https://doi.org/10.33778/kcsa.2023.23.2.011

미국 사이버안보 전략의 경향 분석과 한국에의 함의

배 선 하*, 송 민 경**, 김 동 희***

요 약

미국은 바이든 정부 취임 후 대규모 사이버 공격이 잇따라 발생하고, 사이버안보를 국가 최우선과제로 강조하고 있으며, 미국뿐만 아니라 동맹 및 우방국의 사이버안보 강화를 위한 노력을 추진하고 있다. 특히, 2023년 3월에는 국가 사이버안보 전략을 발표하였는데, 연방정부 및 주요기반시설 보호, 국제협력을 통한 사이버공간의 악의적 행위자 및 위협국에 대한 추적 및 대가부과, 민간의 사이버보안 책임 강화 등을 골자로 하고 있다. 국가 사이버안보 전략은 사이버안보의 최상위 지침으로 공공-민간뿐만 아니라 국외 정책 방향도 포함하고 있어 국제질서에까지 영향을 미칠 것으로 예상된다. 한편, 우리나라는 2022년 새로운 정부가 출범하고, 2019년에 발간된 국가사이버안보 전략의 개정이 필요한 상황이다. 또한, 최근 한-미 협력이 강화되고 있으며, 사이버안보는 한미 정상회담에서 핵심의제로 다뤄지고 있다. 이에 본 논문에서는 바이든 정부의 사이버안보전략을 살펴보고, 기존의 트럼프 정부와 어떻게 달라졌는지 그 특징과 시사점을 정성적·정량적 측면에서 분석하고자 한다. 정량적 분석을 위해서는 텍스트 마이닝 기법 중 하나인 토픽모델링을 활용한다. 그리고 이러한 변화가 한-미 관계를 비롯해 우리나라에 미치는 영향과 한국 사이버안보 정책에 주는 함의를 도출한다.

A Trend Analysis of in the U.S. Cybersecurity Strategy and Implications for Korea

Sunha Bae*, Minkyung Song**, Dong Hee Kim***

ABSTRACT

Since President Biden's inauguration, significant cyberattacks have occurred several times in the United States, and cybersecurity was emphasized as a national priority. The U.S. is advancing efforts to strengthen the cybersecurity both domestically and internationally, including with allies. In particular, the Biden administration announced the National Cybersecurity Strategy in March 2023. The National Cybersecurity Strategy is the top guideline of cybersecurity and is the foundation of other cybersecurity policies. And it includes public-privates as well as international policy directions, so it is expected to affect the international order. Meanwhile, In Korea, a new administration was launched in 2022, and the revision of the National Cybersecurity Strategy is necessary. In addition, cooperation between Korea and the U.S. has recently been strengthened, and cybersecurity is being treated as a key agenda in the cooperative relationship. In this paper, we examine the cyber security strategies of the Trump and Biden administration, and analyze how the strategies have changed, their characteristics and implications in qualitative and quantitative terms. And we derive the implications of these changes for Korea's cybersecurity policy.

Key words : cybersecurity, strategy, U.S., Biden, Trump

접수일(2023년 05월 19일), 수정일(1차: 2023년 05월 25일), (2차: 2023년 06월 05일), 게재확정일(2023년 06월 22일)

* 국가보안기술연구소 안보정책연구실(주저자)
** 국가보안기술연구소 안보정책연구실(공동저자)
*** 국가보안기술연구소 안보정책연구실(교신저자)

1. 서 론

2023년 3월, 미국 바이든 정부는 새로운 사이버안보 정책 방향을 제시한 국가 사이버안보 전략(national cybersecurity strategy)을 발표하였다. 이번에 발표된 전략은 2018년 트럼프 정부의 국가 사이버 전략(national cyber strategy) 이후 처음으로 개정된 전략으로 바이든 대통령 취임 당시 발생하였던 솔라윈즈(SolarWinds), 콜로니얼 파이프라인(Colonial Pipeline) 해킹사고와 점차 심화되고 있는 미-중 기술 패권 경쟁 등 다양한 사이버안보 환경변화에 따른 새로운 정책 방향을 담고 있다.

사이버안보 전략은 국가의 사이버안보 관련 국가의 최상위 지침으로서 파급력이 크고, 공공-민간뿐만 아니라 개인까지 관련한 이해당사자의 범위가 넓으며 장기적인 방향을 제시한다. 또한, 사이버공간이 작전공간, 제5의 영토로 인식되고 있는 상황에 사이버공간을 주도하는 미국의 사이버안보 전략은 대외적으로 국제질서에까지 영향을 미칠 것으로 예상된다. 이에 해당 전략의 목표와 주요한 변화를 면밀히 분석하여 우리 정부의 대응 방향을 마련할 수 있도록 해야 할 것이다. 특히, 한국은 새로운 정부 출범 이후 2019년에 발표한 국가 사이버안보 전략의 개정을 앞두고 있기에, 이번 미국 전략은 한국의 사이버안보 정책 방향에 중요한 참고자료가 될 수 있을 것이다.

더 나아가 새 정부는 한-미 동맹의 중요성을 그 어느 때보다 강조하고 있다. 지난 2022년 5월 한-미 정상회담에서는 '사이버안보'라는 키워드가 수차례 언급되었으며, 2023년 4월 한-미 정상회담에서는 '전략적 사이버안보 협력 프레임워크'를 채택하는 등 사이버안보 관련한 양국 간 협력은 앞으로 더욱 강화될 것으로 예상된다. 이에 향후 한-미 협력의제 구체화 및 실익 있는 협력방안 마련을 위해서는 미국의 사이버안보 전략 및 정책에 대한 이해가 필수적이다.

이에 따라 본 논문에서는 트럼프 정부와 바이든 정부를 중심으로 미국의 사이버안보 전략의 경향을 분석하고자 한다. 먼저 미국 전략에 대한 이해를 위해 미국의 최근 주요 사이버 공격 동향을 살펴보고, 전략과 상호연계를 맺고 있는 사이버안보 정책 동향을 검토한다. 그리고 바이든 정부 전략을 트럼프 정부 전략과 비교하여 특징과 시사점을 정성적·정략적 측면에서 분석한다. 이를 바탕으로, 미국의 전략 변화가 한-미 관계를 비롯한 우리나라에 미치는 영향을 분석하고, 한국 사이버안보 정책에 주는 함의를 도출한다.

2. 미국 주요 사이버 공격과 정책 동향

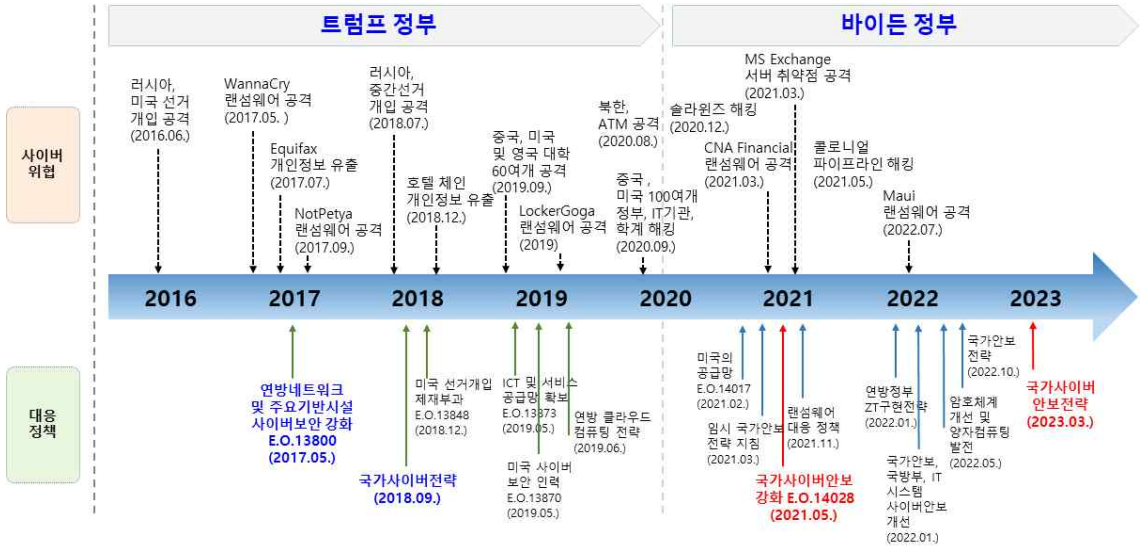
2.1 주요 사이버 공격 동향

트럼프 정부는 취임 전인 2016년부터 러시아로부터 선거 개입 공격을 받아왔다. 2016년 7월에는 민주당(DNC, Democratic National Committee) 서버가 해킹당하고 20,000개의 이메일과 8,000개의 파일이 위키리크스(WikiLeaks)에 유출되었다. 이후에도 해킹조직은 같은 해 8월에 민주당 관련 비밀문서를 공개하고 소셜미디어를 이용해 지속적으로 허위사실을 유포하는 등 트럼프 당선에 영향력을 행사했다[1]. 이에 오바마 정부는 미-러 핫라인을 통해 푸틴에게 대선 해킹을 경고하고, 2016년 12월에는 美 대선개입에 대한 보복으로 러시아 외교관 35명을 추방하고, 러시아 시설 2개를 폐쇄하였다[2].

또한, 2017년에는 워너크라이(WannaCry)와 낫페트야(Notpetya) 등 대규모 랜섬웨어 공격이 발생했다. 워너크라이는 국내에도 널리 알려진 랜섬웨어 도구로 미국을 비롯한 러시아, 유럽, 인도 등 전 세계 150여 개국에서 병원, 학교, 기업, 가정 등 무차별적으로 확산되어 PC 30만대를 감염시켰으며, 북한의 소행으로 추정되었다[3]. 트럼프 정부는 국토안보부(DHS, Department of Homeland Security)를 중심으로 영국, 일본 등 피해국가와 파트너십을 체결하고 공동 대응에 나섰다. 북한으로 공개귀속하고, 악의적인 국가 배후 해킹조직의 범죄를 좌시하지 않고 책임을 물을 것이라고 밝혔다[4].

2017년 7월에는 미국 신용기관인 Equifax에서 1억 5만 명에 달하는 대규모 개인정보 유출 사고가 발생하였으며, 미국 외에도 영국, 캐나다 시민의 개인정보도 유출되었다[5]. 2020년 2월 법무부는 Equifax 해킹 혐의로 중국 인민해방군의 군인 4명을 기소했다[6].

그러나 이러한 노력에도 불구하고 중국으로부터 지재권 탈취 공격이나 러시아의 가짜뉴스 및 허위정보 유포, 선거 개입 등 민주주의 훼손 공격이 지속적으로



(그림 1) 미국의 주요 사이버 공격 및 정책 발표 동향

출처: 美 외교협회(CFR, Council on Foreign Relations), Cyber Operation Tracker 자료 참고 및 재구성

발생했다. 2018년 미국 중간선거에서 2016년에 민주당을 해킹했던 러시아 해킹그룹이 민주당 및 공화당의 선거 활동에 개입하기 위한 공격이 발생했다[7]. 또한, 2019년에는 중국 해킹그룹이 미국의 27개의 대학을 표적으로 하고 군사용 해양 기술을 탈취를 시도하였으며[8], 미국과의 무역협상에서 우위를 점하기 위해 제조업 협회를 침입하는 공격이 발생했다[9].

바이든 정부의 경우, 대통령 당선 직후부터 대규모 사이버 공격이 발생했다. 2020년 11월에는 미국 정부와 기업에서 광범위하게 사용되고 있는 솔라윈즈의 소프트웨어가 러시아 배후로 추정되는 해킹조직으로부터 공격을 받고, 연방정부 및 기업 등 전 세계 약 18,000여 개의 조직이 영향을 받은 것으로 드러났다[10]. 2021년 4월에는 NSA, 사이버보안청(CISA, Cybersecurity and Infrastructure Security Agency), 연방수사국(FBI, Federal Bureau of Investigation)이 공동으로 러시아 외교정보국(Russian Foreign Intelligence)을 위협 행위자로 발표했다[11].

그러나 이후 2021년 3월 미국 금융회사인 CNA Financial에 랜섬웨어 공격이 발생하고, 역대 최대 금액인 4천만 달러가 지급되었다[12]. 또한, Microsoft Exchange Server의 제로데이 취약점을 악용한 공격이 발생하였으며, 미국을 비롯한 영국, 독일 등 유럽 국가에서도 피해가 발생했다. Microsoft는 중국의 국가 배후 해킹조직을 범인으로 지목했으며, 이후 미국 정부는 영국, EU, NATO 등 우방국과 함께 중국의 악의적 행위를 공동 비난하였다[13].

2021년 5월에는 미국 최대 송유관업체인 콜로니얼 파이프라인에 랜섬웨어 공격이 발생하고 가스공급이 중단되는 사고가 발생했다. 당시 콜로니얼 파이프라인은 500만 달러의 랜섬을 지급해서 랜섬의 규모는 CNA Financial 사고보다 적으나 랜섬웨어가 주요기반시설을 공격했다는 사실이 미국을 충격에 빠트리고 바이든 정부는 이 사고를 유례없는 일로 규정하고 국가 비상사태를 선포한 바 있다[14].

2.2 트럼프 정부의 사이버안보 정책 동향

트럼프 정부의 사이버안보 정책 방향은 국가안보전략을 통해 국가 전체적인 안보 비전 및 방향을 검토하고, 연방정부·주요기반시설 사이버보안 강화, 사이버 억지 및 대가부과, 공급망 보안 강화, 측면에서 바라보고자 한다. 그리고 트럼프 정부에서 강조한 선거 보안 강화를 살펴본다.

2.2.1 국가안보전략 방향

2017년 12월에 발표된 국가안보전략은 1) 미국 국민, 영토, 생활방식의 보호, 2) 미국의 번영 촉진, 3) 힘을 통한 평화 유지, 4) 미국의 영향력 증진이라는 4가지 방향을 세우고, 전략과제를 수립하였다[15].

미국은 안보전략을 통해 디지털 네트워크를 추적하고, 민관과 협력하여 사이버 테러리스트 및 범죄자의 은신처를 제거하고, 사이버 시대에 안전한 미국을 위해 연방정부 IT 현대화 및 보안 강화를 추진하며, 설계 시 보안을 고려하도록 권고하였다. 무엇보다도 보안을 갖춘 사이버 인프라가 경제성장을 촉진하며, 자유와 안보를 보장한다는 것을 강조하였다.

2.2.2 연방정부·주요기반시설 사이버보안 강화

트럼프 정부는 2017년 5월 연방 네트워크 및 주요기반시설 사이버보안 강화를 위한 행정명령(EO, Executive Order) 13800을 발표했다[16]. 행정명령 13800은 미국 전체의 사이버안보 역량 및 실태를 전면적으로 평가하고, 이에 따른 체계 구축이라는 트럼프 정부의 공약을 반영한 것으로, 연방 네트워크 사이버보안 강화, 주요기반시설 사이버보안 강화, 국가 사이버안보 역량 강화 3가지 분야에서 방향을 제시했다.

연방 네트워크 사이버보안 강화를 위해서는 연방기관 전체의 일원적 위험관리 체계를 수립하고, 국립표준연구원(NIST, National Institute Standards and Technology)의 사이버보안 프레임워크를 연방기관에 적용 의무화하였으며, 노후 IT 설비를 점진적으로 개선하고 클라우드 등 공유서비스를 도입한다. 주요기반시설 사이버보안 강화를 위해서는 주요기반시설 운영자의 보안 활동을 연방정부가 지원하고, 민관협력 증진 절차를 수립하며, 전력 분야에서 사고대응 역량을 평가한다. 그리고 방위산업 분야에서 위험경감을 위한 조치를 취했다[17].

또한, 인력양성체계 발전 계획 수립을 위한 실태평가에서 사이버보안 인력수요 불균형 문제 해소 조치가 권고되어 국가 사이버안보 인력 행정명령 13870을 발표했다. 트럼프 정부는 행정명령 13870을 통해 연방 사이버보안 인력의 수준 격차 완화를 위한 인력순환체계와 성과에 대한 보상체계를 마련하고, 사이버보안 기관 간 연계 및 통합을 촉진하였다[18].

2.2.3 사이버 억지 및 대가부과

트럼프 정부는 적들은 핵무기에 의존하지 않고, 사이버 무기의 사용, 무력공격 임계치 이하의 전략적 공격을 통해 미국의 경제 및 국방에 해를 끼치고 있으며 전쟁의 방식이 변화하고 있다고 언급하고, 이로 인해 억지 전략 확대와 가능한 모든 전략적 공격에 대한 대응 필요성을 강조하였다[15]. 그리고 억지력 확보를 위한 전략적 선택지를 개발하고, 정보공유, 수사·대응 공조를 포함한 국제협력 전략을 수립할 계획이다[16]. 또한, 대가부과를 위해 군사력을 포함한 “모든 도구(toolkit)”를 활용하겠다는 의지를 밝혔다[19].

사이버사령부를 통합 전투 사령부로 격상하고, 국방수권법을 개정하여 군사 사이버 작전에서 국방부 권한을 명확히 했으며, 국방부 사이버 전략에서 선제대응(defend forward) 원칙을 내세웠다[20]. 선제대응은 적의 행위를 방해 및 중단하기 위한 방어 활동을 말하며, 무력충돌 임계치 이하 활동에서도 군의 선제대응을 가능하게 하는 등 적극적 대응 기조를 보였다.

이에 일환으로 2018년 중간선거 기간에 허위정보를 유포하는 러시아 단체 IRA의 인터넷 접근을 차단하고, 2019년에는 이란이 미국 드론을 격추한 데에 대한 보복으로 이란의 미사일 통제 시스템과 네트워크를 공격하여 무력화시키는 등 사이버사령부의 공세적 작전을 승인하고 성과를 거둔 것으로 나타났다[21].

2.2.4 공급망 보안 강화

IT 공급망을 이용한 악의적 사이버 활동이 국가안보 위협이라는 인식이 확대되고 미-중 간 5G 등 기술패권 경쟁이 심화되면서, 화웨이 등 중국 기업 견제를 목적으로 트럼프 정부는 2019년 5월 정보통신 기술, 제품/서비스 공급망에 대한 외국 적대세력의 개입 시도 증가를 국가안보상 위중한 상황으로 선포하고, 공급망 확보를 위한 행정명령 13873을 발표했다[22].

행정명령 13873은 외국의 적대세력과 관련된 IT 분야 거래를 전면 금지하였으며, 재무부 주관으로 IT 제품 및 서비스의 위험산정을 기술적인 평가 외에 적대적 국가와의 연계성을 기준으로 위험을 산정하였으며, 대상단체를 지정할 수 있도록 하였다. 이는 화웨이를 목표로 한 것으로 보인다[23].

2.2.5 선거보안 강화

오바마 정부는 2016년 12월 러시아의 대선 개입 대응 근거마련을 위해 중대한 악의적 사이버 활동과 관련된 국가 비상사태 해결을 위한 추가조치인 행정명령 13757을 발표하고, 제재 대상 행위에 선거 과정이나 기관을 침해하거나 위해를 가할 목적으로 정보를 부적절하게 변경하는 행위를 추가하고 이를 기반으로 러시아 기관과 해커를 기소한 바 있다[24].

그러나 이후에도 지속적으로 민주주의를 위협하는 선거 개입 공격이 발생하고, 트럼프 정부도 러시아의 지속적인 선거 개입 공격에 대한 우려 표명과 함께 선거에 개입하는 외국인에 대해 제재를 부과하는 행정명령 13848을 발표했다. 행정명령 13848은 선거에 대한 외부 간섭을 광범위하게 정의하고, 공격적인 제재 가능성을 시사했다[25].

2.3 바이든 정부의 사이버안보 정책 동향

바이든 정부의 사이버안보 정책 방향은 트럼프 정부와 동일하게 국가안보전략 방향, 연방정부·주요기반시설 사이버보안 강화, 사이버 억지 및 대가부과, 공급망 보안 강화 측면에서 살펴보고, 바이든 정부에서 강조하고 있는 랜섬웨어 보안 강화 정책을 알아본다.

2.3.1 국가안보전략 방향

2022년 10월에 발표된 국가안보전략은 러시아와 중국을 주요 위협국가로 명시하고, 이란과 북한의 위협도 언급하였다. 특히, 중국을 국제질서를 재편하려는 의도와 목적이 있고 경제적, 외교적, 군사적, 기술적 역량을 갖춘 미국의 유일한 경쟁자로 평가하고, 중국에 대한 대응전략을 제시하였다[26].

안보전략 전체에서 사이버안보를 강조하고, 통합억지 전략에서 사이버를 군사영역의 하나로 포함하는 등 사이버를 안보영역으로 바라보고 있으며, 영역 간 통합을 위해 사이버 활용이 증대될 것으로 예상된다. 또한, 사이버안보 관련 국내 투자 증대를 통한 경쟁력 및 국제협력 강화, 공세적 대응을 강조했다.

2.3.2 연방정부·주요기반시설 사이버보안 강화

바이든 정부는 먼저 연방정부 사이버안보를 강화하고, 모범사례를 제시하여 점차 국가 전반의 사이버안보를 강화하고자 했다. 이를 위해 국가 사이버안보 강화 행정명령 14028을 발표하였으며[27], 행정명령 14028은 연방정부 사이버보안 현대화, SW 공급망 보안 강화, 침해 사고보고 및 대응 개선, 사이버안보 조직 강화를 주요 골자로 한다.

먼저, 연방정부 사이버보안 현대화를 위해서는 연방정부 전체에 제로 트러스트 구조 적용을 의무화하고, 클라우드 기술 도입 및 활용 계획 업데이트, 클라우드 서비스 보안을 가속화 했다.

침해사고 보고 및 대응 개선을 위해서는 침해사고 대응지침 표준화, 연방정부 엔드포인트 탐지 및 대응 역량 강화, 사이버범죄 수사 및 회복 역량 강화를 추진한다[28]. 이에 일환으로 2022년 3월에는 주요기반시설 침해사고 보고법(CIRCIA, Cyber Incident Reporting for Critical Infrastructure Act)을 제정하고, 사이버 사고보고를 의무화하였다.

그리고 사이버안보 조직 강화를 위해서는 당선 초기 국가안전보장이사회(NSC, National Security Council)에 사이버안보국장 및 사이버안보실(ONCD, Office of National Cyber Director)을 신설하고, 2022년 4월에는 국무부 산하에 사이버 외교에 초점을 둔 사이버공간 및 디지털정책국(CDP, Bureau of Cyberspace and Digital Policy)을 설립하였다[29]. 또한, 연방기관 정보시스템/非연방시스템, 위협 활동, 취약점, 위협완화 활동, 기관의 대응 활동 등에 영향을 미치는 중대한 사이버 사고(significant cyber incident)를 검토 및 평가하기 위한 사이버안전심의위원회(CSRB, Cyber Safety Review Board)를 설립하였다.

2.3.3 사이버 억지 및 대가부과

바이든 정부는 트럼프 정부의 방향을 이어받아 사이버 공격에 모든 역량을 활용하여 적에게 대응하고, 대가를 부과한다는 방침이다. 2021년 4월에는 솔라윈즈 사고에 대한 대응으로 러시아의 악의적인 국외 활동과 관련된 재산을 차단하는 행정명령 14024를 발표했다[30]. 그리고 러시아의 악의적 사이버 행위에 지

속적으로 책임을 물을 것(hold accountable)이라 밝혔다. 또한, 같은 날 영국이 솔라윈즈 공격을 러시아로 공개귀속하는 등 공동 대응을 추진하고 있다[31].

2021년 6월에는 콜로니얼 파이프라인 해킹 조직인 다크사이드를 추적해 랜섬의 상당량를 회수하고[32], 2022년 6월에는 FBI가 랜섬웨어 조직인 하이브(Hive)에 침투해 시스템을 파괴하고 복호화 키를 탈취하여 약 1억 3천만 달러의 금전 피해를 막아냈다[33].

이외에도 2022년에는 북한 라자루스 그룹의 가상화폐 자금세탁을 지원한 가상화폐 믹서 도구인 tornado mixer를 제재 대상으로 지정하였으며[34], 북한 IT 인력 활동 제재[35], 2021년 11월에는 이란 악의적인 사이버 활동가에 제재를 부과했다[36].

2.3.4 공급망 보안 강화

바이든 정부는 행정명령 14028을 통해 공급망 보안 강조하고 이후 국제사회에서 공급망 리더십 확보, 국외 위협대응을 위해 연구개발을 추진한다[28].

먼저, 소프트웨어 보안 강화를 위해서는 정부 기관에 ICT 제품 조달 시 소프트웨어 자재명세서(SBOM, Software Bill of Materials) 제공을 의무화하고, 핵심 소프트웨어를 식별·관리하도록 하였다.

공급망 위험관리 가이드를 개정하고, NIST가 안전한 소프트웨어 개발 체계(SSDF, Secure Software Development Framework)를 제시하고 연방기관이 활용하도록 하였다[37].

또한, 사이버보안 계약 요구사항 표준화 및 사고보고 의무화를 위해 소프트웨어 보안연방조달규정(FAR, Federal Acquisition Regulatory) 위원회에서 사이버보안 계약 요구사항 표준화 규칙을 제정하고, 국가안보기관과 계약 시 FAR에 제정된 사이버 사고보고 및 표준계약조항을 적용하도록 했다[38].

2.3.5 랜섬웨어 보안 강화

콜로니얼 파이프라인 사고 이후 미국은 랜섬웨어 대응정책을 발표하고, 랜섬웨어 대응 활동은 회복력 강화, 랜섬웨어 교란, 불법 자금조달 대응, 외교력 활용 4가지 방향으로 추진한다[39].

정책은 랜섬웨어 공격에 대한 효과적 대응과 복구를 위해 사이버보안 개선하는 것으로, CIRCIA를 통해 랜섬 지불 신고를 의무화하고, 랜섬웨어 교란을 위해 공격 행위자 및 조력자에 대한 수사·집행을 개선하고, 제재를 활용할 방침이다. 또한, 랜섬으로 지불된 자금의 세탁을 막고, 랜섬웨어 공격을 수익성 있게 하는 금융 생태계를 방지한다. 그리고 랜섬웨어 대응을 위한 국제협력 협의체(CRI, Counter Ransom Initiative)를 설립하였으며, 국제협력을 기반으로 수사·기소하고, 피난처 제거를 추진한다[40].

2.4. 사이버안보 정책 동향 비교

트럼프 정부는 전반적으로 오바마 정부의 사이버안보 정책과 방향을 같이 하며, 악의적 사이버 행위자에 선제대응 및 대가부과를 통해 억지력을 확보하고자 했다. 연방정부 및 주요기반시설 사이버보안 강화를 위해 DHS를 중심으로 한 중앙집중형 관리·감독, 주요기반시설 운영자의 자발적인 협력을 강조했고, 선거보안을 강화한 것이 특징이다.

‘미국 우선주의’로 미국의 경제발전과 리더십 강화에 초점을 맞춰 사이버안보 정책을 추진하였으며, 이는 공급망 보안 강화 정책에서 잘 드러난다. ‘외국 적대세력’의 제품 및 서비스로 인한 안보위협을 강조하고, 제품 및 서비스의 위험성 평가 시 공급업체 및 국가를 고려하도록 했다. 또한, 중국에 추가 관세를 부과하며 화웨이 퇴출 전략을 추진하고, 우방국에도 다소 강압적으로 화웨이 퇴출 전략 참여를 요구하면서 5G 및 차세대 통신 체계에서 미국의 기술패권을 유지하고[41], 국제사회에서 리더십을 확보하고자 했다.

바이든 정부는 트럼프 정부의 사이버안보 정책을 성과 측면에서 부정적으로 평가하고, “트럼프 대통령과는 다른 방식으로 러시아의 선거방해, 사이버 공격에 대응하고, 중국의 경제안보 위협에 대해 맞설 것이다”라고 언급했다[42]. 또한, 미국의 대표적인 씽크탱크인 전략국제연구센터(CSIS, Center for Strategic International Studies)의 수석 제임스 루이스(Jame Lewis)를 비롯한 여러 사이버안보 전문가로부터 억지전략의 실패와 보다 공세적이며, 강압적인(coercive) 사이버 전략의 필요성에 대한 견해가 있었다[43].

이에 선언적인 사이버 억지력 확보 정책보다는 실질적인 공세적 대응 활동을 통해 미국의 대응 의지를

표명하고, 역량을 과시하고 있다. 사이버안보를 위한 다양한 협력의 중요성을 강조하고, 국가 간 협력, 부처 간 협력, 민관협력을 통해 악의적 사이버 행위자를 추적하고 귀속, 기소, 제재를 수행하며, 신속히 피해를 복구해 공격 효과를 절감시키고자 한다.

연방정부 및 주요기반시설의 사이버보안 강화를 위해서는 제로 트러스트를 도입하고 보안 패러다임을 변화하고자 하며, 소프트웨어 공급망 강화를 추진한다. 그리고 주요기반시설의 사고보고를 의무화하는 등 자발적 참여와 규제 간의 조화를 통해 사이버보안을 강화한다. 또한, 실질적인 경제적 피해를 유발하는 랜섬웨어 보안 강화를 위한 정책을 마련하고, 관련 기관 신설, 부처 및 기관의 역할 정립, 국가 간 협력체계를 구축하는 등 적극적인 대응 활동을 수행하고 있다.

3. 미국의 사이버안보전략 주요내용

3.1 트럼프 정부의 국가 사이버전략

3.1.1 비전 및 접근방식

트럼프 정부는 국가 사이버 전략을 통해 번영하는 사이버 미래를 미국이 계속 주도해 나갈 것이라는 비전을 드러냈다. 그리고 국가안보 목표를 위해 사이버 역량을 사용하고, 사이버공간 전반에서 미국의 국가이익을 증진하고 이를 위한 기술 발전을 추진한다.

전략은 국가안전보장이사회(NSC, National Security Council)를 주도로 추진하되, 자원계획을 위해 예산관리국(OMB, Office of Management and Budget)과의 협력을 강조했다.

3.1.2 전략과제

전략은 트럼프 정부에서 발표한 사이버안보 관련 정책을 포함하며, 안보전략과 같이 4가지 전략과제 방향을 세우고, 하위에 세부과제를 두고 있다.

3.1.2.1 미국의 국민, 영토, 생활방식의 보호

전략과제 1에서는 정부가 국가 정보와 정보시스템의 보안, 회복력 증진을 위한 사이버보안 위험관리를 강화해 나갈 것을 명시하였다. 모든 연방정부가 연방 네트워크를 보호할 수 있도록 권한, 의무, 책임을 명확하게 정의하고자 한다. 또한, 연방정부의 권한을 집중화하여 연방 공급망관리 및 정부 계약시스템 보안 강화를 위한 과제들을 제시하였다. 이외에도 주요기반시설 보호를 위한 대응 활동 우선 순위화와 기반시설에 대한 악의적 사이버 행위자 및 조력자에게 상응하는 비용부과와 억지력 확보 내용을 포함한다.

마지막으로 사이버범죄 대응 및 침해사고 보고절차 개선을 위해서는 법적 권한과 자원 지원을 통해 악의적 사이버 행위자를 체포·기소하고, 범죄 인프라를 무력화하며, 민감한 증거를 사법당국이 원활하게 수집할 수 있도록 민간부문과 함께 기술을 개발할 계획이다.

3.1.2.2 미국의 번영 촉진

전략과제 2는 경제성장과 혁신, 효율성을 위한 동력으로써 기술 생태계와 사이버공간의 발전에 대한 미국의 영향력 유지가 목표이다. 그리고 기술시장 및 혁신 강화, 경제안보를 위한 표준수립을 촉진하도록 하는 등 활기차고 회복력 있는 디지털 경제를 조성하는 내용을 담고 있다.

또한, 미국이 보유한 독창성을 보호하고 사이버공간 상에서 전략적 우위를 점할 수 있도록 신기술 분야에서의 리더십 강화 및 관련 연구개발을 촉진하고, 악의적 M&A와 지적 재산권 탈취에 맞서도록 하고 있다. 사이버보안 인재 양성 계획도 포함한다.

3.1.2.3 힘을 통한 평화 유지

전략과제 3은 국가이익에 위배되거나 사이버공간에서 불안정을 야기하는 행위를 식별, 대응, 방해, 억지하는 것을 목표로 한다. 이를 위해 먼저 미국은 국제법, 자발적이고 구속력 없는 규범을 통해 책임 있는 국가 행동을 장려하고, 신뢰구축 조치를 강화한다. 또한, 동맹 및 우방국과 악의적 사이버 행위자 추적, 대응을 위한 협의를 추진하고 통합전략을 수립할 계획이다.

3.1.2.4 미국의 영향력 증진

전략과제 4는 미국의 국익을 지원하고 이를 뒷받침하는 인터넷의 개방성, 상호운용성, 보안 및 신뢰성을 장기간 유지하는 것을 목표로 한다. 국제표준으로서

개방적 인터넷을 추구하고 인터넷을 통제하고자 하는 권위주의 국가들을 막기 위한 노력을 이행하도록 하고 있다.

또한, 글로벌 사이버역량을 구축하여 사이버위협 정보공유의 확대, 주요기반시설 및 공급망 보호 등 정부간 사이버 협력을 강화하고, 특히, 동맹 및 우방국 역량구축을 통해 미국의 영향력을 확대하고자 한다.

3.2 바이든 정부의 국가 사이버안보 전략

3.2.1 비전 및 접근방식

미국은 사이버안보 환경변화에 대해 보다 방어적(defensible)이고 회복적(resilient)이며, 가치일관적(value-aligned)인 디지털 생태계를 조성하는 것을 전략의 비전으로 제시하였다. 특히, 사이버공간을 국가 핵심가치인 '경제안보와 번영', '인권존중 및 자유', '신뢰할 수 있는 민주주의와 제도', '사회적 평등과 다양성'을 달성하고 이를 반영할 수 있는 중요한 수단으로 인식하고, 전략을 통해 사이버공간을 보호하기 위한 다음과 같은 근본적인 변화를 추구한다.

첫째, 사이버공간 방어를 위한 각 주체 간 책임의 재조정이다. 책임 재조정은 악의적 행위자에 대한 적극적 대응을 통해 적정 비용을 부과하고, 안전하지 않은 소프트웨어 제품 및 서비스 제조·배포 업체에 책임 부과를 통해 최종사용자가 사이버보안 사고에 대한 책임을 지지 않도록 하겠다는 것이다.

둘째, 사이버 방어에 대한 장기적 투자가 이루어질 수 있도록 인센티브를 조정하는 것이다. 긴급한 위협으로부터 스스로를 방어함과 동시에 회복력 있는 미래를 전략적으로 계획하고 투자할 수 있는 균형점을 찾고, 이를 위해 장기적인 투자를 촉진할 수 있는 인센티브를 제공한다.

3.2.2 전략과제

전략은 기본적으로 바이든 정부 출범 이후 발표된 사이버안보 관련 정책을 다시 한번 명시하고, 통합 이행 방향을 제시하였으며, 1) 주요기반시설 방어, 2) 위협 행위자의 분열, 해체, 3) 보안 및 회복력을 견인하는 시장의 힘 형성, 4) 회복력 있는 미래를 위한 투자, 5) 공동의 목표 달성을 위한 국제 파트너십 구축으로 전략과제를 설정하고, 하위에 세부과제를 두고 있다.

3.2.2.1 주요기반시설 방어

전략과제 1은 정부가 주요기반시설과 이들 기반시설이 제공하는 핵심 서비스에 대한 가용성과 회복력을 강화함으로써 국민들에게 안심과 신뢰를 제공하는 것을 목표로 한다. 이를 위해 정부는 국가안보와 공공안전을 보장하기 위해 주요기반시설에 사이버보안 최소 요구사항 적용을 확대한다. 또한, 이로 인한 주요기반시설 소유/운영자의 규제 부담을 경감하기 위한 규제 간 조화를 추진한다.

또한, ONCD는 다양한 연방 사이버보안 부처 및 기관의 역량을 향상시키기 위해 통합, 조정, 협력 계획을 마련한다.

3.2.2.2 위협 행위자 분열, 해체

전략과제 2는 악의적 사이버 행위자의 국가안보와 공공안전을 위협하는 행위가 불가능하도록 모든 국력과 가능한 수단을 동원할 것임을 다시 한번 명시하고 있다. 적을 무력화하기 위해 민간부문의 적극적인 참여를 유도하고, 범정부적 차원에서의 랜섬웨어 대응 및 국제협력을 강화해 나갈 예정이다.

3.2.2.3 보안 및 회복력을 견인하는 시장의 힘 형성

전략과제 3은 정부가 디지털 생태계의 위험을 감소시키고, 사이버보안이 취약한 환경에서 벗어날 수 있도록 최선의 위치에 있는 자에게 책임을 부과할 것임을 명시하고 있다. 이를 위해 데이터 소유자의 개인데이터 보호 및 프라이버시를 강화하고, 소프트웨어 제품 및 서비스의 안전한 개발 관행을 촉진하기 위해 합리적인 예방조치를 이행하지 않은 소프트웨어 개발·배포 업체에 책임 부여하며 책임 회피 방지를 위한 법 제도를 마련한다. 그리고 연방 보조금 프로그램을 통해 보안 및 회복력을 갖춘 인프라에 투자 촉진을 보장할 계획이다.

3.2.2.4 회복력 있는 미래를 위한 투자

전략과제 4는 미국이 전략적 투자 및 조정, 협업을

통해 안전하고 회복력 있는 차세대 기술 및 인프라의 혁신을 지속적으로 주도하는 것을 목표로 한다. 이를 위해 인터넷 기반 및 디지털 생태계 전반에 걸친 기술 취약점을 줄여나감과 동시에 초국가적 디지털 억압에 탄력적으로 대처해나갈 예정이다. 또한, 포스트 퀀텀 암호, 디지털 신원확인 솔루션, 청정에너지 인프라 등 차세대 기술 관련 사이버보안 연구개발에 우선순위를 부여하고 이를 위해 국가 사이버 인력양성에도 힘쓸 예정이다.

3.2.2.5 공동의 목표 달성을 위한 국제 파트너십 구축

전략과제 5는 미국이 사이버공간에서 책임 있는 국가 행동을 권장하고, 무책임한 행동 시 해당 주체를 고립시키고 비용을 부과하는 환경을 만들어 나갈 것을 명시하고 있다. 이를 위해 국제연합 등 유사입장을 가진 국가들과의 파트너십을 활용하여 악의적 사이버 활동에 대한 공동 대응 및 대가부과 등을 추진한다. 또한, 사이버위협으로부터 미국의 동맹 및 우방국이 스스로 방어할 수 있는 역량 강화를 지원하고, 이들과 협력하여 ICT 제품과 서비스의 안전하고 신뢰할 수 있는 글로벌 공급망을 구축해나갈 예정이다.

4. 트럼프 및 바이든 정부의 전략 비교

트럼프 및 바이든 정부의 전략을 정성적·정량적 2가지 측면에서 분석하였다. 먼저, 전략에 대한 정성적 분석을 위해 전략의 비전과 접근방식, 세부 전략과제 비교·분석을 통해 차이점을 식별한다.

둘째, 텍스트 마이닝 기법 중 하나인 토픽모델링 분석에 기반한 정량적 분석이다. 자연어 처리(NLP, Natural Language Processing) 기술과 기계학습 기술의 결합으로 시작된 토픽모델링은 문서의 단어들을 추출하고 단어들이 특정 토픽에 포함될 확률을 토대로 토픽, 즉 주제를 분류하는 방법이다. 이는 전문가 의견을 기반으로 한 기존의 정성적 분석의 한계를 넘어 정량적인 문서 분석을 가능하게 한다는 점에서 의미가 있다. 본 연구에서는 토픽모델링에 최적화된 알고리즘인 잠재의미 분석(LDA, Latent Semantic Analysis)을 활용하여 미국 사이버안보전략의 세부 주제를 살펴보고 그 특징과 경향성을 분석한다.

4.1 정성적 비교·분석

바이든 정부의 전략은 기본적으로 2018년 국가 사이버 전략과 우선순위는 같다. 그러나 구체적인 내용에는 다소 차이가 있다. 트럼프 정부 전략과 비교했을 때 주요 변경사항 및 특징은 5가지이다.

먼저, 전략의 명칭이 '사이버 전략'에서 '사이버안보 전략'으로 변경되었다는 것이다. 2023년 전략은 사이버를 안보영역의 하나로 바라보고, 기존 전략보다 디지털 경제성장, 기술적 우위 확보 등과 관련된 과제가 줄고 디지털 생태계를 악의적 행위자로부터 보호하기 위한 사이버안보 관점에 전략과제가 증가하였다.

둘째, 법과 규제를 통해 사이버공간 보호를 위한 정부 및 기업의 책임을 재조정하고, 주요기반시설에 사고보고 의무화, 최소 요구사항 적용 등 의무적 통제와 정부의 역할이 강화되었다는 것이다. 미국은 기존의 시장이 자발적 협력만으로는 한계가 있다는 것을 인정하고, 소프트웨어 제조 및 배포업체에 최소한의 사이버보안 조치 이행 책임 부과하고 책임 회피 방지를 위한 법제도 마련한다.

셋째, 트럼프 정부의 사이버 억지 전략에서 악의적 사이버 행위자에 대한 선제공격, 제재 및 대가부과 등 공세적 대응 기조가 강화되었는데, 이를 뒷받침하기 위해 2023년 전략에서는 억지(deterrence)라는 용어는 전혀 언급되지 않고, 교란(disrupt), 파괴(dismantle) 등 보다 공세적인 용어를 사용했다.

미국은 오바마 정부부터 기존의 방어역량 강화뿐만 아니라 공세적 사이버역량 개발을 통한 억지력 확보를 추진하였다[44]. 트럼프 정부도 사이버 전략에서 사이버 억지력 확보를 강조한 바 있다. 그러나 이러한 선언적인 억지 전략이 실질적인 유효성을 드러내지 못했고, 공격과 피해가 지속적으로 증가했다. 이에 바이든 정부는 전략을 통해 협력을 기반으로 공격의 출처를 밝히고, 공격자에게 책임을 묻는 징벌적 억지력(deterrence by punishment)을 강화하고자 하는 의지를 드러냈다. 그리고 실질적으로 대응 활동을 하고 공개하여, 보복위협을 가시적으로 보여주고 있다.

넷째, 시장의 원리에 기반하여 공공 및 민간의 자발적인 사이버보안 투자 확대를 위해 인센티브를 조정하는 등 장기적으로 회복력을 갖춘 디지털 생태계를 구축하고자 했다.

마지막으로 ONCD로 전략의 통합·조정 기관이 변경되었다. 트럼프 정부는 전략을 NSC를 중심으로 OMB와 협력하여 추진하도록 하였으며, 연방정부 사이버안보 활동의 통합 관리·감독과 일원적 위험관리 체계 구축을 위해 DHS의 역할을 강조하고, 국가 안보시스템 보안이라는 DoD의 역할을 명시하였다. 그러나 법무부(DoJ, Department of Justice), NSA, FBI 등 다른 부처의 역할은 명시된 바가 없다.

바이든 정부는 ONCD를 신설하고, ONCD가 부처 간 통합·조정 역할을 수행하도록 하였으며, ONCD를 중심으로 국가 사이버안보 전략을 이행하도록 했다. 그리고 DHS, DoD 외에도 DoJ, FBI, NSA 등 사이버안보와 관련 역할과 책임을 보유한 부처 및 기관을 전략에서 명시하고 이들 간의 협력을 강조하고 있다. 또한, ONCD가 NSC, OMB와 협력하여 전략의 효과를 평가하고 대통령 및 의회에 매년 보고하도록 하였으며, 데이터에 기반하여 이행계획을 추진하도록 전략에 명시하였다.

4.2 정량적 비교·분석

4.2.1 분석설계

미국 사이버안보 전략의 특징과 경향성을 분석하기 위해 미국에서 현재까지 발표한 3건의 국가 사이버안보 전략 문서를 대상으로 LDA 토픽모델링을 수행하였다. 다만, 최근 미국의 사이버안보 전략 특징과 경향성에 초점을 맞추고자 2003년도에 발표된 부시 행정부 결과에 대한 별도의 해석 없이, 트럼프·바이든 행정부의 전략 분포를 중심으로 결과를 제시하였다.

LDA 토픽모델링은 단어가 ①특정 토픽에 존재할 확률과 ②문서에 존재할 확률을 추정하여 문서 내 토픽의 종류와 분포를 정량적으로 도출하는 방법으로, 연구자가 설정한 문서 간 토픽분포(α), 문서 내 단어들 간 토픽분포(β), 토픽 개수(k), 3개의 파라미터 값을 기반으로 토픽을 추출한다.

동 연구에서는 최적의 α, β, k 값을 산출하기 위해 상용 소프트웨어인 넷마이너(NetMiner) 4.0의 토픽모델 평가 기능(topic coherence)을 활용, 응집성 지수(coherence score) 값이 가장 높은 파라미터인 α=0.01, β=0.01, k=21 값을 적용하였다[45].

(그림 2) 분석설계

4.2.2 토픽모델링 결과

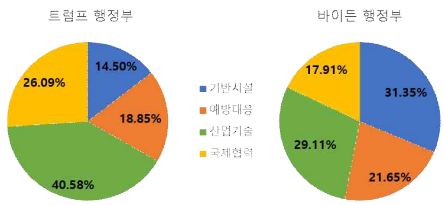
토픽모델링 결과 <표1>과 같이 21개의 토픽에 대해 토픽별 단어의 조합을 통해 토픽명을 정의한 후 국가 사이버안보전략에 대한 토픽모델링 선행 연구에 따라 토픽을 ①주요기반시설 보호 정책, ②예방 및 대응역량 강화 정책, ③인터넷·산업·기술 정책, ④국제협력 정책으로 그룹화하고, 이를 4대 정책 분야로 설정하였다[46].

<표 1> 토픽모델링 결과

토픽			비중(%)	
분야	정책명	단어(상위 10개)	트럼프	바이든
주요기반시설 보호	〔규제·회복력〕 주요기반시설 규제 및 회복력 확보	**critical infrastructure**, administration, regulation, resilience, investment, industry, cost, regulator, operation, marketplace	0.00	8.96
	〔취약점〕 주요기반시설 취약점 완화	cyberattack, vulnerability, system, network, **critical infrastructure**, cyberthreats, information, infrastructure, actor, computer	2.90	0.00
	〔위기관리〕 주요기반시설 공격에 대한 위기관리	system, cyberattack, state, **critical Infrastructure**, emergency, information, system, crisis, incident, information, cyberspace security	0.00	2.24
	〔정보공유〕 주요기반시설 정보공유 파트너십 강화	information, security, industry, coordination, **critical infrastructure**, cyberaware, information, sharing, operation, network, partnership	2.90	4.48
	〔법집행〕	law, agency, enforcement,	8.70	15.67

토픽			비중(%)	
분야	정책명	단어(상위 10개)	트럼프	바이든
	사이버 인텔리전스 및 법집행 강화	cyberthreats, intelligence, capability, infrastructure, incident, partner, **critical infrastructure**		(1순위)
예방 및 대응역량 강화	〔조달〕 공공조달 사이버보안 강화	security, agency, system, administration, contractor, priority, procurement, budget, information, authority	4.35	2.99
	〔취약점〕 SW취약점 완화 및 위험관리	software, vulnerability, patch, system, security, company, risk, flaw, tool, liability	1.45	4.48
	〔공급망〕 국가안보를 위한 공급망 위험관리	risk, supply chain, risk management, national security, ecosystem, responsibility, eo, investment, infrastructure, system	8.70	7.46
	〔랜섬웨어〕 랜섬웨어 대응 활동	ransomware, disruption, operation, actor, campaign, cryptocurrency, progress, CRI, prosperity, payment	0.00	6.72
	〔사고대응·경보〕 사이버 사고대응 및 위기 경보	cyberattack, incident, response, cyberthreats, vulnerability, nation, agency, information, damage, warning	4.35	0.00
인터넷·산업·기술	〔인터넷 취약점〕 인터넷 네트워크 취약점관리	**internet**, DNS, cyberattack, security, BGP, information, network, infrastructure, router, IPv6	0.00	0.00
	〔인터넷망 보호〕 인터넷 네트워크 보안	network, infrastructure, **internet**, control, security, system, code, vulnerability, reliability, interdependency	0.00	0.75
	〔인권보호〕 인터넷 자유 및 인권보호	**internet**, freedom, society, country, principle, human right, connectivity, cyberthreats, commerce, communication	10.14	3.73
	〔인력개발〕 사이버보안 혁신 및 인력 투자	workforce, act, **R&D**, opportunity, leverage, administration, innovation, investment, IoT, CHIPS	7.25	5.22
	〔기업보안〕	network, **business**	4.35	1.49
	사이버공간의 비즈니스 연속성 보장	**environment**, information, agency, nation, contingency, computer, company, system, continuity		
	〔위험관리〕 민간부문 사이버보안 아키텍처	system, security, **business environment**, agency, risk, cyberthreats, access, architecture, control, operation	2.90	4.48
	〔연구개발〕 사이버보안 연구개발 투자 강화	system, **research**, infrastructure, security, nation, quantum, **R&D**, network, intelligence, investment	4.35	4.48
	〔표준·회복력〕 사이버보안 시장 표준 및 회복력 향상	security, marketplace, privacy, ecosystem, administration, standard, resilience, challenge, liberty, power	11.59 (2순위)	8.96
국제협력	〔규범〕 국제법, 규범 및 책임있는 행동	state, behavior, **partner**, consequence, norm, **nation**, international, law, commitment, framework, coalition	7.25	5.97
	〔혁신·리더십〕 사이버보안 혁신 및 글로벌 리더십 영위	**partner**, capability, collaboration, cyberthreats, **ally**, innovation, country, information, leadership, influence	13.04 (1순위)	11.94 (2순위)
	〔범죄대응〕 사이버범죄 대응을 위한 국제협력	cybercrime, barrier, administration, convention, law, **country**, **nation**, cooperation, standard, cyberaware	5.80	0.00

앞서 분류한 4대 정책 분야 중 바이든 행정부에 들어서 더욱 중요하게 다뤄진 정책 분야는 주요기반시설 보호 정책으로 나타난 한편, 인터넷·산업·기술 정책 비중은 감소한 것으로 나타났다.



(그림 3) 트럼프, 바이든 행정부의 정책 분포

주요기반시설 보호 정책의 세부 의제 중 가장 눈에 띄는 변화는 규제·회복력을 강화하고, 법집행 주제의 비중이 증가하고 있다는 점이다. 이는 앞서 정성적 분석결과에서도 살펴보았듯이 주요기반시설에 대한 규제와 의무가 확대되고 정부의 역할이 강화되었음을 보여준다.

예방 및 대응역량 강화 정책에서는 랜섬웨어 주제의 비중이 크게 증가하였는데, 이는 바이든 정부가 랜섬웨어 대응정책을 마련하고 국제협력을 주도하고 있는 것과 맥락을 같이 한다. 또한, 트럼프 행정부 전략과 유사하게 공급망 위험관리에 관한 의제가 가장 높은 비중을 차지했다.

인터넷·산업·기술 정책은 비중이 감소하였으나, 이전 행정부와 마찬가지로 인터넷 취약성이나 망 보호를 위한 기술적 접근보다 시장회복력, 인력개발, 연구개발 등 정책적 조치에 높은 우선순위를 두고 접근하고 있다는 점에서 세부 정책 기조는 유지되고 있는 것으로 도출되었다.

두 행정부 모두 표준·회복력을 가장 높은 비중으로 다루었는데, 이는 미국의 디지털 경제성장과 기술표준 선도를 지속적으로 중요하게 다루고 있음을 반영한다.

국제협력 정책은 미국이 사이버 분야에서 동맹국 및 파트너 국가들과의 혁신과 국제법·규범 형성을 통해 글로벌 리더십과 영향력을 유지하는 의지가 정량적 분석결과에도 드러났다. 한편 바이든 행정부 전략에서는 범죄대응을 위한 국제협력 정책이 0%로 나왔는데, 이는 사이버범죄라는 일반적인 단어를 랜섬웨어나 중대한 사이버 사고로 구체화했기 때문으로 해석할 수 있겠다. 실제로 cybercrime 단어는 트럼프 행정부 전략에서 17번, 바이든 행정부 전략에서 6번 등장하며 언급 횟수도 감소했다.

5. 한국에의 함의

이러한 미국 전략의 변화가 한-미 관계를 비롯해 우리나라에 미치는 영향과 한국 사이버안보 정책에 주는 함의에 대해서 살펴보도록 하겠다.

먼저, 미국 주도로 주요위협국의 사이버 공격에 대한 공동 대응이 증가하고, 한국도 동맹국으로 공동귀속, 공동제재에 대한 참여, 공세적 대응을 위한 역량 지원 요청 등이 확대될 것으로 판단된다. 미국은 전략에서 동맹 및 우방국과 악의적 행위에 대한 다양한 제재 수단을 공동으로 부과하고, 위협대응 및 공급망 보안을 위해 지역 협의체를 통해 연합전선을 구축하겠다는 의지를 밝혔다. 또한, 한국이 중국 및 러시아의 안보위협 대응에 적극적으로 참여하고, 글로벌 중추국가로서 국제적 역할을 확대하길 바라고 있다. 이에 일환으로 2022년에는 NATO가 최초로 중국을 NATO의 위협으로 정의한 NATO 전략개념(strategic concept)을 발표하는 NATO 정상회담에 한국 정상을 초청하였으며, 동맹 및 우방국 간 다자안보 협력을 약속했다. 이러한 상황에서 미국 및 우방국의 공동 대응 요청 시 정책적 결정을 위한 판단 기준과 외교 전략이 마련되어야 할 것이다.

둘째, 한-미간 북한의 사이버안보 위협대응을 위한 협력은 지속적으로 강화될 것으로 보인다. 미국은 전략에서 북한의 랜섬웨어, 가상화폐 탈취 및 자금세탁을 주요한 사이버안보 위협으로 바라보고 있다. 또한, 2022년 한미 정상회담 후속 조치로 북한 사이버위협 대응 한미 실무그룹 회의를 개설했고, 2023년 4월에는 한미 전략적 사이버안보 협력 프레임워크를 발표하였으며, 북한의 사이버공간에서 악의적 활동을 탐지·억지·와해하기 위한 대응 공조과 다양한 원천의 정보공유를 약속했다.

미국은 북한에 대해서도 다른 위협국가와 유사하게 선제적·공세적 대응을 강화하고, 국가 간 연대를 통한 추적·공동귀속을 추진할 것이다. 그리고 이에 대한 정당성 확보와 국제사회의 지지 형성을 위해 일부 증거 및 정보를 공개할 수 있다. 그러나 한국은 공세적 대응 시 북한과 분쟁 가능성이 있으며, 정보공개 시 정보원이나 우리가 가진 기술 및 역량이 노출된다는 딜레마가 있다[47].

북한은 우리나라에는 가장 주요한 위협국가이다. 이에 양국 모두에게 이익이 될 수 있도록 미국과 어떠한 방식으로 사이버 분야의 협력과 공조를 확대해 나갈지에 대한 구체적인 방안에 대한 면밀한 검토가 필요하다.

셋째, 한국도 사이버공간에서 억지력 확보 및 대가부과를 위한 전략과 이를 위한 공세적 역량 강화가 필요하다는 것이다. 미국은 방어력 강화만으로는 사이

버공간에서 적을 억지하기는 어렵다고 판단하고, 적극적 방어를 넘어 대가부과를 강조하고 있으며, 사이버공간에서 우위 확보를 위해 공격력을 강화해 나가고 있다.

한국은 전 세계적으로 높은 빈도의 사이버 공격 위험에 노출된 국가임에도 불구하고, 공개귀속이나 대가부과 사례가 많지 않고, 사고 발생 시 복구 및 재발방지 등 방어역량 강화를 위한 정책추진이 주를 이루었다. 그러나 이러한 방어중심의 대응정책은 한계가 있는 것이 사실이다. 북한 추정 사이버 공격만 살펴봐도 2004년부터 2021년까지 약 300배가 증가했다[48]. 이에 한국도 빈번한 사이버 공격에 대한 억지력을 확보하기 위해서는 악의적 사이버 행위자가 더이상 사이버공간의 은닉성으로 인한 이점을 누릴 수 없도록 법적·기술적 귀속 역량을 강화하고, 대가부과를 위한 전략·기술 개발이 요구된다.

넷째, 사이버안보를 위한 정부 개입의 필요성과 역할이 확대되고 있다는 것이다. 미국은 전략을 통해 사이버위협은 국가안보 이슈로 정부에 책임이 있으며, 민간기관의 자발적인 규정 준수 및 협력만으로는 한계가 있음을 강조했다. 한국은 주요기반시설이 대부분 정부 주체로 운영되어 미국에 비해 민간이 안보이슈에서 차지하는 비중은 낮다. 그러나 주요기반시설의 범위가 의료, 교육, 주요 IT 서비스 등으로 점차 확대되고 있어 향후 민간의 사이버안보 강화방안 마련 시 규제와 협력 간의 조정에 미국의 이러한 정책 방향을 참고할 수 있을 것이다.

마지막으로 전략을 포함한 사이버안보 정책의 지속적인 추진과 실효성 확보를 위해서는 정책 유효성 평가와 주기적 성과관리가 필요하다는 것이다. 미국은 전략이행에 있어 데이터 기반의 접근방식을 적용하여 유효성 평가를 통해 전략 이행의 결과 및 효과를 측정하고, 매년 대통령 및 의회에 보고하며, 전략 목표 달성을 위해 수정 등 후속조치를 수행할 계획을 밝혔다. 한국도 장기적인 사이버안보 전략 및 정책의 목표 달성을 위해서는 측정 가능한 성과지표를 설정하고, 평가를 통해 데이터를 수집하여, 객관적인 데이터에 기반한 과학적인 전략 및 정책 수립이 가능하도록 체계를 마련해야 할 것이다.

참고문헌

[1] DNI, “Background to Assessing Russian Activities and Intentions in Recent US Elections:The Analytic Process and Cyber Incident Attribution”, 2017. 01. 06.

[2] 양정윤, “미국 대선 러시아 개입 사건 분석”, NSR Brief(NSR 내부자료), 2017. 05.

[3] https://www.igloo.co.kr/security-information/ wannacry-ransom ware/ (검색일: 2023. 05. 12.).

[4] The White House, “Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea” 2017. 12. 19.

[5] Thomas Brewster, “Equifax Just Got Fined Up to $700 Million For that Massive 2017 Hack”, Forbes, 2019. 07. 22.

[6] FBI, “Chinese Military Hackers Charged in Equifax Breach”, 2020. 02. 10.

[7] Ryan Duffy, “Microsoft reveals first known Russian hacking attempt aimed at 2018 midterms”, Cyberscoop, 2018. 07. 19.

[8] Emily Price, “Chines Hackers Targeted 27 Universities to Steal Maritime Research, Report Finds”, Fortune, 2019. 03. 06.

[9] https://www.reuters.com/article/us-usa-trade-china-cyber-exclusive/exclusive-u-s-manufacturing-group-hacked-by-china-as-trade-talks-intensified-sources-idUSKBN1XN1AY?il=0 (검색일: 2023. 05. 12.).

[10] Sophie Bushwick “Giant U.S. Computer Security Breach Exploited Very Common Software”, Scientific America, 2020. 12. 15.

[11] https://www.cisa.gov/news-events/alerts/2021/04/15/nsa-cisa-fbi-joint-advisory-russian-svr-targeting-us-and-allied (검색일: 2023. 05. 12.).

[12] Brittany Chang, “One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack”, Business Insider, 2021. 05. 23.

[13] https://en.wikipedia.org/wiki/2021_Microsoft_Exchange_Server_data_breach (검색일: 2023. 05. 12.).

[14] Michael D.Shear, “Colonial Pipeline Paid Roughly $5 million in Ransom to Hackers”, The New York Times, 2021. 06. 07.

[15] The White House, “National Security Strategy”,

2017. 12. 18.
[16] The White House, “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”, 2017. 05. 16.
[17] 김규동, “미국 행정명령 13800 분석”, NSR Brief (NSR 내부자료), 2017. 05.
[18] 송민경, “미국 사이버보안 인력에 관한 행정명령 13870 분석”, NSR Brief(NSR 내부자료), 2019. 07. Institute of World Politics, 2020. 10. 22.
[19] The White House, “National Cyber Strategy of the United States of America”, 2018. 09.
[20] Department of Defense, “DoD Cyber Strategy”, 2018. 09. 18.
[21] https://www.cfr.org/blog/president-trumps-legacy-cyberspace-policy (검색일: 2023. 05. 12.)
[22] The White House, “Executive Order on Protecting Americans’ Sensitive Data from Foreign Adversaries”, 2021. 06. 09.
[23] 김규동, “미국 ICT 공급망에 관한 행정명령 13873 분석”, NSR Brief(NSR 내부자료), 2019. 07.
[24] The White House, “Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enable Activities”, 2016. 12. 28.
[25] The White House, “Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election”, 2018. 09. 12.
[26] The White House, “National Security Strategy”, 2022. 10.
[27] The White House, “Executive Order 14028: Improving the Nation’s Cybersecurity”, 2021. 05. 12
[28] 김동희, “美 ‘행정명령 14028: Improving the Nation’s Cybersecurity 주요 내용 분석”. NSR Brief(NSR 내부자료), 2021. 06.
[29] https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy (검색일: 2023. 05. 12.).
[30] The White House, “Executive Order on Blocking Property with Respect to Special Harmful Foreign Activities of the Government of the Russian Federation”, 2021. 04. 15.
[31] https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise (검색일: 2023. 05. 12.).
[32] 오다인, “美, 콜로니얼 파이프라인 몸값 230만달러 회수”, 「전자신문」, 2021. 06. 08.
[33] 최호, “美, 법무부 랜섬웨어 네트워크 하이브 폐쇄... 구글 맨디언트 추가대응필요”, 「전자신문」, 2023. 1. 27.
[34] Brooker Becher, “U.S. Sanctions on Tornado Cash: What Does This Mean for Cryptocurrency”, builtin, 2022. 11. 1.
[35] Department of the Treasury, Department of State, Federal Bureau of Investigation, “Guidance on the Democratic People’s Republic of Korea Information Technology Workers”, 2022. 05. 16.
[36] Department of the Treasury, “Treasury Sanctions Iran Cyber Actors for Attempting to Influence the 2020 U.S. President Election”, 2021. 11. 18.
[37] NIST, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, 22. 02.
[38] U.S. Whitehouse, Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, 22. 01. 19.
[39] The White House, FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware, 2021. 10. 13.
[40] 박주희, “美 랜섬웨어 대응 활동 분석”, NSR BRIEF (내부자료), 2023. 03.
[41] 주용석, “美, 2.2조원 들여 화웨이 장비 싹 걷어낸다”, 「한국경제」, 2021. 07. 14.
[42] James S. Brady, “Press Briefing by Press Secretary Karine Jean-Pierre and National Security Advisor Jake Sullivan”, The White House, 2022. 05. 18.
[43] James A. Lewis, “Toward a More Coercive Cyber Strategy”, CSIS, 2021. 03. 04.
[44] U.S. DoD, “Department of Defense Strategy for Operating in Cyberspace”, 2011. 07.
[45] R. Egger, ‘Applied Data Science in Tourism’, Springer, 2022.
[46] M. Song, D. H. Kim, S. Bae, S. Kim, “Comparative Analysis of National Cyber Security Strategies Using Topic Modeling”, International Journal of Advanced Computer Science and Applications, Vol. 12, No. 12, pp. 62-69, 2021.
[47] 장노순, “정보기관과 비국가 행위자의 이중관계: 사이버 위협의 공개지목과 사이버 공작을 중심으로”, 국가안보와 전략, Vol. 21, No. 4, pp.

43-78, 2021.
[48] 보안뉴스 기획취재팀, “북한 추정 사이버공격, 2004년부터 2021년까지 300배 이상 증가했다”, 「보안뉴스」, 2022. 05. 09.

〔저자소개〕

사 진
가로 18mm
세로 25mm

배 선 하 (Sunha Bae)
2009년 1월: 한국과학기술원 전기 및 전자공학과(석사)
2009년 1월~2013년 2월: LIG 넥스원 주임연구원
2013년 4월~2015년 1월: 두산중공업 기술연구원 주임연구원
2015년 2월～현재: 국가보안기술연구소 선임연구원
email : sunhabae@nsr.re.kr

사 진
가로 18mm
세로 25mm

송민경 (Minkyung Song)
2017년 8월 과학기술연합대학원대학교 과학기술경영정책(석사)
2017년~현재: 국가보안기술연구소 연구원
email : mksong@nsr.re.kr

사 진
가로 18mm
세로 25mm

김 동 희 (Dong Hee KIM)
2008년~2015년: 한국인터넷진흥원 선임연구원
2009년 2월: 고려대학교 정보보호대학원(석사)
2017년 2월: 고려대학교 정보보호대학원(박사)
2016년~현재: 국가보안기술연구소 정책연구실장, 선임연구원
email : dh_kim@nsr.re.kr