중국의 사이버 안보외교와 글로벌 사이버 안보 질서의 진영화:

중국은 어떻게 사이버 공간 운명공동체를 만들어 가고 있는가?

2024

한국사이버안보학회
KACS

한국사이버안보학회 워킹페이퍼 23호
발간일: 2024년 8월 24일

차정미 (국회미래연구원)

Ⅰ. 서론 : 사이버 안보외교와 사이버 공간 운명공동체

2024년 5월 중국 중앙사이버안보정보화위원회 판공실(中央网络安全和信息化委员会办公室)과 중앙방송총국이 함께 제작한 정치다큐멘터리 〈인터넷 강국으로의 도약(阔步迈向网络强国)〉이 CCTV 황금시간대에 3일간 방영되었다. 총 5편으로 제작된 이 다큐의 마지막편인 제5편은 〈사이버 공간 운명공동체 공동 구축〉이었다. 시진핑의 사이버 공간 운명공동체 구축 이념을 소개하고, 중국의 지혜와 해결책을 제공하는 대국으로서의 책임을 보여줄 것임을 강조하였다(网信中国继续滑动看下一个轻触阅读原文, 2024/05/16). 사이버 공간이 안보와 경제 등 모든 측면에서 강대국 경쟁의 핵심 공간으로 부상하면서, 중국이 중국 방안을 통해 구축하고자 하는 글로벌 거버넌스, 글로벌 리더십의 비전인 인류운명공동체 담론이 사이버 공간으로 확대되고 있다.

중국은 세계일류 인터넷 강국을 목표로, 발전과 안보 이익의 동시 추구라는 틀 하에서 사이버 안보외교를 적극 전개해 가고 있다. 중국은 사이버 안보 외교를 통해 협력국가의 확대와 우호적인 대외 환경 구축, 중국 주도 혹은 적어도 중국에 유리한 글로벌 사이버 안보 거버넌스를 구축하는 한편 디지털 경제시대 중국기술과 중국산업의 경쟁력, 영향력을 제고하고자 하고 있다. 디지털 기술의 발전과 함께 사이버 안보는 점점 더 중요한 국가 안보의제가 되었고, 강대국 경쟁과 지정학 위기 속에서 사이버 공간은 점점 더 진영화되어 가고 있다. 사이버 안보는 국가간 전략 협력, 안보 협력의 핵심의제로 부상하였다. 한편, 사이버 안보는 컨설팅, 상품, 서비스 및 솔루션을 포함하는 거대한 산업으로, 지속 성장추세에 있다. 글로벌 사이버안보 시장은 연평균 성장률 10.5%로 2025년까지 2,480억 달러에 이를 것으로 예상된다(财闻网, 2023/08/07). 글로벌 사이버안보 교육 및 테스트 플랫폼의 매출은 2022년 약 1억 5,330만 달러, 2029년에는 3억 800만 달러에 이를 것으로 예상된다(环洋调研中心, 2023/04/27). 사이버안보 외교는 이러한 사이버 보안 시장 점유는 물론 데이터의 확보로 인한 기술우위의 추구라는 점에서 디지털 경쟁의 핵심 요소가 되고 있다. 이렇듯 사이버 안보 외교는 한편으로는 영향력 확대와 안보 이익 추구, 그리고 미래 디지털 경제 주도라는 발전이익 추구 차원에서 중국의 인터넷 강국화, 중화민족의 위대한 부흥을 위한 발전과 안보의 통합이라는 전략적 과제를 수행하는 데 주요한 축이 되고 있다.

이렇듯 사이버 안보가 미중간 글로벌 영향력 경쟁, 우호그룹 확대와 결집, 미래 경제네트워크 주도를 위한 주요 공간이면서 외교적 수단으로 부상하는 가운데 중국 사이버 안보를 외교적 관점에서 분석한 연구는 취약한 실정이다. 이에 본 연구는 어떻게 미중 경쟁 하에서 중국이 사이버 안보 외교를 글로벌 영향력 확대와 서구에 대항하는 우호그룹 구축의 중요 수단으로 적극 활

용하고 있는지를 분석한다.

중국은 안보와 발전의 이중 목표 하에 개발도상국, 비서구국들과의 전략적 연대, 물리적 결합을 추구하면서 사이버 공간 운명공동체 구축을 목표로 하고 있다. 본 연구는 중국의 사이버 안보외교를 '안보/가치규범외교'와 '인프라/기술외교'의 두 축으로 분석하고, 사이버 안보 운명공동체라는 중국 주도의 사이버 안보 거버넌스, 사이버 안보 블록 구축을 위한 중국의 사이버 안보 가치규범 외교와 사이버 안보 인프라 기술외교를 분석한다. 중국이 이를 통해 중국 주도 혹은 중국에 우호적인 글로벌 사이버 안보 거버넌스를 구축하는 것은 물론 중국의 사이버 안보 시장과 파트너의 확대, 이를 통한 중국의 네트워크 지배력, 디지털 경제 지배력을 제고하는 안보와 발전의 동시 추구 전략을 추구하고 있음을 보여준다. 결론에서 이러한 안보와 발전의 이중목적을 가진 중국의 전방위적 전면적 사이버 안보외교가 비서구 사이버 안보 블록 형성의 주요한 토대가 될 것으로 전망하고, 중국 주도의 비서구 사이버 안보 운명공동체 구축이 갖는 국제정치적 함의를 제시한다.

Ⅱ. 미중 전략경쟁과 중국의 사이버 안보 외교

1. 미중 전략경쟁과 중국의 사이버 공간 안보화

사이버 공간의 안보화에 있어 중국은 중국 특색의 인식과 방향을 설정하고 있다. 국내적으로는 사이버 공간의 사상 의식 수호, 즉 사회주의 가치와 공산당 영도 체제의 수호이고, 대외적으로는 서구의 대중국 비판과 압박에 대응하여 사이버 안보 협력망을 강화하고 중국에 우호적인 대외환경을 구축하면서 발전이익과 안보이익을 수호하는 것이다. 이러한 사이버 공간의 의식 수호와 우호적 대외관계 구축은 적극적 사이버 안보 외교의 주요한 배경이 되고 있다. 체제 안보와 중화민족의 위대한 부흥이라는 목표를 위해 사이버 공간의 가장 큰 위협은 체제에 대한 위협과 발전의 지체이고, 이러한 체제 위협과 발전 지체의 핵심 동력은 미국이 주도하는 사이버 안보 동맹 확대와 서구의 대중국 견제라고 할 수 있다.

중국 사이버 안보의 핵심 목표가 체제 안보라는 점에서 중국은 가치사상의 오염, 중국 방식에 대한 서구의 비판을 주요위협으로 인식한다. 따라서 사이버 안보의 가장 중요한 한 축은 의식형태, 가치사상의 수호이다. 웨이샤오원(魏晓文)과 장처(张策)는 '무엇을 통치할 것인가', 즉 사이버 안보 거버넌스의 중점 과제에 대해 '사이버 의식형태 안보(网络意识形态安全)'를 최우선으로 강조하고 있다. 기술발달에 따라 정보전달 주체가 다양화되고 모든 정보수신자가 정보소스, 정보발행자 역할을 하면서 인터넷 기업들은 빅데이터, 클라우드컴퓨팅, 인공지능 등 신기술을 통해 여론생태에 영향을 미칠 수 있는 능력을 갖게 되었, 전통 미디어의 쇠퇴로 주류 이념의 리더십과 전파력에 새로운 도전을 가져왔다는 것이다. 인터넷의 가상성과 익명성이 잘못된 이념의 온상이 되고 미국을 비롯한 서방 국가들이 인터넷을 이용해 중국에 대한 이데올로기 침투를 늘리고 부르주아 가치를 확산시키고 있어 역사적 허무주의, 자유주의 등 잘못된 사상조류와 각종 유언비어가 사이버 공간에 퍼져 정상적인 온라인 여론 생태계를 파괴하고 사회 안정을 위협하고 있다고 강조하였다. 이러한 의식과 사상의 위협 속에서 당과 국가의 미래 운명은 사상통치의 실효성과 밀접하게 연관되어 있다고 강조하고 있다(魏晓文, 张策, 2022 ; 14-15). 중국 사이버 안보의 핵심 목표는 이러한 사상 의식 안보, 보위 전쟁에서 반드시 승리하는 것이고 공산당 중앙이 사

이버 안보 전쟁의 영도적 핵심지위를 부여받고 있다. 시진핑 또한 사이버 안보 거버넌스의 다양한 주체 중에서 공산당이 영도의 핵심이고 인민이 주요 세력임을 강조한 바 있다(魏晓文, 张策, 2022: 14).

이러한 인식 하에 중국은 미국과 유럽 등 서구국가들이 중국을 디지털 권위주의로 규정하고 사이버 안보 동맹을 확대 강화하는 것을 주요 위협으로 인식한다. 중국은 미국과 유럽이 사이버 안보동맹, 인공지능 동맹 등 유사입장국간 소다자 협의체를 신설하고 확대하면서 기술적 독점과 사이버 패권을 추구하고, 사이버 공간의 국제질서를 진영화시키고 있다고 비판한다(人民论坛, 2024/05/17). 2023년 11월 세계인터넷대회 정상회의에서 시진핑은 사이버 공간 인류운명공동체 발전이 '새로운 단계'에 있다고 언급하였는데 그 새로운 단계의 핵심 배경은 지정학 경쟁이 사이버 공간으로 확대되고 있는 것이라고 할 수 있다. 사이버 공간과 디지털 기술 분야가 지정학 경쟁의 새로운 장으로 부상하면서 미국이 패권을 공고히 하기 위해 사이버 정책과 이념을 연계시키고 군사화를 적극 추진하고 있다고 비판했다. 동맹국의 사이버 전력과 자원을 활용하여 미국의 군사력을 전세계에 투사하면서 사이버 공간 안정을 해치고 있다는 것이다. 또한, 강대국간 지정학 경쟁으로 사이버 공간의 분열과 파편화가 심화되고 있으며, 인공지능 반도체 등 핵심 디지털 기술 산업재배치와 리쇼어링을 유도하고 동맹국 협력을 통해 표준 설정과 유사입장국 서클을 형성하고 다른 국가들을 배제하고 고립시키려고 한다고 비판했다(人民论坛网, 2024/05/16).

중국의 사이버 안보 외교는 미국의 사이버 패권주의, 서방의 '중국 위협론' 확산 등에 대응하고 서방의 사이버 안보담론에 대한 적극적 문제제기와 중국 주도 혹은 중국 우호 사이버 안보 질서 구축을 목표로 하고 있다. 또한, 비서구 국가들과의 디지털 인프라, 플랫폼 연계를 통해 중국 주도의 사이버 안보 인프라를 구축하고 이를 통한 발전의 이익을 추구한다. 최근 중국은 미국 등 서구의 중국 사이버 안보 위협론을 반박하고, 개발도상국, 비서구 국가들을 대상으로 한 양자 다자외교, 디지털 인프라 연결 등 사이버 안보 협력망 구축을 위한 적극적 사이버 안보외교를 전개해 가고 있다.

2. 사이버 공간 안보화 경쟁과 중국의 '서구 위협론' : "누가위협인가"의 담론 경쟁

미중 경쟁 하에서 미국 등 서구국가들이 중국을 사이버 안보 위협으로 규정하고 사이버 안보 동맹과 협력을 확대해 가는 환경 속에서, 중국은 이러한 서구의 중국 사이버 안보 위협론에 대응해 적극적으로 미국 등 서구의 사이버 공격 위험을 부각시키고 이를 적극 선전하고 있다. 중국은 체제 수호와 경제발전의 지속에 유리한 글로벌 사이버 안보 환경을 구축하기 위해 중국 위협론을 불식시키고 미국의 사이버 공격과 침투, 패권주의를 위협으로 부각시키고 있다.

미 국방부가 2023년 9월 발표한 '사이버 전략'에서 중국을 악의적인 사이버 행위자로 규정하는 등 중국 위협론을 확대해 가는 것에 대해, 중국은 미국이 중국의 기술 발전을 이념 및 정치체제와 직접적으로 연결하여 중국의 사회 정치 체제를 공격하고 약화시키려는 것이라고 비판하고 있다(环球时报, 2023/09/14). 중국은 미국이 오히려 전세계 사이버 공격의 주도자라고 비판하고, 미국이 동맹국과 파트너에 대해 무분별한 네트워크 공격을 하는 핵심 위협으로 비판하고, "파이브 아이즈(Five Eyes)" 등을 미국을 핵심으로 하는 글로벌 간첩 네트워크라고 비판하고 있다(人民日报, 2022/06/25). 중국 국가컴퓨터바이러스긴급대응센터와 치후360은 서북이공대학 사이버 공격 사건에 연루된 스파이웨어 기술 분석 결과 해당 소프트웨어가 미국국가안보국(NSA)

에서 개발된 것이고, 이 사이버 스파이 작전 배후에 있는 미국 보안국 직원의 정체를 확인했다고 밝혔다. 2020년 중국이 캡처한 4,200만 개 이상의 컴퓨터 악성 프로그램 중 미국이 해외 악성 프로그램 출처의 53.1%를 차지했다고 비판했다(中国日报网, 2023/09/16).

중국은 또한 미국의 사이버 활동 분석 보고를 통해 사이버 공간에서 '미국 위협론'을 적극 선전하고 있다. 치후360(360公司)은 몇 년간 미국 APT 조직과 그 활동을 계속 추적해 왔으며 미국 최고의 APT 조직이 전 세계 정부 기관, 중요 조직 및 정보 인프라를 대상으로 복잡하고 정교하며 지속적인 APT 공격을 수행했다는 사실을 발견했다고 밝혔다. 치후 360은 2024년 2월 '미국 관련 APT 분석보고(美相关APT组织分析报告)'를 발표하고, 미국 APT 조직의 구조, 공격 무기, 구현 프로세스 등을 확인했다고 밝히며 미국의 무차별적인 사이버 공격은 전 세계에 지속적 안보우려를 초래하고 있다고 강조했다(北晚在线, 2024/02/07). 치후 360의 보고서는 미국 해커조직 사우론(Sauron), 국가정보국(CIA), 국가안보국(NSA)이 배후인 APT 공격이 중국, 러시아, 이란, 스웨덴, 벨기에, 르완다 등을 포함한 30개 이상을 공격해 과학기술연구, 국방부, 정부부처 등 다양한 기관을 공격했다고 밝혔다. CIA는 간첩활동과 비밀활동을 계속하며 색깔혁명을 비밀리에 수행하고, 미국국가안보국(NSA)은 중국 기업, 정부, 대학, 과학연구기관 등 많은 양의 데이터를 훔쳐 잠재적 위협이 매우 크다고 밝히고 있다(北晚在线, 2024/02/07). 치후 360은 또한 미국사이버안보위협역량분석보고(美网络安全威胁能力分析报告)를 발표하여, 7가지 유형의 미국의 사이버안보 위협을 적시하고 사이버 패권을 비판했다(京报网, 2024/02/27).

중국 외교부 왕원빈(汪文斌) 대변인은 기자간담회에서 치후 360의 두 보고서에 주목하고 있다고 말하고, 미국 정부가 어떻게 헤게모니적이고 독점적인 지위를 이용해 사이버 공간에서 무모하게 행동하는지, 사이버 공간의 국제 규칙과 질서를 훼손하고, 사이버 공간의 평화와 안전을 위협하며, 중국을 포함한 모든 국가의 안전과 발전 이익에 해를 끼치는지를 보여주는 것이라고 비판했다. 왕원빈은 미국은 사이버 공격을 위해 첨단 무기를 개발, 확산시켜 세계의 중요한 인프라를 큰 위험에 빠뜨리고 있다고 비판하면서 미국은 사이버 공간 위험 문제에서 '모든 악의 근원(万恶之源)'이라고 할 수 있으며, 어느 나라도 미국의 사이버 공격 위협으로부터 안전할 수 없다고 강조했다(中工网, 2024/02/08). 이렇듯 중국은 미국을 글로벌 사이버 안보의 핵심위협으로 규정하면서 서구의 안보화 담론에 적극 대응하고 있다.

3. 사이버 공간 운명공동체 구축과 중국 사이버 안보외교의 특징 : 안보와 발전의 통합

2023년 7월 시진핑은 사이버 안보와 정보화 공작회의에서 "중국이 글로벌 인터넷 공간에서 발언권과 영향력이 증대하고 있고, 인터넷 강국 건설이 점점 더 새로운 단계에 진입하고 있다"고 강조하고 "사이버 공간 운명공동체 건설을 견지하여 사회주의 현대화 강국, 중화민족의 위대한 부흥에 기여해야 한다"고 강조하였다(金台资讯, 2023/07/28). 사이버 공간 운명공동체(网络空间命运共同体)는 2015년 제2차 세계인터넷대회에서 시진핑이 최초로 제기한 이념으로 사이버 공간은 인류공동의 활동공간이고 사이버 공간의 미래는 세계 각국이 함께 만들어 간다는 것이다(光明网, 2022/03/04). '사이버 공간 인류운명공동체' 이념은 중국이 책임 있는 사이버 강국으로서의 모습을 보여주고, 사이버 주권 원칙 하에 국제사회에서 광범위한 다층 사이버 공간 협력을 전개하는 주요한 담론이 되고 있다(金台资讯, 2023/07/28) 중국은 사이버 공간 운명공동체 건설이 중국 인터넷 강국건설의 주요한 구성부분이면서 전체 '인류운명공동체 건설'의 중요한 구성

요소라고 강조하고 있다.

중국 사이버 공간 운명공동체는 발전과 안보를 양대 축으로 하고 있다. 2022년 11월 발간한 '사이버공간 운명공동체 구축(携手构建网络空间命运共同体)' 백서에서 중국은 사이버 공간은 시진핑의 인류운명공동체의 중요한 부분이라고 강조하고, 발전과 안보를 공히 건설해야 한다고 강조하였다. 본 백서는 사이버 발전공동체, 사이버 안보 공동체(安全共同体) 건설을 주요한 과제로 제시하고 있다(中央网络安全和信息化委员会办公室, 2022/11/07) 중국의 사이버 안보 운명공동체는 전략적 외교적 이익과 경제적 이익을 동시에 추구하는 전략적 접근으로, 사이버 안보는 한편으로 글로벌 거버넌스, 규범 주도를 위한 외교수단으로 활용되면서, 또 한편으로는 사이버 안보 네트워크 인프라의 연결을 주도하면서 중국 기업의 시장과 이익을 극대화하는 상업외교의 주요한 수단이기도 한다.

2023년 11월 시진핑의 세계인터넷대회 정상회의 개막식 연설은 이러한 '발전'과 '안보' 이중목적의 사이버 안보 외교의 특징을 더욱 분명히 보여준다. 사이버 공간 운명공동체 구축을 위한 새로운 단계의 추진으로 제시된 '3대 구상(三大倡导)'은 첫째, 발전을 우선시하여 공동번영의 사이버 공간을 창출하는 것이고, 둘째 안전 공유로 평화안전의 사이버 공간 창출, 셋째, 문명간 상호이해 촉진으로 평등하고 포용적 사이버 공간을 창출하는 것이다(人民论坛网, 2024/05/16).

중국 시진핑 시대 안보관은 발전과 안보의 통합이다. 2016년 12월 정치국회의는 <국가안전공작 강화 의견(关于加强国家安全工作的意见)>을 발표하고 국내와 대외의 통합, 발전과 안전의 병행하는 중국 특색의 국가안보의 길을 강조하였다(姬文波, 2018: 39) 중국의 사이버 공간 운명공동체론과 사이버 안보 외교 또한 발전과 안보의 이중 목적 추구를 위한 가치규범 공유와 기술, 산업망 연결의 양대축으로 추진되고 있다. 사이버 공간의 미중 경쟁 심화와 함께 중국은 미국 위협론과 패권주의적 행위를 적극 부각시키면서 한편으로 미국과 다른 반패권, 평화와 공동번영 등을 내세운 중국 주도의 사이버 안보 협력과 글로벌 거버넌스 창출의 의지를 피력하고 있다. 시진핑 시대 중국은 또한 인터넷 대국에서 인터넷 강국으로의 목표를 명확히 하면서 자국의 인터넷 역량 뿐만 아니라 적극적으로 네트워크 인프라와 플랫폼을 연결하고 있다.

미중 경쟁 하에서 중국 사이버 안보외교의 핵심은 반서구, 비서구 진영의 그룹화와 우호화이다. 러시아, 이란 등 양자협력은 물론 상하이협력기구, 브릭스 등 비서구 다자체제를 통해 중국 주도의, 비서구 기반의 사이버 안보 협력 틀을 확대해 가고 있다. 중국과 러시아의 사이버 분야 협력과 관련하여 양국간 가장 중요한 합의의 포인트는 글로벌 패권과 잠재적으로 체제 전복의 의도를 가진 미국 주도의 패권질서, 서구 주도 '자유주의 질서'에 대한 불신이다(Broeders, Adamson, Creemers, 2019: 2). 이러한 인식 하에 중국 주도의 사이버 안보 규범 공유의 '유사입장그룹' 구축 외교를 강화하고 있다. 한편, 서구의 대중국 기술통제, 사이버 안보 공세 속에서 중국은 네트워크 인프라와 데이터 센터 등 구축을 통해 기술적 산업적 연결로 중국주도의 사이버 안보 공동체를 위한 물리적 결속을 강화하고 있다. 중국 사이버 안보 기술, 네트워크, 인재에 의존하는 지역 및 국가들을 확대하는 사이버 안보 외교가 사이버 공간에서 중국의 대서구 취약성과 의존성을 완화하는 중요한 수단이 되고 있다.

Ⅲ. 중국의 사이버 안보 가치규범 외교와 전략적 연대

1. 중국 주도의 사이버 안보 규범과 글로벌 거버넌스

중국은 중국 주도의 다양한 양자, 소다자, 다자체제를 통해 사이버 안보 가치규범과 사이버 안보 글로벌 거버넌스를 주도하기 위한 사이버 안보외교를 적극 추진해 가고 있다. 중국 '사이버공간 운명공동체 구축(携手构建网络空间命运共同体)' 백서는 사이버 공간의 발전과 안보, 책임과 이익 건설을 강조하고, 사이버 안보에 대한 협력을 심화하고 사이버 공간 거버넌스에 적극 참여할 것이라고 밝히고 있다(中央网络安全和信息化委员会办公室, 2022/11/07). 본 백서는 사이버 안보 협력 심화, 사이버 공간 거버넌스 적극 참여, 포괄적 글로벌 발전 촉진을 중요한 축으로 제시하고 있다.

이러한 사이버 안보 외교의 핵심은 중국식 방식, 중국 솔루션에 기반한 사이버 안보 공동체를 구축하는 것이다. 왕(Wang)은 중국의 디지털 일대일로가 디지털 분야에 대한 중국의 내러티브와 브랜딩을 구축하는 통로로 활용된다고 강조하고, 디지털 인프라 수출 차원을 넘어 글로벌 사이버 거버넌스에 대한 '중국솔루션'을 제공하는 규범적 요소가 강하다고 강조한다. 모든 국가가 자신의 인터넷 발전 경로와 거버넌스 모델을 선택할 권리가 있다고 강조하면서 서구의 침투와 서구의 간섭, 비판에 대항하는 '사이버 주권'이 그 핵심 요소가 되고 있다(Wang, 2024). 중국은 사이버 공간 운명공동체의 기본원칙으로 사이버 주권 존중을 최우선으로 내세우고 있으며, 이는 개발도상국 비서구국가들과의 사이버 안보협력의 주요한 담론이 되고 있다. 중국은 사이버 공간은 모든 주권 국가에 속하는 것으로, 세계 각국이 단결하여 사이버 공간에서 운명공동체를 구축하고 현재의 불공정한 사이버 공간의 패턴을 변화시키고 정의로운 국제 인터넷 환경을 공동으로 구축해야 한다고 강조하고 있다(中国日报网, 2023/09/16).

중국은 분열주의와 극단주의에 대한 공동 대응을 사이버 안보의 주요한 의제로 제시하면서 글로벌 협력을 주도해 가고 있다. 중국 사이버 공간 운명공동체 구축 백서는 사이버 테러(网络恐怖主义)를 핵심 어젠다로 개발도상국과의 협력을 강조하고 있다. 인터넷의 대중화로 인해 사이버 테러가 점차 국가 안보를 위협하는 새로운 문제로 부상하고 있다고 강조한다(汪晓风, 2017: 117). 테러리스트들은 인터넷을 사용하여 극단주의 사상을 퍼뜨리고 자금을 모으고 테러 조직의 구성원을 모집하는 등 인터넷을 중심으로 테러활동을 전개하는 사이버 테러리즘이 강화되고 있다는 것이다. 중국은 이러한 사이버 테러가 중국의 '일대일로' 구상에도 영향을 미칠 수 있다고 강조하고, 사이버 안보 운명공동체 수립에 있어 세계 다수 국가들이 직면하고 있는 사이버 테러의 의제를 중심으로 연대와 협력의 네트워크를 강화해 가고 있다(王道转, 2018: 87). 일대일로 사이버 안보 협력은 일대일로 국가들의 안보뿐만 아니라 중국의 통합과 안정의 차원에서 주요한 과제가 되고 있다.

2. 중국의 비서구, 글로벌 남반구 협력을 위한 사이버 안보 외교

중국의 사이버 안보외교는 미국, 서구의 사이버 공간 안보화에 대응하면서, 중국의 인식과 솔루션을 글로벌화하고 이를 기반으로 중국에 우호적인 사이버 안보 거버넌스를 구축하는데 목표를 두고 있다. 러시아, 이란 등과의 양자 협력은 물론 아프리카 등 비서구 지역, 그리고 글로벌 남반구 국가들과의 사이버 안보 협력을 강화하는 것은 서구의 일방주의에 대항하는 '우리(us)'를 만들고, 중국의 입장에 우호적인 "유사입장국(likeminded)"을 그룹화하면서 중화민족의 위대한 부흥이라는 목표를 실현해 가는 데 주요한 외교적 수단이 되고 있다.

중러 협력은 비서구, 반서구 사이버 안보 양자 외교의 핵심 축이라고 할 수 있다. 양국은 2015년 〈중러국제사이버안보분야 협력 협정(中华人民共和国政府和俄罗斯联邦政府关于在保障国

际信息安全领域合作协定)>을 체결하고, 국가주권원칙이 사이버 공간에 적용되어야 한다는 데 인식을 같이하고, 해커공격에 공동대응 할 것에 합의했다. 같은 해 10월 중러 양국은 상하이협력기구 차원에서 '샤먼 2015(厦门—2015)' 사이버 테러 대응 훈련을 실시했다(高望来, 2017: 70-71). 중러 양국은 2022년 2월 정상회담 공동성명에서 유엔 등 국제기구의 사이버안보 논의에 한목소리를 내며 협력할 것을 강조하고, 국가사이버 주권을 침해하는 어떠한 시도에도 반대하며 국제통신연합(ITU)이 이 문제 해결에 적극적 역할을 하도록 촉진할 것이라고 강조하였다(新华社, 2022/02/05). 중러 사이버 안보 협력은 인공지능 규범과 글로벌 다자협력으로 점차 확대되고 있다. 2024년 5월 정상회담 공동선언문에서 양자간의 사이버 안보, 데이터 안보 등 협력을 강화하는 것은 인공지능 분야 사이버 안보 위험에 대한 협력을 강화하기로 하였다. 또한, 글로벌 다자 메커니즘에서 정보안보 협력을 강화하고 유엔, 국제전기통신연합(ITU), 브릭스, 상하이협력기구, 국제표준화 기구 등 글로벌 인터넷 거버넌스에서의 인공지능 교류협력도 언급하고 있다(央视新闻客户端, 2024/05/16).

상하이 협력기구(SCO)는 중국의 사이버 안보 다자외교의 중요한 축으로, 중국 사이버 안보 외교의 주요한 출발점이었다. 덩하오(邓浩)와 리텐이(李天毅)는 사이버 안보가 상하이협력기구 안보 협력의 신흥이슈이자 새로운 출발점이며, 지역 안보와 안정을 유지하는 데 점점 더 중요한 요소가 되고 있다고 강조한다(邓浩, 李天毅, 2021). 상하이협력기구 사무차장 로그비노프(Logvinov)는 사이버안보를 보장하고 사이버 위협에 맞서 싸우는 것이 SCO 의제의 핵심 문제 중 하나라고 강조했다(俄罗斯卫星通讯社, 2023/07/10). 2006년 중국은 SCO국가들과 함께 <국제정보안전성명(关于国际信息安全的声明)>을 발표하였고, 2009년에는 <국제정보안전보장 정부간협력협정(保障国际信息安全政府间合作协定)>을 체결하였다(汪晓风, 2016: 129). 2006년 SCO는 회원국간 국제사이버안보전문가그룹을 구성하여, SCO 프레임워크 내에서 국제사이버안보 실행계획을 수립하고 국제사이버안보문제를 종합적으로 해결하기 위한 다양한 방향과 방법을 명확히 하기로 하였다. 상하이협력기구의 상설기구인 대테러조직은 사이버안보협력을 핵심 축으로 하고 있으며, 2016년부터 2017년까지 회원국들은 10만 개 이상의 웹사이트를 차단하고 400만 개 이상의 웹사이트를 압수했다고 밝혔다(邓浩, 李天毅, 2021). 중국은 상하이협력기구의 사이버안보 협력을 일대일로 틀에 적용할 수 있는 주요한 사례로 인식하고 있다(汪晓风, 2016: 129).

브릭스(BRICS) 또한 중국 주도 사이버 안보 외교의 주요한 다자외교체이다. 브릭스 국가들은 2013년 스노든 사건 이후 사이버 안보 협력 추진을 본격화하였다. 사이버안보 이슈는 같은 해 브릭스 정상회의 선언문에 처음 포함되었고, '국제협력 강화 및 사이버 범죄 퇴치 결의안'을 통해 유엔에 사이버 문제에 대한 대응을 촉진할 것을 공동으로 요구하였다(高望来, 2017: 70). 2014년 브릭스 국가들은 테러리스트의 정보 통신 기술, 특히 인터넷과 기타 미디어의 사용에 대해 "깊은 우려"를 표명하면서, 2015년 회의에서 정보통신기술 협력 실무그룹을 설립하기로 하고, 2016년 브릭스 통신장관회의에서는 '디지털 파트너십 구축' 목표를 제안했다(高望来, 2017: 67). 브릭스 안보 문제 수석 자문 회의에서는 사이버 범죄 퇴치를 위한 정보 및 경험 공유, 기술 기관과 법 집행 기관 간의 협력 강화, 공동 사이버 보안 연구 개발 및 역량 구축 촉진 등 사이버 안보 협력 조치가 구체화되었다(高望来, 2017: 63-64, 68). 브릭스 국가들은 국제규칙 제정과정에 신흥시장, 개발도상국의 요구와 관심을 적극 표현하고, 글로벌 사이버 공간 거버넌스를 공동으로 추진해 가기로 하였다(高望来, 2017: 63-64). 2017년 중국 샤먼에서 개최된 9차 정상회의에서 '브릭스 사이버 안보 실무협력 로드맵(金砖国家网络安全务实合作路线图)'가 채택되었고, 브릭스 사이버안보실무그룹회의가 매해 개최되고 있다. 실무그룹은 중국외교부사이버업무조정관(网络事务协调员) 왕레이(王磊), 브라질 외교부 전략국장, 국방군축국장, 인도 외교부 신흥전

략과학기술처와 사이버외교처 공동서기, 러시아 외교부 국제사이버안보처 부처장, 남아공 국가안보국 국가연락처장 등이 참석한다(中华人民共和国外交部, , 2022/05/24). 2023년 8월 브릭스 정상선언에서도 사이버 안보는 주요한 의제로 제기되었다. 브릭스 국가간 사이버 안보 협력은 '브릭스 사이버 안보 실무협력 로드맵(金砖国家网络安全务实合作路线图)'의 이행과 사이버안보 실무그룹의 활동을 통해 지속적으로 촉진되어야 한다고 강조했다(中国日报网, 2023/08/25).

3. 중국 일대일로 협력, 1+X 외교를 위한 사이버 안보 외교

중국은 2019년 '일대일로 사이버 안보 정상포럼(一带一路网络安全高峰论)'을 베이징에서 개최한 바 있고(同花顺财经, 2019/11/12), 2021년 4월 중국은 제4차 디지털 중국 건설 정상회의에서 일대일로 연선 국가와 지역 사이버안보 수호를 위해 '일대일로 사이버안보 연구원("一带一路"网络空间安全研究院)'을 정식 설립했다(哈尔滨工业大学网络空间安全学院, 2021/04/26). 중국은 사이버 테러 조직이 일대일로 건설을 방해하거나 여론에 악영향을 미칠 수 있다고 인식한다. 안샤오밍(安晓明 2022: 130)은 '일대일로' 국제협력 포럼, 세계인터넷회의 등을 적극 활용하여 사이버 안보와 디지털 거버넌스에 대화를 모색하고 일대일로 사이버 안보협력을 강화해야 한다고 강조한다. 사이버 안보 전문가 연합을 형성하여 정기적인 의사소통과 대화를 진행 데이터 보안과 정보 보호 메커니즘의 구축 필요성을 제기했다.

중국은 2021년 "중-아프리카 사이버공간 운명공동체구상(中非携手构建网络空间命运共同体倡议)"을 제기하고, 중요한 정보인프라 보호를 위해 정보공유, 조기 경보 및 예방, 비상대응 등 협력을 강화하기로 했다. 또한 유엔인터넷거버넌스포럼(IGF), 국제전기통신연합(ITU) 등 글로벌 거버넌스 체계를 개선하기 위해 중국과 아프리카가 더 적극적 역할을 할 수 있도록 협력 확대를 제안했다(中国网信网, 2021/08/25). 2021년 3월에는 중국외교부와 아랍연맹사무국이 데이터안보 화상회의를 개최하고 '중국-아랍 데이터안보협력구상(中阿数据安全合作倡议)'을 발표했다(中华人民共和国外交部, 2021/03/29). 중앙아시아 5국과도 2022년 6월 "중국+중앙아5국 데이터 안보협력구상("中国＋中亚五国"数据安全合作倡议)"을 발표했다(中华人民共和国外交部, 2022/06/08).

이러한 중국 사이버 안보 외교의 핵심은 각 국의 정치체제와 사회안정을 위협하는 사이버 위협에 대한 공동대응과 기술협력에 있다. 가오왕라이(高望来)는 브릭스 사이버안보협력이 개발도상국이 글로벌 사이버 거버넌스에서의 발언권을 확대하고 사이버 공간의 새로운 글로벌 질서를 구축하는데 심대한 의의를 지닌다고 강조하였다(高望来, 2017: 66-67). 자오루치(赵瑞琦) 또한 기술패권이 기술주권에 도전할 수 없다는 인터넷 발전 이념에 근거하여, 사이버 안보에 대한 새로운 주류논술을 구축해야 한다고 강조하였다(赵瑞琦, 2017: 105). 이렇듯 중국 주도의 사이버 안보외교는 글로벌 사이버 안보 거버넌스에서 중국과 개발도상국의 발언권을 확대하고 서구에 대응하는 대안적 사이버 안보 담론 구성을 주요한 목표로 하고 있다.

Ⅳ. 중국 사이버 안보 기술/인프라외교 : 사이버 공간의 물리적 결합

중국 '사이버공간 운명공동체 구축(携手构建网络空间命运共同体)' 백서는 사이버 공간의 발전

과 안보, 책임과 이익 건설을 강조하면서 디지털 경제협력의 지속 확대, 포괄적 글로벌 발전 촉진을 중요한 축으로 제시하고 있다. 백서는 사이버 안보 규범 뿐만 아니라 사이버 공간 기술발전 또한 중요한 부분으로 강조하고 있다(中央网络安全和信息化委员会办公室, 2022/11/07). 협력국들과의 디지털 연계를 확대하면서 중국의 기술적 산업적 우위를 지속 도모하고자 하는 것이다. 결국 우호적 대외환경 구축이라는 외교안보적 목표와 중국 기술과 산업의 글로벌화를 촉진하는 발전이 모두 사이버 공간 운명공동체의 주요한 목표라고 할 수 있다. 중국은 네트워크 인프라 구축과 데이터 센터 신설 등을 포함한 중국의 사이버 안보 관련 기술과 산업, 사이버 안보 교육에 투자하고 수출하면서 사이버 안보 협력 국가 및 지역들을 기술적 산업적으로 연결하고 상호의존성을 강화하는 '물리적 결속'을 도모하는 사이버 안보외교를 적극 전개해 가고 있다. 이러한 물리적 결속은 한편으로는 사이버 안보 협력의 물적 토대이면서 한편으로는 디지털 경제 시대 지속 발전의 주요한 토대가 될 수 있다는 점에서 안보와 발전이라는 이중 목적에서 추진된다고 할 수 있다.

1. 중국의 반서구, 개발도상국 사이버안보 외교와 디지털 인프라 연결

중국은 2023년 7월 상하이협력기구 23차 정상회의는 〈디지털 전환 분야 협력 상하이협력기구 정상회의 성명(上海合作组织成员国元首理事会关于数字化转型领域合作的声明)〉을 발표, 디지털인프라 상호연결(互联互通)을 강화하고, 데이터 상호운용성을 제고하고, 금융 등 중점분야의 디지털해결 방안 통합을 강화할 것을 강조하고 이에 정보안전의 수요를 충족시키는 데 주력할 것이라고 밝혔다(中国新闻网, 2023/07/05). 중국은 이렇듯 디지털 인프라 협력과 사이버 안보 수요를 연결하면서 사이버 안보 인프라 연계를 통한 중국주도의 사이버 안보 협력진영을 물리적으로 구축해 가고 있다.

중러 양국이 2023년 6월 체결한 '중러 사이버안보 협력협정(中俄间信息安全合作协议)'에는 사이버 범죄 공동대응, 사이버 공격 및 위협 공동대응, 사이버 안보 기술연구 및 인터넷 관리 협력 강화 등이 포함되었다. 또한 양국 사이버 보안 기업은 기술연구개발과 시장협력을 약속하는 MOU를 체결했다. 2023년 중국 화웨이와 러시아 기업이 공동으로 "리야얼 사이버안보 협력실험실(雷亚尔网络安全联合实验室)"을 신설하고, 사이버 안보 기술 공동개발, 사이버 안보 솔루션 등 제공을 계획하고 있다. 2023년 중러 양국이 합작한 영화 〈반격(反击)〉에 사용된 국산위협정보기술은 중국의 사이버안보 기술의 수준과 실력을 보여주는 것으로 중러 양국 사이버안보기술 협력의 성과라고 할 수 있다(数据安全, 2023/06/29).

시걸(Segal)은 사이버 공간의 미래 경쟁의 핵심은 두 개의 기술—5G와 검열-이며, 화웨이 장비가 중국 외 지역에서 상업적으로 출시된 5G 네트워크의 3분의 2 가까운 점유율을 보이고 있으며, 5G 분야의 선두주자인 화웨이와 ZTE는 일대일로에 크게 기여하고 있다고 평가했다(Segal, 2020: 4). 브릭스 국가들은 정보 인프라 구축 강화 측면에서 주요한 공동전략 프로젝트로 브릭스 케이블을 구축해 가고 있다. BRICS 광케이블 프로젝트는 2013년 BRICS 정상회담에서 공식 승인되었으며, 2014년 초 착공해 총 길이 34,000km에 달한다. 브릭스 광케이블이 완성되면 브릭스 국가들은 남아프리카공화국을 비롯한 아프리카 22개국과 직접 연결돼 세계 인구의 절반과 직접 통신을 이루고 개발도상국 상호연결도 촉진하게 된다(高望来, 2017: 68). 2023년 9월 중국 선전에서 개최된 'BRICS 미래 인터넷 혁신 포럼'에서 장윈밍 공업정보화부 차관은 중국이 BRICS 및 BRICS+ 파트너와 정보통신 분야 실무협력을 심화해 사이버 위험 예방 및 대응 역량을 강화하고, 사이버 거버넌스 시스템 구축을 촉진하고자 한다고 강조하였다(人民网,

2023/09/05).

2. 중국의 디지털 실크로드와 일대일로 사이버 안보외교

중국의 '디지털 실크로드' 건설은 국경간 광케이블, 대륙간 해저 광케이블 등 통신 간선망 구축 공동 추진, 항공 및 위성 정보 채널 개선, 지역 국제 통신 연결성 향상, 정보 교류 및 협력 확대 등이 포함된다. 중국은 “디지털 실크로드”를 포함한 상호 연결 프로젝트가 완전한 안보가 보장되어야만 지속될 수 있다고 인식하고 있다(汪晓风, 2016: 123). 사이버 안보는 일대일로 발전, 디지털 일대일로 보장을 위한 주요한 요소로 강조되고 있다. 쉬부(徐步)는 디지털 시대에 일대일로 구상은 큰 활력을 얻어 중국은 연선국가들과 함께 사이버 공간에서 운명공동체 이념을 견지하고, 글로벌 안보구상(全球安全倡议)과 글로벌개발구상(全球发展倡议)을 함께 추진하여 일대일로 국가간 디지털 상호 연결을 촉진하고 디지털 안보 장벽을 구축해야 한다고 강조한다(徐步, 2023/05/09).

중국 정부는 일대일로 지역의 ‘혈맥(血脉经络)’을 열어가기 위해, 연선 국가들과 인터넷 발전 협력 강화 의지를 명확히 하고 있다(汪晓风, 2016: 125). 중국이 추구하는 디지털 일대일로는 연선국가간의 네트워크 연결을 강화하면서 더욱 사이버 안보 협력의 필요성을 제고하고 있다. 왕샤오펑(汪晓风)은 온라인 금융과 온라인 결제의 상호 연결은 '디지털 실크로드'의 중요한 부분이며 인터넷 인프라와 애플리케이션이 풍부할수록 온라인 금융 테러의 가능성이 높아지고 이를 감시하고 대응할 수 있는 요구도 높아진다고 강조하였다(汪晓风, 2016: 124). 중국 기업은 새로운 시장과 고객을 찾고 있으며, 중국은 경제적, 전략적, 정치적 목표를 위해 기업을 지원하고 있다. 중국은 인터넷 기업들에 대출을 지원할 뿐만 아니라 일대일로 국가들에게도 대출을 제공하고 있다. 중국 수출입은행이 중국-파키스탄 광케이블 프로젝트 85%의 자금을 지원했으며, 나이지리아에 화웨이가 구축하는 5G 네트워크 비용 전액을 지원했다. 메르카토르 연구소(Mercator Institute)는 중국이 케이블 및 통신 네트워크 분야에서 70억 달러의 대출과 투자를, 전자상거래 및 모바일 결제 시스템 분야에서 100억 달러 이상, 연구 및 데이터 센터 분야에서 더 많은 수익을 올린 것으로 추산하고 있다.

중국 디지털 실크로드는 전자상거래 등 디지털 플랫폼의 연계도 확대하고 있다. 2018년 중국 알리바바와 르완다 정부가 협력한 '키갈리(Kigali)', 2019년 이집트 기술회사가 협력한 ‘DTOD’ 등 전자상거래 플랫폼 공동 구축을 확대했다. 중국은 이러한 전자상거래 구축과 함께 텐센트, 앤트파이낸셜 등이 아프리카 기업과 중국-아프리카 모바일 결제 협력 시스템을 구축해 왔다. 이러한 중국-아프리카 전자상거래 협력은 이에 필요한 인재 양성 협력과 사이버 안보 협력과도 연계되고 있다(驻外之家, 2021/11/09). 일대일로 국가들의 디지털화, 지능화, 네트워크화의 연계는 사이버보안 회사들이 국제시장을 확장할 수 있는 새로운 기회를 제공하고 있다. 메이야피코(美亚柏科)는 일대일로 국가들에게 사이버보안 분야 전문훈련서비스를 제공하고, 우수기술상품을 홍보하고 있으며, 관안정보(观安信息)도 일대일로 연선국가에게 전문 보안훈련을 제공하며 매년 200명 이상이 훈련을 받았다(前瞻产业研究院, 2018/10/11). 이렇듯 중국은 일대일로 국가들과의 디지털 인프라 연계와 함께 사이버 안보 기술과 인재 등 복합적 측면에서 연결성을 높이면서 사이버 공간 운명공동체 구축의 목표를 추구해 가고 있다.

Ⅴ. 결론 : 중국 사이버 안보 운명공동체 구축의 국제정치적 함의

중국 체제 안보적 차원에서 사이버 안보는 중요한 외교적 수단이면서 미중 사이버 안보 경쟁 우위를 위한 중요한 전략적 공간이기도 하다. 중국은 사이버 안보위협이 주변국들이 직면한 공통 안보위협중 하나이고, 중국이 주변국외교의 주요한 어젠다로 사이버 안보를 포함시키는 것은 중국이 인터넷대국에서 인터넷 강국으로 가는 중요한 단계이자 운명공동체 건설을 위한 중요한 조치라고 강조한다.

중국의 국가안보에 있어 사이버 안보는 점점 더 그 중요성과 위상이 높아지고 있다. 시진핑이 2023년 5월 중국국가안전위원회에서 언급했듯 중국은 대외적으로 기회와 도전에 동시에 직면해 있다. 시진핑은 국가안전위원회 회의에서 '복잡하고 엄중한' 국가 안보 환경을 파악하고 국가안보 시스템의 현대화를 가속화할 것을 촉구했고, 위원회는 위험 모니터링, 조기 경보, 국가 안보에 대한 대중 커뮤니케이션 및 교육과 관련된 문서를 승인했다(Greitens, 2023/07/28). 2023년 4월 중국국가안전위원회 회의에서 시진핑은 정치안전을 잘 수호하고, 네트워크 데이터 인공지능 안보 관리체계 수준을 제고하고, 국가 안보 위험 감시 및 조기 경보 시스템 구축을 가속화하고, 국가 안보를 위한 법치 건설을 추진하고 국가 안보 교육을 강화한다고 강조했다. 그리고 회의에서 〈국가안보위험감시 조기경보시스템 구축 가속화 관련 의견(加快建设国家安全风险监测预警体系的意见)〉과 〈국가안보교육강화에 관한 의견(关于全面加强国家安全教育的意见)〉 등을 심의통과하였다(新华社, 2023/05/31). 중국의 사이버 안보 외교는 점증하는 대내외 도전에 직면한 시진핑 체제가 대내적 사이버 안보강화 조치와 대외적 사이버 안보 협력을 강화하면서 점점 더 확대강화될 것으로 전망된다.

이러한 인식 속에서 중국은 양자적, 다자적 사이버 안보 협력 외교를 적극 전개가면서 제도적 규범적 영향권을 확대강화해 가고 있다. 또한 중국은 사이버 안보기술기업들과 함께 사이버 안보 기술 협력외교와 인프라 구축 협력 외교를 추진하면서 중국과 기술적 물리적으로 연계된 사이버 안보 영향권을 구축해 가고 있다. 이러한 다양한 안보협력과 외교협력체제를 통한 전략과 가치규범 연계, 기술인프라를 통한 물리적 연계를 강화해 가고 있는 중국의 사이버 안보외교는 다음과 같은 국제정치적 함의를 지닌다.

첫째, 글로벌 사이버 안보 거버넌스를 둘러싼 경쟁과 균열, 보편가치 보편정의의 불확실성과 경쟁성이 제고될 것으로 전망된다. 중국은 '사이버 안보'가 미국이 중국을 비방하는 수단으로 사용되어 왔다고 비판해 왔다. 중국은 오히려 미국이 세계 최대 규모의 사이버 공격을 하는 국가라고 비판하고, 러시아 대러 사이버 공격의 71%가 미국에서 발생했다며 서방이 러시아를 사이버 안보 위협으로 묘사하는 것을 비판했다(Sina, 2020/08/16). 2023년 4월 러시아 외무부 국제정보보안국장 류크마노프(Artur Lyukmanov)는 중러 사이버 안보 협력 대화 채널이 운영되고 있고, 브릭스, 아세안, 상하이협력기구 등 다자차원에서도 협력하고 있다고 강조하고 중러 양국의 입장은 매우 가까우며 가장 중요한 것은 사이버 주권으로 내부문제에 간섭하지 않는 것이라고 덧붙였다(俄罗斯卫星通讯社, 2023/04/18). 이렇듯 중국의 양자, 다자차원의 사이버 안보 외교의 확대강화는 글로벌 사이버 안보 거버넌스 경쟁, 규범을 둘러싼 경쟁 심화로 이어질 수 있음을 보여주고 있다.

둘째, 사이버 안보 외교가 주요한 영향력 경쟁, 강대국경쟁의 자원으로 부상하고 있다. 중국은 사이버 안보 협력이 다른 분야에서의 협력으로 확대될 수 있는 토대가 된다고 인식하고 있다.

사이버 안보 기술을 제공하고, 사이버 안보협력 체제를 구축하는 것은 국가관계의 주요한 외교적 자원이 되고 있다.

셋째, 사이버 안보 기술, 역량 경쟁으로 확대되면서 진영화된 투자와 군비경쟁으로 이어질 수 있다. 쿼드는 '쿼드 사이버 챌린지'를 개최하는 등 사이버 사고 및 위협에 대한 지역적 역량과 회복력 강화에 협력을 강화하고 있으며, 소프트웨어 안전을 위한 쿼드공동원칙(Quad Joint Principles for Secure Software)과 핵심인프라 사이버 안보 쿼드 공동원칙(Quad Joint Principles for Cyber Security of Critical Infrastructure)등을 강화하고 사이버 위협에 공동 대응하고자 하고 있다(The White House, 2023/05/20) 이렇듯 미중간의 사이버 안보 경쟁은 사이버 공간의 진영화 추세를 강화할 것으로 전망된다.

넷째, 미래 전쟁의 양상 변화에 따라 사이버 안보 외교는 사이버 전에서의 중요한 협력망, 동맹망 구축에 영향을 미치는 요소로, 향후 강대국간 충돌, 진영 충돌시 사이버 동맹의 인프라로 작동할 수 있다. 2019년 제7차 사이버 안보회의에서 스미로노프(Smirnov) 러시아 국제사이버안보협회장은 사이버 전쟁 위협에 직면한 중러 양국이 사이버 안보 연맹을 맺어 협력을 강화하고 세계 사이버 안보와 평화를 유지해야 한다고 강조한 바 있다(通信世界网, 2019/09/05).

사이버 안보가 미중 전략경쟁의 핵심 공간으로 부상하고, 각자의 영향권을 확대하기 위한 외교전이 치열해 지면서 미래 글로벌 사이버 안보 거버넌스의 균열과 진영화 가능성, 그리고 이에 토대한 사이버 안보 위협 공동대응의 취약성이 높아지고 있다. 본 연구는 중국의 사이버 안보외교에 대한 분석을 통해 글로벌 사이버 안보 거버넌스의 진영화 가능성에 주목하고, 중장기적 거시적 관점의 한국 사이버 안보 외교 환경 분석과 전략 수립의 필요성을 제기한다.

〈참고문헌〉

Segal, Adam. “China’s Alternative Cyber Governance Regime,” Council on Foreign Relations, 2020.03.13. p.4. https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf (검색일: 2023.09.09.)

Broeders, D. W. J., Adamson, L., & Creemers, R. J. E. H. (2019). “A coalition of the unwilling? Chinese and Russian perspectives on cyberspace,” Leiden University. https://hdl.handle.net/1887/136465

Greitens, Sheena Chestnut. “Xi’s Security Obsession; Why China Is Digging In at Home and Asserting Itself Abroad,” Foreign Affairs, 2023.07.28.

The White House, “Quad Leaders’ Joint Statement,” 2023.05.20. https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/quad-leaders-joint-statement/ (검색일 : 2023.08.28.)

Zheng, Wang. “China’s Digital Silk Road (DSR) in Southeast Asia: Progress and Challenges,” 2024.01.23. https://fulcrum.sg/chinas-digital-silk-road-dsr-in-southeast-asia-progress-and-challenges/ (검색일: 2024.01.27.)

姬文波. “习近平国家安全思想的核心要义.”『党的文献』2018年第2期.

魏晓文. 张策, “习近平新时代网络安全治理观探析.”『中学政治教学参考』2022年第44期.

汪晓风. “网络恐怖主义与“一带一路”网络安全合作.”『国际展望』2016年第4期..

王道转. ““一带一路”下中国与东盟国家应对网络恐怖主义研究.”『网络安全』2018年第4期.

高望来. “金砖国家网络安全合作：进展与深化路径.”『国际问题研究』2017年第5期.

邓浩, 李天毅. “上合组织信息安全合作：进展、挑战与未来路径.”『中国信息安全』2021年第8期

安晓明. “一带一路”数字经济合作的进展、挑战与应对.”『区域经济评论』2022年第4期.

赵瑞琦. “金砖国家的“事上练”：网络安全与智库合作.”『公共外交季刊』2017年第2期.

张力. “数字时代的国际秩序前景与中国方案.”人民论坛. 2024.05.17. http://www.rmlt.com.cn/2024/0517/702936.shtml (검색일: 2024.05.19.)

李嘉宝. “美国是全球网络安全最大“病毒”.”人民日报, 2022.06.25. https://m.gmw.cn/baijia/2022-06/25/1303014515.html (검색일: 2023.09.16.)

林明惠. “构建网络空间命运共同体的中国方案.”光明网, 2022.03.04. https://www.gmw.cn/xueshu/2022-03/04/content_35563935.htm (검색일: 2023.09.16.)

徐 步. “徐步等：携手共推“一带一路”倡议下数字互联互通提质升级.”中国网信, 2023.05.09. https://baijiahao.baidu.com/s?id=1765398219977681705&wfr=spider&for=pc (검색일: 2023.08.18.)

财闻网. “全球市场将达2480亿美元, 网络安全面临着机遇与挑战.”2023.08.07. https://baijiahao.baidu.com/s?id=1773545605919510257&wfr=spider&for=pc (검색일: 2023.09.15.)

网信中国继续滑动看下一个轻触阅读原文. “第5集《共建网络空间命运共同体》即将推出.” 2024.05.16. https://www.thepaper.cn/newsDetail_forward_27402314 (검색일: 2024.05.19.)

环洋调研中心. “2023年全球市场网络安全实训演练测试平台总体规模、主要企业、主要地区、产品和应用细.” 2023.04.27. https://www.bilibili.com/read/cv23337167/ (검색일: 2023.09.16.)

人民论坛网. “【核心阅读】构建网络空间命运共同体发展新阶段“新”在哪.” 2024.05.16. https://mp.weixin.qq.com/s?__biz=MzI1ODczMjE0MQ==&mid=2247556759&idx=4&sn=db831db3515a2ff8c805aca7493c693f&chksm=ebe86098deb0149edf9cac2b36097b547ed0d6811967864150fed01e21c11dd737494d7704e8&scene=27 (검색일: 2024.05.19.)

环球时报. “美发布网络战略渲染“中国威胁”, 专家：为越来越明显的攻击性找借口,” 2023.09.14. https://news.dayoo.com/world/202309/14/139998_54573138.htm (검색일: 2023.09.17.)

中国日报网. “快评|抵制网络霸权主义, 共建网络空间命运共同体,” 2023.09.16. https://finance.sina.com.cn/jjxw/2023-09-16/doc-imzmwinh0616425.shtml (검색일: 2023.09.17.)

北晚在线. “《美相关APT组织分析报告》发布：网络攻击属于无差别攻击,” 2024.02.07. https://baijiahao.baidu.com/s?id=1790221178046440490&wfr=spider&for=pc (검색일: 2024.03.10.)

京报网. “美网络安全威胁能力分析报告, 揭示七种威胁,” 2024.02.27. https://baijiahao.baidu.com/s?id=1790222182280174371&wfr=spider&for=pc (검색일: 2024.03.10.)

中工网. “外交部：大量证据全方位揭露美政府在全球推进网络威慑战略,” 2024.02.08. https://baijiahao.baidu.com/s?id=1790299912181752813&wfr=spider&for=pc (검색일: 2024.03.10.)

金台资讯. “坚持推动构建网络空间命运共同体,” 2023.07.28. https://baijiahao.baidu.com/s?id=1772622724763493013&wfr=spider&for=pc (검색일: 2023.09.17.)

中央网络安全和信息化委员会办公室. “携手构建网络空间命运共同体,” 2022.11.07. http://www.cac.gov.cn/2022-11/07/c_1669457523014880.htm?eqid=b87bebe40008e1070000000264269b3b (검색일: 2023.09.16.)

新华社. “加快推进国家安全体系和能力现代化 以新安全格局保障新发展格局,” 2023.05.31. http://www.qdnwm.gov.cn/index.php/toutiao/3615.html (검색일: 2023.08.01.)

新华社. “中华人民共和国和俄罗斯联邦关于新时代国际关系和全球可持续发展的联合声明（全文）,” 2022.02.05. https://roll.sohu.com/a/520629145_119038 (검색일: 2023.09.12.)

央视新闻客户端. “中俄联合声明,” 2024.05.16. https://baijiahao.baidu.com/s?id=1799210604992962324&wfr=spider&for=pc (검색일: 2024.05.19.)

俄罗斯卫星通讯社. “上合组织称合作打击网络威胁很重要,” 2023.07.10.

https://baijiahao.baidu.com/s?id=1770998624265913524&wfr=spider&for=pc (검색일: 2023.09.10.)

“上海合作组织成员国元首关于国际信息安全的声明,”

俄罗斯卫星通讯社. “俄外交部：俄罗斯与中国在网络安全领域密切合作,” 2023.04.18. https://baijiahao.baidu.com/s?id=1763500469902366285&wfr=spider&for=pc (검색일: 2023.09.16.)

中华人民共和国外交部. “中方主持召开金砖国家网络安全工作组第八次会议,” 2022.05.24. http://brics2022.mfa.gov.cn/dtxw/202205/t20220527_10693333.html (검색일: 2023.09.16.)

中国日报网. “金砖国家领导人第十五次会晤约翰内斯堡宣言,” 2023.08.25. https://baijiahao.baidu.com/s?id=1775161009874750257&wfr=spider&for=pc (검색일: 2023.09.16.)

同花顺财经. “一带一路网络安全高峰论坛在北京举办,” 2019.11.12. https://baijiahao.baidu.com/s?id=1649982297959069292&wfr=spider&for=pc (검색일: 2023.09.16.)

哈尔滨工业大学网络空间安全学院. ““一带一路”网络空间安全研究院成立奇安信守护跨国企业网络安全,” 2021.04.26. http://cys.hit.edu.cn/info/1021/1173.htm (검색일: 2023.09.16.)

中国网信网. “中方发起“中非携手构建网络空间命运共同体倡议”” 2021.08.25. http://www.cac.gov.cn/2021-08/25/c_1631480920450053.htm (검색일: 2023.09.16.)

中华人民共和国外交部. “中阿数据安全合作倡议,” 2021.03.29. http://new.fmprc.gov.cn/wjb_673085/zzjg_673183/jks_674633/fywj_674643/202103/t20210329_9176279.shtml (검색일: 2023.09.17.)

中华人民共和国外交部. ““中国＋中亚五国”数据安全合作倡议,” 2022.06.08. https://www.mfa.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/fywj_674643/202206/t20220609_10700811.shtml (검색일: 2023.09.17.)

中国新闻网. “上合组织成员国元首理事会第二十三次会议发表两项声明,” 2023.07.05. https://baijiahao.baidu.com/s?id=1770543464371282519&wfr=spider&for=pc (검색일:2023.09.16.)

数据安全. “合作加强：中俄联手打造网络安全防护体系（中俄网络安全),” 2023.06.29. https://www.dbs724.com/413230.html (검색일: 2023.09.16.)

前瞻产业研究院. “抓住“一带一路”机遇 网络安全企业纷纷“走出去”” 2018.10.11. https://www.qianzhan.com/analyst/detail/220/181010-90c44c92.html (검색일: 2023.09.16.)

人民网. “2023金砖国家未来网络创新论坛在深圳召开,” 2023.09.05. https://baijiahao.baidu.com/s?id=1776157637848334877&wfr=spider&for=pc (검색일: 2023.09.16.)

驻外之家. “一带一路”背景下中国与非洲电子商务合作的现状、挑战及对策,” 2021.11.09. https://www.163.com/dy/article/GOCGVULR0528CJEP.html (검색일: 2023.09.16.)

Sina, “俄罗斯安全官员：全球75%的网络攻击来自美国，他们却反过来指责中俄,” 2020.08.16. https://cj.sina.com.cn/articles/view/1887344341/707e96d502000xohu (검색일: 2023.09.16.)
通信世界网, “俄罗斯网络安全专家：中俄两国应建立网络安全联盟,” 2019.09.05. https://topics.gmw.cn/2019-09/05/content_33138659.htm (검색일: 2023.09.16.)

이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.