국가전략연구위원회 이슈브리핑 25호 (발간일: 2024.5.5.)

# 미 정보공동체의 데이터 기반 인텔리전스와 시사점[1)]

조경환 (성균관대학교)

## Ⅰ. 들어가며

"세계는 빠르게 변화하고 있다. 그런데 그 빠른 변화는 대부분은 과학과 기술에 기인한다." 노벨 물리학상을 수상한 스티븐 추 전 미국 에너지부 장관이 2023년 9월 어느 만찬 강연에서 한 말이다.

초경쟁적이며, 데이터에 기반한 디지털 시대에 다종다양한 디바이스들, 센서들, 사람들 사이의 데이터와 연결성의 기술적 폭발은 혁신을 가져왔다. 기술이 혁신을 추동(technology-push)하고, 수요가 또한 그 혁신을 견인(demand-led)한다(Miles & Rigby, 2013). 뉴밀레니엄에 즈음해 급격히 확장된 과학기술은 네트워크 시대[2)]를 열었다. 모든 출처의 데이터는[3)] 그것이 고전적인 정형 데이터이든 신흥의 비정형 데이터이든 다 디지털화하여 컴퓨터와 전자기기에 저장되고 유통된다. 디지털 흔적(digital trace)은 기하급수적으로 늘어난다. 데이터의 양(volume)과 다양성(variety)의 급속한(velocity) 증가는 빅데이터를 가져

1) 이 글은 2024년 5월 2일 제9차 사이버 국가전략 포럼에서 발표된 발표문을 수정보완한 것이다.
2) 1990년 12월 World Wide Web이 발표되고 보급이 된 이래, 1998년 9월 구글이 창립됨. 2006년 10월 유투브를 인수했음. 2004년 2월에는 페이스북이 창업했음. 2007년 애플의 아이폰이 데뷔했으며 2010년 삼성 갤럭시S가 출시되어 스마트폰의 대대적 보급이 이루어졌음
3) 모든 소스(all sources) 데이터는 인간정보(HUMINT), 과학기술정보(TECHINT), 공개정보(OSINT) 등 모든 정보 기법을 통해 수집되어, 처리되지 않고, 정제되지 않은 생 자료들의 조각들 및 부분들로 정의됨. 그것이 체로 걸러지고 나서야 비로소 정보 혹은 실행 가능한 지식이 됨(Falode, 2021: 72)

왔다. 이는 증거에 기초한 사고(reasoning)와 데이터 기반의 정보를 요구한다. 정책결정자에게 더 나은 이점을 제공한다.

한편, 정보환경의 복잡성과 변동성은 그 어느 때보다 커졌다. 디지털 신기술과 시스템은 혁신을 만들어내는 동시에 위협을 촉발하고 데이터 안보를 부른다. 사이버 공격에 대한 취약성을 내포한다. 미 중앙정보국(CIA)의 AI 책임자인 라만(Lakshmi Raman)은 2023년 9월 폴리티코와 인터뷰에서 "새로운 기술은 가장 큰 위협이자 자원"이라고 했다. 적대세력은 강력한 새 도구들을 가지고 혼란하게 한다. 속이고 회피하며 염탐한다. 주요 디지털 데이터를 절취, 파괴, 오염, 조작한다. 영향을 행사한다. 우리가 직면한 가장 중대한 위협은 이제 디지털 도메인에 있다.

그렇지만, 진보하는 과학기술도, 데이터 쓰나미(tsunami)도, 거대한 양의 오픈소스와 비밀리 획득한 정보를 소화해 내는 AI도 그 과잉에 압도될 것만은 아니다. 인텔리전스[4]의 본질에는 변함이 없다. 국가의 개입이 무한정일 수는 없다. 지켜야 할 데이터는 국가가 보호하고 있는 데이터로 한정되어야 할 것이다. 개인의 영역과 프라이버시는 그대로 보장이 되어야 한다. 스파이 행위는 여전히 인간과 기술 사이에 상호작용한다. 오직 인간만이 수집할 수 있고, 인간만이 수행할 수 있는 비밀공작은 계속해서 비밀의 영역에 남아 있을 것이다. 신흥기술과 인간을 통합하고 엮어내야 한다. 이것 역시 과학기술에 달려 있다.

이 연구에서는 미국 정보공동체(IC: Intelligence Community)의 18개 정보기관이 어떻게 데이터 기반의 정보혁신을 이루어가는지, 데이터와 그 분석가들은 어떻게 의사결정자와 기술을 통합하고 과학과 인간 간의 갭(gap)을 메워가는지, 또한, 그에 파생되어 국가안보를 위협하는 도전요인들을 어떻게 관리해 가는지를 살펴본다. 그리고 그 함의와 실행 가능한 지식(actionable knowledge)을 도출해 보고자 한다.

## Ⅱ. 새로운 스파이전쟁

### 1. 정보 전장이 된 디지털 도메인

냉전은 결코 끝나지 않았다. 디지털 독재국가들이 자국 사회를 모니터하고 통제하기 위해 개발한 데이터 분석과 AI 능력은 이제 서방국가들을 겨루는 화살이고 단검이다.

중국과 러시아 정보기관들의 사이버 간첩(cyber espionage)은 사이버 공격하여 물리적으로 파괴거나 시스템의 교란을 노린다. 데이터와 지식자산을 절취한다(김상배, 2020:13).

4) 인텔리전스의 개념은 그 개념을 현상 수배할 정도로 많음. 로웬탈(Mark M. Lowenthal)이 정의한 실무적 개념(a working concept)을 보면, 인텔리전스는 "국가안보에 중요한 특정 유형의 첩보들이 요구, 수집, 분석되어 정책결정자에게 제공되는 과정임. 이러한 과정의 생산물을 의미하기도 함. 그리고 이러한 과정과 첩보를 보호하는 방첩을 뜻하기도 함. 마지막으로 합법적인 권위체가 요청한 공작의 수행"을 의미하기도 함(김계동 옮김, 2008:12)

2014년 3월 러시아는 우크라이나의 크림반도 점령 과정에서 사이버상의 데이터 절도 및 이를 조작하는 사이버 간첩 활동을 위주로 했다(김상배, 2020:14). 푸틴의 연방보안국(FSB)과 해외정보국(SVR), 군사정보국(GRU)은 서방의 선거에 개입하여 민주주의의 근간을 흔든다. 규칙 기반의 국제질서를 훼손한다. 2016년 미국 대통령선거 개입이 대표적이다. 금년 11월 미 대선도 영향권 내 있다. 시진핑의 국가안전부(MSS)는 2005년 미 정보기관과의 전쟁을 선포했다. 그 이후 최고의 자원과 정보관들을 미 정부와 기업 쪽에 투입한다. 과학 및 기술 비밀 데이터를 훔쳐서 중국의 경제와 군사력을 지탱한다. 중국의 개인 정보 및 지식자산 절취는 체계적이며 산업적 규모이다. 통제가 안 되는 청부업자를 고용하는 식의 해커 생태계를 운용한다(THE CIPHER BRIEF, 2024-1-22).

'철의 장막'은 종언을 고하지 않았다. 과학기술의 장막으로 대체되었다. 물리적 침투는 사이버공간의 침투로 전환됐다. 일례로, 1956년 4월 소련 국가안보위원회(KGB)와 동독 요원들이 CIA가 영국 비밀정보국(MI6)의 협조를 받아 도청을 위해 베를린 거리의 지하에 뚫은 터널을[5] 발견하고 달려왔을 때, 당시 CIA 거점장은 기관총을 겨눈 채 "이 선을 넘으면 미국 관할구역"이라며 허가받지 않은 사람의 진입을 막았다. 현재의 거점장들은 적의 네트워크 침투를 차단하기 위한 노력의 일환으로 자신들의 맥북(MacBook)에 가상사설네트워크(VPN; Virtual Private Network)를 설치해서 IP 추적을 피하고 있다(THE CIPHER BRIEF, 2024-1-22).

테킨트에 의한 데이터의 수집, 처리와 분석은 '양날의 검'이다. 인텔리전스와 방첩(counterintelligence)에 똑같이 이점을 주기 때문이다. 2023년 10월7일 이스라엘이 가자지구 팔레스타인 무장 정파인 하마스의 기습을[6] 받은 것은 과학기술 과신이 초래한 일면이 있다. 상당 규모의 공격 준비는 이스라엘과 미, 영 등 서방의 위성, 신호정보 및 정교한 사이버 기술로 사전에 대부분 탐지된다고 인식하고 있었다. 이스라엘은 하마스를 과소평가했다. 하마스는 그 오인식과 분석관의 상상력 결핍을 파고들었다. 또한, 이란으로부터 사이버 기술을 지원받고 있는 하마스는 공격 의도를 숨기기 위해 철저하게 은닉했고 기만했다. 하마스가 방첩에 성공한 셈이다(조경환, 2023).

소셜 네트워크들은 CIA에게 엄청난 양의 새로운 정보를 주고 있다. 반면에, 거대한 새로운 약점에 노출된다. 디지털 흔적은 정보 타깃을 찾아내기도 하지만, CIA 공작관의 인원 보안을 막는다. 비밀공작을 더 어렵게 한다. AI와 생체 데이터 활용은 흔해졌다. 스마트 도시의 모든 거리에는 비디오카메라가 있다. 거대 카메라 네트워크는 공작관들의 모든 움직임

5) 작전명 "Operation Gold", 미 CIA와 영 MI6는 베를린 칼쇼스트(Karlshorst)에 있는 소련 공군사령부로 들어가는 전화 및 전신선을 도청하기 위해 1951년 터널을 팠음. 지하 6m에 직경 2m, 길이 450m임. 소련은 이중 공작원인 MI6의 블레이크(George Blake)를 통해 이 터널의 존재를 알고 있었으면서도 그를 보호하기 위해 지켜보다가, 1956년 4월21일 우연을 가장해 발견하여 전 세계에 알렸음(Shulsky & Schmit, 신유섭 옮김, 2007: 254-255)

6) 10월7일 유대인의 안식일 오전 6시30분, 가자지구의 팔레스타인 무장 정파인 하마스가 이스라엘에 침투해 수 시간을 광란했음. 양민 1400명 이상과 무방비 군인이 폭사하고 처참히 살해됐음. 220명 넘게 인질로 잡혔음. 이스라엘판 9·11이자, 홀로코스트 이후 최악의 유대인 학살임(조경환, 2023). 이는 이스라엘의 반격으로 이어져 현재 7개월째 전쟁을 이어가고 있음.

을 추적한다. 얼굴인식 기술은 갈수록 보편화한다. 공항의 얼굴 스캐닝은 스파이들이 얼굴을 노출 않고 국경을 드나들기 어렵게 만들었다. 디지털 흔적은 남겨도 문제가 되고, 없어도 의심을 받는다. 빅데이터 마이닝은 공작관들의 활동 패턴을 포착한다.

"뉴욕 타임즈의 보도에 의하면, 2010년 중국 내에 있는 CIA의 가장 중요한 네트워크가 와해했다. 18-20명의 미국 소스들이 살해되거나 투옥되었다. 지금 10년 넘게 지났지만, CIA는 그때의 손실을 회복하지 못하고 있다"(Walton, 2023).

2014년 중국 해커들이 미국 성인의 10%의 개인 정보를 훔쳤다는 주장도 있다(Neale, 2019). 크렘린은 지금도 승진, 보수, 생체 데이터와 같은 디지털 실마리들을 이용하여 CIA 협조자들의 신원을 꼭 집어내고 있다.

## 2. 미·중·러의 데이터 안보 각축

중국과 러시아의 데이터 이전에 대한 강력한 국가 통제, 그리고 무차별적 데이터 절취, 파괴와 오염, 영향 행사와 조작 시도는 데이터의 자유로운 이동을 보장해 왔던 미 데이터 정책의 전환을 가져왔다. 맞대응 책이 속속 나오고 있다.

중국은 2008년 도입된 정보보안등급보호규정(MLPS: Multi-Level Protection Scheme), 2016년 인터넷안전법 제정, 그리고 2019년 본격 시행한 사이버안보법(CSL: Chinese Cybersecurity Law) 등의 법제를 갖추어 네트워크 탐지와 데이터 보안을 강화하고 있다. 공안부(MPS: Ministry of Public Security)와 국가안전부(MSS: Ministry of State Security)가 주축이다. 국가인터넷정보판공실(Cyberspace Administration of China)은 데이터 현지화(data localization)를 지탱한다. 데이터의 보안성을 평가해 외부유출의 흐름, 국가 간 데이터의 이전을 통제한다. 2020년 시행된 외국투자법(Foreign Investment Law)는 외국인 투자기업의 특별 지위를 없앴다. 2023년 7월1일 발효된 개정 반간첩법은 다국적 기업들에 대한 데이터 규제를 대폭 강화했다. 데이터 디커플링이다. 또한, 시진핑 주석의 집권 초기인 2014년에 나온 "사이버공간에서 국가의 입장과 주장을 밖으로 널리 알리며, 이를 듣는 사람이 많아져야 사람들이 따르게 된다"는 주장은(김진형, 2022) 대외 영향공작 및 샤프 파워(sharp powers)의[7] 본격화를 예고했다.

러시아도 2019년 11월1일 인터넷주권법(sovereign internet law)을 발효시켰다. 러시아만의 독자 인터넷망 구축을 합법화했다. 데이터의 국외 이전을 국가안보 목적으로 통제해 오고 있다.

미국은 "자유, 프라이버시, 자유로운 정보의 흐름" 보장을 사이버 안보(채재병·김일기, 2020)와 데이터 안보정책의 근본으로 한다. 그렇지만 이를 재고하고 있다. 중국이 미국의 개

7) '샤프 파워'는 미 비영리 싱크탱크인 '민주주의기금'(NED: National Endowment for Democracy)이 제시한 개념임. 권위주의 정부가 다른 나라의 내정에 알게 모르게 영향을 미치는 전략임. 음성자금, 유인, 매수, 강압 등 탈법 수단과 허위정보를 동원해 상대를 강제함. 상대의 정치체제, 사회제도, 가치 등의 신뢰를 저해하고 혼란과 분열을 조장하며, 체제를 부정하는 것이 목적임(심종현·제성훈, 2022)

인 정보 등 데이터에 무단 접근해 국가안보와 프라이버시를 위협하는 것을 묵과하지 않을 태세이다. 2021년 6월 행정명령 제14034호는[8] "외국의 적으로부터 미국인들의 민감 데이터를 보호하는 조치를 담았다. 2022년 9월 행정명령 제14083호는[9] 외국인의 대미 투자에 대한 미 국가안보 영향 평가를 강화했다(박주희, 2024).

2022년 10월 발효된 행정명령 제14086호는[10] 신호정보 활동에 대한 미국민, 동맹·파트너 국민의 개인 정보와 시민 자유 보호를 강화하려는 조치이다. 1년 내에 법무부장관, DNI의 시민자유보호관[11](CLPO: Civil Liberties Protection Officer), 그리고 '개인 정보·시민 자유 감시이사회'(PCLOB: Privacy and Civil Liberties Oversight Board)의 자문 아래 정책과 절차를 업데이트해 가게 했다. 또한, 법무부 장관에게 60일 내에 개인정보보호평가법원(DPRC: Data Protection Review Court) 창설을 위한 규정을 공포하라고 했다. DPRC는 2023년 10월 만들어졌고, 개인 정보 이전 및 보호를 관리, 감독할 시스템을 갖추게 되었다.

2024년 2월 미국민의 민감 개인 정보를 국가안보 차원에서 보호하기 위한 행정명령 제14117호[12]가 공표됐다. 유전자 데이터, 생체인식 데이터, 개인 건강 데이터, 지리 위치 데이터, 금융 데이터 그리고 개인적인 신원을 추적할 수 있는 데이터를 포함하여 미국인의 가장 개인적이고 민감한 정보에 초점을 맞추어 우려국들에게 판매, 대량 전송되어 착취되는 것을 방지하려고 한다.

## Ⅲ. 미 IC의 디지털 정보환경과 데이터 전략

### 1. 진전된 기술과 의사결정, 의사결정 정보와 데이터 사이언스의 융합

의사결정 과정은 해가 다르게 그 복잡성을 더해 간다. 코로나-19 팬데믹, 나날이 현실화하는 기후변화, 미중 전략경쟁의 장기화 및 2022년 2월 러시아의 우크라이나 침공과 같은 지정학적 변동성의 증대는 '좋은 의사결정'(a good decision making)의 어려움을 가중한다. 불확실성은 커지고 미래는 흐릿하다. 정책의 효과는 잘 보이지 않는다. 원인과 결과의 체인은 길어진다. 데이터의 소스는 휴민트와 테킨트를 망라하여 다양하며, 통합을 요구한다(Pratt

8) Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries, June 09, 2021
9) Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States, September 15, 2022
10) Executive Order on Enhancing Safeguards For United States Signal Intelligence Activities, October 07, 2022
11) CLPO는 2004년 정보개혁 및 테러방지법(Intelligence Reform and Terrorism Prevention Act of 2004)에 의해 프라이버시와 시민 자유 보호를 위해 설립된 직위임. CLPT(Civil Liberties, Privacy and Transparency) 사무실 운영 책임자이며 DNI에 직보함(ODNI 홈페이지, 2024-4.16 검색)
12) Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, FEBRUARY 28, 2024

et al., 2023). 이러한 도전요인들은 데이터에 기반한 의사결정과 데이터 사이언스에 눈을 돌리게 한다.

AI의 도움을 받는 인간의 의사결정 프로세스는 그 숫자가 늘어나고 있다. 모든 데이터가 평등하지는 않다. 가치 있는 데이터는 한정되어 있다. 10%의 데이터가 90%의 전략적 가치를 지닌다(Pratt, 2015). AI와 빅데이터 분석은 방대한 '노이즈'와 유가치의 '시그널'을 분간해 낸다. 이미지를 분류하고 서류를 대조하며, 데이터에서 트렌드를 발견하여 예측한다. AI가 사람의 분석을 대체하지는 못한다고 하더라도 이미 그 생물학적 뇌의 분석력을 돕고 있다.

그렇지만, 데이터만으로는 전략을 넓게 설명하지 못한다. 인간 의사결정에 관한 카너먼의 주장(Kahneman, 2011)을 고려하면, AI는 빠르고 직관적이며 자동적인 "시스템1"에 강하다. 느리고 분석적인 "시스템2"는 인간의 몫으로 남게 된다. 컴퓨팅과 AI는 인간의 능력으로는 도저히 해낼 수 없는 매머드의 복잡한 데이터를 수집하고 분석하여 인간의 판단에 편의를 제공한다. 그래도 '요구와 계획, 수집, 처리와 분석, 배포와 피드백'의 전 정보과정에서 질적인 측면의 비중은 여전히 높다. 결국, 인간과 AI가 콤비를 이루어 복잡한 상황에서의 의사결정을 도울 증강된 솔루션을 내놓아야 한다(Pratt et al., 2023).

## 2. 미 IC의 '2023-2025 데이터 전략': 데이터 기반(data-driven)의 미래

"우리가 하는 모든 것은 데이터로 시작한다." 국가정보장(DNI: Director of National Intelligence)은 데이터 및 그 데이터를 적절하게 다루는 능력을 점증하는 복잡성과 상호 연결된 글로벌 안보환경에서 미 IC의 강점을 유지하는 펀더멘털로 간주한다.

IC의 데이터 전략은 임무와 비전, 가치로 구성된다. 임무로는 IC 데이터의 발견, 접근과 사용의 안전을 보장하여 빠르고 광범하게 가치와 통찰을 제공한다. 미 정부, 외국 파트너국들과 민간영역, 학계에 걸쳐서 데이터의 상호교환이 가능하고 검색할 수 있게 하여 의사결정을 돕고, 실행 가능한 정보를 보장한다. 정책결정자에게 늘 변화하는 도전요인들을 인지하고 그 결정을 하게 한다. <그림1>은 IC의 2023-2025년 데이터 전략도이다(DNI, 2023).

**<그림1> IC의 2023-2025년 데이터 전략도**


출처: The IC Data Strategy 2023-2025, 2023, DNI

미 IC는 데이터 기반의 IC를 최적화하고, 상호 정보교환, 공유, 파트너십, 혁신, 프라버시와 시민자유권 보호를 가치로 하여 4개 전략적 영역에 집중한다. 첫째는 E2E(End-to-End) 데이터 관리를[13] 한다. 둘째, 데이터의 상호 정보교환과 분석을 신속, 광범하게 전달한다. 셋째, 계속적인 디지털 및 데이터 혁신을 위해 모든 파트너십을 진전한다. 넷째, IC 인력을 데이터 기반으로 전환한다.

이를 위해 DNI는 IC의 최고데이터정보관(IC CDO: Chief Data Officer)과 IC의 최고데이터정보관위원회(IC CDOC: Chief Data Officer Council)를 두고 있다. 이들은 IC의 직업적 윤리원칙을 강화하면서도, 데이터의 수송, 섭취, 큐레이션[14], 활용, 확산, 배포, 공유, 데이터의 사용 향상, 인력 개발 등 IC가 취할 전략적 단계를 확인하며, 데이터 기반의 디지털 혁신을 추진하고 있다.

물론 IC의 데이터 전략이 순탄치만은 않을 것이다. IC 내의 각 정보기관이 가지고 있는 오랜 독자성과 신비주의, 강력한 조직 및 직무 보안, 그리고 각 기관 내부에 잠재되어 있을 정통적 수집과 분석의 방식을 신뢰하는 관료제의 저항에다 칸막이문화(compartmentalization)는 극복해야 할 과제이다.

## Ⅳ. 미 IC의 데이터 기반 인텔리전스

13) E2E(End-to-End) 데이터 관리는 데이터의 전체 수명주기를 포괄하는 접근 방식임. 데이터가 생성되고 수집되는 시점부터 분석, 저장, 공유, 보호, 소멸 또는 보관 등 여러 단계를 거쳐 배포와 상호교환 등 최종적으로 사용되는 시점까지의 모든 과정을 포함함(The IC Data Strategy 2023-2025, 2023:1).
14) 데이터 큐레이션은 데이터를 수집, 정리, 구성하고 관리하여 그 가치를 최대화하는 과정임. 데이터의 품질을 향상하고 의미 있는 정보를 도출하기 위해 데이터를 선택, 정제, 구조화하는 것을 포함함. 데이터의 신뢰성을 보장하고 유용한 인사이트를 얻기 위한 작업임

## 1. IC의 신기술, 데이터 기반의 연구개발

2005년 3월 WMD 위원회는[15] 미 IC의 '이라크 WMD 능력과 그 의도에 대한 수집 무능력과 연속적인 분석 실패'를 주요 정보실패(a major intelligence failure)로 규정했다. 그 처방의 하나로서 신기술에 수용적이어야 한다고 권고했다(The WMD Commission, 2005).

오바마 행정부는 빅데이터를 국가 어젠다로 다루었다. 2014년 3월 백악관은 빅데이터 시대의 기회를 포착하되, 프라이버시 가치는 보전한다는 내용의 보고서를 냈다(Executive Office of the President, 2014).

미 IC의 연구개발은 데이터와 네트워크에 집중한다. ODNI국가정보장실 산하에 2006년 신설된 '정보 고등연구계획활동'(IARPA: The Intelligence Advanced Research Projects Activity)은 AI를 통한 혁신 작업, 양자컴퓨팅의 적용 지원, 머신러닝 향상, 최첨단의 합성 생물학의 4개 분야에 '고리스크, 고성과'의 연구프로그램에 투자하고 있다. 기습 등 갑작스러운 위험 예상, 데이터 세트들의 다이내믹스로부터 통찰을 극대화하는 분석, 스마트한 수집, 그리고 위협 감지, 퀀텀 컴퓨팅을 통한 안전한 공작이 핵심 연구영역이다. IC 내 정보기관들 및 산, 학과의 협력에 무게 중심을 둔다. 공개정보를 주로 다룬다(Jani, 2016). 공작 혹은 기술을 현장에 직접 적용하지는 않으며, IC 인텔리전스의 효율 증진을 돕는다.

IARPA는 분석연구와 수집 연구부서가 있다. 분석연구에서는 대량의 분산되고, 신뢰할 수 없는, 동적인 데이터로부터 적기에 통찰을 도출한다. 수집 연구는 새 센서 및 전송 기술을 개발하여 모든 출처 데이터의 가치를 최대한 향상한다. 원하는 정보를 더 정확하게 하는 새 수집 기술, 이전에 접근 불가능했던 출처에서 정보를 수집하는 수단을 개발한다. 또한, IARPA는 여러 출처에서 수집된 데이터를 결합하여 수집 정보의 품질, 신뢰성 및 유효성을 향상하는 메커니즘을 추구하고 있다(IARPA 홈페이지, 2024-4-12 검색).

전장에서의 빅데이터는 군사정보의 개념을 다시 쓰고 있다. 기업과 정보기관들의 증강하는 분석력은 소비자 데이터를 효과적으로 수집, 분석하여 인싸이트를 도출함으로써 현대전에 패러다임 전환을 가져온다. 2012년 3월 패네타(Leon E. Panetta 11.7-13.2) 당시 미 국방장관은 '국방전략리뷰'(National Defense: Defense Strategic Review)를 개관하면서 위성 이미지 정보(IMINT)와 드론 획득 비디오, 텍스트 파일에 이르기까지 광범한 센서 네트워크 사용에 우선순위를 두었다. 전장에서의 시간은 사느냐, 죽느냐의 문제다. 거대 데이터를 신속히 수집, 분석하여 행동 가능한 정보로 전환하는 것은 사활적이다.

1597년 10월 소련의 스푸트니크 1호 위성 성공에 충격을 받아 창설된 미 펜타곤 산

15) The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction은 2004년 2월 조지 W. 부시 대통령의 행정명령 제13328호에 의해 설립된 초당적 위원회(공동위원장 2명, 위원 8명)임. 외국의 WMD 사용 혹은 잠재적, 위협적 사용과 관련 그 능력, 의도와 활동에 관한 미 IC의 능력과 도전을 조사했음. 2005년 3월 31일 "DNI 권한 강화, FBI의 국내정보 기능 제도화" 등을 권고했음(The WMD Commission, 2005, Report to the President of the US).

하 DAPRA(Defense Advanced Research Projests Agency) 방위고등연구계획국는 아프간 전쟁2001-2021년에 데이터 분석 및 시각화 전문팀을 보냈다. 위성 및 감시 장비로 수집한 자료들을 융합해서 전장의 도로망과 교통의 흐름을 시각화해 폭발물의 위치를 파악한 뒤 폭파, 처리했다(Executive Office of the President, 2014).

국토안보부 과학기술국(DHS S&T; Science and Technology directorate) 산하 CVADA(Center for Visualization and Data Analytics)는 2009년 창설되었다. 빅데이터 시각화 및 컴퓨터 그래픽, 데이터 분석학 등 분야에서 40개 이상의 대학과 민간기업, 그리고 정부 기관들과 파트너십을 체결하고 있다. 다양한 기술로 대량의 데이터를 분석하여 DHS 소속 SS(비밀경호국), TSA(교통안전청), USCIS(연방이민국), FEMA(연방재난관리청), CBP(세관국경보호국), CG(해안경비대) 등 22개 연방기관들의 실시간 의사결정을 돕는다. 퍼듀대학의 CVADA가 주도해서 개발한 소셜미디어 분석 도구인 'SMART'는[16] 사용자에게 '리얼 타임 매핑과 탐색'을 제공한다. 또한, 거의 모든 프로 경기 리그에 고객 스크리닝 및 탈출 시뮬레이션 도구를 공급하여 스타디움의 팬들을 테러범의 위협으로부터 보호한다. 럿거스대의 CVADA가 소프트웨어 기업인 'Regal Decision Systems Inc.'와 파트너십을 맺어 개발했다.

## 2. CIA의 디지털 혁신

CIA는 신흥 기술의 숙달을 '사람 대 사람'의 기량과 조합시키고 있다. 오래된 수집, 처리, 분석의 기법에 하이-테크를 접목한다. 공작관들은 조지 오웰식의 끊임없는 기술적 감시 속에서도 스파이 행위를 수행할 도구와 공작기법을 장착한다. 분석관들은 정교한 AI 모델과 데이터 분석기법으로 무장하여 최선의 인간 판단(human judgements)을 한다. CIA는 2022년 4월 최초로 '최고 기술관'(CTO: Chief Technology Officer)직을 신설하고, 실리콘밸리 출신인 물찬다니(Nand Mulchandani)를 임명했다. 내부의 과학기술 역량을 진작한다. 민간영역과 더 좋은 파트너십을 전담하는 미션센터도 설립했다. AI 혁명과 공개정보의 사태 현상(avalache)은 CIA가 그간 비밀리 수집해 오던 것과는 별개로, 분석관들에게는 새로운 기회이다(Burns, 2024).

윌리엄 번즈 CIA 장은 2024년 1월 포린 어페어즈 기고에서 "자체적으로 새 AI를 개발중"이라고 밝혔다. AI는 모든 데이터를 더 빠르고 더 효과적으로 처리하여 정책결정자의 선호와 국가이익에 관한 정연한 판단(reasoned judgements)과 통찰을 제공한다. CIA는 지금 공개정보에 대한 분석관들의 접근 향상 및 엄청난 양의 공개 데이터를 효과적으로 처리할 목적으로 오픈AI의 챗GPT와 같은 AI 툴을 개발 중이다. 이 프로젝트를 두고 CIA 공개정보 책임자인 랜디 닉슨(Randy Nixon)은 2023년 9월 블름버그와 인터뷰에서 "CIA와 국가안보국

16) 'Standard Management Analysis Reporting Tool; SMART'는 SNS 분석 및 보고 도구의 모임임. 이 시스템은 소셜미디어 게시물의 확장 가능한 분석 및 시각화를 분석관에게 제공함. 주제 추출, 키워드 필터의 조합, 단어 클러스터 검사 및 이상 사건 감지를 사용하여 상황을 인식하게 하고, 시간이 촉박한 임무에 대한 의사결정을 향상함(DHS 홈페이지, 2024.4.14. 검색)

(NSA: National Security Agency), 연방수사국(FBI) 등을 포함한 IC 내의 '거대한 18개 정보기관 네트워크'를 향한 논리적, 기술적 발걸음"이라고 묘사했다(Popular Science, 2023-9-27). 이는 중국이 10년 내 AI 글로벌 선도국이 되겠다는 야망을 드러내고, 2023년 7월 국내 간첩행위의 범위를 대폭 확대한 반간첩법 시행 및 데이터 규제 강화에 따른 정보전의 일환이다.

2015년 3월 브레넌(John O. Brennan) 당시 CIA 장은 "모든 활동과 공작들을 디지털 도메인의 바로 그 중심에 위치시켜야 한다"고 선언했다. 그해 CIA 최초로 디지털혁신국(DDI: Directorate of Digital Innovation)이 출범했다. DDI는 감지(sensing) 만능, 사이버 위협, 데이터의 기하급수적 증가라는 정보환경에서 사이버 대응, 공개 출처 수집, 데이터 과학, AI 및 기업정보 기술의 다분야 융합(fusion)을 담당한다.

CIA는 분석관들이 내부 저장소의 비밀데이터 활용과 함께, 폭증하는 공개 데이터로 눈을 더 많이 돌리게 하는 시스템을 만들어 간다. 공개정보에 더 많이 주목하고 자원을 투입하라는 WMD 위원회의 권고에 따라, DNI는 2005년 11월 공개출처센터(OSC: Open Source Center)를 창설했다. CIA 내에 베이스를 두고 CIA 장이 DNI를 대신해 운용했다. 그러다가, 2015년 10월 CIA의 DDI에 편입되어 공개출처부서(OSE: Open Source Enterprise)로 재편됐다.

2016년 3월 데이터 관리와 데이터 플랫폼, 고등 분석전략과 관련한 '클라우데라 연방 포럼'(Cloudera Federal Forum)에서 할만(Andrew Hallman) DDI 담당 부국장은 "CIA의 구식 정보수집 전략과 관료제로는 글로벌로 생성되는 정보의 가속화 속도를 견디어 내기 어렵거나, 정책결정자들의 더 빠른 의사결정 요구에 보조를 맞출 수 없다"고 진단했다. 그리고 그는 "CIA는 더 예측적이길 원한다"면서 빅데이터 기술 및 데이터 분석학 등을 통해 "CIA는 3-5일 내 사회 불안의 진전을 예상할 정도로 예측 능력을 향상시켰다"고 밝혔다.

실제로 카터 행정부의 CIA 장을 지낸 스탠스필드 터너(Stansfield Turner 1977-81)는 포린어페어즈 기고(1991: 155-157)에서 "1978년 이란의 친미 팔레비(Shai Reza Pahlavi) 정권이 무너질 때 이란 내부 반감의 폭과 강도를 제대로 판단하지 못한 것이 최대의 정보실패였다"고 자인했다. 또한, CIA가 1980년대 니카라과 산디니스타 자파 정권을 무너뜨리기 위해 우파의 콘트라 반군을 지원할 때도 "산디니스타 정부에 대한 비콘트라 대중의 반대가 얼마나 강한지 몰랐다"면서 현지인들의 태도에 대한 무지가 결국 무리한 공작을 초래했음을 암시한 적이 있다. 이 같은 실패는 CIA의 데이터에 기반한 예측 노력으로 이어졌고, 해외공작의 효율성과 효과성 증진에 큰 몫을 하게 되는 결과를 가져왔다.

CIA는 '아마존 웹 서비스(AWS: Amazon Web Service)가 구축한 클라우드 컴퓨팅 환경을 포함하여 네트워크, 데이터베이스, 서버 등 같은 기술 기반을 가지고 데이터의 폭발에 마구를 채워서 처리, 분석한다. 빅데이터 기술로 적의 디지털 활동에서 얻은 정보를 조합, 결합하여 그들의 행동이나 의도를 이해하려고 한다. 비록 작은 조각이라 할지라도 분석관들은 서로 다른 형식, 구조 또는 출처에서 나오는 데이터를 분석하여 전체 그림을 그리고 퍼즐을 풀어낸다.

디지털 혁신을 주도하는 DDI의 제니퍼 유뱅크(Jennifer Ewbank) 부국장은[17] 2024년 1월 DDI의 임무로 ① "혁신하지 않으면 소멸된다(Innovate or Perish)."는 점을 절감하여 CIA 업무의 우선순위 조정 ② 새로운 첩보방법, 새 도구, 새 플랫폼과 임무 해법을 만들어서 정보공작에 결정적 이점 제공 ③ 민간 부문과 스마트한 파트십 구축을 들었다(THE CIPHER BRIEF, 2024-1-22).

CIA, NSA 등 미 IC는 민간기업에 대한 패스트 팔로어이다. 실리콘밸리와 긴밀한 파트너십을 형성하고 있다. 실리콘밸리는 IC와 같은 일을 하고 있다(전웅, 2017).

### 3. 미 IC의 데이터베이스와 네트워크

2013년 가을, 미 IC의 데이터 저장소인 유타 데이터센터(UDC)가[18] 신설됐다. ODNI 산하 집행기관인 NSA가 운용하며, NSA의 콜로라도, 조지아, 메릴랜드 등의 데이터 센터와 상호 연동되는 네트워크이다.

개인 이메일, 휴대전화 통화, 인터넷 검색, 그리고 주차영수증, 여행 일정, 도서 구매, 소소한 디지털 데이터 등을 포함한 개인 정보 흔적 등 모든 종류의 통신을 처리할 능력이 있는 것으로 추정된다. 2013년 6월 NSA 계약직인 스노든(Edward J. Snowden)이 "대량의 정보수집이 일반 시민에게까지 미친다"며 그 위험성을 폭로한 프리즘(PRISM)은 NSA가 운용하는 국가안보 목적의 컴퓨터 및 네트워크 감시 프로그램이다. 또한, 유타 데이터 센터는 데이터 수집은 물론, DARPA와 합동으로 개발한 '암호 해독용 슈퍼컴퓨터 플랫폼'을 구동하고 있다(Utah Data Center, NSA 홈페이지, 2024-4-18 검색).

9·11 테러 직후인 2001년 10월 도입된 미 애국자법(USA Patriot Act)은 법 집행기관에 국내와 국제 전화 감청을 포함해 테러리스트 징벌을 위한 감시 수단 강화를 가져왔다. 그렇지만, 인권 침해 논란 끝에 2015년 6월 시효 만료되어 동법 215조에 의거한 자국민에 대한 대량 통신기록 수집과 감청이 금지되었다. 이 법을 대체한 미 자유법(USA Freedom Act)에 따라 '영장 받은 선별적 감청'이 허용된다.

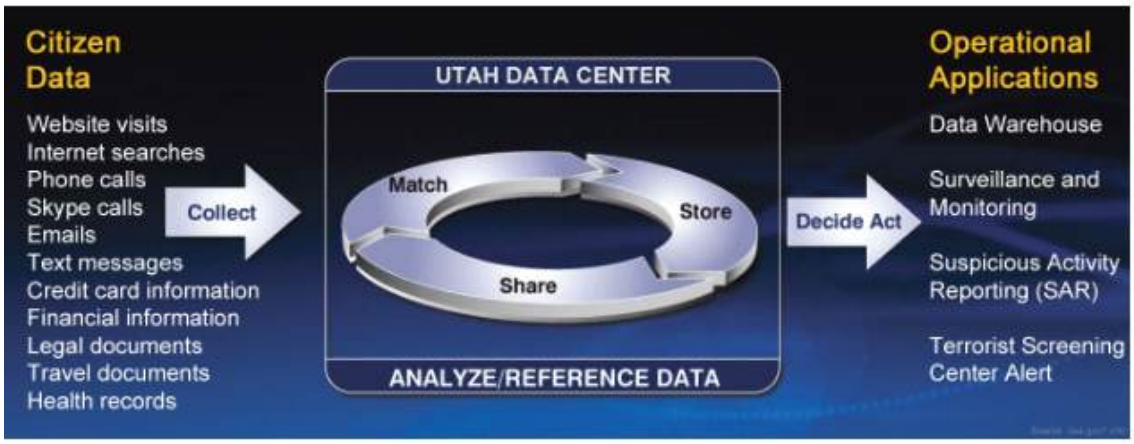
유타 데이터 센터가 처리하고 저장하는 국내 감시 데이터는 프리즘 데이터 수집 프로그램, 미 전역 감청 기지들, 그리고 NSA 자체의 수집, 분석 도구를 사용해서 획득된다. 그리고 이 데이터를 처리, 분석해서 저장, 감시 및 모니터링, 범죄혐의 보고, 테러 검색센터 경보 등 운영에 적용하고 있다. <그림2>는 그 전 과정을 보여 준다.

---

17) 번스 CIA 장은 2024년 2월7일 새 DDI 부국장에 줄리아니 갈리나(Juliane Gallina) DDI 부국장보를 임명했음. 갈리나는 30년 이상 군사, 공무원, 산업 등 정보 및 기술 커뮤니티에 종사했으며, CIA의 CIO(Chief Information Office) 및 정보기술혁신 조직의 장을 지냈음(CIA 홈페이지, 2024-4.15 검색)

18) 미 IC 최초의 종합 국가사이버안보이니셔티브 데이터 센터임. 유타주 블러프데일(Bluffdale) 부근의 캠프 윌리엄스에 위치함. IC를 도와서 국가 모니터, 강화 및 보호 목적으로 설립됨. 1.5억 불이 들어갔고, 100만 평방피트의 부지에 거대한 20여 개 건물의 콤플렉스임. 처리 용량 관련, 2012년 2월 유타주 개리 허버트 주지사는 "세계 최초로 요타($10^{24}$)바이트의 수집, 보관 시설이 될 것"이라고 했으나, 실제 용량은 국가기밀로 분류됨(Utah Data Center, NSA 홈페이지, 2024-4-18 검색)

**<그림2> NSA의 시민 데이터 처리 과정도**




출처: Utah Data Center, NSA 홈페이지, 2024-4-18 검색

NSA의 광범한 감시는 인권 침해 논란을 초래했다. 테러 예방 및 국가안보 노력의 효과성도 아직 분명히 평가된 것은 없다. 그렇지만 NSA가 있기에 테러리스트들이 첨단 과학기술의 편리성을 이용하지 못하고 원시의 불편함을 감수하는 것으로 볼 수는 있다. 9·11 이후 아직 대규모 테러 공격은 없는 것도 이런 시각을 뒷받침하고 있다.

미 IC는 "네트워크에 대항하기 위해서는 네트워크가 필요하다"는 경구를 자주 인용한다(Arquilla and Ronfeldt, 2001). 데이터의 볼륨이 너무 광대해서 데이터 처리의 지속적인 빠른 진전에도 불구하고, 하나의 데이터베이스로는 수집, 저장, 회수, 분석될 수 없다. IC의 국내 정보기관들은 국경을 넘나드는 테러리즘, 마약 거래, 밀수, 자금세탁, 조직범죄 등을 탐지, 처치하기 위해 구축한 데이터베이스 및 기관 간의 데이터를 연동하는 시스템을 구축하고 있다. 복잡한 네트워크로 정보를 공유한다.

2005년 3월의 WMD위원회 권고에 의거, 연방 국내정보의 중앙기구화하고 있는 FBI는 국가안보국NSB내에 대테러부서(CDT: Counterterrorism Division)에서 테러범을 검열하는 데이터베이스(TSDB: Terrorist Screening Database)를 포함해 정보융합 및 데이터 활동을 수행한다. 해외테러범추적(TFFTTTF: Foreign Terrorist Tracking TF)는 FBI가 주도하는 연방 정보기관들의 연합체이다. 모든 출처 데이터 흐름의 마이닝을 강조한다. 또한, 국가 합동대테러(TFNJTTF: National Joint Terrorism Task Force) 시스템은 56개 FBI 지부는 물론 주 및 지방의 법집행기관들과 연계되어 데이터를 공유한다(Jackson at al., 2009: 68-69).

국토안보부(DHS)는 안보 목적에 직접 사용될 개인 데이터를 제공한다. 일례로 TSA는 비행금지(No-Fly) 리스트와 요주의 리스트 데이터베이스를 운용한다. DHS는 정보 임무를 위해 정보시스템과 분석기법을 개발해 왔다. ADVISE(Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement)는 대량의 데이터를 분석하여 감시, 경보하는 소프트웨

어 프로그램이다.

이밖에도 법무부 마약단속국(DEA: Drug Enforcement Administration)의 정보와 조사 데이터, 국방부 국방정보국(DIA: Defense Intelligence Agency)의 대테러 데이터 및 국방정보시스템국(DISA: Defense Information Systems Agency)의 데이터 마이닝 능력, 그리고 옛 재무부 (TECS: Treasury Enforcement and Communication Systems)의 테러·자금세탁·금융 데이터 시스템이 DHS 산하 세관국경보호국(CBP)에 의해 업데이트되어 작동되고 있다. 수많은 독립된 기관들이 상호 연계된 네트워크로 데이터를 저장, 공유, 활용한다. 분산된 채 각각의 권위와 책임을 지닌, 그리고 각기 특별한 장점을 가진 데이터베이스들이 네트워크로 연결되어 작동하고 있다(Jackson at al., 2009).

## Ⅴ. 결론 및 시사점

전쟁에 패했을 때 비로소 인텔리전스를 필요로 한다(Kahn, 2006). 재앙이 발생하거나, 거대한 음모가 발각되어야 국가는 인텔리전스를 주목한다. 역사가 그렇게 말한다. 그렇지만, 막상 위협 앞에서 인텔리전스는 실패했다. 이전에 겪어보지 못한 어떤 것을 예방하기 위해 효과적인 행동을 취한다는 것은 거의 불가능하다(Posner, 2004).

미 IC는 2001년 9·11 이후 테러와의 전쟁, 2003년 이라크 전쟁을 거치면서, 실패하고도 혁신하지 않으면 생존하지 못하는 상황에 직면했다. 인텔리전스는 태생적으로 냉전 시대의 폐쇄된 사회가 타깃이다. 국가안보와 번영을 위협하는, 공개적으로 얻을 수 없는 정보를 획득하는 데 그 목적이 있다. 냉전 때 테킨트는 매우 부족했고 유가치 정보를 찾기 힘들었다. 아주 적은 수량의 정보로 적의 의도와 능력을 추적했다.

지금은 수많은 전자 센서들, 엣지 컴퓨팅(edge computing), 모바일 폰·PC와 같은 앤드포인트(endpoint) 등 너무나 많은 데이터 저장 수단이 네트워크화하여 데이터의 홍수 속에 정보 판단을 해야 한다. 정보의 혁명과 기술진보와 함께 인텔리전스의 기회는 폭증한다.

그러나 기습은 그것이 물리적이든, 사이버 영역이든 예상하지 못할 장소, 시간, 방법을 택한다. 대규모 정보실패를 겪지 않은, 그래서 역설적으로 국가적 자산 동원에 불리한 우리로서는 혁신을 통해 대비역량을 키우는 수밖에 묘수는 없다.

테킨트와 휴민트의 융합은 인텔리전스의 속성상 필연이다. 테킨트가 통찰을 제공하지는 않는다. 항공사진과 위성 정보, 신호 데이터 등은 군사적, 사이버 공격이 있기 전에 그 움직임을 밝히기 어렵다. 적의 심장부를 모른다. 그 의도를 조기 경보할 수는 없다. 더구나 군사적 움직임에 대한 경보는 실상 너무 늦어서 정책결정자에게 의미 있는 옵션을 제공할 수 없다. 휴민트가 효과적이며 신호정보는 보조재로 보는 게 현실적이다. 과학기술은 결국, 과학기술에 당한다. 은닉에는 속수무책이다. 하마스의 사이버 은닉이 그랬다.

전통의 관료적 이익과 고정관념이 강한 정보기관의 특성상 데이터와 AI를 정보활동에

접목하는 것은 결코 쉬운 과제는 아니다. 내부 저항이 잠재되어 있다. 그렇다고 데이터에 기반하는 인텔리전스 프로세스와 판단(human judgement)의 기제 구축을 늦출 수는 없다.

디지털 혁신의 현상과 미래, 그리고 도전요인을 우선 진단해야 한다. 디지털 혁신 전담 부서와 전담 직위가 필요하다. 빅데이터·AI 전문가를 민간에서 영입해 혁신을 끌어가면 좋겠다. 정보기관의 외곽 기업 설립 혹은 연구개발 센터의 운용을 권장한다. 정보활동의 계획, 수집, 처리와 분석, 배포와 피드백의 전 과정에 걸쳐서 단계마다 데이터에 입각한 접근이 이루어지도록 해야 한다.

국가정보기관의 공개정보센터(OSC)는 민간 매체와 파트너십을 통해 인적, 기능적 역량을 보강하는 한편, 가짜뉴스, 허위정보에 대응할 법제적 장치를 갖추어야 한다.

민간 부문과의 협업은 대세이다. 비밀 유지와 보안이 내부 무능력의 노출을 차단하는 방편이 되어서는 곤란하다. 불가피한, 적정 수준의 공개를 겁내서는 미래를 열어 가기 어렵다. 민간과 같이 가면 덜 힘들고 더 효율적일 수 있다. 정보기관은 민간의 '패스트 팔로워'임을 받아들이고, 파트너십을 더 과감하게 추진할 필요가 있다.

행정부 내 인텔리전스 실체들에 분산된 복잡한 각기의 데이터베이스를 큰 틀에서 점검하여, 상호 연동하고 공유하는 시스템이 실행력으로 유효하게 연결되는지는 면밀하게 살펴보아야 한다. 각 기관의 데이터가 통합되고 적기에 이해되어 이상 징후를 포착하는 것은 비현실적일 기대일 수 있다. 또한, 각 기관이 저마다 데이터 수집, 분석 역량의 특수성과 장점을 가지고 창조적으로 접근하는 것은 지극히 타당하다. 그렇지만, 단순히 데이터시스템에 접근만 제공하는 것으로 그치고, 협업의 행동으로 이어지지 않으면 그 효과는 반감되고 말 것이다.

2020년 9월 본격 착수한 과학기술정보통신부 주도의 데이터 댐(Data Dam) 사업은 수력 댐처럼 공공과 민간의 네트워크를 통해서 생성되는 데이터를 수집, 저장, 가공, 표준화해 활용하는 사업이다(과기정통부 보도자료, 2020-9-2). '분산된 데이터베이스를 하나의 네트워크로 지향'한다는 차원에서 국가정보기관의 참여가 요구된다.

새롭고 이상하며 처음 보는 전쟁의 시대, 초연결성, 초불확실성의 이 시대에, 국가 정보기관의 인텔리전스 만으로는 결코 결정적이지 않다.

## <참고자료>

과학기술정보통신부 보도자료. (2020). 디지털 뉴딜의 핵심; '데이터 댐'사업 본격 착수. 9.2.

김상배. (2020). 데이터 안보와 디지털 패권경쟁: 신흥안보와 복합지정학의 시각. 국가전략, 26(2) 여름호, 5-34.

김진형. (2022). 중국 사이버안보의 전략과 체계. CSF(중국전문가포럼). 대외경제정책연구원

전웅. (2017). 빅데이터와 정보활동-미국 정보공동체 사례를 중심으로. 국가정보연구, 10(1), 7-54.

조경환. (2023). 반복되는 정보실패는 죽느냐 사느냐의 문제다. 시사저널, 1776호 (11.7.), 94-95.

박주희. (2024). 데이터·AI 안보로 보는 사이버안보-데이터 규제를 둘러싼 미국과 중국의 대립. 한국사이버안보학회 제7차 사이버 국가전략포럼, 토론문, 83-87.

채재병·김일기. (2020). 주요국 사이버안보 전략과 한국에의 시사점. INSS 전략보고, March, 73. 국가안보전략연구원

Arquilla, John and David Ronfeldt. (2001). Networks and Netwars: The Future of Terror, Crime, and Militancy. RAND Corporation

Burns, Williams J. (2024). Spycraft and Statecraft-Transforming the CIA for an Age of Competition. Foreign Affairs, January 30.

DNI. (2023). The IC Data Strategy 2023-2025-The IC Data-Driven Future: Unlocking Mission Value and Insight(2024-4-20 검색)

Executive Office of the President. (2014). Big Data: Seizing Opportunities, Preserving Values.

Falode, Adewunmi. (2021). Found: A Definition of Intelligence. Joural of Social Sciences, IV(1), 70-73.

Jani, Karan. (2016). The Promise and Prejudice of Big Data in Intelligence Community. https://ca.skku.edu:8443/link.n2s?url=http://arxiv.org/abs/1610.08629

Kahn, David. (2006). The Rise of Intelligence. Foreign Affairs, 85(5), 125-134.

Kahneman, Daniel. (2011). Thinking, Fast and Slow. Farrar Straus Giroux

Lowenthal, Mark M. (2006). INTELLIGENCE: From Secrets to Policy (Third Edition). CQ Press.(한글판 김계동 옮김. 2008. 명인문화사)

Miles & Rigby. (2013). Innovation Policy Challenges for the 21st Century. Demand-Led Innovation(Ch. 2. pp. 36-63.). NY and UK: Routledge of Taylor & Francis

Neale, Spencer. (2019). CIA troubled as biometric tracking and digital footprints pull spies from the shadows. Washington Examiner. 12.30.

Popular Science. (2023). The CIA is building its version of ChatGPT. By Andrew Paul. Sep. 27, 2023 12:00 PM EDT.

Posner, Richard A. (2004). The 9/11 report: A Dissent. The New Times, Aug 29

Pratt, Lorien. (2015). 10% of the data holds 90% of the value: four reasons why. Retrieved from:
https://www.lorienpratt.com/10-of-the-data-holds-90-of-the-value-four-reasons-why/ 2024-4-20 검색

_____, Christophe Bisson, and Thierry Warin. (2023). Bringing Advanced Technology to Strategic Decision-Making: The Decision Intelligence/Data Science (DI/DS) Integration Framework. Futures, 152, September 2023.

Shulsky & Schmit. (2002). Silent Warfare, understanding the World of Intelligence. Potomac Books, Inc. (한글판 신유섭 옮김. 2007. 명인문화사)

THE CIPHER BRIEF. (2024). CIA Deputy for Digital Innovation Talks Mission, Partnerships and Espionage Challenges. 2024.1.22/5:49 AM ET.

The WMD Commission. (2005). Report to the President of the United States. March 31, 2005. Official Government Edition

Turner, Stansfield. (1991). INTELLIGENCE FOR A NEW WORLD ORDER. Foreign Affairs. 70(4), 150-166.

Walton, Calder. (2023). The New Spy Wars: How China and Russia Use Intelligence Agencies to Undermine America. Foreign Affairs, July 19.