Center for Future Warfare Studies,
Institute of International Studies at Seoul National University |
국제문제연구소 미래전연구센터 연구위원 워킹페이퍼 No.16.(발간일: 2025.2.3.)

데이터 안보와 공급망 안보

유인태 단국대학교 정치외교학과 교수

서론

본 연구를 진행함에 앞서 연구의 범위를 밝힌다. 기존 데이터안보에 대한 연구들은 다양한 행위자에 의한 서로 다른 종류의 데이터 관련 사건들을 다루면서, 연구 범위나 연구 대상이 모호해지는 경향이 있었다. 이 연구는, 민간에 의해서 개인 데이터가 불법적으로 수집되거나 이전되는 사례들일지라도, 국가 행위자가 개입되어 있지 않은 그리고 국가안보적 사안이 되지 않은 사례들과는 거리를 둔다. 예를 들어, 구글이 2016년 '스트리트 뷰' 서비스를 준비하면서 불거진 개인정보 불법적 수집, 2019년 아마존 택배용 소형 드론의 무단 촬영, 2016년의 페이스북과 케임브리지 애널리티카와의 거래 등은 연구의 초점이 아니다.

이 연구가 다루는 데이터안보 사례들은 정부뿐 아니라 개인 혹은 민간 행위자들이 다루는 데이터들이 국가안보적 사안으로 전환되는 사례들이다. 이러한 사례들을 이해하기 위한 분석 틀이 존재하나, 상술하지 않고 간략한 소개로 갈음한다. 거시적으로 보면, '신흥안보로서 데이터 안보의 창발'이라는 관점(perspective)을 통해, 미시적 안전 수위가 거시적 안보 사안으로 전환되는 과정을 조망할 수 있다(김상배 2020). 이보다는 좀 더 미시적 층위에서 단계를 나누어서 보면 안보화(securitization)의 분석 틀로도 볼 수 있다. 즉, 데이터의 안보화이다. 안보화란 주로 정부에 의해서, 특정 사안이, '언어행위(speech act)'를 통해, 비정치, 정치화, 그리고 안보화 되는 과정을 거치게 되는 것을 의미한다. 코펜하겐 학파의 안보화에 대한 논의는 잘 알려져 있다(Buzan et al. 1998).

본 연구는 데이터안보와 공급망안보의 교차점에 초점을 둔다. 즉, 어느 한쪽에만 초점을 두는 논의들은 연구의 주 관심 대상이 아니다. 예를 들어, 1999년 러시아가 미 공군 네트워

크에 행한 문라이트 메이즈 작전, 2003년 중국이 미군과 미 정부에 행한 타이탄 레인 작전 등은 국가안보와 직결되는 국방 데이터 절취 사건이지만, 공급망안보와의 연결이 명확하지 않기 때문에 다루지 않는다. 마찬가지로 2015년 불거진 중국 해커들에 의한 미 연방인사관리처(OPM) 해킹을 통한 인사 정보 유출,[1] 2014년 11월 북한에 의한 소니 해킹, 그리고 한국 국방망과 국내 방위산업체들의 네트워크에 침입하여 설계도 및 관련 데이터를 탈취하는 행위들은, 모두 데이터안보와 관련이 있지만, 공급망안보와 반드시 연계되어 있지 않다.

데이터안보와 공급망안보의 교차점에서 일어나는 사건들은 2018년 미 · 중 기술패권 경쟁이 본격화하면서 더욱 부각되기 시작했다. 이는 부분적으로는 첨단기술이 강대국 전략경쟁의 맥락에서 승리하기 위해 더욱 중요해졌기 때문이며, 동시에 첨단기술의 개발과 이를 뒷받침하는 디지털 경제의 성장에 데이터의 중요성이 제고되었기 때문일 것이다. 나아가, 첨단 디지털 기술의 공급망과 데이터 수집, 유출, 조작, 유포 등의 우려가 제기되는 과정에서 공급망안보와 데이터안보가 교차되는 양상이 두드러지기 시작한다. 따라서 데이터와 공급망이라는 두 사안 영역에서, 각각의 영역에서 일어나는 사건들도 빈번해졌지만, 이 두 영역 공통으로 해당되는 사건들도 빈번히 발생하게 되며, 사건의 성질이 복합화되었다.

이 글은 우선, 데이터안보와 공급망안보가 교차하는 사례를 다루고, 그 다음으로 교차하는 영역에서 제기되는 위협에 대한 대응책을 살핀다. 미국의 사례가 조명되는 이유는, 교차하는 해당 영역에서 위협을 꾸준히 그리고 가장 많이 제기하는 국가이며, 해당 영역에의 위협에 대한 대응책 또한 가장 활발히, 앞서서 제기하는 국가이기 때문이다. 이러한 위협 제기와 대응책은 미국의 우방국의 정책에도 영향을 미칠 수 있기 때문에, 한국도 눈여겨봐야 할 사안이다.

1. 데이터안보와 공급망안보가 교차하는 사례

상기하였다시피, 데이터안보와 공급망안보의 교차점을 고찰할 때, 크게 두 경우로 나눌 수 있다. 디지털 기술 관련 공급망안보가 확보되지 않아, 데이터안보가 타협될 수 있는 경우, 그리고 데이터안보가 타협되어 공급망안보가 위협 받는 경우이다. 이하에서는 관련되어 화두가 되었던 대표적 사례들을 검토한다.[2]

---

1) 중국의 미국에 대한 데이터 해킹으로 잘 알려진 사례는 2015년 미국의 Office of Personnel Management를 해킹사건이다. 1,970만명의 미국 정부의 기밀정보취급인가(U.S. government security clearance) 신청자에 대한 국가안보입장에 대한 설문(SF-86, "Questionnaire for National Security Position") 데이터를 빼갔다. 해당 정보는 민감한 개인정보를 가지고 있을 뿐 아니라, 방첩활동을 함에 있어서, 단순히 데이터 브로커들로부터 얻은 데이터보다 훨씬 더 가치가 높다.

2) 해당 장의 일부 내용은 유인태(2024)를 참조한다.

(1) 공급망안보의 타협이 데이터안보의 타협으로

미국에 의해 한때 상업적 사안으로 간주되었던 기술이 국제정치적 그리고 국가안보 사안이 된 것은 한두 건에 그치지 않는다. 다수의 상업적 사안들 중에서도, 특히 공급망을 구성하는 주요 민간 행위자들에 의해 촉발된 데이터안보 사안들은 국가안보적 사안들로 간주되며 미국과 중국 간 전략경쟁의 뜨거운 화두로 부상한다. 해당 데이터들이 탈취, 왜곡, 분석되어, 사회구성원들뿐 아니라 정부 행위자들에 영향을 미치고 그들을 조종하기 위한 자원으로 사용될 수 있기 때문이다.

화웨이의 5세대 네트워크 장비

미 · 중 강대국 전략 경쟁이 수면 위로 나와 본격적으로 진행되기 시작한 것은 2018년이다. 미 트럼프 정부의 시작과 함께 무역 분야에서의 갈등을 서곡으로, 여러 분야로 경쟁이 확대되었다. 그 중에 비교적 초창기부터 거론된 대상이 정보인프라의 글로벌 공급망이다. 이 영역에서 영향력을 넓히던 중국의 네트워크 장비업체 화웨이와 ZTE는 특히 미국 정부에 의해 위협 행위자로서, 특히, 화웨이는 그 시장경쟁력과 시장지배 잠재력 때문에 미국 정부의 타깃이 되었다. 많은 연구에서 이미 화웨이를 사례를 다루었다(김상배 2019; 유인태 2019; 유인태 2021). 하지만 화웨이 사건은 데이터안보와 공급망안보의 교차점에서 일어난 미중 전략 경쟁의 한 선례를 남겼다는 점에서, 그 후 유사한 (후술되는) 사례에 대한 파급력을 갖기 때문에, 그리고 여전히 활동하는 화웨이 회사의 존재가 갖는 적실성을 지닌 사례라는 점에서, 여기서도 재차 간략히라도 다룰 가치가 있다.

화웨이의 5G 사업에 미국이 안보적 우려를 제기한 근거 중 하나가, 화웨이와 중국 공산당과의 긴밀한 관계이다. 화웨이 설립자이자 회장이었던 런정페이는 중국 인민해방군 엔지니어로서 통신장비 개발 등에 관여했었다. 그리고 화웨이의 초고속 성장은, 인민해방군과 각 지역 지방정부에 통신설비를 대규모로 납품한 것에 기반한다. 2020년 6월에 미국 국방부는 화웨이를 인민해방군이 소유 또는 지배하고 있는 회사로 지목한다.[3)]

중국 공산당과의 인적, 사업적 긴밀한 연결은 기술보안에 대한 의구심으로 이어진다. 화웨이가 제공하는 제품과 서비스는 '백도어'를 통해 (기밀) 데이터가 탈취되거나, 왜곡될 수 있었다.[4)] 극단적으로는 '킬 스위치'를 통해 사회 시스템의 작동 불능이라는 시나리오도 가능

3) 이에 대해 화웨이는 지분이 회사 구성원들에게만 있고, 공산당과는 관련 없다는 성명을 내기도 했다.

했다. 제조 당시 없었더라도, 공급업체가 제공하는 소프트웨어 갱신에 의존하는 5G 시스템은, 차후에라도 악성코드가 심겨질 수 있었다. 미국 국내뿐 아니라 전 세계 시장에서 화웨이의 5G 시스템이 지배적 시스템이 된다는 것은, 미 · 중 전략 경쟁의 맥락에서 미국에게는 악몽과 같은 시나리오였다.

이처럼 미국은 연방정부에 의한 5G 사업뿐 아니라 민간에서도 화웨이를 배제시키려고 하지만, 이러한 미국 정부의 행위에는 안보적 이유뿐 아니라 경제적인 이유도 종종 지적된다. 5G 통신장비 경쟁에서 미국 기업들이 밀렸기 때문이다. 화웨이의 5G 장비는 경쟁 제품의 절반도 안 되는 가격뿐 아니라 뛰어난 기술력으로 경쟁력을 보였기 때문이다. 화웨이의 글로벌 시장에서의 지배력은, 당시 글로벌 이동통신장비 업계 1, 2위였던 에릭슨과 노키아를 넘어, 2018년 시장점유율에서 우위를 차지하는 것에서도 드러났다. 미국은 이러한 화웨이의 시장경쟁력이 중국 공산당이나 군이 거액의 보조금을 화웨이에 제공하고, 해킹을 통해 훔친 미국과 서방국들의 첨단기술을 화웨이에 제공했기 때문이라고 보았으며, 이러한 비시장적인 관습이 불공평하다고 보았다.

주요 정보통신 인프라의 공급망안보에 대한 미국의 우려가 점화되었음을 뚜렷이 보이는 사례가 '화웨이 사태'였으며, 해당 인프라는 데이터 이동의 기간(基幹)이기 때문에, 데이터안보와 공급망안보의 교차하는 핵심 사례가 되었다. 또한 화웨이 사태는 최근 계속해서 벌어지고 있는 미 · 중 전략경쟁의 핵심인 기술경쟁의 일부분에 다름 아니다. 5G 네트워크는 미래 반도체, 인공지능, 바이오, 우주 등 첨단 기술 산업 및 군사기술의 발전과 밀접한 관련이 있으며, 자율주행, 드론, 양자컴퓨터의 운영을 위한 기반이기도 하기 때문이다.

ZPMC 항만 대형 크레인

물류 및 교통을 지원하기 위한 물리적 공급망에 대한 데이터안보의 우려 또한 제기되었다. 이 중에서도 항만과 같은 주요인프라(critical infrastructure)에서 중국제 대형 크레인에 대한 미국의 우려가 2023년 3월부터 본격적으로 제기되었다. 특히, 미국 국방정보국(Defense Intelligence Agency)이 ZPMC(Shanghai Zhenhua Heavy Industries, 중국명 '상하이전화(上海振華)중공업')의 대형크레인을 잠재적 스파이 도구로 지목하면서, 데이터안보의 위험성이 제기되었다.

ZPMC는 가격경쟁력을 내세워 전 세계 크레인 시장의 70%를 차지하고 있는데, 미국에서는 80%의 점유율을 보인다. ZPMC 크레인은 대체로 중국에서 완전히 조립되어 미국에 양

4) 이에 대해 화웨이는 지속적으로 그러한 데이터 절취는 기술적으로 불가능하며, 당사 제품이 안전하다는 입장을 내놓고 있다.

도되고, 중국제 소프트웨어를 통해 운영된다. 그리고 크레인에는 출처와 행방을 등록 및 추적할 수 있는 센서가 달려 있기 때문에, 중국 본사가 크레인 현황을 모니터링 할 수 있다고 알려진다.

문제가 되는 것은, ZPMC와 중국 공산당과의 관계이다. ZPMC는 시진핑 중국 국가주석이 주창한 '일대일로' 사업의 주요 계약자인 중국 국영기업 '중국교통건설'의 자회사이다. 해당 기업은 중국의 민군융합(civil–military fusion) 프로그램에 기여를 하고 있다(Viswanatha 2023). 이 때문에 미 당국은 중국 본사가 중국 공산당과의 관계 속에서, 항만 크레인을 통해 미군이 해외 작전에 동원되는 물자 등을 이동시킬 때에, 이에 대한 정보를 수집할 수 있다고 보았다. 더욱이 크레인 운용 소프트웨어 프로그램이 사이버공격에 취약하게 만들어져, 중국군이 원격으로 크레인 작동을 중단시킬 수 있다고 보았다. 이럴 경우, 해군을 동원하지 않고도 미국 항구는 마비될 수 있다는 우려가 미 정보당국에 의해 제기되었다. 실제 2021년에는 FBI가 볼티모어항으로 도착하는 ZPMC를 운반중인 화물선에 정보 수집 장비가 실려 온 것을 발견했다고 보도되었으며(Committee on Homeland Security 2024), 중국산 크레인이 현대판 '트로이의 목마'로 비유되고 있다.

미래자동차의 핵심 기술 라이다(LiDAR)

2023년, 미래 자동차의 핵심 기술인 라이다(LiDAR)는 단순한 민간 산업 사안에서 미·중 간의 강대국 간 경쟁에서의 새로운 전략 경쟁 사안으로 떠올랐다. 라이다는 레이저 센서 기술인데, 전기차 업계의 과열되는 경쟁에 스마트 주행 기술의 통합이 이루어지며, 차량용 라이다에 대한 수요가 급증하고 있다. 해당 기술이 미·중 전략 경쟁 가운데 새로운 갈등 사안이 된 것은, 라이다 기술이 자율주행, 첨단 운전자 보조 시스템(ADAS), 스마트시티 등 다양한 민간 산업에서 활용되고 있으면서, 동시에 잠수함, 군용 차량, 로봇, 무인항공기, 무기 등 방산 산업에서도 활용되는 민감한 이중용도 성격을 가지고 있기 때문이었다. 최근 중국이 차량용 라이다(LiDAR) 기술 특허 출원을 급격히 증가시키고 있으며, 관련 시장에서 점유율을 높이고 있는 상황에서 미국의 이에 대한 안보 우려는 커지고 있다.

문제는 헤사이 기업과 중국 정부의 관계에서 비롯된다. 헤사이의 투자설명서에 따르면 중국 정부는 기업 운영에 대한 감독과 의사 결정 권한을 가지고 있어 운영에 개입할 수 있다.[5] 따라서 중국정부는 데이터 수집을 목적으로 라이다 기술을 남용할 수 있으며, 중국 주권의 영향력 하에 있는 기업들에 압박을 가할 수 있다. 중국의 국가보안법에 의하면 중국 기

[5] 그뿐 아니라 중국 기업들은 중국의 군사 프로그램들과 밀접한 관련이 있다(Sutter and Sayler 2024).

업은 정부의 요청에 따라 데이터를 제공해야하며, 중국산 라이다 기술은 미국의 지도, 인프라, 군사 시스템 등에 대한 방대한 데이터를 중국 정부에 넘기는 데에 사용될 수 있다.

이러한 우려 때문에, 미국 교통부 장관인 피트 부더제지(Pete Buttigieg)는 경제안보나 사이버안보 위협을 가할 수 있는지 해당 사안을 주의 깊게 봐야 하며, 중국으로부터 디리스크 뿐 아니라 필요하면 디커플도 해야 한다고 언급한다(Snyder 2023). 미국 하원의 '미국과 중국공산당 간 전략 경쟁에 관한 특별위원회(United States House Select Committee on Strategic Competition between the United States and the Chinese Communist Party, 이하 '중국특위')'에서도 민주당과 공화당이 함께 바이든 정부에 중국 라이다 기업에 대한 제한을 촉구하였다(중국특위 2023). 중국특위의 촉구 서한에 따르면, 공산당은 라이다에 멜웨어를 심을 수 있어, 미국 시스템의 기능을 저하시킬 수 있다. 미국 정부는 중국의 첩보 활동과 사이버공격을 통제하기 위한 노력을 해오고 있었는데, 상기의 안보화 과정을 통해, 해당 이중용도 기술은 중요 통제 대상이 된다.

그런데 이러한 미국 정부의 인식을 한편으로, 다른 한편으론 헤사이의 라이다 기술에 대한 우려에 대해 다른 시각이 존재한다. 중국은 '중국특위'에서 제기된 혐의와 우려에 대해 부인하고 있으며, 주요 인프라나 전략적 데이터를 훔치는 것에 반대해 왔다고 주장한다(Snyder 2023). 또한 독일의 독립된 두 기술 시험 회사는 미국에서 판매된 헤사이의 주요 라이다 제품을 점검하며, 해당 기술에 차량 밖으로 데이터를 저장하거나 전송할 능력이 없다고 판단했다. 그리고 헤사이 제품의 수요자인 크루즈(Cruise)나 죽스(Zoox)와 같은 미국의 로보택시 기업들이나 코디악(Kodiak Robotics) 회사는 헤사이에게 의회에 가서 설득하도록 요구했다(Snyder 2023). 기술 및 가격 경쟁력이 있는 헤사이 라이다의 대체품을 찾기 쉽지 않은 상황에서, 미 정부의 제한이 해당 회사들의 영업에 악영향을 미칠 수 있기 때문이다.

미국에 의한 제한이 걸리는 것에 대해, 중국의 반응이 단순히 혐의에 대한 부인이 아니라, 해당 기술에 대한 중국의 수출통제로 이어질 수 있다(Dyer et al. 2023). 이렇게 될 경우, 해당 제품에 크게 의존하고 있었던 미국 기업들과 관련 시장에서의 영업 및 기술 개발에 큰 지장이 초래될 수 있다.

중국산 DJI 드론

2023년 11월 1일 미 하원 중국위원회는 미국정부에 의한 중국산 드론 구매금지안을 추진한다. '미국 안보 드론법(American Security Drone Act)'의 제정을 노리고 초당적으로 법안이 제출되었는데, 특정 회사 이름은 적혀 있지 않았지만, 세계 최대 드론 기업인 중국의 DJI를 겨냥하고 있는 것으로 해석되었다(Sevastopulo 2023). DJI는 선전에 본사를 두고 있

으며, 세계시장점유율 58%, 미국 점유율 7.8%을, 그리고 세계 민간용 드론 시장에서는 이보다 높은 70% 이상의 점유율을 보인다. 입안에 참여한 마이크 갤러거 공화당 의원은, 중국 공산당이 드론시장을 독점하며 무기화하고 있으며, 일례로 하마스가 드론 테러 공격을 할 때, 우크라이나로는 드론 수출이 제한되고 있다고 지적하였다.

DJI는 2022년에 이미 미국 정부의 제재를 받고, 미국 디자인 소프트웨어의 사용이 불가능한 상태였다. 당시 DJI는 미국 샌프란시스코의 소프트웨어 회사 피그마(Figma)의 서비스를 이용하고 있었는데, 2022년 3월 12일 서비스 중단을 통고 받았다. 그 전에 트럼프 정부 당시 2020년 12월에는 미국 상무부가 DJI를 제재 명단(entity list)에 올렸었다. 상무부의 허가 없이는 미국 제품을 구매하거나 미국 기술을 수입할 수 없다. 그 후 바이든 정부에 들어서 2021년 12월 16일에는 재무부가 DJI와 다른 중국 기술 기업 7곳을, 신장위구르자치구의 무슬림 소수민족에 대한 감시와 인권 침해를 도왔다는 이유로 투자 블랙리스트에 올렸다. 2023년에 미국 사이버보안 및 인프라보안국(CISA)은 이미 중국산 드론 사용시 데이터 유출과 해커 공격으로 이어질 수 있다고 경고했다. 그리고 2024년 1월에는 미국 FBI가 DJI 드론의 데이터 유출 위험에 대해 제기했다.

미국의 데이터안보 우려에 대해 해당 기업이나 중국 당국은 가만히 있지 않고 대응에 나서고 있다. 데이터 유출 우려에 대해 DJI는 보도자료를 통해 허가 받지 않은 사용자가 드론 데이터에 접근할 수 없도록 사용자가 '오프라인 비행'을 선택할 수 있다고 반박하기도 하였다(유효정 2024). 그리고 로비 회사들을 고용하여 미 의원들을 설득하는 작업을 펼치기도 하였다(Sevastopulo 2022).

또 다른 한편으론 중국 정부는 미국의 블랙리스트 기업들을 방문하며, 정부 차원에서의 관심을 보이고 있다. 2023년 10월 시진핑 중국 국가 주석의 최측근인 딩쉐샹 국무원 상무부총리가 광둥성 선전을 시찰하면서 DJI를 방문하여 기술 혁신을 촉구하며 전폭적 지원을 언급 하였다(Chen 2023). 이에 앞서 리창 중국 총리가 저장성을 시찰하며 미 블랙리스트에 오른 세계 최대 감시장비 제조업체 하이크비전을 방문한 것도 같은 맥락이다. 이러한 중국 당국의 최고 정치적 지도자들의 방문에서, 중국이 해당 기술에 대해 갖고 있는 자신감과 중요성에 대한 인식이 반영되고 있다.

소셜네트워크 서비스, 틱톡(TikTok)

틱톡은 소셜네트워크서비스의 일종으로 동영상 플랫폼이며 처음 출시는 2016년 중국에서 이루어졌다. 동아시아에서의 폭발적 반응을 업고 2018년 전 세계로 진출하였으며 2021

년 9월 기준으로 10억 명의 사용자를 기록한다. 미국에서만도 월 이용자 수가 1억 5천만을 넘는 선풍적 인기를 얻게 된다.

그런데 해당 앱은 2022년 12월 '2023 회계연도 연방정부 예산안'을 통해 미국 의회에 의해 사용금지가 내려진다. 연방정부에서 사용하는 모바일 기기에서 틱톡 사용의 전면 금지가 포함되었기 때문이다. 유사한 선례가 없을 정도로 동영상 앱에 대한 정부 차원의 가장 광범위한 단속이다. 이러한 미국 정부에 의한 틱톡 금지 움직인 이전부터 있어왔다. 미 · 중 전략 경쟁의 맥락에서 가장 최초로 이루어진 시도는 트럼프 대통령에 의한 2020년 8월의 틱톡을 금지하는 행정명령이다.[6] 그러나 이는 연방판사의 제동으로 불발이 되었다.

바이든 정부가 들어서면서, 트럼프의 행정명령을 철회하고 입법 과정을 거치게 된다. 2024년 3월 상원이 발의한 '외국의 적이 통제하는 앱으로부터 미국인들을 보호하는 법(일명, 틱톡 금지법안)'은 4월에는 미국 연방의회를 모두 통과하게 된다.[7] 법안은 틱톡의 미국 사업권을 매각하지 않으면, 미국 내 서비스를 금지해 퇴출시킨다는 내용을 담고 있다.[8] 틱톡뿐 아니라 미국의 적대국이 통제하는 앱의 미국 내 업데이트 및 유지를 금지하고 있는데, 이에 따르면 미 대통령은 중국, 러시아, 이란, 북한과 관련한 앱을 제한할 수 있는 광범위한 권한을 갖게 된다.[9] 이러한 앱에는 소셜네트워크 서비스 관련 앱뿐 아니라, 미국 전자상거래 부문에서 급속히 인기를 얻고 있었던 쉬인, 핀둬둬, 테무, 알리페이 앱 등도 포함된다.

미국 정부가 틱톡을 금지한 이유는 틱톡과 중국 공산당과의 연결 의혹 때문이다. 이러한 연결은 일반 개인들의 데이터가 국가안보적 우려와 연결되게 한다. 우려되는 한 시나리오에 따르면, 중국 정부가 틱톡 혹은 모회사인 중국기업 바이트댄스(ByteDance)에 압력을 가해 미국 사용자들의 개인정보를 넘겨받을 수 있게 되어, 빅데이터를 통한 분석을 통해 국가안보와 관련한 첩보를 얻을 수 있다.[10] 또 다른 시나리오는 중국이 정보 작전(information operation)의 일환으로 미국 사회에 허위정보(disinformation)를 퍼뜨리는 데 틱톡을 사용할 수 있다는 것이다. 연방수사국의(FBI)의 크리스토퍼 레이 국장은, 중국이 대만을 침공하게 된

6) 트럼프 전 대통령은 틱톡이 없다면 페이스북이 더 커질 것이라며, 2024년의 틱톡금지법안에 반대했다. 그러나 공화당 강경파는 트럼프 대통령의 반대에도 불구하고 법안에 찬성했으며, 이를 통해 미국 의회에서 중국 견제 주장이 강한 합의를 이루고 있다고 볼 수 있다.

7) 틱톡 금지를 반대하는 의원들도 존재했다. 젊은 유권자들의 지지를 많이 얻고 있는 민주당 의원들의 경우 특히 그러했다. 미국 하원의 표결 시 찬성 352표 반대 65표라는 압도적 차이는 있지만, 반대표는 민주당에서 50표 공화당에서 15표 나왔다.

8) 이 때문에 틱톡의 퇴출은 페이스북 같은 다른 소수의 소셜 네트워크 서비스회사에 더 많은 이익과 권력을 가져다줄 것이라는 우려도 있다.

9) 미 몬태나주에서는 주 차원의 틱톡 금지법이 2023년 4월 주의회의 가결과 공화당 주지사 서명으로 도입되었다. 하지만 같은 해 11월 연방법원이 언론 · 표현의 자유를 보장하는 수정헌법 제1조 침해 소지로 시행을 중단시키는 판결을 내렸다.

10) 이에 대해 틱톡은 10억 달러를 들여 미국 쪽 데이터를 다른 지역들과 분리해 보안을 강화하는 조치를 취해왔다. 2023년에는 저우서우즈 최고경영자가 하원 청문회에서 틱톡 본사는 미국 로스앤젤레스와 싱가포르에 있으며 미국에서 7천명을 고용하고 있다며 규제 반대 논리를 폈다.

다면, 짧은 형식의 비디오로 미국 내 여론을 형성할 수 있다고 우려를 표한 바 있다.

이러한 틱톡과 중국공산당과의 연결에 대한 인식은 미국 정부에 널리 퍼져 있다. 2023년 3월 23일에 있었던 하원 청문회에서도 공화당 위원장과 민주당 의원들 모두 틱톡 최고경영자에 대한 의혹을 강하게 제기하였다. '미국과 중국공산당의 전략적 경쟁에 관한 특별위원회' 위원장이였던 마이크 갤러거 하원의원은 2024년 법안에 대한 표결 직전에 이 법안에 대해 "틱톡을 중국공산당과 분리하려는 것"이라며 "우리의 국가안보를 위한 상식적 조처"라고 언급하며, 틱톡에 대한 인식을 보이고 있다.

(2) 데이터안보의 타협이 공급망안보의 타협으로

여기에서는 데이터안보가 타협되어, 결과적으로 공급망에 위협이 발생한 경우를 살핀다.

콜로니얼 파이프라인(Colonial Pipeline) 사태

콜로니얼 파이프라인(Colonial Pipeline)에 대한 사이버침해는 2021년 5월에 발생한다. 미국 동부 해안 지역에서 소비되는 연료의 45%를 공급하는 주요인프라 회사에 대한 사이버 공격이다. 이 사건은 바이든 정부 초기에 공급망안보에 대한 경각심을 불러일으킨 대형 사이버침해 사건이다. 하지만, 사건의 주요 내용은 동부의 연료를 담당하는 기능의 정지와 랜섬웨어에 의한 피해액의 규모로만 알려져 있으며, 데이터안보가 추후에 위협되었는지 여부에 대해서는 잘 알려져 있지 않다.

하지만 사건은 데이터의 절취가 선행되어 일어났었다. 2021년 5월 6일 다크사이드(DarkSide)로 알려진 해커 그룹이 2시간 동안 100 기가바이트에 해당하는 데이터를 훔쳤다. 그 다음날, 훔친 데이터를 기반으로 접속 암호를 알게 된 해커들은, 콜로니얼 파이프라인의 IT 네트워크를 랜섬웨어로 감염시킬 수 있었다. 콜로니얼 파이프라인은 랜섬웨어가 확산되는 것을 막기 위해 파이프라인을 중지시키게 된다. 그리고 5월 9일 바이든 대통령이 비상사태를 선언하게 된다.

소프트웨어 공급망 관련 '솔라윈즈(SolarWinds)' 사태

솔라윈즈(SolarWinds) 사태는 소프트웨어 공급망과 관련하여 일어난 큰 사건이었다. (보안)소프트웨어 공급망이란 (기업)조직 내부에서 사용하는 백신 프로그램이나 네트워크를 관리해주는 도구들을 설치 및 업데이트 하는 과정에서 데이터가 이동하는데, 그러한 이동을 위한 경로상의 모든 네트워크를 의미한다. 보통 이러한 공급망에 대한 신뢰도는 일반적으로 굉장히 높은데, 이 경로를 타고 악성 프로그램이 유포된 것이다. 솔라윈즈와 같은 경우, 전 세계 네트워크 관리 도구 업계 중에는 가장 큰 서비스 공급자 였기 때문에 당시 1800개 정도의 회사가 한꺼번에 잠재적 피해자가 되었다. 그리고 서버에 대한 직접적 공격 외에도, 이슈가 되었던 것은 홈페이지에 올려진 고객사 리스트였는데, 해커들이 그런 고객사 레퍼선스를 보고 취약점을 찾아 공격을 하였기 때문이다. 해당 사건 이후로 솔라윈즈(SolarWinds)와 같은 회사들은 모두 레퍼런스 페이지를 내렸다.

솔라윈즈 사태는 소프트웨어 공급망 보안에 대한 국가적 경각심을 높인 사건이 되었다. 솔라윈즈 내부망에 침투한 해커는 IT 관리 툴인 '오리온(Orion)'에 '선버스트(Sunburst)'라는 악성코드를 심어 공격했다. 그 결과 '오리온'을 사용하는 약 1만 8천 곳가량의 기업이나 기관들이 버전을 업데이트하는 과정에서 악성코드가 유포되었는데, 피해 기관 중에는 미국 국무부, 법무부, 국립보건원, 국토안보부, 사이버보안 및 인프라 보안국, 에너지부, 재무부, 항공우주국, 핵안보국, 통신정보관리청 등의 국가기관뿐 아니라, 마이크로소프트, 파이어아이 등의 보안 기업 및 포춘 500대 기업도 있었다.

솔라윈즈 해킹 사건은 소프트웨어 공급망 공격(supply chain attack) 사건이다. 공급망 공격은 파장이 광범위하며 치명적일 수 있는데, 왜냐하면 제품이 개발되거나 생산되는 망을 공격해서 이후 단계에 영향을 미치는 공격이기 때문이다. 가령, 대량 생산되어 유포되는 소프트웨어 제품에 공급망 상에서 사이버 위협을 심었을 경우, 해당 소프트웨어를 사용하는 수많은 기기나 네트워크에 악영향을 미치며, 기기의 작동 불능 혹은 파괴(destruction)나 연결의 중단(disruption)을 초래할 수 있기 때문이다. 또한 데이터의 탈취나, 왜곡, 이동 장애도 유발될 수 있기 때문이다. 이런 소프트웨어에 대한 경로의존적 기술생태계가 형성될 경우, 더욱 광범위하고 장기간에 걸쳐 악영향을 받게 된다. 이러한 치명적 중요성 때문에, 미국 사이버사령부 지휘원 폴 나카소네(Paul Nakasone)도 해당 사건이 국가 전체의 사이버안보 전환점이 되었다고 언급할 정도이다.

2. 데이터–공급망 교차 영역 위협에 대한 미국 정부의 대응

여기서는 이러한 공급망안보에 대한 대응뿐 아니라, 데이터안보를 향상시키기 위한 노력들을 조명한다. 이러한 노력들이 데이터안보와 공급망안보가 교차하는 지점에 해당하는 위협들에 어떻게 대응하는지 검토한다. 미국의 대응은 행정명령을 통해 발 빠르게 대처하거나, 연방 예산안을 통한 구매 과정을 통해 통제하거나, 사이버안보 전략서를 통해 체계화된 대처를 내놓는 등의 행동을 포함하였다. 그리고 CISA나 NIST를 통해 대처 방안들을 부문별로 구체화해서 내놓기도 한다.

2021년에 솔라윈드 사건이나 콜로니얼 파이프라인에 대한 큰 사이버안보 사건들이 발생한 직후, 미 대통령 바이든은 행정명령 14028을 내놓으며 국가의 사이버안보를 강화하려고 했다(The White House 2021). 해당 명령은 소프트웨어 공급업체들이 미국 정부에 판매할 때의 새로운 보안 요구 사항들을 담고 있었다. 소프트웨어 자재명세서(SBOM)가 연방정부 차원에서 공적으로 나온 것도 이때부터이다. 행정명령은 또한 악의적 사이버 행위자로부터 국가를 지키기 위해 연방정부와 민간이 소프트웨어 공급망을 강화하기 위해 반드시 함께 작업해야 한다는 것도 언급하고 있다. 행정명령 14028 이후로, 해당 행정명령의 4절(Section 4)에 따라, 미국 상무부 산하 국립표준기술연구소(NIST)는 보안 강화를 위해 새로운 표준, 도구, 모범 사례 및 기타 가이드라인을 제정했다. 이후 사이버안보 및 인프라보안기관(Cybersecurity & Infrastructure Security Agency, CISA)이 이 가이드라인을 운영하는 역할을 맡았다.

2022년 9월에 백악관은 글로벌 소프트웨어 공급망의 현황을 다루는 각서(memorandum)를 발표했다(Office of Management and Budget 2022a). 미국 정부는 사이버 위협의 위험과 민감한 정보의 손실을 줄이기 위해, 연방 기관이 타사 소프트웨어를 사용할 때 NIST 지침을 준수하도록 요구하는 이 성명을 작성한 것이다. 이 업데이트는 2021년 5월 미국 사이버보안에 관한 행정명령에 따라 도입된 2022년 '미국 사이버 보안 강화법(Strengthening American Cybersecurity Act of 2022)'이 의회에서 통과된 직후에 이루어진 것이다(The White House 2021). 해당 각서를 통해 소프트웨어 개발을 안전하게 하기 위한 접근법을 현대화시켜 나갔는데, 그 방법들이 연방 정부의 '제로 트러스트' 전략(Office of Management and Budget 2022b), 위협 탐지 및 대응(Office of Management and Budget 2021a), 그리고 복구 전략이라(Office of Management and Budget 2021b) 할 수 있다. 이러한 각서들은 모두 소프트웨어에 집중하고 있지만, 공급망과 데이터안보의 관련성을 다루고 있다.

2023년 3월 2일 바이든 정부는 2023년 국가 사이버안보 전략을 발간한다(The White

House 2023a). 그리고 7월에 이행 계획을 발간한다(The White House 2023b). 전략서도 위와 같은 맥락에서 소프트웨어 공급망 노력에 집중하고 있다. 그리고 전략서는 집단적 작전 방어(collective operational defense)를 통해 연방 민간 행정부(Federal Civilian Executive Branch, FCEB) 시스템을 보호하기 위한 계획을 개발할 것을 요구한다(CISA 2024).

미 바이든 대통령은 2024년 2월 28일 데이터에 관한 행정명령 14117 "대량의 미국인 민감 개인정보와 미 정부 관련 데이터에 대한 우려국들의 접근 방지를 위한 행정명령(Executive Order 14117 on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern)"을 내린다. 이러한 행정명령의 배경에는 프라이버시 관련 법의 통과가 연방정부 차원에서 어려웠다는 점과, 미 · 중 전략 경쟁 중이라는 맥락이 있다. 전자와 관련해서 미국은 개인 데이터의 국경 간 이동과 관련해서 EU와 세이프하버나 프라이버시실드의 폐지와 같은 지속적인 외교적 마찰을 경험했다(유인태 2024; Fahye and Terpan 2021; Farrell and Newman 2018). 법제도 차원의 해결이 어렵기 때문에, 개인 데이터의 이동에 관한 행정명령 차원의 대응이라고 할 수 있다.

사실 행정명령14117은 데이터안보에 좀 더 가까운 조치이지만 공급망안보에 대해서도 언급한다. 그리고 그 전의 2019년에 나온 행정명령13873 "정보통신기술과 서비스 공급망을 보호하기(Securing the Information and Communications Technology and Services Supply Chain)"의 확장판이기도 하다(The White House 2024). 행정명령 14117은 데이터 중개에 대한 언급을 하는데, 이는 데이터 브로커들이 우려국에 판매하는 데이터에 미 군인들에 대한 정보도 포함되어 있었다는 우려가 제기되었기 때문이다. 하지만 이러한 조치는 국가 간 데이터 흐름에 영향을 미칠 수 있었기 때문에, 상업적 활동에 최소한의 충격을 줄 수 있도록 그리고 데이터 국지화의 차원으로 여겨지지 않도록 통제의 수위를 조절하고 있다. 또한 해저케이블에 대해 언급하고 있다. 해저케이블을 통해 데이터의 대량 수집이 가능할 것으로 생각되기 때문이다. 해저케이블에 훼손을 가하는 방법도 있으며,[11] 또는 케이블을 소유하고 있는 기업을 통해서도 데이터안보는 위협 받을 수 있다. 그리고 기업의 협조를 강제할 수 있는 중국국가정보법(National Intelligence Law)의 7조 때문에라도, 미국은 국가 행위자에 의한 통신망의 소유를 더욱 우려하고 있다.[12] 통신망에 대한 공급망안보가 데이터안보와 연결되는 지점이다.

---

11) 그리고 이는 트롤선과 같은 배로도 매우 쉽게 이루어질 수 있다(Martin 2022).

12) 이러한 우려는 새로운 것이 아니다. 이미 2000년에 미국 외국인 투자 심사제도(Committee on Foreign Investment in the United States, CFIUS)가 홍콩의 글로벌 크로싱(Global Crossing)이라는 회사의 미국 통신회사의 구매를 심사한 바 있다.

미국 정부는 2024년에 데이터안보와 공급망안보의 교차 영역에 관련된 또 다른 행정명령을 내린다. 행정명령 14117보다 7일 먼저 나온, 즉 2월 21일의 행정명령 14116 "미국의 선박, 항구, 항만 및 해안가 시설의 보호에 관한 규정 개정(Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States)"을 발표한다. 해당 행정명령은 해양 사이버안보를 강화하기 위한 방안을 담고 있는데, 중국산 선박 및 육상 크레인에 대한 해양보안 지침을 발표하게 하고, 해양운송시스템 등 관련 시스템의 보안을 강화하도록 하였다. 그리고 미국 항구 인프라에 향후 5년간 200억 달러 투자할 계획을 발표하며, 항구 크레인 생산 능력 향상을 위한 목적도 포함되어 있다. 해양 사이버안보, 데이터안보, 공급망안보 등의 안보적 고려뿐 아니라 '미국에 투자하기' 아젠다의 일환이기 때문에, 산업정책적 고려도 복합적으로 결합되어 있었다.

이렇게 데이터안보와 공급망안보의 교차점을 인식하고 대처가 명시되는 행정명령은, 시기를 거슬러 올라가자면 2019년까지 추적할 수 있다. 트럼프 정부 때인 2019년에 나온 행정명령 13873 "정보통신기술과 서비스 공급망을 보호하기(Securing the Information and Communications Technology and Services Supply Chain)"의 내용을 통해, 미국이 공급망안보와 데이터안보의 교차점에서 발생하는 우려를 어떻게 대처하려고 했는지를 볼 수 있다. 해당 행정명령은 민감한 정보를 담고 통신하는 정보통신기술과 서비스의 취약점을 파고드는 외국의 적들을 대처하기 위해 도입되었기 때문이다. 해당 명령은, 적대적 외부 세력에 의한 지침이나 사법권에 종속되거나 통제되거나, 소유되거나 하는 개인들에 의해 설계되거나, 개발되거나, 제조되거나 공급되는 정보통신기술의 취득, 수입, 이전, 설치, 취급과 같은 거래를 금지한다. 핵심은 공공과 민간에서의 해당 기술의 획득(procurement)에 대한 규제를 가하는 것이다.[13)]

대통령에 의한 행정명령에 이외에도, 법에 의한 데이터안보와 공급망안보 영역에의 대처도 중요한 국가작위(statecraft)가 되고 있다. 예를 들어 '2018년 연방 획득 공급망 보안법(Federal Acquisition Supply Chain Security Act of 2018)'에서는 고위험군으로부터 연방 정보통신기술 공급망을 보호하기 위한 몇 가지 주요 프로토콜을 수립하고 있다(Congress.gov 2018). 이 법은 우선 행정부 내에 연방조달보안위원회(Federal Acquisition Security Council, FASC)를 설치한다. FASC에는 예산관리처(Office of Management and Budget), 일반 서비스 관리국(General Services Administration), 국토안보부, 국가정보국장실, 법무부, 국방부, 상무부와 같은 주요 기관의 대표자가 참여한다.

2019 회계연도 국방수권법안(National Defense Authorization Act, NDAA)도 공급망안

13) 이와 비슷한 맥락에서 2020년 3월 백악관에서 '5G 보안을 위한 미국 국가 전략(National Strategy to Secure 5G)'이 발표되었고, 2021년 1월에는 이에 따른 '실행 계획(Implementation Plan)'이 발표되었다.

보와 데이터안보가 중첩되는 영역에 대한 우려에 대처하고 있다. 해당 법의 889절(Section 889)에 따르면 화웨이(Huawei), ZTE와 같은 중국 기업들이 제공하는 통신 및 비디오 감시 장비가 스파이 활동과 국가안보에 위협이 된다는 우려에서 해당 법이 도입되었음을 나타내고 있다. 이에 따라 해당 법은 연방 정부와 계약업체들이 이러한 장비를 사용하거나 조달하는 것을 금지한다. 이 법은 단순히 최종 제품에만 국한되지 않고, 해당 부품이 중요한 구성 요소로 포함된 시스템까지 포함하여, 기업들이 공급망을 철저히 점검하도록 요구한다. 계약업체는 해당 장비를 사용하는지 여부를 공개해야 하며, 이를 확인하기 위한 합리적인 조사를 수행해야 하나, 내부 또는 제3자 감사를 반드시 요구하지는 않았다.

상기와 같은 행정명령들 또는 입법과정을 통해서, 연방정부 행위자에게는 다음과 같은 권한 그리고 역할이 부여되었다. 첫째로, 리스크 평가(risk assessment)다. 예를 들어, 국가정보국장(Director of National Intelligence, DNI)으로 하여금 정보통신기술이나 서비스로부터의 미국과 미국시민들에 대한 위협을 관련 부처와 함께 지속적으로 평가하게 하였다. 둘째, 리스크 관리(risk management)인데, 그 한 측면으로서 감독을 들 수 있다. 예를 들어, 연방 정부 당국이 국가안보를 위협하는 거래에 대해 개입할 수 있도록 하였다. 그리고 공급업체와 같은 사업자들로 하여금 자신들의 사업 행위에 대해 점검하도록 하였다. 이는 특히 주요인프라(critical infrastructure) 보호를 위한 맥락에서 중요한 기능이다. 주요인프라에 사용되는 디지털 정보통신기술의 공급망안보를 확보하고, 데이터안보를 확보하려고 하는 것이다. 주요인프라 내부에 멜웨어를 심고 잠재시켜 놓을 수 있으며, 필요시는, 데이터의 삭제나 조작 또는 접근 거부를 통해 대형 사고를 발생시켜 민간에 막대한 피해를 입힐 수 있기 때문이다. 따라서 이러한 기능은 민관협력을 통한 리스크 관리이기도 하다.

민관 협력을 통한 사이버 리스크 관리의 대표적 기구로 CISA를 꼽을 수 있다. 특히, CISA의 국가 위험 관리 센터(National Risk Management Center)는 정부 및 산업계와 협동하며 국가 인프라의 안전과 복원력을 위해 공급망 위험 관리를 담당하고 있다. CISA는 'ICT 공급망 위험 관리 태스크 포스(ICT Supply Chain Risk Management Task Force, SCRM TF)'를 2018년에 11월에 설립되면서 12월에 바로 구성하였다. 이 사실만 보더라도 미국 이 사이버안보와 공급망안보가 얼마나 긴밀하게 연결시켜 인식하고 있는지를 알 수 있으며, 또한 정부와 민간이 협력해야 할 사안이라는 것을 인식하고 있음을 볼 수 있다. 그리고 투명성을 증진시키기 위해 SBOMs이나 HBOMs과 같은 정책적 도구들을 통해, 구성 요소와 그 출처를 식별하여 악성 또는 위조 부품의 포함을 방지하는 데 도움을 주고자 하였다. SCRM TF는 제품 설계, 개발, 유통, 유지보수 과정에서 발생하는 위험을 포함하여 ICT 공급망 내에서 중요한 위험 영역을 식별하는 데 중점을 두었다.

해당 TF에서는 2023년 1월 '중소기업(SMB) 공급망 보호: 정보 및 통신 기술 리스크를

줄이기 위한 리소스 핸드북(Securing Small and Medium-Sized Business (SMB) Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks)'을 발간하며, 중소 규모의 사업자들을 위한 공급망 안보 확보 방안을 발간했다.[14] 2023년의 '리소스 핸드북'을 보게 되면 SMB를 위한 ICT 관련 공통적인 공급망 위험에 대한 개관을 하고 있다. 그리고 공급망안보를 강화를 할 수 있는 실용적인 조치들을 민관 협력의 차원에서 제안하고 있다. 실제 사례를 사용하여 단계적 지침들을 알려주며, 모니터링, 위험 평가, 보안 프로토콜의 설립 등을 위한 도구들과 소재처를 알려주고 있다. 또한 부여되는 역할들에 적절한 인력들의 훈련과 인식 증진을 강조하고 있다. 마지막으로, 제3자에 의한 위험 검증(risk verification)이나 사이버안보 공급망 위험 관리 프로그램(Cybersecurity Supply Chain Risk Management (C-SCRM) program)에 기반한 정기적 평가(evaluation)와 감사(auditing)를 권면하고 있다.

C-SCRM 프로그램이란 CISA에 의해 관리되며, 조직들로 하여금, 한편으론 데이터 보안을 증진시킬 수 있도록 하며, 다른 한편으론 그들의 공급망 내에서의 위험(risks)을 식별, 평가, 완화(identify, assess, and mitigate)하는 것을 돕고 있다. C-SCRM에 대해 2018년에 CISA가 이미 언급하는 것을 보면, 설립 초기 일찍부터 공급망안보와 데이터안보의 교차점에 대한 인식이 있었던 것으로 볼 수 있다(Monette 2018). 그런데 C-SCRM 프로젝트 관리실(C-SCRM Project Management Office)이 2022년 7월에 출범하면서 더욱 중요성이 증가하고 체계적 관리의 필요성이 더 커졌다고 볼 수 있다(Burgan 2023).

위에서, 데이터안보와 공급망안보가 교차하는 방식을 두 가지 제시하고, 데이터안보, 또는 더 넓게는 사이버안보가 타협되면서, 공급망안보가 위험에 빠지는 경우를 언급했다. 이러한 경우에 더 가까운 사건들을 염두에 두고 제정된 법안이 있다. 2021년 9월에 도입된 '중요 기반 시설에 대한 사이버 사고 보고법(Cyber Incident Reporting for Critical Infrastructure Act, CIRCIA)'이다(Congress.gov 2021). 해당 법은 크게 세 가지 의무를 발생시킨다(CISA 2022). 첫째, 사이버 사고 보고이다. 적용 대상 기업은 상당한 사이버 사고가 발생한 것으로 합리적으로 판단되는 72시간 이내에 CISA에 보고해야 한다. 둘째, 랜섬웨어 지불 보고이다. 대상 기업은 랜섬웨어에 대한 대가를 지불한 후 24시간 이내에 CISA에 보고해야 한다. 셋째, 연방 사고 보고서 공유이다. 사이버 인시던트 보고서를 받은 연방 기관은 24시간 이내에 이를 CISA와 공유해야 한다.

CISA는 현재 규칙 제정 절차에 있으며, 2024년 4월 4일 '연방 관보(Federal Register)'

[14] 일반적 사이버안보에서도 국가와 민간 간의 정보차이가 존재하지만, 기업들 간에도 정보차이가 존재한다. 큰 기업과 작은 기업들 간의 역량차이는 사이버 위협의 근원 중 하나인데, 위의 핸드북은 이러한 격차를 줄이려는 노력으로 볼 수 있다.

에 '규칙 제정 제안 공고(Notice of Proposed Rulemaking, NPRM)'를 발표하고 7월 3일까지 공개 의견 수렴을 진행했다. CIRCIA는 전반적인 사이버안보 복원력과 대응 역량의 향상이라는 목적을 위해서, 주요인프라와 관련한 사이버안보 체계의 중요한 발전이라고 볼 수 있다. 미국의 사이버안보 체계는 사이버 사고 보고를 표준화하고 중앙 집중화하는 중요한 단계를 올라가고 있다고 볼 수 있다.

지금까지 미국은 자유롭고 개방된 인터넷을 추구하며, 가능한 최소한의 범위에 제한을 두려고 하는 경향성이 있었다. 그러나 이러한 지금까지의 경향성에서 변화하는 모습이 조금씩 보이기 시작했다. 예를 들어, 최근 들어 나오고 있는 특히 상무부에서 나오는 새로운 정책도구들에서 보인다. 상무부의 '정보통신기술 및 서비스 프로그램(Information and Communications Technology and Services (ICTS) Program)'이 대표적인 예이다. 이 프로그램의 이행은 산업보안국(Bureau of Industry and Security)의 '정보통신기술 및 서비스 실(Office of Information and Communciations Technology and Services, OICTS)'에서 담당하고 있다. OICTS의 임무는 미국의 특정 ICTS 거래가 미국에 국가안보 위험을 가하고 있는지 여부를 조사하는 것이다. 2024년 6월 20일에 최초의 최종결정이 내려졌는데, 안티바이러스 소프트웨어 및 사이버보안 회사인 캐스퍼스키(Kaspersky Lab, Inc.)의 미국에서의 또는 미국인에 대한 제품과 서비스의 사용이 금지되었다. 사용자들의 피해를 최소화하기 위해 2024년 9월 29일까지의 유예기간을 허용하기로 했지만, 동시에 개인이나 민간함 데이터의 노출을 제한할 수 있는 다른 사업자들(vendors)에게 이전하기를 강하게 권장하고 있다.

OICTS는 기술 우선순위(2024 Technology Prioritization)를 표를 만들고 제시하고 있다(OICTS 2024). 이 기술 우선순위는 무엇보다 미국이 국가안보적 관점에서 기술을 접근할 것으로 보인다. 그리고 이후의 정책이나 투자의 향방에 국가가 개입할 것도 보인다. 아울러, 기술의 공급망안보와 수출통제를 추구해나갈 것임이 보인다. 추가적으로 선정된 기술들을 보면 민감한 기술과 데이터를 함께 보호할 것이 보인다. 기술공급망안보 뿐 아니라 데이터안보와 사이버안보(또는 데이터안보를 위한 사이버안보)가 동시에 중요하게 다루어지고 있음이 보인다.

상무부의 ICTS 프로그램은 ICT 인프라나 신기술을 규제하기 위한 새로운 정책도구로 도입되었다. 전기차 공급망만 보더라도 중국내, 중국용, 중국 배제를 구분하고자 한다(Bureau of Industry and Security 2024). 그리고 농업 기술 및 바이오 제조, 자율 및 자동화 시스템, 대규모 언어 AI 모델, 클라우드 기반 컴퓨팅과 같은 연결되는 세시템에 대한 규제가 도입될 가능성이 크다.

상무부 차원에서뿐 아니라 국방부 차원에서도 방산업체들의 사이버안보의 기준을 강화시키고, 통제된 비기밀 정보(Controlled Unclassified Information, CUI)와 같은 민감한 정보

를 방위 기술 공급망 상에서 보호하고자 하였다.[15] 이를 위해 개발된 프레임워크로 사이버 보안성숙도모델인증(Cybersecurity Maturity Model Certification, CMMC)가 있다(DoD CUI Program 2024; Department of Defense Chief Information Officer 2024).[16] 다루어지는 데이터의 민감도에 따라 기본 사이버 위생 관행들에서부터 고급 보안 수단들까지 다섯 단계로 구성되어 있다. 국방부 계약자들은 반드시 이를 준수해야 한다. 그리고 기존에 수행하던 기관들에 의한 자기 증명(self-attestation)이 아니라 반드시 제3자에 의해 평가받아야 한다. 그리고 중소규모의 기업들이 보안 요구사항들을 맞출 수 있도록 지원하기 위한 지침도 제공하고 있다. 이러한 프레임워크가 도입된 데에는 과거 공급망이 타협되면서 민감한 정보가 유출된 사건들이 있었기 때문이다. 예를 들어, 2011년의 Lockheed Martin Breach, 2012년의 BAE Systems Breach, 2020년의 SolarWinds Attack, 2018년의 U.S. Navy Contractor Breach 등에서는 민감한 정보가 공급망이 타협되며 유출된 바 있다.

2024년 미국의 사이버안보 태세에 대한 보고서(2024 Report on the Cybersecurity Posture of the United States) 또한 데이터안보와 공급망안보의 교차점에 대해 언급하고 있다(Office of the National Cyber Director 2024). 특히 공급망안보가 2023년도 다섯 가지 가장 높은 위협 경향 중에 하나였음을 적시하고 있다. 그런데 공급망은 더욱 복잡해지고 상호연결되어가고 있으며, 제3자에 대한 의존이 높아지고 있다. 따라서 공급망 착취가 더 쉬워지고, 추적은 더 어려워지고 있다. 따라서 소프트웨어 보안에 대해 강조를 하고 있다.

보고서에서 강조하는 것은 '더 안전한 제품 및 서비스 생산을 위한 소프트웨어 보안 강화(Advancing Software Security to Produce Safer Products and Services)'이다. 이는 설계에 의한 보안 촉진(Promoting Secure by Design) 원칙, SBOMs의 이행, 메모리 안전 프로그래밍 언어(memory-safe programming languages) 사용 장려이다. 이와 함께 '데이터 보안 및 개인정보 보호에 대한 위험 관리(Managing Risks to Data Security and Privacy)'를 언급하는데, 안전하고 풍부한 데이터의 국경 간 상거래를 활성화할 것과, 프라이버시 강화기술 개발 촉진를 포함하고 있다. 또한 차세대 기술의 복원력에 투자를 언급하면서 그리고 전 세계적인 복원력 강화를 목표로 포함한다. 인터넷의 기술적 토대에 투자하거나 전 지구적인 공급망의 안전과 복원력을 위한 국가들 간 협력을 언급하고 있다. 전략서는 데이터 안보와 공급망안보가 교차하고 있다는 사실을 인식하며, 대처 방안의 채택을 장려하고 있다.

---

15) 관련한 규제로 국방부 연방조달규정 보충자료(Defense Federal Acquisition Regulation Supplement, DFARS)가 있다. 는 방위 계약업체가 데이터 보안 표준에 따라 공급망에서 CUI(통제된 기밀 정보)를 보호하기 위한 요구사항을 설정한다. CUI란 민감하지만 기밀로 분류되지 않은 정보를 의미하며, 정부와 계약자가 보호해야 하는 데이터이다. 이 데이터는 사이버공격의 주요 표적이 될 수 있기 때문에 적절한 보호 조치가 필요하다(National Archives 2024).

16) 참고로 NIST SP 800-171과는 다르다(Redspin 2023).

결론

미 · 중 기술패권 경쟁 가운데, 첨단 디지털 기술의 공급망과 데이터 수집, 유출, 조작, 유포 등의 우려가 제기되는 과정에서 공급망안보와 데이터안보가 교차되는 양상이 두드러지기 시작한다. 그런데, 데이터안보나 공급망안보 각각에 대한 연구는 있었지만, 이 둘의 교차점에 초점을 맞춘 연구는 많이 없다. 따라서 본 연구는 데이터안보와 공급망안보의 교차점에 대해 주목하고 있다. 그러기 위해 우선 연구범위를 명확히 하고자 했다. 데이터안보의 경우, 여러 사례들이 많았지만, 개인 데이터가 불법적으로 수집되거나 이전되는 사례들일지라도, 적대적 국가 행위자가 개입되어 있지 않은 그리고 국가안보적 사안이 되지 않은 사례들은 연구 범위에서 제외하였다.

여기서 다루는 데이터안보 사안들은 정부뿐 아니라 개인 혹은 민간 행위자들이 다루는 데이터들이 국가안보적 사안으로 전환되는 모습을 보인다. 이런 맥락에서 데이터안보와 공급망안보의 교차점은 더욱 특정화된다. 크게 두 가지 교차하는 방식으로 나눌 수 있는데, (1) 한 부류는, 공급망안보가 확보되지 않아, 데이터안보가 우려되거나 침해되는 경우이며, (2) 다른 부류는, 데이터안보가 타협되어, 공급망안보의 침해가 우려되는 혹은 침해된 경우이다. 전자와 관련해서는 화웨이의 5G, ZPMC 항만 대형 크레인, 미래자동차의 핵심 기술 라이다, 중국산 DJI 드론, 틱톡의 사례들을 다루었다. 전자 사례들의 의미를 부각시키기 위해 후자와 관련한 콜로니얼 파이프라인, 솔라윈즈 사태 등도 간략히 언급하였다.

이 연구는 이러한 사례들의 발생에 대해 국가 차원에서 어떤 대응이 있는지 탐구하였고, 특히 어떤 나라들보다, 안보화하고 관련 대응책을 앞서 제시하고 있는 미국에 초점을 맞추었다. 대체로 행정명령을 통해 발 빠르게 대처하려하는 모습과 사이버안보전략서 발간을 통해 전체적 노력들을 체계화하고 있었다.[17] 그리고 연방 예산안을 통해 공급망을 재편 하려고 하였으며, NIST나 CISA를 통해 공급망의 데이터안보 차원을 관리하기 위한 구체적인 표준, 규범, 규제를 설립해 나가고 있다.

예를 들어, 솔라윈드 사건 이후 2021년 5월에 나온 바이든 대통령의 행정명령 14028(Executive Order on Improving the Nation's Cybersecurity)은 SBOM과 같은 소프트웨어 공급업체들에 대한 보안 요구 사항들을 담고 있다. 해당 명령에 따라 상무부 산하 NIST가 표준, 도구, 모범 사례 및 기타 가이드라인을 작성하고, CISA가 가이드라인 운영을 맡았다. 또한 해당 행정명령 14028은 2022년 '미국 사이버 보안 강화법(Strengthening American Cybersecurity Act of 2022)'의 의회에서의 통과로 이어졌다. 그리고 이러한 통

[17] 미국 행정명령을 모아 놓은 사이트로 다음을 참조하라(Federal Register 2024).

과에 이어 2022년 9월 백안관이 글로벌 소프트웨어 공급망의 현황을 다루는 각서를 발표한다. 해당 각서들은 공급망안보와 데이터안보가 교차하는 영역으로서의 소프트웨어에 집중하고 있다.

2024년에는 공급망안보와 데이터안보가 교차하는 영역에서의 위협에 대해 행정명령을 통한 대처가 적극적으로 나타났다. 행정명령 14117(Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern)은 데이터안보의 차원에서 공급망안보, 데이터 브로커들 그리고 해저케이블에 대한 언급을 하고 있다. 행정명령 14116(Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States)은 중국산 선박 및 육상 크레인에 대한 해양보안 지침을 마련케하고, 해양운송시스템 등 관련 시스템의 보안 강화, 항구 크레인 생산 능력 향상을 위한 계획 등을 포함하고 있다. 해양 사이버안보, 데이터안보, 공급망안보 등의 안보적 고려뿐 아니라 '미국에 투자하기' 아젠다의 일환이기 때문에, 산업정책적 개입의 성격도 함께 띠었다.

이렇게 데이터안보와 공급망안보의 교차점을 인식하고 대처가 명시되는 행정명령은, 시기를 거슬러 올라가자면 2019년까지 추적할 수 있다. 2019년에 나온 행정명령 13873(Securing the Information and Communications Technology and Services Supply Chain)은 적대적 외부 세력에 의한 지침이나 사법권에 종속되거나 통제되거나, 소유되거나 하는 개인들에 의해 설계되거나, 개발되거나, 제조되거나 공급되는 정보통신기술의 취득, 수입, 이전, 설치, 취급과 같은 거래를 금지한다. 이러한 금지의 이유 중 하나가 그러한 기술이나 서비스에 의해 데이터가 절취되거나, 위조, 삭제 또는 접근이 제한될 수 있기 때문이다.

대통령에 의한 행정명령에 이외에도, 입법을 통해서도 데이터안보와 공급망안보의 교차 영역으로부터의 위협에 대처하고 있다. 예를 들어 '2018년 연방 획득 공급망 보안법(Federal Acquisition Supply Chain Security Act of 2018)'은 고위험군으로부터 연방 정보통신기술 공급망을 보호하기 위한 몇 가지 주요 프로토콜을 수립하고 있다. 연방조달보안위원회(Federal Acquisition Security Council, FASC)를 설치하며, 위험평가와 완화, 배제와 제거의 명령, 규정 준수 요구, 정보 공유 등의 역할을 수행함으로 고위험 소스(source) 또는 손상된 제품의 잠재적 위협으로부터 연방 ICT 공급망의 보안과 무결성을 강화하는 것을 목표로 한다.

또 다른 예로 2019 회계연도 국방수권법안(National Defense Authorization Act, NDAA)을 들 수 있다. 889절에 따르면 화웨이(Huawei), ZTE와 같은 중국 기업들이 제공하는 통신 및 비디오 감시 장비에 대한 국가안보적 우려를 표명하고 있으며, 단순히 최종 제품

에만 국한되지 않고, 해당 부품이 중요한 구성 요소로 포함된 시스템까지 포함하여, 계약업체들이 공급망을 철저히 점검하도록 요구한다.

상기와 같은 행정명령들 또는 입법 과정을 통해서, 연방정부 행위자에게는 다음과 같은 권한 그리고 역할이 부여되었다. 첫째로, 리스크 평가인데, 예를 들어, 국가정보국장(Director of National Intelligence, DNI) 같은 경우 정보통신기술이나 서비스로부터의 미국과 미국시민들에 대한 위협을 관련 부처와 함께 지속적으로 평가하게 되어 있다. 둘째로 리스크 관리이다. 한 측면으로서 감독 권한을 들 수 있다. 연방정부는 국가안보를 위협하는 거래에 대해 개입할 수 있으며, 공급업체와 같은 사업자들로 하여금 자신들의 사업 행위에 대해 점검을 명령할 수 있다. 주요인프라에 사용되는 디지털 정보통신기술의 공급망안보를 확보하고, 데이터안보를 확보하는 차원에서 중요한 권한이자 기능이라 할 수 있다. 이러한 기능은 민관 협력을 통한 리스크 관리이기도 하다.

민관 협력을 통한 사이버 리스크 관리의 대표적 기구로 CISA를 들 수 있다. CISA는 'ICT 공급망 위험 관리(SCRM) 태스크 포스(ICT Supply Chain Risk Management (SCRM) Task Force)'를 2018년에 11월에 설립되면서 12월에 바로 구성한다. 이 사실만 보더라도 미국에서 사이버안보와 공급망안보가 얼마나 긴밀하게 연결시켜 인식하고 있는지를 알 수 있으며, 또한 정부와 민간이 협력해야 할 사안이라는 것을 인식하고 있다. TF는 제품 설계, 개발, 유통, 유지보수 과정에서 발생하는 위험을 포함하여 ICT 공급망 내에서 중요한 위험 영역을 식별하는 데 중점을 두었다. 2023년 1월에는 '중소기업(SMB) 공급망 보호: 정보 및 통신 기술 리스크를 줄이기 위한 리소스 핸드북'을 발간하며, 중소 규모의 사업자들을 위한 공급망 안보 확보 방안을 담았다. 그리고 이를 지원하기 위한 C-SCRM 프로젝트 관리실(C-SCRM Project Management Office)이 2022년 7월에 출범한다.

위에서 데이터안보가 먼저 타협되며 공급망안보가 위협을 받는 경우도 언급한 바 있다. 이러한 사건들을 염두에 두고 제정된 법안으로 2021년 9월에 도입된 '중요 기반 시설에 대한 사이버 사고 보고법(Cyber Incident Reporting for Critical Infrastructure Act, CIRCIA)'을 들 수 있다. 해당 법은 크게 세 가지 법적 책무를 발생시키는데, 사이버 사고 보고, 랜섬웨어 지불 보고, 연방 기관에 의한 사고 보고서를 CISA와 공유해야 한다. CIRCIA는 전반적인 사이버안보 복원력과 대응 역량의 향상이라는 목적을 위해서, 주요인프라와 관련한 사이버안보 체계의 중요한 발전이며, 사이버 사고 보고를 표준화하고 중앙 집중화하는 과정으로 볼 수 있다.

지금까지 미 행정부에서 나온 행정명령을 보면, 데이터안보와 공급망안보에서의 보호 대상이 비교적 국한되어 있는 모습이다. 그런데, 앞으로 첨단기술의 발전이 경제성장, 방위 역량 그리고 전략경쟁의 승패에 매우 중요한 요소라고 인식되고 있는 상황에서 공급망안보

와 데이터안보가 중첩되는 영역은 앞으로 더욱 확장될 것으로 예상된다. 최근 들어 상무부에서 나오고 있는 '정보통신기술 및 서비스 프로그램(Information and Communications Technology and Services (ICTS) Program)'이 변화되어 가는 모습을 보이고 있다. 해당 프로그램은 산업보안국(Bureau of Industry and Security)의 '정보통신기술 및 서비스 실(Office of Information and Communciations Technology and Services, OICTS)'에서 담당하고 있는데, 기술 우선순위(2024 Technology Prioritization) 표를 보게 되면, 기술공급망안보와 사이버안보가 동시에 중요하게 다루어지고 있음이 보인다. 국방부 차원에서도 사이버보안성숙도모델인증(Cybersecurity Maturity Model Certification, CMMC)을 도입하여, 국방부 계약자들과의 거래시에 고려해야 할 데이터의 민감도에 따라 취해야 할 보안수단들을 제시하고 있다.

국가 사이버안보 전략서에서도 점차 데이터안보와 공급망안보의 교차점을 다루고 있다. '2024년 미국의 사이버안보 태세에 대한 보고서'에서는 '더 안전한 제품 및 서비스 생산을 위한 소프트웨어 보안 강화(Advancing Software Security to Produce Safer Products and Services)'를 강조하고 있다. 동시에 '데이터 보안 및 개인정보 보호에 대한 위험 관리(Managing Risks to Data Security and Privacy)'를 언급한다. 전략서는 데이터안보와 공급망안보가 교차하고 있다는 사실을 인식하며, 설계에 의한 보안 촉진(Promoting Secure by Design) 원칙, SBOMs의 이행, 메모리 안전 프로그래밍 언어(memory-safe programming languages) 사용 등의 대처 방안의 채택을 장려하고 있다.

참고문헌

김상배. 2019. "화웨이 사태와 미중 기술패권 경쟁: 선도부문과 사이버 안보의 복합지정학."『국제지역연구』28권 3호, 125-56.

김상배. 2020. "데이터 안보와 디지털 패권경쟁: 신흥안보와 복합지정학의 시각."『국가전략』26권 2호, 5-34.

박예송. 2024. "라이다, 미중 간 새로운 긴장 요소로 자리 잡았다." https://www.epnc.co.kr/news/articleView.html?idxno=240294(검색일: 2024. 09. 24).

유인태. 2019. "캐나다 사이버 안보와 중견국 외교: 화웨이 사례에서 나타난 안보와 경제·통상의 딜레마 속에서."『문화와 정치』6권 2호, 263-98.

유인태. 2021. "디지털 패권 경쟁 속에서 중견국 연대 외교의 갈림길: 화웨이 사례에서 보는 파이브 아이즈의 연대와 일탈."『동서연구』33권 2호, 5-31.

유인태. 2023. “첨단 과학 기술의 국제정치: 차세대 네트워크 인프라, 인공지능 분야에서의 한·미 간 협력.”『동서연구』35권 4호, 5-28.

유인태. 2024. “경제, 사이버, 안보의 이중 사안 연계: 혁신, 기술 보안, 미중 전략 경쟁의 넥서스 분석.”『국가와 정치』30집 1호, 39-82.

유효정. 2024. “데이터 유출 논란에도...DJI, 첫 美 매장 오픈.” https://zdnet.co.kr/view/?no=20240308034023(검색일: 2024. 09. 24).

Bacon, Madelyn. 2018. “Compromised Supermicro chips reportedly infiltrated US.” https://www.techtarget.com/searchsecurity/news/252450114/Compromised-Supermicro-chips-reportedly-infiltrated-US(검색일: 2024. 09. 24).

Bureau of Industry and Security. 2024. “Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles.” https://www.federalregister.gov/documents/2024/03/01/2024-04382/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles(검색일: 2024. 09. 24).

Burgan, Cate. 2023. “CISA Eyes C-SCRM Training Resources, Information Hub.” https://www.meritalk.com/articles/cisa-eyes-c-scrm-training-resources-information-hub(검색일: 2024. 09. 24).

Buzan, Barry, Ole Waever, and Jaap de Wilde. 1998. Security: A New Framework for Analysis. Boulder, CO: Lynne Rienner Publishers.

Chen, Frank. 2023. “Shenzhen trip, DJI visit by China’s vice-premier offers ‘no-limits support’ amid US tech curbs.” https://www.scmp.com/economy/china-economy/article/3238118/shenzhen-trip-dji-visit-chinas-vice-premier-offers-no-limits-support-amid-us-tech-curbs(검색일: 2024. 09. 24).

Committee on Homeland Security. 2024. “WTAS: Joint Investigation into CCP-Backed Company Supplying Cranes to U.S. Ports Reveals Shocking Findings.” https://homeland.house.gov/2024/03/12/wtas-joint-investigation-intoccp-backed-company-supplying-cranes-to-u-s-ports-reveals-shocking-findings(검색일: 2024. 09. 24).

Confessore, Nicholas. 2018. “Cambridge Analytica and Facebook: The Scandal and the Fallout So Far.” https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout

.html(검색일: 2024. 09. 24).

Congress.gov. 2018. "Text – S.3085 – 115th Congress (2017–2018): Federal Acquisition Supply Chain Security Act of 2018." https://www.congress.gov/bill/115th-congress/senate-bill/3085/text(검색일: 2024. 09. 24).

Congress.gov. 2021. "H.R.5440 – 117th Congress (2021–2022): Cyber Incident Reporting for Critical Infrastructure Act of 2021." https://www.congress.gov/bill/117th-congress/house-bill/5440(검색일: 2024. 09. 24).

Cybersecurity and Infrastructure Security Agency. 2022. "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Fact Sheet." https://www.cisa.gov/sites/default/files/2023-01/CIRCIA_07.21.2022_Factsheet_FINAL_508%20c.pdf(검색일: 2024. 09. 24).

Cybersecurity and Infrastructure Security Agency. 2024. "Federal Civilian Executive Branch Agencies List." https://www.cisa.gov/news-events/directives/federal-civilian-executive-branch-agencies-list(검색일: 2024. 09. 24).

Department of Defense Chief Information Officer. 2024. "About CMMC." https://dodcio.defense.gov/CMMC/About(검색일: 2024. 09. 24).

DoD CUI Program. 2024. "Cybersecurity Maturity Model Certification." https://www.dodcui.mil/CMMC/Cybersecurity-Maturity-Model-Certification(검색일: 2024. 09. 24).

Dyer, Steve, Yuan Yao, and Jack Zhang. 2023. "China's Proposed Export Ban on LiDAR Technology: What Impact Will It Have on the Automotive Industry?" https://insights.alixpartners.com/post/102ic0t/chinas-proposed-export-ban-on-lidar-technology-what-impact-will-it-have-on-the(검색일: 2024. 09. 24).

Fahye, Elaine, and Fabien Terpan. 2021. "Torn between Institutionalisation & Judicialisation: The Demise of the EU-US Privacy Shield." Indiana Journal of Global Legal Studies 28(2): 205-44.

Farrell, Henry, and Abraham L. Newman. 2018. "Linkage Politics and Complex Governance in Transatlantic Surveillance." World Politics 70(4): 515-54.

Federal Register. 2024. "2024 Joseph R. Biden, Jr. Executive Orders."

https://www.federalregister.gov/presidential-documents/executive-orders/joe-biden/2024(검색일: 2024. 09. 24).

Haas, Ernst B. 1980. "Why Collaborate? Issue Linkage and International Regimes." World Politics 32(3): 357-405.

Leebron, David W. 2002. "Linkages." The American Journal of International Law 96(1): 5-27.

Martin, Alexander. 2022. "Fishing vessel, not sabotage, to blame for Shetland Island submarine cable cut." https://therecord.media/fishing-vessel-not-sabotage-to-blame-for-shetland-island-submarine-cable-cut(검색일: 2024. 09. 24).

Monette, Emile. 2018. "Cyber Supply Chain Risk Management: Program Briefing." https://csrc.nist.gov/CSRC/media/Projects/cyber-supply-chain-risk-management/documents/SSCA/Winter_2018/CISA%20C-SCRM%20Overview_SSCA%20Winter%202018.pdf(검색일: 2024. 09. 24).

National Archives. 2024. "CUI Categories." https://www.archives.gov/cui/registry/category-list(검색일: 2024. 09. 24).

Office of Information and Communications Technology and Services. 2024. "2024 Technology Prioritization." https://www.bis.doc.gov/index.php/documents/oicts/3520-2024-oicts-prioritization-table/file(검색일: 2024. 09. 24).

Office of Management and Budget. 2021a. "Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response." https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf(검색일: 2024. 09. 24).

Office of Management and Budget. 2021b. "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents." https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf(검색일: 2024. 09. 24).

Office of Management and Budget. 2022a. "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices."

https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf(검색일: 2024. 09. 24).

Office of Management and Budget. 2022b. "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles." https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf(검색일: 2024. 09. 24).

Office of the National Cyber Director. 2024. "Fact Sheet: 2024 Report on the Cybersecurity Posture of the United States." https://www.whitehouse.gov/oncd/briefing-room/2024/05/07/fact-sheet-cybersecurity-posture-report(검색일: 2024. 09. 24).

Redspin. 2023. "The Relationship Between CMMC & NIST SP 800-171." https://redspin.com/white-papers/the-relationship-between-cmmc-and-nist(검색일: 2024. 09. 24).

Sevastopulo, Demetri. 2022. "Chinese drone maker lobbies to defeat US national security ban." https://www.ft.com/content/8636c764-40ea-4544-8b1f-0b2f1bb417a8(검색일: 2024. 09. 24).

Sevastopulo, Demetri. 2023. "House panel seeks ban on US government purchases of Chinese drones." https://www.ft.com/content/a4c4eaea-2409-4a53-90aa-71d066843018(검색일: 2024. 09. 24).

Sutter, Karen M., and Kelley M. Sayler. 2024. "U.S.-China Competition in Emerging Technologies: LiDAR." https://crsreports.congress.gov/product/pdf/IF/IF12473(검색일: 2024. 09. 24).

Snyder, Tanya. 2023. "The sensors in those self-driving cars have become an international dispute." https://www.politico.com/news/2023/12/28/auto-safety-tech-is-the-newest-front-of-the-u-s-china-trade-war-00130848(검색일: 2024. 09. 24).

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(검색일: 2024. 09. 24).

The White House. 2023a. "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(검색일: 2024. 09. 24).

The White House. 2023b. "National Cybersecurity Strategy Implementation Plan." https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf(검색일: 2024. 09. 24).

The White House. 2024. "Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern(검색일: 2024. 09. 24).

United States House Select Committee on Strategic Competition between the United States and the Chinese Communist Party. 2023. Lidar Letter. https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/2023-11-28-lidar-letter-final_0.pdf(검색일: 2024. 09. 24).

Viswanatha, Aruna, Gordon Lubold, and Kate O'Keeffe. 2023. "Pentagon Sees Giant Cargo Cranes as Possible Chinese Spying Tools." https://www.wsj.com/articles/pentagon-sees-giant-cargo-cranes-as-possible-chinese-spying-tools-887c4ade(검색일: 2024. 09. 24).