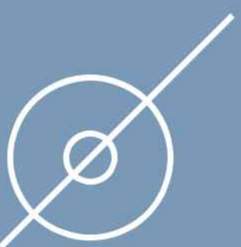
사이버 안보와 경제



2023

한국사이버안보학회
KACS

한국사이버안보학회 워킹페이퍼 6호
발간일: 2023년 12월 28일

유인태 (단국대학교)

〈요 약〉

이 글은 크게 하드웨어, 소프트웨어, 데이터로 분류될 수 있는 사안들이, 경제와 사이버 안보의 연계 넥서스가 되는 사례들을 다룬다. 전반부에서는 사건들, 후반부에서는 국가 정책들에 집중한다. 하드웨어 관련해서, (기술)제품 생산과 서비스를 위한 기간망뿐 아니라, 데이터가 이동하는 정보통신 기간망에 대한 사이버 위협들을 본다. 미국 바이든 대통령 취임 이후, 2021년 5월 미국 동부의 연료를 공급하는 콜로니얼 파이프라인 회사, 6월의 JBS 육류가공회사에 대한 랜섬웨어 공격이 크게 화제가 되었었다. 2023년 3월에는 미국 국방 정보국이 제기한 중국 ZPMC 기업의 대형 크레인과 운용 소프트웨어의 위협이다. 미국에서의 담론은 마치 화웨이의 5G 사태 때와 유사한 전개를 보이고 있다. 소프트웨어 넥서스는 2020년 소프트웨어 공급망 공격 사태로 잘 알려진 솔라윈즈 해킹 사태로 대두되었다. 데이터 넥서스는 데이터 안보와 관련한 수많은 사건들이 알려져 있다. 2015년 미국 연방인사관리처 해킹, 2016년 연방예금보험공사 해킹, 그리고 2007년 중국 해커에 의한 록히드마틴 회사 침투를 통한 F-22, F-35 스텔스 전투기, 2017년 북한에 의한 F-15 전투기, 2018년 중국 해커에 의한 초음속 대함 미사일 세부 계획, 등 민감정보 관련 데이터 절취(cyberespionage)는 경각심을 일으킨 사건들이다. 그 외에도 (전쟁 혹은 민주적 선거 기간 중) 허위정보나, (민간 기업 또는 첩보 기관에 의한) 개인 사생활 침해와 관련한 데이터 안보 문제도 여럿 제기되었다. 최근 2022년 미국 의회는, 국가 안보 상의 이유로 중국의 짧은 동영상 공유 플랫폼 '틱톡' 사용 금지 결정을 내리기도 하였다.

여러 국가들이, 경제, 사이버 보안, 국가 안보를 연계해 왔지만, 특히 미국은 그러한 면모를 강하게 보여왔다. 하드웨어와 관련한 사이버 보안 문제가 크게 제기된 것은 2018년경부터의 중국 화웨이 기업의 5G 인프라에 관한 것이었지만, 그 이후의 미국의 주요 대응은 수출통제 정책들을 통해 이루어졌다, 그리고 수출통제 정책들은 미국의 경제적 이익 도모, 기술적 우위 고수, 사이버 보안 강화, 그리고 국가 안보 확보라는 경제와 안보를 강하게 연계시키는 인식에 기반한다. 소프트웨어 관련해서는, 대내적으로 '제로트러스트' 개념에 기반하여 '소프트웨어 자재명세서(SBOM)' 등이 제시된다. 위협 요소들을 공급망에서 배제하는 방향을 취하는 방향으로 상기의 정책들이 도입된 것에 반해, 데이터 넥서스 관련해서는 자유로운 국경 간 이동을 지향하기 때문에, 경제와 안보의 연계 전략은 그에 맞게 조정되었다. 무역 협정들은 데이터의 자유로운 이동을 위해, 경제와 안보 연계의 가시성을 낮추었으며, 유사한 맥락에서 미국과 EU 간의 '세이프 하버'나 '프라이버시 실드'도 운용되어 왔다. 대조적으로 '클라우드법'은 공공 질서나 국가 안보와의 연계를 통해, 데이터의 자유로운 이동을 촉진하는 미국의 정책으로 2020년 부상하였다. EU 및 다른 나라들도 유사한 제도를 준비해나가고 있지만, 경제와 안보의 연계는 다양한 양상을 띨 것이다.

I. 사안 연계 넥서스: 하드웨어, 소프트웨어, 데이터

이 연구는 경제와 사이버 보안 나아가 국가 안보가 연계되는 사례들을 보인다. 연계에 있어 연결고리가 되는 넥서스(nexus)는 크게 세 부류로 구분한다. 하드웨어, 소프트웨어, 데이터라는 세 부류를 연계의 넥서스 또는 사안 영역으로 본다. 각각의 분류에 따라 취급되는 사례들은 지면의 한계상, 제한적일 수밖에 없는데, 다음의 범위로 한정한다. 하드웨어에는 물리적 기간망, 기술제품 등을 포함한다. 소프트웨어는 각종 프로그램이나 애플리케이션, 그리고 데이터에는 전자기기를 통해 발생하여 전송되는 모든 디지털 데이터가 포함된다. 그런데 각각의 분류는 종종 중첩되기도 한다. 예를 들어, 특정 공급망과 같은 경우, 물리적 기반을 지칭할 때는 하드웨어에, 공급망을 통해 제공되는 서비스를 의미하는 경우 소프트웨어에, 소프트웨어를 통해 전송되는 정보를 지적할 때는 데이터에 포함하는 것과 같이, 여러 분류에 속할 수 있는 지칭 대상이다. 예를 들어, 중국 기업 화웨이의 5G 물리적 기간망은 경제 성장의 하드웨어이면서, 운용을 위해 내포된 소프트웨어에 의해 연결된 기기들이 조작될 수 있는 가능성에 대해, 그리고 소프트웨어를 통해 데이터(혹은 기밀 정보)가 차단 및 변형되거나 원하지 않는 대상에게 이동될 수 있는 가능성에 대한 우려가 종합적으로 제기되었다. 어느 정도의 중첩적인 성격을 감안하더라도, 다양한 사례들을 체계적으로 분류하는 것은, 전통적으로 구분되어 인식되던 사안 영역들을 가로질러 공통적으로 일어나는 현상들을 찾아내거나 또는 그들 간의 미묘한 차이를 식별해내는 데에 유용하다. 이 글은 위와 같은 세 분류에 따라, 분석의 전반부는 사건들을 후반부는 정부 정책을 분석한다.

사례 분석 방법의 특성상, 모든 사례들을 하나의 글에 담을 수 없으며, 연구 목적에 맞게 선택된다. 그럼에도 불구하고, 가급적 기존 연구에서 비교적 덜 주목된 사례들을 다루거나, 혹은 기존 연구에서 자주 언급된 대표적 사례일 경우, 연계가 일어나는 과정에 대한 상세한 내용을 기술하여, 기존 연구에 더하고자 한다.

경제, (기술)사이버 보안, 그리고 국가(사이버) 안보의 연계는, 연계시키려는 행위자들의 특수한 목적에 맞는 성격을 띤다. 즉, 연계시키려는 목적에 따라, 서로 다른 사안 영역들이 연계되더라도 특정한 사안 영역의 특성이 더 강조되기도 한다. 여기서는 국가(사이버) 안보가 강조되는 연계 사례들에 집중적으로 다룬다. 이러한 사례들은, 전통적으로 민간이 주로 담당하던 경제적 사안들, 또는 흔히 하위 정치(low politics) 사안들이라 여겨졌던 것들이, 그러한 사안들의 사이버 보안적 측면이 더해지면서, 국가 사이버 안보의 위기가 강조되고, 정부 행위자들의 재량이 커지는 과정이 수반되는 경향을 보인다.

1. 하드웨어 넥서스

사이버 안보화는 생산 및 서비스 제공을 위한 물리적 주요 인프라망에서의 사이버 보안 사건이 사이버 안보와 연계되며 진행되었다. (기술)제품 생산과 서비스를 위한 기간망뿐 아니라, 데이터가 이동하는 정보통신 기간망에서도 사이버 위협 사건이 크게 부각되며, 사이버 안보의 중요성이 더욱 높아졌다. 이러한 중요 사건들은 국가의 사이버 영역에 대한 개입을 촉진하고 경제와 사이버 보안의 사안들의 연계를 확산시키는 계기를 제공하였다.

정부가 물리적 기간망(physical infrastructure network)의 사이버 안보에 대한 관심을 높이게 된 계기로, 그 국가가 경험한 다수의 큰 사건들이 존재한다. 예를 들어, 미국의 바이든 정부는 공급망의 사이버 안보에 관한 여러 정책들을 내놓는데 이러한 행보의 이면에는 취임 초기부터

공급망 사이버 안보에 대해 관심이 높아질 수밖에 없었던 사건들이 있었기 때문이다. 2021년 1월 취임한지 얼마 되지 않아 발생한 미국의 주요 공급망에 대한 심각한 랜섬웨어 공격은 한 예이다. 2021년 5월 미국 동부의 연료를 공급하는 콜로니얼 파이프라인(Colonial Pipeline)을 타깃으로 하는 사이버 공격은, 미국 사회 전체에 공급망 사이버 안보의 중요성에 대한 경각심을 불러 일으킨 사건었다.[1] 콜로니얼 파이프라인은 미 동부 해안 지역에서 소비되는 연료의 45%를 공급하는 주요 인프라이다. 그런데 단 한 번의 랜섬웨어 공격으로 5500 마일의 파이프라인이 마비되었고, 복구를 위해 440만 달러를 지급해야 했다. 그리고 같은 해 6월에 JBS 육류가공회사도 랜섬웨어의 피해를 입으며 식량 공급망의 안정성에 큰 위기감이 고조되기도 했다. 랜섬웨어 사건은 여러 민간 기관에 적지 않게 일어나는 침해이지만, 특히 상기의 사건은 정부의 대응을 촉발했다.

물론 물리적 기반시설 취약성에 대한 경고가 기존에 없었던 것은 아니다. 사건이 발생하기 전 보안 업체 맨디언트(Mandiant)는 보고서를 통해 랜섬웨어 패밀리들이 2017년부터 산업 제어 시스템을 집중적으로 노리고 있다는 경고를 한 바 있으며, 사건 10개월 전에는 CISA는 국토안보부가 발표했던 '파이프 라인 사이버 보안 계획(Pipeline Cybersecurity Initiative)'를 다시 한번 강조하는 권고문을 내기도 했었다.[2] 하지만 결과적으로 사건이 발생하며, 사이버 공격에 비해 얼마나 미비 그리고 낙후 했는지 그리고 주요 인프라 경영자 혹은 운영자들의 인식이 얼마나 낮았는지를 일깨우는 사건이 되었다.

또 다른 유형의 공급망이 사이버 공간과 결합되며, 사이버 안보의 대상으로 부상한다. 2023년 3월 미국에서 특히 대두된 것은 물류 및 교통을 지원하기 위한 물리적 주요 인프라가 사이버 공격의 수단이 된다는 의혹이다. 미국 국방 정보국(Defense Intelligence Agency)이 미국 전역에 있는 항구에 있는 대형 크레인이 중국산이며, 잠재적 스파이 도구로 지목했다. 대형 크레인은 항구와 선박 사이에서 컨테이너를 옮기는 데 사용되는데, 이러한 크레인에는 출처와 행방을 등록 및 추적할 수 있는 센서가 달려 있어, 중국 본사에 크레인 현황을 모니터링 할 수 있다는 것이다. 더 큰 문제가 되는 것은 미군이 해외 작전에 동원되는 물자 등을 이동시킬 시, 이에 대한 정보를 수집할 수 있게 된다는 것이다. 나아가, 크레인 운용 프로그램이 사이버 공격에 취약해, 중국군이 원격으로 크레인을 망가뜨릴수 있으며, 그럴 경우, 해군을 동원하지 않고도 미국 항구를 마비시킬 수 있다는 우려도 제기되었다.

미 정부 당국이 특히 우려하고 있는 것은 ZPMC(Shanghai Zhenhua Heavy Industries, 중국명 '상하이전화(上海振華)중공업')의 대형 크레인이다. ZPMC는 서방 회사들보다 값싼 가격으로 크레인으로 판매하여 전 세계 크레인 시장의 70%를 차지하고 있는 것으로 알려져 있으며, 미국에서는 80%가 ZPMC 제조의 크레인을 사용하고 있다. ZPMC 크레인은 대체로 중국에서 완전히 조립되어 미국에 양도되며, 중국제 소프트웨어를 통해 운용된다.

ZPMC의 크레인이 특히 국가 안보에의 위협으로 우려된 이유로는, ZPMC가 시진핑 중국 국가주석이 주창한 '일대일로' 사업의 주요 계약자인 중국의 국영기업 '중국교통건설'의 자회사이며, 미국 당국은 중국교통건설이 민군(military-civil) 융합 프로그램에 기여하고 있는 것으로 보고 있기 때문이다.[3] 2021년에는 FBI가 볼티모어항으로 ZPMC 크레인을 운반해 온 화물선에 정보 수집 장비가 실려온 것을 발견했다고 보도되기도 하였다.

---

1) 러시아의 소행으로 추정되는 이 당시 사이버 공격은, 우크라이나의 영토회복이나 군비통제와 함께, 2021년 6월 미·러 정상회담의 아젠다에 상정된다. 바이든은 16개의 주요 인프라 부문의 리스트를 제시하며, 이에 대한 공격은 국제 사이버 안보 규범에 어긋나며, 미국이 설정한 레드 라인을 넘는 것이라고 경고한 바 있다.

2) https://www.reversinglabs.com/blog/black-hat-colonial-pipeline-ransomware-attack-no-surprise

3) https://www.wsj.com/articles/pentagon-sees-giant-cargo-cranes-as-possible-chinese-spying-tools-887c4ade

이에 미 의회는 2022년 12월 8500억 달려 규모의 국방예산안인 국방수권법(NDAA)를 통과시키며, 교통부에 국방부 및 다른 기관과 논의하여 해외에서 제조된 크레인이 미국 항구의 사이버 안보와 국가 안보에 미치는 영향에 대한 보고서를 만들도록 요구하였다. 공화당 소속의 카를로스 히메네스(Carlos Jimenez) 하원의원은 중국산 크레인을 구입하지 못하도록 하는 법안을 제안하기도 했다. 이제 중국산 크레인이 현대판 '트로이의 목마'로 비유되고 있으며, 위와 같은 일련의 흐름은 2018년부터 벌어진 5G를 둘러싼 화웨이 사태 때와 비슷한 흐름의 양상을 보이기 시작했다(유인태 2021).

주요 정보통신인프라 또한 국가 경제를 받치고 있는 핵심 인프라의 대표적인 예이다. 현대전의 첫 번째 공격타깃이 정보통신망이라는 것은 이제 상식에 가깝다. 최근의 러시아-우크라이나 전쟁 개시 전에도, 주요 정보통신인프라에 대한 공격 선행이 이루어졌다. 정보통신인프라에 의존하고 있는 것은 군 뿐만이 아니다. 현대 사회의 주요 부문, 특히 첨단 부문은 더욱 그 의존도가 커서, 첨단 기술의 최대 능력치의 구현을 위해서는 3대 정보보안의 가치(비밀성, 무결성, 가용성, CIA)를 기본으로 고용량의 빠른 데이터 이동이 가능해야 한다. 예를 들어, 4차 산업혁명의 대표적 기술인 무인자동차의 운용을 위해서, 자체 인공지능의 성능도 중요하지만, 외부와의 정보이동이 원활할 때 더욱 완벽한 자율주행이 가능해진다.

이러한 맥락에서 5G와 같은 차세대 네트워크 인프라는 국가 전략 상으로도 종종 강조된다. 5G 네트워크는 향후 초연결사회에서의 모든 것을 연결하는 신경망과도 같아서, 그야말로, 경제, 안보, 정치, 문화 모든 영역을 가로질러 중요한 인프라이며, 모든 산업의 기술, 표준, 공급망 등에 공통으로 영향을 미칠 인프라이다. 이에 따라 5G와 관련한 사이버 안보 이슈는 이미 국제정치, 경제 성장, 기술 표준 등의 이슈들과 연계 되어 연구가 되어 왔다(김상배 2022; 유인태 2023).

5G는 경제 혁신의 핵심 인프라로 인식되며, 동시에 국가 간 경쟁의 주요 이슈로 부상하였고, 그 가운데 5G의 사이버 안보 측면은 그야말로 강대국 간 경쟁의 핵심 사안이 되었다. 여러 다른 인프라 관련 기업들 중에서도, 특히, 화웨이가 지목되었던 것은 그 기업의 경쟁력 뿐 아니라 정치적 연결성 때문이다. 화웨이는 5G 분야에서 뛰어난 기술 및 가격 경쟁력을 가지고 있었는데, 이러한 경쟁력을 바탕으로 글로벌 시장에서 꾸준히 확장해 가며, 글로벌 이동통신장비 업계 1, 2위였던 에릭슨과 노키아를 추격하여, 2018년에는 시장점유율에서 우위를 점하게 되었다. 이러한 정치경제적 위기감 뿐 아니라, 화웨이의 기원도 미국의 사이버 안보에 대한 우려를 한층 높였다. 화웨이 기업의 성장 역사나 최고경영자의 경력을 보았을 때, 중국공산당과 인민해방군과의 정치경제적 유착 개연성은 농후해 보였다. 게다가 5G 시스템은 공급업체가 제공하는 소프트웨어 갱신에 의존하기 때문에, 도입 당시에는 없었더라도, 나중에 언제든지 악성코드를 심는 것이 가능하였기 때문에, 중국의 통신 장비가 미국 국내 뿐 아니라 전 세계 시장에서 지배적인 인프라가 된다는 것은 전략 경쟁을 개시한 미국에게는 악몽과도 같은 시나리오였다.

후술하는 바와 같이 미국이 중국 기업인 화웨이에 대해 철저하게 제재를 가해 온 것은, 화웨이가 가지는 미래 첨단 산업 기술의 군사·사회·경제적 파급력에 대한 우려도 있지만, 근본적 우려는 3대 정보보안의 가치가 타협될 수 있다는 데이터 안보적 측면도 존재한다. 그리고 이러한 측면 또한 국가 안보 우려로 이어진다(유인태 2021). 즉, 화웨이는 공산당과 긴밀히 연결되어 있다고 의심되며, 화웨이가 제공하는 정보통신 제품과 서비스는 '백도어'를 통해 기밀이 탈취될 수도 있었고, 정보가 왜곡될 수 있었고, 극단적으로는 '킬 스위치'를 통해 사회 시스템의 전반적 혹은 부분적 작동 불능이라는 시나리오도 가능했기 때문이다. 즉, 비밀성, 무결성, 가용성 모든 면에서의 사이버 안보가 타협될 수 있었다.

이러한 화웨이에 대한 우려는 해당 기업의 5G 시장에서의 경쟁력과 시장에서의 확대 경향, 코로나19 시기에 급증한 인터넷 사용, 2022년 러시아-우크라이나 전쟁, 그리고 트럼프 정부 이후 미중 전략경쟁의 심화에 따라 더욱 커졌었다(Yoo 2022). 5G 이슈는, 여타 첨단 기술 관련 미중 경쟁과 유사하게, 기술 경쟁력, 경제·산업 경쟁력 뿐 아니라 사이버 안보와 국가 안보에 대한 고려가 혼합되어, 국제 정치의 상호작용 양상에 영향을 미쳤다.

경제적 사안이, 사이버 공간을 통해, 국가 간 상호 작용에 영향을 미치는 사례는 비단 미국에 국한되지 않는다. 또 다른 5G에 대한 국가의 대응에 정부의 전략적 연계가 중요한 사례로 독일을 들 수 있다. 독일은 2018년 중국 화웨이의 5G에 대한 제재 압력이 서방 강대국으로부터 요구되었음에도 불구하고, 동참하지 않고 있었다. 2021년에 올라프 숄츠(Olaf Scholz)가 총리가 되고,[4] 최근 독일 정부는 독일의 통신장비회사들의 화웨이 장비 사용을 줄이게 하기 위한 프로포절을 제출하였다.[5] 독일의 국가 전략이 중국을 파트너로 뿐 아니라, 동시에 세계 시스템 상에서의 경쟁상대(rival)로 인식하기로 전환한 것에 기인한다.

2. 소프트웨어 넥서스

위와 같이 에너지, 식량과 관련한 공급망의 운용에서만 사이버 위협이 제기된 것은 아니다. 소프트웨어와 같은 비물리적 제품 혹은 서비스에서도 사이버 위협이 부상했다. 유례없는 소프트웨어 공급망 공격 사태로 알려진 솔라윈즈(SolarWinds) 해킹 사태를 예로 들 수 있다. 솔라윈즈 사태는 공급망 공격(supply chain attack)이었다.[6] 여기서 공급망 공격이란 제품이 개발되거나 생산되어지는 망을 공격해서 이후의 단계에 영향을 미치는 공격을 의미한다. 따라서 공급망 공격은 파장이 광범위하며 치명적일 수 있다. 왜냐하면 사이버 위협이 심겨져 있는 소프트웨어 제품이 대량 생산되어 유포될 경우, 수많은 기기나 네트워크에 연결되어 파괴(destruction)나 중단(disrupt)을 할 수 있기 때문이며. 해당 기계에 대한 경로의존적 기술 생태계가 형성될 경우, 그 영향력은 더욱 광범위하고 장기간에 걸쳐서 일어날 수 있기 때문이다.

따라서 솔라윈즈 해킹사건은 소프트웨어 공급망 보안에 대한 경각심을 높인 역사적 사건이 되었다. 솔라윈즈 회사는 네트워크, 시스템 및 정보기술 인프라 관리를 지원하는 기업용 소프트웨어를 개발하는 미국 회사였는데, 솔라윈즈 해킹 사건은 시스템 소프트웨어의 공급망 서버에 가해진 사이버 공격이었다. 그리고 해당 사건은 2020년 12월 8일 사이버보안 기업 파이어아이(FireEye)가 충격적인 소식을 발표하며 그 진상이 드러났다. 이 사태를 두고 당시 미국 사이버사령부 지휘관인 폴 나카소네(Paul Nakasone)는 국가 전체의 전환점이 되었다고 언급할 정도였다.

솔라윈즈 사태는 오리온 빌드 서버에서부터 공격을 한 것이다. 해커는 솔라윈즈 내부망에 침투해 IT 관리 툴인 '오리온(Orion)'에 '선버스트(Sunburst)'라는 악성코드를 심는 방식으로 공급망

4) 숄츠는 이전 앙겔라 메르켈(Angela D. Merkel) 수상의 내각에 있었기도 했지만, 메르켈 수상보다는 확실히 덜 친중적 행보를 보이고 있다. 숄츠의 2022년 대중국 방문이 주목 받으며, 친중으로 보는 관점도 있었으나, 메르켈 수상의 동일 기간의 행보에 비교하면 중국과의 교류 시기나 횟수가 확연히 차이가 난다.

5) 물론, 이에 대한 통신회사들의 반대가 일어나기도 했다. https://www.reuters.com/business/media-telecom/german-interior-ministry-wants-force-5g-operators-slash-huawei-use-official-2023-09-19/

6) 물론 공급망에 대한 사이버 공격은 솔라윈즈 사태가 처음은 아니다. 솔라윈즈 사태가 발생하기 한달 전 즈음 한국에서도 북한에 의한 공급망 사건이 있었다. 다음을 참조하라. https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/

을 공격했다. 그 결과 '오리온'을 사용하는 약 1만 8천곳 가량의 기업이나 기관들이 버전을 업데이트하는 과정에서 악성코드가 유포된 것이다. 이 중에는 미국 국무부, 법무부, 항공우주국(NASA), 핵안보국(NNSA), 재무부, 통신정보관리청(NTIA), 국립보건원(NIH), 국토안보부(DHS), CISA, 에너지부(DOE) 등의 국가기관과, 마이크로소프트, 파이어아이 등의 보안 기업 및 포춘 500대 기업도 포함되었다.

솔라윈즈 사태에 대해 미국 정부는 사이버 공격의 배후 세력으로 러시아 첩보 기관인 SVR을 지목했다. 공격 사실이 발견되기까지 10개월 걸렸지만, 탐지되지 않았다면, 더 장기간 지속될 수 있는 공격이었다. 그러나 파이어아이(FireEye) 회사의 신속한 미 국가안보국(National Security Agency, NSA)에의 접촉으로 사태 해결의 시간은 단축되었다. NSA는 주로 해외 IP발 공격에 초점을 두고 있기 때문에, 국내에서 기원하는 사태에 대한 파악이 어려울 수 있었기 때문이다. 이러한 경험에 기반하여 미국 사이버사령부 지휘관인 폴 나카소네는 기조연설에서 파이어아이(FireEye)를 언급하며, 민관 협조 체계의 중요성을 강조하기도 하였다. 그리고 NSA 전문가들과의 파트너십으로, 멜웨어를 발견하여 위협 행위를 단절시켰으며, 공격 시간과 빼앗아 갈 수 있었던 정보의 단축도 가능했다고 보았다.

3. 데이터 넥서스

데이터 또한 사이버 공간과 결합되며, 데이터 안보의 문제로 대두되었다. 데이터의 3대 정보보안의 가치(비밀성, 무결성, 가용성)가 타협될 수 있는 상황이 데이터 보안과 연결될지언정, 모두가 국가 데이터 안보와 연결되지는 않지만, 여기서는 데이터 안보와 관련된 것을 주로 다룬다. 데이터 안보는 크게 세 부류의 위협이 거론되는데, 정부나 기업의 기밀과 지식재산권 절취(흔히 사이버 첩보활동(cyberespionage)라 불리움), 정보 조작(disinformation), 그리고 일반 민간인에 대한 개인 정보 유출에 의한 프라이버시(privacy) 침해이다.

첫 번째 부류에 속하는 다음과 같은 예들이 있다. 정부의 데이터 안보가 위협 받은 잘 알려진 사례로는 2015년 6월 중국 해커들에 의한 미 연방인사관리처(Office of Personal Management) 해킹으로, 미국 상하원 의원과 FBI 요원들의 인사 정보가 유출되었다. 2016년 12월 연방예금보험공사에 대한 해킹도 마찬가지이다. 군사 기술 정보에 대한 절취 사례도 적지 않은데, 군산복합체에 속하는 기업들에 대한 해킹을 통한 사례들이 많이 알려졌다. 2018년 1월 중국 해커들에 의한 초음속 대함 미사일과 수중전 세부 계획, 2017년에 드러난 북한에 의한 미국이 설계한 F-15 전투기 청사진, 2007년에 드러난 중국 해커에 의한 록히드마틴 회사 침투를 통한 F-22, F-35 스텔스 전투기 설계도 등, 매우 민감한 군사 무기에 대한 데이터가 절취되었다. 두 번째 부류에 속하는 최근 예로는, 2022년 2월 러시아가 우크라이나에 물리적으로 침공해 들어가며 병행한 정보 조작 즉, 허위정보(disinformation) 유포 작전을 들 수 있다. 세 번째 부류의 예로는 일반 민간인들의 개인 데이터가 빅테크 기업의 (감시)장치나 플랫폼 서비스 등을 통해서 적절한 보호 없이 국경을 넘어 이동하는 것이, 개인 정보 보안상으로 부각된 사건들이다. 2016년 구글이 '스트리트 뷰' 서비스를 준비하면서, 보안 조치 없이 개인 정보를 수집한 것에 대한 벌금형, 같은 해 페이스북 이용자 수천명의 정보가 영국 데이터 분석 업체 케임브릿지 애널리티카를 통해 트럼프 대선 캠프로 넘어간 것, 중국 알리바바 기업의 전자상거래와 결제 서비스를 통한 이용자들의 소비 행태 데이터의 무분별하고 동의 없는 수집 등이다.[7)]

7) 데이터 안보 관련 여러 다른 사례들은 김상배(2022) 6장을 참조하라.

상기의 첫 번째, 두 번째 부류가, 본질적으로 국가 안보와 가까운 데이터 안보 이슈를 제기하는 사례라고 한다면, 세 번째 부류는 반드시 국가 안보와 직결되어 있다고 볼 수 없는 사례들이다. 그런데 이하에서는 그러한 부류 중, 개인 정보가 국경을 넘어 이동하는 과정에서, 단순 개인 정보 보안의 이슈가 국가 안보 상의 문제가 되기도 한다. 즉, 데이터 전송의 사이버 안보화 사례이다. 사실 이러한 현상은 새로운 현상은 아니다. 중국 하이크비전, 다후아와 같은 CCTV 업체들의 불법적 데이터 수집 및 해외 유출 사건 뿐 아니라, 위에서도 다룬, 감시와 직접적 상관 없는 일반 경제적 행위에서 사용되는 중국산 5G, 크레인과 같은 하드웨어 그리고 (그에 내장된) 소프트웨어를 통한 데이터의 국외 이동도 지속적으로 문제 제기 되어 왔다. 그리고 이러한 문제는 미중 관계가 적대적 경쟁의 성격으로 기울면서 더욱 심각하게 받아들여지고 있다.[8] 이하에서는 최근의 대표적 한 사건을 들어 데이터의 국가 안보 이슈화 과정을 분석한다.

2022년 12월 미국 의회는 중국의 짧은 동영상 공유 플랫폼 '틱톡(TikTok)' 사용 금지를 결정짓는다. '2023 회계연도 연방정부 예산안'에 연방정부에서 사용하는 모바일 기기에서 틱톡 사용의 전면 금지를 포함시킨 것이다. 이러한 금지는 동영상 앱에 대한 정부 차원의 가장 광범위한 단속으로 평가된다. 틱톡은 원래 2016년 중국에서 처음 출시된 동영상 플랫폼인데, 동아시아에서 폭발적 반응을 얻자 2018년 전 세계로 출시하여, 2021년 9월 기준으로 사용자 10억명을 넘어서는 인기를 얻게 된다. 미국에서만 월 이용자수가 1억 5천만을 넘는 선풍적인 인기를 구가한 앱이 된다.

미국정부의 금지 이유로는 국가 안보에 대한 중국의 위협 및 해당 앱을 운영하는 기업의 중국 공산당과의 연결 의혹 등이 결합되어 존재했다. 우려되는 시나리오에 따르면, 중국 정부가 틱톡 혹은 바이트댄스(ByteDance)에 압력을 가해 미국 사용자의 개인정보를 넘기게 하거나, 중국 정보작전을 위해 또는 중국이 지원하는 허위정보를 퍼뜨리는 데 사용될 수 있다.

이전부터 미국 정부는 틱톡을 금지하려는 움직임을 보여 왔다. 트럼프 대통령은 2020년 8월 틱톡을 금지하는 행정명령을 내리기도 하였다. 그러나 이 시도는 연방판사의 제동으로 불발이 되었었다. '수정헌법 1조', 즉 언론 및 표현의 자유가 핵심 근거가 되었다. 그리고 바이든 정부에 들어서자, 트럼프의 행정명령을 철회하고, 대신 틱톡의 운영사 '바이트댄스'가 틱톡 지분을 믿을 반한 기업에 모두 매각하고 틱톡 사용자 정보를 저장한 서버를 미국 IT 기업이 관리하게 하는 방침을 제시하였고, 틱톡 본사도 이를 수용하게 되었다. 그런데 바이트댄스 직원이 바이트댄스 내부 정보에 대해 보도한 파이낸셜타임스 기자 2명의 위치를 감시했다는 의혹이 제기되자, 틱톡은 이에 연루된 직원들을 해고했음에도, 미국 내 여론이 급격히 악화되었고, 마침내 백악관은 2023년 2월 27일에는 30일 이내에 정부 기기에서 틱톡 앱을 모두 삭제하라고 통보하게 된다.

2023년 3월 초에는 연방 상원이 틱톡 사용을 금지하는 '정보통신기술 위험 통제법안'을 발의한다. 더욱이 미 첩보 기관 중 하나인 연방수사국(FBI)의 국장 크리스토퍼 레이가, 중국 정부가 틱톡을 통해 수백만 명의 데이터를 통제할 수 있고, 대만을 침공할 때 짧은 형식의 비디오로 여론을 형성할 수 있다고 구체적인 시나리오를 대며 우려를 나타낸다. 3월 23일의 하원 청문에서도 공화당 위원장 그리고 민주당 의원도 틱톡 최고경영자를 강하게 의혹을 제기하였다.[9]

---

8) 미중과 같은 적대적 관계에만 해당되는 것은 아니고, 미국과 EU와 같은 동맹국 사이에도 해당된다. 2013 스노우든 폭로는 개인 정보를 국가 안보의 사안으로 여기던 첩보 기관들과, 개인 정보는 국가 안보적 고려로부터 절연되어 지켜져야 할 인권으로 생각한 이들 간의 충돌을 부각시키게 된다. 세이프하버, 프라이버시 실드의 설립과 폐지는 이러한 충돌을 반영한다.

9) 틱톡 금지를 반대하는 의원들도 물론 있다. 특히, 젊은 유권자들의 지지를 많이 얻고 있는 민주당 의원들의 경우가 그러한데, 그들로부터 외면을 받을 수도 있다는 우려와 젊은 연령대 유권자들이 선거 운동에 틱톡을 많이 사용하고

이러한 맥락에서, 미국 몬태나 주에서는 2024년부터 '틱톡' 사용이 법적으로 금지된다. 2023년 4월 몬태나 주의회가 의결한 틱톡 금지 법안에 공화당 주지사가 서명했기 때문이다. 구글 플레이스토어 같은 앱 마켓들은 틱톡 앱을 다운 받지 못하게 비활성하게 해야 하며, 어기게 되면 하루 1만 달러 벌금이 부과된다. 미국 50개 주 가운데는 처음이 된다.

이러한 미국의 애플리케이션과 국가 안보의 결합은 다른 중국 앱으로 확산의 가능성이 있다. 실제, 발의된 여러 법안에는 틱톡과 바이트댄스의 동영상 편집 앱 '캡컷'은 물론이고, 나아가 중국의 온라인 패스트패션 브랜드 '쉬인(Shein)', 중국 대형 전자상거래 기업 '핀둬둬'의 미국 온라인 쇼핑몰 '테무(Temu)', 결제 앱인 '알리페이'와 메시지 앱인 '위챗' 등도 금지할 수 있게 된다.[10] 이들 앱들의 공통점은 경제의 큰 부분을 차지하고 있는 전자상거래에서 사용되는 앱들이라는 점이다. 따라서 사람들의 상거래 행위가 사이버 영역을 통하면서, 국가 안보의 사안으로 연계되었고, 이로 인해 정부가 민간의 경제적 상호작용에 개입하여 통제하고 있는 양상이 펼쳐지고 있다고 볼 수 있다.

이러한 미국의 사안 연계 행위로 인해, 미국과 함께하는 동맹국 혹은 파트너 국가들과 중국앱을 받아들이는 국가들로 나누어질 가능성도 거론된다. 캐나다는 2023년 2월 28일부터 캐나다 정부에 등록된 모든 기기에서 틱톡 사용을 금지하도록 했다.[11] 일본의 마쓰노 히로카즈 관방장관도 27일 기자회견에서 틱톡이 기밀정보 취급 기기를 대상으로 이용이 금지되어 있다고 하였으며, 그리고 다른 사회 관계망 서비스 이용도 금지하고 있다고 말하며 중국만을 겨냥한 조치가 아니다는 투로 메시지를 완화시키려고 하였다. 23일에는 유럽연합(European Union, EU) 집행위원회도 집행위에 등록된 개인 및 업무용 휴대용 기기에서 틱톡 사용을 금지하였다.[12] 이들 국가들의 주된 이유는 개인정보 보호와 사이버 보안 등의 이유이지만, 이러한 개인정보나 사이버 보안이 개인의 권리를 침해하기 때문이라는 이유보다, 국가 안보를 위협할 수 있는 대상에게 위협할 수 있는 수단을 제공한다는 점이 더 크게 작동한다.[13]

II. 사안 연계 전략

있다는 사실 때문이다.

10) 이러한 중국 전자상거래 앱들은 2023년 3월 즈음에는 미국에서 가장 인기 있는 앱으로 부상하기도 하였다. 중국 앱에 미국 젊은이들이 열광하는 것은 미국보다 중국 업체의 기술력이 더 좋다는 평가도 있다. (https://www.wsj.com/articles/why-chinese-apps-are-the-favorites-of-young-americans-a9a5064a?page=1). 그리고 틱톡은 미국 아마존 회사와 같은 전자상거래 회사로서 발돋움하고자 하는 움직임을 보여왔고, 이러한 시도가 미국에서 더 큰 압력을 초래했다는 평가도 있다. https://www.wsj.com/articles/tiktoks-next-plan-for-u-s-dominance-selling-made-in-china-goods-44943693; https://www.straitstimes.com/world/united-states/chinese-shopping-app-temu-wows-us-amid-tiktok-fears; https://www.dailymail.co.uk/news/article-12335617/TikTok-takes-retail-giants-Shein-Temu-new-e-commerce-business-selling-shipping-China-goods-one-billion-active-users-video-sharing-app.html

11) 화웨이와 비교하자면, 빠른 조치라 볼 수 있다. 이는 화웨이의 경우, 국내 이해당사자들의 걸려 있던 이익이 컸지만, 틱톡 같은 앱의 사용자들과 관련한 정치경제적 이익이 그리 크지 않았다는 가설을 세울 수 있다.

12) 인도는 이에 앞서 2020년 6월 사이버 안보상의 이유로 틱톡을 비롯한 중국의 59개의 앱 사용을 금지한 바 있다. 2020년 6월 인도군과 중국군이 국경분쟁지역에서 충돌한 이후로 양국 간의 관계가 악화되고 있었다.

13) 한편, 아프리카에서도, 예를 들어 세네갈, 소말리아에서도 금지 되었으며, 2023년 9월 기준으로 케냐, 우간다, 이집트에서도 그러한 노력들이 있어 왔다 (https://www.wsj.com/world/africa/tiktok-ban-africa-3690e6af?mod=Searchresults_pos2&page=1). 그러나 이러한 시도들은 국내 정치 차원에서 정권 유지를 위한 디지털 업압의 사례에 더 가깝다고 볼 수있다

1. 하드웨어 넥서스 관련 정책

여기서는 경제, 사이버 보안, 국가 (사이버) 안보의 연계를 추진하는 국가의 행위를 전략, 정책 그리고 제도(법과 조직)를 통해 살핀다. 모든 나라들의 포괄적인 변화를 살피는 것은 가능하지 않다. 대표적으로 미국의 변화를 중점적으로 살피지만, 미국의 변화는 사이버 초강대국으로서의 변화이기 때문에 국제 정치·경제·사회적 파급효과가 크다. 이러한 이유뿐 아니라, 종종 다른 나라들에게 반향을 일으키며 (유사한) 대응 정책과 제도를 야기하기 때문에 주목할 가치가 있다.

미국은 경제, 사이버 보안, 국가(사이버) 안보를 지속적으로 연계해 왔다. 중국 통신 장비업체 화웨이에 대해 사이버 안보 상의 이유로 수출통제 체제를 재정비하는 방법으로 경제 제재를 가한 미국의 정책은 잘 알려져 있다. 물론 더 큰 맥락에서는 미국의 중국에 대한 위협 인식 증가와 2017년 이후 미·중 관계의 전략 경쟁 성격이 크게 커진 것도 있다(유인태 2021; Yoo 2022). 그러나 동시에 미국 시스코사의 통신장비 인프라 세계시장 점유율의 확대와 대비되는 화웨이사 장비의 세계시장 점유율의 큰 증가 추세 그리고 중국의 5G 네트워크 기술표준 및 특허 최다 보유 등(김상배 2022), 중국의 시장 지배, 나아가 향후의 관련 기술과 산업의 지배에 대한 우려도 있었다. 미국의 화웨이 경제 제재 사례에서 보이듯이 상업적 이익을 잃어가는 현실이 존재했었고, 안보적 이익이 타협되는 것에 대한 우려가 결합되었다. 이러한 우려의 결합은, 두 영역의 연계를 촉진시켰다.

그뿐 아니라, 경제와 사이버 안보의 두 영역의 연계는 정책으로 인해 더욱 강화되었다. 사이버 안보에 대한 우려를 새로운 경제책략(new economic statecraft)을 통해 대처하고자 했다 (Aggarwal and Reddie 2020, Yoo 2022). 미국의 경제 책략은 처음에는 화웨이 기업에서 시작하여, 그 제재 대상의 범위를 넓혀 나갔고, 제재 품목의 범위 또한 처음에는 화웨이의 완제품에서 시작하여, 점차 제품 제조에 필요하나 핵심 소재·부품·장비로 범위를 넓혀 나갔으며, 제재에 참여하는 주체들도, 처음에는 정부 기관들에서 핵심 인프라 사업자들, 민간, 그리고 제3국으로 확장해 나갔다. 2018년부터 여러 차례에 걸쳐, 그리고 2023년 현재에도, 그 기술적 범위와 제재 대상을 확장 시켜가며 진화하고 있는 현재 진행형인 미국 정부의 중국 기업의 화웨이에 대한 경제 제재는 이를 단적으로 보여준다.

미국은, 한편으론 '청정네트워크(Clean Network)' 이니셔티브와 같은 외교 정책을 추진하면서,[14] 다른 한편으론, 일국 차원에서 경제 책략을 동원하여, 경제와 사이버 안보 넥서스에 대한 우려에 대처해 나갔다. 특히, 수출통제정책이 활발히 활용되었다. 주목해야 할 변곡점은 2018년에 제정된 수출통제개혁법안(Export Control Reform Act, ECRA)이다.[15] 대통령에게 이중용도 기술과 재화의 수출통제를 이행하기 위한 폭넓은 입법적 권한을 부여하는데, 이전 수출통제 관련 법들과 달리 만기일(expiration date)이 없다. 2018 ECRA는 미국 의회의 우려를 반영한 행정부 차원에서의 노력이며, 화웨이와 중국의 민군융합 프로그램, 감시와 억압에 사용되는 미국의

14) 중국의 '일대일로' 그리고 '디지털 실크로드' 이니셔티브는 인프라에 초점을 맞추고 있지만, 인프라 설치에 사용되는 ICT 구성 부품이라던가, 이를 통해 이동하는 데이터 안보에 대한 우려도 제기 되고 있다. 이에 대항해, 미국과 그 우방국들은 '블루닷네트워크(Blue Dot Network),' '더 나은 세계 건설(Build Back Better World, B3W)'을 내놓았다.

15) 물론 수출통제 이전에 혹은 수출통제와 병행하여 국방수권법(National Defense Authorization Act , NDAA)를 통해 취득법 차원에서 연방정부의 행동에 제한을 가하는 형태로, 화웨이에 타격을 주었다. 미국 의회는 2018 그리고 2019년 NDAA를 통해, 처음에는 특정 기관들의 화웨이 제품의 조달을 제한했지만, 후에는 모든 행정부 기관의 지출에 제한으로 확대했다. 그러나 이들 NDAA의 제한은 조달, 무상보조(grant), 또는 융자(loan)의 형태로 연방 지출이 되는 거래에만 해당이 된다. 따라서 2019년 5월 트럼프 행정부는, 2018년 수출통제법(the Export Controls Act of 2018)에 근거하여 권한을 행사하여, 화웨이 관련 금지의 범위를 연방정부 지출과 관련된 범위보다 더 넓힌다.

기술을 제한하기 위한 목적을 명시하였다.

2018 ECRA를 통해 수출통제체제의 정비에 시동을 걸며, 2019년 5월 15일에는 수출관리규정(Export Administration Regulations, EAR)이 개정된다. 수출통제법(Export Control Act)은 다른 것들도 포함되지만 특히 이중 용도 기술과 재화들의 수출을 통제할 수 있는 권한을 부여한다. 동법은 또한 상무부 장관에게 거래제한명단(Entity List, EL)을 세우고 유지하도록 요구한다. EL을 작성시에는 국무부, 국방부 그리고 에너지부 장관들과 협의하는 것이 요구된다. EL에 실리는 외국 행위자들은 수출 라이센스 요구사항을 만족시켜야 하는데, 왜냐하면 이들은 미국의 국가안보와 외교정책에 위협으로서 간주되기 때문이다. 동법은 행정부가 EL에 등재된 회사들의 수출, 재수출(re-export), 그리고 대내 이전(in-country transfers)[16]을 통제할 수 있는 권한을 부여한다. 미 상무부(Department of Commerce)의 산업보안국(Bureau of Industry and Safety, BIS)이 EL을 유지한다. BIS는 EAR을 통해 수출통제의 구체적 범위를 조정한다.

따라서 해외 행위자가 미국의 기술이나 소프트웨어를 사용시에는 EAR의 적용을 받게 되는데, 이러한 맥락에서, 화웨이의 반도체를 해외에서 디자인하거나 제조할 시에, 미국 기술이나 소프트웨어를 사용할 능력이 제한된다. 그리고 화웨이나 중국의 다른 전기통신회사들은 미국의 반도체와 같은 제품이나 장비들을 사용하기 때문에, 수출제한은 그들의 사업에 타격을 가하게 된다.[17]

미국의 수출통제체제는 또 다른 정책 수단도 있는데 해외직접제품규칙(Foreign Direct Product Rule, FDPR)이다. 2020년 5월 15일 그리고 연이어 8월 17일의 FDPR개정을 통해, 기존 EAR을 통해 막지 못했던 틈새에서 일어나는 무역 거래 또한 차단하고자 했다. 즉, 화웨이와 같은 우려되는 국가에 속하는 기업들이 해외에 위탁생산하여 그 기업들에 들어가는 반도체를 막고자 하였다.[18]

2. 소프트웨어 넥서스 관련 정책

핵심 인프라의 사이버 보안 위협에 대해, 정부들은 국가 안보 사안으로 여기며 적극적으로 개입하기도 한다. 예를 들어, 미국의 공급망 강화를 위한 행정명령들은 공급망을 구성하는 ICT 제품의 보안 뿐 아니라, 이를 운영하는 소프트웨어의 공급망에 대해서도 대처를 주문하고 있다. 그리고 그러한 안보 우려에 대한 대처 중 하나가, 우려 국가를 (기술)제품과 서비스 제공 공급망에서부터 배제시키는 것이다. 이러한 목적에서 취해진 조치들은, 하드웨어와 유사하게, 소프트웨어의 제조 및 유통 과정에서 우려 대상들의 개입을 철저히 검출해내고, 배제하는 방향성을 띠게 되었다.

소프트웨어 제품의 경우, 제품의 설계, 생산, 배포 등의 모든 단계에서 위조와 변조가 가능하기 때문에, 투명한 관리가 필요한데, 이러한 부담을 덜고, 위·변조된 제품을 타고 들어오는 사이버 공격을 원천으로부터 차단하기 위한 조치이다. 화웨이 사태에서 보였던 미국의 정책은 이러한

16) 외국 국가 내에서의 이전을 의미한다.

17) 일례로, 이러한 미국의 수출통제 체제가 ZTE의 운영에 영향을 미친 사실이 알려져 있다. Sijia Jiang, China's ZTE Says Main Business Operations Cease Due to U.S. Ban, REUTERS (May 9, 018), https://www.reuters.com/article/us-zte-ban/chinas-zte-corp-says-main-business-operations-cease-due-to-u-s-ban-idUSKBN1IA1XF?il=0.

18) 이러한 무역정책이나 후술할 투자정책과 더불어 산업정책도 같이 진행된다. 예를 들어, "안전한 5G와 그 이후에 관한 법(Secure 5G and Beyond Act of 2020)(2020)"을 만들어서 계획 수립 및 시행을 위한 법적 근거를 마련하였고, "안전한 5G를 위한 국가전략(National Strategy to Secure 5G of the United States of America)(2020)"을 작성하여 목표를 설정하였으며, "안전한 5G를 위한 국가 전략 이행 계획(National Strategy to Secure 5G Implementation Plan)(2021)"를 통해 목표 달성을 위한 구현 계획을 내놓았다.

관점에서 채택된 단적인 예이다. 화웨이 사태에서 파생되어, 더욱 확장된 미국의 첨단반도체 공급망의 재편 과정 가운데 채택되는 수출통제 정책은, 크게 보면 중국 기술력의 억제와 전략 경쟁에서의 우위 확보라는 목표도 있지만, 반도체의 물리적 공급 차원에 뿐 아니라 반도체 생산 공급망에서 심겨질 수 있는 소프트웨어에서 비롯되는 사이버 위협을 근원부터 차단하겠다는 정책이 부상한다. 중국 기업 화웨이의 5G 하드웨어는 지속적 운영을 위한 소프트웨어 업데이트가 수반되는데, 이 때 악성 코드가 심기울 수 있다는 우려가 컸다. 이 때문에, 미국의 수출통제체제가 변화하는 가운데, 2020년의 FDPR에서도, 미국 기술이나 부품 뿐 아니라 소프트웨어도 수출통제의 대상으로 포함되었다.

소프트웨어 공급망 공격에 대응하는 과정에서 미국의 경제 영역과 사이버 안보의 연계는 더욱 확충되었다. 위에서 소프트웨어 공급망 보안에 대한 미국 사회에 경종을 울린 솔라윈즈 해킹사건에 대해 언급하였다. 특히, 이 사건은 미 정부 내의 공급망 사이버 안보와 관련한 주요한 변화들을 가져왔다. 대표적인 변화가 유사한 공격에 대비하기 위해 내·외부망 구분 없이 모든 영역에서 보안성을 검증하는 '제로트러스트(zero trust)'가 미국 정부의 사이버 정책에 도입되었다.

2021년 5월 12일, 취임한지 5개월도 되지 않아, 미 바이든 대통령은 행정명령("Executive Order on Improving the Nation's Cybersecurity" 또는 EO14028)을 내리는데, 여기서 연방정부의 사이버 안보를 현대화하기 위한 주요 방안으로 '제로트러스트'가 대두한다.[19] '제로트러스트 아키텍처(Zero Trust Architecture)'는 연방정부가 클라우드 기술을 도입하는데 특히 중요한 보안 정책으로 지목되었다. 그리고 동 명령은 정부 주요 기관들에게 주어진 기간 내에, 현 보안 상황에 대한 파악과 제로트러스트에 기반한 보안 절차의 현대화, 인원 훈련 및 훈련 프로그램의 설립 등을 지시한다. 이러한 제로트러스트의 맥락에서 '주요 소프트웨어(critical software)'를 정의하고, '주요 소프트웨어 공급망 안보(critical software supply chain security)'가 제시된다.[20]

EO14028은 'Software Bill of Materials(SBOM)'이나 'Zero Trust Architecture(ZTA)'라는 용어에 대해서도 자세히 정의를 내리고 있는데, 이를 보아도, 이러한 개념이 도입시에 연방정부 차원에서도 생소했음을 보이며, 또 중요하게 생각했다는 것을 간접적으로 보인다. SBOM이란 소프트웨어를 구축함에 있어 사용된 다양한 요소들의 상세와 공급망 관계를 포함하는 공식적 기록을 의미한다. 즉, SBOM을 통해, 완제품 구성 요소에 대한 심층 분석과 전체 목록, 그리고 결과적으로 발생할 수 있는 잠재적 위험성 등을 제공하는 소프트웨어용 '영양 정보(nutrition facts)'가 생성될 수 있다. 따라서 SBOM은 그러한 기록들을 통해 개발자들이 구성 요소들이 최신 상태인지를 확인할 수 있으며, 새로운 보안 취약성에 신속하게 대응할 수 있도록 한다.[21]

---

19) https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

20) 흥미로운 점은, 연방정부의 기관들이 '제로트러스트 아키텍처'로 이전하는 과정에서, 상무부(Department of Commerce)가 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)가 제시하는 표준, 도구 그리고 모범 사례를 따르라고 언급하는 부분이다. NIST는 미국 혁신과 산업경쟁력 증진에 있어서 핵심 기관이며 경제안보에도 깊이 관련되어 있다. NIST는 미국의 사이버 안보 프레임워크 제작에도 중요한 역할을 해 왔는데, 2014년에 책정되고 2018년에 업데이트 된 'NIST 사이버 안보 프레임워크(Cybersecurity Framework)'는, 후에 행정명령(EO13800), "연방 네트워크와 주요 인프라의 사이버 안보 강화하기(Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)"에서 미 연방정부 기관들의 사이버 안보 프레임워크로 제시되기도 했다. 'NIST 사이버 안보 프레임워크'는, 2019년 '사이버 안보 성숙도 모델(Cybersecurity Maturity Model Certification, CMMC)'로 응용 및 확장되어, 기관들이 얼마나 표준들에 순응하고 있는가를 구체적으로 평가할 수 있도록 하였다.

21) 동 행정명령은 미국 표준기술 연구소(National Institute of Standards and Technology, NIST)로 하여금 SBOMs 지침 개발을 의무화하였고, CISA 또한 SBOMs을 발전시키고 대중화하기 위한 2018년 프로젝트를 더욱 확대시키기 위해 노력해 가기로 했다.

행정명령14028의 연장선상에서, 미 국방부는 2022년 11월 22일 '제로트러스트 전략과 로드맵(Zero Trust Strategy and Roadmap)'을 내놓는다.[22] 그리고 28일 내놓은 '제로트러스트 설계를 통한 사이버 안보로의 길(Path to Cyber Security Through Zero Trust Architecture)'에서 제시하는 제로트러스트 전략은, 네트워크 내에 이미 있는 사용자들에게 어느 정도의 신뢰를 가정하는 전통적인 네트워크 보안 방법과 다르다. 제로트러스트는 이미 네트워크가 타협되었다는(compromised), 즉 침해되었을 수 있다는 것을 가정한다. 그리고 반복적인 사용자 인증(authentication)과 인가(authorization)를 통해, 적의 네트워크 움직임을 좌절시키거나 확인하며, 손해나 취약성을 완화시키고자 한다. ZTA는 "신뢰하나 검증하라(trust but verify)"가 아니라 "결코 신뢰하지 말고, 항상 검증하라(never trust, always verify)"라는 경구로 요약될 수 있다.

미국의 2023년 사이버 안보 전략서는, 러시아에 의한 솔라윈즈 사태와 중국에 의한 마이크로소프트 익스체인지 서버 해킹 사태에 대한 반성을 바탕으로, 미국의 사이버 안보 능력을 향상시켜 왔다고 하고 있다(The White House 2023). 미국의 사이버 안보 향상을 위한 노력은, 새로운 전략과 정책의 도입뿐 아니라, 미국 정부 내의 조직 개편도 있었다. 예를 들어, 솔라윈즈 사태에 의해 촉진된 하나의 변화는 2021년 1월의 국무부 내의 사이버안보·신기술국(Bureau of Cyberspace Security and Emerging Technologies, CSET)의 창설이다. 한정적 분야에 국한된다는 이유로 과거 설립이 반려된 적이 있지만, 마이크 폼페이오 국무부 장관은 솔라윈즈 사태의 맥락에서 2021년 8월 7일 설립을 승인한 것이다. 이는 미 정부 내에서, 사이버 보안이 일부 영역에 국한된 것이 아니라, 국가 안보가 달린 포괄적 문제라는 의식의 전환이 있었다고 할 수 있다. DHS 산하 사이버·인프라안보국(CISA)이 민·관을 사이버 공격으로부터 보호하는 것이 목적이라면, CSET은 사이버 안보 분야의 외교적 접근에 초점을 맞추어, 적국과 사이버 갈등 예방, 사이버 안보 분야 정책과 신기술 추진 등을 담당했다.[23]

3. 데이터 넥서스 관련 정책

미국의 데이터의 국가 간 이동에 대한 기본적 입장은 '신뢰할 수 있는 데이터의 자유로운 이동(Data Free Flow with Trust, DFFT)'로 압축될 수 있다. 2019년 일본 오사카에서의 G20에서 대두되기 시작한 개념이며, 중국의 데이터 주권을 강조하는 원칙과는 대척점에 위치하지만, 유럽의 (개인 사생활권을 포함한) 인권이나 미국의 자유로운 데이터 이동의 절충점을 지향한다(유인태 2020).

미국의 데이터 이동에 대한 원칙 자체는 상업적 이익에 초점을 두고 안보 영역과의 연계는 명시적으로 나타나지 않아 보인다. 이는 자유로운 데이터 이동이 많은 빅테크 기업의 모국이기도 한 미국의 상업적 이익에도 부합하고, 또 국내 헌법적 정신과도 부합하기 때문이기도 하다. 따라서 공공 질서나 국가 안보 상의 이유로 데이터의 자유로운 이동을 제한하는 중국과 같은 권위주의 국가들과는 다른 정책을 표방할 수밖에 없다.[24] 즉, 미국은 상업적 데이터와 국가 안보의 연

22) https://www.defense.gov/News/Releases/Release/Article/3225919/department-of-defense-releases-zero-trust-strategy-and-roadmap/ 상기 전략서는 국가안보국(NSA, National Security Agency)와 협동으로 작성되었다.

23) CSET은 바이든 정부에 들어서고 2022년 4월 '사이버 공간과 디지털 정책국(Bureau of Cyberspace and Digital Policy, CDP)'으로 바뀐다. CDP 설립 공표는 2021년 10월에 있던 바이든 정부의 '30개국의 랜섬웨어 정상회의(30-nation virtual summit on ransomware)' 직후에 나왔다.

24) 예를 들어, 2017년 6월 1일부터 발효된 중국의 네트워크 안전법의 경우, 중국 경내에서 운영 중 수집, 생성된 개인정보와 중요 업무 데이터는 반드시 경내에 저장해야 하며 필요에 의해 해외에 저장하거나 기관이나 개인에게 제공

계를 통해 국가 안보의 목적으로 상업적 데이터의 자유로운 이동을 제한하기가 어렵다. 따라서 데이터 안보에 대한 우려는 데이터 이동 차원에서가 아니라, 데이터를 생성, 처리, 이전 시키는 행위자 차원에서 대처된다. 상기의 중국 플랫폼 틱톡에 대한 미국의 대응은 그 대표적 예이다.

즉, 자유로운 데이터의 이동이라는 원칙을 손상시키지 않는 범위에서 글로벌 데이터 거버넌스를 수립하고자 하는 미국은, 경제와 안보의 연계를 통해 오히려 초국경 데이터 이전을 더욱 강화하고자 한다. 이러한 움직임은 적대적 경쟁국과의 관계에서가 아니라, 대서양 건너편의 동맹국들과의 관계에서 더 명확히 드러난다. 물론, 이러한 연계 전략은 정부 외 행위자인 초국가(transnational) 혹은 국가 내(substate) 행위자로부터 도전을 받고 있다. 특히, 경제와 사이버 안보가 연계되는 데이터 넥서스는 미국 정부에게 도전이 되고 있다.

대표적인 예가 미국과 유럽연합(European Union, EU) 간의 2015년 '세이프 하버(Safe Harbor)', 2020년 '프라이버시 실드(Privacy Shield)'의 폐지이다. 미국과 EU 간의 개인 데이터의 이동을 상업적 목적을 위해 원활히 하기 위한 협정들이었는데, 미국 첩보 기관에 의한 상업적 데이터의 안보적 목적을 위한 사용 정황이 2013년 스노우든 폭로에 의해 드러났다. 폭로된 사실들에 기반해서 오스트리아 인권 운동가 맥스 슈렘스(Max Schrems)가 소송을 제기하였고, 유럽 사법 재판소는 유럽 법과의 불합치 판결을 내리게 되면서, 상기 상업적 데이터 이전을 위한 협정들이 폐기되었다.[25] 이러한 일련의 과정은, 경제, 사이버 안보 뿐 아니라, (프라이버시 레짐을 포함하는) 인권 영역이 서로 연계되며, 역내 정치와 국제 정치가 서로 반향을 일으킨 결과이기도 하다.

데이터 넥서스에 대한 미국의 연계 전략은, 미국의 데이터 이전에 관한 역외 적용 법안에서도 주목되었다. 2020년 8월, 미국의 국경 간 데이터 이동에 관한 법, '합법적인 해외 데이터 활용의 명확화를 위한 법률,' 일명 '클라우드법(Clarifying Lawful Overseas Use of Data Act, CLOUD Act)'이 제정되었다. 미국이 여러 국가들과 맺은 자유무역협정이나, EU와의 양자 간에 여러 데이터 이동 간의 국제 협약을 맺어 왔지만, 국외에 있는 자국 정보(즉, 미국 통신서비스 제공자들이 보유 또는 관리하는 통신 내용, 트래픽 데이터, 가입자 정보 등)에 접근할 수 있는, 더 폭넓게는 합법적으로 해외 데이터 활용의 법적 근거를 마련한 것은 처음이었다. 이 'CLOUD Act'는 '데이터의 위치에 관계 없이'라는 문구를 통해, 기존 법률에 없었던 역외 데이터의 접근 권한에 대해 명확히 하고 있다.

'CLOUD Act'는 실제적으로는 개인정보의 국외 이전을 제한하기보다, 국외에 있는 정보에 보다 신속하고 용이하게 접근할 수 있는, 즉 해외 데이터의 이전을 더욱 용이하게 하는 법적 근거를 제공한다. 그리고 그 근거는 사회적 질서와 국가 안보를 위한 것이기에, 상업적 데이터 넥서스가 경제와 안보를 연계한다. 이러한 성격은 CLOUD Act 도입이 촉발된 사례를 보아도 명확하다. 미국에서 발생한 마약 사범 수사에서, 사법 당국은 2013년에 마이크로소프트를 상대로 이메일을 열람하기 위한 수색영장을 발부 받았다. 그런데 미국 서버에 저장되어 있던 자료는 넘겨받을 수 있지만, 아일랜드 더블린에 있는 서버에 저장된 데이터의 제출은 거부되었다. 영장의 효력이 미국 영토 내에만 국한되었기 때문이다. 이러한 실례가 CLOUD Act 제정의 배경이 되었고, 데이터 보호를 둘러싼 수사기관의 권한 및 허용범위에 대한 분쟁 해결 절차를 마련된다.[26]

할 경우 국가 네트워크 정보 부문 및 국무원 관리부문과 함께 안전성 평가를 진행해야 한다(제37조).

25) 2022년 10월 바이든 대통령이 '미국-유럽연합 데이터 프라이버시 프레임워크(the European Union-U.S. Data Privacy Framework)'를 위한 새로운 행정 명령에 서명하여, 미국과 유럽 간의 데이터 전송 협정은 그 명맥을 유지하고 있다. 하지만 이 또한 이전과 유사한 이유로 폐지될 가능성이 크다.

26) 향후, 클라우드 서버 이용이 더욱 활성화될 것인데, 사이버 범죄와 관련하여 외국 서버에 있는 범죄자들의 정보 수집 필요가 더 클 것으로 전망된다. 많은 국가들이 기존 사법공조조약(Mutual Legal Assistant Treaty, MLAT)의

4차 산업혁명 시대, 데이터의 양적 질적 확보가 중요하기 때문에, 미국은 국가 이익 차원에서도 데이터의 이동에 제한을 가하지 않는 것이 중요하다고 생각한다. 그러나 개인정보는 보호 받아야 하는데 반해, 사법당국은 법의 집행을 위해 개인정보에의 접근이 필요하다. 상업적 이익, 개인의 권리, 사회 안정과 국가 안보라는 상충되는 이익 혹은 가치들에 대해, 미국식 해결 방법은 CLOUD Act에 잘 나타난다. 물론 해당 법은 데이터의 위치에 관계없이 개인정보 보호와 외국의 주권을 존중하며, 동시에 공공의 안전을 보호하기 위한다는 목적을 명확히 하고 있만 이러한 가치들이 상충할 수 있다는 것은 명백하며, 미국은 경제와 안보의 연계를 통해 데이터의 이동을 더욱 자유롭게 하고자 하고, 국가의 대내외적 안보를 우선시 하고 있다.

CLOUD Act는 미국 정부의 사안 연계 해결책을 보인다. 즉, 상업적 데이터에서 공공의 안정과 안보적 목적을 찾고, 이러한 목적을 달성하기 위한 데이터 접근을 명시화 한 것이다. 그런데, 개인의 신상, 행동, 그리고 경제적 행위를 담은 데이터 보호보다, 국가 안보적 목적이 우선시되는 것이 특징이다. EU의 GDPR과 비교해 보았을 때, GDPR은 EU내 저장된 데이터를 EU 외부로 이전할 경우, 여러 제한 규정을 포함하고 있다. 따라서 이 둘 간의 상충하는 문제가 여전히 남아 있다.

비효율성을 극복하기 위해 CLOUD Act와 같은 입법을 추진하고 있다.

<참고문헌>

김상배. 2022.『미중 디지털 패권 경쟁: 기술·안보·권력의 복합지정학』. 서울: 한울아카데미

유인태. 2021. “디지털 패권 경쟁 속에서 중견국 연대 외교의 갈림길: 화웨이 사례에서 보는 파이브 아이즈의 연대와 일탈.” 동서연구 33(2): 5-31.

유인태. 2023(forthcoming). “첨단과학기술 협력의 국제정치: 한국과 미국의 차세대 네트워크와 인공지능 기술 협력.” 동서연구 35(4): 00-00.

Aggarwal, Vinod K., and Andrew W. Reddie. 2020. “New Economic Statecreaft: Industrial Policy in an Era of Strategic Competition.” Issues & Studies: A Social Science Quarterly on China, Taiwan, and East Asian Affairs 56(2).

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

Choucri, Nazli, and David D. Clark. 2018. International Relations in the Cyber Age: The Co-Evolution Dilemma. Cambridge, MA: The MIT Press.

Drake, William J., Vinton G. Cerf, and Wolfgang Kleinwächter. 2016. Internet Fragmentation: An Overview. Geneva, Switzerland: World Economic Forum.

Emmers, Ralf. 2013. “Securitization.” In Contemporary Security Studies, ed. Alan Collins. UK: Oxford University Press, 131-43.

European Union. 2021. “EU Toolbox for 5G Security: A Set of Robust and Comprehensive Measures for an EU Coordinated Approach to Secure 5G Networks.”

Segal, Adam, and Gordon M. Goldstein. ed. 2022. Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet. Washington, DC: Council on Foreign Relations.

Stritzel, Holger. 2007. “Towards a Theory of Securitization: Copenhagen and Beyond.” European Journal of International Relations (13): 357-83.

High Representative of the Union for Foreign Affairs and Security Policy of European Commission (HR). 2021. “Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank: The Global Gateway.” Brussels, Belgium: European Commission.

Yoo, In Tae. 2022. “Emergence of Indo-Pacific Digital Economic Order: US Strategy and Economic Statecraft Toward China.” Asian Journal of Peacebuilding 10(2): 387-410.

Zuboff, Shoshana. 2019. The Age of Surveillance Capitalism: The Fight for A Human Future at the New Frontier of Power. New York: PublicAffairs.

이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.