ISSUE BRIEF

이슈브리프 529호
(2024. 3.29)

최근 국가정보 혁신 동향과 정책적 고려사항 : AI 대응을 중심으로

제529호

김성배 안보전략연구실

국가안보전략연구원
Institute for National Security Strategy

INSS
www.inss.re.kr

국문초록

AI 기술 혁신은 신호정보, 지공간정보 등 과학정보에 대한 대규모 투자와 비중 증대를 초래하고 있으며, 국가정보기관과 민간 부문 간의 정보협력이 갈수록 활성화되고 있다. 국가간 경쟁에서 AI 기술 우위를 점하기 위하여 각국은 경제 및 기술 방첩에 많은 자원과 역량을 투입하고 있다. AI를 활용한 정보 분석과 활동이 본격화되고 있으며, 이를 위해 분석(analysis)-공작(operation)-기술(techology)을 융합하는 임무 중심의 조직 구성 방식이 확대되고 있다. 민관을 오갈 수 있는 유연한 커리어 패스를 제공하고, AI 교육을 강화하는 등 정보기관의 채용과 교육훈련에서도 많은 변화가 나타나고 있다. AI 시대에 대량의 디지털 정보 수집의 효율성과 투명성을 동시에 제고하기 위한 법제도 정비도 중요한 이슈이다. 국가 정보공동체 내의 AI 기술 협력을 보장하고, 심화하기 위한 인프라 구축도 활발히 추진되고 있다. AI 시대에 우리의 국가정보 대응력을 강화하기 위해서는 첫째, AI 등 과학정보 자산에 대한 과감한 투자와 첨단 기술 기업들과의 민관 협력의 적극적 활성화가 필요하다. 둘째, AI 기술의 정보활동 적용을 본격화하기 위해 임무 중심의 융합조직 활성화를 검토할 필요가 있다. 셋째, AI 시대에 정보기관의 효율적 정보활동과 투명성을 동시에 보장하고 법적으로 보호하기 위한 법제도 정비가 절실히 요구된다.

핵심어 : AI와 국가정보, 신호정보, 지공간정보, 정보활동(espionage)과 기술, 정보공동체, 정보활동과 법적 이슈

최근 생성형 AI로 돌파구가 마련된 AI 기술의 혁신은 인간 삶의 전 영역에 침투하고 있으며, 외교안보 분야 역시 예외가 아니다. 국방, 외교, 정보 등 모든 분야에 AI 기술이 이미 적용되고 있거나 AI 기술을 접목하는 시도가 활발히 전개되고 있다. 특히, 인공지능(Artificial Intelligence)라는 용어 자체에 '정보'(intelligence)라는 말이 포함되어 있다는 사실이 시사하듯이 AI 기술이 국가정보 분야에 미치는 파장은 매우 직접적이고 심대하다.

무엇보다 AI 기술 혁신은 과학정보에 대한 대규모 투자와 비중 증대를 초래하고 있다. 최근 AI 기술은 언어, 영상, 음성, 신호 등을 중심으로 발달하고 있는 바, 이러한 신호와 데이터들을 다루는 과학정보 부문이 가장 직접적으로 AI의 영향권 하에 있다. 흔히 '신호정보'(signal intelligence)와 '지공간정보'(또는 영상정보; geospatial intelligence) 등으로 불리는 영역이다. AI의 도움으로 인간의 능력으로는 처리할 수 없는 방대한 신호와 데이터를 수집하고 분석하는 것이 가능해졌기 때문에 과학정보에 AI 기술을 접목하기 위한 투자는 필수적이다. 또한, 인공위성과 다양한 센서들의 확산 덕분에 지구상 모든 사물이 동시에 관측될 수 있는 '지리정보 특이점'(GEOINT Singularity)을 목전에 두고 있는 상황에서, 지공간정보 처리를 위해서는 AI 기술의 장착이 필수적으로 요구된다.[1] AI가 생산하는 유용한 산출물들로 인해 전체 국가 정보자산에서 과학정보가 차지하는 비중도 비약적으로 증대되고 있다. 미국의 경우 신호정보를 다루는 국가안보국(NSA)나 지공간정보를 다루는 국가지리정보국(NGA) 뿐만 아니라 전통적 스파이 활동 중심의 CIA에서도 과학정보에 대한 투자를 강화하고 있다.[2]

---

1) Anthony Vinci, "The Coming Revolution in Intelligence Affairs: How Artificial Intelligence and Autonomous Systems Will Transform Espionage," *Foreign Affairs*(2020.8.30.)

2) 미 CIA는 기존의 과학기술 부서(Directorate of Science and Technology)에 추가하여 디지털 혁신 부서(Directorate of Digital Innovation)를 신설하여 AI 등 신기술의 정보활동 적용에 주력하고 있다.

민관 정보협력의 확대와 경제·기술 방첩 강화

국가정보기관과 빅테크 등 민간 부문 간의 정보협력이 갈수록 활성화되고 있다. 대부분의 정보기관에는 과학기술 파트가 있지만 AI 혁신이 워낙 빠른 속도로 이루어지고 있는 탓에 내부(in-house) 기술에만 의존해서는 민간 주도의 기술 발전 속도를 따라잡을 수가 없기 때문이다. 오늘날의 AI 기술 혁신은 하나의 혁신이 또 다른 혁신으로 이어지는 자기 순환적 속성을 가지고 있으며, 가파른 혁신 속도라는 측면에서 과거와는 비교가 되지 않는다.[3] 따라서, 민간 부문에서 개발되고 있는 기술을 사후에 채택하는 것이 아니라 민관 협력을 통해 동시에 개발해야 할 필요가 있다. 이와 관련, 최근 번스 CIA 국장은 CIA가 처음으로 최고기술책임자(CTO)를 임명했으며 민간 부문과의 파트너십을 강화하기 위한 새로운 미션센터도 설립했다고 밝힌 바 있다.[4]

구체적 사례로서, GPT 같은 민간의 거대언어모델(LLM)은 보안상 이유로 정보기관에서 활용하기 곤란한 바, 정보기관의 독자적 모델 구축이 동시적으로 진행되어야 한다. 이와 관련, 미 CIA는 MS 등 빅테크 기업들의 협조하에 NSA, FBI 등 18개 정보기관이 사용할 수 있는 생성형 AI를 개발하고 있는 것으로 알려지고 있다.[5] MS가 러시아, 중국, 북한, 이란 해커들이 오픈 AI 모델을 활용하여 훈련하고 있다는 것을 폭로하고 정부에 제보한 것도 민관 협력의 또 다른 사례로 볼 수 있다.[6]

---

https://www.cia.gov/about/organization/#directorate-of-digital-innovation

3) Eric Schmidt, "Innovation Power: Why Technology Will Define the Future of Geopolitics," *Foreign Affairs*, March/April 2023.

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

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

6) "Microsoft, OpenAI say U.S. rivals use artificial intelligence in hacking," The Washington

최근에는 미국 국가정찰국(NRO)이 일론 머스크의 우주기업 스페이스 X와 2조원대 비밀 계약을 맺고 수백개의 저궤도 위성을 연결하는 스파이 네트워크를 만들고 있다는 사실이 보도되기도 했다.[7] 중국은 민간 기업이 정부의 통제하에 있어서 새삼 민관 협력을 강화할 필요도 없지만 최근 들어 국가안전부(MSS)가 주도적으로 안면인식 등 AI 시스템 개발에 주력하면서 중국의 AI 기업들을 적극 활용하고 있는 것으로 알려지고 있다.[8] 심지어 북한도 김일성종합대학 인공지능기술연구소, 김책공업종합대 정보기술연구소 등 AI 개발 기관들을 2023년 최우수 정보기술 기업으로 선정한 것에서 보듯이, 최근 AI 개발과 활용에 몰두하고 있어 이를 정보업무에 적용할 가능성이 높다.[9]

민관 협력의 확대와 비례적으로 경제 및 기술 방첩의 중요성이 날로 증대되고 있다. 미중 전략경쟁을 포함하여 국가간 경쟁에서 AI 기술 우위를 점하는 것이 워낙 중요해졌기 때문에, 각국은 AI 관련 경제 및 기술 방첩에 많은 자원과 역량을 투입하고 있다. 경제·기술 방첩 능력의 제고를 위해서는 정부와 기업 양측의 이해와 협력이 절실히 요구된다. AI 기술의 우위는 단지 기업의 경쟁력과 이윤에 국한되는 문제가 아니라 국가 경쟁력을 좌우하기 때문에, 정보기관들은 AI 기술, 그리고 AI 개발의 토대가 되는 첨단 반도체 기술의 탈취와 유출을 막고, 경우에 따라서는 경쟁국의 능력 증대를 저지하는데에도 적극적으로 개입할 수밖에 없다. 이와 관련 미 국가안보국(NSA)는 AI 기술의 적성국 유출을 막기 위해 NSA 산하에 'AI 보안센터'를 설립하기도 하였다.[10]

Post(2024.2.14.)

7) "Musk's SpaceX is building spy satellite network for US intelligence agency, sources say," *Reuter*(2024.3.17.)

8) "Chinese Spy Agency Rising to Challenge the C.I.A." The New York Times(2023.12.27.)

9) 『노동신문』(2023.11.21).

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

AI 기술 적용의 본격화 및 임무 중심 융합 조직의 활성화

AI를 활용한 정보 분석과 활동이 본격화되고 있으며 이를 위해 분석, 공작, 기술을 융합하는 임무 중심의 조직 구성 방식이 확대되고 있다. 원칙적으로 정보기관의 분석이나 활동 부서는 과학기술 부서의 지원을 받지만, 조직문화상 같은 오피스에서 근무할 경우 시너지 효과가 극대화되기 때문이다. 또한, 분석관과 공작관이 같은 정보대상을 두고 협업할 경우의 융합 효과도 기대할 수 있다. 한편, 이러한 인간-기술 융합 조직의 활성화는 모사드의 하마스 공격 예측 실패에서 보듯이 과도한 기술정보 의존이 초래하는 정보실패를 미연에 방지하는 효과도 기대할 수 있다.[11] 미 CIA는 12개 이상의 미션센타가 존재하는 것으로 알려지는데 바로 이러한 임무 중심의 조직으로 구성되어 있다. 임무 중심의 조직에서는 기술 인력도 결합하여 AI를 활용한 정보분석이 더욱 본격화될 수 있으며, 공작관은 AI라는 무기를 장착하게 된다. 예컨대, 중국, 러시아, 북한 같은 독재국가 지도자들의 모든 연설, 언술 등 공개정보 및 휴민트 정보를 학습 데이터로 하는 거대언어모델을 개발하여 정책결정 방향을 추출해볼 수 있다. 방대한 영상과 이미지 데이터 학습을 토대로 군사 행동 패턴을 예측하는 것도 가능할 것이다. 학습 데이터만 정확하다면 결과값에서 "환각" 등 AI 오류를 최소화할 수 있을 것이며, 적어도 분석관들에게 풍부한 영감을 제공할 수 있을 것이다.[12]

국가정보 차원에서의 AI 기술의 적극적 채택과 적용은 정보기관의 채용과 교육훈련 과정에서도 많은 변화를 초래하고

11) Amy Zegart, "Israel's Intelligence Disaster: How the Security Establishment Could Have Unde restimated the Hamas Threat," *Foreign Affairs*(2023.10.11).
12) Michèle A. Flournoy, "AI Is Already at War: How Artificial Intelligence Will Transform the Military," *Foreign Affairs*(November/December 2023)

있다. 미 CIA는 엔지니어나 기술자들의 적극적 채용을 위해 이들 기술 요원들이 민간 부문과 정보기관을 자유롭게 오갈 수 있도록 유연한 커리어 패스를 개발하고 있으며, 채용 기간과 절차도 간소화하는 추세이다.[13] 기존 분석관, 공작관, 방첩관을 막론하고 기존 요원들에게 AI 등 첨단기술에 대한 교육과 훈련을 제공하여, 분석(analysis), 공작(operation), 방첩(counterintelligence) 활동에 AI라는 신무기를 장착하도록 하는 것은 물론이다.

정보기관의 디지털 정보 접근 및 투명성 보장을 위한 법제도 정비

정보기관의 디지털 정보 수집 권한과 관련한 법제도적 쟁점이 부각되고 있다. AI 기술의 급속한 발달에 따라 정보기관이 대량의 데이터를 보다 효율적으로 수집하고 분석할 수 있게 되었기 때문이다. 미국은 정보기관이 국가안보상 필요시 통신정보 수집을 보장하거나 비밀공작 수행시 면책 권한을 부여하는 법제도적 장치가 작동하고 있다.[14] 2008년 미 의회에서 통과된 「외국정보감시법 개정안」(FISA Amendments ACT, FAA) 702조는 정보기관이 영장없이 통신회사나 인터넷 서비스 제공업체로부터 데이터를 수집할 수 있게 보장하고 있다.[15] 원래 이 법안의 유효기간은 2023년까지였으나, 지난 연말 「국방수권법」에 묶여서 4개월 연장되었는데 그 후에는 새로운 법안이 채택되어야 한다.[16] 현재 「자유 보호 및 영장 없는 감시 종료 법안」(HR 6570)과 「FISA 개혁과 재승인 법안」(HR 6611)등 2개 법안이 경쟁 중인데, 전자가 연방정부가

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

14) 1981년 발효된 「행정명령 12333」은 정보기관이 코버트 액션을 수행할 때, 대통령 승인과 의회 통보 등의 절차를 규정하여 법적 보호와 면책을 제공하고 있다. 또한, 매년이나 주기적으로 의회의 승인을 받는 「정보수권법」(Intelligence Authorization Act)에서도 코버트 액션 절차를 제공한다.

15) 1978년 제정된 「외국정보감시법」(Foreign Intelligence Surveillance ACT, FISA)은 미국 정보기관이 통신 정보를 수집할 때의 법적 절차를 규정하고 있으며 비공개의 FISA 법원에서 영장을 발부하도록 하였으나, 2008년 개정안은 영장 없는 조사도 허용하고 있다.

16) https://www.theregister.com/2023/12/14/congress__renews__fisa__section__702/?ref=biztoc.com

조사 이전에 영장을 받도록 하고 있는 반면, 후자는 영장 없는 조사를 유지하는 것은 물론 연방정부와 데이터를 공유해야 하는 전자통신 기업들의 범위를 확대하고 있다.[17] AI 시대에 국가 안보의 효율적 증진과 개인의 자유와 프라이버시 보호 사이에서 적절한 균형점을 찾는 노력이 더욱 중요해지고 있다고 할 것이다. 바이든 행정부가 15개 주요 AI 기업들의 자발적인 협조를 토대로 2023년 10월 30일 발표한 「안전하고 신뢰할 수 있는 인공지능에 관한 행정명령」도 그러한 노력의 일환이라고 할 것이다.[18]

AI 기술의 채택이 확산됨에 따라 국가 정보공동체 내에서의 협력이 심화되고 있는 바, 이를 보장하기 위한 인프라 구축이 요구되고 있다. 신호정보이건 지공간정보이건, 위성이 수집한 것이건 사물인터넷 장치가 수집한 것이건 기본적으로 전자기 정보이기 때문에, AI 시스템으로 모든 데이터의 패턴을 동시에 인식하는 것이 가능하다. 통신 같은 민간 인프라도 군사 통신 시스템만큼 군사적으로 중요하기 때문에 민간 정보와 군사 정보의 구분도 애매해지고 있다. 따라서, 전통적인 정보 기능의 분리는 더 이상 큰 의미가 없으며 통합 관리되어야 할 필요성이 커지고 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.[19] 이는 정보공동체를 운영하고 있는 미국의 누릴 수 있는 상대적 잇점이라고 할 것이다.

---

17) https://www.theregister.com/2023/12/08/competing__section__702__surveillance__bills/

18) White House, "FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence."(2023.10.30.). https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

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

정책적 고려사항

첫째, AI 등 과학정보 자산에 대한 과감한 투자와 첨단 기술 기업들과의 민관 협력의 적극적 활성화가 필요하다. 관련 예산의 확대를 통해 고성능 정보위성, 다양한 센서, 수퍼컴퓨터, 데이터 센터 등 물리적 자산을 확충하는 것은 물론, 우수한 과학기술 인재들을 다수 충원하여 AI 시스템 개발과 교육훈련에 투입해야 한다. 이를 위해서는 민간 기업으로의 이직과 정보기관 요원으로의 복직이 수월하게 이루어질 수 있도록 유연한 커리어 패스를 제공할 필요가 있다. 이들은 민관 협력시 훌륭한 가교역할을 수행할 수 있다. 또한, 정보기관 내에서 모든 과업을 다 수행할 수는 없기 때문에 민간 기업에 임무를 부여하는 아웃소싱도 적극적으로 활성화해야 한다.

둘째, AI 기술의 정보활동 적용을 본격화하기 위해 임무 중심의 융합조직 활성화를 검토할 필요가 있다. 분석과 활동 부서는 기본적으로 과학기술 부서의 지원을 받지만, 아무래도 업무 단위가 다르면 칸막이 문화가 작용할 수밖에 없다. 분석 조직과 공작 조직에 기술 요원을 직접 결합시키거나 아예 하나의 임무 단위에 분석(analysis), 공작(operation), 기술(technology) 요원을 같이 배치하면 업무 효율도 증대될 뿐만 아니라 상호 간의 교육훈련 효과도 기대할 수 있다.

셋째, AI 시대에 정보기관의 효율적 정보활동과 투명성을 동시에 보장하고 법적으로 보호하기 위한 법제도 정비가 절실히 요구된다. 폭증하는 정보통신 데이터에 대한 접근과 국내외에서 코버트 액션의 필요성에도 불구하고, 우리 정보 요원들은 법적 권한 부여나 면책 등 법적인 보호를 거의 받지 못하고 있는 탓에 공격적 정보활동을 주저할 수밖에 없으며,

애국심에만 호소해야 하는 상황이다. 관련 법령의 제·개정을 통해 법적인 근거와 절차 마련이 시급하다. 권한 오남용에 대한 우려는 대통령의 승인 및 국회 정보위원회 사전 통보 절차 등을 통해 충분히 해소가 가능할 것이다.

//끝//