IDAP INSTITUTE OF DEFENSE ACQUISITION PROGRAM

JAMS JOURNAL OF ADVANCES IN MILITARY STUDIES

2022, Vol. 5, No. 3, 23-42.

https://doi.org/10.37944/jams.v5i3.177

Necessity of establishing an open source military R&D platform to promote AI development in defense

Lee, Sanggeun* · Jang, Sangguk**

ABSTRACT

Nations with advanced military capabilities are now focusing on developing AI algorithms for weapon system intellectualization development to retain their dominance. However, such endeavors are expensive in terms of time, effort, and resources, so it is necessary to develop it using open source to expand sharing and cooperation with industry-academic-government research and development collaboration. This study is aimed at elaborating the need for adoption of it and suggesting future implementation and improvement of open source SW in military despite the negative impact of security vulnerabilities when applied to the military weapon system. For this, the present study was design to investigate the benefit (intercommunity and cooperation) and harm (military sovereignty and technology vulnerability) of this open source platform through analysis of domestic and international case with defense area. The results of the study indicate that establishing an appropriate platform can help secure military sovereignty and prevent technology subordination, increase the efficiency of AI R&D, ensure collaboration and connectivity between weapons systems, and strengthen software security.

Keywords : military application of artificial intelligence, military sovereignty, security and technology dependency, open source platform, intercommunity and cooperation

* (First Author) Chosun University, Department of Military Science, Ph.D. Candidate and Army Education Command, Chief of AI Concept Development, rbfl5547@naver.com, https://orcid.org/000-0003-0866-0727.

** (Corresponding Author) Chosun University, Department of Military Science, Professor, skjang1@chosun.ac.kr, https://orcid.org/0000-0001-5258-8107.

Ⅰ. 서론

AI는 경제・안보적 활용가치가 높아 국가 간 기술패권 경쟁의 승패를 좌우할 기술로 판단되고 있으며(Horowitz, Allen, Kania, & Scharre, 2018), 자국 중심 AI 생태계를 강화하여 기술 지배력을 높이기 위한 AI 국가주의가 확산되고 있다.[1] 이러한 선도국에 의한 기술독점 과정에서 우리 군이 AI 경쟁력을 확보하지 못한다면 안보 전반에 위협이 될 것[2]으로 예상된다. 일반적으로 AI 개발은 목적에 맞는 알고리즘(Algorithm) 개념을 구상하고, 해당 개념을 SW로 구현할 수 있도록 프로그래밍 언어로 작성해야 하지만, 목적에 맞는 개발은 시간과 노력, 비용이 소요된다(Cho, J. K, 2021). 그래서 민간 영역에서는 개발 시간과 노력을 단축하기 위해 기개발되어 공개된 소스 코드(Source Code)를 활용하거나, Tensorflow, Pytorch 등과 같은 프로그래밍 인터페이스를 제공하는 Open Source 툴을 사용하기도 한다(Choi, Lee, & Han, 2020). 그런데도 Source Code 개발은 상당한 시간, 노력, 비용이 소요되므로[3] 산・학・연은 Open Source Platform(이하 OSP)을 구축하여 운용하고 있으며, 외국 선진국도 AI 개념연구와 플랫폼 운용을 추진하고 있다.[4]

전장 환경의 변화로 무기체계에서 소프트웨어 비중은 지속적으로 증가하고 있으며, 개발비용도 비례하여 상승하고 있다.[5] 이를 극복하기 위해서 기개발된 군사용 AI Source Code를 특정 보안 공간에 저장하고, 군 개발자 간에 자유롭게 공유하면서 협업할 수 있는 플랫폼 조성이 선행될 필요가 있다.[6] 그러나 군사용 AI는 무기체계에 탑재하여 운용되는 특수성으로 외부 기술에 종속되지 않은 핵심기술 확보가 중요하다. 그리고 민간 Open Source SW(이하 OSS)를 사용할 때 발생할 수 있는 보안 위험을 예방하기 위해 소스 코드를 직접 개발할 필요가 있다. 하지만, 軍 내부적으로 다양한 형태의 디지털 플랫폼 구축이 논의되고 있으나[7] 지금까지 군의 플랫폼 분야 연구는 무기체계 HW 분야에 집중되고 있어 군사용 AI Algorithm 연구개발의 OSP 구축에 대한 선행연구가 거의 없는 실정이다.

---

1) 국무조정실(2021.12.22.). 기술패권 경쟁에 대응한 국가 필수전략기술 선정 및 육성보호 전략. 제 20회 과학기술관계장관 회의.

2) NEWS1(2021.08.17.). [미래읽기] 인공지능은 '기술'이 아닙니다…국제질서 좌우할 AI. https://www.news1.kr/articles/?4404898 (검색일: 2022. 12. 21)

3) AppMaster(2021.12.21.). API 개발 비용은 얼마입니까?. https://appmaster.io/ko/blog/api-gaebal-biyongeun-eolmaibnigga (검색일: 2022. 12. 21).

4) 정승욱 편역, 미 NSCAI「백악관 AI 리포트(*The White House AI Report*)」(서울:쇼팽의 서재, 2021), pp.12-13.

5) 진현욱, 권경용, 손동환, 이창석(2017). 무기체계 소프트웨어 현황조사. 정보과학회지, 35(특집호), 23-27. https://scienceon.kisti.re.kr/commons/util/originalView.do?cn=JAKO201711553400197&oCn=JAKO201711553400197&dbt=JAKO&journal=NJOU00290837

6) 머니투데이(2018.03.12.). "세계는 지금 AI 대전… '협업 플랫폼'으로 승부". https://news.mt.co.kr/mtview.php?no=2018030908385991765 (검색일: 2022. 12. 21)

7) 국방부(2022). 국방 인공지능 추진전략 2.0,「내부문서」. p.11. 국방 지능형 플랫폼 구현 계획.

이에 본 연구의 목적은 국방 OSP가 왜 필요한지, 어떻게 구축하고 활용해야 하는지 밝히는 데 있다. 먼저 Open Source와 OSP에 대한 개념을 정의하고, OSP가 태동하게 된 배경을 “공유와 협업” 관점에서 살펴보았다. 또한, 해외 및 국내에 구축된 OSP를 대상으로 OSP 활용 역할 및 운용방법을 사례 중심의 현상분석을 토대로 軍에 OSP가 왜 필요하고, 어떻게 구축하고, 운용되어야 하는지에 관한 활용 방안을 제언한다.

Ⅱ. 이론적 논의

2.1 Open Source

Open Source는 프로그램 개발 과정에서 필요한 Source Code나 설계도에 누구나 접근해서 열람하고 사용 및 수정, 재배포할 수 있는 SW이다.[8] 보통 Source Code가 공개된 SW는 OSS로 SW 이외에도 개발과정이나 설계도가 공개되는 HW까지도 포함하는 개념이다. 오픈 소스의 운용이념은 Richard Stallman이 1985년 Free Software 재단을 설립하면서 제시한 SW 4대 자유[9]에 기반을 두고 있다. Free Software는 사용자의 자유를 절대적으로 강조하고 있으나 ‘Free’라는 단어가 지니는 또 다른 이념적, 사회운동적 성격으로 비즈니스 채택에 부정적 영향을 미쳤다. 또한, 공개 배포해야 할 대상인 Source Code를 누락하고 있어 전체적인 의미전달에 부족한 점이 있었다. 이후 1998년 Eric Raymond가 주축이 되어 OSI(Open Source Initiative)를 설립하면서 Free Software와 다른 개념으로 Open Source라는 용어가 사용되었다.[10] 그래서 Free Software는 SW 라이선스를 작성하나 OSI는 자체적으로 라이선스를 작성하지 않고, 이미 시장에서 사용되는 라이선스가 일정 요건을 충족할 경우에 Open Source 라이선스로 인정하는 정책을 취하였다. 최근 2010년부터 2021년까지 구글-오라클의 Java API[11] 라이선스 소송은 OSS 지식재산권 침해 관련 대표적인 사례로 구글이 최종 승소하였다.[12] 이에 따라 SW 개발자는 필요한 만큼의 OSS를 활용함으로써 노력의 낭비를 최소화하고, 새로운 영역에 집중할 수 있게 되었고, 회사의 규모와 상관없이 공정한 사용을 보장받을 수 있게 되었다.

---

8) 이진희(2019). 오픈소스 중요성과 시사점. 정보통신산업진흥원. https://www.nipa.kr/main/downloadBbsFile.do?key=116&bbsNo=11&atchmnflNo=8793

9) FREESOFTWARE. https://www.fsf.org/(검색일:2022. 5. 2), 4대 자유 : 실행의 자유, 연구와 수정의 자유, 재배포의 자유, 수정프로그램 배포의 자유

10) Eric Raymond 홈페이지(www.catb.org/~esr/)(검색일 : 2022. 6. 9)

11) API(Application Programing Interface): OS나 시스템, 애플리케이션, 라이브러리 등을 활용하여 응용 프로그램을 작성할 수 있게 하는 인터페이스

12) Google LLC v.Oracle America, Onc, Supreme Court of the United States(2021.4.5.) p.18.

국내의 경우, 2021년 Open Source 활용실태 조사결과에 따르면, 국내기업의 61.5%가 OSS를 활용하고 있으며, 활용율은 2020년 58.8% 대비 4.6%가 증가하였다(Open Source 시장가치는 7조원 규모).[13] 한국전자통신연구원(ETRI)에서 내부 직원 대상의 조사에 따르면, Open Source 중요성을 인식하고 있으며(93%), 과제 해결 시 OSS를 활용한다(68%)고 응답하였다.[14] 최근 연구보고서에 따르면,[15] Open Source 활용은 많은 개발자가 다양한 시각에서 OSS를 보고 분석하므로 성능개선이나 Source Code가 지닌 문제를 손쉽게 해결할 수 있는 장점으로 인해 집단지성이 요구되는 소요를 충족할 수 있다. 보안취약점 예방 측면에서 Source Code를 숨기는 것이 보안에 유리하다고 판단할 수 있으나 공개를 통해 보안 취약점을 신속하게 발견할 수 있어 오히려 보안이 강화되는 장점이 있다.[16] 또한, 비즈니스 측면에서 OSS 활용은 기개발된 SW를 이용하여 개발자가 버전업하기 때문에 SW 개발에 드는 비용과 시간을 절감할 수 있다(Linh, Hung, Diep, & Tung, 2019). Open Source를 많이 공개하는 회사의 인지도가 좋아지는 간접효과로 외부 우수인재 영입이 보다 용이할 수 있다.[17]

2.2 Open Source Platform(OSP)

플랫폼은 초기 HW를 지칭하는 개념에서 점차 범용화되면서 SW 플랫폼으로 이동하고, 응용 SW 플랫폼이 확장되고 있는 추세이다.[18] 최근에는 '서비스의 핵심기반'이란 광의의 관점에서 다양한 의미로 혼용되어 사용되고 있어 산업 및 비즈니스 측면에서 다수의 생산자와 소비자가 연결되어 상호작용하며, 가치를 창출하는 산업 생태계 기반의 場을 의미한다. OSP는 아직 국제적으로 합의된 정의가 없어[19] 플랫폼이 수행하는 주된 역할에 대한 일반적인 공감대에 기초하여 개념을 정리하였다. OSP는 디지털 플랫폼의 한 종류로 Open Source를 개발자(공급자)가 플랫폼에 탑재하면 사용자가 자유롭게 사용하면서 오류수정과 추가 개발을 할 수 있는 플랫폼이라 볼 수 있다(Baek, Ha, & Cho, 2016). 단, 기존 플랫폼과 유사하게 Open Source Platform도 사용자를 종속하는 특성이 있다.

---

13) 정보통신산업진흥원(NIPA). 2021 오픈소스SW(OSS) 실태조사 보고서. https://www.nipa.kr/main/selectBbsNttView.do?key=113&bbsNo=9&nttNo=8859&bbsTy=&searchCtgry=&searchCnd=all&searchKrwd=&pageIndex=1

14) 한국전자통신연구원(2022). R&D Innovation with Open Source. ETRI Open Source Annual Report. p.21.

15) 이한영, 권병규, 차성민(2021). 디지털 플랫폼에 관한 최근 EU의 규제개편 및 우리나라의 통상친화적 제도 개선 방향. 대외경제정책연구원. p.15.

16) 정보통신기획평가원(2019). 미 국방 SW 개발의 개방형 기술개발(OTD) 동향. https://dataonair.or.kr/upload/24/20190411155494941110910.pdf

17) http://m.boannews.com/html, 'Open Source 운동 20주년'(2018.11.23)(검색일: 2022. 6. 9)

18) 최병삼, 김창욱, 조원영(2014). 플랫폼, 경영을 바꾸다. 서울: 삼성경제연구소, pp.20-22.

19) 이한영, 권병규, 차성민(2021). 디지털 플랫폼에 관한 최근 EU의 규제개편 및 우리나라의 통상친화적 제도 개선 방향. 대외경제정책연구원. p.23.

예를 들어, Android는 OS, 미들웨어, Java API를 포괄하는 Open SW로 대부분의 코드가 공개되어 있어 개발자가 자유롭게 Android OSS Code를 활용하여 Android OS 기반의 모바일 기기를 만드는 생태계가 조성되었다.[20] 또한 구글, 네이버 기업 등은 검색엔진 및 포털사이트의 인터넷 사용 환경을 제공하고 있다. 이런 Digital Platform도 참여자의 상호작용을 통해 새로운 가치와 혜택을 만들어 가는 생태계라고 볼 수 있다. 즉, 이용자는 제공된 플랫폼에서 정해진 규칙을 위반하지 않은 범위 내에서 자유롭게 참여하고, 기업과 이용자 또는 이용자 간에 서로 가치를 공유하면서 생태계가 구축될 수 있었다.

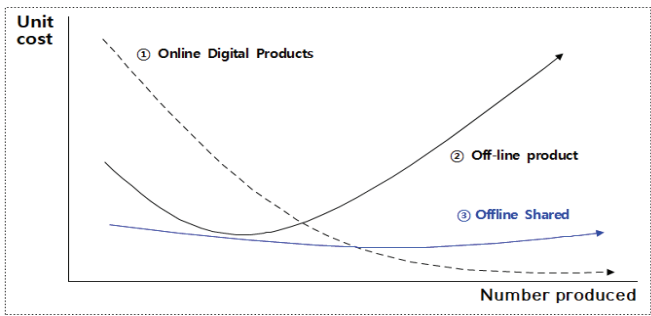
다만 OSS는 4대 자유 원칙에 따라 자유로운 사용을 허용하지만, 라이선스에 의해 사용 범위를 부여하고 있다. Open Source 라이선스는 Source Code의 사용, 생산 및 수정, 배포 등을 규정한 것으로 Source Code 공개 강제보다 Source Code의 사유화 방지에 목적이 있다.[21] 그래서 SW개발에 필요한 Source Code는 사용자 요구를 만족하는 라이선스 특징 검토와 옵션 선택이 가능한 제품 선택이 필요하다(Park & Yang, 2012). OSS 라이선스 준수사항 위반 시에 이용 권리가 박탈되거나 제품화 이후에 판매 불가능 등의 분쟁 발생 위험이 높아질 수 있다(Chun, Yoon, & Jeong, 2020).

2.3 공유와 협업

한계비용 제로 사회[22]는 공유 자원을 네트워크로 연계하여 서비스를 제공하는 모델이다(Figure 1). 초기 생산에 필요한 인력이나 설비에 드는 비용은 고정비용으로 새로운 단위 생산 증가를 위한 비용의 증가분이 한계비용이며, 추가 생산비용이 발생하지 않는 상태를 한계비용 제로 상태라 한다. ①은 온라인 디지털 상품에서 주로 발생하며, 특정 디지털 콘텐츠나 SW 개발 초기에는 많은 시간과 비용이 소요되지만 한번 생산 후에 추가 생산하는 비용이 거의 발생하지 않는다. 그러나 ②와 같은 오프라인 상품은 상품 수가 증가함에 따라 초기 생산비용이 감소하지만, 일정 시점부터 상품 수 증가에 따라 비례하여 생산비용이 증가하게 된다. 반면 ③은 오프라인 상품도 공유 방법을 선택했을 때, ① 온라인 디지털 상품과 같은 비용 감소 효과가 발생한다.

이런 '한계비용 제로' 경제구조를 활용하는 것이 공유경제이다(Cho, 2021). 공유경제는 유휴자원을 '공유'라는 매개체를 통해 경제적 가치로 전환하여 서비스 개발과 플랫폼 확보에서 발생하는 초기비용 발생 이후에 네트워크를 활용하므로 한계비용이 거의 수렴하는 특징이 나타난다. 특히, 이런 공유경제는 참여자들이 경제적 가치가 있는 상품이나 서비스를 만들고 서로 교환, 재사용 및 느슨한 조정 등을 통해 의존하는 혁신・생산 시스템이므로 개방형 협업체계 구축이 중요하다. 해당 협업체계는 생산물의 구조를 직접 볼 수 있어 타인의 작업에 추가하여 직접 누적할 수 있는 이점이

20) 박정숙, 엄승광, 이승윤(2021.12). Open Source의 지식재산권 분쟁 대응 방안. 정보통신기획평가원 주간기술동향. p.21.
21) 이진휘(2019). 오픈소스 중요성과 시사점. 정보통신산업진흥원, 2019-20호, 2-15.
22) Jeremy Rifkin(2014). *The Zero Marginal Cost Society*. 서울: 민음사. pp. 8-10.



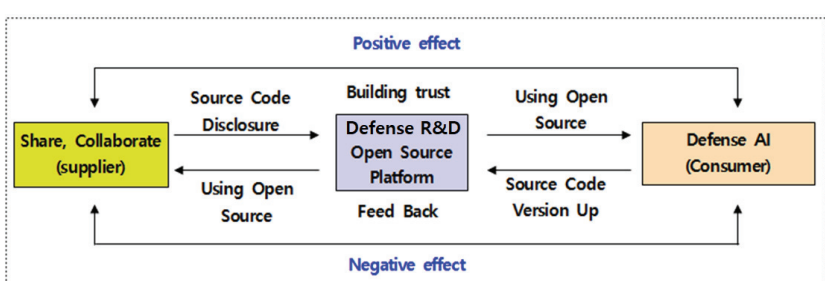
<Figure 1> Offline Zero Marginal Model

있으며, 원천 Source Code를 재사용할 수 있어 기술・시간・비용 절약과 지속적인 Version Up이 가능하다(Levine & Prietula, 2014).

상기한 협업과 공유는 특정 플랫폼이라는 공간을 중심으로 이루어지는 특징이 있다. 이런 공간에서 유사한 문제에 대한 사용자의 참여가 문제해결로 이어지고, 참여자가 문제의 솔루션을 공유하면 기타 참여자는 유사한 노력의 중복을 피할 수 있게 되는 이점이 발생하게 된다.

2.4 분석방법

본 연구는 국방 AI 개발 측면에서 국방 Open Source Platform(OSP) 운영의 필요성과 발전적 운용 방안을 제시하기 위해 Source code 공급자와 국방 AI 수요자 관계에서 OSP 역할의 영향을 국내・외 및 민간・국방 분야 OSP 운용 사례를 중심으로 파악한다. 이를 위해 본 연구는 공급자의 공유・협업 활동이 군사용 R&D OSP에 미치는 직접적 영향관계를 제시하고, 이런 영향관계가 국방 AI 개발을 증대시키고 개발 효율성을 높이는 긍정적 효과뿐만 아니라 부정적 효과를 밝히는 분석틀을 설정한다(Figure 2). 그리고 국방 AI 개발 수준을 높이기 위한 공급자의 공유・협업 간의 관계에서 군사용 OSP 운영에 대한 상호 신뢰 구축과 피드백 제공의 선순환 구조를 제시하고자 한다. 즉, 신뢰구축과 피드백이 형성되어야 AI Algorithm 원천 Source Code가 공개되고, Version Up이 이루어져 활용도가 높아지면서 새로운 군사용 AI Algorithm 개발이 가속화되는 구조를 가질 수 있다.



<Figure 2> Analytical framework

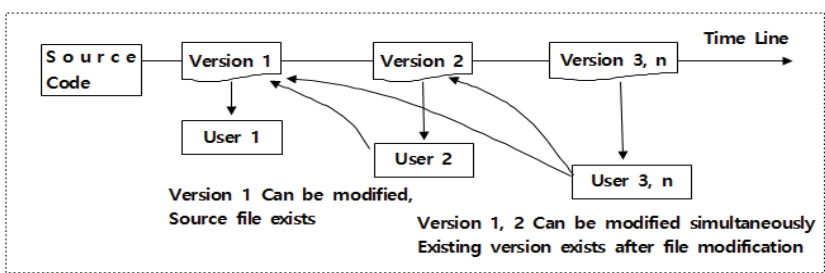
Ⅲ. 사례 분석: Open Source Platform 운용

3.1 긍정적 효과: 개방형 공유와 협업

3.1.1 국외 민간 Open Source Platform (OSP)

대표적인 민간 OSP인 Git은 2005년 Linus Torvalds에 의해 개발되었다. Git은 대부분의 서버-클라이언트 시스템과 달리 기록과 버전 추적기능을 갖춘 저장소로 소스 코드 파일의 수정사항을 추적하고, 다수 이용자 간에 저장된 소스 코드를 공유하여 협업하기 위한 분산 버전관리 시스템이다(Lee & Rim, 2016).[23] 이런 Git 시스템을 도식화하면 다음과 같다(Figure 3). Version 1을 사용자 1, 2, 3이 동시에 수정할 수 있고, 사용자 3은 Version 1과 Version 2도 동시 수정이 가능하다. 이렇게 수정한 내용을 다수의 제3자와 공유하면서 계속해서 보완할 수 있는 체계이다. 즉, 원천 소스 코드를 계속하여 새로운 사용자가 버전 업을 진행할 수 있으며, 파일 수정 이후에도 원작자가 개발한 파일이 삭제되지 않고 보존되어 변경된 기록사항을 추적관리할 수 있다.

이런 Git는 가장 널리 쓰이는 Source Code 관리도구(Weber & Luo, 2014)로 전문 SW 개발자의 사용 비율이 2012년 32%에서 2014년 42.9%, 2022년 93.9%까지 비약적으로 증가하고 있다.[24] 특히, 사용자 공유·협업 편의성을 높이기 위해 웹 방식의 GitHub와 GitLab 서비스를 제공하고 있다. GitHub는 Git의 분산 버전관리와 프로젝트에 대한 접근관리, 버그 추적, 개발자 간 협업, 통합 등의 기능을 제공한다. GitLab은 일부 유료로 사용하는 비공개 GitHub와 달리 개인 프로젝트에도 사용자 코드에 대한 비용 지불없이 비공개 유지가 가능하다는 특징이 있다.



<Figure 3> Git version control system

Note. This figure was created by authors.

3.1.2 국내 민간 OSP

ETRI OSP는 2019년 정부출연 연구원 중에서 최초로 구축된 개방형 플랫폼이다. 이런 개방형 협

23) https://cgit-scm.com/(검색일: 2022. 6. 15)

24) https://www.eclipse.org/foundation/report/annual_report.php(검색일: 2022. 8. 30.)

력 구조로 조직 내부와 외부 협력을 통한 연구개발을 추진할 수 있다.[25] 특히, OSS 위험을 최소화하면서 개발과정에서 검증 기능을 강화하고, 효율성을 극대화하는 방향으로 추진하고 있다. 그래서 단계별(SW 개발, 완료, 배포) 대응체계를 구축하여 개발부터 OSS 라이선스 검증절차를 운영하며 의무사항 준수, 특허 보복, 보안 취약점 등을 식별하고 대응하는 체계를 갖추고 있다. 공개 시에는 공개 라이선스, 범위, 공개 저장소를 검토하고, Source Code 기술이전 때는 OSS 사용, 라이선스 의무사항 준수, 특허 라이선스 허용 여부 등을 검토하고 있다. 특히, 배포 시 Open Source 심의위원회에서 라이선스 사본 첨부, 수정내용 고지 등에 대한 준수 여부를 심의하여 배포하고 있다.[26] 개발된 SW는 개발방법에 따라 Permissive, Weak Copyleft, Strong Copyleft로 분류하여 관리하고 있다. 또한, 서버 운용은 개방형 R&D 플랫폼으로 중앙서버와 클라우드 서버 모두에 저장하는 분산형 방식을 채택하고 있으며, GitHub와 GitLab을 병행 사용하여 Open 프로젝트 및 개인 프로젝트를 모두 지원한다.

민간 기업의 OSP 운용은 Samsung Open Source, SK C&C Tech, 카카오의 Olive 플랫폼 등이 대표적인 사례이다. 지금까지 국내 기업은 사업상 보안 이유로 기업별 독점 SW 개발방법을 고수하였으나 OSS 개발환경으로 변화하고 있다(Ahn, 2005). 다수의 기업은 총 개발 비용 절감, 최신 기술 확보, 내부 기술 역량 강화, 기술 경쟁력 강화, 시장의 확대, 우수인재 확보 등의 이유로 Open Source를 사용하고 있다(Kang, Shim, & Pack, 2015).[27]

국방 분야의 경우도 다수의 전투체계가 동시적으로 정보를 공유하는 네트워크 전에 대비하여 OSS 도입과 활용에 필요한 정책수립이 추진되고 있다(Jang & Kim, 2017). 국방기술 연구기관인 국방진흥연구소는 군사용 AI 개발・운영에 필요한 SW, 필수 Algorithm과 데이터, 컴퓨팅 자원 등으로 구성된 '국방 AI 플랫폼 개발계획'을 발표하였다.[28] 해당 정책은 국방에 특화된 Algorithm 및 데이터 지원, 기개발된 Algorithm과 Source Code, 확보한 데이터를 AI 플랫폼에 지속적으로 축적하고 고도화하는 기본적인 운용계획을 포함하고 있다. 다만, 성공적인 OSP 활동은 내・외부 참여자의 자유로운 공유・협력 활동이 보장되는 체계 구축이 선행되어야 하므로(Jung, D. S., 2021) 개방형 Open Source 커뮤니티 운영과 생태계를 조성하고, 관련 규정 및 활동 지침 등을 마련하는 정책실행이 요구된다.

상기한 바처럼 산・학・연의 AI Algorithm 개발 방향은 경쟁에서 협업, 수직에서 수평, 폐쇄에서 개방, 소유에서 공유로 변화하고 있으며, 개방형 협력과 기반 플랫폼의 구축의 중요성이 강조되고 있다. 이런 의미에서 우리 군도 국방 AI개발 소요비용과 시간의 절감 측면에서 핵심기술의 확보를 위해 군사용 OSP 구축을 검토할 필요가 있다.

---

25) ETRI(2022.4). Open Source 연례보고서 2021. p.17.

26) ETRI(2022). 2022 오픈소스 R&D 활동지원. 내부보고문서. p.15.

27) https://tech.kakao.com/opensource(검색일: 2022. 7. 14).

28) 조준호(2022). 인공지능 적용 국방핵심기술 현황 및 국방 인공지능 발전방향. 22-2차 교육사령부 인공지능 전투발전 세미나. pp.21~23.

3.1.3 미국 군 사례

미 국방성(DoD)은 '08년부터 Forge.mil이라는 플랫폼을 통해 OSS를 활용하고 있으며, '17년부터 핵심기술을 제외한 'Code.mil'이라는 OSP를 통해 제공하고 있다. OSP을 운영하는 이유는 다음과 같다. 첫째, 개별 개발자의 창의적인 활동과 노력이 국방성 내에서 활용되지 않고 사장되어 개발된 Source Code를 타 개발자와 공유하고자 한다.[29] 둘째, 미 연방정부의 정책과 관련하여 연방 소스코드 정책(M-16-21)은 각 정부기관에서 새로운 SW 개발 시 최소 20%를 OSS로 배포하도록 통제를 하고 있다.[30] 2018회계연도 국방수권법에는 "국방부 장관은 M-16-21에서 수립한 OSS 프로그램을 시작해야한다."고 명시하고 있다.[31] 그래서 국방성 개발자는 GitHub와 협력하여 국방성에서 구축된 OSS 프로젝트를 민간 SW 개발자와 다양한 분야에서 협업하고 있다. 미군의 경우도 Open Source 프로젝트를 활용하여 개발자 및 커뮤니티와 공개 협업을 통한 개발을 목표로 추진하고 있다. 미 육군은 군 주도로 미래사령부에 Army SW Factory를 2021년 1월에 창설하여 군사용 SW를 개발하고 있다.[32]

이처럼 미국의 경우는 국방성의 Code.mil의 군사용 OSP 활용[33]과 미군의 Army SW Factory 조직 구성 등을 통해 AI Algorithm 개발을 활성화하고 있다. 반면, 우리 군의 경우는 아직 관련 개념 정립이나 전문 인력이 부족한 실정이며, 민간 부문과 협력에서도 군의 작전개념 이해 부족으로 군사용 AI 개발이 늦어지고 있다(Lee. S. G, 2022).

3.1.4 국내 정부 정책

우리 정부도 SW 산업 패러다임 변화를 인식하고 2020년 12월에 공개 SW 방식의 연구 및 기술개발 촉진 등을 포함한 'SW진흥법'을 개정하였다. SW 및 관련 산업을 보호하고 육성하기 위하여 SW 지식재산권 보호를 강조하면서 동시에 연구개발(R&D)과 기술경쟁력을 강화하기 위하여 연구개발한 SW의 Source Code를 공개하도록 하고 있다.[34] 이는 SW의 개발·유지 및 관리 과정에 해당 SW 개발자 외의 다수 인원이 참여할 수 있도록 개발 방식의 활용과 국가연구개발사업의 결과물에 대해 저작권자가 Source Code를 공개하여 활용·복제·수정 및 재배포가 자유롭게 법제화한 것이다. 이에 과학기술정보통신부는 2021년 6월 '고부가가치 SW중심의 SW생태계 혁신전략' 을 수립하여 공개 SW를 활용한 국내 SW 산업 생태계를 혁신하겠다는 계획을 발표하였다.[35]

---

29) https://code.mil/(검색일: 2022.8. 29). "The goal is to foster open collaboration with the developer community 중략~on DoD open source projects."

30) https://code.mil/=201810315.(검색일: 2022. 6. 15) "Amid congressional mandate to open source DoD's SW code."

31) https://code.mil/=201810315(검색일: 2022. 6. 15)

32) https://armyfuturescommand.com/software-factory(검색일: 2022. 7.20)

33) Open Source Software Support Center (2017.02.28.). [해외소식] 미 국방부의 오픈소스 이니셔티브 'Code.mil'. https://www.oss.kr/news/show/8a81e264-8179-4e01-8c04-335f09679c6f?page=398

34) 법률 제17799호, 'SW 진흥법'(2020).제 17조, 25조

상기 사례에서 살펴본 것처럼 정부는 공개 SW 방식의 연구개발과 Source Code 공개를 원칙으로 SW 생태계를 구축하여 SW 산업발전과 국가 경쟁력 강화 관련 정책을 추진하고 있다. 이런 정부정책 방향과 연계하여 우리 군도 국방 AI 개발 시 외부 Source Code 활용, 재배포 등에 관한 정책 방향 검토 및 수립이 필요하다.

3.2 부정적 효과: 기술 종속화와 보안 취약점 노출

3.2.1 민간 Open Source Platform 운용 사례

OSP 운용을 통한 Source Code 재활용 및 버전관리는 비용절감, 시간・노력 소요의 최소화, 개발과정에서 발생하는 오류 최소화 등의 긍정적 효과가 있으나 여전히 도입・활용 측면에서 취약점이 존재하여 다음과 같은 부정적 효과를 제시한다.

첫째, 디지털 플랫폼이 지닌 “종속화”문제로 글로벌 기업이 많은 투자를 통해 개발한 SW를 공개함으로써 자사 주도의 생태계가 조성되고, 기술 종속화가 공고화되는 현상이 발생하고 있다.[36] 대표적으로 구글의 Android 운영체제는 OSS에 기반을 둔 모바일 운영체제로 Android를 구동하는 스마트폰과 태블릿에 탑재되어 전세계적으로 활용되고 있다.[37] 결국 구글의 플랫폼 활용으로 해당 기업의 생태계에 종속될 수밖에 없게 되는 부정적 효과가 나타났다.

둘째, OSS는 상용 SW와 달리 Source Code가 공개되기 때문에 외부 노출 가능성이라는 취약점이 있다. 이런 OSS 보안 취약점은 꾸준하게 증가하고 있으며, 보안 취약점을 악용하는 경우까지 발생하고 있다(Ryoo, Jo, & Lee, 2021).[38] 게다가 OSS 특성상 문제 발생시 다수 참여자가 수정 및 보완 작업을 진행하므로 특정인을 대상으로 책임소재를 파악하거나 명시하기 힘든 구조이고, 특정 참여자 본인이 직접 개발하지 않은 프로그램에 대한 책임감도 높지 않아 보안 문제에 대처하기 어려운 점이 있다. 그래서 이에 대한 대응으로 한국인터넷진흥원(KISA)는 GitHub를 비롯한 온라인 저장소에 프로젝트 정보 노출, 해킹, 금전적 갈취 시도 등의 사고가 발생에 관한 보안 권고문을 발표하기도 했다.[39]

3.2.2 국방부 정책

민간 OSP를 군에 적용하는 접근은 보안문제로 인한 불안전한 요소가 있어(Lee, Seo, & Chae, 2020) 軍 차원의 독자적인 OSP 운용 방안을 검토할 필요가 있다. 국방부 지침은 정부의 Open Source 정책과 차이점이 있으며, 다음과 같은 이유로 OSS 사용을 금지하고 있다.

---

35) 과기부(2021). SW 생태계 혁신전략. p.4.

36) 이진휘(2019). 오픈소스 중요성과 시사점. 정보통신산업진흥원, 2019-20호.

37) https://www.android.com/intl/lo_kr/(검색일:2022.8.30.)

38) 기태현(2021). 오픈소스 보안관리의 중요성. 공개SW가이드/보고서. p.8.

39) https://zdnet.co.kr/viewno=20210528171253(검색일: 2022. 9. 2)

첫째, 보안 취약성 문제로 민간 기업은 OSS 보안 전담팀이나 보안 전문가를 운용하지 않고 있어 보안 경고나 알람체계, 보안 패치 등의 버전관리가 부족하다고 볼 수 있다.[40] 이러한 OSS는 적이 Back Door를 악의적으로 탑재하여 언제든지 설치된 프로그램 체계에 접속하여 내부를 보거나 원격 조종할 수 있는 위험성이 있다.[41] 그래서 OSS를 사용한 Algorithm 개발 시 Back Door가 설치되어 있다면, 프로그램 설계와 운용개념 및 무기체계나 시스템 특성까지 노출될 수 있어 군 전력화 관련 기밀이 탈취될 수 있는 심각한 보안상의 문제가 발생할 수 있다(i. e., Son, Lee, & Heo, 2022).

둘째, 공개된 OSS를 사용하는 사람은 Algorithm 패턴과 적용된 함수를 알 수 있어 해당 Source Code를 군사용으로 사용할 경우에 특정 무기체계에 적용된 Algorithm의 패턴을 적군(敵軍)이 예측할 수 있다. 그래서 적이 아군의 군사작전을 쉽게 예측하고, 역대응하는데 활용할 수 있다.

이런 군 보안상의 취약점을 사전에 예방하고 대응하고자 방위사업청은 SW 개발단계에서 SW(공개 SW 포함)가 지식재산권 및 라이선스에 저촉되지 않도록 관리하고 있으며, 연구개발 주관기관에게 연구개발 수행 시 공개 의무가 있는 공개 SW(OSS) 사용을 금하고 있다.[42] 또한, 연구개발 주관기관이 SW 지식재산권 및 라이선스 저촉 여부를 검토하여 SW 통합시험결과서에 포함하도록 명시하여 외부 OSS를 군사용으로 사용하지 못하도록 통제하고 있다.

Ⅳ. 군사용 AI R&D OSP 필요성과 구축 방향

Open Source 사용으로 발생할 수 있는 보안상 우려에도 불구하고 군사용 OSP 구축의 필요성과 효과는 다음과 같다.

우리 군의 독자 전력화를 위해서 군 자체적인 AI R&D OSP 구축이 필요하다. 군사 강국은 미래 전장 환경이 인공지능을 탑재한 지능형 로봇 등에 의해 전개될 것으로 전망하고 있어 무인 무기체계를 개발하기 위해 국방 인공지능 모델 개발과 운용 관리에 중점을 두고 있다(Jung, 2021). 이런 변화상황에 한국군이 신속하게 대처하기 위해서 AI 분야 핵심 기술의 독자개발에 필요한 AI R&D OSP 구축을 통해 선진국의 기술 종속화를 방지할 필요가 있다. 실제 기술 종속화의 대표적인 사례를 살펴보면, 반도체는 AI Algorithm의 성능을 결정하는 기본요소로 첨단 무기체계에 탑재되는 필수 부품이기 때문에 이미 특정 국가 중심의 생태계가 구축되고 있다.[43] 이런 점에서 특정 국가의 군사용 AI Algorithm이 군의 핵심 무기체계 플랫폼이 될 경우에는 향후 무기체계의 종속화와 군사

40) 정유진, 류원옥, 정해원, 소서영, 강신각(2019). 미 국방 SW 개발의 개방형 기술개발(OTD) 동향. 정보통신기획평가원. 1-23.

41) TechM(2022.08.10.). 기업 오픈소스 SW 사용 늘어나는데, 보안은 낙제점?…"전담조직 없어 개발자가 직접 대응". https://www.techm.kr/news/articleView.html?idxno=100351

42) 방위사업청(2020). 무기체계 SW 개발 및 관리 매뉴얼. p.102.

43) 정승욱 편역(2021). 미NSCAI. 백악관 AI 리포트(*The White House AI Report*). 서울:쇼팽의 서재, pp.90～93.

주권 침해 등이 발생할 수 있다(Layton, 2018).

군사용 AI 개발에서 OSS를 사용하여 소요 예산・시간・노력 투입의 효율성을 극대화할 필요가 있다. 일반적으로 무기체계 개발 시 중기로 전환되는 전력소요(F+7년)와 중기 대상기간(F+3～F+7년)에 신규로 반영하는데 물리적인 기간이 필요하다.[44] 그러나 4차 산업혁명 시대에 AI 관련 기술 변화가 급격하게 변화면서 발전하고 있어 기존의 무기체계 전력화 기간을 적용하게 되면 기술 진부화가 발생할 가능성이 높다(i. e., Cheon & Jeong, 2019). 따라서 국방 인공지능 능력의 조기 확보를 위해 군사용 OSP를 구축하여 한국군의 독자적인 군사용 AI Algorithm을 연구, 개발할 수 있는 생태계를 구축할 필요가 있다. 특히 이런 개발 생태계 조성을 위해 병과, 군종, 동맹국간 협업과 연결성 보장이 요구된다. 과거 무기체계는 타 무기체계와 연동이 거의 요구되지 않는 야포, 전차, 장갑차, 항공기 등 단일 플랫폼 체계였다. 그러나 현재 무기체계는 'AI 기반의 유・무인 복합전투체계'를 지향하고 있으며[45] 무기체계 간 네트워크 연결과 데이터 공유가 필수화되고 있다. 특히, 우리 군의 연합・합동・협동 작전 능력 극대화 차원에서 유기적인 작전 수행이 가능하도록 효율적인 지휘통제를 담당하는 네트워크 환경이 더욱 중요해지고 있다. 따라서 향후에는 무기 및 전력지원체계에 탑재할 Algorithm Source Code를 OSP에 공유하여 무기체계 간 협업과 연결성을 보장할 수 있어야 할 것이다.

끝으로 국방 AI 보안성 강화 및 취약점 개선 측면에서 군 내 OSP 운용 시, 군 자체 개발한 Algorithm Source Code뿐만 아니라 군에 납품한 SW를 군 내부 개발자에게 공개하여 취약점을 보다 신속하게 식별하고, 납품한 AI Algorithm의 정상 개발 여부를 검증할 수 있어[46] SW 완성도를 높일 수 있는 긍정적 효과를 얻을 수 있다.

4.1 군사용 AI R&D OSP의 역할

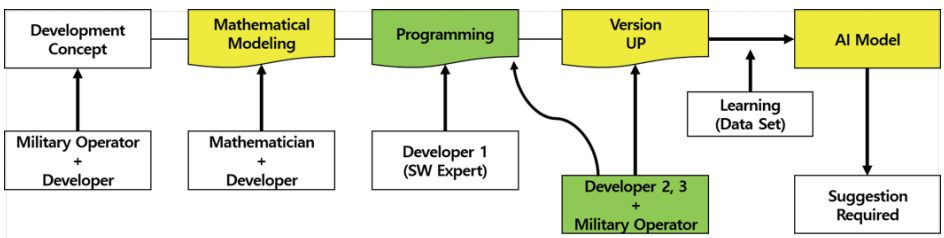
우리 군은 무기체계나 전력지원체계에 적용할 수 있는 AI의 기술적 가능성을 검증하고, 핵심기술과 독자적인 능력을 확보해야 한다. 이를 위해 군 내 AI 관련 전문인력과 과학기술병이 자유롭게 개발에 참여하고, 개발 결과를 공유할 수 있는 OSP 환경을 제공해야 한다. 또한, AI Algorithm의 높은 신뢰성을 보장할 수 있도록 개발단계부터 군 운용자와 수학자, 개발자 등이 협업할 수 있도록 개발하고자 하는 Algorithm 개념을 발전시키고, 수학적 모델링 과정을 거쳐 개발하는 접근이 필요하다. 이를 위해 개발과정에서 개발한 Source Code를 OSP에 공유하여 제2, 제3의 개발자에 의해 검증하고, Version Up하는 과정을 반복하면서 AI Algorithm의 신뢰성을 향상할 수 있을 것이다

44) 국방부(2022). 국방전력발전업무 훈령. p.20.

45) 제20대 대통령직인수위(2022.5). 110대 국정과제, 국방혁신 4.0 추진으로 AI 과학기술 강군 육성. p.175.

46) 교육사(2022). '23～'33 인공지능 종합발전계획. 「내부문서」. p.42. Algorithm 개발절차: 개념도 작성 ⇒ 수학적 모델링 ⇒ 프로그래밍 및 모델화

(Figure 4). 나아가 후속 AI Algorithm 개발의 Source Code로 활용할 때, OSP 활용으로 개발과정의 선순환 구조가 지속될 수 있다.



<Figure 4> Development of AI algorithm

반면, 현재 군은 군별 또는 부서별 주도로 군사용 AI를 개발하고 있으나 상호 간에 공유 없이 별도 개발진행으로 유사한 기능의 AI가 중복적으로 개발될 수 있다. 그렇기 때문에 모든 과제(개발완료, 개발 중, 계획수립) 내역을 OSP에 공유하게 되면, 중복개발 최소화 및 개발 기간 단축의 연구개발 효율성을 높일 수 있을 것이다. 그리고 군 AI 연구 간 OSS 사용으로 라이선스를 검증하여 특허가 있는 Source Code의 무단사용이나 배포를 미연에 방지할 수 있고, 군 납품 Algorithm Source Code를 군 OSP에 공유하여 개발절차 준수 및 민간 OSS 사용 여부, 버그 및 백도어 등을 확인하는 검증 과정을 진행할 수 있게 된다.

4.2 보안체계를 고려한 OSP 운용

군사용 OSP 구축 시 별도의 보안 통제대책 수립없이 인터넷 기반으로 구축된다면, 무기체계에 적용할 Algorithm이 적에게도 실시간 노출되어 군사 작전에 치명적인 문제를 야기할 수 있다. 따라서 군사용 OSP 구축은 보안통제 기술을 고려하여 단계화하여 추진할 필요가 있다.

먼저 군 내부망(Intranet)을 활용한 AI R&D OSP를 구축하여 외부와 물리적으로 차단된 네트워크에서 군 내부 개발자가 자유롭게 AI 모델을 개발할 수 있는 환경을 조성해야 한다. 이를 통해 군 내 인원은 AI Algorithm Source Code뿐만 아니라 Algorithm 개념도, 작업 설계도 등을 포함한 HW 요소까지 저장하고 공유할 수 있다. 그래서 개발자 간에 저장된 Source Code를 포함한 Data 정보를 공유하여 개발 간 협업, 문제점 개선, 추가 개발 등이 가능하게 된다. 반면에 국방 AI Algorithm 개발 시 민간에 개방된 외부 OSS 반입과 활용은 선별적으로 허용해야 한다. 군 무기체계에 적용하는 Algorithm의 논리구조와 Source Code는 절대 비밀 유지가 중요하므로 국방 선진국도 OSP를 운용하면서도 무기체계 AI Source Code는 외부 접속과 공개를 엄격하게 통제하고 있다.[47]

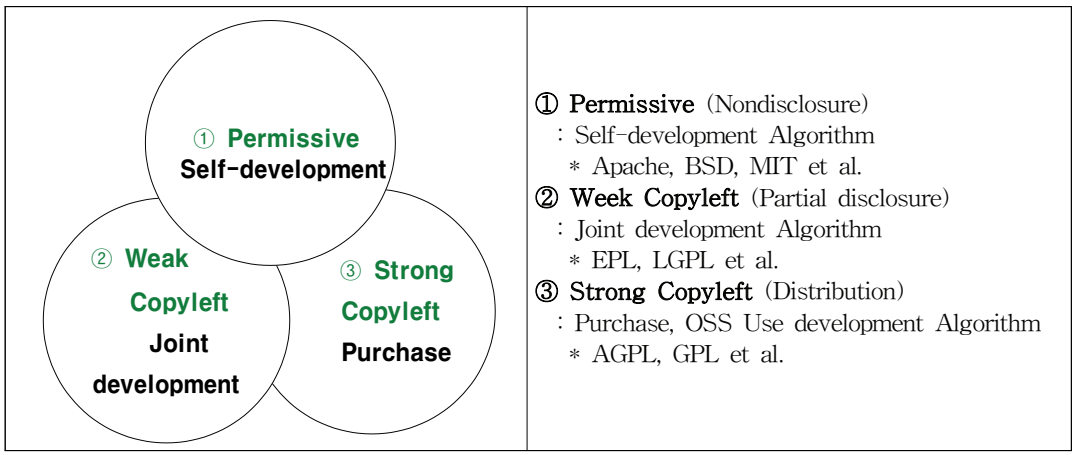
47) 정승욱 편역(2021). 미NSCAI. 백악관 AI 리포트(*The White House AI Report*). 서울:쇼팽의 서재, p.120.

저장방식은 중앙서버와 로컬 저장소를 모두 사용하여 서버와 로컬에 기록이 남는 분산형 방식을 택해야 한다. 단일 중앙서버만 운용하게 되면, 다수 인원 동시 접속의 서버 과부하, 서버 문제 발생 시 일정시간 사용 제한, 관리 부주의에 따른 Source Code의 삭제 등에 따른 다양한 문제가 발생할 수 있다. 그래서 로컬에서도 중앙 서버와 동일하게 접속・작업・저장이 가능해야 하고, 중앙서버와 동기화가 되어 어떠한 환경에서든 동일 작업환경이 제공될 수 있어야 한다.

4.3 개발된 Algorithm Source Code 관리

개발된 AI Algorithm Source Code는 공개 수준 여부 검토에 따라 보안등급을 부여하고 생산부터 폐기까지 관리할 필요가 있다. 핵심 Source Code를 제외한 기타 개발된 소스코드는 군 AI 기술에 대해 엄격한 심의절차를 거쳐 산・학・연에 제공하여 AI 기술 교류를 확대하면서 군 내부의 인력풀과 기술을 통합하여 연구개발을 가속화해야 한다. Source Code는 라이선스 종류에 따라 공개 수준을 판단하는 기준은 Permissive는 자체개발, Weak Copyleft는 공동연구, Strong Copyleft는 민간 상용품을 구매할 때로 구분할 수 있다(Figure 5).

구분	AI Algorithm 설명
Permissive	▸대외기밀 유지가 중요한 무기체계 적용이나 지휘관의 의사결정을 지원하기 위해 자체 개발함. ▸소스 코드는 핵심기술로 분류하여 대외 비공개를 원칙으로 하는 것이 타당함. ▸라이선스는 Source Code 공개의무가 없고, 제약조건이 낮은 Apache, BSD, MIT 등을 사용함.
Weak Copyleft Algorithm	▸군사적으로 중요함에도 자체개발 능력부족이나 기타 사유로 산・학・연 공동연구 및 용역 등의 절차를 통해 개발한 SW ▸개발 초기 단계부터 외부 공개가 안 되는 핵심 Source Code는 사전에 엄격하게 분류하여 통제할 필요가 있음(군사보안에 제한이 없는 내용은 부분공개 등으로 분류하여 관리). ▸외부와 공동연구개발 시에도 OSS 통제나 보안유지 등에 대한 대책을 강구하여 개발해야 함. ▸라이선스는 Source Code 공개의무는 있으나, 제약조건이 낮은 EPL, LGPL 등을 사용함.
Strong Copyleft Algorithm	▸외부 공개 시 군사보안에 저촉되지 않을 SW ▸군 개발보다 민간 상용 AI를 구매・사용하거나 민간 OSS 활용하여 부분 수정하여 사용하는 것이 시간・비용적으로 유리한 경우에 적용할 수 있음. ▸라이선스는 Source Code 공개의무가 있고, 제약조건이 높은 AGPL, GPL 등을 사용함.



<Figure 5> Developed AI algorithm source code management

V. 결론 및 논의

전세계적으로 OSS 활용은 플랫폼을 통하여 활발하게 이루어지고 있으나, Open Source 공유에 따른 보안 취약성과 기술 종속화 등이 부정적 영향이 나타나고 있다.

우리 군은 AI 선진국 중심의 Algorithm 플랫폼에 대한 기술적 종속으로 군사주권의 위협이 발생하지 않도록 무기체계와 전력지원체계에 적용할 독자적인 군사용 AI Algorithm 개발이 중요하다. 또한, 군의 AI 개발 활성화에 따른 분산된 군 내부 인력과 기술을 효율적으로 활용하기 위해 국방 OSP 구축이 필요한 시점이다. 그래서 본 연구는 군 OSP 운용 시 보안 문제의 위험을 최소화하고, 장점을 최대화하기 위한 Algorithm Source Code를 관리하는 방안을 제시하였다. 구체적으로 초기에는 군 내부망을 활용하여 AI R&D OSP를 구축·운영하면서 군 내부 개발자 간의 Source Code 공유를 활성화하고, 관련 제도와 보안체계를 고도화하여 민간의 우수 기술도 적용·활용할 수 있는 산·학·연 협업 연구체계 구축이 필요하다. 특히 이런 협업 연구의 활성화 측면에서 개발된 Algorithm Source Code는 자체개발, 공동연구, 상용품 구매 등을 기준으로 공개의무 여부 및 제약조건을 분류하여 관리함으로써 군사적 비밀의 외부 유출을 방지하면서 상호 간의 공유·협업을 확대할 수 있을 것이다.

본 연구는 군사용 R&D OSP 구축을 위한 필요성과 운용개념을 사례분석 중심으로 진행하여 후속 연구는 이런 한계점을 극복하기 위해 다음과 같은 연구 주제 확대가 필요하다. 첫째, 후속 연구는 실무적 활용도를 높이기 위해 OSP 구축 후에 개발된 Algorithm 학습을 위해서 필요한 데이터 셋을 확보하여 긍정적 및 부정적 효과를 상세화할 필요가 있다. 그래서 기존 구축된 밀리터리 이미지넷(국방망)[48] 및 육군 데이터 랩(독립망)[49]과 연동시킬 수 있는 기술적 연구가 필요하다. 예를

들어 밀리터리 이미지넷은 군 내부 개발자에게 제공하기 위해 피・아 전투장비를 인식할 수 있는 학습이 완료된 Algorithm과 학습 및 평가용 데이터셋이며, 데이터 랩은 국방 AI 개발을 위해 필요한 데이터를 산학연에 제공하기 위해 수집해 놓은 원천 데이터가 저장된 플랫폼이다. 이렇게 군사용으로 구축된 데이터 활용도를 높이기 위해 네트워크 보안 문제가 해소될 필요가 있으며, 이에 관한 기술적・정책적 개선요소를 도출하는 연구가 활성화되어야 할 것이다. 둘째, 민간 부분의 AI 전문가나 비전문가의 국방 AI 개발 참여를 확대하기 위해 관련 AI 모델 개발에 보다 쉽게 접근할 수 있도록 사용자 인터페이스 연구와 OSP 제공 방안에 관한 연구가 필요하다. 특히, AI 개발 완성도를 높일 수 있도록 개발에 필요한 사용자의 요구와 개념 발전 및 개발된 SW의 사용자 개선요구 등에 관한 기초 연구가 지속될 필요가 있다.

Acknowledgements

We would like to thank Editage (www.editage.co.kr) for English language editing.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Author contributions

Conceptualization: LS; Resources and Literature review: LS; Investigation and Methodology: LS and JS; Writing (Original Draft): LS and JS; Writing (Review and Editing): LS and JS; Project administration and Supervision: LS.

48) 육군 국방망에 서버를 구축한 플랫폼으로 피・아 전투장비의 이미지를 인식할 수 있도록 개발된 AI Algorithm과 학습 및 평가용 데이터셋이 구축되어 있음.

49) 국방 AI 개발을 위해 군 학습용 데이터를 산・학・연에 제공할 수 있도록 구축한 플랫폼이며, 인터넷이나 인트라넷에 연결되지 않은 독립망으로 구축되어 있음.

Reference

Ahn, I. T. (2005). Economic Effects of Government's Supports for Open Source Software. *Journal of Economic Theory and Econometrics, 16*(3), 51-76. UCI : G704-000295.2005.16.3.003

Baek, K. H., Ha, E. A., & Cho, J. K. (2016). The Pattern and Meaning of New Creation on Open Source Platforms. *Journal of Basic Design & Art, 17*(6), 271-282. UCI : G704-001069.2016.17.6.003

Cheon, J. U., & Jeong, S. J. (2019). A Study on the Limits and Improvement of the Current Korean Military Weapon System Planning Method according to the Change of Age : Based on the demand pull/technology-push theory. *STRATEGIC STUDIES, 26*(3), 37-57. https://doi.org/10.46226/jss.2019.11.26.3.37

Cho, J. K. (2021). The Analysis and Development Plans of Defense Artificial Intelligence Infrastructure. *The Quarterly Journal of Defense Policy Studies,* 36(4), 109-146. https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002677396

Cho, S. G. (2021). Sharing economy 2.0. Seoul: BOOK21. https://www.book21.com/book/book_view.html?bookSID=5545

Choi, E. J., Lee, J. Y., & Han, I. G. (2020). Deriving adoption strategies of deep learning open source framework through case studies. *Journal of Intelligence and Information Systems, 26*(4), 27-65. https://doi.org/10.13088/jiis.2020.26.4.027

Chun, S. Y., Yoon, S. W., & Jeong, S. J. (2020). A Study on the Business Model Design and Economic Evaluation of Open Source Software License Compliance Platform. *JOURNAL OF THE KOREA SOCIETY FOR SIMULATION, 29*(2), 1-10. https://doi.org/10.9709/JKSS.2020.29.1.001

Horowitz, M. C., Allen, G. C., Kania, E. B., & Scharre, P. (2018). Strategic competition in an era of artificial intelligence. Center for a New American Security. http://www.indexfunds.org/resources/Research-Materials/NatSec/Strategic_Competition_in_Era_of_AI.pdf

Jang, H. S., & Kim, J. B. (2017). Suggestions for Activation of Open Source Software in the Defense Sector. *Jounal of The Korea Society of Information Technology Policy & Management, 9*(3), 407-414. https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002236522

Jung, D. S. (2021). A Study on the Direction of the Defense Artificial Intelligence Ecosystem

Building. *Journal of National Defense Studies, 64*(3), 27-60. https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002765442

Kang, S. H., Shim, D. N., & Pack, P. H. (2015). A Study on the Problems and Policy Implementation for Open-Source Software Industry in Korea: Soft System Methodology Approach. *The Journal of Society for e-Business Studies, 20*(4), 193-208. https://doi.org/10.7838/jsebs.2015.20.4.193

Layton, P. (2018). Algorithmic warfare: Applying artificial intelligence to warfighting. Air Power Development Centre. https://airpower.airforce.gov.au/publications/algorithmic-warfare-applying-artificial-intelligence-warfighting

Lee, W. J., Seo, K. D., & Chae, B, M. (2020). A study on security threats to drones using open source and military drone attack scenarios using telemetry hijacking. *Journal of Convergence Security, 20*(4), 103-112. https://doi.org/10.33778/kcsa.2020.20.4.103

Lee, Y. J., & Rim, S. R. (2016). A scheme of Docker-based Version Control for Open Source Project. *Journal of the Korea Academia-Industrial Cooperation Society, 17*(2), 8-14. https://doi.org/10.5762/KAIS.2016.17.2.8

Lee. S. G. (2022). A Study on the Influence of AI Development on New Arms Competition. *Military Research and Development. 16*(1), 123-151. https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002858550

Levine, S. S., & Prietula, M. J. (2014). Open collaboration for innovation: Principles and performance. *Organization Science*, *25*(5), 1414-1433. https://doi.org/10.1287/orsc.2013.0872

Linh, N. D., Hung, P. D., Diep, V. T., & Tung, T. D. (2019, February). Risk management in projects based on open-source software. *In Proceedings of the 2019 8th International Conference on Software and Computer Applications* (pp. 178-183). https://doi.org/10.1145/3316615.3316648

Park, J. B., & Yang, H. S. (2012). Quality Evaluation Method of Open Source Software. *Journal of the Korea Academia-Industrial cooperation Society, 13*(5), 2353-2359. https://doi.org/10.5762/KAIS.2012.13.5.2353

Ryoo, W. O., Jo, S. H., & Lee, S. Y. (2021). A study on the safe use of open source through open source security vulnerability management. *In 2021 Spring Korean Institute of Communication and Information Sciences Conference* (pp. 854-855).

Son, H. W., Lee, S. J., & Heo, W. S. (2022). Analysis of types of attacks in cyber warfare between Russia and Ukraine. *In Korean Institute of Information Scientists and Engineers Conference* (pp. 2160-2162).

Weber, S., & Luo, J. (2014, December). What makes an open source code popular on git hub?.

In 2014 IEEE International Conference on Data Mining Workshop (pp. 851-855). https://doi.org/10.1109/ICDMW.2014.55

원 고 접 수 일 2022년 11월 26일
원 고 수 정 일 2022년 12월 21일
게 재 확 정 일 2022년 12월 28일

IDAP 광운대학교 방위사업연구소 INSTITUTE OF DEFENSE ACQUISITION PROGRAM

JAMS JOURNAL OF ADVANCES IN MILITARY STUDIES

2022, Vol. 5, No. 3, 23-42.

https://doi.org/10.37944/jams.v5i3.177

국방 AI 개발 활성화를 위한 군 R&D Open Source Platform 구축 필요성*

이상근** · 장상국***

국문초록

군사 선진국은 AI 기반의 무기체계 지능화를 위해 국방 AI Algorithm 개발에 주력하고 있다. 그러나 무기체계에 AI를 접목하기 위한 Algorithm 개발은 많은 시간과 노력, 예산이 소요되므로 산·학·연과 공유·협업을 확대하기 위한 Open Source를 활용한 개발이 필요하다. 본 연구의 목적은 Open Source SW의 군 무기체계에 적용 시 보안 취약점의 부정적 영향에도 군 활용의 필요성을 제기하고, 활용·개선 방안을 제시하는데 있다. 이를 위해 국내외 및 국방 분야의 오픈 소스 플랫폼(Open Source Platform) 활용에 관한 사례분석을 중심으로 Open Source의 개방형 공유와 협업의 긍정적 측면과 기술 종속화와 보안 취약점 노출의 부정적 측면에서 시사점을 도출하였다. 이런 결과를 토대로 우리 군의 군사주권 확보 및 기술 종속화 방지, AI 연구개발의 효율성 증대, 무기체계간 협업과 연결성 보장, SW의 보안성 강화를 위해 Open Source Platform 구축의 필요성을 제기하였다. 또한, Open Source Platform의 역할과 운용 및 Source Code 관리 차원에서 정책적 발전 방향과 후속연구 제언을 제시하였다.

주제어 : 군 AI 적용, 군사주권 확보, 기술 종속화와 보안, 오픈 소스 플랫폼, 공유와 협업

* 2022년 선진국방 융합학술대회에 발표한 논문을 확장한 것임(22.11.26).

** (제1저자) 조선대학교 군사학과 박사과정(육군교육사령부 AI 개념발전과장), rbfl5547@naver.com, https://orcid.org/000-0003-0866-0727.

*** (교신저자) 조선대학교 군사학과, 교수, skjang1@chosun.ac.kr, https://orcid.org/0000-0001-5258-8107.