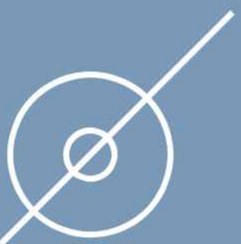
사이버 법제도



2023

한국사이버안보학회
KACS

한국사이버안보학회 워킹페이퍼 5호
발간일: 2023년 12월 27일

오일석 (국가안보전략연구원)

〈요 약〉

시장을 통한 사이버 위험분배의 실패는 정부에 의한 시장개입을 요구하고 있다. 민주주의와 시장경제 체제하에서 국가의 시장 개입은 특별한 경우에 한하여 법적 근거에 기초하여 이루어지고 있다. 국가의 시장 개입이 시장의 자율성을 저해하여 비효율과 비용을 양산할 수 있기 때문이다. 국가는 시장에 개입하여 사이버위험이 이슈연계와 양질전환되어 안보화 과정을 거쳐 사이버안보의 문제로 확산되는 과정을 차단하기 위한 거버넌스 구조를 정립하고자 할 것이다. 이 경우 국가는 위협(threat)과 취약성(vulnerability) 및 결과발생(consequence)을 감소시키거나 제거하기 위한 법제도(거버넌스)를 선택하여 사이버문제의 안보화 과정의 진행을 연결하는 고리를 차단 또는 저지하고자 할 것이다.

미국의 부시 정부는 사이버 문제를 국가안보 이슈의 하나로 인식하지 못하고 사이버 문제가 이슈연계나 양질 전환 되지 못하도록 사이버보안의 기반을 형성하는데 중점을 두었다. 오바마 정부는 초기에 사이버위험에 대한 대응에 있어 국가 중심보다는 시장의 자율에 맞기고자 한 것으로 보인다. 그렇지만 소니 해킹 사건을 계기로 사이버위험이 미국 내에서 현실화 됨에 따라 보다 적극적인 개입으로 정책방향을 선회한 것으로 보인다. 트럼프 정부는 이미 안보화 과정을 넘어선 사이버문제에 대해 사이버위협의 적극적인 감경, 공급망 재편을 통한 취약성의 극복, 회복력의 효율성과 탄력성 확보 등을 위해 적극적으로 국가가 개입하여 위험을 관리하는 방향으로 법제도(거버넌스)를 정비한 것으로 보인다. 바이든 정부는 사이버위험의 안보화를 차단 또는 감경시키기 위하여 사이버위협을 감경시키고 취약성을 감소시키며 결과발생의 방지 즉 회복력 강화를 위한 법제도(거버넌스) 정비와 개선을 지속하고 있다. 그렇지만 바이든 정부는 2023년 3월 발표된 사이버안보전략을 통해 사이버위협 대응을 위한 선제적 방어 전략의 실행보다는 공급망 보안을 중심으로 민관협력을 통해 취약성을 감소시키고 회복력을 강화하는 방향으로 전략의 중심축을 이동한 것으로 보인다.

미국의 사이버 문제에 대한 안보화 과정 대응 법제도(거버넌스) 체계의 실행과 방법을 참고하여 우리 실정에 적합한 법제도(거버넌스)를 구축할 필요가 있다. 한편, 국가가 시장에 개입하여 위협, 취약성을 제거하고 회복력을 강화하여 사이버공간의 안전성을 확보하는 것은 관련된 비용의 증대를 야기하게 된다. 따라서 우리 실정에 적합한 사이버안보 법제도(거버넌스) 구축과 운영을 위해서는 비용과 안보 가치의 사이의 최적 균형점을 찾아야 한다. 결국 국가는 위험의 제거 또는 감소에 소요되는 비용과 사이버 보안 강화로 증대되는 사회적 복리의 비교를 통하여 가장 효율적인 사이버안보 법제도(거버넌스) 체계를 선택할 수밖에 없을 것으로 보인다.

Ⅰ. 서론

정보통신 기술의 발전에 따라 등장한 해킹, 바이러스 유포 등 사이버 문제는 단순히 정보화의 역기능으로 치부된 적이 있었다.[1] 그렇지만 정보화와 세계화 그리고 디지털 전환이 가속화되면서 사이버공간의 안전성을 확보하는 것은 국가의 중요한 안보 문제로 발전하였다. 국가의 핵심 기능 제공, 디지털 경제의 발전, 신산업의 육성 등이 사이버공간에 의존함에 따라 사이버공간의 안전을 보장하는 것이 국가의 핵심 과제로 자리잡은 것이다. 이와 같이 사이버공간의 안전성을 위협하는 문제는 '창발'의 단계를 거쳐 다른 이슈들과의 연계와 양질전환을 통해 '임계'를 지나 전 지구적으로 '확산'되는 안보화 과정을 거쳐왔다.

국가는 사이버 문제의 안보화 과정을 진행시키는 연결고리를 차단하여 사이버안보를 확립하기 위해 시장에 개입하여 왔다. 이는 사이버안보 문제를 시장의 자율에 맡겨 둔 결과 공유지의 비극이 발생하였고 무임승차자들이 양산되었기 때문이다. 민주주의와 법치주의 국가에서 사이버안보 문제에 대한 국가의 개입은 사이버안보 법제도(거버넌스)의 구축과 재정비로 이어졌다. 이러한 국가 개입의 필요성과 정당성을 평가하기 위해서는 어떠한 상황에서 어떠한 목적을 가지고 사이버안보 법제도(거버넌스) 구축과 재정비가 이루어졌으며 그 효과성이 있었는지를 탐색하는 것이 필요하다. 이러한 분석의 바탕 위에서 사이버안보 문제에 대한 국가의 역할과 시장의 수용 방안을 식별하고 국제사회의 대응 방식에 관하여 보다 더 현실적인 거버넌스 구조를 정립할 수 있기 때문이다.

따라서 이하에서는 우선 사이버 문제의 안보화 과정을 식별하고 위험분배에 기초하여 사이버안보에 대한 시장의 실패와 국가의 개입에 대하여 살펴보고자 한다. 또한 위험의 계량화에 기초하여 사이버 문제의 안보화 과정을 저지, 차단 또는 감경하기 위한 방안을 검토하고자 한다. 이러한 방안을 기초로 사이버안보 관련 법제도(거버넌스) 구축 과정을 검토하고 시사점을 도출하고자 한다. 한편 사이버 문제의 안보화 과정은 정보화 사회와 디지털 전환을 주도한 미국을 중심으로 시작되었다고 할 수 있다. 따라서 정보화 사회 도래 이후 즉 2000년대 이후 미국 각 정부가 추진한 사이버 문제의 안보화 진행을 차단 혹은 경감시키기 위해 추진하였던 법제도(거버넌스)를 중심으로 살펴보고자 한다.

Ⅱ. 사이버 문제의 안보화 과정과 위험분배

1. 사이버 문제의 안보화 과정

사이버안보의 법제도(거버넌스) 수립은 사이버 문제가 안보화 과정을 통해 국가안보의 문제로 확산되는 것을 차단·방지하기 위하여 국가가 어떠한 정책과 법제를 선택하고 수립하여 대응할 것인지를 결정하는 데에서 출발하여야 한다. 즉, 사이버위험의 발생에서 심화를 거쳐, 직간접적 연계가 없던 부문으로의 확장을 통해 지정학적 사안과 결합하여 안보화로 이르는 각 단계별 대응 방식에 대한 고찰이 필요한 것이다. 다만 사이버 이슈의 안보화 과정에 대응하여 국가가 해당 정책과 법제를 선택하기 이전에 사이버 문제의 해결에 대해 국가가 개입할 것인지 혹은 시장의

1) 이 글은 국가안보전략연구원의 입장과는 관련이 없는 순수한 개인적 연구의 결과임을 밝힙니다.

자율에 맡길 것인지에 대해서 우선 검토하여야 한다.

사이버보안이 야기하는 신흥안보 전개 양상 또한, 이 같은 창발-임계-확산의 메커니즘을 따르고 있는 현상이 관찰된다.[2] 랜섬웨어, 디도스, APT 등 최근 사이버 공격수법이 다양화되면서 기간 전산망, 지적 재산권, 첨단기술정보 및 데이터 절취의 문제가 심화되고 있다. 특히, AI를 활용한 지능적인 공격과 방어 활동의 증가 뿐만 아니라 사물인터넷(IoT), 확장현실(XR), 메타버스 가상융합현실 기술의 확산으로 디지털화된 사회의 공격표면(Attack Surface) 또한 확장되었다. 2020년 세계를 충격에 빠뜨린 'Log4j'(오픈소스 로깅 라이브러리 소프트웨어)의 보안 취약점 이슈는 광범위하게 사용되는 오픈소스 로깅 라이브러리 소프트웨어가 해킹당할 경우, 컴퓨터 내 모든 데이터를 삭제·손상시킬 수 있고, 악성 프로그램이 전파되어, 해킹당한 컴퓨터가 기하급수적으로 증가, 일반 국민들이 사용하는 컴퓨터 전반이 공격받는 '사이버 팬데믹'의 현실화 가능성을 시사한 바 있다.

이 같은 사이버해킹 이슈의 심화는 금전적 피해규모 증가에 그치지 않는다. 최근 국가가 배후에서 지원하는 해커집단들의 활동들이 에너지, ICT 전산망 등 국가 주요 인프라를 타겟으로한 위협의 '임계국면'으로 발전한다. 행해지고 있다. 이 같은 공격들이 성공할 경우, 사이버 공간의 경제적 피해를 넘어 원활한 물류·유통 체계까지 위험에 놓일 가능성이 증가하며, 이는 사회의 필수적인 '생명선(life-line)'에 대한 국가의 제어·통제력 상실을 유발하는 안보문제로 비화되게 된다. 나아가 배후 세력에 대한 추적, 책임소재, 처벌적 공격을 둘러싼 정치적 갈등을 낳게된다. 위협의 질적 변화를 넘어 지정학적 사안과 연계된 문제로 '확장국면'으로 진입하게 되는 것이다. 최근 발생했던 솔라윈즈 사건(2020.12), 콜로니얼 파이프라인 사건(2021.5)은 러시아 배후로 추정되는 사이버 공격집단에 의해 미국의 에너지·전력 배분 기능이 피해를 입음으로써, 심각한 안보적 문제로 자리매김했던 사례였다. 나아가 사이버 위협의 전개과정에서 창발과 임계단계를 넘어 지정학적 갈등의 문제로 비화되는 경로를 여실히 보여준 바 있다. 이는, 최근 스마트폰 등 주요 ICT 분야에서 신흥 공급망의 거점으로 부상하고 아세안 국가들에 시사하는 바가 크다. 미중 전략경쟁의 심화에 따라 대체 투자지로서 급속한 디지털화를 진행하고 있으나, 이에 부합하는 사이버보안 기술과 제도 기반은 상대적으로 지체되어 있어 취약점을 노출하고 있기 때문이다.

2. 시장을 통한 사이버위험 분배와 한계

사이버 이슈의 안보화 과정에 대한 대응에 있어 국가가 개입할 것인지 혹은 시장의 자율에 맡길 것인지에 대해서 우선 검토할 필요가 있다. 시장에서 시민들은[3] 계약을 통해 재화의 교환이나 서비스의 제공 뿐만 아니라 새로운 가치를 창출하고 있다.[4] 그러나 계약 체결의 당사자인 시민들은 계약 목적을 달성하는데 있어, 예상하였거나 또는 예상할 수 없는 위험에 직면하게 된다. 따라서 계약 당사자는 계약에 기초한 상호간의 관계 설정을 통하여 합리적으로 계약과 관련된 위험을 분배하고자 한다. 또한 당사자는 위험을 분배하는 과정에서 협상력과 교섭력을 강화하여 자신에게 유리하게 위험이 분배되도록 계약을 설계한다. 이와 같이 당사자 사이의 위험분배는 계약 목적 달성을 위해 계약의 전과정에서 발생하거나 내재되어 있는 위험을 당사자 사이에서 합

2) 이하 이 부분의 내용은 오일석, 윤정현, 김경숙, 김유철, 『아세안 신흥안보 협력 강화를 위한 모델 구축에 관한 연구』, 대외경제정책연구원(2022. 12. 30). pp.111-112 참조.

3) 시장을 통한 사이버위험 분배와 한계에 대해서는 오일석, "위험분배의 관점에 기초한 정보통신기반보호법 개선 방안", 법학논집, 이화여자대학교 법학논집(2014. 9), pp.298-302를 참고하여 작성하였다.

4) George Triantis, "The Evolution of Contract Remedies (and Why Do Contracts Professors Teach Remedies First?)", University of Toronto Law Review(2010), p.645.

리적으로 배분 또는 회피하는 것을 말한다. 합리적인 위험분배를 위하여 당사자는 위험 원인의 제거, 실사(實査)의 강화를 통한 위험의 감소, 법률, 계약 및 보험을 통한 위험의 이전, 위험에 대한 내부관리 등에 대해 검토하여야 한다.[5)]

위험이 발생할 경우에 대비하여 각 당사자는 주요 계약조항에서 그 위험에 대응하고 극복하는 방법을 구체적으로 규정함으로써 합리적인 위험분배를 달성할 수 있다. 계약당사자는 계약의 전 과정에서 발생하거나 내재되어 있는 위험을 배분 또는 회피하기 위하여, 위험을 통제·인수할 수 있고, 위험 통제를 통하여 우월한 경제적 이익을 향유할 수 있으며, 이러한 당사자에게 위험을 분배하는 것이 효율적인 경우 그에게 위험이 분배되도록 하여야 한다.[6)] 따라서 가장 최소 비용으로 위험을 회피할 수 있는 당사자가 누구인지, 위험에 상대적으로 민감하지 않는 당사자가 누구인지, 위험이 구체화되는 경우 최소한 비용으로 위험을 감내할 수 있는 당사자가 누구인지 등을 기준으로 효율적인 위험부담자를 식별하여야 한다.[7)] 이 경우 당사자들은 위험에 대한 통제의 정도, 위험에 대한 익숙함, 보상 필요성, 수급인 혹은 보험자에 대한 위험의 전가 가능성 여부, 위험의 이전에 대한 가치 등에 따라 위험분배에 대하여 결정하여야 한다.[8)]

사이버 위험은 컴퓨터와 네트워크로 연결된 사이버 공간을 이용한 해킹, 웜·바이러스 유포, 논리폭탄 등과 같은 사이버 공격이나 전자적 침해행위로 등으로 인하여 불이익이 발생할 개연성 또는 실제로 발생한 불이익으로 정의될 수 있다. 사이버 위험은 과학기술의 발전이 의도하지 않았던 현대적 위험 가운데 하나이다. 이와 같은 사이버 위험을 방지하고 대응하기 위한 사이버 보안 활동은 사이버 공간을 이용하는 모든 사람들의 편익을 증진시킨다. 따라서 사이버 공간을 이용하는 모든 사람들은 사이버 위험에 대한 위험분배에 참여하여야 한다. 이에 따라 사이버 공간을 이용하는 사람들은 일정한 사이버 보안 관련 활동을 실행하여야 한다. 사이버 공간을 이용하는 모든 사람들이 사이버 보안 관련 활동을 실행하는 경우, 사이버 위험을 절대적으로 차단할 수는 없겠지만, 상당 수준 감소시킬 수는 있다. 따라서 사이버 공간을 이용하는 모든 당사자들은 계약을 통하여 자신들이 통제할 수 있는 범위 내에서 사이버 위험에 대한 위험분배에 참여하여, 사이버 보안 관련 활동을 실행하거나 관련된 비용을 부담하여야 한다.

사이버 보안 활동의 일환으로 사이버 공간을 이용하는 특정 개인이나 기업들이 강력한 수준의 사이버 보안을 실행한다면, 이들의 컴퓨터 시스템이나 네트워크에 대하여 사이버 위험이 발생할 가능성은 감소될 수 있다. 그렇지만 이러한 사이버 보안 활동을 수행한 개인이나 기업이라 하더라도, 사이버 보안 활동을 수행하지 않은 개인이나 기업에 대하여 사이버 위험의 발생에 대한 책임을 물을 수 없다. 왜냐하면, 당사자들이 계약을 통하여 사이버 위험을 분배하였다 하더러도, 사이버 위험은, 과학기술의 발전으로 인한 의도하지 않은 새로운 위험으로 그 결과를 즉시 알 수 없는 경우가 대부분이고 원인규명도 명확하게 할 수 없는 경우가 많기 때문에 특정인에 대하

---

5) Patrick Mead, “Current Trends in Risk Allocation in Construction Projects and their Implications for Industry Participants”, Construction Law Journal(2007), p.29.

6) Vincent Hooker, “Major Oil and Gad Project-the Real Risks to EPC Contractors and Owners”, Construction Law Journal(2010), p.106. 그러나 이러한 위험분배의 원칙이 실무에 그대로 적용되는 것은 아니다. 왜냐하면 실무에서는 위험을 가장 잘 관리할 수 있는 당사자에게 위험이 분배되지는 않으며, 공식적인 위험평가가 시행되는 것도 아니고, 위험 관련 계약조항은 모델계약과는 상이하고 다양하며, 위험을 관리하는 것이 불가능한 수급인 및 컨설턴트에게 위험이 이전되는 경우도 있으며, 위험이 입찰자들에게 비용이 되지 않을 수도 있고, 위험이 효과적으로 분배되었더라면 비용절감 효과가 발생할 수도 있었을 터인데 그렇게 되지 않으며, 위험분배의 변경에 대한 합의는 당사자 이외에는 알려지지도 않고, 위험분배 변경의 결과로 인하여 분쟁과 소송이 증가되고 있기 때문이다.

7) George Triantis, “Unforeseen Contingencies. Risk Allocation in Contracts” in Boudewijn Bouckaert and Gerrit De Geest (eds), *Encyclopaedia of Law and Economics*(Edward Elgar, 2000) Vol Ⅲ, p.100.

8) Vincent Hooker, “Major Oil and Gad Project-the Real Risks to EPC Contractors and Owners”.

여 책임을 부담시키기 곤란하기 때문이다. 결국 사이버 보안 활동을 강화한 개인이나 기업은 이러한 활동을 통하여 개별적으로 실질적인 편익을 향유하는 것은 아니다.[9] 따라서 사이버 공간을 이용하는 모든 사람들이 이와 동일한 동인을 갖기 때문에, 모든 사람들이 서로 다른 사람들에게 편익이 되는 사이버 보안 활동이나 조치를 실행하였더라면 얻을 수 있었던 편익을 아무도 향유하지 못하게 된다.[10] 그러므로 사이버 보안은 사이버 공간을 이용하는 모든 사람들의 사이버 보안 관련 활동에 의하여 영향을 받기 때문에, '공공재(public good)'로 인식되어, 시장 실패적 요소가 내재된 것으로 평가되고 있다.[11]

결론적으로 민간 자율에 의한 사이버 위험의 위험분배와 그에 따른 사이버 보안 관련 활동은 한계에 봉착할 수밖에 없다. 따라서 사이버 보안을 강화하기 위해서는 국가가 개입하여 어느 정도 강제적인 사이버 위험에 대한 위험분배를 결정하고, 적합한 보안 수준 등을 지정함으로써 국가 전체적인 사이버 대응 수준을 향상시켜야 한다.[12] 특히 민간 기업들이 전력, 통신, 도로, 항공 등 국가의 핵심시설과 관련되어 있는 경우, 국가는 시장에 개입하여 사이버 위험분배에 개입할 것이다.

3. 정부의 시장 개입을 통한 사이버 문제의 안보화 고리 차단

시장을 통한 사이버 위험분배의 실패는 정부에 의한 시장개입을 요구하고 있다. 민주주의와 시장경제 체제하에서 국가의 시장 개입은 특별한 경우에 한하여 법적 근거에 기초하여 이루어지고 있다. 국가의 시장 개입이 시장의 자율성을 저해하여 비효율과 비용을 양산할 수 있기 때문이다. 민주주의와 시장경체 체제하의 국가는 국가안보, 공공복리, 사회질서 유지 등을 근거로 시장에 개입할 수 있다. 국가는 시장에 개입하여 사이버위험이 이슈연계와 양질전환되어 안보화 과정을 거쳐 사이버안보의 문제로 확산되는 과정을 차단하기 위한 거버넌스 구조를 정립하고자 할 것이다.

미국 국토안보부는 위험에 기반한 보안 접근법을 개발하였고[13] 이를 사이버안보에도 적용하고 있다.[14] 이 접근법에 따르면 위험(risk)은 위협(threat)과 취약성(vulnerability) 및 결과발생(consequence)의 곱으로 평가되고 있다. 위협, 취약성, 결과발생을 감소시키면 위험은 감소하며, 이중 하나라도 완전히 제거하면 위험은 발생하지 않는다.

사이버위협을 제거 또는 감소시키기 위해서는 공격자나 그 배후 국가에 대한 직접적인 타격, 법집행을 통한 수사와 소추, 경제제재 등을 실행할 수 있을 것이다. 취약성의 제거나 감소를 위

9) Hal R. Varian, "System Reliability and Free Riding", P*roceedings of the First Workshop on Economics and Information Security*(University of California, Berkeley(2002. 5. 16).

10) Benjamina Powell, "Is Cybersecurity a Public Good? Evidence from the Financial Services Industry", Journal of Law, Economics and Policy(2005), pp.498-499.

11) Ross Anderson, "Why Information Security is Hard-An Economic Perspective", *Proceedings of the 17th Annual Computer Security Applications Conference* (New Orleans, LA, 2001, https://www.acsac.org/2001/papers/110.pdf (last visited December 27, 2023)

12) 그러나 국가의 개입은 사이버 보안에 대한 시장실패를 가중시킬 뿐이며, 민간영역에서 사이버 보안에 대한 시장실패의 실질적 증거가 없는바 사이버 보안을 민간자율에 맡겨야 한다는 견해도 있다. Benjamina Powell, "Is Cybersecurity a Public Good? Evidence from the Financial Services Industry", pp.507-508.

13) Department of Homeland Security, National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency, 2013.

14) Michael Chertoff, Foreword to Cybersecurity Symposium: National Leadership, Individual Responsibility, Journal of National Security Law and Policy(2010), p, 3.

해서는 컴퓨터와 네트워크에 대한 주지적인 취약성 평가나 점검 체계를 구축하고 공급망 안전성을 보다 강화하기 위한 거버넌스 구조를 정립할 수 있을 것이다. 결과발생의 방지나 축소를 위해서는 사이버위협에 따른 회복력을 구축을 위한 거버넌스 체계 구축에 집중할 것이다. 즉 사이버안보 관련 정부 조직체계의 정비나 개편, 생태계 구축, 연구개발, 인력양성 등이 이에 해당할 것이다.

한편, 국가가 시장에 개입하여 위협, 취약성, 결과발생을 제거하여 사이버 보안을 강화하는 것은 관련된 비용의 증대를 야기하게 된다. 따라서 국가는 비용과 안보 가치의 사이에서 최적 균형점을 찾아야 한다. 결국 국가는 위험의 제거 또는 감소에 소요되는 비용과 사이버 보안 강화로 증대되는 사회적 복리의 비교를 통하여 가장 효율적인 사이버안보 법제도(거버넌스) 체계를 선택할 수밖에 없다.

Ⅲ. 안보화 과정과 위험분배에 따른 법제도(거버넌스) 체계 구축: 미국을 중심으로

1. 사이버보안의 창발: 부시 정부

가. 개요

정보통신 기술의 발전으로 정보화와 세계화가 진행되던 조지 W. 부시 정부시기에 컴퓨터 바이러스와 해킹 공격은 명성을 얻고자 하는 해커, 호기심에 의한 바이러스 유포, 개인정보 탈취를 위한 사이버범죄 등이 사회적 문제로 등장하기 시작하였다.[15] 즉 정보화의 역기능의 하나로 정보보안, 정보보호의 문제가 제기된 바, 사이버위험의 안보화 과정 가운데 창발 혹은 창발의 전단계에 해당한다고 할 수 있다.

부시 정부는 사이버 문제를 국가안보 이슈의 하나로 인식하지 못하고 사이버 문제가 이슈연계나 양질 전환 되지 못하도록 사이버보안의 기반을 형성하는데 중점을 두었다. 특히 주요 기반시설에 대해 해킹, 바이러스 유포 등 사이버위험이 발생하여 국가의 주요 핵심기능이 마비되는 것을 방지하는데 법제도(거버넌스) 구축을 집중하였다. 이는 클리턴 정부 시절 PDD63을 통해 주요 기반시설을 보호하고 정보화 사회에서의 국가의 핵심 기능과 서비스를 유지하기 위한 노력과 닿아있다. 다만 부시 정부의 주요기반시설 보호는 911테러 이후 물리적 테러의 가능성을 염두해두면서 이수연계를 차단하여 사이위험을 방지하고자 한 것으로 보인다.

나. 정책과 제도

부시 정부는 사이버보안에 관한 최초의 독립적 전략이라고 일컫러지는 〈사이버 공간을 확보하기 위한 국가 전략(The National Strategy to Secured Cyberspace)〉을 발표하였다. 전략의 핵심은 주요 기반시설에 대한 사이버공격을 예방하고, 취약성을 감소시키며, 사이버공격으로 인한 피해의 감경이라는 세 가지 목표를 제시하였다. 즉 사이버위험을 감경시켜 안보화 과정이 진행·

15) 'Ⅲ. 안보화 과정과 위험분배에 따른 법제도(거버넌스) 체계 구축: 미국을 중심으로' 부분은 오일석, 「바이든 정부의 사이버안보 정책과 시사점: 사이버억지를 중심으로」, INSS 연구보고서 2022-13, 국가안보전략연구원(2023. 2)을 중심으로 사이버 문제의 안보화 과정과 위험분배의 측면에서 재구성한 것이다.

확산되지 않도록 위협과 취약성 및 결과의 감경을 목표로 제시한 것으로 보인다.

나아가 이 전략은 사이버 공간을 이용하는 개인, 기업은 물론 기관 및 주요기반시설의 소유·운영자에 이르기는 다양한 행위자들의 역할과 책임을 규정하였다. 동 전략은 “사이버 공간에 분산된 자산을 보호하는 것은 미국인들의 노력이 필요하다. 연방 정부만으로는 미국의 사이버 공간을 충분히 방어할 수 없다고 하였다.[16] 이 전략은 사이버 위협을 식별하고, 정보공유를 촉진하며 피해를 경감시키고, 취약성을 감소시키며 국제적 차원에서 사이버 안보를 강화하기 위해 다른 국가들은 물론 비국가 단체들과의 협력을 강화하는 국제적 대응 활동과 다자간 협력을 구축을 포함하는 국가대응시스템을 구축함으로써 사이버공간에서의 미국의 리더십을 강화하도록 하고 있다.

위협의 감경에 대해서는 대부분 국내 형사 기소에 초점을 맞추고 있다. 즉 동 전략은 연방수사국(FBI), 국토안보부(DHS), 법무부(DOJ)로 하여금 국내외 사이버범죄에 대해 미국법 및 국제법 위반으로 처벌하기 위해 사이버범죄의 탐지, 체포 및 기소를 실행하도록 하였다. 그렇지만 부시 정부의 위 2003년 전략은 사이버공격에 대한 국가 간 또는 국제적 차원에서 기소나 소추내지는 적극적 방어나 훈련 등의 대응은 언급하지 않았다. 다만 미국의 대응이 '형사 기소에 국한될 필요는 없으며 적절한 방식으로 대응할 수 있는 권리를 보유한다.'[17]는 완곡한 표현으로 사이버 위협에 대한 대응 가능성만을 열어둔 것으로 보인다.

2003년 전략은 취약성의 감소와 인식제고를 통해 사이버공격의 실효성과 효용성을 제한함으로써 사이버 공격자가 의도하였던 결과 발생을 도출하지 못하게 함으로써 사이버공격의 유인을 갖지 못하도록 하였다. 이는 부시 정부가 2001년에 발표한 행정명령 제13231를 통해 '정보화 시대에' 공공 및 민간 부문의 주요 기반시설에 대한 보호를 조정하고자 한 것을 통하여도 알 수 있.[18] 부시 정부는 또한 2001년 9월 테러 공격 직후 설립된 국토안보부(DHS)로 하여금 미국의 주요 기반시설과 주요 자원을 보호하기 위한 개념, 프레임워크 및 프로세스를 개발하도록 규정한 국토안보부 대통령 지침 제7호를 발표하였다.[19] 국토안보부는 2006년에 제1차 국가기반시설보호계획(NIPP)을 발표했다.[20] NIPP를 통해 부시 정부는 2003년 전략의 세 가지 목적인 공격 예방, 취약성 감소, 피해 경감을 기반으로 하면서 '잠재적인 공격자는 그들이 감내할 수 있는 것보다 더 많은 실패의 위험에 직면하게 될 것이다.'라고 언급하였다. 즉 공격 대상의 가치(Target Value)를 감소시키고, 사이버위협을 예방 및 지연시키며, 공격의 효과를 최소화 및 '감경'하고, 공격으로부터의 회복을 강화하겠다고 하였다.[21]

2. 양질전환에 따른 임계(사이버보안에서 사이버안보) 단계: 오바마 정부

가. 개요

16) The Qhite House, The National Strategy to Secure Cyberspace(2004), p.14.
17) Ibid. pp.50, 59.
18) The White House, Executive Order 13231, Critical Infrastructure Protection in the Information Age(October 2001).
19) Homeland Security Presidential Directive No. 7, Directive on Critical Infrastructure, Prioritization, and Protection, 2003.
20) Department of Homeland Security, National Infrastructure Protection Plan, 2006.
21) Ibid., 45-47.

오바마 정부는 초기에 사이버위험에 대한 대응에 있어 국가 중심보다는 시장의 자율에 맞기고자 한 것으로 보인다. 따라서 오바마 정부는 사이버안보전략은 발표하지 않고 국가 차원에서 '국가사이버안보종합이니셔티브' (2009)를 발표하였다. 그렇지만 소니 해킹 사건을 계기로 사이버위험이 미국 내에서 현실화 됨에 따라 보다 적극적인 개입으로 정책방향을 선회한 것으로 보인다. 이에 따라 오바마 정부는 '국방사이버전략'을 발표하였다. 한편 오바마 후기인 2015년 이후 2018년 사이 러시아의 2016년 대선 개입과 미 주요 국가기반 시설에 대한 렌섬웨어 공격 및 중국에 의한 미국의 선진기술과 지적재산권에 대한 탈취가 확대는 물론 중국이 연방 정부 전현직 직원의 정보를 절취하는 사건이 발생하였다. 그럼에도 불구하고 오바마 정부는 사이버위협을 감경하기 위한 보다 공세적인 작전이나 적극적인 대응 조치를 전개하지 않았다. 다만 취약성 감소나 회복력 강화 등을 통해 사이버위험을 감경시키기 위한 기반을 형성하는데 중점을 두었다. 이러한 오바마 정부의 거버넌스 구조는 사이버위협에 대한 정부의 대응이 지나치게 미온적이라는 비판에 직면하였다.[22)]

나. 정책과 제도

2009년 1월에 취임한 오바마는 대통령 국가안보지침 제54호(NSPD 54) 따라 개발된 "국가사이버안보종합이니셔티브(CNCI)"를 발표하였다.[23)] CNCI는 부시 정부에서 시작되어 오바마 정부에서 마무된 것으로 2003년 전략을 강화한 것이다. CNCI는 미국이 사이버안보에 있어 달성하여야 할 과제를 수립하였는데 그 가운데 10번째 과제가 '지속적인 억지 전략과 프로그램을 정의하고 개발한다.'는 것이다.[24)]

오바마 정부는 2009년 CNCI를 통해 사이버위험에 대한 '경고 역량'의 향상, '민간 부문과 국제 파트너의 역할' 강화, '국가 및 비국가 행위자 모두에 대한 적절한 대응'의 개발 등이 중요하다고 인식하였다.[25)] 이에 따라 2009년에 행정부 사이버안보조정관(the Executive Branch Cybersecurity Coordinator: the White House cyber czar)을 신설하고 마이크로소프트의 보안 책임자였던 Howard Schmidt를 임명되었다. 같은 해 국방부는 NSA와 협력하여 미국 사이버사령부(USCYBERCOM/Cybercom)를 창설하였다. 사이버사령부는 NSA 내에 위치하고 NSA 국장이 이끄는 미국 전략사령부 소속으로 NSA 네트워크를 사용하여 DoD 컴퓨터와 정보 인프라를 보호하는 임무를 맡게 되었다. 사이버사령부는 억지 목적을 위하여 공세적인 사이버 역량을 개발하는 임무도 맡게 되었다.

오바마 정부는 이후 2011년에 〈사이버공간에서의 국방부 작전 전략(DoD Strategy for Operating in Cyberspace)〉을 최초로 정립되었다. 이 전략은 2010년 5월 〈국가안보전략(2010 National Security Strategy)〉과 2010년 2월 〈4년 국방 리뷰(Quadrennial Defense Review)〉에 기초하고 있다. 이 작전 전략은 미 국방부가 사이버 공간을 전쟁의 '작전 영역

22) Joseph Marks, "GOP to Obama: Crack down on Chinese hackers," *Politico,* June 10, 2015, https://www.politico.com/story/2015/06/republicans-obama-chinese-hackers-crack-down-118802 (accessed: October 3, 2023).; Council on Foreign Relations, "President Obama's Pursuit of Cyber Deterrence Ends in Failure," January 4, 2017, https://www.cfr.org/blog/president-obamas-pursuit-cyber-deterrence-ends-failure (accessed: October 3, 2023).

23) The White House, National Security Presidential Directive No. 54, Cybersecurity Policy(2008); US Government, Cyber Space Policy Review, 2009. https://irp.fas.org/eprint/cyber-review.pdf(accessed: October 3, 2023); The White House, Comprehensive National Cybersecurity Initiative(2009).

24) CNCI, p.4.

25) CNCI, 5.

(operational domain)'으로 간주하고 '사이버 공간의 잠재력을 최대한 활용하기 위해 조직, 훈련 및 장비의 정비를 포함한 5개의 전략적 이니셔티브를 정립하였다.[26)]

이후 국방부는 2015년에 최초로 국방 사이버전략(the DoD Cyber Strategy)을 발표하였다. 이는 2014년 북한의 소니 해킹 공격으로 미 본토에서 사이버공격에 따른 위험이 실제로 발생함에 따라 사이버위협에 대한 제거와 감소를 통해 사이버 문제가 안보화 과정에서 확산되는 것을 차단하기 위한 조치로 보인다. 따라서 이 전략은 사이버사령부의 확장된 공세적 목적을 포함시켰다. 국방 사이버전략은 사이버 전쟁(cyberwarfare)과 사이버 방어(cyber defence)에 대해 전반적으로 검토하였다. 국방 사이버전략은 미국의 국익에 반하는 사이버 공격에 대하여 미국 권력의 적절한 수단을 선택·사용하여 미국이 원하는 시간, 장소, 방법으로 지속적으로 대응할 것이라고 하였다.[27)]

한편 오바마 정부는 국제협력과 국제규범 정립을 통해 사이버위협 감경을 위한 활동의 효과성과 정당성을 확보하여 사이버위험이 안보화 과정으로 확산되는 것을 방지하고자 하였다. 즉 오바마 정부는 2011년 정립한 〈사이버 공간 국제 전략(International Strategy for Cyberspace)〉을 통해 '디지털 세계는 더 이상 무법천지가 아니며', '디지털 세계는 국가와 국민 사이에 책임감 있고 정의로우며 평화로운 행위 규범이 자리잡기 시작하였다'라고 하였다.[28)] 이 전략에 기초하여 미국 국무부는 2011년에 세계 최초로 사이버이슈조정관실(Office of the Coordinator for Cyber Issues (S/CCI))을 설립하여 사이버 관련 외교 업무를 조정하고 국제 사이버 규범을 개발하도록 하였다. 사이버이슈조정관실은 2015년 미국과 중국의 사이버를 통한 경제적 정보활동에 관한 협정(중국이 이후에 영국, 캐나다, 호주, G-7, G-20과 서명하기로 쌍무적으로 합의함)을 체결하여, 어느 쪽도 '사이버 상에서 이용 가능한 지적 재산을 도용'을 하지 않기로 성문화하였다.[29)] 이러한 양자 및 다자간 활동은 사이버위협 관련 활동을 감경시킴으로써 사이버 문제의 이슈연계와 양질전환을 차단하고자 한 것으로 보인다. 사이버이슈조정관실 2015년 유엔 정부 전문가 그룹(GGE)이 사이버 규범에 대한 기초적인 사항을 정립하는 기여한 바 있다. 다만 GGE는 2017년에 이러한 규범을 국제법에 포함된 권고사항과 연결하는데에는 실패하였다.[30)]

한편 위 2011년 전략은 자위권(right to self-defense) 행사를 통해 사이버위협을 제거할 수 있음을 강력하게 시사하였다. 동 전략은 '미국은 사이버 공간에서의 적대 행위에 대응할 것이며, 특정 적대 행위에 대해서 미국은 군사적 파트너들과 맺은 조약에 따라 적절한 대응 행동을 취할 수밖에 없으며, 이 경우 외교, 정보, 군사, 경제 등 모든 수단을 사용할 권리를 보유한다.'고 밝히고 있기 때문이다.[31)] 다만 오바마 정부는 합법적으로 간주되는 사이버 정보활동과, 경제적 혹은 국내적 마비 혹은 기반시설 파괴 등을 목적으로 하는 불법적인 사이버 정보활동, 정보 절취, 및 사이버 공격을 구분하고자 하였다. 따라서 2015년 중국이 미국 인사관리국(OPM)으로부터 2,000만 명 이상의 인사 기록을 유출한 것에 대하여 '공격'이 아니라 오히려 (합법적) 정보활동으로 간주하였다. 당시 국가정보국장이었던 James Clapper는 미국도 같은 일을 했을 것이다라고 하였다.[32)]이러한 사실을 통해 볼 때 오바마 정부는 각종 전략 문서를 통해 사이버위협 제거

26) Department of Defense, Strategy for Operating in Cyberspace(2011), pp.5-6.
27) Department of Defense Cyber Strategy(20150, pp.10-11.
28) The White House, International Strategy for Cyberspace(2011, 3).
29) Adam Segal, 'The Top Five Cyber Policy Developments of 2015', Council on Foreign Relations(January 4, 2016).
30) UN General Assembly, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', Seventieth Session, Item 93(2015).
31) David Sanger, "US Wrestles with how to fight back against Cyberattacks", NY Times(July 30, 2016).
32) Mike Levine, "China is "Leading Suspect" in Massive Hack of US Government Networks", ABC

나 감경을 통해 사이버 문제의 이슈연계와 양질전환을 천명하고 그 기반을 구축하기는 하였지만 실제로는 취약성의 감소나 회복력 강화를 통해 사이버위험을 감경하고자 한 것으로 보인다.

다. 법제

오바마 정부는 사이버 문제가 양질전환과 이슈연계를 통해 안보화의 문제로 확산되는 고리를 차단하기 위한 법제 정비 활동에 있어 결과발생의 방지를 통해 회복력을 강화하기 위하여 정보공유를 법제화하였다. 아울러 사이버위협 감경을 위해 군사적인 활동을 동원하기 보다는 현실적인 방안으로 경제제재를 부과하기 위한 법제를 도입하였다.

특히 정보공유 법제화에 있어 시장과 민간에 대한 부담을 경감시키기 위하여 사이버위험에 대한 정보공유를 실행한 시장 참가자들에 대한 면책 규정 도입에 집중하였다. 경제제재 또한 시장을 통해 경쟁국이나 적성국을 압박하기 위한 것으로 사이버 문제의 안보화 과정 차단에 대한 개입을 최소한 자제하고 시장을 통한 해결을 모색하였다고 할 수 있다. 따라서 사이버 경제제재에 대한 법적 토대를 구축하였지만 경쟁국인 중국이나 러시아에 대한 제재를 발동하기 보다는 미 본토에 대한 사이버위험을 야기한 북한의 해커들에 대한 제재 부과를 실행하였다.

1) 정보공유와 면책의 법제화

2015년 12월 18일 오바마 대통령의 서명으로 효력을 갖게 된 미국의 2015년 사이버보안정보공유법(Cybersecurity Information Sharing Act of 2015 : CISA)은 연방 정부와 민간 부문의 사이버 보안 관련 정보공유 체계를 정립하고 있다.[33] 즉, 이 법에 따라 국가정보장관(the Director of National Intelligence), 국방부장관, 법무장관, 국토안보부 장관 등으로 하여금, 미국 연방 정부부처가 다른 연방 기관, 주 및 지방정부는 물론 민간 기관과의 정보공유를 활성화하기 위한 절차를 개발하고 제공하도록 하고 있다.[34]

이 사이버보안정보공유법은 동법에서 규정한 절차와 방법에 따라 사이버 위협 표지(cyber threat indicator) 또는 방어 수단(defensive measure)을 공유 또는 제공받은 민간단체에 대하여 소송을 제기하지 못하도록 규정하고 있다.[35] 즉, 동법 제106조(b)항은 사이버 위협 표지 또는 방어 수단을 공유 또는 제공받은 것을 이유로 민간단체(private entity)에 대하여 소송을 제기하거나 진행할 수 없으며, 만일 이러한 소송이 제기된 경우 법원은 이를 즉시 각하하여야 한다고 규정하고 있다.[36] 이 경우 연방 제정법, 주 또는 지방 정부법 등에서 따로 규정하고 있다고 하더라도 이러한 민간단체는 면책조항의 적용을 받는다.[37]

2) 경제제재의 법제화

News(June 25, 2016).

33) Sullivan & Cromwell LLP, The Cybersecurity Act of 2015(December 22, 2015), p.1.

34) Ibid.

35) Mathew J. Gardner and Moshe B. Broder, "CISA: Hope for More Cybersecurity Challenges in Implementation and Interpretation", the Procurement Lawyer, Volume 51, Number 3(Spring 2016). p.26.

36) Cybersecurity Information Sharing Act of 2015 § 106(b)(1).

37) Joint Explanatory Statement to Accompany the Cybersecurity Act of 2015, p.4, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/jes%20for%20cybersecurity%20act%20of%202015.pdf (accssed December 27, 2023).

오바마 대통령이 2015년 4월 1일 행정명령 제13694호를 발표하여 사이버안보 위반을 이유로 경제제재를 부과할 수 있도록 법제화하였다. 즉 미국은 악의적 사이버 활동 또는 외국에 위치한 사람의 감독 하에 이루어진 악의적 사이버 활동으로 미국의 국가안보, 외교정책 및 경제에 비정상적인 위협을 야기하는 경우 제재(sanction)를 부과할 수 있도록 하였다.

한편 미국 하원은 2018년 북미 화해의 무드가 조성되었음에도 불구하고 북한을 비롯한 중국과 러시아 및 이란의 사이버 공격에 대하여 제재를 강화하는 "사이버 억지와 대응 법안(Cyber Deterrence and Response Act of 2018, H.R.5576)"을 2018년 9월 5일 통과시켰고, 8월 23일에는 상원도 같은 내용의 법안(S.3378)을 통과시켰다. 그렇지만 동 법안은 최종 통과되지 못하였고 폐기되었다.

이러한 점에서 볼 때, 오바마 정부 당시 미국은 사이버위협 감소를 통해 사이버 문제의 안보화 차단 거버넌스 구축에 있어 시장 개입을 통한 법제화에는 상당히 자제하고 있는 모습을 보였다고 할 수 있다. 오히려 시장에 개입하는 경우 시장이 필요로 하는 요구사항을 법제화하여 지원하는데 노력하였다고 볼 수 있다.

3. 확산: 사이버안보의 국제화와 진영화: 트럼프 정부

가. 개요

사이버위험 감경을 통해 사이버 문제의 이슈연계와 양질전환을 차단하는 거버넌스 구축에 있어 오바마 정부가 취하였던 시장에 대한 최소한의 개입 혹은 시장 개입의 자제 기조는 오바마 정부 말기 러시아의 선거 개입으로 시장에 대한 저극적인 개입으로 전환된 것으로 보인다. 이는 2016년 대선 당시 러시아의 2015/16 민주당 및 민주당 전국위원회 자료 해킹, 조작, 유출에 대해 당시 John Brennan CIA 국장이 미국 민주주의 제도를 훼손하고 영향을 미치는 '새로운 수준의 악의적인 활동'으로 간주한 것을 통하여 알 수 있다.[38] 이는 사이버 문제가 이미 양질전환과 이슈연계를 통해 안보화 과정을 거쳐 심각한 국가안보 문제로 확산되고 있음을 인식한 결과라고 할 수 있다. 따라서 트럼프 정부는 이미 안보화 과정을 넘어선 사이버 문제에 대해 사이버위협의 적극적인 감경, 공급망 재편을 통한 취약성의 극복, 회복력의 효율성과 탄력성 확보 등을 위해 적극적으로 국가가 개입하여 위험을 관리하는 방향으로 법제도(거버넌스)를 정비한 것으로 보인다.

이에 따라 트럼프 정부는 중국과 러시아와의 경쟁을 인식하면서 사이버위험 감경을 통해 사이버 문제의 이슈연계와 양질전환을 차단함에 있어 보다 적극적인 개입을 실행하고자 한 것으로 보인다. 이는 미국의 기술과 지적재산권을 탈취하고 있는 중국과, 미국의 선거에 개입한 러시아에 대해 보다 적극적인 대응을 실행할 것임을 천명한 것을 통하여 알 수 있다. 이에 미국은 사이버공간에서 무력분쟁(armed conflict) 수준 이하의 행동을 포함하는 선제적 방어(defend forward)를 수행할 것이라고 하였다.

트럼프 정부가 시장에 대한 적극적 개입을 통해 사이버안보 위험을 관리하고자 하였지만 트럼프 정부는 중국의 기술탈취를 막지 못하였고 러시아의 해킹 및 가짜뉴스에 적절하게 대응하지

38) David Sanger, "US Wrestles with how to fight back against Cyberattacks", NY Times(July 30, 2016).

못했다는 비판에 직면하였다.

나. 정책과 제도

트럼프 정부는 우선 사이버위협을 적극적으로 감경시키기 위해 사이버사령부를 연합전투사령부(Unified Combatant Command)로 격상시켰다. 사이버사령부의 지위 격상으로 사이버사령관과 국방부 장관 사이의 직접적인 통신선을 구축되었고, 사이버사령부는 미국 전략사령부나 유럽사령부 등과 같은 동등한 지위를 얻게 되었다.

이후 2018년 8월, 트럼프 대통령은 사이버 공격이 승인되는 방식을 규제한 오바마 정부의 '대통령 정책 지침 제20호'를 폐지하였다. 따라서 사이버사령관의 판단으로 수행할 수 있도록 한 사이버공격을 대통령의 승인이 있어야 가능한 것으로 만들었다. 사실 사이버사령관의 단독 판단으로 사이버공격을 감행하는 것은 현실적으로 상당한 부담이 있어 실제 사이버공격을 감행하는 것이 곤란하였다. 오히려 대통령의 승인을 얻어 사이버공격을 감행할 수 있는 현실적인 방안을 마련함으로써 보복적이고 공세적인 사이버 작전이 가능하게 되었다.

트럼프 정부에서 미 국무부는 2018년 5월에 '사이버 위협으로부터 적을 억지하고 미국인을 보호하기 위한 대통령 권고안(Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats)'을 발표하였다. 위 대통령 권고안은 사이버 공간에서 사이버위협을 감경시키기 위해서는 기존의 네트워크 방어만으로는 충분하지 못하다고 하였다. 따라서 이 권고안은 미국이 '무력사용의 문턱' 이하로 국가 및 비국가 행위자에게 부과할 수 있는 다양한 결과(consequences)를 개발하도록 권고하였다. 이를 위한 책임귀속 및 강압성의 신뢰성과 관련하여, 이 권고안은 미국으로 하여금 적들에게 신속하고, 비용을 부과하며, 명백한 결과를 보여줌으로써 위협을 식별하는 능력을 공개적으로 보여줄 것을 요구하였다.

2018년 9월 발행된 국방부의 '새로운 사이버 전략(DoD's new Cyber Strategy)'은 선제적 방어(defend forward) 개념을 제시하고 이에 필요한 군사적 사이버 역량을 확충하고 선제적 작전(pre-emptive operations)을 수행하며, 전쟁 대비 및 사이버 정보 수집을 실시할 것임을 특정 적대국들에게 선포하였다. 선제적 방어라는 것은 적대국의 공격을 차단·종료시키기 위해 적대국의 위협이 목표 대상에 도달하기 전에 위협을 차단하기 위하여 미국의 역량을 외부로 집중하는 것'을 의미한다.

이러한 기조 속에서 비국가 행위자들에 대해서도 사이버 처벌(cyber punishment)과 사이버 공세(cyber offense)의 수행도 고려되었다. 사이버 공격과 범죄의 피해자, 즉 기업, 기관, NGO, 개인들로 하여금 가해자에 대해 '적극적 방어(active defense)'를 통해 '반격'하거나 반격할 수 있도록 하자는 것이다. 미국 컴퓨터사기남용법(Computer Fraud and Abuse Act)에 따르면, 개인이 다른 사람의 컴퓨터 시스템에 무단 침입하는 것은 불법이다. 구글과 마이크로소프트를 포함한 몇몇 미국 기업들은 우려를 표명했지만, 미 의회는 '적극적 사이버 방어 확실성 법안(the Active Cyber Defense Certainty Act)'에서[39] 적극적 방어를 위해 CFAA의 예외를 규정하였다. 이에 따라 미국 주요 은행이나 일부 기업들이 자사의 서버·데이터·자산 보호를 위해 반격 해킹의 효용성을 검토한 것으로 알려졌다.[40]

---

39) 이 법안은 2017년 3월에 처음으로 제안되었다.

40) Dan Lohrmann, "Hack Back Law", Government Technology(September 2017); Nicholas Schmidle, "The Digital Vigilantes who Hack Back", New Yorker(May 7, 2018).

한편 트럼프 정부는 다자주의와 특히 유엔(UN)에 대한 불신으로 글로벌 사이버 규범 확립에 대한 역할을 경시하였다. 대신 특정 국가 및 국가 그룹들과 양자 사이버 관계를 모색하였다. 즉 트럼프 정부는 국무부의 사이버조정관실을 폐쇄해 UN 협상에서 미국의 역할을 약화시켰지만, 2018년 10월 미국 동맹국들과의 장관급 회담 후속 조치로 규범 형성 과정을 재개하였다.[41] 이는 미국이 사이버 규범을 위반하는 자들에게 책임을 물어야 하지만 UN을 통해 사이버 규범을 정립하고 책임을 귀속시킬 수 있는지에 대해서는 회의를 가지고 있었기 때문인 것으로 보인다. 따라서 유사입장 국가들과의 협력이라는 구조틀 속에서 사이버공격에 대한 결과를 부과할 수 있는 옵션을 개발하여야 한다고 강조하고 있다.[42] 이러한 맥락에서 미국은 영국, 독일 등 북대서양조약기구(NATO) 동맹국과 손잡고 2019년 사이버전쟁 원칙을 수립한 것으로 보인다.[43]

2018년 8월, 의회는 러시아, 중국, 북한, 이란의 미국 선거에 대한 방해에 관하여 사이버 공간에서 군사적으로 방위하는 것을 승인했다. 이들 국가는 미국의 선거나 민주적인 정치 과정에 영향을 미치기 위하여 사이버 공간에서 미국 정부와 미국인을 적극적이고 조직적으로 공격하고 있다는 결정하면서 의회는 대통령과 국방장관에게 적절하고 비례적인 조치(action)를 통하여 사이버공간에서의 이러한 공격을 방해, 패퇴 및 억지하도록 하였다.[44]

트럼프 정부는 2018년 9월 〈국가사이버안보전략(National Cybersecurity Strategy)〉을 발표하였다. 이 사이버안보전략은 위 국가안보전략을 발전시켜 사이버공간에서의 연방 네트워크와 정보에 대한 보안을 강조하고 주요기반시설에 대한 보호는 물론 사이버범죄 및 침해사고 대응체계를 개선할 것이라고 하였다. 이 전략은 사이버공간에서의 디지털 경제 활성화와 회복력 강화를 강조하였으며 사이버공간을 통한 지적재산권 침해에 대해 적극적으로 대응할 것이라고 하였다. 사이버공간에서의 국가 책임을 인정하는 규범을 통해 사이버 공간의 안전성을 확보하겠다고 하였다. 또한 사이버공간에서의 비상식적 행위를 억지하고 해당 행위에 대한 책임귀속을 강화할 것이라고 발표하였다. 특히 이 전략에서 트럼프 대통령은 "미국에 대한 악의적 사이버 활동의 방지, 대응, 억지를 위해 물리적 및 사이버(both kinetic and cyber) 군사력을 포함한 국가 권력의 모든 수단을 사용할 것"이라고 하였다. 트럼프 대통령은 비슷한 시기 '미국 사이버작전 정책(United States Cyber Operation Policy)'을 '대통령 국가안보 훈령 제13호(National Security Presidential Memorandum 13)'로 발표하였다. 이 훈령은 국방부 장관에게 시간적으로 중요한 사이버공간에서의 군사 작전을 수행하는 명확한 권한을 위임하고 있다.[45]

미 국방부는 2018년 9월 〈국방사이버전략(DOD Cyber Strategy)〉을 발표하였다. 미국 내 네트워크에 대한 방어에 집중하였던 기존의 국방 사이버전략과는 달리 2018년 국방사이버전략은 국방부가 악의적 사이버 활동과 그 원천을 방해 또는 중지하기 위해 무력분쟁(armed conflict) 수준 이하의 행동을 포함하는 선제적 방어(defend forward)를 수행할 것이라고 하였다.[46] 따라서 미국은 선제적 방어를 통해 적들의 활동이나 행동이 의도한 목표물에 영향을 미치

41) Sean Lyngaas, "US Looks to Restart Talks on Global Cyber Norms", CyberScoop(October 2018).
42) The White House, "Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week 2017"(June 26, 2017).
43) Robin Emmott, "NATO mulls "Offensive Defense" with Cyber Warfare Rules", Reuters(November 30, 2017).
44) National Defense Authorization Act for Fiscal Year 2018, §§ 1636, 1642.
45) US Department of Defense, "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference," Remarks by. Hon. Paul Ney, Jr. (March 2, 2020), https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conf (accessed: December 27, 2023)
46) Ibid.

기 전에 관여하여야 한다고 하였다.[47] 이는 미국이 러시아와 중국과의 장기적인 전략경쟁에 관여되었다는 인식에 기초한 것으로 보인다. 또한 사이버공간은 미국에 장기적인 전략적 위험을 야기할 수 있다고 인식함은 물론 사이버공간을 통한 지속적인 군사행동이 이루어지고 있다고 인식에 바타을 둔 것으로 보인다. 따라서 국방부는 일상의 경쟁이 지속되는 사이버공간에서 미국의 이익을 방위하기 위하여 조치를 취하여야 한다고 하였다.[48]

다. 법제의 정비

1) 2019년도 미 국방수권법

2017년 12월 발표된 트럼프 정부의 〈국가안보전략(National Security Strategy)〉을 현실화하는데 필요한 국방 예산을 확정한 「2019회계년도 국방수권법(the Fiscal Year 2019 National Defense Authorization Act)」은 힘과 新기술에 기초하여 국가안보전략에서 문제 삼은 4개 국가(러시아, 중국, 북한, 이란)에 대한 적극적 견제와 억지를 구체화하였다. 이와 같은 기조에서 국방수권법은 국방부로 하여금 사이버전쟁 및 전자전 전략 개발은 물론 역량강화 실행과 관련된 동시적이고 통합된 노력을 다하도록 요구하고 있다. 또한 적대국에 의한 사이버공격에 대하여 적극적이고 체계적이며 즉각적인 대응이 가능하도록 사이버방어를 강화하도록 하였다. 아울러 사이버사령부, 사이버 군부대 및 사이버 전쟁 수단과 역량 강화를 최우선과제로 제시하였다. 특히 주요기반시설 및 네트워크 방어 강화를 위해 국방부와 국토안보부의 협력을 강화하는 기구 설치를 규정하였다. 아울러 사이버공격으로부터 국방 네트워크, 무기체계, 보급망 등에 대한 국방부의 회복력을 강화하도록 하였다. 이 법은 국방장관으로 하여금 사이버공간에서의 은밀한 군사작전과 군사활동을 전개할 수 있도록 승인하였다. 또한 미국을 대상으로 하는 악의적 사이버 활동을 탐지하고 대응하기 위하여 사이버공간, 사이버안보, 사이버전쟁 및 사이버억지 등 관련 정책을 체계화하도록 하였다.

2) 2021년도 미 국방수권법

미 트럼프 대통령은 2020년 12월 23일 「2021회계년도 국방수권법(National Defense Authorization Act for Fiscal Year 2021)」에 대해 거부권을 행사하였다. 트럼프 대통령은 이 법에 대해 중요한 국가안보조치를 반영하지 못하고 있으며 국가안보와 외교정책에 있어 미국 우선주의에 반하는 중국과 러시아에 대한 선물이라고 비난하면서 거부권을 행사하였다. 그렇지만 미 하원은 2020년 12월 28일에 미 상원은 2021년 1월 1일에 동 법안을 재의결하여 최종 통과시켰다. 이 국방수권법은 솔라리움 위원회(Cyberspace Solarium Commission)가 제안한 여러 권고 가운데 약 26개 사항을 규정하고 있다.[49] 또한 동 위원회의 활동을 연장하였다.

이 법률은 상원이 승인한 국가사이버국장(NCD)을 백악관 내에 두도록 규정함으로써 사이버안보 거버넌스 체계를 재구축하였다. 국가사이버국장은 사이버안보에 관한 백악관 내부의 소통

47) Ibid.
48) US Department of Defense, “SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY,” (2018) https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF(accessed: December 27, 2023).
49) https://www.solarium.gov/report(accessed: December 27, 2023).

창구인 동시에 민간 부문과의 연결고리로서의 역할을 수행하여야 한다. 국가사이버국장은 상원의 임명 동의를 받아야 하며[50], 국가안전보장회의(NSC)의 구성원이 된다.[51]

2021 국방수권법에 따라 미 국방부는 주요 국가사이버긴급사태가 발생하는 경우 전문성과 능력 부족을 메우기 위하여 군, 민간 또는 군과 민간 혼합 사이버예비군의 모델과 필요성 등에 대한 평가를 수행하여야 한다.[52] 2021년도 국방수권법에 따라 CISA 국장은 해당 직원을 미국 각 주(州)의 사이버안보조정관(Cybersecurity State Coordinator)으로 임명하여야 한다.

4. 확산의 심화: 사이버안보의 진영화: 바이든 정부

가. 개요

트럼프 정부는 선제적 방어에 기초하여 사이버위협을 차단함으로써 사이버보안의 문제가 사이버안보의 문제로 안보화 과정이 확산되는 것을 차단하고자 하였다. 그렇지만 트럼프 정부 말기부터 바이든 정부의 초기에 걸쳐 진행된 솔라윈즈 사이버보안 사태, 콜로니얼 파이프라인 사건 등은 사이버위험이 양질전환과 이슈연계를 통해 국제적 안보의 문제로 더욱 확산되었음을 보여준다. 더구나 러시아의 선거개입과 코로나 상황에서 중국의 미국 의료기술을 포함한 신기술탈취를 위한 사이버공격이 지속됨에 따라 사이버안보 문제는 국가안보의 최우선 순위를 차지하게 되었다.

그럼에도 불구하고 바이든 정부는 사이버위험의 안보화를 차단 또는 감경시키기 위하여 사이버위협을 감경시키고 취약성을 감소시키며 결과발생의 방지 즉 회복력 강화를 위한 법제도(거버넌스) 정비와 개선을 지속하고 있다. 우선 사이버위협 대응과 관련하여 바이든 정부는 트럼프 정부의 선제적 방어 전략을 계승하고 있다고 볼 수 있다. 바이든 정부가 말하는 미국의 귀환은 미국 우선주의 하에 정립된 트럼프의 사이버위협 감경 법제도를 계승하면서 중국이나 러시아 등 권위주의 국가들에 대해 민주주의 가치를 근거로 동맹국들과 협력하여 보다 강력하게 대응할 것임을 시사하고 있기 때문이다. 이에 바이든 정부는 유사입장 국가(likeminded countries)들과 더불어 사이버공격을 이유로 한 경제제재(cybersanction)와 책임귀속(attribution)의 실질적 작동을 강화시키고자 하였다.

그렇지만 코로나19에 따른 공급망의 붕괴와 솔라윈즈 사테에 따른 공급망 사이버안보 문제는 사이버위협 감경 중심의 법제화(거버넌스) 구조에 대한 수정을 요구하게 되었다. 이러한 점에서 바이든 정부와 트럼프 정부의 사이버 문제의 안보화 차단을 위한 법제도 정비에 있어 가장 큰 차이점은 취약성 감소를 통한 사이버위험 감소에 있다고 할 것이다. 이는 바이든 정부의 출범 전후 러시아로부터 솔라윈스 제품의 취약성을 이용한 사이버공격 사태로 인하여 미국이 심각한 피해를 경험한 바에 따른 것으로 보인다. 즉 코로나19로 정보통신(ICT) 및 사이버안보 관련 하드웨어나 소프트웨어에 대한 공급망 확보와 그 안전성 담보는 주요한 사이버안보 문제가 되었다. 미국은 SolarWinds 제품을 사용한 18,000여 개의 연방 부처와 민간 기업 등의 시스템과 네트워크가 동 제품에 탑재된 악성코드에 의한 해킹 공격을 당하였다. 이에 따라 바이든 정부는 사이버위험 감소를 위한 취약성 감경에 있어 공급망 사이버보안에 특히 집중하고 있는 것으로 보인다. 물론 이는 바이든 정부의 미국 중심 공급망 구축 전략과도 연계되어 있다.

50) NDAA 2021 Section 1752(d).
51) NDAA 2021 Section 1752(b)(1).
52) NDAA 2021 Section 1730(b)(2).

미국 중심 공급망 구축과 그에 따른 사이버보안을 확보하기 위해서는 민관협력이 무엇보다도 중요하다. 따라서 바이든 정부는 2023년 3월 발표된 사이버안보전략을 통해 사이버위협 대응을 위한 선제적 방어 전략의 실행보다는 민관협력을 통해 취약성을 감소시키고 회복력을 강화하는 방안으로 전략의 중심축을 이동한 것으로 보인다.

그렇지만 이러한 바이든 정부의 사이버안보 법제도(거버넌스)는 시장에 대한 보다 적극적인 개입을 의미하고 있다. 따라서 시장에 대한 국가의 보다 적극적인 개입에 따라 생성되는 비효율과 비용을 누구부담할 것인지가 과제로 남는다. 바이든 정부가 트럼프 정부 보다 동맹국과 파트너 국가들과의 협력을 더욱 강조하고 있는데 이는 사이버안보를 위한 시장개입에 따른 비용을 이들에게 전가시키고자 하는 전략으로 보인다.

나. 정책과 제도

미국 바이든 대통령은 2022년 1월 19일 '국가안보, 국방 및 정보공동체의 서이버안보 향상을 위한 지침(Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems)'을 발령하였다. 이에 따라 국가안보국(NSA)의 장은 국가안보시스템에 대한 안정성 확보를 위하여 위 대통령 행정명령에서 정한 것 이상의 권한과 책임을 부여받는다. 동 지침은 국가안보시스템에 대해 연방정보시스템에 요구되는 사이버보안 요건과 동등하거나 그 이상의 요건을 확보하도록 규정하고, 국가안보시스템 고유의 필요성에 대처하기 위한 사항을 실행하도록 하고 있다. 이에 따라 국가안보시스템을 보유 또는 운용하는 각 부처의 장관은 이 지침 시행일로부터 60일 이내에 신뢰 제로(Zero Trust) 아키텍처를 구축하여야 한다. 또한 90일 이내에 국가안보시스탬의 클라우드 이행과 운용에 있어 최소한의 보안 기준과 관리 가이던스를 정립하고 공포하여야 한다.[53]

미국 바이든 정부는 2023년 3월 2일 「국가사이버안보전략(National Cybersecurity Strategy)」을 발표하였다. 이 전략을 통해 바이든 정부는 사이버안보에 있어 컴퓨터와 네트워크에 대한 사이버보안보다는 디지털 경제의 안전성 강화와 신기술 보호로 중심축을 이동시켰다. 다시 말해 공급망 보호, 경제에 타격을 가하고 있는 램섬웨어 대응, 사이버공간을 통한 신기술 탈취의 방지에 중점을 둔 것이다. 이는 동 전략이 디지털 생태계(digital ecosystem)[54]라는 용어를 처음으로 사용하면서 전략의 곳곳에서 강조하고 있는 것을 통해 확인할 수 있다. 아울러 모든 미국인들을 위해 디지털 생태계의 안전성과 보안성 확보를 위하여 동 전략을 발표한다는 바이든 정부의 통지문[55]도 이러한 사실을 의미하는 것으로 볼 수 있다.

이와 같이 디지털 경제와 신기술 보호를 위한 분야로 방향을 전환함에 따라 동 전략은 사이버안보에 있어 민간 주도와 민관협력을 강조하고 있다. 디지털 경제와 신기술 보호에 집중하다

---

53) https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/ (accessed: December 27, 2023)

54) 디지털 생태계는 바이든 정부의 국가사이버안보전략에서 처음으로 사용되고 있으며 전략 곳곳에 핵심 용어로 활용되고 있다. 이에 반해 트럼프 정부의 국가사이버안보전략은 기술적 생태계(technological ecosystem), 생태계의 폭(breadth of the ecosystem), 사이버 생태계(the cyber ecosystem) 등 생태계란 용어를 단 3번 사용했을 뿐이다.

55) The White House, FACT SHEET: Biden-Haris Administration Announces National Cybersecurity Strategy(March 2, 2023). https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/ (accessed: December 27, 2023)

보니 사이버위협 인식에 있어서도 러시아보다는 중국의 위협을 강조하고 있으며 북한이 사이버 공간에서의 감행하고 있는 범죄활동에 대해 인식을 강화하고 있다.

동 전략은 디지털 경제의 안전성 강화와 신기술 경쟁력 확보를 중심으로 사이버위협에 대응하기 위하여 미국 내부의 역량 강화와 회복력 증진을 강조하고 있다. 이는 바이든 정부 이후 발생한 솔라윈즈 사건, 마이크로소프트 이메일 사건, 콜로니얼 파이프라인을 비롯한 수많은 랜섬웨어 공격 등으로 인하여 미국이 실제 국내적으로 심각한 사이버공격의 피해를 경험하였기 때문인 것으로 보인다. 즉 취약성 감소와 회복력 강화를 통해 사이버공격을 감내하여 공격자들로 하여금 비용을 부담하도록 하겠다는 것이다. 사이버공격자들에 대한 선제적 방어 등 군사적 수단의 행사는 자제하고 자국 네트워크와 시스템 보안을 강화하고 공급망 안정성을 보장하여 신기술 경쟁에 대비하는 데에 중점을 둔 것으로 분석된다.

동 전략은 사이버공간에서의 회복력 강화를 접근법으로 제시하면서 디지털 생태계에 참여하는 공공, 민간 기업, 시민사회, 동맹국과 파트너국가들의 전례없는 협력을 강조하고 있다. 동 전략은 사이버공간의 안전성 확보를 위해 국가 주도가 아닌 민간주도로의 정책적 방향 전환을 제시한 것으로 보인다. 디지털 생태계의 보호와 회복력 강화를 위해서는 무엇보다도 민관협력이 강화되어야 함을 강조한 것이다. 그렇지만 정부는 정부 시스템의 보안 강화, 민간 기업 특히 주요기반시설 소유자와 운영자의 시스템 보안 지원은 물론, 외교, 정보활동, 경제제재 부과, 법집행, 사이버위협에 대한 와해 활동(disruptive actions)을 수행하는 것으로 규정하고 있어 시장에 대한 다양한 개입 수단을 사용할 것임을 규정하고 있다.

또한 동 전략은 미래 디지털 시스템 보호와 회복력 강화를 위한 투자 확대를 제시하였다. 투자에 있어서도 민간과 공공 프로그램이 사이버보안과 회복력을 강화하는 경우 보상을 제공하고, 민간과 공공이 건전하고 다양한 사이버인력을 양성하도록 하였다. 사이버안보에 대한 연구개발 투자를 전략적으로 확대하여 회복력을 강화하고, 디지털 생태계를 종합적으로 관리할 것이라고 하였다. 한편 연방 정부는 주요기반시설 개선, 에너지시스템의 디지털화와 탈탄소화, 반도체 공급망의 안전성 확보, 암호기술의 현대화, 외교정책의 개편 등에 투자할 것이라고 언급하였다.

동 전략은 사이버공격을 감행한 해커 조직과 집단 또는 국가에 대하여 사이버 억지(deterrence), 책임귀속(attribution) 등에 기초하여 군사적 수단을 활용한 대응 보다는 민관협력을 통한 대응과 회복력 강화를 강조하였다. 트럼프 정부에서 발표한 「국가사이버안보전략」에서는 사이버 억지와 책임귀속을 전체적으로 사용하면서 러시아, 중국, 이란, 북한 등을 압박하였다면, 바이든 정부는 책임귀속에 대해 두 번만 언급하였다. 이 가운데 국제사회와의 협력을 통해 '합의된 책임귀속 성명(to produce coordinated statement of attribution)을 생성'한다는 언급만이 유의미하다. 따라서 선제적 방어 등 군사력을 이용하여 사이버위협을 감경시키는 정책적 수단의 선택을 자제될 것으로 보인다. 동 전략이 언급하고 있는 해커 조직의 와해와 해체도 특정 국가에 대한 전면적 사이버반격을 의미하는 것이 아니라 디지털 생태계를 교란하여 디지털 경제와 공급망을 위협하거나 신기술을 탈취하는 사이버범죄자를 소탕한다는 측면이 강하다고 보인다.

바이든 정부가 발표한 「국가사이버안보전략」의 가장 큰 특징 중에 하나는 중국의 사이버위협에 대한 인식의 변화라고 생각된다. 트럼프 정부가 사이버위협 국가로서 러시아, 중국, 이란, 북한 등으로 지목하였다면 바이든 정부는 중국을 가장 큰 사이버위협 국가로 인식하여 중국, 러시아, 이란, 북한 순으로 표기하였다. 트럼프 정부는 중국에 대하여 사이버에 기초한 경제적 정보수집에 치중하고 있다는 점만을 부각하였다. 하지만 바이든 정부는 중국이 국제 질서의 재형성은 물론, 경제, 외교, 군사 및 기술 권력에 있어 미국에 대응하고자 하는 의도를 가지고 미국 정부와 민간 네트워크에 대해 지속적으로 위협하고 있다고 지적하였다. 이는 사이버공간에서도 미중 경

쟁이 심화되고 있으며 사이버안보 문제를 진영화를 통해 해결하고자 하는 의지로 보인다. 이러한 사실은 바이든 정부가 북한이 핵개발을 지원하기 위하여 암호화폐 탈취, 램섬웨어, 정보통신기술자의 파견 등 범죄적 수익을 창출하기 위한 사이버활동을 수행하고 있다고 규정한 것을 통하여도 알 수 있다.

이와 같은 사이버안보의 진영화를 기반으로 동 전략은 대외적으로는 가치 공유에 기초한 진영 내부의 협력을 통해 사이버위협에 강력히 대응할 것이라고 하였다. 이는 QUAD, AUKUS 인·태 지역의 안보협력체를 통한 대응 강화를 강조한 것을 통해 확인할 수 있다. 즉 QUAD와는 가치 공유에 기반한 디지털 환경의 발전과 컴퓨터긴급대응팀 사이의 정보공유 강화를 모색하고, AUKUS를 통해서는 핵심 기술의 보호, 사이버 조정 능력의 향상 및 선진 역량의 공유 등의 협력을 강화할 것임을 강조하였다. 아울러 IPEF, APEC 등과의 협력을 통해 공급망과 경제안보를 위한 사이버안보 협력을 강조하였다. 즉 프라이버시 보호에 기초하여 역외 데이터 이전을 활성화하고 공급망과 회복력 강화를 위해 IPEF, APEC 등과의 협력을 강화할 것임을 천명한 것이다.

다. 법제

1) 공급망 사이버보안 강화

바이든 미국 대통령은 2021년 5월 12일 “국가 사이버안보 향상 행정명령(Executive Order on Improving the Nation’s Cybersecurity)”을 발동하였다.[56] 이 행정명령은 SolarWinds와 마이크로소프트 이메일 해킹 공격 및 콜로니얼 파이프라인 렌섬웨어 공격에 따른 연방정부 네트워크 보안과 소프트웨어 공급망에 대한 보안을 강화하기 위한 것이다. 동 행정명령은 침입 예방(preventing intrusion), 침입에 따른 영향력 최소화(사전 탐지)(minimizing impact of intrusion(pre-detection), 침입 탐지와 대응(detecting and responding intrusion), 침입에 따른 학습과 공유(Learning and disseminating) lessons from intrusion) 등으로 구성되어 있다. 동 행정명령은 1) 연방부서와 유관 기관의 개선 2) 정부에 소프트웨어를 판매하는 계약업자들의 필수 보안 기준 3) 정보침해 사례에 대한 보고서 작성과 기관조사에 적극적으로 협조할 것을 의무사항으로 하는 보안조치를 포함하고 있다.[57][58]

이 행정명령에 따라 미국 연방 정부부처는 데이터를 암호화하여야 하며 클라우드 호스팅 서비스의 안전한 사용에 대한 계획을 업데이트 하고, 다중 인증 체계를 구현하여야 한다.[59] 또한 연방 정부부처들은 잠재적 사이버공격을 탐지한 경우 경고를 발령하도록 하는 ‘종점탐지대응소프트

56) The White House, Executive Order on Improving the Nation’s Cybersecurity, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (accessed: December 27, 2023)

57) Robert Chesney and Trey Herr, “Everything You Need to Know about the New Executive Order on Cybersecurity”, LAWFARE (2021. 05. 13), https://www.lawfareblog.com/everything-you-need-know-about-new-executive-order-cybersecurity (accessed: December 27, 2023)

58) Walter Haydock, “The Biden Administration’s Impending Executive Order on Software Security”, LAWFARE (2021. 04. 23), https://www.lawfareblog.com/biden-administrations-impending-executive-order-software-security (accessed: December 27, 2023)

59) Eric Geller, “Biden orders federal cyber upgrade after barrage on hacks”, *POLITICO* (2021. 5. 12), https://www.politico.com/news/2021/05/12/biden-federal-cyber-upgrade-hacks-487731 (accessed: December 27, 2023).

웨어(endpoint detection and response software)'를 설치하여야 한다. 아울러 연방 정부부처들은 신뢰-제로구조를 사용하여 자신들의 네트워크에 해커가 침입한 것으로 가정하고 해커들이 내부 시스템을 해집고 돌아다니지 못하도록 네트워크를 재설계하여야 한다. 또한 이 명령에 따라 연방 정부부처들은 아마존 웹 서비스(Amazon Web Services)와 같은 클라우드 컴퓨팅을 위한 정부의 시장인 페드 램프(Fed RAMP)를 활성화하여 사이버안보를 강화하여야 한다. 또한 연방 클라우드 안보 전략을 제정하여 연방 부처들이 데이터를 안전하게 클라우드로 전송하도록 하여야 한다.

이 행정명령은 국토안보부 사이버안보기반보호국(CISA)으로 하여금 다른 부처의 보안 데이터에, 필요한 경우 CISA가 접근할 수 있도록 보장하는 모니터링 소프트웨어를 해당 부처의 네트워크에 설치하도록 하는 협정을 체결하고 검토하도록 하였다. 또한 이 행정명령은 CISA에 대하여 2021년 국방수권법에 의하여 부여받은 권한에 따라 다른 부처의 네트워크를 사전 승인 없이 점검한 경우 이를 보고하도록 하였다.

또한 이 행정명령은 항공기나 철도 및 차량의 충돌을 조사하는 '국가교통안전국(National Transportation Safety Board)'을 모델로 하여 사이버안보 관련 사고를 조사할 '사이버침해사고조사단'을 설립하도록 하였다. 아울러 연방 정부와 거래하는 계약자(contractor)들에 대하여 데이터 유출시 보고하도록 하고 새로운 소프트웨어 보안 기준을 충족시키도록 하였다.

이 행정명령에 따라 연방정부와 거래한 판매업자들이 확인된 데이터 위반 사례들을 적극적으로 보고하여야 한다. 또한 침해사고가 발생한 경우, FBI와 CISA가 피해를 당한 기관들에 대한 조사를 수행하는데 있어 민간부문은 의무적으로 협조하여야 한다. 정부와 소프트웨어 공급업체 사이의 이러한 요구사항이 추가되는 것은 정당한 것으로 보이며, 민간 기업들 사이에서는 이러한 계약의무조항들이 이미 널리 사용되고 있다.

미 하원은 2021년 10월 20일 '2021년 국토안보부 소프트웨어 공급망 리스크 관리법안(DHS Software Supply Chain Risk Management Act of 2021)'을 가결하였다. 이 법안은 소프트웨어 공급망 위험 관리를 강화하는 것으로 바이든 대통령이 5월 12일 발표한 '국가 사이버안보 향상 행정명령'에 기초하고 있으며 솔라윈즈 사태과 같은 사고의 재발을 막는 것이 목적이다. 법안이 통과될 경우, DHS의 계약업체는 납품하려는 소프트웨어를 목록화 한 소프트웨어 부품표(SBOM), 기존 취약성 대응 현황, 신규 취약성에 대한 대응·복구 계획 등을 의무적으로 제출하여야 한다.[60]

2) 기반시설 보호 등 회복력과 역량 강화

2021년 11월 15일 바이든 대통령은 5,500억 달러 규모의 기반시설투자 및 직업법안에 서명하였다. 이 법은 미국의 기반시설을 현대화하기 위한 것으로 14억9000만 달러 이상의 자금 배정을 포함하여 사이버안보 개선을 위한 내용을 규정하고 있다. 이 법은 사이버안보 위험 평가, 사이버 전문가 양성 및 전력, 수자원 등 주요 기반시설에 대한 사이버보안 강화 등을 위한 프로그램을 규정하고 있다. 주요 기반시설에 대한 사이버보안을 강화하기 위하여 이 법은 민간부문의 협력을 유인하고 국가사이버국장(National Cyber Director)에게 자금을 제공하며 국토안보부(DHS)로 하여금 주요 사이버 침해사고의 공표와 전문가 및 자금의 분배에 관한 권한을 부여하

60) https://ritchietorres.house.gov/posts/rep-torress-software-dhs-supply-chain-risk-management-act-of-2021-passes-u-s-house-of-representatives(accessed: December 27, 2023)

였다. 또한, 10억 달러를 출연하여 미국의 모든 주, 지방, 인디언 보호구역의 사이버보안 인프라를 강화하는 프로그램을 설립하도록 하였다.[61]

바이든 대통령은 2021년 12월 27일 「2022 회계연도 국방수권법(NDAA)」에 서명하고 7700억 달러의 지출을 승인하였다. 동 법은 사이버안보 정책과 관련하여 민간 부문과의 협력을 확대하고, 미국의 현재 사이버안보 상태에 대해 조사하며, 사이버 인력 개선 및 국방부의 사이버 인프로 표준을 업그레이드할 것을 규정하고 있다.[62] 이 법은 민간 부문과의 협력을 위하여 CISA의 사이버센트리(CyberSentry) 프로그램을 확대하도록 입법화하였다. 이 프로그램은 해킹을 선제적으로 대응하기 위하여 주요기반시설과 민간 기업 사이의 온라인 트래픽을 적극적으로 모니터링 하는 활동이다. 또한 이 법은 사이버공격에 대응하기 위하여 민간 부문과 미 사이버사령부 사이의 자발적 협력을 위한 프로그램을 정립하도록 하였으며, 국방부로 하여금 CISA와 협력하여 민간 기업들을 지원하도록 하였다.

이 법은 미국의 사이버 능력(American cyber power), 미국 사이버 역량, 사이버안보 취약성에 대한 평가와 미국의 적성국들이 이를 식별함으로 인하여 받을 수 있는 이익에 대한 평가 등 미국의 현재 사이버 상태에 관하여 다수의 보고서를 작성하도록 하였다. 또한 사이버사령관으로 하여금 이러한 보고서에서 발견된 사항을 반영하여 보다 정교한 사이버 전략을 수립하도록 하고 이에 필요한 기획, 프로그램 및 예산 권한을 부여하였다.

국방부 사이버 인재 육성을 위해, 이 법은 주방위군(National Guard)을 위한 사이버보안 훈련 프로그램을 확대하고, 사이버에 특화된 학생들을 학부 과정에서부터 채용하고 교수를 자문단으로 고용하는 등 학계와의 연계를 강화하도록 하였다. 또한 기존 국방부의 군인 및 민간 사이버 요원의 채용과 역량 강화에 대해 점검하도록 하였다. 아울러 이 법은 사이버 침해사고가 발생한 경우 정부와 시민 사회가 총력으로 대응하도록 하는 새로운 국가 사이버 훈련 프로그램을 창설하도록 하였다.

마지막으로 이 법은 사이버 및 데이터 제품 획득에 있어 기업 마인드에 입각한 점검 프로그램을 정립하고, 군에 있어 불필요한 기존 소프트웨어 시스템을 과감히 제거하는 노력을 개시하며, 국방부 전반에 걸쳐 신뢰 제로(Zero Trust)를 적용한 보고서를 작성하도록 하였다. 또한 이 법은 국방부의 사이버안보 절차를 개선하기 위한 각종 새로운 프로그램과 보고서 작성 등을 규정하고 있다.

미 상원은 2022년 3월 1일 “미국사이버안보강화법(the Strengthening American Cybersecurity Act: SACA)에 대해 만장일치로 통과시켰다.[63] SACA는 2022년 2월 △주요기반시설 운영자들에 대해 사이버공격 사례에 대한 보고의무를 규정하고, △연방 부처의 정보보안을 강화하며, △연방 부처에 대해 클라우드 기반 기술의 조달을 보장하는 등 3개의 법안을 SACA로 패키지한 입법 형식으로 상원에 제출하였다.[64]

---

61) https://www.congress.gov/bill/117th-congress/house-bill/3684?q=%7B%22search%22%3A%5B%22cyber%22%2C%22cyber%22%5D%7D&s=3&r=2(accessed: December 27, 2023)

62) https://rules.house.gov/sites/democrats.rules.house.gov/(accessed: December 27, 2023)

63) Ines Kagubare, “Senate passes cybersecurity bill amid fears of Russian cyberattacks”, THE HILL(March 2, 2022), https://thehill.com/policy/cybersecurity/596628-senate-passes-cybersecurity-bill-amid-fears-of-russian-cyberattacks (accessed: October 3, 2023).

64) John Curran, “Senate Approves FISMA, FedRAMP, Cyber Incident Reporting Legislation” MeriTalk(March 2, 2022), https://www.meritalk.com/articles/senate-approves-fisma-fedramp-cyber-incident-reporting-legislation/(access

‘2022년 주요기반시설 사이버 침해사고 보고법(the Cyber Incident Reporting for Critical Infrastructure Act of 2022: CIRCIA)’은 주요기반시설운영자에 대하여 사이버공격이 발행한 후 72시간 이내에 CISA에 보고하는 의무 등을 규정하였다.[65] 연방정보보안현대화법(Federal Information Security Modernisation Act of 2022: FISMA 2022) 연방 부처의 정보보안 관리를 보다 강화하였다. ‘연방 클라우드 개선과 일자리 보장법(Federal Secure Improvement and Jobs Act of 2022: FSCIJ)은 연방 조달청의 연방위험인증관리프로그램(Federal Risk and Authorization Management Program: FedRAMP)을 승인하였다.

동 법안의 통과로 미국 사이버안보 당국의 숙원 사업 가운데 하나였던 주요기반시설 운영자들의 침해사고 보고 의무의 법률상 강제가 가능하게 되었다. 민간이 대부분인 미국의 주요기반시설 운영자들은 기업의 영업기밀 유출, 주식가치 하락, 평판 침해 등을 이유로 사이버 침해사고에 대한 의무적 보고에 반대하였다.[66]

Ⅳ. 결론

시장을 통한 사이버 위험분배의 실패는 정부에 의한 시장개입을 요구하고 있다. 민주주의와 시장경제 체제하에서 국가의 시장 개입은 특별한 경우에 한하여 법적 근거에 기초하여 이루어지고 있다. 국가의 시장 개입이 시장의 자율성을 저해하여 비효율과 비용을 양산할 수 있기 때문이다. 국가는 시장에 개입하여 사이버위험이 이슈연계와 양질전환되어 안보화 과정을 거쳐 사이버안보의 문제로 확산되는 과정을 차단하기 위한 거버넌스 구조를 정립하고자 할 것이다. 이 경우 국가는 위협(threat)과 취약성(vulnerability) 및 결과발생(consequence)을 감소시키거나 제거하기 위한 법제도(거버넌스)를 선택하여 사이버 문제의 안보화 과정의 진행을 연결하는 고리를 차단 또는 저지하고자 할 것이다.

미국의 부시 정부는 사이버 문제를 국가안보 이슈의 하나로 인식하지 못한 상태에서 사이버 문제가 이슈연계나 양질 전환 되지 못하도록 사이버보안의 기반을 형성하는데 중점을 두었다. 즉 주요기반시설에 대한 사이버공격을 예방하고, 취약성을 감소시키며, 사이버공격으로 인한 피해의 감경이라는 목표를 제시한 것이다. 특히 주요 기반시설에 대해 해킹, 바이러스 유포 등 사이버위험이 발생하여 국가의 주요 핵심기능이 마비되는 것을 방지하는데 법제도(거버넌스) 구축을 집중하였다. 다만 부시 정부의 주요기반시설 보호는 911테러 이후 물리적 테러의 가능성을 염두해 두면서 이슈연계를 차단하여 사이위험을 방지하고자 한 것으로 보인다.

오바마 정부는 초기에 사이버위험에 대한 대응에 있어 국가 중심보다는 시장의 자율에 맞기고자 한 것으로 보인다. 그렇지만 소니 해킹 사건을 계기로 사이버위험이 미국 내에서 현실화됨에 따라 보다 적극적인 개입으로 정책 방향을 선회한 것으로 보인다. 오바마 정부는 사이버위협을 감경하기 위한 보다 공세적인 작전이나 적극적인 대응 조치를 전개하지는 않았다. 다만 취약성 감소나 회복력 강화 등을 통해 사이버위험을 감경시키기 위한 기반을 형성하는데 중점을 두었다. 또한 국제협력과 국제규범 정립을 통해 사이버위협 감경을 위한 활동의 효과성과 정당성을 확보

ed: October 3, 2023).

65) https://www.hsgac.senate.gov/media/majority-media/senate-passes-peters-and-portman-landmark-legislative-package-to-strengthen-public-and-private-sector-cybersecurity- (accessed: October 3, 2023).

66) 이에 대한 보다 자세한 내용은 오일석, “사이버 보안 정보공유의 법적 문제점과 입법적 해결방안에 대한 고찰-민사법적 측면의 쟁점을 중심으로”, 『하경효 교수 정년 기념논문집』(서울: 박영사, 2017), pp.459-480 참조.

하여 사이버위험이 안보화 과정으로 확산되는 것을 방지하고자 하였다. 오바마 정부는 사이버 문제가 양질전환과 이슈연계를 통해 안보화의 문제로 확산되는 고리를 차단하기 위한 법제 정비 활동에 있어 회복력 강화에 중점을 둔 것으로 보인다. 이는 특히 결과발생의 방지를 통해 회복력을 강화하기 위하여 정보공유를 법제화한 것을 통하여 알 수 있다. 아울러 사이버위협 감경을 위해 군사적인 활동을 동원하기 보다는 현실적인 방안으로 경제제재를 부과하기 위한 법제를 도입하였다.

트럼프 정부는 이미 안보화 과정을 넘어선 사이버 문제에 대해 사이버위협의 적극적인 감경, 공급망 재편을 통한 취약성의 극복, 효율적이고 탄력적인 회복력의 등을 목적으로 제시하면서 국가의 적극적인 개입을 통해 사이버 위험을 관리하는 방향으로 법제도(거버넌스)를 정비한 것으로 보인다. 트럼프 정부는 중국과 러시아와의 경쟁을 인식하면서 사이버위험 감경을 통해 사이버 문제의 이슈연계와 양질전환을 차단함에 있어 보다 적극적인 개입을 실행하고자 한 것으로 보인다. 특히 위협의 감경을 적극적으로 추진하기 위해 사이버공간에서 무력분쟁(armed conflict) 수준 이하의 행동을 포함하는 선제적 방어(defend forward)를 수행할 것을 천명하였다. 즉 사이버 문제의 안보화 과정 차단을 위하여 취약성 감소와 회복력 강화 보다는 군사력이나 외교력 등을 활용하여 힘에 의한 평화를 강조하면서 위협 경감을 강하게 추진한 것으로 보인다. 이는 트럼프 정부가 사이버사령부를 연합전투사령부로 격상시키고 선제적 방어 개념을 제시한 것을 통하여도 알 수 있다. 트럼프 정부는 사이버 문제의 안보화 과정에 대한 외교적 대응에 있어 다자주의 보다는 특정 국가 및 국가 그룹들과 양자적 사이버 관계를 선호하였다. 동맹국과 파트너국가들의 협력을 강조하면서 이들 국가에 대해 사이버안보에 대한 국가 개입에 따른 비용을 분담할 것을 요구하였다.

바이든 정부는 사이버 문제의 안보화를 차단 또는 감경시키기 위하여 사이버위협을 감경시키고 취약성을 감소시키며 결과발생의 방지 즉 회복력 강화를 위한 법제도(거버넌스) 정비와 개선을 지속하고 있다. 그렇지만 바이든 정부와 트럼프 정부의 사이버 문제의 안보화 차단을 위한 법제도 정비에 있어 가장 큰 차이점은 취약성 감소를 통한 사이버위험 감소에 있다고 할 것이다. 이는 바이든 정부의 출범 전후 러시아로부터 솔라윈스 제품의 취약성을 이용한 사이버공격 사태로 인하여 미국이 심각한 피해를 경험한 바에 따른 것으로 보인다.

바이든 정부는 2023년 3월 발표된 〈국가사이버안보전략〉을 통해 사이버위협 대응을 위한 선제적 방어 전략의 실행보다는 공급망 보안을 중심으로 민관협력을 통해 취약성을 감소시키고 회복력을 강화하는 방향으로 전략의 중심축을 이동한 것으로 보인다. 다시 말해 바이든 정부는 사이버위험 감소를 위한 취약성 감경에 있어 공급망 사이버보안에 특히 집중하고 있는 것으로 보인다. 물론 이는 바이든 정부의 미국 중심 공급망 구축 전략과도 연계되어 있다.

이러한 바이든 정부의 사이버안보 법제도(거버넌스)는 시장에 대한 보다 적극적인 개입을 의미하고 있다. 따라서 시장에 대한 국가의 적극적인 개입에 따라 생성되는 비효율과 비용을 누구부담할 것인지가 과제로 남는다. 바이든 정부가 트럼프 정부 보다 동맹국과 파트너 국가들과의 협력을 더욱 강조하고 있는데 이는 사이버안보를 위한 시장개입에 따른 비용을 이들에게 전가시키고자 하는 전략으로 보인다.

미중 경쟁과 기술발전, 코로나19와 비대면 사회의 가속화, 우크라이나 하이브리드 전쟁 등으로 사이버공간에서도 진영화가 가속화되고 있다. 사이버공간의 진영화에 따라 미국과 서방은 물론 우리 정부도 자유민주적 가치를 사이버공간을 통해 실현하고자 하고 있다. 즉 자유민주적 가치를 중심으로 사이버공간의 진영화를 강화하고 회색의 경쟁 지대인 사이버공간에서 경쟁력 우위를 확보하기 위해 노력하고 있다. 자유민주적 가치를 중심으로 결집한 미국과 서방 및 우리는

사이버안보 위협을 억지하고 취약성을 감소시키며 회복력을 강화하기 위한 사이버안보 활동을 적극적으로 추진하고 있다.

진영화시대에 있어 우리는 사이버공간의 안전을 보장하기 위하여 사이버공격 대응과 감내 역량을 확대·강화하고 있으며, 국제적 연대를 통해 이익 공유의 범위를 확장하고 있다.[67] 사이버공격 대응을 위한 국내적 역량을 강화하는 것은 크게 취약성 감소와 결과 발생으로부터의 회복력 강화를 모색하는 것이라고 할 수 있다. 가치에 기초한 국제적 연대의 강화는 자유민주적 가치를 공유하는 국제사회와의 협력을 통해 사이버위협을 차단하는 것을 말한다고 할 수 있다. 따라서 미국의 사이버 문제에 대한 안보화 과정 대응 법제도(거버넌스) 체계의 실행과 방법을 참고하여 우리 실정에 적합한 법제도(거버넌스)를 구축할 필요가 있다.

한편, 국가가 시장에 개입하여 위협, 취약성을 제거하고 회복력을 강화하여 사이버공간의 안전성을 확보하는 것은 관련된 비용의 증대를 야기하게 한다. 우리 실정에 적합한 사이버안보 법제도(거버넌스) 구축과 운영을 위해서는 비용과 안보 가치 사이의 최적 균형점을 찾아야 한다. 결국 국가는 위험의 제거 또는 감소에 소요되는 비용과 사이버안보 강화로 증대되는 사회적 복리의 비교를 통하여 가장 효율적인 사이버안보 법제도(거버넌스) 체계를 선택할 수밖에 없을 것으로 보인다. 또한 미국이 자신들의 사이버안보 법제도(거버넌스)를 국내외에 실행함에 있어 발생되는 비용을 우리에게도 전가하고자 할 수도 있으므로 미국과의 사이버안보 동맹을 통해 얻을 수 있는 우리의 안보 가치를 최대화하면서도 그에 따르는 비용은 최소화할 수 있는 사이버안보 법제도(거버넌스) 협력 체계를 구축·운영하여야 할 것으로 보인다.

67) 국가안보전략에 있어 국가 역량 강화에 관한 '자강론'과 국제적 연대 확대라는 '협력론'에 대한 보다 자세한 사항은 김기정, "경제안보의 대강", 전략노트 제17호, 국가안보전략연구원(2022. 2) 참고.

〈참고문헌〉

□ 국내

오일석(2014). “위험분배의 관점에 기초한 정보통신기반보호법 개선 방안”, 법학논집, 이화여자대학교 법학논집.

-----(2023), 「바이든 정부의 사이버안보 정책과 시사점: 사이버억지를 중심으로」, INSS 연구보고서 2022-13, 국가안보전략연구원.

-----(2017). “사이버 보안 정보공유의 법적 문제점과 입법적 해결방안에 대한 고찰-민사법적 측면의 쟁점을 중심으로”, 『하경효 교수 정년 기념논문집』(서울: 박영사).

오일석, 윤정현, 김경숙, 김유철(2022), 『아세안 신흥안보 협력 강화를 위한 모델 구축에 관한 연구』, 대외경제정책연구원.

□ 국외

Anderson, Ross(2001), “Why Information Security is Hard-An Economic Perspective”, Proceedings of the 17th Annual Computer Security Applications Conference(New Orleans, LA, 2001, https://www.acsac.org/2001/papers/110.pdf (accessed: December 27, 2023)

Chertoff, Michael(2010), “Foreword to Cybersecurity Symposium: National Leadership, Individual Responsibility”, Journal of National Security Law and Policy,

Chesney, Robert and Trey Herr(2021). “Everything You Need to Know about the New Executive Order on Cybersecurity”, LAWFARE. https://www.lawfareblog.com/everything-you-need-know-about-new-executive-order-cybersecurity (accessed: December 27, 2023).

Council on Foreign Relations(2017). “President Obama’s Pursuit of Cyber Deterrence Ends in Failure,”https://www.cfr.org/blog/president-obamas-pursuit-cyber-deterrence-ends-failure (accessed: October 3, 2023).

Curran, John(2022). “Senate Approves FISMA, FedRAMP, Cyber Incident Reporting Legislation” MeriTalk, https://www.meritalk.com/articles/senate-approves-fisma-fedramp-cyber-incident-reporting-legislation/(accessed: October 3, 2023).

Department of Defense(2011). Strategy for Operating in Cyberspace.

Department of Defense(2015). Cyber Strategy.

Department of Defense(2018), “SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY”. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF(accessed: December 27, 2023).

Department of Defense(2021), “DOD General Counsel Remarks at U.S. Cyber Command Legal Conference,” Remarks by. Hon. Paul Ney, Jr.,

https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conf(accessed: December 27, 2023).

Department of Homeland Security(2006), National Infrastructure Protection Plan.

Department of Homeland Security(2013). National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency.

Emmott, Robin(2017). "NATO mulls "Offensive Defense" with Cyber Warfare Rules", Reuters.

Gardner, Mathew J. and Moshe B. Broder(2016). "CISA: Hope for More Cybersecurity Challenges in Implementation and Interpretation", the Procurement Lawyer, Volume 51, Number 3.

Geller, Eric(2021). "Biden orders federal cyber upgrade after barrage on hacks", POLITICO, https://www.politico.com/news/2021/05/12/biden-federal-cyber-upgrade-hacks-487731 (accessed: December 27, 2023).

Haydock, Walter(2021). "The Biden Administration's Impending Executive Order on Software Security", LAWFARE, https://www.lawfareblog.com/biden-administrations-impending-executive-order-software-security (accessed: December 27, 2023)

Hooker, Vincent(2010). "Major Oil and Gad Project-the Real Risks to EPC Contractors and Owners", Construction Law Journal.

Kagubare, Ines(2022). "Senate passes cybersecurity bill amid fears of Russian cyberattacks", THE HILL, https://thehill.com/policy/cybersecurity/596628-senate-passes-cybersecurity-bill-amid-fears-of-russian-cyberattacks (accessed: October 3, 2023).

Levine, Mike(2016). "China is "Leading Suspect" in Massive Hack of US Government Networks", ABC News.

Lohrmann, Dan(2017). "Hack Back Law", Government Technology.

Lyngaas, Sean(2018), "US Looks to Restart Talks on Global Cyber Norms", CyberScoop.

Marks, Joseph(2015). "GOP to Obama: Crack down on Chinese hackers," Politico, https://www.politico.com/story/2015/06/republicans-obama-chinese-hackers-crack-down-118802 (accessed: October 3, 2023)

Mead, Patrick(2007). "Current Trends in Risk Allocation in Construction Projects and their Implications for Industry Participants", Construction Law Journal.

Powell, Benjamina(2005), "Is Cybersecurity a Public Good? Evidence from the Financial Services Industry", Journal of Law, Economics and Policy.

Sanger, David(2016). "US Wrestles with how to fight back against Cyberattacks", NY Times.

Schmidle, Nicholas(2018). "The Digital Vigilantes who Hack Back", New Yorker.

Segal, Adam(2016). 'The Top Five Cyber Policy Developments of 2015', Council on Foreign Relations.

Sullivan & Cromwell LLP(2015), The Cybersecurity Act of 2015.
The White House(2004). The National Strategy to Secure Cyberspace.
The White House(2008). National Security Presidential Directive No. 54, Cybersecurity Policy.
The White House(2009). Comprehensive National Cybersecurity Initiative.
The White House(2011). International Strategy for Cyberspace.
The White House(2017). "Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week 2017".
The White House(2021). Executive Order on Improving the Nation's Cybersecurity, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (accessed: December 27, 2023).
The White House(2023). FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/ (accessed: December 27, 2023)
Triantis, George(2000) "Unforeseen Contingencies. Risk Allocation in Contracts" in Boudewijn Bouckaert and Gerrit De Geest (eds), Encyclopaedia of Law and Economics(Edward Elgar) Vol Ⅲ.
Triantis, George(2010). "The Evolution of Contract Remedies (and Why Do Contracts Professors Teach Remedies First?)", University of Toronto Law Review,
UN General Assembly(2015). 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', Seventieth Session, Item 93.
US Government(2009). Cyber Space Policy Review, https://irp.fas.org/eprint/cyber-review.pdf(accessed: October 3, 2023).
Varian, Hal R.(2002). "System Reliability and Free Riding", Proceedings of the First Workshop on Economics and Information Security(University of California, Berkeley).

Cybersecurity Information Sharing Act of 2015.
National Defense Authorization Act for Fiscal Year 2018
National Defense Authorization Act for Fiscal Year 2021
Joint Explanatory Statement to Accompany the Cybersecurity Act of 2015, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/jes%20for%20cybersecurity%20act%20of%202015.pdf (accessed: December 27, 2023)
The White House(2001), Executive Order 13231, Critical Infrastructure Protection in the Information Age.

Homeland Security Presidential Directive No. 7(2003), Directive on Critical Infrastructure, Prioritization, and Protection.

https://ritchietorres.house.gov/posts/rep-torress-software-dhs-supply-chain-risk-management-act-of-2021-passes-u-s-house-of-representatives(accessed: December 27, 2023).

https://rules.house.gov/sites/democrats.rules.house.gov/(accessed: December 27, 2023).

https://www.congress.gov/bill/117th-congress/house-bill/3684?q=%7B%22search%22%3A%5B%22cyber%22%2C%22cyber%22%5D%7D&s=3&r=2(accessed: December 27, 2023).

https://www.hsgac.senate.gov/media/majority-media/senate-passes-peters-and-portman-landmark-legislative-package-to-strengthen-public-and-private-sector-cybersecurity-(accessed: October 3, 2023).

https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/ (accessed: December 27, 2023)

이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.