정 보 보 호 학 회 지
제28권 제6호, 2018. 12

무기체계 사이버 보안 정책 동향

이 정 규*

요 약

무기체계를 대상으로 한 다양한 형태의 사이버 위협에 직면하고 있다. 실제 상대국을 대상으로 한 공격행위도 언론을 통해 발표되고 있다. 무기체계를 대상으로 한 사이버 공격은 실물 공격보다도 더 큰 위력을 발휘하기 때문에 이를 대비하기 위한 보안 검증 강화는 그 무엇보다도 중요하다고 할 수 있다. 본 고에서는 이러한 사이버 위협, 미국과 우리의 보안정책을 알아보고 문제점을 진단하여 현실적 개선방향을 제시하고자 한다.

Ⅰ. 서 론

최근 컴퓨터 기술의 급속한 발전으로 무기체계에서의 비중 또한 커지고 있는 것이 현실이다. 이러한 상황은 사이버전에서도 변화를 보이고 있다. 기존 사이버 공격은 정보체계와 인터넷 망을 대상으로 대부분 이루어 졌으며 당연시 되어 왔었으나 현재는 물리적으로 분리된 환경과 소프트웨어에 대해서도 위협이 실존하고 있고, 그 공격양상 또한 다양화 고도화 융합화 되는 경향을 보이고 있다. 이러한 변화는 향후 사이버전의 양상도 전략·전술 정보체계 마비를 위한 사이버 공격뿐만 아니라 정보통신기술이 접목된 다양한 무기체계의 마비 및 오동작 유발을 위한 공격으로 까지 확대 될 것이다.

우리나라는 정보통신기반체계와 국방의 지휘통신체계 및 무기체계가 북한에 비해 절대적으로 정보화 의존도가 높기 때문에 이와 같은 사이버 공격 발생시 더욱 더 심각한 피해가 발생할 것이라고 전문가들은 예상하고 있다[1-3].

따라서 본 고에서는 정보통신기술이 접목된 무기체계 등 주요체계에 직접적 위협이 될 수 있는 다양한 사이버 위협, 미국과 우리의 무기체계 사이버보안정책을 알아보고, 이러한 상황에 직면한 우리의 무기체계 보안의 현주소를 진단하여 개선방향을 제시하고자 한다.

Ⅱ. 무기체계 사이버 보안

본 장에서는 각종 언론 등을 통해 발표된 무기체계에 영향을 미칠 수 있는 사이버 위협 사례와 미국의 사이버 보안정책을 살펴보고자 한다.

2.1. 위협 사례

2.1.1. 레프트 오브 론치(Left of Launch) 작전

악성코드와 전자기파 등으로 미사일 통제시스템을 교란해 발사 전 시스템을 무력화하는 작전. 미사일 발사를 '준비→발사→상승' 단계로 나눌 때 '발사'보다 왼쪽에 있는 '준비' 단계에서 악성코드나 전자기파 공격으로 시스템을 교란하는 것이다. 그래서 코드명으로 '발사의 왼편'(Left of Launch)이라는 말이 쓰였다. 미국은 2013년 2월 북한의 3차 핵실험 이후에 '레프트 오브 론치' 프로그램을 공개했다. 미국 뉴욕 타임즈는 지난 4월 16일 북한이 발사한 미사일도 발사 직후 곧바로 폭발한 것으로 파악돼 레프트 오브 론치의 결과물일 수 있다고 보도했다[4].

2.1.2. RQ-170

이란은 RQ-170의 제어 탈취에 교란 및 GPS 탐지 공격을 사용하였다고 주장하고 있으나 일부에서는 이 기체가 레이더에 탐지되지 않고 이란의 무인 사막지대

* 명지대학교 보안경영공학과 객원교수 (wjdrb1004@hotmail.com)

에 원인미상의 이유로 고장이 발생하여 불시착 했을 것이라고 주장하는 설도 있다.

어떤 경위든 미군의 RQ-170은 이란이 확보하였고 이란은 미 공군도 인정하는 UAV 약점을 제시하고 있다. 이란은 뜻밖의 기회에 세계를 상대로 선전전을 전개하고 자국의 전자 사이버 능력의 성과라고 선전하였다. 그뿐 아니라 UAV의 취약점을 분석 제시하며 리버스 엔지니어링을 통해 획득한 정보를 활용하여 신형 전투 무인 항공기 Saeqeh를 개발하여 발표했다[5].

2.1.3. 美 차세대 무기체계 해킹에 취약[6]

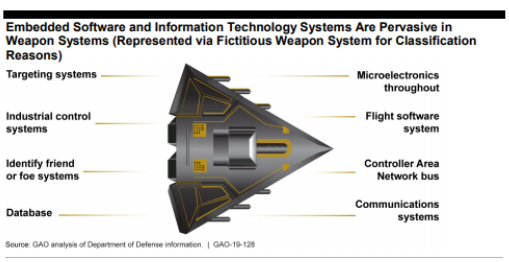
미 회계검사원(GAO)에서 지난 '18.10.9. 미국 국방부가 개발 중인 차세대 무기체계 전산망이 해킹에 취약한 것으로 드러났다고 밝혔다.

실제 2인 1조로 구성된 GAO의 모의해킹팀은 불과 1시간 만에 무기체계 전산망에 접속할 수 있었고, 전체 관리자 권한을 얻는 데는 단 하루밖에 걸리지 않았다고 한다.

차세대 무기체계는 그림 1에서처럼 그 어느 때보다도 많은 시스템들이 더 네트워크화 되어 있으며 그로 인해 액세스 포인트(AP)의 수가 계속 늘면서 전산망 관리자들이 이를 통제하는 것에도 한계가 발생하였을 뿐만 아니라 컴퓨터 의존형 무기의 설계·조달에도 사이버 보안기술을 적용하지 않고 있었다고 밝혔다.

컴퓨터를 이용한 무기체계 등의 상호운용성이 커지면서 해킹 등의 위험 또한 함께 커지고 있다고 지적했다.

특히 이번 테스트에서 기본 암호관리 소홀 및 암호화되지 않은 통신과 이미 인지하고 있는 취약성에 대한 후속조치 미흡으로 인해 너무도 손쉽게 시스템이 장악되었다는 것이 매우 심각한 문제점이라고 밝혔다.



〔그림 1〕 무기 시스템의 예

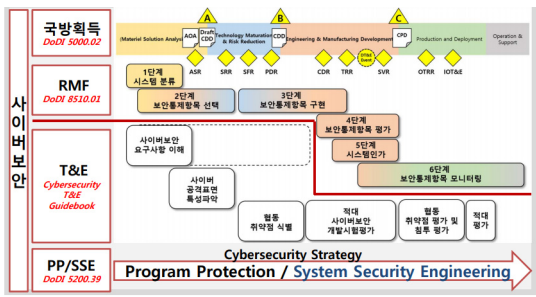
2.2. 미국의 사이버보안 정책

미국은 국방부 시스템과 네트워크는 사이버공격에 늘 노출되어 있으며 거의 모든 국방시스템이 어떤 형식이로든 정보기술(IT)을 포함하고 있기 때문에 사이버 적에 대한 회복력을 갖추고 있어야만 한다고 인식하고 이를 위해 무기체계와 플랫폼, 지휘·통제·통신·컴퓨터·정보·감시·정찰(C4ISR)시스템, 그리고 정보시스템과 네트워크 등 모든 분야에 사이버보안을 적용하고 있다. 또한 사이버보안은 국방부의 중요 우선순위로 미국이 기술우위를 유지하는데 필수적이라는 인식下에 일부 정책을 개정하여 획득사업에 사이버보안을 통합하는 것을 보다 강하게 강조함으로써 시스템 회복력을 보장하고자 했다[7].

이중 사이버보안 시험평가 절차를 살펴보면, 그림 2에서와 같이 '사이버 시험·평가 가이드북(2015)'에 명시하여 국방 획득체계 전 단계에 적용하고 있다. 평가 단계는 크게 '개발시험평가'와 '운용시험평가'로 나누어 실시하고 있다. 개발시험평가 단계에서는 설계·구현상 취약점 검증 및 제거, 침투 데스트 등이 이루어지고 있다. 운용시험평가 단계에서는 실제 환경에서의 취약점 확인 및 제거, 사이버 위협에 대한 대응태세 확인 등을 하고 있다.

시험 평가는 Operational Test & Evaluation, Office of the Secretary of Defense에서 담당하고 있으며 매년 발간되는 'Weapons Testing Cybersecurity Report'에 관련내용(시험평가 결과 등)을 수록하고 있다.

또한 개발단계에서의 오류를 최소화 하기 위하여 'Defense Acquisition University'내 무기체계 획득과정에서 사이버보안에 관한 과목을 교육중에 있다[9-10].



〔그림 2〕 미국 국방획득체계 사이버보안[8]

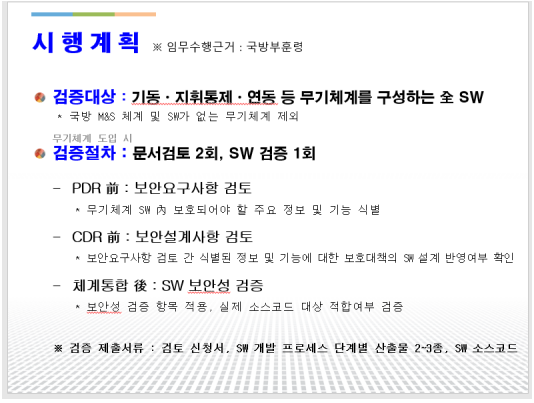
Ⅲ. 국방 무기체계 사이버보안 정책

이 장에서는 국방 무기체계 사이버 보안 정책과 문제점에 대해 알아보고자 한다

3.1. 현황

국방부에서는 2013년 신뢰성 시험을 실시하면서 보안성 검증 일부를 실시하기 전까지는 사실상 무기체계 분야는 보안의 대상이 아니었다. 하지만 2017년 6월 국군기무사령부에서 무기체계에 탑재된 'SW 보안성 검증' 필요성을 제기하여 국방부에서 국방전력발전업무훈령에 반영, 방사청에서 'SW 보안성 검증' 전면시행을 준비 중에 있다.

무기체계 SW 보안성 검증 시행계획[그림 3]을 살펴보면 '기동·지휘통제·연동 등 무기체계를 구성하는 全 SW를 대상으로 검증하는 것으로 되어 있다. 검증절차 또한 체계적으로 잘 정립되어 있다. 설계 검토 등 문서검증 2회, 구현 검토를 위한 소스코드 검증 1회를 실시한다는 계획이다. 사업관리부서와 긴밀한 협조를 통해 사업 진행에 영향요소를 최소화 시킬 수 있는 방향으로 시행될 예정이다.



〔그림 3〕 무기체계 SW 보안성 검증 소개자료(방사청)〔11〕

3.2. 문제점

'SW 보안성 검증 제도'의 시행은 무기체계 보안의 초기 단계로 아직 부족한 부분이 많지만 무기체계의 안정적 운영과 보안도 향상에 크게 기여할 것으로 판단되나 국방부와 방사청 등은 실제 시행을 하지 않고 있다. 훈령 개정후 최초 '18년도 전면 시행을 추진하려 하였으나 1년 이상이 지난 현재에도 아직도 답보상태에 있는 실정이다. 업무 주관부서인 방사청에서도 무기체계 개발업체의 부담과 보안성 검증업무로 인한 사업기간 연장을 지속적으로 우려하며 시행을 미루고 있다.

그럼 과연 지금 운용하고 있는 무기체계들은 사이버 위협에 안전한가. 그림 4의 언론 보도에서도 제기되었듯이 사실상 지금의 무기체계 사이버 보안은 심각한 상황임을 인식해야 한다. 초기 수준인 SW 보안성 검증 정책 시행마저도 이런저런 이유로 미룰 수 있는 상황이 아님을 강조하고 싶다.

〈〈 '18.6.19. 전자신문 〉〉

군이 사용하고 있는 무기체계 소프트웨어(SW) 보안이 위험수준인 것으로 드러났다. 무기체계 SW 소스코드와 주석문, 설정파일 내 관리자 계정정보가 그대로 노출됐다. 해커가 해당 SW를 리버싱하면 무기체계 계정을 탈취, 마음대로 조정한다. 일부 무기체계는 악성코드에 감염됐는데 오작동 가능성 때문에 치료도 못한 채 사용하고 있다. 국군기무사령부에서 시범 검증한 결과 무기체계에 들어간 SW가 기본 보안 요소도 지키지 않은 사례가 다수 발견, 충격을 안겼다.

◇ 소스코드내 암호키 방치
◇ 취약한 암호 알고리즘 사용
◇ 취약점이 공개된 오픈소스 구버전 사용
◇ 사용자 인증 절차 누락 등

〔그림 4〕 언론 보도 내용〔12〕

Ⅳ. 개선방향

이상으로 살펴본 바와 같이 무기체계의 사이버보안 대책이 시행되지 않는 상황에서는 사이버 공격으로 인해 무기체계가 무력화되어 대혼란이 야기될 뿐만 아니라 전장에서 승리 또한 보장받을 수 없을 것으로 예상하며 개선방안을 제시하고자 한다.

첫 번째, 현재 수립된 무기체계 SW 보안성 검증제도의 즉각 시행이다. 개발업체의 부담과 개발기간 연장을 우려하여 발전적 제도를 시행조차 하지 않는다는 것은 문제의 핵심을 제대로 접근하지 못한 잘못된 선택이라고 생각된다. 정책화된 제도 시행과 함께 관계기관(업)의 다양한 부담을 해소하기 위한 방안을 강구해

가는 것이 올바른 선택이다.

두 번째, 관계관들의 인식 전환이 절대 필요하다. 관계관들은 무기체계의 기능만을 강조하고 이를 구현하기 위한 노력만 추구할 것이 아니라 무기체계는 모든 면에서 완벽해야하는 한다는 것을 명심해야 한다. 무기체계가 필요로 하는 모든 기능을 구비하였다고 하더라도 보안 취약성을 내재한 단 하나의 시스템이 모든 기능을 무력화시킬 수 있다는 것을 명심해야 할 것이다. 예산, 개발기간 연장 등의 이유로 보안부분을 등한시할 문제가 아니다.

세 번째, 보안인력 증원 및 양성이다. 미 국방부가 정보통신기술(IT)이 접목된 모든 체계에 사이버 보안을 접목시켰듯이 우리도 모든 체계의 사이버 보안 강화를 위해서는 현재의 보안인력으로는 절대적으로 부족하다. 보안방첩 전문기관인 군사안보지원사령부의 '정보보호인증센터'의 인력 등 무기체계 사이버보안관련부서 보안전문가를 전략적으로 대폭 확대할 필요성이 있다. 보안 전문인력 없이는 그 어떤 대안도 강구할 수 없다. 하지만 증원만으로 모든 것을 해결할 수는 없다. 증원과 함께 현직에 있는 인원들에 대한 전문성 배양 또한 적극 추진하여야 한다. 지속적인 능력개발을 통해 새로운 위협에 능동적으로 대처할 수 있도록 미래 지향적 조직 운영을 해야 한다.

네 번째, 개발 인력들에 대한 교육체계 정립이다. 미 국방부에서도 시행하고 있는 무기체계 사이버보안 교육과정을 국방부 산하기관에 신설 운영하여 개발 관련 인원들이 교육과정을 반드시 이수토록 규정한다면 SW 개발자들의 오류를 최소화하고 개발 단계에서 보안 약점을 제거함으로써 운용단계에서 보안도 향상에 결정적 역할을 할 것이다.

Ⅴ. 결 론

지금까지 무기체계 사이버보안 정책 동향과 주요 문제점 및 개선방향에 대해 살펴보았다. 본 글이 무기체계 사이버보안의 답답한 현실 해결에 기여하기를 기대한다. 더불어. 무기체계 사이버보안 정책은 아직 초기 단계로 향후 더 많은 정책과 연구결과가 기대되는 바, 무기체계 사이버보안과 관련된 이해당사자들의 많은 논의가 있기를 바란다.

참 고 문 헌

[1] 최문정, 최준성, 정익래, "무기체계 내장형 소프트웨어 시큐어 코딩 프레임워크", 한국정보처리학회 2105년 춘계학술발표대회 논문집, 2015

[2] Junesung Choi, "Development of Evaluation Model for Secure Coding Rule Selection Optimized on the System Characteristics", Seoul National University of Science and Technology

[3] Junesung Choi, Wooje Kim, Wonhyung Park, Kwangho Kook, "Defense SW Secure Coding Application Method for Cyberwarfare Focused on the warfare System Embedded SW Application Level", Journal of Korea Association of Defense Industry Studies, 2012, Vol.19, No. 2, pp. 91-103

[4] NYT, https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html

[5] Aviationist, https://theaviationist.com/2016/10/02/iran-unveils-new-ucav-modeled-on-captured-u-s-rq-170-stealth-drone/

[6] GAO, https://www.gao.gov/assets/700/694913.pdf

[7] 美 RMF 가이드북, pp199

[8] 고려대, '사이버보안시험평가를 위한 국방획득체계 RMF 프로세스 적용방안' 발표자료, 2017

[9] DoDI 8500.01 "Cybersecurity"

[10] DoD Cybersecurity Test&Evaluation Guidebook V1.0

[11] 방위사업청, http://www.dapa.go.kr/dapa/na/ntt/selectNttInfo.do?bbsId=462&nttSn=7317&menuId=335

[12] 전자신문, http://www.etnews.com/20180619000155

〈저 자 소 개〉

이 정 규 (Lee Jeong Kyu)
정회원

1990년 2월 : 관동대학교 정보처리학과 졸업
2000년 8월 : 건국대학교 컴퓨터·정보통신학과 석사
2009년 8월 : 수원대학교 컴퓨터학과 박사수료
2016년 12월~2017년 11월 : 국방보안연구소 부소장
2018년 9월~현재 : 명지대학교 보안경영공학과 객원교수
관심분야 : 정보보호, 평가인증, 개인정보보호