사이버안보연구, 1집 2호 2024 가을, 119-162

최근 미국 정보공동체의 디지털 기반 데이터안보와 그 함의

0102-119162

조경환 | 성균관대학교 국정전문대학원

* 이 논문은 2024년 5월 2일 한국사이버안보학회의 국가전략연구위원회가 주최한 제9차 사이버 국가전략포럼에 발표한 내용을 토대로 한 것임

논문접수일 2024년 8월 23일 | 논문심사일 2024년 9월 3일 | 게재확정일 2024년 10월 10일

논문 요약

이 연구는 미국의 대중국·러시아 글로벌 데이터 주도권 각축과 함께, 미국 정보공동체가 어떤 전략 아래 디지털 기반의 데이터안보를 확보하며, 데이터체계와 그 분석관들은 어떻게 과학기술과 인간을 융합해 의사결정과 정보활동을 돕고, 어떤 데이터베이스 연동구조로 연방 차원에서 안보 데이터를 관리해 가는지를 살펴본 뒤, 함의를 도출한다.

디지털 시대에, 방대하고 다양한 데이터와 그들의 빠른 연결성은 데이터 폭발을 가져왔다. 이는 데이터·증거에 기반한 사고와 국가정보활동으로 이어져 정책결정자에게 더 나은 판단정보를 제공한다. 동시에 적대세력도 새 공격 도구를 가지게 되어, 데이터를 절취, 파괴, 오염, 조작하고 영향을 준다. 가장 중대한 위협이 이제 디지털 도메인에 있게 되면서 데이터가 안보의 핵심요소에 위치한다. 데이터를 전략 자산으로 인식하고 그 주권을 안보 관점에서 접근하는 중국과 러시아는 데이터의 국외 이전을 강하게 통제한다. 미국은 데이터의 자유로운 흐름을 전통적으로 보장해 왔으나, 최근 프라이버시·시민 자유권 보호 강화 및 민감 개인 데이터의 대량 전송을 차단하면서 맞대응한다.

미국 정보공동체의 데이터안보는 자체 고등연구계획과 대외 파트너십을 통한 디지털 혁신에 기반을 두며, 인간과 데이터·AI를 조합한 증강된 솔루션을 제공한다. 데이터 및 그것을 다루는 능력을 정보공동체 강점의 펀더멘털로 간주해 데이터 저장, 처리분석, 배포, 공유의 시스템화에 집중한다. 공동체 내 각 기관이 독립된 권한과 책임으로 데이터베이스를 운용하되, 네트워크 거버넌스로 묶어 의심 행동 적출 등 국가위협에 대처한다.

주제어 데이터안보, 정보공동체, 디지털 혁신, 국가정보, 네트워크 거버넌스

Ⅰ. 머리말

"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. 인간이 만든 과학기술이지만, 이제 그 고삐는 풀어졌다. 그리고 그로 인한 변화는 우리의 시간표대로 오지 않는다(Boren 1992, 52).

초경쟁적인 디지털 시대에 데이터에 기반한 다종다양한 디바이스들, 센서들과 사람들 사이의 데이터, 그리고 그 연결성의 기술적 폭발은 혁신을 가져왔다. 기술이 혁신을 추동(technology-push)하고, 시장의 수요가 또한 그 혁신을 견인(demand-led)한다(Miles & Rigby 2013). 뉴밀레니엄에 즈음해 급격히 확장된 과학기술은 네트워크 시대를 열었다. 글로벌 기술 혁신이 진행 중이고, 인터넷은 광범하게 이용 가능하며, 모바일 앱들이 속속 시판되고, 디지털 혁명이 눈 앞에 펼쳐진다. 모든 출처(all sources)의 데이터는[1] 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 가져왔다. 이는 증거에 기초한 사고(reasoning)와 데이터 기반의 정보 요구로 이어지고 있다. 정책결정자에게는 더 나은 통찰을 제공한다.

1) 모든 출처(all sources) 데이터는 인간정보(HUMINT), 과학기술정보(TECHINT), 공개정보(OSINT) 등 모든 정보 기법을 통해 수집된 생 자료들의 조각들 및 부분들로 정의된다(Falode 2021, 72).

정보환경의 복잡성과 변동성은 그 어느 때보다 커졌다. 디지털 신기술과 시스템은 혁신을 만들어내는 동시에 위협을 촉발하여 데이터 안보라는 반작용을 부른다. 디지털화된 데이터는 대부분 네트워크에 연결된 매체에 저장되어 사이버 공격에 대한 취약성을 내포한다. 미국 중앙정보국(CIA)의 인공지능(AI) 책임자인 라만(Lakshmi Raman)은 2023년 9월 폴리티코와 인터뷰에서 "새로운 기술은 가장 큰 위협이자 자원"이라고 했다(POLITICO 2023-9-27). 적대세력은 강력한 새 도구들을 가지고 혼란하게 한다. 이들은 속이고 회피하고 염탐하며, 주요 디지털 데이터를 절취, 파괴, 오염, 조작하고, 영향을 행사한다. 우리가 직면한 가장 중대한 위협은 이제 디지털 도메인에 있게 되었다.

그렇지만, 진보하는 과학기술도, 데이터 쓰나미도, 거대한 양의 공개정보와 비밀리 획득한 정보를 소화해 내는 AI도, 그 과잉에 압도만 될 것은 아니다. 국가정보기관이 정보(information)를 요구·수집·분석·배포하는 순환주기에서 그 과정이자 최종산물인 국가정보(national intelligence)의[2] 본질은 변함이 없다. 그리고 국가의 개입이 무한정일 수는 없다. 지켜야 할 데이터는 국가가 보호하고 있는 데이터로 한정되어야 할 것이다. 개인의 영역과 프라이버시는 그대로 보장되어야 한다. 국가정보는 그것이 디지털 기반으로 진화하더라도 여전히 인간과 기술 사이에 상호작용한다. 오직 인간만이 수집할 수 있고, 인간만이 수행할 수 있는 비밀공작은 계속해서 비밀의 영역에 남아 있을 것이다. 신흥 기술과 인간을 통합하고 엮어내야 한다. 이것 역시

2) 이 연구에서는 국가정보기관의 정보 순환체계 상 투입요소인 가공되지 않은 상태의 생정보(raw data)·정보자료(information)와 이를 분석, 정제한 산출물인 인텔리전스(intelligence)를 구분할 필요가 있어서(정준표 2009, 10-11) 이 인텔리전스를 국가정보로 표기한다.

과학기술에 달려 있다.

이 연구는 미국의 데이터안보와 대중국·대러시아 글로벌 데이터 주권 각축을 살펴본다. 그리고 미국 정보공동체(IC; Intelligence Community)는 데이터 기반의 정보혁신을 어떠한 맥락과 기제를 가지고 이루어가는지, 데이터체계와 그 분석관들은 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 보려고 한다.

Ⅱ. 디지털 시대의 국가정보와 데이터 주도권 경쟁

1. 미국 정보공동체의 진화 및 디지털 시대의 정보공동체 선행연구

1) 미국 정보공동체의 진화

미국 정보공동체(IC)는 집행부처 정보기관들과 조직들의 연방(federation)이다. 국가안보법(The National Security Act of 1947) 및 정보개혁·테러방지법(Intelligence Reform and Terrorism Prevention Act of 2004)에 의거, 대통령의 주된 국가정보 자문역인, 각료급의 국가정보장(DNI; Director of National Intelligence)의 통할 아래 중앙정보국(CIA), 연방수사국(FBI), 국방정보국(DIA)과 국가안보국(NSA), 국무부 정보조사국(INR), 국토안보부 정보분석국 및 각 군 정보기관 등 18개 정보조직이

하나의 공동체를 이루고 있다.[3] 국가정보장을 정점으로 각 기관이 느슨하게 통합되어 있다. 각기 일하면서, 외교 관계 및 미국의 국가안보에 필요한 정보활동을 공동으로 수행한다. DNI는 CIA 및 정보기관들의 소관 부처 장관들이 위원인 '합동정보공동체위원회(JICC; Joint Intelligence Community Council)'의 도움을 받아 정보공동체를 감독한다. 국가정보프로그램(National Intelligence Program)을 개발하고 결정한다. 정보 공유와 협력을 촉진하고, 정보예산 획득·배분권을 가진다. 위계적이고 계층적인 통할 구조이지만, 개별기관의 운영에는 관여하지 않는 방식을 취한다.

미국의 정보기관들은 여러 연방 부처에 분산되어 있다. 1787년 필라델피아 제헌 회의 때부터 확립된 견제와 균형의 원칙은 권력의 집중을 극도로 경계하는 미국인의 인식을 반영한다. 국가정보 조직의 거버넌스도 예외는 아니다. 제2차 세계대전 전에는 INR, FBI, 육군과 해군이 통합된 지시·지침이나 협력 없이 각자 활동했다. 정보기관들은 비밀정보와 조직 보호를 위해 "차단의 원칙"을 적용하며, 지휘계통으로만 보고하는 것을 직업윤리로 삼는다. 상호 긴밀한 공조가 어려운 가치관과 조직문화를 가지고 있다(신성순 2017, 8).

그러나, 전쟁에 패했을 때 비로소 국가정보는 부름을 받는다(Kahn, 2006). 재앙이 발생하거나, 거대한 음모가 발각되면 국가는 정보활동

3) 미국 정보공동체 18개 기관은 행정부처로부터 독립된 국가정보장 사무국(ODNI)과 중앙정보국(CIA)을 필두로, 국방부 소속의 국방정보국(DIA), 국가안보국(NSA), 국가지리정보국(NGA), 국가정찰국(NRO), 육·해·해병·공·우주군의 정보기관 등 9개 기관, 그리고 에너지부의 정보·방첩국, 국토안보부의 정보분석국 및 미국 해안경비대정보국(CGI), 법무부의 연방수사국(FBI)과 마약단속국(DEA), 국무부 정보조사국(INR), 재무부 정보분석국이다(ODNI 홈페이지, https://www.dni.gov/index.php/what-we-do/members-of-the-ic, 검색일: 2024.9.20.).

에 주목한다. 국가적 안보 위기는 국가안보라는 하나의 목적 아래 정보기관들이 공조하도록 요구했다. 유럽에서 2차 대전이 한창이던 1941년 7월, 프랭클린 D. 루스벨트 대통령은 정보조정관(COI; Coordinator of Information)을 창설하여 해외정보를 정부 전체적으로 조율, 조정하게 했다. 이어 같은 해 12월의 진주만 기습을 당하고 나서인 1942년 6월, 미국 역사상 최초의 중앙정보국인 전략사무국(OSS; Office of Strategic Services)이 설립됐다. 전후인 1947년 9월, 트루먼 대통령은 독립적인 민간 정보기관으로서 CIA를 신설하여 정보수집과 분석평가, 배포와 함께 국가정보 활동 조정역할을 부여했다. 분산된 정보를 중앙으로 모아보려는 의도가 반영되었다. CIA의 장은 CIA는 물론 중앙정보장(DCI; Director of Central Intelligence)으로서 미국 정보공동체를 선도했다. 정보공동체라는 용어는 1950년-53년까지 제4대 DCI를 지낸 스미스(Walter Bedell Smith)가 처음 공식적으로 사용했다(Warner & McDonald 2005, 12-13).

1975년 CIA, NSA, FBI, DIA 등 연방 정보기관들의 불법과 권한 남용이 불거지고, 상하 양원이 대대적인 조사위원회를 가동했다. 1년 뒤 2월, 포드 대통령은 행정명령(EO; Executive Order) 11905호를[4] 통해 국가정보를 해외정보와 해외 방첩정보로만 제한한 뒤 CIA 등 9개 기관을 정보공동체로 적시했다. CIA 장에게는 해외정보 관련 대통령의 주된 자문역 및 신설된 해외정보위원회(CFI; Committee on Foreign Intelligence)의 의장을 맡겨 DCI 임무를 명시했다. 이후 1981년 12월, 레

4) President Gerald R. Ford's Executive Order 11905: United States Foreign Intelligence Activities (February 18, 1976)

이건 대통령은 행정명령 12333호로[5] 정보공동체 제도를 정착시켰다.

9·11 테러는 미국 역사상 최악의 정보실패로 평가되었다. 10년 이상 이어진 수많은 공격 징후의 점들은 선으로 연결되지 못했다. 해외정보기관인 CIA의 사전 경고는 정책결정자들의 의사결정에 도달하지 않았고, 국내정보의 중핵인 FBI는 수집 정보를 국가적 우선순위로 끌어올릴 능력이 없었다. DCI는 권위를 잃었다(Tenet 2009, 240-255; The 9·11 Commission 2004). 2004년 조지 W. 부시 대통령은 DCI를 폐지했으며, 정보개혁·테러방지법을 제정하여 국내외를 포괄하는 국가정보의 정립 및 국가정보장(DNI) 직을 창설했다. 지금의 강화된 정보공동체가 이때 완성되었다.

이제 또다시 미국 정보공동체는 전대미문의 기술혁명과 전환이라는 새 시대의 여명에 서 있다. 2013년의 한 조사에 의하면, 전문가들은 예견되는 최악의 글로벌 안보재앙으로 "통제 불능의 기술(runaway technology)"을 들고 있다(Carpenter 2016, 94). 인공지능(AI) 및 클라우드 컴퓨팅, 고등 센서들, 그리고 빅데이터 분석을 포함한 신흥 기술은 정보공동체가 평가할 책임이 있는 글로벌 위협의 본질을 변화시킴과 동시에 그 위협들을 정확하게 포착, 대응할 정보공동체의 능력 전환을 요구한다(CSIS 2021, IX).

2. 디지털 시대의 정보공동체 선행연구

21세기 들어 디지털 네트워크 시대[6]가 급속이 진전되고 있다지만,

5) Executive Order 12333: United States Intelligence Activities (December 4, 1981)

6) 1990년 12월 World Wide Web이 발표되고 보급이 되었다. 1998년 9월 구글이 창립되었고,

이와 관련한 국가정보 연구는 여전히 유아기에 있다(Moran at al. 2023)는 평가이다. 큰 틀에서 정보공동체의 혁신을 제언하거나, 빅데이터 혹은 AI와 국가정보를 다룬 연구들이 제한적으로 이루어졌다.

CSIS는 기술의 혁신·전환기에 정보공동체가 주요 적대국들에 대한 경쟁적 이점을 끊임없이 추구하기 위해서는 AI와 빅데이터 분석 등 기술 혁신을 통해 국가정보를 재창조하고 탈바꿈해야 한다면서 정보혁신위원회 창설, 국가정보 우선순위 조정, 공개출처정보(OSINT) 활동 확대 등의 제언을 내놓았다(2021). 미국 국립학술원(National Academies)은 정보공동체 내 기관들은 고등 기술에 의존해서 그들의 목적을 성취해야 한다고 전제하고, 정보공동체가 역동적인 글로벌 과학기술 지형과 그 생태계를 지렛대로 활용해야 하는 의미를 분석한 뒤, 정보공동체 내부 기관 간의 협력 기제 향상과 함께, 외부의 연관산업 및 글로벌 공동체와의 상호작용에 더 중점을 두라고 권고했다(2022). 그루버와 트라치크(Gruber and Trachik 2023)도 유비쿼터스 감시와 허위정보, 사이버 공격 등 신흥의 과학기술 안보위협들을 거론하고 정보공동체의 혁신을 촉진하는 논문들을 편집하였다.

2015년, CIA가 과학기술국(DS&T)을 신설한 1963년 이래 최초로 디지털 혁신국(DDI; Directorate of Digital Innovation)을 설립했다고 발표한 것을 기점으로, 빅데이터·AI와 국가정보에 관한 연구물이 일부 나오고 있다. 터커(Tucker 2015)는 빅데이터 시대에 즈음해 휴민트 경향(HUMINT-oriented)인 CIA의 재구조화를, 반 푸이벨드 등은 국가안보

2006년 10월 유투브를 인수했다. 2004년 2월에는 페이스북이 창업했다. 2007년 애플의 아이폰이 데뷔했으며, 2010년 삼성 갤럭시S가 출시되어 스마트폰의 대대적 보급이 이루어졌다.

의사결정 과정에서 빅데이터의 역할을 분석했다(Van Puyvelde at al. 2017). AI와 관련해서는 알렌·찬이 AI와 국가안보를(Allen and Chan 2017), 로스는 CIA에서의 AI를(Roth 2019), 빈시는 AI와 자동화 시스템이 비밀이 수집, 분석, 정책결정자에게 배포되는 정보활동의 지형을 근본적으로 바꾸는 국가정보 혁명으로 안내하고 있다는 글을 냈다(Vinci 2020). 모란 등(Moran at al. 2023)은 정보공동체와 글로벌 안보, 그리고 AI를 조망하면서 비밀정보와 스마트 스파이활동을 다각적으로 살펴보았다. 한편 국내에서는 전웅(2017)이 빅데이터와 정보활동을 미국 정보공동체 사례를 중심으로 분석한 외에는 선행연구를 찾아보기 어렵다.

데이터와 AI 등 디지털 기반의 국가정보 연구사례가 손에 꼽을 정도인 것은 정보 부족에 근본 원인이 있다. 국가기밀 문건은 정보자유법(FOIA; Freedom of Information Act)과 CIA정보법(CIA Information Act), 그리고 행정명령 13526호(비밀국가안보정보)에 근거해 25년이 지나면 자동 공개를 검토하지만, 국가안보 등 목적으로 50-75년 비공개를 유지할 수도 있다. 앤드류와 딜크스는 두 가지의 비밀 장벽이 있다고 보았다(Andrew and Dilks 1984). 첫째 장벽은 정보기관들 자체가 세운 것으로서, 출처와 방법이 노출되거나, 적들이 기술 발전을 눈치채는 것을 염려하기 때문이며, 두 번째 장벽은 정보기관들의 기술 협력자들이 정부와 비밀 유지 계약을 체결한 데다, 자사의 첨단 제품을 경쟁사들의 모방과 절취로부터 보호하려는 데 기인한다는 것이다.

결국, 전·현직 정보 당국자들의 공개 발언이나 기고문 등 이용 가능한 조각들을 모아서 윤곽을 잡고 구체성의 살을 붙여 가는 것이 현실적이며, 본 연구도 이 방식을 택한다. 사회과학의 방법론적 관점에서 보더라도, 포퍼(Popper 1963)는 단일 사례에 의해서도 결론에 도달

할 수 있다고 보았다. 한 사례를 깊게 보면 특수성을 발견하게 되고 그 특수성을 통해 보편성을 찾아내 일반화에 이를 수 있다는 접근법을 취하고자 한다.

2. 국가정보의 전장이 된 디지털 도메인

미국 정보공동체가 규정한 국가정보(national intelligence)는 "출처를 불문하고 미국 내 혹은 밖에서 수집된 정보(information)를 포함하여 대통령에 의해 내려진 어떠한 지시와도 일치하게 결정된 것으로서, 하나 이상의 정부 기관과 관련되고 ① 미국, 미국민, 재산, 혹은 이익에 대한 위협들 ② 대량살상무기(WMD)의 개발, 확산, 혹은 사용 ③ 미국의 국가 혹은 국토 안보와 관련된 사항에 관한 모든 인텔리전스"를 말한다(Intelligence Reform and Terrorism Prevention Act of 2004, Section 1012).

그렇지만, 학계에서 국가정보의 개념은 그 개념을 현상 수배할 정도로 정립이 쉽지 않다(Warner 2002). 로웬탈이 정의한 실무적 개념(a working concept)을 보면, 국가정보는 "국가안보에 중요한 특정 유형의 첩보들이 요구, 수집, 분석되어 정책결정자에게 제공되는 과정이며, 이러한 과정의 생산물을 의미하기도 한다. 또한, 이러한 과정과 첩보를 보호하는 방첩(counterintelligence)을 뜻하기도 한다. 나아가 합법적인 권위체가 요청한 공작의 수행을 의미한다"(Lowenthal 2008, 12).

국가정보의 개념만큼이나 국가안보의 개념도 포괄적이고 유동적이다. 간첩, 사보타주, 그리고 외국을 위한 개인들의 행동 등 국가안보 위협요소들로부터 국가와 국민, 국가이익을 지키는 것은 국가의 지정학적 안보환경과 역사적 경험, 국민의 위협인식 등에 따라 가변

적이다. 냉전에서 출발하여 9·11 테러와 코비드-19 팬데믹, 팔레스타인 무장 정파인 하마스의 10·7 이스라엘 기습을[7] 거치면서 "모든 것이 국가안보가 되었다"(Drezner 2024)고 해도 과언은 아니다. 국가들이 다른 국가들로부터 비밀을 지키려고 애쓰는 한, 그들 국가는 서로 그 비밀을 훔치려고 한다. 국가정보 활동은 그 기술과 기법이 계속 진화하더라도 여전히 국가 행위의 통합된 부분이고 앞으로도 그럴 것이다(Burns 2024).

결국, 냉전은 실은 끝나지 않았으며, 그 외양과 과학기술력이 달라졌을 뿐이다. 디지털 독재국가들이 자국 사회를 모니터하고 통제하기 위해 개발한 데이터 분석과 AI 능력은 이제 서방국가들을 겨루는 '화살이고 단검'이다.

중국과 러시아 정보기관들의 사이버 간첩(cyber espionage)은 사이버 공격을 하여 시스템을 교란하거나 물리적인 파괴를 노리며, 데이터와 지식자산을 훔친다. 2014년 3월 러시아는 우크라이나의 크림반도 점령 과정에서 사이버상의 데이터 절도 및 이를 조작하는 사이버 간첩 활동을 위주로 했다(김상배 2020, 13-14). 러시아 푸틴 대통령의 연방보안국(FSB)과 해외정보국(SVR), 군사정보국(GRU)은 서방의 선거에 개입하여 민주주의의 근간을 흔든다. 나아가 규칙 기반의 국제질서를 훼손한다. 2016년 미국 대통령선거 개입이 대표적 사례이며, 2024년 11월 미국 대선도 좌시하지만은 않았을 것이다. 시진핑의 국가안

7) 2023년 10월 7일 유대인의 안식일 오전 6시 30분, 가자지구의 팔레스타인 무장 정파인 하마스가 이스라엘에 침투해 수 시간을 광란했다. 양민 1400명 이상과 무방비 군인이 폭사하고 처참히 살해됐다. 220명 넘게 인질로 잡혔다. 이스라엘판 9·11이자, 홀로코스트 이후 최악의 유대인 학살이다(조경환 2023). 이는 이스라엘의 반격으로 이어져 2024년 10월 말 기준, 전쟁 1년 넘기고 있다.

전부(MSS)는 2005년 미국 정보기관과의 전쟁을 선포한 이후, 최고의 자원과 정보관들을 미국 정부와 기업 쪽에 투입하고 있다. 과학 및 기술 비밀데이터를 훔쳐서 중국의 경제와 군사력을 뒷받침한다. 중국의 개인 정보 및 지식자산 절취는 체계적이고 산업적 규모이며, 통제가 안 되는 청부업자를 고용하는 식의 해커 생태계를 운용한다(THE CIPHER BRIEF 2024-1-22).

'철의 장막'은 종언을 고하지 않았으며, 과학기술의 장막으로 대체되었다. 물리적 침투는 사이버공간의 침투로 전환됐다. 일례로, 1956년 4월 소련 국가안보위원회(KGB)와 동독의 정보요원들이 미국 CIA가 영국 비밀정보국(MI6)과 공동으로 도청을 위해 베를린 거리의 지하에 뚫은 터널을[8] 발견하고 달려왔을 때, 당시 CIA 지부장은 기관총을 겨눈 채 "이 선을 넘으면 미국 관할구역"이라며 허가받지 않은 사람의 진입을 막았다. 그런데, 현재의 지부장들은 적의 네트워크 침투를 차단하기 위한 노력의 일환으로 자신들의 맥북(MacBook)에 가상사설네트워크(VPN)를 설치해서 IP 추적을 피하고 있다(THE CIPHER BRIEF 2024-1-22).

과학정보(TECHINT)에 의한 데이터의 수집, 처리와 분석은 '양날의 검'이다. 국가정보 수집·분석은 물론 방첩에도 똑같이 이점을 준다. 2023년 10월 7일 이스라엘이 하마스의 기습을 받은 것은 과학기술 과신이 초래한 일면이 있다. 상당 규모의 공격 준비는 이스라엘과 미

8) 작전명 "Operation Gold", 미국 CIA와 영국 MI6는 베를린 칼쇼스트(Karlshorst)에 있는 소련 공군사령부로 들어가는 전화 및 전신선을 도청하기 위해 1951년 공동으로 터널을 팠다. 지하 6m에 직경 2m, 길이 450m이다. 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 알렸다(Shulsky & Schmit 2007, 254-255).

국, 영국 등 서방의 위성, 신호정보 및 정교한 사이버 기술로 사전에 대부분 탐지된다고 이스라엘 방위군(IDF)은 인식하고 있었다. 이스라엘은 하마스를 과소평가했다. 하마스는 그 오인식과 분석관의 상상력 결핍을 파고들었다. 이란으로부터 사이버 기술을 지원받고 있는 하마스는 공격 의도를 숨기기 위해 철저하게 은닉했고 기만했다. 하마스의 방첩성공이 이스라엘에는 정보실패였다(조경환 2023).

디지털 흔적은 남겨도 문제가 되고, 없어도 의심을 받는다. 소셜 네트워크들은 CIA에게 엄청난 양의 새로운 정보를 주고 있다. 반면에, 거대한 새로운 약점에 노출된다. 디지털 흔적(digital footprints)은 정보목표를 찾아내게 하지만, 디지털 먼지(digital dust)는 CIA 공작관의 인원 보안을 허물 수 있고(Cohen 2015), 비밀공작을 더 어렵게 한다. AI와 생체 데이터 활용은 흔해졌다. 스마트 도시의 거의 모든 거리에는 CCTV, 비디오카메라가 있다. 거대한 카메라 네트워크는 공작관들의 움직임을 추적한다. 공항의 얼굴 스캐닝은 스파이들이 얼굴을 노출하지 않고서는 국경을 드나들기 어렵게 만들었다.

얼굴인식 기술은 갈수록 보편화한다. 안면인식 회사인 미국 '클리어뷰 AI(Clearview AI)'는 러시아가 우크라이나를 침공한 몇 주 뒤인 2022년 3월, 우크라이나 정부에 러시아 병사들의 생사 및 전쟁 난민들 확인을 위한 얼굴인식 앱과 기술 제공을 제안했다. 현재, 우크라이나 국방부와 경찰청 등이 클리어뷰 AI 계정에 가입해서 서비스를 받고 있다. 클리어뷰 AI는 러시아판 페이스북인 브콘탁테(VKontakte)를 포함한 공공 웹으로부터 획득한 20억 개 이상의 얼굴 사진 데이터베이스와 대조해서 사망자와 스파이들을 인식한다(Hill 2022).

빅데이터 마이닝은 공작관들의 활동 패턴을 포착한다. "뉴욕 타임즈의 보도에 의하면, 2010년 중국 내에 있는 CIA의 가장 중요한 네트

워크가 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.

3. 미국의 대중국·러시아 데이터 주권 각축 및 데이터안보 법제화

데이터는 "21세기 원유"라는 비유가 진부할 정도로 4차 산업혁명 시대의 필수 자산이 되었다. 데이터는 처리되지 않고, 정제되지 않은 생 자료들의 조각들 및 부분들로 정의된다. 그것이 체로 걸러지고 나면 정보 혹은 실행 가능한 지식이 된다(Falode 2021, 72). 클라우드 서버 간 접속 과정에서 일시적으로 생성되는 세션 데이터와 프라이버시 데이터에서부터 기업의 핵심기술 혹은 영업비밀, 그리고 국가의 금융·보건의료·교육·외교·국방 빅데이터까지 다양하고 방대하다. 이들 데이터는 디지털화되고 네트워크에 연결되어 디지털 저장매체에 저장된다(윤정현 2004, 1-2). 그리고, 그 저장과 유통의 특성상 사이버 공격에 취약하다. 데이터 유출(data breach) 혹은 탈취, 데이터 조작(data manipulation), 데이터 오염(data poisoning), 허위조작정보(disinformation)에 의한 영향 공작(influence operations)에 노출되어 있다. 각국이 데이터의 활용 진작과 함께, 상쇄적 속성인 데이터안보에 골몰하는 이유이다. 데이터의 기밀성(confidentiality)과 무결성(integrity), 그리고 가용성(availability) 보장이 그 목표다.

중국과 러시아는 데이터를 전략 자산으로 인식하고 데이터 주권

(data sovereignty)을 추구한다. 자국에서 생성된 데이터는 자국 내 정보시스템에 그 데이터가 보관되어야 한다는 데이터의 현지화(data localization)를 법제화하며, 국경 간 데이터 이전에 대한 국가 통제를 강력하게 한다. 소스 코드 강제 이전을 요구하고, 개인 정보 보호를 강조한다. 그리고는 목표 국가들에 대해 무차별적 데이터 절취, 파괴와 오염, 영향 행사와 조작을 시도한다.

중국은 2008년 도입된 정보보안등급보호규정(MLPS), 2016년 인터넷안전법 제정, 그리고 2019년 본격 시행한 사이버안보법(CSL) 등의 법제를 갖추어 네트워크 탐지와 데이터 보안을 강화하고 있다. 공안부(MPS)와 국가안전부가 주축이다. 국가인터넷정보판공실은 데이터의 현지화를 지탱한다. 데이터의 보안성을 평가해 외부유출의 흐름을 통제한다. 2020년 시행된 외국투자법은 외국인 투자기업의 특별지위를 없앴다. 2023년 7월 1일 발효된 개정 반간첩법은 다국적 기업들에 대한 데이터 규제를 대폭 강화했다. 데이터의 탈동조화(decoupling)가 진행되고 있는 양상이다. 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[9] 본격화를 예고했다.

러시아도 2019년 11월 1일 인터넷주권법(sovereign internet law)을 발

9) '샤프 파워'는 미국 비영리 싱크탱크인 '민주주의기금'(NED; National Endowment for Democracy)이 제시한 개념이다. 권위주의 정부가 다른 나라의 내정에 알게 모르게 영향을 미치는 전략이다. 음성자금, 유인, 매수, 강압 등 탈법 수단과 허위정보를 동원해 상대를 강제한다. 상대의 정치체제, 사회제도, 가치 등의 신뢰를 저해하고 혼란과 분열을 조장하며, 체제를 부정하는 것이 목적이다(심종현·제성훈 2022).

효시켰으며, 이를 통해 러시아만의 독자 인터넷망 구축을 합법화했다. 데이터의 국외 이전을 국가안보 목적으로 통제해 오고 있다.

데이터의 자유로운 이동을 보장해 왔던 미국은 데이터 정책의 전환을 가져왔다. "자유, 프라이버시, 자유로운 정보의 흐름"을 사이버 안보(채재병·김일기 2020)와 데이터 안보정책의 근본으로 하여, 빅 테크를 중심으로 한 자유로운 데이터 이동을 보장해 왔던 미국이다. 그렇지만, 이제 미국은 이를 재고하고 있다. 그리고 맞대응 책을 속속 내고 있다. 중국이 미국의 개인 정보 등 데이터에 무단 접근해 국가안보와 프라이버시를 위협하는 것을 묵과하지 않을 태세이다. 2021년 6월 행정명령 제14034호는[10] "외국의 적으로부터 미국인들의 민감 데이터를 보호하는 조치를 담았다. 2022년 9월 행정명령 제14083호는[11] 외국인의 대미 투자에 대한 미국 국가안보 영향 평가를 강화했다(박주희 2024).

2022년 10월 발효된 행정명령 제14086호는[12] 신호정보 활동에 대한 미국민, 동맹·파트너 국민의 개인 정보와 시민 자유 보호를 강화하려는 조치이다. 1년 내 법무부 장관, 국가정보장(DNI) 산하의 시민자유보호관(CLPO; Civil Liberties Protection Officer)[13], 그리고 프라이버

10) Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries, June 09, 2021

11) Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States, September 15, 2022

12) Executive Order on Enhancing Safeguards For United States Signal Intelligence Activities, October 07, 2022

13) CLPO는 2004년 정보개혁 및 테러방지법(Intelligence Reform and Terrorism Prevention

시·시민자유감시이사회(PCLOB; Privacy and Civil Liberties Oversight Board)의 자문 아래 정책과 절차를 업데이트해 가게 했다. 또한, 법무부 장관에게 60일 내 개인정보보호평가법원(DPRC; Data Protection Review Court) 창설을 위한 규정을 공포하라고 했다. DPRC는 2023년 10월 만들어졌으며, 개인 정보 이전 및 보호를 관리, 감독할 시스템을 갖추게 됐다.

2024년 2월에는 미국민의 민감 개인 정보를 국가안보 차원에서 보호하기 위한 행정명령 제14117호[14]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.

Act of 2004)에 의해 프라이버시와 시민 자유 보호를 위해 설립된 직위이다. CLPT(Civil Liberties, Privacy and Transparency) 사무실 운영 책임자이며 DNI에 직보한다(ODNI 홈페이지 2024-4-16 검색).

14) Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, FEBRUARY 28, 2024

Ⅲ. 미국 정보공동체의 의사결정정보 요구와 데이터전략

1. 진전된 기술과 의사결정: 의사결정 정보와 데이터 과학의 융합

의사결정 과정은 해가 다르게 그 복잡성을 더해 간다. 코비드-19 팬데믹, 나날이 현실화하는 기후변화, 미·중 전략경쟁의 장기화 및 2022년 2월 러시아의 우크라이나 침공과 같은 지정학적 변동성의 증대는 '좋은 의사결정'(a good decision making)의 어려움을 가중한다. 모호함과 불확실성은 커지고 미래는 흐릿하다. 원인과 결과의 체인은 길어지고, 정책의 효과는 잘 보이지 않는다. 데이터의 소스는 휴민트와 테킨트를 망라하여 다양하며, 통합을 요구한다(Pratt et al. 2023). 이러한 도전요인들은 데이터에 기반한 의사결정과 데이터 사이언스에 눈을 돌리게 하고 있다.

AI의 도움을 받는 인간의 의사결정 프로세스는 그 숫자가 늘어나고 있다. 데이터는 폭증하는데, 그 데이터는 모두 평등하지는 않다. 가치 있는 데이터는 한정되어 있으며, 10%의 데이터가 90%의 전략적 가치를 지닌다(Pratt 2015). AI와 빅데이터 분석은 방대한 무가치의 '노이즈'와 유가치의 '시그널'을 분간해 낸다. 이미지를 분류하고 서류를 대조하며, 데이터에서 추세를 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 빠르

고 직관적이며 자동적인 “시스템 1”에 강하다. 느리고 분석적인 “시스템 2”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. 정보공동체의 데이터전략: ‘2023-2025 데이터전략’

“모든 것은 데이터로 시작한다.” 국가정보국(ODNI) 수석 부국장인 딕슨(Stacey A. Dixon)의 말이다. DNI 헤인스(Avril D. Haines)는 미국 정보공동체의 데이터 및 그 데이터를 적절하게 다루는 능력을 점증하는 복잡성과 상호 연결된 글로벌 안보환경에서 정보공동체가 그 강점을 유지하는 펀더멘털로 보고 있다(‘The IC Data Strategy 2023-2025’ 2023).

미국 정보공동체의 데이터전략은 임무와 비전, 가치로 이루어진다. 임무로는 정보공동체 데이터의 발견, 접근과 사용의 안전을 보장하여 빠르고 광범하게 가치와 통찰을 제공한다. 미국 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. 〈표1〉은 미국 정보공동체의 ‘2023-2025년 데이터 전략’이다(DNI 2023).

〈표 1〉 미국 정보공동체(18개 기관)의 '2023-2025 데이터전략'

임무	비전	가치
• 정보공동체의 데이터 발견, 접근 및 사용 안전 확보 • 빠르고 큰 규모로 가치 및 통찰 제공	의사결정 및 공작 이점에 부합하는 위치에 지정되고, 맞춤형의 데이터 기반 정보공동체(data-driven IC)	상호 연동, 공유, 파트너십, 혁신, 프라이버시와 시민자유권 보호

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

미국 정보공동체는 데이터 기반의 정보공동체를 최적화하고, 상호 정보교환, 공유, 파트너십, 혁신, 프라버시와 시민자유권 보호를 가치로 하여 4개의 전략적 영역에 집중한다. 첫째는 E2E(End-to-End) 데이터 관리를[15] 한다. 둘째, 데이터의 상호 정보교환과 분석을 신속, 광범하게 전달한다. 셋째, 계속적인 디지털 및 데이터 혁신을 위해 모든 파트너십을 진전한다. 넷째, 정보공동체 인력을 데이터 기반으로 전환한다.

이를 위해 DNI는 정보공동체의 최고데이터정보관(IC CDO: Chief Data Officer)과 최고데이터정보관위원회(IC CDOC: Chief Data Officer Council)를 두고 있다. 이들은 정보공동체의 직업적 윤리원칙을 강화

15) E2E(End-to-End) 데이터 관리는 데이터의 전체 수명주기를 포괄하는 접근 방식이다. 데이터가 생성되고 수집되는 시점부터 분석, 저장, 공유, 보호, 소멸 또는 보관 등 여러 단계를 거쳐 배포와 상호교환 등 최종적으로 사용되는 시점까지의 모든 과정을 포함한다('The IC Data Strategy 2023-2025' 2023, 1).

하면서도, 데이터의 수송, 섭취, 큐레이션,[16] 활용, 확산, 배포, 공유, 데이터의 사용 향상, 인력 개발 등 정보공동체가 취할 전략적 단계를 확인하며, 데이터 기반의 디지털 혁신을 추진하고 있다.

물론 정보공동체의 데이터전략이 순탄치만은 않을 것이다. 정보공동체 내의 각 정보기관은 오랜 독자성과 고유의 신비주의를 간직하고 있다. 이 비밀주의와 보안성은 칸막이문화(compartmentalization)를 유지하게 한다. 강력한 조직 및 직무 보안, 그리고 각 기관 내부에 잠재되어 있을 정통적 수집·분석 방식에 대한 관성적 신뢰가 저항 요인으로 작용한다.

Ⅳ. 미국 정보공동체의 데이터 기반 정보와 네트워크 거버넌스

1. 정보공동체의 신기술 및 데이터 기반의 연구개발

미국 정보공동체의 대량살상무기(WMD) 대응 능력을 조사한 WMD 위원회는[17] 2005년 3월 정보공동체의 '이라크 WMD 능력과

16) 데이터 큐레이션은 데이터를 수집, 정리, 구성하고 관리하여 그 가치를 최대화하는 과정이다. 데이터의 품질을 향상하고 의미 있는 정보를 도출하기 위해 데이터를 선택, 정제, 구조화하는 것을 포함한다. 데이터의 신뢰성을 보장하고 유용한 인사이트를 얻기 위한 작업이다.

17) 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)이다. 외국의 WMD 사용 혹은 잠

그 의도에 대한 수집 무능력과 연속적인 분석 실패'를 주요 정보실패로 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).

정보공동체의 연구개발은 데이터와 그 네트워크에 집중한다. 2006년 국가정보국(ODNI) 산하에 신설된 '정보고등연구계획활동'(IARPA; The Intelligence Advanced Research Projects Activity)은 AI를 통한 혁신 작업, 양자컴퓨팅의 적용 지원, 머신러닝 향상, 최첨단의 합성 생물학의 4개 분야에서 고위험, 고성과의 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. 정보공동체 내 정보기관들 및 산·학과의 협력에 무게 중심을 두고 있다. 공개정보를 주로 다룬다(Jani 2016). 공작 혹은 기술을 현장에 직접 적용하지는 않으며, 수집·분석·공작 등 정보공동체 정보활동의 효율 증진을 지원하고 있다.

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

재적, 위협적 사용과 관련 그 능력, 의도와 활동에 관한 미국 정보공동체의 능력과 도전을 조사했다. 2005년 3월 31일 "DNI 권한 강화, FBI의 국내정보 기능 제도화" 등을 권고했다(The WMD Commission Report to the President of the US 2005).

수집 기술, 이전에는 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) 당시 미국 국방부 장관은 '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 것에 사활이 걸려 있다.

1957년 10월 소련의 스푸트니크 1호 위성 성공에 충격을 받아 창설된 미국 펜타곤 산하 방위고등연구계획국(DARPA; Defense Advanced Research Projects Agency)은 아프간 전쟁(2001-2021년)에 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) 산하 시각화·데이터분석센터(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 국토안보부 소속의 비밀경호국(SS), 교통안보청(TSA), 연방이민국(USCIS), 연방재

난관리청(FEMA), 세관국경보호국(CBP), 해안경비대(CG) 등 22개 연방 기관들의 실시간 의사결정을 돕는다. 퍼듀대학의 CVADA가 주도해서 개발한 소셜미디어 분석 도구인 '스마트(SMART)'는[18] 사용자에게 '실시간의 지도화(mapping)와 탐색'을 제공한다. 또한, 거의 모든 프로 경기 리그에 고객 스크리닝 및 탈출 시뮬레이션 도구를 공급하여 스타디움의 팬들을 테러범의 위협으로부터 보호한다. 이는 럿거스대의 CVADA가 소프트웨어 기업인 '주식회사 리갈 디시전 시스템즈(Regal Decision Systems Inc.)'와 파트너십을 맺어 개발했다.

2. 미국 중앙정보국의 디지털 혁신

CIA 장은 2004년 국가정보장(DNI)이 정보공동체를 통할하기 전까지 중앙정보장(DCI)로서 정보공동체를 이끌어왔으며, 지금도 정보공동체의 디지털 혁신을 선도하고 있다. 이 같은 "혁신의 추진력은 컴퓨터 귀재들이 즐비한 NSA가 아니라 CIA 지도부가 위치한 '7층'에서[19] 시작되었다는 점"(Moran at al. 2023)은 주목할 만하다. CIA는 여전히 휴민트가 중심이지만, 신흥 기술의 숙달을 '사람 대 사람'의 기량과 조합시키고 있다. 오래된 수집, 처리, 분석의 기법에 하이테크를

18) 'Standard Management Analysis Reporting Tool (SMART)'은 SNS 분석 및 보고 도구의 모임이다. 이 시스템은 소셜미디어 게시물의 확장 가능한 분석 및 시각화를 분석관에게 제공한다. 주제 추출, 키워드 필터의 조합, 단어 클러스터 검사 및 이상 사건 감지를 사용하여 상황을 인식하게 하고, 시간이 촉박한 임무에 대한 의사결정을 향상한다(DHS 홈페이지 2024-4-14 검색).

19) 미국 정보공동체는 버지니아 랭리 소재 CIA 청사에서 수뇌부가 위치한 7층을 "The 7th Floor"로 별칭한다.

접목한다. 공작관들은 주재국에 의한 '빅 브라더' 식의 끊임없는 광범한 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 최고기술관(CTO; Chief Technology Officer)직을 신설하고 실리콘밸리 출신인 물찬다니(Nand Mulchandani)를 임명했으며, 내부의 과학기술 역량을 진작하고 있다. 민간영역과 더 좋은 파트너십을 전담하는 미션센터(Mission Center)도[20] 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 개발 중"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 오픈 AI의 챗GPT와 같은 AI 툴을 개발 중이다. 이 프로젝트를 두고 CIA 공개정보 책임자인 랜디 닉슨(Randy Nixon)은 2023년 9월 『블룸버그』와 인터뷰에서 "CIA와 NSA, FBI를 포함한 정보공동체 내의 '거대한 18개 정보기관 네트워크'를 향한 논리적, 기술적 발걸음"이라고 묘사했다(Popular Science 2023-9-27). 이는

20) 미션 센터는 국가안보 과제를 해결하기 위해 공작, 분석, 지원, 기술 및 디지털 역량의 전 범위를 하나로 묶어서 합동 근무를 통해 모든 기능을 자체적으로 수행할 수 있는 다기능 조직이다(신성순 2017, 132-136). CIA는 2015년 3월 조직을 개편해 미션 센터를 창설했으며, 현재 지역 및 우선순위의 임무를 수행하는 12개 정도의 미션 센터를 운용 중이다.

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)을 창설하여 디지털혁신 부국장에게 맡긴 것이다. DDI는 감지(sensing) 만능, 사이버 위협, 데이터의 기하급수적 증가라는 정보환경에서 외국의 사이버 공격으로부터 CIA와 민감 데이터를 보호한다. 공개 출처 수집, 데이터 과학, AI 및 기업정보 기술의 다분야를 융합(fusion)하며, 이를 바탕으로 정책결정자에게 필요한 판단정보를 제공한다(Cohen 2015).

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

2016년 3월, 데이터 관리와 데이터 플랫폼, 고등 분석전략과 관련한 '클라우데라 연방 포럼'에서 할만(Andrew Hallman) DDI 담당 부국장은 "CIA의 구식 정보수집 전략과 관료제로는 글로벌로 생성되는 정보의 가속화 속도를 견디어 내기 어려우며, 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 향상했다"고 밝혔다.

실제로 1977-81년간 카터 행정부의 CIA 장을 지낸 터너(Stansfield Turner)는『포린 어페어즈』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 좌파 정권을 무너뜨리기 위해 우파의 콘트라 반군을 지원할 때도 "산디니스타 정부에 대한 비콘트라 대중의 반대가 얼마나 강한지 몰랐다"면서 현지인들의 태도에 대한 무지가 결국은 하지 않아도 될 무리한 공작을 초래했음을 암시한 적이 있다. 이 같은 정보실패는 CIA의 데이터에 기반한 예측 노력으로 이어졌고, 그 예측 능력은 해외공작의 효율성과 효과성 증진에 큰 몫을 하게 되는 결과를 가져왔다고 볼 수 있다.

CIA는 '아마존 웹 서비스(AWS)'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.

2024년 1월, 디지털 혁신을 주도하는 DDI의 유뱅크(Jennifer Ewbank) 당시 부국장은[21] DDI의 임무로 ① "혁신하지 않으면 소멸한다(Innovate or Perish)."는 점을 절감하여 CIA 업무의 우선순위 조정 ②

21) 번스 CIA 장은 2024년 2월 7일, 유뱅크 후임으로 새 DDI 부국장에 줄리아니 갈리나(Juliane

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 미국 정보공동체는 민간기업에 대한 '패스트 팔로어'이다. 실리콘밸리와 긴밀한 파트너십을 형성하고 있다. "실리콘밸리는 정보공동체와 같은 일을 하고 있다"고 해도 틀린 말이 아닐 정도이다(전웅 2017). CIA와 정보공동체 기관들은 1999년 9월 테닛(George Tenet)이 CIA 장이던 시절, 독립된 민간의 비영리 회사로서 인큐텔(IQT)를 설립했다. CIA가 한때는 혁신의 리더였지만, 어느 순간 최첨단 기술과 혁신에서 소외되고, 영향력 있는 기술들이 실리콘밸리에서 나오고 있는 것을 인지하게 된 귀결이었다. 인큐텔은 기업, 벤처캐피털 자금, 일반사업체, 비영리단체, 정부의 연구개발 모델을 혼합했다. CIA가 국가안보 영역에서 시급한 문제를 파악하면, 인큐텔은 그것을 해결할 최신의 정보기술을 제공하며 국가안보에 결정적인 기술을 식별하고 분석한다. 이러한 생태계는 CIA가 결코 최고 자리를 놓쳐서는 안 될 영역인 기술 분야에서 선두를 유지하게 만들고 있다(Tenet 2009, 56-57).

3. 정보공동체의 데이터베이스와 네트워크 거버넌스

거버넌스를 이야기할 때 '집중 대 분산', '통합 대 경쟁'은 해묵은

Gallina) DDI 부국장보를 임명했다. 갈리나는 30년 이상 군사, 공무원, 산업 등 정보 및 기술 커뮤니티에 종사했으며, CIA의 CIO(Chief Information Office) 및 정보기술혁신 조직의 장을 지냈다(CIA 홈페이지, 2024-4-15 검색).

논쟁거리이다. 현대 조직들의 다중화와 도전요인들의 복잡성은 국가정보에서 더 중앙집중된 지시와 공작의 기준을 요구한다. 중앙집중적이고 피라미드식의 거버넌스는 수많은 독립된 기관들을 상호 연계된 단일의 구조로 묶음으로써 권한과 책임 소재를 분명히 한다. 의사결정과 그 집행의 과정 전체를 지배하고 선도할 한 개인을 정해 두어 불확실성을 줄이고, 합목적성과 효율을 기할 수 있다고 본다. 기관 간 경쟁 및 의심에서 유발되는 분석 결과물 공유기피 현상을 줄일 수도 있을 것이다(Jackson at al. 2009).

그렇지만, 중앙집중적 접근은 의사결정자의 광범한 대안 탐색을 방해한다. 컨센서스를 이룬 것처럼 보이는 것은 다른 문제들을 억압한 결과일 수 있다(최병선 2015, 87). 경쟁적 분석(competitive analysis)을 저해하고, 집단 사고(herd thinking)를 키운다. 정보의 볼륨이 너무 크고 광범해서 하나의 데이터베이스 거버넌스로는 감당이 힘들다. 내부의 각 기관이나 부문들이 보안을 우려해 정보 공유를 꺼릴 가능성이 발생한다. 정보 집중이 오히려 결심과 행동을 느리게 할 가능성이 있다(Posner 2004). 미국 정보공동체는 단일의 전속적 국내 정보기관을 세우는 것에 신중한 편이다. 대체로 분산된 기구들을 네트워킹하여 합목적성을 추구하는 접근법을 아직은 취하고 있다.

2013년 가을, 미국 정보공동체의 데이터 저장소인 유타 데이터센터(UDC)가[22] 신설되어 글로벌 네트워크 부상에 수반하는 디지털 데

22) 유타 데이터센터는 미국 정보공동체 최초의 종합 국가사이버안보이니셔티브 데이터 센터이다. 유타주 블러프데일(Bluffdale) 부근의 캠프 윌리엄스에 위치한다. 정보공동체를 도와서 국가를 모니터, 강화 및 보호 목적으로 설립되었다. 1.5억 불이 들어갔고, 100만 평방 피트의 부지에 거대한 20여 개 건물의 콤플렉스이다. 처리 용량 관련, 2012년 2월 유타주 개리 허버트 주지사는 "세계 최초로 요타(10^{24})바이트의 수집, 보관 시설이 될 것"이라고 했으나, 실제 용량

이터 급증에 대처하고 있다. NSA가 운용하며, NSA의 콜로라도, 조지아, 메릴랜드 등의 데이터센터와 상호 연동되는 네트워크이다.

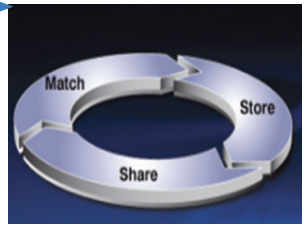
UDC는 개인 이메일, 휴대전화 통화, 인터넷 검색, 그리고 주차영수증, 여행 일정, 도서 구매, 소소한 디지털 데이터 등을 포함한 개인정보 흔적 등 모든 종류의 통신을 처리할 능력이 있는 것으로 추정된다. 2013년 6월 NSA 계약직인 스노든(Edward J. Snowden)이 "대량의 정보수집이 일반 시민에게까지 미친다"며 그 위험성을 폭로한 프리즘(PRISM)은 NSA가 운용하는 국가안보 목적의 컴퓨터 및 네트워크 감시 프로그램이다. 또한, UDC는 데이터 수집은 물론, DARPA와 합동으로 개발한 '암호 해독용 슈퍼컴퓨터 플랫폼'을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

9·11 테러 직후인 2001년 10월 도입된 미국 애국자법(USA Patriot Act)은 법 집행기관에 국내와 국제 전화 감청을 포함해 테러범 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.

UDC가 처리하고 저장하는 국내 감시 데이터는 프리즘 데이터 수집 프로그램, 미국 전역의 감청 기지들, 그리고 NSA 자체의 수집, 분석 도구를 사용해서 획득된다. 그리고 이 데이터를 처리, 분석해서 저장, 감시 및 모니터링, 범죄혐의 보고, 테러범검열센터에 경보 등 운영에 적용하고 있다. 〈그림1〉은 그 전 과정을 보여 준다.

은 국가기밀로 분류된다(Utah Data Center, NSA 홈페이지 2024-4-18 검색).

〈그림1〉 NSA의 시민 데이터 처리 과정도

시민 데이터, 수집	유타(UTAH) 데이터 센터	운영 적용(Operational Applications), 행동 결정
• 웹싸이트 방문 • 인터넷 탐색 • 전화 통화 • 스카이프 통화 • 이메일 • 문자 전송 • 신용카드 정보 • 금융정보 • 법률 문서 • 여행 서류 • 건강 기록	대조(Match), 저장(Store), 공유(Share)  참고 데이터 및 분석(analyze)	• 데이터 창고 (Data Warehouse) • 감시 및 모니터 • 의심 행동 보고 (Suspicious Activity Reporting) • 테러범검열센터 경보 (Terrorist Screening Center Alert)

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

한편, NSA의 광범한 감시는 인권 침해 논란을 초래했다. 테러 예방 및 국가안보 노력의 효과성도 아직 분명히 평가된 적은 없다. 그렇지만, NSA가 존재하기에 테러범들이 NSA의 감시 네트워크를 피하려고, 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.

미국 정보공동체는 "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, 분석이 잘될 수 없는 상황이다. 정보공동체의 국내 정보기관들은 국경을 넘나드는 테러리즘, 마약 거래, 밀수, 자금세탁, 조직범죄 등을 탐지, 처치하기 위해 구축한 데이터베이스 및 기관 간의 데이터를 연동하는 시스템을

구축하고 있다. 복합적 네트워크로 정보를 공유한다.

2005년 3월의 WMD 위원회 권고에 의거, 연방 국내정보의 중앙 기구화하고 있는 FBI는 미국 정보공동체 네트워크 거버넌스의 대표성을 띤다. FBI 내부 국가안보국(NSB)의 대테러부서(CTD)에서 테러범을 검열하는 데이터베이스(TSDB; Terrorist Screening Database)를 포함해 정보융합 및 데이터 활동을 수행한다. 해외테러범추적 TF(FTTTF; Foreign Terrorist Tracking Task Force)는 FBI가 주도하는 연방 정보기관들의 연합체이다. 모든 출처 데이터 흐름의 마이닝을 강조한다. 또한, 국가합동대테러 TF(NJTTF; National Joint Terrorism Task Force) 시스템은 56개 FBI 지부는 물론 주 및 지방의 법집행기관들과 연계되어 데이터를 공유한다(Jackson at al. 2009, 68-69).

국토안보부는 안보 목적에 직접 사용될 개인 데이터를 제공한다. 산하의 교통안보청(TSA)은 비행금지(No-Fly) 리스트와 요주의 리스트 데이터베이스를 운용한다. 국토안보부는 정보활동 임무 수행을 위해 정보시스템과 분석기법을 개발해 왔다. ADVISE(Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement)는 대량의 데이터를 분석하여 감시, 경보하는 소프트웨어 프로그램이다. 또한, 산하 세관국경보호국(CBP)은 옛 재무부의 테러리즘·자금 세탁·금융 데이터 시스템인 TECS(Treasury Enforcement and Communication Systems)를 업데이트하고 보완해서 입국 심사 및 결정에 운용하고 있다(Privacy Impact Assessment Update, CBP TECS-SAR 2024-5-4 검색).

이밖에도 법무부 마약단속국(DEA)의 정보와 조사 데이터, 국방부 국방정보국(DIA)의 대테러 데이터 및 국방정보시스템국(DISA; Defense Information Systems Agency)의 데이터 마이닝 능력이 국가정보 활동에 활용되고 있다.

이처럼 정보공동체 내 수많은 독립된 기관들이 각기 데이터를 저장, 공유, 활용하며, 다른 데이터베이스와 상호 연동한다. 기관별로 권한과 책임은 분산하고, 각기의 특수한 장점을 보장하되, 네트워크로 데이터베이스들을 묶고 있다. 그렇지만, 이 데이터베이스들을 하나의 리더십과 하나의 네트워크로 집중하는 중앙집중적, 피라미드식 거버넌스 구조의 필요성은 여전히 논쟁으로 남아 있다(Jackson at al. 2009).

V. 맺음말: 정책적 함의

전쟁이나 테러와 같은 위협이 닥칠 때면 국가정보에 주목하지만, 막상 그 위협 앞에서 정보는 실패했다. 이전에 겪어보지 못한 어떤 것을 예방하기 위해 효과적인 행동을 취한다는 것은 거의 불가능하다(Posner 2004).

미국 정보공동체는 2001년 9·11 이후 테러와의 전쟁, 2003년 이라크 전쟁을 거치면서, 실패하고도 혁신하지 않으면 생존하지 못하는 상황에 직면했다. 국가정보는 태생적으로는 냉전 시대의 폐쇄된 사회가 타깃이다. 국가안보와 번영을 위협하는, 공개적으로 얻을 수 없는 정보를 획득하는 데 그 목적이 있다. 냉전 때에는 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 앤드 포인트(endpoint) 등 너무나 많은 데이터 저장 수단이 네트워크화함에 따라 데이터 과잉의 '데이터 스모그(Data Smog)' 속에서 정보 판단을 해야 한다.

미국 정보공동체는 "모든 것은 데이터로 시작한다"는 인식 아래,

최고데이터정보관(IC CDO)과 최고데이터정보관위원회(IC CDOC)를 주축으로 하여 정보활동을 데이터 기반으로 최적화하고 있다. 공유와 파트너십, 시민자유권 보호 등의 데이터전략을 추진하고 있다. 또한, 자체 고등 연구개발과 함께, 외국기관, 민간기업, 학계와 파트너십을 통해 기술 혁신을 도모하고, 정보순환의 전 과정에 데이터와 AI 등 디지털 기술을 접목해 인간과 자동화 시스템이 콤비를 이루게 함으로써 정책결정자와 정보사용자에게 더 정확한 정보 판단을 적기에 제공하여 결심과 행동을 돕는다. 특히, 정보공동체 내 독립기관들이 테러리즘 등 국가안보를 위협하는 각종 데이터를 기관별로 대조, 저장, 활용하여 의심 행동을 적출한 뒤 상호 공유함으로써 각기의 강점을 살리되, 거대 네트워크로 각각의 데이터베이스들을 연동하는 거버넌스가 효과적으로 작동하고 있다.

정보의 혁명과 기술진보와 함께 국가정보의 기회와 위기는 폭증한다. 그러나 기습은 그것이 물리적이든, 사이버 영역이든, 예상하지 못할 장소, 시간, 방법을 택한다. 대규모 정보실패를 겪지 않은, 그래서 역설적으로 국가적 자산 동원에 불리한 한국으로서는 혁신을 통해 대비역량을 키우는 수밖에 묘수는 없다.

테킨트와 휴민트는 상호 보완적이어서 융합은 필연이다. 테킨트가 인간의 통찰을 제공하지는 않는다. 항공사진과 위성 정보, 신호 데이터 등은 군사적, 사이버 공격이 있기 전에 그 움직임을 밝히기 어렵다. 적의 심장부를 모르고서 그 의도를 조기 경보할 수는 없다. 더구나 군사적 움직임에 대한 경보는 실상 너무 늦어서 정책결정자에게 의미 있는 옵션을 제공할 수 없다. 휴민트가 여전히 효과적이며 신호정보는 보조재로 보는 게 현실성이 있다. 과학기술은 결국, 과학기술에 침해당한다. 데이터체계와 네트워크상에서 은닉될 경우는 속수무

책이다. 하마스의 10·7 공격 시 사이버 은닉이 그랬다.

첫째, 고도의 보안이 요구되고, 전통의 관료적 이익과 고정관념이 강한 정보기관의 특성상 데이터와 AI를 기존 정보활동에 접목하는 것은 난제(wicked problem)이긴 하다. 그렇지만, 데이터에 기반하는 국가정보 프로세스와 판단의 기제 구축을 늦출 수는 없다. 디지털화에 따른 보안 취약성과 내부 저항을 기회비용으로 삼아 하나씩 실행해 가야 한다. 미국 정보공동체는 DNI와 CIA 지도부가 이에 앞장서고 있음을 유념할 필요가 있겠다.

둘째, 한국판 정보공동체가 당면한 디지털 혁신의 현상과 그 미래, 그리고 도전요인을 진단해야 한다. 먼저, CIA를 원용한 디지털 혁신 전담부서와 전담 직위가 필요하다. 빅데이터·AI 전문가를 민간에서 영입해 혁신을 끌어가면 좋겠다. 그리하여 정보활동의 계획, 수집, 처리와 분석, 배포와 피드백의 전 과정에 걸쳐서 단계마다 디지털 혁신과 데이터에 입각한 조합이 이루어지도록 해야 한다. 정보기관들의 외곽 기업 설립 혹은 연구개발센터 운용도 권장한다. 마침 국가정보원이 2024년 9월 5일 국가안보기술연구원법 제정안을 입법 예고했다. 신기술로 파생되는 안보위협에 대응하고, 국가안보기술의 적기 수급 및 대학·연구기관 등과의 협력의 허브가 될 수 있을 것이므로, 국회의 초당적인 접근이 마땅하다.

셋째, 미국과 중국·러시아 모두 데이터안보 및 사이버안보 법제를 조밀하게 구축해 가고 있으며 글로벌 파급은 진행형이다. 더욱이 한국은 강력한 사이버 공격 주체로 자리 잡은 북한의 공격에 상시 노출되어 있다. 개인 프라이버시 보호와 국가안보 가치의 양립 속에서 침해 사익과 보호 공익의 비교형량을 통해 사이버안보 법제화를 진전시켜갈 필요가 있다. 현행 개인정보보호법, 신용정보의 이용 및 보호

에 관한 법률, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등 이른바 '데이터 3법'은 국가의 전략 자산으로서 데이터의 보호와 육성, 그리고 국가안보 관점의 관리 측면을 반영하지 못하고 있다는 것이 학계의 평가이다. 따라서, 관련법의 제정·개정 숙의와 함께, 필요시 우선 법령으로 법제화해 가고, 국가정보원 차원에서 데이터안보 전략과 지침을 수립해 부문 정보기관들을 선도할 지점에 와 있다.

넷째, 행정부 내 정보활동 기관들에 분산된 복잡한 각기의 데이터베이스를 큰 틀에서 점검하여, 상호 연동·공유하는 시스템이 유효하게 실행으로 연결되는지를 확인해야 한다. 각 기관의 데이터가 통합되고 적기에 이해되어 이상 징후를 포착하는 것은 실제로는 비현실적일 기대일 수 있다. 또한, 각 기관이 저마다 데이터 수집, 분석 역량의 특수성과 장점을 가지고서 창조적으로 접근하는 것은 타당하다. 그렇지만, 단순히 서로 데이터시스템에 접근만 제공하는 것으로 그치고, 협업의 행동으로 이어지지 않으면 그 효과는 반감될 것이다.

관련해서, 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 묶어 내는 것을 지향한다는 차원에서 국가정보기관이 데이터 댐 사업의 초기 단계에서부터 능동적인 참여가 요구된다고 하겠다.

다섯째, 공개출처정보(OSINT)를 핵심 국가정보로 제고시켜야 한다. 공개정보를 기존의 수집 및 분석기법에 더 시스템적으로 통합하며, 국가정보원의 공개정보센터(OSC)는 민간 매체와 파트너십을 통해 인적, 기능적 역량을 보강하는 한편, 이를 토대로 가짜뉴스, 악성의 허위조작정보에 대응할 메커니즘을 만들어 가야 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. 정보기관들은 민간의 '패스트 팔로어'임을 받아들이고, 파트너십을 더 과감하게 추진할 필요가 있다. 새롭고 이상하며 처음 보는 전쟁의 시대, 초연결성, 초불확실성의 이 시대에, 국가 정보기관의 정보 능력만으로는 결코 결정적이지 않다.

〈참고문헌〉

과학기술정보통신부 보도자료. 2020. “디지털 뉴딜의 핵심; ‘데이터 댐’사업 본격 착수.” (9월 2일).

김상배. 2020. “데이터 안보와 디지털 패권경쟁: 신흥안보와 복합지정학의 시각.” 『국가전략』 26권 2호, 5-34.

김진형. 2022. “중국 사이버안보의 전략과 체계.” 『CSF(중국전문가포럼)』. 대외경제정책연구원.

박주희. 2024. “데이터·AI 안보로 보는 사이버안보-데이터 규제를 둘러싼 미국과 중국의 대립.” 제7차 KACS 국가전략포럼. 한국사이버안보학회 국가전략연구위원회. 서울. 토론 (2월 6일), 83-87.

신성순. 2017. “국가 정보기구 구조개혁에 관한 연구-미국 정보공동체를 중심으로.” 건국대학교 박사 학위 논문.

심종현·제성훈. 2022. “러시아의 ‘샤프 파워(sharp power)’ 전략과 서방의 대응: RT와 스푸트니크 뉴스를 중심으로.” 『중소연구』 45권 4호, 219-246.

윤정현. 2024. “사이버 안보와 데이터 안보: 데이터안보 측면에서의 사이버 공격 유형과 도전 과제.” 제7차 KACS 국가전략포럼. 한국사이버안보학회 국가전략연구위원회. 서울. 발표 (2월 6일), 1-18.

전웅. 2017. “빅데이터와 정보활동-미국 정보공동체 사례를 중심으로.”『국가정보연구』 10권 1호, 7-54.

정준표. 2009. “미국의 ‘Intelligence’ 개념 고찰.” 『국가정보연구』 제2권 1호, 7-46.

조경환. 2023. “반복되는 정보실패는 죽느냐 사느냐의 문제다.” 『시사저널』 1776호 (11월 7일), 94-95.

조재학. 2023. “[단독]국정원, 첫 산하기관 생기나…‘국가안보기술연구원’ 설립 추진.” 『전자신문』(12월 18일).

채재병·김일기. 2020. “주요국 사이버안보 전략과 한국에의 시사점.”『INSS 전략보고』 73권 (March). 국가안보전략연구원.

최병선. 2015. “윌다브스키의 정책학.” 『행정논총』 53권 4호, 47-104.

Allen, Greg, and Taniel Chan. 2017. Artificial Intelligence and National Security. Cambridge, MA: Harvard Kennedy School.

Andrew, Christopher and David Dilks (eds.). 1984. The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century. London: Palgrave.

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).

Boren, David. 1992. "THE INTELLIGENCE COMMUNITY: HOW CRUCIAL?." Foreign Affairs 71(3): 52–62.

Carpenter, Charli. 2016. "The Future of Global Security Studies." Journal of Global Security Studies 1 (1): 92–94.

Cohen, David S. 2015. Deputy Director Cohen Delivers Remarks on CIA of the Future at Cornell University. (Sept. 18).

CSIS. 2021. Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation. A Report of the CSIS Technology and Intelligence Task Force. Washington DC.

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

Drezner, Daniel W. 2024. "How Everything Became National Security." Foreign Affairs (August 12)

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

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

Gedeon, Joseph. 2023. "CIA's AI director says the new tech is our biggest threat, and resource." POLITICO (9/27/2023 08:17 PM EDT).

Gruber Craig W. and Benjamin Trachik (eds). 2023. Fostering Innovation in the Intelligence Community: Scientifically-Informed Solutions to Combat a Dynamic Threat Environment. Annals of Theoretical Psychology 19.

Hill, Kashmir.2022. "Facial Recognition Goes to War." New York Times (Apr. 7).

Jackson A. Brian, Darcy Noricks, and Benjamin W. Goldsmith. 2009. "CHAPTER THREE Current Domestic Intelligence Efforts in the United States." In The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency, 49-78. RAND's National Security Research Division.

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. 저· 김계동 역. 2008.『국가정보-비밀에서 정책까지』. 서울: 명인문화사.

Miles, Ian and John Rigby. 2013. "Demand-Led Innovation." In Innovation Policy Challenges for the 21st Century, edited by Deborah Cox and John Rigby, 36-63. NY and UK: Routledge of Taylor & Francis.

Moran, Christopher R., Joe Burton, and George Christou. 2023. "The US Intelligence Community, Global Security and AI: From Secret Intelligence to Smart Spying." *Journal of Global Security Studies*, 8(2): 1-18.

National Academies. 2022. Improving the Intelligence Community's Leveraging of the Full Science and Technoligy Ecosystem. NW Washington, DC.

Neale, Spencer. 2019. "CIA troubled as biometric tracking and digital footprints pull spies from the shadows." Washington Examiner (December 30).

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

Popper, Karl. 1963. Science: Conjectures and Refutations. In Conjectures and Refutations: The Growth of Scientific Knowledge(pp. 33-59). Routledge & Kegan Paul.

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).

Privacy Impact Assessment Update, CBP TECS-SAR. 2011. (August 5).

Roth, Marcus. 2019. "Artificial Intelligence at CIA." Emerj (November 22).

Shulsky, Abram N. and Gary J. Schmit 저· 신유섭 역. 2007.『국가정보의 이해-소리없는 전쟁』. 서울: 명인문화사

Tenet, George 저·이남규 역. 2009.『폭풍의 한복판에서』. 서울: 조갑제닷컴

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

The 9·11 Commission. 2004. The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States.

The WMD Commission. 2005. Report to the President of the United States.

Official Government Edition (March 31).

Tucker, Patrick. 2015. "Meet the Man Reinventing CIA for the Big Data Era." Defense One (October 1).

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

Van Puyvelde, Damien, Stephen Coulthart, and Shahriar Hossain. 2017. "Beyond the Buzzword: Big Data and National Security Decision-making." *International Affairs* 93 (6): 1397-1416.

Vinci, Anthony. 2020. "The Coming Revolution in Intelligence Affairs." Foreign Affairs (August 31).

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

Warner, Michael. 2002. "Wanted: A Definition of Intelligence." *Studies in Intelligence* 46(3): 15-22.

_____ and Kenneth McDonald. 2005. US INTELLIGENCE COMMUNITY REFORM STUDIES SINCE 1947. Center for the Study of Intelligence. Washington DC.

The recent digital-based data security within the U.S. Intelligence Community and the implications

Kyunghwan Cho | Graduate School of Governance, Sungkyunkwan University

This study examines how the U.S. secures digital data amid global competition with China and Russia for data dominance. It explores the strategies employed by the U.S. Intelligence Community to ensure data security, how data systems and their analysts integrate science and technology with human insights to assist in decision-making and intelligence activities, and the database integration structures at the federal level for managing security data, finally drawing implications from these findings.

In the digital era, the vast and diverse data, along with their rapid connectivity, has led to an explosion of data. This has resulted in data-driven thinking and national intelligence, providing policymakers with enhanced judgements. At the same time, adversarial forces have gained new tools for attacks, enabling them to steal, destroy, corrupt, and manipulate data, thereby exerting influence. With the most significant threats now residing in the digital domain, data has been positioned as a core element of national security. Recognizing data sovereignty as a national security and viewing data as a strategic asset, China and Russia impose strict controls on the cross-border transfer of data. Traditionally, the U.S. has guaranteed the free flow of data but is now responding by tightening privacy protections and blocking the mass transfer of sensitive personal data.

The data security initiatives of the U.S. Intelligence Community are based on digital innovation through its own advanced research programs and external partnerships, offering augmented solutions by combining human input with data and AI. The Community considers its capacity to manage data as fundamental to its strengths, focusing on the systematic storage, processing, analysis, distribution, and sharing of data. While each agency within the Community operates its own database with independent authority and responsibility, they are interconnected through network governance to effectively address national threats, including the identification of suspicious behaviors.

Keyword data security, Intelligence Community, digital innovation, national intelligence, network governance

* I greatly appreciate the valuable comments from the anonymous reviewers, which have helped improve the completeness of the paper.