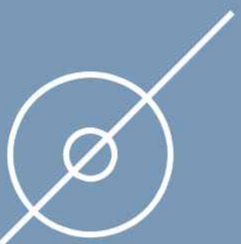
러시아의 사이버 안보외교:



중러의 전략적 협력과 권위주의 국가의 사이버 국제 연대

2024

한국사이버안보학회
KACS

한국사이버안보학회 워킹페이퍼 26호
발간일: 2024년 8월 25일

두진호 (한국국방연구원)

I. 문제제기

세계적 차원의 전략경쟁이 디지털 플랫폼 경쟁으로 변화하고 있다. 첨단기술을 탑재한 디지털 플랫폼은 사이버 공간에서 광범위하게 영향력을 행사할 수 있으므로 군사력 등 물리적 자원과 역량 투입 없이 소기의 전략목표를 달성하는 이점을 갖는다. 러시아는 푸틴 대통령 집권 이후 슬라브주의 복원 및 역사 공정이라는 국가 대전략을 추구하고 있다. 2022년 2월 러시아의 우크라이나 침공이 국가 대전략 실현을 위한 '직접 전략'이라면, 침공에 앞서 러시아군이 우크라이나를 상대로 장기간 지속적으로 실시한 DDos 공격 및 허위조작정보 확산, 네트워크 교란 등 '영향력 공작'은 대표적인 '간접전략'이다.[1)]

역설적으로 러시아의 우크라이나 침공은 사이버 영향력 공작 등 간접전략의 실패로 인한 극단적 행위이다. 2014년 러시아군은 크림 자치공화국과 세바스토폴 특별시 등 크림지역에 무혈입성했다. 러시아군은 군사적 관여 이전에 '영향력 공작'을 통해 결정적 군사행동은 최소화하면서 러시아의 승리를 '기정사실화' 했다. 우크라이나군은 크림 피탈 이후 북대서양조약기구(NATO·나토) 등 서방의 조력을 받아 전방위적 국방개혁을 추진했다. 우크라이나는 나토와 연합 사이버 방위센터를 개소한 이후 러시아의 사이버 공격에 효율적으로 대응할 수 있었다. 우크라이나에 대한 러시아의 사이버 영향력 공작은 크림 병합 이후 실효성을 상실했다. 오히려 러시아가 우크라이나 및 나토의 사이버 공격에 노출되면서 '디지털 주권'에 도전을 받는 역전 현상이 발생하고 있다.

〈표 1〉 전통적 경쟁 사이버전의 비교분석

구 분	직접 전략(전통적 경쟁)	간접 전략(사이버전)
속도	• 물리적 한계	• 순간적
비용	• 고비용	• 저비용(고효율, 가성비)
공격 행위자	• 가시적, 직관적	• 비가시적, 불분명
전·평시 구분	• 비교적 분명	• 불분명
공격 원점 식별	• 공격 징후 관측 및 식별 가능	• 식별 제한
대상 범위	• 인명 및 주요 인프라에 집중 등 치명적 효과	• 다양한 종류의 피해 발생, 사안에 따라 치명적 효과 유발

1) 러시아는 정찰총국 산하의 해커집단 샌드웜(Sandworm)을 이용해 우크라이나에 여러 와이퍼(Wiper) 악성코드를 활용한 공격을 수행하고 있다. 와이퍼 악성코드는 시스템의 철저한 불능화를 목적으로 개발돼 여타 악성코드에 비해 대처와 복구가 까다롭다고 평가된다.

출처: 한국국방연구원「국방논단」제1431호 및 국방기술진흥연구소 국방과학기술정보 제118호 등을 참고하여 일부 수정

우크라이나는 나토 회원국 등 서방 30개국의 전력 제공에 힘입어 전쟁 지속 능력을 강화하면서 러시아의 총체적 국력 약화를 강요하고 있다. 푸틴 대통령은 5선 취임 이후 첫 해외 일정으로 중국을 국빈 방문하여 연합 훈련 강화 및 경제 분야에서 무제한적 협력에 합의하는 등 2019년 체결된 '신시대 전면적 전략 협력동반자 관계'를 질적·양적으로 격상하고 있다.[2] 한편, 중국은 2010년대 중반부터 '사이버 주권' 개념을 본격적으로 사용하며 금융-빅테크 부문의 연계를 통해 생산우위와 가격 경쟁력을 앞세워 서방의 디지털 시장에 파고드는 등 미국의 디지털 패권에 대응하고 있다. 미중 전략경쟁 및 우크라이나 전쟁 장기화, 그리고 이스라엘-하마스 전쟁 발발 등 글로벌 전략환경은 중러의 전략적 협력을 촉진한다.

중국은 러시아에 대한 물리적 지원 대신 인공지능(AI) 및 사이버 안보협력 등 비물리적 차원의 협력을 통해 미국의 일극주의에 대응하기 위한 '디지털 권위주의 블록'을 구성할 가능성이 커지고 있다. 한편 러시아는 재래식 무기와 탄약이 고갈되면서 지리적 접근성과 상호운용성을 갖춘 북한과 '위험한 거래'에 나섰다. 특히 푸틴 대통령이 24년 만에 평양을 방문해 양국 관계를 '포괄적 전략동반자 관계'로 수직 격상시키고, 사실상 동맹 관계를 부활해 한미 동맹 및 한미일 안보협력에 대한 대응은 물론 허위조작 정보 및 인공지능 등 사이버 공간에서 협력에 합의했다.

II. 러시아의 사이버 안보: 위협인식과 사이버 주권

푸틴 집권 기간 네 차례에 걸쳐 발표된 국가안보전략서를 검토해보면, 나토의 확장과 동유럽 지역에서 미국이 주도하는 미사일 방어 시스템(Missile Defense, MD) 및 중·단거리 미사일 배치 등은 러시아를 위협하는 가장 심각한 전통적 요인으로 평가된다. 한편, 비전통 안보 분야에서 위협 요인은 테러 및 색깔 혁명[3], 정보 왜곡 등으로 파악된다.[4] 국가안보전략서에 기술된 정보 왜곡에 대한 러시아의 위협인식은 미국의 사이버전, 정보통신기술을 활용한 서방의 반러 선전·선동 및 러시아의 이미지와 역사 왜곡, LGBT(Lesbian, Gay, Bisexual, Transgender)의 사회적 확산 등 전통적·종교적 측면에서 러시아 고유의 가치 왜곡과 정체성 형해화 등으로 요약된다.

러시아는 2023년 3월 대외정책개념을 발표했다. 사실상 '전시 문서' 성격의 대외정책개념은 '러시아는 독자적 문명권을 가진 국가로서 서방의 위협으로부터 고유의 전통과 정체성 수호 등의 사명'을 기술하고 있다. 즉, 슬라브주의를 독자적인 문명으로 규정하고 러시아 문명의 시각에서 세계질서를 해석하고 확립하겠다는 의지를 재확인했다. 러시아의 사이버 안보는 국가안보전략 및

2) 중국은 러시아의 침공에 대해 소극적인 찬성 입장을 취할 뿐 적극적인 협력에는 선을 긋고 있다. 양국이 장기간 군사협력 등 초보적 수준에서 연합태세를 확립한 만큼 러시아는 중국이 어떤 행태로든 특별군사작전에 대한 관여를 기대하지만 중국의 물리적 지원 가능성은 적다.

3) 색깔혁명 (color revolution)은 CIS 지역에서 발생한 민주화를 위한 시민운동을 의미한다. 2003년 조지아의 '장미혁명'으로 셰바르드나제 대통령이 퇴진하고 친미 성향의 사카슈빌리 대통령이 당선됐다. 2004년 우크라이나에서는 '오렌지 혁명'을 통해 친서방 성향의 유셴코 대통령이 집권했다. 2005년 키르기스스탄에서는 국회의원 부정선거를 규탄하는 시위가 정권 퇴진운동으로 발전하면서 '튤립 혁명'을 통해 정권 교체가 이루어졌다. 러시아는 색깔혁명을 서방의 '정치 공작' 혹은 '영향력 공작'으로 인식한다. 러시아는 CIS에 대한 서방의 '영향력 공작'은 정보조작 및 허위정보 유포, 역사 왜곡 등 인터넷 등 디지털 수단을 활용해 궁극적으로 러시아의 연방제 붕괴를 추구한다고 인식한다.

4) Стратегия национальной безопасности Российской Федерации; Концепция внешней политики Российской Федерации; Доктрина информа-ционной безопасности Российской Федерации.

대외정책개념의 전략지침을 적극적으로 수용하고 있다. 러시아는 미국 등 서방에 대해 서구식 민주주의 확산 및 NGO 등의 정치 공작을 통해 러시아의 정체성을 무력화하고 궁극적으로 러시아 연방 붕괴 등 국가전복을 시도하는 '악한 세력'으로 인식한다.[5] 따라서 러시아 관점에서 사이버 공간은 서방의 영향력 공작과 슬라브주의가 경쟁하는 '제2전선'과 다름없으며, 러시아의 영토적 완전성 실현 및 헌정 질서 유지 등 국가통합을 위해 반드시 확보해야 할 주권적 영역이다.

III. 중국의 사이버 안보 인식과 중러의 전략적 협력

중국은 대내적으로 정보화 및 경제성장으로 정보의 양 증가는 물론 정보의 자유로운 유통이 중국 공산당의 통제 수준을 벗어나고 있는 상황에 대한 대응이 요구된다. 한편 대외적으로 정부 및 기업의 정보통신 의존도는 외부로부터의 사이버 공격, 테러및 관련 범죄 양산 등 내부의 취약성을 키우는 위협 요인으로 인식한다. 이에 따라 중국은 금융-빅테크 부문의 연계를 통해 사이버 주권을 강화하고 있다. 모바일 결제의 보편화 등 디지털 수단의 발전으로 중국 사회에서 현금 결제가 사라지고 있으며, 현금 유통의 보편적 수단인 ATM 활용도 감소하고 있다.[6] 반면 알리페이와 위챗페이 등 대규모 핀테크 전자 거래를 통한 자금 유통은 시·공간을 초월해 중국의 거대 금융망을 형성하고 있다.

문제는 모바일 결제의 경우 중국 은행 계좌 보유가 전제되어야 하며, 중국 국적을 보유하거나 6개월 이상의 체류 비자가 있어야 중국 은행 계좌 개설 가능하다는 점이다. 알리페이나 위챗페이 계정을 통한 모바일 결제는 중국의 국가 통제 시스템에 개인 정보의 유통과 통합을 의미한다. 모바일 결제 서비스는 사회 신용 시스템과의 연동을 지향하며, 모바일 서비스를 통해 수집된 내·외국인의 모든 통신 및 금융 정보는 중국 정부의 사회보장 정책에 활용되는 측면과 함께 사이버 공간에서 주요 통제 수단으로 활용될 수 있다.

중국은 미국이 전략경쟁 수단으로 사이버 안보를 활용한다는 인식을 견지하고 있으며, 미국 중심의 사이버 패권을 중요한 대외 위협 요인으로 간주한다. 이에 따라 중국은 사이버 안보에서 국가의 주도적 역할을 기반으로 내부적 관리 및 통제력을 확립하여 공산당의 통치 안정성과 예측성을 높이고 대외적으로 디지털 독립을 추구하여 국익을 보호하고자 한다.

2016년 중국은『국가 사이버 공간 안전전략』과『사이버 공간 국제협력전략』등의 전략문서를 통해 사이버 주권을 강조하면서 국가 안전 유지 및 사이버 국제협력 강화 등 일련의 전략목표를 제시하고 있다.[7] 특히 해킹으로 인한 국가 분열과 반란 및 선동, 국가기밀 누설 등의 행위를 중대 범죄행위로 간주하고 이를 예방하기 위한 군사적 수단의 동원 필요성을 정당화한다.[8] 또한

5) 러시아는 미국과 서방세계의 합의된 개념과는 매우 다른 사이버 공간의 본질과 잠재성, 그리고 이용에 대한 관점과 인식을 가지며, 이러한 서로 다른 인식과 관점의 차이는 미국-서방과 러시아 사이에 사이버 안보에 대한 근본적인 불일치와 갈등을 야기한다. 러시아의 인식에서 인터넷은 지배적인 미국 과학기술과 문화 그리고 패권의 부산물이며, 이 같은 인터넷은 러시아의 과학기술 및 문화의 온전성과 독립에 대한 중대한 위협이다. 정보의 자유롭고 개방적 공간인 인터넷의 확장을 미국이 일방적으로 주도하는 것은 러시아의 정치, 경제, 군사, 문화, 역사, 종교적 주권에 대한 중대한 지정학적 도전이며 위협으로 받아들여진다. 신범식·윤민우, "러시아의 사이버안보 전략 실현의 제도와 정책,"『국제정치논총』제60집 2호(2020), p. 169.

6) 최선경, "중국의 사이버 안보와 국가의 확장,"『Sungkyun China Brief』제11권 1호(2023), pp. 43-44.

7) 9가지 전략목표는 다음과 같다. △국가안전 유지, △정보 기반시설 보호, △사이버 문화 건설, △사이버 범죄와 테러 예방, △사이버 거버넌스 체제 개선, △사이버 안전 기초 마련, △사이버 방어력 향상, △그리고 사이버 국제협력 강화

8) 김상배, "세계 주요국의 사이버 안보 전략: 비교 국가전략론의 시각," 국제지역연구 제26집 3호(2017), pp. 83-86.

사이버 공간에 대한 전략적 실행은 미국의 대중국 견제 및 사이버 패권 확보에 대항하기 위해 우호적인 국제 연합전선 구축 및 자체 기준의 국제 표준화를 지향한다. 2014년부터 2018년까지 중국에서 개최된 〈세계인터넷대회〉, 상하이협력기구(Shanghai Cooperation Organization, SCO)와 아세안지역안보포럼(ASEAN Regional Forum, ARF) 내 영향력 확대, 국제연합(UN)과 국제기구 규범 수립 과정 참여, 국제전기통신연합(ITU)이 주도하는 인터넷 관장 권한 요구가 이를 뒷받침하는 대표적인 사례다.[9)]

〈표 2〉 중러의 사이버 안보 인식과 전략적 협력

구 분	중국	러시아
위협요인	• 디지털 수단에 대한 의존 심화 • 해킹, 허위정보, 정보탈취 등 국가기밀 유출 • 미국의 사이버 패권	• 러시아 전통 및 정체성을 부정하는 허위정보 유통 등 국가전복 행위 • 미국과 나토의 사이버 패권
대응개념	• 국가중심적 사이버 주권 확립	• 국가중심적 사이버 주권 확립
대응목표	• 공산당 통치 안정성 확보, 사이버 강국 달성	• 주권 보호 및 영토적 완전성 보장, 헌정 질서 확립
국제협력	• 상하이협력기구(SCO), 아세안지역안보포럼(ARF) 영향력 확대	• 상하이협력기구(SCO), 집단안보조약기구(CSTO), 아세안지역안보포럼(ARF) 영향력 확대

사이버 안보에 대한 중국과 러시아의 공통적인 관점은 '사이버 주권'과 같은 국가중심적 역할의 필요성과 정당성이다. 중국과 러시아는 사이버 공간에서 벌어지는 각종 허위조작정보 유통과 각종 기밀 누설, 특정 개인과 단체를 대상으로 발생하는 해킹 공격 및 정보 탈취 행위 등에 대해 '국가전복'이라는 극단적인 위협인식을 공유한다. 양국 모두 사이버 공간을 통해 장벽 없이 유입되는 서구식 민주주의 가치는 궁극적으로 '색깔 혁명'을 인위적으로 조작한다는 인식을 같이한다. 따라서 중러의 사이버 공간은 고유의 전통과 정체성, 정권의 안정성 확보를 위해 주권과 같은 불가침 영역이다. 이런 점에서 사이버 안보에 대한 중러의 이해관계는 일치한다.

한편, 중국과 러시아는 사이버 분야에서 국가 주도의 자원과 역량 동원 등 중앙 집권적 관리 및 통제라는 유사성을 공유한다. 특히 러시아는 특별군사작전의 시행착오를 통해 수많은 인명피해와 사이버 기술의 진화적 발전을 촉진하는 광범위한 데이터 수집을 교환했다. 러시아 국방 당국이 향후 인공지능의 군사적 목적을 천명한 만큼 인명피해와 교환된 데이터는 러시아의 중앙집권적 통제 아래 디지털 권위주의 강화에 적극 수용될 것이다.

중러 정상은 2024년 베이징 정상회담 공동성명에서 "개별 국가의 인공지능 개발을 악의적으로 억지하는 데 반대한다"는 입장을 내는 듯 첨단 산업에 대한 미국 견제에 공동 대응 의지를 밝혔다. 특히 푸틴 대통령이 방중 이튿날 중국의 지능화 사회를 첨단 혁신기술로 뒷받침하는 하얼빈 공대를 방문한 것은 향후 사이버 안보 협력 고도화 등 인공지능 협력을 위한 정치적 의지로 보인다. 이런 배경에서 특별군사작전을 통해 습득 및 검증된 러시아의 데이터와 사이버 안보

9) 김진형, "중국 사이버안보의 전략과 체계," KIEP 전문가 오피니언(2022), pp. 2-3.

기술 등은 중국에 매력적이다.

IV. 권위주의 국가의 사이버 연대

1. 디지털 권위주의 블록의 출현과 지향성

중국과 러시아는 미국 중심의 단극적 사이버 패권을 경계한다. 형식상 민주주의 체제를 유지하고 있으나 내용상 공고화된 권위주의 체제를 지향하는 러시아에 사이버 공간을 통한 서구식 민주주의 확산 등 색깔 혁명 가능성은 푸틴 정권의 안위에 치명적이다. 푸틴 정권의 안위는 러시아 연방의 불확실성과 맞닿아 있으므로 사이버 주권 수호는 사활적 이익이다. 여기에 특별군사작전 장기화로 나토 등 서방의 사이버 공격에 빈번하게 노출된 러시아의 상황은 유사한 사이버 안보 위협을 공유하는 동맹 및 우방국들과의 협력을 촉진하는 요인이다.[10)]

2024년 5월 푸틴 대통령의 5선 취임 이후 중국 국빈 방문을 계기로 중러 양국은 2019년 합의한 '신시대 전면적 전략 협력동반자 관계'를 심화·발전시키는 데 합의했다.[11)] 다만, 러시아의 우크라이나 침공에 대한 중국의 소극적인 입장으로 중러의 전략적 협력이 정치적 수사 수준에 갇혀 있다는 평가도 존재한다. 중국은 내수 활성화 등 경제 회복을 위해 서방과 디커플링(탈동조화)을 회피하고 리스리킹(De-risking·위험 억제)을 견인해야 하는 상황에서 러시아와는 물론 북중러 3각 협력 등 민감한 분야에서 적극적인 행보에 나서는 데 부담을 안고 있다.

하지만 미국의 사이버 패권에 대한 중국과 러시아의 위협인식은 유사하다. 기본적으로 양국은 미국의 사이버 패권에 반대하며, 독자적 사이버 질서를 확립하여 독립적이고 고유한 디지털 생태계를 추구한다. 특히 미국의 사이버 패권에 대해 '국가전복'과 같은 냉전적·대결적 관점을 견지한다는 측면에서 사이버 공간에서 양국의 전략적 협력은 합리적이다.

중국의 디지털 실크로드(Digital Silk Road) 전략에 주목할 필요가 있다. 중국의 디지털 전략은 중국 기업과 표준에 유리한 무역 네크워크 구축을 추구한다. 중국은 일대일로 참여국을 중심으로 네트워크 통신인프라를 구축하여 자국 중심의 디지털 생태계를 확대해 왔으며, 제도 구축과 규범 설정과 같은 '중국식' 사이버 거버넌스 표준의 수출도 병행했다. 중국 인민 해방군 및 공안 등 정부 당국은 스리랑카 공무원들에게 웹사이트 필터링 기술을, 공안은 캄보디아 경찰에 감시 카메라 설치에 관해 자문을 제공했으며, 탄자니아에 국가 데이터 센터 건설 방안 경험을 공유했다. 상기 국가들은 중국과 지정학적 관계를 맺고 있으며, 중국 기업들의 활동이 활발하고 범죄율

10) 러시아 선거 당국은 지난 3월15일부터 17일까지 치러진 대통령 선거에서 원격 전자투표를 대상으로 한 다수의 사이버 공격을 차단했다고 밝혔다. 러시아 선거 당국은 모스크바의 선거 정보 시스템에 대한 사이버 공격이 미국과 영국에서 일어났으며, "사이버 공격 주체의 서버는 미국과 영국에 위치하고 있다"고 주장했다. Российская Газета. (2024. 3. 17). "Московская система ДЭГ отразила в ходе выборов свыше 4,6 млн кибератак."

11) 푸틴 대통령과 시진핑 주석 간 정상회담 계기 중러 양국은 공동성명을 채택하고, 정치·경제·군사·인공지능(AI) 등 모든 분야에서 협력을 심화·발전하는 데 합의했다. 중러 정상은 공동성명에서 "미국과 그 동맹국의 군사적 위협 행동(military intimidation)과 북한과의 대결을 유발하는 무장 충돌 도발로 한반도 정세의 긴장 격화에 반대한다"고 적시했다. 한편 푸틴 대통령은 중국 방문 계기에 '동방의 모스크바'이자 양국 간 교류협력을 상징하는 하얼빈을 찾아 중국과의 경제 협력에 공을 들였다. 푸틴 대통령은 중러 엑스포 개막식과 지역 협력 포럼에 각각 참석해 "에너지 분야에서 양국의 전략적 동맹은 강화될 것이라며, 러시아는 중국에 환경친화적 에너지 자원을 중단없이 공급할 준비가 돼 있다"고 강조했다. 중국은 경제 분야에서 러시아와의 무제한적 협력을 강조했고, 군사 분야와 관련해 향후 연합훈련을 확대한다는 원론적인 입장을 채택했다.

이 높은 국가들이다.

Freedom House의 인터넷 자유 지수에 따르면, 중국의 인터넷 사용 환경은 매우 억압적이며, 9년 연속 세계 최악의 인터넷 자유 침해 국가로 평가받고 있다. 중국인터넷 사용자는 약 10억 7000만 명으로 전체 인구의 약 75.6%에 달한다. 중국의 인터넷 연결 속도는 정부의 광범위한 검열 장치로 인해 의도적으로 조정되고 있으며, 외국에서 호스팅되는 웹사이트의 콘텐츠 연결도 선택적으로 지연되는 것으로 추정된다. 중국 지역별로 인터넷 속도의 편차가 존재하며, 분리주의 움직임이 강한 신장 위구르 자치구의 경우 상하이에 비교해 현격하게 낮은 인터넷 속도를 보인다. 중국의 인터넷 자유는 '만리 방화벽(Great Firewall)'과 같은 중국 당국의 비공식 인터넷 검열 시스템에 의해 구속된 상태라고 할 수 있다.

러시아의 인터넷 자유 지수는 중국과 비교해 상대적으로 높게 나타나고 있으나, 중국과 마찬가지로 인터넷 자유 억압이라는 측면에서 유사하다. 러시아는 우크라이나 침공 이후 정보 공간을 통제하기 위해 비민주적인 인터넷 규제를 시행하고 있으며, 특히 전면적인 침공에 대한 국내 비판을 억제하기 위해 인터넷 자유가 후퇴하고 있다. 러시아 당국은 페이스북, 인스타그램, 트위터 등 글로벌 소셜 미디어 플랫폼을 원천적으로 차단했으며, 사이버 공간에서 우크라이나 침공을 비판하는 개인과 조직에 대해 '허위조작정보'를 유포하는 범죄 세력으로 처리하고 있다. 러시아 정보통신 당국은 통신 사업자가 연방보안국(FSB)와 더욱 긴밀하게 협력하도록 의무화하는 법률을 도입했다. 상기 법안은 웹사이트 차단 및 감시를 용이하게 하는 TSPU(Technical Measures to Combat Threats) 시스템 설치 의무이행을 거부하는 운영자에게 벌금을 부과하는 등 인터넷 공간 감시 및 감독 활동을 강화하고 있다.[12)]

<표 3>에서 보는 바와 같이 미국과 한국 등은 비교적 높은 인터넷 자유 지수를 보여주는 것과 대조적으로 중국과 러시아, 중국의 디지털 실크로드에 영향을 받고 있는 스리랑카 및 캄보디아 등의 인터넷 자유 지수는 상대적으로 낮은 수준을 보이고 있다. 특히 러시아의 주요 동맹 및 우방국인 벨라루스와 이란은 각각 25점과 11점으로 중국과 러시아 등 디지털 권위주의 국가와 유사한 수준을 보인다.

12) https://freedomhouse.org/country/russia/freedom-net/2023 (검색일: 2024. 5. 18.).

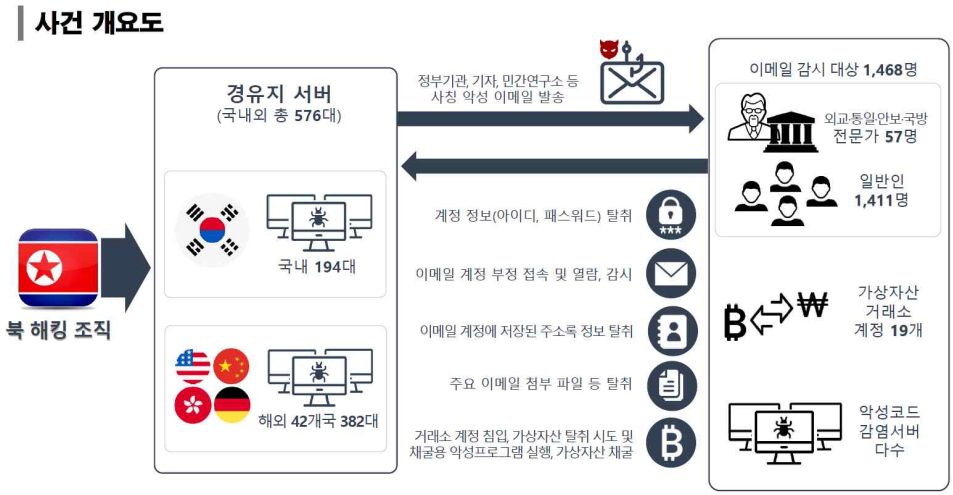
〈표 3〉 인터넷 자유 지수[13)]

구 분	Total Score and Status (100)	Obstacles to Access (25)	Limits on Content (35)	Violations of User Rights (40)
미국	76 / Free	21	30	25
한국	67 / Partly Free	22	24	21
중국	**9 / Not Free**	**7**	**2**	**0**
러시아	**21 / Not Free**	**10**	**5**	**6**
스리랑카	52 / Partly Free	12	22	18
캄보디아	44 / Partly Free	13	17	14
탄자니아	데이터 없음			
북한	데이터 없음			
이란	11 / Not Free	6	4	1
벨라루스	25 / Not Free	13	7	5

출처: https://freedomhouse.org/countries/freedom-net/scores

한편, 북한은 인터넷 자유 지수를 평가할 수 있는 데이터 자체가 존재하지 않는다. 북한은 일반 주민의 인터넷 자유를 억압하고 통제하고 있으나, 이메일 계정 탈취 및 가상자산 탈취 시도 등 인터넷을 사이버 공격 수단으로 활용하고 있다. 북한 사회의 특성상 인터넷 자유 지수 평가는 의미 자체가 구성될 수 없으므로 북한의 사이버 안보 인식은 감시 및 감독 등 내부 단속보다 외부의 특정 표적에 대해 정보 및 가상자산 탈취, 허위조작정보 유통 등 정치·경제적 목적 달성을 위한 공세적 사이버 공격에 집중되어 있다고 볼 수 있다.

〈그림 1〉 북한 해킹조직 '김수키'의 해킹 공격 개요



출처: 동아일보[14)]

13) 인터넷 자유 지수(Internet Freedom Status)란 인터넷 사용자들에게 제공되는 서비스의 접근성과 개방성 등 인터넷 사용자의 권리 보장의 수준을 보여준다. 인터넷 자유지수는 인터넷 접근 제한(25점), 콘텐츠 이용 제한(35), 사용자 권리 침해(40) 등 총 3개 요소 100점으로 구성된다. 인터넷 자유가 억압될수록 0에 수렴하고, 그 반대의 경우는 100으로 수렴한다. 한편, 인터넷 자유 지수 총점을 기준으로 0-39는 Not Free, 40-69는 Partly Free, 70-100은 Free를 의미한다.

최근 경찰청 국가수사본부에 따르면, 북한의 공세적 사이버 공격은 정찰총국 산하 해킹조직인 '김수키'(Kimsuky)는 외교안보 분야 전·현직 공무원과 전문가 등을 사이버 공격을 감행하여 내국인 1468명의 이메일 계정을 탈취했다. 김수키는 국내·외 서버 500여 개를 경유하며 인터넷주소(IP주소)를 변경한 뒤 피싱용 이메일을 발송해 표적 대상의 개인용 컴퓨터의 내부 정보를 유출할 수 있는 악성 프로그램이 설치 및 실행되는 수법을 사용한 것으로 나타났다. 북한의 사이버 공격은 한국 사회의 유력 계층에 대한 '영향력 공작'을 통해 국가정책에 영향을 미치고, 가상자산 탈취를 통해 통치자금을 확보하는 한편 국내 디지털 금융시장에 혼란을 유도하고 우리 정부의 대응 능력을 약화하기 위한 목적으로 볼 수 있다.

중국·러시아·북한 그리고 이들과 연결된 이란·벨라루스 등 디지털 권위주의 국가들의 인터넷 자유는 사실상 존재하지 않으며, 사이버 공간의 주권적 위상은 사안에 따라 개인의 정보 자율성과 이익을 침해하고 압도한다. 또한 디지털 권위주의 블록의 사이버 공간은 국가의 특정 이익과 목표 달성을 위해 정부 당국에 의해 광범위하게 조작되고 동원될 수 있는 잠재적 유사성을 공유한다고 볼 수 있다.

2. 디지털 권위주의 블록의 예상 행태

중국의 국가인터넷 정보판공실과 중앙군사위 산하의 Net-Force, 61398·61486 부대와 러시아의 해외정보국(SVR) 및 정보총국(GRU)과의 교류협력을 통해 사이버 협의 체계를 형성해 왔을 것으로 추정된다. 다만 중러의 전략적 협력이 초보적 수준에 정체되어 있으므로 사이버 안보 공동 기획 및 실행 등은 확장성의 한계를 갖는다.

이런 배경에서 북중러는 한미· 한미일 안보협력 발전을 고려해 서방 연대의 사이버 협력을 모방한 디지털 권위주의 블록 고유의 사이버 협력을 추구할 가능성이 있다. 지난 5월 중러 정상회담 공동성명에 "미국과 그 동맹국의 군사적 위협 행동(military intimidation)과 북한과의 대결을 유발하는 무장 충돌 도발로 한반도 정세의 긴장 격화에 반대한다"고 적시됐다. 푸틴 대통령이 평양 방문을 고려해 중국을 끌어들여 '북한의 뒷배'를 자처한 만큼 이번 정상회담에서 북중러 3각 협력 의제도 논의됐을 가능성도 배제할 수 없다. 이런 배경에서 특히 중국과 러시아는 북한의 참여를 전제로, 한미가 워싱턴 선언을 계기로 합의한 핵협의그룹(NCG)과 한미일 캠프 데이비드 정상회의 결과를 고려한 유사한 경로를 모방해 공동대응에 나설 가능성도 있다. 북중러 디지털 권위주의 블록이 전개할 사이버 안보 연대는 △정치적 연대(사이버 협의체 구성), △기술 및 데이터 공유, △사이버 공동대응 등을 고려할 수 있다.

〈표 4〉 한미일 캠프 데이비드 정상회의 결과 중 사이버 분야

구 분	내 용
역내 평화	• 인도-태평양 수역에서 중국의 일방적 현상변경 시도 반대 • 해외 정보조작·감시기술 오용에 따른 위협 대응 노력
대북 공조	• 북한의 완전한 비핵화와 자유롭고 평화로운 통일 한반도 지지 • 북한 불법 사이버 활동 대응 '사이버 협력 실무그룹' 신설

14) https://www.donga.com/news/Society/article/all/20231121/122282660/1 (검색일: 2023. 11. 22).

1) 정치적 연대

중국·러시아·북한 그리고 이들과 연결된 이란과 벨라루스 등 권위주의 진영은 사이버 안보 인식에서 유사한 정체성을 공유하며, 다양한 형태의 협력을 통해 '디지털 권위주의 블록'을 가시적으로 구성할 가능성이 있다. 중국·러시아·북한은 한미일 안보협력에 비례적으로 대응하기 위해 점진적으로 사이버 안보 분야에서 협력을 모색할 것으로 전망된다.

미국의 인도-태평양 전략은 대중국 견제뿐만 아니라 중국과 연계된 러시아와 북한의 위협 대응도 포함한다. 하지만 중국이 북러와 즉각적으로 물리적이고 가시적인 안보협력에 나설 가능성은 적다. 이런 점에서 중국은 군사 협력과 비교해 비가시적이고 정치적 부담이 적은 사이버 분야에서 북러와 연대를 선호할 수 있다.

중국과 러시아는 수년간 초보적인 수준에서 연합태세를 발전시켜 왔다. 시진핑 주석과 푸틴 대통령 모두 중러 연합 훈련이 특정 국가를 겨냥하지 않는다고 강조하지만[15], 미국의 패권 약화 및 다극 질서 형성 등 전략 균형 달성은 중러의 공통된 이익이다. 따라서 한미일 안보협력에 대응하기 위한 회색지대 전략은 중러 및 북중러의 합리적 선택이 될 수 있다. 특히 세르게이 쇼이구 러시아 전 국방장관이 안보 서기로 영전함에 따라 중러 간 사이버 협력 등 정보 공조는 보다 높은 수준으로 격상될 가능성이 있다.

한편, 2024년 3월 지난 3월 북한 조선중앙통신은 세르게이 나리시킨 러시아 대외정보국장(SVR)의 평양 방문 사실을 보도하고, '적대세력들의 정탐모략 책동에 대처해 협력을 더욱 강화하기 위한 실무적 문제들이 폭넓고 진지하게 토의됐다'고 강조했다. 통상적으로 정보수장 간 회동에 대해 비공개 관례를 고수해 온 북한 당국이 러시아 대외정보국장의 방북 사실을 공개한 것은 푸틴 대통령의 방북 준비를 넘어서는 정보 협력 가능성을 의미한다. 북러 정보수장의 전례 없는 만남은 향후 북러 간 해외 파견 북한 노동자 관련 인원 및 시설에 대한 방첩은 물론 사이버 안보 분야에서 협력 가능성을 시사한다. 중러·북러 양자 간 정보 공조 및 사이버 공동대응 등 정치적 연대는 북중러 3각 협력을 견인할 수 있다.

2) 기술 및 데이터 공유

중국과 러시아는 국가 주도의 사이버 대응 체계를 구축해 기술 및 데이터를 중앙집권적으로 통제하고, 국가의 자원과 역량도 비교적 수월하게 동원할 수 있다. 이런 점에서 디지털 권위주의 블록은 민주주의 국가와 비교해 상대적으로 우월한 기술 역량과 빅데이터를 구축하고 있다. 중국의 경우 핀테크 기업을 활용해 전자금융거래 플랫폼을 통해 개인정보 수집 및 처리 등 핵심 기술과 데이터를 확보하고 있으며, 러시아도 중국의 경로를 밟고 있다. 특히 특별군사작전 등 실전 경험을 통해 축적된 러시아의 광범위한 데이터가 사이버 첨단기술과 결합될 경우 상당한 파괴력을 갖출 수 있다.

국제사회는 점증하는 사이버 위협에 효과적으로 대응하기 위한 사이버 기술 개발에 박차를 가하고 있다. 초지능형 사이버 지휘통제 및 방어기술의 경우, 네트워크 영역별로 네트워크 이상징후를 인공지능으로 실시간 감시하여 사이버 위협 상황을 조기에 식별하고, 노드 차단을 통해 피해 확산 방지 및 비인가자의 침입 예방을 차단한다. 특히 빅데이터와 인공지능 기반으로 생성되

15) SPUTNIK, "Путин: Россия и Китай не создают военных союзов." (2023. 11. 8.).

는 악성코드 등 사이버 위협정보를 자동 수집 및 분석해 새롭게 식별되는 사이버 위협으로부터 내부 자산을 효과적으로 보호할 수 있다. 한편, MTD(Moving Target Defense) 기반으로 IP를 기만하여 공격자가 내부 네트워크 구조를 파악하지 못하게 침입을 방지하고 데이터를 분산 저장하여 자산을 보호하는 등의 기술 개발이 완료됐거나 추진되고 있다.

〈표 5〉 국내 사이버전 핵심기술 개발 동향

구 분	기술 개요
사이버 공간의 객체이동 및 침입감내 기술	• 정보 수집, 취약점 분석을 제공하며 시나리오 및 객체 기반의 공격 기술 • 미상의 사이버 공격 탐지 및 자원 제어, 서비스 복구를 통한 침입 감내
다중 사이버 센터 융합 및 위협분석 기술	• 다중 사이버 센서 정보 융합 및 사이버자산 구성정보 자동분석을 통한 사이버 위협정보 융합모델 개발
초지능형 사이버 지휘통제 및 능도방어 기술	• 빅데이터 및 인공지능 기반 사이버 정보 수집 및 분석 • MTD 기반의 네트워크 능동 방어
허니팟 기반 공격패턴 DNA 추출 사이버게놈 기술	• 허니팟 기반 기만 네트워크 구성 • 악성코드 DNA 추출 및 유사도 분석

출처: 국방과학기술정보, No. 118.

중국과 러시아 또한 빅데이터를 활용해 다양한 사이버 방호기술 및 사이버 회복 탄력성(Cyber Resiliance) 개발에 공을 들이고 있다. 미국 주도의 기밀정보 공유 동맹체인 '파이브 아이즈(five eyes)'가 중국의 인공지능 등 첨단기술 탈취 시도 등을 위협으로 인식하고 공동대응을 강화하고 있다. 미국 주도의 대중국 '사이버 포위'는 중국이 러시아·북한 등 권위주의 국가에 기술과 데이터를 공유해 미국 등 적대세력에 사이버 공동대응을 유인하는 기제로 작용할 수 있다. 인공지능의 능력은 학습 데이터의 질과 양에 의해 결정된다. 학습할 데이터양을 기하급수적으로 늘리고, 성공 및 실패 등 광범위한 사례를 모두 학습한다면 인공지능의 역량 또한 고도화된다. 개발도상국이자 군사 강국 북한과 이란 등 인공지능 분야의 후발주자에 중국과 러시아가 보유한 사이버 기술과 빅데이터 역량은 매력적이다.

3) 사이버 공동대응

북중러는 잠재적 경쟁 상대이자 '비우호' 국가인 미국과 유럽연합, 한국과 일본 등과 관련된 광범위한 정보공유를 통해 다른 공간에서 같은 표적에 대한 사이버 공격 등의 공동 실행을 모색할 수 있다. 즉, 북중러는 비우호국의 특정 기관 및 조직, 유력 인사에 대한 해킹 등을 통해 제3의 공간에서 공통 표적을 향해 정보 및 가상자산 탈취 등 약탈적 범죄는 물론 허위조작정보 확산 및 선거 개입을 통한 정치 관여 등의 행태도 예상된다.

중국은 공산당 산하의 다양한 요소들이 운용하는 통전 공작 조직들이 한국에서 유학생, 화교 등을 중심으로 광범위하게 조직되어 운영 중이며, 국내 시민단체와의 직·간접적 연대를 통해 선거 개입 및 여론 조작 등 '영향력 공작' 가능성이 제기된다. 또한 북중러는 이란·시리아·벨라루스 등 전통적 우방국은 물론 중동 및 아프리카, 아시아 저개발 국가 등에 '영향력 공작'을 통해 디지

털 권위주의 블록의 영향력을 확산할 수 있다. 북중러가 공통적으로 국제사회 제재의 표적이고, 이란 시리아· 벨라루스 등도 제재 대상인 만큼 제재 회피 및 무력화를 위한 디지털 권위주의 블록의 연대는 '비가시권 영역'에서 영향력 확장을 모색할 가능성이 있다.

V. 시사점

우크라이나 침공을 계기로 러시아의 대외정책은 권위주의 국가들에 대한 접근성 선호 및 강화 현상이 심화하고 있다. 국제형사재판소(ICC)가 전쟁범죄의 사유를 들어 2023년 3월 푸틴 대통령에 대해 체포영장을 발부하면서 푸틴 대통령은 124개 ICC 회원국[16] 입국이 금지된 상태이다. 러시아는 최근 상하이협력기구(Shanghai Cooperation Organization, SCO) 및 집단안보조약기구(Collective Security Treaty Organization, CSTO) 등 전통적 영향권 국가에 대한 구심력 강화는 물론 아프리카 및 중동 등 권위주의 국가들과의 협력에 공을 들이고 있다. 여기에 기존 5개국 중심의 브릭스(BRICS) 체제는 올해부터 10개국 체제로 확대 출범했다. 중국은 BRICS-Plus를 기반으로 미국 중심의 경제 및 사이버 패권에 대한 대응을 강화할 것으로 보이며, 러시아는 중국의 사이버 위협인식을 활용해 우크라이나 전쟁에 활용하는 '사이버 편승 전략'을 구사할 가능성이 있다.

미중 전략경쟁과 우크라이나 전쟁, 이스라엘-하마스 무력충돌 등 중동 사태 불안정 등 변화된 안보환경은 중러 중심의 '디지털 권위주의 블록'을 창출할 가능성을 높인다. 중러는 지정학적 리스크 관리 차원에서 당분간 전략적 협력을 고수할 것이며, 우크라이나 침공을 계기로 러시아는 이란·시리아·북한 등 전통적 우방국들과 권위주의 연대 등 전략적 공조에 더욱 의존할 것이다. 여기에 중동발 반이스라엘·반미 정서의 확산 추세는 디지털 권위주의 블록의 출현을 가속화 할 수 있다. 디지털 공간의 세력권 분리 현상은 북한의 정보 탈취 및 해킹 등 사이버 공격 강화로 이어질 수 있다는 점에서 사이버 위협 공동대응 및 사이버 회복 탄력성 강화를 위해 디지털 민주주의 블록의 적극적인 정보 공조가 필요하다.

16) The States Parties to the Rome Statute. https://asp.icc-cpi.int/states-parties (검색일: 2024. 6. 25).

〈참고문헌〉

논문

신범식·윤민우. “러시아의 사이버안보 전략 실현의 제도와 정책.”『국제정치논총』제60집 2호 (2020).

김상배. “세계 주요국의 사이버 안보 전략: 비교 국가전략론의 시각.”『국제지역연구』제26집 3호(2017).

인터넷 및 기타 자료

김진형. “중국 사이버안보의 전략과 체계” 『KIEP 전문가 오피니언』(2022).

송유근. “北해킹조직 ‘김수키’, 1400명 이메일 해킹…일반인 가상자산 노렸다”『동아일보』, 2023년 11월 23일, https://www.donga.com/news/Society/article/all/20231121/122282660/1 (검색일: 2023. 11. 30).

손태종·김영봉. “국방 사이버전 수행 발전방향.”『국방논단』제1431호 (2012).

장욱. “러시아-우크라이나 사이버전 사례로 보는 사이버전 동향과 핵심기술 발전방향.” 『국방기술정보』제118호(2024).

최선경, “중국의 사이버 안보와 국가의 확장”『Sungkyun China Brief』제11권 1호(2023).

https://freedomhouse.org/country/russia/freedom-net/2023 (검색일: 2024. 5. 18).

https://asp.icc-cpi.int/states-parties (검색일: 2024. 6. 25).

SPUTNIK. “Путин: Россия и Китай не создают военных союзов” (2023. 11. 8), https://sputnik.by/20231108/putin-rossiya-i-kitay-ne-sozdayut-voennykh-soyuzov-1080991096.html (검색일: 2024. 04. 05).

Концепция внешней политики Российской Федерации; Доктрина информационной безопасности Российской Федерации.

Российская Газета. “Московская система ДЭГ отразила в ходе выборов свыше 4,6 млн кибератак” (2024. 3. 17), https://rg.ru/2024/03/17/moskovskaia-sistema-deg-otrazila-v-hode-vyborov-svyshe-46-mln-kiberatak.html (검색일: 2024. 04. 05).

Стратегия национальной безопасности Российской Федерации.

이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.