국가전략연구위원회 이슈브리핑 2호 (발간일: 2023.05.15.)

사이버 안보 분야 한미 정상회담의 성과와 과제: 국방의 관점[1)]

박용한 (한국국방연구원)

1. '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. 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.[2)]

양국 정상은 선언적 수준보다 좀 더 구체적인 협의안을 꺼냈다. 사이버안보 협력 프레임워크(SCCF)를 채택해 사이버 협력의 범위·원칙·체계를 구체화했다.[3)] 공동성명에서 언급한

1) 이 글은 2023년 5월 10일 제1차 국가전략포럼에서 발표된 발표문을 수정보완한 것이다.
2) 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.
3) 한미 사이버안보 협력 프레임워크(SCCF)은 협력 분야, 협력 원칙, 협력 메커니즘에 관한 내용을 포함한다. 보다 구체적인 논의를 추후 지속 진행할 전망이다. SCCF는 '한·미는 상호방위조약이 어떻

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 활동'에 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.[4] 여기서 북한을 중국·러시아·이란 등과 함께 주요 위협으로 적시했다. 특히 북한이 사이버 가상자산을 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 협력 지속 심화 등을 협력 대상으로 언급했다.

양국 정상은 지난해 5월 한미정상회담에서 사이버 안보 협력을 논의한 이후 공통의 인식 공유와 협력을 지속했다. 8월 한미 사이버작전사령부는 '한미 간 사이버 작전 분야 협력과 발전을 위한 양해각서(MOU)'를 체결했다.[5] 9월 개최한 제3차 한미 고위급 확장억제전략협의체(EDSCG)에서 사이버 위협에 대한 한미 공조 강화를 약속하는 공동성명을 냈다. 이어 10월 미국 사이버사령부가 주최한 '사이버 프래그(Cyber Flag) 훈련'에 한국 사이버작전사령부가 최초로 참여했다.[6] 12월에는 '제6차 한미 사이버정책협의회'을 열어 관련 협의를

게 적용될지와 어떤 상황에서 적용될 것인지에 대한 논의를 시작할 예정'이라고 언급했다.

4) *National Cybersecurity Strategy* 2023.3

5) 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.)

6) 사이버 프레그 훈련에는 한국을 비롯해 미국, 영국, 캐나다, 호주, 뉴질랜드 등 총 25개국이 참가했다. 공격훈련에서 참가국 간 위협정보를 공유하고 가장 효과적인 대응방법을 도출하여 방어작전의

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 사이버사고에 관해 적절히 협력하며, 사이버 위기관리 모범사례를 교환하고, 관행, 연구 및 훈련에 상호 참여'한다는 합의를 했다.

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.[7)]

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.[8)] 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.

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.[9)] 쿼드(QUAD) 협력체계에서는 이미 중국 배제라는 공통의 접

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.)

7) 시기별 사어버 협력의 기조 변화는 다음을 참조. 신승휴, "한미 사이버 안보협력의 진화: 복합지정학의 시각," 『4차 산업혁명 시대의 한미관계』(정보세계정치학회 춘계학술대회 발표자료, 2023.4.28.), p. 4.

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

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

근이 이뤄지고 있다. 향후 인태전략에서도 유사한 동조화 추진이 예상될 수 있다.[10]

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.[11] 2023년 SCCF에서도 개방성을 강조한다. '개방되고, 상호운용이 가능하며, 안전하고, 신뢰할 수 있는 인터넷과 안정적인 사이버공간을 증진하는 것의 중요성을 강조'한다고 명시했다.

3. 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 망라한다.

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,[12] 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 같이 공동의 노력이 필요하다고 예상된다.

양국은 공동으로 침해에 대응할 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.

---

10) 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.

11) 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.

12) 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.

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 간 정보 및 인식을 공유하고, 특화된 역량을 통합 운용할 필요가 있다. 연합/합동작전 계획·수립과정에서는 사이버 및 전자전 등에서의 상황 공유와 인식, 임무와 표적식별, 결심 및 전력 운용 등 전영역 협력이 필요하다.[13)]

4. 사이버 동맹의 미래와 과제

미국은 통합억제 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 발전의 필요성을 확인, 사이버 영역 협력에 관한 구체적·실질적 실행 방안을 최적화하는 협의가 필요하다.

한미의 안보·군사적 협력은 경제 등 여타 분야로 확장될 전망이며, 한미 동맹 활용과 국익을 보전하기 위한 사이버 협력 방안을 모색할 필요가 있다. 미국은 미국을 중심으로 형성된 다자적 체제와 동맹 관계를 묶어 전략적 경쟁에 수단으로 활용한다는 구상을 하고 있으며, 군사적 수단은 이전보다 더 공고하게 연계될 것이고, 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 안보 위협 가능성이 우려된다.[14)] 미래전은 NPW 특징을 내포하며, 사이버와 전자전 효과를 병행하는 통합작전이 요구되고, 초연결 시대는 지휘통제망·무기체계망·기반체계망이 복합적으로 연결돼 군사적 중추기능이 마비될 취약성을 내포한다.[15)]

한미는 국방 분야에서 이미 높은 수준의 상호운용성을 지속하고 있으며, 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 있기 때문에 사이버 침해 발생 시 상호 동조 및 심화 파급이 우려된다. 한미 연합군은 높은 수준의

13) 이수진 외, 『지상군 사이버·전자전 작전수행절차 정립방안 연구』(논산: 국방대학교, 2021), pp. 72~77.
14) 홍규덕 외, 『초연결사회 국가보안의 위기, 왜 융합보안인가?』 (군포: 북메이크, 2021), p. 193.
15) 송운수, 『사이버 군사전략 개관』(인천: 진영사, 2022), pp. 173~179.

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 영역으로의 피해 확산도 대비해야 한다.

국방 영역에서 과학·기술이 고도화하면서 한미는 사이버 영역에서 상호운용성을 더욱 점증하며, 궁극적으로 국방 및 안보 전반 영역에서 상호 의존성도 심화할 전망이다. 한국은 최근 우주 분야 능력을 보유하면서 한미는 우주 영역에서도 협력을 촉진할 여건을 마련, 사이버 차원 협력도 병행된다. 한미는 우주 감시를 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.

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.

최근 한국 정부는 공공기관에서 중국 통신 장비 업체인 화웨이 제품을 비롯한 국제사회 제재 대상 품목 사용에 대한 조사를 진행했다.[16] 중국 통신 장비 사용에 대해 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. 뿐만 아니라 사이버 및 통신 관련 장비 공급망에 대한 긴밀한 조율로 간극을 좁혀야 한다.

16) 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.)