국가전략연구위원회 이슈브리핑 1호 (발간일: 2023.05.15.)

2023 한미 "전략적 사이버안보 협력 프레임워크(SCCF)" 실현을 위한 과제: 정보의 관점[1)]

김소정 (국가안보전략연구원)

1. 서론

2023년 4월 한미정상회담을 계기로 "전략적 사이버안보 협력 프레임워크(Strategic Cybersecurity Cooperation Framework)"가 공동 발표되었다. 이는 2022년 5월 한미정상회의에서 설정된 기조를 유지하면서 사이버안보를 국가의 정책 및 전략적 우선순위로 설정하고 개방적이고 상호운영이 가능하며 안전하고 신뢰성 있는 인터넷과 사이버공간을 목표로 한다.

2022년 한미정상회담 공동성명은 문서의 성격에도 불구하고, 기술 및 협력 분야를 명기함으로써 양국 간 협력의 구체화를 시작한 계기가 되었다. 동 문서에는 사이버가 10회 이상 언급되면서, 통신, 양자, 암호화폐 등 사이버공간의 이슈들에 대한 양국의 중요성을 재확인한 바 있다. 이에 우리나라는 △ 북한 사이버 위협 공동 대응을 위한 기술정보 사전확보 및 공유 강화, △ 사이버분야 공동 훈련 참여 확대, △ 사이버공격 대응을 위한 공통 판단기준 개발, △ 위기시 국가이익 보장을 위한 의사결정지원체계 확보, △ 사이버분야 규범질서 및 가치외교 쟁점 대응력을 강화, △ 실효성 있는 협력을 위한 구체성과 지속성 추구 등을

1) 이 글은 2023년 5월 10일 제1차 국가전략포럼에서 발표된 발표문을 수정보완한 것이다.

제안한 바 있다.[2)]

이를 계승한 2023년 "전략적 사이버안보 협력 프레임워크"는 기술, 정책, 전략 분야에서 협력을 증진하고 신뢰를 구축하며, 진영 간 경쟁 구조 속에서 한국의 입장을 명확히 하고 이를 명문화한 점이 주요한 특징이다. 이를 위해 후속조치 및 시행 실행력 확보가 프레임워크 도출 성과의 안정화를 위한 전제 요건이다.

이하에서는 2022년 공동성명 및 2023년 프레임워크에서 합의한 협력분야별 한미 협력 현황과 향후 과제를 살펴보고, 추가 협력 가능한 분야를 식별해보고자 한다. 이를 통해, 앞으로 진행될 양국 간 협력의 방향 정립에 참고하며, 한미 간 협력뿐 아니라, 주요 우방국 간 협력 방향 설정에도 활용할 수 있을 것으로 기대한다.

2. 국가 전략 목표 구현을 위한 정책 수행 체계 구축

우리나라가 2019년 발표한 국가 사이버안보 전략은 현존하는 최상위 사이버안보 분야 정책문서이다. 2022년부터 급격히 진행되었던 사이버안보 분야 협력 활동과 이를 뒷받침하기 위한 정책의 시행은 큰 틀에서는 2019년 전략과 궤를 같이한다고 볼 수 있다. 하지만 전략을 현실화하기 위해 수립 및 시행된 국가 사이버안보 기본계획 및 부처 차원의 시행계획, 국가 차원의 사이버안보 분야 R&D 계획 등이 양국의 협력 추진 방향을 정확히 담아내고 있는지에 대해서 객관적으로 평가해야 한다. 예를 들어, 국가의 사이버안보 분야 R&D 계획이 전략의 추진 방향과 정합성을 갖는지, 전략 구체화를 위한 연구개발 목표가 R&D 계획과 예산배분 계획에 적절히 반영되고 있는지 등에 대해 판단·평가하는 것이다. 이 과정에서 주요 협력 분야에 가시적 성과를 도출할 수 있는 제반조치가 취해질 수 있도록 관련 규정 및 체계를 확보하고, 불필요하거나 중요성이 줄어든 항목에 대해서는 예산 배분 등을 재조정해야 한다. 필요한 경우 현재 개정논의가 진행중인 국가 사이버안보 전략에 반영할 수도 있다.

3. 차단 및 억지, 정보공유

2022년 정상회담 이후 북한의 악의적 사이버 행위 대응은 한미 간 공조가 가장 명확한 분야이다. 양국은 북한의 IT인력 외화벌이 차단과 암호화폐 탈취를 통한 제재 우회 저지 및 핵미사일 프로그램 자원조달 차단에 큰 노력을 기울이고 있다. 사이버워킹그룹 설치 및 운영, 3차례 정례회의 개최를 통해 직접적 대응방안을 논의했다. 그 결과 2022년 12월 8일 외교부·국가정보원 등은 국적과 신분을 위장한 북한 IT 인력을 고용하거나 이들과 업무 계약을 체결하지 않도록 국내 기업들이 주의와 신원확인을 강화할 것을 요청하는 정부 합동주

2) 김소정, "2022 한미정상회담과 사이버안보 : 억지력 강화를 위한 전략적 과제", 국가안보전략연구원 이슈브리프 제361호, 2022년 5월 31일

의보를 발표하였다.[3] 동시에 북한인 4명과 기관 7곳을 첫 사이버 분야 독자 제재 대상으로 지정한 바 있으며, 최근 한국과 미국이 불법 사이버 활동을 통해 북한의 대량살상무기(WMD) 자금 조달에 관여한 북한 국적자 1명을 한미 양국이 동시에 제재 대상으로 지정했다.[4] 국가정보원은 미국 국가안보국(NSA)・연방수사국(FBI) 등 정보기관과 합동으로 북한의 사이버공격 위협 실태를 알리고 이를 예방하기 위한 보안 권고문을 발표하기도 했다.[5]

이러한 노력은 정부간 협력 외에도 연구계 및 관련 산업계의 연계와 함께 이루어졌다는 점에서 협력의 실질성을 더하고 있다. 2022년 UN 대북제재 패널보고서에 처음 북한 가상자산 탈취자금의 핵무기 개발 프로그램 사용을 언급한 미국 CNAS(Center for a New American Security)는 한국과 공동으로 라운드테이블을 개최하였고[6], 제3차 워킹그룹과 연계한 비공개 1.5트랙 회의 개최, 제4차 한국안보서밋(Korean Security Summit)과 같은 주요 국제 학술회의에서 주제로 다루는 등[7] 관・학・연・산 협력이 활발히 진행했다. 또한 2023년 상반기 발표된 UN 대북제재 패널보고서는 북한의 악의적 사이버 행위와 인물 등에 대해 상세한 내용을 다루고 있으며[8], 미국 제재 담당 부서인 OFAC(Office of Foreign Assets Control)은 가상자산이 유통되는 분산 금융환경 위험 경감을 위한 보고서[9]를 발표하기도 했다.

우리나라는 한미 간 공조를 적극적으로 수행해 왔음에도 불구하고, 분산금융 서비스의 규제정책 구성에는 상대적으로 늦게 관심을 기울였다. 관련 정책포럼이 최근 결성되어 논의를 시작하면서 기존 금융전문가들과 가상자산 전문가 간 교류가 이제 막 시작되었다. 가상자산 탈취에 적절히 대응하기 위해서는 기술적으로 특수한 내용이라 할지라도, 기존 금융권에서의 악의적 행위에 대한 대응 활동을 먼저 이해하고 참고할 필요가 있기 때문에, 이런 활동들은 고무적이다. 예를 들어, 재래식 대테러 자금 추적 및 자금세탁 방지 방식이 분산 환경에서도 일정 정도 차용될 수 있으므로 양방 간 이해 강화가 선행되어야 한다.

또한 한미 간 북한의 사이버 역량과 위협 평가 등에 있어 공통의 시각을 갖고, 상호

3) 외교부, "북한 IT 인력에 대한 정부 합동주의보 (국문)," 2023년 2월 22일. https://www.mofa.go.kr/www/brd/m_25605/view.do?seq=1&page=1
4) 오수진, "한미, 사이버분야 첫 동시 대북제재...'암호화폐 세탁' 북한인", 연합뉴스, 2023년 4월 24일
5) 길민권, "국정원, 北의 랜섬웨어 공격에 '韓美 합동 사이버 보안 권고문' 발표", 데일리시큐, 2023년 2월 10일
6) Center for a New American Security, "Virtual Event | U.S.-ROK Strategy for Enhancing Cooperation on Combating Cyber-enabled Financial Crime." August 9, 2022. https://www.cnas.org/events/virtual-event-u-s-rok-strategy-for-enhancing-cooperation-on-combating-cyber-enabled-financial-crime
7) Kuksung Nam, "US, South Korea experts call for practical cooperation to tackle North Korean crypto theft," The Readible, April 14, 2023. https://thereadable.co/us-south-korea-experts-call-for-practical-cooperation-to-tackle-north-korean-crypto-theft/
8) ODS – Sédoc, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N23/037/94/PDF/N2303794.pdf?OpenElement
9) US Department of the Treasury, "Illicit Finance Risk Assessment of Decentralized Finance," April 2023. https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf

간 이해에 기반한 협력이 가능한 환경 구축이 필요하다. 이 지점은 정부간 협력 외 연구기관 간 협력이 필수적이다. △ 사이버공격 및 자산 탈취대응을 위해 부과된 제재의 유효성 평가, △ 가상자산 탈취를 포함한 악의적 행위자 식별·공개 과정의 절차적 정당성 확보, △ 공격자 식별 및 지목 과정의 신뢰성 보장, △ 국가차원의 정책결정 과정 지원용 데이터 기반 정책자료 생산, △ 국가 대응 매트릭스 고도화 등이 공동 연구 어젠다가 될 수 있다.

이 과정에서 양국 간 정보공유는 필수적으로 선행되어야 한다. 현재 정보·외교·국방·법집행·IT 등 부처별 협력체계는 구성 및 운영 측면에서 그 역할을 충분히 잘 수행해 왔다. 앞으로는 국가안보 이슈들에 대한 통합적 정책결정이 가능하도록 안보실을 중심으로 한 정보공유 체계를 굳건히 하고, 부처별 단독행동 및 불협화음을 상당수 줄일 수 있을 것이다. 동시에 민간분야의 자생적 교류 활성화를 위한 체계를 마련해야 할 것이다. 특히 사이버안보 분야 트랙2 활성화를 통해 부처 간 직접적 협력이 어렵거나, 사전 공감대 형성이 필요한 분야에 적극적으로 활용할 필요가 있다.

또한, 미국과의 정보공유 강화는 향후 일본을 포함한 한·미·일, 나아가 파이브아이즈(Five Eyes)와의 정보공유까지도 고려해야 한다. 상호 간 정보 강점과 수요를 적절히 조정해야 할 것이며, 특히 정보공개 딜레마에 대해 주의가 필요하다. 즉, 국가 간 통합 및 조정된 정보공유 체계 활성화와 정보공유의 범위와 대상 등의 구체화가 추가적으로 필요할 것이다.

4. 국제규범 형성과 역량강화

사이버공간의 규범 형성 노력은 지난 25년간 지속적으로 추구되어왔으나, 구체적 결과물 도출에는 아직 이르지 못했다. 2004년 이후 지속된 UN의 사이버안보 정부 전문가 그룹(GGE)회의는 6차 회의를 끝으로 정체되어 있다. GGE는 도출한 결과는 3차 회의 시 합의한 "기존 국제법과 주권의 온라인공간 적용" 원칙과 제4차 회의에서 합의한 11개 규범뿐이다. 제6차 GGE와 병행된 개방형 워킹그룹(OEWG)도 현재 2차 회의를 진행하고 있으나, GGE에서 합의한 결과 외에 추가 결과물은 아직 도출하지 못한 상태이다. 그럼에도 불구하고 GGE와 OEWG는 사이버공간에서의 악의적 국가행위에 대한 규범 제정의 필요성을 촉발 시켰으며, 사이버공간에서 발생하는 행위에 대한 국제법 적용을 위한 노력을 유도함으로써 탈린매뉴얼 등의 연구결과물이 도출되는 계기가 되었다는 점에서 그 활동 의의가 있다.

2022년 초 발생한 러시아-우크라이나 전쟁으로 진영 간 대립은 더욱 심해지고 있다. 미국을 중심으로 한 서방측은 AUKUS나 IPEF와 같은 소다자 협의체를 새로 구성하고 반도체 등 경제안보 이슈를 중심으로 논의를 활성화 시키고 있다. 이들 협의체에서도 일부 사이버안보 이슈가 다루어지기도 한다. 랜섬웨어 대응 이니셔티브(CRI)가 랜섬웨어 대응을 위한 국가 간 협의체라는 점에서 사이버안보 이슈에 특화된 협의체이며, 30개국 이상이 참여하여 랜섬웨어 대응을 위한 국가별 모범사례 개발 및 공동 모의훈련 시행 등을 지속하고 있다.

미국은 UN 중심의 논의에는 소극적으로 대응하고 있으며, 자국이 중심이 된 양자 및

소다자 협의체를 통해 실무차원의 협력을 강화하고 있는 것으로 보인다. 특히, 민주주의 가치 보호를 강조함으로써 냉전시기로의 회귀에 대한 우려도 발생하고 있다. 이에 워싱턴 소재 주요 싱크탱크는 UN을 중심으로 한 사이버안보 규범 논의의 한계를 명확히 인식하고, 이를 대체할 수 있는 논의체 구성에 주의를 기울이기 시작했다. 하지만, 사이버공간이 인류의 보편적 공공재의 역할도 수행하고 있기 때문에 UN을 논의에서 완전히 배제시킬 수는 없다는 점도 명확히 인식하고 있다.

앞으로의 논의가 어떤 형태로 지속되더라도, 가상자산으로 대변되는 IT기술의 급격한 발전과 탈중앙화된 환경변화는 국가의 기능과 역할, 미래에 많은 고려사항을 제기하고 있다. 블록체인, 프라이버시 보호 기술 등 IT 기술의 발전은 탈중앙화된 정치·경제 체계 구축 가능성을 높였고, 전통적인 국가의 기능과 역할의 변화 가능성도 높아졌다. 예를 들어, 러시아-우크라이나 전쟁에서 큰 기여를 한 민간 업체와 전문가들은 기술적 측면에서 전쟁 수행 방식의 변화를 가져왔으며, 이는 앞으로의 규범 형성에 그들의 의견 반영도 고려해야만 하는 상황을 유도하게 되었다. 이와 유사하게, 가상자산 등 탈중앙화된 금융시스템이 보편화되면, 중앙집권적 금융체계에 기반한 국가의 권력과 기능 유지는 또 다른 국면을 맞을 수도 있다. 분산 금융 시스템에 대한 전통 금융방식으로의 규제를 검토하고 있는 미국 정부에 대한 반대가 강하다는 점이 이를 보여준다.[10)]

미국과 마찬가지로 우리나라도 분산금융 환경에 대한 정책이 불명확하기 때문에, 현재로는 양국 간 협력을 바로 시작하기는 어려울 것이다. 국제적으로도 민간사업자와 전문가의 의견이 얼마나 반영될 수 있느냐는 점에 대해서는 향후 논란의 여지가 있다. 공개 귀속 및 식별에 대한 GGE 논의 시 미국은 MS, 시만텍 등 민간 전문가들을 회의 과정에 참여시켜 이들의 의견을 반영한 규범 정립을 주장했다. 중국 등은 민간사업자들의 의견은 국가별로 국내에서 청취하고, 국제기구에서는 정부가 이들의 의견을 포함한 대표의견만 논의하자고 주장한 바가 있었다. 이를 현재에 다시 적용해 본다면, 민간사업자들 및 전문가들의 의견이 직접적으로 규범 형성에 반영되기는 어려울 수 있지만, 러-우 전쟁에서와 같이 위성서비스 제공 등 국가의 기반시설 운영에 결정적 기여를 했다는 점에서 그 적용이 다르게 될 여지도 있을 수 있다.

이러한 상황에서 한미가 국제규범 정립을 위한 협력 논의에 있어서는, 국제법 적용과 같은 진영 간 논리가 첨예한 분야보다는 북한 가상자산 탈취대응과 같은 개별 사안별 협력을 중심으로 대응하는 것이 우리 의견 반영과 역할 구체화를 통한 기여에 긍정적일 것이다. 2022년 한미정상회의 및 이번 프레임워크 발표를 통해, 진영 간 규범경쟁에서 미국 측에 한층 가까운 입장을 보인 것은 주지의 사실이다. 그럼에도 불구하고 진영 간 경쟁구도 속 전략적 자율성 확보를 위한 여지를 갖기 위해, 상대적으로 이해관계가 첨예하지 않은 사이버 역량 강화 활동 등에 적극적으로 기여함으로써 논리적 대립보다는 실질적 이익을 추구하는

10) 가상자산 및 분산금융 전문가들의 OFAC 보고서 초안에 대한 의견, 한미 제3차 사이버워킹그룹 연계 비공개 전문가간담회, 2023년 3월 6일,

것이 바람직할 것으로 판단된다.

사이버 역량 강화는 의미 그대로의 역량강화 지원과 동시에 우리의 안보적 목적도 달성할 수 있는 수단이 된다. 세계은행(World Bank)이나 국제전기통신연합(ITU: International Telecommunication Union) 등을 통해 동남아의 저개발국 및 개발도상국들은 한국의 사이버 분야 전략 및 정책 수립, 법제도 개발, 훈련 및 인력양성을 적극적으로 요청하고 있으며, 한국의 경험과 노하우를 공유해주기를 희망하고 있다. 이를 개발협력의 형태 혹은 공적개발원조(ODA) 사업으로 사이버안보 역량강화를 지원함으로써 우리나라의 사이버안보 수준 향상에 기여할 수 있다. 특히 동남아 국가 등 북한이 IT 인프라를 악용하고 인력을 파견시키고 있는 국가들 대상의 역량강화 활동에 집중하는 것이 효과적일 것이다.[11] 러-우 전쟁 개전 이전 미국이 우크라이나의 전략과 정책 수립, 인력양성 및 역량강화 등에 기여했다는 점은 시사하는 바가 크다.[12] 다만, 개발협력사업의 전단계(기획에서 평가까지)상 사이버안보 이슈는 비주류적 아젠다에 그치고 있으며, 국무조정실이 발표한 ODA 사업 성과지표 모델(안)에도 CCB 사업의 성과를 측정할 수 있는 항목이 부재하다는 점에서 한국의 연계 접근 및 CCB 선진화를 위한 향후 과제로 주목할 수 있다.[13]

이 외에 실질적인 역량강화 유도 활동에 적극적으로 참여해야 한다. 우리 정부는 2022년 4월 북대서양조약기구(NATO) 사이버방위협력센터(Cooperative Cyber Defence Centro of Excellence)의 기여국(Contributing Partner)으로 가입하였고, CCDCOE 주관의 Locked Shields에 참여해 왔다. 국가 간 사이버공간에서 발생한 악의적 행위 혹은 무력공격에 적용 가능한 국제법이 성문화되지 않은 상황에서, 개별국가의 사례별 판단에 따른 대응이 가능해짐에 따라 이에 대한 국가별 해석과 적용은 추후 사이버공간에 적용 가능한 국제법 개발에 적극적으로 활용될 것으로 예상된다. LS는 기술 공방훈련 외에도 전략훈련, 미디어 대응 등 정책결정 지원을 위한 다양한 분야가 포함되며[14], 이는 사이버공간의 갈등 대응을 위한 국가 간 대응체계 파악뿐만 아니라 참여국들 간 유사한 프로토콜 및 국제법 적용 관습을 만들어가는데 중요한 요소가 되고 있기 때문이다.

이 외에도 미국 주관의 사이버스톰 및 분야별 훈련이 다양한 만큼 훈련 참여를 확대하여 전략・정책・기술 모든 층위에서의 공통 인식과 대응 절차 개발에 초점을 맞출 필요가 있다. 재래식 분야에서처럼 훈련, 전술 및 정책, 전략 측면 공조가 가능한 통합훈련 등도 필요할 것이다. 이를 통해 한미 간 악의적인 행위자에 대한 공통의 책임 부과 기준을 개발하고, 국가차원의 대응체계를 조율해 나갈 수 있을 것이다.

러시아-우크라이나 전쟁 발발로 기술선진국들에 대한 지원요청과 미국 주도의 전진방

11) https://directionsblog.eu/south-koreas-indo-pacific-strategy-promotes-cyber-cooperation/
12) 김소정, "러시아-우크라이나 전쟁과 사이버안보 전략구상의 함의", 국가안보전략연구원 이슈브리프 358호, 2022년
13) 이지선・김소정, "사이버 안보와 개발협력 연계 접근에 관한 연구: 영국과 한국 사례 비교", 21세기정치학회보 제33집 1호, 2023년, p.46.
14) https://ccdcoe.org/exercises/locked-shields/

어 전략의 적극적 활용이 증가할 것이다. 이번 전쟁 수행 과정에서 미국은 수십 차례의 "선제적 예방 활동(hunt forward)" 시행을 청문회에서 공개했다. 전쟁 전과 진행 중 과정에서 민간 전문가 및 기업의 지원이 적극적으로 활용된 상황에서, 전후 복구 및 역량 강화를 위해 동맹국에 지속적인 지원요청이 예상된다. 우리나라는 특히 IT 및 사이버보안 분야 전문가들의 역량이 높아, 이들에 대한 지원이 가시화될 수 있을 것이다[15]. 미국과 캐나다 등은 사이버분야 국가예비군(Natioonal Reserve Guard)를 상시적으로 운영하고, 국가위기 시 활용하고 있다. 우리나라도 상비군 개념의 전문가집단을 운영 및 관리하고, 이들을 적법하게 활용할 수 있는 법 제도적 준비가 필요할 것이다.

5. 결론

사이버 분야에서의 강대국 간 경쟁은 매우 치열해지고 있고, 미국의 정보통신기반서비스 기업에 대한 의존도가 높은 현 상황에서, 한미 간 사이버안보 분야 협력을 공고히 할 것을 천명한 것은 중요한 의미를 갖는다. 한편으로는 전략적 규범경쟁 속에서 입지가 좁아졌다고 판단할 수 있으나, 우리나라가 기술적 자생력을 갖고[16], 전략적 자율성을 도모할 수 있도록 핵심분야 공동 연구개발과 규범 형성에 적극적으로 참가하여, 국제사회 및 동북아 지역에서 우리나라의 입지와 전략적 요충지로서의 중요도를 공고히 하는 기회로 삼아야 할 것이다.

15) 이에 대한 구체적인 내용은 김소정, "러시아-우크라이나 전쟁과 사이버안보 전략구상의 함의", 국가안보전략연구원 이슈브리프 358호, 2022년 5월 20일, pp.7-8 내용 참고.
16) Ibid., p.6