주변4망(網)과 한국의 사이버 국제관계

2024

한국사이버안보학회
KACS

한국사이버안보학회 워킹페이퍼 14호
발간일: 2024년 8월 20일

김상배 (서울대학교)

Ⅰ. 머리말

사이버 안보는 이제 국가전략의 핵심 사안이 되었다. '정보보호'나 '시스템보안'의 기술·공학 시각뿐만 아니라 전통적으로 '국가안보'를 다루어 온 국제정치학 시각에서도 그러하다. 사이버 보가 글로벌 패권을 다투는 미중 갈등의 주요 쟁점이 된 지는 이미 오래됐다. 최근 발발한 러시아-우크라이나 전쟁에서 사이버전(戰)은 물리적 전쟁의 한 축을 담당하는 양상을 드러냈다. 대만해협의 위기 시마다 중국의 사이버 공격은 큰 변수로 거론되고, 북한의 핵·미사일 행보의 이면에는 해킹 공격을 통해서 벌어들인 자금이 있다. 그야말로 사이버 안보는 전통적으로 한반도의 외교안보 의제를 구성했던 미·일·중·러 네 강대국의 국제관계 속에서 고민해할 국가전략의 논제가 되었다.

그러나 사이버 안보의 국제정치를 '주변4강(强)'이 부국강병을 추구하며 '세력균형(balance of powers)'의 지정학적 시소게임을 벌이는 기존 국제정치학의 비유로만 담아낼 수는 없다. 일국 차원에서 사이버 안보 역량을 강화하고 이를 바탕으로 공격과 방어의 밀고 당기기에서 승리하는 것은 물론 중요하다. 그러나 사이버 안보의 지정학은 이러한 '단순지정학'이 아니라 영토 공간을 초월하는 다양한 변수들이 복잡하게 연루된 '복합지정학'의 성격을 지닌다. 또한 사이버 안보는 일국 차원의 역량과 전략 이외에도 이들 국가가 형성하는 양자-삼자-소다자-다자 등 국제관계의 다층적 네트워크, 즉 '세력망(network of powers)' 속에서 풀어가야 할 문제가 되었다. 이러한 와중에 네트워크의 빈틈을 공략하고 전략적으로 입지를 굳히면서 주변국들과의 관계를 유리하게 활용해야 할 문제가 되었다. 이러한 문제의식을 바탕으로 '주변4강' 대신에 '주변4망(網)'이라는 용어를 제안해 본다.

사이버 안보는 전통안보와 그 속성이 다르다는 점도 잊지 말아야 한다. 사이버 안보는 미시적 차원의 '안전' 문제가 집단의 '보안' 문제를 거쳐서, 가장 거시적인 차원에서는 국가의 '안보'까지도 거론케 하는 '신흥안보(emerging security)' 문제의 대표적 사례다. 따라서 전통안보 분야에서 주로 동원되던 '단순 방어'의 대책만으로는 부족하고, '예방-치료-복원'의 좀 더 복합적인 거버넌스의 메커니즘이 요구된다. 참여 주체라는 점에서도 복합위협의 성격을 가진 사이버 안보는 국가 행위자가 혼자서 풀어가기 어려운 종류의 난제이다. 전통적인 국민국가의 정부 이외에 민관협력을 통한 기업과 사회, 개인의 적극적인 참여가 필요하다. 또한 주변국이나 국제사회와의 초국경 협력도 중요하다. 국가가 중심이 되어 안과 밖의 다양한 행위자들과 네트워크를 형성하는 새로운 국가 모델, 즉 '네트워크 국가(network state)'의 발상이 필요한 분야이다. 그렇다면 주변4망 사이에서 한국이 풀어야 할 과제는 무엇인가?

첫째, 한미동맹의 구도에서 보는 사이버 안보협력의 강화가 제일 큰 과제이다. 그런데 주변4망 국제관계론의 시각에서 보면, 사이버 동맹을 논하는 수준에까지 이른 한미관계는 단순히 '강화론'의 관점에서만 볼 문제는 아니다. 무엇보다도 미국이 펼치는 인도·태평양 지역 동맹전략의 네트워크 구도 속에서 한미관계의 본질을 냉정히 바라보아야 한다. 이러한 구도에서 미국이 추구하는 '통합억지'와 한국이 원하는 '확장억제'가 상정하는 사이버 억지는 다를 수 있다. 게다가 오늘날 한미관계는 단순 군사동맹을 넘어서는 복합 상호의존의 관계로 발전했기 때문에, 일방적으로 받기만 하는 것이 아니라 서로 주고받는 관계가 되었다는 사실도 명심할 필요가 있다. 또한 사이버 안보협력은 한미관계의 '링크'만 강화해서 달성될 성격의 문제가 아니라는 점도 알아야 한다. 최근 파이브 아이즈(Five Eyes), 쿼드(Quad), 오커스(AUKUS), 나토(NATO) 등과의 사이버 안보협력 필요성이 꾸준히 제기되고 있고, 더 나아가 아세안이나 인도·태평양 지역의 다른 나라들과의 사이버 안보협력도 적극 고려할 필요가 있다.

둘째, 최근 개선된 한일관계의 구도에 사이버 안보협력을 제대로 착상시키는 문제도 주변4망론의 관점에서 풀어야 할 중요한 과제다. 2차대전 이후 미일동맹은 미국이 추구한 동아시아 전략의 주축을 이루었으며, 최근에는 일본의 적극적 대응에 힘입어 사이버 안보를 비롯한 첨단기술 분야에도 그 협력의 기조가 투영되고 있다. 이러한 미일관계의 구도와 앞서 언급한 한미관계의 양상에 비추어 볼 때, 최근의 한일관계는 '약한 고리'가 아닐 수 없다. 이를 보완할 목적으로 최근 한미일 3국은 '캠프 데이비드 선언'을 통해서 국제협력의 프레임워크를 마련했고 그 안에 사이버 안보를 포함한 첨단기술 협력이 포함되었다. 향후 한일관계는 한일 두 나라만의 문제가 아닌 한미일 관계와 여타 소다자 협력체, 그리고 인도·태평양 지역 국가들과의 협력도 염두에 두면서 그 방향과 내용을 고민할 문제다. 특히 아세안(ASEAN)을 매개로 한일 또는 한미일 관계를 어떻게 설정할지, 그리고 또 다른 삼각관계인 한일중 관계나 북중러 관계와의 중첩과 대립의 구도를 어떻게 풀어나갈지가 관건이 될 것이다.

셋째, 사이버 안보의 주변4망 구도에서 한미관계나 한미일 관계가 강화될 경우, 파생될 가능성이 큰 빈틈은 한중관계이다. 최근 중국의 사이버 위협 공세가 거세지는 가운데 이에 대응하는 미국의 동맹전략에 보조를 맞추면서 한국이 어떠한 입지를 추구할지가 중요한 관건이 되었다. 실제로 최근 중국의 사이버 공격은 다양한 패턴 변화를 보이고 있는데, 특히 사이버 영향력 공작의 수행이 큰 논란거리다. 중국은 사이버 군사전략의 정비뿐만 아니라 사이버 외교의 수행 차원에서도 미국에 대항하는 국제적 연대의 전선을 형성하고 있다. 이러한 과정에서 미국과 중국은 단지 사이버 안보 분야뿐만 아니라 디지털 패권경쟁 관련 분야 전반에서 다층적인 표준경쟁을 벌이고 있다. 그 사이에서 제기되는 한국의 전략적 고민은 단순히 중국의 사이버 위협에 대해서 미국과 공동으로 대처하는 문제를 넘어선다. 특히 미국의 안보 요구를 따라가면 한중 경제협력의 기회를 놓치게 될 뿐만 아니라, 중국이 북한과 밀착하게 될 빌미를 제공하게 될지도 모른다는 우려가 제기되고 있다. 이러한 맥락에서 최근 재개된 한일중 정상회담을 어떻게 발전시킬지의 문제는 큰 관건이 아닐 수 없다.

끝으로, 주변4망의 국제관계 중에서 가장 소홀히 다루기 쉬운 링크는 한러관계이다. 최근 러시아-우크라이나 전쟁은 물리전과 사이버전이 적극 결합하는 양상을 보여주었으며, 사이버전이 우주전이나 인지전 등과 같은 여타 미래전의 양식과도 연계되는 모습을 드러냈다. 사이버 안보의 시각에서 보아도 러시아-우크라이나 전쟁에서 드러난 대결의 구도는 러시아 대 우크라이나가 아니라 러시아 대 나토로 대변되는 서방 진영 간에 형성되었다. 그동안 우크라이나를 비롯한 동유럽 국가들을 효과적으로 공략했던 러시아의 사이버 공격은 이번 러시아-우크라이나 전쟁에서는 나토의 적극적 대응으로 인해 큰 성과를 거두지 못했다. 그럼에도 러시아의 사이버 전략은 사이

버 공격의 기술적 역량뿐만 아니라 중러연대를 포함한 사이버 외교의 추진, 그리고 사이버 국제규범의 형성 과정에 적극 참여 등과 같은 요인으로 인해서 앞으로도 계속 주목해야 할 중요한 변수이다. 이러한 '러시아 변수'는 한국에도 사이버 안보협력의 지평을 확장해야 할 큰 숙제를 안겨 주고 있다. 특히 러시아의 사이버 위협에 대응하는 서방 진영, 특히 나토와의 관계 설정이 최근 쟁점으로 제기되고 있다. 게다가 최근 북러 관계의 밀착이 새로운 변수로 부상하면서 한러관계의 관리는 한국 외교의 새로운 고민거리가 되었다.

한국 사이버 안보전략의 일차적 목표가 북한의 사이버 공격에 대한 효과적인 대응임은 물론이다. 랜섬웨어 공격이나 암호화폐 해킹, 사이버 영향력 공작 등 날로 교묘해지는 북한의 사이버 위협에 대응하기 위한 국내적으로 역량을 강화하고 법제도를 정비하는 노력의 중요성은 아무리 강조해도 지나치지 않다. 그러나 사이버 안보는 자강의 전략만을 통해서 달성될 목표가 아니다. 또한 공격과 방어의 당사자인 남북한의 양자구도에서만 볼 문제도 아니다. 좀 더 입체적인 네트워크 발상을 가지고 미·일·중·러 주변4망과 협력하고 여타 동지국가들과 연대하며 인도·태평양 지역과 글로벌 공간을 복합적으로 활용하는 지혜가 필요한 문제다. 이러한 과정에서 한국이 미국을 비롯한 우방국들과 형성하는 국제관계와 북한이 중국, 러시아 등과 모색하는 국제관계가 어떻게 경합하고 또는 중첩되면서 사이버 안보의 영역으로 투영되는지를 살펴보려는 노력이 필요하다. 주변4망의 사이버 국제관계 속에서 글로벌 중견국으로서 한국의 '사이버 국가책략(cyber statecraft)'에 대한 본격적인 고민이 필요한 때다.

이러한 문제의식을 바탕으로 이 글은 크게 네 부분으로 구성되었다. 제2장은 한미동맹 구도에서 보는 사이버 안보협력 강화의 움직임을 소개하고, 한미협력이 실질적인 성과를 거두기 위해서는 입체적인 네트워크 발상이 필요함을 지적하였다. 제3장은 '미일 사이버 동맹'의 전개와 확장이라는 맥락에서 2023년 한미일 캠프 데이비드 정상회의 이후 제기되고 있는 3국 간 사이버 안보협력의 과제를 짚어 보았다. 제4장은 안보와 군사 및 외교 차원에서 전개되는 중국의 사이버 전략과 이러한 과정에서 가속화되고 있는 미중 사이버 갈등 사이에서 한국이 추구할 과제를 짚어 보았다. 제5장은 러시아의 사이버 안보 전략의 관점에서 최근 발발한 러시아-우크라이나 사이버전의 복합적 양상을 살펴보고, 그 연장선에서 파생되는 한-나토 사이버 안보협력의 과제를 살펴보았다. 끝으로, 맺음말은 한국이 펼쳐나갈 사이버 안보 국가전략의 국내외적 과제를 간략히 짚어 보았다.

Ⅱ. 한미동맹과 한미 사이버 안보협력의 과제

최근 한미동맹의 구도에서 사이버 안보협력을 강화하자는 논의가 펼쳐졌다. 지난 70여 년의 역사를 지닌 한미동맹을 사이버 공간으로 확장하고, 이를 바탕으로 북한의 사이버 위협에 대처하는 굳은 태세를 보여주자는 것이었다. '사이버 부국강병론'을 지향하는 기술·공학적 시각도 가세하여, 한미동맹 강화를 사이버 안보 분야에서 더 많은 정책적 지원을 확보하는 계기로 삼자는 주장도 제기되었다. 이러한 논의는 나름의 결실을 보아 2023년 4월 한미 정상회담에서 한미동맹을 사이버 공간에까지 확장하기로 선언하는 데 이르렀고, '전략적 사이버 안보 협력 프레임워크(SCCF)'라는 별도의 문서를 채택하여 양국 협력의 범위와 원칙 및 체계를 구체화했다. 사이버 적대세력 억지, 핵심 인프라 보호, 사이버 범죄 및 자금세탁, 가상자산 및 블록체인 앱 보호, 역량강화, 공동훈련, 정보공유, 군사 분야 사이버 협력 심화, 법 시행, 기술개발, 인력양성, 민관협

력 등 핵심 사안을 명문화해서 향후 한미 사이버 안보협력의 플랫폼을 마련했다고 평가할 수 있다.

그 이후 한미 사이버 안보협력을 이행하고 확대하는 차원에서 다양한 후속 조치가 이루어졌다. 글로벌 사이버 위협에 범국가적으로 신속히 대응하기 위해 2023년 6월 '한미 사이버 안보 고위운영그룹(SSG)'이라는 이름으로 협의체를 출범시켰으며, 2024년 5월에는 '고위급운영그룹' 제3차 회의를 개최했다. 한편, 2023년 2월 북한의 사이버 공격 위협 실태를 알리고 이를 예방하기 위해 한미 양국의 정보기관들이 '한미 합동 사이버 보안 권고문'을 발표한 데 이어, 2024년 7월에는 영국도 가세하여 '한미영 합동 사이버 보안 권고문'을 발표했다. 또한 2023년 11월에는 일본도 참여하여 한미일 협력 차원에서 '고위급 사이버 협의체'도 신설됐다. 이밖에 한미 양국은 국방 분야에서 사이버 정책·작전·인력·훈련 교류를 추진하고 있으며, 사이버 범죄수사 분야에서도 양국 간 협력 강화 및 교류의 다변화를 모색하고 있다.

이렇게 안보·국방·범죄수사 등의 분야에서 활발히 진행되고 있는 한미 사이버 안보협력이 제대로 안정적인 궤도에 진입하여 실질적인 성과를 거두기 위해서는, 역설적으로 들릴 수도 있겠지만, '한미 사이버 동맹'을 강화하겠다는 생각에만 집착하지 말고 오히려 좀 더 유연한 접근을 가미해야 한다. 다시 말해, 한미관계라는 양자의 '링크'만을 강화하겠다는 다소 협소한 발상을 넘어서, 한미를 둘러싼 사이버 국제관계의 '네트워크' 전반을 입체적으로 성찰하는 좀 더 넓은 시각이 필요하다.

첫째, '한미 사이버 동맹'의 강화는, 우리의 희망 사항만을 투영시킬 문제가 아니라, 상대국인 미국이 구상하는 동맹전략의 구도 내에서 한미동맹이 어떠한 위상과 비중을 차지하는지를 성찰해야 할 문제다. 미국의 사이버 억지 전략이 원용하는 '통합억지'는 주로 양자관계에 기초한 기존의 동맹을 '연맹해서(federated)' 중국발 위협에 대응하겠다는 개념이다. 한국을 비롯한 동맹국과 파트너 국가들을 미국 주도 동맹 네트워크에 참여시키고, 전진 배치된 미국의 전략자산을 통합·사용하는 맞춤형 전략을 구사하겠다는 것이다. 이에 비해 우리가 생각하는 '한미 사이버 동맹론'은 북한발 사이버 위협을 억지하는 차원에서 미국의 재래식 능력과 핵 능력을 빌려 쓰듯이 사이버 능력을 빌려 쓰자는 이른바 '확장억제'에 기반을 둔다. 이렇게 보면 글로벌 공간에서 중국의 위협을 염두에 둔 미국의 '통합억지'는 한반도 공간에서 북한의 위협을 상정한 한국의 '확장억제'보다 좀 더 포괄적인 구도에서 설정된 개념이라고 할 수 있다. 여기서 관건은 '통합억지'를 추구하는 미국의 목표와 '확장억제'에 대한 한국의 기대를 얼마나 조율할 수 있느냐의 문제일 것이다.

둘째, '한미 사이버 동맹'의 강화는, '사이버 안보'라는 좁은 범위에만 국한해서 추진할 문제가 아니라, 한미관계의 성격 변화를 전반적으로 고려하여 여타 분야와의 균형을 맞춰서 진행할 문제이다. 최근 사이버 이슈의 외연이 확장하고 내포가 심화하고 있는 상황에서, 좁은 의미의 사이버 안보 분야가 아니라 디지털 분야 전반에 걸쳐서 한미협력의 내용을 고민할 필요가 있다. 최근 한미관계는 과거와 같은 정치·군사동맹을 넘어서 기술·경제 동맹과 가치·규범 동맹의 성격도 가미된 '비대칭 복합동맹'으로 발전했다. 한미관계가 과거와 같이 한국이 일방적으로 미국에 의존하는 구도가 아니라, 분야에 따라서는 한미 양국이 상호의존하는 구도로 변화했다. 한미동맹 관계에서 한국이 일정한 역할을 담당해야 한다는 목소리가 부쩍 커진 것은 바로 이러한 맥락이다. 한국이 미국으로부터 '사이버 동맹'의 약속을 받아내는 대신에, 한국이 기술경쟁력을 보유한 여타 디지털 분야에서 미국에 양보해야 할 상황이 벌어질 수도 있다. 게다가 최근 가속화되는 미중 디지털 패권경쟁의 와중에, 한국이 좀 더 적극적으로 자국의 편을 들어 중국 견제에 나서 달라는 미국의 요구를 거절하기가 어려워질 수도 있다. 2019년의 '화웨이 사태'처럼, 미국이 기술안보를 내세워 중국과 관련된 특정 기술을 배제하라고 압박하는 상황이 발생할 수 있다는 말이다.

실제로 최근 경제안보와 데이터 안보 분야에서 이러한 전략적 딜레마가 발생할 조짐이 보이기도 했다.

셋째, '한미 사이버 동맹'의 강화는, 미국과의 협력을 통해서만 이루어지는 것이 아니라, 미국의 동맹 전선에 참여한 여타 우방국들과의 협력도 병행해야만 실효성이 있는 문제다. 다시 말해, 전통안보와는 성격을 달리하는 사이버 안보 분야의 국제협력은 수직적 차원에서 한미 간의 '허브-스포크(hub-spoke)' 관계를 강화해서만 되는 것이 아니라, 수평적 차원에서 우방국들과의 '인터-스포크 관계(inter-spoke relation)'도 활성화해야 할 문제다. 최근 미국은 파이브 아이즈(Five Eyes), 쿼드(Quad), 오커스(AUKUS), 한·미·일 협력, 미·일·필리핀 협력 등과 같은 소다자 안보 협력체의 결속 및 확장을 추진하고 있다. 이들 소다자 협력체와의 관계 설정은 한국 외교의 과제로도 제기되었는데, 현재 공식(de jure) 가입까지는 아니더라도 참여국들과 사실상(de facto) 협력을 양자 또는 삼자 차원에서 추진하고 있다. 실제로 2023년 한국과 영국은 '전략적 사이버 파트너십'을 체결했고, 2023년 한국과 미국, 일본은 캠프 데이비드 정상회담을 통해서 협력 강화의 고삐를 당겼다. 또한 여타 자유민주주의 가치를 공유하는 국가들과도 협력을 강화하고 있다.

끝으로, '한미 사이버 동맹'의 강화는, 미국이 구축한 동맹 프레임 내의 협력만이 아니라, 인도·태평양 지역 여타 나라들과의 다자협력이라는 좀 더 넓은 프레임을 설정해야만 그 실효성이 더 커질 수 있다. 최근 협력관계가 확대되고 있는 인도·태평양 지역 국가들과의 관계를 염두에 두면, 북한의 사이버 안보위협에 대응하기 위해서 한미동맹의 '강한 고리(strong tie)'만을 강화하겠다는 발상은 다소 협소한 프레임 설정이라고 할 수 있다. 사이버 안보 분야의 국제협력은 그 특성상 네트워크상의 '약한 고리(weak tie)'의 활용도 놓치지 말아야 한다. 한반도를 향해서 가해지는 사이버 공격의 성격과 주체가 다변화되고 있는 최근의 양상을 제대로 이해하고 적절히 대응하기 위해서는, 사이버 안보협력의 대상과 프레임을 넓혀서 볼 필요가 있다. 이러한 연장선에서 볼 때, 인도·태평양 지역뿐만 아니라 국제기구 차원의 글로벌 프레임을 적극 활용한 국제협력의 모색도 병행해야 할 것이다.

2차대전 이후 미국은 아시아·태평양 지역에서, 나토로 대변되는 유럽 지역의 안보협력과는 다르게, 양자동맹으로 구축된 '허브-스포크 관계'를 기반으로 지역안보질서를 유지해 왔다. 이른바' 샌프란시스코 체제'라고 불리는 미국 주도의 질서가 그것이다. 그러던 것이 최근에는 이른바 '격자형(lattice) 동맹 네트워크'로 불리는 소다자 안보 협력체의 구성 및 운영을 추구하고 있다. 사이버 안보 분야에도 이러한 미국 동맹전략의 변화 양상이 그대로 투영되었다고 할 수 있다. 그런데 올해 말 미 행정부가 바뀌게 되면 이러한 미국의 동맹전략뿐만 아니라 한미동맹의 구도도 변화할 가능성이 거론되고 있다. 누가 집권하든지 간에 동맹전략과 국제협력은 추진하겠지만 그 형식과 내용은 바뀔 가능성이 크다는 것이다. 사이버 안보 분야에서도 사정은 마찬가지일 것이다. 미국이 차기 행정부에서도 중국을 견제하는 공세적 태세는 계속 유지되겠지만, 그것을 실천하는 동맹전략과 그 네트워크의 아키텍처는 정권의 향배에 따라서 다르게 설계될 수 있다. 이러한 동맹 구도의 변화는, 한미동맹을 사이버 안보협력의 주축으로 삼아온 한국의 입장에서 볼 때, 사이버 안보 전략뿐만 아니라 미래 국가전략 전반에도 영향을 미칠 중요한 변수가 아닐 수 없다.

이 책의 제1부 "미국의 사이버 안보-국방-외교 전략과 한미관계"는 이상에서 제기한 문제의식을 발전시킨 세 편의 논문을 실었다. 제2장 "미국의 사이버안보 전략과 한미동맹"(김소정)은 한미 사이버 안보협력의 최근 현황과 전망에 대해서 다루었다. 2022년 윤석열 정부 출범 이후, 한미 사이버안보 분야 협력은 공고해졌고 그 협력 분야들은 가시화되고 있다. 그 시작은 2022년

한미 정상회담인데 회의 직후 공개된 공동성명은 광범위한 기술 및 협력 분야를 명기함으로써 양국 간 협력을 구체화하는 계기를 마련했다. 이 문서에는 '사이버'가 10회 이상 언급되면서, 통신, 양자, 암호화폐 등 사이버 공간 이슈들의 중요성에 대한 양국의 인식을 재확인하였다.

이후 개최된 2023년 4월 한미 정상회담에서 양국은 '전략적 사이버안보 협력 프레임워크(Strategic Cybersecurity Cooperation Framework)'를 채택하였고, 이 프레임워크의 구도 내에서 양국 간 사이버 안보협력을 더욱 구체적으로 진행할 것을 선언했다. 양국은 2022년 5월 한미 정상회담에서 설정된 기조를 유지하면서 사이버안보에 국가의 정책 및 전략적 우선순위를 부여하였고 개방적이고 상호운영이 가능하며 안전하고 신뢰성 있는 인터넷과 사이버 공간의 구축을 목표로 하였다.

2023년 8월 개최된 캠프 데이비드 한미일 정상회담에서 한미 사이버안보 분야 상호협력 활동을 일본과의 협력으로 확대·적용하는 계기를 마련했다. 3국 간 사이버 협력을 수행하기 위해 북한의 사이버 활동에 대응하는 한미일 3국 고위급 '사이버 협의체'를 출범시켰고, 그 신설을 위한 실무 작업을 시작했다. 이러한 한미 양국 간 협력 강화 과정에서는 후속되는 조치 및 정책의 실행력 확보가 관건이며, 이를 통해 2023년 체결한 양국 간 협력 프레임워크가 도출하는 주요 성과를 얻을 것으로 기대된다. 아울러 제2장은 미국이 그동안 공개해 온 사이버안보 전략과 국방 사이버안보 전략에 대한 개괄적 이해를 통해 미국이 추진하고자 하는 사이버안보 협력 방향도 가늠해 보았다.

제3장 "미국의 사이버 국방 전략과 한미동맹"(박용한)은 국방 분야의 시각에서 한미 사이버 안보협력의 이슈를 다루었다. 미래 전장은 모든 전투체계가 연결된 네트워크 환경에서 작전을 수행하게 된다. 사이버 작전 환경은 육·해·공뿐만 아니라 우주와 사이버 및 전자기 영역으로 확대된다. 미 국방부는 미국의 동맹 및 파트너가 보유한 독자적인 기술과 관점을 활용하기 위해 군사관계를 지속적으로 강화하고, 미국의 동맹 및 파트너가 공동의 사이버안보 태세에 기여할 수 있도록 이들의 역량을 구축하기 위해서 협력할 방안을 제시했다. 미국은 동맹 차원에서 향후 포괄적·전면적 협력 참여를 요구할 것으로 전망된다.

한국과 미국은 사이버 공간으로 양국 동맹의 영역을 확장하고 한미 전략적 사이버안보 협력 프레임워크를 체결했다. 양국의 동맹 관계가 사이버 '영역'을 포괄하는 관계로 진화했다. 미국은 북한을 중국·러시아·이란 등과 함께 주요 위협으로 주시한다. 북한은 김정은 집권 이후 불법 경제활동으로 사이버 활동의 범위를 확장했다. 한미 양국은 북한 핵 개발을 지원하는 수익 창출 수단인 북한의 불법적 사이버 활동을 차단해야 한다는 공통의 목표 아래, 관련 활동을 차단하기 위한 '정보공유 확대'와 '국제사회 인식 제고'라는 이행 과제를 도출했다. 앞으로 한미 양국은 정보공유를 확대하고 상호운용성을 고도화하면서 기술적 연대를 모색하고, 동시에 기술적 역량을 강화해야 한다. 한미는 상호 국익을 극대화할 방안을 고심하며, 사이버 및 통신 관련 장비 공급망에 대해도 긴밀하게 조율해야 한다.

제4장 "미국의 사이버안보 동맹 전략(정성철)은 동맹전략의 시각에서 미국의 사이버안보 전략을 살펴보았다. 19세기 아메리카 패권을 차지한 미국은 대서양과 태평양에 둘러싸인 해양국의 이점을 활용하며 국제정치를 선도하였다. 하지만 9.11 테러 이후 미국은 자국의 사이버 취약성을 우려하며 이를 극복하고자 노력을 기울여 왔다. 하지만 지리적 이점을 발휘할 수 있는 물리적 공간과 달리 사이버 공간에서 미국은 세력균형, 상호의존, 수비우위를 활용하여 분쟁을 방지하거나 공격을 억제하는 전략의 한계를 꾸준히 절감하였다. 이라크 전쟁과 글로벌 금융위기 이후 탈냉전기 미국의 자유패권 전략에 대한 비판 속에 현실주의에 기초한 축소전략을 지지하는 목소리가 거세졌다. 그러나 사이버 위협이 일상화된 상황에서 미국이 유럽과 중동의 분쟁과 거리를

둔 채 해외개입을 선별적으로 취하겠다는 역외 세력균형 전략의 효용성은 점차 의심받고 있다.

지정학 공간에서 '민주주의 대 권위주의' 대립 구도는 사이버 공간에서 뚜렷하게 펼쳐지고 있다. 미국의 적대세력이 사이버를 활용해 다른 국가를 상대로 심리전과 국내 개입을 시도하고, 미국의 핵심 인프라에 대한 사이버 공격의 위험성은 줄어들지 않고 있으며, 미국 주도 질서에 도전하는 비(非)민주국가들은 사이버 활동을 통하여 자국의 역량과 정보를 확보하는 전략을 펼치고 있다. 비록 미국 우선주의를 내세우면서 글로벌 리더십을 행사하는 전략을 비판하는 국내세력이 늘어났지만, 미국의 사이버 전략은 2000년대부터 꾸준히 '다영역 억지' 혹은 '통합억지'를 추구하였다. 이는 국가안보를 위해 국방·경제·외교 등의 총체적 노력을 우방과 함께 기울이는 전략으로 확장된 안보개념에 바탕을 둔다. 최근 바이든 행정부의 사이버 전략은 유사 국가 및 민간 행위자와 함께 규범과 규칙에 기초한 디지털 생태계를 구축하는 데 집중하고 있다. 최근 사이버 협력을 중심으로 한미 양국은 다영역·다공간에서 안보협력을 제도화하면서 글로벌 포괄적 동맹으로의 변환을 지속하고 있다.

Ⅲ. 미일동맹과 한미일 사이버 안보협력의 과제

최근 한미일 사이버 안보협력에 대한 기대가 커졌다. 2023년 8월 18일 '캠프 데이비드 선언'은 한미일 3국이 전통안보 분야의 협력 강화를 넘어서 '정보·사이버 동맹'의 형성을 모색할 가능성을 기대케 했다. 캠프 데이비드 정상회의에서 한미일 정상은 인공지능·양자·우주·사이버안보 등 분야의 기술개발과 인력양성 및 표준화·규제 등에서 긴밀하게 협력하기로 했다. 특히 한미일 3국은 북한의 사이버 위협 및 허위조작정보에 대한 공동 대응과 함께 인도·태평양 지역의 디지털 인프라 구축을 위한 공동 지원에 협력하기로 천명했다.

이후 한미일은 캠프 데이비드 합의의 이행을 위해 고위급 및 실무급 회동을 마련하여 후속 조치를 논의하고 있다. 2023년 11월 한미일 3국은 '고위급 사이버 협의체'를 신설하기로 했으며, 12월에는 한미일 고위급 사이버 워킹그룹 회의를 개최하여 캠프 데이비드 합의를 재확인했다. 외교 분야에서도 한미일은 2023년 12월 '북한 사이버 위협 대응 한미일 외교 당국간 워킹그룹'을 창설하는 데 합의했고, 2024년 3월에는 외교 당국 간 워킹그룹 제2차 회의를 개최했다. 국방 분야에서도 한미일은 2024년 7월 한미일 국방장관회의를 개최하여 해상·공중 및 사이버 공간에서 3국의 공동 군사훈련을 정례화하기로 했다.

캠프 데이비드 선언을 통해서 기본적인 프레임워크를 정비한 한미일은 고위급 회동의 정례화나 협력 의제의 설정이라는 성과를 거두었지만, 아직 협력의 내용이 주로 선언적인 단계에 머무는 한계를 안고 있다. 특히 한미일 협력에 참여하는 세 나라의 동상이몽도 극복해야 할 과제다. 북핵에 중점을 두는 한국과 포괄적 지역안보에 초점을 맞춘 미일 사이에는 상당한 이견이 존재한다. 사이버 안보 분야에서도 북한의 사이버 위협에 대한 공동 대응의 계기를 마련했지만, 3국 간에는 이를 수행할 국내외적 여건의 차이가 존재한다. '캠프 데이비드 1년'을 맞는 현시점에서 한미일 사이버 안보협력이 실질적인 성과를 달성하기 위해서는 한미일을 포함한 주변국들과의 사이버 국제관계를 고려하는 입체적 발상이 필요하다.

첫째, 한미일 사이버 안보협력의 '주축 링크'인 '미일 사이버 동맹'의 전개와 그 성격을 이해하는 것이 필요하다. 미국과 일본은 2013년 '사이버 방호정책 워킹그룹'을 창설한 뒤 지속적으로 사이버 안보협력에 대한 논의를 진행했다. 2015년 4월 미일 정상회담에서 합의한 '방위협력지

침’ 개정안에 사이버 안보협력을 포함시켰는데, 미국은 일본의 군사시설과 국가 기반시설에 대한 사이버 공격에 대응하는 지원을 약속했다. 이는 일본이 미국의 사이버 방위역량에 기대어 자국의 사이버 안보를 보장받았다는 점에서 미국의 ‘사이버 우산’에 일본이 편입됐다고 평가받기도 했다. 이는 2019년 4월 ‘미일안보조약’ 제5조 집단자위권 조항에 사이버 공격을 포함하는 행보로 이어졌는데, 미일 양국이 집단자위권을 사이버 공격에도 적용한다고 확인하였다. 2023년 1월 발표한 공동성명에도 미일 양국은 합동 태세를 강화하여 사이버 억지력을 확장할 것이라고 강조했다.

둘째, ‘미일 사이버 동맹’을 기반으로 펼쳐지는 일본의 전략적 행보를 파악하는 것이 필요하다. 일본은 미일동맹의 제고를 위해서 일본의 사이버안보 능력 강화가 필요하다는 미국의 요청을 활용하여, 이러한 역량의 강화를 집단자위권 행사를 실현할 수단으로 이용하려고 한다. 더 나아가 일본은 파이브 아이즈(Five Eyes) 국가들과 개별 협정을 맺어 사실상 파이브 아이즈 참여국 모두와 협력하고 있다. 미일동맹 차원에서 일본은 미국과 ‘주둔군지위협정(SOFA)’을 맺고 있으며, 영국과도 협력하여 2022년 5월 일본 자위대와 영국군의 공동 훈련절차를 규정한 ‘상호접근협정(RAA)’을 체결했다. 일본은 호주와도 이미 상호접근협정을 체결한 상태인데, 2022년 4월에 개시하기로 합의된 뉴질랜드와의 정보보호협정이 체결되면 파이브 아이즈 중에서 캐나다를 제외한 모든 나라와 군사협력과 정보공유가 가능해진다.

셋째, ‘미일 사이버 동맹’과 이를 기반으로 확장하는 일본의 전략 구도에서 한일관계가 ‘약한 고리’임을 인지하는 것이 필요하다. 한일 양국은 각각 미국과 ‘사이버 동맹’ 수준의 협력체제를 구축하고 있다. 한국은 미국과 ‘전략적 사이버안보 협력 프레임워크(SCCF)’를 체결했다. 일본은 2015년 사이버 안보 협력 조항을 미일 방위협력지침에 추가한 데 이어, 2019년에는 집단자위권을 사이버 공격에도 적용한다고 밝힌 바 있다. 이렇듯 이미 고도화된 한미 및 미일 간 사이버 안보협력에 비해, 한일 간의 사이버 안보협력 수준은 아직 보안 인프라 구축이나 민관 기술협력 등과 같은 기본적인 수준에 머물러 있다. 한일 간에 활발한 협력이 진행되지 못했던 것은, 일본이 한국보다는 사이버 위협에 덜 노출된 까닭도 있고, 일본의 사이버 대응 역량이 그리 높지 않았던 때문이기도 했다. 최근 개선되고 있지만, 한동안 악화했던 한일관계 전반의 분위기도 부정적인 환경요인으로 작용했다.

넷째, 한일관계를 회복하여 장차 한미일 관계를 어떠한 아키텍처로 구성할지를 고민할 필요가 있다. 사실 한미일 캠프 데이비드 정상회의는 미국이 주도하는 미일동맹 구도에 한국을 끌어들이는 데 그 목적이 있었다고 볼 수 있다. 이를 통해 기대하는 한미일 관계의 구도는 당분간은 ‘비대칭 삼각관계’가 될 가능성이 크다. 한국과 일본 사이에는, ‘사이버 동맹’에 준하는 ‘강한 고리’를 만들기보다는, 고위급 사이버 대화 등을 통해서 정책 공조를 진행하는 정도의 포괄적인 형태를 모색할 가능성이 크기 때문이다. 그러나 향후 한미일 사이버 안보협력의 진행 과정에서 한미일 정보공유협정(TISA)과 같이 미국을 매개로 한 한일 협력의 방식이나 한일 간의 빈틈을 메우기 위해 체결된 한일 군사정보보호협정(GSOMIA) 등과 같은 기존의 안보협력 모델을 고려할 필요가 있다. 한편, 2024년 7월 개최된 한미일 국방장관회의에서 공동 군사훈련의 정례화를 명문화한 ‘안보협력 프레임워크(TSCF) 협력 각서’도 고려해야 할 것이다.

끝으로, 한미일 관계의 외연을 확장 문제도 고민할 필요가 있다. 이는 미국이 주도하는 소다자 협력체에 한국과 일본이 참여하는 문제이다. 제일 많이 거론된 것은 한국과 일본의 파이브아이즈(Five Eyes) 참여였는데, 최근에는 파이브 아이즈의 ‘구조적 확장’보다는 ‘기능적 확장’이라는 차원에 힘이 실리고 있다. 이밖에도 한국의 쿼드(Quad) 참여도 제기된 바 있지만, 이보다는 한국과 일본의 오커스(AUKUS) 필러-II 참여가 더 큰 쟁점이다. 최근 미국은 오커스 필러-II에 일본을 초청하기도 했으나, 오히려 일본이 신중한 태도를 보였다. 미국의 전략도 오커스 구도와 한미일 구

도를 '결합'하기보다는 '병행'하는 쪽으로 방향을 잡는 조짐이 감지된다. 최근에는 나토와 인도·태평양 4대 파트너 국가(IP-4)인 한국, 일본, 호주, 뉴질랜드와의 협력이 주목받고 있는데, 2024년 7월 나토 정상회의에서는 우크라이나 지원, 사이버 방위, 허위조작정보 대응, 첨단기술 협력 등에서 나토와 IP-4 간의 협력이 언급되었다.

궁극적으로 한국이 당면한 핵심 과제는 한미일이나 여타 소다자 구도 내에서 한국의 위상을 설정하는 문제다. 북핵 대응이 한국이 원하는 바라면, 한미일 구도의 강화는 나쁘지 않은 방안이다. 미국이 주도하여 인도·태평양 지역질서를 재편하는 상황에서 한미일 구도의 적극적 수용은 중국 견제에 나선 미국의 요구를 들어주는 모양새를 띠는 데다가, 북중러 삼각관계에 대응하는 효과도 크기 때문이다. 그러나 이러한 과정에서 한국의 위상이 미국-일본-한국으로 이어지는 위계적 구도에서 설정될 가능성이 있다는 점도 염두에 두어야 한다. 또한 최근 미중갈등의 양상을 볼 때, 한미일에 대한 지나친 밀착과 미국의 정책에 대한 적극적 동조화가 초래할, 예기치 않은 외교적·경제적 비용 발생도 고려해야 한다. 이러한 변수들에 대한 복합적인 고려를 바탕으로 '주변4망(網)의 사이버 국제관계'라는 맥락에서 한미일 사이버 안보협력의 구도를 입체적으로 보는 발상이 시급히 필요하다.

이 책의 제2부 "일본의 사이버 안보-국방-외교 전략과 한일관계"는 이상에서 제기한 문제의식을 발전시킨 세 편의 논문을 실었다. 제5장 "일본의 '능동적 사이버 방어' 수용과 전수방위 원칙"(이정환)는 일본의 사이버안보 정책을 '능동적 사이버 방어(active cyber defense, ACD)' 개념에 초점을 맞추어 검토하였다. 일본 정부는 2022년 '안보3문서'에서 명시된 '능동적 사이버 방어' 개념 도입에 대한 법적 기반 구축 작업을 진행하고 있다. '능동적 사이버 방어' 개념은 헌법 21조의 통신 비밀 규정과 헌법 9조에 대한 전수방위 원칙과 논리적으로 충돌하기 때문에, 이에 대한 논리 체계 구축 작업이 요구되는 상황이다. 사이버 공간에서 잠재적 공격을 감시하고, 공격자를 특정하고, 이에 대한 실력 대항조치를 전방 방위로 추진하는 '능동적 사이버 방위' 개념의 도입 자체는 이미 결정된 미래다.

무엇보다도 '능동적 사이버 방위'는 미국이 제시하는 국제표준으로서 일본에 수용되고 있다. 일본의 보통국가화는 외부 위협에 대한 적극 대응이 필요하다는 논리와 더불어 일본의 국가 역할이 다른 국가들과 동일해야 한다는 보편주의적 국제주의 논리에 입각해 전개되고 있다. 미국 주도로 새로운 국제규범이 된 '능동적 사이버 방위'의 도입은 국제표준 수용 차원에서 당연한 것으로 일본 정책관여자들에게 인식되는 사항이다. 국제표준 수용으로서의 정책 변화에도 불구하고, 일본은 국제표준에 맞춘 헌법 해석 변경을 전면적으로 추진하지 않고 있다. '능동적 사이버 방어' 수용은 글로벌 보편 현상인 가운데, 새로운 국제표준이 된 '능동적 사이버 방어'와 정합성을 지니는 차원의 적극적 국내 법제도 변경을 회피하는 것은 일본의 특수적 현상이다.

제6장 "일본 방위성의 사이버안보 정책과 미일협력"(조은일)은 국방의 시각에서 최근 일본의 안보전략에서 중요하게 다뤄지고 있는 사이버안보 이슈를 살펴보았다. 2022년 12월 발표한 일본의 '국가안보전략서'는 사이버안보가 언급하면서, 안전하면서 안정되게 사이버 공간을 이용할 수 있는 정책을 추진하겠다고 밝혔다. 이를 위해 '능동적 사이버 방어'라는 개념을 도입하고 '중대한 사이버 공격을 미연에 방지하며 피해 확대를 방지'하기 위한 사이버안보를 강화할 것으로 보인다.

이를 위해 일본 방위성은 전시뿐만 아니라 평시에도 사이버 공간을 감시할 수 있도록 방위정책을 재정비할 전망이다. 첫째, 육해공 자위대 합동의 사이버 방위부대 창설과 같은 부대구조의 재편이다. 둘째, 군과 민간 인력을 충분히 활용하는 인력 양성이다. 이러한 두 가지 노력을 통해 사이버 공격 가능성을 사전에 무력화할 수 있는 방위력을 갖춘 좀 더 적극적인 형태의 사이버안

보 정책이 추진될 수 있다. 그리고 일본은 사이버 분야에서 미국과의 안보협력을 심화시키면서 능동적 사이버 방어를 완성해 갈 것이다. 이를 위해 일본 국회는 능동적 사이버 방어 도입을 위한 입법 조치를 추진할 것인데 통신의 자유와 같은 헌법을 포함한 논의가 전개될 수 있다. 향후 방위성은 국회 논의 및 정부 입장을 반영한 사이버안보 전략을 구체화할 것으로 보인다.

제7장 “일본의 사이버안보 전략과 국제협력”(윤대엽)은 아베 내각 이후 일본의 안보개혁이 미중경쟁, 북핵위협, 양안위기와 상호작용하면서 인도·태평양 지역의 전후 안보질서를 변화시키고 있다고 주장한다. 일본은 미일 동맹을 기반으로 방위력의 증강, 다자협력의 확대는 물론 우주, 사이버, 인공지능을 연계하는 포괄적인 방위개혁을 추진하고 있다. 특히 일본은 이미 2000년대 인도·태평양 국가 중 가장 먼저 사이버 공간을 안보화하고 포괄적인 사이버안보 전략을 추진해왔다. 2006년 처음 발표된 ‘정보시큐리티 기본계획’은 2010년 ‘정보시큐리티 전략’으로 변경되었고, 아베 내각은 2013년 ‘사이버시큐리티전략’으로 수정하고, 국가안전보장회의가 총괄하는 사이버안보 거버넌스를 재편했다. 그리고 2021년에는 디지털 전환(DX)을 목표로 2000년 제정된 ‘IT 기본법’을 ‘디지털사회형성기본법’으로 개정하고 디지털 정책을 총괄하는 디지털청을 신설했다. 주목되는 특징은 디지털 전환에 앞서 사이버 공간의 안보화가 선행되었던 일본의 사이버안보 전략에서 일관되게 국제협력이 강조되었다는 점이다.

일본이 사이버 공간의 안보화가 디지털 전환보다 우선되었던 이유는 무엇인가? 그리고, 다자안보협력보다 앞서 사이버안보 전략에서 국제협력이 강조된 이유는 무엇인가? 제7장은 역사적·비교적 시각에서 일본의 사이버안보 전략이 전후 안보개혁과 점진적·창발적으로 형성·전환되어 온 과정을 구조와 행위자 측면에서 분석하고 사이버 국제협력의 특징을 분석하였다.

일본의 사이버안보 전략과 국제협력은 1) 정보시큐리티 기본계획(2004-2012) 단계와 2) 사이버시큐리티 전략(2013-2022) 시기로 구분하여 검토할 수 있다. 정보시큐리티 기본계획은 9/11 사태 이후 비전통 안보가 새로운 안보위협으로 인식되는 가운데, 탈(脫)전후 안보전략을 추진한 고이즈미 내각에 의해 추진되었다. 잠재적 안보위협에 대한 선제적 인식에도 불구하고 정보통신기술이 가진 경제적·기술적 이해가 중심이 되면서 경제협력 기반의 국제협력이 추진되었다. 2000년대 일본의 정보시큐리티 정책과 국제협력을 주도한 것도 경제산업성(METI)과 총무성이었다. 아베 내각 이후 사이버안보 전략은 포괄적인 안보개혁의 일부이자, 위협주체에게 직접적인 영향을 미치는 ‘전략’으로 재정립되었다. 미중경쟁이 본격화된 2018년 방위규범이 개정 이후에는 사이버 영역의 방어, 억지, 상황인식에 대한 전략이 되는 한편, 2021년 사이버시큐리티 전략에는 능동적 억지 개념이 명시되었다. 아베 내각 이후 사이버 공간이 군사화가 되는 가운데 역량구축, 사이버 법치 및 신뢰구축을 위한 사이버 국제협력도 확대되었다. 사이버안보와 동시에 2019년 이후 ‘신뢰에 기반한 데이터의 자유로운 유통(DTTF)’의 국제적인 규범화와 제도화를 위한 국제협력도 주도하고 있다.

Ⅳ. 중국의 사이버 전략과 미중갈등 사이의 한국

최근 한국을 겨냥한 중국발 사이버 공격이 늘어났다. 북한발 사이버 공격보다 양적으로는 적지만, 실제로 유발하는 피해는 더 큰 것으로 알려졌다. 게다가 중국발 사이버 공격은 그 대상과 수법도 새로운 양상으로 변화하고 있다. 이전에는 국가기간시설 교란이나 첨단기술·데이터 탈취를 목적으로 하거나 랜섬웨어 공격 등의 형태로 나타났다면, 최근에는 우주공간을 매개로 한 위

성통신 해킹, 허위조작정보 유포를 통한 사이버 영향력 공작, 인공지능(AI)을 활용한 사이버 공격 등의 형태로 진화하고 있다. 이들 공격은 독립적인 해커 그룹에 의해 수행되기도 하지만, 그 배후에 중국 정부나 군이 있다는 지적이 제기되면서 국제적 갈등의 빌미가 되기도 했다.

실제로 중국은 사이버 안보를 국가안보의 중요한 구성요소로 인식하고 국가적 차원에서 적극적인 전략을 펼쳐왔다. 게다가 미래전(戰)의 새로운 양식으로 사이버전(戰)이 자리 잡아가면서, 중국은 사이버 안보의 군사전략에도 각별히 역점을 두어 왔다. 2010년 이후 여러 차례에 걸쳐서 출간된 중국의 '국방백서'는 사이버전을 수행할 역량의 구비를 지속적으로 강조하고 있다. 군사작전 차원에서도 중국은 2015년 12월 '전략지원부대'를 창설하여 그 예하의 '네트워크계통부'가 사이버 작전을 담당하게 했는데, 2024년 4월 군 구조 개편이 단행되면서 '전략지원부대'가 해체된 이후, 새로 편성된 '사이버공간부대'가 관련 업무를 담당하는 것으로 알려져 있다.

사이버 외교 차원에서도 중국은 서방 진영에 대항하는 연대의 전선을 구축하고 사이버 분야의 국제규범 형성을 주도하려는 노력을 펼치고 있다. 이러한 노력의 이면에 디지털 인프라를 구축하고 중국 기업들의 이익 극대화를 지원하는 기술·경제 외교의 속내가 작동하고 있음은 물론이다. 이를 위해 일대일로(一帶一路) 선상의 국가들과 협력을 확대하고 있으며, 이외에도 상하이협력기구(SCO), 브릭스(BRICS) 등의 다자협력체에도 참여하고 있다. 중국은 서방 진영이 주도하는 자유주의적 사이버 질서에 반기를 들고 사이버 공간의 '주권' 원칙에 기반을 둔 '사이버 인류운명공동체'의 건설을 지향하고 있다. 궁극적으로 사이버 공간에 중국이 내세우는 담론과 표준을 세우겠다는 것이다.

이렇듯 전방위로 펼쳐진 중국의 전략적 행보가 미국과의 갈등을 유발했음은 물론이다. 2020년대 들어 미국에 대한 중국발 사이버 공격은 유난히 세간의 관심을 끌었다. 미국은 국내적으로 이에 대응하는 역량의 강화를 위한 적극적인 정책을 펼쳤으며, 국제적으로도 중국의 불법적 사이버 활동을 비난하기 위해 나토 동맹국들과 외교적 보조를 맞추기도 했다. 한편, 2018-19년 '화웨이 사태'를 계기로 미중 사이버 갈등은 공급망 안보의 이슈로 확장됐다. 특히 최근에는 데이터 안보 이슈가 논란거리인데, 중국산(産) 드론, CCTV, 안면인식AI, 항만크레인, 자율주행차, SNS 플랫폼, 이커머스 등이 도마 위에 올랐다. 이러한 논란거리들이 늘어나면서 '사이버 공간의 진영화'를 우려하는 목소리도 높아지고 있다.

미중 사이버 갈등의 현실은 한국에 쉽지 않은 과제들을 던지고 있다. 우선 양적으로 늘어났을 뿐만 아니라 질적으로도 점점 더 교묘해지는 중국의 사이버 공격에 능동적으로 대응할 필요성이 커졌다. 이를 위해 한미 사이버 안보협력을 강화하면서도 좀 더 포괄적인 의미의 국제협력도 동시에 모색해야 할 필요가 생겼다. 그러나 미중 사이버 갈등의 대상이, 좁은 의미에서 본 해킹 공격에만 국한된 것은 아니라는 사실을 명심해야 한다. 앞서 살펴본 바와 같이, 다양한 분야를 아우르는 미중 표준경쟁은 좀 더 넓은 시야에서 다양한 문제들에 주목할 것을 주문한다. 특히 사이버 외교 분야에서 전개되는 미·일·중·러 주변4망(網)의 국제관계 속에서 사이버 안보의 국제협력 전략을 고민하는, 좀 더 입체적인 시각이 필요하다.

무엇보다도 중요한 과제는 미중 사이버 갈등 사이에서 한중협력의 위상을 적절히 설정하는 문제일 것이다. 미중 사이의 균형보다는 한미동맹의 강화가 강조되는 현 상황에서 한중협력의 운신폭이 좁아진 것은 사실이다. 그럼에도 디지털 경제 분야 전반으로 넓혀서 보면, 한중협력은 여전히 한국에 이익을 안겨줄 여지가 있다. 다양한 분야에서 중국은 우리에게 경쟁의 상대이기도 하지만 협력의 상대가 될 수도 있음을 염두에 두어야 한다. 사이버 안보 분야에서도 사이버 범죄와 같은 비(非)정치적 사회문제를 놓고 한중 양국이 협력할 상황도 상정할 필요가 있다. 중국의 불법적인 공격에는 단호하게 대응하지만, 안전한 사이버 공간을 구축하기 위한 양국 협력의 필요

성을 외면할 필요는 없다.

더 나아가 사이버 안보 분야의 한중관계를 좀 더 입체적인 주변4망(網)의 소다자 대립 구도 속에서 볼 필요가 있다. 예를 들어, 최근 대중국 견제를 목표로 가동된 한미일 협력의 구도에서 새롭게 설정될 한중관계의 방향을 가늠해 볼 필요가 있다. 또한 최근 4년 5개월 만에 정상회담을 개최하여 주목받은 한일중 협력의 구도에서 한중관계가 차지하는 위상도 꼼꼼히 살펴봐야 한다. 중국은 한일중 구도를 한미일 협력을 견제하기 위한 고리로 활용하려 하겠지만, 한국의 입장에서 보면, 한일중 정상회담을 통해 그간 소원했던 한중 간의 소통 채널이 마련된 의미도 크다. 국제정치 일반을 넘어서 사이버 안보 분야에서도 한미일 및 한일중의 구도에서 한국이 담당할 역할을 좀 더 복합적으로 고민할 필요가 있다.

한편, 북중 또는 북중러 구도에서 한중관계가 어떠한 의미를 갖는지 성찰하는 것도 중요하다. 북한발 사이버 공격을 귀속하는 문제에서 한중이 협력할 가능성이나, 최근 사이버·데이터 안보 관련 의혹을 낳고 있는 중국 디지털 플랫폼의 북한 및 한국 진출의 의미가 무엇인지 고민할 필요가 있다. 한국의 입장에서 볼 때, 중국은 북한의 사이버 공격을 견제하는 수단일 될 수도 있지만, 동시에 좀 더 포괄적이고 새로운 '사이버 위협'을 야기할 주체가 될 수도 있기 때문이다. 아울러 최근 물밑 진행되는 것으로 알려진, 러시아와 북한의 군사협력을 견제하는 차원에서 한중관계를 어떻게 활용할 것인지도 고민해야 한다.

당장 우리에게 닥친 사이버 안보위협에 신속하게 대응하는 것이 매우 중요하고 시급한 문제임은 물론이다. 그러나 주변4망(網) 구도에서 사이버 안보의 국제협력 전략을 풀어가는 입체적 발상도 필요함을 잊지 말아야 한다.

이 책의 제3부 "중국의 사이버 안보-국방-외교 전략과 한중 관계"는 이상에서 제기한 문제의식을 발전시킨 세 편의 논문을 실었다. 제8장 "중국 사이버 공격 양상 변화와 사이버 안보에의 함의"(김상규)는 중국의 사이버 공격이 어떤 형태로 변화하고 있는지, 그리고 그것이 사이버 안보에 주는 함의는 무엇인지를 고찰하였다. 이를 위해 사이버 공격의 일반적 정의와 방식에 대해 살펴본 뒤, 중국이 감행하는 사이버 공격의 주요 주체와 방식, 목표 등을 보여주는 사례를 분석하였다.

연구 결과, 중국은 초창기의 부족한 기술력과 제도적 미비점을 마련하기 위한 전략을 수립하고 이에 따라 관련 정보 탈취와 기술 축적을 위한 공격을 진행하였으며, 이후 국가 차원에서 사이버 공간에 관한 인식과 목표, 전략을 천명하고 정보 수집, 군사 기밀 획득, 정치적 영향력 확장, 경제적 이익 추구 등 다양한 형태의 사이버 공작을 진행하는 것을 확인하였다. 공격의 주체는 국가기관을 비롯한 민간 사이버 해킹 단체 등을 망라하고 있으며 대상 역시 중국에 반하는 행동을 하는 국가와 민간 단체, 개인 등을 포괄해 전방위적으로 행동 범위를 넓히고 있다. 중국은 전통적인 수법에 기반을 둔 사이버 공격뿐만 아니라, 인공지능(AI) 등 고도화된 기술력을 활용하여 소프트웨어 공급망까지 침투하는 방식을 활용하고 있다. 더욱이 평시에는 가짜 뉴스를 생성하고 사회 인프라 곳곳에 악성코드를 유포하여, 유사시 사회적 혼란을 초래하는 것을 넘어 군사력 동원까지 제어하려는 영향력 공작과 사이버 심리전, 인지전의 행태를 보이기도 한다.

그러나 중국의 입장에서도, 중국을 경유하거나 중국 내부의 사이버 공격과 범죄는 물론 북한과 러시아를 비롯한 미확인 대상의 위협 행위에 대한 방어와 통제를 위한 협력이 필요한 상황이 있을 수 있다. 따라서 한국은 중국의 불법적이고 공격적인 행태에 대해 단호하게 대응하면서도, 다른 한편으로는 중국과 양자 간 혹은 다자 간 공통 의제를 찾는 노력을 병행한다면 사이버 공간의 안보와 국가의 이익 실현할 기회가 될 것이다.

제9장 "중국 사이버 안보와 군사전략: 중국 사이버 안보와 군사전략의 연계, 미래 안보에의 함

의”(양정학)는 중국의 사이버안보에 대한 인식과 전략적 접근을 분석하였다. 중국은 사이버 공간을 국가주권의 핵심 영역으로 간주하고 있으며, 이에 따라 사이버안보를 국가 전체 안보의 중요한 구성요소 중 하나로 인식하고 있다. 이러한 배경하에 중국은 ‘사이버 안보법’과 ‘국가 사이버 공간 안보전략’ 등을 만들어 사이버 공간을 체계적으로 관리 및 통제하고 있다.

사이버안보는 중국의 군사전략에서도 매우 중요한 위치를 차지하고 있다. 중국군은 사이버 공간을 새로운 전장으로 정의하며 사이버 공간을 통해 정보 수집, 정찰, 공격 및 방어 등의 작전을 수행하고 있다. 특히, 2024년 4월에 신설된 ‘사이버공간부대’는 사이버 작전을 수행하는 군내의 핵심 조직으로 민간과의 협력을 통해 기술개발은 물론 기술적 우위를 확보하고자 노력하고 있다. 중국의 사이버 군사전략은 단순히 방어에 그치지 않고 사이버 공격을 통해 사이버 공간에서의 상대국 ‘작전중심(作戰重心)’을 무력화시키고, 상대국의 정치·경제 영역 등 국가 차원의 위기를 초래시키는 것을 목표로 하고 있다. 이러한 전략적 접근은 중국이 사이버 강국의 지위를 확립하고 향후 전쟁에서의 승리를 보장하기 위한 것이라 볼 수 있다.

오늘날 사이버 공간에서의 안보 이슈는 ‘항상 존재하는 문제’로 인식되고 있으며 중국은 사이버 공간을 국가주권 차원으로 격상시켜 대응하고 있다. 이에 따라 중국군은 사이버 공간에서의 작전능력을 강화하고 민간과의 협력을 적극적으로 추진하고 있다. 한국 정부는 이러한 중국의 움직임을 면밀히 주시하고, 동맹 및 우방국들과의 협력을 강화하며, 사이버 안보 체계 정립과 사이버 공간에서의 능력 강화를 위한 대규모 투자를 진행해야 한다

제10장 “중국의 사이버 안보외교와 글로벌 사이버안보 질서의 진영화: 중국은 어떻게 사이버 공간 운명공동체를 만들어 가고 있는가?”(차정미)는 사이버 공간이 안보와 경제 등 모든 측면에서 강대국 경쟁의 핵심 공간으로 부상하면서, 중국이 구축하고자 하는 글로벌 거버넌스, 글로벌 리더십의 비전인 인류운명공동체 담론이 사이버 공간으로 확대되고 있다고 주장하였다. 사이버안보가 미중 영향력 경쟁의 주요 공간으로, 우호그룹 확대와 결집의 주요한 외교수단으로 부상하는 가운데 중국의 사이버안보를 외교적 관점에서 분석한 연구는 취약한 실정이다. 이에 제10장은 미중경쟁 하에서 중국이 어떻게 사이버 안보외교를 글로벌 영향력 확대와 서구에 대항하는 우호그룹 구축의 중요 수단으로 적극 활용하고 있는지를 분석하였다.

중국은 안보와 발전의 이중 목표하에 개발도상국 및 비서구국들과의 규범적 연대, 물리적 결합을 추구하면서 사이버 공간 운명공동체 구축을 목표로 하고 있다는 점에 착안해서, 제10장은 중국의 사이버 안보외교를 ‘안보·가치규범 외교’와 ‘인프라 외교·기술 외교’의 두 분야를 중심으로 고찰하고, 사이버안보 운명공동체라는 중국 주도의 사이버안보 블록, 사이버안보 거버넌스 구축을 위한 중국의 사이버안보 규범 외교와 사이버 안보 기술 외교를 분석하였다. 중국이 이를 통해 중국 주도 혹은 중국에 우호적인 글로벌 사이버안보 거버넌스를 구축하는 것은 물론 중국의 사이버안보 시장과 파트너의 확대, 이를 통한 중국의 네트워크 지배력, 디지털 경제 지배력을 제고하는 안보와 발전의 동시 추구 전략을 추구하고 있음을 보여주었다. 결론적으로 이러한 안보와 발전의 이중목적을 가진 중국의 전방위적 전면적 사이버 안보외교가 비서구 사이버안보 블록 형성의 주요한 토대가 될 것으로 전망하고, 중국 주도의 비서구 사이버안보 운명공동체 구축이 갖는 국제정치적 함의를 지적하였다.

Ⅴ. 러시아-우크라이나 전쟁과 한·나토 사이버 안보협력의 과제

러시아의 사이버 공격은 글로벌 차원에서는 오래전부터 논란거리였지만 한반도 차원에서는 큰 주목을 받지 못했던 것이 사실이다. 2018년 평창동계올림픽 당시 러시아 해커들의 공격이 발생하긴 했지만, 그 외에 국내적으로 관심의 대상이 된 큰 사건은 별로 없었다. 그러나 시야를 넓혀서 보면, 러시아의 사이버 공격 및 전략은 무시할 수만은 없는 중요한 변수이다. 특히 최근 러시아가 일으킨 우크라이나에서의 전쟁은, 사이버전(戰)이 사이버 공간에만 국한되는 것이 아니라, 육·해·공·우주 공간에서의 물리전과 결합하는 방식으로 진화했음을 여실히 보여주었다. 특히 러-우 전쟁에서 드러난 사이버 공격은 개전을 전후한 전쟁 초기 단계에서 지휘통제체제를 공략하는 최초의 수단이 될 수 있음을 잘 보여줬다.

실제로 러시아는 2022년 1~2월 개전 직전 네 차례에 걸쳐 디도스 공격을 감행했는데, 대규모 사이버 공격이 이루어진 다음 날인 2월 24일에 개전 선언과 함께 본격적인 군사작전을 우크라이나 곳곳에서 단행하였다. 그러나 사이버 공격으로 승기를 잡고 전쟁을 속전속결로 끝내려는 러시아의 전략은 기대했던 것만큼의 성과를 보지는 못했다. 우크라이나의 사이버 방어역량도 만만치 않았으며, 나토(NATO)와 국제사회의 적극적 지원도 큰 역할을 했다. 우크라이나의 'IT 군(IT Army)' 소집에 국제적 지원이 이루어졌고, 유명한 핵티비스트 그룹인 어나니머스도 참전했다. 이밖에 MS, 구글, 메타 등 서방의 민간 기업들도 나름의 기여를 했다. '사이버 세계대전'이라는 말이 나올 정도로 러-우 사이버전에는 다양한 주체들이 참여했다.

러-우 사이버전은 양국만의 전쟁이 아니라 러시아와 나토로 대변되는 서방 진영이 벌인 국제전이었다. 나토는 사이버 공격 대응뿐만 아니라 허위조작정보 대응, 교육·훈련과 민간협력 등의 분야를 지원했다. 우크라이나도 크림반도 병합 이후 나토식 표준에 부합한 전방위적 국방개혁을 추진하면서 나토와 함께 사이버 방어 협력의 전선을 구축했다. 또한, 서방 기업들의 지원으로 데이터센터를 해외 클라우드에 분산시킴으로써 러시아 사이버 공격의 예봉을 막았다. 아울러 러시아에 대한 서방의 '사이버 공격'도 가해졌다. 2022년 6월, 폴 나카소네 미 국가안보국장 겸 사이버사령관은 영국 언론과의 인터뷰에서, 러-우 전쟁에서 미국이 '선제적 사냥(Hunt Forward)'이라고 불린 사이버 작전을 실시했다고 밝혔다.

러-우 전쟁이 장기화 국면에 들어섰지만, 러시아는 물리전의 수행과 함께 자신들의 독특한 방식으로 사이버전을 지속할 것으로 예견된다. 사실 러시아의 사이버 안보 전략은 러시아의 독특한 역사적 전통과 지정학적 정세 인식에서 비롯된 산물이다. 독자적인 슬라브 문명국으로 자부하는 러시아는 서방의 위협으로부터 자신의 정체성을 수호하고 국가안보를 지키는 차원에서 사이버전의 수행을 이해한다. 러시아의 관점에서 사이버 공간은 서방 진영의 공세로부터 자국의 영토적 완결성을 보전하고 국가적 통합을 이루기 위해 지켜야 할 '주권 공간'이다.

이런 이유로 러시아는 미국이 내세우는 '사이버전'보다는 '정보전(戰)'의 개념을 강조한다. 러시아가 1997년에 처음 '국가안보전략'을 발표한 이후 다섯 번째로 나온 2021년 6월의 '국가안보전략'은, 사이버 안보 전략과 관련해서 '정보전'에 상당히 큰 비중을 두고 있다. 러시아는 이러한 '정보전' 개념에 기반을 두고 전시와 평시를 막론하고 '사이버전'을 수행하는 전략을 펼치고 있다. 러시아의 '사이버전' 수행은 연방보안국(FSB), 연방군 총참모부 정보총국(GRU), 대외정보국(SVR) 등과 같은 국가 정보기관과 군이 수행하는데, 이밖에도 다양한 민간 또는 비국가 행위자들이 동원되고 있다.

사이버 외교의 추진 차원에서도 러시아는 서방 진영이 주도하는 자유주의 질서의 규칙을 그대로 수용하기보다는, 자신들이 주장하는 '주권' 개념에 입각해서 새로운 질서의 규칙을 만들자고 주장한다. 미국 주도의 자유주의 진영과 러시아와 중국을 위시한 권위주의 진영 간의 대립 구도

가 사이버 안보 분야에서도 드러나고 있다. 양자외교 관계에서도 러시아는 중국과의 사이버 연대를 통한 '디지털 권위주의' 블록 형성을 도모하고 있다. 미중 전략경쟁이 심화하면서 러중 디지털 협력의 필요성은 더욱 커지고 있는데, 첨단 디지털 기술 분야와 함께 사이버 안보 분야에서도 다양한 모색이 이루어지고 있다.

최근 북러 군사협력의 전개는 한국의 안보에 큰 위협이 아닐 수 없다. 북러 군사협력을 통해서 북한 문제는 핵·미사일 이슈를 넘어서 새로운 지평으로 확장되고 있다. 러시아의 러-우 전쟁 수행을 지원하는 북한의 대러시아 무기 지원이나 북한의 군사 정찰위성 개발을 지원하기 위한 러시아의 대북한 첨단 군사 기술 이전 등이 새로운 쟁점으로 부상하였다. 이와 더불어 북러 양국 간에 사이버 안보 분야의 협력이 진행될 가능성도 우려된다. 북한이 세계적 앞선 사이버 공격력을 지닌 러시아로부터 기술을 지원받거나, 러시아가 주도하는 국제규범의 플랫폼 위에서 사이버 안보협력을 전개할 가능성도 없지 않다.

이렇게 러시아의 사이버 위협이 직간접적으로 제기되는 상황에서 한국과 나토 간에도 새로이 협력관계를 마련할 필요성이 제기된다. 사이버 위협 대비 공동 지휘체제 운용이나 사이버 훈련 및 작전 수행 등의 차원에서, 나토의 사이버 방위 모델이 우리에게 주는 시사점이 매우 크다. 여기에 더불어 최근에는 미국 주도의 동맹협력 차원에서 한-나토 사이버 안보협력의 움직임도 활발히 진행되고 있다. 이미 한국은 나토 '사이버방위센터(CCDCOE)'에 기여국으로 가입했고, 나토 차원의 사이버 방어 훈련인 '락드쉴즈(Locked Shields)'에도 참가했다. 일반 안보협력 차원에서도 한국은 2023년 7월 나토 정상회의에서 기존 안보협력을 한 단계 격상시킨 '개별맞춤형 파트너십 프로그램(ITPP)'을 체결했으며, 나토의 '전장정보 수집활용체계(BICES)'에도 참여했다.

2024년 7월 열린 나토 정상회의는 나토와 '인도·태평양 4대 파트너 국가(IP-4),' 즉 한국, 일본, 호주, 뉴질랜드의 협력을 언급하면서, 우크라이나 지원, 사이버 방어, 허위조작정보 대응, 첨단기술 등을 주요 협력 분야로 명시하였다. 마이클 카펜터 미 국가안보회의(NSC) 특보도 나토와 인·태 파트너 국가들이 많은 이해를 공유하며, 사이버 안보와 허위조작정보 등과 같은 다양한 현안에서 협력할 수 있다고 밝혔다. 아울러 나토 회원국 정상들은 북러 군사협력 강화에 대한 우려를 표명하는 내용을 담은 '워싱턴 정상회의 선언'을 발표했는데, 나토와 IP-4의 방위산업 협력 강화를 위한 '나토 산업 역량 확대 선언'도 채택했다.

이렇듯 사이버 안보와 관련된 '러시아 변수'의 전개는, 한반도 차원을 넘어 시야의 지평을 넓힐 것을 요구한다. 멀리 유럽 지역에 발발한 러-우 전쟁에서부터 미러 대결을 배경으로 한 러시아의 정보전 수행 및 국제규범·외교 전략, 그리고 북러 군사협력과 한-나토 협력으로 이어지는 사태 전개의 연장선에서 '러시아 변수'가 한국에 주는 의미를 되새겨 보아야 한다. 이러한 과정에서 문제시되는 이슈 영역도 좁은 의미의 사이버 안보만이 아니라, 좀 더 넓은 의미의 국제정치적 이슈들, 즉 전쟁과 외교, 경제와 규범으로 확장되고 있음도 놓치지 말아야 한다. 주변4망(網)의 사이버 국제관계를 복합적으로 활용하는 차원에서 '러시아 변수'를 보는 발상의 전환이 요구된다.

이 책의 제4부 "러시아의 사이버 안보-국방-외교 전략과 한러관계"는 이상에서 제기한 문제의식을 발전시킨 세 편의 논문을 실었다. 제11장 "러시아의 사이버 안보전략"(윤민우)은 한국을 둘러싼 주요 사이버안보 주변 강대국들 가운데 러시아의 사례를 살펴보았다. 러시아의 사이버 안보 전략은 러시아의 독특한 지정학적이고 전략적인 인식과 개념을 반영하는 독자적인 전략 전통의 결과물이다. 러시아는 글로벌 인터넷을 미국의 패권공간으로 인식한다. 따라서 러시아 국가의 통제 아래 러시아의 주권이 작동하는 독립된 공간으로 사이버 공간을 구축하고 싶어 한다. 러시아의 이와 같은 주권과 사이버 공간에 대한 인식은 근본적으로 미국·서방의 주권과 사이버 공간에 대한 인식과는 다르다.

러시아의 이와 같은 주권적 사이버 공간의 시각에 기초하여 사이버 위협을 복합적으로 인식한다. 이에 따라 러시아는 사이버 위협이라는 개념 대신에 정보 위협이라는 개념을 사용한다. 러시아의 정보 위협에는 악성코드와 같은 물리적·기술적 침해뿐만 아니라 러시아의 문화적·정신적·도덕적 가치를 위협하는 정보 내용이 포함된다. 러시아는 이를 정보-기술과 정보-심리의 위협으로 구분하며 모두 정보충돌 또는 정보전쟁의 위협으로 인식한다. 러시아의 격리된 배타적 사이버 공간에 대한 방어는 외부로부터의 정보-기술과 정보-심리의 위협 모두를 의미한다.

이처럼 러시아의 사이버 안보전략은 러시아의 유라시아 문명으로서의 독특한 자기인식과 철학과 가치관, 세계관을 담고 있으며, 이를 구체화한 국가 안보전략의 기반 위에 세워져 있다. 또한 이와 같은 러시아의 사이버 안보전략은 군사부문과 비군사부문으로 나뉘어 추진된다. 전자는 러시아의 군사 및 정보 부문과 관련이 있으며 전·평시를 막론한 정보전쟁 수행으로 구체화 된다. 후자는 경제산업, 법제, 국내보안 등의 문제와 관련되며, 독자적인 러시아 인터넷망 구축이라는 구체적 추진 전략으로 구현된다. 이러한 러시아 사이버 안보전략은 적어도 2000년 이후로 지난 20여 년간 꾸준히 지속적으로 일관되게 추진되어 오고 있다.

제12장 “우크라이나 전쟁과 사이버전: 러시아-나토의 맥락”(신범식)은 러시아의 사이버 공격에 대응하고 우크라이나의 사이버 전쟁 수행을 지원하는 나토의 전략과 이에 따른 영향 및 함의를 고찰하였다. 2022년 2월 24일 발발한 러시아-우크라이나 전쟁의 사이버전 양상과 전쟁을 지원하는 타국의 역할은 현대전에 새로이 등장한 사이버 공간이 전쟁에 미치는 영향에 대한 통찰력을 제공한다. 세계적으로 최고 수준의 사이버 공격 역량을 보유한 것으로 알려진 러시아는, 전쟁 개시 이래 사이버 공간을 활용한 사이버전, 정보전, 심리전, 하이브리드전을 다면적으로 수행하였다.

이에 대응하여 우크라이나도 미국과 나토를 위시한 서방 국가들의 적극적인 지원을 통해 러시아의 사이버 공격에 대응하고 있다. 전쟁 전후 대대적 사이버 공격을 실행하여 전쟁에서 승기를 잡고 전쟁을 속전속결로 끝내려는 러시아의 전략은, 우크라이나의 강화된 사이버 방어역량과 나토의 적극적 지원으로 실패하였다. 나토는 분쟁을 확대하지 않으면서 가시성이 낮은 사이버 영역에서 우크라이나를 적극적으로 지원하고 있다.

그러나 우크라이나전의 확대는 나토는 물론 러시아도 우려하는 상황으로, 러시아의 사이버 공격의 영향이 지리적 경계를 넘어 나토 회원국에 미칠 경우, 나토 조약 제5조의 집단방위체제가 가동될 것이 우려되고 있으며, 전쟁에서 나토의 역할이 커짐에 따라 전쟁 확전의 계기 내지는 게임 체인저가 될 수 있는 우크라이나 전쟁의 사이버전적 측면은 우려와 관심의 대상이 되고 있다.

제13장 “러시아의 사이버 안보외교: 중러의 전략적 협력과 권위주의 국가의 사이버 국제연대”(두진호)는 사이버안보에 대한 러시아 및 중국의 위협인식을 식별하고, 이들이 전개하는 사이버 국제연대의 특징과 실태를 살펴보았다. 2022년 러시아의 우크라이나 침공으로 시작된 글로벌 차원의 세력권 분리 현상은 사이버 공간에서 민주주의 진영과 권위주의 진영 간 갈등과 대결을 심화하는 요인으로 작용하고 있다. 러시아의 안보 정체성에서 사이버 영역은 주권적 영역이자 사활적 이익의 대상이다. 러시아는 서구식 민주주의 유입 등 이른바 ‘색깔 혁명’을 신흥안보 영역에서의 가장 심각한 위협으로 인식하고 있다. 이런 맥락에서 사이버 공간은 국가의 전통적 가치를 훼손하고 국가통합을 방해하는 서방의 사이버 영향력 공작에 대비해 반드시 확보해야 할 ‘전장영역’이다.

사이버 영역에 대한 러시아와 중국의 위협인식은 국가주의 및 국가 중심성이라는 ‘사이버 안보 정체성’으로 수렴된다. 중국에도 정보화 및 경제성장은 정보통신기술과 시장의 성장을 견인하지

만 동시에 사이버 공격 및 테러 등 내부 취약성을 키우는 요인이다. 또한 중국도 미국이 전략경쟁 수단으로 사이버 안보를 활용한다는 인식을 견지하고 있는 만큼 사이버 영역은 중국 공산당의 핵심적인 관리 대상으로 인식하고 있다. 이렇듯 사이버 공간에 대한 러시아와 중국의 일치된 인식은 미국 등 서방의 사이버 패권에 대응해 연대를 강화하고 이란 및 북한 등 동지국가들의 연대를 촉진하고 있다. 여기에 우크라이나 전쟁과 이스라엘-하마스 무력충돌로 촉발된 세력권 분리 현상이 글로벌 차원의 사이버 영역의 진영화를 가속화하고 있다.

Ⅵ. 맺음말

오늘날 사이버 안보는 국가안보의 핵심 어젠다로 명실상부하게 부상했다. 우리에게 제일 큰 과제는 북한의 공세적 사이버 공격에 대한 대응이다. 그 대응 방안으로 사이버 안보 분야의 기술역량 강화와 위협정보 공유, 공급망 안보의 확보 등이 필요하다. 사이버 범죄 및 테러의 예방·대응 역량 제고도 큰 과제이다. 이에 효과적으로 대응하기 위해서는 사이버 안보 관련 법제도와 국가적 수행체계를 정비해야 한다. 국방 분야에서도 사이버전 수행 역량의 강화, 사이버 불법 활동과 사이버 영향력 공작의 차단 및 이를 위한 사회적·제도적 기반의 조성, 그리고 사이버 군사전략의 추진 등이 중요한 과제이다. 이외에도 외교 분야에서 사이버 안보 동맹 협력 및 소다자 협력체에의 참여, 사이버 안보 국제규범 및 지역협력 외교의 추진, 사이버 안보 분야 국제 민관협력 추진 등의 필요성도 제기된다.

공격자가 우위에 서는 사이버 안보 분야의 특성상 방어와 억지 역량의 구축이나 추진체계 정비와 법제정의 노력만으로 효과적인 대응 방안을 마련할 수 없다. 이런 점에서 초국적으로 발생하는 사이버 공격에 적절히 대응하기 위해서는 주변 국가들과의 국제협력과 이러한 과정에서 발생하는 문제들을 풀어가는 외교적 노력이 병행되어야 한다. 전통적인 우방국인 미국과 일본, 그리고 최근 그 중요성이 커지고 있는 중국 및 글로벌 변수로서 의미를 갖는 러시아 등과의 사이버 외교 추진에 대한 인식의 제고와 적극적인 실천은 매우 중요한 과제가 아닐 수 없다. 특히 북한의 사이버 공격과 관련하여 관건이 되는 것은 이들 국가와의 정보공유 네트워크를 구축하고, 사법공조를 위한 외교적 노력을 펼치거나, 국제규범의 형성 과정에 참여하여 호소하는 문제이다.

사이버 안보의 국제정치를 기존의 '세력균형' 시각을 넘어서 '세력망'의 입체적 시각으로 보는 발상의 전환이 필요하다. 물론 사이버 안보의 이슈가 장차 한반도의 고질적인 지정학적 이슈와 결합할 가능성도 놓쳐서는 안 된다. 그러나 동시에 냉전 시대에 잉태된 단순동맹 전략의 시각에서 주변4망(網)과의 관계를 풀어가는 오류도 경계해야 한다. 그도 그럴 것이 사이버 안보를 위한 바람직한 대응방안은 어느 일면만을 강조하는 접근이 아니라 기술과 전략, 국가와 사회, 일국적 대응과 외교적 대응, 양자적 해법과 다자적 해법, 지역적 협력과 글로벌 협력 등을 다방면으로 아우르는 복합전략에서 찾아야 하기 때문이다. 사이버 안보 문제가 급속히 국가안보의 문제로 부상하는 속도만큼 우리 모두의 중지(中智)를 모아서 이 분야에서 제기되는 위협에 대한 대응방안을 시급히 탐구하는 국제정치학적 연구가 시급히 필요한 때이다.

〈참고문헌〉

이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.