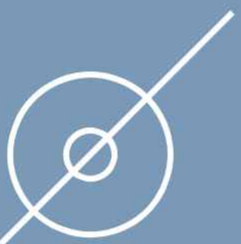
미국의 사이버 국방 전략과 한미동맹



2024

한국사이버안보학회
KACS

한국사이버안보학회 워킹페이퍼 16호
발간일: 2024년 8월 20일

박용한 (한국국방연구원)

Ⅰ. 군사 분야 사이버 위협 특징

1. 네트워크 마비전

미래전장은 모든 전투체계가 연결된 네트워크 환경에서 작전을 수행하게 된다. 초연결된 네트워크 환경은 사이버공간과 전자기스펙트럼 공간으로 구성된다. 무기체계가 발전하면서 두 영역에 대한 의존도는 높아진다. 따라서 사이버작전 환경은 지해공뿐 아니라 우주와 사이버 및 전자기 영역으로 확대된다. 특히 분리된 폐쇄망도 침투 및 접속 가능성을 완전하게 배제하기 어렵다. 모든 제대가 노출될 수 있다. 사이버작전은 비물리적 작전 뿐 아니라 물리적 수준도 포함하는 작전으로 전개될 수 있다. 지휘체계뿐 아니라 무기체계와 기반시설도 포함될 수 있다. 이러한 공격에서 군사 영역뿐 아니라 민간 영역도 표적화 될 수 있다. 이러한 네트워크 마비전은 다영역으로부터 제공되는 다양한 수단과 방법을 포괄한다. 따라서 합동작전 또는 다영역작전(MDO) 개념으로 통합해 접근해야 한다.[1] 미래 다영역 작전은 과거 물리적 타격에 초점을 둔 효과중심작전(EBO)과 달리 이제는 네트워크 중심 작전(NCO)을 바탕으로 전개된다고 전망된다.

시간적 영역에서 보자면 전평시를 구분하기 어려운 상황도 예상된다. 사이버 공간은 물리적 영역과 달리 평시에도 은밀한 활동이 전개되며 임의의 상황을 예비한 공격이 이뤄진다. 여기에는 군사적 대상뿐 아니라 기반 시설을 포함한 민간 영역도 포함된다. 전시에 두 영역을 동시 공격해 효과를 높일 가능성이 있으며, 이러한 혼합 공격 양상에 따른 위협 대비가 필요하다.

다만, 이러한 위협에 적절한 대응도 가능하다. 우크라이나 전쟁 개전에 앞서 러시아 사이버 공격에 대비한 서버 분산과 대응이 효과를 보았다. 모든 사이버 공격이 만능이 아니라는 경험이다. 이는 과거 러시아 공격 양상을 분석했고, 공격 징후를 판단한 적절한 대응의 결과다. 나토와 미국이 우크라이나 전쟁에 대응한 '회복력' 구축을 교훈으로 분석해야 한다.

2. 하이브리드 전쟁

하이브리드 전쟁은 사이버 선제공격 후 물리적 전쟁을 개시하는 특징을 내포하며, 북한은 전면적 침공을 앞두고 한미 연합군에 대규모·동시적 사이버 공격에 나선다고 전망된다.[2] 본격적인

1) 송운수, 『사이버 군사전략 개관』(인천: 진영사, 2022), pp. 189~193.

공격에 앞서 평시에는 스피어 피싱 공격 전략으로 전시 공격을 위한 여건을 조성한다. 악성 이메일로 안보 관련 연구자를 대상으로 공격하면서 악성 명령어가 포함된 파일을 첨부해 발송한다. 컴퓨터 정보를 외부로 유출하려는 목적이며 이를 통해 통제권을 얻어낸다.[3)]

특히 우크라이나 전쟁에서 정보전의 위력을 확인할 수 있다. 2021년 가을부터 러시아는 군사훈련 및 병력 이동과 함께 우크라이나 현지 저항 감소와 국제사회 동조를 견인하기 위한 내러티브를 확산했다. 특히 침공에 대해서 자국 방위를 위한 제한적 군사작전이라고 주장했다. 러시아는 동시에 개전 첫날 우크라이나 통신 시스템과 인터넷 인프라를 공습했다. 이에 대응한 우크라이나는 러시아 주장을 반박하는 내러티브를 신속하게 발신했다. 젤렌스키 우크라이나 대통령이 도주했다는 러시아 주장을 반박하는 등 항전 의지를 소셜미디어를 통해 확산했다. 일론 머스크는 스타링크를 제공해 통신 시스템을 정상화하도록 도왔다. 미국 IT 기업 마이크로소프트는 러시아 공격 패턴을 분석해 우크라이나 대응에 도움을 줬다. 구글은 정찰과 감시, 물리적 타격을 위한 목표물 탐지 및 식별에 필요한 공간 정보를 제공했다.[4)]

이처럼 정보전은 진화하고 있다. 전쟁 초반부터 전자전 사이버전 정보작전 물리적 포격이 유기적으로 활용된 작전 형태를 확인할 수 있다. 정보작전이 심리적 교란이나 마비의효과를 추구하는 기존 개념을 탈피해 보다 유기적으로 물리적 살상에 기여했다는 평가다. 결정적 작전을 위한 지원 차원을 넘어 전쟁 수행의 핵심 위치를 차지했다. 정보전의 영역이 초연결된 사이버 영역으로 확장됐다.이는 데이터를 정보로 활동하게 되면서 가능해졌다. 데이터가 결정중심전의 핵심적인 위치를 차지하게 됐다. 장기적으로 미군이 추구하는 모자이크전의 핵심도 데이터에 있다.[5)]

이처럼 미래 전쟁의 양상은 앞서 살펴본 바와 같이 다영역작전(MDO) 개념이 실증적으로 구현될 전망이며 이미 일부분 현실에서 확인되고 있다. 또한, 데이터 중심의 정보전으로 이동하는 추세도 드러나고 있다. 사이버 전의 중요성과 취약성이 함께 부각된다. 미래 전쟁의 성패가 사이버전 결과에 따라 좌우될 수 있다는 전망이 나오는 배경이다.

3. 우주자산 위협[6)]

우주 분야 발전에 따라 사이버 공간 의존도가 증가하며 동시에 사이버 위협 영향을 피할 수 없다. 2022년 2월 유럽 우주국(ESA)은 우주 사이버 보안 강화를 위해 실시간 인공위성 해킹을 시도할 참가자를 모집했다. 2019년 12월 궤도 515㎞ 고도에 올려둔 위성을 상대로 기술을 검증했다. 사이버 인공위성 해킹으로 위성을 물리적으로 공격하지 않더라도 위성을 무력화하거나 운용자 의도와 다르게 제3자의 통제가 가능하다. 인공위성을 손쉽고 저렴한 방법(300달러)으로 해킹한 사례는 꽤 많다. 사실상 대부분의 상용 위성은 당장이라 비전문가의 공격으로도 일시적·영구적인 침해가 가능한 상황이다.

위성에 대한 직접적인 사이버 공격뿐 아니라 지상 관제소에 침투해 통제권을 빼앗거나 무력화

2) 러시아는 2022년 2월 24일 우크라니아 침공에 앞서 사이버 공격은 두 달 전인 2021년 12월 28일 시작했다는 기록도 발견됐다. 박동휘 외, 『사이버전의 모든 것』(서울: 플래닛미디어, 2022), pp. 147~148.

3) '엔드포인트보안연구개발실' 위협 분석 보고서(2023.9.26)

4) 송태은, "러시아-우크라이나 전쟁의 정보심리전," 김상배 엮, 『신흥기술·사이버 안보의 국가전략』(서울: 사회평론아카데미, 2023), pp. 94~100.

5) 손한별, "새로운 정보전 양상과 데이터 안보," 김상배 엮, 『신흥기술·사이버 안보의 국가전략』(서울: 사회평론아카데미, 2023), pp. 107~112.

6) 다음의 내용을 바탕으로 재구성. 박용한, "우주국방의 시각에서 본 신흥기술·사이버 안보," 김상배 엮, 『신흥기술·사이버 안보의 국가전략』(서울: 사회평론아카데미, 2023)

도 가능하다. 만약 위성을 운용하는 서버가 해킹 공격이나 물리적인 침해를 받는다면 위성 운용에도 큰 차질이 불가피하다. 지구에서 3만 6000㎞ 떨어진 정지궤도 위성을 해킹하기 위해 멀리 갈 필요가 없다. 3000㎞ 바다 건너에서 사이버 공격으로 원하는 목적을 달성할 수 있다. 사이버 공격에 성공할 경우 내가 쏜 위성이 없더라도 다른 국가에서 쏜 위성으로 원하는 목적 달성도 가능하다. 사이버 해킹으로 침투한 뒤 군집 드론 공격처럼 500㎞ 저궤도 상공에 올라가 있는 다수의 인공위성을 활용한 군집 위성 공격도 가능하다. 컴퓨터 게임 하듯 '분산제어' 기술을 적용해 삼삼오오 짝을 지어 임무를 받고 수행할 수 있다. 우주에 올려 둔 정찰위성이라는 '눈'과 통신망이라는 '귀'를 잃어버리면 현대전 수행은 불가능하다. 이런 이유로 미국에선 오래전부터 사이버 진주만 공습을 우려했다. 랜드 연구소에서 1995년 분석한 결과에는 고속열차 탈선이나 항공기 추락, 송전망 파괴 등이 거론했다. 대량 파괴무기가 아닌 대량 혼란의 무기가 된다.[7] 사이버 공간의 통제권을 상실하면 우주를 포함한 모든 걸 빼앗기게 된다.

4. 초연결성의 파급효과

앞서 데이터 전쟁 양상과 함께 네트워크마비전의 파급효과를 확인했다, 이는 초연결의 취약성으로 설명된다. 2022년 10월 15일 발생한 판교 데이터 센터 화재는 의존성에 따른 취약성을 보여준다. 데이터 센터에서 대규모 정보를 저장 및 처리한다. 개별 운용 이용자 사이 정보 교환이 이뤄지는 장소이며 여기서 데이터를 전달 및 저장한다. 특히 AI와 같은 연산 도구를 활용해 데이터를 가공 및 처리한다. 여기에는 서버를 비롯한 네트워크, 저장 공간인 스토리지, 메모리 반도체 등이 집약돼 있다. 네트워크와 상시 연결된 상태를 유지하면서 안정적인 운용이 필요하다.

군에서는 분리된 통합데이터센터를 구축해 군사 정보 처리를 민간 영역과 구분해 별도 운용한다. 그러나 군 위성 운용을 지원하는 국방 관련 데이터 운용에 장애가 발생한다면 정상적인 군 지휘통신 보장을 장담하기 어렵다. 국내에 설치된 민간분야 데이터 침해 사고도 국방과 무관하지 않다. 사회적 기반 시설 침해는 필연적으로 공공부분은 국방에도 영향을 미친다. 국방에 어떠한 직접적·간접적 영향을 파생하며 어떤 대응을 준비 및 이행 해야하는지 면밀히 살펴야 한다.[8]

사이버전의 특성은 공격의 실체를 오랜 기간이 지나 밝히더라도 이미 공격자는 전략적인 목적인 달성한 이후며, 피해자가 이를 복원하기 어렵다. 사이버 공격을 마친 공격자는 피해 국가에서 해킹과 무관한 다른 국가에서 공격했다고 오판하도록 가짜 증거를 조작해 남겨 둘 수도 있다.[9]

Ⅱ. 북한 사이버 안보 위협 동향

7) 정보 체계의 취약성에 관한 내용은 다음을 참조. 로렌스 프리드먼(조행복 옮김), 『전쟁의 미래』(서울: 비즈니스북스, 2020), pp. 364~367.

8) 한국데이터센터연합회 자료에 따르면 국내 소재 데이터센터(IDC)는 2000년 53개에서 2020년 156개로 증가했다. 2025년에는 188개까지 늘어나며 시장 규모는 10조 원 규모로 전망된다. "미래 먹거리라 박수 받지만 위기 대응은 허점투성이…흔들리는 데이터센터 산업" 『한국일보』, 2022년 10월 19일.

9) 2018 평창 올림픽을 앞두고 러시아는 해킹을 공격을 했다. 사건 발생 초기 공격 주체로 북한을 유력하게 추정하는 단서가 발견됐다. 그러나 이는 의도된 오인이며 공격 주체로 러시아를 규명하기까지 상당한 시간이 필요했다.

1. 북한 사이버전 역량 평가

북한의 사이버전 능력은 자세하게 파악되지 않았으나 1980년대 중반부터 관심을 갖고 전문인력을 양성한 것으로 알려졌다. 북한은 군 장비 현대화 및 사이버전 전력 확보를 위한 전문가 양성을 목적으로 1981년도에 인민무력부 산하에 5년제 '미림대학'을 설립했고, 연 100여 명 규모의 교육생을 배출한다고 알려졌다. 이후 1986년 '평양 자동화 대학'으로 그리고 1990년대 초 '김일 군사대학'으로 개칭하기도 했다. 졸업생은 북한군 지·해·공 및 사이버 유관 부서 및 정찰국 산하 '121부대' 등에서 임무를 수행한다고 추정된다.[10)]

121부대는 허위정보, 사이버 범죄, 스파이 활동을 하며 산하에 김수키와 라자루스 등 해킹 그룹을 두고 운용하며 소속 해커는 대부분 벨라루스와 중국과 러시아 등 해외에서 활동한다는 분석도 있다.[11)] 이들은 2019년 대북제재가 강화된 이후 북한 출신 해외 노동자가 북한으로 돌아가면서 현지에 머물기 어렵게 됐다. 최근에는 북한 내부에 거점을 두고 활동하는 경우가 많다고 알려졌다.

사이버 부대는 다른 군 조직보다 더욱 베일에 가려있다. 정확한 편재와 규모가 확인되지 않지만, 다수의 탈북자 및 관련 연구자 견해를 보면 사이버 공격을 수행하는 부서가 존재한다고 파악된다. 또한 국내외 다양한 해킹관련 수사를 통해 북한 사이버 부대의 활동이 드러나고 있다. 대북제재 대상에도 사이버 관련 인물이 포함되고 있다.

121부대는 정찰총국 산하 조직으로 알려졌다. 북한 정찰총국은 전시 및 평시에 대남 및 주변국을 대상으로 특수전 수행, 정보수집, 공작활동 등을 수행하는 부대로 파악된다.[12)] 따라서 해당 조직 목적에 부합하는 평시 사이버테러도 수행한다고 추정된다. 최근에는 불법적 외화 획득에 있어 가장 중요한 기능도 수행한다. 북한 권력의 핵심 계층이 사이버 관련 조직을 관리하고 관련 분야에 지속적인 관심을 보여주는 등 IT분야를 육성하고자 하는 의지를 확인할 수 있다.[13)] 최고지도자 의지가 반영된 만큼 북한에서 군사적, 사회적으로 상당한 자원 투입이 예상되는 분야로 평가된다.

국방부는 북한군이 '기습공격, 배합전, 속전속결을 중심으로 하는 군사전략을 달성하기 위해 재래식 전력뿐 아니라 핵무력과 함께 사이버·전자전 부대 등 비대칭 전력증강을 추진하고 있다'며 '사이버전 인력은 6,800여명으로 추정되며 최신 기술에 대한 연구 개발을 지속하는 등 사이버전력 증강을 위해 노력하고 있다'고 평가했다.[14)] 또한 '북한은 한국 내부의 심리적·물리적 마비를 위해 군사작전 차질 유발, 주요 국가기반 체계 공격 등 사이버전을 수행하고 있다'고 밝혔다.[15)]

2. 북한 사이버전 역할과 위협

북한이 사이버 공격 능력을 배양한 배경은 세계적 추세와 부합하는 부분인 동시에 북한이 직

10) 최선우, 류재형, "북한의 사이버 테러리즘에 관한 연구," 한국공안행정학회,『한국공안행정학회보』, 46권(2012), pp. 223~224.
11) 김보미, "김정은 시대 북한 사이버 위협의 특징과 대응 방안," 김상배 엮, 『신흥기술·사이버 안보의 국가전략』(서울: 사회평론아카데미, 2023), p.74.
12) 정찰총국의 역할, '121부대'의 편제 등은 모두 언론 출처를 종합하여 판단한 것으로 언론에 인용된 탈북자 증언, 관련 연구 등 다수의 문헌에서 제기한 주장을 수용한 것임을 주지한다.
13) 북한의 핵심 권력층과 사이버 관련 기관의 연계성은 다음을 참조,『시사인』, 제290호(2013).
14) 국방백서 2022(2023.2) p. 25.
15) 국방백서 2014(2014.12) p. 24.

면한 특수한 사정을 반영한 결과로도 평가될 수 있다. 2003년 이라크 전쟁(OIF)으로 대표되는 '2세대 사이버전(2003~2007년)' 이후 세계적으로 군이 주도하는 사이버 공격이 본격화됐다. 전장에 참여하는 제 전력요소에 관해 정보통신 기술의 발전을 이용한 네트워크를 구축하면 전장상황 인식 공유와 전력의 통합화가 가능해지고 이에 따라 작전 수행 효과를 획기적으로 높일 수 있다.[16)]

최근 전쟁 양상에서 공통적으로 발견하는 하이브리드 전쟁 양상에서 확인하듯 포성이 울리기 전에 사이버 공격이 먼저 또는 동시에 수행하면서 적성국 시스템을 파괴하면서 전쟁 수행 능력을 소멸 또는 저해한다. 한국군 역시 이와 같은 네트워크 중심전(NCW)을 지향하고 있다. 이러한 의존도 심화는 취약성으로 연결된다. 네트워크에 대한 방호가 실패할 경우 심각한 작전 능력 손실이 우려된다. 관련 분야에서 선진화된 미군도 해킹 공격에 취약하며 다수의 침해 사례를 확인할 수 있다.[17)]

북한도 이러한 NCW 추세를 지향하는 동시에 한국군의 취약성을 공략한다고 합리적으로 예측할 수 있다. 북한은 세계적 흐름에 부합하는 전자전 능력을 제고하고 비대칭적인 남북한의 군사력 차이를 극복하기 위한 수단으로 전자전 능력을 배양한다고 판단된다. 재래식 군사력의 열세를 극복하기 위해 탄도미사일 개발과 은밀성이 뛰어난 잠수함 전력을 강화하는 비대칭전력 강화 전략처럼 사이버/전자전 능력 배양에 중점을 두고 있다.

북한이 전시 전력운용의 측면에서 한국군 기반 역량을 붕괴하기 위해 사이버 공격능력을 배양한다면, 평시에는 테러의 수단으로 사이버 공격을 활용할 수 있다. 테러의 개념을 적용함에는 논란의 여지가 있을 수 있으나 사이버 공격도 광의적으로는 폭력으로 간주되며 심리적인 영향과 공포, 정치적인 목표를 위해 민간인을 직접적 가해의 대상으로 공격하며, 불법 및 비합리성 등 테러의 특징에 상당부분 부합되기 때문에 테러의 수단으로 규정하는데 어려움이 없다.[18)]

북한 사이버 안보 위협은 기반체계 공격 특성, 점차 변화. 김정은 집권 이후 불법 경제활동으로 위협으로 범위를 확장했다. 2022년 3월 미국 재무부는 북한 해킹 조직 라자루스가 암호화폐 6억 2천만 달러를 온라인 게임 '액시 이피니티'에서 탈취했다고 밝혔다, 이는 역대 암호화폐 피해 중 가장 큰 규모로 평가된다. 미국 블로페인 데이터 분석업체 '체이널리시스'는 최근 발표한 보고서에서 북한 정권과 연계된 해킹 조직이 불법적으로 암호화폐 자산을 세탁한다고 알려진 러시아 거래소 사용은 크게 늘었다고 분석했다. 북한이 지난해 미국 블로체인 기술 기업 '하모니'에서 탈취한 1억 달러(약 1300억원) 규모의 암호화폐 중 2190만 달러를 러시아 소재 거래소로 이체했다.[19)] 가상 자산은 안정적으로 현금화 하기 위해 북한과 가까운 러시아 소재 거래소로 보냈다고 분석된다. 앞서 2023년 2월 체이널리시스는 '2023 가상자산 범죄 보고서'에서 지난해 북한이 가담한 암호화폐 해킹 피해규모를 17억 달러(728억원)으로 추정했다. 더욱 큰 문제는 이런 자금이 북핵 개발에 쓰여지면서 군사적 위협을 심화하는 중요 수단으로 활용되고 있다.

Ⅲ. 미국의 사이버 전략과 한미 협력

16) 노훈, 손태종, "NCW: 선진국 동향과 우리 군의 과제," 한국국방연구원,『주간국방논단』, 제1046호(2005.5.9),
17) 미군의 해킹 취약성과 관련된 내용은 다음을 참조. 피터 W.싱어 저, 권영근 역,『하이테크 전쟁』(서울: 지안, 2011), pp. 289~290.
18) 박재풍, "뉴테러리즘의 의미재정립과 대응에 관한 연구," 한국정책학회,『한국정책학회 춘계학술발표논문집』(2011), pp. 471~474.
19) 중앙일보 2023년 9월 19일

1. 미 국방부의 사이버 전략

2018년 9월 미국은 '국방 사이버 전략'(Defense Department Cyber Strategy)에서 美 사이버사령부는 '전진방어'(defending forward) 개념을 사이버작전에 차용하며, 적국의 악의적 사이버 행위를 중단 및 파괴하여 선제적으로 무력화 하겠다는 입장을 표명했다. '전진방어' 개념은 미국이 강조해 왔던 적극방어(active defense)의 하위개념이다. '적극적 방어' 작전은 공격자로부터 공격수단을 뺏는 공격도 포함한다.[20]

미국은 2023년 3월 '국가 사이버안보 전략'(NCS)를 발표했다.[21] 여기서 코로나19 시기에 전례 없는 수준의 인터넷 개방성과 연결성의 경험을 지적하면서 '미국이 디지털 미래의 모든 이점과 잠재성을 실현하기 위해 가장 유리한 위치를 점유할 수 있도록 정부가 취하고 있는 포괄적 접근 방식'을 제시했다. 또한, '사이버 안보는 국가를 방위하는데 있어 핵심적 역할을 한다'고 강조했다. 특히 "선제적으로 방어하는 국방부의 전략적 접근법은 위협 행위자를 식별하고, 악성 소프트웨어를 발견 및 노출하며, 위협 행위가 공격 대상에 영향을 미치기 전에 이를 차단하는 데 도움이 되었다"고 평가했다.

발표된 전략은 미국 국방부는 미국의 동맹 및 파트너가 보유한 독자적인 기술과 관점을 활용하기 위해 군사 관계를 지속적으로 강화하고, 미국의 동맹 및 파트너가 공동의 사이버안보 태세에 기여할 수 있도록 이들의 역량을 구축할 방침이라며 협력의 방안을 제시했다. 이어 미국 사이버 사령부와 기타 국방부 구성원이 미국의 이익에 전략적 위협을 가할 수 있는 국가 및 비국가 행위자로부터 방어하기 위한 노력을 사이버 영역 작전과 통합하는 방안을 분명히 제시하겠며 구체적인 후속 조치 추진 계획을 밝혔다.

미 국방부도 같은 해 9월 '국방 사이버 전략'을 공개했다.[22] 여기서 중국, 러시아, 북한, 이란, 극단주의세력, 초국가범죄조직 등을 핵심위협 대상으로 언급했다. 핵심 과제는 첫째, 국가방위를 위한 중요 인프라 방어, 군사준비태세 등을 위해 유관기관과 공조를 강화하는 데 뒀다. 둘째, 전투 준비와 전쟁에서 승리하기 위해 합동군 목표달성 지원, 사이버보안 강화를 제시했다. 셋째, 동맹·파트너에 대한 사이버공간 보호를 위해 '헌트 포워드' (Hunt Forward) 작전 지속과 기술공조를 강조했다.[23] 마지막으로 사이버공간 내 항구적 이점을 구축하기 위해 조직·교육훈련·장비 등을 최적화한다는 계획이다. 앞서 발표했던 국방 사이버 전략과 비교하면 동맹·파트너 국가의 사이버역량 강화를 통해 집단적 사이버 회복력 구축하는 데 방점을 뒀다. 또한, 사이버 역량을 기존 전투역량과 통합운용을 강화해야 한다는 과제를 제시했다. 이는 미 국방부가 추구하는 통합억지(Integrated Deterrence) 개념에 따른 전략으로 해석된다. 따라서 미국은 집단적 사이버역량을 구축하는 데 있어 우방국과 연합 작전을 강화하는 노력에 나선다고 전망할 수 있다.

---

20) 백민정, 「국제법적 시각에서 본 사이버 작전 관련 미국의 입장」, 『동북아안보정세분석』, 한국국방연구원, (2020.5.15)

21) *National Cybersecurity Strategy 2023.3*

22) Defense *Cyber Strategy 2023.9*

23) 미 사이버사령부 예하 국가사이버임무군(Cyber National Mission Force)은 우방국에 전개하여, 위협세력의 악의적 사이버 활동을 관찰 및 탐지하는 헌트 포워드 작전을 지속 강화하고 있다. 국가사이버임무군은 2014년 1월 창설한 이후 미국 선거 방어, 랜섬웨어 대응, 외국의 악의적 사이버 행위 퇴치, 헌트 포워드 작전 등 사이버 방어 및 공격 작전 모두 수행한다. 2018년 이후 우크라·리투아니아·라트비아 등에서 활동한다고 알려졌다. 작전 사례는 다음을 참조. Sharon Rollins, "Defensive Cyber Warfare Lessons from Inside Ukrain," *Proceedings*, Vol. 149/6/1,444, June 2023.

미국은 통합억지력을 강화하는 노력과 함께 우주군 사례와 같이 사이버 사령부를 별도 군으로 창설하는 방안도 검토하고 있다. 2023년 7월 공개한 2024회계연도(FY24) 국방수권법(NDAA) 법안에서 '독립적인 사이버 부대 창설' 가능성을 연구하라는 미 상원 군사위원회 요구가 확인됐다. 해당 법안은 "우주군 창설에서 얻은 교훈을 사이버군 창설에 적용해야 한다"고 법안에 명시했다.

군 안팎에선 현재의 통합 사령부 조직이 진화하는 위협에 충분히 대응하지 못한다고 지적한다. 적성국(중국, 러시아 등) 사이버 작전 능력이 크게 확장하는 데 대응하기 위해 사이버 대응 역량을 더욱 강화해야 한다는 목소리에 힘이 실렸다. 해당 법안은 구체적으로 현재 미군의 사이버 역량을 평가할 뿐 아니라 훈련과 교육 등 전반을 검토하도록 했다. 또한, 독립된 별도의 사이버 군을 창성 할 경우 얼마나 개선 될 수 있는지도 평가하도록 요구했다.

2. '전략 동맹'과 '사이버 동맹'

사이버 위협은 일국 차원에서 해결할 수 없어 초국적 해법을 강조하는 비지정학적 협력의 특징을 갖는다. 악의적 국가 행위자가 가상자산 탈취 등 불법 사이버 활동이나 다른 국가 공공 및 민간 시스템에 대한 해킹 공격을 배후에서 지원하면서 국가 간 사이버 범죄 대응 협력이 필요했기 때문이다. 그러나 최근 전통적인 지정학 공간과 같이 사이버 공간에서의 안보적·경제적 이익 증대를 목적으로 하는 사이버 안보협력이 강화되는 추세를 보인다. 한미 간 사이버 협력도 2000년대 초반 이후 한동안 초국적 사이버 범죄 대응에 초점이 있었다. 그러나 미중 전략경쟁이 심화하기 시작하면서 협력의 대상과 수준이 강화됐다.[24)]

전략 경쟁의 구도는 2023년 5년 만에 개정한 NCS에서도 확인할 수 있다. NCS는 "미중 전략경쟁과 진영대립이 사이버 공간에서도 심화하는 상황을 반영해 큰 틀에서 주요기반시설 보호 체계 강화, 국제협력을 통한 위협국가 대응 활동 강화, 신기술 도래로 인한 미래 대비에 방점을 둔다"고 평가된다.[25)] 미국은 한국에 중국을 견제는 역할을 기대하고 참여를 요구하고 있으며, 동맹 차원에서 향후 포괄적·전면적 협력 참여를 요구한다고 전망된다. 2022년 5월 한미 양국 정상이 발표한 '글로벌 포괄적 전략 동맹'은 이런 기대를 담으며, 미국은 전통적 동맹을 복원하면서 미중 전략 경쟁에서 협력을 요구하고 있다.

3. '2023년 한미 정상회담' 사이버 분야 평가

2023년 4월 26일 미국에서 열린 한미 정상회담에서 윤석열 대한민국 대통령과 조 바이든 미국 대통령은 사이버 공간으로 양국 동맹의 영역을 확장했다. 양 정상은 공동성명에서 "동맹이 사이버 공간에 적용된다는 것을 인식하였으며, 한미 전략적 사이버안보 협력 프레임워크를 체결하기로 했다"고 발표했다. 한미 양국 정상이 한미동맹을 사이버 공간으로 확장한 첫 선언이다. 이는 양국 동맹이 사이버 '영역'을 포괄하는 관계로 진화했다는 뜻이다. 사이버 관계를 중심으로 본다면 군사동맹과 달리 '협력' 수준에 머물던 양국 사이버 관계는 이제 '동맹' 수준으로 격상했다.

---

24) 신승휴, "한미 사이버 안보협력의 진화: 복합지정학의 시각," 『4차 산업혁명 시대의 한미관계』(정보세계정치학회 춘계학술대회 발표자료, 2023.4.28.), p. 4.

25) 미국이 2023년 개정한 '국가사이버안전략'의 주요 특징과 함의는 다음을 참조. 김소정, "2023 미국 사이버안보 전략 주요내용과 한국에의 시사점," 『이슈브리프 423호』(국가안보전략연구원, 2023.3.8.), p. 6.

사이버를 안보의 주요 영역으로 인식한다면 미완적 동맹을 완성했다는 해석이 가능하다. 만약 사이버를 안보적 기제 또는 범주에서 제외할 수 있다면 동맹의 범주를 확대했다고 설명할 수 있다.[26)]

양국 정상은 선언적 수준보다 좀 더 구체적인 협의안을 꺼냈다. 사이버안보 협력 프레임워크(SCCF)를 채택해 사이버 협력의 범위·원칙·체계를 구체화했다.[27)] 공동성명에서 언급한 내용을 보면 ▶사이버 적대세력 억지에 관한 협력을 확대 ▶핵심 기반시설의 사이버안보를 증진 ▶사이버 범죄에 대처 ▶가상화폐 및 블록체인 애플리케이션을 보호 등을 언급했다.

한미는 이번 선언에서 사이버 협력을 언급하면서 전략적 관점을 특별히 강조했다. 전략적 관점은 북한 대량살상무기 개발과 이를 지원하는 사이버 불법 활동 차단이다. 공동선언에서 양국은 '북한의 불법적인 대량살상무기 및 탄도미사일 프로그램의 자금을 조달하는 북한의 불법 사이버 활동에 대해 우려를 표명했다. 또한, 북한의 사이버 위협에 대응하고 사이버 외화수익을 차단하기 위해 정보공유를 확대하고 국제사회의 인식을 제고했다.

사이버 위협에 대한 미국의 인식은 이미 국가사이버안보전략(NCS)에서 지적된 바 있다.[28)] 여기서 북한을 중국·러시아·이란 등과 함께 주요 위협으로 적시했다. 특히 북한이 사이버 가장 자산을 탈취하고 핵 위협을 고도화하면서 대북 위협을 대응하는 사이버 협력도 차원을 달리하고 있다.

한미는 점증하는 북핵 위협을 인식하면서 그러한 위협을 지원하는 수단으로 북한 사이버 활동이 전개되고 있다고 판단한다. 따라서 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.

양국 정상이 2022년 5월 21일 정상회담 공동성명에서 '국가 배후의 사이버 공격 등을 포함하여 북한으로부터의 다양한 사이버 위협에 대응하기 위한 협력을 대폭 확대'하기로 했던 기조를 이어갔다고 평가할 수 있다. 지난해 성명에서 제안했던 협력을 대부분 지속하고 있다. 2022년 정상회담에서 ▶사이버 적대세력 억지 ▶핵심 기반 시설의 사이버 보안 ▶사이버 범죄 및 이와 관련한 자금세탁 대응 ▶가상화폐 및 블록체인 애플리케이션 보호 ▶역량 강화 ▶사이버 훈련 ▶정보 공유 ▶군 당국 간 사이버 협력 및 사이버 공간에서의 여타 국제안보 현안에 관한 협력 지속 심화 ▶지역 및 국제 사이버 정책에 관한 한미 간 협력을 지속 심화 등을 협력 대상으로 언급했다.

양국 정상은 2022년 5월 한미정상회담에서 사이버 안보 협력을 논의한 이후 공통의 인식 공유와 협력을 지속했다. 같은 해 8월 한미 사이버작전사령부는 '한미 간 사이버 작전 분야 협력과 발전을 위한 양해각서(MOU)'를 체결했다.[29)] 이어 9월 개최한 제3차 한미 고위급 확장억제전략

---

26) 동맹에 대한 사전적 정의는 "서로의 이익이나 목적을 위하여 동일하게 행동하기로 맺는 약속"이며, 통상적으로 안보적 목적을 위해 두 개 이상의 국가 간 상호 군사적 지원을 협약(다자적 동맹 포함)하는 경우로 해석한다. 다만, 동맹이 내포한 의미와 영역을 군사적 범주를 초월하거나, 안보적 의미를 경제 등으로 확대, 또는 안보 이외의 범주를 포괄해 해석하는 경향도 보인다.

27) 한미 사이버안보 협력 프레임워크(SCCF)은 협력 분야, 협력 원칙, 협력 메커니즘에 관한 내용을 포함한다. 보다 구체적인 논의를 추후 지속 진행될 전망이다. SCCF는 '한·미는 상호방위조약이 어떻게 적용될지와 어떤 상황에서 적용될 것인지에 대한 논의를 시작할 예정'이라고 언급했다.

28) *National Cybersecurity Strategy 2023.3*

29) 2022년 8월 한미 사이버작전사령부 MOU 체결을 통해 사이버 위협에 효과적으로 대응하기 위해 정보·작전분야 교류를 통한 역량 강화와 연합 훈련을 정례화하기로 했다. 구체적으로 ▶사이버 위협정보 공유 ▶교육 및 연습 ▶훈련기회 확대 등 협력 관계를 지속 발전시켜 작전 역량을 강화하기로 했다. "이종섭 국방부장관, 미 사이버사령관 접견"『국방부 보도자료』(2022.8.18.)

협의체(EDSCG)에서 사이버 위협에 대한 한미 공조 강화를 약속하는 공동성명을 냈다. 10월에도 미국 사이버사령부가 주최한 '사이버 플래그(Cyber Flag) 훈련'에[30] 한국 사이버작전사령부가 최초 참여했다.[31] 12월에는 '제6차 한미 사이버정책협의회'을 열어 관련 협의를 지속했다.

한미는 앞으로 기관 협력과 상호 위협 인식을 지속하며, 연구와 훈련 등에서 긴밀한 협력이 예상된다. 양국은 SCCF에서 '광범위한 사이버위협에 대응하기 위해 다수의 매커니즘을 통해 사이버안보 활동을 지속적으로 조정'하기로 했다. 또한, '사이버 위협 정보를 계속해서 공유하고, 상호 이해관계가 있는 사이버 사고에 관해 적절히 협력하며, 사이버 위기관리 모범사례를 교환하고, 관행, 연구 및 훈련에 상호 참여'한다는 합의를 했다.

4. 미국의 사이버 인태전략

미국의 사이버 전략은 인도태평양 전략과 개념적으로 유사하다. 미국은 인태전략을 통해 동맹 및 파트너 국가들과 협력을 통해 ▶자유롭고 개방된 ▶연결된 ▶번영하는 ▶안전한 ▶회복력 있는 인도-태평양을 구축하려 한다. 미국과 동맹국은 핵심 이익으로서 자유롭고개방된 인도-태평양을 요구한다.[32] 쿼드(QUAD) 협력체계에서는 이미 중국 배제라는 공통의 접근이 이뤄지고 있다. 향후 인태전략에서도 유사한 동조화 추진이 예상될 수 있다.[33]

2022년 한미 정상회담에서 '디지털 권위주의'에 대응하는 '개방적인 인터넷'을 강조했다. 양국은 '자유로우며 글로벌하고 상호 운용가능하며 신뢰할만하고 안전한 인터넷이 제공하는 특별한 혜택에 대한 공통된 인식'을 바탕으로 '투명하며 안전한 5G 및 6G 네트워크 장비와 구조를 발전시켜 나가기 위해 협력'하기로 했다. 미국의 인태 전략이 중국의 영향력 확대를 견제하는데 한미 사이버 위협 인식도 유사하다. 네트워크 장비를 언급한 부분은 미국이 안보 위협을 우려해 중국 통신 장비 사용을 금지하는 기조와 맥락이 같다.[34] 2023년 SCCF에서도 개방성을 강조한다. '개방되고, 상호운용이 가능하며, 안전하고, 신뢰할 수 있는 인터넷과 안정적인 사이버공간을 증진하는 것의 중요성을 강조'한다고 명시했다.

5. 북핵 고도화에 대응

북핵 고도화에 따라 한미 동맹 사이버 작전 협력 중요성이 부각된다. 위기 발생 이전 단계부터 다층적·실실적 협력이 필요하다. 여기에는 군사적 기능 뿐 아니라 국가의 주요 기반 능력이 대부분 포괄된다. 또한, 직접적인 군사적 대응 뿐 아니라 사이버 금원 탈취 등 불법적 활동을 망

30) 사이버 플레그 훈련은 2010년 5월 창설한 미 사이버사령부가 2011년 12월 영국 등과 연합 훈련을 실시하면서 시작됐다.

31) 사이버 플레그 훈련에는 한국을 비롯해 미국, 영국, 캐나다, 호주, 뉴질랜드 등 총 25개국이 참가했다. 공격훈련에서 참가국 간 위협정보를 공유하고 가장 효과적인 대응방법을 도출하여 방어작전의 효과를 검증했다. 이를 통해 사이버 위협에 대한 식별·분석·공유·제거·거부 등 방어적 작전 절차를 숙달했다. "우리 군, 미 사이버사 주관 사이버 플래그 훈련 최초 참가" 『사이버작전사령부 보도자료』(2022.10.24.)

32) 미국 인태전략의 주요 내용과 특징은 다음을 참조. 민정훈, "바이든 행정부의 인도-태평양 전략과 한국에의 함의," 『IFANS FOCUS』(국립외교원, 2022.2.23.)

33) 2021년 5월 쿼드 참여 국가는 중국이 배제된 글로벌 공급망 구축을 논의했다. 관련 동향과 쟁점은 다음을 참조. 송태은, 『연합 사이버 전력의 역할과 한·미 사이버 안보협력의 과제(정책연구시리즈 2022-12)』(서울: 국립외교원, 2023), pp. 35~39.

34) 2021년 바이든 미 대통령은 유럽 국가에 중국 통신장비를 사용하면 정보가 유출 될 우려가 있어 화웨이(華爲) 장비 사용을 자제해야 한다고 촉구했다. 앞서 2020년 로버트 스트레이어 미 국무부 부차관보는 한국 통신사(LG유플러스)에 화웨이 통신장비 사용 중단을 요구했다.

라한다.

양국은 SCCF에서 '자금세탁, 가상자산 탈취를 포함하여 사이버공간에서의 악성활동을 탐지·억지·와해하기 위해 협력하고, 다양한 원천으로부터 정보공유를 지속한다'고 했다. 북핵 개발에 전용하는 금원 창출을 원천적으로 차단하기 위한 노력 강화를 예상할 수 있다.

하이브리드 전쟁은 사이버 선제공격 후 물리적 전쟁을 개시하는 특징을 내포하며,[35] 북한은 전면적 침공을 앞두고 한미 연합군에 대규모·동시적 사이버 공격에 나선다고 전망된다. 한미는 동일한 유형의 공격에 대응해 피해를 최소화 해야 할 필요성이 있다. 따라서 SSCF에서 '악의적인 사이버활동 방어를 위한 대비를 포함하여 에너지, 금융 분야와 같은핵심 국가 기반시설 보호를 위한 핵심기술 연구·개발에 협력한다'고 확인 한 바와 공동의 노력이 필요하며 예상된다.

양국은 공동으로 침해를 대응 할 전망이다. SCCF는 '국익 또는 핵심 기반시설에 영향을 미치는 중대한 사이버사고가 발생한 경우, 긴밀한 양국간 협의와 정보 공유를 통해 조율된 행동 그리고/또는 병행 대응 조치를 적절히 실행한다'는 협력의 원칙을 제시했다.

SCCF에서 명시적으로 언급하지 않았지만 북핵 대응 측면에서는 '발사왼편 전략'(Left of Launch) 등 선제적 및 비물리적 군사 작전의 필요성과 실행 가능성이 부각 받고 있으며, 이와 같은 네트워크마비전(NPW) 차원에서 북핵에 대응한 한미 간 협력 필요하다. 북한 사이버 취약성을 식별하고 효과적인 작전을 수행하기 위해서는 한미 상호 정보 및 인식 공유하고, 특화된 역량을 통합 운용할 필요가 있다 연합/합동작전 계획 수립과정에서 사이버 및 전자전 등에서 상황 공유과 인식, 임무와 표적식별, 결심 및 전력 운용 등 전영역 협력이 필요하다.[36]

Ⅳ. 사이버 동맹의 미래와 과제

1. 워싱턴 선언 그 이후

워싱턴 선언에 따른 구체적인 조치가 나오기 시작했다. 2023년 6월 한미는 '고위운영그룹'(SSG)를 공식 출범하며 협력의 수준을 높였다. 협의체는 사이버 공간에서 발생하는 다양한 국제적 과제와 사이버안보 관련 양국 현안을 신속하게 처리하는 역할을 맡는다. 양국은 출범회의에서 ▶위협정보 공유 ▶훈련 상호 참여 ▶인력교류 ▶북한 불법 가상자산 탈취 차단 ▶기반시설 보호 ▶주요 사이버안보 정책 및 표준개발 ▶주요 국가 시스템 보안 강화 ▶ 악성 행위자에 의한 네트워크 취약점 제거 ▶사이버위협 대응을 위한 보안 강화 정책 도입 ▶암호체계 점검 등 다양한 논의를 진행했다. 양국의 정책 결정 핵심 기관과 사이버 안보 관련 핵심 기관이 모두 참여했다. 2023년 12월 서울에서 2차회의를 개최했고 2024년 5월 미국에서 3차 회의를 열었다. 양국은 1주년을 맞은 사이버안보 협력 프레임워크rk 양국 사이버안보 협력의 구심점 역할을 성공적으로 했다고 평가했다.

사이버 협력의 대상은 넓어진다. 2023년 8월 18일 개최한 한미일 정상회의에서는 '한미일 사이버 협력 실무그룹'(Trilateral Working Group)을 발족하기로 합의했다. 북한이 핵과 WMD 개발을 위한 불법적인 자금을 획득하는 걸 막기 위한 한미일 3자 협력을 촉진하게 된다.

---

35) 러시아는 2022년 2월 24일 우크라니아 침공에 앞서 사이버 공격은 두 달 전인 2021년 12월 28일 시작했다는 기록도 발견됐다. 박동휘 외, 『사이버전의 모든 것』(서울: 플래닛미디어, 2022), pp. 147~148.

36) 이수진 외, 『지상군 사이버·전자전 작전수행절차 정립방안 연구』(국방대학교, 2021), pp. 72~77.

한미 안보 협력은 민간 분야로 확장된다. 2023년 9월 한미 양국은 '제7차 한미 ICT 정책 포럼'을 미국에서 개최했다. 박윤규 과기정통부 2차관을 비롯한 총 38명의 민관 합동 대표단은 미국 정부기관 및 국제기구 주요 인사를 만났다. 여기서 한국 정부의 '디지털 신질서 정책'을 소개하며 지지를 요청했다. 한미 양국은 포럼 개설 이후 처음으로 공동성명문(Joint Statement)을 발표하며 AI, 오픈랜, 6G 등 첨단 디지털 분야에서의 구체적 협력 방안을 논의했다. 대표단은 방미 기간에 알랜 데이비슨 국가통신정보관리청(NTIA) 청장과 면담에서도 Open RAN, 6G 분야에서 양측 통신 사업자 및 장비업체와 공조해 통신 공급망 다양성을 제고하는 데 협력하기로 합의했다.

2. 한미 융합안보의 필요성

미국은 통합억지 전략을 구상하면서 한국의 정치·경제·산업을 포괄하는 전면적인 대중국 견제 참여를 희망한다. 이에 사이버 분야 협력은 기존보다 포괄적·전면적 수준으로 심화한다고 예상할 수 있다. 2023년 워싱턴 선언은 그러한 기대를 반영한 결과로 해석된다. 한국과 미국은 가치를 공유하며, 포괄적 동맹 발전을 추구하면서 다층적 위협에 대응해 상호 국익을 극대화하는 동맹 발전 필요성 확인했다. 사이버 영역 협력에 관한 구체적·실질적 실행 방안을 최적화하는 협의가 필요하다.

한미는 안보·군사적 협력은 경제 등 여타 분야로 확장될 전망이며, 한미 동맹 활용과 국익을 보전하기 위한 사이버 협력 방안을 모색할 필요가 있다. 미국은 미국을 중심으로 형성하는 다자적 체제와 동맹 관계를 묶어 전략적 경쟁에 수단으로 활용한다는 구상하며, 군사적 수단은 이전보다 더 공고하게 연계될 것이며, 동맹협력과 대중국 경쟁의 수단은 경제를 비롯한 다양한 영역으로 지속 확장될 전망이다.

이처럼 '융합안보 시대'를 맞아 다차원적인 한미 동맹 발전 필요성이 확인된다. 특히 초연결 시대 고도화는 기존 정보보안 수준을 넘어서는 포괄적 안보위협을 내포하며, 이에 융합안보 중요성이 본격화되고 있는 상황이다. 4차 산업혁명 시대에 진입하면서 기존 통신기술을 넘어서는 초고속·초저지연·초고용량 데이터 송수신이 급격하게 증가하면서 사이버 침해에 따른 치명적인 안보위협 가능성이 우려된다.[37] 미래전은 NPW 특징을 내포하며, 사이버와 전자전 효과를 병행하는 통합작전 요구, 초연결 시대는 지휘통제망·무기체계망·기반체계망이 복합적으로 연결돼 군사적 중추기능이 마비될 취약성을 내포한다.[38]

한미는 국방 분야에서 이미 높은 수준의 상호 운용성 지속, 사이버 영역에서 상호 의존성은 더욱 심화될 전망이다. 한미 연합군은 다양한 유·무선 체계(지휘·통제·정보·통신 등)가 밀접하게 연결돼 있고, 무기체계 상호운용성도 높은 수준을 지속하고 있으며, 사이버 침해 발생 시 상호 동조 및 심화 파급이 우려된다. 한미 연합군은 높은 수준의 연합 작전을 구현하기 위해 연합 지휘·통제 체계(센트릭스-K 등)와 통신 체계(데이터 링크 등)가 연결돼 있어 사이버 침해가 발생할 경우 다양한 영역으로 피해 확산도 대비해야 한다.

국방 영역에서 과학·기술이 고도화 하면서 한미는 사이버 영역에서 상호운용성은 더욱 점증하며, 궁극적으로 국방 및 안보 전반 영역에서 상호의존성도 심화할 전망이다. 한국은 최근 우주분야 능력을 보유하면서 한미는 우주 영역에서도 협력을 촉진할 여건을 마련, 사이버 차원 협력

37) 홍규덕 외, 『초연결사회 국가보안의 위기, 왜 융합보안인가?』 (군포: 북메이크, 2021), p. 193.
38) 송운수, 『사이버 군사전략 개관』(인천: 진영사, 2022), p. 173~179.

도 병행된다. 한미는 우주감시를 비롯한 국방을 비롯한 포괄적인 우주 분야 협력 촉진이 예상되며 양자 통신과 사이버 등 우주 분야와 연계한 협력이 이뤄질 전망이다. 우주 자산 활용이 증대할수록 사이버 통제권이 중요하며, 사이버 분야 의존도가 비례 증가하고 치명적 취약성은 사이버 영역에서 발생할 가능성도 우려된다.

3. 한미 융합안보의 과제

한미는 정보공유를 확대하고 상호운용성을 고도화하면서 기술적 연대가 필요하며, 동시에 기술적 역량을 강화해야 한다. 다만, 동맹 간 협력에서 고려할 사안은 꽤 많다. 여러 요인 중 일부는 상호 충돌하기도 한다.

한국은 미중 경쟁 구도에서 미국의 대중국 전략에 연루되는 상황을 고민해야 하며, 전면적인 편승 전략을 구사할지, 선택적 협력을 할 것인지, 어떤 분야에서 어떠한 형식과 수준으로 협력할 것인지 대안 마련이 필요하다. 한국은 인태전략을 발표하면서 특정 국가를 대상으로 하거나 배제하지 않는다는 원칙을 제시했다. 미국에선 이에 대해 모호한 전략이라는 비판도 나온다. 사이버 동맹을 추진함에 있어서도 유사한 동맹 간 간극 존재가 불가피해 보인다.

2023년 9월 미 하원에서 '해외 비신뢰통신 대응에 관한 법안'이 상원에 회부됐다. 법안은 미국의 동맹국에 대한 화웨이·ZTE 통신장비 사용 실태를 조사하는 걸 목적으로 한다. 한국 정부는 공공기관에서 중국 통신 장비 업체인 화웨이 제품을 비롯한 국제사회 제재 대상 품목 사용에 대한 조사를 진행했다.[39] 앞서 2022년 바이든 정부는 첨단 반도페 생산이 가능한 장비와 기술을 중국 기업에 판매를 금지하는 조치를 했다. 동맹국에 대해서도 '해외직접제품규정'(FDPR)을 적용해 미국 기술이 포함된 제품의 유출을 통제하려 한다.

중국 통신 장비 사용에 대한 한국과 미국의 견해는 다소 차이가 있다. 2019년 도널드 트럼프 미 행정부는 화웨이를 '수출 금지 블랙리스트'에 올렸다. 2020년 한국에 관련 장비 사용 중단도 요청했다. 그러나 한국 정부는 "5G와 관련해 보안 문제가 있는지 계속 확인하고 있다"면서도 "기업이 알아서 하는 것"이라며 직접적인 규제와 개입은 피했다.

따라서 한미는 정보공유를 확대하고 상호운용성을 고도화하면서 기술적 연대가 필요하며, 동시에 기술적 역량을 강화해야 한다. 동시에 기술적 종속이나 특정 기술 배제 강압에 대응할 필요도 있다. 한미는 상호 국익을 극대화 할 수 있는 방안을 고심하며, 사이버 및 통신 관련 장비 공급망에 대해 긴밀하게 조율해야 한다. 안보와 산업의 여러 요인을 살피면서 통찰력 있는 대안을 창출해야 한다. 이러한 전략적 목적을 달성하기 위해서는 충분한 분석과 논의, 호혜적인 협력이 필요하다.

39) 국정원은 "우리 정부 기관·IT 보안업체의 국제사회 제재 위반 연루로 인한 피해 방지 차원에서 공공기관을 대상으로 화웨이를 포함한 국제사회 제재 IT제품 도입현황을 파악했다"고 밝혔다. 뉴시스(2023.4.19.)

〈참고문헌〉

'엔드포인트보안연구개발실' 위협 분석 보고서(2023.9.26)

"우리 군, 미 사이버사 주관 사이버 플래그 훈련 최초 참가" 『사이버작전사령부 보도자료』(2022.10.24.)

"이종섭 국방부장관, 미 사이버사령관 접견"『국방부 보도자료』(2022.8.18.)

『시사인』, 제290호(2013).

『한국일보』, 2022년 10월 19일.

Defense Cyber Strategy 2023.9

National Cybersecurity Strategy 2023.3

Sharon Rollins, "Defensive Cyber Warfare Lessons from Inside Ukrain," Proceedings, Vol. 149/6/1,444, June 2023.

김보미. "김정은 시대 북한 사이버 위협의 특징과 대응 방안," 김상배 엮, 『신흥기술·사이버 안보의 국가전략』(서울: 사회평론아카데미, 2023)

김소정, "2023 미국 사이버안보 전략 주요내용과 한국에의 시사점," 『이슈브리프 423호』(국가안보전략연구원, 2023.3.8.)

노훈 외. "NCW: 선진국 동향과 우리 군의 과제," 한국국방연구원,『주간국방논단』, 제1046호(2005.5.9),

뉴시스(2023.4.19.)

대한민국 국방부. 『국방백서 2014』(2014.12)

대한민국 국방부. 『국방백서 2022』(2023.2)

로렌스 프리드먼(조행복 옮김), 『전쟁의 미래』(서울: 비즈니스북스, 2020)

민정훈. "바이든 행정부의 인도-태평양 전략과 한국에의 함의," 『IFANS FOCUS』(국립외교원, 2022.2.23.)

박동휘 외. 『사이버전의 모든 것』(서울: 플래닛미디어, 2022)

박용한. "우주국방의 시각에서 본 신흥기술·사이버 안보," 김상배 엮, 『신흥기술·사이버 안보의 국가전략』(서울: 사회평론아카데미, 2023)

박재풍. "뉴테러리즘의 의미재정립과 대응에 관한 연구," 한국정책학회, 『한국정책학회 춘계학술발표논문집』(2011)

백민정. 「국제법적 시각에서 본 사이버 작전 관련 미국의 입장」, 『동북아안보정세분석』, 한국국방연구원, (2020.5.15)

손한별. "새로운 정보전 양상과 데이터 안보," 김상배 엮. 『신흥기술·사이버 안보의 국가전략』(서울: 사회평론아카데미, 2023)

송운수, 『사이버 군사전략 개관』(인천: 진영사, 2022)

송운수. 『사이버 군사전략 개관』(인천: 진영사, 2022).

송태은. "러시아-우크라이나 전쟁의 정보심리전," 김상배 엮. 『신흥기술·사이버 안보의 국가전략』(서울: 사회평론아카데미, 2023)

송태은. 『연합 사이버 전력의 역할과 한·미 사이버 안보협력의 과제(정책연구시리즈 2022-12)』(서울: 국립외교원, 2023)

신승휴. "한미 사이버 안보협력의 진화: 복합지정학의 시각," 『4차 산업혁명 시대의 한미관계』(정보세계정치학회 춘계학술대회 발표자료, 2023.4.28.)

이수진 외.『지상군 사이버·전자전 작전수행절차 정립방안 연구』(국방대학교, 2021)
『중앙일보』 2023년 9월 19일
최선우 외. “북한의 사이버 테러리즘에 관한 연구,” 한국공안행정학회,『한국공안행정학회보』, 46권(2012)
피터 W.싱어 저, 권영근 역,『하이테크 전쟁』(서울: 지안, 2011)
홍규덕 외,『초연결사회 국가보안의 위기, 왜 융합보안인가?』(군포: 북메이크, 2021)

이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.