ISSUE BRIEF

이슈브리프 423호
(2023. 3. 8)

2023 미국 사이버안보 전략 주요내용과 한국에의 시사점

제423호

김소정 안보전략연구실

국가안보전략연구원
Institute for National Security Strategy

INSS
www.inss.re.kr

국문초록

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.

앞으로 한미 양국의 사이버안보 분야 협력을 위해 한국은 아래의 사항에 대해 심층적인 고민해야 한다. 우선, 한국은 국가 주요기반시설 보호체계 강화를 위한 정부역할 강화의 의미를 살펴보아야 한다. 국가의 사이버안보 강화를 위한 최종 책임을 정부가 지겠다는 점을 명확히 했다는 점에서 미국의 변화된 접근법을 엿볼 수 있다. 또한 소프트웨어 공급망 안전성 확보와 신기술 발달에 따른 대비책 마련을 적극적으로 준비해야 한다. 특히 양자컴퓨팅의 발달로 국가 암호체계가 흔들릴 수 있다는 점은 미래 준비의 필요성을 여실히 보여준다. 동시에 사이버공격으로 발생하는 피해 대응과 미국의 제재조치 시행에 동참하거나 독자 제재 등을 부과하는 우리의 기준 마련이 필요하다. 마지막으로 미국과의 협력을 위한 구체적 의제 설정이 필요하다. 양국의 지향목표에 기반한 구체적 협력 의제를 도출하기 위한 허심탄회한 의견 나눔의 장이 필요하다. 한미동맹 70주년인 올해 미국의 새로운 사이버안보 전략 수립을 계기로 구체적이고 실질적인 양국간 협력 플랫폼의 구성·운영이 본격적으로 논의되어야 한다.

핵심어: 미국 국가 사이버안보 전략, 주요기반시설보호체계, 공급망, 소프트웨어 안전성, 사이버공간 국제규범

2023년 3월 2일 미국 정부는 국가 사이버안보 전략((National Cybersecurity Strategy)을 공개하고 그 주요내용을 미 국제문제연구소(CSIS)가 개최한 라운드테이블 회의에서 소개했다. 이번에 발표된 국가 사이버안보 전략은 중국, 러시아, 이란 및 북한을 주요 위협으로 적시하면서, 사이버공간의 안전성 확보, 사이버공간에서의 악의적 행위 저지를 위한 정부 역할을 크게 강조하고 있다. 또한 신기술 발달이 국가안보에 미치는 영향에 대한 미래준비 역시 강조하고 있다.

동 전략은 바이든 정부 출범 이후 발표된 다양한 정책문서들과 궤를 같이하고 있다. 2022년 발표한 국가안보 전략(National Security Strategy), 국가 사이버안보 개선을 위한 행정명령 14028, 주요기반시설 통제 시스템 사이버보안 개선을 위한 국가안보 메모랜덤 5, 관리예산처(OMB)의 연방정부기관 대상 제로트러스트 보안 원칙에 관한 메모랜덤 M-22-09, 양자컴퓨팅 발전과 국가 암호체계 개선에 관한 국가안보 메모랜덤 10 등에서 이미 국가차원의 사이버안보 강화, 주요기반시설 및 제어시스템 보안 강화, 양자컴퓨팅 등 신기술 발전에 따른 미래 대비 등이 언급되었다. 동 전략은 바이든 정부가 지속적으로 강조해 온 사이버안보, 신기술 대비, 주요기반시설 보호 역량 강화 등 중점 정책을 전략에 다시 한번 명시함으로써 추진을 위한 정책 의지를 공고히 하고 있다.

미국은 2000년대 이후 다양한 정책문서를 통해 사이버안보의 중요성을 지속적으로 강화해 왔다. 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. 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 갖출 것을 명확히 했다. 또한, 다양한 행정명령(Executive Order)과 대통령 정책 지침(Presidential Policy Directive)을 통해 주요기반시설 사이버안보 활동을 지속적으로 강화시켜 왔다.

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.

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.

이번에 발표된 2023년 국가 사이버안보 전략은 2018년 이후 5년 만이다. 동 전략은 주요 정보통신 기반시설 보호, 공급망 보호, 신기술 발달에 따른 국가안보 강화 방안 및 보안 생태계 구축, 민관 협력 강화 등이 명문화되었다. 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.

이하에서는 본 전략의 주요 내용을 살펴보고, 향후 한국의 사이버 안보 향상을 위한 참고사항을 도출할 것이다. 이 과정에서 한미간 협력에 필요한 요소도 식별해보고자 한다.

2023 전략 주요 내용 및 특징

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

에만 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 사고대응 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 중소규모 기업의 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,[1] 우리나라도 북한의 사이버활동에 대한 단독 대북 제재를 시행한 바 있다.[2]

1) U.S. Department of State, PRESS RELEASE, Imposing Sanctions on Virtual Currency Mixer Tornado Cash, AUGUST 8, 2022
2) 조상진, "한국 첫 '대북 사이버 독자제재'…개인 4명·기관 7곳 지정", VOA, 2023년 2월 11일

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.

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), 오커스(AUKUS), 인도·태평양 경제프레임워크(IPEF) 등 모든 소다

자간 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 규제의 조화를 유도하는데 앞으로 큰 역할을 지속할 것으로 예상된다.[3)]

한국에의 시사점

한미는 2022년 개최된 한미정상회담 공동성명에서 제시했던 많은 분야에 있어 협력을 가시화시키고 있다. 공동성명에는 특히 사이버를 포함한 기술 적용과 국가안보적 함의 분야에서 다양한 협력을 예고하고 있었고, 실제 그 후속 조치들이 지속해서 추진됐다. 한미 사이버사령부는 MOU를 체결하였고, 랜섬웨어 대응 이니셔티브에 한국도 참여하는 등 실무차원의 협력을 시작했으며, 특히 북한 IT 인력의 외화벌이와 가상자산 탈취 대응에 있어 한미간 공조는 괄목한 성과를 거두고 있다.

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. 이는 우리나라가 주요 관심을 두고 있는 분야와 일맥상통한 부분도 있으나, 앞으로 양국간 협력 강화를 위해 대내적으로 긴급히 정책방향 마련이 필요한 분야도 있다. 미국의

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

새로운 사이버 안보 전략 추진이 한국에 주는 시사점은 아래와 같다.

첫째, 미국이 강조하는 정부주도의 국가주요기반시설 보호체계 강화는, 기존 한국의 기반 보호 체계와 궤를 같이하는 부분이다. 정부 역할 시행과 운영 등에 우리나라의 경험을 공유하고, 이들의 논리를 우리 상황에 활용할 수 있는지 면밀한 판단이 필요하다. 비록 주요기반시설의 소유나 운영 주체가 민간이라 할지라도, 미국도 국가안보적 중요성을 갖는 부분에 대해 정부의 영향력과 지휘력을 행사하는 것이 결국 국익에 득이 된다는 결론을 내린 것으로 보여진다. 우리나라도 실무상 어려움이나 불편함으로 인해 기반보호시설 지정을 회피하거나 유보하는 경우가 많은 상황에서, 민관과 정부의 역할과 기능을 유기적으로 조율하는데 미국의 정책 추진 방향을 참고할 수 있을 것이다.

둘째, 소프트웨어 공급망 안전성 확보 노력을 주의 깊게 살펴보아야 한다. 현시대를 구성하는 인프라와 제품 대부분은 소프트웨어에 의존하고 있는데, 이 소프트웨어가 안전하게 만들어지고 이를 공급망 상의 전 과정에서 보장할 수 없다면, 실생활의 많은 부분에 위험요소가 내재되어 있는 것과 같다. 또한 미국에서 정부차원의 획득과정에 소프트웨어 안전성을 강제하면, 한국에서 생산 및 수출하는 제품에 대한 도입 제한 등이 추가적으로 발생할 수 있다. 또한 상호 호환 가능한 소프트웨어 사용을 위해 한국내 시스템에 이들 소프트웨어 안전성과 관련된 규격 반영을 강제해야 할 경우도 발생할 수 있다. 한국에서는 공급망 이슈가 특히 반도체를 중심으로 논의되고 있지만, 사회기반을 구성하는 정보통신기술과 제품, 시스템의 근간을 구성하는 소프트웨어의 공급망 안정성 확보는 사이버보안 뿐만 아니라 국가안보의 근간이라는 점을 인식해야 한다.

셋째, 신기술 발달에 따른 대비책 마련을 선도적으로 추진해야 한다. 양자컴퓨팅 및 AI 등 신기술 발달에 따른 국가안보 위해요소 식별과 대응방안 마련, 민간 주도의 기술경쟁 우위 확보, 정보통신기술의 현대화는 더 이상 미룰 수 없는 일이다. 양자컴퓨팅 기술의 발달은 기존의 국가암호체계와 보안생태계를 송두리째 뒤흔들 수 있다.

넷째, 사이버공격으로 발생하는 피해 대응과 공격자 처벌에 적극적인 접근이 필요하다. 북한의 가상자산 탈취 대응에 있어 이미 한미는 공조한 바가 있으며, 북한인 및 교육시설, 해킹그룹과 암호화폐 지갑주소 등에 대한 한국의 독자 제재도 미국 등 우방국들과 결을 같이해 이미 시행해 오고 있다. 또한, 2015년 UN 사이버안보 정부 전문가 그룹 회의(GGE)에서 합의한 11개 규범은 보편적으로 적용 가능한 국제규범으로 자리잡아 가고 있다. 이런 상황을 감안할 때, 미국이 법 혹은 행정명령을 근거로 시행한 다양한 제재조치들은 앞으로도 지속될 것이다. 미국은 2023년 사이버안보전략을 통해 사이버공간에서 발생하는 악의적 행위에는 책임과 대가가 따른다는 것을 다시 한번 명확히 하고 있다. 따라서, 동맹인 한국은 책임 부과, 대가 지불의 방식 결정 및 이행에 동참을 요구받을 것이다. 최근 북한의 가상자산 탈취에 대응하기 위해 우리나라도 제재 조치를 시행한 바 있어, 향후 대응 행위 시행 여부 및 정도의 판단을 위한 구체적인 기준 마련에 양국간 협의가 필요할 것이다. 이에 앞서 우리나라의 자체적인 시행 판단기준과 근거를 마련해야 할 것이다.

다섯째, 미국과의 협력을 위한 차기 의제 설정이 필요하다. 미국 국가 사이버안보 전략 전반에서 핵심기술의 연구개발, 표준화 활동 강화, 인증 및 검증 체계 개선, 시스템 간 상호운용성 확보, NATO의 사이버역량 강화 활동 지원, 저개발국 및 개발도상국 대상 역량 강화 지원, 전문인력 양성 및 교육·훈련 강화 등의 중요

성을 여러 번 언급하고 있다. 특히 양자컴퓨팅으로 인한 국가 암호체계에 대한 전반적인 재고려는 한시가 급한 이슈이다. 각 분야별 양국간 기술 및 필요성, 목표와 기대치는 공식 문서로만 파악하기는 어렵다. 아이러니하게도 한미 양국간에는 아직 정례화된 사이버안보 분야 1.5트랙 및 트랙2 회의체가 없다. 한미 동맹 70주년인 올해 미국의 새로운 사이버안보 전략 수립을 계기로 구체적이고 실질적인 양국간 협력을 위한 플랫폼을 구성·운영할 필요가 있다.

//끝//