논문접수 2021.05.20 | ISSN 1738-6144 | Journal of The Korea Association of Defense Industry Studies Vol. 28, No. 1(2021)
논문확정 2021.06.14 | http://journal.kadis.or.kr/ | 한국방위산업학회지 제28권 제1호 | http://doi.org/10.52798/KADIS.2021.28.1.6

국방 암호장비 유지보수 발전방안 연구

A study on development plan for the maintenance and repair of defense cryptographic equipment

박승기*, 유동현**, 황선호***, 구한림****, 류연승*****
Seung-Kee Park* and Dong-Hyun Yoo** and Seon-Ho Hwang*** and Han-Lim Koo**** and Yeon-Seung Ryu*****

ABSTRACT

Despite the rapid development and changes in the IT environment due to the advent of the 4th industrial revolution, the military's defense coded equipment maintenance system has been operating in the same system as the existing system without any improvement until now. As a result, various problems have arisen in the maintenance work of cryptographic equipment. In addition, due to the repeated development of the defense information system, it is now difficult to perform the maintenance work of cryptographic equipment without improving the maintenance system of cryptographic equipment. Therefore, in order to convert the defense coded equipment maintenance system into a maintenance system, this study uses a deductive method to prove the validity of the variable after selecting variables that affect the defense coded equipment maintenance system through interviews with a group of experts related to encryption equipment maintenance. Therefore, a plan was proposed to solve the defense code equipment maintenance work through an agency in charge of maintenance and secure the efficiency, expertise, and security of the encryption equipment maintenance work.

초 록

4차 산업혁명 시대의 도래로 인해 IT 환경의 급속한 발전과 변화에도 불구하고 군의 국방암호장비 정비체계는 지금까지 개선되는 부분이 없이 기존과 같은 체계로 운영되고 있다. 이로 인해 암호장비 정비 업무는 다양한 문제점들이 발생하고 있으며, 이뿐 아니라 국방 정보체계의 거듭된 발전으로 이제는 암호장비 정비체계를 개선하지 않고는 더 이상 암호장비 정비관련 업무를 수행하기 힘든 수준에 도달하였다. 이에 본 연구는 국방 암호장비 정비시스템을 유지보수체계로 전환하기 위해 암호장비 정비관련 전문가 그룹의 인터뷰를 통해 국방 암호장비 유지보수체계에 영향을 미치는 변수를 선정한 후 변수의 타당도를 증명하는 연역법을 활용하여 국방 암호장비 정비 업무를 유지보수 전담기관을 통해 해결하고, 암호장비 정비 업무의 효율성, 전문성, 보안성을 확보할 수 있도록 방안을 제시하였다.

Key Words : Encryption equipment(암호장비), maintenance(유지보수), dedicated agency(전담기관), Professional maintenance company(전문정비업체), information security system(정보보안시스템),

* 박승기: 명지대학교, 석박사통합과정, keepdkagh@hanmail.net
** 유동현: 명지대학교, 박사과정, 보안경영공학과, dhy8906@naver.com,
*** 황선호: 공학박사, 한국조폐공사, 前 육군본부 정보보호기술발전장교, seonho68@naver.com,
**** 구한림: 대덕대학교, 군사학과 교수, 前 육군통신보안장교, ask366@naver.com,
*****류연승: 명지대학교, 보안경영학과 교수, soncg2209@naver.com,

Ⅰ. 서 론

1. 연구의 배경

국방용 암호장비는 자체 정비기술이 부족하여 제작회사로부터 정비문제를 전적으로 의존하고 있다. 또한 암호장비의 신규개발, 전력화, 보안관리 운영에 관한 절차 및 방법은「국방정보보안시스템 업무훈령」과 각 군의「군사보안 규정」등을 통해 규정하고 있으나, 이미 도입된 국방용 암호장비의 정비절차를 구체적으로 규정하고 있는 법제는 마련되어 있지 않은 것이 현실이다.

대부분의 국방용 암호장비는 주체계의 패키지로 획득하며, 전력화 이후 주 체계는 전력화 이후에도 종합군수지원체계나 정보화 유지보수체계를 통해 정비가 이루어지고 있으나, 국방용 암호장비는 정책 및 관련규정의 부재로 이러한 지원범위에 포함되어 있지 않다. 이에 따라 국방용 암호장비의 고장 시 정비에 대한 대책이 없으므로 고스란히 사용부대에 부담으로 작용하고 있다. 이를 해소하기 위해서 국방용 암호장비 정비체계에 대한 실태를 파악하고, 문제점을 분석하여 이를 해결하기 위한 방안을 모색하는 연구가 필요하다.

따라서 본 연구는 국방용 암호장비 정비 시 정보화 유지보수체계를 따르도록 유지보수체계로 전환하여 전문성·보안성·신뢰성·신속성이 보장하도록 국방용 암호장비의 유지보수 발전 방향을 연구하였다.

2. 연구의 범위

국방용 암호장비는 1984년 통신용으로 개발을 시작으로 현재는 다양한 종류의 암호장비를 개발하여 운영하고 있다. 또한, 2000년대 이후에 각 군 특성에 적합한 암호장비 도입이 급속하게 확대되었으나, 국방용 암호장비의 정비체계는 1984년 최초 도입시기의 정비의 수준을 벗어나지 못하고 있다. 그동안 국방용 암호장비는 소량으로 제작업체를 통해 무상으로 정비문제를 해결해 왔으나, 암호장비의 종류와 도입 수량이 급격히 증가하면서 무상정비가 한계에 도달하게 되었고, 정비체계의 문제가 현실화 되었다.

국방용 암호장비의 정비체계는 암호장비가 국가비밀장비라는 점에서 그 문제가 시작된다. 종합군수지원을 받기 위해서는 장비의 부품을 공개하고 수급을 지원해야 하지만 암호장비의 경우 정비부품을 공개하지 못하므로 종합군수지원을 받지 못하는 문제점이 있다.

따라서 본 연구는 국방용 암호장비의 정비체계의 문제점을 해결할 수 있는 유지보수체계로의 전환에 대해 연구하였다. 연구수행 간 직·간접적으로 국가암호체계가 노출되지 않도록 보안 관리를 철저히 하였으며, 비밀 내용이 연구에 포함되지 않도록 하였다.

3. 연구의 방법

본 연구는 국방 암호장비 정비체계에 대해 실증적 연구를 위해 연구자의 경험을 바탕으로 하는 Field Study 방법으로 연구를 수행하였다.

정정묵(2014, pp. 5)에 따르면 Field Study에 대하여 사용자 입장에서 실시하는 연구방법으로 개인의 경험과 현장 전문가 및 사용자 입장에서 주관적인 생각을 찾아내는 것으로, 장점은 표본오차가 거의 없고 실질적인 개선방향을 도출할 수 있는 점이며, 단점은 다양한 경험을 가진 현장 전문가의 참여가 필요하며, 시간이 많이 소요된다는 점이다.

국방용 암호장비의 경우 일반적인 장비와 달리 인가된 인원만 다룰 수 있으며, 정비의 경우 암호장비 관리자만이 경험할 수 있으므로 국방용 암호장비 정비체계를 연구하는데 있어서 참여할 수 인원은 극히 제한적이며, 암호장비의 현장 관리자 및 사용자의 경우 정비체계의 실태와 문제점을 정확히 알고 있으므로 본 연구에 있어서 Field Study 방법은 가장 적합한 방법으로 판단하였다.

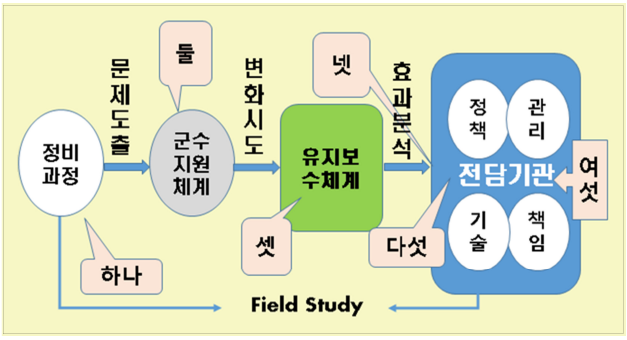
국방용 암호장비가 종합군수지원체계의 지원을 받지 못하는 한계점에 봉착하면서 국방부는 2018년 암호장비 정비문제를 정보화 유지보수체계로 전환하기 위한 시범시업을 시행하게 되었다.

본 연구는 국방용 암호장비 정비과정의 문제점을 도출하여 군수지원체계에서 유지보수체계로 전환되는 과정을 〈그림 1〉과 같이 Field Study 방법으로 연구하였으며, 다음의 순서로 연구를 진행하였다.

첫째, 국방암호장비 및 정비체계를 Field Study 경험을 통해 주관적 견해와, 이론적 배경을 연구하였다.

둘째, 암호장비 정비의 문제점을 연구하였다.

셋째, 유지보수체계가 정비체계에 미치는 변수들의 타당도를 연구하였다.



〈그림 1〉 연구의 방법 Tool

넷째, 국방부가 실시한 시범사업을 통해 유지보수 발전방향을 연구하였다.

다섯째, 유지보수 전환의 시사점을 연구하였다.

여섯째, 결론과, 향후 발전방향을 제시하였다.

본 연구의 검증을 위해서는 FGI(Focus Group Interview) 21명을 선정하여 2020년 6월 5일부터, 2020년 10월 3일까지 면접조사를 실시하였다.

Ⅱ. 연구의 이론적 배경

2.1. 국방 암호장비 정비체계

2.1.1 암호장비 정비업무의 시작

군의 암호장비 정비체계는 1984년 최초 암호장비가 보급되면서 기무사(현재 군사 안보지원 사령부)에서 관리 및 운용지원 하였다. 이후 국방용 보안시스템이 점진적으로 증가하면서 보안시스템 업무를 안보사에서 각 군으로 1990년 이관하게 되었다.

암호장비가 가장 많았던 육군(전체장비 80%)은 1통신여단으로, 해군(10%) 및 공군(10%)은 각 군 본부에 정비 업무를 이관 받게 되었다. 그러나 2년 후 1992년 육군 보안시스템 정비기능을 가지고 있던 1통신여단은 지금에 국군통신사령부로 승격하여 이전하면서 정비조직 및 임무 모두를 가지고 가게 되었다. 따라서 육군은 국직부대인 국군통신사령부에서 보안시스템을 지원을 15년 동안 지원받아 오다가, 2007년에서야 국군지휘통신사령부로부터 보안시스템 정비업무를 육군으로 이관하여 군수사 등 3개 지역으로 창 정비업무를 분산 운용하였다.

2.1.2 암호장비 정비체계의 한계

각 군에서는 암호장비의 정비지원체계가 없이 각급부대가 알아서 제작업체를 통해 무상으로 정비하여 왔으나, 2004년 C4I 체계가 도입되면서부터 암호장비 정비비를 종합군수지원체계로 전환하였다.

그러나 암호장비가 비밀장비라는 이유로 제원 및 특성 등이 공개가 제한되어 정상적인 지원이 어려웠다.

따라서 암호장비가 고장이 발생하면 종합군수지원체계의 지원 없이 사용자로부터 야전정비[1]단계를 거쳐 제작업체로 이어지는 업체정비에 의존하여 왔다.

따라서 정비기간이 최장 6개월이나 소요되었고, 실시간 긴급조치가 필요한 현장 기술지원은 전무하였다. 또한 고장을 예방하는 예방정비의 개념이 없고 운용자 및 관리자에 대한 정비교육도 미실시 되고 있다.

이러한 현실을 개선하고자 국방부는 2018년 전문정비업체를 선정 유지보수 시범사업을 실시하게 됨으로써 암호장비의 유지보수 업무의 필요성이 대두되었다.

2.2. 암호장비 정비체계의 정의

2.2.1 암호장비와 보안시스템

「국가 정보보안 기본지침(2020)」에 따르면 암호장비란 비밀의 보호 및 정보통신 보안을 위하여 사용되는 암호기술이 적용된 장치나 수단 중에서 국가정보원장(이하 “국정원장”이라 한다)이 승인하여 개발·제작·보급되는 하드웨어 형태의 암호자재를 말한다. 「국방정보보안업무훈령(2020)」에서는 국방용 암호장비를 군의 무기체계, 전력지원체계를 통하여 생산, 처리, 저장, 송수신되는 정보의 유출, 변조, 훼손 등을 방지하기 위하여 암호논리를 이용하는 장비(암호모듈)로 정의하고 있다. 암호장비는 지난 2000년 이전에는 보안장비라는 명칭으로 사용하였으나 상용 장비(CCTV, 검색장치 등)등의 출현으로 보안장비라는 이름이 혼용되자 국정원은 「국가 정보보안 기본지침」에 기존의 보안장비 명칭을 암호장비로 변경하였다.

한편, 「국방정보보안시스템 업무훈령(2020)」에 따르면 암호체계를 사용하고 있는 ‘암호장비’, ‘암호자재’, ‘암호논리’ 등을 총칭하여 ‘정보보안시스템’ 또는 ‘보안시스템’이라고

주1) 야전정비 : 사용 불가능한 부분품, 소결합체의 수리, 분해 등의 정비를 수행함

한다. 또한 국가정보보안시스템을 국방용으로 사용하고자 할 때는 국정원으로부터 사용승인을 받아야 하며, 암호장비를 취급하는 전임암호사[2]를 임명하여야 한다.

2.2.2 종합군수지원체계

종합군수지원(ILS, Integrated Logistics Support)[3]는 "무기체계의 요구 성능을 유지하고 경제적인 군수지원이 보장되도록 무기체계의 소요제기로부터 폐기까지의 제반 군수지원 사항을 종합 관리하는 활동으로 무기체계의 획득 및 운용에 필수적인 11부분으로 구성되어 있다."「

「방위사업관리규정(2020.12.23.)」 제137조에 따르면 종합군수지원요소는 ① 연구 및 설계반영, ② 표준화 및 호환성, ③ 정비계획, ④ 지원장비, ⑤ 보급지원, ⑥ 군수인력운용, ⑦ 군수지원교육, ⑧ 기술교범, ⑨ 포장, 취급, 저장 및 수송, ⑩ 정비 및 보급 시설, ⑪ 기술자료 관리로서, 효율적이고 경제적인 군수지원 보장을 위하여 주장비와 병행하여 개발·확보하도록 하고 있으며, 수명주기 전 과정을 종합적으로 관리하고 있다.

이러한 종합군수지원 제도는 1990년 육군조직을 편성하면서 부터 시행하게 되었으며, 현재 방위사업 청 법 제3조 2항은 군수품을 무기체계와 전력화지원체계로 구분하여 지원하고 있다.

2.2.3 군수지원체계

군수지원체계[4]는 "군수지원을 위한 조직, 절차, 기능 등 제반 요소들이 유기적으로 결합되어 지원하는 방법과 계통이며, 적용되는 체계에는 보급지원체계, 정비지원체계, 수송지원체계가 있다."

「보급지원체계」는 급식·유류·물자지원체계, 7·9종 지원체계로 구분되며, 「정비지원체계」는 정비수준에 따라 부대정비, 야전정비, 창정비로 구분한다.「수송지원체계」는 부대별로 보유한 수송자산을 우선 활용하고, 수송능력을 초과하는 수송소요가 발생하면 상급부대에 지원받는다.

2.2.4 전담기관과 정비업체

전담기관이란, 「국방정보화업무훈령, 제189조(전담기관 지정 분야 및 운영 원칙)④항」에 의해 군사비밀자료를 포함하여 보안을 필요로 하는 정보시스템 유지보수 및 기술지원에 관한업무에 한하여 전담기관을 지정하여 운영할 수 있도록 하고 있다. 이렇게 유지보수 업무를 전담기관으로 지정하는 목적은 「국방 정보화업무훈령」 제188조 국방정보화 기반조성 및 국방 정보 자원관리에 관한 법률(약칭: 국방 정보화법) 제11조 제1항에 따라 국방정보화 정책개발, 사업추진 및 국방정보 자원관리 지원을 통해 일관성 있고 체계적인 업무 추진, 책임성 보장, 예산의 효율적 집행 제고를 위하여 분야별로 전문적인 전담기관을 지정하여 운영하도록 한 것이다. 현재 국방 정보시스템 유지보수 및 기술지원 전담기관은 한국국방연구원(국방정보체계관리 단), 국방기술품질원(국방과학기술평가원), 군인공제회(C&C)를 운영하고 있다.

정비업체란, 「국방정보보안시스템 업무훈령」제 15조에 의해 정비업체는 정보보안시스템에 관하여 전·평시 정보보안시스템 정비, 고장원인 파악 및 장애조치 등 현장정비, 정보보안시스템의 수리부속 지원, 정비요원 및 운용자에 대한 교육, 패치 및 이전설치, 예방정비, 정보보안시스템 고장 원인 및 정비현황 정기보고, 운영유지단계의 RAM분석 등의 업무를 수행하는 업체를 말한다.

「국방보안시스템 업무훈령」에서는 전담기관과 정비업체를 〈표 1〉과 같이 정의하였다.

〈표 1〉 국방부 훈령 전담기관과 정비업체의 정의

구분	정의(국방부 훈령)
전담기관	1. 국방정보화 기반조성 및 국방정보자원관리에 관한 법률(국방정보화업무훈령 제188조) 규정에 의해 국방 유지보수전담기관으로 지정된 기관 및 업체 2. 국가용 암호장비 사용 승인기관(국가정보원) 또는 연구 개발기관(국가보안기술연구소)으로 부터 전담하고자 하는 암호장비의 전체장비에 대해 기술을 이전받은 기관이나, 전문정비 업체 3. 정비업체를 지정하고 암호장비 관련 보안관리 업무, RAM 분석결과 통보, 장비 및 부품의 수명주기관리, 암호장비 관리자 양성을 위한 교육지원
정비업체	1. 전·평시(대규모 훈련, 작전 시) 근접정비 2. 제작업체와 구분되는 전문정비기능을 확보 하고, 첨단 정비시스템을 구축하여, 고장장비의 원인 파악을 통한 재발 방지대책을 제공하고, 고장 및 장애조치 3. 수리부속확보 및 지원, 부품의 표준화 4. 정비요원 및 운영자에 대한 정비기술과 장애 복구 교육 5. 패치, 이전설치 시 기반체계와 연동지원 6. 장비별 수명주기를 고려한 부품별 표준화 및 규격화를 지원하고, 현장지원을 통한 예방 정비 활동 7. 고장원인 및 정비현황에 대한 정기보고 8. 운용유지 및 정비단계의 RAM분석 보고

출처: 국방부 『국방정보보안시스템 업무훈령』(2020.07.)

주2) 국방부,『국방정보보안시스템 업무훈령』, 국방부2020, p.13).

주3) 이성윤, 홍석진, 『종합군수지원 실태진단 및 발전방향』,국방정책연구 2005, P.36.

주4) 육군본부,『야전교범 운용-6-11, 군수업무』(2016), PP.3-8-15.

2.3. 암호와 관련된 기존 연구 사례

인터넷을 통해 '암호', '암호장비', '암호장비', '정비' 등의 키워드로 검색한 결과 암호의 구조, 논리, 알고리즘, 함수, 비밀 키 등과 관련해서는 다양한 연구의 결과가 존재하였으며, 검색한 결과를 정리하면 〈표 2〉와 같다.

〈표 2〉 암호관련 연구의 조사 결과(2021.2.5.)

구분	검색 키워트			
	암호	암호장비	암호정비	정비
RISS	5,653	895	249	78,164
KIISC	334	338	335	1
KIDA	192	17	0	819
국방보안 학술지	1	0	0	0
DBpia	4,803	92	17	13,104

〈표 2〉와 같은 수 많은 연구가 있음에도 암호장비 정비와 관련된 연구사례는 조사되지 않았다. 군 암호와 관련된 연구사례를 살펴보면, 김홍태, 이문식, 강순부(2014)는 군사 분야 자료를 효과적으로 관리할 수 있는 검색 가능 암호 알고리즘을 제안하였고, 남길현(2001)은 대중적인 전자서명을 구현하는데 필수적인 공개키 기반 인증기관을 구축하여 군 업무에 활용하는 방안을 제시하였다. 윤은준(2012)은 군사목적의 위성 데이터와 같은 대용량 자료를 암호화하기 위해서는 전통적인 비대칭 암호시스템에 3DES 또는 AES와 같은 대칭키 알고리즘을 혼용해서 사용할 것은 제안하였다. 최준, 강성문, 최인수(2015)는 암호분야에 있어서 세계 최고의 기술력을 보유하고 있다고 알려진 미군의 암호장비의 변천 동향을 알아보고 이를 토대로 향후 정보통신 환경 변화에 부합된 발전방향을 제시하였다. 송원석, 강성문, 이민우(2020) 체계마다 다양한 암호장비를 도입함에 따라 증가되는 장비관리 어려움, 복잡해지는 네트워크 환경, 제한되었던 지휘통제의 어려움으로 인해 체계 간 정보를 공유할 수 있도록 암호장비에 대한 표준화가 필요하다고 제안하였다. 이러한 연구사례에서 대부분의 주제는 암호장비 운영방안에 대한 연구였으며, 암호장비의 정비에 대한 연구 결과는 찾지 못하였다.

따라서 본 연구에서는 지금까지 연구된 바 없는 국방용 암호장비 정비와 관련된 최초의 연구로서의 의미가 있다.

Ⅲ. 암호장비 정비의 문제점

3.1. 외부의 부정적 인식

국방부는 신규 암호장비를 지속적으로 개발하고 있으며, 수명주기는 7년으로 지정하여 정보통신망 변화에 대응하고 노후(老朽)장비는 조기에 도태하도록 하고 있다. 그러나, 20년이 지나도 노후 된 암호장비를 30% 이상 사용하고 있다. 이러한 현실은 언제까지 지속될지 모르는 상황으로 정보통신망의 안정성 및 신뢰성에도 매우 나쁜 영향을 주고 있다.

2016년 보안뉴스 원별철 기자는 '北 보안위협 높아지는데 군 암호장비 일부먹통[5]'이라는 제목으로 "경대수 국회의원이 국감에서 1990년대 도입된 암호장비 중 4,000 ~ 5,000여 대는 지금도 사용하여 취약하다고 하였다"는 보도를 하였다.

이러한 보도와 같이 정보통신망에 장애가 발생되면 대부분 노후화된 암호장비의 문제로 전가 되어 암호장비부터 분리하고 사용하지 않는 현상이 반복되어 정보통신망 내 소통되는 군사자료 및 비밀 등이 보호되지 못하는 등의 문제로 고스란히 전투부대의 부담으로 작용하여 전투력을 약화 시키는 요인이 되고 있다.

경대수 국회의원 또 "우리 군이 사용하는 암호장비의 유지관리가 방치되어 있어 군사보안에 문제가 있다.[6]" 라고 지적하였다. 이렇듯 암호장비는 군내부에서는 물론 군 밖에서 까지도 유지보수에 대한 다양한 문제점을 제기하는 등 더 이상 암호장비에 문제를 방치할 수 없는 상황에 도달하였다.

3.2. 암호장비 정비전문가 부재

암호장비 정비 업무는 1984년부터 1990년까지 국군지휘통신사령부, 해군, 공군에서 각각 담당하였다. 육군은 2017년에 들어서야 국군지휘통신사령부로부터 창정비 업무를 인수하고, 창정비소를 3개소로 분리하여 운영하여 왔으며, 이때부터 각 군에서는 암호장비 정비 업무를 종합군수지원체제를 통해 해결하려는 다양한 노력을 기울여 왔다.

주5) 보안뉴스, 2016,10,10. "北 보안위협 높아지는데 군 암호장비 일부'먹통'", https://blog.naver.com/dskyung79/220834533680, 2021.3.29

주6) 경대수 의원 개인 블로그 홈페이지, https://blog.naver.com/dskyung79/220830123001, 2021.3.29

그러나 암호장비는 국가용 암호체계를 가진 비밀장비로 지정되어 종합군수지원체제가 요구하는 기술정보 제원(제원, 특성, 형상, 부품정보, 기능, 운영제대, 용도 등)의 정보를 제공할 수 없었다. 이러한 이유로 2007년부터 현재까지 암호장비에 필요한 정비 , 저장, 분배, 구매, 품질보증, 수명주기 관리는 「국방정보보안시스템 업무훈령」제 69조에 따라 자체적으로 보안부서가 운영·관리하고 있다.

현재 국방용 암호장비는 정비인력 양성을 위한 교육체계가 없고, 정비체계와 관련한 정책과 규정이 마련되어 있지 않다. 따라서 암호장비 정비는 제작한 업체의 무상 수리에 의존하고 있다. 이러한 이유로 암호장비의 제작과정의 부품 결함이나 근본적인 원인의 규명이 불가할 뿐만 아니라 장애가 발생하여도 문제를 파악하고 복구할 수 있는 전문가가 군에는 없는 것이 현실이다.

더 큰 문제는 4차 산업기술의 발달로 국방 정보통신 기반체계의 대부분이 상용기술을 사용하고 있어서 상용 정보통신장비와 암호장비의 연동과 정비에는 고도의 전문성과 많은 경험을 가진 전문가가 필요한데, 군에는 고도화된 상용기술을 정비할 수 있는 전문가가 없이 최신 정보통신 환경의 변화에 대응하지 못하는 문제점을 드러내고 있다.

3.3. 암호장비 유지보수체계 미 구축

암호장비 환경에는 많은 변화가 있었다. 정보통신 기술의 발전에 따라 암호기술이 변화하면서 다양한 형태의 암호장비가 제작·운영되고 있으며, 1984년 통신용 암호장비에서 2000년대의 네트워크 중심의 암호장비로, 현재는 특정화된 서버, 개인 특정체계용으로 변화가 있었다. 또한, 아날로그에서 디지털로, 하드웨어에서 소프트웨어나 칩 형태로, 최근에는 형상이 없는 소프트웨어 형태로 변화하고 있다. 〈표 3〉는 국방용 암호장비가 1980년부터 현재까지의 변화과정을 나타낸 것이다.

〈표 3〉 암호장비의 변천 과정

구분	1980년~1990년	1990년~2000년	2000년~현재
수량	5,000여대	50,000여대	150,000여대
용도	통신용 단말기 중심	네트워크 중심	개인(휴대) 중심
신호처리	아날로그 장비	디지털 장비	
운영현황	대부분 폐기	20년 이상 된 (노후)장비 30% 이상 사용	

2016년 10월 보안뉴스 원별철 기자는 "경대수 국회의원은 우리 군이 운영 중인 80여종의 암호장비 14만 여대 가운데 2015년 한 해 동안 전제 암호장비의 26%인 4만 여대가 단순 기계결함으로 고장을 일으켜 기능을 발휘하지 못했다고 했다."고 보도한 바 있으며, 이윤찬 이코노미21 기자는 '국방예산 펑펑 암호장비는 엉망[7]'이라는 기사에서 "군 암호장비 사업 추진은 5공이 출범하기 직전인 80년 11월 대통령의 군용 비화기(비밀 암호화 기기) 개선지시에 따라 〈표 4〉와 같이 시작되었다."고 보도하였다.

〈표 4〉 이윤찬 이코노미 21, 군 암호장비사업 추진 과정

연 도	내 용
1980. 11. 10.	대통령 군용비화기 감도개선 지시
1981. 10. 2.	국방과학연구소 샛별연구실(현 국정원 산하보안연구소) 주관으로 암호장비 사업 추진
1995. ~ 현재	국정원 주관으로 암호장비사업 추진(비밀사업)

출처: 이윤찬 이코노미 21, (2007.04.23)

군에서는 암호장비 정비문제를 해결하기 위해 종합군수지원체계[8]에 정형화 편성을 시도하였으나, 국가용 비밀의 한계로 제한적으로 지원할 수 밖에 없었다.

반면에 국방정보체계의 경우 '태극 합동전장모의 모델'(이하 '태극 JOS')[9] 등 13개의 체계를 유지보수를 하는 전문기관으로 한국국방연구원과 군인공제회 C&C를 지정하고, 사용자에게까지 유지보수업체가 직접 정비 및 기술지원을 하고 있다.

최근에는 암호장비가 소형화, 모듈화 되고, 운영 환경에 따라 기반체계와 연동이 필수가 되어 IP주소, 라우팅 정보 등 기반체계와의 연동 정보를 암호장비에 입력해야 한다. 그러나 이러한 정보의 입력은 전문지식이 없는 사용자에게는 매우 어려운 일이다. 이 점을 고려하면 암호장비도 국방정보체계의 유지보수 개념을 도입하여 유지보수 일체를 전문기

주7) 이윤찬기자 『이코노미21』 스페셜리포트, "국방예산'펑펑'암호장비는'엉망'" (2007.04.23.) http://www.economy21.co.kr/news/articleView.html?idxno=58137,

주8) 종합군수지원체계 : 이성윤, 홍석진 「종합군수지원(ILS) 실태진단 및 발전방향」 "군수지원을 보장하기 위하여 소요부터 설계, 개발, 운영 및 폐기까지 종합 관리하는 활동"육군군사연구소.2019, (30 pages)

주9) 정상윤, 박태훈, 「합동전장 모의모델 개발 방안」한국국방연구원, 국방정책연구 59권3호, 2003년 03월, 9-27(p20) 태극 합동전장모의 모델(이하 태극 JOS) : 지상·해상·공중 합동작전 모의에 중점을 둔 모델.

관에 아웃소싱을 함으로써 전문지식이 부족한 사용자를 근접 지원하는 시스템을 갖출 필요가 있다. 〈표 5〉는 정보화 유지보수의 지원 항목의 사례이다.

〈표 5〉 정보화 유지보수체계 지원 사례

유지보수 항목	주요 내용
① 유지보수 시스템 구축	전문정비업체를 통한 전문가 기술 지원
② Help Desk, One - Stop서비스	운영 간 발생한 간단한 장애처리
③ 즉시 정비지원	제작업체 정비소요일 단축 가용도 증가
④ 정비업무 일원화,	군별 제작업체 방문 중복 및 예산낭비 해소
⑤ 기술교육 및 컨설팅	상용 기술을 전문가에 의해 군내 유입
⑥ RAM 분석	장비 및 부품에 대한 수명주기 고려
⑦ 예방정비	고장 이전에 조치
⑧ 통제기관 역할	전문정비업체의 통제 및 관리
⑨ 훈련지원	전시 및 대규모 훈련 시 현장지원
⑩ 각종 고장원인 및 사례분석	정비실적에 의한 사례분석 재발방지
⑪ 표준화 및 규격화자료 제공	부품의 단종 및 단가의 급격한 증가에 대비
⑫ 수리부속 지원	소모성 수리부속 지원

Ⅳ. 유지보수 타당도 분석

4.1 FGI(Focus Group Interview) 대상 선정

정보화 유지보수체계를 암호장비 정비에 적용하는 방안을 연구하기 위해 Field Study 방법을 사용하였고, 연구 진행을 위해 FGI(Focus Group Interview) 대상을 선정을 진행하였다. FGI 대상은 현재 국방부, 각 군 본부, 제작회사, 정비업체, 연구기관 등에서 암호업무 수행경험이 5~10년 이상인 숙련자 및 전문가 21명을 선정하였다.

〈표 6〉 FGI 대상 인원

그룹	그룹설명	경력별 인원	
		5년 이상	10년 이상
계		5명	16명
A	암호전문가	0명	5명
B	암호관련자	1명	2명
C	제작회사	0명	3명
D	정비업체	2명	3명
E	정책담당자	1명	2명
F	연구기관	1명	1명

FGI 대상은 총 6개 그룹으로 〈표 6〉과 같이 구성하였다. 암호전문가 그룹(A)은 현직에서 암호장비를 관리하는 책임자 또는 직접 정비업무 종사자를 대상으로 하였다. 암호관련자 그룹(B)은 암호장비 사용자 그룹으로서 관련 참모 및 지휘자(중대장, 담당관)를 대상으로 하였다. 제작회사와 정비업체(C)의 그룹은 등록된 11개 업체 중 장비 수가 많은 3개 회사의 담당직원 대상으로 하였고, 정비업체(D)는 시범사업체 참여한 본부장급 이상의 관리자들을 대상으로 하였다. 정책담당자(E) 그룹은 국방부, 각 군 본부에서 암호업무를 수행하거나 암호업무를 감독하는 과장급을 대상자로 하였으며, 연구기관(F)의 그룹은 암호장비의 개발기관 또는 암호장비의 개발업무에 참여한 경험이 있는 연구소의 직원을 대상으로 선정하였다.

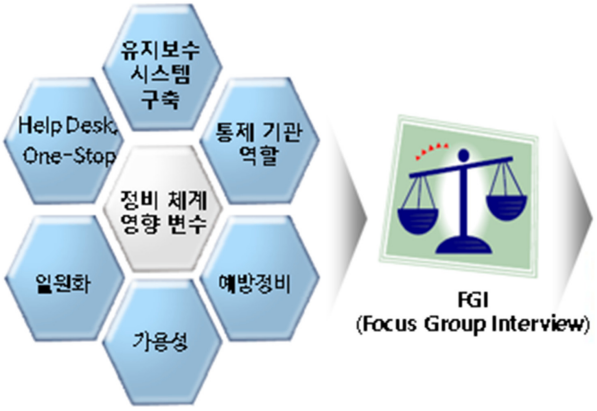
4.2. FGI 유지보수 변수의 선정

정보화 유지보수체계를 암호장비 정비에 적용 시 영향을 미치는 변수들을 선정하기 위해 정보화 유지보수 사업의 제안서 평가요소 및 유지보수 수행결과 보고에서 〈표 7〉과 같이 유지보수의 변수 12개를 선정하고, FGI를 통해 〈그림 2〉와 같이 암호전문가들이 암호장비 유지보수에 영향력이 있는 것으로 판단한 항목 중 우선순위가 높다고 판단한 항목 6개를 변수로 최종 선정하고, 암호장비의 유지보수에 비교적 영향력이 적다고 판단된 평균 30% 이하의 6개는 버리기로 하였다.

〈표 7〉 정보화 유지보수의 변수

항목	변수의 구성	FGI
1	유지보수 시스템 구축	21명
2	Help Desk운영, One - Stop서비스	19명
3	즉시 정비지원(가용성)	19명
4	정비업무 일원화,	17명
5	기술교육 및 컨설팅	7명
6	RAM 분석	5명
7	예방정비	14명
8	통제기관 역할	16명
9	훈련지원	5명
10	각종 고장원인 및 사례분석	6명
11	표준화 및 규격화자료 제공	4명
12	수리부속 지원	5명

선정된 변수들이 암호장비 유지보수체계와 관련하여 변수로서 타당한지에 대한 검증은 확인적 연구[10] 방법을 사용하였으며, 유지보수 시범사업 결과를 통해 입증하였다.



〈그림 2〉 FGI 유지보수 변수

4.3. FGI 유지보수 변수 검증

FGI로 선정한 유지보수 변수에 대한 검증을 위해 FGI 대상인 암호전문가를 대상으로 그룹만족도, 체감만족도 등의 만족도와 항목중요도를 평가하고, 이를 종합하여 종합만족도를 평가하였다.

그 결과 〈표 8〉와 같이 변수들의 종합만족도는 87%였으며, 선정된 변수들의 중요도는 94%로 유지보수에서 변수들의 중요도가 높았음을 알 수 있었다.

암호장비 정비체계를 정보화 유지보수체계와 같이 개선함으로써 나타날 수 있는 효과는 국방부의 유지보수 시범사업의 만족도 조사를 통해 검증하였다. 시범사업의 만족도는 국방부가 시범사업에 참여한 부대와 관련 부대, 각 군 본부 및 유관기관 소속의 관계자 150명을 대상으로 실시한 고객만족도 설문조사 결과를 분석하였다.[11] 설문조사 결과를 보면, 사용자 만족도는 92.8%의 사용부대가 만족하는 것으로 나타났으며, 시범사업에서 드러난 효과로, 기존에는 정비업체 입고 후 정비 완료 시까지 약 7개월이 소요되었으나, 유지보수체계를 통해 정비 시 시범사업 기간 내 평균 11.3일이 소요되어 정비 기간이 대폭 감소하는 효과를 확인하였고, 야전부대와 창 정비기관의 담당자들로부터 긍정적인 평가를 받았다.

〈표 8〉 FGI 변수 만족도

측정 구분	정 의	그룹	변수	측정값 평균
종합만족도	만족도의 평균	-	-	87%
그룹만족도	유지보수 항목 (83%)	A	①, ②, ③, ④, ⑦, ⑧	100%
		B	①, ②, ④, ⑦	66%
		C	①, ③, ④, ⑧	66%
		D	①, ②, ③, ④, ⑦, ⑧	100%
		E	①, ②, ③, ④, ⑧	83%
		F	①, ③, ④, ⑦, ⑧	83%
체감 만족도	유지보수 체감 (85%)	A	①, ②, ③, ④, ⑦, ⑧	100%
		B	①, ②, ④, ⑦, ⑧	83%
		C	①, ③, ④, ⑦	66%
		D	①, ②, ③, ④, ⑦, ⑧	100%
		E	①, ③, ④, ⑧	83%
		F	①, ②, ④, ⑦, ⑧	83%
중요도	유지보수 항목 중요도 (94%)	A	①, ②, ③, ④, ⑦, ⑧	100%
		B	①, ②, ③, ④, ⑦	83%
		C	①, ②, ③, ④, ⑧	83%
		D	①, ②, ③, ④, ⑦, ⑧	100%
		E	①, ②, ③, ④, ⑦, ⑧	100%
		F	①, ②, ③, ④, ⑦, ⑧	100%

[비고]
① 유지보수 시스템구축, ② Help Desk 및 One-Stop, ③ 정비업무 일원화, ④ 즉시 정비지원(가용성), ⑦ 예방정비, ⑧ 통제기관 역할

이렇듯 시범사업의 결과는 유지보수체계를 통해 국방보안 시스템의 안전성을 높이는 계기가 되었으며, 유지보수체계로 전환이 군의 작전 운용성능을 높이고 전투력 발휘에 적합하였음을 증명하였다. 또한, 각급 부대의 구체적인 요구사항을 식별함으로써 유지보수체계로의 변화에 대한 확신을 갖도록 하는 기회가 되었다.

〈표 9〉은 FGI를 통해 암호전문가들이 유지보수에 필요하다고 선정한 6개의 변수의 항목을 시범사업 평가항목 8개 변수들과 비교한 결과 FGI 결과로 선정한 변수들은 모두가 일치하였다. 특히 FGI에서는 One-Stop 서비스와 Help Desk가 하나의 같은 변수로 선정한 반면, 시범사업에서는 분리되어 평가되었다. 기타 시범사업간 사용자들이 요구한 6개 항목은 향후 유지보수사업에 포함되어야 할 것으로 나타났다.

주10) 확인적연구: 성태제·시기자『연구방법론』학지사,2021.2.25.(3판) p44쪽.

주11) 국방부, 「'19년 보안시스템 유지보수 확대 운영준비지시」 문서, 보안암호정책과-4669,(2018.10.29. 붙임3-2,

〈표 9〉 변수요인의 비교

순위	유지보수의 임무	시범사업평가
1	① 유지보수체계 전환	100%
2	② Help Desk,	86%
3	② One - Stop 서비스	93%
4	③ 정비창구 일원화	95%
5	⑤ 예방정비, 서비스	88%
6	④ 정비시간단축, 가동률	81%
7	⑥ 국방부 역할 강화	100%
8	훈련지원	99%
9	전시유지보수보장	사용자추가 요구
10	국방암호장비전산화	
11	정비조직개편	
12	정비업체개선	
13	고장원인 분석	
14	RAM분석	

4.4. 소결론

Ⅲ장 3절의 유지보수체계 미 구축으로 조작화 한 가설과 Ⅳ장의 유지보수 타당도 분석에서 FGI로 선정한 변수들을 비교한 결과 〈표 10〉과 같이 변수들이 상관관계가 있으며 변수 내용이 일치하는 것으로 나타났다. 따라서 가설로 선정한 6가지 변수(유지보수 시스템구축, 창구일원화, 암호장비 가용성, 예방정비, 통제기관의 역할)를 포함하는 유지보수체계로 전환하면 정비문제가 해결될 수 있다고 판단되었다.

〈표 10〉 변수요인의 비교

항목	유지보수체계 미구축(가설)	FGI 선정변수
1	유지보수 시스템구축	① 유지보수 시스템 구축
2	Help Desk, One-Stop	② Help Desk, One - Stop 서비스
3	창구 일원화	④ 가용성 증가
4	예방정비로 정비부담 해소	③ 창구 일원화
5	정비시간단축, 가용성	⑤ 예방정비
6	국방부 역할 강화	⑥ 통제기관 역할

따라서 2018년 국방부 주관 유지보수 시범사업에서 드러난 긍정적인 내용과 사용자가 요구한 6개의 변수들을 분석함으로써 유지보수의 발전 방향을 정할 수 있었다.

Ⅴ. 유지보수 발전 방향

5.1. 국방 암호장비 정비조직 유지보수체계로 개편

정비업체가 유지보수에 관한 업무를 담당하게 됨으로써 정비업체와 군의 정비관의 업무가 일부 중복되게 된다. 따라서 가뜩이나 부족한 암호인력이 축소될 우려가 있다. 군은 암호체계를 관리 및 운영하면서 암호장비정비관[12] 및 전임암호사로 분리 운영하고 있다. 그들은 앞서 언급된 바와 같이 과중한 업무로 피로도가 높은 상태이나, 이러한 업무가 외부로 노출되거나 공개되지 못하고 있는 것이 현실이다. 업무의 공개가 암호체계나 암호기술에 직접적인 영향이 있기 때문이다. 따라서 암호장비정비관 및 전임암호사는 진급, 휴가, 포상 등으로부터 매우 인색하다. 국가 암호체계라는 이유로 관련 참모는 물론 지휘관까지도 암호업무 내용이 공개되지 않기 때문에 업무수행에 대한 공로를 인정받기 어렵다.

〈표 11〉 암호인력 재편(안)

구분	정보처 / 보안과	정보화 / 통신부대 참모부
육본	• 암호계획장교 : 중령(4급) • 암호관리장교 : 소령(5급) • 암호보안장교 : 준위 • 암호기술지원관 : 원/상사	• 암호장비 획득담당 : 4급 • 암호운영장교 : 준위 • 암호장비 운영담당관: 원/상사
지작사, 2작사	• 암호정책개발장교 : 소령(5급) • 암호관리장교 : 준위	• 암호운영장교: 준위, • 암호키관리담당관: 부사관(원/상사) • 암호 유지보수담당: 6급, 7급
군단	• 암호보안장교 : 준위	• 암호운영장교 : 준위, • 암호키관리담당관: 부사관(원/상사) • 암호유지보수담당 : 7급, 8급
사/여단	• 암호보안장교 : 준위	• 암호운영관: 부사관(상/중사) • 암호유지보수담당 : 9급
연대급	-	• 암호담당관(중/하사)
지역정비소 (노드부대)	-	• 준위, 상/중사, 정비병(2), 암호병(2)

정비업체의 유지보수체계로 전환되면서 그동안 미흡해 왔던, 암호장비의 프로그램 관리와, 암호 key의 관리, 배부, 운영, 정비업체 등장으로 나타나는 품질보증활동, 검사, 성

주12) 암호장비 정비관 : 암호실에서 암호장비를 정비하는 사람.「국방정보보안 시스템업무훈령」 제 69조 정비, (2020.7.23.), 국방부, P50.

능평가, 시험, 정비업체 보안관리 등 개선된 임무와 부합되는 “암호 유지보수담당관”으로 직책명칭이 변경되어야 한다. 군의 특성상 직무는 직책명칭으로 엄격하게 이루어지기 때문에 수행업무와 직책명이 다른 경우 국방개혁 2.0의 효율성, 투명성 개념에 의해 직무분석을 통해 업무가 위축되거나 삭감되기도 한다.

따라서 부사관은 암호담당관, 정비관은 유지보수담당관으로 직책명칭을 변경하여 직책명에서 어떤 임무를 수행하는지 식별되게 하고, 정비업체와 직책이 중복되어 정비인력이 삭감되는 일이 없도록 〈표 11〉 안과 같이 재편성하여야 한다.

5.2. 정비업체 운영 개선 및 공공성강화

국방부「국방정보보안시스템 업무훈령」제47조에서는 “정비업체(유지보수전담기관)는 연구기관으로부터 기술이전을 받은 정보보안시스템에 한하여 정비할 수 있다.” 제15조 정비업체의 업무와 책임에서는 ‘운영유지단계의 RAM분석[13]’ 결과를 수요 군에 제공하도록 명시하고 있다.

따라서 연구기관인 국가보안기술연구소로부터 전체 암호장비의 기술이전을 받는 정비업체(유지보수전담기관)는 시험용 암호프로그램과 시험용 암호 key를 함께 이전되도록 제도적인 보완 장치가 필요하며, 운영유지단계의 RAM 분석은 신뢰도, 가용도, 정비도의 분석을 위한 ‘유지보수도’[14]으로써 “시스템이 고장 났을 때 시스템을 정비하여 그 성능을 원상복귀 시키는 일련의 과정을 분석하는 것을 말한다.” 따라서, 정비업체(유지보수전담기관)는 RAM 분석 결과를 사용부대가 알 수 있도록 전달하도록 유지보수 제안요청서에서 명시하여야 한다.

정비업체(유지보수전담기관)은 효율성, 전문성, 보안성을 확보하기 위해서는 유지보수 업체의 공공성이 확보되어야 한다. 현재 암호장비 제작업체는 대부분 영세하여 재정난을 이유로 중도에 암호장비 제작업체를 포기하거나 도산 등으로 이어져 운용 중인 암호장비의 부품 구입 및 정비에 큰 제한요소를 경험 하였다.

따라서 정비업체(유지보수전담기관)도 예산규모가 크지 않아서, 영세한 업체가 유지보수업무에 참여하고 있어 중도에 포기하거나, 도산함으로서 운용중인 암호장비의 유지보수 업무가 원활하게 수행하지 못할 가능성이 높다.

따라서 정비업체를 복수업체로 지정하여 업체 간 상호 건전한 경쟁을 통하여 우수한 기술 및 양질의 서비스를 제공받을 수 있도록 하거나, 국방부에서 운영되고 있는 정보화 유지보수 전담기관이 암호장비 유지보수까지 맡는 방안이 필요하다.

Ⅶ. 결 론

암호기술의 미래는 양자암호 체계로 전환을 앞두고 있다. 시대적 환경 변화에 군이 암호장비 정비체계를 유지보수체계로 전환하는데 적극적으로 공감한다. 이런 변화에는 각 군에서 묵묵히 암호업무에만 전념해온 암호사들의 끈질긴 노력의 결과이다. 동시에 암호장비 사용자들의 간절함이 담겨져 있다.

그동안 소홀하였던 암호장비 정비체계의 중요성이 다시 주목을 받기 시작하였다. 정비업체에 의한 유지보수 사업을 통해 사용자의 인식이 크게 변화되었고 유지보수의 중요성에 대해 다양한 공감대가 형성되었기 때문이다. 유지보수체계로 전환에 대한 군의 만족도는 92.8%로 유지보수체계로의 전환이 절실함을 증명하였다. 특히 제작업체의 도산에 대비할 수 있고, 전·평시 암호장비의 안정적 지원으로 군은 전투임무에만 전념할 수 있게 된다.

미래 암호장비는 하드웨어적이 문제는 점진적으로 줄어들어 정비의 대상이 소프트웨어의 상호연동 기술과 안티템퍼(Anti-Tamper)[15]기술의 발전을 통한 정보보호 기술로 변화가 예상된다. 현재 우리는 스마트 전자화 시대를 거치면서 자율주행자동차, AI를 이용한 주거환경의 변화 등 Deep Learning에 의한 상용화 기술을 직접 접하고 있다. 따라서 미래의 국방 암호장비의 운영환경이 유지보수체계로만 정체

주13) 램(RAM) 분석(Reliability, Availability, Maintainability Analysis) : 어떤 체계의 고장 빈도, 정비 업무량 및 전투 준비 태세 등을 측정하는 척도. 공학 분야에서 RAM은 신뢰도(Reliability), 가용도(Availability), 정비도(Maintainability)의 약어로서 장비의 기본 임무 수행 능력 이외의 성능을 나타내는 기준이 되며, 연구 개발 시부터 폐기 시까지 분석되고 평가된다.

주14) 출처 : 최광석. (2017). “도시철도 2호선 전기식 도어시스템의 RAM분석을 통한 유지보수 적용 연구” . 서울과학기술대학교 석사학위 논문.

주15) 안티템퍼(Anti-Tamper) : 변조 방지는 개념적으로 장치에 대한 무단 액세스 또는 보안 시스템 우회를 방해하거나 억제하거나 감지하는 데 사용되는 방법론으로 암호체계의 노출을 방지하는 물리적, 전자적 기술을 말함, 위키백과사전, https://en.wikipedia.org/wiki/Tamperproofing, 2020.11.6.

되지 않고 지속적으로 발전하기 위해서는 끝임 없이 노력하여야 하며, 시스템을 보완하기 위해 두 가지의 국방정책을 제안한다.

첫째, 암호장비 유지보수전담기관 지정이 필요하다.

암호장비의 사용자 및 관리자들의 시대적인 욕구를 충족시키고 암호장비가 타 정보통신 유지보수 수준으로 도약하기 위해서는 아직도 많은 부분의 제도와 시스템이 개선되기 위해서는 정형화된 암호장비의 업무체계의 정착이 요구된다.

현재의 정비업체로 유지보수 업무의 전환은 당면한 문제점을 해결하는 것에 불과하며 미래의 정보통신 기반체계의 NCW[16]로의 전환과 암호장비의 소형화 또는 형상이 없는 소프트웨어(KCMVP[17] 등) 형태로 진화되면서 미래 통신 구조는 양자통신, 양자암호로 변화되는 업무에 대응이 제한될 것으로 예상이 된다.

특히, 암호장비를 전담기관으로 지정하여야 하는 이유는 「국방정보화업무훈령」 제189조(전담기관 지정 분야 및 운영 원칙)에 따르면 "군사비밀자료를 포함하여 보안을 요하는 정보시스템 유지보수 및 기술지원에 관한업무에 한하여 정보화 정책개발, 사업추진 및 국방정보 자원관리 지원을 통해 일관성 있고 체계적인 업무 추진, 책임성 보장, 예산의 효율적 집행을 통해 그동안 낙후 되어왔던 암호장비 관리 및 운영체계를 시대적 상황에 맞게 개선함으로서 국방 데이터 및 군사비밀, 주요자료의 유통을 보장"하기 위함이다.

둘째, 유지보수 운영지침 마련이 필요하다.

유지보수체계에서는 다양하게 요구를 하는 사용자 및 관리자들의 욕구를 충족시키고 암호장비의 운영이 타 정보통신 수준으로 유지되도록 제도와 시스템이 함께 개선되어야 한다.

유지보수체계로 전환은 그동안 경험하지 않았던 새로운 업무의 시작이다. 따라서 관련 훈령을 포함하여 새로운 형태의 유지보수체계운영지침이 마련되어야 할 것이다.

유지보수의 운영지침은 기존의 「국방정보화 업무훈령」 제189조(전담기관 지정 분야 및 운영 원칙)과 더불어 상호 호환되도록 작성되어야 한다. 기반체계 유지보수 업무와 암호장비 유지보수가 따로 분리되어서 현재의 상호운영성에 문제가 발생하지 않도록 상호보완이 되어야 한다.

본 연구의 한계점으로는 암호장비 정비체계를 어떻게 개선할 것인가에 대해 연구자의 경험과 암호전문가 그룹의 주관적인 관점으로 연구가 진행된 점이다. 연구를 진행함에 있어서 우선 암호장비 정비체계 관련 자료를 다양하게 조사를 해 보았으나, 국방 암호장비 정비기술에 대한 연구를 찾아볼 수가 없었고, 특히 외국군의 사례에도 학문적인 암호체계의 기술의 논리 이외 암호정비기술의 운영관리 분야에 관한 연구는 매우 부족하였다. 그동안 암호장비의 연구는 국가용 비밀이라는 이유와 암호정비기술의 접근이 어렵기 때문인 것으로 판단된다. 따라서 본 연구에서는 국가 암호체계와 관련되지 않는 범위 내에서 연구자가 직접 경험한 내용과 암호전문가 그룹을 대상으로 수행한 Field Study 방법으로 암호장비의 운영과 정비체계에 대해 연구를 진행하였으며, 또한 일부 정비기술에 대해 상세히 언급할 수 없는 한계가 있음을 밝힌다. 향후 암호장비 정비에 대한 기술적인 연구결과를 얻기 위해서는 좀 더 다양한 관점에서 깊이 있는 연구가 필요하다.

주16) NCW : Network Centric Warfare(네트워크중신전), 다음 백과사전, https://100.daum.net/search/entry?q=NCW, 2021.4.21

주17) KCMVP : 다음블로그, 행복하자, 암호검증 모듈(Korea Cryptographic Module. Validation Program: KCMVP): 전자정부법 시행령 제 69조와 [암호모듈 시험 및 검증지침]에 의거, 국가·공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않은 중요 정보의 보호를 위해 사용되는 암호모듈의 안전성과 구현 적합성을 검증하는 제도, ,https://swiftcam.tistory.com/292, 2020.12.8.

참고문헌

1. 연구논문

1) 김홍태·이문식·강순부. (2014). “군사분야 비밀자료 관리를 위한 암호 알고리즘”. 『융합보안 논문지』, 제14권 제6호. p.121-128.
2) 남길현. (2001). “암호기술과 PKI(공개키 기반구조)의 군사적 응용” . 『敎授論叢』. 21권. p.15-42.
3) 방대선·박효선. (2019). “한국군 군수지원체제 변화요인에 관한 연구”. 『군사연구』, 제148호. p.201-230.
4) 송원석·강성문·이민우. (2020) “함정용 통합 암호장비의 물리적 표준화 대상 및 요건 제안”. 『종합학술대회 논문집』, 제24권 제1호. 서울: 한국정보통신학회. p.96-98.
5) 이성윤·홍석진. (2005). “종합군수지원(ILS) 실태진단 및 발전방안”. 『국방정책연구』, 제70호. 서울: 한국국방연구원. p.35-58.
6) 윤은준. (2012). “군사 목적의 대용량 자료 암호화를 위한 ECC 기반 암호시스템”. 『합동학술대회 논문집』, 제8회. 서울: 제어로봇시스템학회. p.701-705.
7) 이영욱. (2016). “전력지원체계의 종합군수지원”. 『연구 융합보안 논문지』,제16권 제3호. p.77-85.
8) 정상윤·박태훈. (2003). “합동전장 모의모델 개발 방안”. 『국방정책연구』, 제59권. 서울: 한국국방연구원. p.9-27.
9) 정정묵. (2014). “공공기관의 정보시스템 유지보수에 영향을 미치는 요인에 관한 실증적 연구”. 숭실대학교 박사학위 논문.
10) 정선현·한근희·임채호·변옥환. (1998). “암호화 장비 구현 연구”. 『한국통신학회 워크샵』. 서울: 한국통신학회. p.9.
11) 최광석. (2017). “도시철도 2호선 전기식 도어시스템의 RAM 분석을 통한 유지보수 적용 연구” . 서울과학기술대학교 석사학위 논문.
12) 최준·강성문·최인수. (2015).“美軍 암호장비 현황 및 상호운용성 전략”. 『정보보호학회지』, 제25권 제2호. 서울: 한국정보보호학회. p.58-63.

2. 관련교범 및 서적

13) 성태제·시기자. (2021).『연구방법론 (3판)』. 학지사.
14) 국방부. (2020).『국방보안업무훈령』. 국방부.
15) 국방부. (2020).『국방정보보안시스템 업무훈령』. 국방부.
16) 국가정보원. (2020).『국가정보보안기본지침』. 국가정보원.
17) 국방부. (2021).『국방 정보화업무 훈령』. 국방부.
18) 육군본부. (2020).『201 군사보안 규정』. 육군본부.
19) 육군본부. (2016).『야전교범 운용-6-11, 군수업무』. 육군본부.
20) 김호근. (2018). 『군사정보 용역연구관 : 국방 암호장비 정비체계 개선 성과분석』. 국방부.
21) 김호근. (2017).『군사정보연구 용역과제(암호장비 유지보수전담기관 적용대비 효율적인 적용방안 연구』. 국방부.
22) 박승기. (2009).『암호장비 운영관리지침』. 육군본부.

3. 인터넷 및 블로그,

23) 이윤찬. (2007.4.23.). “국방예산 ‘평펑’ 암호장비는 ‘엉망’”. 『이코노미21』[온라인]. http://www.economy21.co.kr/news/articleView.html?idxno=58137. (검색일: 2020.11.27.)
24) 원병철. (2016,10,10.). “北 보안위협 높아지는데 군 암호장비 일부‘먹통’”. 『보안뉴스』(언라인). https://www.boannews.com/media/view.asp?idx=52012&direct=mobile. (검색일: 2021.3.2.)
25) 경대수. (2016.10.7.). “軍 암호장비 먹통!! 뻥 뚫린 군사기밀”. 『경대수의원실 [보도자료]』[온라인]. https://blog.naver.com/dskyung79/220830125226. (검색일: 2020.11.27.)
26) 다음 백과사전. “유지보수”. https://100.daum.net/search/entry?q=%EC%9C%A0%EC%A7%80%EB%B3%B4%EC%88%98. (검색일: 2021.3.13.)
27) 다음 백과사전. “야전정비”. https://100.daum.net/search/entry?q=%EC%95%BC%EC%A0%84%EC%A0%95%EB%B9%84. (검색일: 2021.3.13.)
28) 다음 백과사전. “연구소기업”. https://100.daum.net/search/entry?q=%EC%97%B0%EA%B5%AC%EC%86%8C%EA%B8%B0%EC%97%85. (검색일: 2021.4. 7.)
29) 국방과학기술용어사전. “네트워크중심전(NCW)”. http://dtims.dtaq.re.kr:8070/search/list/index.do. (검색일: 2021.4.21.)
30) 다음 백과사전, “양자암호통신”. https://100.daum.net/search/entry?q=%EC%96%91%EC%9E%90%EC%95%94%ED%98%B8%ED%86%B5%EC%8B%A0. (검색일: 2021.4.21.)
31) 국방과학기술용어사전. “작전운용성능(작전요구성능)”. http://dtims.dtaq.re.kr:8070/search/list/index.do. (검색일: 2020.11.20.)
32) 국방과학기술용어사전. “램 분석”. http://www.linetecheng.co.kr/theme/business/html/business/02.php. (검색일:020.11.20.http://dtims.dtaq.re.kr:8070/search/list/index.do. (검색일: 2020.12.8.)
33) 국방과학기술용어사전. “치명도분석”. http://dtims.dtaq.re.kr:8070/search/list/index.do. (검색일: 2020.12.8.)
34) 위키백과사전, “안티템퍼(Anti-Tamper)” https://en.wikipedia.org/wiki/Tamperproofing. (검색일: 2020.11.6.)
35) 라인테크이엔지. “종합군수지원”. http://www.linetecheng.co.kr/theme/business/html/business/01.php(검색일: 2020.11.20.)