Center for Future Warfare Studies,
Institute of International Studies at Seoul National University |
국제문제연구소 미래전연구센터 연구위원 워킹페이퍼 No.20.(발간일: 2025.2.7.)

데이터 안보와 정보기관 첩보

오일석 국가안보전략연구원 연구위원(법학 박사)

이 글의 내용은 국가안보전략연구원의 입장과는 전혀 관계가 없는 순수한 개인의 연구에 바탕을 둔 것임을 밝힙니다.

Ⅰ. 서론

국가의 생존과 번영을 위해서는 최고 의사결정자에 대하여 적시에 정확하고 투명한 정보를 제공할 수 있는 정보력이 담보되어야 한다. 정보력은 국가의 자원을 효율적으로 배분하여 사용하고 국가의 영향력을 강화하여 국력을 극대화하기 위한 수단이라고 할 수 있다. 즉 정보력을 통해 국가의 자원과 영향력 각 부문에 필요한 정보를 제공하고 순환하도록 함으로써 국력을 극대화할 수 있는 것이다. 정보력은 마치 인체의 주요 자원과 같은 각 생체기관은 물론 의사결정과 소통을 담당하는 뇌에 영양분을 공급하는 혈액과 같이 자원과 영향력을 연계하여 국가의 주권을 유지하고 국력을 발휘하여 국민의 생활과 가치를 담보하도록 하는 역할을 수행하고 있다. 혈액 순환이 원활하여야 건강한 삶을 영위할 수 있는 것과 마찬가지로 국가가 자원과 영향력을 발휘하여 국력을 신장시키고 국민의 생활과 번영을 담보하며 국가의 가치를 확산하기 위해서는 국력의 요소에 대한 정확한 정보를 수집 · 축적하고 적시에 분석하여 의사결정에 반영될 수 있도록 하는 정보력이 담보되어야 한다.

한편 지구화와 정보화 및 비대면 사회가 도래하기 이전에 정보기관은 보이는 적 즉 주로 다른 국가를 상대로 활동을 수행하였다. 즉 정보기관은, 외국 정부의 의사결정에 접근할 수

있는 해당국 관료나 고위 인사를 포섭하거나, 외국 정부 당국에 대한 물리적, 전자적 감시를 실시하거나, 외국의 군사훈련 계획을 탈취하고, 무기 정보를 획득하며, 다른 정부의 협상 전략을 탐지하고, 적대국 정부를 전복시키는 등의 활동을 수행하였다.

기술발전과 지구화 시대의 새로운 위협에 대응하고 자원과 영향력 각 부문에 필요한 정보를 제공하여 국력을 신장시키고 국민의 생활과 번영을 담보하며 국가의 가치를 확산하기 위해서는 정보 패러다임의 변화가 요구된다. 냉전의 해체와 더불어 시작된 정보통신기술의 발전은 전 지구적 네트워크를 구축하고 국제 공급망을 작동시켜 새로운 안보위기를 초래하였기 때문이다. 새로운 안보위기는 군사적, 비군사적 영역 모두에서 발생할 수 있으며 세계화와 정보화의 영향으로 인하여 변화의 템포가 빠르고 예측이 곤란하다.[1] 이는 과학기술의 발전이 전혀 의도하지 않았던 위험으로, 그 위험의 결과를 즉시 알 수 없는 경우가 대부분이고 원인규명도 명확하게 할 수 없는 경우가 대부분이다.[2]

기존의 전통적 안보위협은 물론 정보통신의 발달과 지구화의 확산으로 등장하고 있는 기후변화, 환경오염, 신종 감염병, 사이버 공격 등 새로운 안보위협에 적극적으로 대응하기 위해 정보기관은 데이터에 대한 지배력을 확보하여야 한다. 초연결 비대면 사회가 도래하고 생성형 AI가 일상에서 실행되면 위성정보가 실시간으로 공유되는 상황에서 데이터에 대한 지배 여부는 국가 경쟁력과 국력을 좌우하기 때문이다. 이를 위하여 데이터 안보와 정보기관의 정보활동에 대해 살펴볼 필요가 있다.

데이터 안보와 정보기관의 첩보를 살펴보기 위하여 우선 정보환경의 디지털 전환과 데이터 정보활동에 대해 고찰하고자 한다. 이후 데이터에 기반한 정보활동의 수행과 운용을 통해 데이터 지배를 달성하여 국가 경쟁력을 강화하기 위한 정보기관의 각종 활동에 대해 고찰하고자 한다.

---

1) 허태회·이희훈, "위기관리와 국가안전보장회의–법·제도적 고찰," 『한국위기관리논집』, 제9권, 제1호 (2013), pp. 113–130.
2) 김영호, "정보사회와 위험사회의 성찰," 『사회과학연구』, 제18집 (1999), pp. 168–169.

Ⅱ. 정보환경의 디지털 전환과 정보활동의 변화[3)]

1. 정보환경의 변화: 정부와 시장의 경쟁?

정보기관은 보이는 적 즉 주로 다른 국가를 상대로 활동을 수행하였다. 즉 정보기관은, 외국 정부의 의사결정에 접근할 수 있는 해당국 관료나 고위 인사를 포섭하거나, 외국 정부 당국에 대한 물리적, 전자적 감시를 실시하거나, 외국의 군사훈련 계획을 탈취하고, 무기 정보를 획득하며, 다른 정부의 협상 전략을 탐지하고, 적대국 정부를 전복시키는 등의 활동을 수행하였다. 즉 국가 정보활동은 보이는 적에 대한 첩보를 수집하고 분석하여 적시에 정확한 정보를 의사결정자에게 제공하는 활동이 중심이 되었다.

그렇지만 정보통신 기술의 발전과 초연결 시대의 등장은 인간 생활영역을 극지와 심해, 우주와 사이버 등으로 확장시키면서 새로운 위험을 탄생시켰다. 기후변화에 따른 이상기후와 신종 감염병의 등장, 사이버와 우주 공간에서의 위험 증대, 디지털 경제의 안정성 위협, 가짜뉴스와 허위조작정보에 의한 민주적 정당성의 왜곡 등 새로운 위험과 이러한 위험의 초연결은 정보기관으로 하여금 보이지 않는 적이나 위험에 대한 정보활동의 수행을 요구하고 있다.

미국 국토안보부의 위험평가 기법에 의하면 위험(Risk)은 위협(Threat)과 취약성(Vulnerability) 및 결과발생(consequence)의 곱으로 평가하고 있다.[4)] 이 평가 기준에 의하면, 위협, 취약성, 결과 발생을 감소시키면 위험은 감소하며, 이중 하나라도 완전히 제거하면 위험은 존재하지 않는다. 위협을 제거하기 위해서는 공격원점에 대한 타격이 가장 확실한 수단이 될 수 있다. 공격원점에 대한 타격은 군사력을 동원하여 실행하는 경우 분쟁으로 확산될 것이며 외교력을 통해서는 실행력을 담보할 수 없다. 정보활동을 통해 공격원점에 대해 공작을 수행하여 타격을 가함으로써 위험을 사전에 예방할 수 있다. 이는 정보기관만이 수행할 수 있는 선제적 위협 대응이다. 다만 정보활동을 통한 위험의 선제적 대응이 무력분쟁으로 확산되지 않도록 극도의 기밀성이 유지되어야 한다. 한편 정보기관은 정보(intelligence)와 첩보(information)에 대한 보안 활동을 강화하여 자국의 취약성을 감소시킴으로써 위험을 사전에 제거할 수 있다. 지구적 공급망을 통해 공급되는 각종 제품과 소프트웨어에 대해 보안성을 강화하고, 자국의 첨단기술이 해외에 유출되지 않도록 관련 정보활동

3) 이 부분의 내용은 오일석, "코로나19 시대 정보기관의 새로운 역할", 국가안보전략연구원 전략보고 제111호(2021 1), pp.6-7을 참고하여 정리하였다.

4) Michael Chertoff, "Foreword to Cybersecurity Symposium: National Leadership, Individual Responsibility", Journal of National Security Law and Policy, Vol.4.(2010), p.3.

을 강화하여야 한다. 사이버안보의 경우 보안 활동의 일환으로 취약성 감소를 위하여 컴퓨터 네트워크 시스템에 대한 취약성 분석 평가 및 관리체계를 구축하고 일정 시점마다 평가하도록 지원하는 것이 필요하다. 또한 정보기관은 결과 발생의 방지나 최소화와 관련하여 필요한 정보를 제공함으로써 신속한 복구 및 회복력의 담보를 지원하여야 한다.

그렇지만 정보기관이 정보활동 수행 과정에 있어 권한을 남용하거나 기본권을 침해한 경우가 많이 발생하였기 때문에 이에 대한 적절한 감독과 통제 또한 증가하고 있다. 이러한 감독과 통제는 정보활동에 대한 법의지배로 이어져 각종 법률과 지침이 도입 · 적용됨은 물론 정보기관 내부에서도 그 활동에 대한 법적 근거 마련을 통해 그 활동의 정당성을 추구하고 있다. 이에 따라 정보기관이 새로운 위험에 적극적으로 대응함에 있어 자율성을 발휘는데 일정한 제약이 존재하는 것도 사실이다.

이와 같이 정보활동에 대한 제한과 민주적 정당성 요구에 따른 자율성의 위축은 정보기관 종사자들의 민간 이전을 촉진하였다. 자본주의 사회가 고도화되면서 사명감보다는 연봉에 의한 사회적 평가에 따른 박탈감으로 인해, 정보기관 종사자들이 민간으로 이직하거나 퇴직 후 이전하는 것이 추세가 되었다. 정보기관 종사들의 민간 이전을 통해 정보수집 및 분석 기법 등이 민간으로 전수되었다. 일례로 2019년 10월 16일 이스라엘 정보기관 산하의 Unit 8200에 근무하던 전문가가 UAE에 기반을 둔 사이버보안 회사에 입사한 사례가 있다.[5] 민간기업 등에서는 이렇게 유입된 정보기관 종사자를 통하여 정보수집과 분석 기법을 전수받아 민주적 통제 없이 적극적으로 민간 정보활동을 수행하고 있다.

한편 SNS와 포털의 발전은 구글, 페이스북, 네이버와 같은 기업에 데이터를 집중시키고 정보 공유를 촉진시킴으로써 민간의 정보수집과 분석 능력 향상시키고 있다. 적성국 스파이, 테러범이나 조직범죄자 등의 일상적인 활동이 SNS 등에 노출될 가능성이 증대되고 있다. 또한 SNS를 통하여 이러한 정보가 공유되고 축적될 수 있으므로, 민간이 정보기관보다 더 많은 데이터를 확보하고 이에 대한 분석을 통해 유의미한 정보를 생산하는 정보 경쟁력을 축적하고 있다.

민간기업은 인공지능을 적극 활용하여 정보기관보다 향상되고 선도적인 정보 분석을 통해 정보 경쟁력을 확대하고 있다. 이들은 민주적 정당성에 따른 통제로부터 자유롭기 때문에 보다 신속하고 효과적이며 분석적인 알고리즘 개발하여 활용하고 있다. 고도자본주의사

5) Times of Israel, "UAE-based Intelligence Firm Said Recruiting IDF Veterans from Elite Cyber Unit," October 18, 2019, https://www.timesofisrael.com/uae-based-intelligence-firm-said-recruiting-idf-veterans-from-elite-cyber-unit/ (accessed: August 28, 2024).

회로의 변화와 인공지능, 빅데이터, 사물인터넷 등 4차 산업혁명 기술 발전은 정보기관보다 경쟁력 있는 민간기업이 등장할 수 있는 생태적 환경을 형성하고 있는 것이다.

<표1> 정보기관과 민간기업의 정보활동 차이점

	정보기관	민간 기업
통제	민주적 통제 강화	민주적 통제로부터의 자유
디지털	디지털 전환에의 저항 – 조직문화의 경직성 – 관료주의	디지털 기술의 적극 활용 – 조직문화의 유연성 – 성과주의
데이터	데이터 수집 분석의 한계 –개인정보 보호에 따른 제한	데이터의 적극 활용 –계약과 동의를 통한 데이터의 수집, 분석 및 유통
AI	AI 활용에 대한 책임 –기본권 보호와 연계	AI를 통한 정보 효율성 추구 –기본권으로부터 상대적 자유

(저자 작성)

결국 정보환경의 디지털 전환과 정보환경이 변화하고 있는 상황에서 데이터의 수집, 분석, 공유에서의 경쟁력을 확보하고 데이터 지배력을 강화하기 위하여 정보기관은 민간기업과의 데이터 협력을 강화하지 않을 수 없다.

정보기관과 민간기업의 데이터 협력은 국가의 기능과 시장의 역할에 대한 본질적인 의문을 함께 제기한다. 원래 안보, 보안, 정보활동 등은 국가의 핵심 기능 가운데 하나이다. 그렇지만 정보화와 지구화, 디지털 경제 등 21세기 상황은 이러한 국가 핵심기능의 수행이 국가기관 단독으로 행사되기 곤란하고 민간과의 협력을 통해 경쟁 우위 혹은 실행 가능한 구조를 창출하였다. 민간의 도움이 없이는 국가가 그 기능을 수행하기 곤란한 것이다. 한편 X, 구글, MS 등 플랫폼 기업의 영향력 확대는 플랫폼 기업에 의한 데이터의 축적과 인공지능 개발로 이들의 영향력을 더욱더 가속화시키고 있다. 심지어 이들을 통한 정보제공 서비스나 보안 기능의 제공을 통해 특정 국가의 기능이 대체되기도 하는 추세이다.

이와 같은 플랫폼 기업에 의한 시장의 국가 기능 대체 상황은 향후 더욱 지속될 것으로 보인다. 이에 더하여 이러한 플랫폼의 확장으로 인하여 권위주의 국가들이 오히려 손쉽게

정보를 취득할 수 있게 되었다. 정보나 데이터를 거래를 통해 수집하거나 서비스 이용을 통해 사용할 수 있게 됨은 물론 국가 배후해커를 활용한 사이버공격을 통해 손쉽게 탈취할 수도 있기 때문이다. 자유로운 데이터의 흐름을 강조한 미국과 서방은 데이터가 자유롭게 권위주의 국가로 흘러들어감에 따라 권위주의 국가의 데이터 지배력이 강화되어 데이터 지배력과 인공지능 기술 경쟁력에서 위기감을 느끼게 되었다. 이에 따라 미국은 우려국가로의 데이터 이전을 금지하는 행정명령을 발동하기에 이르렀다. 아울러 이러한 행정명령 이전에는 권위주의 국가로의 데이터 흐름을 차단하고 사이버공간의 안전성을 보장하기 위하여 인터넷 분할을 논의하기도 하였다.

결국 인터넷의 분할이나 데이터의 우려국으로의 이전을 제한하는 것은 국가와 시장이 데이터의 지배력을 놓고 벌이고 있는 경쟁에 있어 국가가 시장을 통제하기 위한 수단으로 작동하고 있는 것이다. 따라서 아직까지는 데이터의 지배에 있어 국가가 시장에 통제력과 영향력을 행사할 수 있는 권력이 있음을 알 수 있다. 그렇지만 데이터의 수집가 분석에 있어 국가는 여전히 시장의 도움이 필요하기 때문에 민관협력을 강조하고 있는 것이다. 그러므로 현재의 상황은 시장과 국가가 데이터의 지배력을 놓고 불편한 동거를 하고 있다고 할 수 있다. 즉 데이터의 수집은 시장이 하고 정부는 수집된 데이터를 민관협력을 통해 이전받아 분석하고 처리하고 있기 때문이다. 이러한 불편한 동거가 얼마나 지속될 것인지는 모를일이다. 그렇지만 한가지 반듯이 유념할 사항이 있다. 시장에 의한 데이터의 지배가 가속화되고 특정 기업이 데이터에 대한 독점적 지배를 확립한다면 정치적 독재로 연결될 수 있다는 점이다. 이는 중국이 국영기업을 앞세워 데이터를 절대적으로 축적하고, 법률을 정비하여 개인정보 보호를 무시하고 보다 공세적으로 데이터를 수집함에 따라 정치적 독재가 더욱 강화되고 있는 상황을 통해서도 알 수 있다. 따라서 시장이 국가의 데이터 지배력을 능가하는 상황이 발생하더라도 국가는 시장에서 데이터에 대한 독점이 이루어지지 못하도록 하고 플랫폼들 사이의 경쟁이 지속되도록 법제적 수단을 견지하여야 한다.

2. 정보활동의 변화와 데이터 안보

정보활동은 정보 수집의 수단을 기준으로 인간정보(HUMINT), 과학정보(TECHINT) 및 공개출처정보(OSINT)로 나누어 볼 수 있다. 이 가운데 과학정보는 인간이 아닌 다양한 과학기술을 이용하여 정보를 수집하는 것을 말한다. 과학정보는 신호정보(SIGINT), 영상정보(IMINT) 및 징후계측정보(MASINT)로 나누어진다.[6] 여기에 방첩(Counter Intelligence) 활동을 더하면 모든 종류의 정보활동을 포섭할 수 있다.

정보통신 기술의 발전으로 과학정보는 그 중요성을 더해가고 있다. 신호정보는 각종 통신장비 및 전자장비에서 방출되는 전자기파를 감청하여 취득되는 지식 또는 그것을 생산하기 위한 수집, 처리, 분석 등의 제반활동을 통칭한다. 영상정보는 지상 또는 공중에서 광학이나 전자적으로 획득한 정보를 분석하여 생산한 정보를 말한다. 징후계측정보는 감지장치로부터 탐지되는 자료에 대해 양적 및 질적 분석을 통해 획득되는 정보로서 적국의 무기체계를 탐지하고 그 특성과 성능을 파악하는데 이용된다.[7]

한편 정보통신기술의 발전과 전 지구적 공급망 구축으로 인터넷과 모바일 통신이 증가하고 4차 산업혁명 기술발전에 따라 신호정보활동은 사이버공간으로 확장하고 있다. 즉 단순히 전자기파를 통한 감청에 머무는 것이 아니라 인터넷 통신과 모바일 통신은 물론 위성통신에 대한 정보 획득을 실행하고 있다. 아울러 이러한 통신 내용뿐만 아니라 인터넷, 모바일, 위성통신과 관련된 매타데이터를 수집, 분석하여 보다 정확한 정보를 획득할 수 있게 되었다.

또한 주요국은 접근하기 곤란하여 정보 획득이 불가능한 지역에 대한 정확한 정보를 수집하기 위하여 인공위성을 활용한 영상정보 획득을 위해 노력하고 있다. 첨단 광학기기를 탑재한 인공위성은 물리적 접근이 불가능한 지역에 대하여도 정밀한 시진과 이미지를 제공함으로써 정보의 가치를 높이고 있다. 과학정보가 점점 더 중요해 지고 있기 때문에 CIA와 FBI도 NSA와 NRO 등 정보기관들도 과학정보 활동을 증대시키고 있다.

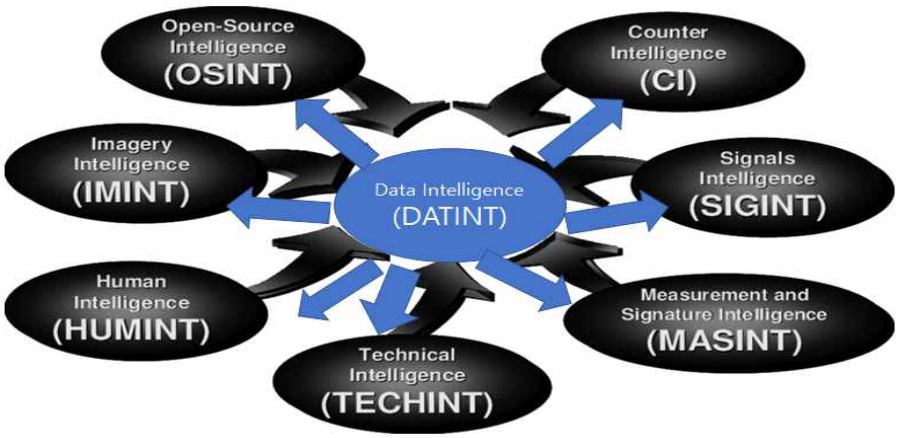
과학정보활동이 중요해지고 있는 것은 사실이지만 인간정보와 단절될 수는 없다. 인간정보는 과학정보를 통해 획득한 정보의 가치를 평가해 주거나 과학정보의 정확성을 확인 또는 평가해 줄 수 있다. 아울러 인간정보를 과학정보활동을 보완해 주기도 한다. 즉 인터넷이나 모바일로 접근할 수 없는 특정 외국의 내부 시스템에 대한 물리적 침입을 통해 악성코드나

6) 전웅, "첩보수집 수단의 유용성 비교: 인간정보와 기술정보를 중심으로", 『국가정보연구』 제7권 제2호(2014. 12), p.83.
7) 전웅, 앞의 논문, pp.83-89.

감청 장비를 설치하여 신호정보활동을 통해 해당 시스템의 정보를 획득할 수 있도록 할 수 있다. 미국 NSA와 CIA 또는 FBI가 상호 긴밀하게 협력하여 이러한 작전을 수행하고 있다. 과학정보와 인간정보의 보완을 위하여 미국 NSA와 NRO는 CIA 및 FBI와 협력을 증가하고 있다. 과학정보활동을 수행하는 정보기관과 인간정보 활동을 수행하는 정보기관이 상호 연락관을 파견하거나 특정 분야 협력을 위해 아예 직원을 파견하여 근무하도록 하는 경우도 있다.

그런데 정보통신기술의 발전과 4차 산업혁명 그리고 코로나19로 인한 디지털화와 비대면 사회의 가속화는 현실과 가상공간을 넘나드는 다양하고 새로운 정보를 창출 및 유통시키고 있다. 즉 다양한 디바이스와 플랫폼을 통한 정보의 생산과 유통은 공개출처정보를 통해 정보를 축적, 분석, 유통하는 공개출처정보를 통한 정보활동의 강화를 요구하고 있다.

<그림 1> 각종 정보활동의 관계도



(저자 편집)

결국 정보기관이 정보화와 지구화 및 비대면 사회에 적응하여 경쟁력을 확보하기 위해서는 디지털 전환을 실현하는 동시에 인간정보(HUMINT), 과학정보(TECHINT) 및 공개출처정보(OSINT) 사이의 유기적인 협력과 상호보완적인 관계를 구축 · 운영하여야 한다. 그런데 이러한 다양한 정보활동의 대상인 동시에 수단이 되면서도 그 협력과 상호보완성의 교차점에 데이터정보(DATINT) 활동이 자리잡고 있다고 볼 수 있다. 이러한 정보활동의 수행으로 구축되는 결과가 데이터이며 이러한 정보활동이 대상으로 하는 것이 정확한 데이터를 적시에 확보하는 것이기 때문이다. 또한 이들 정보활동으로 생성된 데이터를 상호 비교 보완함으로써

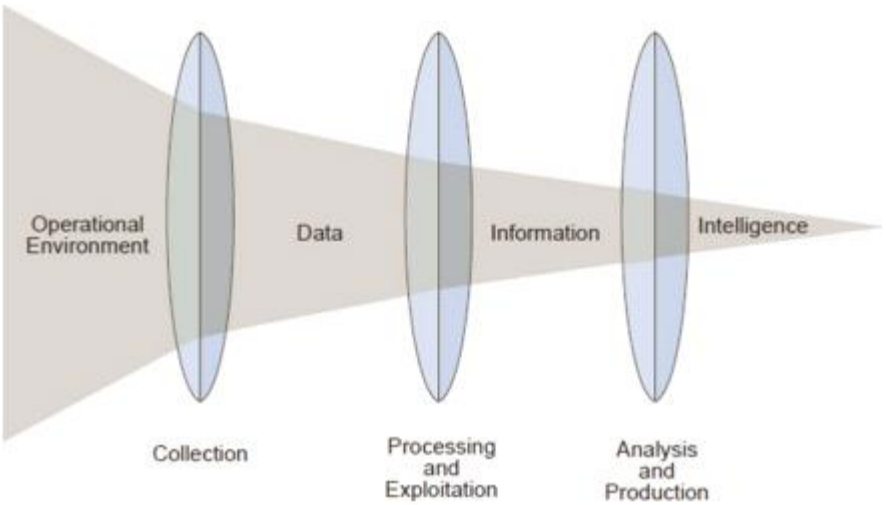
더욱 가치가 있는 새로운 데이터 또한 생산할 수 있기 때문이다.

Ⅲ. 데이터의 처리에 기초한 정보활동

1. 정보분석과 데이터 처리

디지털 전환과 초연결 사회의 도래는 다양한 소스로부터 데이터가 엄청난 속도로 생성 및 축적되고 있다. 데이터 정보활동의 핵심은 이렇게 증가하는 데이터에서 유의미한 데이터를 찾아 분석하여 국가 최고의사결정의 실행에 필요한 정확한 정보를 적시에 제공함에 있다.

<그림 2> 정보분석: 적극적 정제 절차



(Defense Technical Information Center, DTIC; Department of Defense, 2013, I-2)

정보분석 활동은 방향설정, 수집, 처리 및 활용, 분석, 공유, 피드백의 과정을 통해 이루어진다.[8] 방향 설정은 의사 결정권자가 일반적으로 위협평가의 일부로서 특정 정보

[8] Alexander Blanchard, Mariarosaria Taddeo, The Ethics of Artificial Intelligence for Intelligence Analysis: a Review of the Key Challenges with Recommendations, Digital Society (2023), pp.4–6, https://link.springer.com/article/10.1007/s44206-023-00036-4 (accessed: August 28, 2024).

(intelligence) 운영의 범위, 접근 방식, 목표를 주도하고 형성하여 우선순위를 결정하는 것을 말한다. 수집은 방향 설정 단계에서 정의된 우선순위에 따라 수집 방법, 출처, 다른 기관으로부터의 데이터 이전 등을 말한다. 처리 및 활용은 데이터에 대한 라벨링, 선별 및 조합, 가치부여 등 수집된 데이터에서 유의미한 정보를 추출하는 과정을 말한다. 분석은 방향성 단계에서 파악한 우선순위에 대해 처리된 데이터의 관련성을 평가하고, 이러한 데이터를 다른 데이터와 통합하여 관련 정보 및 패턴을 추출하는 것이다. 공유는 위협의 수준, 긴급성, 획득한 정보의 유형 등에 따라 확정된 정보에 정도(라벨)를 표시하고 다른 정보 및 문서와 비교하여 우선순위를 표시하는 것을 말한다. 마지막으로 의사 결정권자가 정보기관에 대해 피드백을 공유함으로써 정보분석의 방향 설정을 업데이트하게 된다.

결국 정보분석에 있어 가장 중요한 것은 수집된 데이터를 처리 및 활용하여 그 관련성을 분석하고 정보 및 패턴을 추출하는 것이라고 할 것이다. 다시 말해 정보분석은 데이터의 자유로운 흐름을 추적하여 데이터를 수집, 처리, 분석하는 것이 핵심이라 할 수 있다. 따라서 정보활동은 데이터에 대한 지배와 처리가 확보되지 않으면 경쟁력 우위를 담보할 수 없게 되었다고 해도 과언이 아니다.

2. 데이터 처리 정보활동의 방법

가. 컴퓨터 네트워크 탐사(CNE)

정보기관은 컴퓨터 네트워크 탐사(CNE) 활동을[9] 통해 정보활동의 표적인 컴퓨터 네트워크에 침입하여 데이터를 수집하거나 탈취하는 데이터 정보활동을 수행하고 있는 것으로 알려져 있다. CNE는 ①표적 대상인 컴퓨터 시스템으로부터 직접 데이터를 취득하는 활동(collection activities)과 ② 표적 대상인 컴퓨터 시스템에 대한 접근 권한을 획득해 필요한 정보를 수집하는 활동(enabling activities)으로 구분된다. ②는 ①을 위한 사전 전제 활동임과 동시에 컴퓨터 네트워크 공격(CNA)의 전제 활동인 경우도 있다. CNE 기법으로서는, 원격지로부터 인터넷망을 매개로 침입을 실행하는 원격 침입(remote access)과 인근에서 직접 침입하는 근접 침입(close access)이 있다. CNE는 미국 국가안보국(NSA)의 맞춤형 접근 작전(Tailored Access Operation: TAO) 부서에서 수행하고 있지만, 필요에 따라 중앙정보국(CIA) 및 연방수사국(FBI) 등의 기관과 협력 활동도 수행한다.

9) https://www.aclu.org/wp-content/uploads/legal-documents/CNO%20Legal%20Authorities_0.pdf (accessed: August 28, 2024)

TAO 부서의 내부 구성은 작전에 필요한 소프트웨어나 하드웨어 개발 부서(ANT, DNT, TNT), 작전의 실시 부서(ROC, AT&O), 작전의 기획 조정을 실시하는 부서(R&T), 그리고 작전을 지지하는 네트워크 인프라 부서(MIT) 등 4개 부서로 이루어져 있다.[10] 그 기술력은 상당히 고도화되어 있는 것으로 알려져 있으며, NSA 내부 자료 중에서도 TAO 구성원들이 '데프콘'이나 '블랙햇' 등 해커가 모이는 대회에 참가해도 탑클래스를 차지할 정도로 기술력이 뛰어나다.[11] 각종 시스템에 대해 NSA가 조작 가능한 악성 프로그램을 주입한 건수가가 2008년에는 21,252건, 2011년에는 68,975건에 이른다고 한다. 악성 프로그램 주입 건수는 2013회계연도 기준으로 8만 5천에서 9만 6천 건에 이를 것으로 추정되고 있다(운용 예정을 포함하면 9천 건에서 1만 건). NSA는 또한 악성 프로그램에 대한 조작원이 필요 없는 자동 운용 시스템을 개발 중이라고 한다.[12] 익성 프로그램 운용 효율화의 한 예로, 2013회계연도에 침입한 네트워크의 통신 가운데 특정인의 음성을 감지해 자동적으로 추출하여 송신하는 소프트웨어를 개발 중이었던 것으로 알려졌다.

또한 TAO는 단순히 데이터 수집을 담당할 뿐만 아니라 사이버방어, 사이버공격에도 관여하고 있다. 2011년에는 사이버공격 작전을 231건 실시했는데, 그 중 4분의 3이 우선 목표 대상국인 이란, 러시아, 중국, 북한 등을 대상으로 한 것이었다. 사이버공격 작전의 대부분은 시스템을 파괴하기 보다는 시스템상의 데이터와 시스템의 기능에 악영향을 주는 것이었다.[13] 다만 알렉산더 전 NSA 국장은 2013년 가을 인터뷰에서 임기 8년에 걸친 사이버공격 작전은 손에 꼽을 정도(only a handful of times)밖에 안 된다고 말한 바 있다.[14] 그가 말하는 사이버공격 작전이란 시스템에 대한 파괴적인 공격에 한정하고 있는 것으로 보인다.

---

10) Electronic Frontier Foundation, 20150117-Speigel-Interview With An Employee of NSA's Department For Tailored Access Operations About His Field of Work, https://www.eff.org/ko/document/20150117-speigel-interview-employee-nsas-department-tailored-access-operations-about-his (accessed: August 28, 2024): Electronic Frontier Foundation, NIOC Maryland Advanced Computer Network Operations Course, https://www.eff.org/files/2015/01/28/20150117-spiegel-nsa_training_course_material_on_computer_network_operations.pdf (accessed: August 28, 2024)

11) Ryan Gallagher and Peter Maass, "Inside the NSA's Secret Efforts to Hunt and Hack System Administrators," *The Intercept*(March 20, 2014), https://theintercept.com/2014/03/20/inside-nsa-secret-efforts-hunt-hack-system-administrators/(accessed: August 28, 2024)

12) https://www.eff.org/de/node/84459

13) 공격적 작전이란 컴퓨터나 컴퓨터 네트워크 자체 또는 이에 존재하는 데이터를 조작, 방해, 파괴하는 작전으로, 2010년에 NSA가 279건이나 실행하였다고 한다.

14) David E Sanger, "Syria War Stirs New U.S. Debate on Cyberattacks," *The New York Times*(February 24, 2014), https://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html(accessed: August 28, 2024)

원격 침입은 인터넷 침입(On-net), 소프트웨어 주입(software implant) 등으로도 불린다. NSA의 원격작전센터(ROC: Remote Operations Center)가 담당하고 있다. 또한 원격 침입 이외의 컴퓨터 시스템 침입 방법을 물리적 침입, 근접 침입, 또는 오프넷 침입(Off-net)이라 한다. 이는 우선 공급망 작전 등을 통해 대상 기기에 물리적으로 접근하여, 악성코드를 주입하거나 특정 하드웨어를 장착하는 것을 말한다. NSA가 물리적 침입을 시도하는 경우 FBI나 CIA의 지원을 받는 것으로 알려져 있다. 물리적 침입을 위해 NSA의 TAO 전문가들을 신속히 필요한 지점으로 이동시키기 위해 FBI 소유 제트기를 이용한 요원 이송 지원도 받고 있는 것으로 알려져 있다.[15)]

악성코드의 주입이나 하드웨어 장착에 성공한 이후에는 일반적으로는 앞에서 언급한 원격작전센터(ROC)에 의해 원격 수집으로 전환되는 것으로 보인다. 그러나 주입한 악성코드 또는 장착한 하드웨어를 통해 근접 지점에서 수집(short-rage collection)을 하는 경우도 있다. 이 물리적 침입은 비밀의 정도가 매우 높아 관련된 자료나 보도가 적은데 다음 작전들이 폭로와 언론을 통해 식별되었다.

고도 네트워크 기술(ANT)은 TAO 내부의 기술부문 중 하나로, 네트워크에 침입하거나 휴대전화, 컴퓨터로부터 데이터를 수집하기 위한 악성코드와 하드웨어 장비를 개발하고 있다. 그 ANT가 개발한 장비의 일부가 슈피겔지의 웹사이트에 소개되기도 하였다. 소개된 장비는 구형이기는 하지만 NSA가 데이터 수집에 있어서 어떤 장비와 기법을 사용하고 있는지 등을 알 수 있다.

또한 악성코드(malware)은 기본적으로 바이오스(BIOS, (컴퓨터의 메인보드에 있는 소프트웨어) 내에 주입하거나 장착되도록 하고 있다. 따라서 하드 드라이브를 삭제하고 운영체제 등의 소프트웨어를 모두 삭제해도 이 악성코드는 살아남을 수 있도록 고안되어 있다. 또 하드드라이브 내 펌웨어에 주입되어 탐지되지 않도록 내장된 악성코드도 있다.[16)] ANT의 장비는, 원격 침입으로도 주입이 가능한 것이 있다고 알려졌지만 슈피겔에 소개된 장비는 근접한 물리적 침입에 사용되는 것이 대부분을 차지하고 있다.

---

15) SPIEGEL Staff, Inside TAO: Documents Reveal Top NSA Hacking Unit(December 29, 2013), https://goodtimesweb.org/covert-operations/2014/spiegel-tao-nsa-hacking-unit-dec-29-2013.html(accessed: August 28, 2024)

16) Jacob Appelbaum, et. al., "NSA's Secret Toolbox: Unit Offers Spy Gadgets for Every Need," Spiegel Online(December 30, 2013), https://www.spiegel.de/international/world/nsa-secret-toolbox-ant-unit-offers-spy-gadgets-for-every-need-a-941006.html(accessed: August 28, 2024)

나. 사이버공격

정보기관은 생성형 AI를 이용한 사이버공격을 통해 데이터를 수집할 수도 있다. 사이버공격자들은 생성형 AI 코드를 재작성하여 사이버공격에 대한 추적을 곤란하게 할 수 있다. 또한 컴퓨터 프로그래밍 기술이 부족한 공격자라 하더라도 생성형 AI 시스템을 활용하여 보다 효과적인 사이버공격을 위한 코드를 생성할 수 있다.

생성형 AI를 이용한 공격자는 방어자보다 비대칭적 우위의 입장에서 공격을 진행할 수 있다. 이 공격자들은 인공지능과 기계학습(AI/ML)을 기반으로 보다 정교한 공격을 저렴한 비용으로 막대한 규모로 실행할 수 있기 때문이다. 또한 이들은 합성 텍스트, 음성, 이미지 등을 이용하여 소셜 엔지니어링 기법을 활용한 피싱 공격도 극대화할 수 있다. 국세청이나 부동산중개인을 사칭해 피해자에게 송금을 유도하는 피싱 공격 등을 자동화하여 감행할 수 있는 것이다.

사이버공격자는 생성형 AI 기술을 사용하여 보다 발전된 악성 코드를 제작한 다음 새롭고 효과적인 공격을 대규모로 실행할 수도 있다.[17] 향후 10년 동안 AI를 이용하거나 AI를 대상으로 한 새로운 유형의 사이버공격이 발생할 것으로 보인다. 공격자들은 생성형 AI를 이용하여 식별하기 곤란한 악성 모델을 만들어 피해를 가중시킬 것으로 보인다. 공격자들은 다양한 방법으로 AI 시스템을 기망함은 물론, 사용하는 데이터를 오염시키거나 민감한 데이터를 추출하는 등 새로운 유형의 공격을 확대할 것으로 보인다. 또한 AI에 의해 생성되는 소프트웨어 코드가 증가함에 따라 공격자들은 이러한 시스템에 내재된 취약점을 악용하여 대규모 공격을 감행할 수도 있을 것으로 보인다.

다. 인공위성과 드론

정보기관은 인공위성이나 정찰기 혹은 드론 등을 이용하여 데이터 정보활동을 수행하고 있다. 우주와 공중으로부터 영상과 이미지 데이터를 수집하고 분석하여 공유하는 것이다. 이러한 데이터에 기초하여 △ 대량살상무기 확산 감시, △국제 테러리스트, 마약 밀매인, 범죄조직 추적, △고정밀 군사목표 데이터 작성 및 폭격 피해 평가, △국제평화유지활동 및 인도적 활동의 지원, △ 지진, 해일, 홍수, 화재 등 자연재해의 영향 파악 등을 수행할 수 있는

17) Aakash Shah, "How generative AI is creating new classes of security threats", Venture Beat, https://venturebeat.com/ai/how-generative-ai-is-creating-new-classes-of-security-threats/ (accessed: August 28, 2024).

것이다. 또한 우주와 공중으로부터 획득한 데이터에 기초하여 적대국이나 경쟁국의 군사 활동 감시와 평가, 전 지구적 통신, 정밀 항행, 미사일 발사와 같은 군사적 공격의 성공 유도 등에 필요한 데이터를 제공한다.[18]

정보기관은 인공위성이나 드론 등을 이용한 감시정찰 시스템을 기반으로 국가 전략에 필요한 데이터를 수집하고 분석함은 물론 정책 수요자에게 제공되는 데이터의 지속성을 유지하기 위해 노력하고 있다. 인공위성을 활용한 첨단 데이터 수집 시스템의 획득함으로써 정보 우위의 확보는 물론 접근 불가능한 지역에 대한 데이터 정보활동이 가능하도록 노력하여야 한다.

라. 공개출처정보 정보활동(OSINT)

공개출처정보(Open Source) 정보활동(OSINT)은 국가안보, 기업 경쟁력 향상, 연구개발과 기술력 우위, 법질서 유지, 언론 보도 등을 위해 사용 가능한 모든 공개정보를 활용하여 데이터를 수집, 분석, 공유하는 것을 의미한다. 정보화와 지구화의 영향으로 공개정보의 양이 기하급수적으로 증가함에 따라 그 중요성을 더하고 있다. 미국의 싱크탱크인 RAND는 2018년 연구에서 2011년 미국 국가정보국장실에서 발행한 문서를 인용하면서 OSINT를 "특정 정보 요구 사항을 해결하기 위해 적시에 적절한 대상에게 수집, 활용, 배포되는 공개적으로 이용 가능한 정보로부터 생산되는 정보"라고 정의하였다.[19] 디지털 전환으로 개인적 감정이 표현된 콘텐츠, 지역 및 사건의 사진, 소셜 미디어를통해 제공된는 전문적인 정보 등이 대량으로 유통되고 있는 상황에서 컴퓨터와 인공지능(AI)을 이용한 데이터 분석 기술의 발전은 데이터를 정보를 처리하고 정보적 가치가 있는 함의를 찾아내는 정보기관의 역량 또한 향상시켰다.

한편 정보기관의 OSINT는 2차 세계대전으로 거슬러 올라간다. 1941년 출범한 외국방송감시국(Foreign Broadcast Monitoring Service)은 그해 12월 일본군이 진주만을 공격한 직후 외국방송정보국(Foreign Broadcast Intelligence Service: FBIS)으로 명칭을 변경하였다. 이 조직은 2차 대전 이후 중앙정보국(CIA) 산하의 외국방송정보국이 되었다. 이 조직은 해외의 모든 메스미디어, 라디오, TV, 인쇄물 등을 통해 정보를 수집, 분석하는 임무를 수행하였다.[20]

---

18) National Reconnaissance Office, SUPRA ET ULTRA(NRO Brochure)

19) Heather J Williams, Ilana Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, (Santa Monica, RAND, 2018), p.1.

20) Joseph E Roop, Foreign Broadcast Information Service: History Part I 1941–1947 (Central Intelligence

2005년에 FBIS는 CIA가 관리하던 오픈소스센터(Open Source Center)로 통합되었지만 국가정보국(DNI)의 부서로서 역할을 하고 있다. 동 센터는 국가기술정보국(National Technical Information Service: NTIS)을 통해 세계 통신사, 신문, 라디오, TV 방송국에서 수집한 번역본과 정보를 제공하는 월드 뉴스 커넥션(WNC)이라는 온라인 뉴스 서비스를 운영하였다.[21] 그러나 2013년에 WNC는 종료되었고 오픈소스센터는 일반에 대한 정보제공을 중단하였다. 했습니다.[22] 오픈소스센터는 2015년에는 오픈소스엔터프라이즈(OSE)가 되어 CIA의 디지털 혁신국(Directorate of Digital Innovation)으로 흡수되었습니다. 이후 2019년부터 OSE는 웹사이트를 폐쇄하고 일반인의 정보접근을 차단하고 있다. 이는 공개출처정보의 중요성을 인식한 미국 정보당국의 결정에 따른 것으로 보인다. 이러한 사실은 2021년 9월, 미국 하원이 국방장관과 국가정보국장에게 "오픈소스 정보를 인간 정보, 신호 정보, 지리공간정보 등을 통해 수집된 정보와 동등하게 취급되는 전략 정보의 기초 정보로 승격시키는 계획을 시행하라."고 지시한 것을 통하여 알 수 있다.[23] 특히 허위조작정보와 가짜뉴스 등의 대응에 있어 공개출처정보가 유용한 것이라 판단했을 것으로 보인다.

공개출처정보 활동의 대상인 데이터의 폭발적인 증가는 민관협력을 통한 해당 정보활동의 수행이 요구되고 있다. 디지털 전환의 시대에는 수천 개의 기업이 데이터 수집 및 분석을 위한 소프트웨어를 설계하고 관련 플랫폼을 제공하고 있는 실정이다. 이러한 소프트웨어와 플랫폼을 통해 용의자, 범죄조직, 주소, 전화, 신분증 번호, 차량, 금융 등 모든 유형의 데이터 사이의 연관성을 식별할 수 있다. 여기에는 관련 데이터의 네트워크, 관계망, 가치 비중, 빈도, 활동 패턴, 사건의 연속성 등을 시각적으로 보여주는 알고리즘도 있다. 또한 데이터 소스를 모니터링하고 사용자가 설정한 기준에 따라 사용자에게 데이터 변경 사항을 알려주는 기능도 있습니다. 이러한 소프트웨어와 플랫폼의 상당수는 구글이나 페이스북과 같은 빅테크 기업이 상업적 목적으로 개발했다. 예를 들어, 지리적 위치는 사기 방지, 화물 배송 추적 또는 소비자 선호도 파악에 사용된다. Google은 IP 주소 추적, 쿠키 및 광고 추적 업계에서 사용되는 기타 웹 추적 기술을 통해 데이터를 수집하고 있다. 이러한 상황은 정보기관으

Agency, April 1969), https://www.cia.gov/readingroom/sites/default/files/FBIS_history_part1_0.pdf,(accessed: August 28, 2024).

21) University of Delaware, "World News Connection," https://library.udel.edu/databases/wnc/#:~:text=World%20News%20Connection%20is%20an,and%20radio%20and%20television%20stations, (accessed: August 28, 2024).

22) Stephen Aftergood, "CIA halts public access to Open Source Service," Federation of American Scientists blog(October 8, 2013), https://fas.org/publication/wnc-ends/, (accessed: August 28, 2024)

23) US House of Representatives, National Defense Authorization Act for Fiscal Year 2022 (HR 4350). Section 1612 "Strategy and Plan to Develop Certain Defense Intelligence Reforms," Congressional Record, Volume 167, Number 163, September 21, 2021, https://irp.fas.org/news/2021/09/intel-reforms.html, (accessed: August 28, 2024)

로 하여금 빅테크 기업 등 민간과의 협력을 통해 공개출처정보 정보활동을 수행하고 있다. 미국의 우주 정보기관인 국가정찰국(NRO)가 2022년 5월 민간과의 정보협력을 위해 향후 10년간 블랙스카이, 플래닛, 맥사르와 같은 유명 기업에 수십억 달러를 제공할 것이라고 발표한 것을 통하여도 알 수 있다. 이 상업용 공간정보(지오인텔리전스) 기업들은 지난 수십년 동안 NRO가 우주에 투입한 자산보다 훨씬 더 많은 자산을 우주에 투입하고 있다.

OSINT를 위해서는 데이터의 출처를 정확히 파악하여 인텔리전스 목적에 유용하게 사용할 수 있는 특수한 지리적 위치 도구가 필요하다.[24] 지리적 위치는 GPS 및 IP 주소와 같은 위치 기술을 사용하여 연결된 전자 기기의 위치를 식별하고 추적한다. 인터넷에서 공유되는 많은 사진에는 사진을 촬영한 시간, 위치, 심지어 카메라의 종류와 사용자가 사진을 업로드한 장소와 시간에 대한 메타데이터가 인코딩되어 있기 때문에 이 과정이 더 용이하다.

공개출처정보는 일반 대중이 공개적으로 이용하능한 정보(PAI)와 상업적으로 이용할 수 있는 정보(CAI)로 구분할 수 있다. 이 가운데 상업적 정보를 정보기관이 사용하기 위해서는 몇 가지 조건과 원칙이 필요하다.[25] 우선 미국 정보공동체(IC)는 18개 정보기관에 대해 CAI의 획득 및 사용을 목록화하기 위한 다층적 접근 방식을 개발하여야 한다. 다음으로 IC는 CAI 사용에 대한 지식을 축적함에 따라 CAI에 대한 일련의 표준과 절차를 개발하고, CAI의 획득 및 관련 정책 결정에 대해 정기적인 재평가를 실시하고 이에 따라 해당 정보를 관리하여야 한다. 이러한 표준 및 절차의 일부로, 혹은 이를 보완하기 위해 IC는 CAI에 관한 민감도 측정 및 개인정보 보호 지침을 개발하여야 한다. 민감도 측정에 따라 CAI의 민감성, 비식별화/재식별화 문제, CAI가 제공하는 임무의 중요성과의 균형성 평가(CAI의 민감도와 균형을 맞추기 위해), CAI과 임무 간의 연계 강도, 대안의 가용성, 실현 가능성, 비용 및 위험, 개인정보 보호 조치의 가용성 등을 고려할 필요가 있다.

---

24) Manoj Joshi, 「Open-Source Intelligence Has Arrived」, Occasional Paper No.415, Observer Research Foundation(October 2023), p.18, https://www.orfonline.org/research/open-source-intelligence-has-arrived(accessed: August 28, 2024)

25) ODNI Senior Advisory Group Panel on Commercially Available Information, Repoet to the Director of National Intelligence(January 27, 2022), https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf(accessed: August 28, 2024)

3. 인공지능(AI)을 이용한 데이터 처리

인공지능 특히 생성형 AI는 사용자의 요청에 따라 텍스트, 이미지, 오디오 또는 비디오 등을 포함한 콘텐츠를 생성할 수 있는 기술이다. 생성형 AI는 인터넷 상의 텍스트 및 이미지와 같은 오픈소스 정보를 통해 학습한 내용을 토대로 알고리즘을 사용하여 답변을 생성한다. 생성형 AI는 일반적으로 인지능력이 없으며 인간과 같은 판단력은 부족한 것으로 알려져 있다. 생성형 AI는 교육, 의료, 법률 등 다양한 분야에서 활용되고 있다. 즉 사용자가 입력한 질문이나 설명에 기초하여 결과를 생성 · 구체화하기 때문에 복잡한 연구 결과를 요약하거나 법률 문서에 대한 평가 등에 활용될 수 있다. 또한 음악 작곡, 시적 언어 등 예술 작품도 만들어 낼 수 있다. 나아가 새로운 의약품의 분자를 설계하거나 프로그래밍 코드를 생성하는 등의 업무도 처리할 수 있다.[26] 이러한 생성형 AI를 이용하여 이제는 데이터의 수집, 분석 및 공유까지도 효율적으로 실행할 수 있게 된 것이다.

인공지능 기술의 발전은 정보분석관의 데이터 분석에 필요한 수고와 시간 및 비용을 절감시키고 있다. 일반적으로 정보기관 종사자들은 수십만 건의 데이터와 이미지, 인공위성 정보 등을 분석하여 유의미한 정보를 채굴하고 가치 있는 분석정보를 정책당국에 제공하고 있다. 이들의 활동에는 상당한 시간과 비용이 소요되는데, 2016년 오바마 대통령이 정부 내에서의 인공지능 활용을 강화하는 백서를 발표한 결과 2017년부터 미국 정보기관도 정보분석에 있어 인공지능을 적극적으로 활용하고 있다.[27]

방대한 데이터를 수집하고 분석하여 유의미한 정보를 추출하고 공유함으로써 정보우위를 확립하는 것이 데이터인텔리전스의 핵심이다. 초연결 비대면의 정보사회에 있어 이러한 데이터인텔리전스를 실행하기 위해서는 AI의 활용이 무엇보다도 중요하다. 머신러닝 알고리즘과 대규모언어모델(LLM)은 수집된 방대한 양의 데이터나 이미지에서 특정 패턴을 찾아 학습한 다음 필요한 데이터나 이미지를 추적하여 유의미한 정보를 생산할 수 있기 때문이다. 이를 위해서는 클라우드 컴퓨팅, 첨단 센서 등에 대한 역량 강화도 필요하다.

---

26) Government Accounting Office, GENERATIVE AI, GAO-23-106782, https://www.gao.gov/assets/830/826491.pdf(accessed: August 28, 2024).

27) Elana Lyn Gross, "How Artificial Intelligence Is Transforming the Intelligence Community", DELL Technology, February 2018, https://www.dell.com/en-us/perspectives/how-artificial-intelligence-is-transforming-the-intelligence-community/ (accessed: August 28, 2024).

그렇지만 데이터의 처리를 인공지능에만 맡겨둘 수는 없다. 특히 대규모 언어 모델(LLM)을 기반으로 하는 현재의 생성형 AI는 본질적으로 지식에 한계가 있기 때문이다. 생성형 AI는 대답을 찾지 못하는 경우 그에 상응하는 무언가를 생성해 내는 소위 '환각(hallucinating)'을 만들어 내어 데이터 처리를 왜곡할 수 있다. 따라서 데이터 처리에 있어 인간 분석관이 인공지능(AI)을 활용할 수 있는 구조와 체계를 형성하여야 한다. 정보활동은 보이는 적 혹은 보이지 않는 적의 의도나 경향까지도 파악함은 물론 데이터의 맥락을 이해하여야 하는 측면도 있기 때문에 인간 분석관의 경험과 직관 또한 무시할 수 없기 때문이다.

그렇지만 인공지능을 이용한 데이터 처리를 통해 맥락 정보나 의도 분석까지 가능하게 하는 인공지능 기술 또한 발전하고 있다. 데이터를 처리하는 가장 오래된 방법은 아마도 콘텐츠 분석을 수행하는 것이었을 것입니다. 예를 들어, 김정은을 '지도자'로 언급하는 언론 기사에서 '김주애'가 언급된 횟수를 파악하여 '김주애의 후계자 가능성'을 분석해 보는 것이다. 알고리즘을 사용하여 텍스트를 분석하는 딥 러닝의 발전은 이러한 데이터 분석의 가치를 높이고 메시지에 대한 맥락 정보를 제공함으로써 적성국이나 경쟁국의 '의도'를 분석할 수 있게 하고 있다.[28)]

결국 다양한 정보활동을 통해 방대한 양의 데이터를 수집, 분석, 공유하기 위해서는 인공지능을 사용하지 않을 수 없다고 하더라도 기존 분석관의 활동과 균형을 찾는 방안을 실행하는 것이 중요하다. 인공지능은 정보 분석관이 처리하지 못할 정도의 방대한 데이터를 쉬지 않고 일정한 시간 내에 처리할 수 있다. 또한 분석관 개인이 갖는 편견이나 취향 또는 입장으로부터 자유롭기 때문에 데이터 수집, 분석, 공유에 있어 객관성을 담보할 가능성이 크다. 그렇지만 인공지능 특히 생성형 인공지능은 환각을 야기할 수도 있으며 설정된 알고리즘에 따라 편견이나 확증편향된 데이터 처리를 감행할 수도 있다. 따라서 데이터의 처리와 보호에 있어 분석관의 경험적 판단이나 직관도 무시할 수 없다. 결국 데이터 처리와 보호에 있어 인공지능을 활용하되 분석관의 경험적 판단과 직관이 투영될 수 있는 균형적 체계를 수립하여 운영하는 것이 필요하다.

28) https://www.publichealth.columbia.edu/research/population-health-methods/content-analysis#:~:text(accessed August 28, 2024)

Ⅳ. 데이터 지배력 강화: 데이터 보안 활동과 데이터 공작

1. 데이터 보안 활동

수집, 분석 공유된 데이터를 어떻게 보호할 것인지가 데이터 지배력 강화를 위한 첫번째 정보활동이라 할 것이다. 데이터 보호 활동은 사이버안보 활동과 중첩된다고 할 수 있다. 사이버안보 활동은 네트워크 보안, 암호, 공급망 보안으로 크게 구별될 수 있다. 한편 데이터에 대한 이전을 제한함으로써 데이터를 보호하는 방안도 있다.

가. 네트워크 보안

북한의 해킹 공격으로 주요한 신기술 데이터가 지속적으로 탈취당하고 있다. 첨단 정보보안 제품의 도입과 운영, 정보통신기반시설의 지정과 지원, 정기적인 취약점 분석 평가와 대응책 마련, 정보보호 관리체계 인증 등 기술적 관리적 대책에도 불구하고 국가배후에 의한 해킹 공격으로 인한 데이터 탈취 또한 지속되고 있다.

적대국이나 경쟁국의 사이버공격을 통한 데이터 탈취를 방지하기 위한 네트워크 보안 대책의 하나로 추진한 것이 망분리 정책이다. 주요 데이터와 시스템 운영을 폐쇄망이나 내부망으로 실햄함으로써 외부로부터의 사이버공격을 통한 데이터 탈취나 유출에 효과적으로 대비할 수 있기 때문이다. 그렇지만 망분리를 효과적으로 수행하여 유지하고 있다 하더라도, 앞에서 살펴본 바와 같이, CNE 활동을 통해 내부망 또는 폐쇄망에 침입하여 주요한 데이터를 탈취하는 것을 완벽하게 차단할 수 없는 실정이다. 또한 망분리 정책은 초연결 비대면 사회에서 인공지능과 클라우드 등 첨단기술발전과 보조를 맞추어야 할 정보활동에 방해가 될 가능성도 있다. 특히 매우 민감한 내부 데이터를 보유한 정보기관은 망분리 정책으로 인하여 업무망에서 민간 클라우드를 사용할 수 없으며 인공지능 분석모형 개발을 위하여 외부업체에 내부 데이터를 제공할 수도 없는 것이 현실이다.[29]

망분리 정책의 한계를 극복하고 클라우드 환경에서 데이터 보안과 활용을 확대할 수 있는 방안으로 제로트러스트 보안 패러다임이 확산되고 있다. 미국 바이든 대통령은 2022년 1월 19일 '국가안보, 국방 및 정보공동체의 서이버안보 향상을 위한 지침(Memorandum on

[29] 이석윤, "데이터 활용과 보호의 상충문제 해소방안", 「데이터 첩보(DATINT)와 사이버안보」, 제9차 사이버 국가전략포럼 자료집, 한국사이버안보학회(2024. 5. 2), p.60.

Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems)'을 발령하였다. 이에 따라 국가안보국(NSA)의 장은 국가안보시스템에 대한 안정성 확보를 위하여 위 대통령 행정명령에서 정한 것 이상의 권한과 책임을 부여받는다. 동 지침은 국가안보시스템에 대해 연방정보시스템에 요구되는 사이버보안 요건과 동등하거나 그 이상의 요건을 확보하도록 규정하고, 국가안보시스템 고유의 필요성에 대처하기 위한 사항을 실행하도록 하고 있다. 이에 따라 국가안보시스템을 보유 또는 운용하는 각 부처의 장관은 이 지침 시행일로부터 60일 이내에 제로트러스트(Zero Trust) 아키텍처를 구축하여야 한다. 또한 90일 이내에 국가안보시스템의 클라우드 이행과 운용에 있어 최소한의 보안 기준과 관리 가이던스를 정립하고 공포하여야 한다.[30] 이후 미 관리예산처(OMB)는 2022년 1월 26일 연방 정부부처 시스템을 제로트러스트 보안모델로 이행하는 사이버보안 원칙을 지침으로 발표하였다. 이 지침에 따르면 연방 정부 부처는 시스템 보호나 보안사고의 위험을 억제하기 위하여 필요한 대책을 수립하여야 한다. 동 지침 시행 후 30일 이내에 연방 정부부처는 제로트러스트 전략을 수행할 담당관을 지정하고 식별하여야 한다. 동 지침은 현재의 사이버위협 환경에서 기존의 방식으로는 주요 데이터를 보호할 수 없다는 인식 하에 연방 부처들로 하여금 제로트러스트를 이행할 것을 제안하고 있다. 특히 기술 대책에서는 다층 인증(MFA)을 포함한 ID와 접근통제의 강화에 중점을 두고 있다.[31]

나. 암호

데이터 보호를 위한 강력한 조치는 데이터를 암호화함으로써 데이터의 내용을 보호하는 것이다. 적대국이나 상대국이 사이버공격 등을 통해 데이터를 탈취하더라도 해당 데이터에 대한 암호화 조치가 시행되는 경우 그 내용을 파악하기 곤란하기 때문이다. 그렇지만 기존 암호기술은 저장/송수신하기 위해 데이터를 암호화하거나 복호화 하는 과정에서 데이터 보호에 한계를 보이고 있다. 즉 데이터의 검색이나 연산 과정에서 암호화된 평문으로 복호화해야 하는데 이 복화화 과정의 취약성을 이용하여 데이터를 탈취할 수 있기 때문이다.[32]

---

30) https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/(accessed: August 28, 2024)

31) https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf(accessed: August 28, 2024)

32) 이석윤, 앞dml 토론문, p.63.

이러한 취약성에 대응하기 위하여 미국은 연방부처와 관련 기업들에 대해, 보다 광범위한 암호화와 다방면의 인증시스템을 요구하고 있다. 즉 미국은 뒤에서 설명할 "국가 사이버안보 향상 행정명령"에 따라 미국 연방 정부부처로 하여금 데이터를 암호화하여야 하며 클라우드 호스팅 서비스의 안전한 사용에 대한 계획을 업데이트하고, 다층 인증 체계를 구현하도록 요구하고 있는 것이다.[33]

따라서 동형암호, 기밀컴퓨팅 활용시 서버에서 암호화된 상태로 데이터를 연산하거나 CPU와 메모리를 공유하는 클라우드 환경에서 하드웨어 내 안전한 실행공간을 마련할 필요가 있다. 특히 동형암호는 인공지능 모델 개발업체에 암호화된 상태에서 데이터를 제공하고 그 서버에서 통계분석, 머신러인(추론) 등의 수행을 가능하도록 하기 때문에 데이터의 보안성을 강화할 수 있다.[34]

다. 공급망 보안

네트워크 보안과 암호 정책을 통해 데이터 보안을 강화하더라도, 정보통신(ICT) 및 사이버안보 관련 하드웨어나 소프트웨어에 대한 공급망 안전성을 강화하여야 데이터에 대한 지배력을 확보할 수 있다. 2021년 솔라윈즈 사이버공격, 마이크로소프트 이메일 공격, 카세야 랜섬웨어 공격 등으로 미국의 주요 데이터가 유출된 것은 하드웨어나 소프트웨어에 대한 공급망 안전성 확보가 데이터 보안의 기본으로서 국가안보 차원의 과제가 되엇음을 여실히 보여주고 있다. 미국은 SolarWinds 제품을 사용한 18,000여 개의 연방 부처와 민간 기업 등의 시스템과 네트워크가 동 제품에 탑재된 악성코드에 의한 해킹 공격을 당하여 상당한 데이터가 유출되는 피해를 입었다. 이로 인해 미국 사회가 상당한 충격을 받았으며 보다 강력한 공급망 사이버안보 정책을 추진하고 있다.

바이든 미국 대통령은 2021년 5월 12일 "국가 사이버안보 향상 행정명령(Executive Order on Improving the Nation's Cybersecurity)"을 발동하였다.[35] 이 행정명령은 SolarWinds와 마이크로소프트 이메일 해킹 공격 및 콜로니얼 파이프라인 렌섬웨어 공격에

33) Eric Geller, "Biden orders federal cyber upgrade after barrage on hacks", *POLITICO* (2021. 5. 12), https://www.politico.com/news/2021/05/12/biden-federal-cyber-upgrade-hacks-487731(accessed: August 28, 2024)
34) 이석윤, 앞의 토론문, p.63.
35) The White House, *Executive Order on Improving the Nation's Cybersecurity*, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (검색일: 2022. 7. 22).

따른 연방정부 네트워크 보안과 소프트웨어 공급망에 대한 보안을 강화하기 위한 것이다. 동 행정명령은 침입 예방(preventing intrusion), 침입에 따른 영향력 최소화(사전 탐지)(minimizing impact of intrusion(pre-detection), 침입 탐지와 대응(detecting and responding intrusion), 침입에 따른 학습과 공유(Learning and disseminating) lessons from intrusion) 등으로 구성되어 있다. 동 행정명령은 1) 연방부서와 유관 기관의 개선 2) 정부에 소프트웨어를 판매하는 계약업자들의 필수 보안 기준 3) 정보침해 사례에 대한 보고서 작성과 기관조사에 적극적으로 협조할 것을 의무사항으로 하는 보안조치를 포함하고 있다.[36][37]

이 행정명령에 따라 미국 연방 정부부처는 데이터를 암호화하여야 하며 클라우드 호스팅 서비스의 안전한 사용에 대한 계획을 업데이트 하고, 다층 인증 체계를 구현하여야 한다.[38] 또한 연방 정부부처들은 잠재적 사이버공격을 탐지한 경우 경고를 발령하도록 하는 '종점탐지대응소프트웨어(endpoint detection and response software)'를 설치하여야 한다. 아울러 연방 정부부처들은 제로트러스트를 사용하여 자신들의 네트워크에 해커가 침입한 것으로 가정하고 해커들이 내부 시스템을 해집고 돌아다니지 못하도록 네트워크를 재설계하여야 한다. 또한 이 명령에 따라 연방 정부부처들은 아마존 웹 서비스(Amazon Web Services)와 같은 클라우드 서비스 보안인증제도(Federal Risk and Authorization Management Program: Fed RAMP)를 활성화하여 사이버안보를 강화하여야 한다. 또한 연방 클라우드 안보 전략을 제정하여 연방 부처들이 데이터를 안전하게 클라우드로 전송하도록 하여야 한다.

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

또한 이 행정명령은 항공기나 철도 및 차량의 충돌을 조사하는 '국가교통안전국(National

---

36) Robert Chesney and Trey Herr, "Everything You Need to Know about the New Executive Order on Cybersecurity", *LAWFARE* (2021. 05. 13), https://www.lawfareblog.com/everything-you-need-know-about-new-executive-order-cybersecurity (검색일: 2022. 7. 22).

37) Walter Haydock, "The Biden Administration's Impending Executive Order on Software Security", *LAWFARE* (2021. 04. 23), https://www.lawfareblog.com/biden-administrations-impending-executive-order-software-security (검색일: 2022. 7. 22).

38) Eric Geller, "Biden orders federal cyber upgrade after barrage on hacks", *POLITICO* (2021. 5. 12), https://www.politico.com/news/2021/05/12/biden-federal-cyber-upgrade-hacks-487731 (검색일: 2022. 7. 22).

Transportation Safety Board)'을 모델로 하여 사이버안보 관련 사고를 조사할 '사이버침해 사고조사단'을 설립하도록 하였다. 아울러 연방 정부와 거래하는 계약자(contractor)들에 대하여 데이터 유출시 보고하도록 하고 새로운 소프트웨어 보안 기준을 충족시키도록 하였다.

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

미 하원은 2021년 10월 20일 '2021년 국토안보부 소프트웨어 공급망 리스크 관리법안(DHS Software Supply Chain Risk Management Act of 2021)'을 가결하였다. 이 법안은 소프트웨어 공급망 위험 관리를 강화하는 것으로 바이든 대통령이 5월 12일 발표한 '국가 사이버안보 향상 행정명령'에 기초하고 있으며 솔라윈즈 사태과 같은 사고의 재발을 막는 것이 목적이다. 법안이 통과될 경우, DHS의 계약업체는 납품하려는 소프트웨어를 목록화한 소프트웨어 부품표(SBOM), 기존 취약성 대응 현황, 신규 취약성에 대한 대응 · 복구 계획 등을 의무적으로 제출하여야 한다.[39]

미국 바이든 대통령은 2022년 1월 19일 '국가안보, 국방 및 정보공동체의 서이버안보 향상을 위한 지침(Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems)'을 발령하였다. 이에 따라 국가안보국(NSA)의 장은 국가안보시스템에 대한 안정성 확보를 위하여 위 대통령 행정명령에서 정한 것 이상의 권한과 책임을 부여받는다. 동 지침은 국가안보시스템에 대해 연방정보시스템에 요구되는 사이버보안 요건과 동등하거나 그 이상의 요건을 확보하도록 규정하고, 국가안보시스템 고유의 필요성에 대처하기 위한 사항을 실행하도록 하고 있다. 이에 따라 국가안보시스템을 보유 또는 운용하는 각 부처의 장관은 이 지침 시행일로부터 60일 이내에 제로트러스트(Zero Trust) 아키텍처를 구축하여야 한다. 또한 90일 이내에 국가안보시스템의 클라우드 이행과 운용에 있어 최소한의 보안 기준과 관리 가이던스를 정립하고 공포하여야 한다.[40]

---

39) https://ritchietorres.house.gov/media/press-releases/rep-torres-software-dhs-supply-chain-risk-management-act-2021-passes-us-house (accessed: August 28, 2024).

40) https://www.whitehouse.gov/briefing-room/presidential-actions/2022/0

2. 데이터 이전 제한

데이터에 대한 지배력을 바탕으로 정보활동의 우위를 확보하기 위해서는 국가 간의 데이터 이전에 대해서도 정보기관 혹은 방첩기관이 관여할 수 있는 방안을 마련하여야 한다. 이러한 사실은 최근 미국의 사례를 통해 알 수 있다.

미국 바이든 대통령은 2024년 2월 28일 특정 국가로의 미국인의 개인 데이터와 민감한 정부 데이터가 거래되는 것을 제한하는 '우려 국가에 의한 민감한 대량의 미국인 데이터 및 미국 정부 관련 데이터의 접근 금지'에 관한 행정명령(EO 14117)을 발령하였다.[41] 이러한 데이터에 대한 우려국의 접근과 거래가 국가안보에 심각한 악영향을 미치고 있다고 판단하였기 때문이다. 바이든 정부는 이 행정명령이 미국 데이터 보안을 위한 가장 강력한 조치라고 설명하였다.[42] 아울러 우려국과의 데이터 거래로 인하여 심각한 개인정보 침해, 방첩활동 방해, 군사 및 정보기관에 대한 다량의 이메일 발송 등 국가안보 문제가 야기되고 있다고 지적하였다.

이 행정명령은 데이터 중개, 제3자 공급업체 계약, 고용 계약, 투자 계약 및 기타 계약이 대량의 미국인 민감 데이터에 대한 직접적이고 자유로운 접근을 제공하여 국가안보를 심각하게 위협하고 있다고 하였다. 따라서 법무부 장관으로 하여금 미국인의 데이터가 "우려 국가"로 대규모로 이전되는 것을 방지할 수 있는 권한을 부여하였다. 또한 연방 부처 및 기관에 대하여 민감한 개인 데이터"를 "우려 국가"로 전송하는 것을 억지하기 위하여 새로운 규칙과 규정 제정을 포함한 필요한 조치를 취하도록 하였다.

한편 미 법무부는 이 행정명령과 관련하여 발표한 규칙제안사전예고(Advance Notice of Proposed Rulemaking: ANPRM)를 통해 중국(홍콩 및 마카오 포함), 북한, 러시아, 쿠바, 이란, 베네수엘라 등을 '우려 국'으로 지정하는 것을 고려하고 있다고 하였다.[43] 이는 '정보

1/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/ (accessed: August 28, 2024).

41) Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern(Executive Order 14117 of February 28, 2024), https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related(accessed: August 28, 2024)

42) The White House, "FACT SHEET: President Biden Issues Executive Order to Protect Americans' Sensitive Personal Data," February 28, 2024.

43) ANPRM, p.36.

통신 기술 및 서비스 공급망 보안'에 관한 행정명령 13873호[44]의 실행을 위한 지침에서 지정한 우려국과 궤를 같이하고 있는 것으로 보인다.

법무부는 "고도로 민감한 데이터 거래"는 금지하는 반면에, 그 밖의 거래는 제한하되 "우려 국가"의 데이터 접근을 완화하기 위해 미리 규정된 특정 보안 요건을 준수하는 것을 조건으로 거래를 진행할 수 있도록 하는 2단계 접근 방식을 고려하고 있다.[45] 즉 법무부는 (1) 데이터 중개 거래, (2) 대량의 인간 게놈 데이터 또는 인간 게놈 데이터를 도출할 수 있는 인간 생체 표본의 전송과 관련된 거래 등에 대해서는 거래를 금지하고 있다.[46] 그러나 (1) 공급업체 계약(기술 서비스 계약 및 클라우드 서비스 계약 포함), (2) 고용 계약, (3) 투자 계약 등에 대해서는 제한적 거래를 고려하고 있다.[47] 이러한 제한적 거래의 경우 충족하여야 할 보안 요건에 대해서는 미 국토안보부의 사이버기반보호청(CISA)으로 하여금 정립하도록 하고 있다.[48]

민감 데이터 거래 금지에 관한 행정명령은 데이터에 대한 지배력을 강화하고 디지털 경제에서의 우위를 확보하고자 하는 미국 정부의 강력한 노력으로 보인다. 특히 미국 민감 데이터의 거래가 우려국에 의하여 미국에 대한 방첩 활동, 영향력 공작, 무력공격 및 사이버공격 등에 악용될 수 있다는 인식에 기초하여 이를 강력히 저지하고자 하는 의지로 보인다. 이는 사이버공간의 안정성 확보를 위한 바이든 정부의 공세적 사이버방어 활동의 일환으로 추진되고 있는 것으로 보인다. 즉 정보통신기술과 서비스의 국외 이전에 대한 규제, 5G네트워크 장비 공급업체 및 개방형 RAN 아키텍처, 해저 케이블 연결 면허 등에 대한 조사 활동 강화는 물론 2018년 외국인투자위험검토현대화법(Foreign Investment Risk Review Modernization Act of 2018) 및 2022년 CFIUS 행정명령[49]에 따라 확대된 법적 권한에 의하여 민감한 개인 데이터가 포함된 미국에 대한 투자에 관하여 CFIUS의 조사를 강화하는

---

44) Securing the Information and Communications Technology and Services Supply Chain(Executive Order 13873 of May 15, 2019).

45) ACT SHEET: Justice Department Will Issue Advance Notice of Proposed Rulemaking Following Forthcoming Groundbreaking Executive Order Addressing Access to Americans' Bulk Sensitive Personal Data by Countries of Concern, p.3.

46) ANPRM, p.11.

47) ANPRM, p.12.

48) ACT SHEET: Justice Department Will Issue Advance Notice of Proposed Rulemaking Following Forthcoming Groundbreaking Executive Order Addressing Access to Americans' Bulk Sensitive Personal Data by Countries of Concern, p.3.

49) Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/09/15/executive-order-on-ensuring-robust-consideration-of-evolving-national-security-risks-by-the-committee-on-foreign-investment-in-the-united-states/ (accessed: August 28, 2024).

조치 및 첨단 반도체에 대한 수출통제의 확대 등과도 관련된다고 할 것이다.

미국의 위 행정명령을 참고하여 민감한 데이터와 국가안보와 직결되는 데이터에 대한 지배력과 통제력을 확보할 수 있는 입법적 조치를 마련할 필요가 있다. 즉 데이터의 자유로운 흐름은 강조하되 국가안보 및 법집행 활동과 관련된 민감 데이터에 대한 통제권을 강화하면서도 프라이버시와 인권 보호의 조화를 위한 방안을 모색하여야 할 것으로 보인다. 또한 한미일과 중러북의 대립이 강화되고 있는 한반도 상황에서 우리의 데이터가 '우려 국가'로 대규모로 이전되는 것을 방지할 수 있는 강력한 입법적 조치도 고려할 필요가 있다.

3. 데이터 공작

디지털 전환과 초연결 사회에서 데이터 지배력을 확보하기 위해서는 자국에 유리한 데이터나 경쟁국이나 적성국에 불리한 데이터를 생성, 유통시킬 필요가 있다. 자국에 유리하고 경쟁국이나 적성국에 불리한 막대한 데이터가 생성되고 유통되면 특히 생성형 AI가 해답을 찾기 위하여 이러한 데이터를 이용한 해답을 찾을 수밖에 없고 이를 통해 조작된 데이터에 기반하여 경쟁국이나 적성국이 정책결정을 잘못하거나 오인 혼동을 일으킬 수 있기 때문이다.

생성형 AI의 경우 데이터의 정확성이나 편향성 등을 따지지 않고 학습 데이터에 의하여 결과를 도출하기 때문에 페이크 데이터, 편향 데이터, 오인된 데이터에 의해 학습된 AI는 오염된 결과의 데이터를 생성할 수밖에 없다.[50] 생성형 AI는 신뢰할 수 있는 것처럼 보이는 가짜뉴스나 허위조작정보를 생성하고 대규모로 유포할 수도 있다. 가짜뉴스나 허위조작정보는 사용자가 학습 데이터에 없는 정보를 요청할 때 생성될 가능성이 크다. 또한 사용자가 AI를 사용하여 부정확하거나 오해의 소지가 있는 텍스트를 의도적으로 빠르게 생성함으로써 가짜뉴스나 허위조작정보를 신속하게 확산시킬 수도 있다. 생성형 AI는 피싱 이메일을 생성할 수 있으며 소셜미디어에 사실과 매우 유사한 가짜뉴스나 허위조작정보가 게시되거나 포함되도록 할 수 있다. 또한 학습 데이터의 편향성에 기초하여 생성형 AI가 확증 편향된 정보와 데이터를 생성하도록 함으로써 가짜뉴스나 허위조작정보로 인한 피해를 증폭시킬 수 있다. 이와 같이 생성형 AI에 의한 가짜뉴스와 허위조작정보의 생성과 유통은 민주적 정당성을 침해

50) Laure Soulier, "Demystifying generative AI: true, false, uncertain", INSTITUT POLYTECHNIQUE DE PARIS(February 7, 2024), https://www.polytechnique-insights.com/en/columns/science/demystifying-generative-ai-true-false-uncertain/(accessed: August 28, 2024)

할 수도 있다. 시카고대학교 피어슨 연구소의 여론조사에 따르면 정치적 성향에 관계없이 미국 성인의 91%는 가짜뉴스가 문제라고 생각하며, 50% 정도는 가짜뉴스의 유통을 우려하는 것으로 조사되었다.[51] 미국에서는 선거 부정 의혹과 관련된 가짜뉴스가 유포되면서 민주주의 제도 자체에 대한 대중의 불신을 초래하였다. CNN이 실시한 여론조사에 따르면 응답자의 56%는 선거가 민의를 대표한다고 점을 전혀 신뢰할 수 없다고 하였다.[52] 따라서 정치적 영향력 행사를 위하여 생성형 AI를 이용해 가짜뉴스나 허위조작정보를 유포하여 저렴하고 신속하게 원하는 방향으로 정치적 여론을 유도하고자 하는 시도들이 증가하고 있다.

한편 대규모 언어 모델(LLM)을 기반으로 하는 현재의 생성형 AI는 본질적으로 지식에 한계가 있으며, 대답을 찾지 못하는 경우 그에 상응하는 무언가를 생성해 낸다. 이러한 현상을 소위 '환각(hallucinating)'이라고 하는데, 이는 생성형 AI의 발전이 초래한 의도치 않은 결과이다. 생성형 AI의 발전은 이러한 환각이 조작되어 급속하게 유포될 가능성을 내포하고 있다. 호주의 한 시장은 자신이 실제로는 사건의 내부고발자였는데도 ChatGPT가 자신을 뇌물수수 혐의로 수감되었다고 결과를 생성함으로써 심각한 명예훼손을 일으킨 사건은 이러한 환각을 보여주는 전형적인 실례라 할 수 있다.[53]

따라서 이 학습 데이터를 오염시켜 특정 국가에 유리한 영향력이 발휘되도록 하는 데이터 공작이 가능하게 된다. 데이터 공작에 공세적으로 대응하기 위한 데이터 정보활동에 대해서도 관심이 필요할 것으로 보인다.

Ⅴ. 결론

정보통신 기술의 발전과 초연결 시대의 등장은 인간 생활영역을 극지와 심해, 우주와 사이버 등으로 확장시키면서 새로운 위험을 탄생시켰다. 이러한 새로운 위협에 대응하여 국력을 신장시키고 국민의 생활과 번영을 담보하며 국가의 가치를 확산하기 위해서는 정보 패러

51) https://news.uchicago.edu/story/nearly-all-adults-think-misinformation-increasing-extreme-political-views-and-behaviors (accessed: August 28, 2024)

52) Gabriel R. Sanchez and "Keesha Middlemass, Misinformation is eroding the public's confidence in democracy", BROOKINGS(July 26, 2022).

53) Byron Kaye, "Australian mayor readies world's first defamation lawsuit over ChatGPT content", REUTERS(April 6, 2023), https://www.reuters.com/technology/australian-mayor-readies-worlds-first-defamation-lawsuit-over-chatgpt-content-2023-04-05/(accessed: August 28, 2024)

다임의 변화가 요구되고 있다. 특히 디지털 전환과 초연결 사회의 등장으로 변화하고 있는 정보환경 하에서, 정보기관은 데이터의 수집, 분석, 공유에서의 경쟁력을 확보하고 민간기업과의 데이터 협력을 통해 데이터 지배력을 강화하여야 한다.

정보기관이 정보화와 지구화 및 비대면 사회에 적응하여 경쟁력을 확보하기 위해서는 디지털 전환을 실현하는 동시에 인간정보(HUMINT), 과학정보(TECHINT) 및 공개출처정보(OSINT) 사이의 유기적인 협력과 상호보완적인 관계를 구축 · 운영하여야 한다. 그런데 이러한 다양한 정보활동의 대상인 동시에 수단이 되면서도 그 협력과 상호보완성의 교차점에 데이터 정보활동(DATINT)이 자리잡고 있다고 볼 수 있다. 이러한 정보활동의 수행으로 구축되는 결과가 데이터이며 이러한 정보활동이 대상으로 하는 것이 정확한 데이터를 적시에 확보하는 것이기 때문이다. 또한 이들 정보활동으로 생성된 데이터를 상호 비교 보완함으로써 더욱 가치가 있는 새로운 데이터 또한 생산할 수 있기 때문이다.

데이터 안보를 위한 정보활동(DATINT)은 크게 데이터의 처리에 기초한 수집 · 분석 · 공유 활동과 데이터 지배력 강화를 위한 데이터 보호 활동 및 데이터 공작 활동으로 나누어 볼 수 있다. 정보의 처리 과정에 따른 데이터에 대한 수집 · 분석 · 공유 활동은 국내외 각종 데이터베이스, 오픈 소스 등을 대상으로 한다. 데이터 수집 활동은 컴퓨터 네트워크 탐사(CNE), 사이버공격(cyber attack), 인공위성과 드론, 공개출처정보 정보활동 등을 통하여 이루어진다.

정보기관은 컴퓨터 네트워크 탐사(CNE) 활동을 통해 정보활동의 표적인 컴퓨터 네트워크에 침입하여 데이터를 수집하거나 탈취하는 데이터 정보활동을 수행하고 있는 것으로 알려져 있다. CNE는 ①표적 대상인 컴퓨터 시스템으로부터 직접 데이터를 취득하는 활동(collection activities)과 ② 표적 대상인 컴퓨터 시스템에 대한 접근 권한을 획득해 필요한 정보를 수집하는 활동(enabling activities)으로 구분된다.

정보기관은 생성형 AI를 이용한 사이버공격을 통해 데이터를 수집할 수도 있다. 사이버공격자들은 생성형 AI 코드를 재작성하여 사이버공격에 대한 추적을 곤란하게 할 수 있다. 또한 컴퓨터 프로그래밍 기술이 부족한 공격자라 하더라도 생성형 AI 시스템을 활용하여 보다 효과적인 사이버공격을 위한 코드를 생성할 수 있다.

정보기관은 인공위성이나 정찰기 혹은 드론 등을 이용하여 데이터 정보활동을 수행하고 있다. 우주와 공중으로부터 영상과 이미지 데이터를 수집하고 분석하여 공유하는 것이다.

공개출처정보(Open Source) 정보활동(OSINT)은 국가안보, 기업 경쟁력 향상, 연구개발과 기술력 우위, 법질서 유지, 언론 보도 등을 위해 사용 가능한 모든 공개정보를 활용하여

데이터를 수집, 분석, 공유하는 것을 의미한다. 정보화와 지구화의 영향으로 공개정보의 양이 기하급수적으로 증가함에 따라 그 중요성을 더하고 있다. 공개출처정보 활동의 대상인 데이터의 폭발적인 증가는 민관협력을 통한 해당 정보활동의 수행이 요구되고 있다.

인공지능 기술의 발전은 정보분석관의 데이터 분석에 필요한 수고와 시간 및 비용을 절감시키고 있다. 방대한 데이터를 수집하고 분석하여 유의미한 정보를 추출하고 공유함으로써 정보우위를 확립하는 것이 데이터인텔리전스의 핵심이다. 다양한 정보활동을 통해 방대한 양의 데이터를 수집, 분석, 공유하기 위해서는 인공지능을 사용하지 않을 수 없다고 하더라도 기존 분석관의 활동과 균형을 찾는 방안을 실행하는 것이 중요하다. 분석된 정보는 정보기관 내부, 정보기관 상호 간, 정보기관과 민간기업, 국외 정보기관 등과 공유하는 것도 중요하다.

이와 같이 수집 · 분석 · 공유된 데이터를 어떻게 보호할 것인지가 데이터 지배력 강화를 위한 정보활동의 중요한 한 축이라고 할 것이다. 데이터 보안 활동은 사이버안보 활동과 상당 부분 중첩된다고 할 수 있다. 네트워크 보안 강화를 위해서는 망분리 정책의 한계를 극복하고 클라우드 환경에서 데이터 보안과 활용을 확대할 수 있는 제로트러스트로의 데이터 보안의 패러다임을 전환할 필요가 있다. 데이터 보안을 위한 기존 암호 기술은 복호화 과정에서의 취약성으로 인하여 한계를 보이고 있다. 따라서 동형암호, 기밀컴퓨팅 활용시 서버에서 암호화된 상태로 데이터를 연산하거나 CPU와 메모리를 공유하는 클라우드 환경에서 하드웨어 내 안전한 실행공간을 마련할 필요가 있다. 네트워크 보안과 암호 정책을 통해 데이터 보안을 강화하더라도, 정보통신(ICT) 및 사이버안보 관련 하드웨어나 소프트웨어에 대한 공급망 안전성을 강화하여야 데이터에 대한 지배력을 확보할 수 있다.

한편 데이터에 대한 지배력을 바탕으로 정보활동의 우위를 확보하기 위해서는 국가 간의 데이터 이전에 대해서도 정보기관이 관여할 수 있는 방안을 마련할 필요가 있다. 마지막으로 디지털 전환과 초연결 사회에서 데이터 지배력을 확보하기 위해서는 자국에 유리한 데이터나 경쟁국이나 적성국에 불리한 데이터를 생성, 유통시킬 필요가 있다.