

중국 사이버 안보의 진화와 군사전략적 함의



양정학 | 육군사관학교

I. 머리말

II. 선행연구 검토

III. 이론적 배경

1. 중국의 총체적 국가안보관과 사이버 안보
2. 주권으로서의 사이버 공간

IV. 중국의 사이버 안보 전략 분석

1. 사이버 안보법과 국가 사이버 공간 안보전략
2. 사이버 공간의 군사적 중요성

V. 사이버 안보와 군사전략과의 관계

1. 중국 국방백서를 통해 본 사이버 안보
2. 사이버 안보와 중국인민해방군

VI. 결론 : 미래 안보에의 함의

* 이 논문은 한국사이버안보학회(KACS)와 한국국제정치학회(KAIS)가 공동주최한 2024년 특별 기획 컨퍼런스(2024. 5. 24.)에서 발표한 글을 수정·보완한 글임

논문접수일 2024년 8월 30일 | 논문심사일 2024년 9월 10일 | 게재확정일 2024년 10월 4일

논문 요약

21세기 들어 사이버 공간은 국가 안보의 핵심요소 중 하나로 부상하였으며, 중국은 이를 국가주권의 새로운 영역으로 인식하여 강력한 사이버 안보 전략을 추진하고 있다. 본 논문은 중국의 사이버 안보 강화 추세와 사이버 안보와 군사전략 간의 관계를 분석하고 있다. 중국은 2014년 시진핑이 제시한 ‘총체적 국가안보관’을 바탕으로 사이버 안보를 국가 안보의 필수적인 부분으로 규정하고 있으며 2016년 사이버 안보법과 국가 사이버 공간 안보전략을 통해 이를 구체화하고 있다. 이는 중국의 군사전략과도 깊은 연관성을 지니고 있으며 사이버 공간에서의 군사적 우위를 확보하기 위한 중국의 노력을 보여준다. 중국의 사이버 안보 전략과 군사전략의 연계는 국제 안보환경에 큰 영향을 미치기 때문에 이에 대한 주변국들의 대응방안 마련이 필요하다.

주제어 중국의 사이버 안보, 군사전략, 전략지원부대, 사이버공간부대, 총체적 국가안보관

I. 머리말

21세기 들어 사이버 공간은 국가 안보의 핵심 요소로 부상하고 있으며, 이에 따라 각국은 사이버 안보를 강화하기 위한 다양한 정책과 전략을 수립하고 있다. 특히, 중국은 사이버 공간을 단순한 정보 교환의 도구가 아닌 국가 주권의 새로운 영역으로 인식하고 이를 기반으로 한 강력한 사이버 안보 전략을 추진하고 있다. 이러한 변화는 중국의 군사전략에도 큰 영향을 미치고 있으며 사이버 공간에서의 군사적 우위를 확보하기 위한 다양한 시도가 이루어지고 있다.

중국은 2014년 시진핑 주석이 제시한 ‘총체적 국가안보관(總體國家安全觀)’이라는 ‘大安보이념(大安全理念)’을 바탕으로 사이버 안보를 국가 주권의 핵심 요소로 규정하고 있다. 이는 2016년 11월 7일에 통과된 중국 최초의 사이버 안보 관련 기초법인 ‘사이버 안보법(網絡安全法)’과 같은 해 12월에 발표된 ‘국가 사이버 공간 안보전략(國家網絡空間安全戰略)’에 구체적으로 반영되어 있다. 이 법적·정책적 틀은 사이버 공간에서의 주권을 강조하고 있으며, 타국의 사이버 활동이 중국의 국가 안보에 미치는 영향을 엄격히 통제하는 것을 목표로 하고 있다.

본 논문은 중국의 사이버 안보 강화 추세와 중국의 사이버 안보 전략이 어떻게 군사전략과 결합되고 있는지를 분석하고자 한다. 이를 위해 중국이 사이버 안보를 어떻게 인식하고 있는지, 중국의 사이버 안보 관련 주요 법률과 정책 문서에는 무엇이 있는지에 대해 분석한 후 사이버 공간에서의 군사적 활동이 중국의 군사전략에서 어떤 역할을 하고 있는지 살펴볼 것이다. 끝으로 사이버 공간에서의 중국의 움직임이 국제 안보환경에 미치는 영향을 살펴보고 주변국의 대응 방안을 모색하고자 한다.

II. 선행연구 검토

중국의 사이버 안보 전략과 군사 전략에 대한 연구는 미국, 중국, 한국 등 다양한 국가에서 이루어지고 있으며, 그 방향과 접근법도 상이하다. 그 가운데 몇 개 주요한 글들을 살펴보도록 하겠다.

먼저, 중국학자들의 연구를 살펴보면 왕아이링(王爱玲)과 다니사(达妮莎)는 사이버 주권 개념을 중심으로 중국의 사이버 안보 전략을 분석하면서 중국이 사이버 공간에서 국가 주권을 확립하고 이를 통해 발전도상국의 권익을 보호하려는 전략적 목표를 추구하고 있음을 강조한다. 이들은 특히 데이터 주권과 네트워크 정보 관리의 중요성을 강조하며 다중이해당사자 거버넌스(多利益攸关方治理模式, Multistakeholder governance)가 강대국의 이익을 대변하는 ‘정글’과 같은 구조라고 지적하면서 이는 결국 미국 주도의 사이버 규범을 강화하는 수단이라고 비판하고 있다(王爱玲、达妮莎 2020). 상덩(项登)은 사이버 공간이 전 세계적으로 군사화되고 있음을 지적하고 있다. 사이버 공간은 국가 간 군사적 경쟁의 새로운 전장이 되었으며, 특히 미국이 주도하는 사이버 공간 군사화가 이 문제를 더욱 심화시키고 있다고 주장하고 있다. 세계 주요국들은 사이버 사령부를 설립하고 사이버 무기를 개발함으로써 군사적 우위를 확보하려 경쟁하고 있고, 그로 인해 사이버 공간에서의 군사적 충돌 가능성도 점진적으로 증가하고 있다고 경고하고 있다. 이것이 바로 중국이 자국의 사이버 주권과 군사전략을 강화하려는 이유라고 설명하고 있다(项登 2018). 또한 양난(杨楠)은 사이버 공간의 군사화가 국제 정치에 미치는 영향을 분석하며, 2010년 이란의 핵 시설을 공격한 스텍스넷(Stuxnet) 사건 이후 사이버 공간의 군사화가 본격화되었다고 설명하고 있다. 동시에 그는 주요 국가

들이 사이버 공간에서의 군사적 대응 능력을 확대하고 사이버 전쟁이 국제적 갈등의 주요 형태로 자리 잡아가고 있다고 주장하고 있다(杨楠 2020).

미국에서도 중국의 사이버 안보와 관련한 분석 글들이 많이 있다. 그중 피터 W. 싱어(P.W. Singer)와 알란 프리드만(Allan Friedman)은 중국의 사이버 활동을 중심으로 사이버 공간에서의 군사적 우위를 확보하려는 중국의 전략을 분석하며 중국의 사이버 주권 개념이 미국의 사이버 자유주의적 접근과 대비된다고 지적하고 있다. 중국의 사이버 주권 개념이 미국과 달리 국가 주권의 확장으로 인식되며, 이를 통해 사이버 공간에서의 공격적 전략이 강조되고 있음을 지적하고 있다. 특히 중국의 정보전과 심리전 전략이 미국의 국가 안보에 미치는 영향에 대해 주목하고 있다(P.W. Singer & Allan Friedman 2014). 아담 시갈(Adam Segal) 역시 중국은 사이버 공간에서 자국의 주권을 강화하려는 목적으로 사이버 스파이 활동과 지적 재산권 도용을 비롯한 다양한 수단을 활용하고 있다고 지적하고 있다. 또한 중국의 사이버 전략이 단순한 방어를 넘어 경제적, 정치적, 군사적 목표를 달성하는 데 중점을 두고 있음을 강조한다. 특히, 중국 인민해방군의 사이버 부대가 다양한 사이버 공격을 통해 중요한 정보를 탈취하고, 이를 군사적 우위를 확보하는 데 이용한다고 지적하고 있다(Adam Segal 2016).

미·중 경제안보검토위원회(US-China Economic and Security Review Commission, USCC)의 2022년 연례 보고서(2022 Annual Report to Congress)는 중국의 사이버 군사 전략이 미국과의 군사 경쟁에서 중요한 요소로 작용하고 있음을 지적하고 있으며 중국이 지난 10년 간 사이버 능력을 대폭 강화하여 국제 안보 환경에 중대한 변화를 가져오고 있다고 평가하고 있다. 중국은 사이버 공간을 자국의 규범과 법률을

적용하여 국가 주권을 확립하려한다고 인식하고 있으며, 미국이 인터넷 공간에서의 자유와 개방성을 강조하는 것과 달리 중국은 국가에 의한 통제를 중시한다고 설명하고 있다. 특히, 중국 인민해방군의 전략지원부대(戰略支援部隊)를 사이버 공간에서의 핵심 역량으로 보고 있으며 미국 군사 자산 및 중요 인프라를 목표로 사이버 공격을 수행하는 임무를 가지고 있다고 분석하고 있다. 또한 이 보고서는 중국의 사이버 역량 강화가 미국과의 전략적 경쟁에서 핵심적 역할을 하고 있음을 강조하고 있다(2022 Annual Report to Congress 2022).

끝으로 한국에서의 주요 연구로는 박남태와 백승조가 중국의 사이버 군사 전략이 한국 안보에 미치는 위협을 분석한 바 있다. 이들은 중국이 사이버 공간에서 군사력을 증강시키는 과정에서 주변국, 특히 한국에 대한 사이버 공격 가능성을 경고하며, 한국의 사이버 방어 체계 강화를 촉구하였다. 이는 한국의 안보 환경에 미치는 실질적인 영향을 강조하는 연구로서, 중국의 전략지원부대가 군사적 위협 요소로 작용할 수 있음을 지적하고 있다(박남태·백승조 2021).

중국의 연구는 사이버 안보를 자국의 주권과 군사 전략을 강화하기 위한 긍정적인 시각에서 설명하고 있으며, 미국과 한국의 연구들은 주로 중국의 사이버 전략이 자국의 안보에 미치는 위협을 분석하고, 중국의 공격적 사이버 전략에 대한 대응 방안을 모색하려고 한다. 이에 본 연구는 이와 같은 기존 연구와는 달리 중국 내부의 사이버 전략 발전 과정과 사이버 안보 전략이 군사전략과 어떠한 연계성을 가지고 있는지에 대해 집중적으로 분석하고, 이를 통해 중국 사이버 안보 전략이 국제 안보환경에 미치는 영향을 고찰하고자 한다.

Ⅲ. 이론적 배경

1. 중국의 총체적 국가안보관과 사이버 안보

2023년 12월 기준 중국 인터넷 사용 인구는 약 10억 9천 2백만 명 규모로 이는 전세계 인터넷 사용자 51억 6천만 명의 약 1/5 규모에 해당된다(新華網 2024/03/25; 199IT 2024/04/14). 인터넷은 극히 제한되었던 중국인들의 독립적인 언론 공간을 제공해줄 뿐 아니라 국내외 정보의 자유로운 교류 증진에도 큰 도움을 주었다. 이는 중국인들의 사고방식과 일상생활에도 깊은 영향을 미쳤고, 중국정부도 인터넷 공간에서 다양한 선전활동과 교육을 실시하였다. 한편 중국인들의 인터넷 활용도가 높아지면 질수록 중국정부는 정부의 입장과 다른 의견들이 속출하는 현상에 직면하게 되었고, 이로 인해 중국정부의 고민도 깊어졌다. 결국, 중국정부는 인터넷 사용을 국가안보와 결부시켜 인터넷에 대한 강력하고 촘촘한 통제를 시행하기 시작하였다.

중국의 사이버 안보 전략을 이해하기 위해서는 ‘총체적 국가안보관(總體國家安全觀)’의 개념을 먼저 이해할 필요가 있다. 2014년 4월 15일, 시진핑 주석은 중앙국가안보위원회(中央國家安全委員會) 제1차 회의에서 ‘총체적 국가안보관’을 제시하면서, 전통적 안보 개념을 넘어서는 포괄적이고 통합적인 안보 접근을 강조했다. 이 새로운 안보관은 정치, 군사, 국토, 경제, 금융, 문화, 사회, 과학기술, 사이버, 식량, 생태, 자원, 핵, 해외이익, 우주, 심해, 극지(極地), 생물(BIO), 인공지능, 데이터 등 다양한 영역을 포함하여 국가 안보의 범위를 대폭 확장하

였다(共產黨員網 2023/07/01).¹⁾

‘총체적 국가안보관’에서 사이버 안보는 중요한 구성 요소 중 하나로 자리 잡고 있으며, 중국의 사이버 안보 전략은 이러한 큰 틀 안에서 한층 더 구체적으로 수립되었다. 중국 정부는 사이버 공간을 국가 주권의 차원으로 격상시키고, 사이버 안보를 국가의 핵심 이익 중 하나로 규정함으로써 사이버 공간에서의 통제와 방어를 강화하고 있다. 이러한 이념적 틀은 중국의 사이버 안보법 및 국가 사이버 공간 안보전략에 반영되어 있으며 이는 중국의 군사전략에도 큰 영향을 미치고 있다.

2. 주권으로서의 사이버 공간

주권(sovereignty)이란 국가가 “(자국의) 영토 내에서 갖는 최고의 권한”(supreme authority within a territory)을 의미하며, UN 헌장에 따라 각국의 주권은 평등하기 때문에 이러한 최고의 법적 권한을 타국에 대해 행사할 수 없다(박주희 2020). 주권은 크게 내적 주권(internal sovereignty)과 외적 주권(external sovereignty)으로 구분되며, 내적 주권은 자국민들에 대한 국가의 권위에 관한 것이고, 반면 외적 주권은 국가 간 관계에 관한 것으로 독립 혹은 국가의 자율성에 관한 것이다(차정미 2024). 즉, 주권은 국가가 자신의 영토에 대해 통제를 행사할 권한이고, 국제적으로는 자신의 영토와 국민을 대표하여 행사하는 권한

1) 총체적 국가안보관은 기존의 안보관보다 안보영역이 크게 확대된 것이고, 안보문제의 복합성으로 인한 각 영역 간 유기적 협조와 조정을 강조하고 있으며, 무엇보다 중국 지도부의 국가안보에 대한 인식이 한층 더 강화되었다는 특징을 보이고 있다.

인 것이다(박주희 2022). 그러나 사이버 공간은 물리적 영토와 경계가 존재하지 않는 속성으로 인해 기존의 전통적 영토 주권개념을 적용하는 데에는 한계가 있다. 전통적 주권개념은 영토를 기반으로 한 권한 행사로 비교적 명확하지만, 사이버 공간은 물리적 영토의 범위를 초월하는 속성으로 인해 주권의 모호성을 초래할 유인이 크다. 이는 국가 간 사이버 공간에서 발생하는 다양한 활동을 규제하거나 자국의 데이터 및 정보 인프라를 보호하기 위한 주권적 권리를 주장하게 될 때, 국가 간에 마찰이 발생할 확률도 높아진다. 이러한 이유로 사이버 공간에서의 주권 이슈는 국제사회에서 새로운 논쟁거리로 부상하였다.

오늘날 사이버 공간에서의 주권 논쟁은 주로 중국을 위시한 권위주의 정권과 서구의 민주주의 정권 간의 첨예한 대립 구도 형태로 나타나고 있다. 특히, 중국은 국제법상 사이버 주권의 원칙을 강력히 주장하고 있는 데 반해 미국과 유럽연합(EU) 국가들은 이와 반대되는 입장을 취하고 있다(김두진 2022). 중국을 중심으로 한 권위주의 국가들은 사이버 주권을 국가 안보와 국내의 정치적 안정 유지를 위한 수단으로 인식하고 있어, 사이버 공간에서의 각종 통제와 감시를 강화하고 있다. 반면, 미국과 유럽연합을 중심으로 한 민주주의 국가들은 사이버 주권의 강화가 사이버 공간의 개방성과 자율성을 저해할 수 있다는 우려를 나타내고 있다. 미국의 경우 사이버 공간에서의 자유로운 정보 흐름과 기본적 자유, 프라이버시 등을 보장하는 것이 사이버 안보의 기본원칙이라고 주장하고 있다(채재병·김일기 2020).

중국의 경우 사이버 공간에서의 주권을 중국 사이버 안보 전략의 핵심으로 인식하고 있다. 중국은 사이버 공간을 물리적 영토, 영해, 영공과 동등한 국가 주권의 영역으로 간주하며, 이를 기반으로 한 강

력한 통제 및 방어 체계를 구축하고 있다. 이러한 접근은 2016년 통과된 사이버 안보법에서 명확히 드러나고 있으며, 이 법은 사이버 공간에서의 주권을 보호하기 위한 다양한 조치를 규정하고 있다. 예를 들어, 중국은 사이버 공간에서 외국의 간섭을 배제하고 자국의 이익을 보호하기 위해 인터넷의 국경 통제, 실명인증제도, 데이터 국외 반출 규제 등의 조치를 시행하고 있다(界面新聞 2017/06/09). 또한, 중국의 군사 관련 사이버 안보도 중앙군사위원회에서 별도로 규정하고 있다고 명시하고 있지만 그 내용에 대해서는 대외적으로 알려진 바가 없다(中華人民共和國中央人民政府 2016/11/07).

사이버 공간에서의 주권은 중국의 군사전략과도 밀접하게 연결되어 있다. 사이버 공간이 국가 안보의 중요한 영역으로 인식되면서 중국은 군사적으로도 사이버 공간에서의 우위를 확보하기 위해 다양한 전략을 개발하고 있다. 이는 사이버 공격과 방어 능력의 강화, 사이버 전력의 확충 그리고 관련 인프라와 인력의 확보 등으로 나타나고 있다. 이러한 전략은 중국의 국방백서 및 군사전략 문서에서도 여러 차례 언급되고 있으며, 이는 중국의 군사전략이 사이버 공간에서의 주권 수호를 중요한 목표로 삼고 있음을 보여주는 것이기도 하다.

IV. 중국의 사이버 안보 전략 분석

1. 사이버 안보법과 국가 사이버 공간 안보전략

중국의 ‘사이버 안보법(網絡安全法)’은 2016년 11월 7일에 통과된 이래 중국의 사이버 안보 정책의 기초법으로서 가장 근간이 되는 중심 역할을 담당하고 있다. 이 법은 사이버 공간을 국가 주권의 중요한 영역으로 규정하며, 사이버 공간에서의 모든 활동이 국가 안보와 일치하도록 엄격히 통제하고 있다. 사이버 안보법의 주요 특징 몇 가지를 살펴보면 다음과 같다. 첫째, 사이버 공간에 대한 주권개념 적용을 들 수 있다. 중국은 이 법을 통해 사이버 공간 개념을 국가주권 차원으로 격상시킴으로써 타국 또는 해외조직에 의한 중국의 사이버 권익 침해를 중국의 국가주권 침해로 간주하여 대응할 것이라는 점이다.²⁾ 중국의 사이버 주권 개념은 단순한 방어적 목적을 넘어 자국의 이익을 적극적으로 추구하는 방향으로 발전하고 있다. 중국은 사이버 주권을 통해 국가가 사이버 공간에서의 모든 활동을 통제할 권리가 있다고 주장하며, 이를 UN 헌장의 국가주권 원칙과 결부시켜 설명하고 있다. 이는 중국이 국내 인터넷 통제와 사이버 검열을 강화하는 방식으로 구현되고 있다(Michael Kolton 2017). 둘째, 사이버 안보 등급 보호제

2) 중국에서 ‘국가주권’은 핵심이익 중 가장 먼저 나열될 만큼 중요한 사안이다. 『중국의 평화발전(中國的和平發展)』 백서에 따르면, 중국의 핵심이익은 ①국가주권(國家主權), ②국가안보(國家安全), ③영토완정(領土完整), ④국가통일(國家統一), ⑤중국 헌법에 의해 확립된 국가 정치제도 및 전반적인 사회안정(中國憲法確立的國家政治制度 and 社會大局穩定), ⑥ 경제 및 사회의 지속 가능한 발전의 기본보장(經濟社會可持續發展的基本保障) 등을 포함하고 있다.

도를 확립함으로써 등급이 높을수록 국가정보안보감독부서의 개입이 커진다. 셋째, 실명인증제도를 명문화하여 투명하고 엄격한 인터넷 감시체계를 구축하였다. 넷째, 국외로 데이터를 송출할 때 심사 및 평가하는 제도가 규정되어 국내에 저장된 자료를 국외로 송출하고자 할 때 관련 데이터는 국가안보와 사회공공이익 등에 위해(危害)가 되면 안 된다는 것이다(界面新聞 2017/06/09). 이렇듯 중국의 사이버 안보법은 단순한 국내 통제의 도구일 뿐만 아니라 외국과의 데이터 흐름을 제한하는 수단으로도 작동된다. 또한, 이 법률은 중국의 사이버 주권 강화를 위한 중요한 기제임과 동시에 해외 기업과 국가들이 중국의 사이버 규제를 준수해야 하는 법적 근거를 제공하고 있다(EU-RObiz magazine 2023).

사이버 안보법에 이어 발표된 ‘국가 사이버 공간 안보전략(國家網絡空間安全戰略)’은 중국 최초의 사이버 공간 관련 전략서이자 강령성 문건(綱領性文件)으로 규정하고 있다(中國日報 2016/12/29). 이 전략서는 중국의 사이버 주권 개념을 더욱 구체화하고 확장한 것이라고 볼 수 있다. 중국은 이 전략서에서 사이버 공간에서의 발전과 안보에 관한 중대한 입장과 주장을 밝히고 있는데, 사이버 안보를 인류의 공동이익, 세계 평화와 발전, 각국의 국가안보와 관련이 깊다고 보고 있다. 또한 ‘중국몽(中國夢)’ 실현을 위해 사이버 안보를 수호해야 한다고 강조하고 있다(人民網 2016/12/27). 이는 중국이 사이버 안보를 단순한 기술적 문제가 아닌 국가 발전의 핵심 요소로 인식하고 있음을 보여준다. 전략 임무로는 ①사이버 공간에서의 주권 수호, ②국가안보 수호, ③핵심 정보인프라 보호, ④사이버 문화건설 강화, ⑤사이버 테러 및 불법범죄 단속, ⑥사이버 관리체계 개선, ⑦사이버 안보 기반 강화, ⑧사이버 공간 방호능력 향상, ⑨사이버 공간 국제협력 강화 등

9가지를 제시하고 있다. 이러한 포괄적인 접근은 중국이 사이버 공간을 총체적으로 통제하고자 하는 의도를 반영한다고 볼 수 있다. 이외에서 전략서에서는 ‘총체적 국가안보관’의 지도하에 ‘적극방어와 효과적 대응(積極防禦、有效應對)’을 통해 국가주권과 안보, 그리고 발전 이익을 수호하여 사이버 강국 건설이라는 전략목표를 실현할 것을 요구하고 있다(中華人民共和國中央人民政府 2016/12/28). 이와 같은 접근 방식은 중국의 공세적인 사이버 전략을 정당화하는 근거가 될 수 있다는 점에서 주목할 필요가 있다. 또한, 이러한 전략목표는 중국이 사이버 공간에서의 군사적·정치적 우위를 확보하고자 하는 전략적 의도를 반영하고 있다. 더 나아가 이는 중국이 글로벌 사이버 거버넌스 체제에서 자국의 영향력을 확대하려는 야심을 드러내는 것으로도 해석될 수 있다.

2. 사이버 공간의 군사적 중요성

오늘날 군사 분야와 사이버 공간과의 관계는 밀접한 정도를 초월하여 이미 상호불가분(相互不可分)의 수준에까지 이르렀다고 해도 과언이 아니다. 이러한 관계가 향후 군사 패러다임의 근본적 변화를 초래할 것으로 예측하기도 한다(Jon R. Lindsay 2015). 누가 사이버 공간에서의 ‘감제고지(瞰制高地)’를 먼저 선점하느냐는 향후 군사작전에서의 자유로운 행동과 합동작전의 효과에 지대한 영향을 미치게 될 것이다. 군사 분야에서 사이버 공간에 대한 중요성이 점차 증대됨에 따라 각국의 군사전략에도 사이버 안보에 관한 비중이 크게 늘고 있다. 중국도 예외가 아니다.

중국의 사이버 안보 전략은 단순히 국내적 차원의 통제와 방어를

넘어 군사적 목표와도 깊이 연계되어 있다. 이러한 전략은 중국의 ‘정보화 전쟁’ 개념과 밀접하게 연관되어 있다(Jon R. Lindsay 2015). 사이버 안보법과 국가 사이버 공간 안보전략은 모두 중국 군대의 작전 수행능력을 향상시키기 위한 기반을 제공하며 이를 통해 중국은 사이버 공간에서의 군사적 우위를 강화하고자 한다. 특히, 중국의 군사전략 문서들에서 반복적으로 언급되는 사이버 공간에서의 주권 수호와 정보전 능력 강화 등의 내용은 사이버 공간과 군사와의 연계성을 잘 보여주고 있다.

중국은 사이버 공간에서의 군사 활동을 통해 적국의 네트워크 체계를 무력화시키고 자국의 군사적 행동의 자유를 보장하고자 한다. 또한 이러한 접근을 중국의 ‘비대칭 전략’의 핵심 요소로 평가하기도 한다(Jon R. Lindsay 2015). 이는 사이버 공격, 방어 그리고 정보전에 대한 능력 강화로 이어지고 있다. 이러한 전략적 움직임은 중국의 군사전략의 중요한 부분을 차지하고 있다. 또한, 중국 국방백서에서는 사이버 공간에서의 군사적 활동이 국가 안보에 미치는 영향을 명확히 인식하고 있으며 사이버 공간에서의 군사력 증강을 강조하고 있다. 이러한 강조는 중국의 ‘적극방어’ 전략의 현대적 해석이라고 할 수 있을 것이다. 즉, 군사 분야에서 사이버 공간의 중요성이 나날이 증대되고 있음을 알 수 있다.

V. 사이버 안보와 군사전략과의 관계

1. 중국 국방백서를 통해 본 사이버 안보

중국의 국방백서들은 사이버 공간과 군사전략 간의 관계를 명확히 드러내고 있다. 특히, 2010년 이후 발간된 국방백서에서는 사이버 공간이 중국의 국가 안보와 군사전략에서 차지하는 비중이 급격히 증가하고 있음을 확인할 수 있다.

중국은 2010년 중국 국방백서에서 일부 대국들이 우주·사이버·극지(極地) 전략을 수립하고 있으며, 사이버 작전능력을 증강시키고 있다고 평가하였다. 또한, 중국 국방의 목표 및 임무를 소개하면서 영토, 내수(內水), 영해, 영공을 지키고 동시에 우주·전자기·사이버 공간에서의 국가안보이익을 수호할 것을 명시하고 있다(中華人民共和國國務院新聞辦公室 2011). 이는 이전까지 발간된 국방백서에는 없던 내용으로 ‘사이버 공간’에서의 안보 이익을 처음으로 명시하였으며, 이는 중국이 사이버 공간을 군사적으로 활용할 수 있는 중요한 영역으로 인식하기 시작했음을 보여주고 있다.

2013년 발간된 『중국 무장역량의 다양화 운용(中國武裝力量的多樣化運用)』에서는 우주 및 사이버 공간 등을 포함한 전략 감제고지의 선점이 정보화 조건 하 국부전쟁에서의 승리와 직결된다고 강조하고 있다. 이는 사이버 공간에서의 군사적 우위가 전통적인 물리적 전장에서의 우위와 동등하게 중요하다는 인식의 반영이라 볼 수 있다.

2015년 국방백서인 『중국의 군사전략(中國的軍事戰略)』에서는 우주와 사이버 공간 등 새로운 형태의 안보영역에서의 위협에 대응해야

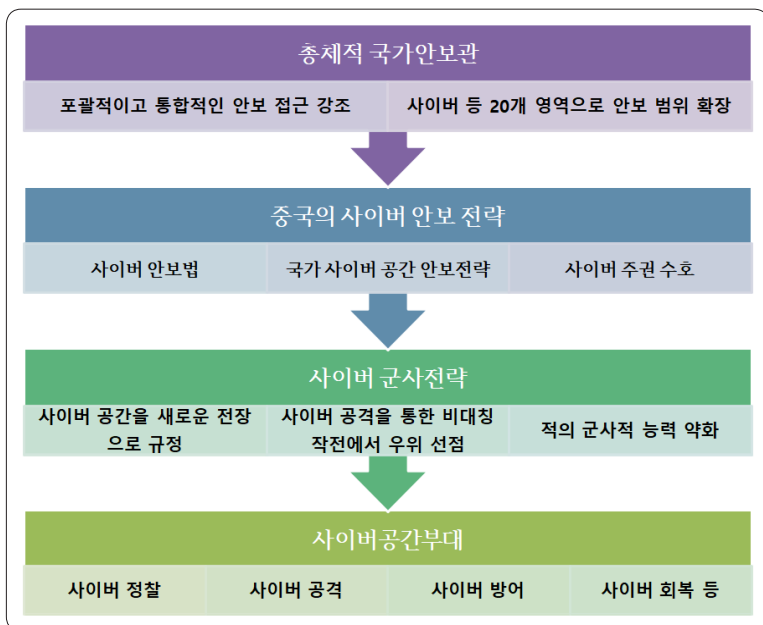
함을 제시하면서 사이버 공간을 국가 안보의 새로운 영역으로 규정하고 있다. 또한, 타국에 의한 해킹 공격의 최대 피해자는 중국이라는 인식을 보여주었다. 사이버 공간이 군사안보에 미치는 영향이 점차 증대되고 있으므로 사이버 공간에서의 상황인식과 사이버 방어, 사이버 공간에서의 투쟁 등의 능력을 강화시키는 것이 군사전략의 중요한 목표임을 명시하고 있다(中華人民共和國國務院新聞辦公室 2015).

가장 최근에 발간된 2019년 국방백서에서는 사이버 공간을 국가 안보와 경제 사회 발전의 핵심 영역으로 평가하며, 사이버 안보를 글로벌 차원의 도전으로 격상시켰다. 특히, ‘중국 군대(中國軍隊)’가 사이버 공간에서의 역량 건설을 가속화 하고, 사이버 안보의 방어 수단을 대폭 발전시킬 것을 요구하고 있다. 이는 중국이 사이버 공간에서의 군사적 활동을 통해 자국의 국제적 지위와 영향력을 강화하려는 의도를 명확히 표출하고 있는 것이라 볼 수 있다(中華人民共和國國務院新聞辦公室 2019). 실제로 중국 국방부 대변인 런궈창(任國強) 대교(大校)는 정례브리핑에서 중국군대는 지금까지 어떠한 사이버 해킹 행위를 지지한 적이 없으며, 중국군대는 사이버 공간 방어능력을 적정 수준에서 발전시켜 국가 사이버 주권과 정보안전을 수호하고 있다고 설명하기도 하였다(人民網 2019/11/29).

앞에서 살펴본 바와 같이 중국은 국방백서를 통해 사이버 안보에 대한 중요성과 사이버 안보를 위한 실질적인 능력을 갖추어야 한다고 반복적으로 강조하였다. 2010년 사이버 공간에서의 안보이익을 최초로 언급한 이후 2013년에는 사이버 공간에 대한 선점의 중요성을 강조하였고, 2015년에는 사이버 공간을 국가안보의 새로운 영역으로서 향후 군사안보에 미칠 영향이 증대될 것이라 평가하였다. 더 나아가 2019년에는 사이버 안보를 글로벌 차원의 도전으로 상향 조

정하고, 이에 대응하기 위해 사이버 강국 수준의 사이버 방호능력을 갖추어 국가 사이버 주권과 정보안정을 지켜야 한다고 역설하였다.

〈그림 1〉 중국의 사이버 안보 전략과 사이버 군사전략의 연계



출처 : 저자가 제작함.

중국군은 정부 공식문건을 통해 사이버 안보에 관한 중요성을 점진적으로 강조하는 한편 사이버 안보의 군사전략으로서의 가치를 언급하였다. 사이버 공격의 작전효능은 군사적 능력을 제고시켜줄 수 있다. 사이버 공격을 통해 비대칭 작전에서의 우위를 점하는 한편 적의 군사적 능력을 약화시킬 수도 있기 때문에 중국은 미래 전쟁에서 승리하기 위해 사이버 공간에서의 작전능력을 강화시켜 나갈 것임을 분명히 밝혔다.

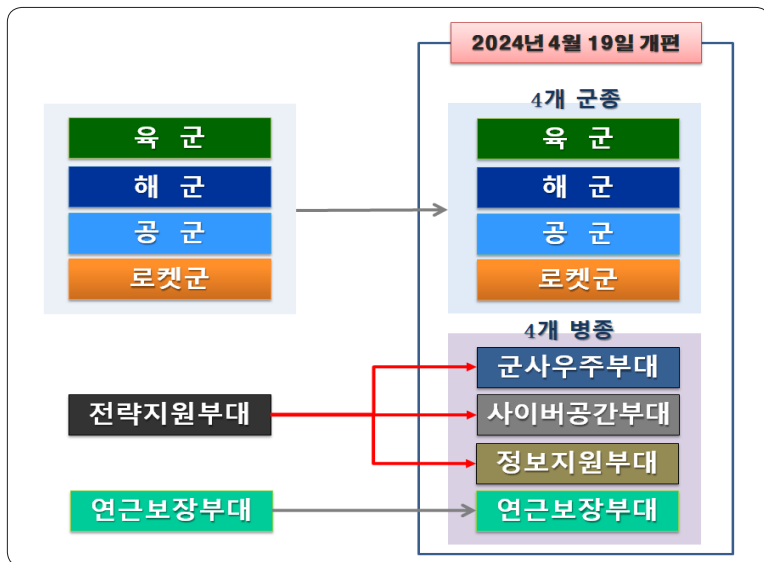
이처럼 중국의 국방백서 내용의 변화는 중국이 사이버 공간을 단순한 기술영역이 아닌 국가안보와 군사전략의 핵심요소로 인식하는 과정을 보여주고 있으며, 그 중 특히 주목해야 할 부분은 다음과 같이 네 가지로 요약할 수 있다. 첫째, 전략적 중요성의 상승을 들 수 있다. 2010년부터 2019년까지 사이버 공간의 중요성이 점진적으로 강조되어 현재에는 글로벌 차원의 도전으로까지 격상되었다는 것이다. 이는 중국이 사이버 공간을 국제정세와 국가 간 경쟁의 새로운 전장으로 인식하고 있음을 보여주는 것이다. 둘째, 군사전략으로의 통합을 들 수 있다. 사이버 공간이 점진적으로 군사전략의 핵심요소로 통합되고 있음을 알 수 있다. 2013년 국방백서에서 언급된 ‘전략 감제고지의 선점’은 사이버 공간에서의 우위가 전통적인 군사력 못지않게 중요해졌음을 의미한다. 셋째, 방어에서 공세로의 전환을 들 수 있다. 초기에는 사이버 공간에서의 방어를 강조했지만 점차 ‘사이버 공간에서의 투쟁’ 등 보다 적극적이고 공격적인 표현을 사용하고 있다. 이를 통해 중국이 사이버 공간에서 단순한 방어적 태세를 넘어 공세적 능력을 개발 및 표출하고 있음을 간접적으로 알 수 있다. 넷째, 국제적 영향력의 확대를 위해 도구로 사용된다는 점이다. 2019년 국방백서에서 언급된 ‘국제적 지위와 영향력 강화’는 중국이 사이버 공간을 국제무대에서의 영향력 확대 수단으로 인식하고 있음을 명확히 보여주고 있는 것이다.

이러한 변화는 중국이 사이버 공간을 미래전쟁의 핵심영역으로 인식하고, 이를 통해 군사적 우위를 확보하려는 전략적 의도를 반영하고 있다. 또한, 사이버 공간에서의 능력 강화가 단순히 군사적 목적뿐 아니라 국제정세에서의 영향력 확대를 위한 수단으로도 활용될 수 있음을 시사하고 있다.

2. 사이버 안보와 중국인민해방군

중국의 군사전략에서 사이버 공간의 중요성은 중국인민해방군 전략지원부대(戰略支援部隊)의 창설과 관련이 깊다. 중국인민해방군 전략지원부대는 2015년 12월에 창설된 이후, 사이버 공간과 우주, 전자기 영역에서의 군사 작전을 지원하는 핵심 부대로 기능해왔다. 중국 정부는 이 부대를 국가안보 수호를 위한 ‘신형 작전역량’이며 새로운 형태의 작전능력의 중요한 성장점이라고 소개하고 있다. 전략지원부대는 합동작전체계에 융합되어 새로운 영역에서의 대항훈련과 긴급 응전훈련을 충실히 전개할 것이라고 설명하였다(中華人民共和國國務院新聞辦公室 2019). 전략지원부대는 중국인민해방군의 육군, 해군, 공

〈그림 2〉 2024년 4월 19일 군 구조 개편 전후 비교

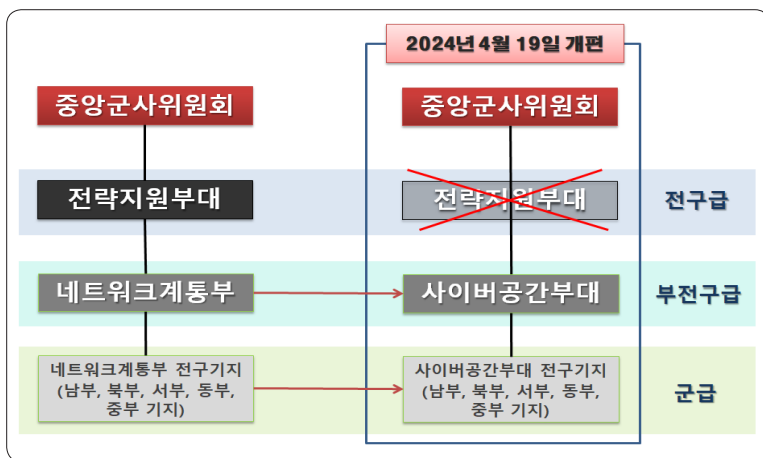


출처 : 중국 국방부 대변인 브리핑과 각종 언론보도 내용을 바탕으로 저자가 제작함.

군, 로켓군과 동등한 지위에서 운영되었으며, 정보, 기술정찰, 전자대항, 사이버 공격 및 방어, 심리전 등의 임무를 수행해왔다. 전략지원부대의 주요 임무는 사이버 공간을 포함한 새로운 전장에서의 군사적 우위를 확보하는 것이었다. 이를 위해 전략지원부대는 우주와 사이버 공간에서의 정보 수집 및 제공, 적의 정보 체계에 대한 공격, 그리고 전자전 및 심리전을 통해 중국 군대의 작전을 지원했다. 이 부대의 창설은 중국이 사이버 공간을 새로운 전장으로 인식하고, 이를 활용한 군사 작전을 본격적으로 추진하고 있음을 보여주었다.

그러나 전략지원부대는 2024년 4월 19일 군 구조 개편 과정에서 해체되었고, 사이버 관련 임무는 새로 설립된 ‘사이버공간부대(網絡空間部隊, Cyberspace Force)’로 이관되었다(中華人民共和國國防部 2024/04/19). 사이버공간부대는 전략지원부대의 네트워크계통부의

〈그림 3〉 2024년 4월 19일 군 구조 개편 후 사이버 관련 임무 담당 조직



출처 : J. Michael Dahm 2024를 참조하여 저자가 제작함.

기능을 이어받아 사이버 정찰, 사이버 공격 및 방어, 사이버 회복 등의 임무를 수행하며, 중국의 사이버 공간에서의 군사 활동을 더욱 전문화하고 있다(J. Michael Dahm 2024).

1) 인민해방군의 사이버 안보 핵심역량 : 사이버공간부대

사이버공간부대는 중국의 사이버 안보 전략에서 핵심적인 역할을 담당하는 부대로, 사이버 정찰, 사이버 공격, 사이버 방어, 그리고 사이버 회복 등 다양한 임무를 수행한다. 사이버 공간에서의 임무를 담당하게 된 사이버공간부대의 주요기능은 2017년 중국 국방대학에서 발간한 『전략학(戰略學)』에 제시되어 있는 사이버전 기능을 통해 유추해 볼 수 있을 것이다(肖天亮 2017).

첫째, 사이버 정찰은 상대방의 네트워크 시스템을 정찰하고, 정보를 탈취하는 것을 목적으로 한다. 이를 위해 사이버공간부대는 사이버 공간, 전자기파, 미디어 등을 주요 정찰수단으로 활용한다.

둘째, 사이버 공격은 정보 교란, 정보 파괴, 네트워크 시스템 침투 등을 통해 상대방의 인터넷망과 호스트 정보를 교란하거나 파괴하는 활동을 의미한다. 이는 중국 군대가 적의 군사 능력을 무력화하고, 자국의 군사적 우위를 확보하기 위한 중요한 수단으로 사용된다.

셋째, 사이버 방어는 상대방의 사이버 정찰 및 공격을 방어하고, 아군의 네트워크 설비와 시스템을 보호하는 것을 목표로 한다. 사이버 공간부대는 아군의 네트워크 시스템의 안정성을 확보하고 적의 사이버 공격을 차단하는 데 중점을 두고 있다.

끝으로, 사이버 회복은 사이버 공격을 받은 후, 사이버 공간, 통신 네트워크, 컴퓨터 시스템 및 관련 프로세서가 안정적으로 운용되도록 복구하는 과정을 의미한다. 이를 위해 사이버공간부대는 하드웨

어, 소프트웨어, 데이터의 백업 및 복원 작업을 신속히 수행하여, 전시에 아군의 군사 작전이 원활히 진행될 수 있도록 지원한다.

사이버공간부대는 사이버 공간에서 사이버 정찰, 사이버 공격 및 방어, 사이버 회복 등을 지속적으로 수행함으로써 평시에는 사이버 공간에서의 우위를 달성하고자 노력하고, 전시에는 물리적 전력의 실제 작전을 수행하는 데 유리한 여건을 조성하는데 집중할 것이다. 기존의 네트워크계통부 기술정찰국은 사이버 작전을 수행하는 핵심 부대로 대상국(또는 목표)과 임무는 아래와 같으며 새롭게 개편된 사이버공간부대는 이를 그대로 인수했을 것으로 추정된다.

〈표 1〉 사이버공간부대(舊전략지원부대 네트워크계통부) 기술정찰국 현황

부서명	통상명칭	위치	주요 임무
제1국	61786	베이징시 하이톈구 (海澱區)	• 암호화, 정보안전
제2국	61398	상하이시 푸둥신구 (市浦東新區)	• 미국과 캐나다 정보수집 • 위성사진 처리분석
제3국	61785	베이징시 다싱구(大興區)	• 무선통신 수집 및 관리 • 네트워크 통제
제4국	61419	칭다오시	• 한국과 일본 정보수집
제5국	61565	베이징시 다싱구	• 러시아 정보수집
제6국	61726	우한시 우창구 (武昌區)	• 위성, 공공정찰 사진, 전자파, 네트워크 데이터 정보수집
제7국	61580	베이징시 하이톈구	• 네트워크 공격 • 서부지역(우루무치) 방향 위성 관리
제8국	61046	베이징시 한자촨 (韓家川)	• 유럽, 중동, 아프리카, 남미 정보수집 • 베이징 서부의 위성통신센터 관리
제9국	미상	베이징시	전략정보 분석 데이터베이스 관리
제10국	61886	베이징시 하이톈구	중앙아시아, 러시아 정보수집

부서명	통상명칭	위치	주요 임무
제11국	61672	베이징시 하이덴구	러시아 정보수집 및 분석
제12국	61486	상하이시 자베이구 (閘北區)	위성통신 차단 및 신호정보 분석 네트워크 공격

출처: 黃鬱文 2022, 27; 朱鈺德、李建鵬 2021, 74-76.

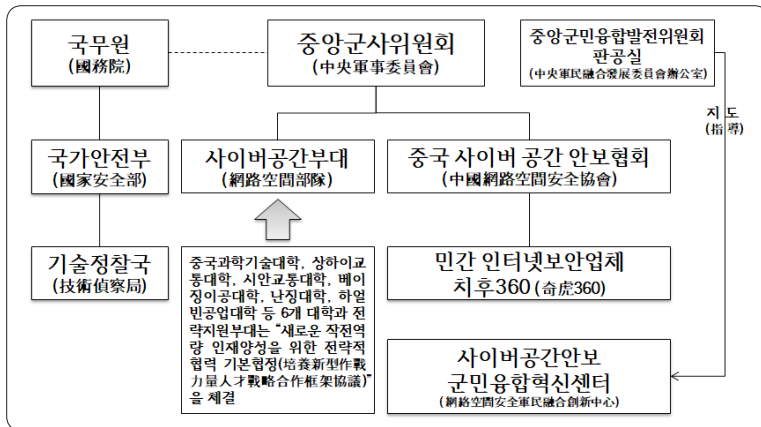
2) 사이버 분야에서의 군민협력 강화

2024년 4월 군 구조 개혁 전의 전략지원부대는 사이버 작전능력을 확보하기 위해 민간과의 사이버 분야에서의 협력을 강화해 나아갔다. 사이버 분야의 특성상 민간과의 협력은 필수적이라 사이버공간 부대도 전략지원부대가 추진했던 것처럼 민간과의 협력 모멘텀을 지속유지하려 할 것이다.

중국은 2017년 전략지원부대를 통해 민간 대학 및 기업과 “새로운 작전역량 인재양성을 위한 전략적 협력 기본협정(培養新型作戰力量人才戰略合作框架協議)”을 체결하여, 사이버 안보 분야의 첨단기술 인재를 확보하고자 했다. 여기에는 중국과학기술대학(中國科技大學), 상하이교통대학(上海交通大學), 시안교통대학(西安交通大學), 베이징이공대학(北京理工大學), 난징대학(南京大學), 하얼빈공업대학(哈爾濱工業大學) 등 6개의 명문대학과 우주과학기술그룹(航天科技集團公司), 우주과학공업그룹(航天科工集團公司), 전자과학기술그룹(電子科技集團公司) 등 3개의 방산업체가 포함되어 있다(新華網 2017/07/12). 또한, 2017년 12월 26일에는 중앙군민융합발전위원회판공실(中央軍民融合發展委員會辦公室)과 군 관계부서의 지도하에 민간 인터넷보안업체인 ‘치후 360(奇虎360, 三六零安全科技股份有限公司)’가 이끄는 “사이버 공간 안보 군민융합혁신센터(網絡空間安全軍民融合創新中心)”를 만들었다. 사

이버 공간 안보 군민융합혁신센터는 사이버 분야 국방안보 싱크탱크로서의 역할과 기술 개발 서비스를 제공할 것으로 알려졌다(每日頭條 2017/12/27). 사이버전에서의 전장은 전시와 평시 구분이 없고, 작전 수행 인원이 군인인지 민간인인지도 알기 어렵다. 이러한 특징들은 중국군이 사이버 분야와 관련하여 민간과의 협력을 한층 더 강화하려는 강한 동인으로 작용하고 있다.

〈그림 4〉 중국의 사이버 공격 조직도



출처 : 王清安 2018, 122³⁾

사이버공간부대는 이러한 협력의 연장선에서 민간 부문과의 협력을 더욱 강화하여 사이버 공간에서의 군사적 우위를 지속적으로 유지하고자 한다. 이는 사이버 공간에서의 전쟁이 단순히 군사적 영역

3) 王清安(2018) 글의 내용 중 전략지원부대를 삭제, 전략지원부대의 사이버공간작전부대를 새로 신설한 사이버공간부대로 대체, 중앙군사위원회와 국무원과의 관계도를 수정하여 재제작하였음.

을 넘어 민간 부문과의 긴밀한 협력에 의해 좌우될 수 있음을 보여주는 것이기도 하다.

VI. 결론 : 미래 안보에의 함의

중국은 ‘총체적 국가안보관’을 기반으로 사이버 공간을 국가주권의 중요한 요소로 격상시키며 사이버 안보를 국가 안보의 핵심 영역으로 규정하였다. 이러한 접근은 사이버 안보법과 국가 사이버 공간 안보전략을 통해 구체화되었으며 이 법적·정책적 틀은 중국의 군사전략과도 깊이 연결되어 있다. 특히, 중국의 군사전략 문서들에서 강조되는 사이버 공간에서의 주권 수호와 군사적 우위 확보는 이러한 연계를 잘 보여주고 있다. 중국인민해방군 사이버공간부대는 이러한 전략의 핵심 실행부대로 사이버 정찰(적국의 네트워크 시스템 탐지 및 정보 수집), 사이버 공격(적국의 정보 시스템 교란 및 파괴), 사이버 방어(자국 네트워크 및 정보 시스템 보호), 사이버 회복(공격을 받은 후 시스템 복구 및 안정화) 등의 기능을 통해 사이버 공간에서의 군사적 우위를 확보하고자 한다.

또한, 중국군은 민간 부문과의 협력을 통해 사이버 안보 능력을 강화하고 있다. 2017년 체결된 “새로운 작전역량 인재양성을 위한 전략적 협력 기본협정”은 6개 주요 대학 및 3개 방산업체와의 협력을 규정하고 있으며, “사이버 공간 안보 군민융합혁신센터” 설립은 이러한 노력의 구체적 사례이다. 이는 사이버 공간에서의 군사 활동이 민간 영역과 불가분의 관계에 있음을 시사한다.

중국의 사이버 안보 및 군사전략은 국제 안보환경에 중대한 영향

을 미치고 있다. 첫째, 글로벌 차원에서의 안보질서 변화를 초래하고 있다. 사이버 공간이 국경을 초월한 새로운 전장으로 부상함에 따라 중국의 사이버 전략은 기존의 안보 패러다임을 변화시키고 있다. 둘째, 주권 개념이 확장되었다. 중국의 사이버 주권 강조는 타국의 사이버 활동에 대한 통제 강화로 이어질 수 있으며 이는 국제적 마찰의 소지가 있다. 셋째, 사이버 공간에서의 전쟁 위험성이 증대되었다. 중국 사이버공간부대의 군사적 활동 강화는 사이버 공간에서의 충돌 가능성을 높이고 있다. 넷째, 국제 사이버 규범 형성에 영향을 미치고 있다. 중국의 사이버 전략은 글로벌 사이버 거버넌스 체제 구축 과정에서 커다란 영향을 미치고 있다.⁴⁾

이러한 상황은 국제사회가 직면한 사이버 안보 도전에 대한 대응 방안을 시급히 마련해야 할 필요성을 높이고 있다. 특히, 미국과의 전략경쟁이 심화 및 장기화 되고 있는 상황에서 중국의 사이버 안보 및 군사전략은 지역 및 글로벌 안보 질서에 중대한 영향을 초래할 가능성이 높다. 이로 인해 중국의 사이버 안보 및 군사전략에 대한 대응은 주변국들에게 중요한 과제로 부상하고 있다. 특히, 한국과 같은 주변국은 중국의 사이버 능력 강화와 사이버 공간에서의 군사 활동을 면밀히 모니터링할 필요가 있다. 한국은 동맹국 및 우방국과의 사이버 안보 협력을 강화하고, 사이버 공간에서의 정보 공유 및 공동 대응전

4) 글로벌 사이버 거버넌스 체제 구축 과정에서의 중국의 전략과 영향력 관련 내용은 다음 글을 참조. Adam Segal. 2020. "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace." NBR Special Report no. 87; Xinchuchu Gao. 2022. "Sovereignty and Cyberspace: China's Ambition to Shape Cyber Norms." <https://blogs.lse.ac.uk/cff/2022/08/18/sovereignty-and-cyberspace-chinas-ambition-to-shape-cyber-norms/>(검색일 : 2024. 10. 06).

락을 조속히 마련해야 한다. 또한, 국가 및 군 차원에서 사이버 안보 체계를 강화하기 위한 지속적인 투자와 지원을 확대해야 한다. 특히, 고도의 기술력을 갖춘 사이버 전사(인재) 양성을 위한 전문인력 육성 프로그램을 개발하고 이에 대한 집중적인 투자가 이루어져야 한다. 끝으로 사이버 공간의 평화적 이용을 위한 국제 규범 수립에도 적극적으로 참여하여 더 많은 국가들이 동참할 수 있도록 역할을 해야 한다.

결론적으로 중국의 사이버 안보 및 군사전략에 대한 이해와 대응은 21세기 국제안보 환경에서 중요한 주제로 부상하였다. 각국은 이에 대한 전략적 대비와 함께 사이버 공간의 평화적 이용을 위한 국제적 협력을 지속적으로 모색해 나가야 할 것이다.

- 김두진. 2022. “전통적 주권 개념과 사이버공간의 ‘탈근대’의 주권 논의: 새로운 ‘베스트 팔렌’ 모형의 가능성.” 『한국정치연구』 제31집 제1호.
- 박남태·백승조. 2021. “중국어 전략지원부대의 사이버전 능력이 한국에 주는 안보적 함의.” 『국방정책연구』 제131호.
- 박주희. 2020. “사이버공간에 적용되는 주권의 규범적 성격과 사이버안보.” 『국가안보와 전략』 제20권 1호(통권77호).
- . 2022. “데이터의 탈영토성과 사이버공간 주권.” 『국제법학회논총』 제67권 2호(통권165호).
- 차정미. 2024. “사이버 공간의 안보화와 ‘사이버 주권’ 논쟁: 중국과 EU의 사이버 주권 담론 비교를 중심으로.” 『국제정치논총』 제64권 1호.
- 채재병·김일기. 2020. “주요국 사이버안보 전략과 한국에의 시사점.” INSS 전략보고 제73호.
- Adam Segal. 2016. *The Hacked World Order*. New York: PublicAffairs.
- . 2020. “China’s Vision for Cyber Sovereignty and the Global Governance of Cyberspace.” NBR Special Report no. 87.
- EURObiz magazine. 2023. “China’s Cybersecurity Law.” <https://www.eurobiz.com.cn/chinas-cybersecurity-law/>(검색일 : 2024. 09. 16).
- J. Michael Dahm. 2024. “A Disturbance in the Force: The Reorganization of People’s Liberation Army Command and Elimination of China’s Strategic Support Force.” <https://jamestown.org/program/a-disturbance-in-the-force-the-reorganization-of-peoples-liberation-army-command-and-elimination-of-chinas-strategic-support-force/>(검색일 : 2024. 04. 27).
- Jon R. Lindsay. 2015. “The Impact of China on Cybersecurity: Fiction and Friction.” *International Security* 39(3).
- Michael Kolton. 2017. “Interpreting China’s Pursuit of Cyber Sovereignty and

- its Views on Cyber Deterrence.” *The Cyber Defense Review*. Vol. 2, No. 1(WINTER).
- P.W. Singer & Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press.
- US-China Economic and Security Review Commission. 2022. *2022 Annual Report to Congress*.
- Xinchuchu Gao. 2022. “Sovereignty and Cyberspace: China’s Ambition to Shape Cyber Norms.” <https://blogs.lse.ac.uk/cff/2022/08/18/sovereignty-and-cyberspace-chinas-ambition-to-shape-cyber-norms/>(검색일 : 2024. 10. 06).
- 共產黨員網. “總體國家安全觀.”<https://www.12371.cn/special/xxzd/hxnr/aqg/>(검색일 : 2023. 07. 01).
- 黃鬱文. 2022. “中共軍事作戰支援能力：戰略支援部隊.”『國防情勢特刊』第22期(2022.11). 27.
- 界面新聞. 2017. “《網絡安全法》十大要點解讀.”<https://www.jiemian.com/article/1367047.html>(검색일 : 2023. 09. 05).
- 每日頭條. 2017. “我國‘網絡空間安全軍民融合創新中心’成立.”<https://kknews.cc/tech/4eykenx.html>(검색일 : 2023. 09. 05).
- 人民網. 2016. “《國家網絡空間安全戰略》全文.”<http://politics.people.com.cn/n1/2016/1227/c1001-28980829.html>(검색일 : 2023. 09. 05).
- 人民網. 2019. “解放軍有網絡戰部隊？國防部：毫無事實根據，純屬捏造.”<http://military.people.com.cn/n1/2019/1129/c1011-31481479.html>(검색일 : 2023. 09. 05).
- 王爱玲、达妮莎. 2020. “坚持‘网络主权’的中国声音及国际认同分析.”『大连理工大学学报(社会科学版)』41(06).
- 王清安. 2018. “中共網路戰攻擊手段與能力之研析.”『陸軍學術雙月刊』第五十四卷第562期(2018.12), 122.
- 项登. 2018. “全球网络空间军事化问题评析.”『信息安全与通信保密』(01).

- 新華網. 2017. “戰略支援部隊與地方9個單位合作培養新型作戰力量高端人才.” http://www.xinhuanet.com//politics/2017-07/12/c_1121308932.htm(검색일 : 2023. 09. 05).
- 新華網. 2024. “我國網民規模達10.92億人 互聯網普及率達77.5%.” <http://big5.news.cn/gate/big5/www.xinhuanet.com/20240325/a4a792347c274b2ba86a60d9e9e7ba1c/c.html>; 199IT. 2023. “We Are Social : 2023年全球數字報告.” https://www.199it.com/archives/1579981.html#google_vignette(검색일 : 2024. 03. 27).
- 肖天亮. 2017. 『戰略學』. 北京: 國防大學出版社. 403-405. 재인용: 박남태·백승조. 2021. “중국군 전략지원부대의 사이버전 능력이 한국에 주는 안보적 함의.” 『국방정책연구』 제131호. 150-151.
- 杨楠. 2020. “网络空间军事化及其国际政治影响.” 『外交评论(外交学院学报)』 37(03).
- 中國日報. 2016. “解讀國家網絡空間安全戰略規劃中的挑戰與任務.” https://china.chinadaily.com.cn/2016-12/29/content_27814398.htm(검색일 : 2023. 09. 05).
- 中華人民共和國國務院新聞辦公室. 2011. 『2010年中國的國防』. http://www.scio.gov.cn/zfbps/ndhf/2011n/202207/t20220704_130059.html(검색일 : 2023. 09. 05).
- 中華人民共和國國務院新聞辦公室. 2015. 『中國的軍事戰略』. http://www.scio.gov.cn/zfbps/ndhf/2015n/202207/t20220704_130108.html(검색일 : 2023. 09. 05).
- 中華人民共和國國務院新聞辦公室. 2019. 『新時代的中國國防』. http://www.scio.gov.cn/zfbps/ndhf/2019n/202207/t20220704_130617.html(검색일 : 2023. 09. 05).
- 中華人民共和國國防部. 2024. “國防部舉行信息支援部隊成立專題新聞發布會.” <http://www.mod.gov.cn/gfbw/xwfy/zjtzh/16302133.html>(검색일 : 2024. 04. 19).

- 中華人民共和國中央人民政府. 2016. “中華人民共和國網絡安全法.”https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm(검색일 : 2023. 09. 05).
- 中華人民共和國中央人民政府. 2016. “《國家網絡空間安全戰略》發布 提出捍衛網絡空間主權.”https://www.gov.cn/xinwen/2016-12/28/content_5153643.htm(검색일 : 2023. 09. 05).
- 朱鈺德、李建鵬. 2021. “中共戰略支援部隊功能發展與對我資訊戰影響之研究.”『陸軍學術雙月刊』第五十七卷第580期(2021.12). 74-76.

The Evolution of China's Cyber Security and Its Military Strategic Implications

Yang Jeong Hak | Korea Military Academy

In the 21st century, cyberspace has emerged as a critical component of national security, with China recognizing it as a new domain of national sovereignty and implementing a robust cyber security strategy. This paper analyzes the evolution of China's cyber security policies and their integration into military strategies. Guided by President Xi Jinping's 2014 concept of the "holistic approach to national security(總體國家安全觀)," China has elevated cyber security to a core element of its national security framework, formalized through the 2016 Cyber security Law(網絡安全法) and the National Cyber security Strategy(國家網絡空間安全戰略). These legal and policy frameworks are deeply intertwined with China's military strategies, reflecting efforts to secure dominance in cyberspace. The strategic linkage between cyber security and military objectives underscores China's intent to fortify its cyber capabilities and influence the global security landscape. This paper also explores the implications of China's cyber and military strategies for international security, emphasizing the need for neighboring countries to develop appropriate countermeasures.

Keyword China's Cyber Security, Military Strategy, Strategic Support Force, Cyberspace Force, Holistic Approach To National Security

* I would like to thank the anonymous judges for their valuable comments on improving the completeness of the paper.