국가전략연구위원회 이슈브리핑 15호 (발간일: 2023.11.01.)

러시아의 사이버 안보: 중러의 전략적 협력과 권위주의 국가의 사이버 국제 연대[1)]

두진호 (한국국방연구원)

1. 문제 제기

세계적 차원의 전략경쟁이 기술 패권에서 디지털 플랫폼 경쟁으로 변화하고 있다. 디지털 플랫폼은 기술 패권을 기반으로 사이버 공간에서 광범위하게 영향력을 행사할 수 있으므로 군사력 등 물리적 자원과 역량을 투입하지 않고도 소기의 전략목표를 달성하는 이점을 갖는다. 러시아는 푸틴 대통령 집권 시기 슬라브주의 복원 및 역사 공정이라는 국가 대전략을 추구해 왔다. 지난해 2월 24일 러시아의 우크라이나 침공이 국가 대전략 실현을 위한 '직접전략'이라면, 침공에 앞서 러시아군이 우크라이나를 상대로 장기간 지속적으로 실시한 DDos 공격 및 허위조작정보 확산, 네트워크 교란 등의 하이브리드 전술은 대표적인 '간접전략'이다.

역설적으로 러시아의 우크라이나 침공은 사이버 공격 등 간접전략의 실패에 따른 극단적 행위이다. 2014년 러시아군은 크림 자치공화국과 세바스토폴 특별시 등 크림지역에 사실상 무혈입성했다. 러시아군은 군사적 관여 이전에 DDos 공격 등 사이버 공격을 통해 우크라이나에 허위조작 정보를 광범위하게 유포하면서 심리적으로 러시아의 승리를 기정사실화했다. 하지만 크림 병합 이후 우크라이나군은 북대서양조약기구(NATO·나토) 표준에 부합한 전방위적 국방개혁을 추진하면서 서방과 함께 연합 사이버 방위 센터를 운용했고, 러시아의

1) 이 글은 2023년 10월 25일 제5차 국가전략포럼에서 발표된 발표문을 수정보완한 것이다.

사이버 공격에 효율적으로 대응해 왔다. 사이버 공간에서 우크라이나에 대한 러시아의 영향력 행사는 크림 병합 이후 능력과 실효성을 상실했다. 오히려 러시아가 우크라이나 및 나토의 사이버 공격에 노출되면서 '디지털 주권'에 도전을 받는 역전 현상이 발생하고 있다.

우크라이나는 나토 회원국 등 서방 30개국의 전력 제공에 힘입어 전쟁을 장기화하면서 전쟁지속능력 러시아의 총체적 국력 약화를 강요하고 있다. 러시아는 재래식 무기와 탄약이 고갈되면서 지리적 접근성과 상호운용성을 갖춘 북한과 '위험한 거래'에 나섰다. 중국과 러시아는 2019년 이후 전략적 협력 동반자관계로 양국 관계를 격상하고 전방위적인 협력을 강화하고 있으나 러시아의 침공에 대해 중국은 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 관여해주길 기대하지만 중국의 물리적 지원 가능성은 희박하다.

한편, 중국은 2010년대 중반부터 '사이버 주권' 개념을 본격적으로 사용하며 금융-빅테크 부문의 연계를 통해 미국의 디지털 패권에 대응하고 있다. 미중 전략경쟁 및 우크라이나 전쟁 장기화, 그리고 이스라엘-하마스 전쟁 발발 등 세계적 차원의 전략환경은 중러의 전략적 협력 촉진 가능성을 높이고 있다. 중국은 러시아에 대한 물리적 지원 대신 사이버 안보 협력 등 비물리적 차원의 협력을 통해 미국의 일극주의에 대응하기 위한 '디지털 권위주의 블록'을 구성해 나갈 가능성이 커지고 있다.

2. 러시아의 사이버 안보: 위협인식과 사이버 주권

푸틴 집권 기간 네 차례에 걸쳐 발표된 국가안보전략서를 검토해보면, 나토의 확장과 동유럽 지역에서 미국이 주도하는 MD 시스템 및 중·단거리 미사일 배치 등은 전통 안보 분야에서 러시아에 가장 심각한 위협요인이다. 한편, 비전통 안보 분야에서 위협요인은 테러 및 색깔 혁명, 정보 왜곡 등으로 파악된다.[2] 국가안보전략서에 기술된 정보 왜곡과 관련된 러시아의 위협인식은 미국의 사이버전, 정보통신기술을 활용한 서방의 반러 선전·선동 및 러시아의 이미지와 역사 왜곡, LGBT(Lesbian, Gay, Bisexual, Transgender)의 사회적 확산에 따른 러시아식 가치의 왜곡 등 전통적·종교적 측면에서 러시아 고유의 형해화 등으로 요약할 수 있다.

러시아는 올해 3월 대외정책개념을 발표했다. 사실상 '전시 문서' 성격의 이번 대외정책개념은 '러시아는 독자적 문명권을 가진 국가로서 서방의 위협으로부터 고유의 전통과 정체성 수호 등의 사명'을 기술하고 있다. 즉, 슬라브주의를 독자적인 문명으로 규정하고 러시

[2] Стратегия национальной безопасности Российской Федерации; Конце-пция внешней политик и Российской Федерации; Доктрина информа-ционной безопасности Российской Федерации.

아 문명의 시각에서 세계 질서를 해석하고 확립하겠다는 의지를 재확인했다. 사이버 안보에 대한 러시아의 관점도 국가안보전략 및 대외정책개념의 전략지침이 그대로 반영되고 있다. 러시아는 미국 등 서방은 서구식 민주주의 확산 및 NGO(Non-governmental organization·비정부 기구) 등의 정보 공정을 통해 러시아의 정체성을 무력화하고 궁극적으로 러시아연방 붕괴 등 국가전복을 시도하는 세력으로 인식한다.[3] 따라서 러시아 관점에서 사이버 공간은 서방의 정치 공작과 슬라브주의가 경쟁하는 '제2전선'과 다름없으며, 러시아의 영토적 완전성 실현 및 헌정 질서 유지 등 국가통합을 위해 반드시 확보해야 할 주권적 영역이다.

3. 중국의 사이버안보 인식과 중러의 전략적 협력

중국은 대내적으로 정보화 및 경제성장으로 인해 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, 테러와 범죄 양산 등 내부의 취약성을 키우는 위협요인으로 인식한다. 이에 따라 중국은 금융-빅테크 부문의 연계를 통해 사이버 주권을 강화해 왔다. 이런 배경에서 모바일 결제의 보편화 등 디지털 수단의 발전으로 인해 중국 사회에서 현금 결제가 거부되고 있으며, ATM은 반강제적으로 활용률이 감소하고 있다.[4] 반면 알리페이와 위챗페이 계정을 통한 자금 유통은 시간과 공간을 초월하여 중국의 거대 금융망을 형성했다.

문제는 모바일 결제의 경우 중국 은행 계좌 보유가 전제되어야 하며, 중국 은행 계좌는 중국 국적을 보유하거나 6개월 이상의 체류 비자가 있어야 개설이 가능하다는 점이다. 알리페이나 위챗페이 계정을 통한 모바일 결제는 중국의 국가 통제 시스템에 반강제적으로 가입해야 한다는 것을 의미한다. 모바일 결제 서비스는 사회 신용 시스템과의 연동을 의미하며, 모바일 서비스를 통해 수집된 내·외국인의 모든 통신 및 금융 정보는 중국 정부의 사회보장 정책에 활용되는 측면과 함께 사이버 공간에 대한 주요 통제 수단으로 활용될 수 있다.

중국은 미국이 전략경쟁 수단으로 사이버 안보를 활용한다는 인식을 견지하고 있으며,

3) 러시아는 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. 러시아는 독자적인 규범과 인식, 그리고 개념을 주장하고 국제적인 규범 표준으로 제시하고자 한다. 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 (2)호 (2020), p. 169.

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

미국 중심의 사이버 패권을 중요한 대외 위협요인으로 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 국가안전 유지 및 사이버 국제협력 강화 등 일련의 전략목표를 제시하고 있다.[5] 특히 해킹으로 인한 국가 분열과 반란 및 선동, 국가기밀 누설 등의 행위를 중대 범죄행위로 간주하고 이를 예방하기 위한 군사적 수단의 동원 필요성을 정당화한다.[6] 또한 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.[7]

사이버 안보에 대한 중국과 러시아의 공통적인 관점은 '사이버 주권'과 같은 국가중심적 역할의 필요성과 정당성이다. 중러 양국은 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 민주적 가치는 궁극적으로 '색깔 혁명'의 원인이 될 수 있다는 인식을 같이한다. 따라서 중러 양국의 사이버 공간은 고유의 전통과 정체성, 정권의 안정성 확보를 위해 주권과 같은 불가침 영역이다. 이런 점에서 사이버 안보에 대한 중러의 이해관계는 일치한다.

5) 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

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

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

표 1. 중-러의 사이버안보 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

4. 권위주의 국가의 사이버 연대 전망 및 시사점

중국과 러시아 양국은 미국의 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 치명적인 영향을 미친다. 푸틴 정권의 안위는 러시아연방의 불확실성과 맞닿아 있기 때문에 사이버 주권 확립은 핵심 이익이다. 여기에 우크라이나와의 전쟁 장기화로 인해 나토 등 서방의 사이버 공격에 빈번하게 노출된 러시아의 불리한 상황은 유사한 사이버 안보 위협을 공유하는 동맹 및 우방국들과의 협력을 촉진하는 요인이다.

중러 양국은 2019년 신시대 전면적 전략협력 동반자관계로 양국 관계를 격상하고 전방위적인 협력을 모색하고 있다. 중국은 러시아의 우크라이나 침공에 대해 소극적 찬성 및 선택적 중립과 같은 모호한 입장을 유지하고 있다. 하지만 미국의 사이버 패권에 대한 중국과 러시아의 위협인식은 유사하다. 기본적으로 양국은 미국의 사이버 패권에 반대하며, 독자적 사이버 질서를 확립하여 디지털 독립을 추구한다는 입장이다. 특히 미국의 사이버 패권에 대해 '국가전복'과 같은 냉전적·대결적 관점을 견지한다는 측면에서 비전통적 영역에서 양국의 전략적 협력은 합리적이다.

한편, 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 병행했

다. 중국 인민 해방군은 스리랑카 공무원들에게 웹사이트 필터링 기술을 제공했고, 공안은 캄보디아 경찰에 감시 카메라 설치에 관한 컨설팅을 했다. 또한 중국 당국은 탄자니아에 국가 데이터 센터 건설 방안 경험을 공유했다. 상기 국가들은 중국과 지정학적 관계를 맺고 있으며, 중국 기업들의 활동이 활발하고 범죄율이 높은 국가들이다.

우크라이나 침공을 계기로 러시아의 대외정책은 권위주의 국가들에 대한 접근성 선호 및 강화 현상이 심화하고 있다. 국제형사재판소(ICC)가 전쟁범죄의 사유를 들어 지난 3월 푸틴 대통령에 대해 체포영장을 발부하면서 푸틴 대통령은 최소 123개 ICC 회원국 입국이 금지된 상태이다. 러시아는 최근 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 내년부터 11개국 체제로 확대된다. 중국은 BRICS-Plus를 기반으로 미국 중심의 경제 및 사이버 패권에 대한 대응을 강화할 것으로 보이며, 러시아는 중국의 사이버 안보 전략에 편승해 우크라이나 전쟁에 활용하는 '지대 추구' 전략을 구사할 가능성이 있다.

미중 전략경쟁과 우크라이나 전쟁 장기화, 하마스 무장정파의 이스라엘 침공 등 변화된 안보 환경은 중러 중심의 '디지털 권위주의 블록'을 창출할 가능성을 높인다. 중러는 지정학적 리스크 관리 차원에서 당분간 전략적 협력을 고수할 것이며, 러시아의 우크라이나 침공을 계기로 이란과 시리아, 레바논, 북한 등 전통적 권위주의 국가들은 러시아의 영향권 편입 및 전략적 공조를 선호한다. 여기에 이스라엘-팔레스타인 사태에 따른 중동발 반이스라엘·반미 정서의 확산 추세는 디지털 권위주의 블록의 출현을 가속화 할 수 있다. 이러한 흐름은 한국에 대한 북한의 허위조작정보 유통 및 정보 탈취 등의 사이버 공격 강화로 이어질 수 있다는 점에서 동맹 및 파트너 국가들과의 정보 공유 및 사이버 위협 공동 대응 등 실천적인 공조 방안 모색이 시급하다.