Journal of KOSSE. (2020. 6) Vol. 16, No. 1 pp. 36-42
DOI: https://doi.org/10.14248/JKOSSE.2020.16.1.036
www.kosse.or.kr

ISSN (print) : 1738-480X
ISSN (online) : 2288-3592

무인화 무기체계의 안정적인 운용을 위한 Cybersecurity 및 Anti-Tamper의 적용

이민우*

방위사업청

Applying Cybersecurity and Anti-Tamper Methods for Secure Operating of Unmanned Weapon Systems

Min Woo Lee*

Defense Acquisition Program Administration

Abstract : Due to the population of the Republic of Korea is getting less, the shortage of available troops has become a big issue. In response to this, the need for Unmanned weapon systems is rising. To operate an Unmanned weapon system near borderlines or low altitude, it is necessary to protect not only the system itself but also operational information communicated between the Unmanned system and control station, so that they should be safe using Cybersecurity measures. Besides, it is critical to protect a few core technologies applied to Unmanned weapon systems throughout the Anti-Tamper measures. As the precedent studies only focus partially, Cybersecurity or Anti-Tamper, it is acknowledged that comprehensive studies are needed to be conducted. This study is to incorporate both concepts into Korea's defense acquisition process. Specifically, we will outline the concepts and needs of Cybersecurity and Anti-Tamper, and briefly present ways to apply them simultaneously.

Key Words : Unmanned weapon systems, Cybersecurity, Anti-Tamper, Defense acquisition process, Weapon systems R&D

Received: April 20, 2020 / **Revised**: May 14, 2020 / **Accepted**: May 28, 2020

* 교신저자 : Min Woo Lee, ftstblue@korea.kr

1. 서 론

최근의 병력부족 문제와 함께, 장병들이 위험에 노출되지 않도록 하려는 사회적 요구가 증가하고 있다. 이에 따라 지상, 공중, 해상 및 수중 등 모든 전장환경에서 무인화(無人化, Unmanned) 무기의 필요성이 점증하고 있다. 한편, 사이버공간에서의 다양한 위협은 비단 국방 분야뿐만이 아닌 전 국가 기반체계에 경각심을 주고 있으며, 국가자산인 첨단 기술의 탈취 위협 역시 날로 심각해지고 있어 기술 보호 제도, 조직, 수단 등이 강하게 요구되고 있다.

무인화 무기체계를 투입하기 위한 두 가지 선결 조건이 있다. 첫째, 의도적 또는 비의도적으로 무기체계가 제3자의 손에 나포 또는 탈취되지 않도록 다양한 유통정보, 특히 자율운행을 위한 항법정보 또는 운용자의 조작정보 등에 대한 철저한 보안성 확립이 필요하다. 둘째, 무인화 무기체계에 적용된 기술들은 상당수가 안보상 민감한 최신기술이므로 부적절한 나포 또는 탈취에도 불구하고 공격자들의 핵심기술에 대한 접근을 최대한 저지하여야 한다.

이를 위해 무기체계에 Cybersecurity 및 Anti-Tamper 적용이 필요한데, 한국은 아직 연구개발 프로세스에 명문화되지 않는 등 제도적으로 미비점이 있다. 또한, 두 가지 개념을 각각 적용하기 위한 부분적인 선행연구들은 있었지만, 통합적 시각에서 연구가 수행된 실적은 거의 없으므로 무인화 무기체계의 안정적인 운용과 기술보호 목표를 동시에 달성하기 위한 노력이 필요하다.

본 연구는 국내 연구개발 프로세스에 양 개념을 접목시키기 위한 노력의 출발점이다. 제2장에서는 Cybersecurity, Anti-Tamper를 앞서 정착시킨 미국 관점에서 살펴보고 이들의 무인화 무기체계 적용 필요성에 대해 짚어보았다. 제3장과 제4장에서는 국내외의 관련 제도 및 선행연구의 현황과 그 한계점을 제시한 뒤 두 가지 개념을 국내 연구개발 프로세스에 적용할 수 있는 방안을 제시하였다. 결론인 제5장에서는 연구내용을 요약하고 향후 발전 방안에 대해 논하였다.

2. Cybersecurity와 Anti-Tamper

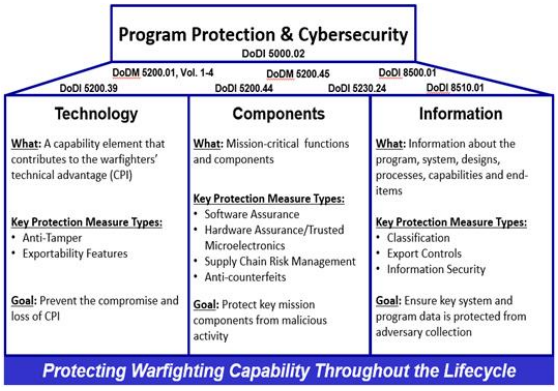
2.1 개념의 정의

미국 정부는 Cybersecurity를 "컴퓨터, 전자통신, 시스템 및 서비스, 유선통신, 전자통신과 그 안에 담긴 정보에 대한 피해를 예방 보호, 복원하여 기밀성, 무결성, 가용성, 인증, 부인방지를 보장하는 것"이라고 정의하고 있다[1]. 무기체계 관점에서 이를 바라본다면, 네트워크 중심의 작전환경(Net- Centric Operation Environment, NCOE) 내에서 정보교환의 기밀성, 무결성, 가용성 등을 확보하기 위해 무기체계 및 전장망에 대한 인증 및 부인방지 등을 수행하는 것으로 해석할 수 있다. 무인화 무기체계는 네트워크 없이 운용될 수 없기에, 반드시 Cyber-security 적용이 필요하다고 하겠다.

한편, 미 국방성은 "비의도적 기술이전 또는 역설계로 인한 시스템 변경 및 대응수단이 개발되는 것에 대비하기 위해 무기체계로부터 중요한 정보(Critical Program Information) 유출을 방지 또는 지연시키는 시스템공학 활동"을 Anti-Tamper로 정의하고 있으며[2], 이는 단독으로 적용되는 것이 아니라 아래 그림 1과 같이 Program Protection 및 Cyber-security 등 활동과 통합적으로 이행된다.

2.2 무인화 무기체계를 위한 적용 필요성

서론에서 언급한 바와 같이, 무인화 무기체계는 적성국 또는 제3국의 Jamming, Spoofing 및 Sniffing



[Figure 1] Program Protection & Cybersecurity[3]

등의 사이버공격에 대한 취약점을 최소화해야 한다. 또한, 운용자의 조작 실수나 뇌전, 강우 등의 환경적 요인, 오동작으로 인한 비의도적 유실 등에도 불구하고 시스템에 적용된 기술이 함부로 유출되지 않도록 하는 조치들이 필요하다. 해외로 수출된 무인화 무기체계의 경우 수출대상국 운용자의 조작 미숙으로 인한 유실 가능성이 클 것이므로, 수출대상국의 적성국 또는 접경국에 의한 기술탈취 가능성 역시 상당하다고 하겠다. 한편, 수출대상국 역시 정비능력의 향상 또는 기술탈취를 목적으로 국내개발 무인화 무기체계에 무단접근할 가능성을 배제하기 어렵다. 정리하자면, 무인화 무기체계의 특성을 고려할 때 네트워킹을 위한 기밀성, 무결성, 가용성 등의 확보와 함께 중요기술의 유출을 방지 또는 지연시켜야 함이 자명하며, 이를 위해 반드시 Cybersecurity와 Anti-Tamper를 적용해야 한다.

3. 관련제도 및 선행연구 분석

3.1 미국과 대한민국의 제도 비교

본 장에서는 미국과 우리나라의 Cybersecurity및 Anti-Tamper 관련 현주소를 짚어보고자 한다. 그림 2와 같이, 미국은 관련활동이 국방성의 획득 프로세스에 통합되어 있고 전담조직이 운영될 뿐만 아니라 연합작전을 수행하는 동맹국의 연동체계까지도 Risk Management Framework (RMF)라는 보증 프로세스의 준수를 요구하는 등 보다 완벽한 보안환경을 구축하고자 노력하고 있다.

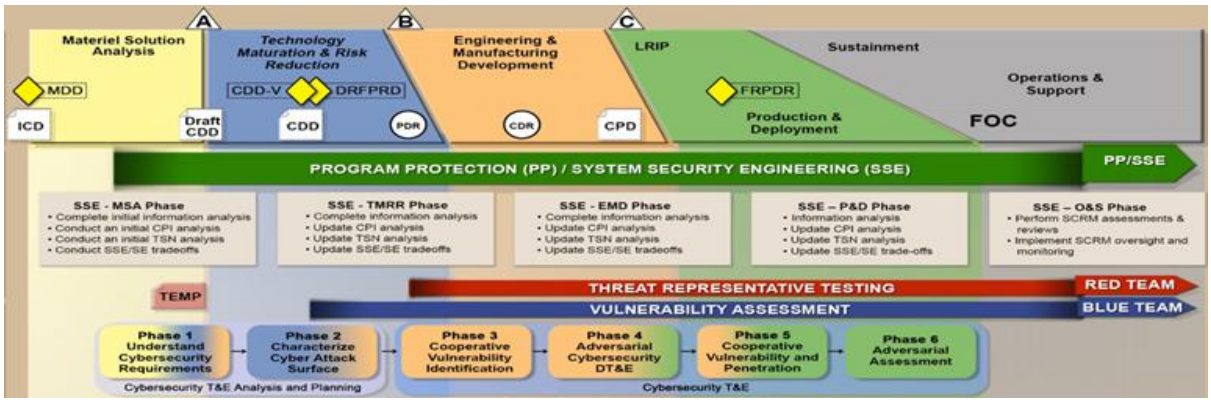
우리나라는 Cybersecurity 적용을 위한 제도적 기반은 마련되어 있으나 이행 방법론이 정립되지 않았고, 보호 또는 통제수단의 적절성을 평가하는 수준에 그치는 등의 한계가 지적된 바 있다[5, 6].

한편, 최근 방위사업청은 Anti-Tamper에 대한 방산업체의 인지도가 매우 낮으며 몇몇 기업들만이 그 개념과 필요성을 인지하고 있음을 직접 확인한 바 있다. 따라서, Anti-Tamper의 경우 제도 도입 논의에 앞서 인식 제고가 필요하다고 판단된다.

3.2 선행연구 분석

본 논문에서 살펴본 선행연구는 요소기술 확보보다는 프로세스 확립 차원에서 수행된 것들을 위주로 분석하였으며, 따라서 무인체계의 강건한 기동성이나 신뢰성 등에 대한 연구들은 배제하였다.

먼저 Cybersecurity 관련 선행연구로서, 사이버공격에 대한 UAV의 취약점을 분석한 발표[7, 8], 시험평가 프로세스와 접목[1], 다양한 플랫폼 대상 보안취약성 분석[9, 10] 등의 연구가 수행되었다. Anti-Tamper와 관련된 국내 선행연구는 2017년 이후에야 활성화되기 시작하였는데, SW 보호기법 위주의 연구[11, 12]와 일부 절차를 활용한 적용사례 연구[13, 14] 등에 이어 저자에 이르러서야 국내 획득프로세스 적용을 위한 연구[2, 15, 16]가 이루어졌다. 한편, 우리나라에 Cybersecurity 및 Anti-Tamper를 모두 적용하기 위해 수행된 선행



[Figure 2] Acquisition process of the U.S.[4]

연구는 찾아볼 수 없었으며, 이들 중 하나의 개념을 적용하기 위한 연구만이 수행된 것으로 식별하였다.

4. Cybersecurity 및 Anti-Tamper의 대한민국 획득 프로세스 적용방안

앞서 언급한 바와 같이, 현재 한국의 제도와 선행 연구들로는 Cybersecurity, Anti-Tamper의 적용 및 이행에 제한사항이 많다고 판단되는 바이다. 본 장에서는 이들 개념을 적용하기 위해 공통적으로 필요하다고 판단되는 부분을 먼저 짚어 본 이후, 각 개념별로 필요한 사항을 제시하고자 한다.

4.1 적용방안 공통사항

기존에 없던 새로운 개념을 적용함에 있어 가장 먼저 필요한 것은 바로 인식제고를 위한 공감대 형성이라 하겠다. 이를 위해 무기체계 획득에 관계된 정부조직과 출연기관, 합참과 군, 방산업체 모두가 Cybersecurity 및 Anti-Tamper의 적용 필요성과 효율적인 구현방안 마련에 대한 인식을 공유해야 할 것이다. 미국 정부의 RMF 적용에 따른 우방국 준수 요구와 함께 최근 대두되는 보안이슈 등으로 인해 Cybersecurity 분야에 대한 인식은 충분히 확산되고 있다고 판단되며, 따라서 Anti-Tamper에 대한 인식 제고를 위한 노력이 요구되는 바이다. 다행히 최근 몇몇 방산업체에서 수출소요가 발생함에 따라 무기체계 기술보호를 위한 Anti-Tamper 적용방안 연구를 자체적으로 수행하는 등 긍정적인 신호가 있어 이를 합참 및 각군 등으로 확장하려는 시도가 필요하다.

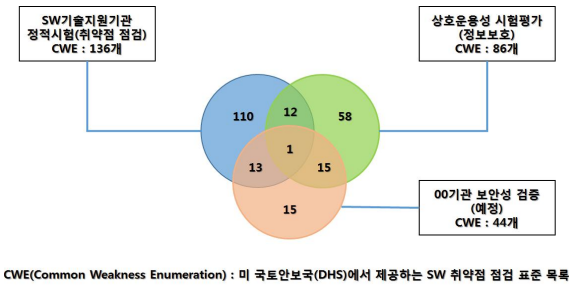
다음으로, 전문인력 양성이 필요하다. 현재까지는 운용중인 무기체계에 대한 보안취약점 분석 도구와 인력만이 운영되고 있는 바, 군에서 2016년 최초로 임관한 '사이버전문사관' 인력을 Cybersecurity 분야에 투입되도록 하고 이들이 사회로 복귀하여 방산업체에서 유사업무를 수행할 수 있도록 하는 배려가 필요하다고 판단된다. Anti-Tamper 분야 역시 민-관-군 전문인력의 양성과 함께 전문조직 설립을 통해 지속적인 선순환 구조가 이루어지도록 해야 한다. 상호운용성 분야의 기술지원 목적으로 국군지휘통신사령부 예하에 설립된 합동상호운용성 기술센터가 벤치마킹을 위한 좋은 사례라고 본다. 전문조직이 설립되면 그들에게 설계과정뿐 아니라 시험평가 및 운영유지 단계까지 포함한 총수명주기 동안 취약점 진단 등을 수행하는 'Blue Team', 화이트해커와 같이 무기체계 위협 시험을 수행하는 'Red Team'을 구성하여 운영하면 좋을 것이다. 한편으로는 외부 보안전문인력의 집단지성을 적극 활용하기 위해 '버그 바운티' 제도를 도입하는 방안을 장기적으로 도입한다면 더욱 완벽한 보안성 확립에 도움이 될 것으로 판단된다.

마지막으로, 무인화 무기체계의 중요한 구성요소, 즉 Cybersecurity 및 Anti-Tamper를 적용해야 하는 통신·암호화/복호화·자율연산 등에 관련된 부체계 및 구성품의 경우 모듈화 설계를 적용하고 공급망 신뢰성을 확인하고 부품 단위까지 확장하여 이력을 관리하여야 한다. 2019년 10월 발표된 4차 산업혁명위원회 대정부 권고안 부록[17] 중 사이버 보안 정책제언 역시 이러한 조치를 통하여 백도어 이슈에 대응해야 함을 제시하고 있다.

4.2 Cybersecuriy의 적용방안

기술적으로는 Cybersecurity 적용을 위한 핵심 기술개발 사업들이 추진되고 있으므로, 본고에서는 제도적 측면과 프로세스 측면에서의 개선점에 대해 제시한다. 먼저, 국방 상호운용성 분야와 무기체계 SW 신뢰성 분야 간 중첩되거나 누락되는 영역들을 종합적으로 검토 및 보완하여야 한다. 김성남[6]이 제시한 그림 3과 같이, 무기체계 SW 점검항목은 중복되거나 단일 기관에 의해 확인되고 있다.

이러한 상황에서 우려되는 점은 점검이 필요한 항목을 누락하거나 불필요한 중복점검이 이루어질 수 있다는 것이다. 누락된 점검항목은 자연스럽게 취약점으로 이어질 것이고, 중복점검에 따른 일정 지연은 군의 전력화 일정에 차질을 야기할 것이다. 따라서, 관련 기관이 이해관계를 벗어나 머리를 맞



[Figure 3] Weapons' SW Vulnerability Checklist[6]

대고 점검항목의 효율적인 통합이 이루어지도록 개선하려는 노력이 필요하다.

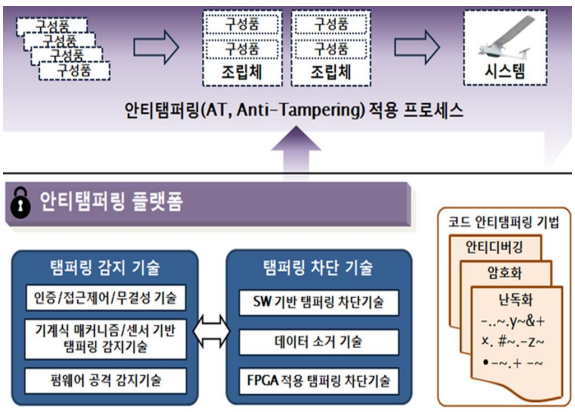
하지만, Cybersecurity는 소프트웨어 분야로만 한정된 것이 아니므로 연구개발사업 초기부터 모든 이해관계자에 의한 개발·검증 요구사항의 도출과 개발 및 운용시험평가 적용방안 확립 등의 노력이 추가로 요구된다. 이는 4.1절에서 제시한 전문기관 설립과 모듈화 설계, 공급망 신뢰성 확보 등과 함께 이루어져야 한다. 최종적으로 획득 프로세스에 통합되어 무기체계 Cybersecurity 적용과 함께 미국의 RMF 적용 요구까지 충족할 수 있을 것이다.

4.3 Anti-Tamper의 적용방안

Cybersecurity 관련 국내 핵심기술 개발이 비교적 활발하게 수행되고 있는 반면, Anti-Tamper 관련 핵심기술 개발은 2019년 말에 비로소 시작되었다. 해당 개발과제는 국방과학연구소 주관으로 2023년까지 수행될 예정이며, SW 기반으로 탬퍼링 공격을 감지하고 이를 차단하기 위한 기법과 이를 검증할 수 있는 플랫폼 등이 개발될 예정이다.

개발과제를 통해 도출된 기법들은 방위사업청의 국방기술보호국 주도로 철저히 관리하며, 통합사업관리팀이 연구개발 사업을 추진할 때 연구개발주관기관(국방과학연구소 또는 방산업체)이 무기체계에 적용할 수 있도록 하는 가이드라인을 관련 규정에 반영해야 할 것이다.

한편, 무기체계에 이러한 기법들을 효율적·효과적으로 적용하기 위한 프로세스 역시 해당 과제의 위탁연구를 통해 도출될 예정인데, 기존 선행연구[2, 13-16]에서 이미 논의되었던 사항들이 있어 비교적 수월하게 도출될 것으로 기대되는 바이다. 특히 이민우 등[15]이 제시한 바와 같이 보호기법 적용 대상이 되는 기술과 적정한 보호수준의 결정, 무기체계 설계를 위한 개발·검증 요구사항의 도출, 시험평가 등 Anti-Tamper 적용을 위한 연구개발 프로세스 개선 포인트는 이미 어느 정도 식별되어 있으므로, 사업 담당자 및 개발자들이 효율적으로 적용할 수 있는 방향으로 다듬어가면 좋을 것이다. 이렇게 Cybersecurity 및 Anti-Tamper를 무인화 무



[Figure 4] Concept of Weapons' SW platform Anti-Tampering technology R&D Project[18]

<Table 1> Methodologies for applying Cybersecurity and Anti-Tamper (Summarized)

분 야	내 용	비 고
공 통	인식제고	Anti-Tamper 인식제고 시급
	전문인력 양성 및 전문조직 설립	합동상호운용성 기술센터 벤치마킹
	주요 구성요소의 모듈화 설계	적용 효율성 상승
	HW 공급망의 신뢰성 확보	백도어 대비 가능
Cyber-security	유사분야 점검항목 통합	상호운용성, 무기체계 SW
	국내 무기체계 획득 프로세스와 통합	미국의 RMF 적용 요구에 대응 가능
Anti-Tamper	보호기법 개발 및 관리, 제도 반영	방위사업청 국방기술보호국이 주도
	국내 무기체계 획득 프로세스와 통합	선행연구를 토대로 발전시킬 필요

기체계를 대상으로 적용하고, 점진적으로 다양한 무기체계로 확대해 나갈 수 있을 것으로 판단된다. 지금껏 제시한 적용방안을 종합하면 표 1과 같다.

5. 결 론

서론에서 언급한 바와 같이, 무인화 무기체계의 중요성이 증진되는 현 상황에서 Cybersecurity 및 Anti-Tamper를 동시에 적용하여 안정적인 운용을 도모하는 것은 반드시 이루어야 할 중요한 과제라 하겠다. 아직은 이러한 제도의 도입이나 적용방안 연구가 다소 미비한 것으로 보이며, 지금부터라도 인식 제고를 위해 노력하고 전문인력 양성을 통해 전문조직을 설립하는 한편, 무인화 무기체계의 중요 구성요소에 대한 모듈화 설계와 HW 공급망 신뢰성 확보 등의 노력이 필요하다. 또한 요소기술의 개발 및 관리와 더불어 국내 무기체계 획득 프로세스와 통합하여 적용하는 방안 마련이 필요하며, 이러한 노력을 통해 비로소 무기체계 획득과 관계된 모든 이해관계자들이 연구개발 과정에서 Cybersecurity 및 Anti-Tamper를 적용하는 데 참여할 수 있을 것이다. 향후에는 무인화 무기체계뿐만 아니라 해외 수출, 접경지 운영 등을 고려하여 다른 무기체계도 Cybersecurity와 Anti-Tamper의 적용을 검토할 필요가 있다.

본 연구에서 제시하는 방안들이 정답은 아니지만 최소한의 가이드라인을 제시하였다고 판단되는 바, 후속 연구를 통해 부족한 부분은 보완하고 도출된 방안은 강화할 수 있도록 논의하는 장이 열리기를 기대한다.

References

1. 이지섭, 차성용, 백승수, 김승주, “무기체계의 사이버보안 시험평가체계 구축방안 연구,” 정보보호학회논문지, Vol. 28, No. 3, pp. 765-774, 2018.

2. 이민우, 이재천, “무기 시스템 개발에서 기술보호를 위한 위험관리 기반의 Anti-Tampering 적용 기법,” 한국산학기술학회논문지, Vol. 19, No. 12, pp. 99-109, 2018.

3. K. Baldwin, “Program protection,” in Proc. DAU Acquisition Training Symposium, Fort Belvoir, VA, Apr 27, 2016.

4. U.S. Defense Acquisition University (DAU), “Cybersecurity & the Acquisition Lifecycle Integration Tool,” Sep 2018.

5. 임재혁, “사이버위협 대비 소프트웨어 보증 전략:미국의 동향과 시사점,” 국방논단, Vol. 1752, 2019년 4월.

6. 김성남, “국방 상호운용성과 무기체계 SW 보안성 확보에 관한 연구,” 2019년 한국군사과학기술학회 종합학술대회, 제주, 2019년 6월, pp. 2102-2103.

7. A. Y. Javaid, W. Sun, V. K. Devabhaktuni and M. Alam, “Cyber security threat analysis and modeling of an unmanned aerial vehicle system,” 2012 IEEE Conference on Technologies for Homeland Security (HST), Waltham, MA, 2012, pp. 585-590.

8. K. Hartmann and C. Steup, “The vulnerability of UAVs to cyber attacks - An approach to the risk assessment,” 2013 5th International Conference on Cyber Conflict, Tallinn, 2013, pp. 1-23.

9. 김현주, 강동수, “전투기 감항 보안 인증을 위한 위험기반 보안위협 평가 프로세스 설계,” 정보처리학회논문지:소프트웨어 및 데이터공학, Vol. 8, No. 6, pp. 223-234, 2019년 6월.

10. 강태경, 정대연, 성기열, 김종원, “상용차량 공격사례 기반 무인수색차량 위험분석,” 2018년 한국군사과학기술학회 종합학술대회, 제주, 2018년 6월, pp. 1631-1632.

11. M. H. Jang, Y. S. Ryu, H. K. Park, “A FPGA-based scheme for protecting weapon system software technology,” In Proc. ICCSA 2018, Jul 2018. pp. 148-157.

12. 이규호, 유재관, 김인성, 김태규, “무기체계 안

티탬퍼링을 위한 소프트웨어 소스코드 난독화 도구 구현," 정보과학회논문지, Vol. 46, No. 5, pp. 448-456, 2019년 5월.
13. 이효근, 이운순, 오유진, 박신석, "방위산업 기술보호 동향분석 및 기법적용," 한국군사과학기술학회지, Vol. 20, No. 4, pp. 579-586, 2017.
14. H. S. Chae, C. S. Lee, T. H. Kim, "The Anti-tampering Process and Case Study by the Operating Mode of Various UGV," In Proc. 2018 IEEE/ASME International Conference on AIM, Jul 2018.
15. 이민우, 이재천, "무기시스템 기술보호를 위한 수명주기 프로세스," 2019년 한국시스템엔지니어링학회 춘계학술대회, 서울, 2019년 5월.
16. 이재율, "연구개발 사업을 위한 방산기술보호 업무 프로세스에 대한 연구," 2019년 한국군사과학기술학회 종합학술대회, 제주, 2019년 6월, pp. 2064-2065.
17. 대통령직속 4차산업혁명위원회, "4차 산업혁명 대정부 권고안," 2019년 10월.
18. 국방과학연구소, "시제제작 제안요청서(사업명 : 무기체계 소프트웨어 플랫폼 안티탬퍼링 기술)", 2019년 3월.