

국가전략연구위원회 이슈브리핑 12호 (발간일: 2023.09.25.)

중국의 사이버 안보 외교와 글로벌 사이버 안보의 진영화: “중국은 어떻게 사이버 안보 운명공동체를 만들어 가고 있는가?”¹⁾

차정미 (국회미래연구원)

1. 서 론

시진핑 시대 중국은 인터넷 대국에서 인터넷 강국으로의 목표를 명확히 하면서 자국의 인터넷 역량 뿐만 아니라 중국 인터넷 인프라, 인터넷 정책, 인터넷 가치규범의 확산과 영향력 확대를 모색하고 있다. 2023년 7월 시진핑은 사이버 안보정보화 공작회의에서 “중국이 글로벌 인터넷 공간에서 발언권과 영향력이 증대하고 있고, 인터넷 강국 건설이 점점 더 새로운 단계에 진입하고 있다”고 강조하고 “사이버 공간운명공동체 건설을 견지하여 사회주의 현대화 강국, 중화민족의 위대한 부흥에 기여해야 한다”고 강조하였다.²⁾ 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.³⁾ 중국은 사이버 공간 운명공동체 건설이 중국 인터넷 강국건설의 주요

1) 이 글은 2023년 9월 20일 제4차 국가전략포럼에서 발표된 발표문을 수정보완한 것이다.

본 원고는 자료수집과 분석이 진행 중인 연구 중간 단계의 원고임을 말씀드립니다. 감사합니다.

2) 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.)

3) 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.

한 구성부분이면서 전체 '인류운명공동체 건설'의 중요한 구성요소라고 강조하고 있다.

중국 사이버 공간 운명공동체는 발전과 안보를 양 대 축으로 하고 있다. 중국은 2022년 11월 '사이버공간 운명공동체 구축(携手构建网络空间命运共同体)' 백서를 발간하고, 사이버 공간은 시진핑의 인류운명공동체의 중요한 부분으로 발전과 안보, 책임과 이익을 공히 건설해야 한다고 강조하였다. 본 백서는 사이버 발전공동체, 사이버 안보 공동체(安全共同体) 건설을 주요한 과제로 제시하고 있다.⁴⁾ 중국의 사이버 안보 운명공동체는 외교적 이익과 경제적 이익을 동시에 추구하는 전략적 접근으로, 사이버 안보를 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.

사이버 위협의 부상과 진화 등으로 사이버 안보는 점점 더 중요한 국가과제이면서 글로벌 어젠다가 되었고, 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.⁵⁾ 글로벌 사이버 안보 교육 및 테스트 플랫폼의 매출은 2022년 약 1억 5,330만 달러, 2029년에는 3억 800만 달러에 이를 것으로 예상된다.⁶⁾ 사이버안보 외교는 이러한 사이버 보안기술, 기업의 글로벌화로 시장점유율은 물론 경험과 데이터의 확대에 의한 기술역량의 지속 제고를 기대할 수 있다.

이렇듯 사이버 안보는 중국에게 우호적인 대외환경, 중국 주도 혹은 적어도 중국에 유리한 글로벌 사이버 안보 거버넌스를 구축하는 한편 디지털 경제시대 중국기술과 중국산업의 경쟁력, 영향력을 제고하기 위한 주요한 공간이 되고 있다. 중국은 이러한 발전과 안보의 이익 동시 추구라는 틀 하에 사이버 안보 외교를 적극적으로 전개해 가고 있다. '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.⁷⁾

본 연구는 중국의 사이버 안보 외교를 '거버넌스, 규범외교'와 '기술, 인프라외교'의 두 분야를 중심으로 고찰하고, 사이버 안보 운명공동체 구축을 기치로 중국 주도의 사이버 안보 협력망, 사이버 안보 거버넌스 구축을 위한 중국의 전방위적 전면적 사이버 안보 외교를

https://www.gmw.cn/xueshu/2022-03/04/content_35563935.htm (검색일: 2023.09.16.)

4) 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=b87bebe40008e10700000000264269b3b (검색일: 2023.09.16.)

5) 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.)

6) 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.)

7) 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.)

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 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.

2. 미중 전략경쟁 시대 중국 특색의 사이버 안보화와 사이버 안보 외교

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.

웨이샤오원(魏晓文)과 장처(张策)는 우선 '무엇을 통치할 것인가', 즉 사이버 안보 거버넌스의 중점 과제에 대해 '사이버 의식형태 안보(网络意识形态安全)' 공고화를 최우선으로 강조하고 있다. 기술발달에 따라 정보전달 주체가 다양화되고 모든 정보수신자가 정보소스, 정보 발행자 역할을 하면서 인터넷 기업들은 빅데이터, 클라우드컴퓨팅, 인공지능 등 신기술을 통해 여론생태에 영향을 미칠 수 있는 능력을 갖게 됐고, 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 유연비어가 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.⁸⁾

이렇듯 중국 사이버 안보 거버넌스의 핵심 중점은 의식 형태, 가치사상의 수호이다. 중국 사이버 안보의 핵심 목표는 이러한 사상 의식 안보 보위 전쟁에서 반드시 승리하는 것이고 공산당 중앙이 사이버 안보 전쟁의 영도적 핵심지위를 부여받고 있다. 시진핑 또한 사이버 안보 거버넌스의 다양한 주체 중에서 공산당이 영도의 핵심이고 인민이 주요 세력임을 강조한 바 있다.⁹⁾ 중국 체제 안보적 차원에서 사이버 안보는 중요한 외교적 수단이면서 미중 사이버 안보 경쟁 우위를 위한 중요한 전략적 공간이기도 하다. 중국은 사이버 안보위협

⁸⁾ 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 (44), pp. 14-15

⁹⁾ 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 (44), p. 14.

이 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 사이버 안보 외교는 미국의 사이버 패권주의, 서방 주도의 중국, 러시아 등의 사이버 안보 위협론 확산 등에 대응하고 미국 등 서방의 사이버 안보담론에 대한 적극적 문제제기와 질서 재편의 의미를 지니고 있다. 최근 중국은 미국 등 서구의 중국 사이버 안보 위협론을 반박하고, 개발도상국, 비서구 사이버 안보 협력망 구축을 위한 적극적 사이버 안보외교를 전개해 가고 있다.

중국 시진핑 시대 안보관은 발전과 안보의 통합이다. 2016년 12월 정치국 회의는 <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.¹⁰⁾ 시진핑은 사이버안보와 정보화는 양날개로 강조하고, 사이버 발전을 통해 안전을 촉진하고 지속안정의 추세 속에서 성장이 가능하다는 사이버 안보와 발전의 통솔을 강조하였다.¹¹⁾ 중국의 디지털 일대일로 건설에 있어 사이버 안보는 이러한 발전과 안보의 연계를 분명히 보여주고 있다. '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. 이러한 "디지털 실크로드"를 포함한 상호 연결 프로젝트는 완전한 안보가 보장되어야만 지속될 수 있다는 것이다.¹²⁾

3. 중국의 사이버 안보 규범, 거버넌스 외교

중국은 중국 주도의 소다자, 다자체제에서 사이버 안보 협력과 가치규범의 공동체를 구축해 가고 있다.

상하이 협력기구(SCO) 사이버안보협력

중국의 사이버 안보외교는 상하이협력기구 차원의 협력이 주요한 출발점이었다. 덩하오(邓浩)와 리텐이(李天毅)는 사이버안보 협력은 상하이협력기구(SCO, Shanghai Cooperation Organization) 안보 협력의 싹이슈이자 새로운 출발점이며, 지역 안보와 안정을 유지하는데 점점 더 중요한 요소가 되고 있다고 강조한다.¹³⁾ 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.¹⁴⁾ 2006년 SCO는 회원국간

10) 姬文波, "习近平国家安全思想的核心要义," 『党的文献』 2018 (2), p. 39.

11) 姬文波, "习近平国家安全思想的核心要义," 『党的文献』 2018 (2), p. 43.

12) 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, p. 123.

13) 邓浩, 李天毅(2021), "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

14) 汪晓风(2016), "网络恐怖主义与'一带一路' 网络安全合作," 『国际展望』 2016 (4), p. 129.

국제 사이버 안보 전문가그룹을 구성하여, SCO 프레임워크 내에서 국제사이버안보 실행계획을 수립하고 국제 사이버 안보문제를 종합적으로 해결하기 위한 다양한 방향과 방법을 명확히 하기로 하였다.¹⁵⁾

브릭스(BRICS) 사이버안보협력

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 것으로 공동으로 요구하였다.¹⁶⁾ 2014년 브릭스 국가들은 테러리스트의 정보 통신 기술, 특히 인터넷과 기타 미디어의 사용에 대해 "깊은 우려"를 표명하고, 2015년 회의에서 정보통신기술 협력 실무그룹을 설립하기로 하고, 2016년 브릭스 통신장관회의에서는 '디지털 파트너십 구축'이라는 공동 목표를 제안했다.¹⁷⁾ 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 사이버안보 실무그룹회의가 매해 개최되고 있다.¹⁸⁾

중러 사이버안보 협력

중러 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.¹⁹⁾ 중러 양국은 2023년 6월 사이버 안보 분야 협력 초점과 영역을 구체화한 '중러 사이버안보 협력협정(中俄间信息安全合作协议)'을 체결했다. 사이버 범죄 공동대응, 사이버 공격 및 위협 공동대응, 사이버 안보 기술연구 및 인터넷 관리 협력 강화 등이 포함되었다.²⁰⁾

일대일로 사이버안보 협력

중국은 사이버 테러조직이 일대일로 건설을 방해하거나 여론에 악영향을 미칠 수 있다고 인식한다. 안샤오밍(安晓明)은 '일대일로' 국제협력 포럼, 세계인터넷회의 등을 적극 활용하여 사이버안보와 디지털 거버넌스에 대화를 모색하고 일대일로 사이버 안보협력을 강화해

15) "上海合作组织成员国元首关于国际信息安全的声明,"

16) 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, p. 70.

17) 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, p. 67.

18) 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.)

19) 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, pp.70-71.

20) 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.)

야 한다고 강조한다. 사이버 안보 전문가 연합을 형성하여 정기적인 의사소통과 대화를 진행 데이터 보안과 정보 보호 메커니즘의 구축 필요성을 제기했다.²¹⁾ 중국은 2019년 '일대일로 사이버안보정상포럼(一帶一路网络安全高峰论坛)'을 베이징에서 개최한 바 있고,²²⁾ 2021년 4월 중국은 제4차 디지털 중국 건설 정상회의에서 일대일로 연선국가와 지역 사이버안보 수호를 위해 '일대일로 사이버안보연구원(“一帶一路”网络空间安全研究院)'을 정식 설립했다.²³⁾

1+X 메커니즘을 통한 개발도상국 사이버안보 협력

중국은 2021년 “중-아프리카 사이버공산 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, 비상 대응 등 협력을 강화하기로 했다.²⁴⁾ 2021년 3월에는 중국외교부와 아랍연맹사무국이 데이터안보 화상회의를 개최하고 '중국-아랍 데이터안보협구상(中阿数据安全合作倡议)'을 발표했다.²⁵⁾ 중앙아시아 5국과도 2022년 6월 “중국+중앙아5국 데이터 안보협력구상(“中国+中亚五国”数据安全合作倡议)”을 발표했다.²⁶⁾

이러한 중국의 개발도상 지역 사이버 안보 외교의 핵심은 각국의 정치체제와 사회안정을 위협하는 사이버 위협에 대한 공동대응과 기술협력에 있다. 중국 주도의 사이버 안보외교는 글로벌 사이버 안보 거버넌스에서 중국과 개발도상국의 발언권을 확대하고 서구에 대응하는 대안적 사이버 안보 담론 구성을 주요한 목표로 하고 있다.

4. 중국의 사이버 안보 기술/인프라외교

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)> 발표하고, 디지털 인프라 상호연결(互联互通)을 강화하고, 데이터 상호운용성을 제고하고, 금융

21) 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, p.130.

22) 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.)

23) 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.)

24) 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.)

25) 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.)

26) 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.)

등 중점분야의 디지털해결 방안 통합을 강화할 것을 강조하고 이에 정보안전의 수요를 충족시키는 데 주력할 것이라고 밝혔다.²⁷⁾

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.²⁸⁾

중국은 이러한 광통신망 뿐만 아니라 전자상거래 등 디지털 플랫폼의 연계도 확대하고 있다. 2018년 중국 알리바바와 르완다 정부가 협력한 '키갈리(Kigali)', 2019년 이집트 기술회사가 협력한 전자상거래 플랫폼 공동 구축을 확대했다. 중국은 이러한 전자상거래 구축과 함께 텐센트, 엔트파이낸셜 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.²⁹⁾

중국 정부는 일대일로 지역의 '혈맥(血脉经络)'을 열어가기 위해, 연선 국가들과 인터넷 발전 협력 강화 의지를 명확히 하고 있다.³⁰⁾ 중국이 추구하는 디지털일대일로는 연선국가간의 네트워크 연결을 강화하면서 더욱 사이버 안보 협력의 필요성을 제고하고 있다. 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 200명이상이 훈련을 받았다.³¹⁾

중국 기업은 새로운 시장과 고객을 찾고 있으며, 중국은 경제적, 전략적, 정치적 목표를 위해 기업을 지원하고 있다. 중국은 이렇듯 디지털 인프라 협력과 사이버 안보 수요를 연결하면서 사이버 안보 인프라 연계를 통한 중국 주도의 사이버 안보 협력진영을 물리적으로 구축해 가고 있다.

5. 결론 : 중국 사이버 안보 운명공동체 구축의 국제정치적 함의

중국의 국가안보에 있어 사이버 안보는 점점 더 그 중요성과 위상이 높아지고 있다.

27) 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.)

28) 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, p. 68.

29) 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.)

30) 汪晓风(2016), "网络恐怖主义与"一带一路"网络安全合作," 『国际展望』 2016 (4), p. 125.

31) 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.)

시진핑은 2023년 5월 중국국가안전위원회에서 언급했듯 중국은 대외적으로 기회와 도전에 동시에 직면해 있다. 시진핑은 국가안전위원회 회의에서 '복잡하고 엄중한' 국가 안보 환경을 파악하고 국가 안보 시스템의 현대화를 가속화할 것을 촉구했고, 위원회는 위험 모니터링, 조기 경보, 국가 안보에 대한 대중 커뮤니케이션 및 교육과 관련된 문서를 승인했다.³²⁾ 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.³³⁾ 중국의 사이버 안보 외교는 점증하는 대내외 도전에 직면한 시진핑 체제가 대내적 사이버 안보강화 조치와 대외적 사이버 안보 협력을 강화하면서 점점 더 확대 강화될 것으로 전망된다.

이러한 인식 속에서 중국은 양자적, 다자적 사이버 안보 협력 외교를 적극 전개하면서 제도적 규범적 영향권을 확대강화해 가고 있다. 또한 중국은 사이버 안보기술기업들과 함께 사이버 안보기술 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 안보 외교는 다음의 국제정치적 함의를 지닌다.

첫째, 글로벌 사이버 안보 거버넌스와 규범을 둘러싼 경쟁과 균열을 제고할 것으로 전망된다. 둘째, 사이버 안보 외교가 영향력 경쟁, 강대국 경쟁의 자원으로 지속 활용되면서 이러한 추세를 더욱 가속화할 수 있다. 셋째, 사이버 안보 기술, 역량 경쟁으로 확대되면서 진영화된 투자와 군비경쟁으로 이어질 수 있다. 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. 다섯째, 이러한 추세는 미래 글로벌 사이버 안보 거버넌스의 진영화로 이어질 수 있다.

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 공동 대응의 취약성이 높아지고 있다. 본 연구는 중국의 사이버 안보외교를 통해 글로벌 사이버 안보 거버넌스의 진영화 가능성에 주목하고, 중장기적 거시적 관점의 한국 사이버 안보 외교 환경 분석과 전략 수립의 필요성을 제기한다.

※ 이슈브리핑에 수록된 내용은 필자 개인의 의견이며, 한국사이버안보학회의 공식적인 입장이 아님을 알려드립니다.

³²⁾ Sheena Chestnut Greitens, "Xi's Security Obsession; Why China Is Digging In at Home and Asserting Itself Abroad," *Foreign Affairs*, 2023.07.28.

³³⁾ 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.)