국가전략연구위원회 이슈브리핑 19호 (발간일: 2024.2.10.)

사이버 안보와 데이터 안보[1)]

윤정현 (국가안보전략연구원)

Ⅰ. 들어가며

최근 디지털 전환 및 인공지능(AI) 활용의 고도화에 따라 데이터의 중요성은 더욱 높아지고 있다. 흔히 반도체는 '산업의 쌀', 데이터는 '21세기의 원유'로 비유될 만큼 데이터는 4차 산업혁명 시대의 필수 불가결한 자원이 되었다. 인류가 생산하는 글로벌 데이터의 규모 역시 2018년 33 ZB(330억 GB)에서 2025년도에는 175 ZB(1750억 GB) 이상으로 급격히 증가할 것으로 예상된다(Reinsel et al, 2018). 여기에는 서버간 접속 과정에서 일시적으로 생성되는 세션 데이터 뿐만 아니라 프라이버시 데이터에서국가 기밀에 이르기까지 다양한 정보가 포함된다.

이처럼 데이터가 경제·안보적으로 중요한 가치를 내재한 자원으로 인식되면서, 사이버 공간 속 데이터의 확보와 통제·활용에 대한 문제를 안보화의 메커니즘에서 조명하는 연구들도 나타나고 있다. 지금까지 사이버 보안은 현실과 밀접한 가상공간에서 정보를 보호하고 안정적인 생성과 유통, 서비스를 보장하는 환경을 구현하는데 초점을 맞춰왔다. 그러나, 최근 제기되는 사이버 안보의 쟁점들을 살펴보면 2000년~2010년대와 구별되는 경향들이 포착된다. 바로 데이터가 사이버 공간의 질서와 경쟁, 안보적 이해관계를 결정하는 주요 변수로 부상하고 있는 것이다. 여기에서 주목할 부분은 데이터의 중요성이 증대되면서 사이버 공격 양상 역시 변하고 있다는 점이다. 국가나 국가 배후의 악의적 공격집단들, 심지어 개인 수준에서 국가 기밀이나 기업의 지적 재산 확보 까지 다양한 목적을 실행하는 도구로서 데

1) 이 글은 2024년 2월 6일 제7차 사이버 국가전략 포럼에서 발표된 발표문을 수정보완한 것이다.

이터를 노린 공격을 시도하고 있다. 이 같은 변화는 이제 안보적 관점에서의 데이터를 바라보고, 사이버 공격이 어떠한 형태와 유형으로 데이터를 노릴 것인가에 대비해야 하는 숙제를 던져준다고 할 수 있다.

Ⅱ. 데이터 안보 이슈를 부상시키는 최근 사이버 공격 유형들

1. 고도화된 데이터 유출 공격 유형

이른바 데이터 안보 시대에 주목해야할 첫 번째 사이버 공격 양상의 유형은 해킹을 통한 데이터 유출이라 할 수 있다. 데이터 유출은 데이터의 소유주나 관리자가 의도하지 않게 보호되지 않는 환경으로 빠져나가는 것을 의미한다. 이는 공격자의 입장에서는 데이터 탈취라 볼 수 있다.[2] 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 유출의 대표적인 사례는 '피싱(Phishing)'이다. 피싱은 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 수법이며, 전통적으로 초기 침투 공격(Initial Access)에 많이 사용한다.[3] 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. 스피어 피싱은 지난 2016년 미국 대선에서 힐러리 클린턴 민주당 후보의 메일 내용 유출 파문을 일으키며, 곤경에 빠뜨림으로써, 대선 결과에도 치명적인 악재로 작용한 바 있다.

랜섬웨어(Ransomware) 공격도 중요한 데이터 유출의 사례이다. 악성 코드를 사용하여 사용자의 데이터를 암호화하고 이를 복구하기 위한 몸값을 요구하는 것으로,[4] 주로 기업들을 대상으로 하였으나 점차 지자체나 국가 기관은 물론 핵심 기반 시설까지로 확대하고 있다. 2017년 발생한 WannaCry 랜섬웨어 사례가 대표적이며, 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 이르렀던 것으로 보고되었다[5]. 2021년에는 미국 최대 송유관 관리업체인 콜로니얼 파이프

2) https://www.cloudflare.com/ko-kr/learning/security/what-is-a-data-breach/
3) https://www.trendmicro.com/ko_kr/what-is/phishing.html
4) https://en.wikipedia.org/wiki/Ransomware
5) https://nordvpn.com/ko/blog/wannacry-ransomware-attack/

라인(Colonial Pipeline)이 '다크사이드(DarkSide)' 해킹그룹의 랜섬웨어 공격을 받아 동부지역 연료 공급이 일시 중단되는 피해도 나타났다.

맬웨어(Malware) 공격은 웜(Worm), 와이퍼(Wiper), 트로이목마(trojans) 등 악성 소프트웨어를 사용하여 정보를 유출하거나 시스템을 손상시키는 공격이다.[6] 대표적으로 2010년에 발견된 스턱스넷(Stuxnet) 웜이 있다. 당시 이란이 보유한 14개 핵 시설의 2만 개 넘는 제어장치를 감염시킨 뒤 원심분리기를 못쓰게 만듦으로써, 수년 동안 이란의 핵 프로그램을 멈춘게 한 바 있다. 스텍스넷 공격은 산업시설의 제어시스템에 대한 사이버 공격의 위험을 상기시키는 계기가 되었다. 이렇게 맬웨어는 데이터 탈취 및 암호화, 제어시스템 마비 등 다양한 목적으로 사용되어 사이버 안보와 데이터 안보에 위협요인이 되고 있다.

2. 알고리즘의 오작동을 유발하는 데이터 오염 유형

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.[7] 최근 머신러닝(ML)이나 AI의 알고리즘을 훈련하는 데이터의 정확성과 신뢰성이 중요해지고 있다. 이 때, 훈련 데이터가 오염될 경우 AI의 알고리즘에 편향성과 환각(Hallucination) 현상을 일으켜 정확한 정보를 생성하지 못하고 가짜 뉴스를 생성하거나 인간의 의사 결정에 잘못된 판단을 유도하게 된다. 즉, 악의적인 학습 데이터로 훈련을 시켜서 머신러닝 모델을 망가뜨리는 중독 공격(Poisoning attack)이나 입력 데이터에 최소한의 변조를 가해 머신러닝을 속이는 회피 공격(Evasion attack), 알고리즘의 취약점과 악의적 데이터 오염에 의해 적대적 환경에서 발생할 수 있는 적대적 공격(Adversarial Attack) 등은 AI 시스템을 오작동 시킨다는 점에서 다양한 위험 요소로 작용하고 있다.[8] AI 기술의 급속한 발전과 활용이 확대되면서 학습 알고리즘의 오작동이나 부작용을 방지하기 위한 안전성 확보가 데이터 안보의 또 다른 중요한 과제가 되고 있는 것이다.

3. 사실을 왜곡하는 데이터 조작·변조 유형

데이터의 조작은 정보의 정확성과 신뢰성, 무결성을 의도적으로 손상하는 행위라 할 수 있다. 이러한 조작은 데이터의 변조, 주입, 삭제 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.[9] 2021년 초 플로리다 수처리 시설에 침입한 해

6) https://www.ibm.com/kr-ko/topics/malware
7) https://terms.naver.com/entry.naver?docId=6653405&cid=69974&categoryId=69974
8) https://www.kisec.com/rsrh_rpt_det.do?id=221
9) https://www.mbaknol.com/information-systems-management/data-tampering-meaning-types

커가 물속의 유독물(수산화나트륨)을 안전하지 않은 높은 수준으로 높이는 사건이 발생하기도 하였다[10]. 최근 사이버물리 영역간의 연결성을 구현하는 메타버스와 IoT의 활용 확대로 사이버 공격을 통한 데이터의 변조 피해가 물리적 영역에서도 발생하고 있다. 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 주입하여 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.[11] 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.[12].

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.[13] 대표적으로 2010년 트위터(Twitter, 현재 X)가 XSS 공격을 받아서 공격 코드가 삽입된 글을 클릭하지 않고 단지 글에 마우스를 접촉하기만 해도 악성코드나 포르노와 같은 유해 정보가 담겨있는 사이트로 연결되는 현상이 나타나기도 하였다.

4. 민주주의 국가의 주권을 위협하는 영향공작

'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.[14] 영향공작은 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

-and-countermeasures/

10) https://www.protocol.com/enterprise/data-integrity-security-cyberattacks-threat
11) https://www.cdnetworks.com/ko/cloud-security-blog/what-is-a-sql-injection-attack/
12) https://www.joongang.co.kr/article/21628794#home
13) https://tibetsandfox.tistory.com/5
14) 송태은, "중국의 사이버 영향력 공작과 대응방안", 『제6차 KACS 국가전략포럼 자료집』, (2023. 12. 7.), p. 1.

익명성을 이용하여 해킹이나 SNS 등을 수단으로 다양하게 이루어지고 있다.[15]

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 자리잡고 있다.[16] 대표적인 영향공작의 유형은 해킹을 통해 민감한 정보를 유출하여 공개함으로써 여론에 영향을 미치는 데이터 유출(Hacking and Data Leaks)이라 할 수 있다. 소셜 미디어 플랫폼을 이용하여 여론을 왜곡하는 소셜미디어 조작(Social Media Manipulation)도 심각한 문제가 되고 있다. 이는 가짜 계정, 봇넷(botnet), 또는 트롤(troll)을 사용하여 특정 메시지를 확산시키거나 특정 주제에 대한 토론과 여론을 왜곡시키는 수법으로 악용된다. 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.

Ⅲ. 시사점

살펴본 바와 같이 데이터 안보의 패러다임에서는 ICT 기반의 초연결, AI 융합의 시대를 맞아 데이터는 광범위하게 생산, 유통, 저장되고 있다. 특히, 데이터 안보를 위협하는 사이버 공격의 방식 또한 변화하고 있음을 확인하였다. 각국은 데이터의 중요성을 인식함은 물론, 점점 더 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 시급한 문제로 부상하고 있다. 보다 고도화되고 있는 사이버 공격 유형과 그것이 초래하는 데이터 안보 문제의 심각성을 고려하여 우리는 다음과 같은 전략과 세부 실천 방안을 모색할 필요가 있다.

첫째, 한국적 상황에 맞는 데이터 안보 전략을 수립하고 거버넌스를 확립해야 한다. 데이터가 지니고 있는 활용과 보호라는 이중적 속성을 어떻게 균형을 맞춰 국가 디지털 경제를 활성화하고 국가와 국민의 안전을 보장할 것인가에 초점을 두고 데이터 안보에 대한 기

15) 김일기. (2023). 북한의 영향력 공작과 우리의 대응 방향. 이슈브리프 497호. 국가안보전략연구원.
16) 이 같은 허위조작정보의 문제는 결국 국가의 정치적 정당성을 훼손하는 국가 주권에 대한 개입 행위로 간주될 수 있다. 송태은(2023), "허위조작정보를 이용한 사이버 영향공작과 국가안보: 실태와 대응책", 『정책연구시리즈 2023-13』, 국립외교원 외교안보연구소. p. 2.

본적인 전략이 시급하기 때문이다. 특히, 개인과 민간 기업 등에 흩어져 있는 데이터를 국가 차원에서 어떻게 효율적으로 관리하고 보호하며 민간 협력과 국민과의 소통을 강화하는 등의 정책을 총괄하는 거버넌스를 확립해야 한다.

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 회복력(resilience)을 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.