https://doi.org/10.33778/kcsa.2020.20.4.047

4차 산업혁명에 따른 군사보안 발전방안 연구

김 두 환*, 박 호 정**

요 약

군은 4차 산업혁명을 통해 도약적 변혁을 추진해야 하지만, 군사보안측면 4차 산업혁명의 부작용과 역기능에 대한 준비도 필요하다. 이에 본 연구는 4차 산업혁명 선진국들의 '군사보안' 관련 연구의 방향과 국내연구와의 차이점과 보완요소가 없는지를 분석해 보았다. 이를 위해 빅데이터 텍스트마이닝과 의미연결망분석을 활용해 국내연구와 국외연구간의 차이점들을 추출해내었으며, 다음과 같은 7가지 과제를 도출해 내었다. 첫째, 민·관·군 및 산·학·연과의 융합연계 체계 강화, 둘째, 사이버보안 국제협력·공조 정보공유방안, 셋째, 군사혁신과 軍 비대칭 사이버보안 혁신, 넷째, 4차 산업혁명에 따른 군사보안 융합연동접점 관리체계 구축, 다섯째, 기술공학에서 사회공학으로의 접근방식 전환, 여섯째, 군내 군사보안 거버넌스 체계 확립, 일곱째, 군사 디지털자료의 비밀등급 구체화 등이다. 이러한 대응방안에 대한 추가연구를 통해 4차 산업혁명 신기술 혁신의 시대에 군의 혁신과 함께 취약한 군사보안 측면에서의 보완적인 연구도 병행해서 이루어질 수 있기를 기대해 본다.

A Study on the Efficient Countermeasures of Military in Accordance with Changing Security Environments

Kim Doo Hwan*, Park Ho Jeong**

ABSTRACT

The Army, which is dreaming of a military leap forward through the fourth industrial revolution, needs to also consider the side effects and adverse functions of the fourth industrial revolution. In particular, this study conducted an analysis of whether it was consistent with the global technological trend of normal 'military security'. This paper focuses on the countermeasures that could result from 4th industrial revolution by utilizing the text-mining technique and social network technique of big data. 1. Active promotion of a convergence program with private, public, militaryand industrial, academic, and solidarity, 2. Information Sharing for International Cooperation and Cooperation in Cyber security, 3. Military Innovation and Military Unsymmetric Cyber security innovation, 4.The Establishment of Military Security Convergence Interface Management System in accordance with the Fourth Industrial Revolution, 5. Cooperation in the transition from technology engineering to social technology, 6. Establishing a military security governance system in the military, 7. Specifying confidential military digital data We look forward to providing useful information so that the results of this study can help develop the military and enhance military confidentiality.

key words: military, security, Big-data, Text mining, 4th Industrial Innovation, semantic network analysis

접수일(2020년 8월 28일), 게재확정일(2020년 10월 14일)

* 육군본부 정보작전참모부 4급 김두환

** 건양대학교 국방경찰행정학부 교수(교신저자)

1. 서 론

보안이란 '국가와 조직, 더 나아가 개인에 이르기까지 그 존립을 보장할 수 있고 적으로부터의 경쟁 및 전쟁에서 승리하기 위해 반드시 필요한 핵심요소들을 찾아서 보호하는 것[1]'을 말한다. 이러한 보안은 단순히 개인에게만 국한되는 이슈가 아닌, 국가나 기업, 군(조직)까지 직·간접적으로 모두 연계될 수 있으며, 자기방어로서의 보안 활동과 전체가 통합된 보안 활동이 어우러질 수 있는 보안정책이 중요하다.[2] 그런데, 이렇듯 중요한 보안과 관련하여 보안을 위협하는 주변 환경은 점점 더 열악해 지고 있다. 기술의 진보와 IT정보통신기술의 급격한 발전은 과거와는 다른 보안환경으로 심각한 위험성과 함께 우려와 더불어 경각심을 지속적으로 요구하고 있다. 특히, 4차 산업혁명은 초연결성(Hyper-Connectivity), 초지능성(Hyper-Intelligene), 사물인터넷(IoT, Internet of Things) 등으로 표방되는 기술혁신의 혁명으로써, 사회·경제를 변혁시킬 만큼 그 변화의 파고가 이전 3차례 혁명의 그것과는 비교도 할 수 없을 정도로 크기 때문에 군내 군사보안에 미치는 영향역시도 심대하지 않을 수 없다. 심지어 능동적인 군사혁명을 달성한 전 세계 유일한 국가인 미국조차도 4차 산업혁명의 기술혁신 속에서 과거와는 전혀 다른 새로운 전장기능 구현을 목표로 한 '다영역 작전(Multi-Domain Operation)' 전쟁개념을 구체적으로 준비하고 있으며, 대한민국 육군역시 Army-TIGER 4.0을 통해 변혁의 '육군미래비전 2030'을 제시하며, 4차 산업혁명의 기술혁신을 적극적으로 군에 접목시켜 능동적으로 군의 변화와 혁신을 추진 중에 있다.

문제는 이러한 군사혁신과 기술혁신의 이면에 있을 수 있는 부작용과 역기능들이다. 미처 생각하지 못한 요소들이 심각한 도전적 요소들로 될 수 있는 것이다. 이것은 민간에서 심각하게 대두될 수 있는 '새로운 가치관의 문제, 데이터 소유권의 문제, 개인정보 침해 문제, 기계가 인간을 대체하고, 인간의 기능을 대신 수행했을 때의 윤리적 문제' 등과는 또 다른 軍에 있어서의 치명적인 문제들이다. 군을 위협하는 내·외의 부정적인 요소들은 바로 치명적인 보안 위해요소가 될 수 있으며, 이는 軍 혁신과 도약의 발목을 잡을 수도 있다.

따라서 본 연구는 4차 산업혁명 기술의 혁신으로 인해 미칠 수 있는 군내·외부적인 위험요소들에 대해 조사하고, 군내 4차 산업혁명시대의 군사보안에 대한 새로운 대응전략을 연구하고자 한다. 이를 위해 4차 산업혁명을 주도하는 빅데이터(Big data) 분석기술을 사용하여 군사보안에 영향을 미치는 변화된 환경 요소에 대해 분석한다. 다년간 연구된 각종 군사보안 관련 국내 및 해외 연구 자료를 참고로 텍스트 마이닝(Text mining) 기법을 통해 그동안의 군사보안과 관련한 연구 트랜드 및 패턴을 분석하고, 이러한 군사보안과 관련한 학술적 연구 추세들이 4차 산업혁명의 변화되어야 할 군사보안 트랜드를 어느 정도 반영하고 있는지에 대해 비교해 보고자 한다. 이 과정에서 해외의 학술논문과 국내의 학술논문 등을 상호 비교하면서, 전 세계적으로 4차 산업혁명의 보안 트랜드가 적절하게 국내연구 패턴에 어느 정도의 의미론적 연관성(Semantic association)을 보이는지에 대해서도 살펴볼 예정이다.

본 연구는 이를 통해, 전 세계적으로 진행 중인 4차 산업혁명과 그에 따른 군사보안의 추세와 트랜드들과 비교하여 부족했던 연구 분야와 추가 연구가 반드시 요구되는 보완요소들을 분석하고자 하는 것이다. 이러한 보완요소들은 곧, 4차 산업혁명과 그에 따른 기술혁신에 따라 촉발된 군사보안의 변화된 환경을 간접적으로 표방할 수 있는 것들이며, 이에 대한 대응방안을 모색하는 것이야 말로 변화된 보안환경에 대한 효율적인 대응방안이 될 수 있을 것이다.

2. 이론적 배경

2.1 군사보안에 대한 이해

'군사보안'은 "군조직의 안정적 유지와 전투력

보전을 위하여, 이를 의도하는 모든 분야의 적들을 감시하고 관측하며, 기술적으로 차단 및 방어하는 모든 활동"을 의미한다. 이러한 군사보안은 군이 곧 국가의 안녕과 국민의 생명 및 재산을 수호하는 최후의 보루로서의 가치를 가지고 있다는 측면에서 역사적으로 국가적 차원의 일로 인식되곤 하였다. 그런데, 군의 보안을 훼손하기 위해 공격하는 활동들은 수단과 방법을 가리지 않기 때문에 매우 위험하다. 다양한 루트와 여러 방향으로 침투를 고민하고 공격할 만한 취약한 지점을 찾아 용의주도하고 치밀하게 공격하기 위해 모든 수단을 동원하게 된다. 그래서 '군사보안'의 범위는 광범위하며, 그 방어수단 역시 스펙트럼이 넓을 수밖에 없다. 군사보안을 위협하는 형태는 특히 기술의 진보와 궤를 같이하여 수법이 보다 과학화되고, 치밀해지며 지키는 방어수단 역시 훨씬 난해하고 복잡한 방법이 되어 간다. 기술혁신과 IT의 진보로 상징되는 4차 산업혁명이 국방에 미치는 영향자체가 과거와는 현격히 다르기 때문일 것이다.

<표 1> 기술의 진보가 국방에 미치는 영향[3]

구 분	4차 산업혁명 이전	4차 산업혁명 이후
기 간	단기전	초단기전
C4I	· 개별, 분리 행동	· 각종 무기체계와의 결합된 공격, 상호운용성 기반 미래전 강조
사이버전	· 해킹위주 단편적 개별전	· 국가와 군에 대한 총체적인 인프라 공격 등 국방전산망 통합전
군사기술	· 군사과학기술과 민간기술 구분	· 구분 모호, 상호 융합기술 진보
작전개념	· 수평위주 3차원 개념	· 5차원 입체공간 개념으로 범위확대
정보공간 측면	· 3차 산업혁명에 따른 일정수준 사이버전	· 군 컴퓨터·서버네트워크화,군 정보통신시스템 규모 비례 광대한 정보공간의 출현(사이버전 극대화)
미래전 정의	· 육·해·공 국한 지상파괴전 · 기초적 C4ISR	· 미래전 우주·사이버 포함 5차원 공간 동시전장화, 통합작전전개
전쟁 특징	· 개별작전,개별 통신 네트워크	· 합동성 구현을 정보통신(IT) 필수.
		· IoT기반 네트워크 중심의 무기체계로 정보보호 대상 및 범위 확대
		· 모바일, 클라우드 컴퓨팅(Cloud Computing), 빅데이터(Big Data)+AI(인공지능) 등 신기술 활용 확대에 따른 새로운 사이버위협

현대에 있어서는 군사보안에 대한 개념이 앞서의 전통적 분야 외에도 사이버 보안·융합보안 및 드론 보안 등과 같이 새로운 형태로 군을 위협하는 요소와 분야가 확대되어 가고 있다. 본 연구에서는 기술혁신에 따라 새롭게 부각되어 군을 위협하는 제4차 산업혁명시대에 직면하는 변화된 보안개념 위주로 연구하였다.

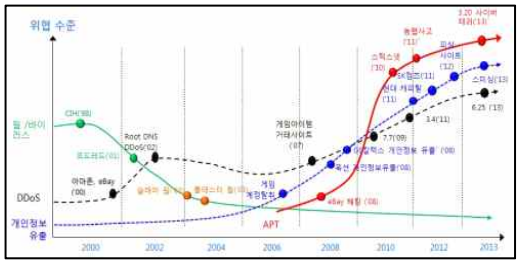
2.2 4차 산업혁명과 연계된 최근 군사보안 환경

4차 산업혁명 시대에는 IoT(Internet of Things) 기기들을 통해 온 세상과 연결이 가능하다. 인공지능이 스스로 사고·분석하여 인간의 의사결정에 유용한 정보를 제공해주는 등 사회 전반이 지능적이고도 스마트하게 변화하게 된다. 그러나 이러한 변화가 우리에게 꼭 편의성만을 제공하는 것만은 아니다. 최근 다양한 IoT기기들을 이용하여 대규모 DDoS(Distribute Denial of Service) 공격이 발생하였고, 이런 DDoS공격의 피해액은 무려 1조원에 육박하고 있는 수준이다.[4] 이에 대해 군은 상대적으로 일반사회의 기업이나 조직보다 철저하게 사이버방호체계와 인프라 보안체계가 훌륭하게 구축되어 있는 것은 사실이나, 전혀 예상하지 못하는 경로를 따라, 어떤 연동접점을 따라 군내부 통신망이 해킹되고, 멀웨어(Malware)가 침투하고, 바이러스에 감염될 수 있다. 특히, 우리가 처한 특수한 안보환경 상 우리는 100% 완벽한 통신보안조치를 했다 해도, 이를 능가하는 기술적 능력을 가지고 있는 북한 해커들이 있을 수 있다. 이외에도 국정감사에서 논의되었던 군사보안 사고사례들도 유념해 볼 필요가 있다. 2016년 국방위원회 국감 질의 시 군사기밀 유출에 군 장교가 개입된 사례가 해마다 증가한다는 것이 언론에 의해 밝혀진 바 있다. 유출된 기밀은 국방부가 F+2년부터 F+7년까지의 중기 5개년 예산편성을 계획한 문건인 국방 5개년 중기계획을 포함, 군 무기체계의 요구성능(ROC, 작전 요구성능), 북한의 잠수함발사 탄도미사일(SLBM) 시험 발사 등의 비밀이었다.

우리는 항상 군내 군사보안의 환경이 과거 그 어느 때보다도 열악한 환경과 더불어 복합적인 환경변화 속에 놓여 있다는 위기인식이 필요하다. 이전과는 다른 '복합문제 해결능력(complex problem solving skills)과 고도의 인지능력'이

요구되는 현실에 직면해 있다.[5] 4차 산업혁명의 기술혁신에 따른 디지털 보안의 위협요소들이 물밀 듯이 밀려오는 시대이면서도, 과거의 전통적인 위협들까지도 융합하여 군사 보안 측면에서는 더욱 취약한 시기일 수 있다는 판단에서 그렇다. 우리는 군조직 내 보안이라는 측면에서 어쩌면 전통적인 보안 위협과 기술의 혁명으로 대비되는 새로운 보안 위협들과 동시에 마주하고 있다고 보아야 할 것이다. 전자는 과거로부터 꾸준히 있었던 군내부 군조직원과 군사시설, 군사 문서 등과 같이 고전적인 유형의 보안 위협들이며, 후자는 전자보다 미래지향적이고 기술 혁신적인 '사이버', '해킹', '좀비(zombie) PC', '드론' 등과 같은 기술 진보적인 신개념 디지털 보안위협, 사이버 보안위협을 의미한다. 이러한 인식이 중요한 것은 과거와 달리 군이 민간과 단절되어 존립할 수 없는 기술과 IT 정보통신의 세계에 살고 있기 때문이다. 민간의 사이버 범죄와 사이버 공격들은 그대로 군에 비례하여 위협으로 인식될 수 밖에 없다.

<그림 1> 사이버 공격의 발생추이 및 특징[6]



*출처 : 한국인터넷 진흥원, '14년

<그림 1>과 같이 이미 민간에서 기술의 혁신과 함께 사이버 디지털 보안공격의 양상을 보면, 그 위험성이 얼마나 심각한 지를 여실히 보여주고 있다. 한국인터넷진흥원이 발표한 국내 사이버 공격의 발생추이에 대한 그래프는 우리나라가 사이버상에서의 얼마나 취약한 국가인지를 여실히 보여주고 있는 것이다. 상호 연계될 수 밖에 없는 것이지만, 사이버 범죄 역시도 <그림 2>와 같이 매년 약 14만건 정도가 지속적으로 발생하고 있으며, 그에 반해 검거율은 약 65~70%정도에 머물러 있다. 이는 우리 주변 생활 곳곳에 사이버범죄가 일상으로 만연되어 있다는 것을 의미하면서, 개인의 정보탈취, 그로인한 불법적인 악용 등에 무감각하게 노출되어 있음을 간접적으로 방증하는 것이기도 하다. 이러한 위협들이 전혀 군과 무관할 것인가?

<그림 2> 사이버 범죄의 연도별 추이[7]

*출처 : 사이버 경찰청(2016)

이 모든 것들은 얼마든지 군에서 발생할 수 있으며, 軍을 위협할 수 있다. 실지로도 군과 관련한 이러한 사이버 공격과 그것이 확대된 사이버 전쟁의 사례들은 얼마든지 확인할 수 있다.

<표 2> 주요 사이버전 사례[8]

구 분	내 용
걸프전 (1991)	미국,이라크 공격 과정에서 전자기파 폭탄(EMP) 사용
코소보전 (1999)	알바니아와 세르비아 간 내전 시 유고 해커가 NATO, 백악관, 미국방부 웹사이트에 침투, 미국 CIA 유고 밀로세비치 대통령 해외예금 계좌 해킹 시도
이라크전 (2003)	미국, 이라크 주요 지휘관 및 간부들을 대상으로 사이버 심리전 병행 실시
에스토니아 사태(2007)	러시아의 DDoS(분산서비스거부) 공격으로 정부,언론,방송,은행 전산망 등 2주간 마비
남오세티아전(2008)	러시아,그루지아 지휘부 작전·통신 시스템 해킹으로 전쟁 수행 능력 마비
이란핵시설 공격(2010)	미국과 이스라엘이 이란 핵시설에 스턱스넷 악성코드를 이용한 공격으로 원심분리기 1,000여개 파괴, 이란 핵 프로그램 지연
북·미 사이버공격 (2014)	북한, 소니픽처스 엔터테인먼트 사이트 공격 및 정보유출, 미국은 북한의 노동신문 등 주요 웹사이트를 마비시키는 보복 조치

*출처 : 국방일보(2016.3.15.)

이러한 위협이 무서운 것은 대한민국을 적화하기 위한 북한이 있기 때문이다. 북한은 세계 3위 수준의 사이버 전력(Cyber Power)[9]을 가지고 이를 수소폭탄이 포함된 핵과 다양한 탄도미사일, 유사시 한국을 순식간에 결정적 사회적 혼란을 야기시킬 강력한 10만 특수전 부대와 함께 3대 비대칭전력(Asymmetric Power)으로 인식하고 있다. 김정은은 이를 특별히 강조하며

[10], 꾸준히 사이버 핵심역량 강화를 진행하고 있다. 현재까지 확인된 것으로만 전체 7개 부대 약 7.000여 명으로 추산되는 될 정도의 역량을 갖추고 있다.[11]

무엇보다 2016년의 국방망 해킹사건[12]을 통해 군내 비밀자료 다수가 북으로 유출된 사례에서도 볼 수 있듯이 북한으로부터의 사이버 전쟁 위협은 더 이상 허상이 아닌 반드시 대비해야할 전쟁위기(Warfare Crisis[13])임이 모든 학자들의 공통된 위기의식이다. 군내 군사보안의 중요성과 그에 대한 철저한 대비는 군이 갖추어야 할 가장 핵심적인 방어조치라 할 수 있다.

2.3 빅데이터 분석(Big-data Analysis)

빅데이터(Big data)는 기존 데이터에 비해 그 양이 너무 방대하고 세밀하여 기존 과거의 수단으로는 그 데이터를 가공하거나 유의미한 데이터로 분석할 수 없는 데이터를 의미한다. 데이터를 수집하고 저장하며 검색하여 분석하고 유의미한 산출로서의 시각화 등이 어려운 정형(직업, 주소, 성별, 나이, 웹메일 등), 또는 비정형 데이터(이미지, 동영상, 음원, 음악, 텍스트, 클릭, 타이핑, 채팅 데이터 등)를 총칭하는 말이다. 또한, 빅데이터의 개념 안에 그것의 양(volume)과 분석활용, 그것의 활용적인 측면 모두가 포함된 개념이라고 할 수 있다.[14] 이러한 빅데이터(Big-Data)는 대용량의 데이터를 수집하고 축적·분석하여 활용이 가능한 부가가치 정보를 유출해내어, 미래를 예측하거나, 리스크를 경감시키는 등의 새로운 부가가치를 창출하는 신기술로서 4차 산업혁명을 대표하는 상징적인 용어이기도 하다. 일반적인 빅데이터의 특징은 <표 3>과 같다

<표 3> 빅데이터의 4가지 구성요소[15]

구 분	주 요 내 용
규모(Volume)	IT 일상화로 디지털 정보량 기하급수적 증가 → 빅데이터의 기준인 제타바이트(ZB) 시대 진입
다양성 (Variety)	SNS, GPS, 인터넷쇼핑, 현실데이터 등 증가, 텍스트 외 멀티미디어 데이터 등 비정형 데이터, 유형의 다양화
복잡성 (Complexity)	구조화되지 않은 데이터, 데이터 저장방식의 차이, 중복성 문제, 데이터 종류 확대 등 관리 대상 증가
속도(Velocity)	사물 정보, 스트리밍 정보 등 실시간성 정보 증가 실시간성으로 인한 데이터 생성, 이동(유통) 속도 증가 대규모 데이터 처리 목적 데이터 분석 속도 중요

이러한 빅데이터 분석을 통해 아직 무의미한 대량의 데이터를 분석하여 향후 부가가치가 있는 데이터를 획득하기 위해서는 항상 인프라기술이 필요하다. 통상적으로 하둡(Hadoop), NoSQL 기술(이질적 데이터 형식에 대한 처리·분석), 논리적 데이터 웨어하우스 기술 등과 같은 빅데이터 분석 인프라 기술이 요구되며, 그 이후 데이터의 종류에 따른 다양한 세부적인 분석기법들에 대한 적용이 필요하게 된다. 데이터의 종류에 대해서는 앞서도 언급한 바와 같이 정형, 비정형, 반정형 데이터로 구분되는데 이러한 데이터의 유형마다 적용해야 할 분석기술과 기법은 약간씩 차이가 있을 수 있다.

이러한 빅데이터 분석법에는 모두 다 데이터를 활용하여 그 의미없이 분산되어 있는 데이터들의 무더기속에서 미처 알지 못했던 규칙과 패턴 및 숨겨진 함의를 추출해 낸다는 점에서는 동일하다. 그래서 용어 자체도 마이닝(mining)인 것이며, 방대하게 쌓여 있는 일견 무가치해 보이는 데이터의 늪속에서 형이상학적인 북다가치를 창출해낸다는 점에서는 앞서 말했듯 지식의 또다른 발견으로서 그 가치가 높다 하겠다. 이러한 마이닝 기법에도 방식에 따라 다음과 같이 구분할 수 있다.

<표 4> 빅데이터 분석을 위한 마이닝 기법

구 분	내 용
데이터마이닝 (Data Mining)	대용량의 데이터, 데이터베이스 등에 감춰진 지식, 기대하지 못했던 경향, 새로운 규칙 등의 유용한 정보를 발견하는 과정
텍스트마이닝 (Text Mining)	자연어로 구성된 비정형 텍스트 데이터에서 패턴 또는 관계를 추출하여 가치와 의미있는 정보를 찾아내는 마이닝 기법
웹 마이닝 (Web Mining)	인터넷상에서 수집된 정보를 데이터 마이닝 방법으로 분석 통합하는 기법
소셜 마이닝 (Social Mining)	소셜 미디어에 올라오는 글과 사용자를 분석해 소비자의 흐름이나 패턴 등을 분석하고 판매나 홍보에 적용
현실 마이닝 (Reality Mining)	사람들의 행동패턴을 예측하기 위해 사회적 행동과 관련된 정보를 기기(휴대폰, GPS 등)를 통해 얻고 분석하는 방법

*출처 : 한국정보화진흥원(2012), 2쪽.

2.4 사회연결망 분석(Social network Analysis)

사회연결망 분석(Social Network Analysis, SNA)이란 객체(노드)가 포함된 연결망(network)의 상관관계 및 그 특징을 분석하여 그 연결망에 포함된 객체(node)나 행위자들의 사회적 행위나 관계성(Relationship)을 설명하고자 하는 분석법이다.[16] 즉, 사람들을 이해하고, 그들이 하는 사회적 행위를 그들 자신에 대한 이해 없이도 그들이 맺고 있는 관계 네트워크의 특성과 상관성을 통해 간접적으로 이해할 수 있다는 시도이다.[17] 사회연결망 분석(Social Network Analytics)은 소셜 네트워크(Social Network)상에서의 수많은 사람 간의 공유와 공감 포인트를 집어내어 영향 관계를 모니터링하고 분석하기 위한 분석 방법이다.

2.4.1 사회연결망 분석(SNA) 단계설명

다수의 사회연결망 분석 전문가들은 사회연결망 분석이 통상적으로 다음 4단계로 구분되어 진행된다고 설명하고 있다.[18]

첫째, '분석문제 설정' 단계는 연구문제 설정 및 분석하고자 하는 목표를 정한다.

둘째, '연결망 데이터 조사' 단계는 문제를 해결하기 위해 양질의 데이터를 수집하여 분석하게 된다.

셋째, '연결망 생성' 단계는 앞 단계에서 적합하게 수집된 데이터를 연결망 데이터로 변환하여 통계적인 기법분석을 통해 시각화와 도식화를 구현한다.

넷째, '연결망 분석' 단계는 시각화와 도식화된 연결망 데이터를 통해 최종적인 결과를 분석하고, 그렇게 획득된 분석 결과로부터 부가가치가 있는 유의미한 정보·패턴들을 추출하고 이를 해석한다.

이러한 절차를 통해 연결망 데이터간의 관계상황을 이해하고, 연결 정도나 유의미한 연결강도, 영향을 미치는 영향 관계를 추출함으로써 창의적인 관계맥락을 분석해 내는 것이 사회연결망 분석이라 할 수 있다.

2.4.2 사회연결망 분석(SNA) 시각화

사회연결망 분석에서의 사회연결망(Social Network)은 가시적인 시각화를 통해 더욱 효과적인 분석환경을 제공할 수 있다. 이는 복잡하게 이해할 수 없는 연결망을 노드(node)와 링크(links)로 표현하여 한눈에 확인할 수 있도록 하기 위함이다. 사회연결망 분석에는 수집된 데이터를 실질적으로 분석하기 위한 분석 도구와 그러한 분석 데이터를 보다 시각적으로 표현해 주는 시각화 도구가 있다. 사회연결망 분석에서의 시각화 도구는 주로 사회연결망 분석 도구의 시각화 모듈로 개발되거나 별도의 시각화 도구로 개발되어 왔으며[19], 이를 통해 직관적인 판단을 지원해준다. 대표적인 범용 사회연결망 분석 도구들은 UCINET6, Pajek, NodeXL, KRkwic, Netdraw 등을 포함하여 약 70여 개 이상의 프로그램이 있다.[20]

2.4.3 의미연결망 분석(Semantic Network Analysis)

어떤 사회현상을 분석하는데 있어 대상이 사람인 관계에서의 분석을 사회연결망 분석이라고 하면, 대상이 사람이 아니라 '단어나 구', 목표한 대상을 의미하는 '언어'와의 관계를 분석하는 것이 의미연결망분석이다. 큰 틀에서 의미연결망 분석은 보다 내용분석(content analysis)에 가깝지만, 그런데도 개념은 사실상 동일하다. 통상적으로 사람 간의 관계를 중시하는 사회연결망 분석대비 그들이 나누는 언어, 카톡 메시지, 표현하는 단어, 압축해서 발설한 짧은 문장(구)들이 바로 그 사람의 마음을 대변하고, 표현하는 커뮤니케이션 메시지라고 하는 수단을 통해 의미론적 연관성을 분석하는 것이 다를 뿐이다. 의미연결망 분석은 사회연결망 분석을 응용하여 보다 진화된 형태라고 할 수 있다. 따라서 세부적인 진행절차와 분석하는 기법, 상관관계를 도출해내는 방식은 크게 차이가 없다.

3. 빅데이터 텍스트마이닝 설계

3.1 빅데이터 텍스트마이닝 연구과제

본 연구의 목적은 빅데이터(Big data)의 분석기법인 텍스트마이닝(text mining)과 의미연결망

분석기법 등을 수단으로 하여 키워드 '군사보안'의 정형화된(structured) 이미지를 분석하고, 그 도출된 '군사보안'에 대한 이미지를 통해 4차 산업혁명의 시대에 필요한 '군사보안'의 발전 방향과 세부적인 대응 방안에 대한 시사점을 도출하고자 하는 것이며, 이 과정에서 김두환(2019)이 연구한 텍스트마이닝 기법과 의미연결망 방식을 준용하여 분석하였다.[21]

본 연구의 목적에 따라 다음과 같은 3가지 연구문제를 중심으로 연구를 진행하였다.

<표 5> 연구과제

연구과제 1. '군사보안'에 영향을 미치는 단어와 이미지 형성에 영향을 미치는 실제 요소는 무엇인가?
연구과제 2. '군사보안'을 표현하는 단어들과 연관되는 이미지 요소는 무엇인가?
연구과제 3. 군사보안'을 연구한 국외자료와 국내 '군사보안' 연구와의 차이를 통해 살펴본 세계적인 '군사보안'의 환경변화는 어떠한가?

상기 연구과제 분석을 위해 수집한 원천데이터는 <표 6>과 같이 국내논문과 해외논문을 포함하여 전체 4,078편을 통해 최종 정제한 2,261편을 대상으로 진행하였고, 시간 범위는 4차 산업혁명 시기 전후 단계를 고려하여, 2010년 1월 1일부터 2019년 6월 30일까지 약 10년으로 한정하였다.

<표 6> 연구대상 국내·외 논문 편수 현황

구분	단행본	국내 학술지	학위논문	합계	
				정제전	정제후
계	945	312	2,821	4,078	2,261
해외논문	-	-	2,457	2,457	1,896
국내논문	945	312	364	1,621	375

이를 유의미한 단어키워드와 주제유형별로 변환시킬 목적으로 빅데이터 분석 툴인 TEXTOM을 활용하여 데이터 자료로 변환하였다.

<그림 3> TEXTOM 데이터 변환자료

3.2 빅데이터 텍스트마이닝 연구절차

본 연구는 빅데이터의 텍스트마이닝과 의미연결망 분석(Semantic Network Analysis, SNA)을 통하여 '군사보안' 키워드를 분석하고 의미연결망 분석을 위해 다음과 같은 절차로 연구를 진행하였다.

첫 번째 단계는 수집하고자 하는 데이터의 대상과 수집 범위를 선정하는 단계이다. 수집대상은 국내 및 국외 학술 논문에서 군사보안을 주제로 기술한 자료를 수집하였다. 이 과정에서 빅데이터 분석 솔루션 프로그램 중 하나인 Textom[22]을 활용하였다.

두 번째 단계는 수집된 데이터를 정제하는 단계이다. 첫 번째 단계에서 수집된 데이터 중 연구목적에 불필요하다고 판단되는 부수적인 단어나 부호 등의 요소를 삭제하였다. 그리고 '군사보안'과 관련된 가치 있는 텍스트만을 선정하여 정제하였다.

세 번째 단계는 텍스트 마이닝 되어 정제된 데이터의 의미연결망 분석(semantic network analysis)이다. 매트릭스 데이터(matrix data)는 마지막까지 정제된 데이터를 변화하는 목적으로 사용되는데, 최종적으로 이를 연결망 분석기법용 프로그램인 Ucinet 6과 연계시킨다. 이를 통해 의미연결망을 분석하고 분석 결과를 시각화 및 도식화하기 위해 NetDraw 프로그램을 이용한다. 그 이후 다시 군집분석을 위해 Ucinet 6 프로그램을 이용하여 단어 간의 유의미한 유형 군집 분류를 실시하였다.

4. 빅데이터 텍스트마이닝 실증분석 결과

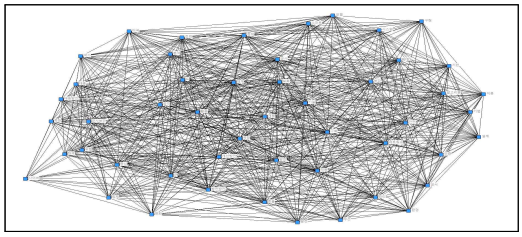
4.1 텍스트 마이닝 분석결과(연구과제 1)

분석결과, 군사보안을 표현한 학술적 빈도가 높은 단어는 '사이버'였다. 이는 군사보안의 영역 중에서 그 중요성이 한층 강조되고 있는 사이버공간에 관한 관심이 반영된 것으로 판단되었다. 상위 10위에 선정된 단어들은 사이버, 보

안, 방안, 군, 네트워크, 해킹, 기술, 시스템, 분석, 활용 등의 단어가 많이 나타났다. 빈도수를 고려하여 '군사보안'을 표현하면 '군은 사이버 보안을 중심으로 네트워크 기반의 시스템을 이용하여 분석하고 해킹에 기술적으로 대비하여 활용'하는 이미지로 군사보안이 표현되고 있음을 알 수 있다. 즉, 종래에 보안을 유지하면 지켜야하고 감추어야 하는 이미지에서 지금은 네트워크 기반의 시스템으로 활용하는 발전된 기술과 함께 변화하는 군사보안의 이미지를 확인할 수 있었다.

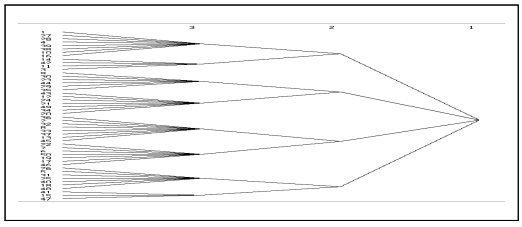
본 연구에서는 앞에서 수집한 단어들을 CONCOR(Convergence of Iterated Correlation) 분석을 실시하였는데, 이 분석을 통해 단어 간 상호 연계성이 높은 단어들끼리 구분되어 군집분석(Cluster Analysis)이 가능하다.

<그림 4> 군사보안 CONCOR 분석



위 [그림 4]은 '군사보안'을 주제로 유사한 단어끼리 군집을 구성한 네트워크인데 반해, 아래 [그림 5]은 이를 트리형 기법으로 군집분석한 결과이다.

<그림 5> 군사보안 트리형 분석



위와 같이 '군사보안'을 주제로 군집분석을 한 결과, 단어 유형별로 군집이 구성되었으며, 아래 <표 7>과 같다.

<표 7> 군사보안 관련 유형군집분석 결과

유형분류	연관된 세부단어
4차산업 연계 발전방향	중심, 드론, 개선방안, 군, 체계, 발전방안, 활용, 군사보안
보안구축	국방, 개발, 방안, 구축
보안전략방향	분석, 한국, 국가, 변화, 미국, 전략
사이버보안대응	공격, 사이버, 대응, 북한, 법제, 위협, 대응방안
IT기술과 정보보안	RFID, 보안, 보호, 시스템, 알고리즘, 안전, 설계, 스마트
보안기술	구현, 이용, 기반, 정책, 기술, 군사, 모델
정보통신보안	무선, 네트워크, 관리, 센서, 기법, 환경, 효율
보안인증	인증, 적용, 발전

이를 통해 군사보안과 관련한 국내학계에서의 연구이미지를 유추해 볼 수 있다. 군사보안이 학술적으로 어떤 이미지와 연계성을 가지고 연구되고 있는지에 대한 트렌드를 알 수 있는 것이다. 4차 산업혁명시대와 연계된 군사보안의 발전방안을 필두로, 보안인증에 이르기까지 4차 산업혁명에 따른 기술혁신과 IT기술이 군사보안에 미치는 영향연구에 집중하고 있다는 것을 알 수 있다. 다만, 연구의 방향과 트렌드가 기술혁신에 따른 군사보안의 기술공학적인 대응방안에 집중하고 있다는 점이 특기할만 하다. 최근의 사이버 해킹과 네트워크 정보보안 위협이 사회공학적인 부분에도 관심이 크게 대두되고 있는 것에 비해 상대적으로 기술적인 측면에 치우쳐져 있는 부분은 아쉬운 부분이다.

4.2 텍스트 마이닝 분석결과(연구과제 2)

연구수행을 목적으로 추출 데이터 대상 의미연결망 분석을 진행하였다. 동시출현 빈도분석 실시 데이터를 Textom 매트릭스(matrix) 변환 프로그램을 사용하였으며, 대칭형 매트릭스(matrix) 변환후 Ucinet 6 툴을 이용하여 분석가능한 데이터의 유형으로 변환시킴으로써 의미연결망 분석을 진행하여 다음 <표 8>과 같은 결과를 획득하였다.

<표 8> 의미연결망 분석 결과

키워드	의미론적 연관성을 갖는 단어
공격	군, 중심, 북한, 법제, 위협, 대응방안, 공격
방안	군사보안, 개선방안, 발전방안

적용	국방, 발전, 구축, 인증
구현	보안, 이용, 기술, 기반, 스마트, 모델, 시스템, 설계
센서	네트워크, 환경, 무선, 관리, 기법, 효율

이에 따르면, 군사보안과 관련한 가장 관련한 의미연결망 분석하에서의 가장 강한 연결성은 사이버 공격(북한)에 대한 대응방안을 마련하고 이와 관련한 군 중심의 법제화에 방점이 찍혀 있음을 알 수 있었다. 또한, 군사보안의 향후 발전 및 개선 방향과 국방인증 체계 구축, 기술혁신과 연계된 군사보안의 기술적 발전 구현의 필요성을 강조하고 있었다. 그에 더해 보안과 관련한 다양한 센서를 활용한 능동적인 군사보안의 첨단관리가 군사보안 환경의 주요한 변화의 추세임을 알 수 있었다.

4.3 텍스트 마이닝 분석결과(연구과제 3)

국외자료에서 가장 많이 '군사보안'을 이미지화한 단어는 '안보'였다. 이는 군사보안의 역할이 국외 연구에서는 안보와 연계하여 많은 연구가 이루어지고 있음을 <표 9>과 같이 알 수 있다.

<표 9> 유형군집분석 결과

유형분류	연관된 세부단어
국가간 협력	군사,보안,협력,연구,미국,중국,관계,러시아,사회,문제
군개혁	군사력,개혁,군대
세계평화	정치,세계,공공,국토
민간기업참여	민군,회사,개인,기업,위험,전략,영향,국방,년
분쟁지역보안문제	국제,아프리카,유럽,전쟁,안보
정보기술발전	평화,경제,정보,기술,시스템
서비스로서의 보안지출	아시아,환경,보장,국가,지출,군,서비스
민간정책산업 안전기여정책	민간,정책,안전,산업,지역,역할

'군사보안'이 국가 안보와 밀접하게 연계된 연구과제로 진행되고 있음을 알수 있다. 국외자료로 본 군사보안의 우선순위는 국가 간 협력, 군사보안 개혁, 세계평화, 민간기업 참여, 분쟁지역 보안 문제, 정보기술발전, 서비스로서의 보안 지출, 민간산업 안전 정책 기여 순으로 정리할 수 있었다. 이를 분석할 때, 국외연구 방향은 보안이 국가적인 문제로서 국가 간 협력이 필요하고 군사보안 개혁을 통한 세계평화에 기여하는 이미지로 흐르고 있음을 알 수 있다. 단순한 보안이 안보 세계평화에 기여하는 세계 안보의 측면으로 연구가 진행되고 있음을 알 수 있다.

4.4 군사보안의 국내·외 연구 차이

동일한 '군사보안' 키워드 입력 결과 그 이미지는 국내연구의 경우 '중심'을 우선적으로 제시하고 있으나 국외연구는 '군사'를 가장 앞에 내세우고 있었다. 본 연구에서는 선행연구에서 정의한 군사보안의 키워드들과의 비교를 통해 문헌적 연구(Literature Review)와 실증적 연구(Empirical Study)의 차이에서 분석된 보안 환경의 변화를 정리하였다.

<표 10> 국내·국외연구 중점 비교

선정된 주요단어			
국외연구		국내연구	
군사	전쟁	중심	무선
보안	보장	보안	드론
안보	협력	방안	개선방안
국가	개인	군	미국
미국	아시아	네트워크	한국
민간	국토	기반	관리
군	군사력	이용	보호
국제	민군	시스템	알고리즘
정책	경제	분석	위협
유럽	아프리카	활용	전략
정치	영향	개발	RFID
중국	개혁	사이버	안전
관계	기업	설계	발전방안
회사	평화	국방	체계
문제	국방	적용	기법
정보	위험	군사보안	인증
전략	지출	군사	구축
기술	군대	환경	공격
역할	년	기술	변화
환경	서비스	대응방안	스마트
러시아	연구	북한	모델
안전	시스템	구현	발전
세계	산업	국가	효율
지역	사회	대응	법제
위협	공공	센서	정책

그 결과, 국내연구와 국외연구의 차이는 대한민국이 처한 안보적 환경과 위협에 큰 영향을 받은 것으로 분석되었다. 즉, 국외연구에서의 '군사보안'이 보다 거시적인 측면에서의 국가간 협력과 공조체계, 세계평화 등의 과제에 집중되어 있는 반면, 국내연구는 국제적인 방향보다는 국내적인 북한의 사이버 위협과 그에 따른 대응방안 마련이 가장 시급한 연구흐름을 좌우하였고, 나아가서는 군사보안의 개선방향과 국방인증체계 구축과 같은 보다 기술적인 측면에 국한되는 모습을 보였다. 향후 국내연구의 방향이 지향해

야 할 분명한 상이와 보완요소가 식별된 셈이다. 이에 따른 보완요소와 도출과제분석은 아래 <표 11>와 같다.

<표 11> 군사보안 발전방안 도출과제

① 민·관·군 및 산·학·연 융합협력 프로그램 강화
② 사이버보안 국제협력·공조 정보공유방안
③ 군사혁신과 軍 비대칭 사이버보안 혁신
④ 4차 산업혁명 군사보안 융합연동접점 관리체계 구축
⑤ 기술공학에서 사회공학으로의 접근방식 전환
⑥ 軍內 군사보안 거버넌스 체계 확립
⑦ 군사 디지털자료의 비밀등급 구체화

5. 군사보안을 위한 실질적 대응방안

5.1 민관군 및 산학연 융합협력 프로그램 강화

군사보안을 위해서 개방적으로 군을 공개하고, 민관, 산학연과의 정보보안 기술공유, 사이버보안 협력체계 구축 강화가 절실한 시대가 아닐 수 없다. 민·군 간, 산·학·연·군간의 협력과 공조체계 구축은 피할 수 없는 4차 산업혁명의 융합 트랜드이며, 융합형 국방 R&D 체계로의 급속한 전환은 국가의 핵심역량과 닿아 있는 최우선 과제임을 명심해야 할 것이다. 사이버보안과 관련한 사항은 더욱 더 절실한 논의가 필요하다. 사이버 보안관련 국내·외에서의 협력, 가령 국내적으로는 KAIST·ADD·KIDA·기품원·고려대 정보보호대학원 등과의 협력과 같은 것은, 가히 전 세계적인 사이버보안의 트랜드이며, 이러한 트랜드를 바탕으로 군사보안과 관련한 세부적인 사이버 전략을 발굴하고, 국제적인 협력 메커니즘을 고안해 내는 것이 우리의 군과 국방부의 향후 비전이 되어야 한다.[23]

5.2 사이버보안관련 국제협력·공조 정보공유 방안

대한민국은 美-이스라엘 수준의 사이버 협력 공유국을 위해 미국과 긴밀히 협의해야 한다. 한-미 상호방위조약을 한-미 사이버 상호방위조약 수준으로 격상시키고자 하는 정부 차원, 군차원의 적극적인 사이버 협력 노력이 필요하다. 물론 국내에서도 128개 기관이 사이버 위협정보를 공유하는 C-TAS를 구축하고, 글로벌 사이버위협 인텔리전스 네트워크를 출범('16. 11월)한 바 있으나[24], 국방부와 육군이 적극적으로 이러한 민관군 협력 네트워크에 참여할 수 있어야 한다. 당연히 합동 및 연합 사이버전 수행체계 정립과 관련하여 국방부 및 각 군(육·해·공군)과 사이버사령부, 국정원, 경찰, KISA 등과는 실시간 업무협업, 정보공유 등의 밀착된 공조 관계가 구축되어 있어야 함은 당연하다. 국내 민관군, 산학연 협업프로그램과 더불어 국제적인 한-미 간 사이버 협력 채널 구축에 반드시 나서야 한다.

5.3 군사혁신과 군 비대칭 사이버보안혁신

軍內 진화적(evolutionary)인 사이버 군사 혁신을 위해서는 대한민국 內 10만 명, 軍內 1만 명 화이트해커 양병 혁신을 추진해야 한다. 軍內 일시적인 혁명적인 조치는 가능하지도 않고 사실 불가능하다. 소수정예일지라도 군내에 사이버 핵심전사 1만 명을 양성하여, 軍內 사이버 군사 혁신의 숙주로 삼아야 한다. 현재 우리나라의 화이트해커의 수는 약 200여 명으로 식별되고 있는바[24], 사이버 선진국들처럼, 우리도 핵심 사이버 전사들을 양적으로 크게 양성하고, 사이버 전쟁무기들을 극대화한 비대칭(非對稱)적 사이버 킬체인 수준의 군사혁신을 추구해야만 한다.[25]

5.4 군사보안 융합연동접점 관리체계 구축

군과 민간과의 연동접점(Interlocking contact)은 군이 운용되는 과정에서 불가피하게 양산될 수밖에 없다. 이러한 연동접점에 대한 관리는 4차 산업혁명의 시대에 반드시 유념해야할 보안 위해요소이다. 이렇듯 취약한 군사보안 융합 연동 접점들은 해킹 세력들에 의해 반드시 활용되고, APT(Advanced Persistent Threat, 지능적 지속 위협) 공격을 준비하는 불순 세력들에 의해 타겟이 된다. 따라서, 이러한 군사보안 융합 연동접점들을 기존 국방정보자원관리체계(DRIMS)와 유사하거나, DRIMS의 성능을 개량하는 방식으로, 관리되고 실시간으로 관제될 수 있는 체계구축이 필요하다.

5.5 기술공학에서 사회공학으로의 접근방식 전환

산업안전 분야에서 안전사고의 원인을 과거 불완전한 시설, 취약한 산업 환경과 시스템, 산업위생과도 같이 외부에서 원인을 찾는 것에서, 조직 내 안전에 대한 의식과 경각심, 안전에 대한 문화(Safety Culture), 안전의식, 안전 분위기(Safety Climate)같이 조직 내부 구성원에 기인한 원인(사회공학적 요인) 연구로 급격히 전향되고 있다. 이러한 경향을 사회공학적인 접근방식이라고 하며, 군내 보안사고도 통신 보안 시스템, 과학화 출입통제시스템 등의 외부적인 요인도 중요하지만, 조직 내부 구성원(Insider)에 대한 사회공학적 요인들이 과거와는 또 다른 보안위협요인으로 작용하고 있는 추세이다. 따라서, 이에 대한 각별한 관심과 통제대책이 절실한 실정이다.

5.6 군내 군사보안 거버넌스 체계 확립

조직구성원의 참여를 중시한다는 차원의 성숙한 접근방식이 중요한 시점에서 군내 군사보안 거버넌스 체계 확립이 필요하다. 이러한 체계확립이 선행되었을 때 비로소, 4차 산업혁명을 주도하고 있는 민간의 다양한 협의체와 군내 전 조직구성원간 공조와 융합이 가능해진다. 또한, 그로써 군내 군사보안 인식 자체가 능동적이고 효율적인 군사 혁신의 형태로 승화될 수 있으며, 이를 통해 '하나 됨(붐, Boom)'의 문화형성도 가능하다. 군내 동등한 지위를 갖는 다양한 조직구성원들이 기존 계급제도를 벗어나, 새로운 네트워크를 형성하여 정책 결정에 참여하고 상호 협력하는 군사보안 거버넌스 체계 구축은 그동안의 수동적인 군사보안으로부터 능동적인 군사보안 혁신의 길로 지향케 할 것이다.

5.7 군사 디지털자료의 비밀등급 구체화

군사 전자 데이터에 대한 비밀등급의 개념 정립이 새롭게 이루어져야 한다. 군이 가지고 있는 가장 큰 애로사항 중의 하나는 국가가 정한 기밀(비밀)은 하드웨어(Hard ware) 암호 장비를 통해서만 통신하도록 법률로 지정되어 있기 때문이다.[26] 당연한 듯 이 법률이 드론봇과 같은 기타 전장에서의 최첨단 신기술체계와 암호 장비라는 제약과 만나게 된다. 군에서는 지속적으로 군에 유입되고 있는 군사디지털자료에 대한 적정한 비밀등급구분으로 불필요한 보안통제와 암호장비 소요를 확대하지 않도록 디지털자료에 대한 꼼꼼한 분석과 검토를 통해 합리적인 디지털자료 비밀등급 구체화를 실현시켜야 할 것이다.

6. 결론

본 연구는 4차 산업혁명에 따라 변화된 군사보안 환경과 이에 대한 혁신적인 대응전략 모색을 주제로 선행연구를 통한 문헌적 연구(Literature Review)와 빅데이터 텍스트마이닝과 의미연결망 분석을 수행하고 이를 통해 의미 있는 연구 결과를 도출하였다.

'군사보안'이라는 다소 특별한 문제를 국내외 학술연구 자료를 통해 트랜드를 통한 이미지 연구 기법으로 접근한 새로운 기법의 연구 방법을 적용하였다. 이러한 실증분석 결과를 토대로 다음과 같은 군사보안 대응 방안을 제언한다.

첫째, 민·관·군 및 산·학·연과의 융합연계 프로그램 적극적으로 추진

둘째, 사이버보안 국제협력·공조 정보공유방안

셋째, 군사혁 신과 軍 비대칭 사이버보안 혁신

넷째, 4차 산업혁명에 따른 『군사보안 융합연동접점(融合 保安 接點, The Convergence Military Security Interface) 관제체계』 구축

다섯째, 기술공학에서 사회공학으로의 접근방식 전환(내부자 보안위협)

여섯째, 군내 군사보안 거버넌스 체계 확립

일곱째, 군사 디지털 자료의 비밀등급 구체화

본 연구는 4차 산업혁명의 급격한 환경 변화와 따른 군조직의 효율적인 대응방안으로서 상기 7개 과제를 도출하였다. 군의 혁신과 더불어 군사보안분야 사이버 혁신이 이루어지고, 이를 통해 군내외 협력과 공조체계 구축을 통한 군사보안의 새로운 발전과 도약이 이루어질 수 있는

계기가 되기를 소망하며, 군사보안과 관련된 지속적인 후속연구과 연계된 분석자료들이 양산될 수 있기를 기대해 본다.

참고문헌

[1] 한국국가정보학회, '국가정보학', 서울: 박영사, p. 194, 2013.

[2] 김두환·박호정, "군보안상 해킹대응방안에 관한 연구", 융합보안논문지, 17(5), p.134, 2017.

[3] 이종섭, "미래전 수행을 위한 국방시스템 구축 및 발전방안 연구", 한국군사문제연구원, p. 14, 2016.

[3] 최창일, "4차 산업혁명과 연계한 한국방위산업의 수출확대 방안", 목원대학교 석사학위논문, p. 66. 전체 내용 변용 재인용, 2018.

[4] 양대일, '정보보안개론(개정 3판)', 서울: 한빛아카데미, p.138, 2019.

[5] 최경화, "블록체인 활성화를 위한 거버넌스 구축에 관한 연구", 부경대학교 박사학위논문, p.70, 2019.

[6] 손경호, "빅데이터 보안이벤트 상관분석을 통한 APT 공격탐지 방안에 관한 연구", 성균관대학교 박사학위 논문, p.7, 편집 재인용, 2015.

[7] 고경민 외, "사이버 안보화 문제와 사이버 위협의 포괄적 대응 방안", 2017년 춘계학술발표대회 논문집, 24(1), p.364, 2017.

[8] 심재용, 김병조, "군 사이버 전문인력 운영정책에 대한 제언", 국방정책연구, 35(1). p.107, 2019.

[9] 백승구, '進化하는 북한사이버테러', 월간조선, (2019.12.8.검색), 2015. 9.

[10] 신경수, "북한의 사이버위협과 대응전략에 관한 연구", 충남대학교 박사학위논문, p.342, 2018.

[11] 국방부, '2016국방백서', 서울: 국군인쇄창. p.23, 2016.

[12] 국방일보, '국방부 국방망 해킹, 北 해커조직 추정세력 소행', 2017.5.3.

[12] 김두환, "군보안상 해킹대응방안에 관한 연구", 융합보안논문지, 17(5), p.136, 2017.

[13] 신경수, '전게논문'. p.46, 2018.

[14] 남태우, '지식구조론', 서울: 한국도서관협회, p.xi, 2015.

[15] 김정숙, "빅데이터 활용과 관련기술 고찰", 한국콘텐츠학회지, 10(1), pp.34-40, 2012.

[16] 김병국, "사회연결망분석 기법을 이용한 온라인 쇼핑몰의 상품전략 수립에 관한 연구", 경일대학교 박사학위논문, p.27, 2014.

[17] 한혜정, "마을교육공동체의 관계 구조와 행위에 관한 사회연결망 분석", 공주대학교 박사학위논문, p.48, 2019.

[18] 서정아, '전게 논문', pp.37-38, 2016.

[19] 열린공동체사회, '사회연결망분석', Open Project B, (2019. 12.28.검색), 2017.2.3.13:28.

[20] 김성수, "사회연결망 분석을 활용한 패션 디자인 컨셉 변화연구", 중앙대학교 박사학위논문, pp.23-24, 2017.

[21] 김두환·박호정, "빅데이터와 텍스트마이닝 기법을 활용한 군사보안정책 탐구", 융합보안논문지, 19(4). pp.23-34, 2019.

[22] 김정숙, "빅데이터 활용과 관련기술 고찰", 한국콘텐츠학회지, 10(1). pp.34-40, 2012.

[23] 서정아, "사회연결망 분석을 활용한 대구의 관광지 이미지 분석: 온라인 빅데이터를 중심으로", 계명대학교 박사학위논문, pp.37-38, 2016.

[24] 육군본부, '4차 산업혁명과 사이버전', 계룡: 국군인쇄창, p.17, 2017.

[25] 고한석, "국가사이버 안보체계 구축에 관한 연구", 고려대학교 박사학위논문, p.113, 2015.

[25] 신동만, '사이버전 승리를 위한 제언', 육군정책연구, p.10, 2015.

[26] 이용석, "국방사이버안보 역량 강화방안 연구", 고려대학교 박사학위논문. p.2, 2019.

〔저자소개〕

김 두 환 (Kim Doo Hwan)

1998년 금오공대 공학사
2013년 건양대학교 행정학석사
2020년 건양대학교 행정학박사
email : highmt2015@naver.com

박 호 정 (Park Ho Jeong)

1990년 경찰대학교 행정학사
2004년 충남대학교 법학석사
2013년 충남대학교 법학박사

email : phj1041@hanmail.net