국가전략연구위원회 이슈브리핑 41호 (발간일: 2025. 12. 8.)

트럼프 2기 미국의 사이버 안보 전략과 러시아의 대응

두진호 (국한국국가전략연구원 유라시아연구센터장)

Ⅰ. 문제제기

도널드 트럼프 미국 대통령 취임 이후 자유주의 국제질서의 형해화 및 대서양 동맹의 약화 등 불확실성 시대가 도래했다. 일부 공개된 트럼프 2기 국방전략지침(INDSG)과 국방전략(NDS)에 비추어 볼 때 미국은 전 지구적 차원의 작전 공간을 미 본토, 인도-태평양 및 중남미 지역으로 제한할 것으로 보인다. 피트 헤그세스 미국 국방부 장관은 지난 5월 말 싱가포르에서 개최된 제21차 아시아안보회의(샹그릴라 대화) 기조연설에서 트럼프 2기 행정부 국방전략의 일부를 공개했다. 헤그세스 장관은 미국의 정체성을 '인도-태평양 국가'로 정의했는데, 이는 미국이 대서양 동맹과 결별을 선언하고, 세계 경찰국가로서의 패권적 지위를 철회한 것으로 해석됐다.

최근 미국 정치전문매체 폴리티코는 최근 트럼프 2기 미국의 국방전략(NDS)은 미국 본토와 서반구 방어로 수정됐다고 단독으로 보도한 바 있다. 폴리티코 보도가 사실이라면, 트럼프 2기 행정부는 중국과의 전면적 패권 경쟁에 나서기보다 미중 관계를 안정적으로 관리하면서, 불법 이민자 및 범죄자 단속 등 국내 문제에 국방 역량을 활용하려는 의도로 풀이된다. 다만, 적대적 보복 관세 및 세컨더리 제재 등 미중이 극한의 관세전쟁을 벌이고 있고, 미국은 대만 해협 유사시 동맹 및 유사입장국의 참여를 압박하는 등 트럼프 2기 미국의 국가안보전략에서 중국은 즉각적이고 유일한 적국이라는 사실은 변함이 없다.

중국이 미국의 생성형 인공지능 챗봇 ChatGPT 대항마로 추론형 AI 모델인 DeepSeek-R1로 맞대응하면서 미중 패권 경쟁이 첨단 기술분야로 확장하고 있다. 트럼프 2기 미국의 국가안보전략이 중국에 적대적인 것과 비교해 러시아에 비교적 관대

하다. 조 바이든 행정부 시기와 달리 러시아를 즉각적인 위협으로 규정하지 않았고, 사이버 위협 대상에서 러시아를 의도적으로 배제하는 흐름도 읽힌다. 트럼프 2기 출범 이후 미국의 사이버 당국은 러시아에 대한 사이버 작전을 축소하거나 중단하고 있다. 물론 사이버 작전이 작전수행의 근원지를 특정하기 어렵다는 측면에서 미국의 유화적인 발언은 레토릭이 그칠 수 있다는 평가도 있다. 하지만 조 바이든 행정부가 러시아를 국제사회에서 퇴출해야 할 적대적 대상으로 인식했다면, 트럼프 2기 미국은 '핵심 이익'으로 관리하는 등 미국의 국가안보 및 사이버 안보전략에서 대러 정책은 상당한 변화가 예상된다. 다만 미러 관계는 우크라이나 전쟁 종식 해법만큼이나 불확실성의 영역이다.

지난 8월 미러 알래스카 정상회담 이후 우크라이나 종전 논의가 교착 상태를 타개하기 미국은 우크라이나에 토마호크 미사일 판매 승인 여부를 검토하고 있다. 또한 우크라이나 전쟁에 군사 개입 최소화 등 MAGA 정책에 앞장섰던 헤그세스 국방부 장관이 최근 '우크라이나 방위 연락 그룹(UDCG)'에 참여해 군사원조를 독려하는 등 대서양 동맹과 함께 러시아에 대한 징벌적 조치를 예고했다. 여기에 트럼프 대통령은 국방부 핵실험 재개를 지시했고, 이에 앞서 미국 재무부는 러시아 최대 에너지 기업 로스네프트와 루코일을 상대로 전방위 경제 제재에 착수했다. 본 글은 트럼프 2기 대러 사이버 전략이 미국의 이익을 위해 거래의 대상이 될 수 있다는 전제 하에 최근 미러 관계 변화가 사이버 분야에서 러시아의 대응에 미치는 영향을 평가하고자 한다.

II. 트럼프 2기 사이버 안보 전략과 러시아적 해석

트럼프 대통령은 취임과 동시에 행정명령-14148 『Initial Rescissions of Harmful Executive Orders and Actions』 서명을 시작으로 바이든 행정부의 여러 정책을 뒤집고 있다. 하지만 사이버 안보 관련 행정명령은 유지했으며, 새로운 행정명령 "Achieving Efficiency Through State and Local Preparedness"을 발효해 지방정부 및 개인 차원의 사이버 복원력과 대비태세를 강화하는 조치를 시행하고 있다. 마이크 왈츠 전 국가안보보좌관은 "방어 우선의 사이버 안보 전략은 효과적이지 않으며, 공격자들에게 더 많은 비용과 결과를 부과해야 한다"고 주장했다. 존 랫클리프 CIA 국장은 미국이 공격자에게 사이버 보복을 가할 수 있는 수단을 강화하는 사이버 전략 기조를 강조하는 등 트럼프 2기 미국의 사이버 안보 전략은 '힘에 의한 평화'를 달성하기 위해 공세적 억제 전략을 추구하는 것으로 해석된다.

트럼프 2기는 압도적 사이버 능력을 우선적으로 확충하고, 자국의 데이터 주권을 보호하는 대신에 동맹의 데이터를 수집하는 등 미국의 이익 수호를 위해 사이버 안보 분야에서도 동맹 현대화 정책을 적극 주장할 것으로 예상된다. 이런 점에서 동맹 및 유사 입장국과의 협력 등 '사이버 확장억제' 정책은 느슨하게 유지되는 반면 바이든 행정부와 달리 동맹의 책임 분담을 압박한다는 측면에서 주권적 영역에 대한 도전과 사이버 안보의 거래 가능성이 제기된다.

트럼프 대통령은 각 기관과 지방이 자율적으로 기술 표준과 보안 절차를 선택하게 하는 분권형 거버넌스를 추진할 것으로 예상된다. 다만, 2020년 대선에서 '부정선거를 부정'했다는 이유로 트럼프 대통령이 CISA(Cybersecurity and Infrastructure Security Agency, 사이버 보안 및 인프라 보안국)의 책임자를 해고했고, 같은 정치적 맥락에서 정권 출범 이후 CISA의 예산 및 인력 감축 조치가 현실화하는 등 연방정부 차원의 사이버 위협 정보공유체계(Information Sharing Ecosystem)에 대한 대내·외 신뢰도 약화와 '정보의 정치화'도 우려된다. 공세적 인지전과 허위조작정보 확산 등 수정주의 세력의 사이버 영향력 행사에 대한 미국과 동맹의 사이버 대응 능력이 상대적으로 후퇴할 수 있기 때문이다.

트럼프 2기 출범 이후 미국의 사이버 위협인식에 변화가 식별된다. 사이버 안보 관련 미국 정치 엘리트들의 기존 발언을 고려할 때 중국, 북한, 이란 등 수정주의 세력이 위협의 대상으로 언급되는 반면, 러시아는 위협의 대상에서 일시적 선택적으로 제외되었다. 특히 미국의 중재로 전쟁 종식에 대한 기대감이 높았던 시기에 헤그세스 국방부 장관은 러시아에 대한 사이버 작전 중단을 지시하는 등 미국의 이익 실현을 위해 러시아와 '사이버 거래'도 불사하는 듯한 전향적인 태도를 보였다.

러시아는 미국이 보복 수단 강화 등 압도적인 사이버 억제력 확충을 러시아에 대한 잠재적 도전으로 해석할 여지가 충분하다. 특히 미국의 골든 돔(Golden Dome) 구상이 '발사의 왼편' 능력을 확충한다면 전략적 균형 달성에도 상당한 부담으로 작용할 수 있다. 반면, 국내 정치문제로 CISA 등 '정보의 정치화'는 궁극적으로 미국의 사이버 역량과 동맹에 대한 사이버 방위공약을 후퇴시켜 상대적으로 중국, 러시아, 북한 등의 동맹 및 유사입장국이 사이버 주도권을 확보하는 데 유리하게 작용할 수 있다. 미국이 러시아에 대한 사이버 작전을 중단하는 등 군사적 신뢰 조치를 강구한다면 러시아는 유럽 전역에 사이버 역량을 집중해 회색지대 전술의 효과도 제고하는 등 전쟁 수행 능력을 확충할 수 있다.

III. 러시아의 사이버 전략과 미러 관계

러시아는 전통 안보 분야에서 북대서양조약기구(NATO·나토)의 확장과 동유럽 지역에 미국의 미사일 방어 시스템(Missile Defense, MD) 및 중·단거리 미사일 배치 등을 가장 심각한 위협으로 인식해왔다. 비전통 안보 분야에서 테러 및 색깔 혁명[1], 허위조작정보 확산 및 정보 왜곡 등이 주요 위협이다.[2] 허위조작정보 확산 및 정보 왜곡 등 러시아의 위협인식은 정보통신기술을 활용한 러시아의 이미지와 역사 왜곡 등

1) 색깔혁명 (color revolution)은 CIS 지역에서 발생한 민주화를 위한 시민운동을 의미한다. 러시아는 색깔혁명을 서방의 '정치 공작' 혹은 '영향력 공작'으로 인식한다. 러시아는 CIS에 대한 서방의 '영향력 공작'은 정보조작 및 허위정보 유포, 역사 왜곡 등 디지털 수단을 활용해 궁극적으로 러시아의 연방제 붕괴를 추구한다고 인식한다.

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

사이버 영향력 행사, LGBT(Lesbian, Gay, Bisexual, Transgender)의 사회적 확산 등 전통적·종교적 측면에서 러시아 고유의 가치 왜곡과 정체성 형해화 등으로 요약된다.

러시아는 2023년 3월 '전시 문서' 성격의 대외정책개념을 발표했다. 이에 따르면, 러시아는 슬라브주의를 독자적인 문명권으로 규정하고, 슬라브주의 시각에서 세계질서를 해석하고 확립하겠다는 의지를 재확인했다. 러시아의 사이버 안보 전략은 이러한 정치적·역사적 맥락에 기반한다. 러시아는 미국 등 서방의 사이버 작전에 대해 서구식 민주주의 확산 및 NGO 등의 정치 공작을 통해 러시아의 정체성을 무력화하고 궁극적으로 러시아 연방 붕괴 등 국가전복을 시도하는 정치 공작으로 인식한다.[3)]

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. 특히 우크라이나 전쟁을 계기로 사이버 분야가 주요 전장 영역으로 확장했으며, 사활적 이익의 대상인 중앙아시아 및 캅카스 등 유라시아 공간에 대한 푸틴 대통령의 정치·경제적 집착이 강화하는 등 러시아 '사이버 안보의 안보화(securitization)'가 심화하고 있다.

우크라이나 전쟁이 러시아와 서방의 대리전으로 발전한 이상 푸틴 대통령의 결심만으로 전쟁이 종식될 가능성이 작아졌다. 이런 배경에서 푸틴 대통령은 북한 특수작전군을 동원해 전쟁 장기화에 사활을 걸었고, 트럼프 2기가 출범할 경우 러시아에 유리한 전략환경이 조성될 것으로 기대했다. 실제 스티브 위트코프 특사가 수차례 모스크바를 방문해 러시아와 우크라이나를 중재했고, 종전 조건에서도 러시아의 주장을 상당 부분 미국이 인용하는 등 우크라이나에 불리한 협상 여건이 조성됐다.

트럼프 대통령의 중재 노력에도 불구하고 종전 협상 개시 자체가 불투명한 상황이 장기화하자 미국은 우크라이나에 토마호크 미사일 판매 승인 검토와 동시에 부다페스트 미러 정상회담 준비 등 투 트랙 전략을 병행해 왔다. 하지만 당근과 채찍 등 어떤 조치에도 러시아가 종전 조건에서 이른바 '최대주의'를 주장하고 나오면서 미국의 대러 정책이 다시 강경 모드로 전환하고 있다. 최근 트럼프 대통령은 러시아의 부레베스트니크(Буресестник·SSC-X-9 Skyfall) 순항미사일과 포세이돈(Посейдон) 핵추진 무인 잠수정 시험발사에 대응해 국방부에 핵실험 재개를 지시했다. 푸틴 대통령도 국가안전보장회의(NSC)를 소집해 상응하는 조치를 선언했다.

미러가 상대를 향한 핵강압 카드를 꺼내 들면서 미국의 대러 전략과 사이버 안보 전략에도 상당한 부침이 예상된다. 다만, 미러 알래스카 정상회담을 앞두고 미러 양국이 핵태세 강화 등 '긴장 고조를 통한 긴장 완화' 이후 대화의 장으로 나온 만큼, 상호 핵강압 이후 일시적 데탕트가 조성될 가능성도 있다. 사이버 작전의 특성을 고려

3) 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.

할 때 트럼프 2기 행정부의 대러 사이버 유화책의 진실 또한 특정하기 어렵다. 대러 사이버 강압이 핵강압과 비교해 효능감이 크지 않다는 점에서 러시아에 대한 미국의 사이버 정책이 낮은 수준에서 상호 신뢰 구축을 위한 거래의 수단으로 활용될 가능성은 여전히 열려 있다.

Ⅳ. 러시아의 대응

1. 국가 주도의 사이버 억제 역량 확충과 미국과 나토 분리

미국의 대러 사이버 작전 중단 등 미국의 신뢰 구축 조치는 러시아가 사이버 역량을 유럽 전역에 집중할 수 있는 호기가 될 수 있다. 러시아에 적대적 인식을 갖고 있는 미국 조야는 트럼프 2기의 사이버 작전 중단 조치에 대해 러시아의 대미 사이버 도발 활성화로 이어질 수 있다고 경고한 바 있다. 헤그세스 장관이 사이버 작전 중단을 지시한 이후 APT28, Sandworm, Killnet(Black Skills) 등 러시아 GRU(정보총국)가 직접 지휘하거나 연계된 해커 그룹이 우크라이나 및 나토 회원국 정부 기관에 대한 사이버 공격을 확대했고, 랜섬 웨어 공격 및 정보 유출 시도도 눈에 띄게 증가한 것으로 나타났다. 미 정보기관이 사이버 작전 중단이 러시아에 사이버 행동의 자유를 확대시킨 결과라고 평가하는 이유이다.[4)]

미국의 사이버 작전 중단으로 유럽 전역에 사이버 역량을 집중하게 된 러시아는 GRU와 SVR(해외정보국) 주도로 민간 해킹 조직 핵티비스트를 활성화해 나토 회원국을 대상으로 한 사이버 영향력 공작을 공세적으로 수행할 것으로 예상된다. 특히 우크라이나에 대한 군사원조 허브 기지 역할을 담당하는 폴란드와[5)] 수바우키 회랑과[6)] 인접한 리투아니아 등에 대한 사이버 공격을 통해 군사원조와 관련된 부정적인 국내 여론을 확산하고, 수바우키 강점을 위한 여건조성 작전도 적극 전개할 가능성이 있다.

---

4) Reuter, “Democrats question pause in offensive US cyber ops against Russia,” (2025. 3. 4).; The Diplomat, “The Geopolitical Fallout of a Potential US Cyber Stand-Down,” (2025. 3. 10). Reuter, “Exclusive: US suspends some efforts to counter Russian sabotage as Trump moves closer to Putin” (2025. 3. 20). 유럽연합 사이버보안기구(ENISA)의 2025년 연례 보고서에 따르면, EU 국가들은 핵티비스트(hacktivist) 등 러시아 해커 국영·연계 조직들에 의해 공공기관, 통신망, 금융 부문을 겨냥한 집중 공격을 받고 있는 것으로 나타났다. 나토는 사이버 영향력 행사와 물리적 사보타주를 결합한 러시아 위협이 “사실상 하이브리드 전쟁의 개시”라고 평가하고, 동맹 차원의 공동 대응을 모색하고 있다. 폴란드, 핀란드, 리투아니아 등 러시아와 인접한 동유럽 국가들은 사이버 방위예산을 20~30% 증액하는 한편 러시아 관련 통신장비와 소프트웨어 사용 금지령을 확대하고 있다.

5) 2024년 한 해 동안 칼리닌그라드 인근 반경에서 폴란드를 향한 최대 30건의 GPS 교란이 기록된 것으로 나타났다. 폴란드 당국은 러시아가 특정 항공기를 겨냥하기보다 폴란드 인접한 동유럽 국가들의 항공기를 상대로 공세적 전자기파 공격으로 분석된다. 특히 2024년 8월 러시아의 지원을 받는 해커 단체가 주요 도시의 상수도 공급을 교란하는 등 병원, 정부 행정 시스템 등을 대상으로 폴란드는 일일 평균 20~50건, 최대 300건 이상의 사이버 공격을 받고 있다.

6) 수바우키 회랑(Suwałki Gap, 또는 수바우키 간극)은 폴란드 북동부와 리투아니아 남부 사이에 위치한 약 96~104km 폭의 좁은 육상 통로로, 벨라루스와 러시아의 칼리닌그라드 자치주 사이에 끼어 있는 전략적 완충지대이다.

미국이 공개적으로 사이버 작전 중단을 선언한 이상 러시아 또한 대미 사이버 작전을 공세적으로 수행해야 할 명분이 약해졌다.

트럼프 2기 출범 이후 해외 군사 개입 최소화 등 MAGA 정책에서 대서양 동맹도 예외가 아닌 만큼 나토에 대한 러시아의 공세적 사이버 공격에 대해 미국이 과거와 같은 수준에서 나토의 위협인식에 동조할 가능성이 적어졌다. 궁극적으로 러시아는 미러 관계 개선 흐름을 활용해 나토에 대한 사이버 영향력 공작의 수준과 범위를 확대해 미국과 대서양 동맹의 간극을 유도하는 한편, 우크라이나에 대한 군사원조 중단 여론을 적극 형성해 나갈 것으로 보인다. 이를 위해 연간 13만 명 규모로 징집되는 일반 병사 중 사이버 특기 전문인력을 대거 양성하고, 민간 핵티비스트를 활성화해 하이브리드 전술을 더욱 고도화할 것으로 예상된다.

2. 디지털 권위주의 연대 강화

중러 양국은 2019년 신시대 전면적 전략협력 동반자 관계로 양국 관계를 격상하고 전방위적인 협력을 모색하고 있다. 미국의 사이버 패권에 대한 중국과 러시아의 위협인식은 유사하다. 중러는 미국의 사이버 패권에 반대하며, 독자적 사이버 질서 확립 등 디지털 독립을 추구한다. Freedom House의 인터넷 자유 지수에 따르면, 중국의 인터넷 사용 환경은 매우 억압적이며, 9년 연속 세계 최악의 인터넷 자유 침해 국가로 평가받고 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 방식으로 인터넷 공간을 규제하고 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 간주하여 처리하고 있다.

중국과 러시아는 2025년 4월 사이버 안보 협력 협정을 체결해 정보보호, 악성코드 탐지 및 차단, 사이버 위협정보 공유, 인터넷 거버넌스 분야에서 전향적 협력에 합의했다. 중러는 서방 중심의 인터넷 질서와 사이버 규범 체계 등 기존의 사이버 현상을 변경하고자 하는 공유된 정체성을 바탕으로 중국의 첨단 디지털 기술과 러시아의 사이버 실전 경험이 결합된 중러판 사이버 복합 넥서스의 출현 가능성도 커지고 있다.

김정은 북한 국무위원장의 중국 전승절 80주년 열병식 참석으로 계기로 북중러 연대 가능성이 주목받고 있다. 한국 정보 당국은 북중러 정상의 9.3절 연대에 대해 정치적 상징성 외에 진전된 협력 플랫폼이 가시화되지 않았다고 평가하고 있으나 사이버 작전이 수행 주체를 식별하기 어렵다는 점에서 사이버 공조는 권위주의 진영이 손쉽게 접근할 수 있는 협력 분야가 될 수 있다. 중러 간 전면적 전략협력 동반자 관계의 심화·발전과 북러가 체결한 '포괄적 전략 동반자 관계 조약'에 명시된 사이버 분야

협력 조항 등 북중러 3각 공조를 위한 양자 간 여건은 일부 조성된 것으로 평가된다. 여기에 북중러 3국이 사실상 반미, 반제국주의를 표방하며 중국의 대미 견제에 힘을 싣고 있는 만큼 회색지대 공조 가능성도 배제할 수 없다.

Ⅴ. 결론

트럼프 2기 미국의 대러 사이버 전략은 거래의 수단이다. 미국과 러시아는 우크라이나 전쟁 종식을 위해 우선적으로 상호 신뢰를 구축해야 한다. 이를 위해 상호 간 사이버 공격 중단 등의 선언적 정책을 통해 바이든 정부에서 점철됐던 상호 간 적대의식을 제거하는 노력을 추진해 왔다. 하지만 러시아가 종전 조건에서 '최대주의'를 주장하고, 각종 전략무기 시험발사에 나서면서 미국은 더 이상의 유화책을 포기하고 핵실험 재개 카드로 대응하면서 미러 관계가 다시 시험대에 올랐다. 트럼프 2기 미러 관계는 우크라이나 전쟁 종식 여부에 달려있다. 전쟁이 장기화할수록 미러 관계는 트럼프 2기 출범 당시로 역주행할 가능성이 크다. 반면, 미국이 제안한 평화구상을 러시아가 받아들여 불완전한 종전이든 일시적 정전 합의가 전격적으로 이루어진다면 양국 관계는 적대적 경쟁 관계에서 협력적 경쟁 관계로 전환될 수 있다.

미러 관계의 맥락에서 사이버 전략은 양국의 이익에 중요한 영역이다. 미국은 러시아와의 신뢰 구축을 위해 사이버 전략을 거래 수단으로 내세울 수 있고, 러시아는 미국을 상대로 투입해야 하는 사이버 역량을 우크라이나와 대서양 동맹에 집중할 수 있기 때문이다. 특히 상호 간 긴장 완화를 위해 사이버 공격 중단을 선언해도 공격 주체를 특정할 수 없고, 책임에서 자유로운 만큼 매력적인 거래 수단이다. 이런 배경에서 트럼프 2기 행정부의 대러 사이버 전략은 나토 중심의 다자 공조 체제로부터 이탈(decoupling)할 구조적 유인을 내포하고 있다. 한편, 러시아는 사이버 역량을 유럽의 대서양 동맹에 집중하기 위해 미국과의 제한적 사이버 협력 또는 암묵적 상호 자제(tacit mutual restraint)를 추구할 가능성이 제기된다.