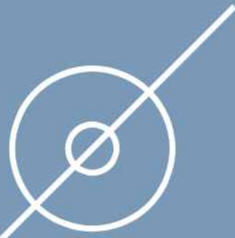


미국의 사이버안보 전략과 한미동맹



2024

I. 서론

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

2022년 한미정상회담 공동성명은 광범위한 기술 및 협력 분야를 명기함으로써 양국간 협력의 구체화를 시작한 계기가 되었다. 동 문서에는 사이버가 10회 이상 언급되면서, 통신, 양자, 암호 화폐 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, △ 위키시 국가이익 보장을 위한 의사결정지원체계 확보, △ 사이버분야 규범질서 및 가치외교 쟁점 대응력을 강화, △ 실효성 있는 협력을 위한 구체성과 지속성 추구 등을 제안한 바 있다.¹⁾ 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.

이후 2023년 8월 개최된 캠프 데이비드 한미일 정상회의에서 한미간 사이버안보 분야 상호협력 활동이 일본과의 협력으로 확대 적용될 것이며, 이를 시행하기 위해 한미일 고위급 안보 책임자가 함께 북한의 사이버 활동에 대응하는 '사이버 협의회'를 출범시키고, 한미일 3국 간 고위급 사이버 협의회 신설을 위한 실무 작업을 시작했다. 동 협의회는 핵·대량살상무기(WMD) 등 북한 무기 개발의 주요 자금원으로 악용되는 사이버 활동에 대한 차단 방안을 함께 마련할 것으로 알려지고 있다.²⁾

이를 위한 후속조치 및 시행 실행력 확보가 프레임워크 도출 성과의 안정화를 위한 전제 요건이 될 것이다. 이를 위해서는 미국이 그 동안 공개해 온 사이버안보 전략과 국방 사이버안보 전략에 대한 개괄적 이해를 통해 미국이 추진하고자 하는 사이버안보 협력 방향을 가늠해 보아야 할 것이다. 이하에서는 미국의 사이버안보 전략과 국방 사이버안보 전략, 한미간 협력을 위한 고려사항에 대해 살펴보고자 한다. 이를 통해, 앞으로 진행될 양국간 협력의 방향 정립에 참고하며, 한미간 협력 뿐 아니라, 주요 우방국간 협력 방향 설정에도 활용할 수 있을 것으로 기대한다

1) 김소정, "2022 한미정상회담과 사이버안보 : 역지력 강화를 위한 전략적 과제", 국가안보전략연구원 이슈브리프 제 361호, 2022년 5월 31일

2) <https://www.yna.co.kr/view/AKR20231106061900001>

다.

II. 미국의 사이버안보 전략

1. 2023년 이전 국가 및 국방 사이버안보 전략

21세기 정보기술의 발전으로 국가안보를 위협하는 새로운 유형의 안보영역으로 사이버분야를 고민하게 되었다. 위협의 주체와 공격의 방법이 다양화 되면서 전통적 방법의 대응책만으로 사이버 위협을 막는다는 것은 한계가 있다. 2000년대 이후 발생한 국내외 주요 공격들은 국가 간 전략목표 달성을 위해 국가차원에서 실행되었으며 안보적 차원의 위협으로 가시화되었다. 국가안보에 주축을 이루었던 전통적 분야인 군사영역을 넘어서 사이버 역량(cyber power)이 중요한 안보 요소로 등장하게 된 것이다. 사이버 공격자에게 사이버 수단은 전략적으로 유용하지만, 방어자에게는 대응전략과 체계구성에 어려움을 가중시킨다. 특히 사이버 공간이 공격 우위의 안보 구조라는 주장으로 이는 뒷받침된다.³⁾ 공격 의도를 가진 국가는 심지어 상대국에 사이버 위협을 직접 가하지 않더라도 개인이나 집단을 사주하는 등 다양한 방식을 연계하여 국가 전략 목적을 실현할 수도 있다.⁴⁾

미국은 2000년대 이후 다양한 정책문서를 통해 사이버안보의 중요성을 지속적으로 강화해 왔다. 2001년 직후 추진된 사이버 관련 법, 전략, 정책, 프로젝트, 계획들은 대부분 전자 정부 보안, 주요기반시설 보호에 초점이 맞추어져 있었다. 2001년 9.11 테러 직후 국토안보부 신설시 백악관에는 사이버안보 담당 보좌관이 임명되었다. 이후 거버넌스 체계의 변화는 있었지만, 최상위 정책결정 그룹에서는 항상 사이버안보 이슈를 중요하게 다루어왔다. 국가기관이 사용하는 인터넷과 네트워크의 안전성 확보는 가장 중요한 문제로 인식되어 2001 ~ 2003년 2년 동안에만 관련법 4건 이상 제정, 2개 이상 전략 수립, 4개 이상 대통령 명령 발표가 이루어졌고 이를 담당할 실무기관으로 국토안보부가 설립되었다. 특히 2003년 최초로 사이버공간 보호를 위한 국가 전략이 수립 및 발표되면서, 미국의 사이버공간 안보 강화를 위한 미국의 의지를 확인할 수 있다.

2003년 발표한 ‘안전한 사이버공간을 위한 국가전략(National Strategy to Secure Cyberspace)’은 미국 정부의 최초 사이버안보 전략으로 민관협력 체계 구축과 사이버사고 대응을 위한 연방차원의 대응계획을 수립하는데 기여했다. 2009년 오바마 정부 집권 초기에 발표한 사이버공간 정책 논평(Cyberspace Policy Review)은 전략은 아니나, 당시 집권한 오바마 정부의 사이버안보 강화 활동의 기본이 되었다. 2011년 사이버공간 국제 전략(International Strategy for Cyberspace)은 사이버공간에서 책임 있는 행위에 관한 국제규범과 표준 제정의 필요성을 강조하고, 미국 국익을 위한 적극적 방어(active defense) 태세를 갖추 것을 명확히 했다. 또한, 다양한 행정명령(Executive Order)과 대통령 정책 지침(Presidential Policy Directive)을 통해 주요기반시설 사이버안보 활동을 지속적으로 강화시켜 왔다.⁵⁾

3) Christopher Whyte & Brian Mazanec, Understanding Cyber Warfare: Politics, Policy and Strategy, Routledge, 2019

4) 김소정, “미국의 사이버공격 대응정책과 한국에의 시사점 - 솔라윈즈 해킹 대응사례를 중심으로”, 국가안보전략연구원 연구보고서 2022-04, 2022. p.19.

5) 김소정, “오바마 정부의 사이버안보 정책 추진현황과 정책적 함의”, 외교안보연구 제7권 제2호, 2011.12.

2018년에는 2003년 사이버안보 전략을 개정한 국가사이버전략(National Cyber Strategy)을 발표했다. 2018년 전략은 △ 미국의 정보와 기밀 보호를 위한 사이버공격 대응 및 방어 능력 강화, △ 사이버 위협에 대한 정보 수집·분석 능력 강화를 위해 민간 협력 강화 및 정보공유 확산, △ 인프라와 중요시스템을 보호 역량 강화, △ 국제사회와 협력하여 사이버공격에 대한 규제와 법적 대응체계 구축, 국제적인 사이버안보 협력 강화를 추진했다. 특히 2014년 크리미아반도 합병, 2016년 러시아의 미국 대선 개입 등 러시아의 공격 행위에 적극적으로 대응할 것을 분명히 했다. 이때에도 러시아, 중국, 이란, 북한을 4대 위협국가로 평가하고 있었다.

미국 국방부(DoD: Department of Defence)는 ‘악의적인 네트워크 행위자에 대한 행위 탐지와 대응의 필요성을 인식하여 적의 위협 및 취약성을 발견, 탐지, 분석 및 완화하도록 동기화된 즉각적인 역량’을 적극적 사이버 방어(ACD: Active Cyber Defence)라는 개념으로 정의하기도 했다.⁶⁾ 사이버 공격자에게 사이버라는 공간과 수단은 전략적으로 유용하지만, 방어자에게는 대응 전략과 체계를 갖추기 어렵게 하는 요소이다. 악의적 의도를 가진 국가들은 상대국의 사이버안보를 위협하는 직접적인 공격을 하지 않더라도 개인이나 집단을 사주하거나, 사회공학적 방식으로 회유 및 포섭하는 등 다양한 방식으로 국가의 전략목적 실현을 위한 악의적 행위를 시행할 수 있다. 이러한 사이버 위협의 완화와 방지를 위해서는 공격자에 대한 응징, 처벌이 필수적이다. 이를 위해 2015년 미국 국방부는 2015년 국방부 사이버 전략에서 귀속(attribution)을 효과적인 사이버 억지전략의 근본적인 요소로 식별하고 있다.⁷⁾

2018년 발표된 국방부 사이버안보 전략은 미 국방부가 평시, 위기 시 또는 갈등 시를 포함해 어느 상황에서도 미국 국내법 및 국제법을 준수하며 미국에 대한 모든 공격을 억지하고 미국의 국익을 저해하려는 목적을 가진 적으로부터 미국을 보호하기 위해 노력하고 있으며, 이를 위해 사이버 작전을 위한 역량을 개발하였고 이러한 사이버 역량을 미국 정부가 국익을 보호하기 위해 사용하는 외교, 정보, 군사, 경제, 금융, 법집행 등의 여러 가지 수단과 통합하고 있다고 설명하고 있다. 또한 “국방부는 상호 기관 파트너, 민간 부문, 동맹국, 파트너 국가와 협력하여 미국 국토와 국익에 심각한 결과를 초래할 수 있는 사이버 공격을 억지하고 필요할 경우 무력화시킨다. 정보, 경고, 작전 역량을 개발하여 경고하고 악의적인 사이버 공격을 완화하여 미국의 국익에 실질적인 여파를 미치지 못하도록 한다. 국방부는 모든 적용 가능한 법과 정책에 따라 글로벌 네트워크, 시스템, 적군의 역량, 악성 소프트웨어 브로커 및 시장에 관한 상세하고 예측가능하며 조치를 취할 수 있는 정보를 수집하도록 한다. 국가 방위를 위해 정부 내 다른 기관과 협력하여 연합 사이버 작전을 수행하고 이를 통해 사이버공간에서의 공격을 억지하고 필요할 경우 무력화시키도록 한다.”는 전략목표를 설명하고 있다.⁸⁾ 이를 구체화하기 위한 전략적 개념이 2018년 미국 국방부의 사이버안보전략에서 명시한 지속적 개입(persistent engagement)과 전진 방어(defend forward) 개념이다.⁹⁾

위협국가들은 그들의 국가이익 달성을 위해 경제적 강압, 정치적 영향력 개입, 정보작전, 사이버작전, 재래식 및 비재래식 군사작전을 통합하고 있다는 점이 지속적 개입의 필요성을 강화시켰

6) U.S. Department of Defense, Strategy for operating in cyberspace, Washington, DC: Department of Defense, 2011.

7) 김소정, “미국의 사이버공격 대응정책과 한국에의 시사점 - 솔라윈즈 해킹 대응사례를 중심으로”, 국가안보전략연구원 연구보고서 2022-04, 2022. pp.25-26.

8) U.S. Department of Defense, Summary of the Department of Defense Cyber Strategy, Washington, DC: Department of Defense, September 2018.

9) Jenny Jun, “The Promises and Limits of “Defend Forward” in the ROK Context,” GCPR 2022 (서울, 플라자 호텔, 2022년 9월 21일).

다. 악성코드를 침투시킨 사이버공격 뿐만 아니라 정치적 목적을 띤 선거 개입 등의 공격이 동시다발적 발생이 이러한 적성국의 의지를 확인시켜주고 있다.

지속적 개입은 기존의 억지전략을 강화하여 가장 직접적이고 일상적인 형태의 억지를 강제하고자 하는 개념으로, 미국 및 동맹국의 국가 안보 및 경제안보를 저해하려는 무력충돌에 미치지 않는 지속적인 사이버공격을 가하는 지능형 지속적 위협(APT : Advanced Persistent Threat)에 대한 대응을 말한다.¹⁰⁾ 지속적 개입의 주목적은 무력충돌의 기준에 미치지 않는 경쟁에서 주도권을 잡고 사이버 우위를 차지하는 것이다.¹¹⁾

"Defend forward" 전략은 미국이 사이버 공격에 대응하기 위해 적극적으로 행동하는 데 있어 다양한 사례를 포함한다. 이 전략은 실제로 사이버 공간에서의 위협에 대응하기 위해 국방부와 사이버 보안 기관들이 협력하여 다양한 활동을 실시하고 있다. 사전에 공격자의 활동을 탐지하고 그들의 공격을 막기 위해 사이버 위협을 모니터링하고 분석하는 능력을 강화시키고 있고, 다양한 사이버 공격의 원천이 되는 국가와 조직을 대상으로 정보 수집 및 사이버 공격을 미리 예방하기 위한 작전을 수행한다.

예를 들어, 미국은 2015년 키예프에 대한 러시아의 공격으로 전력망이 마비되었던 시점 이후 적극적으로 우크라이나를 지원해왔다. 폴 나카소네 NSA 국장은 미 의회 청문회에서 "실제 침공이 이루어지기 전에 ... 우크라이나의 기반시설을 공고히 하기 위해 NSA, 사이버사령부, 관계기관, 민간 파트너들과 함께 했습니다... 우리는 "hunt forward" 팀도 우크라이나에 보냈습니다¹²⁾"라고 청문회에서 언급했다.¹³⁾

2022년 발표된 국가안보전략에서는 사이버(cyber)라는 단어만 30회 이상이 언급되며, 위협인식, 대러·대중 경쟁우위 달성, 책임있는 행위에 기반한 국제 규범 수립, 역량 강화, 인력 양성 등 모든 분야에서 사이버의 중요성과 이를 통한 전략적 억지력 달성을 언급하고 있다.

2. 2023년 국가 사이버안보 전략¹⁴⁾

2023년 3월 2일 미국 정부는 국가 사이버안보 전략(National Cybersecurity Strategy)을 공개했다. 5년 만에 개정된 이번 미국의 사이버안보 전략은 미중 전략경쟁과 진영대립이 사이버 공간에서도 심화되는 현 상황을 반영해 큰 틀에서 주요기반시설 보호 체계 강화, 국제협력을 통한 위협국가 대응 활동 강화, 신기술 도래로 인한 미래 대비에 방점을 두고 있다고 요약할 수 있다. 시장에 기반한 자율적 보안을 추구한다는 원칙에는 변함이 없지만, 그 속에서 백악관 등 연방정부의 역할을 강화하고 실질적 보안수준 향상을 이끌 수 있는 구체적인 제도개선안들을 제시하고 있다.

우선, 국가 주요기반시설의 보호를 강조하면서 정부의 역할 강화를 통한 종합적인 책임 구조 구축을 강조하고 있다. 우리나라의 주요정보통신기반보호법 체계와 달리 미국은 전기, 에너지,

10) Michael P. Fischerkeller 외, Cyber Persistence Theory : Redefining National Security in Cyberspace, Oxford University Press, 2022.

11) John Mallery(전 MIT Media Lab 교수) 인터뷰, 2019년 9월 30일.

12) Paul M. Nakasone. The U.S. Senate Select Committee on Intelligence. '22. 3. 10.

Paul. M. Nakasone. Subcommittee on Intelligence and Special Operations Hearing: "Defense Intelligence Posture to Support the Warfighters and Policy Makers". '22. 3. 17

13) 김소정, "러시아-우크라이나 전쟁과 사이버안보 전략구상의 함의", 국가안보전략연구원 이슈브리프 358호, 2022

14) 이하 내용은 아래 문서의 내용임

김소정, "2023 미국 사이버안보 전략 주요내용과 한국에의 시사점", 국가안보전략연구원 이슈브리프 423호, 2023.

의료, 금융 등 영역별 보안 활동을 자발적으로 시행해 왔다. 1998년 대통령 행정명령 (Presidential Policy Directive) 63에서 주요기반시설 보호의 중요성을 언급한 이래, 약 90%에 해당하는 민간 주요기반시설 소유자 및 운영자들은 자발적으로 소유 및 운영하는 시스템의 보안 향상을 위해 노력해 왔다. 하지만 2021년 5월 발생한 콜로니얼 파이프라인 해킹 공격으로 자발적 보안체계만으로는 사이버안보 위협에 효과적으로 대응하지 못한다는 점을 인식하게 되었다. 주요 기반시설의 소유자 및 운영자가 민간에 속함에 따라 정부는 국토안보부를 통해 간접적으로 관리해 왔지만, 사이버공간과 주요기반시설에 대한 국가 및 국민의 의존성 증대, 이러한 주요기반시설의 인프라 대상 공격 증대는 정부의 직접적 개입과 강제적 보안 요구사항 적용 필요성을 제기하게 되었다. 이에, 민간 자율에만 맡겨두던 주요기반시설 보호 체계 변화를 수용할 수 있는 시작점으로써 이번 전략이 기능하게 된 것이다. 특히 영역별 보안수준의 편차가 크게 발생했던 점을 인식하고, 영역별 보안 수준 조정 및 최소 보안요구사항 강제가 진행될 것으로 보인다.

둘째, 주요기반시설과 시스템 보안 강화를 위한 민관협력 강화, 연방 네트워크 현대화 및 사고 대응 정책 개선을 강조하였다. 민간과의 협력 강화와 산업 촉진을 위해 시장주도의 기술혁신을 위한 인센티브를 지속적으로 제공하고, 정보공유를 강화할 것으로 언급하고 있다. 자발적 보안 활동 강화를 통한 방어력과 복원력(resiliency) 향상을 유도하고자 한다. 특히, 클라우드 서비스의 확산으로 중소기업의 보안 수준 향상에 크게 기여할 것을 기대하고 있다.

셋째, 악의적 행위자에 책임성을 강화하고 비용 부과를 지속한다는 것이다. 미국이 지난 약 20년간 사이버 공격에 대응해 온 방식은 1) 기소나 형사사법공조와 같은 법집행 활동, 2) 개인에 대한 여행제한, 자산동결, 수출입 제한, 3) 국가에 대한 개발원조 및 안보지원 등 중단, 무기수출 금지, 해당국 정부와의 금융거래 금지 등의 제재, 4) 가해국에 대한 항의, 비난, 국제기구 제재 추진, 외교관 추방 혹은 공관폐쇄 등의 외교적 조치, 5) 사이버를 이용한 대응 작전 시행 등이다. 그 연장선에서 공격자에게 책임과 비용을 부과하는 제재조치 시행이 지속될 것이다. 미 재무부는 ‘악의적 사이버 활동(malicious cyber activities)’을 이유로 행정명령 13694 및 13757에 의한 제재를 부과한 바 있으며,¹⁵⁾ 우리나라도 북한의 사이버활동에 대한 단독 대북 제재를 시행한 바 있다.¹⁶⁾

넷째, 공급망 보안 강화, 특히 소프트웨어 안정성 확보를 위해 노력할 것이다. 해당 내용들은 이미 기 발표되었던 대통령 행정명령 및 관련법 제개정 등을 통해 연방정부기관을 대상으로 시행 중인 정책이다. 이들을 지속적으로 추진함으로써, 소프트웨어의 세부내용에 대해 명확히 식별할 수 있는 소프트웨어 자재명세서(SBOM : Software Bill of Materials) 제도를 도입하고, 소프트웨어 개발, 배포 및 적용 전 과정을 관리감독하고, 소비자가 직관적으로 소프트웨어의 안전성을 인지 가능하도록 하며, 정부차원의 획득 및 조달 과정에 이러한 내용을 요구함으로써, 소프트웨어의 보안 강화를 질적으로 유도하고자 한다. 이러한 내용을 전략에 명문화함으로써 앞으로의 공급망 강화 노력도 이에 기반하여 출발할 것임을 분명히 하고 있다.

다섯째, 신기술 개발 및 인센티브 지원 등 시장의 자발적 참여를 유도하고, 보안인식 제고를 강조한다는 점이다. 신기술 개발은 이미 국가의 비교우위 달성을 위한 기본 전제조건이 되고 있다. 특히 양자컴퓨팅 및 AI를 통한 보안생태계 변화는 막대할 것이지만, 이와 관련된 정책결정, 보안생태계 및 거버넌스 구축에는 어려움을 겪고 있다. 이에 이러한 신기술의 연구개발, 표준 및 인증 등 과정에서 창의적 대안 모색과 국제사회와의 협력을 강조하고 있다.

15) U.S. Department of State, PRESS RELEASE, Imposing Sanctions on Virtual Currency Mixer Tornado Cash, AUGUST 8, 2022

16) 조상진, “한국 첫 ‘대북 사이버 독자제재’…개인 4명·기관 7곳 지정”, VOA, 2023년 2월 11일

여섯째, 국제협력을 강화하여 구체적이고 가시적인 결과물을 도출하고자 한다. 랜섬웨어 대응 이니셔티브 사례와 같이, 다수국이 공동으로 아이디어를 도출하고, 그 과정에서 참여국의 역할과 기여를 명확히 함으로써 책임감을 갖도록 유도할 것이다. 또한 UN의 사이버안보 정부전문가그룹(Group of Governmental Experts) 논의와 개방형 워킹그룹(Open-Ended Working Group)의 규범형성 노력도 지속할 것을 명시하고 있다. 이 외에도 쿼드(QUAD), 오키우스(AUKUS), 인도-태평양 경제프레임워크(IPEF) 등 모든 소다자간 협력체계와 사안별 양자협력도 활성화 시킬 것이다.

본 전략에서 다루는 제도개선 사항들은 앞으로의 방향을 명확히 제시하고 있다. 하지만, 전략에서 제시한 내용을 구현하는 데는 어려움이 있을 수 있기에, 대통령실 내 국가 사이버 국(Office of National Cyber Director)의 역할과 책임이 막중하다. 사이버 국은 현재 80명 규모의 인력을 100명 수준으로 확대하고, 부처간 업무조율과 규제 조화를 유도하는데 앞으로 큰 역할을 지속할 것으로 예상된다.¹⁷⁾

3. 2023년 국방 사이버안보 전략

또한 개정한 2023년 미국방 사이버안보 전략 요약문에 따르면, 2018년 이후 지속된 미국의 적극적 개입 정책도 지속될 것으로 설명하고 있다. 동 전략은 2022 국가안보전략, 2022 국방전략, 2023 국가사이버안보 전략과 함께, 바이든 정부의 사이버 국방 활동의 기본 전략으로 사용된다. 중국 및 러시아, 국제범죄조직이 야기하는 사이버위협 증대, 러시아의 우크라이나 침공으로 드러난 현대전에서의 사이버의 기능과 역할, 민간협력을 통한 통합적 작전 수행이 적극 및 국가후원 해킹조직의 공격 피해를 최소화하고, 사이버분야 국방에 적극적 노력을 기대할 수 있다는 점을 명시하고 있다. 특히 미 국방부는 캠페인을 목적으로 사이버 공간 작전을 수행하여 무력 충돌 수준 이하에서 적의 활동을 제한, 좌절시키거나 방해하고 유리한 안보 조건을 달성하기 위한 조치를 취하여, 지속적으로 적극적인 방어와 공세적 활동을 이어갈 것을 명확히 했다.¹⁸⁾

III. 한미 사이버안보 협력을 위한 고려사항

1. 차단 및 억지, 정보공유 강화

2022년 정상회담 이후 북한의 악의적 사이버 행위 대응은 한미간 공조가 가장 명확한 분야이다. 양국은 북한의 IT인력 외화벌이 차단과 암호화폐 탈취를 통한 제재 우회 저지 및 핵미사일 프로그램 자원조달 차단에 큰 노력을 기울이고 있다. 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 합동주의보를 발표하였다.¹⁹⁾ 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 1명

17) CSIS, "The Biden-Harris Administration's National Cybersecurity Strategy", Roundtable, 02 March, 2023

18) U.S. Department of Defense, 2023 Cyber Strategy of Department of Defense, 2023, pp.1-2.

19) https://www.mofa.go.kr/www/brd/m_25605/view.do?seq=1&page=1

을 한미 양국이 동시에 제재 대상으로 지정했다.²⁰⁾ 국가정보원은 미국 국가안보국(NSA)·연방수사국(FBI) 등 정보기관과 합동으로 북한의 사이버공격 위협 실태를 알리고 이를 예방하기 위한 보안 권고문을 발표하기도 했다.²¹⁾

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 개최하였고²²⁾, 제3차 워킹그룹과 연계한 비공개 1.5트랙 회의 개최, 제4차 한국안보서밋(Korean Security Summit)과 같은 주요 국제 학술회의에서 주제로 다루는 등²³⁾ 관·학·연·산 협력이 활발히 진행했다. 또한 2023년 상반기 발표된 UN 대북제재 패널보고서는 북한의 악의적 사이버 행위와 인물 등에 대해 상세한 내용을 다루고 있으며²⁴⁾, 미국 제재 담당 부서인 OFAC(Office of Foreign Assets Control)은 가상자산이 유통되는 분산 금융환경 위험 경감을 위한 보고서²⁵⁾를 발표하기도 했다.

한미 간 북한의 사이버 역량과 위협 평가 등에 있어 공통의 시각을 갖고, 상호 간 이해에 기반한 협력이 가능한 환경 구축이 필요하다. 이 지점은 정부간 협력 외 연구기관간 협력이 유용할 것이다. △ 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 양국간 정보공유는 필수적으로 선행되어야 한다. 현재 정보·외교·국방·법집행·IT 등 부처별 협력체계는 구성 및 운영 측면에서 그 역할을 충분히 잘 수행해 왔다. 민간 전문가들간 전문가 교류 및 민관학 협력도 부처별 층위에 맞추어 다층화되어 시행되었다. 앞으로는 국가안보 이슈들에 대한 통합적 정책결정이 가능하도록 안보실을 중심으로한 정보공유 체계를 굳건히 해야 한다. 동 프레임워크 발표를 통해 부처별 단독행동 및 불협화음 상당수 줄일 수 있을 것이다. 동시에 다층 및 다분야 전문가 교류, 민관학 협력을 장려하며, 민간분야의 자생적 교류 활성화를 체계를 마련해야 할 것이다. 특히 사이버안보 분야 트랙2 활성화를 통해 부처간 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 정보공유 까지도 고려해야 할 것이다. 상호간 정보 강점과 수요를 적절히 조정해야 할 것이며, 특히 정보공개 딜레마에 대해 주의가 필요하다. 국가 간 통합 및 조정된 정보공유 체계 활성화와, 정보 공유의 범위와 대상 등을 구체화가 추가적으로 필요할 것이다.

2. 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 회의시 합의한 "기존 국제법과

20) 오수진, “한미, 사이버분야 첫 동시 대북제재…‘암호화폐 세탁’ 북한인”, 연합뉴스, 2023년 4월 24일

21) 길민권, “국정원, 北의 랜섬웨어 공격에 ‘韓美 합동 사이버 보안 권고문’ 발표”, 데일리시큐, 2023년 2월 10일

22) <https://www.cnas.org/events/virtual-event-us-rk-strategy-for-enhancing-cooperation-on-combating-cyber-enabled-financial-crime>

23) <https://thereadable.co/us-south-korea-experts-call-for-practical-cooperation-to-tackle-north-korean-crypto-theft/>

24) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N23/037/94/PDF/N2303794.pdf?OpenElement>

25) <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>

주권의 온라인공간 적용“ 원칙과 제4차 회의에서 합의한 11개 규범 뿐이다. 제6차 GGE와 병행된 개방형 워킹그룹(OEWG)도 현재 2차 회의를 진행하고 있으나, GGE에서 합의한 결과 외에 추가 결과물은 아직 도출하지 못한 상태이다. 그럼에도 불구하고, OEWG에서 사이버사고 대응을 위한 컨택포인트 설정에 회원국이 합의하고, 이를 구체화하는 활동을 지속하고 있어, 규범의 전세계적 적용을 시작하고 있다는 점과, 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 있다고 볼 수 있다. 특히 한국은 2024-2025년 비상임이사국 기간 동안 한국이 집중하고자 하는 분야에 사이버를 포함시켰고 관련한 활동을 적극적으로 개시하고 있어 상당한 논의의 진전이 예상되는 바이다. 다만, UN 대북제재 패널 운영이 종료됨에 따라, 북한의 애북제재 위반에 대해 어떻게 대응할 것인지에 대해 지속적으로 관심을 가져야 한다.

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, 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 민간업체와 전문가들은 기술적 측면에서 전쟁 수행 방식의 변화를 가져왔으며, 이는 앞으로의 규범형성에 그들의 의견 반영도 고려해야만 하는 상황을 유도하게 되었다.

국제적으로도 민간사업자와 전문가의 의견이 얼마나 반영될 수 있느냐는 점에 대해서는 향후 논란의 여지가 있다. 공개 귀속 및 식별에 대한 GGE 논의시 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, 민간사업자 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 진영간 논리가 참여한 분야보다는 북한 가상자산 탈취 대응과 같은 개별 사안별 협력을 중심으로 대응하는 것이 우리 의견 반영과 역할 구체화를 통한 기여에 긍정적일 것이다. 2022년 한미정상회의 및 이번 프레임워크 발표를 통해, 진영간 규범경쟁에서 미국측에 한층 가까운 입장을 보인 것은 주지의 사실이다. 그럼에도 불구하고 진영간 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 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 사이버분

야 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. 이런 부분이 우리나라가 2022년 발표한 인태전략에 다수 반영되어 있다는 점을 매우 고무적이라고 판단할 수 있다. 특히 동남아 국가 등 북한이 IT 인프라를 악용하고 인력을 파견시키고 있는 국가들 대상의 역량강화 활동에 집중하는 것이 효과적일 것이다.²⁶⁾ 러-우 전쟁 개전 이전 미국이 우크라이나의 전략과 정책 수립, 인력양성 및 역량강화 등에 기여했다는 점은 시사하는 바가 크다. 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.²⁷⁾

이 외에 실질적인 역량강화를 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. 국가간 사이버공간에서 발생한 악의적 행위 혹은 무력공격에 적용가능한 국제법이 성문화되지 않은 상황에서, 개별국가의 사례별 판단에 따른 대응이 가능해짐에 따라 이에 대한 국가별 해석과 적용은 추후 사이버공간에 적용가능한 국제법 개발에 적극적으로 활용될 것으로 예상된다. LS는 기술측면의 공방훈련 외에도 전략훈련, 미디어 대응 등 정책결정 지원을 위한 다양한 분야가 포함되며, 이는 사이버공간의 갈등 대응을 위한 국가간 대응체계 파악 뿐만 아니라 참여 국가들간 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 대응절차 개발에 초점을 맞출 필요가 있다. 재래식 분야에서처럼 훈련, 전술 및 정책, 전략측면 공조가 가능한 통합훈련 등도 필요할 것이다. 이를 통해 한미간 악의적인 행위자에 대한 공통의 책임 부과 기준을 개발하고, 국가차원의 대응체계를 조율해 나갈 수 있을 것이다.

러시아-우크라이나 전쟁 발발으로 기술선진국들에 대한 지원요청과 미국 주도의 전진방어 전략의 적극적 활용이 증가할 것이다. 이번 전쟁 수행 과정에서 미국은 수십차례의 “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 지원 요청이 예상된다. 우리나라는 특히 IT 및 사이버보안 분야 전문가들의 역량이 높아, 이들에 대한 지원이 가시화될 수 있을 것이다. 미국과 캐나다 등은 사이버분야 국가예비군(National Reserve Guard)를 상시적으로 운영하고, 국가위기기 활용하고 있다. 우리나라도 상비군 개념의 전문가집단을 운영 및 관리하고, 이들을 적법하게 활용할 수 있는 법제도적 준비가 필요할 것이다.

3. 사이버기술의 무기화와 대응

26) <https://directionsblog.eu/south-koreas-indo-pacific-strategy-promotes-cyber-cooperation/>

27) 이지선·김소정, “사이버 안보와 개발협력 연계 접근에 관한 연구: 영국과 한국 사례 비교”, 21세기정치학회보 제 33집 1호, 2023년, p.46.

2010년 이란에서 발생한 스텝스넷 공격으로 취약점이 사이버공간에서 전략무기가 될 수 있다는 점이 증명되었다. 이 후 제로데이 취약점은 실제 무기로 블랙마켓을 통해 거래되고 있다. 해커들이 취약점을 통해 막대한 이익을 얻게 되면서 취약점 시장이 중국 등 다른 나라로 확대되고, 여러국가가 제로데이 취약점을 비축하게 되었다. 전 세계적으로 실력을 보유한 해커가 다양한 국가에서 생겨남으로써 국가들은 사이버무기 시장에서 통제권을 상실하고, 안보를 위협하는 결과를 가져오게 되었다. 실제 해킹으로 자동차, TV 등의 제품 뿐만 아니라 군사시설, 드론 등 해킹범위가 확장되고 있으며, 제로데이 취약점을 활용한 국가간 공격행위도 발생하고 있다.

이러한 상황은 규범의 문제에 있어 또 다른 쟁점을 제기한다. 지금까지 전략무기나 이중용도 기술은 바세나르체제에 따라 수출입을 관리 및 통제해 왔다. 하지만, 특정국가에 치명적인 손실을 입힐 수 있는 제로데이 취약점이 개인에 의해 개발, 생산 및 유통되고, 손쉽게 구할 수 있게 되면서 기존 바세나르체제를 통한 수출입규제는 더 이상 적용하기 어렵게 되었다. 이 과정에서 국가들은 취약점을 분석 및 취득하는 주요 기능을 정보기관에 의존하고 있으며, 이는 정보기관이 전통적인 정보수집 방법과 함께 사이버공간에서 취득·모니터링한 결과를 통합함으로써 상대적 우위를 갖게 되는 또 다른 이유가 되고 있다.

국제연합은 국가 및 국가가 후원하는 공격자들, 테러리스트들에 의한 사이버공격 위험에 대해 UN차원에서 대응해야 한다고 판단하고 있으며, 특히 ICT를 활용하거나 ICT에 대한 테러리스트의 활동을 심각하게 다루고 있다. 이 과정에서 사이버안보 침해행위 및 보호활동 양측면에서 정보기관의 역할과 기능이 점점 중요해지고 있다. 공격자들은 정보기관의 정보와 해킹기술력을 산업기밀 절취 등에 실제로 활용하고 있거나, 정부가 재정적·인적 자원을 지원하여 악의적인 행위를 수행한다. 방어자들은 상대편 네트워크에 실제 침투하거나 원격으로 제어된 시스템을 통해 공격활동 모니터링 및 방어, 공격근원지 관리 및 제어 등의 활동을 한다. 이러한 직간접적인 지원 혹은 직접수행된 국가행위에 대한 책임을 묻기 위해서는 공격 원점에 대한 식별이 필수불가결하며, 여기에서 정보기관과 민간전문기업들에의 의존도가 높아지고 있다.

이를 위해 정보기관은 위협 인텔리전스 활동과 사이버보안 활동을 동시에 수행하며, 이 행위들은 국가안보적 목적을 띄게 될 때, 사이버안보 활동이 된다. 우선 기술적으로 사용되는 위협 인텔리전스 활동과 사이버보안 행위에 대한 구분이 필요하다. 일반적으로 얘기되는 위협 인텔리전스는 애플리케이션 및 시스템을 대상으로 하는 위협과 관련된 정보를 수집, 처리, 분석 및 배포하는 지속적인 활동으로 정의된다. 이 정보는 다양한 출처에서 실시간으로 수집되는데, 단일 데이터베이스에 집계되어 보안 전문가에게 악의적인 행위자가 악용하는 취약점 및 활성 위협에 대한 중앙 집중식 정보 소스를 제공한다. 사이버보안은 위협을 모니터링 뿐만 아니라 공격에 대처한다는 점에서 위협 인텔리전스와 구분된다. 사이버보안의 목표는 무단 접근 또는 사이버 공격으로부터 중요한 네트워크, 애플리케이션, 장치 및 데이터를 보호하는 것이다. 사이버보안 조치는 침입 방지를 목표로 새로운 공격보다 앞서려고 시도하며, 가능한 한 빨리 피해를 완화할 목적으로 공격에 대한 대응책을 개발한다.

사이버공간에서의 활동이 갖는 은밀성과 촉박함은 실제 발생한 행위의 세부사항에 대해 공개하기 어렵게 하고 있고, 정보기관이 수행한 실제 행위들이 정보수집 행위인지 사이버공간의 방어 행위인지 구분하기도 어렵다. 더욱이 발생한 행위에 대한 책임을 묻기 위해 필수 전제조건인 공격자 식별이 명확히 이루어졌던 사례도 없다. 설령 피해국 혹은 피해국과 유사입장을 가진 국가들이 특정 국가를 공개지목 할지라도, 가해국으로 지목된 국가가 그 행위를 실제 당사국의 행위로 인정하지 않았다. 2007년 에스토니아, 2010년 이란에 대한 스텝스넷, 2014년 소니해킹 이후 발생한 북한에서의 전산마비, 2018년 동계올림픽 개막식에서 발생한 공격 사례 등이 모두

이에 해당한다.

국제규범을 형성하는데 있어 정보기관이 주도하는 사이버안보는 이러한 이유로 새로운 고려사항을 제시한다. 전통적으로 정보기관의 활동은 명시적 규율대상이 아니었기 때문에, 사이버안보 담당기관의 적극적인 악의적 행위 저지는 규율의 공백 혹은 일종의 회색지대로 인식될 여지가 있다는 지적이 생긴 이유이다. 이 공백을 어떻게 규율할 것인가는 전통적인 정보기관의 활동에 대한 국제관습에 변경을 요구할 수도 있는 사안이기도 하다. 또한 사이버안보 기관이 사전에 공격을 탐지하고 방어하는 행위는 국가안보적 차원에서 중요한 활동이지만, 상대국의 입장에서는 직간접적으로 주권, 영토, 국민에 대한 침해가 발생할 수 있는 소지가 있다. 이는 정보기관이 아니라도 사전적 예방행위를 적극적으로 수행하는 모든 경우에 해당한다. UN GGE에서 협의하고자 했던 “사이버공간에서의 책임있는 행동(responsible behaviour in cyberspace)”을 규범화하는데는 국가별 이해관계가 다르게 적용될 수 밖에 없는 실정이다.

IV. 결론

사이버분야에서의 강대국간 경쟁은 매우 치열해지고 있고, 미국의 정보통신기반서비스 기업에 대한 의존도가 높은 현 상황에서, 한미간 사이버안보 분야 협력을 공고히 할 것을 천명한 것은 중요한 의미를 갖는다. 한편으로는 전략적 규범경쟁 하 우리의 입지가 좁아졌다고 판단할 수 있으나, 우리나라가 기술적 자생력을 갖고, 전략적 자율성을 도모할 수 있도록 핵심분야 공동 연구 개발과 규범 형성에 적극적으로 참가하여, 국제사회 및 동북아 지역에서 우리나라의 입지와 전략적 요충지로서의 중요도를 공고히 하는 기회로 삼아야 할 것이다.

이를 가능하게 하기 위해서는 한미 간 북한의 사이버 역량과 위협 평가 등에 있어 공통의 시각을 갖고, 상호 간 이해에 기반한 협력이 가능한 환경 구축이 필요하다. 이 과정에서 양국간 정보공유는 필수적이다. 최근 개최된 UN의 OEWG 회의에서 전 국가를 대상으로 한 사이버안보 위기 대응을 위한 컨택포인트 디렉토리 설립이 추진되고 있다는 점은 정보공유 강화의 필요성을 전세계가 공감하고 있다고 볼 수 있는 점이다.

현재 정보·외교·국방·법집행·IT 등 부처별 협력체계는 구성 및 운영 측면에서 그 역할을 충분히 잘 수행해 왔다. 민간 전문가들간 전문가 교류 및 민관학 협력도 부처별 층위에 맞추어 다층화되어 시행되었다. 앞으로는 국가안보 이슈들에 대한 통합적 정책결정이 가능하도록 안보실을 중심으로한 정보공유 체계를 굳건히 하고, 부처별 단독행동 및 불협화음 상당수 줄일 수 있을 것이다. 동시에 다층 및 다분야 전문가 교류, 민관학 협력을 장려하며, 민간분야의 자생적 교류 활성화를 체계를 마련해야 할 것이다. 특히 사이버안보 분야 트랙2 활성화를 통해 부처간 직접적 협력이 어렵거나, 사전 공감대 형성이 필요한 분야에 적극적으로 활용할 필요가 있다.

또한, 미국과의 정보공유 강화는 향후 일본을 포함한 한·미·일, 나아가 파이프라이즈(Five Eyes)와의 정보공유도 고려해야 할 것이다. 상호간 정보 강점과 수요를 적절히 조정해야 할 것이며, 특히 정보공개 딜레마에 대해 주의가 필요하다. 국가 간 통합 및 조정된 정보공유 체계 활성화와, 정보 공유의 범위와 대상 등을 구체화가 추가적으로 필요할 것이다.

〈참고문헌〉

- 국가보안기술연구소 옮김, 사이버 전쟁에 적용 가능한 국제법 : 탈린매뉴얼, 글과 생각, 2014
- 길민권, “국정원, 北의 랜섬웨어 공격에 ‘韓美 합동 사이버 보안 권고문’ 발표”, 데일리시큐, 2023년 2월 10일
- 김소정, “오바마 정부의 사이버안보 정책 추진현황과 정책적 함의”, 외교안보연구 제7권 제2호, 2011.12.
- 김소정, “사이버안보 국제협력과 국가전략”, 제주평화연구원 Peace-Net 2013-17, 2013.
- 김소정, “2022 한미정상회담과 사이버안보 : 역지력 강화를 위한 전략적 과제”, 국가안보전략연구원 이슈브리프 제361호, 2022년 5월 31일
- 김소정, “러시아-우크라이나 전쟁과 사이버안보 전략구상의 함의”, 국가안보전략연구원 이슈브리프 358호, 2022
- 김소정, “미국의 사이버공격 대응정책과 한국에의 시사점 - 솔라윈즈 해킹 대응사례를 중심으로”, 국가안보전략연구원 연구보고서 2022-04, 2022.
- 김소정, “2023 미국 사이버안보 전략 주요내용과 한국에의 시사점”, 국가안보전략연구원 이슈브리프 423호, 2023.
- 오수진, “한미, 사이버분야 첫 동시 대북제재…'암호화폐 세탁' 북한인”, 연합뉴스, 2023년 4월 24일
- 이지선 · 김소정, “사이버 안보와 개발협력 연계 접근에 관한 연구: 영국과 한국 사례 비교”, 21세기정치학회보 제33집 1호, 2023년, p.46.
- 장노순 · 김소정, “미국의 사이버전략 선택과 안보전략적 의미”, 정치정보연구, 19권 3호, 2016.
- 조상진, “한국 첫 ‘대북 사이버 독자제재’…개인 4명·기관 7곳 지정”, VOA, 2023년 2월 11일
- Christopher Whyte & Brian Mazanec, Understanding Cyber Warfare: Politics, Policy and Strategy, Routledge, 2019
- CSIS, “The Biden-Harris Administration’s National Cybersecurity Strategy”, Roundtable, 02 March, 2023
- Jenny Jun, “The Promises and Limits of “Defend Forward” in the ROK Context,” GCPR 2022 (서울, 플라자 호텔, 2022년 9월 21일).
- Michael P. Fischerkeller 외, Cyber Persistence Theory : Redefining National Security in Cyberspace, Oxford University Press, 2022.
- Paul M. Nakasone. The U.S. Senate Select Committee on Intelligence. '22. 3. 10. Paul. M. Nakasone. Subcommittee on Intelligence and Special Operations Hearing: “Defense Intelligence Posture to Support the Warfighters and Policy Makers”. '22. 3. 17
- So Jeong KIM, “South Korea’s Indo-Pacific Strategy Promotes Cyber Cooperation”, 2023.05.
- UN General Assembly. “Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security,” 2021.7.14.
- U.S. Department of Defense, Strategy for operating in cyberspace , Washington, DC :

Department of Defense, 2011.
U.S. Department of Defense, Summary of the Department of Defense Cyber Strategy ,
Washington, DC: Department of Defense, September 2018.
U.S. Department of State, PRESS RELEASE, Imposing Sanctions on Virtual Currency
Mixer Tornado Cash, AUGUST 8, 2022
U.S. Department of Defense, 2023 Cyber Strategy of Department of Defense, 2023,

<웹사이트>

<https://www.koreancenter.or.kr>
<https://www.yna.co.kr/view/AKR20231106061900001>
https://www.mofa.go.kr/www/brd/m_25605/view.do?seq=1&page=1
<https://www.cnas.org/events/virtual-event-u-s-rok-strategy-for-enhancing-cooperation-on-combating-cyber-enabled-financial-crime>
<https://thereadable.co/us-south-korea-experts-call-for-practical-cooperation-to-tackle-north-korean-crypto-theft/>
<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N23/037/94/PDF/N2303794.pdf?OpenElement>
<https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>
<https://n.news.naver.com/article/023/0003836147?sid=104>
<https://directionsblog.eu/south-koreas-indo-pacific-strategy-promotes-cyber-cooperation/>

*이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.*