 3부를 통해서는 방어적 사이버작전과 신호정보 수집 및 분석을 수행하도록 하고, 최소 1999년부터 총참모부 4부가 공세적 사이버작전과 전자전을 수행하도록 임무를 배분했던 것이다(Sharma 2010, 39). 이후 중국은 2009년 미국 국방장관이 사이버사령부의 창설을 지시하자 그에 상응하는 조직개편을 모색했다. 그에 따라 2010년대

9) 『전자신문』, 2015년 4월 14일자, "中 사이버 공격 시스템, 구조는?"

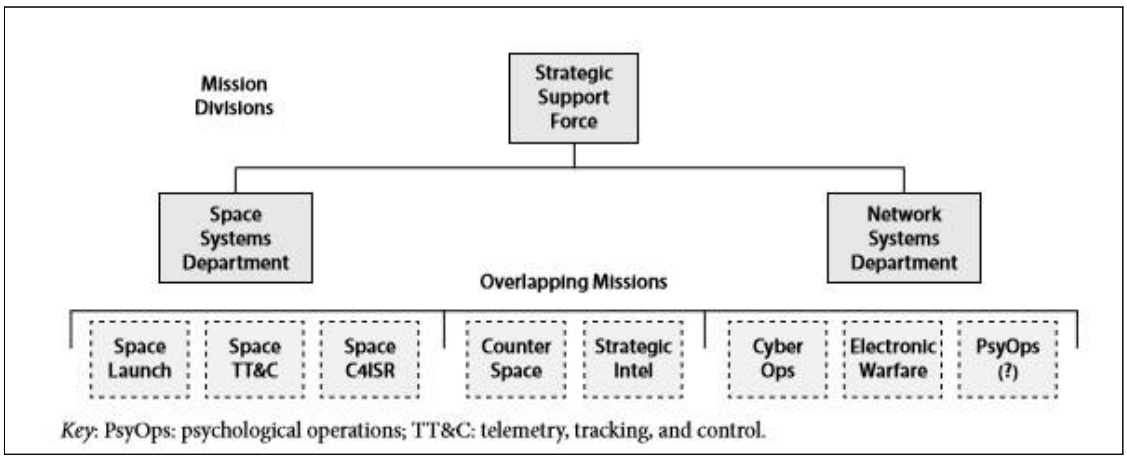
10) 출처: https://nationalinterest.org/blog/buzz/meet-j-16d-real-chinese-plane-america-should-fear-forget-stealth-91641 (검색일: 2020. 6. 3).

11) 출처: https://www.defenseworld.net/news/24435/China_Develops_New_Electronic_Warfare_Aircraft#.XtdHr2Z7ncs (검색일: 2020. 6. 3).

초반 중국측 전문가들은 중국이 정보화전쟁의 관련요소인 네트워크전, 전자전, 심리전 전력을 개념적이고 조직적인 측면에서 통합할 필요가 있다고 강조했고(Costello 2018, 8), 2015년 12월 31일에는 사이버전, 우주전, 전자전의 3대 부문으로 구성된 전략지원부대가 창설되었다. 중국은 전략지원부대의 창설로 중국은 기능과 투자의 중복을 없애고 사이버, 전자, 우주 전력의 합동작전 능력을 강화할 수 있을 것으로 기대하고 있다. 기존에는 각 단위가 각자의 전투지원 부대를 갖춰 기능과 투자의 중복이 초래되었었다는 인식 하에, 전략지원부대 창설이 기존 체제의 비효율성을 해소하고 관련 요소 간의 통합을 심화하며 합동작전 능력을 강화할 수 있을 것으로 보고 있는 것이다(최현호 2016, 42).

참고로, 중국의 전략지원부대 창설과 관련해서는, 중국이 미국의 전략사령부(USSTRATCOM)를 본따서 전략지원부대를 창설한 것이라는 주장도 있다. 미국의 전략사령부 역시 우주, 사이버, 전자, 전략적 전자전, 전략 정보 지원 임무에 대한 포괄적 책임을 지니고 있기 때문에, 전략지원부대가 미국의 전략사령부와 유사하다는 주장이다(Costello 2018, 10). 하지만, 중국 전략지원부대와 미국 전략사령부 간의 차이점도 간과할 수 없다. 전략지원부대는 전략사령부와 달리, 통합군사령부가 아니라 하나의 군종이다. 나아가, 핵무기 사용과 직접 관련된 임무를 수행하지는 않는다. 그리고 전략지원부대의 사이버영역 접근방식도 정보화전쟁에 대한 통합적인 시각을 더욱 전향적으로 반영하고 있다. 사이버전과 전자전 관련 임무를 하나의 부서가 다루도록 했기 때문이다. 이점에서, 중국 전략지원부대의 사이버전 관련 접근방식은 미국 사이버사령부의 시각보다 광범위하고 포괄적인 것으로 이해된다(Kania and Costello 2018, 108).

〈그림-4〉 전략지원부대의 임무 관련 조직체계(추정)



출처: Costello and McReynolds 2018, 11.

특히, 중국의 사이버, 전자전 임무는 전략지원부대의 네트워크계통부(Network Systems

Department, 网络系统部) 아래로 통합되었다. 전략지원부대는 참모부, 정치공작부, 후근부, 장비부를 제외하고 임무 관련 조직으로 항천계통부, 네트워크계통부를 설치하고 있는데, 이 가운데 항천계통부는 우주영역 관련 임무를 수행하며 네트워크계통부가 사이버, 전자전, 심리전 임무를 담당하는 조직이다. 이 네트워크 계통부는 기존의 총참모부 3부와 4부가 통합된 조직으로 여겨지고 있다. 총참모부 3부의 기술적 정찰과 사이버 첩보활동 임무와, 총참모부 4부의 전자전 여단이 네트워크 계통부로 통합되었다는 것이다. 아울러, 사이버 및 전자전 역량 강화에 필요한 연구기관들인 54연구소 및 56 · 57 · 58연구소도 네트워크 계통부로 이전된 것으로 알려져 있다(Kania and Costello 2018, 111).[12] 이러한 조직개편은 정찰, 공격, 방어 등 임무의 유형과 상관없이 전투수행 영역을 중심으로 한 재조직화를 도모한 결과로 이해되고 있기 때문에, 중국 전략지원부대의 네트워크계통부는 중국이 사이버와 전자기 영역을 서로 떼어내기 어려운 하나의 전투수행 영역으로 바라보고 있음을 이해할 수 있게 해준다(Kania and Costello 2018, 109).

동시에, 중국의 정보화 작전 전력은 전략지원부대에만 집중되어 있는 것이 아니라, 국가 기구 및 군대 내의 전구에까지 복합적, 다층적으로 나눠져 있다. 중국 인민해방군의 각 전구와 전구 휘하의 육 · 해 · 공군도 각자의 사이버 혹은 네트워크 · 전자 작전 역량을 가지고 있으며, 사이버 방어 임무에는 총참모부와 중국 사이버공간청도 일익을 담당한다. 또한 기존에 전자전 대항과 레이더 관련 임무를 맡았던 총참모부 4부가 전부 전략지원부대로 이전되지 않고, 4부의 본부조직이 총참모부 산하에 네트워크 · 전자국으로 남아 있다. 이에 따라, 전략지원부대의 창설 이후에도 다양한 수준의 사이버 작전 및 전자전 전력이 나누어져 있으며, 본격적인 사이버·전자전 수행을 위해서는 여러 사이버·전자전 자산의 운용을 조율하는 메커니즘이 마련될 필요가 있다. 아직 그에 필요한 기능적 메커니즘은 마련되지 않은 것으로 관측되고 있다(Kania and Costello 2018, 112-113).

Ⅴ. 사이버 · 전자전/안보 영역의 미중경쟁 전망

미국과 중국의 사이버 역량에 대한 평가와 관련된 의견차들에도 불구하고, 전반적으로 기반능력과 방어능력은 미국이 우위에 있고, 사이버 공격능력은 중국이 우세한 것으로 평가할 수 있다(〈표-1〉 참조). 흥미로운 것은 2010년대 초중반부터 미국은 사이버 공격에 대한 관심과 투자를 확대하고 있다는 것이다. 이는 다른 나라의 공격 능력이 증대되고 있기 때문에 사이버 방어 역량만이 아니라 사이버 공격 능력을 정교화하여 외국의 대규모 사이버 공격을 억지하려는 노력으로 이해된다. 향후에는 무선 네트워크로 사이버공간의 기반이 더욱더 확장될 것이라는 관점에서, 사이버전자전의 활용이 공격과 방어 양 측면에서 중요해질 것이다. 이러한 배경에서, 사이버

12) 뿐만아니라, 네트워크 계통부의 담당영역에는 과거 총정치국이 수행하던 '삼전(三战: 心理战, 舆论战, 法律战)' 임무 가운데 작전 수준의 임무도 포함된 것으로 논의되고 있다(김태호 2018). 삼전 관련 전략적인 사안은 군사위원회 정치공작부에서 지도된다.

전과 전자전의 통합을 모색함에 있어 미국과 중국이 보이고 있는 강점과 취약점을 살펴보고, 미중경쟁의 향후 전망을 생각해볼 필요가 있다.

〈표-1〉 미, 중의 사이버전 역량 평가

구분	사이버기반능력	사이버공격능력	사이버방어능력	종합점수
미국	4.96	3.87	4.73	4.51
중국	3.35	3.93	3.42	3.62

출처: 박찬수, 박용석 2015, 1256

1. 미국의 강점과 취약점

미국의 사이버 · 전자전 준비는 작전 차원에 강점을 지니고 있다고 생각해볼 수 있다. 특히, 미 육군은 작전적 수준에서 다영역의 공격 및 방어조치들을 조율하는 메커니즘을 개발하기 위한 노력도 미 육군이 제시한 '사이버전자기 활동(CEMA)' 개념 등을 통해 보여주고 있다. 뿐만아니라 미 공군도 다영역 지휘통제(Multi-domain Command and Control)의 개념을 발전시키고 있다(Zadalis 2018, 10-15). 또한 – 육군 차원에서 우선 드러난 것이지만 – 미군은 각 부대들이 사이버 및 전자기파의 정보환경이 중요한 다영역작전 환경에서 작전임무를 수행할 수 있도록 부대의 구조와 시스템도 변화시키려는 노력을 보여주고 있다(주정율 2020, 17).

다만, 미국의 취약점은 사이버 · 전자전을 위한 군사전략 프레임과 컨트롤타워가 부재하다는 것이다. 물론, 미 육군은 사이버전 전력과 전자전 전력을 통해 재래식 군사활동의 효과를 배가시키는 다영역 전투 개념을 제시했으나, 육군의 이해관계를 반영하듯 무력분쟁의 핵심적인 단계에서 타 영역 작전보다 육군 포병의 타격능력을 더욱 부각시키고 있다. 따라서 사이버와 전자전 영역의 무기체계를 통해 우세를 확보하고 다른 경합영역의 전투에 영향을 미치려는 노력은 충분히 강조되고 있지 못하다. 한편, 미군의 사이버 전력도 육군, 공군, 해군, 해병대 등으로 분산되어 있고, 전자전 전력은 임무의 성격에 따라 다소 차이가 있기는 하지만 그 운용은 결정적으로 전투사령관의 판단에 따라 이루어진다. 이 때문에 미군 내 사이버 전력 간의 상호통합이나 사이버 수단과 전자기 수단의 동시 운용에는 일정한 한계가 존재할 수 있다고 생각되는 것이다.

2. 중국의 강점과 취약점

중국의 경우에는 작전 차원보다는 전략과 조직 차원, 즉 군사전략의 통합적 프레임과 전략

지원부대의 조직체계에 미래의 사이버 · 전자전 수행과 관련한 강점을 보유하고 있다고 생각된다. 다시 말해서, 망전일체전 개념을 통해 전략적인 차원에서 반접근 전략을 위해 사이버 · 전자전을 적극적으로 활용하겠다는 통합적 군사전략을 지니고 있고, 전략지원부대 내의 네트워크계통부가 사이버, 전자전을 관할함으로써 두 영역 간의 정보장벽을 극복하는 해법을 모색하고 있다.

중국의 사이버 · 전자전 관련 취약점은 작전 수준의 조율 능력과 관련된 불확실성에서 노출되고 있다. 중국은 망전일체의 관점에서 사이버 · 전자전의 통합을 위한 노력을 경주해왔으나, 육, 해, 공, 사이버, 우주의 다양한 전투무대에서 서로 상이한 종류의 전력을 동시에 운용하기 위해서는 각 전력들 간의 조율 메커니즘도 필요하다. 현대전의 영역이 사이버·전자전을 포함하는 방향으로 늘어났기 때문에, 군사작전과 임무의 복잡성이 매우 커졌기 때문이다. 그에 따라, 복잡해진 전쟁수행방식은 실제 작전 시의 혼란과 혼선을 막기 위한 세밀한 조율노력을 더욱 중요한 과제로 만들고 있는 것이다.

3. 미중 상호경쟁과 향후 전망

미국과 중국이 서로에 대해 경쟁적인 태도를 가시화해가는 가운데, 향후 미국과 중국은 각자의 약점은 극복하고 강점은 배가하기 위한 방향에서 경쟁적으로 사이버 · 전자전의 발전을 도모해갈 것이다. 우선, 미국은 정교한 사이버 방어와 사이버 무기를 동시에 발전시키는 방식으로 사이버 억지 체계를 수립하고, 전략적인 수준에서도 사이버 · 전자전, 나아가 우주전까지 포괄하는 전략적 차원의 다영역 전투 개념을 모색해갈 것으로 생각된다. 현재 미 육군의 다영역 전투 개념이 육군의 이해관계를 반영하고 있다면, 향후에는 사이버전, 전자전, 우주전의 가능성을 반영한 다영역전의 합동작전개념이 출현할 수 있다는 것이다. 아울러, 미국은 어떠한 방식으로든 사이버, 전자전, 우주전 전력을 통합하는 컨트롤 타워를 구축하려는 모습을 보일 수도 있다.

한편, 중국도 취약성을 극복하기 위해 실제 작전 수행과정에서 사이버, 전자전, 우주전 및 재래식 전력의 활동을 원활하게 하기 위한 작전 메뉴얼을 발전시켜가는 동향을 보일 것으로 전망된다. 동시에 미국의 사이버 공격 능력이 강화되는 데 반응하여 사이버 방어 능력을 재정비하면서 방어적 사이버 작전을 위한 능력과 더불어 체제안정을 위한 대내적 검열정책을 강화해갈 수 있다고 전망해보게 된다.

물론, 미중 간의 사이버 · 전자전 경쟁의 결과는 미지수이지만, 향후 미중경쟁의 영향은 사이버 · 전자전 분야의 통합을 가속할 것이라는 점은 분명하다. 아직 위성감시능력과 ISR, 첨단 무기체계와 공중과 해상에서 미국의 우위는 지속되고 있고 이러한 우위를 따라잡기 위해 중국이 보다 전략적인 투자를 사이버·전자전 분야에 투입하고 있으나, 중장기적으로 양국 간의 군사력 격차가 줄어들게 된다면 미국도 사이버 · 전자전 분야의 통합과 군사적 운용에 중국 못지않은 국

가적 관심을 투입하게 될 것이다. 그 결과, 미국과 중국 모두 전략적 수준에서 분쟁 초기에 사이버 · 전자전 전력을 운용하는 개념의 전략 방향으로 나아가고, 사이버 · 전자전을 전쟁의 승패를 가르는 핵심변수로 주목하게 될 것이다.

Ⅵ. 맺음말

미국과 중국의 경쟁이 단시일 내에 군사적 경쟁으로 비화되지는 않겠지만, 미중 간의 장기적 경쟁은 4차 산업혁명으로 인한 전쟁과 작전의 양상 변화를 촉진시켜 갈 것이다. 2020년대로 접어들면서 빈번해진 중국 군용기와 러시아 군용기의 동해 진입도 전자정보 수집을 위한 것으로서, 주변 강대국들이 이미 구축한 사이버전 능력을 바탕으로 전자전 능력을 군사활동에 활용하려는 의도를 가지고 있음을 보여주고 있다(〈국방일보〉 2021. 03. 11). 이러한 상황에서 전략적 요충지에 위치한 한국은 미래의 전쟁방식이 어떻게 정립되는지를 면밀히 파악하면서, 국가적 안전을 유지, 확대하기 위한 구상을 가다듬어가야 한다. 이를 위해서는 사이버 · 전자전에 대한 방어 역량을 우선적으로 제고시키면서 적극적 방어의 개념을 모색해야 할 필요성도 있어 보인다. 나아가 사이버 · 전자전을 위한 전략과 작전의 수행에 필요한 컨트롤 타워의 수립도 선제적으로 고민될 필요도 있다. 작전과 전술 차원에서 세밀한 조율방식도 고려하여, 복합적인 미래 전쟁에서 최대 효과를 달성하기 위한 방안도 고찰해가야 한다. 일본 역시 전자전 능력이 주변 강대국에 열세라는 판단 하에서, 대대적으로 전자전 능력을 발전시키고 있다.

한국의 사이버·전자전 능력 확보 노력도 이제 가시화되고 있으며, 이러한 성장노력은 미중 경쟁을 배경으로 한국의 전략적 가치에 영향을 미칠 것이다. 육군은 2025년까지 사이버·정보전 개념연구를 마무리짓고, 2030년까지는 우주정보통합체계 및 소형위성지상발사체를 확보하겠다는 목표를 밝힌 바 있다. 이러한 노력의 향배는 사이버전과 전자전 능력이 결정적인 역할을 할 미중경쟁의 맥락에서 한국의 중요성과 영향력을 더욱 확대시키는 요소가 될 것이다. 예컨대, 중국의 동·서해 전자정보 수집 활동에 대한 기만능력 확충 등 한국의 대응책은 한미동맹의 시설 및 세력 보호에 도움이 될 수 있다. 오늘날에는 디지털 기술의 발전에 따라 지리적인 거리를 뛰어넘는 동맹활동이 가능해지고 있고, 다영역전투의 개념 속에서 사이버·전자기파 공간의 중요성이 더욱 증대되고 있다. 이러한 차원에서 근거리 및 원거리 사이버·전자전 역량의 확대 역시 한국의 전략적 가치를 높이는 방향의 노력이 될 것이다.

[참고문헌]

김문조, 유석봉. 2019.『최신무기체계학』. 인천: 진영사.

김상배 편. 2017.『사이버 안보의 국가전략』. 서울: 사회평론.

김상배. 2018.『버추얼 창과 그물망 방패』. 경기: 한울아카데미.

김태호. 2018. "비밀스런 중국군 개혁 진행중…신형 미래전 준비에 박차."『중앙일보』(2018년 2월 26일자).

노 훈, 이재욱. 2001. "사이버전의 출현과 영향, 그리고 대응방향."『국방정책연구』(2001년 가을): 177-201.

민병원. 2015. "사이버공격과 사이버억지: 국제정치적 의미와 대안적 패러다임의 모색."『JPI 정책포럼』(2015-19).

박찬수, 박용석. 2015. "사이버전의 역량평가 개선과 역량 강화 방안에 관한 연구."『한국정보통신학회논문지』19(5): 1251-1258.

성인모. 2014. "중국 인민해방군의 현대화 및 전문화 추진: 군사교리 변화를 중심으로."『전략연구』제62호: 35-61.

엄정호, 김남욱, 정태명. 2020.『제4차 산업혁명 시대의 사이버전 개론』. 서울: 홍릉출판사.

이강규. 2011. "세계 각국의 사이버 안보 전략과 우리의 정책방향-미국을 중심으로."『정보통신방송정책』23(16): 1-27.

장노순. 2012. "사이버 무기와 국제안보."『JPI 정책포럼』(2012. 10. 12).

장수덕. 2000. "레이더 전파방해 기법과 전자공격 기술."『주간국방논단』제566호(2000).

조성렬. 2016.『전략공간의 국제정치: 핵, 우주, 사이버 군비경쟁과 국가안보』. 서울: 서강대학교출판부.

차정미. 2019. "미중 사이버 군사력 경쟁과 북한 사이버 위협의 부상 -한국 사이버안보에의 함의-."『통일연구』23(1): 43-93.

최현호. 2016. "중국, 군사굴기를 드러내다. 중국 국방 개혁의 의미."『국방과 기술』445: 34-43.

한국인터넷진흥원. 2014. "주요 국가별 사이버방어 체제 및 대응 동향."『Internet&Security Bimonthly』, 제4호.

황선한. 2018. "GPS 전파교란 동향 및 대응 기술."『주간기술동향』(2018. 7. 4).

David L. Adamy 저. 김하철, 홍우영, 최현철 공역. 2010.『전자전 모델링과 시뮬레이션 기초』. 서울: 도서출판 아진.

Sanger, David E 저. 정혜윤 역. 2019.『퍼펙트 웨폰: 핵보다 파괴적인 사이버 무기와 미국

의 새로운 전쟁』. 서울: 미래의창.

『연합뉴스』. 2016. 10. 6. "美, 러·中 방공망 뚫는 차세대 전자전체계 배치 서둘러."

『아주경제』. 2017. 7. 6. "中, 리퍼 버금 전투무인기 양산체제."

『국방일보』. 2021. 3. 11. "일본 자위대의 미래 전자전(EW) 준비 현황."

Costello, John and Joe McReynolds. 2018. Chinese Strategic Force: A Force for a New Era. Washington, D.C.: National Defense University Press.

Cyber and Electronic Warfare Division. 2014. Cyber 2020 Vision: DSTO cyber science and technology plan. 출처: https://www.dst.defence.gov.au/sites/default/files/publications/documents/Cyber-2020-Vision.pdf (검색일: 2020년 6월 1일).

Elsworth, Adam T. 2010. Electronic Warfare. New York: Nova Science Publishers.

Gurtov, Melvin, Byong-Moo Hwang. 1998. China's Security: the new roles of the military. Boulder: Lynne Rienner Pub.

Hoehn, John R. 2019. U.S. Airborne Electronic Attack Programs: Background and Issues for Congress. Washington D.C.: Congressional Research Service.

Information Office of the State Council. 2011. China's National Defense in 2010. 출처: https://media.nti.org/pdfs/1_1a.pdf (검색일: 2020년 5월 29일).

Joint Chiefs of Staff. 2012a. JP 3-13.1 Electronic Warfare. 출처: https://info.publicintelligence.net/JCS-EW.pdf (검색일: 2020년 6월 2일).

. 2012b. JP 6-01 Joint Electromagnetic Spectrum Management Operations. 출처: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp6_01.pdf (검색일: 2020년 6월 2일).

. 2018. JP 3-12 Cyber Operations. 출처: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf (검색일: 2020년 6월 2일).

Libicki, Martin C. 1998. "Information War, Information Peace." Journal of International Affairs 51(2): 411-428.

Porche III, Isaac R. 2013. Redefining Information Warfare Boundaries for an Army in a Wireless World. Santa Monica, CA: Rand Corporation.

Raska, Michael. 2017. "How China Plans to Win the Next Great Big War in Asia," 출처: https://nationalinterest.org/blog/the-buzz/how-china-plans-win-the-next-great-big-war-asia-19733 (검색일: 2020년 5월 31일).

Reily, Jeffrey M. 2016. "Multidomain Operations: A Subtle but significant Transition in Military Thought," Air and Space Journal 30(1): 61-73.

Shakarian, Paulo, Jana Shakarian and Andrew Ruef, 2013. Introduction to cyber-warfare. Amsterdan: Morgan Kaufmann Publishers, an imprint of Elsevier.

The Department of Defense. 2015. "The DOD Cyber Strategy." 출처: https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf (검색일: 2020년 6월 2일).

. 2018. "Summary of the 2018 National Defense Strategy of the United States: Sharpening the American Military Competitive Edge." 출처: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (검색일: 2020년 6월 2일).

The Information Office of the State Council. 2015. China's Military Strategy. 출처: http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm (검색일: 2020년 5월 29일).

The State Council Information Office of the People's Republic of China. 2019. China's National Defense in the New Era. 출처: (검색일: 2020년 5월 29일).

The White House. 2017. "National Security Strategy of the United States." 출처: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (검색일: 2020년 6월 2일).

U.S. Army. 2014. FM 3-38 Cyber Electromagnetic Activities. 출처: https://fas.org/irp/doddir/army/fm3-38.pdf (검색일: 2020년 6월 2일).

. 2017. FM 3-12 Cyberspace and Electronic Warfare Operations. 출처: https://fas.org/irp/doddir/army/fm3-12.pdf (검색일: 2020년 6월 2일).

U.S. Joint Chiefs of Staff. 2010. Joint Terminology for Cyberspace Operations. 출처: http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf (검색일: 2020년 6월 2일).

Winder, Davey. 2019. China Fires 'Great Cannon' Cyber-Weapon At The Hong Kong Pro-Democracy Movement." 출처: https://www.forbes.com/sites/daveywinder/2019/12/05/china-fires-great-cannon-cyber-weapon-at-the-hong-kong-pro-democracy-movement/#2cfcc7567c85 (검색일: 2020년 5월 29일).

Zadalis, Timothy M. 2018. "Multi-Domain Command and Control: Maintaining Our American Advantage." The Journal of the JAPCC Edition 26: 10-15.