국방 지휘통제체계의 클라우드 도입 방안*

Deployment Strategies of Command and Control System to Cloud Computing

박준규(Jun-Gyu Park) (제1저자) I 세종대학교 시스템보안연구실 연구원 I wnsrb3001@gmail.com
이상훈(Sang-Hoon Lee) (공동저자) I 국방과학기술연구소 수석연구원 I sanghoon@add.re.kr
박기웅(Ki-Woong Park) (교신저자) I 세종대학교 정보보호학과 교수 I woongbak@sejong.ac.kr

목 차

초 록

미래의 군 작전환경은 네트워크를 기반으로 모든 무기체계가 하나의 통합된 정보통신망 내에서 실시간으로 전장정보를 상호공유하며 작전을 수행하게 되는 네트워크 중심전(NCW)으로 급변하게 될 것이다. 이와 같은 네트워크 중심전에 대비하기 위해 클라우드 컴퓨팅은 작전 임무를 수행중인 군인들이 언제 어디서든 간단히 접속할 수 있는 플랫폼 구축의 핵심이다. 우리 군도 국방정보자원의 운용효율화를 위해 클라우드 도입을 추진하고 있지만, 아직까지는 제한된 클라우드 서비스만을 제공하고 있다. 따라서 본 논문에서는 국방 지휘통제체계(C4I)의 성공적인 클라우드 도입을 위해 서비스 가용성과 상호운용성 문제를 해결한 도입 방안을 제시한다.

＊**키워드 :** 클라우드 컴퓨팅, 국방 클라우드, C4I, 가용성, 상호운용성

ABSTRACT

Future military operational environment will be rapidly changed to Network Centric Warfare(NCW), in which all weapon systems share the battlefield information in real time within one integrated information communication network and perform operations based on the network. To prepare for such a Network Centric Warfare, cloud computing is at the heart of building a platform where soldiers on mission missions can easily access the system at anywhere, anytime. Although our military is promoting cloud adoption to improve the operational efficiency of defense information resources, it still provides only limited cloud services. In this paper, we propose strategies that solves the problem of service availability and interoperability in order to successfully deployment of Defense Command and Control System(C4I) to cloud computing.

＊**Keywords :** Cloud Computing, Defense Cloud, C4I, Availability, Interoperability

* 이 논문은 2018년 국방과학연구소의 국방 지휘통제 통합·연동 기반기술 특화연구실 과제의 지원(UD180012ED) 및 한국연구재단 지원사업(2017R1C1B2003957)의 지원을 받아 수행된 연구의 일부를 확장한 것임.
• 논문접수일 : 2019년 2월 24일 • 최초심사일 : 2019년 2월 24일 • 게재확정일 : 2019년 4월 19일

1. 서론

21세기에 들어서면서 과학기술의 비약적인 발전으로 민간뿐만 아니라 국방에서도 전쟁 수행개념의 변화 및 무기체계의 발전과 전쟁의 패러다임을 가져왔다(정종, 계중읍, 2012). 미래의 군 작전환경은 <그림 1>과 같이 네트워크를 기반으로 하여 항공기, 레이다, 전차 등 모든 무기체계가 하나의 통합된 정보통신망 내에서 실시간으로 전장정보를 상호공유하며 작전을 수행하게 되는 네트워크 중심전(NCW, Network Centric Warfare)으로 급변하게 될 것이다(채제욱, 최의중, 김현준, 이준호, 이성배, 2012; 민경만, 이정태, 류기열, 2010). 이에 대비하여 세계 각국에서는 군사력의 정비·전환 혹은 시스템 재구축 등의 군사혁신을 활발하게 추진하고 있다(김도엽, 이철규, 2008). 네트워크 기반 전장 환경에서 전쟁의 주도권 확보 및 유지를 위해서는 적보다 신속하고 정확하게 전장상황을 파악하는 것이 중요하다. 또한, 이를 바탕으로 지휘관이 언제 어디서라도 작전부대를 지휘 및 통제하여 실시간으로 변화하는 전장 상황에 효과적으로 대응할 수 있도록 지원하는 군의 핵심 요소는 국방지휘통제체계(C4I: Command, Control, Communication, Computer and Intelligence System)이다(김혜진, 이상훈, 2014). 이러한 첨단 지휘통제체계(C4I) 구축을 위해 우리 군도 컴퓨팅 및 네트워크 능력을 활용하여 정보전에서의 우위를 보장하고 군사력을 향상시키기 위해 네트워크 중심전(NCW)의 구현을 추진하고 있다(민경만, 이정태, 류기열, 2010).

<그림 1> 무기 체계가 유기적으로 연결 된 미래 전장 환경의 모습

미 국방부는 클라우드 컴퓨팅을 네트워크, 플랫폼 및 응용을 포함한 공통 서비스들을 범세계적으로 통합된 환경으로 구축하여 공유할 수 있도록 하는 합동정보환경(JIE, Joint Information Environment) 실현하기 위한 핵심 요소로 인식하여 전 세계 14개 지역에 나뉘어 있는 국방부 전용 데이터센터를 하나로 묶고, 세계 어디든 관계없이 전투에 들어간 군인들이 현장에서 간단히 접속할 수 있는 플랫폼인 RACE 출범을 공식화하였다

(안보경영연구원, 2016). 이를 통해 네트워크 중심전에 대비하기 위하여 나뉘어진 국방 정보들을 한 군데로 집약시킴으로써 언제 어디서든 지휘관의 신속하고 효과적인 지휘 및 통제가 가능하도록 지원하기 위해 국방 지휘통제체계(C4I)의 클라우드 도입은 필수적인 것을 알 수 있다. 또한, 우리 군도 국방정보자원을 효율적으로 운용하기 위해 클라우드 도입의 필요성을 인식하여 각 군(육·해·공군)의 전산소를 통합한 국방통합데이터센터(DIDC)를 설립하였지만, IaaS(Infrastructure as a Service) 형태의 제한적인 클라우드 서비스만을 전군 공통의 특정 시스템을 대상으로 제공하고 있다(6). 이를 통해 우리 군도 네트워크 중심전에 대비하여 국방정보자원의 중앙 집중화를 위해 클라우드 도입을 추진하고 있지만, 아직까지 제한된 클라우드 서비스만을 제공하고 있는 것을 알 수 있다.

국방 지휘통제체계(C4I)는 서로 다른 군 조직, 부대 혹은 체계 간 특정 서비스, 정보 혹은 데이터를 막힘없이 공유, 교환 및 운용할 수 있도록 상호운용성이 보장되어야 하며 급진적인 전장 상황의 변화에 대응하기 위해 안정적으로 서비스를 제공할 수 있도록 기능을 지속적으로 유지할 수 있는 가용성을 확보하는 것이 매우 중요하다(Davis S. Alberts, Richard E. Hayes, 2003; 민경만, 이정태, 류기열, 2010). 이에 관한 기존의 연구(박준규, 전우진, 이상훈, 박기웅, 2018)는 물리적으로 분리된 하이브리드 클라우드 도입을 통해 서비스 가용성을 확보할 수 있다는 장점을 가지고 있다. 하지만, 이로 인해 서로 다른 데이터센터 간 상호운용성이 결여되는 문제가 발생할 수 있으며 더욱 안정적인 서비스 제공을 위한 가용성 확보를 위해 추가적인 방안이 필요하다.

따라서 본 논문에서는 국방 지휘통제체계의 성공적인 클라우드 도입을 위하여 로 다른 데이터센터의 사용자 인증 및 접근제어 역할을 수행하는 인증 서버의 중앙 집중화를 통해 상호운용성을 보장하고, 서비스 장애에 대한 사전 방지 및 장애가 발생함에도 불구하고 지속적인 서비스 제공을 위한 장애 허용 시스템 구축을 통해 서비스 가용성을 확보하는 두 가지 방안을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 국방 클라우드 도입 관련 연구를 분석하고 한계점을 도출한다. 3장에서는 도출된 한계점을 해결하는 성공적인 국방 지휘통제체계(C4I)의 클라우드 도입을 위한 두 가지 방안을 제안하고, 4장에서는 결론을 기술한다.

2. 국방 클라우드 도입 관련 연구

본 장에서는 국방 분야에 클라우드를 도입하기 위한 방안에 관한 기존 연구에 대해 설명하고 그에 관한 한계점을 도출한다.

2018년 한국정보보호학회(박준규, 전우진, 이상훈, 박기웅, 2018)에서 연구 발표된 국방 클라우드 도입 방안에서는 성공적인으로 국방 클라우드를 도입하기 위한 방안을 도출하기 위해 기업의 민간 클라우드 도입을 저해하는 장애 요인 중 국방 클라우드 도입과 관련성이 높고 기술적으로 해결 가능한 장애 요인인 서비스 가용성 문제와 보안에 대한 우려를 다루었고, 이에 대한 해결방안으로 물리적으로 분리된 베어 메탈 방식의 하이브리드 클라우드를 제안하였다. 데이터센터를 물리적으로 분리할 경우 천재지변 등으로 인해 서비스 장애 발생 시 다른 데이터센터에서 지속적으로 제공하는 서비스 이용을 통해 가용성 확보가 가능한 이점이 있다. 하지만, 한 데

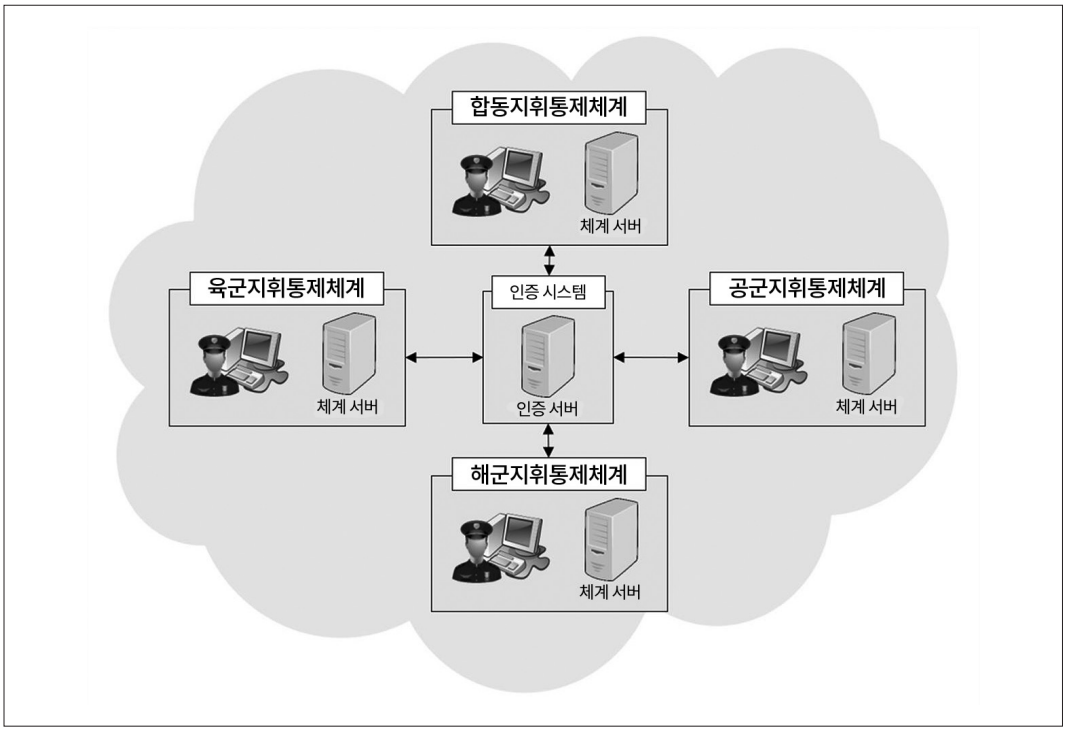
이터센터에 장애 발생 시 다른 데이터센터로 네트워크 트래픽이 집중되는 트래픽 과부하 현상이 발생할 가능성이 존재하며, 이로 인하여 발생하는 또 다른 장애의 원인이 될 수 있기 때문에 데이터센터를 물리적으로 구분하는 것만으로 서비스 가용성을 확보하였다고 단정 지을 수 없다. 이러한 이유로 물리적으로 구분하여 장애 발생 시 다른 데이터센터에서 서비스를 제공하는 것뿐만 아니라 데이터센터 내에서 장애를 사전에 방지하고, 장애가 발생하더라도 지속적으로 서비스를 제공하여 가용성을 확보할 수 있는 추가적 방안이 필요하다. 또한, 데이터센터를 물리적으로 구분할 경우 서로 다른 데이터센터 간 서비스, 정보 혹은 데이터를 공유, 교환 및 운용하지 못하는 상호운용성 결여 문제가 발생한다. 가용성 확보를 위해 데이터센터를 물리적으로 분리하였지만 장애 발생 시 다른 데이터센터에서 정상적인 서비스 이용이 불가능하다면 가용성이 확보되었다고 할 수 없다.

3. 국방 지휘통제체계(C4I) 클라우드 도입 방안

본 장에서는 성공적인 국방 지휘통제체계(C4I) 클라우드 도입을 위한 방안을 제안한다. 첫 번째는 인증 서버의 중앙 집중화를 통한 상호운용성 보장이다. 각 데이터센터의 사용자의 인증 및 권한을 관리하여 서비스에 대한 접근을 제어하는 인증 서버의 중앙 집중화를 통해 한 데이터센터의 장애 발생 시 다른 데이터센터의 클라우드 서비스 및 데이터에 대한 접근이 가능하여 상호운용성이 보장된다. 두 번째는 장애 허용 시스템(Fault Tolerance) 구축을 통한 가용성 확보이다. 장애 허용 시스템 구축을 통하여 중앙집중화된 데이터센터로의 트래픽 과부하, 예기치 못한 장비 고장 등의 장애에 대한 사전 대비 및 발생 시 정상적인 서비스를 제공하는 가용성을 확보하는 것이 가능하다.

3.1 인증 서버의 중앙 집중화를 통한 상호운용성 보장

물리적으로 분리된 데이터센터 구축 시 타 데이터센터에서는 존재하지 않는 사용자 정보 및 권한으로 인해 클라우드 서비스, 정보 또는 데이터에 대한 접근이 제한되는 상호운용성 결여 문제가 발생한다. 현재 우리 군도 각 군의 지휘통제체계들을 각자 독자적으로 개발하였고, 이로 인해 체계 간 정보교환 및 상호운용성 문제가 대두되고 있다(손태종, 서민우, 김영도, 2005). 우리는 2018년 10월 10일 합동참모본부에 방문하여 합동참모본부에서 사용하는 지휘통제체계인 합동지휘통제체계(KJCCS) 실무자들을 인터뷰한 결과 각 체계 접속 시 사용되는 사용자 계정과 암호 모듈이 연동되지 않는 등의 사용자 인증 및 접근 제어 관련 상호운용성 문제가 존재하는 것을 확인하였다. 이를 방지하기 위해서는 <그림 2>과 같이 서로 다른 데이터센터의 사용자 인증 및 접근 제어 역할을 수행하는 인증 서버를 별도의 구성을 통해 중앙 집중화하여야 한다. 중앙 집중화된 인증 서버에 등록된 사용자 정보 및 권한 등을 통해 특정 데이터센터에 구애받지 않고 클라우드 서비스 이용이 가능한 장점이 있다. 하지만, 인증 서버를 단일로 배치할 경우 단일 장애점(Single Point of Failure) 문제에 노출되기 때문에 인증 서버에 대한 장애 허용 시스템을 구축하여 정상적인 인증 및 접근 제어 서비스 제공을 위한 가용성을 확보하여야 한다.

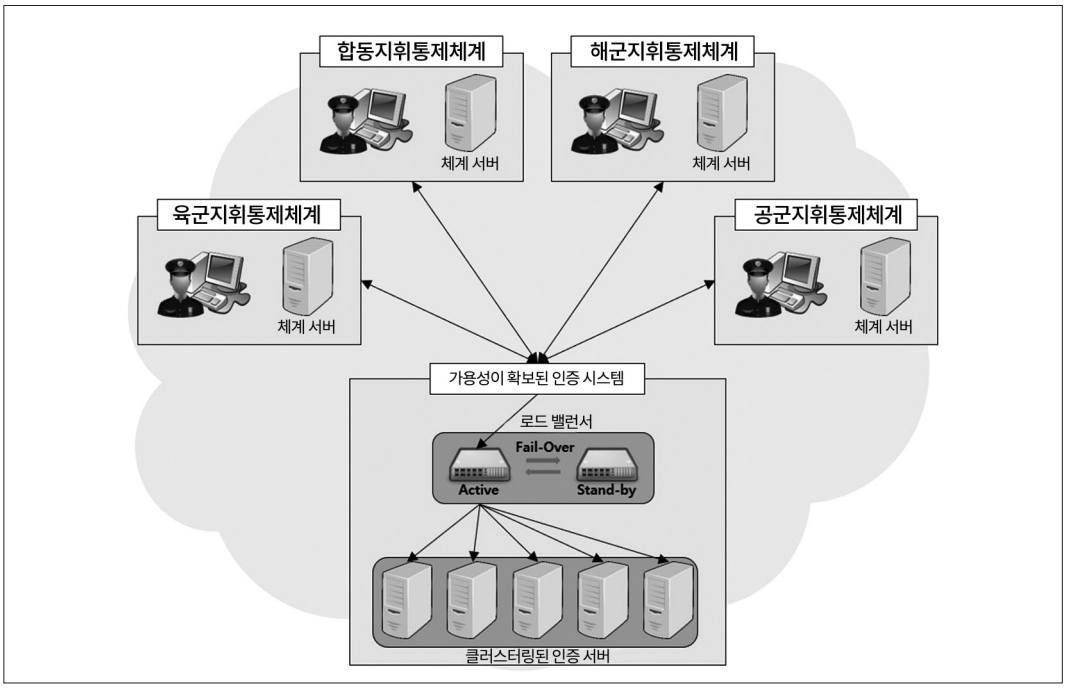


<그림 2> 중앙 집중화된 인증 서버를 통한 상호운용성이 보장된 국방 지휘통제체계 클라우드 구성도

3.2 장애 허용 시스템 구축을 통한 가용성 확보

군 내부망에 침투한 악성코드의 서비스 거부 공격(DDoS: Distributed Denial of Service)과 같은 보안 위협 및 예기치 않은 서비스 장애로부터 살아남아 안정적인 서비스를 제공할 수 있게 하는 서비스 가용성을 확보하는 것은 매우 중요하다. 'K-ICT 클라우드 컴퓨팅 활성화 계획(미래창조과학부, 2017)'에 따르면 중앙행정기관, 지자체, 공공기관 대부분 정보 자원의 중요도가 높으므로 정보 유출 방지 등을 위해 민간 클라우드보다 정부 클라우드 및 자체 클라우드를 이용하도록 하고 있다. 이로 인하여 중요도가 높은 군 정보자원의 특성상 자체적으로 클라우드를 구축하여 운용하여야만 한다. 시스템 가용성 확보를 위해 클라우드 데이터센터를 물리적으로 분리하여 구축 및 운용할 경우, 3.1장과 같이 인증 서버의 중앙 집중화와 같은 방법을 통해 상호운용성을 보장할 수 있다. 하지만, 중앙 집중화된 시스템에서 과도한 사용자 요청 및 응답으로 인한 과부하로 시스템에 장애가 발생하여 전체 시스템이 마비될 가능성이 존재한다. 하지만, 장애 허용 시스템을 구축할 경우 이와 같은 중앙 집중화된 자원의 장애뿐만 아니라 DDoS 공격 등의 보안 위협을 사전에 방지하고 장애 발생 시 서비스 중단 없이 지속적으로 서비스를 제공하는 가용성을 확보할 수 있어 안정적인 서비스 제공이 가능한 이점이 있다. 장애 허용 시스템은 <그림 3>과 같이 다수의 서버들을 하나로 묶어서 하나의 시스템 같이 동작하게 하는 클러스터링(Clustering)과 클러스터링된 서버에 작업을 균등하게 분배하는 작업 부하 분산(Load Balancing)

기술을 적용하여 구축한다. 만약, 클러스터링된 시스템 자원 중 특정 자원에 장애 발생 시 시스템 자원에 대한 작업 분할 할당을 담당하는 로드 밸런서(Load Balancer)는 해당 자원에 대한 작업 할당을 제거하여 지속적인 서비스 제공이 가능하도록 한다. 또한, 단일로 로드 밸런서를 배치할 경우 로드 밸런서에 집중되는 과도한 트래픽 양으로 인한 과부하, 예기치 않은 장애 등의 사고 발생 시 전체 시스템이 중단되어 서비스 이용이 불가능해지는 단일 장애점(Single Point of Failure) 문제에 노출된다. 이를 해결하기 위해 여분의 로드밸런서를 배치하여 분산 작업을 수행하는 Active 로드 밸런서의 장애 발생 시 대기 중이던 여분의 Stand-by 로드 밸런서가 Active 상태로 전환하여 작업 부하 분산 기능을 수행하도록 하는 장애 극복 기능(Fail-Over) 을 사용하여 구성해야 한다.



<그림 3> 장애 허용 시스템 구축을 통해 중앙 집중화된 인증 서버의 가용성을 확보한 국방 지휘통제체계 클라우드 구성도

4. 결론

본 논문에서는 국방 지휘통제체계(C4I)의 성공적인 클라우드 도입을 위한 두 가지 방안을 제안하였다. 데이터센터를 물리적으로 분리함으로 가용성을 확보하는 기존 연구에서 더 나아가 시스템 자원을 병렬화하고 해당 자원에 대한 작업을 분할하여 할당하는 부하 분산을 통해 시스템 자원의 장애 발생 시 해당 자원에 대한 작업 분배를 제거하여 정상적인 서비스를 지속적으로 제공하도록 하는 장애 허용 시스템을 구축함으로써 가용성을 확보한다. 또한, 데이터센터를 물리적으로 분리함으로써 발생하는 상호운용성 결여 문제를 사용자의 인

증 및 접근 제어 역할을 수행하는 인증 서버의 중앙 집중화를 통해 데이터센터의 장애 발생 시 다른 데이터센터의 클라우드 서비스에 접근이 가능하도록 해결하였다. 추후 연구에서는 더욱 빠르게 변화하는 미래 전장 환경 및 부대 구조에 적합한 클라우드 기반의 지휘통제체계 구축을 위한 방안에 대한 연구를 수행할 것이다.

참고문헌

김도엽, 이철규 (2008). 국방 M&S체계 발전방향. 정보과학회지, 26(1), 13-20.

김혜진, 이상훈 (2014). 육군전술지휘정보체계(ATCIS) 장애요인분석. 한국정보과학회 학술발표논문집, 108-110.

미래창조과학부 (2017). K-ICT 클라우드 컴퓨팅 활성화 계획.

민경만, 이정태, 류기열 (2010). 군 지휘통제체계를 위한 역할기반 소프트웨어 아키텍처. 정보화연구(구 정보기술아키텍처연구), 7(2), 189-200.

박준규, 전우진, 이상훈, 박기웅 (2018). 민간 클라우드 도입 장애요인 분석을 통한 국방 클라우드 도입 전략 도출. 한국정보보호학회 동계학술대회 CISC-W `18.

서민우, 김영도, 손태종 (2005). 국방 공통운용환경 (COE) 아키텍처 설계. 정보과학회지, 23(7), 18-26.

안보경영연구원(SMI) (2016). 국방 클라우드컴퓨팅 운영환경 구축방안 연구.

정종, 계중읍 (2012). 미래전 양상 전망과 무기체계 발전방향. 제어로봇시스템학회 합동학술대회 논문집, 306-318.

채제욱, 최의중, 김현준, 이준호, 이성배 (2012). NCW 기반 미래병사체계 연구개발 기술동향. 제어로봇시스템학회 합동학술대회 논문집, 465-470.

David S. Alberts, Richard E. Hayes (2003). Power to the Edge. Command and Control Research Program.

국한문 참고문헌의 영문 표기

(English translation / Romanization of reference originally written in Korean)

Chae, Je-Wook, Choe, Eui-Jung, Kim, Hyun-Jun, Lee, Jun-Ho, & Lee, Sung-Bae (2012). NCW based Research & Development Technology for Korean Future Soldier System. Control Robot System Society Conference Proceedings, 465-470.

David S. Alberts, & Richard E. Hayes (2003). Power to the Edge,. Command and Control Research Program.

Jung, Jong & Kye, Joongeup (2012). Aspect a Future War and Development Direction of Weapon-system. Control Robot System Society Conference Proceedings, 306-318.

Kim, Do-Yeob & Lee, Cheol-Gyu (2008). Military Defense Modeling and Simulation System Development. Communications of the Korean Institute of Information Scientists and Engineers, 26(1), 13-20.

Kim, Hye-Jin & Lee, Sang-Hoon (2014). Fault Factor Analysis of Army Tactical Command Information System(ATCIS). Korean Information Science Society Proceedings, 108-110.

Min, Kyung-Man, Lee, Jung-Tae, & Ryu, Ki-Yeol (2010). Role-based Software Architecture for Command and Control System. Informatization Research (former Information Technology Architecture Research), 7(2), 189-200.

Ministry of Science, ICT and Future Planning (2017). K-ICT Cloud Computing Activation Plan.

Park, Jun-Gyu, Jeon, Woo-Jin, Lee, Sang-Hoon, & Park, Ki-Woong (2018). Deployment Strategies of Military Cloud by Analyzing Obstacles to Deployment of Commercialized Cloud Services. Conference on Information Security and Cryptography-Winter 2018.

Security Management Institute(SMI) (2016). Exploring the Establishment of Operating Environment of Defense Cloud Computing.

Seo, Min-Woo, Kim, Young-Do, & Son, Tae-Jeong (2005). A Design of an Architecture for The Common Operating Environment in MND. Communications of the Korean Institute of Information Scientists and Engineers, 23(7), 18-26.