https://doi.org/10.33778/kcsa.2020.20.5.075

국방정보시스템에서의 랜섬웨어 위협 대응방안: 정보보안 위험관리 관점에서★

유 진 철*, 문 상 우**, 김 종 화***

요 약

지난해에 이어 랜섬웨어로 인한 피해가 계속 증가되고 있으나 군내 사이버작전 수행지침에 별도의 랜섬웨어 유형 분류없이 사이버 작전 상황을 관리하고 있는 실정이다. 그러나 랜섬웨어는 다른 악성코드와 달리 조치내용과 파급력을 고려할 때, 한 순간 모든 국방업무를 마비시킬 수 있는 위협요소로 군은 랜섬웨어를 재평가하고 이에 따른 대비책을 강구해야 한다. 이에 따라 본 논문에서는 정보보안 위험관리 기반의 국방정보화 관련 자산, 취약점, 위협 등을 분석하고, 랜섬웨어 위협으로부터 국방업무의 연속성을 확보하기 위한 대안을 제시하고자 한다.

Ransomware Threat Countermeasures for the Defense Information System: In terms of Information Security Risk Management

Jincheol Yoo*, Sangwoo Moon**, Jong-hwa Kim***

ABSTRACT

Damage caused by ransomware has continued to increase since last year, but cyber operations are managed without any separate classification of ransomware types in the military's guidelines for carrying out cyber operations. However, unlike other malware, ransomware is a threat that could paralyze all defense operations in one moment, and the military should reevaluate ransomware and take countermeasures. Accordingly, this paper aims to analyze the assets, vulnerabilities, and threats related to defense information service based on information security risk management, and propose alternatives to ensure continuity of defense work from ransomware threats.

Key words : ransomware, information security risk management, defense information system

접수일(2020년 11월 30일), 수정일(2020년 12월 13일), 게재확정일(2020년 12월 22일)

★ 본 논문은 2018년 육군사관학교 화랑대연구소와 2020년 육군사관학교 사이버전연구센터 지원에 의해 연구되었음.

* 육군사관학교 컴퓨터과학과(주저자)

** 육군사관학교 컴퓨터과학과 & 서울대학교 컴퓨터공학부

*** 육군사관학교 사이버전연구센터(교신저자)

1. 서 론

사이버 전문 업체의 조사에 따르면 사이버 범죄로 인한 경제 손실 추정액이 2021년에 약 6,426조원으로 예상되며, 이는 2015년과 비교해 2배에 해당되는 금액이다. 또한, 주요 국가 정부 웹사이트들과 주요 기업들의 내부망까지 전방위적인 해킹 공격이 이루어질 것이라 판단했다[1]. 특히 최근들어 랜섬웨어 침해 현황은 <표 1>에서 보듯이 해를 거듭할수록 점점 늘어나고 있는 추세이다[2].

<표 1> 신고기준 연도별 국내 랜섬웨어 침해 현황

구 분	2015년	2016년	2017년	2018년
신고건수 (건)	2,678	3,255	4,475	4,283
피해자수 (천 명)	53	130	260	285
피해금액 (억 원)	1,090	3,000	7,000	15,000

군에서도 2016년 내부 단독망으로 운영되던 국방망에서 침해사고가 발생하였으며, 이러한 우려는 이전부터 제기되었었다[3]. 이제는 더 이상 폐쇄망이라는 특수성으로 안심할 수 없다는 것을 뜻한다. 또한, 군내 사이버작전과 관련된 수행지침에도 랜섬웨어에 대한 별도의 유형 분류없이 사이버 작전 상황을 관리하고 있는 실정이다[4]. 그러나 랜섬웨어의 파급력과 조치내용을 고려할 때, 랜섬웨어가 군 내부에 침입한다면 매우 심각한 위험을 초래하고 이는 언제든지 모든 내부망에 침입이 가능하다는 것이다. 따라서 군에서도 랜섬웨어 위협에 대해 심각하게 고민하고 재평가해서 심도 깊은 대응방안을 마련해야 한다.

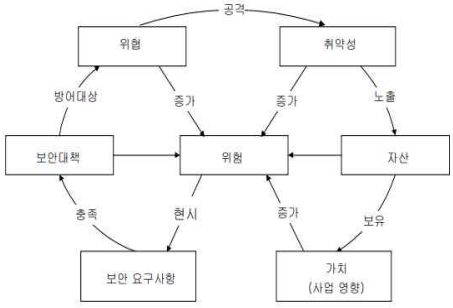
이에 따라 본 논문에서는 랜섬웨어가 일반적으로 컴퓨터 기능을 정상화하는 대가로 금전을 요구하는 악성코드라는 기존의 고정관념에서 벗어나 국방업무를 마비시키는 사이버 무기라는 인식 하에 정보보안 위험관리 관점에서 국방정보화 관련 자산, 취약점, 위협 등을 분석하고 특히, 랜섬웨어 위협으로부터 국방업무의 연속성을 확보하기 위한 대안을 제시한다.

2. 정보보안 위험관리 기반 실태 분석

정보보안 위험관리(Information Security Risk Management, ISRM)란 조직의 정보화 자산에 대한 위험을 감수할 수 있는 수준으로 유지하기 위하여 자산에 대한 위험을 분석하고 이러한 위험으로부터 자산을 보호하기 위한 비용 대비 효과적인 보호대책을 수립하는 일련의 과정을 의미한다[5].

위험(risk)은 외부 위협이 내부 취약점을 이용하여 보유한 각종 자산에 위해를 입힐 수 있는 잠재적인 가능성으로 자산(assets), 취약점(vulnerability), 위협(threat)으로 구성되며 구성요소 간의 관계는 (그림 1)과 같다[6].

- 자산 : 조직이 보호해야 할 대상으로 정보, 하드웨어, 소프트웨어, 시설, 인력 등
- 취약점 : 위협에 의한 정보체계의 모든 보안 상의 허점으로 사용자에게 허용된 권한 이상의 동작이나 범위 이상의 정보 열람을 가능하게 하는 약점과 사용자 및 관리자의 부주의나 사회공학(social engineering) 기법에 의한 약점 등
- 위협 : 자산에 손실을 초래할 수 있는 원치 않는 사건의 잠재적 원인이나 행위자 등



(그림 1) 위험분석 요소간의 관계

국방정보화 분야의 위험관리를 위해 앞에서 언급한 위험의 구성요소인 자산, 취약점, 위협에 대한 구체적인 문제점을 분석한다.

2.1 자산 분석

사이버 위협으로부터 보호해야할 군의 정보화 자산은 국방정보시스템(Defense Information System)으로 국방전력을 구축 및 운영하는데 필요한 요소로써 전장관리 정보체계(지휘통제, 전투지휘, 군사정보체계)와 자원관리 정보체계(기획·재정, 인사·동원, 군수·시

설, 전자행정, 군사정보지원, 상호운용성) 및 국방 M&S 체계(연습·훈련용, 분석용, 획득용)를 포함하는 응용 소프트웨어와 주장비, 통신망, 단말기, 주변장치, 시설, 사이버 방호체계, 상호 운용성 관리에 필요한 시스템, 그 밖의 시스템 소프트웨어를 포함하는 기반 운영환경을 포함한다[7].

특히, 기반환경인 통신망은 국방정보시스템의 응용 소프트웨어가 지원하는 업무 영역에 따라 외부망과 내부망으로 분리하여 업무 영역간 폐쇄성을 유지하고 있으며, 사용자의 업무 연속성을 보장하기 위해 분리된 망간 자료전송 환경인 망연계 시스템을 구축하여 운영하고 있다.

현재 국방정보화 자산에 대한 관리는 국방 정보자원 관리시스템(Defense IT Resource Information Management System)을 통해 국방정보화 사업 예산으로 획득 혹은 운영·유지하는 IT 자산과 책임 운영기관의 예산으로 운영·유지하는 IT 자산 및 자체개발 SW를 포함하여 관리하고 있다[8]. 국방 정보자원 관리시스템은 정보보안 위험관리 측면에서 보면 취약점을 가진 자산을 식별하기에는 구축된 자산의 항목과 입력 내용이 충분하지 않을 수 있다.

이러한 이유에서 위험관리를 지원하기 위한 시스템인 취약점 관리시스템에서는 국방 정보자원 관리시스템의 자산DB를 사용하지 않고 별도의 자산DB를 구축하여 취약점 업무를 수행하고 있다. 자산관리 관점에서 보면 중복된 자산관리는 자산의 불일치가 발생할 수 있고 이들 자산관리를 위한 자원이 중복되어 투입되고 있어 이에 대한 개선이 요구된다.

2.2 취약점 분석

군 내부망인 국방정보화시스템에 대한 취약점은 패치되지 않은 운영체제, 또는 오래된 소프트웨어 버전을 실행하는 프로그램과 애플리케이션, 서버와 네트워크 장비의 펌웨어, 네트워크에 연결된 불법 애플리케이션 등 최신화 관리를 하지 않는 모든 요소들이 취약점이 될 수 있다.

이러한 취약점을 제거하기 위해 군은 시스템 개발 시 SW개발 보안을 적용하거나 각종 보안인증을 획득한 제품을 도입하고 있으며 시스템 운영간 발생한 신규 취약점이나 개발 간 식별하지 못한 취약점은 유지보수를 통해 조치하고 있다. 현재 군이 시행하고 있는 취약점 관리는 계획된 취약점 관리와 긴급 취약점 관리로 구분하여 시행하고 있으며 다음과 같다.

계획된 취약점 관리는 국방정보체계 취약점 분석 및 평가 실무지침서를 기준으로 정보화 자산에 대해 매년 웹 / 응용체계의 해당 항목에 대해 취약점 점검 계획을 수립 후 일정 계획에 의거 해당 시스템의 취약점을 점검하고 있다.

긴급 취약점관리는 운용중 식별된 취약점에 대한 즉각적인 조치나 CVE(Common Vulnerabilities and Exposures) DB를 포함하여 발표되는 다양한 취약점에 대해 해당 취약점을 지닌 자산을 군이 보유하고 있는 지 확인하고, 보유하고 있다면 해당 취약점에 대한 적절한 조치를 통해 취약점을 제거하고 있다. 이를 지원하기 위해 취약점 전파로부터 자산식별 및 최종 조치가 완료될 때 까지 취약점 조치에 관련된 모든 이력을 관리할 수 있도록 취약점 관리시스템을 운용하고 있다.

취약점 관리의 출발점은 전파된 취약점을 지닌 자산을 보유하고 있는 가에 대한 것으로 취약점 관리시스템의 자산DB에 누락된 자산이 있어서는 안된다. 앞서 설명한 것처럼 현재 취약점 관리시스템의 자산DB 구축은 국방 정보자원 관리시스템과 별개로 서버 정보는 사용자가 직접 입력을 통해 구축하고 단말 정보는 엔드-포인트 보안체계를 활용하여 네트워크에 존재하는 단말에 대한 정보를 자동으로 구축하고 있다.

현재 국방 정보자원 관리시스템의 자산DB 구축은 정보화 사업 간에 해당 자산정보를 입력하여야만 유지보수가 가능하게 되어 있어 자산이 누락 될 확률이 거의 없지만 취약점 관리시스템은 정보화 사업이 종료된 이후 추가적인 입력을 통해 DB를 구축하기 때문에 자산이 누락 될 여지가 충분하다. 만약 자산 누락으로 인한 취약점 조치가 안된 자산은 위협에 노출되기 때문에 자산 누락 방지를 위한 개선이 요구된다.

2.3 위협 분석

과거에는 공격자가 <표 2>와 같은 방식을 통해 불특정 사용자를 대상으로 랜섬웨어를 유포하였으나, 최근에는 신속한 서비스 재개를 위해 금전을 지불할 수 있는 기업으로 공격 목표가 바뀌고 있다.

<표 2> 랜섬웨어 유포방식

구 분	방 법	랜섬웨어		실행 주체
		설 치	실 행	
이동식 저장매체	USB를 컴퓨터 연결	오토런 기능		공격자
		파일복사	파일실행	사용자
이메일	첨부파일에 악성코드삽입	첨부파일		사용자
		다운로드	실행	
웹페이지	웹페이지를 공격자가 장악	웹페이지 접속 시, 설치 / 실행		사용자

일반적으로 랜섬웨어는 C&C 서버와의 통신을 통해 암호화를 하기 때문에 통신이 차단될 경우에는 암호화가 진행되지 않지만 SamSam과 같은 일부 랜섬웨어는 <표 3>과 같이 C&C 서버와의 통신을 하지 않아도 암호화가 가능하기 때문에 더 이상 폐쇄망도 랜섬웨어로부터 안전하지 않다[9].

<표 3> 통신망별 랜섬웨어 위협

구 분	랜섬웨어	통신	공격기술
외부망 (인터넷)	온라인 랜섬웨어	○	워터링-홀,이메일, 크리덴셜 스터핑 등
내부망 (국방망)	오프라인 랜섬웨어	×	Bad USB, 크랙된 SW와 외부망 공격기술

현재 전 세계적으로 2018년도에만 악성파일 생성건수가 약 35만개에 달하고 있어 매일 발생하는 신규 또는 변종 랜섬웨어에 대해 다각적인 대응방안이 모색되어야 하는 상황임에도 군의 대응방안은 기존 시그니처 중심의 백신이나 악성코드 탐지 체계의 정책 최신화를 통해 랜섬웨어를 차단하고 있는 실정이다.

특히 랜섬웨어에 감염이 된 경우에 복구를 위해 필요한 자료백업은 각종 정보시스템에 대한 DB백업 위주로 실시 중이며 개인별 임무수행에 필요한 업무용 PC에 저장된 자료는 백업을 전혀 하지 못하고 있다. 따라서 업무용 PC가 랜섬웨어에 감염될 경우 해당 자료는 사용할 수가 없게 되어 대부분의 업무가 지장을 받거나 심할 경우 업무마비까지 될 수 있는 상황까지 전개될 수 있어 이에 대한 근본적인 대책이 요구된다.

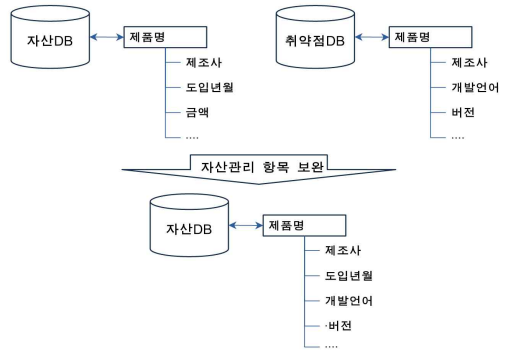
3. ISRM 관점의 랜섬웨어 대응 방안

3.1 자산관리 대응 방안

사이버 위협을 100% 예방할 수는 없다. 그러므로 사이버 침해 발생 시 신속하게 침해를 차단하고 복구하는데 소요되는 시간을 최소화하는 것이 관건이다. 이를 위해 보유한 자산에 대한 관리는 위협대상을 식별하고 조치하기 위한 출발점이어서 매우 중요하다.

기존 국방 정보자원 관리시스템에 자산관리 기능을 강화하기 위해 기능 개선을 하였듯이 취약점 관리를 위해서 국방 정보자원 관리시스템에 대한 기능 개선이 전제되어야 한다. 즉, 현재 운용중인 국방 정보자원 관리시스템을 (그림 2)와 같이 취약점 관리시스템과 비교하여 취약점DB와 관련되어 누락된 항목을 추가하거나 기존 항목의 세분화 등을 통해 취약점 관리시스템에서 활용할 수 있도록 국방 정보자원 관리시스템의 자산DB를 개선할 것을 제안한다.

다만, 국방 정보자원 관리시스템에서 항목 보완이 제한될 시 임의의 취약점 항목을 추가하여 해당 자산의 주요 키워드를 해시태그 형태로 관리하여 취약점 발생 시 취약점 조치를 위한 대상 자산현황을 보다 빠르고 정확하게 찾을 수 있을 것이다.

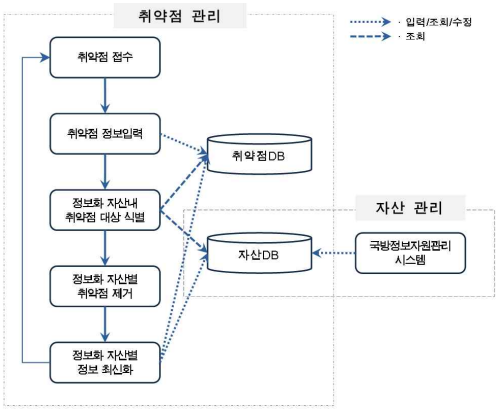


(그림 2) 자산DB의 취약점 관리 항목 보완

3.2 취약점 관리 대응 방안

사이버 위협에 대응하기 위해서는 각종 취약점 정보 출처에서 전파된 취약점을 최단 시간 내 제거할 수 있도록 해야 한다. 이를 위해 현재와 같이 취약점 관리시스템에서 자산DB를 독립적으로 구축할 필요없이 (그림 3)에서 보듯이 국방 정보자원 관리시스템의 자산DB를 취약점 DB와 연계하여 활용하도록 개선하여

야 한다[10]. 이를 통해 국방 정보자원 관리시스템의 신뢰성 있는 자산DB를 제공받아 취약점 관리시스템에서 사용함으로써 정확한 자산을 기초로 취약점 관리시스템의 본래 목적인 취약점을 지닌 자산의 신속한 식별과 조치에 전념할 수 있게 되어 취약점 관리 업무의 완전성과 신속성을 보장받을 수 있다.



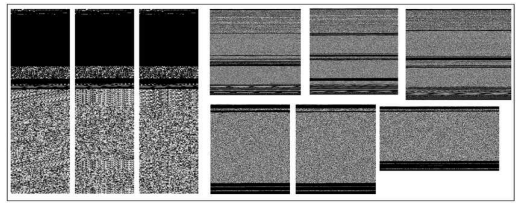
(그림 3) 자산관리와 연계된 취약점 관리

3.3 랜섬웨어 위협 관리 대응 방안

랜섬웨어의 위협에 대응하기 위해서 랜섬웨어를 식별하고 차단하기 위한 사전 대응방안으로 악성코드 식별을 위한 인공지능 기술 도입과 침해 시 자료를 신속하게 복구하기 위한 클라우드 컴퓨팅 환경을 구축하는 사후 대응방안을 통해 사이버 위협으로부터 보다 강건한 정보화 환경으로 개선시켜야 한다. 인공지능 기술 도입과 관련해서 (그림 4)와 같이 악성코드를 유형별로 이미지화하여 분석 및 비교하는 방법[11]을 랜섬웨어에 적용하여 분류시킨 후 머신러닝 기법을 통해 학습을 시킴으로써 신종 또는 변종의 랜섬웨어를 차단할 수 있다.

이러한 이미지 분석결과를 축적하고 유형 분류를 통해 공격자를 특정할 수 있게 됨으로서 해당 공격자의 TTPs(Tactics, Techniques, Procedures)에 대해 선제적으로 대응을 할 수 있어 주도적인 입장에서 방어작전을 수행할 수 있다.

그러나 현재의 인공지능 솔루션은 랜섬웨어 여부만을 제시할 뿐 방어작전을 뒷받침하기 위해 필요한 추가적인 설명 제시가 제한된다. 이를 해결하기 위해 사



(그림 4) 악성코드 유형별 이미지 분석

용자에게 인공지능 시스템의 동작과 최종 결과를 이해시키고 올바르게 해석하여 결과물이 생성되는 과정을 설명 가능하도록 해주는 기술이 포함된 설명 가능한 인공지능인 XAI(eXplainable Artificial Intelligence)[12] 도입을 통해 작전수행 간 이루어지는 지휘결심을 위한 정보분석 결과나 참모판단 근거로 설명 가능한 인공지능의 분석결과를 제공함으로써 방어작전 수행과정에서 지휘결심간 합리적 근거로 활용할 수 있다.

따라서 이러한 충분한 분석 및 검증절차를 거쳐 식별된 신종 및 변종 랜섬웨어를 최단시간 내 차단하여 공격자에게 새로운 랜섬웨어를 제작하도록 하여 자원 소모를 강요하고 우리의 자원은 다른 작전으로 전환 또는 절약할 수 있는 작전적 우위의 달성이 가능하다.

그동안 국방분야에서 네트워크의 이동성 향상과 보안관리 강화를 위한 클라우드 컴퓨팅 환경의 도입이 꾸준히 제기되어 왔다[13]. 랜섬웨어의 사후 대응방안으로 클라우드 컴퓨팅 환경을 도입하여 클라우드에 저장되는 모든 자료들의 콜드 백업(cold backup)을 통해 유사시 자료를 복구할 수 있도록 준비하는 방안을 제안한다. 또한 이는 국방 정보화자원의 효율적인 사용을 위한 IT 인프라 관리 뿐만 아니라 최신 클라우드 보안을 적용하여 H/W 및 S/W에 대한 통합된 보안관리로 강화된 보안체계를 구축할 수 있다. 따라서 군 업무에서 생성되는 모든 자료에 대해 랜섬웨어가 감염되었을 경우를 대비하여 백업체계의 역할과 강화된 보안체계 적용 및 효율적으로 정보화 자원을 관리할 수 있도록 클라우드 컴퓨팅 환경을 조기에 구축하여야 한다.

4. 결 론

군의 보안정책(사이버위협 대응 매뉴얼)에는 악성

코드나 바이러스 확산시 대응 방법이 체계화 되어 있으나, 랜섬웨어에 특화된 대응 방법은 아직까지는 정립되어 있지 않다[14]. 또한, 군 통신망은 외부망과 내부망으로 분리한 폐쇄망 환경으로 구축되어 있고 대부분의 국방업무를 내부망인 국방정보시스템에서 처리하고 있기 때문에 폐쇄망인 내부망을 외부에서 침해하지 못할 거라는 안심에서 랜섬웨어에 대한 실질적인 대응 방안을 강구하지 않았을 수 있다.

본 연구에서는 랜섬웨어에 대한 해결 방안으로 명확한 자산관리의 선행과 이와 연계된 취약점 관리, 그리고 의사결정을 위해 설명 가능한 인공지능 기술을 적용한 안티-랜섬웨어 솔루션 운영, 만일의 사태를 위한 자료백업과 자원 및 업무 효율화를 위한 클라우드 컴퓨팅 환경이 구축하여야 한다고 제안하였다.

랜섬웨어에 대한 실질적인 대응을 위해서는 단편적인 기술적 대응이 아닌 국방 정보화 환경에 대한 근본적인 변혁을 통해 대응하여야 하며 이를 위해 국방정보화 정책의 시행이 선도적으로 이루어져야 한다. 향후 군에 클라우드를 도입하기 위한 최적의 설계와 클라우드 보안에 대한 심층적인 연구를 통해 사이버 위협에 대비함과 동시에 효율적인 정보자원의 관리와 업무의 효율성을 달성할 수 있도록 하여야 한다.

참고문헌

[1] 위클리 비즈(http://weeklybiz.chosun.com/site/data/html_dir/2018 /03/09/2018030901739.html)

[2] 한국랜섬웨어침해대응센터(https://www.rancert.com/bbs/bbs.php?bbs_id=news&mode=view&id=539)

[3] 최광복, “국가사이버위협에 따른 국방사이버대응 실태”, 정보보호학회지, 제22권, 제8호, pp. 36-40, 2012.

[4] 육군본부, “육군 사이버방호 규정”, 2019.

[5] NIST, ‘Managing Information Security Risk(SP 800-39)’, U.S. Department of Commence, 2011.

[6] 황경태, ‘정보보호 위험관리 가이드’, 한국인터넷진흥원, 2004.

[7] 국방부, ‘국방전력발전업무훈령’, 2020. 5.

[8] 국방부, ‘국방정보화업무 훈령’, 2020. 6.

[9] Check Point Blog(https://blog.checkpoint.com/2016/03/28/check-point-threat-alert-samsam-and-maktub-ransomware-evolution/

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

[11] Mark Stamp, Fabio Di Troia, Wei-Chung Huang. “Robust Hashing for Image-based Malware Classification.”, International Workshop on Behavioral Analysis for System Security. 2018.

[12] 정승준, 변준영, 김창익, “설명 가능한 인공지능 기술의 소개”, 전자공학회지, 제46권, 제2호, pp. 55-63, 2019. 2.

[13] 장월수, 최중영, 임종인, “국방 클라우드 컴퓨팅 도입에 관한 보안체계 연구”, 정보보호학회논문지, 제22권, 제3호, pp. 645-654, 2012.

[14] 유진철, 문상우, “최신 랜섬웨어 해킹사례 분석을 통한 군사보안 대응 방안”, 화랑대연구소, 2018.

〔저자소개〕

유 진 철 (Jincheol Yoo)
1989년 3월 육군사관학교 학사
1993년 8월 미국 아이오와 주립대학교 (Iowa State Univ.) 석사
2003년 5월 미국 펜실베니아 주립대학교 (Pennsylvania State Univ.) 박사
email : jyoo@kma.ac.kr

문 상 우 (Sangwoo Moon)
2012년 3월 육군사관학교 학사
2017년 6월 미국 텍사스 주립대학교 (Univ. of Texas at Dallas) 석사
2020년 현재 서울대학교 박사과정
email : sangwoo.moon@vision.snu.ac.kr

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