https://doi.org/10.33778/kcsa.2019.19.3.101

안전한 공급망 관리를 위한 국방사이버보호 파트너십 인증 방안 연구★

김 종 화*, 김 용 철*, 김 경 민*, 강 정 홍*

요 약

우리 軍의 사이버 공간은 적들로부터 지속적인 위협을 받고 있다. 이러한 사이버 위협은 軍이 보유하고 있는 정보화 자산을 대상으로 한 것으로 조직의 정보화 자산에 대한 안전성 확보는 매우 중요하다. 그러나 정보화 자산은 軍 뿐만 아니라 어떠한 조직도 100% 자급자족할 수는 없기 때문에 공급망에 의한 정보화 자산 획득은 어쩔 수 없는 선택이다. 따라서 군 공급망에 대한 안전을 확보하기 위해 공급망 보호대책 검토 후, 이를 근거로 공급망 업체를 검증된 신뢰모델 기반의 파트너십 인증(引證)을 통해 군 공급망 안전을 확보하기 위한 방안을 제시하였다.

A Study on the Citation of Defense Cyber Protection Partnership for Safe Supply Chain Management

Jong-hwa Kim*, Yongchul Kim*, Kyoung Min Kim*, Jeongheung Kang*

ABSTRACT

Our military's cyberspace is under constant threat from the enemy. These cyber threats are targeted at the information service assets held by the military, and securing the security of the organization's information service assets is critical. However, since Information assets can not be 100% selt-sufficient in any organization as well as the military, acquisition of information assets by the supply chain is an inevitable. Therefor, after reviewing supply chain protection measures to secure the safety of the military supply chain, we proposed a method for securing supply chain companies through the citation of partnership based on the validated trust model.

Key words : Supply Chain, Information Security, Cyber Threat, Cyber Protection, Validated Trust

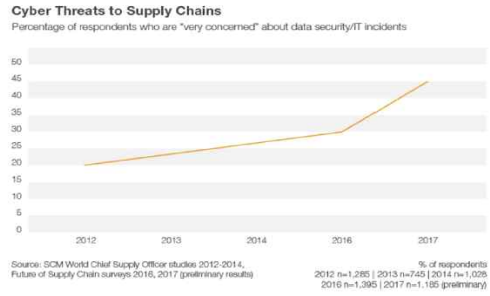
접수일(2019년 8월 27일), 게재확정일(2019년 9월 21일)

* 육군사관학교 사이버전 연구센터

★ 본 논문은 육군사관학교 사이버전 연구센터 연구활동비 지원에 의하여 연구되었음.

1. 서 론

최근 제품이나 서비스가 공급자로부터 소비자에게 전달되기까지의 조직, 사람, 정보, 자원 등에 대한 시스템인 공급망을 이용한 공격이 사이버 위협으로 떠오르고 있다. 주로 S/W 개발社의 네트워크에 침투하여 소스코드를 수정하여 악의적인 목적의 코드를 삽입한다거나 배포를 위한 서버로 접근하여 파일을 변경하는 방식으로 이루어지는 공급망 공격은 (그림 1)과 같이 급증하고 있는 추세로[1] 레노버, 화웨이, ZTE 등 중국업체에서 생산하는 전자제품에 설치된 불법 백도어 프로그램에 의한 사이버 공격 가능성에 대한 우려가 확산되면서 영국 정보기관들은 전산망 사이버 침해 가능성을 우려해 중국 레노버가 생산한 PC의 공무 활용을 전면 금지하기도 하였다[2][3].



(그림 1) 공급망에 대한 사이버 위협

특히, 미국은 외부 위협으로부터 미국 정보통신을 보호하는 행정명령인 '정보통신 기술 및 서비스 공급망 확보'를 통해 중국과 같이 적대관계에 있는 기업들이 미국 정부의 허가 없이 미국 내에서 제품을 판매할 수 없도록 제한하였고[4] 동맹국에게 중국 통신장비업체인 화웨이社 제품 사용 배제를 요구하며 배제하지 않을 경우 정보협력 축소를 경고하고 있다[5]. 또한 영국 브리티시텔레콤은 차세대 이동통신(5G)의 핵심장비 분야에서 화웨이社 제품을 제외한데 이어 프랑스 통신업체인 오렌지 SA도 화웨이社 제품을 사용하지 않겠다고 밝히는 등 유럽의 주요 국가들도 화웨이社 제품의 배제를 고려하고 있다[6].

공급망 위협은 우리 군도 공급망을 근간으로 정보화 자산을 획득하고 운영유지를 하고 있기 때문에 결코 간과해서는 안될 위협으로 체계적인 논의를 통해 공급망 위협에 대한 대응태세를 완비해야 한다.

따라서 본 논문은 군 공급망에 대한 안전을 확보하기 위해 공급망 보호대책 검토와 이를 근거로 공급망 파트너(업체)를 검증된 신뢰모델 기반의 파트너십 인증(引證)을 통해 군 공급망 안전을 확보하기 위한 방안을 제시하였다.

2. 관련 동향 및 개념 고찰

2.1 공급망 사고

2013년 OECD 리포트에 의하면 전 세계에서 만들어지는 제품의 50%이상이 반제품(중간 제조품)이고, 완제품으로 조립하기 위해서 글로벌 공급망을 이용하고 있으며 노트북 제조에 이용되는 공급망의 경우, 약 400여개 회사로 구성된다고 한다[7]. 이것은 우리가 사용하고 있는 노트북에 대한 광범위한 공격표면을 보여주는 것으로 이와 같이 공급망과 관련된 최근 사고는 <표 1>과 같으며 실제 공급망을 통한 사이버 위협의 심각성을 보여준다[1].

<표 1> 최근 공급망 사고 사례

공격사례	공격대상	
	국 가	대 상
Petya	우크라이나	정부 기관
넷사랑	전 세계	금융 추정
CCleaner	전 세계	전문기술회사
국내 ATM	한국	특정 ATM
해외 ATM	호주	특정 ATM

2.2 각 국의 동향

미국의 오바마 행정부는 9·11테러 이후 지속적으로 강화되어 온 공급망 안보정책의 대폭 확대 및 강화를 핵심으로 하는 '신 글로벌 공급망 안보 전략'의 추진계획을 공표하였다[8]. 또한 국립표준기술연구원은 공급망의 위험성을 인식하고 모든 수준에서의 정보통신기술(ICT) 공급망 위험을 판별, 평가 감소시킬 수 있는 지침인 연방정보시스템 및 조직을 위한 공급망 위험관리 실무 가이드[9]를 제공하였으며 2018년 10월

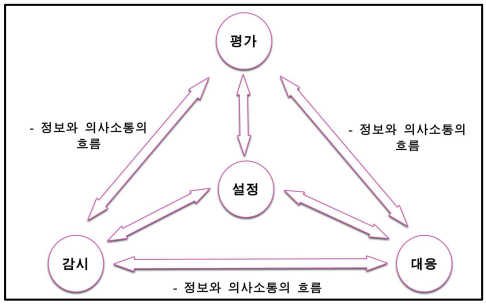
국토안보부와 민간부분 파트너가 공급망 위험을 해결하기 위한 장단기 전략을 개발하기 위해 정보통신 기술 공급망 TF의 구성 및 승인을 발표한 바 있다[10].

영국은 ICT 기술발전과 함께 증가하는 사이버 공간 내 범죄예방을 위해 2011년 11월 새로운 사이버안보 전략을 수립하였으며 사이버공격에 대한 복원력 강화와 사이버 상의 권익보호를 달성하기 일환으로 정부와 산업계가 국방사이버보호 파트너십을 체결하여 공조를 하고 있으며 2013년 하반기부터 전 공급망에 걸친 사이버 위협에 대한 인식 증가, 사이버 보안 표준을 적용한 위험 기반의 접근방법 정위, 그리고 위협 정보 공유 등 세 가지 특정 분야에 초점을 맞추고 있다[11].

또한 유럽은 '유로2020'이라는 이름 아래 미래 먹거리로 중요한 아이템을 발굴해 막대한 예산을 투입하고 있는데 그중 하나가 '서트 밀스(CERT MILS)'로 군에 들어가는 무기체계나 중요한 시스템에 대해 어떻게 하면 높은 수준으로 개발하고 평가할 것인지 연구하는 과제를 추진 중이다[12].

2.3 공급망 위험관리 개념

위험관리는 조직이 소유하고 있는 자산과 자산에 대한 위협과 취약점을 파악하여 위험을 평가하고 보안대책을 수립하는 일련의 과정으로 (그림 2)와 같이 수행되는 포괄적인 프로세스로 (i) 위험설정 (ii) 위험평가 (iii) 결정된 위험에 대응 (iv) 조직의 위험 관련 활동의 지속적인 개선을 위한 효과적인 조직 의사소통 및 피드백을 통해 지속적으로 위험을 감시하며 전략적 수준에서 전술적 수준까지의 위험을 다루는 전사적인 활동으로 수행되어 위험기반의 의사결정이 조직의 모든 측면에 통합되도록 보장한다[13].



(그림 2) 위험관리 프로세스

공급망 위험관리는 위험관리를 정보화 자산의 획득부터 운영유지 및 폐기에 이르는 생명주기와 관련되는 공급망 위협요소의 식별과 대응을 통해 신뢰성을 확보하기 위한 총제적인 관리활동이다.

2.4 신뢰모델 개념

신뢰모델은 공급망에서 협력관계를 형성하고 다른 조직과 공동 작업을 수행하고 정보를 공유하거나 정보시스템 / 보안 서비스를 받는데 필요한 신뢰 수준을 조직에서 얻을 수 있는 방법을 설명한다. 이러한 신뢰모델의 유형은 다른 조직의 활동에 관한 증거를 획득하고 그러한 증거를 사용하여 다른 조직과 신뢰수준을 설정하는 검증된 신뢰, 과거 조직이 보여준 실적, 특히 위험 및 정보보안 관련 활동과 의사결정을 통해 신뢰수준을 결정하는 직접적인 역사적 신뢰, 상호 신뢰할 수 있는 제 3자에 의해 제공되는 보증을 기반으로 신뢰수준을 결정하는 중재된 신뢰, 권한이 있는 제 3가가 발행한 특정 위임에 따라 다른 조직과 신뢰수준을 결정하는 위임된 신뢰, 여러 신뢰모델을 사용하는 하이브리드 신뢰가 있다[13].

2.5 인증(引證) 개념

본 연구에서 적용할 인증(引證)은 IT분야에서 일반적으로 사용하는 인증(認證)과는 다른 개념으로 사전적 의미는 다음과 같다.

- 인증(認證, Authentication) : 제 3자에 대해 어떠한 인적 물적 객체나 서비스 또는 문서나 행위가 정당한 절차로 이루어졌다는 것을 공적 기관에 증명하는 절차 및 제도를 말한다[14]. 인증은 신뢰모델 관점에서 보면 위임된 신뢰(Mandated Trust)에 해당된다.

- 인증(引證, Citation as Evidence) : 인용하여 증거로 삼음 또는 그 증거를 말한다[15]. 인증은 신뢰모델 관점에서 보면 검증된 신뢰(Validated Trust)에 해당된다.

인증(引證)은 기존의 인증(認證)과 다른 개념으로 정보시스템 수명주기에서 발생하는 보호대책 검토업무의 결과를 축적하여 축적된 결과를 통해 공급자들의 신뢰도로 산출하고 이를 증거로 전체 생명주기 내에서 공급자 선정 시 지표로 활용하는 개념이다.

3. 국방정보시스템의 보호 실태

3.1 국방정보시스템 보호업무

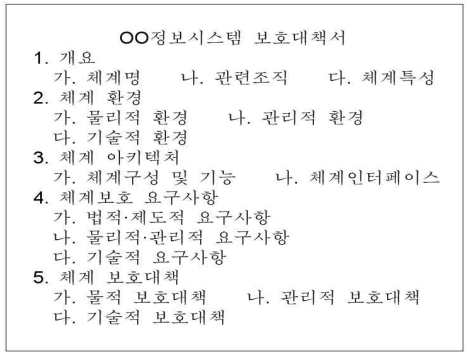
정보시스템 보호관리 및 사이버보안에 관한 업무는 국방전력발전업무 훈령과 국방정보화업무 훈령 상에 「국방사이버안보훈령」에 따르도록 되어 있으며, 보호 관련 업무는 <표 2>와 같이 안보지원사가 수행하도록 업무분장이 되어 있다[16][17].

<표 2> 안보지원사의 보호 관련 업무

구 분	주 요 내 용
국방정보시스템 보호	·국방정보시스템 보호대책을 최초 수립하거나, 개발·운영관리 중에 보호대책이 변경 시 보호대책 검토
무기체계 보호	·무기체계로 분류되는 국방정보시스템 및 내장형 SW에 대해 탐색개발/체계개발 단계에서 보호대책 검토 ·시험평가 등 전력화 이전 단계에서 보안측정 ·그밖에 무기체계 보안지원 활동
전력지원체계 보호	·전력지원체계로 분류되는 국방정보시스템 보호대책 최초 수립(재개발 포함)하거나, 개발·운영관리 중에 보호대책이 변경 시 보호대책 검토

3.2 국방정보시스템 보호대책

현재 각 군 및 기관의 국방정보시스템 보호대책은 개발 또는 성능개선 단계에서 국방정보시스템의 기밀성, 무결성, 가용성 측면에서 중요도와 위험을 판단하여 대상 시스템의 보호요구수준을 설정하고 있으며 설정된 보호요구수준을 충족하기 위해 해당 보호통제항목과 보호요구사항으로 이루어진 보호구조를 기준으로 해당 정보시스템에 대해 <그림 3>과 같이 국방정보시스템 보호대책서[18]를 작성하여 안보지원사로 검토를 의뢰하면 제시한 보호대책 적절성 및 충분성을 검토하여 해당 정보시스템의 보호대책 검토결과를 통보하며 미흡한 분야는 보완을 수행하고 있다.


OO정보시스템 보호대책서
1. 개요
가. 체계명 나. 관련조직 다. 체계특성
2. 체계 환경
가. 물리적 환경 나. 관리적 환경
다. 기술적 환경
3. 체계 아키텍처
가. 체계구성 및 기능 나. 체계인터페이스
4. 체계보호 요구사항
가. 법적·제도적 요구사항
나. 물리적·관리적 요구사항
다. 기술적 요구사항
5. 체계 보호대책
가. 물적 보호대책 나. 관리적 보호대책
다. 기술적 보호대책

(그림 3) 국방정보시스템 보호대책서 형식

운용단계에서 정보시스템을 보호하기 위해 수행하는 취약점 관리는 컴퓨터 정보자산의 기밀성 또는 가용성을 손상시키는데 사용될 수 있는 취약점을 파악하여 제거하는 과정으로 국방정보체계 취약점 분석·평가 실무지침서를 활용하여 정보시스템의 중요도에 따라 평가주기를 고려하여 취약점에 대한 분석·평가를 <표 3>과 같이 분야별로 수행한다.

<표 3> 취약점 분석·평가분야

구 분	분석·평가분야
국방	서버, 보호체계, 네트워크, DB, 단말기, 웹/응용체계, 기타 등
KISA	유닉스, 윈도우즈, 보안장비, 네트워크장비, 제어시스템, PC, 데이터베이스, 웹 등

그러나 현재의 보호대책은 기능구현 중점의 신뢰성 점검과 취약점 식별에 중점을 두고 보안성 검토를 하고 있는 실정으로 복잡하고 글로벌화 된 ICT 환경에서 공급망 위협에 대한 보호대책은 정보시스템 개발단계나 운용단계에서 명확하게 식별되지 않는다.

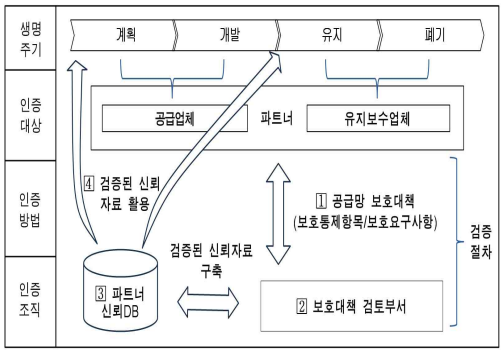
또한, 현재의 정보시스템 보호대책에 공급망 관련 보호대책을 추가하여 내·외부 위협요인으로부터 정보시스템의 보호가 이루어지기 위해서는 관련 조직의 전문인력 보강과 검토도구의 확충 등 공급망 보호대책 검토를 위한 역량강화가 요구되며 이를 통해 정보시스템의 위협요인을 조기에 식별하여 효과적인 위험관리가 가능할 것으로 판단된다.

4. 국방사이버보호 파트너십 인증방안

글로벌 공급망 하에서 군 공급망을 안전하게 관리하기 위해 정보시스템에 대한 공급망 보호대책을 검토하고 그 검토결과를 증거로 파트너(공급업체)의 신뢰수준을 결정 후, 활용하는 검증된 신뢰기반의 국방사이버보호 파트너십 인증(引證) 방안을 제안한다.

4.1 파트너십 인증을 위한 신뢰모델 선정

신뢰모델 선정은 파트너 인증을 위한 신뢰수준을 결정하기 위해 적용할 개념 선정에 관한 것으로 앞서 설명한 당사자 간에 일정 정도의 통제가 있거나 증거를 확보하고 검증할 시간적 여유가 있을 때 사용하는 검증된 신뢰모델을 현 보호대책 업무를 적용하는 것이 업무 프로세스 특성과 일관성 측면에서 적합하다.



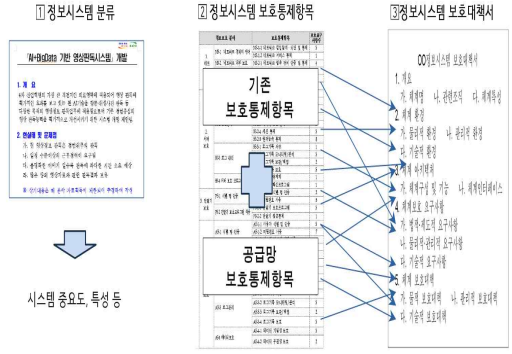
(그림 4) 검증된 신뢰모델 기반 파트너십 인증

또한 이 모델은 주로 정부와 외부업체간 사용하는 신뢰모델로 본 논문에서는 (그림 4)와 같이 파트너십 인증을 위한 기반으로 검증된 신뢰모델을 적용한다.

4.2 공급망 보호대책 개발 및 인증

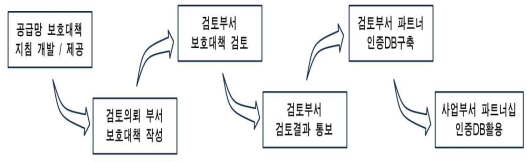
검증된 신뢰모델을 적용을 위해 필요한 증거 개발을 위해 정보시스템 정보보호 구조내 보호통제항목과 보호요구사항과 NIST가 제안하고 있는 공급망 위험관리 실무 가이드내 공급망 보호대책을 비교·분석하여 공급망 보호대책 검토를 위해 필요한 보호통제항목과 보호요구사항을 개발하여 보호대책으로 권고한다.

검토의뢰 부서는 (그림 5)와 같이 개발할 정보체계에 맞는 공급망 보호대책을 선택·작성하여 검토부서에 의뢰하면 검토부서는 보호대책 검토 후, 결과를 검토의뢰 부서와 파트너십 인증을 위한 DB에 저장한다.



(그림 5) 공급망 보호대책 적용

이렇게 구축된 인증DB는 향후 공급망 파트너 선정 시 신뢰도가 더 높은 파트너가 공급망에 유입될 수 있도록 활용함으로써 보다 안전한 군 공급망을 구축하고 유지하도록 기여한다. (그림 6)은 검증된 신뢰모델 기반의 파트너십 인증절차를 개략적으로 나타낸다.



(그림 6) 파트너십 인증 및 활용절차

4.3 공급망 보호 역량강화를 위한 전사적 노력

정보시스템 보호대책 검토범위에 공급망을 포함하여 검토하기 위해서는 현 조직의 역량강화가 절대적으로 필요하다. 여기에는 분야별 전문 인원과 검토도구의 확보 및 검토항목에 대한 세부 지침 개발과 함께 최근 논란이 되고 있는 각종 IoT기기나 컴퓨터 완제품 및 부품에 대한 안전성 확보를 위해 생산에서부터 유통 및 폐기에 이르는 전 과정에 블록체인 기반 이력관리 도입 등 기존의 개발단계 중심에서 유지보수 및 폐

기 단계까지의 전 생명주기에서 공급망 위협에 대비한 역량강화를 위해 전사적인 노력을 기울여야 한다.

4. 결 론

파트너십은 “협력”을 뜻한다. 글로벌화 된 ICT 환경 하에서 군 사이버 자산을 안전하게 보호하기 위해서는 군 단독의 노력으로는 한계가 있으며 군 공급망에 관련된 업체와의 협력을 통해 사이버 위협 대응태세를 구비할 때 비로소 사이버 공간의 안전을 더욱 견고히 할 수 있다.

이를 위해 본 논문은 군 공급망에 신뢰수준이 높은 파트너가 공급망에 참여 수 있도록 파트너십 인증(引證) 프로세스 구축을 통해 군 공급망의 안전을 향상시키는 방안을 제안하였다.

향후 연구할 분야는 정보시스템 개발 간 공급망 보호대책 선정과 구현을 위해 필요한 참조모델로서의 역할을 수행하는 공급망 보호통제항목과 보호요구사항을 개발하는 것으로 이를 통해 실질적인 공급망 보호대책 강구를 위한 기본 토대를 마련할 수 있다.

사회에서 긍정적 관계 형성의 전제조건은 신뢰로 사이버 위협 역시 신뢰에 반 하는가 그렇지 않은가에 대한 결과이다. 본 논문이 제시한 검증된 신뢰 기반의 파트너십 인증은 공급망 위협으로부터 군 사이버공간을 안전하게 지키는데 기여할 수 있을 것이다.

참고문헌

[1] 한국인터넷진흥원, “2018년 2분기 사이버 위협 동향보고서”, pp. 32-33. 2018.

[2] “레노버-화웨이-ZTE 中 백도어 논란”, KINE WS, 2015.02.25.

[3] “‘해킹의혹 중국산 PC, 영국 정보기관서 퇴출”, 연합뉴스, 2013.07.30.

[4] “미국, 中화웨이·70개 계열사 거래제한...안보침해 위협제기”, MK뉴스, 2019.05.16.

[5] “미국에게 화웨이 5G장비 배제 압박...정보공유 축소 경고”, KINEWS, 2019.04.30.

[6] “화웨이 유럽퇴출 움직임...BT 등 통신업계 제외 발표”, NewDaily, 2018.12.06.

[7] 김태호, 박태형, “SW공급망 사슬 위험관리”, 월간 SW중심사회, pp.41-44. 2015.

[8] 국립외교원, “미국의 신 글로벌 공급망 안보 전략 검토”, 주요국제문제분석, 제 2012-13호, pp. 1-13, 2012.

[9] NIST SP 800-161 Supply Risk Management Practices for Federal Inforamtion System, NIST, April 2015.

[10] www.dhs.gov/cisa, ICT SCRM TF. 2018.

[11] 배병환, “영국 사이버보안 전략 분석 및 시사점”, 주간기술동향, 제 1775호, pp. 1-14, 2014.

[12] “사이버무기도 해킹...평가체계·기술확보 시급”, 아이뉴스24, 2017.09.29.

[13] NIST SP 800-39 Managing Information Security Risk, NIST, March 2011.

[14] 위키백과, https://ko.wikipedia.org/wiki/인증

[15] 네이버 국어사전, https://ko.dict.naver.com

[16] 국방부, 국방전력업무발전훈령, 2019.

[17] 국방부, 국방정보화업무훈령, 2019.

[18] 마소팀, ‘마이크로소프트웨어 396호:리터러시 아드레날린’, IT조선, 2019.

[19] 방위사업청, ‘무기체계 소프트웨어 개발 및 관리 매뉴얼’, 2018.

[20] 국방부. “미래 사이버위협 양상 변화에 따른 국방 정보보호정책 발전방향”. 한국융합보안학회 제11회 사이버테러정보전 컨퍼런스 및 학술대회, pp. 49-63, 2010.

[21] 김종화, 임재성, “사이버 위협 대응을 위한 軍 정보화자산관리시스템과 연계한 軍 취약점 관리 방안”. 융합보안논문지, 제18권, 제1호, pp. 111-116, 2018

[22] 이대성, 안영규, 김민수, “북한의 사이버전 위협에 대한 분석과 전망”. 융합보안논문지, 제16권, 제5호, pp. 11-16, 2016.

〔저자소개〕

김 종 화 (Jong-hwa Kim)
2010년 아주대 NCW학과 박사수료
현 재 육군사관학교 사이버전 연구센터 연구실장
email : joakim_kma@mnd.go.kr

김 용 철 (Yongchul Kim)
1998년 육군사관학교 전자공학 학사
2001년 Surrey대 전자공학 석사
2012년 NCSU 박사
현 재 육군사관학교 전자공학과 교수, 사이버전연구센터 기획총괄
email : kyc6454@mnd.go.kr

김 경 민 (Kyoung Min Kim)
2003년 육군사관학교 운영분석 학사
2008년 Auburn대 전산학 석사
현 재 육군사관학교 컴퓨터과학과 조교수, 사이버전 연구센터 선임 연구원
email : kimpro@mnd.go.kr

강 정 흥 (Jeongheung Kang)
1987년 육군사관학교 수학과 학사
1995년 미 Illionis대 수학 석·박사
현 재 육군사관학교 수학과 교수, 사이버전 연구센터 센터장
email : jkang@mnd.go.kr