국가전략연구위원회 이슈브리핑 27호 (발간일: 2024.5.5.)

데이터 안보 시대의 국가정보 방향[1)]

김일기 (국가안보전략연구원)

Ⅰ. 데이터 안보 시대와 국가정보

제4차 산업혁명 시대의 디지털 전환과 빅데이터 및 인공지능(AI)의 등장으로 데이터의 중요성이 높아지고 있다. 인터넷, 스마트폰, 각종 감지장치, 네트워크, 통신 장비 등 다양한 출처에서 빅데이터가 발생·수집되고 있으며, 거의 모든 자료가 디지털 데이터로 축적되고 있다. 글로벌 데이터의 규모는 2018년 33 ZB(330억 GB)에서 2025년도에는 175 ZB(1750억 GB) 이상으로 급격히 증가할 것이라는 보고도 있다.[2)] 인공지능을 통해 처리·분석되는 데이터는 대부분의 사회경제 활동에서 촉매로 활용되고 있으며,[3)] 경제·산업을 넘어 정치·외교는 물론 국가안보 분야로까지 그 활용성이 확대되고 있다. 세계 각국이 데이터 문제를 국가안보 관점에서 접근하는 데이터 안보 시대가 개막된 것이다.

데이터는 경제와 전쟁영역을 지배할 신기술과 관련된 군사・경제 안보의 필수적 자원이며, AI와 결합하면서 국가안보 영역에서 그 파급력이 더욱 확대되고 있다. 이러한 측면을 반영하듯이 최근 미·중 디지털 패권 경쟁은 반도체 등 첨단기술에서 데이터로 그 영역을 확대하고 있다. 데이터 안보 시대의 빅데이터는 인공지능 사이버, 우주 자율시스템 등 최첨단 산업의 기초 자원이며, 데이터를 얼마나 보유했고 어떻게 잘 활용할 수 있는지가 경제 안보와 군사 안보의 성패를 좌우한다고 할 수 있다.[4)] 한편, 데이터는 개인이나 집단의 정치적

1) 이 글은 2024년 5월 2일 제9차 사이버 국가전략 포럼에서 발표된 발표문을 수정보완한 것이다.
2) David Reinsel·John Gantz·John Rydning, *The Digitization of the World From Edge to Core*(IDC, 2018).
3) 정희영, "데이터기반 사회에서 데이터 주권 이슈와 대응기술 동향," 정보통신기획평가원, 『주간기술동향』(2020.4.1). pp. 1-12.

성향, 여론의 변화, 정부 정책에 대한 호감 및 호응도, 국내외 안보 위기 상황 포착, 국가 위기 발생 가능성 예측 등의 국가안보 분야에서도 다양하게 활용되고 있다.[5)]

데이터 안보 시대의 개막은 정보기관의 정보활동의 방식에 있어서 상당한 변화를 발생시키고 있다. 데이터와 인공지능의 등장에 따른 변화의 흐름에서 정보기관은 데이터가 보유하고 있는 의미와 데이터의 활용 방안에 대해 고민해야 한다. 이미 데이터 안보 시대의 도래와 함께 미국을 비롯한 선진국 정보기관들은 데이터를 활용한 첩보 수집, 정보 분석, 방첩 등 정보활동 역량 강화에 노력하고 있다. 데이터 안보 시대는 정보기관에 새로운 도전과 기회를 제공한다. 데이터 안보 시대를 맞이하여 정보기관은 기능과 역량을 강화하고, 새로운 기술과 전략을 통합하여 더욱 복잡해진 글로벌 안보 환경에서 효과적으로 기능할 수 있도록 준비해야 할 것이다.

Ⅱ. 첩보 수집과 정보 분석 역량의 혁신

첩보 수집은 크게 비밀 첩보 수집(clandestine collection)과 공개 첩보 수집(open-source collection)으로 분류할 수 있다. 비밀 첩보 수집은 수집 수단에 따라 인간정보(human intelligence, HUMINT) 수집과 기술정보(technical intelligence, TECHINT) 수집으로 구분된다.

정보활동에서 데이터의 중요성 증가와 AI의 도입은 기술정보의 비중을 높이고 있다. 특히 AI가 생산하는 산출물의 중요도가 증가함에 따라 국가 정보자산에서 기술정보가 차지하는 비중이 증대하고 있다. 이미 미국 CIA는 데이터의 중요도를 반영하여 기존의 과학기술국(Directorate of Science and Technology)에 추가하여 디지털 혁신국(Directorate of Digital Innovation)을 신설하였다. 디지털 혁신국은 사이버 대응, 공개 출처 수집, 데이터, AI 및 기업정보 기술 등을 담당하고 있다.

데이터 안보 시대가 도래하면서 공개 출처를 활용한 첩보 수집의 효용도와 중요성 역시 증가하고 있다. 인터넷과 정보기술 발전의 영향으로 첩보(information)와 정보(intelligence)의 차이가 불분명해지면서 공개 정보의 중요성이 중가하고 있다. 공개 정보는 가치 있는 정보를 위험부담 없이 저렴한 비용으로 합법적 수집이 가능하다는 점에서 비밀 첩보 수집 수단으로 획득할 수 없는 내용을 보충하는 보완적 기능을 수행한다.[6)] 공개 정보의 중요도가 증가하면서 미국은 2005년 국가정보장(DNI) 산하에 공개 정보 활용을 위한 공개출처센터(OSC: Open Source Center) 설치하였으며, 이후 2015년 CIA 디지털 혁신국(DDI)의 공개 출처 사업처(OSE: Open Source Enterprise)로 재편하였다.

---

4) 김민호, "디지털 패권경쟁 속 데이터 안보와 한국: 데이터 주권을 중심으로,"『워킹페이퍼』No. 159 (서울대 국제문제연구소 미래전 연구센터, 2023) p. 2.
5) 이상호, "빅데이터 기반 정보 수집·분석 체계구성 및 활용 방안,"『국가정보연구』제15권 1호(2022).
6) 전웅,『현대국가정보학』(서울: 박영사, 2016), pp. 154-161.

비밀공작 및 첩보 수집의 과정을 거쳐서 정보기관에서 최종적으로 생산하는 결과물은 정보분석보고서이며, 정책결정권자는 이에 기초하여 정책 결정을 내리게 된다. 정보학 분야의 저명 학자로 알려진 포커(Robert Folker)는 "정보 실패의 결정적 요인은 분석의 실패에서 기인한다"고 지적한 바 있다.[7] 정보 분석은 정보기관의 성패, 즉 정보 실패에 결정적인 영향을 미칠 수 있으며, 그로 인해 국가안보와 국익에 엄청난 파급효과를 초래할 수 있다는 점에서 매우 중요하다.[8]

4차산업의 도래로 불어닥친 정보환경의 변화에 따라 데이터와 AI를 이용한 정보 분석의 고도화가 가능해지면서 AI를 활용한 정보역량 강화가 정보기관들의 중요한 과제로 부상하고 있다. AI는 대량의 데이터 처리를 통해 실시간 정보를 제공할 수 있으며, 반복적인 작업을 자동화하고 새로운 데이터 분석 방법을 제공함으로써 정보 분석(Intelligence Analysis)에 새로운 돌파구를 제공할 것으로 기대되고 있다.[9] 최근 해외정보기관들은 위기 상황에 대비하여 텍스트와 같은 정형화 데이터뿐만 아니라 비정형 데이터를 분석하는 AI 프로그램의 개발에 주력하고 있다.[10] 이미 CIA는 MS 등 민간 기업들의 협조하에 미국 18개 정보기관의 분석관들이 사용할 수 있는 챗GPT와 같은 생성형 AI를 개발하는 것으로 알려져 있다.[11]

Ⅲ. 정보공유와 정보 협력의 확대

데이터 안보 시대에 들어서면서 정보활동은 '독점과 폐쇄'에서 '공유와 개방'으로 변화하고 있다.[12] 정보의 경계 구분에 따른 개별 정보기관의 정보독점과 보안 중시로 인한 폐쇄성은 정보 실패와 정보 왜곡으로 이어져 국가안보를 위협한다. 이러한 차원에서 본다면 정보공유와 정보 협력은 데이터 안보 시대를 맞이하는 정보기관이 갖추어야 할 필수적 요인이라고 할 수 있다.

데이터 안보 시대에 정보 실패의 방지는 분산된 정보의 통합성과 실시간 공유가 중요하며, 이를 위해서는 '정보통합 플랫폼'의 구축이 중요하다.[13] 정보공유 및 정보 협력을 위해서는 문자, 음성, 이미지로 된 데이터 정보를 신속하게 통합·분석하는 '정보통합 플랫폼'의

7) Robert D. Folker, "Intelligence in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods," Joint Military Intelligence College Occasional Paper Number Seven (Washington, D.C., January 2000), p.3.
8) 김일기 외, 『한국의 정보강국 전략(상)(하)』(서울: 국가안보전략연구원, 2021), pp. 113-114.
9) Daniel Ish, Jared Ettinger, Christopher Ferris, "Evaluating the Effectiveness of Artificial Intelligence Systems in Intelligence Analysis," RAND Corporation, 2021.
10) Daniel Ish, Jared Ettinger, Christopher Ferris, "Evaluating the Effectiveness of Artificial Intelligence Systems in Intelligence Analysis," RAND Corporation, 2021.
11) "CIA Builds Its Own Artificial Intelligence Tool in Rivalry With China," Bloomberg(2023.9.27).
12) 김일기·채재병. "정보 패러다임 변화와 정보 강국 전략." 『이슈브리프』 310호 (서울: 국가안보전략연구원, 2021).
13) 이길규 외 공역, 『정보분석을 위한 구조화 분석기법』(서울 박영사, 2016), pp. 23-32.

구축이 선결과제가 된 것이다. 오늘날 정보기관들은 전출처 정보(All-source Intelligence)에 기반하여 정보활동을 추진하기 때문에, 정보역량 강화를 위한 정보공유 통합시스템의 구축은 시급한 과제라고 할 수 있다.

CIA의 경우에는 'A-Space'라는 온라인 플랫폼을 개발하여 분석관들이 첩보 수집과 분석을 공유하고 협력하도록 하고 있으며, 정보고등연구기획국(IARPA)이 주도하여 개발한 Mercury 프로그램을 개발하여 운용하고 있는 것으로 알려져 있다.[14] 최근에는 정보 분석을 위한 AI 사용이 확산함에 따라 국가 정보공동체 내에서의 협력을 강화하고 있으며, 이를 위한 시스템 구축에 박차를 가하고 있다. 정보공동체 내에서 공동의 데이터 표준, 인가된 데이터 세트, AI 모델 평가 도구, 비밀등급을 통제하는 인터페이스 등을 포함하는 공동의 디지털 인프라를 구축하려는 시도들이 나타나고 있다.[15]

인공지능과 빅데이터로 대표되는 4차 산업혁명 시대에 들어서면서 전 지구적 분업화가 가속화됨에 따라 데이터에 대한 정보기관의 배타적 독점은 이제 불가능해졌고, 기존의 정보활동 방식으로는 새로운 안보 위협에 효과적으로 대응할 수 없는 한계에 봉착했다. 따라서 기존의 정보활동 방식을 획기적으로 전환하여 정보기관은 물론 민·관이 함께 수집·분석하고 이를 공유할 때 안보 위기에 보다 효과적이고 신속한 대응을 할 수 있다.[16]

데이터 안보 시대는 국가정보기관과 민간 부문 간의 정보 협력을 촉진하고 있다. IT 분야의 새로운 기술・기법은 정보기관보다 주로 민간 기업의 주도로 개발이 이루어지고 있다. 정보기관을 비롯한 정부와 산하 기관들이 다양한 연구 프로젝트를 수행하기는 하지만 각종 첨단기술을 개발하여 실제 현장에서 적용하고 유용성을 검증하는 데는 민간 영역이 훨씬 앞서 있다.

최근 번스 CIA 국장은 CIA가 처음으로 최고기술책임자(CTO)를 임명했으며 민간 부문과의 파트너십을 강화하기 위한 새로운 미션 센터도 설립했다고 밝힌 바 있다.[17] 한편, 새로운 IT 기술을 국가정보 분야에서 활용하기 위해 학계 및 민간 전문가들 간의 협업시스템을 관장하는 비영리 기구로서 1999년 설치된 인큐텔(In-Q-Tel) 조직도 주목할 만하다. 인큐텔은 자체적으로 R&D를 진행하지는 않지만, 광범위한 인터넷 정보의 활용, 정보보안, 분석 자료의 처리 및 관리능력 향상, 효율적 정보의 배포・관리체계 운용 등과 같이 CIA 업무를 기술적으로 지원하는 전문 인력을 관리하는 역할을 담당하고 있다.

정보기관 분석관들은 업무 특성상 비밀성을 중시하여 외부 전문가들과의 협력에 수동적이며 적극적인 태도를 보여주지 않는 경향이 있다. 그러나 인큐텔 조직처럼 내・외부 전문가들을 연결해 주는 협력체계의 제도화는 향후 정보기관과 민간의 상호 유기적 협력에 상

14) https://chat.openai.com/c/76392b7f-74cd-4f2e-8975-ed710a0cbb1f.
15) Michèle A. Flournoy, "AI Is Already at War: How Artificial Intelligence Will Transform the Military," Foreign Affairs(November/December 2023)
16) 김일기 외, 『한국의 정보강국 전략(상)(하)』(서울: 국가안보전략연구원, 2021), p. 11.
17) William J. Burns, "Spycraft and Statecraft: Transforming the CIA for an Age of Competition," Foreign Affairs(March/April 2024)

당한 기여를 할 것으로 보인다.

Ⅳ. 임무 중심 조직으로의 변화

미국 정보공동체 조직구조의 가장 큰 특징은 첩보 수집, 정보 분석, 비밀공작, 방첩 등 정보활동의 분야에 따른 기능별 전문화(specialization)이다. 이러한 기능별 전문화에 따라 미국 정보공동체는 CIA(비밀공작), FBI(방첩), NSA(신호정보), NRO(영상정보) 등 여러 개의 독립된 정보기관이 전문화된 임무를 수행하고 있다. 이러한 지나친 전문화 구조는 정보공유와 협력 즉, 정보통합에 결정적 장애요인으로 작용하였으며, 그 결과 2001년 9.11 테러를 막지 못하는 참담한 결과를 초래하였다. 미국은 9.11 테러 이후 정보통합의 필요성에 따라 국가정보장(DNI) 체제하에 정보공동체의 조직구조를 기능적 특성(functional specialities)보다 임무(missions) 중심으로 개편하였다. 미국 CIA는 2015년 3월 브레넌(John Brennan) 국장 주도하에 공작·분석 기능의 구분을 폐기하고 10개의 '미션 센터'를 설립하여 공작관, 분석관, 과학기술 담당관, 행정지원 담당관 등이 쟁점 현안 별로 한 팀을 이루어 근무하는 조직 개편을 단행했다.[18]

우리의 국가정보원 조직은 분야(해외, 북한, 방첩, 수사, 행정지원)와 기능(수집, 분석, 배포, 비밀공작 등)에 따라 분리되어 있다. 과거에는 이러한 기능 중심의 운영 모델이 적절했다고 볼 수 있지만, 데이터 안보 시대에는 임무 중심 조직으로 방향을 전환해야 한다. 특히 빅데이터와 AI를 활용한 정보 분석과 활동이 본격화되는 데이터 안보 시대에는 정보수집과 분석, 공작과 함께 기술이 융합하는 임무 중심의 조직 운영이 바람직하다.

임무 중심 조직 운영과 함께 정보기관 구성원의 채용과 훈련 역시 변화와 혁신이 필요하다. 데이터와 인공지능 등에 탁월한 업무 능력을 보유하고 혁신적이며 적응력이 강한 인력들을 많이 채용할수록 정보기관의 정보역량 역시 한층 증가할 것이다. 특히 국가정보 차원에서 빅데이터 활용과 AI 기술의 적극적 채택과 적용은 정보기관의 채용과 교육훈련 과정에서도 많은 변화를 초래할 것으로 기대된다.[19] 미국 CIA는 엔지니어와 기술자들의 채용을 위해 기술 요원들이 민간 기업과 정보기관 사이를 자유롭게 이동할 수 있도록 유연한 커리어 패스를 개발하고 채용 기간 및 절차도 간소화하고 있다.[20] 이들은 민간과 정보기관 간 협력에서 가교역할을 담당하고 있다.

---

18) 미국 정보공동체 조직구조의 개편에 대한 자세한 논의는 신성순, "국가 정보기구 구조개혁에 관한 연구-미국 정보공동체를 중심으로," 건국대학교 대학원 박사학위 논문 (2017), pp. 130-136.

19) 김성배, "최근 국가정보 혁신 동향과 정책적 고려사항 : AI 대응을 중심으로,"『이슈브리프』529호 (국가안보전략연구원, 2024.3.29), p. 5..

20) William J. Burns, "Spycraft and Statecraft: Transforming the CIA for an Age of Competition," *Foreign Affairs*(March/April 2024)

Ⅴ. 경제·기술 방첩과 디지털 정보 접근을 위한 법·제도 정비

데이터 안보 시대는 데이터를 둘러싼 경제 및 기술 방첩의 중요성을 증가시키고 있다. 데이터에 대한 보호와 AI 기술의 우위가 중요해지면서 세계 각국은 데이터와 AI 관련 경제 및 기술 방첩에 많은 관심과 노력을 기울이고 있다. 미국 바이든 대통령은 2024년 2월 28일 발령한 「우려 국가에 의한 민감한 대량의 미국인 데이터 및 미국 정부 관련 데이터의 접근 금지」에 관한 행정명령(EO 14117)을 통해 중국, 북한, 러시아, 쿠바, 이란, 베네수엘라 등 '우려 국가'에 대한 데이터 이동을 제한하였다.[21] 한편, 국가안보국(NSA)는 AI 기술의 적성국 유출을 막기 위해 NSA 산하에 'AI 보안센터'를 설립하였다.[22]

데이터의 중요성이 증대되면서 사이버 공격 양상 역시 변화하고 있으며, 국가나 국가 배후의 악의적 공격집단들, 심지어 개인 수준에서 국가 기밀이나 기업의 지적 재산 확보 등 데이터를 노린 공격을 시도하고 있다. 이러한 공격의 유형으로는 고도화된 데이터 유출 공격 유형, 알고리즘의 오작동을 유발하는 데이터 오염 유형, 사실을 왜곡하는 데이터 조작·변조 유형, 민주주의 국가의 주권을 위협하는 영향공작 등이 있다.[23] 따라서 이러한 우리의 데이터를 비롯한 사이버 공격에 대비하기 위해서는 「사이버 안보법」 제정이 조속히 추진되어야 한다.

데이터와 인공지능 등 첨단기술 확보를 중심으로 하는 외국의 정보활동이 증가하는 상황은 우리에게 방첩 관련 법제의 정비가 필요함을 시사하고 있다. 우리는 경제 방첩을 「산업기술 유출방지 및 보호에 관한 법률」에서 규정하고 있으나, 침해행위의 내부 주체에 초점이 맞추어져 외국이나 외부 세력에 의한 침해행위에 대해서는 처벌 조항이 불분명하다. 따라서 외국의 경제이익 침해로부터 우리의 국익을 보호하기 위해서는 「경제간첩법」과 「외국인 등록법」 등의 제정을 통한 법적 근거 확보 노력이 필요하다.

정보기관의 디지털 정보 수집 권한과 관련한 법·제도의 정비 역시 필요하다. 미국은 정보기관이 국가안보상 필요시 데이터 정보의 수집을 보장하는 법·제도적 장치를 운용하고 있다. 미국은 「해외정보감시법」(Foreign Intelligence Surveillance Act, FISA)과 대통령 행정명령 12333호(Executive Order 12333, EO 12333)에 근거하여 데이터를 수집·보관하고 있다. 특히 FISA 제702조에 따르면, 정보기관은 영장 없이 통신회사나 인터넷 서비스 제공업체로부터 데이터를 수집할 수 있다. 이 법안의 2023년으로 종료되어야 했으나 지난 연말 「국방수권법」에 묶여서 4개월 연장되었으며, 올해 4월 12일 하원을 통과하고 상원에 상정될 예정이며 통과될 경우 2년 더 연장될 예정이다.

---

21) 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

22) "NSA announces new artificial intelligence security center." Fox News(2023.10.3)

23) 윤정현, "사이버 안보와 데이터 안보," 한국사이버안보학회, 『이슈브리핑』 19호(2024.2.10), pp. 2-5.

데이터 안보 시대에 정보기관의 디지털 정보 수집은 필수적인 요소이다. 우리의 경우 디지털 정보수집을 규정하고 있는 「통신비밀보호법」과 「국가정보원법」은 효율적인 디지털 정보활동을 보장하기에는 미흡하다고 할 수 있다. 디지털 데이터에 대한 접근의 중요성을 고려한다면 디지털 정보수집 활동에 대한 권한과 방법 등을 법률로 규정해야 한다. 잠재적 오남용 역시 법률에서 명확하게 규정한다면 투명성을 보장할 수 있을 것이다.

<참고자료>

김민호, "디지털 패권경쟁 속 데이터 안보와 한국: 데이터 주권을 중심으로,"『워킹페이퍼』No. 159(서울대 국제문제연구소 미래전 연구센터, 2023).

김성배, "최근 국가정보 혁신 동향과 정책적 고려사항 : AI 대응을 중심으로,"『이슈브리프』529호(국가안보전략연구원, 2024.3.29).

김일기 외,『한국의 정보강국 전략(상)(하)』(서울: 국가안보전략연구원, 2021).

김일기·채재병. "정보 패러다임 변화와 정보 강국 전략."『이슈브리프』310호 (서울: 국가안보전략연구원, 2021).

신성순, "국가 정보기구 구조개혁에 관한 연구-미국 정보공동체를 중심으로," 건국대학교 대학원 박사학위 논문 (2017).

윤정현, "사이버 안보와 데이터 안보," 한국사이버안보학회,『이슈브리핑』19호(2024.2.10).

이길규 외 공역,『정보분석을 위한 구조화 분석기법』(서울 박영사, 2016).

이상호, "빅데이터 기반 정보 수집·분석 체계구성 및 활용 방안,"『국가정보연구』제15권 1호(2022).

전웅,『현대국가정보학』(서울: 박영사, 2016).

정희영, "데이터기반 사회에서 데이터 주권 이슈와 대응기술 동향," 정보통신기획평가원,『주간기술동향』(2020.4.1).

Daniel Ish, Jared Ettinger, Christopher Ferris, "Evaluating the Effectiveness of Artificial Intelligence Systems in Intelligence Analysis," RAND Corporation, 2021.

David Reinsel·John Gantz·John Rydning, The Digitization of the World From Edge to Core(IDC, 2018).

Michèle A. Flournoy, "AI Is Already at War: How Artificial Intelligence Will Transform the Military," Foreign Affairs(November/December 2023)

Robert D. Folker, "Intelligence in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods," Joint Military Intelligence College Occasional Paper Number Seven (Washington, D.C., January 2000).

William J. Burns, "Spycraft and Statecraft: Transforming the CIA for an Age of Competition," Foreign Affairs(March/April 2024)

"CIA Builds Its Own Artificial Intelligence Tool in Rivalry With China," Bloomberg(2023.9.27).

"NSA announces new artificial intelligence security center." Fox News(2023.10.3)

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

※ 이슈브리핑에 수록된 내용은 필자 개인의 의견이며, 한국사이버안보학회의 공식적인 입장이 아님을 알려드립니다.