Center for Future Warfare Studies,
Institute of International Studies at Seoul National University |
국제문제연구소 미래전연구센터 연구위원 워킹페이퍼 No.17.(발간일: 2025.2.7.)

# 데이터 안보 이슈의 부상과 사이버 공격의 진화

윤정현 국가안보전략연구원 연구위원

## Ⅰ. 서론

오늘날 데이터는 디지털 전환 사회의 필수 불가결한 자원으로 자리매김하하고 있다. 실제로 데이터는 '21세기 원유'로 상징될만큼 디지털 사회를 작동시키는 핵심자원으로 인식되고 있기 때문이다(김상배, 2014: 6). '국제데이터주식회사(International Data Corporation, IDC)'에 따르면, 전 세계에서 생성, 복제되는 글로벌 데이터의 규모는 2018년 33 ZB에서 2025년도에는 175 ZB 이상으로 급격히 증가할 것으로 전망된 바 있다(IDC, 2018)[1]. 이에 따라 각국은 데이터 정책을 혁신과 산업경쟁력 강화를 위한 제도적 기반으로 삼고 있다. 실제로 디지털 기반 사회에서 방대한 데이터는 클라우드·플랫폼을 통해 저장되며, 특정 임무를 위한 AI와 자동화시스템을 거쳐 생산·활용된다. 그리고 이는 다시 또다른 목적을 위한 자원으로 순환 과정을 거치며 새로운 부가가치를 창출한다. 이 같은 흐름 속에서 최근 각국은 데이터를 생산, 저장, 유통, 폐기하는 전주기적 과정에 대한 국가의 배타적 권리 확보를 전략적으로 인식하고 주권의 문제로 접근하기 시작했다(윤정현·홍건식, 2022: 28). 특히 최근 AI의 성능을 결정하는 대규모 학습데이터의 중요성이 부각되면서, 데이터를 국가안보를 위한 전략 자산으로 바라보는 추세 또한 강화되는 중이다(김상배, 2018; 구태언, 2019).

---

1) 여기에는 클라우드와 서버간 접속 과정에서 일시적으로 생성되는 세션 데이터 뿐만 아니라 프라이버시 데이터에서부터 기업의 핵심기술이나 영업 비밀, 국가의 외교 국방의 기밀까지 다양한 정보가 포함된다. David Reinsel, John Gantz, John Rydning. (2018). "The Digitization of the World From Edge to Core" Segate and IDC. (https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf).

이처럼 데이터가 경제·안보적으로 중요한 가치를 내재한 자원으로 인식되면서, 사이버 공간 속 데이터의 확보와 통제·활용에 대한 문제를 안보화의 메커니즘에서 조명하는 연구들도 나타나고 있다(김상배, 2020; Liu, 2019). 여기서 주목할 부분은 '사이버 안보'가 아닌 '데이터 안보'라는 용어를 부상시킨 이슈들의 맥락이다. 최근 데이터의 중요성이 더욱 부각되었지만, 양자는 혼용되거나 어느 한 편을 포함하는 개념으로 이해되어왔다. 사실 광의의 정의로서 데이터(data)는 정보화·컴퓨팅 시대 이전부터 존재해왔다고 볼 수 있다(김석준, 2019; 김현철, 2019) 또한 그 자체로는 의미를 포함하지 않은 단순한 수치에 불과한 것으로 간주하며, 일련의 처리과정을 거쳐 특정 목적을 위한 정보로 탈바꿈할 때에야 비로소 그 가치를 부여하곤 했다.[2] 이 때문에 사이버 보안은 현실과 밀접한 가상공간에서 정보를 보호하고 안정적인 생성과 유통, 서비스를 보장하는 환경을 구현하는데 초점을 맞춰왔다. 또한, 그러한 활동이 국가적·지구적 차원에서의 대내외적인 함의를 가질 때 우리는 '사이버 안보'의 개념을 통용해왔다(김상배, 2020: 76).

그러나, 최근 제기되는 사이버 안보의 쟁점들을 살펴보면 2000년~2010년대와 구별되는 경향들이 포착된다. 바로 데이터가 사이버 공간의 질서와 경쟁, 안보적 이해관계를 결정하는 주요 변수로 부상하고 있기 때문이다. 실제로 지난 코로나 팬데믹 기간동안 세계는 온라인 가상세계의 활동이 현실세계를 상당부분 대체·융합하는 '메타버스(metaverse)'[3]를 경험하기도 했으며, 구현 공간으로서 사이버 영역의 범위는 더욱 확장되었다. 나아가, 이 같은 흐름은 사이버 공간을 둘러싼 기술혁신과 주요 행위자를 확장시키며 변화를 더욱 가속화시키고 있다. 기술혁신의 측면에서 보면, AI로 상징되는 지능화와 5G/6G 등 클라우드 기반의 초연결, 플랫폼 신경제 트렌드는 정보 뿐만 아니라 비정형·빅데이터의 활용을 증진시키면서 그 중요성을 심화시킨다. 여기에는 빅테크 기업을 비롯해 자발적으로 참여하고 데이터를 생산·축적하는 민간·다중이해관계자의 비중과 역할이 커지고 있음이 확인된다.

그러나 무엇보다도 데이터의 중요성이 증대되면서 사이버 공격 양상 역시 변하고 있다는 점을 간과하지 말아야 한다. 국가 또는 국가 배후의 악의적 공격자들은 전시, 평시의 정치·외교적 압박에서부터 국가 기밀이나 전략기술과 밀접한 기업의 지적 재산 확보 까지 다양한 목적을 실행하는 도구로서 데이터를 노린 공격을 시도하고 있다. 또한, 데이터를 암호화한

---

2) 데이터(data)는 '사람이나 기기를 통해 관찰·수집·측정 등을 거쳐 확보한 가공되지 않은 원시자료'로 정의된다. 김석준(2019); 김현철(2019). 반면, 컴퓨터 분야의 협의적 의미로서는 프로그램 등을 통해 개별 값들을 읽고 처리하며 저장하는 등의 작업이 수행된다. 이 때, 데이터는 디지털의 최소 단위로서 0과 1의 이진법으로 표기된다. https://en.wikipedia.org/wiki/Data_(computer_science)#cite_note-1

3) 메타버스는 초월적 의미의 'meta'와 우주를 상징하는 'universe'의 합성어로서, 다양한 현실세계의 활동가치가 통용되는 디지털 기반의 3차원 가상공간을 의미한다. 또한, 다중의 사용자가 아바타를 통해 소통하며, 물리적 현실세계와 공존할 수 있는 디지털 기반의 광범위한 융합 공간인 것이다. J.M., Cascio, J. Smart, and Paffendorf, J. "Metaverse Roadmap Overview", (2010), Accelerated Studies Foundation. Retrieved.

후 복구키를 제공하는 대가를 요구하는 단순한 수법에서 벗어나 데이터를 탈취, 조작, 오염시켜 기업과 정부, 국가 간 신뢰를 훼손하려는 시도를 감행하기도 한다. 즉, 오늘날 사이버 공간에서의 보호 대상과 안보적 쟁점은 '스몰 데이터'의 시대와는 구별되는 특징들이 나타나고 있는 것이다.

그렇다면 "데이터 안보 시대의 특징은 무엇이며, 사이버 공격의 진화와 글로벌 차원의 안보화 경쟁이 시사하는 바는 무엇인가? 본고는 위 질문에 답하기 위해 다음의 세부적인 논의를 전개하고자 한다. Ⅱ장에서는 데이터 안보 패러다임을 설명하는 도구로서 사이버 안보와 데이터 안보 개념이 기반하고 있는 구성 요소들의 중첩·전환적 특징을 도식화한 분석틀을 제안한다. 이어 Ⅲ장에서 데이터를 표적화하여 벌어지는 최근의 사이버 공격 양상들을 검토한다. 데이터 유출·조작·오염·영향공작 등이 이를 구성하는 유형이 될 것이다. 그리고 Ⅳ장에서 데이터 안보 강화를 위한 주요국의 전략 초점들을 추진정책 등을 토대로 살펴본다. 결론에서는 데이터 기반 안보화 이슈가 국제정치적 쟁점에 시사하는 바를 짚어보고, 향후 데이터 기반 사이버 위협의 안보화 메커니즘, 이해관계자와 대응 거버넌스의 주도권 경쟁 등에 시사하는 바를 정리한다. 나아가 데이터 안보 시대로의 전환적 국면에서 한국에 필요한 접근 방향과 주요 실천과제를 제안하고자 한다.

# Ⅱ. 데이터 안보환경의 전환적 특징

## 1. 디지털 전환의 고도화와 사이버 공간의 확장

'4차 산업혁명 시대'의 도래와 함께 일상의 변화를 상징하였던 키워드는 '디지털 전환(digital transformation)'이었다. 디지털 기술을 사회 전반에 적용하여 전통적인 사회 구조를 혁신시키는 것을 뜻하는 디지털 전환은 일반적으로 인공지능(AI), 사물 인터넷(IoT), 클라우드 컴퓨팅, 빅데이터 솔루션 등 핵심 정보통신기술(ICT)과 긴밀히 연계되어 있으며, 이들을 기반으로 고도화되어 기존의 전통적인 방식과 서비스 등을 혁신하는 것을 의미(한국정보통신기술협회, 2017). 그러나 단순히 ICT 기반의 특정 시장·품목에서 통용되는 의미를 넘어 새로운 산업을 창출하고 기술과 서비스를 융합하며, 구성원과 사회 전반의 연결을 강화시키는 거시적 흐름으로 설명되기도 하였다.[4)]

특히, 장기간의 코로나19 확산이 낳은 팬데믹 국면에서의 비대면 트렌드의 확산은 디지

4) "기업이 디지털과 물리적인 요소들을 통합하여 비즈니스 모델을 변화시키고, 산업에 새로운 방향을 정립하는 전략"이라고 정의되기도 한다. https://terms.naver.com/entry.naver?docId=3596818&cid=42346&categoryId=42346

털 전환의 효과를 더욱 광범위하게 확산시켰으며, AI, IoT, 가상·증강현실 등 사이버물리세계가 융합된 메타버스 기반 융복합 서비스의 대중화를 앞당겼다. 현실세계를 대체하는 사이버 공간에서의 다양한 활동 경험은 정치, 경제, 사회, 문화, 국방·외교 분야를 가리지 않고 글로벌 메가트렌드로 자리매김한 바 있다(NIC, 2021). 그 결과 일상에서 사이버 공간 활동이 갖는 빈도와 중요성은 지속적으로 증가하였으며 나아가, 현실과 가상이 분리된 패러다임에서 매우 제한적 영역에서만 구현되었던 사이버 공간의 활동은 한층 진화된 형태로 사이버–물리세계 간의 상호작용이 가능한 환경을 제공한 측면도 존재한다.

이처럼 물리적 공간과 사이버 공간이 연결되고, 사이버 공간의 기술을 활용해 물리적 환경과 소통할 수 있는 환경이 구현되면서 가상의 영역이었던 사이버 공간의 활동 범위는 비약적으로 증가하였다. 그러나 이는 새로운 혁신 창출의 기회를 제공하는 긍정적 효과 뿐만 아니라 사이버 공간에 대한 의존 증대, 사이버 공격 위협에 대한 공동체, 국가, 초국가 차원의 취약성으로 이어지는 문제를 낳기도 하였다. 사이버 위협의 양적 증대 측면에서 비대면 패러다임은 사회의 광범위한 디지털 전환과 AI, IoT, VR·AR 등 융복합 서비스를 확대, 일상의 사이버위협 피해 가능성 역시 증대시켰기 때문이다. 사이버 공간의 의존도가 심화되면서, 악의적 행위자에 의한 '공격표면(attack surface)' 역시 확대·노출되었고, 경제적 범죄 조직에서부터 국가 배후의 전문그룹에 이르기까지 사이버공격 양상의 다양화로 이어졌다. 문제는 이 같은 사이버 위협의 변화들이 양적인 수준을 넘어, 질적인 측면에서도 전환적 특징을 가져왔다는 점이다. 무엇보다도 기술 및 경재 패권을 놓고 벌어지는 미중 간의 지정학적 경쟁 역시 디지털·플랫폼 분야를 중심으로한 경쟁이 두드러지면서 사이버 공간은 지정학적 갈등과 대결구도가 뚜렷해지는 무대로 변질되었기 때문이다(김상배, 2020; 이승주, 2022). 실제로 불법적 감청문제를 야기시킨 스노든 사건(2013)과 통신장비의 백도어 논란을 낳았던 화웨이·ZTE 사태는 이러한 디지털 사회에서의 취약해진 데이터 안보 문제를 상징하는 대표적인 쟁점으로 각인된 바 있다. 나아가, 이 같은 일련의 사건들은 전략적 중요성이 증대된 사이버 공간의 확장성을 보여줌과 동시에 그 안에서도 디지털 경쟁에서 우위 확보를 위한 미중 전략경쟁의 양상이 디바이스, 네트워크 인프라, 소프트웨어, 콘텐츠를 넘어 '데이터'를 대상으로 이행되고 있음을 보여주는 것이다. 즉, 데이터를 중심으로 사이버 공간의 전환기적 맥락과 안보적 파급력을 이해해야함을 상기시킨다.

## 2. 데이터 안보 부상의 원동력

그러나 데이터 안보 문제의 쟁점을 논의하기에 앞서 사이버 공간의 확장과 디지털 전환의 고도화를 견인한 주요 동인들을 살펴볼 필요가 있다. AI·지능화 기술과 초연결, 플랫폼 경

제의 부상은 그것이며, 데이터 안보 패러다임을 낳은 기술혁신과 디지털 전환의 토대이자 지향 가치로 작용하고 있다. 또한, 이들은 데이터에 기반한 최근의 글로벌 디지털 경쟁 구도와 안보화 메커니즘을 이해하기 위한 근원적 맥락이라 할 수 있다. 동시에 정보화·컴퓨팅 시대 이전부터 존재해왔으나 그 자체로는 유의미한 가치를 갖지 않았던 데이터를 국가의 중요한 전략 자산으로 변모시킨 원동력이기 때문이다.

전술한 바와 같이 데이터(data)는 현실 세계에서 측정하고 수집한 자료에 불과하며, 어떠한 목적이나 의도에 맞게 가공·처리한 정보(information)가 될 때, 의미를 부여해 왔다. 가치 판단과 의사결정은 필요한 정보에 근거하여 이뤄질 수 있었기 때문이다(김현철, 2019). 컴퓨터 시스템에서 사용하는 로그파일은 단순한 자료일 뿐이나, 로그파일로 어느 유의미한 결과를 얻으면 이 결과는 정보가 되는 것이다. 예를 들어, 전국 단위로 매 시간 기온을 측정한 수치는 데이터에 지나지 않으나, 이를 처리·분석하여 평년 기온을 구하고, 지역별, 일자별로 정리하여 계절별 취약지역 냉난방 지원정책을 수립하게 된다면 비로소 유의미한 정보로 기능하게 된다.

그러나 최근에 목도되는 기술혁신과 융합의 가속화는 기존 데이터와 정보를 구분하였던 차별적 가치를 허물고 있다. 대표적으로 AI와 지능화 도구의 발전은 비정형 데이터를 유의미한 정보로 만들기 위해 투입되었던 시간과 비용을 대폭 감소시켰다. 또한, 수집·분석·가공의 자동화 패턴을 부여하는 학습데이터 알고리즘은 특정 목적을 위한 정보 뿐만 아니라 또다른 정보로 활용할 수 있는 유용한 데이터베이스를 스스로 발전시켰고, 이는 데이터의 잠재적 활용가치의 확장으로 귀결된 바 있다. 여기에 5G·6G 등 클라우드 컴퓨팅 기반의 네트워크 기술의 등장으로 수많은 사용자들은 광범위하게 연결되었으며, SNS 등 국경을 초월한 소통 과정에서 막대한 데이터를 산출하는 결과를 낳았다. 이 같은 변화에 발빠르게 대응한 행위자는 이른바 '빅테크'로 상징되는 거대 플랫폼 기업이었다. 개개인의 생활 패턴을 기록·저장한 데이터베이스를 자체의 지능화 분석체계와 네트워크를 통해 유의미한 정보로 활용하였으며, 편리한 디지털 서비스를 제공함과 동시에 해당 플랫폼 하에서 또다른 연계가치를 창출하는 낳은 새로운 경제구조를 출현시켰다. 이른바 '플랫폼 경제'의 부상이라 할 수 있다. '디지털 중개자"(digital matchmaker)'로 명명되는 거래 플랫폼을 보유한 아마존(Amazon), 바이두(Baidu) 등과 '혁신 플랫폼(innovation platform)' 그룹의 마이크로소프트(Microsoft), 메타(Meta, 舊페이스북) 및 해당 생태계에 속한 수많은 독립 개발자(independent developer)들이 플랫폼 내 호환되는 공통적인 기술 프레임워크를 제공하며 부가가치를 창출하는 거대한 경제적 전환이 나타난 것이다(Wikipedia 2023).

문제는 이 같은 데이터의 잠재력과 활용가치들이 더 나은 서비스 경쟁을 유발시키는 것을 넘어, 해당 플랫폼에 사용자를 묶어두는 '락인효과(lock-in effect)'[5]를 강화하는 등 막대

한 데이터를 권력화하는 움직임을 보이기 시작했다는 점이다. 플랫폼에서의 데이터의 유통과 통제의 문제는 기업 간 표준화 논의 뿐만 아니라 국가 간, 진영 간의 무역 갈등의 문제로 확산되었다. EU의 경우, 역내 플랫폼 기업을 육성하고 역내에서 생산·수집된 개인정보 및 데이터가 반출되는 것에 제동을 걸기 시작했으며, 중국은 공익을 해치는 데이터를 검열·통제하고 국외 유출을 위해서는 당국의 허가와 안전평가 절차를 거쳐야함을 의무화하기도 하였다(김상배, 2018: 36-41). 이와 같이 데이터의 초국경적 유통 규범을 모색하는 입장에 맞서 자국의 데이터 시장을 통제·보호하려는 데이터 국가주권의 입장이 첨예하게 경합하기 시작하였고, 국방 분야에서도 AI 도입이 가속화되면서 해당 사안은 첨예한 안보적 쟁점으로까지 전환되었다고 볼 수 있다(김상배, 2020: 20; 윤정현, 2021: 38-39).

즉, 기술혁신과 초연결이 가속화한 데이터의 플랫폼 경제의 촉진은 혁신의 반대급부로 데이터 자원 유통의 비대칭성을 낳았고, 자체 지능화 알고리즘과 통신인프라로 무장한 플랫폼 기업들의 영향력을 더욱 증대시키는 결과로 이어졌다. 그리고 이러한 양상은 방대한 데이터를 장악하고 있는 소수의 플랫폼 기업 뿐만 국가 간 갈등의 사안으로 작용하게 된다. 디지털 무역과 규범에서의 데이터 독점을 방지함은 물론, 개인정보보호와 관련된 논의를 촉발과도 이어지게 된 것이다. 이러한 일련의 논의들은 과거와 달리 데이터의 잠재적 가치를 보다 용이하게 활용가능하게 된 맥락이 작용한 결과라 할 수 있을 것이다.

## 3. 사이버 안보와 데이터 안보의 전환적 메커니즘

이처럼 오늘날 데이터의 중요성이 커짐에 따라 사이버 안보의 주된 보호 대상과 접근방식 또한 변화하고 있다. 그리고 이 같은 변화의 필요성을 압박하는 요인으로 사이버 공격 방식의 유형별 특징과 진화가 자리하고 있음에 주목해야 한다. 최근 생산되는 데이터 대부분은 디지털화되어 있다. 그리고 네트워크에 연결된 데이터 센터, 엣지 컴퓨팅(Edge computing), 엔드포인트(Endpoint) 등의 디지털 저장매체에 저장되어 다양한 사이버공격에 취약한 특성을 지니고 있다. 즉, 데이터 안보를 위협하는 행위는 사실상 사이버 공간을 통해 이루어지며 생성·유통·저장된다. 이를 간파한 국가 또는 국가 배후의 악의적 공격자들은 전시, 평시의 정치 · 외교적 압박에서부터 국가 기밀이나 전략기술과 밀접한 기업의 지적 재산 확보 까지 다양한 목적을 실행하는 도구로서 데이터를 노린 사이버 공격 무기를 활용하고 있다. 또한, 데이터를 암호화한 후 복구키를 제공하는 대가를 요구하는 단순한 수법에서 벗

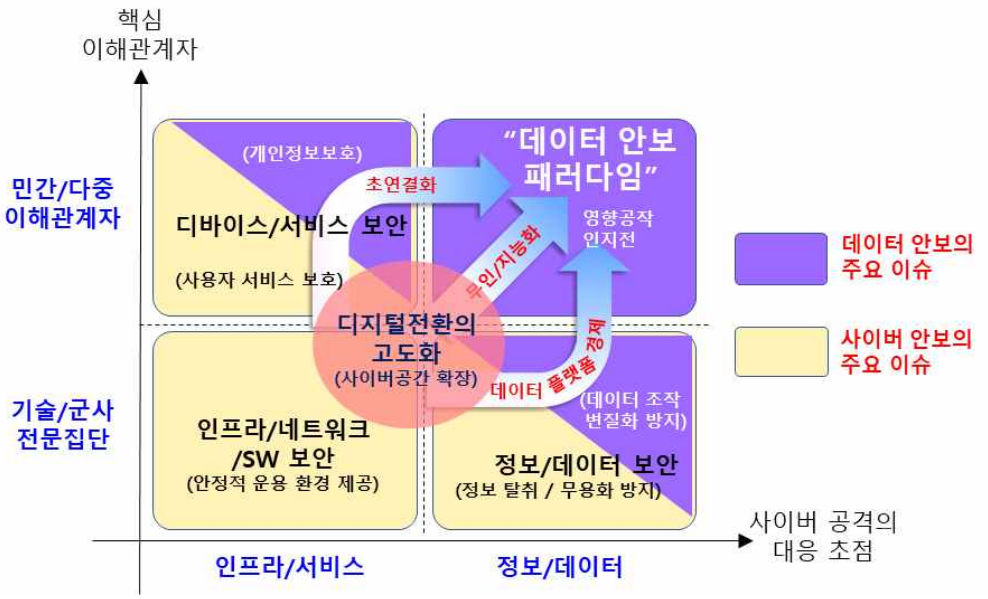
5) '잠금효과'로 번역되기도 하며, 특정 서비스에 소비자를 묶어 두는 효과를 의미한다. 아마존, 이베이 등 막강한 사용자 데이터와 플랫폼을 보유한 글로벌 전자 상거래 기업이 발휘하는 영향력으로서, 자사의 서비스를 경험한 고객들이 더 매력적인 다른 플랫폼의 서비스로 이탈을 방지하는 효과로 나타난다. https://en.wikipedia.org/wiki/Vendor_lock-in

어나 데이터를 탈취, 조작, 오염시켜 기업과 정부, 국가 간 신뢰를 훼손하려는 시도를 감행하기도 한다. 이처럼 사이버 공격 양상의 진화는 데이터 안보의 가장 위협적인 도전으로 작용한다. 이러한 맥락에서 기존의 사이버안보 이슈에서 주요한 문제가 되었던 부문과 핵심 이해관계자에 대한 검토와 전환적 차원의 접근이 시급해지고 있다.

우선, 사용자의 안정적 운용 환경을 제공하기 위한 인프라, 네트워크, 소프트웨어 보안 등은 사이버 공격행위에 대비하기 위한 주된 방향이었다. 디바이스와 서비스 측면에서는 애플리케이션 보안 등 사용자 서비스 보호를 위한 접근이 이루어졌으며, 정보 및 데이터 보안의 사안에서는 정보 탈취, 유출 등을 막기위한 대책 마련에 방점을 두어왔다. 즉, 그간의 사이버 안보의 기본적인 접근방식은 기술/군사전문 집단을 노린 동시다발적 해킹, 군사기밀 정보 유출과 탈취, 삭제 등 '정보·데이터 무용화' 공격들에 대한 대비를 전제하였다고 볼 수 있다.

그러나 데이터 안보적 관점에서는 민간/다중이해관계자를 겨냥한 개인정보의 유출과 악용, 양질의 정보 뿐만 아니라 데이터 조작, 변조, 오염 등 '데이터의 변질화'를 목표로한 공격 역시 예의주시해야할 도전이 되고 있다. 그리고 이를 토대로 중요 국면에서 허위정보와 가짜뉴스를 생산·유통 시키는 등 민간과 불특정 다중이해관계자를 위협하고 사회공학과 결합된 공격 유형들이 빈번해지고 있다. 사이버 안보를 총괄하는 국가의 임무에는 개인정보보호와 '데이터의 변질화' 공격에 대응해야 함을 시사하는 것이다. 이 같은 사이버 안보와 데이터 안보가 내재한 전환적 특징들을 도식화하면 〈그림 1〉과 같다. 본고는 아래의 분석틀을 토대로 데이터 안보 시대의 주요 사이버 공격 유형과 사례를 검토하고 안보적 시사점 및 대응방안을 제시하고자 한다.

〈그림 1〉 사이버 공격의 위협 대상, 대응 초점으로 본 데이터 안보 패러다임




출처: 저자 작성.

## Ⅲ. 데이터 안보 시대의 사이버 공격 유형과 사례

### 1. 해킹으로 인한 데이터의 유출 고도화

데이터 안보 시대에 데이터 자체를 겨냥한 사이버 공격 유형의 대표적인 특징 중 하나는 '데이터 유출'이라 할 수 있다. 데이터 유출은 데이터의 소유주나 관리자가 의도하지 않게 보호되지 않는 환경으로 빠져나가는 것으로, 공격자 기준으로는 데이터 탈취라고 할 수 있다.[6] 이러한 유출은 내부자의 실수나 악의적인 행위, 물리적 도난이나 분실, 네트워크나 서버나 잘못된 설정 등 다양한 형태로 발생하는데, 오늘날 디지털 의존도와 연결성이 높아지면서 사이버 공격이 데이터 유출의 주요 수단이 되고 있다. 데이터 탈취를 목적으로 하는 해킹은 데이터가 저장된 서버와 PC에 존재하는 취약점이나 사람의 심리를 악용하는 사회공학(Social Engineering) 기법 등 다양한 형태로 활용하고 있다.

먼저, '피싱(Phishing)'은 불특정인을 대상으로 이메일, 문자메시지, SNS 등을 이용하여 믿을 만한 사람이나 기업이 보낸 메시지처럼 가장한 뒤 악성 URL이나 피싱 사이트로 유도하여 사용자의 개인 정보(Credential)나 금융 정보를 훔치거나 악성 코드를 감염시키는 수법

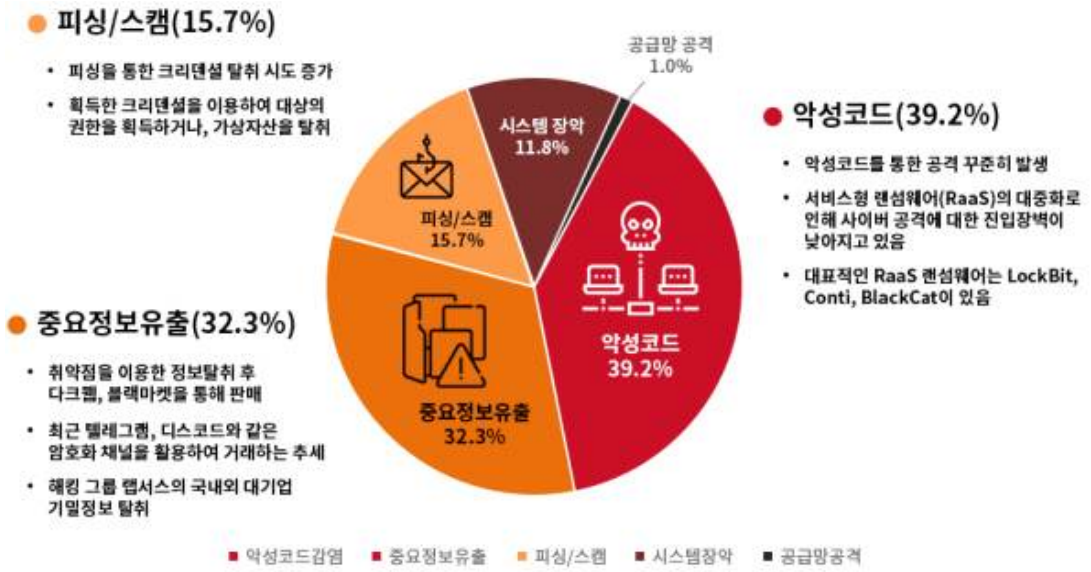
6) https://www.cloudflare.com/ko-kr/learning/security/what-is-a-data-breach/

이며, 전통적으로 초기 침투 공격(Initial Access)에 많이 사용한다.[7] 피싱은 특정인이나 조직을 대상으로 정교하게 만든 비즈니스 이메일 등을 통해 공격하는 스피어 피싱(Spear Phishing)으로 발전하였고, 최근에는 생성형 AI에 적용되어 매우 정교한 조작 메일의 형태로 피해를 입히고 있다. 표적화된 사용자의 계정, 비밀번호 등 사용자가 이용할 만한 시스템이나 사이트에 무작위로 대입(Stuffing)하여 로그인되면 추가로 정보를 탈취해 가는 이른바 '크리덴셜 스터핑(Credential Stuffing)'으로 이어진다. 대표적인 사례는 2016년에 스피어 피싱을 통해 미국 민주당 전국위원회(DNC)의 이메일 시스템에 침입한 것이다. 당시 미국의 FBI와 DHS의 공동보고서에 따르면 러시아의 한 해킹그룹(APT29)이 스피어 피싱으로 미국 정당 관계자 1명의 계정에 들어가 먼저 악성코드를 심고, 또 다른 해킹그룹(APT28)이 2016년 봄부터 감염된 미국 정당 관계자 계정을 이용하여 이메일 교신 내용을 모니터링하고 정보를 유출한 것으로 조사되었다[8]. 이러한 경로로 유출된 미국 민주당의 이메일 내용은 '위키리스크' 등을 통해 폭로되기 시작하여 민주당의 힐러리 클린턴 후보를 곤란에 빠뜨림으로써, 대선 결과에도 치명적인 악재로 작용한 것이다. 피싱 역시 최근 생성형 AI와 결합되어 고도화되고 있다. 해킹 · 악성코드와 관련된 데이터를 대량 학습해 스피어피싱 이메일 제작에 특화된 '웜GPT(WormGPT)'가 다크웹과 텔레그램에서 유료로 거래되고 있어[9], 향후 불특정 다수에 의한 스피어 피싱 공격이 데이터 안보에 커다란 위협으로 작용할 전망이다.

실제로 비근한 2022년 상반기의 사이버 침해사고 유형별 발생 통계를 살펴보면, 악성코드 감염이 39.2%로 가장 높은 비중을 차지했으며, 중요 정보 유출이 32.3%, 피싱/스캠이 15.7%을 차지했다. 그 외 시스템 장악이 11.8%, 공급망 공격이 1.0%인 것으로 보고된 바 있다(한국재정정보원, 2022. 9. 29.)

7) https://www.trendmicro.com/ko_kr/what-is/phishing.html
8) https://blog.naver.com/gowit_sps/221566173768
9) https://www.edaily.co.kr/news/read?newsId=03011046635835568&mediaCodeNo=0

〈그림 2〉 2022년 국내 사이버 공격유형별 피해사례




출처: 한국재정정보원(2022. 9. 29.)

둘째로, 랜섬웨어(Ransomware) 공격은 악성 코드를 사용하여 사용자의 데이터를 암호화하고 이를 복구하기 위한 몸값을 요구하는 것으로,[10] 주로 기업들을 대상으로 하였으나 점차 지자체나 국가 기관은 물론 핵심 기반 시설까지로 확대하고 있다. 최근에는 다크웹 등에서 손쉽게 구매할 수 있는 서비스형 랜섬웨어(RaaS)의 등장으로 기술이 부족한 초심자도 공격이 가능하고 시간과 비용을 줄일 수 있게 됨에 따라 랜섬웨어는 범죄자의 새로운 저비용 고수익 비즈니스 모델로 인식되어 확대되고 있다. 또한 이른바 '정보 인질'을 통한 협상력을 높이기 위해 범죄자는 암호화하기 전에 데이터를 유출하고 민감한 정보를 공개하겠다고 위협하는 이중 전략을 구사함으로써 적극적 대응을 제약할 가능성이 높다. 대표적인 사례는 2017년 발생한 WannaCry 랜섬웨어이며, 당시 미국, 영국, 러시아 등 150여 개국의 PC 30만 대를 감염되어 영국 공립병원, 프랑스 자동차 제조사 르노, 스페인 통신업체 텔레포니카, 닛산 등의 서버와 PC가 마비되는 등 경제적 피해가 40억 ~ 80억 달러에 이르렀다[11]. 2021년에는 미국 최대 송유관 관리업체인 콜로니얼 파이프라인(Colonial Pipeline)이 '다크사이드(DarkSide)' 해킹그룹의 랜섬웨어 공격을 받아 동부지역 연료 공급이 일시 중단되는 등 피해를 본 가운데, 임직원 5,800여 명의 개인 정보도 유출된 것으로 밝혀진 바 있다[12]. 이후 다크사이드는 정치적 목적은 없으며, 파트너 중 하나가 잘못된 표적을 선택하여 발생

10) https://en.wikipedia.org/wiki/Ransomware
11) https://nordvpn.com/ko/blog/wannacry-ransomware-attack/
12) https://www.cctvnews.co.kr/news/articleView.html?idxno=229908

한 것이라고 밝혔지만[13] 서비스형 랜섬웨어(RaaS) 공격에 대한 통제의 어려움이 부각되고 사회기반시설이 마비되었다는 점에서 데이터 안보를 위한 사이버 보안의 중요성을 일깨워 주고 있다. 특히 국가 또는 국가배후 해킹조직의 경우 공격 주체를 위장하기 위해 랜섬웨어를 이용하여 데이터를 탈취하거나 삭제하는 수법을 사용하기도 하고 있어 이제 랜섬웨어 공격을 단순한 금전을 노린 사이버 협박 범죄로만 취급할 것이 아니라 데이터와 사이버안보 차원에서 다루어야 할 상황이다.

셋째로, 맬웨어(Malware) 공격은 바이러스(viruses), 웜(Worm), 트로이목마(trojans), 와이퍼(Wiper), 루트킷 등 악성 소프트웨어(Malicious software)를 사용하여 정보를 유출하거나 시스템을 손상시킨다.[14] 일반적으로 사이버공격은 침투, 확산, 정보 탈취 등 단계에 따라 여러 종류의 맬웨어를 복합하여 사용한다. 대표적으로 2010년에 발견된 Stuxnet 웜은 이란의 14개 핵 시설에 있는 2만 개 이상의 제어장치를 감염시키고 약 900대의 원심분리기를 망가뜨려서 수년 동안 국가의 핵 프로그램을 둔화시킨 복잡한 악성 코드 공격 중 하나였다[15]. 스턱스넷은 미국과 이스라엘이 개발했으며, USB에 담겨서 네덜란스 정보기관(AIVD)의 스파이가 이란 나탄츠에 위치한 핵실험 시설 급수 펌프에 설치하였다[16]. 인터넷에 연결되지 않은 시스템까지 마비시킨 높은 기술력과 파괴력으로 인해 스텍스넷 공격은 산업시설의 제어시스템에 대한 사이버 공격의 위험성이 부각되는 계기가 되었다. 이외에도 2015년에 미국의 의류 제조업체(Hanesbrands)가 웹 사이트를 통한 사이버공격으로 인하여 약 백만 개의 주소, 전화번호 등의 고객 데이터가 유출되기도 하였다. 이렇게 맬웨어는 데이터 탈취 및 암호화, 제어시스템 마비 등 다양한 목적으로 사용되어 사이버 안보와 데이터 안보에 위협요인이 되고 있다.

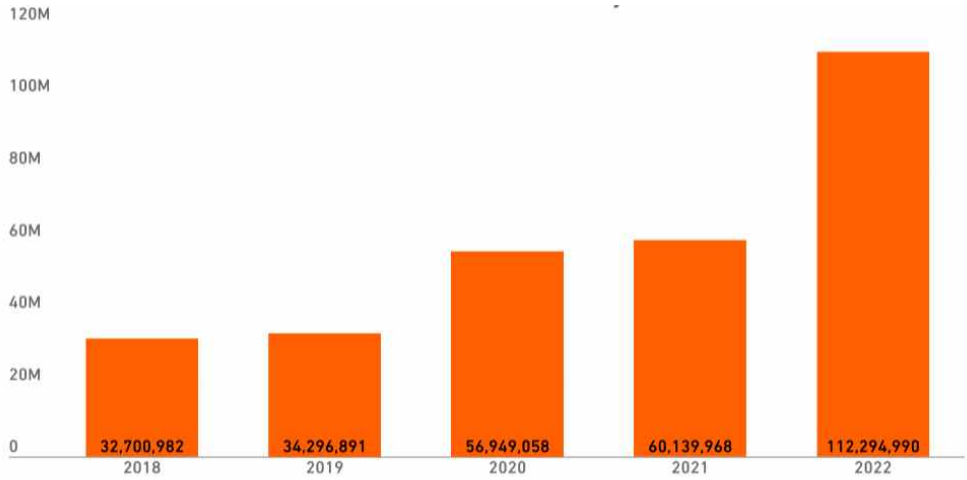
서버와 시스템을 대상으로 하는 기존의 해킹과 달리, IoT는 인터넷에 연결된 디바이스를 타겟으로 한다. 여기에는 공격에 취약한 TV, 스피커, 보안 카메라, 의료 기기와 같은 스마트 가전제품들이 포함된다. 연결된 디바이스의 수가 계속 증가함에 따라 2022년 IoT 멀웨어 발생 건수는 전년 대비 87% 급증하여 1억 1,230만 건으로 사상 최대치를 기록했다.[17] 또한, 전세계적으로도 IoT 기반의 멀웨어 발생량이 눈에 띄게 급증하였음이 보고되었다.

---

13) https://www.cyberone.kr/news-trends-detail?id=73372&page=1
14) https://www.ibm.com/kr-ko/topics/malware
15) https://nordvpn.com/ko/blog/stuxnet/
16) https://techrecipe.co.kr/posts/61913
17) https://www.techopedia.com/kr/cybersecurity-statistics

〈그림 3〉 글로벌 멀웨어 감염 피해 규모의 증대(2018–2022)

(단위: 백만달러)




출처: https://www.techopedia.com/kr/cybersecurity-statistics

마지막으로, 네트워크 스니핑(Network Sniffing) 공격은 네트워크를 통해 전송되는 데이터를 무단으로 캡처하고 분석하여 계정 정보, 암호, 기타 민감한 데이터를 절취하는 수법이다. 대표적인 사례로 2007년부터 시작한 구글의 스트릿 뷰(street view) 서비스를 위해 특수 차량으로 거리를 찍으면서 주변의 와이파이 데이터도 함께 수집했는데, 여기에는 주민의 와이파이 이름, MAC 주소, 사용자 이름, 암호, 개인 이메일, 개인 전자문서 등 정보까지 포함되어 법적 분쟁으로 이어지기도 하였다[18]. 암호화되지 않는 무선 네트워크가 주된 표적이 되지만, 유선 인터넷 환경에서도 데이터가 암호화되지 않는 프로토콜을 사용하는 사이트일 경우, 역시 스니핑에 취약한 것으로 보고된 바 있다.[19]

## 2. 활용 데이터 조작(Data Manipulation)

데이터 안보 시대에 두드러진 사이버 공격 중 하나인 '데이터 조작'은 데이터 기반 플랫폼 경제의 순환가치를 훼손하고, 주요 자동화 인프라의 혼선을 야기시킴으로써 대형 사고를 유발하는 치명적인 공격이 될 수 있다. 나아가 이를 토대로 산출된 정보의 정확성과 신뢰성, 무결성을 의도적으로 손상하는 행위라 할 수 있다. 이러한 조작은 데이터의 변조, 주입, 삭

18) https://www.boannews.com/media/view.asp?idx=33794&kind=3
19) 최근 대부분의 사이트는 웹 브라우저와 웹 사이트 간에 데이터를 SSL(Secure Socket Layer) 프로토콜로 암호화하여 전송하는 https를 사용하여 스니핑에 비교적 안전한 편이다.

제 등 다양한 형태로 발생하며, 일부는 본인이 연구 데이터 등을 조작하는 경우도 있지만, 대부분 외부 세력의 악의적인 사이버공격을 통해 발생한다.

먼저, 데이터 변조(Data Tampering)는 데이터의 내용을 의도적으로 '승인없이' 변경하거나 왜곡하는 행위를 의미한다.[20] 대표적으로 2010년 Stuxnet 웜은 이란에 소재한 원심 분리기의 제어시스템 데이터를 변조하여 기계를 파괴한 사례이다. 또한 2021년 초 플로리다 수처리 시설에 침입한 해커가 물속의 유독물(수산화나트륨)을 안전하지 않은 높은 수준으로 높이는 사건이 발생하기도 하였다[21]. 최근 사이버물리 영역간의 연결성을 구현하는 메타버스와 IoT의 활용 확대로 사이버 공격을 통한 데이터의 변조 피해가 물리적 영역에서도 발생하고 있다. 실제로 제약 기업의 경우, 데이터의 도난이나 랜섬웨어 감염이 보고되지 않은 가운데 임상 시험의 일부 데이터만 은밀하게 변경된 사건이 발생하기도 하였으며, 변조된 임상데이터를 기반으로 잘못된 약을 개발하여 출시하게 될 경우, 결국 손실로 이어질 수 있음을 보여주었다.[22]. 무엇보다도 외부 해커나 악의적 내부자에 의한 데이터의 변조 공격은 삭제나 유출보다 탐지와 정정이 어렵다. 만약 변조 데이터 보고에 기반해 국가적 중대 결정을 내릴 경우, 그 피해는 가늠하기 어려울 것이다.

두 번째로 시스템에 가짜 데이터를 주입(Data Injection)하여 결과를 왜곡하는 유형도 증대되고 있다. SQL 인젝션(SQL Injection) 공격이 여기에 해당하는데, SQL 인젝션(SQL Injection) 공격은 데이터베이스(DB) 시스템에 대한 공격으로, 데이터베이스에 대한 질의 내용(SQL 구문)을 조작하여 정보를 빼내거나 조작하는 해킹 수법이다.[23] 대표적인 사례는 2017년 숙박앱인 '여기어때'에 해킹 사건이다. 해커는 DB 접근 페이지의 보안상 취약점을 이용한 'SQL인젝션(injection)' 등의 기법을 사용하여 99만명의 고객 개인정보 341만 건을 탈취하여 수치심을 유발하고 금전을 요구하는 데 악용한 바 있다.[24].

세 번째로 데이터베이스 시스템에 악의적 코드(Query)를 주입하여 민감한 정보를 유출하거나 데이터베이스(DB)를 손상시키는 수법도 빈번해지고 있는 중이다. 대표적으로 크로스 사이트 스크립팅(XSS) 공격의 경우, 웹 애플리케이션의 취약점을 이용해 악의적인 스크립트를 사용자의 브라우저에 삽입하는 수법으로 개인정보 및 쿠키정보를 탈취하고 악성코드 감염, 웹페이지 변조의 피해를 입힌다.[25] 대표적으로 2010년 트위터(Twitter, 현재 X)가 XSS 공격을 받아서 공격 코드가 삽입된 글을 클릭하지 않고 단지 글에 마우스를 접촉하기만 해

20) https://www.mbaknol.com/information-systems-management/data-tampering-meaning-types-and-countermeasures/
21) https://www.protocol.com/enterprise/data-integrity-security-cyberattacks-threat
22) https://www.protocol.com/enterprise/data-integrity-security-cyberattacks-threat
23) https://www.cdnetworks.com/ko/cloud-security-blog/what-is-a-sql-injection-attack/
24) https://www.joongang.co.kr/article/21628794#home
25) https://tibetsandfox.tistory.com/5

도 악성코드나 포르노와 같은 유해 정보가 담겨있는 사이트로 연결되는 현상이 나타나기도 하였다. 당시 회원 정보 등의 데이터가 유출되는 피해로는 이어지지 않았지만, 이용자의 혼란을 야기함은 물론, 해당 서비스 기업의 이미지 악화와 시장의 불신을 낳기도 하였다.[26]. 또한, 악성 사이트로 연결되거나 악성코드가 삽입되었다면 개인정보유출 등의 추가적인 피해를 낳을 수도 있었다.

데이터 조작의 또 다른 유형은 정보시스템의 데이터를 의도적으로 삭제(Data Deletion)하여 시스템을 마비시키거나 주요 정보를 유실시키는 수법이다. 주로 와이퍼(Wiper) 맬웨어가 사용된다. 2022년 발생한 러시아–우크라이나 전쟁에서 와이퍼가 많이 사용되었으며, 전쟁 직전 친러시아계 해킹조직이 '위스퍼 게이트(WhisperGate)' 맬웨어로 사이버 공격하여 우크라이나의 외무부를 포함한 70여 개의 정부 웹사이트를 중단시켰다(이형동 외, 2022: 353–362). 데이터 삭제는 정보 절취를 넘어서 시스템을 파괴하는 가장 위협적인 사이버 공격 중 하나로서 전쟁이나 외교 · 군사적 목적을 달성하기 위한 국가가 관여하는 경우가 많다.

## 3. AI·자동화를 겨냥한 데이터 오염(Data Corruption)

데이터 오염은 의도하지 않은 데이터의 변경이나 삭제 등을 의미하며, 데이터 저장 장치의 물리적 훼손이나 전원 차단으로 인한 자료의 멸실, 소프트웨어 등의 충돌, 사용자의 조작 실수 등 다양한 원인으로 발생한다.[27] 데이터 변경의 결과를 낳는다는 측면에서 유사점이 있지만, 데이터 조작이 좀 더 악의적인 행위를 의미한다면 데이터 오염은 고의성이 다소 낮은 행위를 표현한다고 할 수 있다. 최근 생성형 인공지능(AI)의 등장으로 머신러닝(ML)이나 AI의 알고리즘을 훈련하는 데이터의 정확성과 신뢰성이 주요한 과제로 등장하였다. 훈련 데이터가 오염될 경우 AI의 알고리즘에 편향성과 환각(Hallucination) 현상을 일으켜 정확한 정보를 생성하지 못하고 가짜 뉴스를 생성하거나 인간의 의사 결정에 잘못된 판단을 유도하여 AI 시스템에 대한 신뢰성을 저하하게 하는 원인이 된다. 대표적으로, 악의적인 학습 데이터로 훈련을 시켜서 머신러닝 모델을 망가뜨리는 중독 공격(Poisoning attack)은 AI 모델 자체를 공격해서 모델에게 영향을 주는 방식이다[28].

이들 유형 중 또다른 공격 방식은 입력 데이터에 최소한의 변조를 가해 머신러닝을 속이는 '회피 공격(Evasion attack)'이다. 2017년 워싱턴대학의 연구팀은 도로 교통 표지판에 이

26) https://www.boannews.com/media/view.asp?idx=22941&kind=1
27) https://terms.naver.com/entry.naver?docId=6653405&cid=69974&categoryId=69974
28) https://www.lgcns.com/blog/cns-tech/ai-data/9616/

미지 스티커를 부착해 자율주행 자동차의 표지판 인식 모듈을 교란하여 자율주행차가 '정지' 표시를 '속도제한' 표시로 잘 못 인식하도록 만드는 회피 공격을 시연한 바 있다. 이러한 머신러닝 알고리즘의 취약점과 악의적 데이터 오염에 의해 적대적 환경에서 발생할 수 있는 적대적 공격(Adversarial Attack)은 AI 시스템을 오작동 시킨다는 점에서 다양한 위험 요소로 작용할 것이다[29]. 사이버 공격을 통해 훈련 데이터나 입력 데이터를 오염시켜 자율자동차의 표지판 인식, CT 영상 자동 판정, 가짜뉴스 생성 등에 AI 오작동을 유도하는 경우, 국민의 생명을 위협하고 사회 혼란을 유발할 위험성이 상존한다.

## 4. 민주국가의 주권을 위협하는 '영향공작(Influence Operations)'

'영향공작(influence operations)'은 전시와 평시 경쟁국이나 적국의 정보환경과 여론을 자국의 군사적 · 국제정치적 입지에 유리하게끔 조작 하거나 조성하는 활동을 의미한다. 즉 비군사적 수단을 사용하여 개인, 주요 세력, 대중이 자국의 이익에 부합하는 의사결정 내리도록 군사, 경제, 정치적 수단 동원하는 포괄적 행위를 의미한다(송태은, 2023a: 1). 영향력 공작은 국가차원에서도 자국의 전략, 목적, 또는 정책목표 등을 위해 감행될 수 있다. 영향공작은 상대 국가에 대해 비교우위를 점하기 위한 선전 · 선동과 함께 전술적 정보를 수집하는 작업까지도 포함하는 심리전(psychological warfare)의 일환으로[30] 전시뿐만 아니라 평시에도 전개되고 있으며, 국가 안보에 심각한 위협이 되고 있다. 과거 영향공작은 불온전단이나 라디오 · TV 방송 등을 통해 진행되었지만, 이제 대부분 사이버 공간의 복잡성과 익명성을 이용하여 해킹이나 SNS 등을 수단으로 다양하게 이루어지고 있다(김일기, 2023).

특히 선거 국면에서 영향공작과 허위조작정보의 유포 행위는 '민주주의 국가에서 후보자에 대한 검증과 정보 제공은 유권자의 정당한 권리'라는 점을 악용할 수 있는 대표적인 사이버 공격 형태로 자리잡게 된 것이다.[31] 대표적인 영향공작의 유형은 해킹을 통해 민감한 정보를 유출하여 공개함으로써 여론에 영향을 미치는 데이터 유출(Hacking and Data Leaks)이라 할 수 있다. 2016년 미국 민주당 전국위원회(DNC)의 이메일 시스템을 해킹하여 수집한 이메일 내용을 '위키리크스' 등으로 폭로하여 민주당 힐러리 대통령 후보를 곤란에 빠뜨

29) https://www.kisec.com/rsrh_rpt_det.do?id=221

30) 미국과 NATO는 이를 '인지전(Cognitive Warfare)' 개념으로 발전시키고 있으며, 특히, EU에서는 용어를 상대적으로 순화하여 FIMI(Foreign Information Manipulation and Interference · 해외정보조작개입)라는 개념으로 규정하고 적극적으로 대응하고 있다. 윤민우, 2023. "기존 국가보안법 등으로는 중국의 영향력 공작 등 대처 못 해" 『월간조선』. (2023년 9월호), https://monthly.chosun.com/ client/news/viw.asp?nNewsNumb=202309100042

31) 이 같은 허위조작정보의 문제는 결국 국가의 정치적 정당성을 훼손하는 국가 주권에 대한 개입 행위로 간주될 수 있다. 송태은(2023) a, "허위조작정보를 이용한 사이버 영향공작과 국가안보: 실태와 대응책", 『정책연구시리즈 2023-13』, 국립외교원 외교안보연구소. p. 2.

린 사건이 그 예이다. 또 다른 유형은 소셜 미디어 플랫폼을 이용하여 여론을 왜곡하는 소셜 미디어 조작(Social Media Manipulation)이다. 이는 가짜 계정, 봇넷(botnet), 또는 트롤(troll)을 사용하여 특정 메시지를 확산시키거나 특정 주제에 대한 토론과 여론을 왜곡시키는 수법이다.[32] 실제로 2016년 러시아의 인터넷 리서치 에이전시(IRA)는 수천 개의 소셜 미디어 계정을 만들어서 친(親)트럼프, 반(反)클린턴 허위정보, 가짜 뉴스를 외부로 확산시켜 약 1억 2천 6백만 명의 유권자가 시청한 것으로 보고된 바 있다.[33]. 2016년 초에는 케임브리지 애널리티카(Cambridge Analytica)가 8,700만 페이스북 가입자의 프로필을 그들의 동의 없이 수집해서 정치적 선전을 하려는 목적으로 2016년 미국 대통령 선거와 영국의 브렉시트 국민투표, 인도, 이탈리아, 브라질 등에 사용되었다[34].

단순히 잘못된 정보(misinformation)가 아닌 특정한 목적을 위해 의도적으로 만들어진 거짓 정보인 '허위조작정보(disinformation)'를 유포하는 것은 정치적, 사회적, 경제적 영역에서 강력한 영향을 미치며, 때로는 국제 관계에도 중대한 영향을 끼칠 수 있다. 특히 ChatGPT 등 다양한 생성형 AI이 등장하면서 딥페이크 영상이나 이미지 등을 활용한 허위조작정보는 더욱 위력적인 사이버 공격무기가 되고 있다. AI가 생성한 조작정보가 초연결·개인화된 불특정 다수의 SNS를 통해 확산되고, 다중의 여론을 형성함으로써 사회적 혼란을 야기하는 영향공작의 바현 메커니즘은 데이터 안보 시대의 가장 위협적이고 고도화된 사이버 공격 양상의 진화를 보여주는 단면이라 할 수 있을 것이다.

# Ⅳ. 데이터 안보 강화를 위한 주요국의 전략 초점

## 1. 민간 · 다중이해관계자와의 협력 강화

이처럼 최근 데이터에 기반한 사이버 보안의 중요성이 부상하면서 미중 역시 확장된 이해관계자와 사이버 공격 방식의 전환을 염두에 둔 대응책을 마련하고 있다. 첫 번째 특징은 국가안보 기관의 기술 · 군사 전문집단 대상에서 민간과 다중 이해관계자를 고려한 파트너십의 확장이다. 특히 미국은 국가 중요 인프라 보호를 위한 핵심 방안으로서 민관 협력의 확대를 기조로 하고 있다. '국가 사이버보안 전략 실행계획'과 민간 플랫폼 수집 데이터의 윤리적 활용을 위한 프레임워크가 대표적이다. 중국 역시 국영, 민간 기업들과의 긴밀한 연대를 강조하고 있으나, 주로 데이터 수집 및 활용, 군민 융합 전략의 실천과제로서 민간의 데이터

32) https://www.kisdi.re.kr/bbs/view.do?bbsSn=114317&key=m2101113043145
33) https://m.boannews.com/html/detail.html?idx=58122&kind=3
34) https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal

보안 문제들을 개선하는데 주력하고 있는 상황이다.

미국의 경우, 사이버보안 및 인프라 보안국(Cybersecurity and Infrastructure Security Agency, CISA)이 2023년 7월에 수립한 '국가 사이버 보안 전략 실행계획(National Cybersecurity Strategy Implementation Plan)'에는 부문별 위험 관리 기관(SRMA)과 협력하여 시스템과 자산을 보호할 책임이 있는 각 분야의 인프라 소유주와 운영자에게 지원을 제공하고, ISAO(정보 공유 및 분석 조직), ISAC(부문별 정보 공유 및 분석 센터)은 사이버 방어 작전을 수행할 것을 명시하고 있다. 이를 위해 보안 기반의 설계 및 보안기술 기본 설계 채택 촉진을 위한 공공-민간 파트너십 확대를 하위 이니셔티브로 설정하였는데, ▲CISA는 기술 제조업체, 교육자, 비영리 조직 등 기타 기관과의 공공-민간 파트너십을 주도하여 설계 및 안전한 소프트웨어 및 하드웨어의 개발 및 채택을 장려할 것 ▲CISA는 NIST, SRMA를 포함한 연방 기관, 민간 부문과 협력하여 정부 표준 및 관행을 활용하기 위한 기본 보안 원칙을 개발할 것 등의 내용을 담고 있다(천곤웅 · 김성훈, 2024: 4). 또한, 적대적 활동에 대해 연방 정부보다 민간 부문이 수집한 정보가 부분적으로 더 포괄적이고 상세하며 위협을 추적하는 역량이 빠르게 발전하고 있으므로 이러한 악의적인 활동을 차단하기 위해서는 민 · 관 협력이 중요하다는 인식하에 국가 사이버 포렌식 교육연합(NCFTA, National Cyber-Forensics and Training Alliance)과 같은 연방 정부와의 운영 협력 허브 역할을 할 수 있는 비영리 파트너 조직을 통해 공동 대응하는 것을 권장하고 있다(천곤웅 · 김성훈, 2024: 10).

또한, '국가정보장실(Office of the Director of National Intelligence: ODNI)'은 정보기관들이 업무 과정에서 민간 플랫폼 · 브로커 등이 수집한 '상업적 이용 가능 정보(CAI)를 구매 및 활용하는 것과 관련하여 '프라이버시 침해' 등 우려 여론 해소와 함께 윤리적인 데이터 이용 거버넌스를 구축하기 위해 상업적 데이터 윤리적 활용을 위한 프레임워크를 공개하며, 정보 공동체에게 상업적 데이터 활용 관련 보호조치 강화 등 내부 시행 절차를 마련하도록 지시한 바 있다. 프레임워크의 주요 내용으로는 ①상업적 데이터 활용시의 기본 원칙과 ②'민감' 상업적 데이터 활용시 보호 조치로 구성되어 있다. 또한, ODNI는 성공적인 임무 수행을 위해서는 기술 투자가 필수적이라는 인식하에 민간 정보공동체의 IT 역량을 제고하기 위해 '정보기술 로드맵'을 통해 최우선 투자 필요 5대 분야를 제시한 바 있다.

| | |
|---|---|
| 안정적 · 탄력적 디지털 기반 강화 | 정보 공동체의 미래 역량 강화를 위해서는 네트워크 · 컴퓨팅 · 스토리지 등 IT 분야 투자 필수 |
| | △IC 클라우드 환경 최적화를 통해 임무에 활용가능한 첨단 툴 추가 확보 △컴퓨팅 · 스토리지 · 전송 역량 제고 △현장 중심 임무 수행이 가능토록 모바일 역량 강화 |
| 강력한 사이버보안 체계 확립 | 진화된 안보위협에 대처할 수 있는 '제로트러스트(ZT)' 등 최신 사이버보안 시스템 조기 구축 |
| | △IC 시스템 전반에 ZT 보안체계 구축 △첨단 리스크 관리 확대 △기관 간 보안 협업으로 IC 집단 방어 역량 강화 △IC의 S/W 개발 · 보안 · 운영방식 개선 △양자내성(QR) 암호화 체계 구축 △크로스 도메인 솔루션(CDS) 조기 개발 |
| 최신 관행 및 파트너십 구축 | IC 임무 성공은 △해외 동맹국 △민관 파트너와의 협업 △IC 인력의 기술 접근성 보장이 관건 |
| | △협업 방해 요소 제거 등 협업체계 강화 △민첩하고 비전통적인 파트너십 구축 △IC 인력의 IT 접근성 확대 △IC 구성요소 간 상호운용성 촉진 |
| 데이터 중심 환경 구현 | IC의 첨단기술 활용 확대를 위해서는 △'조직 · 시스템 중심 패러다임'에서 '데이터 중심 패러다임'으로 전환 △조직의 자산 · 권한 · 권리 보존 △보안 강화 등이 필수 |
| | △'End-to-End' 데이터 관리체계 구현 △IC의 데이터 중심 아키텍쳐 개발 및 실행 △민감한 데이터 사일로(데이터 단절)를 데이터 중심 앤클레이브(enclave)로 전환 |
| 첨단기술 및 인력 준비 강화 | IC는 미래 대비를 위해 첨단기술 도입 · 배포와 함께 전문인력을 양성 · 유지할 필요 |
| | △AI 개발 · 활용 가속화 △양자 등 신기술 연구 · 개발 △미래 IT 인력 육성 |

〈표 1〉 정보기술 로드맵 내 5대 중점 분야

美ODNI 홈페이지, (2024. 5. 30).

반면, 중국은 정보통신 · AI 등 첨단기술 발전과 함께 데이터 수집 · 공유 · 연계 등이 핵심 경쟁력이라고 판단한 이래로 국영 · 민간 기업들을 적극적으로 동원하여 데이터 수집 및 활용에 나서고 있다. 일례로 중국의 사이버보안 업체인 아이순(I-Soon)은 중국 시짱자치구를 포함한 11개 성 이상의 공안청 및 국가안전부, 인민해방군과 계약을 체결하여 직접 외국 정부 기관 · 기업 등 반중단체를 대상으로 이메일 · 휴대전화를 해킹하는 동시에 '레드알파', '레

드호텔', '포이즌 카프' 등과 같은 별도의 해킹조직과 악성코드 프로그램 · 데이터를 공유하며 직간접적으로 해킹에 관여해 왔다. 중국 정부는 아이순을 통해 중앙아시아, 동남아시아, 홍콩, 대만의 네트워크를 해킹하여 반체제인사를 통제하고 소수민족을 탄압하고자 했는데, 이러한 중국 당국의 목표를 위해 아이순은 전 세계 약 20개국의 공공 · 민간 단체를 해킹하여 티베트 망명정부 인사, 위구르 이민자 사회, 홍콩 민주화 인사 등 중국 본토를 위협하는 위협요인으로 간주되는 세력에 대한 집중 공격을 시도해왔다.

중국의 군민 융합 전략의 또 다른 위협적 측면은 전 세계에서 유전자 데이터를 지속적으로 수집함으로써 전개되고 있다. COVID-19 팬데믹 당시 외국에 의료 지원을 제공한다는 명목하에 확대된 접근 권한을 악용하여 중국은 인간 DNA 데이터베이스 확장을 시도하고 있다. 중국은 유전자 관련 지원이 필요한 국가에 유전자 염기서열 분석 장비를 제공하고 유전자 연구를 위한 파트너십을 구축하는 형태로 파트너십 국가의 유전자 데이터를 수집해 오고 있다. 유전자 염기서열 분석 장비를 생산하는 중국 기업인 파이어랩스의 소유주는 중국 군사기업인 BGI로, BGI는 전 세계에 판매하는 산전 검사 키트로 유전자 데이터를 수집하기도 했다. 미국은 BGI 자회사들이 중국 정부의 유전자 데이터 분석을 도와 소수민족과 종교적 소수자를 탄압하는데 앞장섰다며 이들 기업을 블랙리스트에 등재하고, 2023년 3월 미 상무부는 '중국의 군사 프로그램에 전용될 위험'을 근거로 미국 기업이 BGI 자회사 두 곳과 거래하는 것을 금지한 바 있다.[35] 이러한 데이터 보안과 관련한 군 · 민 융합 전략은 시진핑 주석이 2049년까지 중국인민해방군을 세계 초일류 군대로 만들기 위해 추진 중인 계획의 일환으로 전개되고 있으며, 반체제인사에 대한 데이터 해킹은 중국의 군민 융합 전략의 정치적 활용 의도를 드러낸다고 할 수 있다.

## 2. 데이터의 안정성 · 무결성 지향

데이터의 훼손, 악용, 조작 등은 국가안보의 사안으로 부상하고 있으며, 특히 적대국가나 경쟁국으로의 데이터 유출 및 개인정보의 국외 이전을 통한 전략적 자원의 손실 및 국가안보의 위협을 초래할 수 있는 것으로 인식되고 있다. 특히, 미국과 EU는 자국의 데이터 관련 경쟁력 수준 및 관리 체계 등을 보다 강화하고 있으며 나아가 초국가 차원의 데이터 안보를 위한 통상 규범 도입 과정에도 이 같은 인식을 반영 중이다(이효영, 2024: 1).

35) Indo-Pacific Defense FORUM(2024), "중국의 감시 및 DNA 수집 회사, 시진핑 군 · 민 융합 전략의 위험성 부각" https://ipdefenseforum.com/ko/2024/03/%EC%A4%91%EA%B5%AD%EC%9D%98-%EA%B0%90%EC%8B%9C-%EB%B0%8F-dna-%EC%88%98%EC%A7%91-%ED%9A%8C%EC%82%AC-%EC%8B%9C%EC%A7%84%ED%95%91-%EA%B5%B0%C2%B7%EB%AF%BC-%EC%9C%B5%ED%95%A9-%EC%A0%84%EB%9E%B5%EC%9D%98/ (검색일: 2024. 8. 13.).

미국의 사례를 보면, 바이든 행정부는 2024년 2월 28일 미국 데이터가 특정 국가로 거래되는 것을 제한하는 것을 골자로 하는 '우려국가에 의한 민감한 대량의 미국인 데이터 및 미국 정부 관련 데이터의 접근 금지(Preventing Access to Americans' Bulk Sensitive Data and United States Government-Related Data by Countries of Concern)'에 관한 행정명령(EO 14117)을 발표했다(U.S. White House, 2024). 이는 데이터 우려국가로부터 미국인의 개인 민감 데이터 및 미국 정부 관련 데이터 보호를 위한 행정명령으로, '우려국가'와의 데이터 거래를 통한 간첩 활동, 영향공작, 사이버 작전 및 기타 전략적 우위 행사 등 국가안보 우려에 대응하고 미국의 데이터 안보를 강화하기 위한 강력한 조치를 내포하고 있다(이효영, 2024: 7). 동 행정명령에 따라 각 부처는 데이터 거래 제한 및 금지 규정을 발표하고, 데이터 보호를 위한 메커니즘 구축에 나서고 있는 것이다.

〈그림 5〉 우려국가로부터 데이터 보호를 위한 행정명령(EO 14117)의 주요 내용

| 추진기관 | 추진내용 |
|---|---|
| 법무부 / 국토안보부 | ① 데이터 거래 제한 및 금지 규정 발표<br>② 데이터 보호 규정 발표 |
| 보건복지부 / 국방보훈처 | ③ 의료 시장·서비스의 민감 데이터 이전 관련 조치 시행 |
| 소비자보호금융국 | ④ 데이터 중개산업의 데이터 수집, 유포 관련 조치 시행 |
| 통신·서비스 부문 외국인참여평가위원회 | ⑤ 우려국가 연결 통신서비스 해저케이블 구축 허가 검토 |
| 국가정보국 등 기타 관련 부처 | ⑥ 데이터 이전으로 발생하는 국가안보 위험 평가<br>+ 인간 오믹(Omic) 데이터와 관련된 위험 평가 |

출처: 오정미(2024)

나아가, 미국 법무부는 미국인의 데이터가 '우려국가'로 대량 이전 및 유출되는 것을 방지할 수 있도록 권한을 부여하고 있다. 이에 따라 '데이터의 중개 거래', '대량의 인간 게놈 데이터 또는 인간 게놈 데이터를 추출할 수 있는 인간 생체 표본의 전송과 관련된 거래' 등 고도로 민감한 데이터의 거래를 전면 금지하는 추세이다. 또한, 그 외 데이터에 대해서도 우려국가의 접근을 차단하기 위해 별도의  보안 요건 준수를 조건으로 제한적인 거래를 허용하고 있다. 미 법무부는 '규칙제안 사전예고(Advanced Notice of Proposed Rulemaking, ANPRM)'을 통해 중국(홍콩, 마카오 포함), 북한, 러시아,쿠바, 이란, 베네수엘라 등을 '우려국가'로 지정했는데, 이를 통해 '우려국가'의 접근이 어려운 데이터 확보를 통한 기술 발전 노력을 지연시키고, '우려국가'에 의한 빅데이터 입수를 통한 영향력 공작 및 첩보 활동을 무력화시켜 여론과 정보조작 행위를 견제하려는 전략적 목표를 가지고 있는 것으로 평가할 수 있다(이효영, 2024: 15). 이러한 미국의 데이터 안보에 대한 접근방식은 신뢰할 수 있는 국가와는 '데이터의 자유로운 국경 간 이전'이라는 근본적인 대원칙을 준수하되, 안보적 우려가 있는 국가에 대해서는 데이터의 이동과 유출을

제한하는 '분절화'된 접근방식을 취하고 있다고 볼 수 있다.

EU의 경우, '데이터 거버넌스 법안(Data Governance Act)'을 기반을 토대로 역내 데이터 단일시장을 형성하였는데, 이 안에서 데이터의 안정성 확보와 데이터 공유를 활성화하는 접근을 펼치고 있다. 데이터에 대한 '공정한 접근(fair access)' 및 '사용자의 권리(user rights)'를 강조하는 데이터 법안은 사물인터넷(IoT) 기기에서 생성되는 산업 데이터(industrial data)에 대한 기존 데이터 시장의 약자(개인, 중소기업 등)의 접근성을 강화해 데이터 공유를 활성화하는 것이 목적이며, 데이터 공유의 안정성과 합법성을 확보하기 위한 보안규정을 활용하고 있다(이효영, 2024: 15). 특히, 데이터법은 커넥티드 제품을 통해 그 구성 요소와 관련된 서비스 제공 과정에서 수집한 개인정보 및 비개인정보를 모두 포괄하며 사용자 인터페이스 및 기기 자체에서 생성된 원시 데이터 역시 적용 대상에 포함한다(한국인터넷진흥원, 2024: 5).

더 나아가 지난 2024년 3월 유럽 의회는 AI 규제법(EU AI Act)을 통과시킨 바 있다. EU의 AI 규제안은 AI의 위험을 차등화하고 적극적인 관리를 실천하기 위한 최초의 인공지능 규제법안으로 인식되지만, 동시에 AI 성능에 핵심이 되는 데이터의 생산과 활용, 폐기에 이르는 전주기 과정에 대한 책임성을 기업에 부여한 데이터 위험을 관리하는 규제 법안으로서 의미가 있다. 이를 통해 의도적인 데이터 오염 등 데이터 무결성 훼손이 야기하는 AI 활용의 부작용, 대표적으로 사회집단을 점수화한 차별(social scoring), 생체정보의 악용 등에 대응하고자 한 것이다.[36] 나아가 이러한 규제를 통해 EU는 AI 시스템이 인간의 안전, 보안, 기본권을 침해하는지를 추적 · 관찰 · 수정할 수 있는 생태계를 마련하여 AI를 활용하는 과정에서 생성되는 데이터의 안정성과 무결성을 확보하려 하고 있다. 또한, 다수의 개인으로 하여금 개인정보 악용의 두려움을 완화시켜주는 효과 또한 기대하고 있다(강진원 · 김혜나, 2024, 2),

## 3. 무인화 · 지능화된 사이버 영향력 공작에 대비

최근의 광범위한 데이터 안전 확보를 위한 노력들은 이제 전통적 조직 뿐만 아니라 비인간 행위자에 대한 취약성 대비에까지 이르고 있다. 데이터 조작이나 오염과 같이 AI의 학습 훈련 과정이 안고 있는 편향성이나 환각 가능성을 파고들고 잘못된 정보를 유출 · 주입 시킴으로써 오작동 등의 문제를 유발하는 방식인 것이다. 최근 생성형 AI의 등장으로 AI 활용의 진입장벽이 대폭 낮아진 상황에서 AI에 필요한 데이터의 정확성과 신뢰성 훼손을 무기로 이

36) 구체적인 활용에 대한 위험에 대응하는 것을 목표로 위험을 4가지 단계–허용할 수 없는 위험(unacceptable risk), 고위험(high risk), 저위험(low risk), 최소한의 위험(minimal risk)–로 범주화하고 위험 수준에 따라 차등적으로 규제하고 있다. 윤정현 · 조은정, "EU AI Act 통과의 의미와 시사점", 『ISSUE BRIEF』, (2024. 3. 25.), 제527호, p. 2.

같은 악의적 시도가 발생할 경우, 사회적 파급력은 전방위적으로 확대될 수 있다. 이미 미국은 2016년 대선을 시작으로 러시아와 이란 등 권위주의 국가로부터 생성형 AI 알고리즘을 활용한 '컴퓨터 프로파간다(Computational Propaganda)'를 겪어왔다. 생성형 AI 알고리즘의 내러티브 구사 능력을 지닌 챗봇과 봇 부대(bot army)와 같은 대규모 정보 확산 알고리즘 프로그램은 여론을 교란하고 사회갈등을 증폭시키며 민주주의와 정부의 '정치적 정당성(political legitimacy)'을 훼손하는 전복적 행위로 이어질 수 있다.

이에 따라 최근 미국은 이러한 허위조작정보 유포 행위를 사이버 테러이자 주권을 위협하는 개입으로 간주하고 군사적 차원에서 대응하고 있다(송태은, 2023b: 2). 미국이 AI 알고리즘을 활용한 영향공작을 심각한 주권 침해 행위로 인식하는 이유는 AI 챗봇에 대한 적대적 공격 혹은 의도적으로 오염된 데이터를 학습시킴으로써 허위조작정보를 생성할 수 있고, 민감한 개인정보를 쉽게 유출할 수 있으며 프로파일링(Profiling)을 통해 AI 챗봇 서비스 제공업체가 저장하고 있는 데이터를 해킹하기에도 수월하기 때문이다. 미국은 정보의 자유로운 초국경적인 이동 원칙을 지지하는 대표적인 국가이지만, 특히 선거 국면에서 이러한 AI 알고리즘과 데이터를 활용한 사이버 영향공작에 적극적으로 대응 중이다. 사이버사령부(U.S. Cyber Command)와 국가안보국(National Security Agency)을 중심으로 '합동선거안보그룹 Joint US CYBER COM–NSA Election Security Group(ESG)'을 설치했으며 FBI, 국토부, 국방부 역시 ESG와 공조한 바 있다. 또한, 2019년 미 의회는 '미국의 국익을 수호하기 위해 타국의 허위조작정보 공격에 반격하는 미군의 심리작전 수행을 용인하는 법안인 〈Section 1631〉을 통과시킨 바 있다. 그리고 이를 근거로 미군은 최근 러시아–우크라이나 전쟁에서 X(구 트위터), 페이스북과 같은 소셜 미디어에서 봇 계정을 활용하여 해외 정보전 및 심리전을 전개하기도 하였다. 국방부 주관으로 실시되는 대표적인 사이버 방어훈련인 '사이버쉴드 훈련(Cyber Shield Excercise)'은 2020년부터 사이버 공간에서 허위조작정보가 유포되는 상황을 가정한 정보작전 훈련의 일환으로 수행되고 있다(송태은, 2023b: 27–28).

반면, 중국의 경우, 데이터 기반 사이버 영향공작 차단을 자국민을 대상으로 하는 정보 검열 및 감시 정책인 금순공정(金盾工程, Golden shield project)의 일환인 '만리방화벽'과 '인터넷 정보 서비스 알고리즘 추천 관리 규정' 등을 통해 추진하고 있다. 2022년 3월 제정된 '인터넷 정보 서비스 알고리즘 추천 관리 규정'은 세계 최초의 알고리즘 규제로서 알고리즘이 사회와 국가의 안전은 물론 개인의 권익을 침해할 수 있기에 적극적으로 규제해야 한다는 인식하에 제정되었다. 중요한 점은 본 규제를 통해 중국 정부가 텐센트, 알리바바, 바이트댄스 등 중국에 모체를 두고 있는 글로벌 플랫폼 기업들의 알고리즘을 확보할 수 있게 되었다는 점이다. 이를 통해 중국은 알고리즘을 활용한 콘텐츠의 선별적 노출, 특정 이슈 차단이 가능해짐에 따라 내부에서의 민주화 요구 및 체제에 대한 불만을 억제하고 서구의 반

중국 영향공작을 효과적으로 차단할 수 있게 되었다(이중희, 2023).

또한, 기술적 차원에서 적극적인 해외 투자 및 합병을 통해 데이터, 데이터 분석 기술을 비롯하여 디지털 플랫폼 개발에 필요한 역량을 획득하고 있으며, 해외 데이터 · 플랫폼 기업의 인수합병을 활용 기반을 증대시키고 있다. 일례로 중국 정부의 전폭적인 지원을 받고 있는 BGI 그룹은 2012년 미국에 본사를 둔 컴플리트 제노믹스(Complete Genomics)를 인수하여 DNA 염기서열 분석 역량을 획득하였으며, 2015년에는 중국 컨소시엄이 세계에서 세 번째로 큰 이미지 센서 공급업체인 옴니비전(OmniVision)을 인수한 것으로 전해졌다(Emily et al., 2022: 56). 그러나 이 같은 중국의 움직임은 대항작용을 낳았는데, 바이트댄스가 2017년에 뮤지컬리(Musical.ly)를 인수한 이후 틱톡(TikTok)이 미국 내에서 선풍적인 인기를 얻게 되자 미 상원이 틱톡 앱이 중국 공산당의 개입을 받고 있으며 미국인 사용자의 개인 데이터는 물론 정부 중요 데이터가 유출될 수 있다고 발표한 사례가 그것이다. 이후 미 의회는 정부 부처와 계약을 맺고 있는 회사가 사용하는 모든 디지털 기기에서의 틱톡 사용을 금지했으며, '외국인투자위험심사현대화법(FIRRMA: Foreign Investment Risk Review Modernization Act of 2018)'을 제정하기에 이르렀다. 가장 최근인 2024년 4월에는 '21세기 힘을 통한 평화(21st Century Peace through Strength Act)'라는 법안으로 틱톡 강제 매각을 법제화했다. 이처럼 미국 기업에 대한 중국의 인수 합병 증가는 반작용을 낳았다. 또한, 핵심기술 · 핵심 인프라 · 민감한 개인정보 · 데이터와 관련된 분야에 대한 국가안보적 고려에 따른 투자 규제로 이어졌다.

유럽의 경우, 최근 데이터를 악용한 국가나 비정부 집단, 개인의 허위조작정보 유포(state-sponsored disinformation campaign) 활동을 차단하기 위한 조치들을 취하고 있다. 일례로 2023년 2월 EU 대외관계청(European External Action Service, EEAS)은 산하에 '정보공유분석센터(Information Sharing and Analysis Center, ISACs)'를 설치했는데, 이를 통해 EU 역내의 사이버안보 기관과 민간단체가 함께 러시아, 중국 등 권위주의 국가 배후의 적대적 허위조작정보 유포에 대응하는 역할을 수행하고 있다. 나아가 '지난 2021년 제정된 디지털 서비스법(Digital Service Act, DSA)'과 '디지털 시장법(Digital Markets Act, DMA)'을 활용하여 인터넷 서비스 사업자(ISP) 및 소셜 미디어 플랫폼, 앱, 콘텐츠 제공 사업자들이 정보의 문지기(gatekeeper)로서 자기규제를 실시하도록 유도함으로써 데이터 조작으로 형성된 허위조작정보, 불법 콘텐츠 확대에 대처하고 있다(송태은, 2023c: 4). 이 같은 일련의 대응들은 주요국들이 무인화 · 지능화되고 있는 영향공작에 적극적으로 대응하기 위해 AI 알고리즘 뿐만 아니라 데이터 자체의 안전한 관리에 초점을 두고 있음을 보여준다.

# Ⅴ. 결론

살펴본 바와 같이 데이터가 사이버 안보 이슈의 핵심으로 부상한 고도화된 디지털 사회에서는 데이터 자체의 안정성과 무결성을 훼손하고자 하는 사이버 공격의 방식 또한 진화하고 있다. 이에 각국은 데이터의 중요성을 인식함은 물론, 이를 전략 자산의 관점에서 접근하고 있다. 그 결과 데이터가 함의하고 있는 경제, 사회, 안보 차원의 가치는 활용과 보호라는 국내적 차원의 의미를 넘어 그것이 야기하는 국제정치적 쟁점을 살펴볼 필요성을 제기한다. 특히, 미중 전략 경쟁 시대의 데이터 이슈는 주권과 안보의 문제로 발전하고 있으며 미 · 중을 중심으로 데이터 패권을 위한 세계 각국의 경쟁을 유발하는 중이다. 잠재적 가치를 지닌 데이터의 유출, 조작, 오염 그리고 영향공작 등 위험 요인이 보다 선명해지고 있다. 이 같은 상황에서 한국의 데이터 안보 환경이 갖는 취약성과 이를 개선하기 위한 대응 방향의 수립 역시 시급하다 볼 수 있다. 고도화되고 있는 사이버 공격 유형과 그것이 초래하는 데이터 안보 문제의 심각성을 고려하여 우리는 다음과 같은 전략과 세부 실천 방안을 모색할 필요가 있다.

우선, 거시적인 전략적 방향 수립 측면에서 사이버 공격의 진화가 보여주는 표적 대상에 대한 전환이 요구된다. 인프라/네트워크/SW 뿐만 아니라 비정형/다중의 개인정보데이터에 대한 보호를 강화해야 하는 것이다. 둘째, 대응 주체로서 민간/다중 이해관계자를 포함한 다층적 거버넌스로의 전환이 필요하다. 대량의 정보를 생산·유통하는 플랫폼 기업 뿐만 아니라 일상의 방대한 데이터를 제공·축적하는 다중의 데이터와 개인정보 역시 향후 데이터 변질화를 노린 사이버 공격의 표적이 될 수 있기 때문이다. 셋째, 향후의 데이터 안보화 메커니즘을 고려한 복합적 경쟁구도에 대비해야 한다. 최근 공급망 재편 따라 제기된 인태지역의 IPEF 디지털 경제 분야 필라에서도 데이터의 투명성과 자유로운 이동이 명시된 바 있다. 동시에 복합지정학 국면에서의 AI, 바이오 등 첨예한 이중용도 전략기술을 고도화하는 자원으로서 데이터의 군사안보적 중요성 또한 증대되고 있다. 즉, 데이터의 통제와 이전, 공유에 대한 사안은 미중 전략경쟁 구도에서의 동맹과 연대 외교를 위한 주요 품목으로 자리하게 될 것이며 안보화 담론을 구성하는 핵심 요소로 작용할 것이다. 우리로서는 국가적 차원에서 데이터 생태계 조성 전략을 수립함과 동시에 외교안보 관점에서 관리할 수 있는 병행적 접근이 필요하다. 이 같은 거시적인 데이터 안보 전략을 추진하기 위해서는 다음과 같은 세부적인 실천 과제를 마련할 필요가 있다.

첫째, 데이터가 지니고 있는 활용과 보호라는 이중적 속성을 균형있게 고려한 제도적 기반이 필요하다. 특히 국가 사이버안보 전략과의 연계성을 고려한 상위의 데이터 안보전략이 필요하다. '(가칭)데이터 안보 기본법'의 제정이 하나의 대안이 될 수 있다. 2020년 소위 '데

이터 3법'[37]이 통과되었지만 데이터 기반의 신산업 육성에 초점을 두었을 뿐 국가의 전략 자산으로 다루어지고 있는 데이터 보호의 중요성과 각국의 경쟁을 반영하지 못한 한계가 있었다. 따라서 초연결 사회와 AI 시대의 핵심 자원인 데이터를 경제 활성화와 국내 기업 육성을 고려하면서 국가안보 차원에서 어떻게 체계적으로 관리하고 보호할 것인가 등에 대한 데이터 안보 기본법으로 제도화해야 한다. 사이버안보와 밀접한 관계가 있는 만큼, 계류 중인 '국가 사이버안보 법안'은 데이터 안보를 포함하여 제정될 필요가 있다.

둘째, 데이터 안보 환경의 변화와 기술 발전 속도를 고려하여 사이버안보 체계 또한 보다 강화될 필요가 있다. 네트워크의 연결성과 클라우드 서비스의 확대와 함께 해킹기술의 은밀성과 생존성이 강화되는 사이버 환경의 변화로 기존의 경계선 보안만으로는 사이버공격을 차단하기 어려운 상황이 되었다. 또한 가짜 피싱 메일 생성, 악성코드 작성 등 통해 AI의 학습 데이터를 오염시켜 편향성과 환각을 일으키거나 오작동을 유발할 가능성도 증대되고 있다. 이러한 변화에 대응하여 '제로트러스트(Zero Trust)' 정책과 최소 권한 부여 및 멀티팩터 인증(Multi-Factor Authentication), 공급망 보안을 위한 SBOM(Software Bill Of Materials) 도입 등 변화된 환경에 부합하는 강화된 보안 정책과 기술 채택이 요구된다. 또한 사이버공격을 완벽하게 차단할 수 없는 만큼 선제적으로 사이버공격을 탐지하여 예방하는 한편, 피해를 최소화하고 신속하게 복구할 수 있는 회복력을 강화하는 방향으로 나아가야 한다. 기존 암호체계를 무력화하는 양자컴퓨팅 기술의 개발에 대응하기 위한 양자내성 암호 및 양자통신 실용기술 개발 등 차세대 사이버 안보 기반을 구축해야 한다.

셋째, 진화된 사이버 공격과 영향공작에 대비하기 위한 국제공조와 소통이 필요하다. 데이터 이동과 통제 문제는 미 · 중간의 패권 경쟁의 핵심 요소가 되고 있으며, 국가 간 안보와 이익이 첨예하게 엇갈리는 사안으로 전환되었다. 이러한 상황에서 데이터 안보는 일국 수준에서 추구하기 어려운 문제이며, 신뢰할 수 있는 우방국을 중심으로 국제적 연대와 공조 필요성이 제기된다. 한국은 지난 2019년 9월 유엔총회 내 '정보와 민주주의 파트너십(International Partnership for Information and Democracy)'에 동아시아 국가 최초로 서명-민주주의와 언론의 자유 증진 및 디지털 정보와 데이터의 자유로운 이동, 규범 형성을 위한 국제협력에 적극 동참해왔다. 러시아-우크라이나 전쟁 사례를 적용하여 미-일-NATO 간의 사이버안보 공조 연대-공동의 영향공작 대응 시나리오 훈련의 촉진, 위협대응 모델 개발 등을 추진할 필요가 있다. 나아가 국제 규범 논의에서 우리와 비슷한 고민을 안고 있는 유사 국가들과의 양자 및 소다자 협력을 통해 안보적 · 경제적 목표를 관철시키기 위해 노력해야 한다. 또한, 공공 부문에 비해 민간 부문에서의 데이터 유통과 사이버 위협이 훨씬 큰 상황에서 민간 부문의 사이버 공격 정보와 대응 방안을 상호 공유하며 유기적인 파트너십을 공

37) 개인정보보호법, 신용정보법 이용 및 보호에 관한 법률, 정보통신망 이용촉진 및 정보보호 등에 관한 법률

고히 하는 일은 결국 국가 차원의 사이버 안보 역량과 데이터 안보를 강화하는 시작점이 될 것이다.

## 〈참고문헌〉

국가법령정보센터. 2023. “신용정보의이용및보호에관한법률” (시행일: 2023. 9. 15.).

김상배. 2015. “사이버 안보의 미중관계: 안보화 이론의 시각”, 『한국정치학회보』, 제49집 1호, (2015), pp. 71–97.

. 2018. “초국적 데이터 유통과 정부주권: 국가주권 변환의 프레임 경쟁”, 이승주 편. 『사이버 공간의 국제정치경제』, 서울: 사회평론, pp. 17–51.

. 2020. “데이터 안보와 디지털 패권경쟁: 신흥안보와 복합지정학의 시각”, 『국가전략』, 제46권 2호, pp. 5–34.

김석준. 2019. 『문과생을 위한 ICT 이야기』, 서울: 커뮤니케이션즈북스

김현철. 2019. 『정보적 사고에서 인공 지능까지』, 서울: 한빛아카데미.

김일기. 2023. “북한의 영향력 공작과 우리의 대응 방향” 『이슈브리프』, 497호. 국가안보전략연구원.

김소정. 2024. “국가 사이버안보 전략 개정의 특징과 시사점”, 『이슈브리프 512호』, 국가안보전략연구원.

강진원, 김혜나. 2024. “EU 인공지능 규제 현황과 시사점”, 『KISTEP 브리프 119』, 한국과학기술기획평가원.

과학기술정보통신부. 2023. “우리 정보보호산업의 경쟁력 강화를 위한 ’튼튼한 사이버 안보‘ 실현”, (2023.9.5.)

. 2023. “디지털서비스 상시 위기관리 강화를 통해 신뢰할 수 있는 디지털 기반 구축”, (2023.3.30.)

개인정보보호위원회. 2023. “신뢰 기반 인공지능 데이터 규범, 첫 발 떼다”, (2023.8.2.)

경향신문, 2024. “국정원 ‘작년 공공기관 해킹 시도 80%가 북한 소행”, (2024.1.24.) https://www.khan.co.kr/politics/north-korea/article/202401242055005 (검색일: 2024. 8. 18)

디지털투데이, “국가사이버안보기본법 재추진,,,직속 연구기관도 설립”, (2024.3.6.) https://www.digitaltoday.co.kr/news/articleView.html?idxno=508091 (검색일: 2024. 8. 18)

보안뉴스. 2010. “트위터 XSS 공격 받아...“헉! 포르노 사이트로 연결” (2010. 9. 22.). https://www.boannews.com/media/view.asp?idx=22941&kind=1 (검색일: 2024. 1. 2.).

. 2012. “와이파이 스니핑, 통신비밀보호법 위반인가?” (2012. 11. 22.),

https://www.boannews.com/media/view.asp?idx=33794&kind=3 (검색일: 2024. 1. 9.).

. 2017. “러시아의 전직 ‘트롤’, 가짜뉴스에 대해 밝히다” (2017. 11. 20.). https://m.boannews.com/html/detail.html?idx=58122&kind=3 (검색일: 2024. 1. 6.).

변상정, 윤정현. 2024. “북한의 사이버 영향공작 진화와 시사점”, 『이슈브리프 549호』, 국가안보전략연구원.

송태은. 2023a. “허위조작정보를 이용한 사이버 영향공작과 국가안보: 실태와 대응책”, 『정책연구시리즈 2023-13』, 국립외교원 외교안보연구소.

. 2023b. “AI 알고리즘의 내러티브 구사능력과 허위조작 정보의 유포 문제: 민주주의 국가의 대응” (2023. 5. 22.), 『IFANS FOCUS』, 국립외교원 외교안보연구소.

. 2023c. “중국의 사이버 영향력 공작과 대응방안”, 『제6차 KACS 국가전략포럼 자료집』, (2023. 12. 7.).

이효영. 2024. “데이터 안보와 국제통상: 현안과 시사점” 『주요국제문제분석』, 국립외교원 외교안보연구소

윤민우. 2023. “기존 국가보안법 등으로는 중국의 영향력 공작 등 대처 못 해” 『월간조선』. (2023년 9월호), https://monthly.chosun.com/client/news/viw.asp?nNewsNumb=202309100042 (검색일: 2024. 1. 13.).

윤정현. 2021. “국방분야 인공지능 기술 도입의 주요 쟁점과 활용 제고 방안”, 『STEPI Insight』, Vol. 279.

윤정현·홍건식. 2022. “디지털 전환기의 국가전략기술과 기술주권 강화방안”, 『INSS 연구보고서 2022-16』, 서울: 국가안보전략연구원.

이데일리. 2023. “짙어지는 'AI해킹' 위협…2024년 범죄 AI 활개", (2023. 12. 5.), https://www.edaily.co.kr/news/read?newsId=03011046635835568&mediaCodeNo=0 (검색일: 2024. 1. 18.).

이상우. 2023. “중국의 데이터 안보와 딥페이크 · 알고리즘 규제의 시사점”, 『이슈&트렌드』, (2023. 2. 20.), 대외경제정책연구원.

이승주. 2022. “미중 디지털 경쟁과 산업정책의 지정학” 『국제문제연구소 이슈브리핑』, No.153. (발간일: 2022.2.14.).

이형동·윤준희·이덕규·신용태. 2022. “러시아-우크라이나 전쟁에서의 사이버공격 사례 분석을 통한 한국의 대응 방안에 관한 연구”, 『정보처리학회논문지. 컴퓨터 및 통신시스템』,

제11권 제10호, pp. 353-362.

이중희. 2023. “중국 빅테크의 알고리즘에 대한 규제의 배경과 의미”, 『전문가 오피니언』, CSF 중국전문가포럼 (검색일: 2024. 8. 15)

https://csf.kiep.go.kr/issueInfoView.es?article_id=49303&mid=a20200000000&board_id=4

임현철. 2024. “EU 인공지능법 최종 확정: 2021년 초안과 무엇이 달라졌나”, 『KIPA 규제동향』, 한국행정연구원.

오정미. 2024. “미국, 외국 적국으로부터 데이터 보호 위한 행정명령 발표”, 『수출통제 Issue Report 2024-16』, 전략물자관리원.

윤정현 · 조은정, 2024. “EU AI Act 통과의 의미와 시사점”, 『ISSUE BRIEF』, (2024. 3. 25.), 제527호.

정용찬·김성옥·고동환. 2021. “미 · 중 데이터 패권 경쟁과 대응전략”, 『KISDI Premium Report』, 제21권 제09호, 정보통신정책연구원.

최계영. 2023. “인공지능과 선거 개입” 『KISDI 전문가칼럼』, (2023. 12. 21.). 정보통신정책연구원.

https://www.kisdi.re.kr/bbs/view.do?bbsSn=114317&key=m2101113043145 (검색일: 2024. 1. 23.).

천곤웅, 김성훈. 2024. “미국 Cybersecurity 전략 및 실행계획 분석과 시사점”, 『KISA INSIGHT Vol.01』,

한국인터넷진흥원. 2024. “개인정보보호 월간동향분석 1월호”.

한국데이터산업진흥원. 2024. “DATA ECONOMY:global news trends in EU, US”.

Bruyère, Emily. Strub, Doug and Marek, Jonathon ed. 2022. “중국의 디지털 야망 : 자유 질서를 대체하는 글로벌 전략”, 『NBR 특별 보고서 #97』, The National Bureau of Asian Research, P. 56. https://www.nbr.org/wp-content/uploads/pdfs/publications/sr97_chinas_digital_ambitions_mar2022_korean.pdf (검색일: 2024. 8. 18)

CCTV NEWS. 2021. “콜로니얼 파이프라인, 랜섬웨어 공격으로 5800여 명 개인정보 유출” (2021. 8. 18.). https://www.cctvnews.co.kr/news/articleView.html?idxno=229908 (검색일: 2024. 1. 7.).

Cyberone. 2024. “[해외동향] 미국 최대 송유관 업체(콜로니얼 파이프라인), DarkSide 랜섬웨어 공격 받아”, (2021. 5. 13.), https://www.cyberone.kr/news-trends-detail?id=73372&page=1 (검색일: 2024. 1. 20.).

Hansen, Lene and Helen Nissenbaum. 2009. “Digital Disaster, Cyber Security, and the Copenhagen School,” International Studies Quarterly, 53(4), pp. 1155–1175.

Indo-Pacific Defense FORUM. 2024. “중국의 감시 및 DNA 수집 회사. 시진핑 군·민 융합 전략의 위험성 부각”

KISEC. 2020. “AI를 활용한 공격은 무엇이 있을까?” (2020. 8. 20.).
https://www.kisec.com/rsrh_rpt_det.do?id=221 (검색일: 2024. 1. 11.).

Liu, Jinhe, 2019. “China’s Data Localization.” Chinese Journal of Communication. (20 Aug 2019), pp. 84–103.

LG CNS. 2020. “머신러닝 보안 취약점! 적대적 공격의 4가지 유형” (2020. 2. 13.).
https://www.lgcns.com/blog/cns-tech/ai-data/9616/ (검색일: 2024. 1. 16.),

MBA Knowledge Base. 2024. “Bitcoin Trading Strategies for Bear Markets” (January 8, 2024). https://www.mbaknol.com/information-systems-management/data – tampering-meaning-types-and-countermeasures/ (검색일: 2024. 1. 26.).

NordVPN. 2022. “워너크라이는 어떤 원리로 작동하며, 아직도 위협적인가요?” (2022. 3. 1.).
https://nordvpn.com/ko/blog/wannacry-ransomware-attack/ (검색일: 2024. 1. 1.)
. 2022. “스턱스넷이란 무엇인가? - 핵이 된 디지털 웜”, (2023. 2. 17.).
https://nordvpn.com/ko/blog/stuxnet/ (검색일: 2024. 1. 24.).

Protocol. 2024. “A 'nightmare scenario': Data-tampering attacks are hard to detect, with devastating consequences”, (August 22, 2022). https://www.protocol.com/ enterprise /data-integrity-security-cyberattacks-threat (검색일: 2024. 1. 8.).

U.S. White House. 2024. “Executive Order on Preventing Access to American’s Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern”, February 28, 2024.

Reinse, David., John Gantz and John Rydning. 2018. The Digitization of the World From Edge to Core. Segate and IDC.

Smart, J.M., Cascio, J. and Paffendorf, J. 2010. “Metaverse Roadmap Overview, 2007”. Accelerated Studies Foundation. Retrieved.

Tech Recipe. 2024. “이란 핵시설 파괴 작전…네덜란드 스파이가 실행했다?” (2024. 1.

17.)

https://techrecipe.co.kr/posts/61913 (검색일: 2024. 1. 25.)

https://blog.naver.com/gowit_sps/221566173768 (검색일: 2024. 1. 23.).

https://www.cloudflare.com/ko-kr/learning/security/what-is-a-data-breach/

(검색어: 2024. 1. 26.).

https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal

(검색일: 2024. 1. 25.).