ISSN 1976-5967
제12권
2019년 12월

군사과학정책연구

Military Science & Technology Annual Report

연구논문

RINSA
국 방 대 학 교
국가안전보장문제연구소

ISSN 1976-5967
제12권
2019년 12월

군사과학정책연구

Military Science & Technology Annual Report

국방대학교 국가안전보장문제연구소

목 차

연구보고 2019

한반도 주변국의 안보분야 운영분석기법 활용사례 연구

조 남 석

2019. 12.

국방대학교 국가안전보장문제연구소

목 차

그림목차

표 목 차

요 약 문

본 연구는 한반도의 주변국 중 미국 그리고 영국의 국방 및 안보분야에서의 운영분석 기법의 활용 사례를 소개하고 있다. 미국은 수많은 연구를 통해 운영분석 기법을 발전시켜왔고 여러 전쟁/전투를 통해 실제로 운영분석 연구를 현장에 적용한 경험이 가장 많은 국가이다. 거기에는 찬란한 성공의 경험도 있고, 뼈아픈 실패의 경험도 있다. 영국은 운영분석 기법의 선구자로서 2차 세계대전 시 많은 성공사례를 가지고 있고 그 지식과 철학을 미국에게 고스란히 전해주었다. 최초 연구의 대상이었던 일본의 운영분석 연구 사례는 관련 연구의 양적 부족으로 보고서의 범위에서 제외하였다.

본 연구는 운영분석의 학문적 태동기부터 2000년이 되기 전까지의 사례들을 시간의 순서에 따라 기술하고 있다. 운영분석 연구의 여러 토픽들로 보고서의 뼈대를 잡아 기술하는 것도 하나의 대안이었지만 그 보다는 독자들이 시간의 흐름에 따라 운영분석 연구자 그리고 조직의 노력과 어려움을 함께 경험할 수 있는 것이 더 좋겠다고 판단하였다.

잘 알려진 운영분석의 연구자, 연구소, 그리고 군의 운영분석 조직들이 어떻게 국방 및 안보 분야의 문제를 풀기 위해 노력해 왔는지를 중점적으로 기술하였으며 그러한 노력 끝에 탄생한 그들의 연구물의 성과도 함께 평가하였다. 보고서의 흥미를 위해 시대의 배경이 되었던 여러 가지 사건은 설사 그것이 운영분석 기법과 크게 연관이 있지 않더라도 포함하였다. 또 성공사례와 실패사례를 함께 소개하여 독자들이 필요한 교훈을 얻을 수 있도록 하였다.

마지막 장에서는 우리 군의 운영분석 발전을 위한 다양한 시사점을 기술하였다.

본 연구보고서는 기본적으로 여러 도서, 보고서, 논문 등을 리뷰하여 작성되었다. 그 중 가장 큰 참고가 되었던 자료는 미 육군에서 발행한 Charles R. Shrader 박사의 History of Operations Research in the United States Army 1권, 2권, 3권이었다.

본 연구보고서를 통해 일반 독자들은 의사결정 지원을 돕는 도구로서의 운영분석 학문에 대한 우수성을 체감하고, 운영분석 전문가들은 주변국의 운영분석 연구 사례 및 성과 등을 학습하여 본인의 연구 및 실무에 도움을 받을 수 있기를 기대한다.

1. 연구개요

1.1 연구 배경 및 필요성

운영분석 기법의 성공적인 활용사례는 많이 알려져 있다. 5천만 달러의 손실을 내고 있던 정유회사(CITGO)가 공정 과정의 최적화를 통해 일 년 만에 7천만 달러의 이윤을 기록한 사례, 샌프란시스코 경찰이 순찰 경로의 스케줄링을 통해 연간 17만 시간(Man Hour)를 창출한 사례 등[1] 다양한 분야에서 효율적인 경영을 위한 기법으로 인정받고 있다. 하지만 국방 및 안보 분야에서의 운영분석 기법 활용 사례는 많이 알려져 있지 않다. 운영분석이 제 2차 세계 대전 시 영국군의 레이더 배치 문제로부터 시작되었고 큰 성공을 거둔 후 다른 나라 및 다양한 분야에 전파되었다는 정도로만 알고 있을 뿐 학문의 구체적인 발전 역사 및 성과에 대해서는 잘 알지 못하는 것이 대부분이다.

안보 및 국방 분야에서의 의사결정은 국방 자원(예산, 무기, 인력 등)의 방대함과 의사결정이 미치는 파급효과(전투·전쟁의 승패, 전쟁 억지력 제공 등)를 고려했을 때 민간분야에서의 의사결정보다 더 중요하다고 할 수 있다. 군은 효율적인 국방 경영, 방위력 개선 등을 위하여 많은 분석기관을 두고 다양한 과학적 기법을 활용하여 의사결정을 지원하고 있다. 예를 들어 지난 43년간 우리나라 육군에서 분석업무를 하면서 활용한 방법론의 횟수와 비율은 아래와 같다.

〈표 1-1〉 육군의 분석업무 시 활용한 방법론[2]

방법론	횟수	비율(%)
특정 모델 사용 (CASAGE 등)	72	38.5
비용 대 효과 분석	57	30.5
AHP	29	15.5
시뮬레이션	10	5.3
비용 대 편익 분석	6	3.2
회귀 분석	4	2.1
PERT, TOPSIS	4	2.1
델파이, SWOT	3	1.6
최적화	2	1.0

1) 홍성필, 경영과학, 율곡출판사, p. 22
2) 조남석, 최적화 이론의 국방분야 적용 방안, 군사과학정책연구 제 10권, 2017

〈표 1-1〉은 그 동안 군(육군)이 어떤 방법론을 주로 사용해 왔고 또 어떤 방법론을 많이 활용하지 못했는지를 보여주고 있지만, 현실의 어떤 문제를 풀기 위해 그 방법론을 활용했는지, 그리고 결국 어떤 성과를 달성했는지는 설명하고 있지 않다. 우리는 본 연구를 통해 한반도 주변국의 운영분석(Operations Research) 기법의 실제 활용사례를 설명하고 사례별로 연구결과가 작전 및 국방 운영에 어떤 영향을 미쳤는지를 조사한다. 마지막으로 이를 통해 도출할 수 있는 우리의 시사점에 대해 논의한다.

1.2 연구목표 및 범위

본 연구의 목표는 아래와 같이 요약된다.

1) 한반도 주변국의 안보분야 운영분석기법 활용사례 조사 : 본 연구의 가장 중요한 목표로서 한반도 주변국 (미국, 영국 등) 의 운영분석 연구 중 안보 및 국방 분야와 연관된 연구를 조사한다.
2) 시사점 도출 : 1항에서 조사된 내용들을 바탕으로 현 우리 국방 및 안보 발전에 필요한 다양한 시사점을 논의한다.

다만, 조사의 대상이 되는 한반도 주변국을 미국과 영국으로 한정하여 연구를 진행하였음을 밝힌다. 먼저 중국, 러시아는 한반도 주변국으로 그 영향이 크고 중요하지만 자료의 접근성, 공개된 연구의 영어 원문 제공 여부 등을 고려하여 연구의 범위에서 제외하였다. 최초 연구의 제안 시 연구의 범위에 포함되었던 일본 역시 최종적으로는 보고서에 반영하지 않았다. 일본의 안보 및 국방 분야 운영분석 연구사례 조사를 위해 저자는 영어 원문 서비스를 제공하는 Journal of the Operations Research Society of Japan의 과월호 중 군사 분야의 토픽을 다룬 논문을 찾고 그 내용을 분석하였다. 하지만, 그러한 연구물의 수가 많지 않아 분석이 제한되었다. 몇몇의 단편적인 연구 결과를 일관성 없이 나열하는 것은 본 연구의 취지와도 일치하지 않는다는 판단을 하였다. 일본의 운영분석 연구 소개를 범위에서 제외하였지만 그 대신 영국의 운영분석 연구 사례를 포함하였고 미국의 운영분석 연구 사례를 보다 더 자세히 다루기로 결정하였다.

1.3 연구의 방법 및 기대효과

연구는 기본적으로 기존 연구논문을 리뷰하는 방식으로 진행한다. 이를 위해 다양한 기간의 많은 논문을 조사하며, 논문 발간 당시의 해당국의 안보 환경의 대내외적 변화를 파악하기 위하여 뉴스, 인터넷 자료와 같은 내용 또한 조사한다. 본 연구는 기존 연구의 리뷰가 중점이 되는 연구로서 다양하고 광범위한 자료 조사가 우선시 되며, 자료의 획득이 완료된 후에는 보고서의 논리적 연결성에 중점을 두고 연구를 진행하였다.

본 연구를 통해 독자들은 운영분석이 하나의 방법론으로서 국방 및 안보분야에 어떻게 기여해 왔는지를 이해하고 기법의 우수함 또한 알 수 있게 될 것으로 기대한다. 모든 학문은 명암이 있기 마련이다. 따라서 운영분석이 해당국의 국방 발전을 위해 기여한 점 뿐 아니라 실패한 사례 역시 보고서에 포함하여 소개한다. 이를 통해 독자는 향후 자신의 연구 및 업무에서 어떻게 운영분석 방법론을 잘 사용할 수 있을지에 대한 아이디어를 가질 수 있을 것이다. 본 보고서의 독자는 크게 운영분석 기관의 실무자, 운영분석을 공부하는 학교 기관의 학생 및 교수, 운영분석 방법론을 활용하는 연구자, 그리고 야전 실무에서 과학적 의사결정을 발전시키고 싶은 일반 독자로 구분할 수 있을 것이다. 각 독자들에 대한 저자의 기대효과는 다음과 같다.

1) 운영분석 기관의 실무자 : 현재 우리 군의 운영분석 기능 편성(조직/인력)은 다른 선진국의 그것과 크게 다르지 않다. 우리 군의 조직은 아마도 초창기에는 선진국(미국)의 조직 편성을 많이 참고하였고 그 이후 우리 실정에 맞게끔 조직과 인력을 조정해 왔으리라 생각한다. 운영분석 선진국들은 운영분석 기능을 잘 발휘하기 위해 끊임없이 고민하고 또 조직과 임무를 개선해 왔다. 본 보고서는 선진국 운영분석 조직들의 흥망성쇠를 최대한 다루고자 하였다. 다른 국가 조직의 역사를 이해함으로서 곧 우리 조직의 역사를 이해하는 시각을 갖출 수 있기를 기대한다.

2) 교육 기관의 교수 및 학생 : 군사 운영분석을 교육하는 많은 기관의 교육자들 또는 학생들이 느끼는 어려움 중 하나는 연구하는 토픽의 문헌을 찾아서 리뷰

하는 일일 것이다. 해당 토픽의 최신 연구 동향을 파악하는 것만큼 중요한 일은 그 토픽에 대한 연구의 뿌리를 찾는 일이다. 예를 들어 비용 대 효과분석을 연구하는 경우 그 연구가 언제 어떠한 배경으로 시작이 되었고 어떤 과정을 거쳐 학문적으로 발전해 왔는지를 알 수 있다면 현재의 연구에 큰 도움이 될 것이다. 본 연구 보고서는 많은 운영분석 토픽들의 발전 과정을 담고 있고 교육기관의 운영분석 연구자들에게 도움이 될 것으로 기대한다.

3) 야전의 일반 지휘관 및 참모 : 본 보고서는 운영분석을 학문으로 공부하지 않았거나 또는 운영분석 기관에서 실무자로서 근무한 경험이 없는 일반 지휘관 및 참모에게도 도움을 주고자 하였다. 운영분석 기능은 현장의 지휘관 및 참모들의 의사결정을 돕는데 그 주 목적이 있다. 또한 운영분석은 그 동안 그러한 현장의 소요를 연구하면서 학문적으로 발전해 왔다. 일반 독자들은 본 보고서를 통해 국방 및 안보 분야에서 지휘관 및 참모들이 어떤 문제를 과학적 기법으로 해결하고자 했으며 또 그 성과는 어떠했는지를 설명하고 있다. 보고서는 운영분석 연구 사례를 다루고 있지만 수리적이거나 공학적인 내용은 포함하고 있지 않기 때문에 일반 독자들에게도 쉽게 읽힐 수 있고 그래서 도움이 될 것으로 기대한다.

2. 영국의 운영분석 기법 활용사례

2.1 개요

미 국방부(DOD, Department of Defense)에서 발간한 군사용어사전 상 운영분석에 대한 정의는 아래와 같다 [3].

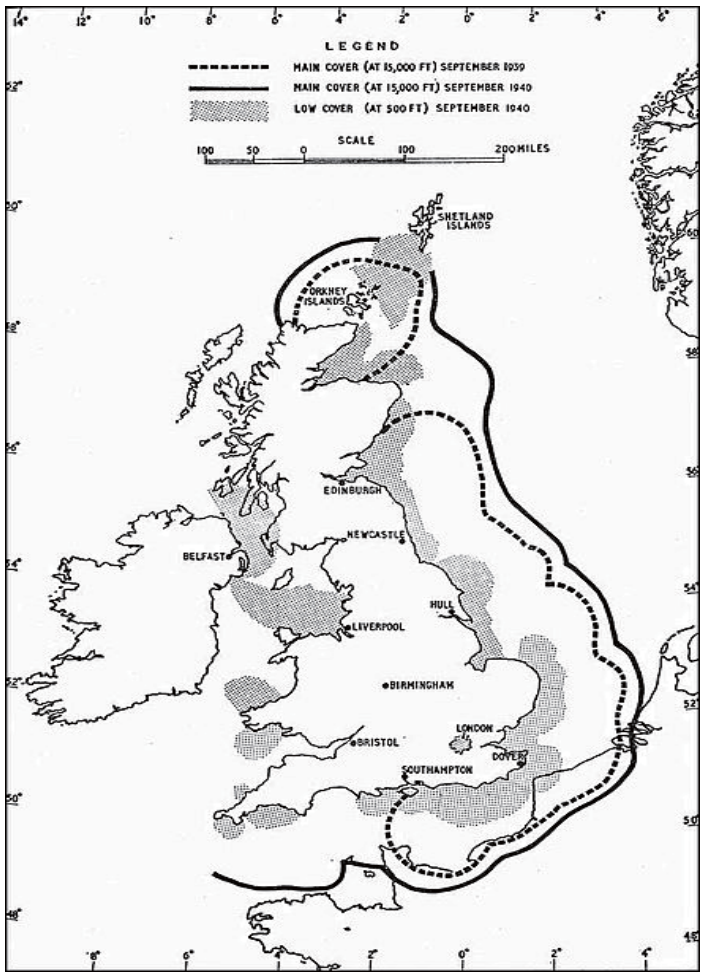
The analytical study of military problems undertaken to provide responsible commanders and staff agencies with a scientific basis for decision on action to improve military operations.

정의에 따르면 운영분석은 학문의 목적 자체가 국방의 문제를 해결하기 위함이며 군사 작전에서의 의사 결정에 대한 과학적 근거를 제공하고 있다고 밝히고 있다. 또한 그 수요자를 군의 지휘관과 참모부서로 정의하고 있다. 이처럼, 또한 이미 알려진 바와 같이, 운영 분석은 군의 작전을 보조하기 위해 시작된 학문이다. 따라서 운영 분석 방법론이 본격적으로 연구되기 시작한 학문의 태동기부터 시간의 흐름에 따라 활용 사례를 조사하는 것은 매우 의미 있는 일이다. 미국의 운영분석 기법 사례를 연구함에 있어 주로 활용된 자료는 2006년부터 2009년까지 미 육군 Office of the Deputy under Secretary of the Army에서 발행된 History of Operations Research in the United States Army이다. 총 3권으로 이루어진 책자의 저자인 Charles R. Shrader는 미 육군 보병장교로서 1987년 대령으로 전역하기 전까지 보병 장교로서 베트남 등에서 근무하였으며, 군 생활의 많은 시간을 미 육군사관학교에서 군의 전쟁 역사를 가르치는 역할을 수행하였다. 그는 수 없이 많은 군의 연구 보고서를 리뷰하고 관련 종사자들과 인터뷰를 하여 3권의 운영분석 '역사책'을 완성하였다. 본 보고서의 많은 부분이 Dr. Shrader의 책에서 발췌되었음을 미리 밝히나, 보고서의 내용이 본 책들에 대한 단순 번역 또는 요약은 아님을 밝힌다. 보고서 작성에 참조한 모든 자료는 보고서의 마지막 참고자료에 기술되어 있다.

2.2 제 2차 세계대전 시 영국의 운영분석 연구

미국의 전통적인 동맹국인 영국(Great Britain)의 첫 번째 운영분석 연구 사례는 적(독일군) 공습에 대한 레이더 배치 연구이다. 1934년 영국군의 최대 위협은 독일군의 폭격기였다. 영국군은 당시 해협에 많은 음향 경보 시스템을 갖추고 있었는데 영국군 장교이자 공학자였던 H. E. Wimperis는 이러한 경보 시스템이 무용지물임을 간파하고 새로운 기술을 도입한 조기 경보 시스템의 설치를 주장한다. Wimperis와 다른 여러 과학자들은 "Committee for the Scientific Study of Air Defense"라는 조직에 배치되어 적 공습에 대비하기 위한 다양한 수준의 공학적 연구들을 개시하는데 여기에는 "death ray"와 같은 SF 영화에서나 가능한 아이디어에서부터 오늘 날 레이더의 시초격에 해당하는 레이더 파(radar wave)를 측정하는 장비까지 논의된다. 중요한 것은 이러한 연구들을 통해 여러 이질적인 자산들(방공포, 지상관측수단, 아군 전투기 등)을 작전적 목표를 위해 효율적으로 통합 운용할 수 있는 연구들이 본격적으로 이루어 졌다는 것이다. 즉, 운영분석의 학문적 시작점은 효율적인 의사 결정을 지원하기 위한 다양한 자산의 운용 방안이라고 볼 수 있다.

1938년에는 이들이 이끄는 팀에 의해 여러 대의 레이더 기지를 실제 운용하는 훈련이 이루어졌다. 흥미로운 점은 훈련 당시 영국군은 레이더 기지를 기계적으로 운용하는 것은 이미 훈련이 잘 되었지만 여러 대의 레이더로부터 수집되어진 데이터를 효율적으로 활용하는 분석능력이 부족하여 어려움을 겪었다. 더구나 이들이 분석해야 할 정보는 겨우 5개의 레이더 기지에서 오는 정보뿐이었다. 빅 데이터를 다루는 지금의 기술정보 수준을 고려했을 때 불과 80여년 전 5개의 레이더 정보를 다루는 데 어려움을 가졌다는 점에서 학문의 발전 속도를 체감할 수 있기도 하다. 운영분석 팀은 전쟁이 발발한 후 2년 뒤인 1941년 영국 공군(RAF, Royal Air Force)에 통합되어 ORS(Operational Research Section)로 재창설된다. 이것이 군 조직의 공식적인 명칭에서 운영분석이 처음 등장하는 사례로 판단된다.



〈그림 2-1〉 1939-1940년 영국군의 독일공습에 대비한 레이더 커버리지 (출처: 위키피디아)

1941년 여름에는 공군에서만 운용하던 운영분석 조직이 공군 내 다른 조직, 육군, 국방성(Ministry of Home Defense) 등으로 확대되고 서로의 조직간 연락장교를 파견하는 등 운영분석 기능이 전 군으로 확대되기 시작한다. 1942년 당시 운영분석 기능에서 임무 수행을 할 수 있었던 장교의 숫자는 약 500여명이었지만 전쟁이 끝날 무렵 이 숫자는 2배 가량 증가하게 된다. 현재 50만 병력의 우리나라 육군 조직에서 운영분석 기능을 담당하는 960 특기 장교의 숫자가 약 100여명임을 감안해 보면 운영분석 기능이 전쟁 당시 영국군에서 많은 역할을 수행하였음을 짐작할 수 있으며 방법론의 중요성이 더욱 확대된 현 시점 우리 군의 운영 분석

기능이 많이 부족함을 알 수 있는 부분이기도 하다. ORS의 구성원으로는 주로 물리학자, 공학자, 그리고 수학자가 포함되었으며 소수의 생물학자, 지리학자, 통계학자, 심지어 예술학자 역시 포함되기도 하였다. 영국군의 이 임무를 수행하는데 있어 정작 중요한 것은 정형적인 과학 지식이 아니라 "과학적 사고방식(scientific mind)"을 갖추는 것임을 깨우치게 된다. 즉, 문제의 해결의 위해 가정을 수립하고, 실험을 하며, 대량의 데이터를 분석하고, 효율적인 해를 구성하는 일련의 절차들을 통섭적으로 해낼 수 있는 능력이라고 할 수 있다. 그럼에도 불구하고 ORS에는 각 분야의 최고 전문가들이 섭외가 되었는데 이는 참여자들이 운영분석 기능이 정부의 정책과 의사 결정에 가장 깊게 관여할 수 있는 학문이라는 것을 간파했기 때문이다.

〈그림 2-2〉 독일군의 암호를 해독한 앨런 튜링(Alan Mathison Turing) : 전쟁 당시 활약한 민간인 과학자들의 활약을 보여주는 예 (사진은 앨런 튜링에 대한 영화의 한 장면)

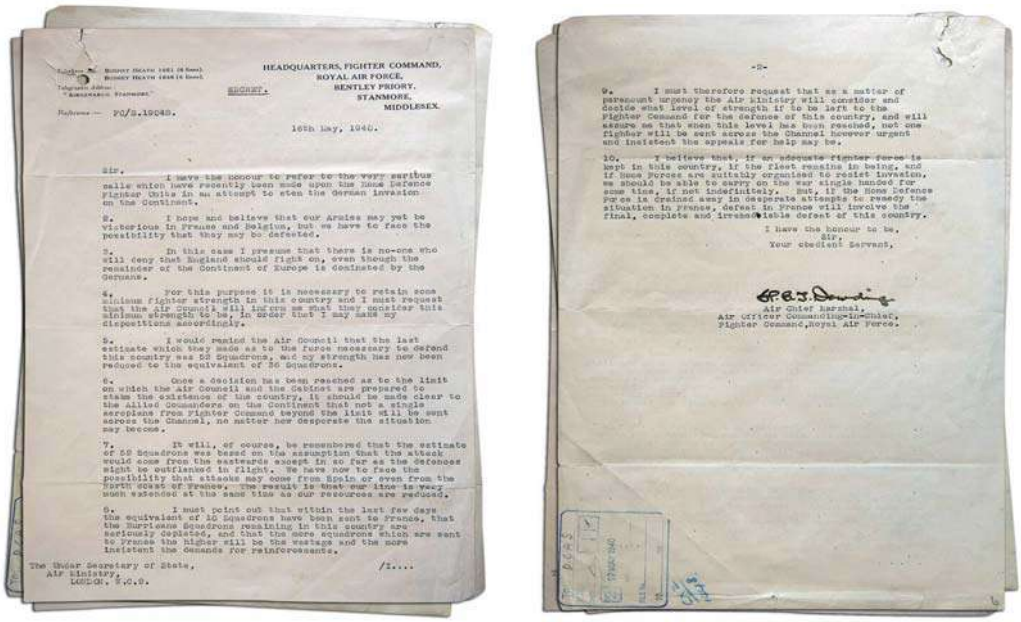
ORS는 기본적으로 전장에서의 지휘관 문제를 해결해 주었으며 부여받은 프로젝트는 지휘관이 제안하기도 하지만 대부분은 ORS의 자체 발제에 의해 연구가 시작되었다. 이들의 연구 환경은 보안상의 이유로 제약받지 않았으나, 전시 초기에는 군의 전술과 전략에 대해 과학자들이 개입하는 것에 대해 지휘관들이 반감을 가지고 이들을 배척(anathema)하기도 하였다. 하지만 군 장교들과 과학자들이 함께 일하는 시간이 늘어나면서 서로에 대한 신뢰를 바탕으로 이러한 배척은 사라졌고 과학자들은 자신들에게 주어진 특권(privilege)을 결코 남용하지 않았다. 결과적으로 ORS는 전쟁을 승리하는데 있어 크게 기여하였다고 평가받는다. 성공적으로 작전에 기여했다고 평가받는 주요 연구 주제는 다음과 같다.

〈표 2-1〉 2차 세계대전 시 영국군의 대표적인 운영분석 연구 주제

연구 주제
(1) integrated radar-based air defense system
(2) enemy bomber and escort tactics
(3) the most profitable use of weapons under various conditions
(4) The effects of weather and other factors on defensive air operations
(5) Research on transfer of additional aircraft and pilots to France
(6) Research on depth charge settings
(7) Planned Flying and planned maintenance
(8) Bombing accuracy : effect of given bomb on different types of targets, aeriel gunnery and the causes of bomber losses.
(9) The best deployment of the available guns and radar around London

연구주제 중 일부는 지금도 여전히 운영분석에서 연구되고 있는 것들이다. (9)번의 레이더 및 방공포 전개 문제는 여전히 활발하게 연구가 되고 있는 주제이며 지금은 정수계획법(Integer Programming)으로 구성하는 Set Covering Problem으로 문제를 해결하고 있다. 당시에 어떤 방법론을 활용하여 이 주제가 연구되었는지는 알려져 있지 않다.

이 중 (5)번 프로젝트는 1940년 전세가 불리해진 프랑스가 영국에게 공군의 원조를 요청한 것에 대해 과연 공군 전력을 보내는 것이 옳은 것인지 그렇지 않은지를 평가하기 위한 연구였다. 분석 결과 영국 공군의 파견은 자국의 위험을 증가시킬 수 있다는 결론이었고 당시 공군 지휘관은 이해하기 쉬운 그래프와 그림으로 보고서를 작성해 윈스턴 처칠에게 이를 잘 설명하였고 공군을 파견하지 않기로 하는 결정을 이끌어 낸다. 만약 이러한 과학적 분석 기능이 없었더라면, 또는 수학적 분석 결과를 비전문가인 처칠 수상에게 쉽게 설명하지 못했다면 처칠은 순전한 정치적 이해관계 등에 의해 결정을 내렸을지 모른다. 이처럼 운영분석은 전시에 높은 수준의 의사결정(higher-policy)에서도 그 기능을 활발하게 수행하였다. 〈그림 2-3〉은 영국의 RAF의 지휘관이었던 Dowding이 처칠 수상에게 보냈던 편지이다. 이 편지 2장이 영국 역사를 바꾸어 놓았다고 평가 받기도 한다.



HEADQUARTERS, FIGHTER COMMAND,
ROYAL AIR FORCE,
BENTLEY PRIORY,
STANMORE,
MIDDLESEX.

SECRET.

Ref. No. — FC/S.19049.

16th May, 1940.

Sir,

I have the honour to refer to the very serious calls which have recently been made upon the Home Defence Fighter Units in an attempt to sten the German invasion on the Continent.

2. I hope and believe that our Armies may yet be victorious in France and Belgium, but we have to face the possibility that they may be defeated.

3. In this case I presume that there is no-one who will deny that England should fight on, even though the remainder of the Continent of Europe is dominated by the Germans.

4. For this purpose it is necessary to retain some minimum fighter strength in this country and I must request that the Air Council will inform me that they consider this minimum strength to be, in order that I may make my dispositions accordingly.

5. I would remind the Air Council that the last estimate which they made as to the force necessary to defend this country was 52 Squadrons, and my strength has now been reduced to the equivalent of 36 Squadrons.

6. Once a decision has been reached as to the limit on which the Air Council and the Cabinet are prepared to stake the existence of the country, it should be made clear to the Allied Commanders on the Continent that not a single aeroplane from Fighter Command beyond the limit will be sent across the Channel, no matter how desperate the situation may become.

7. It will, of course, be remembered that the estimate of 52 Squadrons was based on the assumption that the attack would come from the eastwards except in so far as the defences might be outflanked in flight. We have now to face the possibility that attacks may come from Spain or even from the North coast of France. The result is that our line is very much extended at the same time as our resources are reduced.

8. I must point out that within the last few days the equivalent of 10 Squadrons have been sent to France, that the Hurricane Squadrons remaining in this country are seriously depleted, and that the more squadrons which are sent to France the higher will be the wastage and the more insistent the demands for reinforcements.

The Under Secretary of State,
Air Ministry,
LONDON, S.W.1.

/I....

-2-

9. I must therefore request that as a matter of paramount urgency the Air Ministry will consider and decide what level of strength if to be left to the Fighter Command for the defence of this country, and will assure me that when this level has been reached, not one fighter will be sent across the Channel however urgent and insistent the appeals for help may be.

10. I believe that, if an adequate fighter force is kept in this country, if the fleet remains in being, and if Home Forces are suitably organised to resist invasion, we should be able to carry on the war single handed for some time, if not indefinitely. But, if the Home Defence Forces is drained away in desperate attempts to remedy the situation in France, defeat in France will involve the final, complete and irremediable defeat of this country.

I have the honour to be,
Sir,
Your obedient Servant,

Air Chief Marshal,
Air Officer Commanding-in-Chief,
Fighter Command, Royal Air Force.

〈그림 2-3〉 전쟁의 역사를 바꾼 영국 공군 Dowding의 처칠에게 보낸 편지

또 하나의 성공적인 연구사례는 (6) 독일군의 유보트(U-boat)를 격침시키기 위한 폭뢰(depth-charge)의 폭발 수심에 대한 연구이다. 영국군은 폭뢰를 폭발시키는 방식으로 유보트를 제대로 공략하지 못하고 있었는데, 1939년부터 1941년 사

이에 이루어진 215건의 공격에서 단 한 척의 유보트를 격침시키는데 그쳤으며 심각한 피해를 입힌 것은 4%에 불과했다[5]. 운영분석 팀은 유보트의 평균 공격 수심을 추정하고, 유보트가 해표면에서 이탈하는 시간을 분석하여 근접 신관(proximity fuse) 방식의 폭뢰를 고안해 낸다. 이 연구의 결과로 1942년 7월부터 12월까지 단 6개월간 7대의 유보트를 격침시키는 등, 대 유보트 전투의 효율이 400%에서 700% 증가한 것으로 보고되었으며 이를 통해 영국 해안에서의 유보트 활동을 거의 중단시키는 작전적 성과를 달성한 것으로 평가받고 있다. 프로젝트에 대한 구체적인 설명은 M. W. Kirby의 저서를 통해 확인할 수 있다. [5] 비록 이러한 연구들이 대부분 현실의 문제를 해결하기 위한 응용 연구들이었지만 영국의 운영 분석 팀은 일반적인 방법론의 개발에도 힘을 썼고, 다양한 정리(Theorem)등을 발표하는 등 운영분석의 학술적 발전에도 기여하였다.

영국은 운영분석 연구의 선도자였다. 다양한 운영분석 연구가 전쟁의 승리에 크게 기여하였다고 평가하고 있다. 이후 전쟁에서의 운영분석 방법론의 성공 사례가 미국 그리고 전 세계적으로 전파되고 운영분석이 국방 뿐 아니라 사회 전반적으로 통용되는 과학 기법이 되는 중요한 계기가 된다.

3. 미국의 운영분석 연구 사례

3.1 개 요

미국의 운영분석 연구의 뿌리는 2장에서 논의된 영국군의 연구로부터 비롯되었다. 전통적인 동맹국인 미국과 영국은 군사 분야에서의 교류도 활성화 되어 있었고, 2차 세계대전 시 영국군의 운영분석 연구 성공 사례를 인지하고 있었다. 따라서 미국의 운영분석 연구 또한 제 2차 세계대전과 시간대를 함께 하고 있다. 본 장에서는 2차 세계 대전에서부터 시작하여 걸프 전쟁이 발발한 1990년대까지 이르는 미국의 운영분석 연구 사례를 조사 분석한다.

3.2 2차 세계 대전 시 미국의 운영분석 연구 사례

앞 절에서 밝힌 바와 같이 미국은 영국의 운영분석 연구 사례를 익히 파악하고 있었으며 1939년부터 다양한 정보를 교환하고 있었다. 하지만, 공식적으로 정부와 정부 간 협약을 통해 운영분석 연구가 대서양을 건너간 시기는 1940년 Tizard 임무를 통해서이다. Tizard는 영국 수상 처칠의 명을 받아 다양한 전시 운영분석 연구에 대한 미국과의 교류 활성화를 위해 파견되었고 여러 차례 방문을 통해 1940년 7월 미국 대통령 루즈벨트의 확답을 받기에 이른다. 미국의 과학자 및 군 관계자들은 영국의 성공적인 연구 결과물들에 고취되었고, 자국의 군사 기밀이 영국으로 흘러갈 수 있다는 일부의 반감을 극복하고 본격적인 공동 연구의 장이 마련되게 된다. 미국의 본격적인 운영분석 관련 조직은 전기공학 박사인 Bush를 조직의 장으로 하는 NDRC(National Defense Research Committee)와 그 후에 설립된 OSRD(Office of Scientific Research and Development)로 보인다. 이 두 국가 간 연구 협약은 정보의 교환에 그치지 않고 연락 사무소를 런던과 워싱턴에 각각 파견하는 등 본격화 되었고 이는 미국 내에서도 운영분석 연구의 활기를 가져와 미 육군과 해군 등 군 조직과 MIT(Massachusetts Institute of Technology) 등 민간학교에서도 연구소가 설립되기에 이른다.

〈그림 3-1〉 미국 MIT의 과학자들과 신기술에 대해 토의하고 있는 Henry Thomas Tizard (사진 가운데)
(출처 : MIT Museum)

미국 내에서 자체적인 운영분석 기능이 발전되기 시작한 계기는 일본의 진주만(Pearl Harbor) 공습이다. 1941년 행정명령 8807호에 의거 NDRC가 OSRD에 통합되고 국방에 연계된 과학 연구들을 연구하기 시작한다. OSRD의 수장인 Bush는 사실 조직에서 운영분석 기능이 크게 확대되는 것을 경계하였다. 이는 OSRD가 순수 과학을 연구하는 집단이며 운영분석 기능이 들어오게 되면 다양한 의사결정에 관여하게 되고 이는 결국 기초 과학연구에 좋지 않은 영향을 줄 것이라고 생각했기 때문이다. 이때 Bush의 철학은 순수과학 그 자체는 운영분석으로 대표되는 의사결정 과정에 큰 도움을 줄 수 있지만, 운영분석이 순수과학을 발전시키는 데 어떠한 역할도 하지 못할 것이라는 생각으로 가득 차 있었다. 하지만 그의 부하들은 효율적인 전쟁 수행을 위한 운영분석 기능의 기여 분야에 대해 의심이 없었고 운영분석 기능의 확장에 힘을 실어주기 시작한다. 1943년에 이르러, 결국 이 싸움은 Bush의 패배로 끝이 나고 OSRD는 새로운 조직인 OFS(Office of Field

Service)를 창설하며 군이 요구하는 다양한 연구를 받아들이게 된다. 일례로 OSRD의 하부 조직인 응용 수학 패널은 수학 이론의 발전에만 힘을 쏟지 않고 야전의 소요를 받아들여 폭격의 정확성을 연구하는데 수학과 통계기법을 적용시키기 시작한 것이다. 미국에서도 수학, 물리학과 같은 기초 과학이 전쟁의 승리에 기여하기 위한 움직임을 보이기 시작한 것이다. 〈표 3-1〉은 2차 세계대전 시 미군이 수행한 대표적인 운영분석 연구 주제들을 보여주고 있다.

〈표 3-1〉 2차 세계대전 시 미국군의 대표적인 운영분석 연구 주제

군	연구 주제
해군	(1) Techniques for sweeping for magnetic mines (German)
	(2) Offensive use of mines in the Pacific against Japanese
공군[3]	(3) Measuring the accuracy of visual formation bombing
	(4) Estimating the size of sighted ships (to discover the *Yamato*)
	(5) Effective methods for attacking moving ships from low altitudes using radar
육군	(6) Technical Research on weapons (quality, ballistics tables, etc.)
화학(병과)	(7) Estimating number of gas bombs to produce a minimum gas concentration over a specified area
의무(병과)	(8) Treating casualties and evacuating for medical equipment

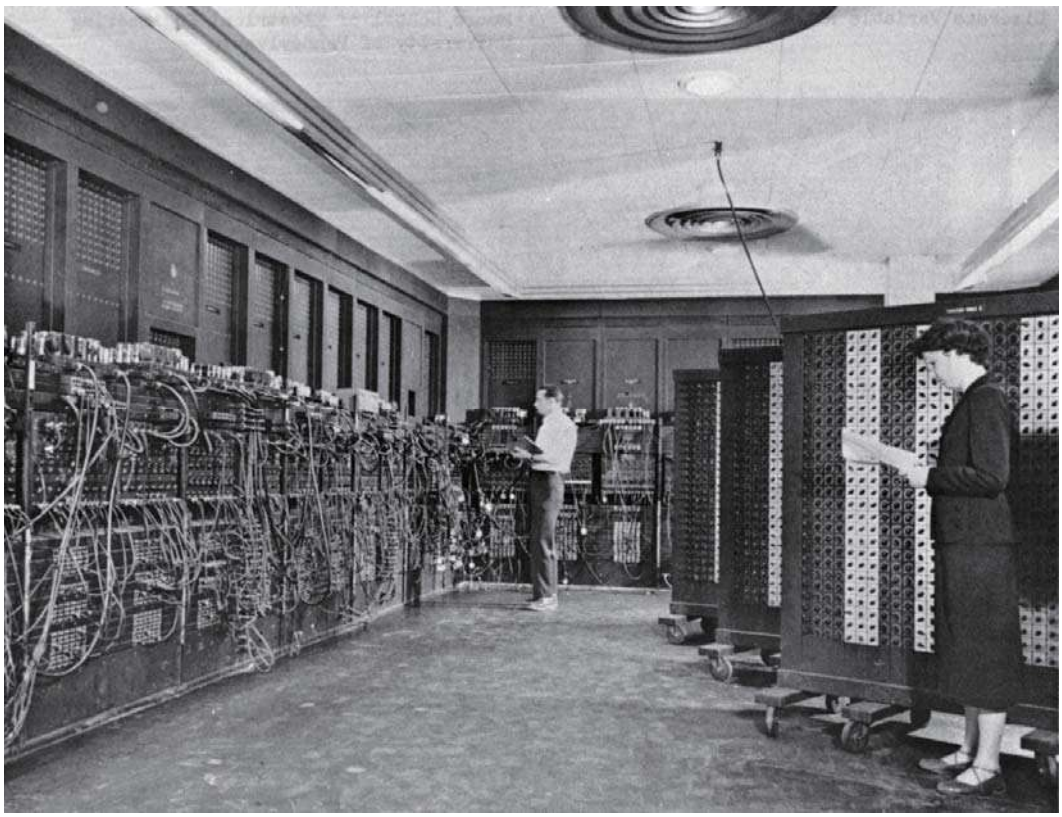
이 중 (2)번 연구의 성공에 힘입은 미국은 Operation STARVATION을 개시한다[6]. 1945년 3월에 시작된 이 작전에서 미 해군은 약 1,000여개의 낙하산 투하 방식의 기뢰를 태평양에 매설하였으며 이 작전으로 일본은 미국의 전략 폭격 그리고 잠수함 공격을 합친 것보다 더 큰 피해를 입었으며 군수물자 수송량이 85%나 감소하는 위기를 맞게 된다. 이 작전에 대한 보다 자세한 정보는 랜드 연구소의 보고서를 참조하면 된다[7].

3) 2차 세계대전 당시 미 공군의 정식 명칭은 AAF (Army Air Force)임.

〈그림 3-2〉 (좌) Operation STARVATION에서 기뢰를 투하하는 모습. (우) B-17 폭격기의 폭격 포메이션 (출처 : 위키피디아 / 위키미디아 코먼스)

(3)번은 미국 제 8 공군(Eight Air Force)의 운영분석 팀에서 수행하였으며 폭격기의 폭격 정확성을 향상시키기 위한 포메이션에 대한 연구였다. 이들은 작전계획 수립 시 전투기가 촬영한 항공사진을 사용하여 폭격지점(bombfalls)을 확인하였는데 이를 정찰기가 촬영한 항공사진으로 대체하였고 2개의 결정적인 변수(i.e., 폭격지점과 조준점의 거리(distance of center of bombfall from aiming point), 포메이션 패턴의 크기(pattern size))가 폭격의 정확성을 향상시키는 데 주요한 역할을 한다는 것을 파악하였다 [8]. 이 두 변수를 최소화 하는 포메이션에 대한 연구를 진행하였고 결과적으로 정면과 폭이 감소한(정면은 4,600피트에서 3,200피트로, 종심은 2,600피트에서 2,500피트로) 포메이션을 통해 폭격 작전의 60%의 효율성을 향상시킨 것으로 평가받는다. 이는 기존에 1,000개의 폭격기로 수행할 수 있는 임무를 250대의 폭격기로 대체할 수 있다는 것을 의미한다.

특정한 작전 목표를 달성하기 위해 시행된 해군과 공군의 연구와 다르게 미 육군의 연구는 무기 체계에 대한 기초적인 연구에 집중한 것으로 보인다. 〈표 3-1〉의 연구 (6)은 미육군병참부(The Army Ordnance Department)의 산하에 있는 BRL(Ballistic Research Laboratories)에서 주로 실시된 연구로 재래식 무기체계의 물리, 화학, 수학적 성질을 활용하여 무기체계의 개선, 품질 향상, 계산 방법, 그리고 무기체계의 성능 테이블을 만드는 등의 연구를 진행하였다. 이를 통해 다양한 무기 체계 시험평가 방법, 신뢰성 분석을 위한 통계학적 이론 등이 발전한 것으로 평가받는다.



〈그림 3-3〉 미국 BRL(Ballistic Research Laboratories)연구소에서 ENIAC(Electronic Numerical Integrator And Computer)을 이용해 연구를 하는 모습 (출처 : 위키피디아)

2차 세계대전 당시 미국의 운영분석 기능 역시 영국의 성공사례와 함께 전쟁의 승리에 크게 기여한 것으로 평가 받는다. 다만, 영국은 제한된 자원을 효율적으로 사용하기 위한 방법론에 집중하였다면 미국은, 영국에 비해 자원이 여유가 있었기 때문에, 새로운 기술과 방법론의 개발에 그 노력을 집중한 것으로 생각된다.

2차 세계대전 당시의 운영분석은, 결과적으로는 크게 흥행하였지만, 조직원을 모집하고 훈련시키는 인적 개발이 쉽지 않았다. 국방의 조직이 이익을 추구하며 조직 구성원에게 그만큼의 보상을 지급하는 민간 기업과의 경쟁에서 우위를 점하기 어려웠던 것이다. 또한 역사적으로 만난 적이 없었던 두 그룹, 민간 과학자와 군인의 갈등 역시 연구의 어려움이 되었다. 심지어 일부 민간 과학자가 스파이로 오해받는 일도 종종 발생했다고 하며, 민간 과학자들은 생소하고 경직된 군 문화에 적

응이 어려웠다. 이들의 문화 차이에서 오는 갈등은 시간이 지나면서 점차 해소되었고 이러한 상처마저도 전후 운영분석 기능의 발전에 큰 디딤돌이 되었을 것이라고 생각된다.

3.3 전후 미국의 운영분석 연구 사례

제 2차 세계대전이 승리로 돌아가고 여기서 중요한 역할을 수행한 운영분석 조직들은 역설적으로 조직의 크기를 줄여나가기 시작한다. 이는 큰 전쟁 직후 거대하고 현존하던 위협이 제거되고 나서 나타나는 자연스러운 현상으로 생각된다. 전시 고용되어 전쟁에서 큰 역할을 수행했던 민간 과학자들은 대부분 본인의 원 직장으로 복귀하였다. 위협이 사라진 군은 운영분석 조직을 재정비하기 시작한다.

전쟁에서 중요한 역할을 수행한 OSRD와 OFS는 새로운 조직원을 모집하기 시작하고, 해군은 MIT 대학을 향후 연구 파트너로 하여 지속 연구방안을 모색한다. 이러한 환경에서 1948년 미 공군(AAF)은 새로운 비영리 연구기관인 RAND 연구소를 설립한다. 지금까지도 미국 국방 및 안보 연구의 중심 역할을 하고 있는 랜드 연구소가 이때 창립된 것이다. 전시에 상대적으로 운영분석 연구가 뒤쳐졌던 육군은 여러 운영분석 조직을 창설하고 미국 존스 홉킨스 대학과 공동연구를 진행하는 등 발 빠르게 움직이기 시작한다. 지속적으로 감축되는 예산으로 OSRD는 해체의 수순을 밟고 1947년 NSF(National Science Foundation)으로 재창설되며 이로서 각 군은 전체의 통합된 운영분석 조직이 아닌 본인들의 고유한 운영분석 조직을 가지게 된다.

해군은 OEG(Operations Evaluation Group)라는 조직을 유지하고 확장시켰는데 한국 전쟁이 발발하기 전 40명의 과학자를 포함한 60명의 부원과 $500,000의 연 예산을 가지고 있었던 것으로 보고된다. 운영분석의 중요한 고전 연구 중 하나인 Morse와 Kimball의 Methods of Operations Research도 해군 OEG의 보고서(Report 54)로 처음 시작되었다[9].

공군은 해군과 다르게 중앙 집권화된 운영분석 조직이 아닌 분산된 조직의 형태로 기능을 유지하려 하였고 군사 정책, 계획, 기술 등을 모두 연구할 수 있는 프로젝트를 계획하며 이것이 RAND(Research AND Development) 연구소의 창설로 이어진다. RAND 연구소는 전시에 수행되었던 여타의 연구와 다르게 조금 더 이

〈그림 3-4〉 워게임 분석을 하고 있는 초창기 RAND 연구소의 모습 (사진은 1966년의 모습이다)
(출처 : 랜드 아카이브)

론적이고 정치, 경제 등 사회 전반에 걸친 고려요소가 관여된 연구에 착수한다.

미 육군은 전후 새로운 위협이 될 수 있는 소련을 견제하고 전쟁 능력을 전 세계적으로 투영할 수 있는 글로벌 이슈에 초점을 맞추고 ORO(Operations Research Office)라는 조직을 체계화 하여 무기체계와 장비 위주의 기초 연구를 시작한다. ORO와 미 육군의 새로운 연구 파트너 존스 홉킨스 대학이 이 시기에 실시한 주요 프로젝트는 〈표 3-2〉와 같다.

〈표 3-2〉 전후 미 육군의 대표적인 운영분석 연구 주제

프로젝트명	연구 내용
ANALAA	(1) development of anti-aircraft missiles
EVANAL	(2) analyze the performance of Army equipment under various environmental (especially, arctic)
MAID	(3) Potential value of U.S. military aid programs to foreign countries
ALCLAD	(4) individuals protection means from all known forms of warfare
GUNFIRE	(5) determine the nature and extent of existing deficiencies in equipment
POWOW	(6) scientific analysis and synthesis the effectiveness of weapons in psychological warfare
DONKEY	(7) analyze the use of surface to surface guided missiles
TREMABASE	(8) feasibility of transporting by air, sea, or land to maintain an advanced base
TEAM	(9) the most important factors in interpersonal relations
SITE	(10) the most effective methods for planning Army training
ATTACK	(11) evaluate on a continuing basis the use of atomic weapons
ARMOR	(12) methods of destroying enemy by the use of land mines

(4)번 연구는 다양한 형태의 전투에서 개인의 방호 장비를 어떻게 구성해야 하는지를 목표로 1948년에 착수한 연구로서 수없이 많은 전상자들의 데이터를 분석하는 것부터 시작되었다. 이 연구는 몇 가지 흥미로운 결론을 이끌어 내었는데 전투에서 적을 조준 사격하는 것이 무작위(랜덤)로 사격하는 것보다 크게 좋지 않다는 점을 분석하였고 이 연구결과를 토대로 미군이 소구경 연발사격의 장점을 갖기 위한 무기체계인 5.56mm 소총을 개발하는데 도움을 주었다 [10]. 이때의 연구결과

로 개발된 AR 소총은 향후 수 십년간 미 육군의 주력 소총으로 사용된 M16 소총의 개발로 이어진다.

그 외에도 개인방호 장비의 경량화 필요성, 훈련 간 방독면 착용의 필요성 등을 이끌어 내었다. 대부분의 소부대 전투는 300미터 이내에서 효력이 발생하며 대부분의 소총 살상은 100미터 이내의 교전에서 발생한다는 보병 장교들에게는 매우 친숙한 전투 교리 역시 이때 도출되었다. 이 연구가 중요한 또 하나의 시사점은 연구의 시작 당시 야전 지휘관들은 개인의 방호를 증가시키기 위해 강력한 방호장비가 필요하다는데 대부분 동의했다는 것이다. 하지만 데이터에 입각한 분석 결과 전혀 다른 결과, 개인의 방호는 오히려 경량화 되어야 한다는, 를 이끌어 내고 그것을 정책적으로 반영시켰다는 점이다. 〈표 3-2〉에서 기술한 ORO의 다른 초기 연구들은 지금도 관련보고서가 남아있어 인터넷 검색을 통해 자세한 내용을 확인해 볼 수 있다.

〈그림 3-5〉 ORO의 프로젝트를 통해 탄생한 AR-15 소총을 미스 아메리카가 들고 있다.
(출처 : 라이프지)

3.4 한국전쟁 그리고 1950년대의 미국 운영 분석 연구 사례

1940년대까지를 운영분석의 유년기라 한다면 1950년대 이후를 운영분석의 청소년기라 부를 수 있을 것이다. 한국전쟁이 발발한 1950년 ORO의 수장인 Dr. Ellis A. Johnson은 한국전쟁을 기존에 자신들이 완료해온 연구, 그리고 진행되고 있는 연구를 직접 적용해 보고 또 유용한 현장의 데이터를 획득할 수 있는 좋은 기회로 생각하였다. ORO는 150여명 이상의 조직원을 한국에 파견한다. 이들은 부산에서 치열한 전투가 진행되고 있던 1950년 9월에 한국에 도착하였고, 가장 실력 있는 그룹을 미 제 8군 본부에 배치한다. 1951년에는 파견된 ORO의 본부가 일본 도쿄로 이동하긴 하였지만 전쟁 기간 동안 50% 이상의 조직원들이 한국 현장에서 근무한 것으로 알려져 있다. 이들 중 많은 수가 전쟁의 공로를 인정받아 유엔(UN) 메달을 획득하였고 그러나 일부는 북한군에게 총상을 입기도 하였다. 한국전쟁에서 ORO의 주요 연구는 다음의 두 중심 토픽으로 구분할 수 있다.

1) recommendations concerning current operations : 현행작전 지원
2) collection of data for later and broad studies : 장차연구를 위한 자료수집

현행작전 지원을 위한 많은 문제들은 2차 세계대전 시 연구했던 문제와 크게 다르지 않았고 단지 한반도 실정에 맞게 약간의 조정이 필요했다. 예를 들어 동계작전을 위한 피복 및 장비에 대한 연구가 여기에 속한다. 이러한 연구는 2차 세계대전 시에도 이루어 졌던 연구지만 한반도에서는 동계작전이 특히 중요했기 때문에 추가적으로 실시되었다고 할 수 있다. 하지만 전쟁이 진행되면서 이들은 전혀 새로운 응용 분야의 문제를 해결해야 했다. 대표적인 연구 주제들은 다음과 같다.

〈표 3-3〉 한국전쟁 시 미국군의 대표적인 운영분석 연구 주제

연구 주제
(1) use of atomic bombs (tactical weapons)
(2) close air support of ground forces
(3) armor operations
(4) infantry tactics and weapons
(5) airborne operations
(6) mobilization and use of South Korean manpower
(7) combat service support
(8) counter-guerrilla operations
(9) psychological warfare operations

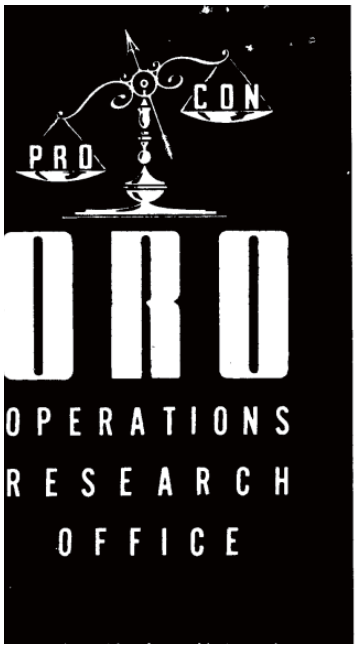
우리가 한국 전쟁사를 통해 익히 알고 있듯이 연합군의 근접항공지원(CAS, Close Air Support)은 북한군에게 커다란 위협이었다. ORO는 (2)번 연구를 통해 야간에 공군이 B-29 폭격기를 운용하는데 큰 도움을 주었고 결과적으로 한국전쟁에 크게 기여하였다. 비록 현실화 되지는 못했지만 (1)번 연구인 전술핵의 사용에 대해 꽤 깊은 연구가 이루어졌고 이때의 연구 결과는 차후에 미 육군이 핵 개발을 위한 시뮬레이션 분석 등에서 활용되기도 한다.

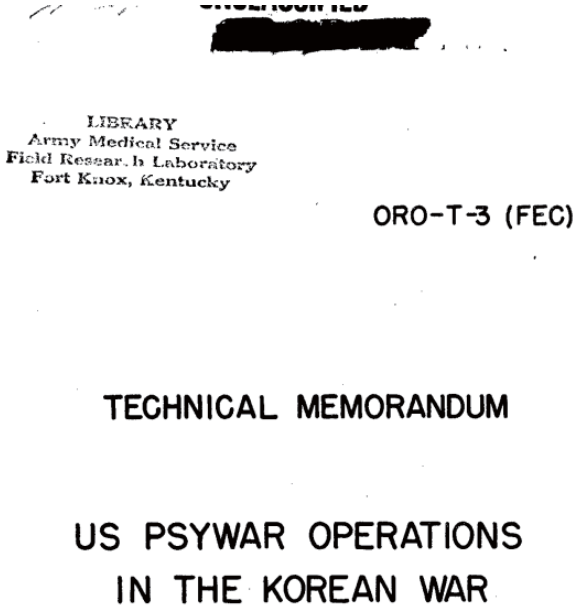
미 육군은 이처럼 현행작전 지원 뿐 아니라 장차 연구를 위한 데이터 수집에도 공을 들이는데 ORO는 전쟁 시 파괴된 전차의 데이터를 모두 수집하여 전차의 취약성에 대한 중요한 데이터를 얻어간 것으로 평가하고 있다.

또한 전쟁 포로들을 활용하여 사회주의(communist) 전투원의 데이터를 수집하여 장차 심리전에 활용할 수 있는 기반을 다지기도 한다. 만약 ORO가 한국전쟁에 파견되지 않았더라면 이처럼 적은 비용에 수없이 많은 사회주의 구성원의 샘플을 확보할 수 없었을 것이다. 데이터 분석을 통한 심리전은 한국전쟁 시에도 빈번했는데 '삐라', 확성기 등 다양한 심리전이 전개되었다. ORO의 전술 전문가였던 S. L. A. Marshall은 적군 포로 또는 한국군들의 인터뷰를 통해 자신의 소부대 교리를 검증 및 발전시키기도 하였다. 이후 그는 한국전쟁을 다룬 유명한 저서인

The River and the Gauntlet and Pork Chop Hill에서 이때 이루어진 다양한 연구결과를 공개하기도 한다. 이러한 심리전 연구는 〈표 3-2〉에서 소개한 POWOW 프로젝트의 일환으로 실시되었다.

한국 전쟁에서 운영분석 연구가 가지는 가장 중요한 대목은 미 해군과 공군이 제 2차 세계대전 시 보여주었던 운영분석 분석이 전쟁에 크게 기여했다는 성공 사례를 육군에서도 보여줄 수 있었던 장을 제공했다는 것이다. 미 육군은 한국 전쟁을 통해 운영분석 기능에 대한 자신감을 획득한다. ORO의 입장에서는 한국전쟁을 통해 조직의 예산이 기존에 비해 4배로 증가하였고[4] 이때 증가한 예산은 이후에 결코 감소하지 않았다.





〈그림 3-6〉 한국전쟁에서의 심리전을 다룬 ORO의 보고서 (출처 : asiancorrespondent.com)

한국 전쟁이 한창이던 1950년 초반에 ORO의 많은 인원들이 현장에서 작전을 지원하였다. 이 뿐만 아니라 미 본토에서는 파견되지 않은 ORO 조직에서 장차 작전을 위한 주제들에 대한 꾸준한 연구를 진행하였다. 이 연구들은 전쟁과 직접적으로 연관되지 않았지만 장차 미 육군의 방향성을 정립하는 연구들이 대부분이

4) 1949년에 $1 million 이었던 예산이 1954년 $4 million 으로 증가함

었다. 1951년부터 1954년까지 ORO가 중점적으로 진행한 프로젝트는 〈표 3-4〉과 같다. 〈표 3-4〉에는 〈표 3-2〉에서 이미 기술한 연구 주제와 시기 상 중복되는 것이 있지만 그 내용은 제외하였다.

〈표 3-4〉 1950년대 미 육군의 대표적인 운영분석 연구 주제

프로젝트명	연구 내용
BALANCE	(1) balance of weapon systems
CAPWAR	(2) cost effectiveness
COBRA	(3) chemical, biological, and radiological warfare
DOUGHBOY	(4) infantry weapons
LEGATE	(5) military government
OPSEARCH	(6) OR methodology
PARABEL	(7) guerrilla warfare
REDLEG	(8) artillery
SHOP	(9) human factors
TACIT	(10) intelligence
TEAR	(11) air support of ground operations

여기서 주목할 만한 연구는 (2)번 연구(CAPWAR)이다. 무기체계의 개발 및 구매 등 획득 프로세스에서 해당 무기 시스템의 비용 대 효과(cost-effectiveness)를 분석하는 것은 필수적이다. CAPWAR 프로젝트를 통해 ORO가 비용 대 효과 연구를 진행한 것으로 나타나지만, 미국에서의 비용 대 효과 연구는 그보다 먼저인 1948년 RAND 연구소의 창립과 함께 본격적으로 이루어졌다고 알려져 있다 [11]. 이후 1950년대 RAND 연구소의 수장이었던 Hitch 박사는 이 문제를 “System Analysis”라는 문제로 정의하고 이를 발전시켜 훗날 계획예산제도(PPBS, Planning, Programming, Budgeting System)와 5개년 방위계획 수립의 제도적인 근간을 마련하게 된다. 그리고 여기서 발생한 시스템적 사고는 후일 1960년대 미국 국방정책을 지배하는 운영분석 철학의 근간이 된다. PPBS와 시스템 분석에

대한 자세한 내용은 후에 다시 기술한다.

무기체계의 효율적인 획득을 위해 개시되었던 시스템 분석 연구는 1960년대 후반에 이르러서는 헬스 서비스, 교육, 도시 계획, 기후 문제 등 다양한 분야로 확대되기에 이른다. 대부분의 운영분석 주제가 그러하듯이, 군에서 시작된 연구 주제가 일반 민간 사회의 문제로 확대, 재생산 되는 모습을 여기서도 보여주고 있는 것이다.

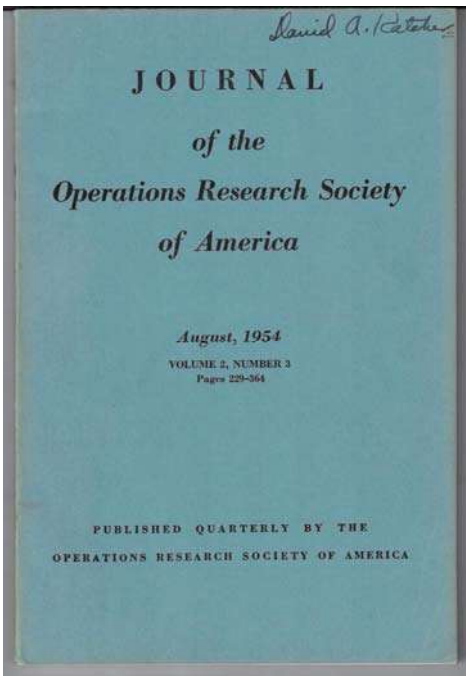
ORO의 연구들이 수 많은 성과를 거두었지만 비판이 없었던 것도 아니다. ORO의 연구 결과물들에 대한 첫 번째 비판은 연구 결과를 확인할 수 있는 정확하고 일반화된 측정 방법이 없었다는 것이다. 사실상 이 비판은 지금 우리 운영분석이 겪고 있는 현실의 모습과 많이 다르지 않다. 전시에는 운영분석의 결과물들이 적시에 현장에 적용되어 피드백을 받고 또 개선된다. 즉, 연구의 질적 평가가 현장에서 실증을 통해 바로 이루어지는 것이다. 하지만 평시에는 운영분석의 해(solution)들을 평가할 별다른 방안이 존재하지 않는 것이 사실이다.

1950년대는 군이 주도하는 운영분석 연구가 민간으로의 본격적인 전파가 시작되는 시기이기도 하다. 미국의 민간 업체들은 1940년대 후반부터 운영분석 섹터(부서)를 회사 내에 두기 시작하였고 1953년에는 75%의 연구기관들이 운영분석 섹터를 가지게 되었다. 학교 기관에서 운영분석을 학문으로 가르치기 시작한 시기도 이와 일치한다.

미 해군과 협약을 가진 MIT, 미 육군과 협약이 있는 존스 홉킨스 대학을 필두로 비 군사적(non-military) 운영분석을 가르치기 시작한다. 1951년에는 Case 공과대학이 최초로 운영분석 석사학위를 수여하는 대학이 된다. 1954년에는 12개의 대학에서 운영분석을 교육하게 된다. (Case Institute, Johns Hopkins, MIT, Columbia, University of California – Los Angeles, Penn State, Illinois Institute of Technology, Stevens Institute of Technology, Tufts Univeristy, American, the Naval Postgraduate School, and Wright Field Air Development Center) 그리고 1955년에는 MIT와 존스 홉킨스에서 최초로 운영분석 박사 학위자가 배출된다.

이와 같이 민간으로 전파되기 시작한 운영분석은 학문적으로 발전하면서 다양한 학술지 역시 창간되기 시작하는데 Operations Research Quarterly(1950년), MORS(1957년, Military Operations Research Symposia), Journal of the Operations Research Society of America (JORSA, 1952년) 등이 이때 발간

되었다. JORSA는 이후 1995년에 운영분석의 가장 큰 학회 중 하나인 INFORMS로 재창설되기도 한다.



〈그림 3-7〉 1954년 발간된 JORSA 학술지 모습

3.5 컴퓨터의 발전과 운영분석의 새로운 영역 - 워게임

현대에서 운영분석과 컴퓨터는 별도로 생각할 수가 없을 정도로 밀접하게 연관되어 있다. 최초의 계산기로 알려진 Mark I의 제작 배경에는 2차 세계대전 시 복잡하고 어려운 계산을 빨리 해야 하는 수요에서 비롯되었다는 것은 익히 알려져 있다. 또한 미국의 개인용 컴퓨터 ENIAC(Electronic Numerical Integrator and Calculator)은 미 육군의 운영분석 조직인 BRL[5]의 연구 요구와 연관되어 있다 (ENIAC은 실제로 탄도의 궤적 계산을 목적으로 제작되었다). 컴퓨터 발전의 역사에 대한 자세한 설명은 본 연구 보고서의 범위에 포함되지 않는다. 다만, 정확

5) 본 장의 2절 참고

하고 빠른 운영분석 연구의 필요에 의해 전산장비의 개발이 가속화 되었다는 것은 사실이다.

컴퓨터의 발전으로 운영분석 연구의 중요한 한 축이 되는 워게임[6] 연구가 본격화된다. 1955년 미 육군의 운영분석 조직인 ORO는 ERA 1103이라는 컴퓨터를 이용하여 워게임을 시작한다. 하지만 이 장비는 워게임을 운용하기에는 턱없이 부족한 사양을 가졌고 1957년이 되어 UNIVAC 1103A라는 장비를 통해 본격적으로 워게임을 할 수 있게 된다. 당시 ORO에서 활용되었던 워게임 모델은 다음과 같다.

〈그림 3-8〉 초창기 워게임을 위해 사용되었던 ERA 1103 컴퓨터 (출처: 위키미디어)

6) 워게임의 넓은 정의에는 체스게임, Rock-Drill과 같은 것도 모두 포함되지만 본 연구에서는 컴퓨터를 활용한 워게임만을 다룬다.

〈표 3-5〉 미 육군의 초기 워게임 모델

워게임명	설명
STRATSPIEL	(1) 전구급 작전 묘사, 현역 군인이 플레이어를 담당
FAME	(2) TACSPIEL에서 제작한 모델로 전술 제대 묘사 및 지형과 기상요소 도입 - 중동(요르단)에서의 제한된 전투 묘사
Carmonette	(3) Monte Carlo 시뮬레이션 기반의 워게임 - 사격과 이동 등 전술행동 묘사 - 1950년대에는 중대급 묘사, 60년대 이후 대대급 묘사로 확장
INDIGO	(4) 숙련된 군 장교를 훈련하기 위한 two-sided 워게임
LOGSPIEL	(5) 군수와 관련된 의사결정을 지원하기 위한 워게임

이후 워게임의 급속한 활용과 함께 시뮬레이션 방법론을 발전시키기 위한 육군 내 조직인 Strategy and Tactics Analysis Group (STAG)가 1960년 창설된다. STAG는 1961년 74명의 조직원으로 시작하여 2년 후 162명으로 증가하는 등 전폭적인 인적지원을 받고 항상 최신 사양의 전산장비를 지원받는 등 급속한 성장을 하게 된다. STAG의 주요 연구 성과로는 유도미사일을 묘사하는 FABMDS(Filed Army Ballistic Missile Defense System) 모델, 미 육군의 글로벌 작전을 평가하기 위한 CENTAUR 모델 등이 있다. 특히, STAG는 1961년 주한 미 8군의 워게임 훈련을 주도하기도 한다. CENTAUR 워게임 모델을 활용한 훈련은 지금 우리가 실시하고 있는 워게임의 형태와 매우 유사하다. 이들은 청군, 홍군, 통제소, 게이머실 총 4개의 방으로 구성된 훈련장에서 청군의 부대지휘절차를 훈련하였다. STAG의 성공으로 미 육군은 인력과 비용을 크게 절감할 수 있는 하나의 훈련체계 대안인 워게임 훈련 방안을 확보하게 된다.

STAG의 성장과는 별개로 오랫동안 미 육군의 운영분석을 담당한 ORO는 쇠퇴하게 된다. ORO는 연구 분야를 끊임없이 확장해 갔지만 그만큼 연구의 질이 받쳐주지 못했고 대부분의 연구는 기약 없이 기간이 연장되기만 하였다. 여기에 ORO의 디렉터인 Johnson의 지휘관들과의 불화까지 겹쳐 결국 현장에서의 군이 더 이상 연구결과를 신뢰하지 못하는 상황에 이르게 되었다. 또한 연구 파트너였

던 존스 홉킨스 대학과의 교류도 1961년 단절되면서 ORO는 새로운 조직인 RAC(Research Analysis Corporation)으로 변경된다. RAC는 ORO의 인적 자원을 거의 그대로 가져가고 ORO에서 진행하던 연구 역시 계속 진행하였다. 하지만 일부 예하 조직의 변화는 피할 수 없었다. ORO와 존스 홉킨스 대학 그리고 미 육군의 13년 간의 공생 관계는 이렇게 종료되었지만 ORO가 남긴 648 건의 연구 결과는 미 육군 발전에 지대한 공을 했다고 평가받기에 부족함이 없다.

1950년 그리고 이른 1960년대의 미국의 운영분석 기능은 중대한 변화를 맞이하였다. 연구결과가 그대로 의사결정에 반영되던 전시와 다르게 운영분석은 미래의 소요를 예측하고 연구하는데 몰두해야 했고 이로 인해 연구의 영역이 비대해 지기 시작했다. 한국 전쟁 참전을 제외하면 별다른 실제 전투를 하지 않았던 시기여서 국방 예산은 점점 줄어들었고 이로 인해 워게임 시뮬레이션의 중요성이 대두되었다. 또한 민간 대학교에 스폰서를 받아 군의 문제를 연구하던 방식의 한계를 맞으면서(이 시기에는 대학교 내에서 군과의 연구를 반대하는 시위가 늘어나기도 하였다) 독립된 연구기관의 필요성을 느끼게 되었다. 이렇게 미군의 운영분석은 혼란스러운 청소년기를 마치게 된다.

〈그림 3-9〉 1960년대 미 국방정책을 이끈 8대 국방장관 맥나마라
(출처 : 더 뉴욕 타임스)

3.6 맥나마라(McNamara) 혁명

로버트 맥나마라(Robert S. McNamara)는 미국의 제 8대 국방부장관이다. 미국 캘리포니아 버클리 대학에서 경제학 학사, 하바드 대학에서 MBA를 취득하고 1943년에는 육군 항공대 장교로서 제 2차 세계대전에 참전하기도 하였으며 중령으로 전역하여 포드 자동차 회사에 입사하여 대표(vice president)의 자리까지 오른 특별한 경력을 가진 자이다. 미국의 케네디 대통령은 1961년 맥나마라를 국방부 장관으로 임명하는데 임명 후 그가 실시한 여러 급진적인 정책들을 맥마나라 혁명으로 부른다.

군사 운영분석 연구사례를 소개하는 본 보고서에서 맥마나라 혁명을 언급하는 이유는 바로 그의 정책들이 미 국방 의사결정 체계를 급진적으로 변화시켰기 때문이다. 맥마나라는 국방부의 의사 결정 시스템을 중앙 집권화 시켰으며 PPBS(Planning, Programming, and Budgeting System)로 대변되는 시스템 분석(System Analysis) 기법을 각 분야에 적극적으로 적용한다. 미 육군의 지휘관들은 군 생활의 경험적 요소를 저평가 하는 그의 정책에 반기를 들지만 그의 추진력을 막기에는 역부족이었다. 운영분석의 관점에서 그의 정책은 새로운 것이 아니다. 제한된 자원을 가지고 성과(return)를 최대화하는 가장 기본적인 최적화의 철학을 국방의 의사결정에 적용한 것이기 때문이다. 케네디 행정부 그리고 맥나마라의 이런 결정에는 냉전이 언제까지 지속될지 모른다는 위기감과 점점 더 정교해지고 높아져 가는 무기체계의 비용 그리고 신속한 의사 결정 시간의 요구 속에서 국방의 효율화를 추진해야 한다는 시대적 요구가 있었음이 분명해 보인다. 취임 후, 맥나마라는 당시 국방 의사결정의 문제점을 다음과 같이 지적하였다.

1) 국방 문제에서의 의사결정 프로세스가 너무 느리고 비효율적이다.
2) 기존의 의사결정은 정량적인 분석에 의한 판단보다는 경험과 직관에 의존한다.

그리고 이러한 문제점을 해결하기 위한 방법으로 새로운 의사결정 툴(tool)이 필요하다고 판단하였다. 그는 이를 실현하기 위해 3가지 목표를 설정하는데 첫 번째는 조직의 지역주의 성향을 타파하기 위해 의사결정 권한을 중앙집권화 시키는 것이었으며 두 번째는 여러 국방 조직을 기능적 계선(functional line)으로 재조직

하는 것이었고, 마지막은 아이젠하워 대통령의 군사 철학이었던 “대량 살상(massive retaliation)” 전략을 “융통성 있는 대응(flexible response)”으로 전환시킨 것이었다. 특히 세 번째 목표인 국방 전략을 바꾸는 일은 그 동안의 관성을 이겨내고 새로운 철학을 침투시켜야 하는 작업으로 오랜 시간 동안 철저히 계획해야만 가능한 일이었다.

〈그림 3-10〉 미국 케네디 행정부는 소련과의 Arms-race 전략으로 “flexible response”를 채택한다. (출처 : 위키피디아)

이를 위해 맥나마라는 PPBS를 도입한다. 맥나마라는 PPBS를 다음과 같이 정의한다.

“A mission oriented planning and programming process to assist in defining and balancing the total effort.”

PPBS의 첫 번째 단계는 계획(Planning)으로 주로 소요군, 합동참모본부에 그 책임이 있으며 마지막 단계인 예산 편성(Budgeting)은 민간인에게 책임이 있다. 맥나마라의 PPBS의 핵심은 Planning과 Budgeting의 중간단계인 Programming에 있는데 이 단계에서는 처음과 마지막을 연결해 주어야 하는 책임이 있기 때문이다.

PPBS의 적용을 통한 가시적인 성과는 국방에서의 의사결정 권한을 입법부(legislative)에서 행정부로 전환할 수 있었다는 것인데 이는 행정부에서 판단하는 군사적 요구와 의회에서 이루어지는 예산 승인의 충돌 가능성을 사전에 제거할 수 있기 때문에 가능한 것이다. 두 번째 성과는 각 군의 요구를 균형성 있게 통제할 수 있다는 것이다. 각 소요군의 이해관계에서 오는 서로 다른 요구를 정량적인 방법으로 선별하고 선택하게 함으로써 객관적인 설득 논리를 만들어 내고 이로 인해 불필요한 예산의 낭비를 막을 수 있다는 분석이다.

맥나마라의 PPBS의 도입은 운영분석 연구를 주도하는 집단을 수학자, 물리학자 집단에서 경제학자들로 변화시킨다. 주로 RAND 연구소의 박사들로 구성된 이들은 "Defense Economists"로 불리어졌다. 기존의 경제학 이론들이 매우 복잡한 국방의 문제를 다루기 시작하면서 도메인 전문가들이 평가하는 가치를 객관적인 비용으로 전환하는 새로운 기법들에 대해 관심을 가지게 된다. 맥나마라의 최측근이었던 Hitch는 시스템 분석의 단계를 다음과 같이 정의한다.

1) 목적의 정의 (The definition of the objective)
2) 목적을 달성할 수 있는 다양한 방안의 발견(The description of alternative means by which the objective may be accomplished)
3) 각 방안의 비용을 정의(Determination of the costs associated with each alternative)
4) 적합한 모델의 구성(Construction of a model of the situation)
5) 최선의 대안을 선택하기 위한 기준 정립(Selection of criteria for choosing the preferred alternative)

〈그림 3-11〉 케네디의 국방 정책을 이끈 맥나마라와 그의 참모들(Whiz-kids)
(출처 : intelligentcollector.com/blog/tag/whiz-kids)

기술한 절차에 따른 System Analysis는 한 번에 종료되는 것이 아니라 연속적으로 계속 평가하며 대안과 가정 등을 지속적으로 수정한다. 이러한 분석에서 가정의 적합성은 결과에 직접적인 영향을 미친다. 비단 가정뿐만 아니라 모델에서 정의하는 목적 그리고 다양한 제약 조건들이 모두 그 결과에 큰 영향을 미치기 때문에 시스템 분석가들은 이들을 정교하게 수립하기 위해 심혈을 기울였다.

하지만 그보다 더 중요하고 어려운 작업은 최선의 대안을 선택하기 위한 기준을 설정(5번 단계)하는 것이었다. Hitch는 국방에서의 문제는 불확실성이 다른 문제보다 더 크기 때문에 그 가치를 평가하는 것이 어렵다고 진술한다. 통계학적으로 발생하는 불확실성은 다양한 시뮬레이션 기법으로 극복이 가능하지만 전장 자체가 가지고 있는 불확실성은 그것을 정의하는 것도 어렵고 이를 제거하는 것 또한 어려운 일로 여겨졌다. 때문에 '좋은' 시스템 분석가들은 최대한 많은 데이터를 수집

하고 그것을 적절하게 활용하며 해석하고 또 결과를 지휘관에게 효과적으로 잘 설명하여 불확실성을 최소화하는 것을 목표로 하였다.

불확실성을 제거하는 좋은 방안 중 하나는 시스템 분석가들이 최선의 대안을 바로 제시하는 것이 아니라 의사결정자가 고려해 볼 수 있는 대안과 전혀 생각하지 않아도 될 대안을 구분하는 정도로 대안을 분류하는 일이었다. 이러한 이유로 당시에는 대안을 "긍정적인 대안(optimistic one)", "회의적인 대안(pessimistic one)", "가장 좋은 대안(a best or single most likely one)"으로 구분하여 의사결정자에게 보고되었다.

맥나마라의 새로운 기법은 혁신적인 하나의 방법론이었지만 이것의 도입은 단순히 학술 분야에서 변화만 가져온 것이 아니었다. 미 국방부의 조직이 변화하게 되었고 각 부서의 권한이 줄어들거나 늘어났으며 새로운 군사 전략에도 영향을 미쳤다. 조직의 의사결정권자들은 기존에는 온전히 자신의 몫이었던 대안의 비교와 선택을 시스템 분석가들의 도움으로 수행할 수 있었다.

〈그림 3-12〉 맥나마라의 시스템 분석은 지휘관의 경험과 직관을 지나치게 무시했다는 평가를 받기도 했다. (출처 : HistoryNet.com)

맥나마라의 PPBS 기법은 때론 극심한 비난을 받기도 하였다. 첫 번째는 새로운 기법 자체가 가진 제한점에 대한 비판이었다. 두 번째는 경험있는 군 전문가들이 주로 가진 시스템 분석결과에 대한 불신 문제였다. 이들 베테랑들은 새로운 기법의 적용을 "군인과 민간인의 대결"로 까지 인식하기에 이르며 크고 작은 많은 충돌이 야기되었다. 이들은 "죽고 사는 문제(life-and-death)"가 고작 수학식이나 컴퓨터에 의해 결정되는 것에 대한 반감이 있었다. 세 번째는 새로운 기법을 소요군이 함께 이해하고 동참하지 못했다는 점이다. 네 번째는 새로운 기법의 적용이 그동안의 군 경험과 전문성을 무시한다는 점이었으며 마지막으로, 항상 대두되어온 문제인, 전쟁 문제에서 정량적 접근의 효용성에 대한 것이었다.

여타의 비난은 차치하고 현 시점에서 우리가 생각해 볼 가치가 있는 항목은 바로 시스템 분석가들의 연구 보고서의 질적 수준에 대한 비난이다. 실패한 시스템 분석 연구는 대부분 문제를 잘 이해하지 못하는 데서 비롯되었다. 문제를 이해하지 못한다는 것은 소요군의 요구를 모르고 또 그 배경과 관련 지식이 전무 하다는 것을 의미한다. 당시 기술된 실패한 시스템 분석 연구의 공통적인 과오는 다음과 같다.

1) 운영분석 전문가들이 의사결정권자와 다른 세상에 살고 있다. (의사소통의 문제)
2) 운영분석가들은 기술에만 신경을 쓰고(technique-oriented) 결과(result-oriented)에는 관심이 없다.
3) 어려운 전문용어가 의사결정권자와 운영분석가 사이의 장벽이 된다.
4) 컴퓨터 등의 발전으로 쉽게 도출되는 수없이 많은 데이터를 여과 없이 의사결정권자에게 제공한다. (꼭 필요한 데이터가 무엇인지 모른다)
5) 의사결정권자를 설득할 수 있는 개인의 역량이 부족하다.
6) 기약 없이 계속되는 연구에 소요군이 지치게 된다.
7) 의사결정권자들이 자신이 미리 세워놓은 결론에 분석결과를 대입하고자 한다.

기술한 문제들은 대부분 지금 우리 현실에서도 생각해 볼 필요가 있는 것들이다. 운영분석가들이 본인의 학업적 성취에만 몰두하여 그것이 어떻게 쓰이는지는 관심이 없는, 또는 결과를 설명하는 것에 대해 너무 쉽게 생각하는 현상 등이 지금도 많이 목격되기 때문이다.

3.7 1960, 70년대 미국의 운영분석 연구 사례

시스템 분석, PPBS, 비용 대 효과 분석 등으로 대표되는 맥나마라의 급진적인 정책들을 따르기 위해 또는 변화하는 세계에 대응하기 위한 자체적인 필요성에 의해 각 군은 운영분석 기능을 재정비해야 할 필요를 느끼게 된다. 미 육군은 당시 작전지역을 전 세계로 확장하며 몸집을 키우고 있었다.[7] 이러한 상황에서 기존의 운영분석이라는 타이틀은 ORSA(Operations Research and System Analysis)로 확대되고 맥나마라의 정책방향과 일치하게끔 운영분석 기능의 중앙집권화가 시작된다.

육군장관(Secretary of the Army)[8] 산하에 OOR(Office of Operations Research)이 설립되어 육군의 자체 운영분석 기능을 수행하고 맥나마라가 이끄는 국방부 장관실(OSD, Office of the Secretary of Defense)의 분석업무를 돕게 된다. 육군은 좋은 운영분석 시스템을 가지고 있었음에도 각 구성 요소를 통합하여 평가하는 능력(total effort)에 한계가 있다고 느끼고 있었으며 맥나마라의 정책을 조직이 발전하는 기회로 삼으려 하였다. 그럼에도 불구하고 육군은 맥나마라의 지나치게 복잡한 요구 사항과 간섭(국방부는 초기에 육군을 신뢰하지 않아 OSD의 민간인을 육군에 파견한다. 육군은 이 인원을 OSD spy로 부르며 배척하기도 하였다) 등으로 곤혹을 겪기도 하였다. 60년대의 미국의 운영분석 기능은, 비록 기능의 중앙집권화에 힘을 쏟았지만, 어느 한 조직이 모든 업무를 총괄하여 수행하지 않았고 다양하고 전문화된 많은 조직들이 제 역할을 하였기 때문에 그 조직 전체를 일일이 나열하는 것은 불필요 하다.

1970년 여름 미 육군 본부에서 ORSA 기능을 수행한 인원은 총 660명으로 이 중 절반에 해당하는 321명은 민간인이었다. 660명의 인원 중 덜 숙련되어 주로 행정을 담당한 인원은 266명이었고 능숙하게 숙련된 운영분석 특기자는 394명으로 보고되었다. 육군은 외부 민간인을 계속 고용하는 것 보다는 육군 내에서 특기자를 양성하는 것에 관심을 기울였으며 몇몇의 장교를 외부대학에 위탁교육을 보내기도 한다.[9] 하지만 계속 증가하는 운영분석 소요에 대응하기 위해 자체 ORSA

7) 1969년 미 육군은 약 2백만의 병력을 유지하고 50개국 이상의 900여개의 기지를 관리하고 있었다. 또한 약 15,000 종의 장비를 관리하였다.
8) Secretary of the Army는 육군참모총장(Chief of Staff U.S. Army)과 다르다.
9) 1966년 육군은 총 48명의 장교를 11개 대학(알라바마, 아리조나, 아리조나 주립, 조지아 공대, 인디아나,

프로그램을 계획한다.

1963년 35개의 TO를 할당한 육군은 1969년에는 550개의 TO를 할당하는 등 프로그램을 확장해 나간다. 당시 미 육군은 굉장히 깊은 수준의 지식을 갖춘 전문가를 양성하려 했다고 판단된다 (“a hard core of expertise”). 미 정부 산하 교육기관인 미국 해군대학원(Naval Postgraduate School)은 1961년 운영분석 학부(Department of Operations Research)를 개설하고 1960년대 중반부터 타 군 장교 및 해외 동맹국의 장교들을 받기 시작하며 이후 육군 ORSA 교육의 가장 큰 공급처가 된다. 육군 뿐 아니라 국방부에서도 대학원 수준의 ORSA 교육 소요에 관심이 있었고 맥나마라 팀의 핵심 인물인 Hitch는 다음과 같은 교육 소요를 제안하기도 한다.

1) Strategic studies and analysis of defense policy decisions
2) Economics – price and allocation theory and national income analysis
3) Probability statistics and inference from uncertain data
4) Mathematical operations research and computers

그가 ORSA 능력을 갖추기 위한 교육소요로 제시한 많은 부분이 우리나라의 현 국방대학교 관리대학원 학과의 구성과 상당 부분 유사함을 확인할 수 있다. ORSA 교육은 운영분석 전문가 뿐 아니라 전체 군 지휘자들에게 소양교육으로도 이루어졌다. 육군대학(U.S. Army Command and General Staff College)은 ORSA 소개, 자원관리, 워게임 교육을 12시간 이상 반영하였고 The Army War College는 ORSA의 방법론을 포함한 교육을 4일간 반영하기도 한다. 육군은 이처럼 다양한 수준의 교육을 통해 ORSA 전문가를 수준에 따라 세 그룹으로 구분하여 각각의 목표에 맞추어 계획적으로 양성한다 : 전문가 수준(specialist)[10], 행정업무 가능 수준[11](executive), 친숙화 수준(familiarization level). 당시 각 ORSA 관련 부서별 교육 소요에 대한 수치 자료는 Shrader의 연구 보고서 132p-133p[12]를 참조하면 된다.

오하이오, 펜스테이트, 퍼듀, 스탠포드, 툴레인, 위스컨신)에 위탁교육을 보낸다
10) 항상 ORSA 관련 업무에 종사하는 자로 대학원 이상의 학위 교육을 실시
11) ORSA 부서에서 실무를 할 수 있는 수준으로 4-6주 정도의 단기과정 교육을 제공

〈그림 3-13〉 미국 운영분석 교육을 이끌고 있는 두 학교 (출처 : 각 대학 홈페이지)

맥나마라와 그의 시스템 분석 체계는 1969년 미국 닉슨 대통령(Richard M. Nixon)의 취임과 새로운 국방 장관 Melvin R. Laird의 임명으로 약화되기 시작한다. 그들은 맥나마라의 새로운 분석 기법 자체에는 이견이 없었으나 국방의 의사결정이 중앙집권화 되어 군의 원로 핵심 세력들의 경험이 무시되는 것에는 반대하는 입장이었다. 군의 ORSA 기능은 더 이상 확장되지 못하거나 그 속도가 완화되었다. 육군은 RAC(Research Analysis Corporation), HumRRO(Human Resources Research Office), SORO(Special Operations Research Offcie)와 같은 외부 연구 기관의 참여도를 줄이는 대신 육군 내에서 ORSA 기능을 수행하기를 원했고 Army Analytical Community와 같은 인하우스(in-house) 조직을 그 대안으로 생각하게 된다.

하지만, 육군의 제안을 받아 연구를 수행하는 외부 연구소와 육군의 인하우스 운영분석 조직들이 20여개에 이르렀지만 이들은 서로 각자의 연구를 지속할 뿐 어떤 연구가 중복되는지 또는 어떤 연구가 참고할 만한 가치가 있는지 서로 알지 못했다. 이에 1964년 당시 육군참모차장의 지시를 받은 Bonesteel 장군은 “The Bonesteel Study”라고 불리는 그 동안의 연구보고서를 집대성 하는 프로젝트를 개시한다. 이 프로젝트는 그 동안의 연구결과들을 리뷰하고 효율적으로 통합하며 우선순위에 따라 연구물들을 분류하는 작업을 포함하고 있었다. Bonesteel 프로젝

트에 의해 1962년부터 1964년까지 2년에 걸쳐 이루어진 연구물들을 조사한 결과는 다음과 같이 요약된다.

〈표 3-6〉 1962년-1964년 ORSA 주요 연구 분석 요약 (Bonesteel 프로젝트)

비고	내용
연구실적	36개 육군기관에서 567건의 보고서 작성 : 전략연구(89), 개발연구(347), 행정/관리(91), 방법론(40)
주제	- 유럽전역에서의 단위부대 철수 및 합병 연구 - 군수분야에서의 컴퓨터 시뮬레이션 - 핵전쟁에서의 육군의 역할 - 민간 방호를 위한 군사 지원 - 지상군 공중 수송을 위한 연구 - 기타 소부대급 연구 : 소대에서의 기관총 활용, 전투식량의 장기 보존 등

Bonesteel 프로젝트는 다음과 같은 시사점을 도출한다. 1) 연구의 중복을 방지하기 위해 가장 중요한 것은 과제 제기부서에서의 사전 중복성 검토이다. 2) 운영분석을 전공한 연구 협조관(Study Coordinator)을 육군의 주요 부서마다 배치하여 각 기관의 장을 보좌해야 한다. 3) 기록물 보관소(repository)는 정기적으로 참고문헌 카달로그를 작성해야 한다.

Bonesteel 프로젝트는 크게 호응을 얻고 육군의 전 부서에서 이를 적용하기 시작하며 이와 함께 연구 성과물을 객관적으로 평가할 수 있는 평가체계에 대한 연구가 후속하여 이루어지기도 한다.

본 보고서의 5절에서 설명한 바와 같이 1961년 ORO가 쇠퇴하고 그 역할을 대신한 연구소가 RAC였다. RAC는 1960년대에 미 육군의 제 1 연구 파트너로서 수많은 프로젝트를 수행하였다. RAC 펀딩의 80% 정도를 육군이 차지하고 있을 정도였다. 하지만, 1960년대 중반부터 미 육군의 펀딩이 감소하면서 RAC는 DOD 또는 정부의 다른 기관의 연구를 받는 등 고객의 다양화를 모색해 나간다. 하지만, RAC 역시 결국 해체의 수순을 밟게 되고 1972년 영리단체인 GRC(General Research Corporation)에게 매각된다. 육군이 제안하고 RAC가 수행했던 주요 연구 결과물을 다음과 같다.

〈표 3-7〉 1960년대 미 육군과 RAC의 운영분석 연구 주제

프로젝트명	연구 내용
FOREWON	(1) A computer assisted largely automated planning system for determining future US requirements for Amy forces
CONAF	(2) Conceptual Design for the Army in the Field (for next decades)
MARS	(3) Models of Army Supply - dealt with logistical support problem
SIGMALOG	(4) Simulation and Gaming Methods for Analysis of Logistics
COMPLIP	(5) Computation of Manpower Programs by Linear Programming

이 중 연구 (1) FOREWON은 RAC가 수행한 육군의 프로젝트 중 가장 큰 규모의 연구로서 미래 전력 소요를 반영한 미 육군의 전력 소요를 예측하기 위해 수행되었다. 미 본토 뿐 아니라 전 세계적으로 미 육군의 전력을 어떻게 구성해야 할지에 초점을 두었고 실무에 반영되었다. 변화하는 상황의 반영을 위하여 다양한 파라미터를 변경하며 분석할 수 있도록 분석의 틀을 전산화, 자동화 하는데 그 초점을 두었다.

(2)번은 미 육군의 전력을 계획한다는 점에서 (1)번 연구와 유사점이 있지만 당시에는 미래였던 1980년대까지의 미 육군 운용을 위해 조금 더 개념적인 소요를 창출하기 위해 실시된 연구이다. 외에도 전통적인 운영분석 주제인 군수분야 문제를 해결하기 위해 (3), (4)와 같은 연구가 실시되었다.

1960, 70년대의 미국의 ORSA 연구에 가장 큰 영향을 미친 사건 중 하나는 바로 베트남 전쟁일 것이다. 베트남에 파병된 미군 본부(MACV, Military Assistance Command, Vietnam)는 자체적인 ORSA 기능을 갖추고 있었으며 (MACVEVAL 등) 전술급 제대 뿐 아니라 중대 단위 레벨까지 ORSA 기법을 적용하고자 했다. 예를 들어 외곽 방어진지 편성, 순찰 계획 스케쥴링, 콘보이 차량 적재 최적화, 차량 정비 최적화 등 다양하고 일상적인 의사결정에까지 운영분석 기법의 도움이 필요했다. 이러한 인하우스 조직 뿐 아니라 RAC와 같은 외부 연구소 역시 전쟁을 지원하기 위한 많은 연구를 수행하게 된다.

하지만 베트남 전은 통계학과 수학에 기반을 둔 운영분석 기능의 '이면(dark side)'을 확인해 준 계기가 되기도 한다. 예를 들어 미 육군은 단순히 사상자의 수치(body count)를 인용해 해당 지역 전투의 승리여부를 판단하고 전쟁의 진행경과를 설명하려 하였다. 하지만 실제 전쟁에서는 단순히 피아 사상자의 수치가 전술의 승리와 실패를 결정짓지 않으며 또한 미 육군의 통제 아래 있는 베트남 마을의 숫자가 곧 베트남 인들의 미국 지지도를 설명하지 않았던 것이다. 실제로 미국이 객관적인 숫자를 통해 설명한 많은 주장이 큰 오판이었던 경우가 발생하기 시작하며 베트남의 미 육군 지휘관들은 어느새 사상자의 수에 집착하기 시작한다. 적 사상자의 수보다 우군의 사상자의 수가 많더라도 그것이 상급제대 작전에 기여한 좋은 작전이 될 수 있음에도 잘못된 전투 성패 측정방식에 익숙해진 지휘관들이 자신의 경력 관리를 위해 'Kill Ratio'와 이를 높이기 위한 전투 방식에 매몰되기 시작한 것이다.

또한 사람들은 사상자의 숫자를 대입해 전쟁의 비용을 계산하는 cost-effectiveness 기법에서 비인간적인 면모를 발견한다. 또한 잘못된 주장을 '변호'하기 위해 통계 데이터를 가져와 쓰거나 심지어는 데이터를 선택적으로 취용하는 등 여러 가지 문제가 발생하였다. 이뿐 아니라 대인 지뢰 공중 살포 작전, 정글을 무력화하기 위한 제초제(herbicide) 살포작전 등 윤리적인 문제를 야기하는 작전 등에 대한 비판도 거세진다. 이러한 작전은 순전히 운영분석 관점에서 보면 제한된 자원에서 최대의 효과를 이끌어 낼 수 있는 '최적의' 작전이었을지 모르는데 말이다. 결과적으로 베트남 전쟁으로 ORSA는 객관성과 공정성에 큰 흠을 입게 된다. 이기지 못한 전쟁에서는 그 과가 모든 기능에게 돌아가는 것이 당연하지만 특히 베트남 전쟁에서 ORSA가 겪은 과오는 분명 짚고 넘어갈 만한 가치가 있다.

〈그림 3-14〉 에이전트 오렌지(고엽제)를 살포하는 휴이 헬기 (출처: 위키피디아)

3.8 1970 - 90년대 미국의 운영분석 연구 사례

1973년 닉슨 대통령의 종전 선언으로 베트남 전쟁이 종료된 이후 미 국방정책의 방향은 크게 두 가지로 진행되는데 첫 번째는 전후 수습과 당시 가장 위협이 되었던 공산주의 체제에 대한 대비이며 두 번째는 소련의 해체(1991)와 독일의 통일(1989) 이후 전 세계 유일무이한 경찰국가(superpower)가 된 미국의 새로운 위협에 대한 대비("new world order")라고 할 수 있다.

베트남 전 역시 냉전의 일부였지만, 전쟁 이후 미 육군은 소련의 위협으로 위시되는 냉전에 대한 적극적인 대응을 피할 수 없었다. 닉슨 행정부는 케네디의 "Flexible Response" 국방 기조를 유지해 가지만 베트남 전쟁을 통해 미국의 힘에 대한 한계를 경험하였고 냉전 전략 수행에 있어 기존 미국의 능력에 비해 훨씬 낮은 단계의 개입을 천명하는 '닉슨 독트린(Nixon Doctrine)'을 1967년 발표한다.[14]

닉슨 독트린에 따라 국방 정책에도 많은 변화가 온다. 징병제 대신 모병제가 도입되고, 군사 작전은 '지역 방어'의 개념 대신 최대한 신속하게 전개하여 최소한의 피해로 전쟁을 종결 짓는 개념(AirLand Battle Doctrine)으로 변모하며 이에 따라 새로운 개념의 훈련방식, 조직, 무기체계가 필요해 진다. 이에 따라, 미 육군은 1980년대에 이른바 Big Five의 무기체계에 집중하고 M1A1 Abrams Tank, M2/M3 Bradley infantry vehicle, AH-64 Apache Attack Helicopter, UH-60 Black Hawk, Patriot Missile System을 우선적으로 개발한다.

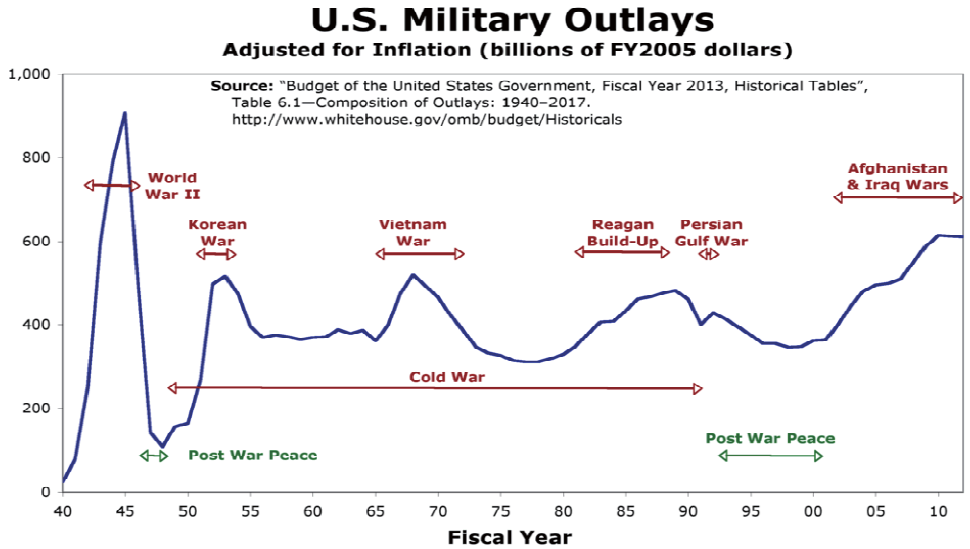
또한, 주 이란 대사관 인질사건(1979년)에서부터 시작된 중동의 위협이 본격화되었고 그레나다 침공(Operation Urgent Fury, 1983), 파나다 침공(Operation Just Cause, 1989) 그리고 걸프전쟁(Operation Desert Shield, Operations Desert Storm, 1990-1991)에까지 이르게 된다. 국제 정세의 변화에 대한 자세한 설명은 본 보고서의 범위에 벗어나며 여기서는 이러한 변화들이 운영분석 연구에 어떤 영향을 주었는지를 분석한다.

〈그림 3-15〉 1982년 AH-64 아파치의 프로토타입 (출처 : 위키피디아)

먼저 1970년대 초부터 90년대까지 국방의 가장 큰 변화는 기술적 진보의 속도

가 빨라졌다는 점이다. 무기체계에 필요한 기초 기술의 범위는 전방위적으로 확대되었다. 예를 들어 스마트 유도탄의 경우 물리, 전자, 기계, 통신, 지구 과학, 신소재, 위성 등 거의 모든 분야의 과학 기술들의 집약을 통해 만들어 지게 된다. 베트남 전 이전까지는 신 무기체계에 큰 노력을 기울이지 않았던 미군이 소련과의 경쟁을 통해 새로운 무기체계 개발에 힘을 쏟았으며 1970년부터 약 20년 동안 앞서 기술한 빅 파이브 무기체계와 더불어 지휘통신 체계, 군수품 등 전투지원체계의 비약적인 발전이 이루어진다.

이 시기 미 국방정책에 영향을 끼친 두 번째 요소는 자원의 제약을 들 수 있다. 미국 국방 예산은 1968년 베트남 전쟁 당시를 피크로 하여 1973년 이후 점점 하락세를 타게 된다. 1968년 GDP 대비 9.4%에 이르던 국방예산은 1973년에 5.5% 이하로 떨어진다. 이후 1980년대 레이건 대통령이 국방 예산을 증액하기도 하지만 여전히 이전과 같은 전폭적인 증대는 기대하기 어려웠다. 자원의 제약은 예산 뿐 아니라 인력의 제약도 포함한다. 베트남 전쟁 당시인 1968년 150만에 이르던 미 육군은 그로부터 5년 뒤 80만으로 감축된다. 지속적인 감축세에 있던 병력 규모는 한때 레이건 대통령의 빌드업으로 소폭 상승하기도 하지만 다시 감축되며 1995년에는 1940년 이후 최소 병력인 50만의 육군이 유지되기 시작한다.



〈그림 3-16〉 미군의 국방 예산
(출처 : www.art-in-society.de/AS14/PLA/MILITARY-SPENDING.html)

미 육군의 ORSA 기능은 시시각각 변화하는 복잡한 대내외 국제 환경과 급속하게 발전하는 무기체계 과학기술 그리고 제한된 자원이라는 환경 속에서 최선의 대안을 찾아내야 할 숙명을 갖게 된다. 2차 세계 대전 이후 미 육군의 씽크 탱크 역할을 주로 수행하였던 외부 연구기관들은(예를 들어, ORO, RAC, HumRRO 등) 문을 닫거나 매각되거나 다른 조직에 통합되었다. 이에 따라 미 육군은 인하우스 조직에 온전히 의지해야 하는 입장에 처하게 된다. 이러한 가운데 육군의 조직을 재편성하기 위한 연구인 STEADFAST 프로젝트가 1972년 시행된다. STEADFAST는 ORSA 기능 수행을 위한 조직을 TRADOC(미 육군 교육사령부, U.S. Army Training and Doctrine Command), AMSAA(육군 물자시스템 분석기구, U.S. Army Material Systems Analysis Activity), CAA(육군 분석센터[12], U.S. Army Concepts Analysis Agency), OTEA(Operational Test and Evaluation Agency)로 크게 구분하여 재편한다. 물론 이 네 조직이 ORSA의 모든 기능을 전부 수행하지는 않지만 당시 그리고 지금까지 운영분석 기능의 중요한 역할을 하고 있는 대표적인 기관이며 따라서 이 기관들을 중점적으로 소개한다.

TRADOC은 베트남 전쟁 이후 육군의 훈련, 개혁, 현대화 작업 등을 중앙집권화하여 통일성 있게 추진하기 위한 철학으로 전투 발전과 훈련에 관여되는 기능 등을 모두 통합하며 1973년 버지니아주의 Fort Monroe에서 창설되었으며 예하에 12개의 병과학교 등 총 17개의 조직을 보유하였다[13]. TRADOC이 맡은 ORSA 기능은 시험평가(후 기술할 OTEA와 중복), 전투 발전(Combat Development), 시뮬레이션과 워게임, 비용 대 효과분석 등이었다.

먼저 TRADOC은 각 병과학교의 운영분석 셀(부서)을 통합하여 전투 발전 업무의 주무 부서로 활용하였다. 하지만 병과별로 수준의 차이가 있었고(1978년 기준 탄약학교[14]의 근무 인원은 9명으로 50명이 편성된 기갑학교와 큰 차이가 있었다) 무엇보다도 보고서는 각 병과의 이익만 대변하는 내용들뿐이었다. TRADOC은 전투 기능별로 전투병과, 전투지원병과, 행정병과 등으로 기능을 통합하여 센터를 설립하여 여러 병과를 통합하려는 노력을 기울이기도 한다.

12) 당시 CAA의 정확한 해석은 육군 분석센터가 아니다. 하지만 현재 CAA가 Center for Army Analysis 라는 조직명으로 변경되었기 때문에 모체 부대의 이름 역시 육군 분석센터로 하는 것이 무방해 보인다.
13) 1978년 기준 총 1,193년의 부대원이 있었고 이 중 ORSA 전문가는 924명이었다. ORSA 인원 중 현역의 비율은 45% 정도였다.
14) Missile and Munitions School

TRADOC의 중요한 임무 중 하나는 워게임을 위한 전쟁 시나리오를 준비하는 것이었다. 미 육군은 이때부터 고해상도 훈련(대대급 이하), 저해상도 훈련(군단급 이상)에 대한 각각의 시나리오를 따로 발전시켜 워게임에서 활용할 수 있도록 하였다. 이 때 TRADOC이 미 해군대학원과 공동 연구하여 개발된 워게임 시뮬레이션은 STAR(Simulation Tactical Alternative Response), AMORE(Analysis of Military Organizational Effectiveness), DIME(Division Map Exercise), CAMMS(Condensed Army Mobility Management System) 등이 있다. 특히 대대급에서 여단급 까지 묘사가 가능한 시뮬레이션 모델 JANUS[15]도 이때 개발되었다. JANUS는 고성능 그래픽에 기반을 둔 User-friendly 워게임 모델로서 Stochastic 요소 등 현대 워게임 모델의 요소를 많이 보유하고 있다. JANUS는 다양한 인원에 대한 훈련용 모델로서 많이 활용되었다.

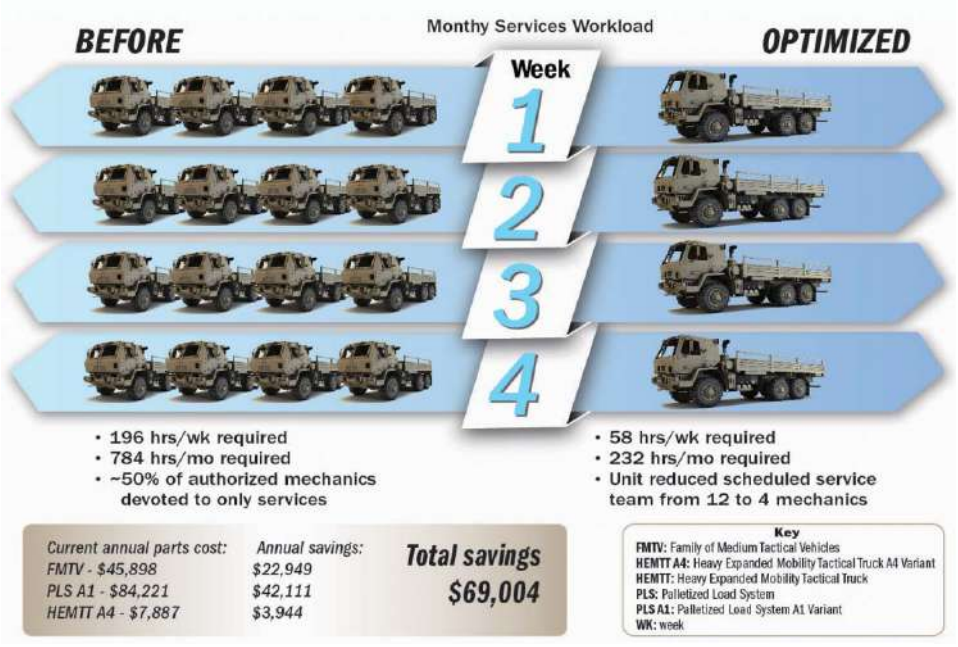
〈그림 3-17〉 현재 TRADOC의 근무 모습 (출처 : TRADOC 홈페이지)

AMSAA는 STEADFAST 프로젝트 이전인 1968년 창설되었고 STEADFAST 프로젝트 이후에도 살아남아 원래 조직을 그대로 유지하게 된다. AMSAA는 (1) 아이템 레벨의 물자들 (예를 들어, 개인화기 및 개인장비) (2) 전투지원을 위한 각 종 물자들의 통합 (3) 군수(logistics) 준비태세 등 세 가지 영역에 중점을 두고 연구 및 분석 / 시뮬레이션 모델링 분석 등을 실시하였다. 학술적으로 보면 AMSAA는

주로 시스템 신뢰성(Survivability, Reliability, Availability and Maintainability) 방법론에 중점을 두고 있었고 일부 시스템의 시험 평가(TD&E)에도 관여했다. 또한 아이템 레벨 시스템에 대한 비용 대 효과 분석 방법론도 연구하였고 그에 대한 운영요구서를 검토하는 역할을 수행하였다.

군수 분야의 준비태세를 유지하기 위해 시뮬레이션 데이터를 수집하고 각 종 훈련 데이터를 수집하는 것 또한 AMSAA의 역할이었다. AMSAA는 전 세계적으로 파견되어 있는 미 육군의 물자를 통합 관리하여 군수 분야의 대비태세를 유지하였다. AMSAA는 헬리콥터부터 소총의 탄약에 이르기까지 아이템 단위의 장비 및 물자의 수명을 관리하고 데이터를 수집하며 이를 통해 군수 작전태세를 확립하는 중요한 역할을 수행하였다.

AMSAA의 연구적 성과는 겉으로 드러나지 않지만 미군이 best-equipped 군이 되는데 크게 공헌하였으며 특히 1990년 걸프 전쟁을 통해 관리 능력을 한껏 입증한 것으로 평가받고 있다.



〈그림 3-18〉 전술차량의 예방정비 시점이 필요보다 5,000마일 정도 이르다는 결과를 도출한 AMSAA의 2018년 보고서
(출처 : asc.army.mil/web/news-alt-ond18-if-it-aint-broke)

무기체계가 복잡해지고 발전 속도가 빨라지면서 무기체계의 성능을 평가하는 것이 주요한 군의 업무로 자리 잡게 되었다. OTEA(Operational Test and Evaluation Agency)는 1972년 STEADFAST 프로젝트의 일환으로 육군의 T&E(Test and Evaluation) 업무를 관할하기 위해 설립되었다. 지금 우리 군과 마찬가지로 당시 미 육군의 시험평가 체계는 개발시험평가(DT&E, Development T&E)와 운영시험평가(UT&E[15], User T&E)로 구분되었다. DT&E는 개발업체가 성능을 평가하는 것이고 UT&E는 군이 무기 획득과 관련된 각 의사결정 단계에서 그 무기를 실제로 운용할 비슷한 환경과 조건에서 무기 성능을 평가하는 것이다.

이전에는 무기 체계를 군이 직접 개발하는 사례가 빈번하였으나 현대의 방산 생태계에서는 개발자와 운용자가 명확히 구분되는 경우가 많다. 미 육군이 OT&E와 DT&E를 서로 독립적인 기관에서 하도록 명확히 선을 그은 것도 1972년 OTEA의 설립부터이다.

OTEA의 주 임무는 (1) 운용시험평가를 기술적으로 지원 (2) 5개년 시험평가 계획의 수립 (3) 테스트 디자인 (4) 시험평가의 계획, 실행, 보고 등으로 구분할 수 있다. OTEA의 주요할 만한 성과로는 “Continuous and Comprehensive Evaluation” 체계를 수립한 데 있다.

1983년 OTEA는 현 시험평가의 문제점으로 (1) OT&E가 너무 빨라 무기체계의 실제 지원성(supportability)을 평가하기 어렵다 (2) OT&E가 너무 늦어 육군이 결점을 보완할 수 있는 시간적 여유가 없다 (3) OT&E의 평가가 너무 좁은 분야의 평가에만 집중한다고 평가하였다. 이에 대한 대응으로 OTEA는 연속 평가 개념을 도입한다.

이것은 운용시험평가를 기존보다 더 일찍 시작하고 더 늦게까지 지속한다는 간단한 개념이며 해당 결과를 지속적으로 관련 기관에 보고해 주는 것을 포함한다. OTEA는 이처럼 개발 단계 전 기간에 걸친 연속 평가를 위해 과제별로 대령급의 해당 무기체계의 경험자를 Test Manager로 편성하고 테스트와 관련된 일체의 업무를 지속적으로 수행할 수 있도록 여건을 보장해 주기도 한다. OTEA는 1990년 OPTEC(U.S. Army Operational Test and Evaluation Command)로 변경되고 이 조직은 다시 1999년 ATEC(U.S. Army Test and Evaluation Command)으로 재조직된다.

15) 우리나라에서는 OT&E(Operational T&E)로 기재한다.

〈그림 3-19〉 현재 ATEC의 T&E 사이트 모습 (출처 : ATEC 홈페이지)

OTEA/OPTEC은 아파치 헬기, 브래들리 장갑차, 험비와 같은 무기 체계부터 헬파이어, 스팅어, SAM 미사일 등 유도무기에 이르기까지 전 세계적으로 많은 성과를 거둔 무기체계의 개발에 큰 역할을 해낸다. OTEA/OPTEC은 "Adequacy. Quality. Credibility."라는 부대 철학을 유지하며 현재도 미 육군의 무기체계 획득 및 개발에 중요한 역할을 하고 있다.

마지막으로 CAA(U.S. Army Concepts Analysis Agency) 역시 1973년 STEADFAST 프로젝트의 결과로 설립되었다. CAA는 지휘관의 다양한 의사결정 지원을 위해 모든 가용한 방법론을 활용하여 분석하고 방법론을 발전시키는 역할을 하였다. CAA는 위에서 언급한 다른 조직과 다르게 고정된 반복 업무가 있는 것이 아니라 지휘관과 참모를 적시에 직접 지원하는 역할을 하였기 때문에 중요하게 평가받았다. 즉, 최고 지휘자의 "씽크탱크"역할을 수행한 것이다. CAA가 지원하는 의사결정 문제가 policy-level의 문제가 많았기 때문에 이들은 국내외 경제, 정치, 사회 등 안보 환경 변화 요소에 민감하게 반응해야 했다.

CAA는 창설 초기에는 베트남 전 이후 미 육군의 재편성에 대한 연구를 진행하였고 이후에는 서유럽에서의 미군의 역할 그리고 걸프전 무렵에는 새로운 질서 재편 등 최고 의사결정권자의 높은 수준의 결정을 지원하기 위한 역할을 수행하였

다. CAA의 연구 결과물에는 '첫' 이라는 수식어가 많이 따라 붙었는데 예를 들어 첫 번째 인공지능 Expert 시스템인 Expert System Initiative in Logistics Readiness Study, 타국을 대상으로 처음 실시된 워게임 모델인 TROMSO, 첫 번째 mixed-integer linear program model인 AAMTOR(Army Aviation Modernization Trade-off Requirement) 등이 있다. 또한 후일에 많이 활용이 되는 공학적 모델 역시 많이 개발되었다. 예를 들어 지금도 가끔 우리 군에서 활용하고 있는 COSAGE(Combat Sample Generator) 모델도 이때 개발되었다. CAA에서 개발한 모델의 전체 리스트는 [13]의 256페이지에서 확인할 수 있다.

베트남 전쟁 이후 STEADFAST 프로젝트를 통해 TRADOC, AMSAA, CAA, OTEA 등 운영분석 기능이 재편되었고 제한된 자원을 효율적으로 활용하여 최대의 성과를 획득하는 의사결정에 대한 연구가 지속되었다. 1990년 발발한 걸프전은 미 육군에서 진행된 그 동안의 연구의 성패를 가늠해 볼 수 있는 좋은 기회가 되었다. 54만의 병력과 약 9천억 톤에 해당하는 탄약, 1.7천억 갤런의 연료를 효율적으로 수송해야 했고 전쟁을 단기간에 마칠 수 있는 효과적인 작전 계획 수립이 필요했다. 미 육군 Thurman 장군은 다음과 같은 말을 남겼다.

"사막의 폭풍 작전의 승리는 7개월의 전투, 또는 44일의 공중 작전, 또는 100시간의 지상군 작전의 결과물이 아니다. 이 승리는 1970년 이후부터 꾸준히 육군을 발전시켜 온 수없이 많은 이들이 있기 때문에 가능했다."

〈그림 3-20〉 걸프전쟁에서 파괴된 T-72, BMP-1 장갑차 (출처: 위키피디아)

그러면서 그는 이라크 전쟁의 승리 요소는 다음과 같이 기술하였다.

1) Superior weaponry and equipment (in particular the so-called Big Five)
2) Superior organization
3) Superior tactical doctrine and operational strategy
4) Superior leadership, soldier skills, and morale, training
5) Superior overall allocation of resources, planning and execution of plans.

우리는 본 장에서 70년대 이후 미 육군이 위 5개의 승리요소를 달성하기 위해 운영분석 기능을 어떻게 활용하였는지를 살펴본바 있다. 이라크 전에서 그 능력을 발휘한 빅 파이브 장비(본 절의 앞 단락 참조)의 개발에 AMSAA와 OTEA가 역할을 하였다. 이들은 작전 중에도 끊임없이 데이터를 수집하고 현장에서 무기에 대한 정보를 제공한다. TRADOC은 새로운 무기 체계를 적용한 새로운 전투 교리(AirLand Battle 등)를 제공하였다. TRADOC의 새로운 훈련 시스템도 그 몫을 다했는데 이라크 전쟁에서 MILES(Multiple Integrated Laser Engagement System) 훈련의 성과는 주요했다고 평가받고 있다. CAA는 다른 기관과 다르게 직접적으로 이라크 전쟁에 기여하지는 못한 것으로 보이지만, 사막의 방패, 폭풍 작전 간 지휘관의 복잡한 의사결정을 지원하였고 무엇보다 PERSIAN TIGER 89라는 시뮬레이션 워게임을 통해 전쟁에 기여한다.

〈그림 3-21〉 미 육군의 마일즈 장비 착용 모습 (출처 : asc.army.mil)

1991년 제 59회 MORS 학회에서는 걸프 전쟁에서 컴퓨터 시뮬레이션과 분석평

가 기능 지원을 통해 미 육군이 획득한 교훈을 주제로 세미나가 개최된다. 회의에서 논의된 주장은 다음과 같이 정리된다. 의역이 들어간 경우 원문을 함께 표기하였다.

〈표 3-8〉 걸프전쟁을 통해 본 운영분석 기능의 역할

구분	교 훈
Class A (constant)	- 분석가들을 현장에 위치시키고 지휘관과 참모에게 신뢰를 얻게 할 것 - Be timely, roughly right : 정확성보다는 신속성이 더 중요하다 - 항상 예상하지 못한 질문에 대비하라 - 항상 단순함, 투명함, 기본을 유지하라 - 전시 분석을 위해서는 평시 훈련이 반드시 필요하다
Class B (trends)	- 분석에서 컴퓨터의 영향은 커지고 있다 - 소프트웨어 분석 틀은 점점 더 사용이 쉬워지고 있다(비전문가도 사용 가능) - 양질의 데이터에 대한 수요는 그 공급보다 훨씬 더 빠르게 발생한다 - 연합 및 합동 분석의 필요성이 증대되고 있다 - 전쟁술(art)에 대한 분석 필요성이 커지고 있다 - 잘못된 분석과 데이터에 대한 위험성이 이전보다 커지지는 않는다
Class C (variables)	- 환경의 특별함(peculiarities)이 무기체계의 사거리, 마모, 정확성에 미치는 영향이 크다. - 많이 연구되었지만, 아직 풀리지 않은 문제들은 그 쓰임새가 많다 - 항상 명확하고 robust한 해를 추구하라. 복잡한 가정 하에 도출된 해는 반드시 그 가정이 반하는 상황이 발생하며 해가 쓸모없어진다.

4. 시사점

본 장에서는 2장, 3장을 통해 분석한 영국, 미국의 운영분석 연구 사례들을 통해 우리가 얻을 수 있는 시사점에 대해 논의한다.

운영분석 학문의 성격 : 본 연구 보고서 제 2장에서 제 2차 세계대전 시 운영분석 기능에서 활약을 했던 전문가들에 대해 설명하며 이들이 각자의 분야에서 깊은 전공 지식을 가지고 있었지만 국방 현장에서 도출되는 다양한 문제 해결을 위해서는 오히려 여러 분야의 지식과 경험을 통섭할 수 있는 능력이 필요하다고 소개한 바 있다. 대부분의 의사결정 문제가 그러하듯 현실의 문제는 단순히 한 분야의 상황만 고려하여 해결되지는 않는다. 따라서 운영분석 전문가들은 다양한 지식, 변화하는 환경을 잘 이해하고 가장 효과적인 분석 방법을 찾아야만 한다. 운영분석은 이러한 면에서 통섭적 인재를 양성할 수 있는 훌륭한 학문이다. 많은 교육 전문가들은, 4차 산업혁명 시대에는 반복된 업무를 수행하기 위한 Specialist 보다는 창조적인 업무를 수행할 수 있는 Generalist 가 필요하다고 말하고 있다. 여러 학문 분야를 잘 어울려서 최선의 대안의 도출해내야 하는 운영분석 학문이 그래서 더 필요해질 것이라고 생각된다.

연구 결과물의 질적 수준 제고 : 2차 세계대전 이후 미 육군의 든든한 연구 파트너였던 ORO(Operations Research Office)가 몰락한 이유, 맥나마라의 시스템 분석 개혁이 마지막에 비판받았던 이유에는 여러 가지를 들 수 있겠지만 가장 근본적인 원인 중 하나는 이들 연구 결과물의 질적 하락을 들 수 있다. 많은 예산과 오랜 기다림을 통해 수행된 프로젝트가 수요자이면서 제안자였던 군의 기대 수준에 못 미치는 상황이 반복되면 연구기관은 점점 신뢰를 잃게 된다. 그리고 결국 기관의 존재 이유마저도 찾기 어려운 상황이 된다.

ORO는 자신들의 연구 도메인(범위)을 무리해서 확장해 나간 과오를 범했고 이것이 연구물의 질적 하락을 가져왔다. 맥나마라는 시스템 분석에 입각한 자신의 국방 철학을 군과 잘 공유하지 못했다. 군은 숫자와 컴퓨터로 모든 것을 설명하려는 그의 시도에 반감을 가졌음이 당연해 보인다. 이처럼, 비록 어떤 연구물의 질적 수준이 실제로는 높았다 하더라도 그것을 잘 설명하고 공유하고 이해를 구하지 못하

면 좋은 연구로 인정받지 못하게 된다. 2차 세계대전 시 영국 수상 처칠에게 논리정연한 '눈높이' 보고를 통해 자신의 주장을 관철시킨 Dowding의 지혜가 필요한 이유가 여기에 있다. 특히, 연구 결과물의 수요자가 '비전문가'라면 이러한 노력은 더더욱 중요해 진다. 운영분석가들은 결국 정책을 반영하고 실현하는 이들은 자신의 아니라 그들임을 깨달아야 한다.

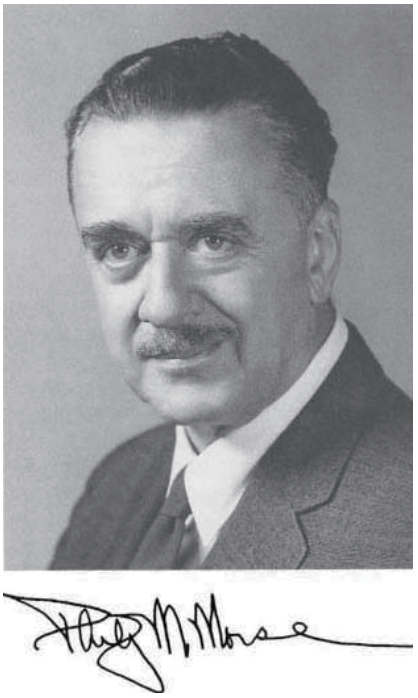
민간과 군의 연구 협력 : 운영분석이 생겨나고 학문으로 발전하여 오늘에 이르기까지 운영분석 기능에는 항상 민간인 전문가와 군 전문가가 함께 자리하고 있었다. 성공한 운영분석 연구 사례에서 공통적으로 나타나는 현상은 민간 과학자들과 군인이 각자의 몫을 잘 해내었고 협력이 잘 되었다는 점이다. 어느 시대, 어느 조직에서나 항상 서로 다른 태생을 가진 두 집단에 크고 작은 문제가 있었지만 대부분의 경우 서로를 잘 이해하면서 원만하게 해결이 되었다. 미 해군은 2차 세계대전 시 민간 과학자들이 out of uniform인 상태를 유지하게 끔 해주었고 이들은 모든 계급으로부터 자유로울 수 있었고 이를 통해 그들의 지적 자유(intellectual freedom)를 영위할 수 있다고 진술한바 있다. 반면, 맥나마라의 "군사적 직관/경험 보다는 팩트를 선호(preference for fact over experienced military judgement)"하는 사상은 민간 국방장관으로서 군을 이해하기 위한 노력이 부족했음을 보여주는 것이며 결국 마지막에는 성공한 정책을 이끌어 내지 못했다. 우리 군 역시 다양한 조직에 군인과 민간인이 함께 근무하고 있다. 두 집단의 역량 각자의 장점을 잘 융합하여 시너지 효과를 발생시킬 것인지 아니면 독립된 두 개의 섬처럼 존재할 것인지는 서로의 노력에 달려 있다.

운영분석 연구의 실용성 : 운영분석은 학문이 생겨난 그 시작점에서는 분명 실용(application)을 추구하였다. 전쟁에서 승리하기 위한 다양한 문제들에 대해 해결책을 찾아야 했기 때문이다. 운영분석이 전후 일반 학문으로 자리를 잡으면서 수학, 통계 등이 강조되며 특히 최적화(optimization) 이론이 크게 발전하고 있다. 하지만 한편으로는 운영분석가들이 너무 이론에만 치중하는 것이 아닌가 하는 우려가 생기기도 한다. 예를 들어 대표적으로 어려운 문제로 뽑을 수 있는 Steiner Tree Problem (STP)의 경우 많은 최적화 이론가들이 이 문제를 연구하고 있지만 정작 이 문제가 세상의 어떤 문제를 풀어낼 수 있는지에 대한 관심이

크지 않다는 것이다. 군사운영분석 연구의 선구자인 P. M. Morse의 우려를 우리는 주의 깊게 살펴볼 필요가 있다.

"Operations Research is an experimental science, concerned with the real world. It is not an exercise in pure logic"

Morse는 운영분석이 현실의 문제를 풀기 위한 연구를 지속해야 함을 강조하고 있다. 또한 이를 위해서는 어떤 "분석의 결과(prediction)"와 "실제 결과(actual occurrences)"를 정량적으로 비교할 수 있어야 하며 그것을 끊임없이 추구해야 한다고 말하고 있다.



〈그림 4-1〉 Philip McCord Morse

운영분석 연구의 이면(Dark Side) : 맥나마라의 시스템 분석 개혁은 결국 베트남 전쟁의 패배라는 '결과'를 통해 실패한 것으로 평가받고 있다. 만약 이 전쟁이 승리하였더라면 맥나마라의 시스템 분석은 성공한 사례가 되어 있을지 모른다. 이

렇듯 시대의 평가는 그것의 결과에 따라 달라지며 정치적, 사회적 평가가 덧 붙여져 본래 그것 그대로의 평가를 온전히 받지 못하게 된다. 이러한 면을 차치하고서라도 맥마나라의 정책이 비판받는 이유는 사실 운영분석 학문이 가지고 있는 이면을 그대로 노출시켰기 때문이다. 베트남 전쟁에서 미군은 'body count' 신드롬에 빠진다. 작전의 성과를 적 사상자 대비 우군의 사상자 비율로 계산하기 시작하면서 지휘관들이 경쟁에 빠지게 되었고 이는 'body count' 인플레이션 이라는 초유의 사태를 유발하기도 한다. 어느새 지휘관들은 그렇게 '비율'을 늘이는 것이 잘한 작전이라는 착각에 빠지기 시작했고 전략, 전술, 전투기술 등이 그 숫자를 늘리기 위한 테크닉으로 전락해 버린다. 우리는 숫자는 거짓말을 하지 않는다고 얘기하지만 때로는 숫자가 불필요한 이야기를 우리에게 해주기도 한다. 국방 및 안보 분야에서 운영분석이 단순히 공학자들의 놀이터가 되어서는 안되는 이유가 여기에 있다.

항상 최선을 전략을 추구하는 운영분석의 철학이 전쟁에서는 큰 윤리적 문제를 야기하기도 한다. 어느 전쟁에서든 비용을 최소화하면서 성과를 극대화하기 위한 대안을 운영분석이 제공하고 있다. 그것이 최소의 비용으로 최대한 많은 적을 살상할 수 있는 비대칭무기의 개발이든, 정글을 적은 비용으로 제거하기 위한 고엽제의 사용이든, 데이터 수집을 목적으로 하는 전쟁포로에 대한 무자비한 심문이든 말이다.

참고문헌

[1] 조남석, “최적화 이론의 국방분야 적용 방안”, 군사과학정책연구 제 10권, 2017
[2] 홍성필, 『경영과학』, 율곡출판사, p. 22
[3] JCS, Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms, 1994 , p. 277.
[4] Charles R. Shrader, History of Operations Research in the United States Army Vol I : 1942-1962, 2006
[5] M. W. Kirby, Operational Research in War and Peace : The British Experience from the 1930s to 1970., Imperial College Press, 2003
[6] Wikipedia.org , 검색어 : Operation Starvation, 검색일 : 2019. 9.
[7] Frederick M. Sallagar., Lessons from an Aerial Mining Campaign (Operation Starvation), Rand, 1974
[8] Charles W. McArthur, Operations Analysis in the U.S. Army Eighth Air Force in World War II, American Mathematical Society, 1985
[9] Morse PM, Kimball GE., Methods of Operations Research, Peninsula Publishing, 1970
[10] History of AR, Website : ccijax.com
[11] Alain Enthoven, How systems Analysis, Cost-Effectiveness Analysis, or Benefit-Cost Analysis First Became Influential in Federal Government Program Decision-Making, Journal of Benefit-Cost Analysis, Vol 10, Issue 2, pp. 146-155.
[12] Charles R. Shrader, History of Operations Research in the United States Army Vol II : 1961-1973, 2008
[13] Charles R. Shrader, History of Operations Research in the United States Army Vol III : 1973-1995, 2009
[14] Wikipedia.org , 검색어 : Nixon Doctrine, 검색일 : 2019. 9.
[15] M.D.Bowley and M.S.Lovaszy, Use of Combat Simulations and Wargames in Analytical Studies.

연구보고 2019

북한의 사이버위협 변화 양상과 정책적 함의

이 수 진
(국방대학교 교수)

2019. 12.

국방대학교 국가안전보장문제연구소

목 차

그림목차

표 목 차

요 약 문

본 연구는 2004년부터 본격적으로 대한민국을 향하기 시작한 북한발 사이버위협 사례를 조사하고, 그 결과를 바탕으로 사이버위협의 양상이 어떻게 변화되어 왔는지를 분석한 후 그러한 변화가 가지는 전략적 의도 추정을 통해 대한민국이 대비해 나가야 할 정책방향을 도출하기 위해 실시되었다.

북한의 사이버위협 양상은 크게 3단계에 걸쳐 변화하였다. 1단계는 사이버전의 중요성을 인식하고 사이버역량 확충을 도모하기 시작했던 2004년부터 2009년까지의 시기로, 대한민국의 정부기관을 대상으로 한 정보수집 목적의 사이버공격이 주로 수행되었으며, 결정적인 사이버공격을 수행하기 위한 준비작업이 꾸준하게 진행되었다. 2단계는 김정은의 후계 구도가 거론되기 시작한 2009년부터 국제사회 제재가 본격화되기 시작한 2016년까지로, 사이버역량이 성숙해진 이 시기에는 김정은의 후계구도를 공고히 하기 위한 과시목적의 사이버공격을 시작으로 국제사회에 북한의 존재를 확실하게 각인시키는 대규모 사이버공격들을 활발하게 수행하였다. 대부분의 공격들이 군사적 도발행위와 교묘하게 연결되어 있으며, 사회불안을 조장하고 국민적 불안감을 증폭시킬 수 있는 사회기반시설 공격이 주로 수행되었다. 3단계는 대북제재가 본격화되기 시작한 2016년 이후로, 이 시기에는 대한민국을 대상으로 하는 사이버공격이 확연하게 감소하였으며, 대부분의 사이버역량을 금융권 공격에 집중시켜 단기간에 막대한 재화를 마련하였다.

이상과 같은 3단계에 걸친 북한의 사이버위협 양상변화는 한반도 안보상황과 국제안보환경 변화에 유연하게 대처하기 위해 사이버역량 사용의 전략적 목표를 잠깐 전환한 것으로 볼 수 있으며, 북한발 사이버위협의 본질은 변화하지 않았고 언제든지 다시 대한민국의 사이버공간을 위협할 수 있을 것으로 판단된다. 따라서 잠시 동안의 평화모드에 안주하지 않고 미래를 대비하는 준비가 필요하다.

1. 연구개요

1.1 연구배경 및 목적

북한에게 있어 사이버능력의 사용은 실현 가능하고 지속가능한 군사적 선택을 제공해 왔다. 책임귀속에 비교적 자유로운 상태에서 대한민국을 비롯한 적대국가의 국익을 저해하고 심리적·물리적·경제적 측면에서 타격을 가할 수 있는 효과적인 수단이 바로 사이버능력의 사용이었으며, 미사일 발사 및 핵실험과 병행하여 군사적 긴장을 더욱 고조시키면서 사회불안을 조장하는 보조적인 수단으로 사이버능력을 사용하기도 했다. 2018년 신년사를 통해 평창동계올림픽을 계기로 대한민국과의 관계개선 의지를 밝힌 이후에는 대한민국을 향하는 직접적인 사이버공격이 확연하게 줄어들기는 했지만, 한반도 상황 변화를 의도된 방향으로 이끌고 좀 더 유리한 입장에서 지향하는 바를 달성하기 위해서라면 언제든 사이버역량을 사용할 가능성은 존재하며, 즉시 실행에 옮길만한 충분한 역량도 갖추고 있다.

미국의 사이버보안업체 '크라우드 스트라이크(CrowdStrike)'가 2019년 2월 발표한 연례 보고서 『Global Threat Report』에 의하면, 북한은 러시아에 이어 세계 2위의 사이버공격 능력을 갖추고 있는 것으로 나타났다.[1] 미국 국방부도 2015년 새로운 국방사이버안보전략을 발표하면서 북한을 러시아, 중국, 이란과 함께 미국에 가장 심각한 사이버위협을 가할 수 있는 잠재적 적성 국가로 분류한 바 있다.[2]

대한민국을 대상으로 한 북한의 대규모 사이버공격 시도는 2004년 처음으로 발생하였다. 당시 국회, 원자력연구원, KIDA, ADD 등을 포함한 정부기관 서버 235대 및 기업 · 대학기관 서버 79대 등 총 314대의 컴퓨터가 DDoS 공격 및 해킹을 당하였으며, 공격의 근원지는 북한에 임대된 중국 IP 주소임이 확인되었다.[3]

---

1) 데이터를 훔치기 위해 침입자가 초기 진입 지점을 넘어 네트워크의 다른 시스템에 도달하는 데 걸리는 시간을 의미하는 '브레이크 아웃 타임(breakout time)'이라는 측정지표를 조사하기 위해 2018년 발생한 3만 건의 사이버공격을 분석하였다. 그 결과 북한은 목표까지 도달하는 시간이 2시간 20분으로, 4시간인 중국을 가뿐하게 앞지르며 러시아에 이어 2위를 차지했다.

2) U.S. Department of Defense, "Summary: Department of Defense Cyber Strategy 2018", 2018. 9. 18.

3) Mansourov, "North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance", 2014.12.2.

2005년 8월에는 군 통신채널에 대한 침투가 시도되었으며, 2007년 8월에는 3군 사령부 및 화학관련 기관이 공격을 당한 바 있다. 이렇듯 초창기의 북한 사이버공격은 주로 군 관련 기관 및 정부기관을 대상으로 하여 기밀정보수집 활동 위주로 진행되었다. 이후 2009년의 7.7 DDoS 공격을 계기로 사회기반시설을 대상으로 한 DDoS 공격 및 APT 공격을 활발하게 수행되었으며, 2016년 후반기부터는 국제사회 제재가 가속화되면서 악화된 경제상황을 극복하기 위해 금전적 이득을 취하기 위한 방향으로 사이버공격이 전환되었다.

UN 안전보장이사회 산하의 대북제재위원회가 2019년 9월 5일에 공개한 중간보고서에 의하면, 최근 북한의 사이버활동이 가상화폐 해킹을 중심으로 진행되고 있으며, 북한 정찰총국 산하 121국 등이 지난 2015년 12월부터 2019년 5월까지 최소 35차례의 사이버공격을 통해 최대 20억 달러(한화 약 2조4천억 원)를 벌어들인 것으로 분석되었다. 또한 총 17개국을 대상으로 이뤄진 사이버공격에서 대한민국의 피해 건수가 10건으로 가장 많았다.[4] 미국이 북한을 공식적인 공격의 배후로 지목했던 2017년의 워너크라이 사태도 전 세계적으로 총 99개국의 컴퓨터 12만대 이상이 감염되면서 40억 달러의 피해가 발생하였다.[5]

그러나 최근 들어 북한의 사이버공격 빈도가 과거에 비해 획기적으로 감소하면서 북한의 사이버위협에 대한 관심도 서서히 줄어들고 있다. 미국을 비롯한 주요국들은 대부분 북한의 사이버역량에 대해 우려를 표하면서 사이버안보에 대한 최대 위협국으로 북한을 지목하고 있는 상황임에도 불구하고, 그와 마주하고 있는 대한민국은 큰 경각심을 느끼지 못하고 있다. 표면적으로는 북한의 사이버위협이 줄어든 것처럼 보이지만, 사이버능력의 사용을 통해 북한이 추구하고자 하는 바는 시간이 흐르더라도 달라지지 않을 것으로 판단된다. 이에 본 연구에서는 2004년부터 대한민국을 대상으로 진행되었던 북한의 사이버공격에 대해 조사하고, 한반도 안보상황과 국제정치의 변화로 인해 북한의 사이버위협 양상이 어떻게 변화되어 왔는지를 분석하여 그 이면에 담겨진 전략적 의도를 추정할 것이다. 또한 최근의 사이버위협 양상 변화가 대한민국의 사이버안보에 미칠 수 있는 영향과 정책적 함의에 대해 논의한다.

4) 연합뉴스, 『해상환적부터 가상화폐까지… 유엔, 北 전방위 제재회피 '경고등'』, 2019. 9. 6.
5) VOA, 『북한 사이버 공격 능력 세계 최상위…정예요원 7천명』, 2019. 8. 16.

본 연구의 목표는 다음과 같이 요약된다.

① 공개된 문서상에서 공식적으로 공격주체로 언급되기 시작한 2004년 이후의 북한發 사이버공격들을 조사하고, 해당 시기에 발생했던 핵실험과 미사일 발사 등의 군사도발행위와의 연관성을 분석한다.

② 상기 ①항에서의 결과를 바탕으로 사이버위협의 양상 변화에 따른 북한의 전략적 의도 변화를 추정한다.

③ 상기 ①항과 ②항의 연구 결과를 바탕으로 국방 및 국가 사이버안보 발전에 참고할 수 있는 정책적 시사점을 도출한다.

1.2 연구범위 및 방법

북한에 의한 사이버위협의 심각성을 경고하고 굳건한 사이버안보태세 강화를 위한 쟁책추진방향을 제시한 연구들을 다수 발표된 바 있다. 그러나 최근 들어서는 사이버공격의 양상이 금전적 이득을 노리는 랜섬웨어 공격이나 가상화폐 거래소 공격으로 전환되면서, 북한의 사이버위협을 안보차원에서 다루는 연구들은 확연하게 줄어들었다. 그리고 북한의 사이버공격을 단편적으로 정리하고 분석한 자료는 일부 확인할 수 있었으나, 북한발 사이버공격을 전체적인 차원에서 분석하면서 변화양상과 더불어 전략적 의도의 변화까지 종합적으로 분석하여 제시한 연구는 확인할 수 없었다. 이러한 측면에서 본 연구는 독창성을 가질 수 있을 것으로 판단되며, 북한의 사이버위협을 보다 넓은 시각으로 바라볼 수 있도록 해주는 좋은 참고자료가 될 것으로 기대한다.

연구목표를 달성하기 위해 다음과 같은 내용을 중점 조사하고 분석하며, 인터넷상 공개된 문서를 기준으로 공격주체를 명확하게 북한으로 지목한 사이버공격만을 연구대상으로 한다.

① 북한發 사이버공격 현황 : 공격 형태, 대상 및 시기, 피해 규모, 정부 차원의 대응 유무, 해당 시기에 발생한 군사도발행위 등

② 시기 구분에 의한 북한發 사이버공격의 전략적 의도 추정

③ 북한發 사이버공격의 양상 및 전략적 의도 변화가 국방 및 국가 사이버안보에 미치는 영향 분석 및 정책적 대응방안 제시

연구진행은 기본적으로 출처 확인이 가능한 공개된 자료를 위주로 조사 및 분석을 실시한다. 자료를 정리함에 있어서는 사이버공격의 기술적 내용에 대한 배경지식이 부족한 독자들을 고려하여 세부적인 공격기술에 대한 분석은 배제하고, 공격의 형태 및 대상, 해당 공격 발생 시기의 한반도 안보상황 및 연계된 남북한의 군사행동 등을 중점적으로 조사한다. 그리고 사이버공격이 가지는 전략적 의도의 추정은 동일한 유형을 보이는 공격을 하나의 집단으로 분류하여 당시의 안보상황과 연계하여 실시한다. 마지막으로 공격양상 및 전략적 의도의 변화에 부합하는 정책 추진 방향을 제시함에 있어서는 국방 및 국가 사이버안보에 미치는 영향을 분석한 후 국방영역에서 사이버안보태세 강화를 위해 중점적으로 고려해야 할 정책방향을 제시하고자 한다.

2. 북한의 사이버역량

북한이 사이버공간을 전략적 중요성이 높은 전장으로 인식하고, 비대칭전력으로서의 사이버역량을 적극 활용하고 있음은 자명한 사실이다. 이는 북한의 전현직 최고 지도자들이 사이버공간의 중요성과 사이버전 수행역량 강화의지를 적극적으로 천명했던 것에서 쉽게 확인할 수 있다.

김정일 국방위원장은 '이라크전쟁'을 지켜보면서, 지금까지의 전쟁이 총알과 석유에 관한 전쟁이었다면 21세기의 전쟁은 정보에 관한 것이며, 누가 평시에 적의 군사기술정보에 더 많이 접근할 수 있는지, 그리고 적의 군사지휘통제정보를 얼마나 효과적으로 교란시킬 수 있으며 자신의 정보는 얼마나 효과적으로 활용할 수 있는지에 의해 전쟁의 승패가 좌우된다고 말하면서 사이버전의 중요성을 강조한 바 있다.[6] 현재 북한의 지도자인 김정은 역시 집권 초기인 2013년 간부들에게 "사이버전은 핵, 미사일과 함께 인민군대의 무자비한 타격 능력을 담보하는 만능의 보검"이라고 강조하며, 사이버전 수행역량을 확충시켜 나가겠다는 의지를 천명한 바 있다.[7] 그 해 2월에는 정찰총국 예하 해커부대를 방문, "강력한 정보통신 기술, 정찰총국과 같은 용맹한 (사이버) 전사들만 있으면 그 어떤 제재도 뚫을 수 있고, 강성국가 건설도 문제없다"고 말하며, 북한의 사이버역량에 대해 강한 자신감을 내비치기도 했다.[8]

이와 같은 최고 지도자들의 의지에 발맞춰 북한은 비대칭전력으로서의 사이버전 수행역량 확충을 위해 조직을 보강하고, 교육체계의 정비를 통해 인력을 지속적으로 확보해 왔으며, 기술개발에도 박차를 가한 결과 현재는 전 세계의 사이버공간을 위협하는 강력한 강자로 부상하고 있다.

그러나 북한의 사이버역량을 정확하게 평가할 수 있는 공개된 자료는 거의 없다. 그동안 발생했던 사이버공격들 중 북한이 공격주체로 지목된 공격들에 대한 분석을 근거로 북한이 상당한 능력을 가졌을 것이라 추정할 뿐이며, 조직이나 인력과 관련해서도 탈북자의 증언에 의존하여 추정하는 자료들이 대부분이다. 따라서 본 보고서에서도 구체적이고 검증 가능한 자료를 제시하는 것은 제한되기 때문에,

6) J. Y. Kong, K. G. Kim, and J. I. Lim, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies", 2019 11th International Conference on Cyber Conflict: Silent Battle, 2019. 5.
7) DailyNK, 『 '만능의 보검' 北사이버 전사, 암호화폐부터 군사기밀까지 노린다』, 2019. 9. 16.
8) 조선일보, 『김정은, "용맹한 사이버 전사 있으면 어떤 제재도 뚫어"』, 2013. 4. 8.

공개된 인터넷 상 자료와 주요국들의 북한에 대한 평가 결과들을 바탕으로 사이버 역량을 가늠해 보고자 한다.

2.1 사이버 인프라

북한 사이버 인프라의 특징은 인터넷과 인트라넷의 이원화와 인터넷에 대한 강력한 국가통제를 들 수 있다. 1990년 초 과학원, 김일성 종합대학 등 주요기관에 대한 LAN 설치를 시작으로, 1998년에는 처음으로 인트라넷 개념의 컴퓨터네트워크인 '광명'를 완성하였다. 2000년 10월 노동당 창건 55주년을 계기로 전국을 광케이블로 연결하는 인트라넷을 구축하기 시작했고, 2002년 11월부터 전국적인 국가범위의 인트라넷 서비스를 개시했다.[9] 그러나 인터넷으로 인한 체제오염을 우려하여 인터넷과 인트라넷을 이원화하여 운영하면서, 북한 주민들의 인터넷 사용뿐만 아니라 인트라넷 사용까지도 철저하게 통제하고 있다.[10]

인트라넷은 다시 일반 주민을 위한 '광명'과 국가보안성 전용망인 '붉은검', 국가보위부 전용망인 '방패', 인민군 전용망인 '금별'로 구분된다. 2013년 5월 초, 국제 해커단체인 '어나니머스(Anonymous)'가 북한 정부기관의 인트라넷과 일반 웹사이트 수십 곳을 공격하겠다고 예고했을 때, 주요 인트라넷 4개 망도 공격 대상으로 지목된 바 있다.[11]

북한이 인터넷에 등장하기 시작한 것은 2001년 중국의 퉁티엔 부동산회사의 이름으로 중국 선양과 북한 평양에 각각 인터넷 서버를 구축하여 북한주민과 외국인

9) 이수진, "사이버테러 및 사이버전 대응 동향", 국방대학교 안보문제연구소 군사과학정책연구 제5권, p.105, 2011. 9.

10) 2011년 2월 15일, 미국 상원 빌딩에서 미 방송위원회(BBG) 주최로 '뉴미디어 혁명과 지구촌 참여(engagement)'를 주제로 한 토론회가 개최되었다. 토론회에서 발표된 자료에 의하면, 외부와 연결된 인터넷은 없지만 북한 안에서만 연결되는 인트라넷은 상당히 발달되어 있다고 한다. 인트라넷 주소를 갖고 있는 기관이 수천 개나 되며, 2004부터 2007년까지 인트라넷용 광케이블을 주요 도시와 읍까지 연결한 덕분에 평양의 데이터 전송속도는 70~80Mbps, 지방은 10Mbps로 대한민국의 2000년대 초반 수준은 유지하고 있다. 그러나 2000년대 중반까지 비교적 자유롭게 사용했던 내부 인트라넷이 2006년의 사건을 계기로 통제되기 시작한다. 2006년 6월 평양의 한 누리꾼이 북한 최초 홈페이지 조선컴퓨터센터(컴퓨터 관련 국영연구소)의 '내나라' 개설 10주년을 기념해 '평양체육관에서 농구경기를 하자'는 글을 게시판에 올리자 실제로 300여 명이 체육관에 나타난 사건이 발생하면서 가정에서의 인트라넷 접속이 차단되었고, 당국은 즉시 인트라넷 집중검열을 실시하기 시작했으며, 북한 전역에서 우후죽순처럼 생겨났던 PC방이 모두 폐쇄되는 결과로 이어졌다. 현재 북한의 인트라넷은 가정에서의 접속이 불가능하며, 기관을 통해서만 접속이 가능하다.(출처: 동아닷컴, 『지구촌 인터넷 혁명, 북 파고들 가능성은…' 美방송위 토론회』, 2011. 2. 17.)

11) VOA, 『어나니머스, 다음달 25일 북한 전산망 공격 예고』, 2013. 5. 8.

사이에 이메일 교환서비스를 제공하는 '실리뱅크'(www.silibank.com) 사이트가 개설되면서 부터이다.[12] 그리고 2010년 8월에는, 트위터와 페이스북, 유튜브 등에 우리민족끼리 계정을 개설하기 시작했다. 그러나 페이스북 계정은 이용약관 위반을 이유로 개설된 지 5일 만에 폐쇄조치를 당했다.[13]

상당히 폐쇄적으로 운영되어 왔기에 외부에 거의 알려지지 않았던 북한의 IT 환경이 전 세계 미디어의 주목을 받게 된 결정적 계기는 2013년 1월에 실시된 구글의 에릭 슈미트 회장과 빌 리처드슨 뉴멕시코 주지사의 방북이었다. 비록 에릭 슈미트 회장은 북한 주민들의 인터넷 사용이 철저하게 차단되고 있으며 대학생들도 두 명이 서로 감시를 하면서 사용해야 하는 상황을 두고 세계 최악이라고 평가했지만,[14] 이들의 방북을 계기로 북한 내에도 가시적인 변화가 일어났다. 북한은 2013년 1월 21일 3G 이동전화서비스를 외국인에게도 허용할 것을 발표하였고, 1월 29일에는 구글의 지도 카테고리에 북한 및 평양지도가 업데이트 되었다. 이어서 2월 26일에는 북한의 3G 망을 이용한 첫 번째 인스타그램(Instagram) 포스팅이 북한 내 AP통신 기자를 통해 이루어졌는데, 이것이 북한에서 발신한 첫 번째 공식적 소셜미디어 포스팅이라 할 수 있다.[15]

김정은 집권 이후 북한 사회의 가장 큰 변화 중 하나는 이동통신의 보편화를 들 수 있다. 탈북자의 증언에 의하면, 평양 거리에서도 '스몸비'(스마트폰 좀비)의 모습은 종종 포착된다고 한다. 2013년 외국인에게 인터넷 접속 권한이 허용되기 시작한 이후, 현재에는 현지에서 국제유심을 구입하여 장착하면 인터넷 접속과 국제전화까지도 가능하다. 2018년 5월 풍계리 핵실험장 폐기 행사에 참석했던 한국 취재진도 이런 방식을 이용하여 취재 내용을 전송한 것으로 알려져 있다. 그러나 국제유심을 이용한 북한 내 전화 및 인트라넷 접속은 제한되며, 그와 마찬가지로 북한 주민들의 이동통신사용은 북한 정부가 관리하는 인트라넷인 광명을 통해서만 이루어진다.[16]

이상에서 살펴본 바와 같이 북한의 사이버 인프라는 정부의 철저한 통제 속에서 인터넷 사용은 거의 불가능하며, 내부 인트라넷인 광명을 통해서 통제된 정보만

12) 김유향, "북한의 통신·인터넷 현황과 전망", KISO 저널 제32호, 2018. 9.
13) 조선닷컴, 『페이스북, 북 계정 '우리민족끼리' 5일만에 폐쇄』, 2010. 8. 24.
14) VOA, 『구글 회장 "북한 인터넷 상황 세계 최악"』, 2015. 4. 27.
15) 김유향, "북한의 통신·인터넷 현황과 전망", KISO 저널 제32호, 2018. 9.
16) 한겨레, 『평양 거리에도 '스몸비'…북 400만~500만명이 셀카·채팅』, 2019. 3. 11.

이용 가능한 상황이지만, 이러한 통제와 인터넷에 대한 낮은 의존도는 방어 측면에서 보면 북한에게 아주 강력한 전략적 이점을 제공해 준다.

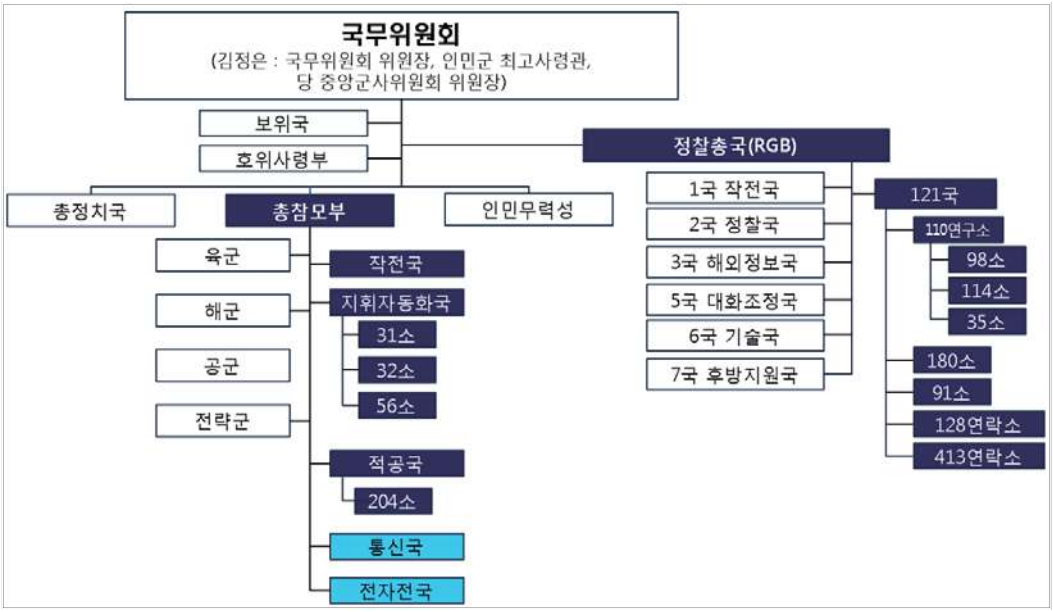
2.2 조직 및 인력

북한의 높은 사이버전력 수준을 가늠하기 위해 언론에서 가장 많이 거론되고 있는 부분이 바로 북한 사이버전 조직 및 인력 규모일 것이다. 그러나 조직은 탈북자 증언 및 정보분석 등을 통해 비교적 유추를 해내고 있지만, 인력규모에 대해서는 상당한 논란이 많은 상황이다. 6,000~7,000명 수준의 추정이 대세이기는 하지만, 지원인력까지 포함하면 30,000명 수준에 이른다는 주장도 있다.

주로 언급되는 사이버전 인력 양성기관에서 매년 배출되는 졸업생 수를 역추적하여 규모를 산정하기도 하지만, 각 교육과정의 목적이나 배출되는 인력의 성격이 명확하게 규명되지 않아 이러한 추산 방식 또한 정확한 산출 근거가 되지는 못한다. 그러나 전문적인 실력을 갖춘 사이버전사라면 불과 수십 명만 보유하더라도 한 국가를 마비시킬 수 있을 정도의 큰 위력을 발휘할 수 있기 때문에 인력 규모에 대해 지나치게 집착할 필요는 없을 것으로 판단되어, 본 연구보고서에서는 세부적으로 다루지 않기로 한다.

북한의 사이버전 수행 조직은 〈그림 2-1〉에서 보는 바와 같다. 군사지휘구조에서 사이버작전 수행을 전담하는 조직은 크게 총참모부와 정찰총국으로 구분할 수 있다. 그 중 정찰총국은 그림에서 확인할 수 있는 바와 같이 총참모부 및 인민무력성과는 독립적인 조직으로서, 평시와 전시 모두 김정은에게 직접 보고를 실시하기 때문에 전략적 중요도가 높은 조직이라고 할 수 있다.[17] 각 조직이 담당하고 있는 임무는 〈표 2-1〉에서 확인할 수 있다.

17) Jr. Bechtol and E. Bruce, North Korean Military Proliferation in The Middle East and Africa. Kentucky: The University Press of Kentucky, 2018.



〈그림 2-1〉 북한의 사이버전 수행조직[18)]

18) J. Y. Kong, K. G. Kim, and J. I. Lim, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies", 2019 11th International Conference on Cyber Conflict: Silent Battle, 2019. 5. p.4의 그림을 재작성하여 포함하였음.

〈표 2-1〉 북한의 사이버전 수행 조직[19]

부서		주요 임무
총참모부	작전국	• 기획, 전략 개발 및 운영 • 사이버작전 수행 간 전략적 결심 수행
	지휘 자동화국	• 군 통신교란 등 전자전 수행 • 31소, 32소, 56소 운영 - 31소 : 악성코드 개발 - 32소 : 군사용 소프트웨어 개발 - 56소 : 지휘통제용 소프트웨어 개발
	적공국 204소	• 한국군 대상 사이버심리전 전개 • 역정보, 허위정보유출(인터넷 심리전 전담)
	전자전국	• 레이더 및 GPS 교란 • 사이버작전 지원
정찰총국	121국	• 사이버전 지도국으로도 지칭 • 사이버전 수행 총괄 조직으로서, 1998년 결성
	414 및 128 연락소	• 한국 및 해외정보 수집, 해킹 • 전담요원 해외파견, 사이버테러 수행
	110연구소	• 舊 기술정찰조 확대 • 한국 주요 정보 수집 및 해킹, 사이버테러
	해외정보국 자료조사실	• 한국 전략정보 수집, 해킹 전담 • 사이버 전담요원 해외 주재
225국		• 사이버드보크 개발 및 설치 • 한국 전략정보 수집, 해킹전담(스테가노그라피 등)
당	통일전선부	• 120여개 친북사이트 운영, 트위터/페이스북 등 SNS 공작 • 대남 사이버심리전 전담, 여론조작 댓글팀 운영 • 남남갈등, 사회교란 시도

19) 신충근, 이상진, "북한의 대남 사이버테러 전략 분석 및 대응방안에 관한 고찰", 경찰학연구 제13권 제4호 (통권 제36호), 2013. 12.;CSIS, "North Korea's Cyber Operations: Strategy and Responses", 2017; Duri Lee, "How to Improve the ROK and US Military Alliance Against North Korea's Threats to Cyberspace: Lessons from NATO's Defense Cooperation", NPS Paper, 2018. 12..)

이상과 같은 북한의 조직들이 전 세계를 대상으로 다양한 사이버공격을 감행하면서 그러한 공격들과 관련된 다양한 해킹그룹들이 계속해서 등장하고 있다. 현재 활동하고 있는 대표적인 북한 관련 해킹그룹들은 〈표 2-2〉에서 확인할 수 있으며, 주요 보안업체들이 각기 다른 이름으로 북한의 해킹그룹 활동을 추적하고 있는 상황이다.

〈표 2-2〉 북한의 대표적인 해킹그룹

명칭	특징 및 연관된 주요 사건
라자루스(Lazarus)/ 히든코브라 (Hidden Cobra)/ ZINC	• 정찰총국 소속의 해킹 그룹 • 미국 정보기관들은 히든코브라로 언급 • 한국은 히든코브라가 2009년 정찰총국 산하로 재편된 것으로 판단 • 주요 활동 - Operation Troy(2009년~2012년) - Ten Days of Rain(2011년) - Dark Seoul(2013년) - 소니픽처스 해킹사건(2014년 후반) - 에쿠아도르 Banco del Austro에서 1,200만 달러, 베트남 Tien Phong 은행에서 백만 달러 탈취(2015년) - Operation Blockbuster(2016년 초) - 방글라데시 중앙은행 해킹 통해 8,100만 달러 탈취(2016년) - WannaCry & Cryptocurrency attacks(2017년)
안다리엘[20] (AndAriel)	• 라자루스의 하위 그룹 • 2015년부터 활동 확인 • 보안프로그램의 취약점이나 엑티브X 취약점, 중앙관리시스템 취약점 등을 이용한 공격 다수 수행

20) 보안뉴스, 『해커그룹 안다리엘, 액티브X 취약점 악용 국내 지속 공격』

명칭	특징 및 연관된 주요 사건
블루노로프 (Bluenoroff)	• 2017년 카스퍼스키랩은 라자루스 그룹 내에서 금융분야 사이버공격에 특화된 해킹 그룹을 블루노로프로 명명하고, 북한과의 직접적인 연관성에 대해서도 언급 • Mandiant 사는 'APT38'로 지칭 • Crowdstrike 사는 'Stardust Chollima'로 지칭
APT 37/ Reaper/ Group 123	• 2018년 2월, FireEye의 보고서 "APT37(Reaper): The Overlooked North Korean Actor"를 통해 처음 언급되었으며, 최소 2012년부터 활동 시작 • 한반도를 넘어 중동, 베트남 등도 공격 시도 • 하부 조직 - 미로 천리마 : 정보 탈취 - 침묵의 천리마 : 파괴적 공격 - 별똥 천리마 : 금융시스템 해킹 및 금전 탈취 • 북한 IP 사용, 북한 타임존으로 작업하는 시간과 사용하는 악성코드의 컴파일 시간 일치, 주 공격 대상이 한반도 통일 관련 조직이나 개인인 점을 이유로 북한 연계 조직으로 추정
스카크러프트 (ScarCruft)	• 2016년 카스퍼스키랩에 의해 처음 공개 • 2012년부터 활동 시작 • 2019년 5월, 모바일 환경 공격을 위해 블루투스 연결 장비들로부터 정보 수집활동 개시 (모바일 기기 데이터 탈취 목적) • 워터링홀 공격, 이미지 파일에 악성코드를 숨기는 스테가노그래피 기법 등 사용 • 수집된 정보는 4개의 클라우드서비스(Box, Dropbox, pCloud, Yandex.Disk)로 전송

2.3 교육훈련체계

1970년대에는 IT 인프라라 할 수 있는 소프트웨어가 없어 주로 하드웨어를 중심으로 IT 인력을 양성해 왔던 북한은 1984년부터 김책공업대학과 평리리과대학, 김일성 종합대학, 평성리과대학 등에서 전문적인 소프트웨어 인력을 양성함과 동시에 각 도, 직할시별로 11개의 자동화 기능공 학교를 설립하여 전자, 반도체, 소프트웨어 분야의 고급 기능공들을 양성하기 시작했다. 그리고 그 중 우수인력을 선발하여 동구권 국가로 유학을 보내기도 했다.[21]

1998년부터는 본격적으로 과학기술과정에 고등학교로부터 박사원까지 컴퓨터 교육을 체계화함과 동시에 컴퓨터기술과 정보기술에 관한 자격시험을 도입하고, 김일성 종합대학 및 김책공대에 컴퓨터과학원을 신설하는 등 다양한 교육기관을 운영하기 시작했다.[22] 특히 지휘자동화대학(舊 미림대학, 현 김일자동화대학)은 과거 소련의 지원을 받아 1986년부터 C3I(지휘, 통제, 통신, 정보)체계 연구를 진행하여 왔고, 군 지휘자동화, 전산 프로그램 개발, 사이버 타격수단 및 전술, 전자전 분야 등의 전문인력을 매년 100여명씩 양성하고 있으며, 졸업생 중 연간 10여명이 기술정찰조에 배치되어 온 것으로 알려져 있다.[23]

2013년 하태경의원이 자신의 저서[24]에서 언급한 바에 따르면, 북한은 우수한 인재들을 어린 시절부터 선발하여 최고의 교육기관에서 중등, 고등, 부서교육 등의 세 단계로 나누어 전문해커 양성을 위한 집중 교육훈련을 실시한다. 또한 방어보다는 공격능력 배양을 주목적으로 교육이 진행되고 있으며, 특히 사이버공격과 관련된 교육 내용은 철통 보안사항이라고 한다.[25] 사이버 인프라 측면에서는 다른 국가들에 비해 상당히 열세임에도 불구하고 북한이 사이버공간상에서 가장 위협적인 존재로 부각될 수 있었던 이유는 바로 이렇듯 강력한 교육훈련시스템 때문일 것이다.[26] 또한 전 세계에서 유일한 해커들의 천국이라고 불릴 정도로 사이버공격

21) 이수진, "사이버테러 및 사이버전 대응 동향", 국방대학교 안보문제연구소 군사과학정책연구 제5권, p.104, 2011. 9.
22) 박경은, "북한 '강성대국'의 미래 '컴퓨터'에 건다", 『통일한국』, 2001. 7.
23) 연합뉴스, 『북한 사이버전 주요 조직도』, 2009. 7. 8.
24) 하태경, 『삐라에서 디도스까지』. 서울: 글통, 2013.
25) TV조선, 『앞으로 북한이 노릴 사이버공격 대상은?』, 2013. 10. 17.
26) Global Post, "North Korea: How the least-wired country became a hacking superpower.", 2013.05.22.

이 문제시되지 않고 인정받는다는 점, 그래서 뛰어난 해킹능력을 가진 인재를 더욱 더 우대하고 영웅 대접을 해주는 내부 분위기도 북한이 안정적으로 사이버역량을 강화하는데 크게 기여했을 것으로 짐작된다.

2.4 북한의 사이버역량에 대한 국제사회의 평가

북한의 사이버역량에 대한 평가는 2014년 12월에 발생한 소니픽쳐스 해킹사건을 계기로 크게 달라졌다. 그전까지는 북한의 열악한 사이버 인프라로 인해 중국의 도움을 받을 수밖에 없을 것이며, 자체적으로 충분한 역량을 키워나갈 능력이 부족하다고 평가했었다. 그러나 공격수행 의지에서만큼은 계속 탁월한 평가를 받아왔으며, 사이버 인프라에 대한 의존도가 상대적으로 낮다는 점을 고려하여 방어측면에서 상당히 유리할 것이라는 평가를 받기도 했다.

2009년, 미 Technolytics 사가 전 세계 주요국의 사이버역량을 '의지(cyber capabilities intent)', '공격역량(offensive cyber capabilities)', '사이버정보 평가능력(cyber intelligence rating)' 3가지 분야를 종합하여 평가한 결과, 중국, 미국, 러시아, 인도 및 이란에 이어 6위에 랭크되었고, 한국은 9위를 차지하였다. 미국 국가안보위원회 위원과 대통령 사이버안보 특별자문위원을 역임한 바 있는 리처드 클라크(Richard A. Clarke)는 그의 저서[27]에서 북한이 사이버 공격 측면의 능력은 낮지만, 사이버공간에 연결된 시스템이 거의 없음을 들어 방어 및 네트워크 의존도 측면을 높은 수준으로 평가하였다.

2009년 7.7 DDoS 사건 이후에도 북한의 사이버전 수행역량에 대해 의구심을 가지고 있던 미국은 2013년 3.20 사이버테러를 기점으로 북한이 충분한 역량을 갖춘 것으로 평가하기 시작했다.[28] 그러나 HP 연구소는 2014년 8월 자사의 보고서[29]를 통해, 북한의 사이버전 수행역량을 하향 평가하기도 했다. 보고서에 의하면, 북한은 대규모 사이버전 수행에 필요한 대규모 인프라가 없어 가까운 미래에 전 세계적으로 큰 위협이 될 가능성은 없으며, 전통적인 군사력을 유지하기 힘든

27) Richard A. Clarke and Robert K. Knake, "Cyber War: The Next Threat to National Security and What to do about it", ECC 2010 pp.147-149
28) 임종인 외, 북한의 사이버전력 현황과 한국의 국가적 대응전략, 국방정책연구 제 29권 제4호, 2013
29) HP, "Profilling an enigma: The mystery of North Korea's cyber threat landscape", HP Security Briefing Episode 16, 2014. 8.

상황에서 새로운 비대칭 전력으로 사이버전 수행 능력을 무기로 삼고 있는 상황으로 평가되었다. 또한 2009년부터 사이버전에 대한 준비를 본격적으로 시작했기 때문에 현재 사용 가능한 전력은 한정되어 있고, 작전수행능력도 부족할 것으로 전망했다.

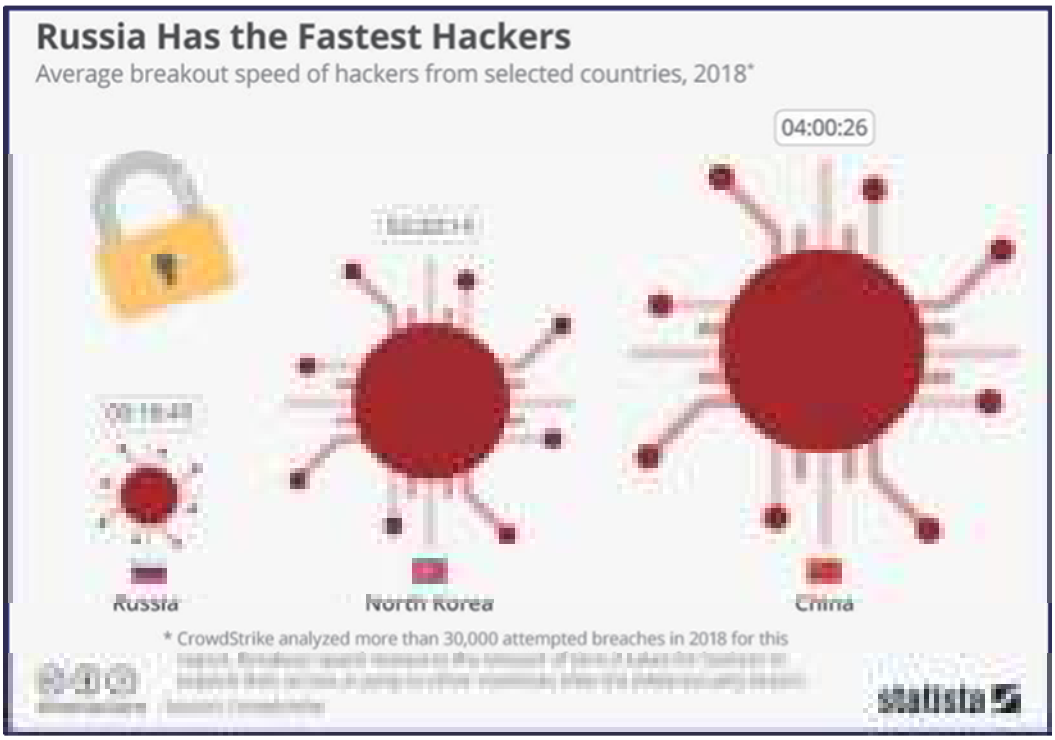
미 헤리티지(Heritage) 재단은 『2015 Index of U.S. Military Strength』보고서를 통해 북한의 사이버공격 역량이 미국에 버금가는 수준이라고 평가했다. 2014년 12월 소니픽처스 해킹사건을 경험한 미국은 2015년 4월 새로운 국방사이버전략을 발표하면서, 중국, 러시아, 이란과 함께 북한을 잠재적 위협국으로 지목하였다. 전 주한미군 사령관을 역임했던 빈센트 브룩스 대장은 북한이 전 세계에서 가장 우수한 역량을 갖춘 국가 중 하나이자 가장 조직적인 국가라고 평가하면서, 북한의 비대칭전력이 그런 우수하고 조직적인 사이버공격 역량에 의해 강화되고 있는 중이라고 말했다.[30] 2017년 8월 3일 발표된 미국 의회의 보고서[31]에서는 사이버능력으로 미국을 위협하는 국가 중 중국, 러시아, 이란 정도가 북한보다 우월한 능력을 보유하고 있으며, 북한은 국제무역을 방해하거나 사이버능력의 사용을 통해 국제제재를 교묘하게 회피할 수 있는 능력까지도 보유하고 있는 것으로 평가하였다. 반면 호주 정부는 북한의 사이버역량을 높게 평가하지만, 아직 호주의 사이버 인프라를 전복시킬 수준의 역량을 갖춘 것은 아니라고 언급했다.[32]

2018년 8월 개최된 블랙햇에서 F-Secure사의 연구원인 미코 히포넨(Mikko Hypponen)은 북한의 사이버위협에 대해 언급하면서, 북한을 “정보수집 목적의 스파이 행위와 고의적으로 시스템과 데이터를 파괴하는 사보타주 행위 외에 절도 행위까지 수행하는 국가”, “잃을 것이 없는 국가”, “지구상에서 유일하게 국가 예산 적자를 해결하기 위해 다른 나라들로부터 도둑질을 하는 국가” 등으로 표현하였다.

미국 사이버보안업체 크라우드스트라이크(CrowdStrike) 사는 『2019 Global Threat Report』(2019. 2. 19 발표)를 통해 2018년도에 발생한 3만개의 공격에 대한 분석 결과를 기준으로 측정한 ‘breakout’ 시간을 발표하였는데, 〈그림 2-2〉에서 보는 바와 같이 북한이 러시아에 이어 전 세계 2위를 차지하였다.

---

30) Bloomberg, "North Korean Cyber Capability Among World's Best, Brooks Says", 2016. 4. 20.
31) U.S. Congression, "North Korean Cyber Capabilities: In Brief", 2017. 8. 3.
32) New Zealand Herald, “North Korea cyber attack capabilities: What could Kim Jong-un do?”, 2017. 10. 25.



〈그림 2-2〉 크라우드스트라이크 사의 'breakout' 시간 측정 결과

미 사이버사령부는 2019년 8월 8일, 북한의 APT-38 조직과 연계된 악성코드 표본을 '바이러스토털(VirusTotal)'을 통해 공개한데 이어,[33] 9월 9일에는 '히든코브라(HiddenCobra)'가 제작한 악성코드 표본 11종을 공개하였다. 미 사이버사령부가 악성코드를 공개한 것이 이번이 처음은 아니지만, 북한정권 창건일에 맞춰 공개한 것을 두고 특별한 의미를 부여하는 전문가도 있다. FireEye 사의 연구원인 앤드류 톰슨(Andrew Thompson)은 그동안 방어에만 치중했던 사이버사령부의 전략이 상대의 정체, 사이버작전 수행 위치 등을 알고 있음을 적국 또는 해커단체에게 주입시킴으로써 그들의 행동 변화를 야기하는 '지속적 개입 전략'으로 변화하고 있음을 암시하는 것이며, 북한에게 모든 활동이 감시되고 있다는 신호를 주기 위한 조치일 것이라고 평가했다.[34]

33) Techcrunch.com, "US Cyber Command has publicly posted malware linked to a North Korea hacking group", 2019. 8. 16; Cyberscoop, "U.S. Cyber Command warns of North Korea-linked Lazarus Group malware", 2019. 8. 15.
34) 동아닷컴, 『美 사이버사령부, 9·9절 맞춰 '북한 악성 코드' 샘플 공개』, 2019. 9. 11.

3. 북한의 주요 사이버공격

북한이 대한민국을 대상으로 수행했던 주요 사이버공격은 인터넷에 공개된 문서상에서 공격주체가 명확하게 북한으로 지목된 공격들만을 대상으로 정리를 수행하였으며, 사이버공격의 목적 및 유형에 따라 다음과 같이 크게 3단계로 구분하였다. 물론 사이버공격의 양상이 해당 시기에 따라 명확하게 변화되는 것은 아니며, 일부 사이버공격은 3단계로 구분한 시기를 벗어나서 발생하기도 하였다. 그러나 사이버공격을 시기의 구분 없이 개별 사건별로 분석하는 것은 북한이 사이버역량의 사용을 통해 달성하려는 전략적 의도를 추정함에 있어 큰 도움이 되지 않는다. 따라서 본 연구에서는 특정 유형의 공격이 다수 포함된 구간을 시기 구분의 기준으로 설정하고, 해당 구간에 일부 다른 유형의 사이버공격이 포함되더라도 그에 대해서는 개별적인 의도 추정을 실시하지 않는다.

- 1단계 : 정부기관을 대상으로 한 기밀유출 시도 공격(1999~2009)
- 2단계 : 파급효과가 큰 사회기반시설에 대한 공격(2009~2016)
- 3단계 : 재화 취득을 목적으로 한 금융권 공격(2017~현재)

3.1 1단계 : 정부기관을 대상으로 한 기밀유출 시도 공격

북한이 대한민국을 대상으로 사이버공격을 감행한다는 사실을 군이 처음으로 공개한 시점은 2004년이다. 2004년 4월부터 6월까지 다수의 국가 기관 서버 및 PC가 전면적인 사이버공격을 받았고, 당시 송영근 기무사령관은 “북한이 김정일 국방위원장의 지시로 정예 해킹부대를 만들어 우리 국가기관을 공격해 정보를 수집하고 있다”고 발표했었다.[35] 그러나 실질적인 준비는 1990년대부터 진행되었던 것으로 알려져 있다. 군사기술 전문 교육기관인 미림대학 출신인 조명래가 1997년 제작한 것으로 알려진 ‘JML’ 악성코드는 윈도우운영체제의 시스템 폴더를 감염시킨 후 정보 유출을 위한 백도어를 설치한다. 구체적인 활동사례는 확인되지 않았지만, 우리나라의 사이버보안업체 Ahnlab에서는 ‘Win32/JML’이라는 이름으로 명

35) 한국경제, 『[사이버 냉전 공습경보] (상) 남북대화 순간에도...』, 2008. 1. 27.

명하고 백신에 의한 진단을 실시하였으며, 2003년 이후에는 진단명을 'Win32/Weird.C'로 변경하기도 하였다. 그리고 2002년에는 변종까지 발견되었다.[36]

• **정부기관 대상의 기밀정보 수집을 위한 사이버공격(2004)**

2004년 4월부터 6월까지 발생한 북한의 사이버공격으로 인해 국회를 비롯한 해양경찰청, 원자력연구원, 국방연구원, 국방연구소, 공군대학, 해양수산부, 중소기업청, 통일교육원 등의 정부기관 서버 235대 및 기업·대학기관 서버 79대 등 총 314대의 컴퓨터가 해킹을 당하였으며, 공격 근원지는 북한에 임대된 중국 IP주소임이 확인되었다.[37] 국가정보원은 2004년 7월, 북한에 의한 해킹피해가 발생했으며, 국회의 경우 개인 이메일 비밀번호 관리 소홀로 전·현직 국회의원 및 국회 사무처 직원 등 122명의 아이디가 도용당했다고 발표했다.[38] HP 보고서[39]에 의하면, 당시 북한이 군의 무선통신 네트워크에도 접속했었다고 한다.

이러한 북한의 사이버공격에 앞서 참여정부는 범 국가차원에서의 사이버안전체계 구축을 위해 2003년 말~2004년 초에 걸쳐 한국정보보호진흥원에 '인터넷침해사고대응센터'를 설립하고, 국가정보원에는 '국가사이버안전센터'를 설립한 바 있다. 그리고 국가 및 공공분야의 사이버안전은 국가사이버안전센터가 담당하고, 민간 및 공공분야는 정보통신부를 주축으로 인터넷침해사고대응센터가 담당하며, 국방부의 정보전대응센터가 국방분야 및 각급 부대의 사이버안전을 책임지는 국가사이버안전 종합대응체계가 구축되었다. 참여정부 출범 직전에 벌어졌던 2003년의 1.25 인터넷대란이 계기가 되어 범 정부차원에서 실절적인 종합 대응체계가 구축되긴 했지만, 미처 예상하지 못했던 북한의 사이버공격에 효율적으로 대응하지는

36) Rowman & Littlefield, "North Korea's Cyber Operations: Strategy and Responses", 2016.; 뉴데일리, 『"北컴퓨터 해커 책임자 '조명래 JML' 자료 입수"』, 2012.7.13.

37) J. chae, "The Changing Security Environment and cyber Security", The Journal of Political Science and Communication, Vol.16 No.2, pp.171-193, 2013; A. Mansourov, "North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance", 2014. 12. 2.; J. M. Park, N. Rowe, and M. Cisneros, "Responding to North Korean Cyberattacks", The 15th European Conference on Cyber Warfare and Security, pp.245-252, 2016. 7.

38) 중앙일보, 『'국가정보통신망' 사이버 테러…北 소행?』, 2013. 3. 20.; 고려대학교 산학협력단, 『사이버위협 시나리오 개발 및 대응방안 연구』, 연구보고서, 2014. 11.

39) HP, "Profilling an enigma: The mystery of North Korea's cyber threat landscape", HP Security Briefing Episode 16, 2014. 8.

못했다.

• 을지포커스렌즈 훈련 기간 중 군 통신망 침투(2004)

한국군 당국은 2004년 8월 군단급 훈련과 한·미 연합훈련인 을지포커스렌즈 훈련이 진행되던 시기에, 북한이 사이버공격을 감행해 한국군의 14개 부대에서 사용하던 80개의 무선 네트워크 가운데 33개를 도청했음을 확인했다.[40]

• 논리폭탄 실험(2007)

논리폭탄(Logical bomb)은 특정 날짜나 시간 등 조건이 충족되었을 때 악의적인 기능이 수행되도록 만든 코드의 일부분으로 소프트웨어 시스템에 의도적으로 삽입된 것이다. 약간의 프로그래밍 지식만 있으면 손쉽게 만들 수 있기 때문에 초보자들이 선호하는 해킹 프로그램이다. 사전에 지정한 시간이 도래하거나 특정 조건이 발생할 경우 컴퓨터의 운영에 필요한 기본 파일을 삭제하여 컴퓨터의 작동을 중단하도록 하는 경우 또는 특정기관의 통상적 컴퓨터 프로그램에 중대한 과오를 발생시키는 루틴이나 부호를 무단으로 삽입하여 데이터를 파괴하거나 변조함으로써 예상치 못한 큰 장애를 유발하거나 부정행위를 실행시키는 경우 등이 이에 해당한다.[41]

본 사건은 일부 논문 및 보고서[42]에서 인용하고 있기는 하나, 구체적인 피해 사례 또는 정보를 확인하기는 불가능했다. Mansourov는 한국의 정부 소식통을 인용하면서, 중국 다롄(大連)에 있는 북한 관련 소프트웨어 개발업체 30여 곳이 중국의 논리폭탄 제조를 위해 하청업체로 일하고 있으며, 한국 정부가 다롄에서 생산된 컴퓨터 소프트웨어와 하드웨어가 기술적으로 조작되었을 가능성이 있음을 의심하고 있다고 전했다.[43]

---

40) 신 스티브, “한국과 주한미군에 대한 북한과 중국으로부터의 사이버 위협”, 국방과 기술 통권 364권, pp.28-33, 2009. 6.

41) 위키백과: 검색어 -“논리 폭탄”

42) 임종인 외, “북한의 사이버전력 현황과 한국의 국가적 대응전략”, 국방정책연구 제29권 제4호, 2013년 겨울(통권 제102호), 2013. 12.; 고려대학교 산학협력단, 『사이버위협 시나리오 개발 및 대응방안 연구』, 연구보고서, 2014. 11.

43) A. Mansourov, "North Korea's Cyberwarfare and Challenges for the U.S.-ROK Alliance.", Korea's Economy, Vol.20, 2014.

• 장교를 대상으로 한 트로이목마 메일 전파(2008)[44]

2008년 9월, 정부는 육군 대령에게 트로이목마 바이러스가 포함된 이메일을 전송하여 사이버 스파이 행위를 시도하려 한 혐의로 북한을 비난한 바 있다. 국방부는 이 사건으로 인한 기밀누출은 없었다고 밝히면서, "북한은 상당히 오랫동안 군사 시스템에 대한 해킹을 시도하였으며... 북한은 해킹 기술자를 양성하고 있는 것으로 알려져 있다"라고 언급하였다.

• 3군 사령부 및 화학 관련 기관 해킹에 의한 정보 유출(2009)[45]

2009년 3월 5일, 북한의 사이버공격에 의해 육군 3군사령부가 해킹당하면서 3군사령부가 환경부 산하 국립환경과학원의 화학물질안전관리센터에 들어갈 수 있는 인증암호를 도용당했다. 북한은 도용한 인증암호를 이용해 국립환경과학원이 구축한 '화학물질 사고대응 정보시스템(CARIS, Chemical Accident Response Information System)'[46]에 접속하여 700여 개의 화학물질 제조업체와 관련된 정보와 함께 1,350여 종에 달하는 유해 화학물질, 기상정보 등을 탈취해 간 것으로 확인되었다.

사고 발생 이후, 국가정보원이 국가사이버테러대응센터 주관으로 긴급 대책회의를 개최하고, 국방부, 기무사령부, 국군화생방방호사령부, 환경부, 국립환경과학원 관계자들이 참석하여 향후 대책을 논의하였으며, 국가정보원은 10여 일간의 로그파일 분석을 통해 본 사건의 주체를 북한 해커부대로 확정지었다.

김흥광 전 북한컴퓨터기술대학 교수(NK지식인연대 대표)는 "남한의 화학물질 정보, 제조업체 리스트가 적의 수중에 넘어간 초유의 사건"이라고 표현하며, 북한이 입수한 정보를 북한 특수부대들에 공격목표로 통보하는 등 전략적으로 활용할 가능성도 있음을 경고했다.

---

44) 정구연, 이기대, "과학기술발전과 북한의 새로운 위협: 사이버 위협과 무인기 침투", KINU 연구총서 16-04, 2016. 12.; 신 스티브, "한국과 주한미군에 대한 북한과 중국으로부터의 사이버 위협," 『국방과 기술』,2009년 6월호, p.30, 2009. 6.

45) 오동룡, "[특종] 軍 인터넷망, 북한 해커 부대에 뚫렸다! 국무총리실 외교안보정책관실이 작성한 'CARIS 북한 유출내역' 문서 단독 입수", 월간조선 2009년 11월호, 2009. 11.

46) CARIS는 정부가 2002년부터 2005년까지 총 25억원의 예산을 들여 3단계에 걸쳐 구축한 '화학물질 사고대응 정보시스템' 이다. 정부는 2002년 1단계 사업을 통해 일선 소방서와 경찰서, 지방자치단체 등 사고대응기관에 화학물질의 유해성과 방제 관련 정보, 화학물질 확산범위·대처요령 등을 포함한 대응 시나리오를 제공해 왔다. 2004년에는 2단계 사업 추진을 통해 국립환경연구원 화학물질안전관리센터와 사고대응기관 간의 쌍방향 사고전파가 가능하도록 개선하였다.

• Operation Troy(2009~2012)[47]

2009년부터 2012년까지 한국에서 발생한 한국군과 주한미군을 목표로 하는 정보수집 목적의 조직적이고 지속적인 사이버공격을 의미한다. 사이버공격에 사용된 악성코드를 미 사이버보안업체 맥아피가 '트로이 작전(Operation Troy)'이라고 명명하였으며, 최소한 4년 이상 한국 정부와 군의 컴퓨터들을 감염시킨 후 '미국 육군', '비밀', '키 리졸브 작전', '합참 직원' 등의 용어를 적용하여 군사 기밀을 검색 및 수집한 것으로 파악되었다.

공격 주체로 지목된 라자루스 그룹은 'Operation Troy'를 실시하는 과정에서 다양한 종류의 자료 삭제형 악성코드를 배포하였는데, 이들 악성코드는 서로 코드를 공유하고 있는 것으로 밝혀졌다. 그리고 라자루스 그룹이 제작했다고 알려져있는 기존 악성코드들과도 'YARA' 시그니처가 일치하였다. 또한 2011년 발생한 3.4 DDoS 공격뿐만 아니라 2013년의 3.20 사이버테러에서 사용된 악성코드들과도 연관되어 있는 것으로 확인되었다.[48]

3.2 2단계 : 파급효과가 큰 사회기반시설에 대한 공격

앞서 살펴본 바와 같이 2004년부터 2009년까지의 공격은 정부기관이나 국방 관련 기관을 대상으로 한 정보유출 시도 목적의 사이버공격이 주를 이루었다. 물론 2009년도 이후 현재까지도 정보유출을 시도하는 사이버공격은 지속적으로 발생하고 있다. 그러나 북한의 사이버공격은 2009년을 기점으로 상당히 다른 양상을 보이며 전개되기 시작한다.

• 7.7 DDoS 공격(2009)[49]

2009년 7월 4일, 미국의 주요 사이트들을 대상으로 공격이 실시된 이후 7월 10일까지 국내·외 주요 웹사이트들을 대상으로 동시다발적으로 DDoS 공격이 발생하였다. 명령제어(C&C) 서버를 이용했던 기존 DDoS 공격과 달리 115,000여대

47) CNB News, 『美보안회사 '맥아피', "2009년부터 한국 해킹한 세력 포착"』, 2013. 7. 9.
48) Novetta,, "Operation blockbuster; Unraveling the long thread of the Sony attack", 2016. 2.
49) 보안뉴스, 『국정원, 'DDoS공격 배후, 북한과 그 추종세력으로 추정' 발표』, 2009. 7. 9.; 중앙일보, 『대북정보, 손발 안 맞는 통일부·국정원·외교부』, 2009. 12. 8.

의 좀비 PC를 이용한 공격이 수행되었다.

국내 사이트 22개, 국외(미국) 사이트 14개 등 총 36개의 웹사이트가 공격을 받았으며, 국가기관, 금융기관, 주요 포털사이트 등 국내외적으로 DDoS 공격으로 인한 사회적 파장이 큰 사이트들이 공격 목표지로 설정됐다. 해당 공격으로 인한 경제적 피해는 크지 않았으나, 당시에는 DDoS 공격에 대한 국가적인 대응체계가 확립되기 전이었기 때문에 큰 사회적 혼란이 빚어졌다.

7.7 DDoS 공격이 기존 DDoS 공격들과 차별화되는 점들은 〈표 3-1〉에서 확인할 수 있다.

〈표 3-1〉 기존 DDoS 공격과 7.7 DDoS 공격의 차이점[50]

구분	기존 디도스 공격	7.7 디도스 공격
명령 · 제어서버 존재여부	해커로부터 명령을 받는 명령 · 제어 서버 존재	악성코드 업데이트 서버 존재
공격 방법	명령 · 제어 서버의 네트워크를 통한 실시간 공격 제어	일정 주기로 악성코드를 업데이트 받아 스케줄링을 통한 공격
감염 경로	윈도우즈 또는 브라우저 취약점을 악용한 악성코드로 인한 감염	공격자가 정상적인 프로그램에 숨겨둔 악성코드가 동작
방어 방법	명령 · 제어 서버 차단	공격 PC의 악성코드 제거
공격 대상	홈페이지 1~2개	다수 홈페이지에 동시 다발 공격
악성코드 갯수	디도스 공격을 수행하는 악성코드 1개 다운로드	압축파일 형태의 악성코드 다운로드, 디도스 공격 외에도 다양한 공격 수행
네트워크 연결정보	일반 채널을 통한 통신, 공격명령 내용 확인 가능	암호화된 채널로 통신, 통신내용 확인 불가
악성 행위	해커의 명령을 지속적으로 수행	단기공격 수행 후 하드디스크 삭제
공격 목적	금전적 이득	사회혼란 유발
공격 주체	주로 중국 등에 위치한 해커 조직	북한

50) 보안뉴스, 『7.7 DDoS 공격, "어떤 사건이었나?"』, 2010. 7. 7.; 신종환, "국내 주요 인터넷 사고 경험을 통해 본 침해사고 현황", Internet & Security Focus 2013년 9월호, p.44, 2019. 9.

• 작전계획 5027 설명자료 유출(2009)

작전계획은 북한이 지속적으로 유출을 시도하는 매력적인 해킹대상일 것임은 분명하다. 지난 2005년도에도 모 부사관이 인터넷 공유사이트에 접속하는 과정에서 개인 노트북에 저장하고 있던 '작계 5027-04 전투세부시행규칙' 등의 기밀자료가 유출되는 사고가 발생했었다. 2016년도에 국방망 해킹사고가 발생했을 때에도 작전계획 5027을 담은 훈련용 시나리오가 유출되었으며, 군은 작전계획 5015에서 작전계획 5027을 승계한 부분을 일부 수정하기도 했다.[51]

2009년의 작전계획 5027 설명자료 유출사건은 11월 중순 연합사에 근무하는 영관급 장교가 인터넷과 인트라넷 간 망전환이 가능한 듀얼 PC에서 USB 메모리를 사용하는 과정에서, 11쪽 분량의 파워포인트 형식으로 제작된 작전계획 교육용 슬라이드 자료와 기타 군사관련 자료가 해킹에 의해 유출된 사건이다. 이 사건을 계기로 한미연합사는 재발 방지를 위해 인트라넷과 인터넷을 함께 사용할 수 있도록 한 PC를 각각 분리해 사용하는 것으로 전환했다.[52]

조사 결과, 중국발 IP를 사용하는 해커에 의해 해킹을 당한 것으로 확인되었으며, 국군기무사령부와 국가정보원은 북한의 전문 해커부대의 소행일 것으로 추정했다.[53]

• 3.4 DDoS 공격(2011)

2011년 3월 3일부터 4일까지 이틀간 국내의 주요 정부기관, 포털 및 은행 웹사이트 등을 대상으로 DDoS 공격을 수행하여 일시적으로 두 차례 마비시킨 사건으로 2009년의 7.7 DDoS 공격에 비해 한층 진화된 형태의 공격이 진행되었다.[54] 공격에 사용된 악성코드는 난독화가 적용되어 대응에 시간이 걸리게 하였고, 좀비 PC의 공격시간을 특정하지 않아 한 번 감염되면 치료될 때까지 지속적으로 공격이 이루어지도록 하는 것이 특징이다.[55]

악성코드는 P2P 파일 공유 사이트인 쉐어박스와 슈퍼다운에 업로드된 일부 파

51) 중앙일보, 『북 해킹으로 작전계획 5027 유출 확인』, 2017. 4. 3.
52) 연합뉴스, 『'작계 5027' 교육용 자료 해킹』, 2009. 12. 18.
53) 오동룡, "[특종] 이번에는 '작전계획 5027 해킹당했다!' 한반도 유사시 韓美 연합군의 전쟁계획 담긴 극비문서 유출", Daily 월간조선, 2010. 1.
54) 한국일보, 『'3.3 디도스' 제 2차 디도스 대란 일어나나』, 2011. 3. 7.
55) Novetta,, "Operation blockbuster; Unraveling the long thread of the Sony attack", 2016. 2.

일에 삽입된 상태로 유포되었으며, 최초 상태는 4일 혹은 7일이 지나면 하드 디스크가 파괴되도록 프로그래밍이 되어있었다.[56] 그러나 DDoS 공격으로 의도했던 큰 피해가 발생하지 않자 예정보다 일주일 앞당긴 3월 7일에 파괴를 시작하도록 하는 명령과 보호나라 사이트 접속을 차단하는 명령을 내리는 등 공격계획이 수정된 정황도 확인되었다.[57]

• **농협 전산망 해킹(2011)**[58]

2011년 4월 12일, 농협 전산망에 있는 자료가 대규모로 손상되고 4월 30일 정상화될 때까지 농협의 전체 또는 일부 서비스 이용이 마비된 사건이다. 사건 초기에는 협력 업체에 의한 사고 가능성이 제기되기도 하였으나, 검찰은 북한 IP 주소가 공격에 사용되었고 공격패턴이 7.7 DDoS 및 3.4 DDoS 공격 당시와 유사한 점을 근거로 북한의 소행이라고 발표하였다. 이 사건으로 인해 대한민국의 정보보안 분야 전반에 대한 여러 가지 문제점들이 지적되었고, 이를 보완하는 조치들이 시행되었다.

• **중앙일보사 해킹(2012)**[59]

보수성향 일간지 중앙일보 웹사이트를 대상으로 'IsOne'이라는 해커가 디페이스 공격을 가한 사건이다. 경찰은 중앙일보의 신문제작시스템과 보안시스템 접속기록, 악성코드, 공격에 이용된 국내 경유지 서버 2대와 10여개국으로 분산된 경유지 서버 17대 등을 분석하여, 공격 경유지의 IP 주소 및 악성코드(암호해독 키 값 포함)가 7.7 DDoS와 3.4 DDoS 공격 당시와 동일하다는 점과 북한 체신성 IP가 공격 2개월 전부터 중앙일보 웹사이트에 접속한 사실을 확인하였으며, 이를 근거로 공격의 진원지를 북한으로 지목했다.

• **3.20 사이버테러(2013)**

북한으로 추정되는 해커그룹의 악성코드 유포로 32,000대가 감염되었으며, KBS

56) 전자신문, 『[3.3 디도스 공격] 악성코드, 일주일 뒤 PC 망가뜨려』, 2011. 3. 7.
57) Novetta,, "Operation blockbuster; Unraveling the long thread of the Sony attack", 2016. 2.
58) 중앙일보, 『농협 해킹, 북한 소행 가능성 크다』, 2011. 4. 26.; 연합뉴스, 『조선민주주의인민공화국이 농협 전산망 공격 결론』, 2011. 5. 3.
59) 매일경제, 『경찰 '중앙일보 해킹 사건은 북한 소행' 결론… 北 체신성 IP 확인』, 2013. 1. 16.

· MBC · YTN 언론사와 신한은행 · 제주은행 · 농협은행에서 전산업무가 마비되는 피해가 발생하였다. 악성코드는 하우리와 안랩의 백신 프로그램 구성파일로 위장되어 패치관리시스템(PMS, Patch Management System)을 통해 전파되었으며, 마스터 부트 레코드(MBR)와 볼륨 부트 레코드(VBR)를 파괴함으로써 PC가 작동되지 않도록 하는데, 2013년 3월 20일 14시에 실행되도록 설계되어 있었다.[60] 또한 같은 날 우리은행은 서비스 거부 공격을 받았으며, 자칭 'Whois'라는 해커 그룹이 LG유플러스의 그룹웨어를 해킹하는 사건도 발생하였으나, 세 사건들 사이의 연관성은 밝혀내지 못했다.

미국 보안업체 포티넷은 북한 정찰총국이 배후로 지목되는 이번 공격에 특정 날짜와 시간이 되면 하드드라이브 파일이 자동 삭제되는 논리폭탄이 동원됐을 가능성이 있다고 지적했다.[61]

• 6.25 사이버테러-'Dark Seoul'(2013)[62]

청와대와 국무조정실 홈페이지가 위·변조되는 등 정부 4곳과 정당 1곳, 언론사 11곳 등 16개 이상 기관의 서버 131대가 공격을 받았다. 이로 인해 청와대 홈페이지 접속화면에 '위대한 김정은 수령', '통일대통령 김정은 장군님 만세! 우리의 요구조건이 실현될 때까지 공격은 계속될 것이다. 우리를 맞이하라. We Are Anonymous' 등의 문구와 박근혜 전 대통령의 사진이 게재되었고, 새누리당원 250만명, 군장병 30만명, 청와대 홈페이지 회원 10만명, 주한미군 4만여명등의 개인정보가 유출되었다. 한편, 같은 날 북한도 어나니머스라고 주장하는 해커의 공격으로 '우리민족끼리', '노동신문', '내나라', '고려항공' 등 주요사이트가 차단되고, 북한 군 간부 20명의 인적사항이 공개되었다.

• 서울 메트로 해킹(2015)[63]

서울메트로의 서버 2대가 북한의 해킹을 당해 업무용 PC 213대에 인가받지 않

60) Red Alert, 『3.20 사이버테러 사고 분석 보고서』, 2013. 4. 19.
61) 보안뉴스, 『[보.알.남] 내 PC에 폭탄이 숨어 있다, 로직 밤』, 2019. 5. 29.
62) 머니투데이, 『6.25 사이버공격 67곳 타격… 14곳은 정보파괴』, 2013. 7. 4.; 이투데이뉴스, 『6.25 사이버테러는 북한 소행 정부 공식 발표』, 2013. 7. 16.; 미디어잇, 『6.25 사이버 공격, 취약한 웹하드 서버 관리가 원인』, 2013. 6. 27.
63) 연합뉴스, 『서울메트로 사무용 PC 5개월간 해킹…北 소행 추정(종합)』, 2015. 10. 5.; 뉴스1, 『서울메트로 서버, 북한에 장기간 해킹』, 2015. 10. 5.

은 사용자가 접속하였으며, PC 58대는 악성코드에 감염되었고, PC 3대에서는 업무자료 12건이 유출되는 피해가 발생하였다. 해킹 수법은 3.20 사이버테러와 유사한 APT 방식을 사용하였으며, 2014년 3월 이전부터 시작되어 2014년 8월까지 지속되었다.

2015년 9월, 현장조사를 실시한 국가정보원은 "APT 해킹방식을 쓰는 사이버테러 조직(북한 정찰총국)의 소행으로 추정된다"는 의견을 서울메트로 측에 통보했으나, 서울시는 해킹 주체를 "북한이라고 단정지을 수 없다"고 답했다.[64]

• **한국수력원자력 해킹(2014)**[65]

'원전반대그룹'이라고 밝힌 해커조직은 2014년 12월 15일부터 2015년 3월 12일까지 총 6회에 걸쳐 한수원 관련 자료를 공개하며 원전중단을 요구하였다. 유출된 자료는 한수원 임직원 개인정보, CANDU 제어 프로그램 자료, 원전 설계도, 내부 직원의 원자력발전소 주민 방사선량 평가 프로그램 파일 등이다.

해커조직은 최초 2014년 9월부터 12월까지 한수원 직원 3,571명에게 5,986통의 파괴형 악성코드 이메일을 발송해 PC 하드디스크 등을 파괴하려고 시도했으나 PC 8대만 감염되고 그 중 5대의 하드디스크가 초기화되는 정도에 그치는 등 사실상 공격이 실패로 돌아가자 피싱 메일을 보내 한수원 관계자들의 이메일 비밀번호를 수집한 후, 해당 이메일 계정에서 자료들을 수집하였다. 이를 바탕으로 트위터 등에 '크리스마스 때까지 원전 가동을 중지하고 100억 달러를 주지 않으면 보유한 원전 관련 자료를 공개하겠다'는 협박을 하였다.

※ Operation Kimsuky(2009)

카스퍼스키 랩은 한국의 주요 기관을 노린 사이버스파이 활동을 발견하고, 'Operation Kimsuky'로 명명하였다.[66] 해커의 활동은 주로 세종연구소, 국방연구원, 통일부, 현대상선, 통일생각 등 북한과 관련된 연구기관이나 정책기관을 대

64) 중앙일보, 『[사회] 서울메트로 업무용 PC 해킹, "북한이라고 단정 짓기 어려워"』, 2015. 10. 5
65) 보안뉴스, 『한수원 해킹 사태! 최초 보도 이후 보름여의 기록들』, 2014. 12. 28.; 뉴스1, 『한수원 자료 유출…"북한 해커조직 사이버테러"』, 뉴스1, 2015. 3. 17.; 보안뉴스, 『2014년: 카드사 사태와 한수원 해킹, 대형사고로 얼룩진 한해』, 2019. 8. 19.
66) D. Tarakanov, "The 'Kimsuky' Operation: A North Korean APT?" Securelist, 2013. 9. 11.(https:// securelist.com/the-kimsuky-operation-a-north-korean-apt/57915)

상으로 수행되었으며, Kimsuky 트로이 목마 샘플은 2013년 5월 5일 최초로 발견되었다. 악성코드는 특정 대상만을 목표로 중요정보를 캐내기 위한 스피어피싱 이메일로 전달되었고, HWP 파일만 유출하는 전문 악성코드도 포함되어 있었다.[67]

Operation Kimsuky의 첫 번째 공격은 2013년 9월 11일 벨기에 메일 계정을 통해 악성코드가 담긴 스피어피싱 이메일이 발송되면서 시작됐다. 악성코드를 통해 수집된 모든 정보는 두 개의 마스터 메일 계정('kimsukyang'이라는 이름으로 등록된 iop110112@hotmail.com과 'kim asdfa'이라는 이름으로 등록된 sh1213@hotmail.com)으로 전송되는 것이 확인되면서, 'Operation kimsuky'로 불리게 되었다.[68] 두 번째 공격은 2014년 2월 25일에 시작되었으며, 더 많은 공격이 3월 11일과 12일, 17일 및 19일에 실시되었다.[69]

2018년부터는 프로세스 할로윙(Process Hollowing) 기법을 적용하여, 아래한글의 취약점과 스피어피싱을 그대로 활용하면서 윈도우즈 운영체제에 내장된 정상 프로세스에 악성코드를 삽입하여 실행하는 방법으로, 정보탈취 및 첩보활동을 지속하였다. 2019년초에도 남북한 상황에 대한 질문 내용을 수록한 "자문용 질문 190101.hwp" 라는 제목의 한글 파일과 프로세스 할로윙 기법을 접목하여 정보탈취를 시도하려는 사이버공격이 식별되었다.

• GPS 재밍(2016)

현대 무기체계는 대부분 GPS를 기반으로 작동하고 있어, GPS 교란공격은 아군의 작전 수행에 심각한 영향을 미칠 수 있다. 2016년의 GPS 재밍공격은 2010년 8월, 2011년 3월, 2012년 4월에 이은 4번째 군사적 도발 행위로서, 키리졸브 연습에 대한 대응과 2016년 5월로 예정되어 있던 제7차 당 대회 이전에 전쟁준비가 차질없이 진행되고 있음을 대내외에 과시하기 위한 행동으로 볼 수 있다. 그리고 GPS 재밍공격에 의해 영향을 받는 범위가 얼마만큼인지를 가늠해보려는 의도도 가지고 있었을 것으로 판단된다. 이러한 측면에서 당시 각종 언론들이 대한민

67) 보안뉴스, 『한국 주요기관 노린 사이버스파이 활동 발견!』, 2013. 9. 12.
68) D. Tarakanov, "The 'Kimsuky' Operation: A North Korean APT?" Securelist, 2013. 9. 11. (https:// securelist.com/the-kimsuky-operation-a-north-korean-apt/57915)
69) AhnLab, 『APT Attack - New 'Kimsuky' malware emerged.』, ASEC Threat Research & Responding Blog, 2014. 3. 19.(http://asec.ahnlab.com/993)

국의 피해상황을 상세한 숫자까지 언급하며 앞다투어 우려를 표명했던 부분은 많은 아쉬움으로 남는다.

3.3 3단계 : 재화 취득을 목적으로 한 금융권 공격

북한의 미국과의 협상무대에서 유리한 위치를 선점하기 위해 미사일 시험발사를 가장 활발하게 진행하면서 한국과의 군사적 긴장도 고조시켰던 시기는 2016년이다. 그리고 북한의 사이버공격 양상이 사화기반시설에 대한 공격에서 탈피하여 본격적으로 금융권 위주의 공격으로 전환된 시점도 2016년이다. 계속되는 미사일 발사 실패와 국제사회의 제재 강화로 인해 경제적 상황이 악화되면서 돌파구를 모색할 수밖에 없었던 북한은 손쉽게 재화를 마련할 수 있으면서도 국제사회의 제재는 교묘하게 회피할 수 있는 수단으로서의 사이버역량을 그 어느 때보다 활발하게 사용하기 시작하였다.

- **인터파크 해킹 및 고객정보 유출(2016)**[70]

2016년 5월 3일부터 5월 6일까지 4일 동안 북한이 인터넷 쇼핑몰 운영업체인 인터파크의 패스워드 관리 및 서버 접근통제 관리 취약점을 악용하여 회원정보 26,658,753건을 외부로 유출시킨 사건이다. 해커는 우선 스피어피싱으로 직원 PC에 악성코드를 최초 감염시킨 후 다수의 단말에 악성코드를 확산시키면서 내부정보를 수집하였다. 그리고 수집된 내부 정보를 이용해 DB 서버에 접근이 가능한 개인정보취급자 PC를 파악한 다음에는 해당 PC의 제어권을 획득하고 DB 서버에 접속하여 개인정보를 탈취하여 외부로 몰래 유출한 것으로 확인되었다. 7월 28일, 경찰청은 중간 수사결과를 발표하면서 해킹의 주체로 북한 정찰총국을 지목하였으며, 민·관 합동조사단은 공격 주체를 명확하게 지목하지는 않았다.

70) 방송통신위원회 보도자료, “인터파크 개인정보 유출 침해사고 조사 결과 - APT(지능형 지속 위협) 공격으로 개인정보 유출 발생”, 2018. 8. 30.

• 국방망 해킹 및 자료 유출(2016)[71]

북한으로 추정되는 해커 그룹은 국방부에 백신을 납품하는 업체의 백신자료를 해킹하여 국방통합데이터센터 백신 중계서버까지 침투하였다. 업체가 규정을 어기고 분리된 군 내부망과 외부망을 연결해 작업하는 사이 해커는 악성코드를 심어 군사자료를 탈취하였다. 해킹 그룹은 8월 4일 백신 중계서버를 최초로 공략해 악성코드를 심었다. 9월 23일 악성코드 감염징후를 포착하였으며, 9월 25일 서버를 물리적으로 분리하였다. 한민구 국방부 장관의 컴퓨터 등 3천대가 넘는 군 내부 PC가 악성코드에 감염되었고, 일부 기밀자료도 유출된 것으로 추정된다. 해킹에 사용된 일부 IP가 북한 해커들의 근거지인 중국 선양 IP로 식별됐고, 악성코드도 과거 북한의 사이버 공격 코드와 유사성을 들어 배후세력을 북한으로 추정하였다.

• ATM 해킹으로 신용카드 정보 유출(2016~2017)

북한 해커가 ATM 해킹으로 2,500여개의 카드정보를 빼낸 뒤, 유출된 카드정보를 이용하여 카드를 복제해 현금인출 등 1억 264만원을 사용한 사건이다. ATM에서 유출된 정보는 카드번호, 유효기간, 비밀번호 등의 카드정보와 결재은행, 결제계좌, 잔액 등의 은행정보, 이름, 주민번호, 법인번호 등의 개인정보를 포함하고 있다.

2017년 3월, 금융감독원이 경찰청 등 관계기관으로부터 '청호이지캐쉬'가 운영하는 ATM이 악성코드에 감염됐을 가능성이 있다는 정보를 입수하고, 사실여부를 확인한 결과, 편의점 및 대형할인점 등에 설치된 ATM 63대가 악성코드에 감염되어 있다는 사실을 확인하였다.[72] 경찰 수사 결과에 의하면, 북한 해커는 국내 ATM 업체 백신 중계서버의 취약점을 이용하여 전산망을 해킹한 뒤, 전국 대형마트 및 편의점 등에 설치된 ATM 63대에 악성코드를 설치하고, 해킹된 ATM을 이용한 피해자들의 전자금융거래 정보 238,073건을 국내에 설치한 탈취 서버를 통해 유출한 것으로 확인되었다. 또한 북한 해커로부터 금융정보를 전달받은 공범들은 한국, 대만, 태국, 일본 등 각국에 퍼져있는 인출책들에게 유통하고, 복제카드를 만들어 국내외에서 현금을 인출하거나 대금 결제, 하이패스 카드 충전 등에 부

71) 뉴시스, 『軍기밀 털린 곳은 국방데이터센터…육·해·공군 정보의 '심장'』, 2016. 12. 7.; 보안뉴스, 『국방부 해킹 사건 수사결과 발표 "북한 해커조직 주도"』, 2017. 5. 2.; MBC, 『軍 "北 해킹 못 막은 책임자 20여 명 징계 방침"』, 2017. 5. 22.

72) The Science Times, 『해킹에 취약한 ATM 기기, 국내 1억 여원 피해 발생해』, 2017. 12. 6.

정사용해 온 것으로 확인되었다.[73]

금융보안원은 사건이 진행되었던 기간에 국내에서 발생한 일련의 침해사고 시도를 종합적으로 분석하는 과정에서 라자루스 그룹과 연관성을 가진 새로운 조직을 발견하고 그들의 행위를 추적한 결과 라자루스의 하위 그룹으로 활동하고 있는 '안다리엘(Andariel)'을 발견하였다. 그리고 조사과정에서 발견된 악성코드와 명령제어(C&C) 서버 등의 공통점을 근거로 국내에서 발생한 총 8개의 사이버공격을 하나의 캠페인으로 판단하고, '라이플 캠페인(Rifle Campaign)'으로 명명하였다. 라이플 캠페인이라 부르는 이유는 이 그룹을 프로파일링할 때 처음 본 샘플에 'Rifle'이라는 문자열이 포함되어 있었기 때문이다. 라이플 캠페인의 주요 공격 대상은 금융, 국방, 대기업, 보안 솔루션 제작 회사 등이었다.

※ 미 국토안보부(DHS)는 2018년 10월 2일 북한 정부가 지원하는 '히든 코브라'라는 이름의 해킹그룹이 악성코드를 이용해 현금자동인출기(ATM)에서 현금을 빼돌리고 있다고 밝혔다. 악성코드와 IOC를 이용해 은행 내 소매결제 시스템을 감염시킨 뒤 ATM에서 현금을 빼돌리는 수법을 사용하였다. 특히 2016년 후반 이후 이런 수법으로 아시아와 아프리카 은행을 상대로 수 천만 달러를 빼돌렸고, 2017년에는 30개 나라, 2018년에는 23개 나라의 ATM에서 동시에 상당한 규모의 현금을 인출하였다.[74]

북한 해커가 가짜 직업 구직을 위한 스카이프 인터뷰를 통해 ATM 네트워크 관리업체 근무자의 컴퓨터에 침투한 후, 칠레 전체의 ATM기 네트워크를 마비시킨 사이버공격도 발생하였다. 칠레 ATM기 네트워크 관리업체에 근무하는 직원은 개발자 자리에 대한 링크드인(Linkedin) 채용공고를 발견하고 이에 응신하였다. 스카이프 인터뷰 계획이 확정되고 컴퓨터에 'ApplicationPDF.exe' 프로그램을 설치하라는 요구를 받은 후 해당 파일을 설치하자 컴퓨터에 악성코드가 설치되고 해커들은 중요 정보를 빼낸 후 칠레 전체의 ATM 네트워크를 마비시켜 버렸다.[75]

---

73) 보안뉴스, 『한국 범죄자와 손잡은 북한 해커, ATM 해킹해 23만건 금융정보 탈취』, 2017. 9. 6.

74) Foxnews,, 『North Korean hackers accused of stealing millions from global banks』, 2018. 10. 3.; VOA, 『미 국토안보부, 북한 해킹그룹 주의 경보…"악성코드로 ATM 현금 빼돌려"』, 2018. 10. 4.

75) Ubergizmo, "North Korean Hackers Set Up Fake Interview To Access Chile's ATM Network", 2019.1. 1 6.; ZDNet, 『North Korean hackers infiltrate Chile's ATM network after Skype job interview』,

• 워너크라이 사태(2017)[76]

2017년 5월 12일부터 등장하여 전 세계 150개국 약 20만 여대의 PC를 감염시킨 워너크라이(WannaCry) 랜섬웨어는 북한의 소행으로 공식화된 랜섬웨어로서, 병원, 학교, 기업과 가정을 가리지 않은 무차별적 공격으로 인해 수십억 달러에 이르는 손실을 초래하였다. 5월 13일, 킬 스위치가 발견되면서 감염 확산은 손쉽게 차단되었다. 워너크라이 랜섬웨어 분석 결과 특정 도메인으로의 접속을 시도하는 것이 확인되었고, 해당 도메인은 등록되지 않은 상태로 남아 있어, 10.69달러의 등록비를 지불하고 도메인을 활성화시키는 것으로 워너크라이의 활동은 중단되었다. 그러나 변종인 워너크라이 2.0은 킬 스위치 없이 동작한다.

• 하나투어 개인정보 유출 사고(2017)

2017년 10월 17일, 언론을 통해 먼저 하나투어의 고객정보 유출 사실이 언론매체를 통해 보도되고 난 후, 하나투어는 바로 다음 날인 10월 18일 자사 홈페이지를 통해 2004년 10월부터 207년 8월 사이에 생성된 개인정보 파일이 사이버공격에 의해 유출되었음을 공지했다. 그리고 유지보수업체 직원의 개인 PC가 악성코드에 감염된 사실을 인지하고 조사하는 과정에서 해당 PC를 통해 개인정보 파일의 일부가 유출된 사실을 발견하였으며, 유출된 개인정보는 고객 이름, 주민등록번호, 휴대폰 번호, 집 전화번호, 집 주소 및 이메일 등으로 확인되었다.[77]

하나투어에 대한 사이버공격에 사용된 악성코드는 2015년 북한 해커조직이 방산업체 컨퍼런스인 '서울 ADEX' 참가업체를 노린 사이버공격에서 사용했던 악성코드 및 대기업 S그룹과 H그룹 계열사 해킹 사건에 사용했던 악성코드와 매우 유사한 것으로 알려지면서, 일련의 사건들이 동일범의 소행인지와 대규모 사이버 공격의 일부일 가능성에 대해서 관심이 증폭되기도 했다.[78]

공격으로 인해 유출된 개인정보의 규모와 관련해 최초 언론보도에서는 100만 건을 언급하였으나, 수사당국에서는 45만 건으로 발표하였으며, 자료를 유출했다고 주장하는 해커는 유출 건수가 2,800만 건이라고 주장하였다. 그리고 고객 정보

76) WSJ, 『"It's Official: North Korea Is Behind WannaCry』, 2017. 12. 18.; 자유아시아방송, 『백악관 "워너크라이 랜섬웨어 공격은 북한 소행"』, 2017. 12. 19.
77) Bloter, 『하나투어 고객정보 유출…해커, 비트코인 요구, "당국 수사에 따르면 45만 건 유출…2차 피해 방지 위해 노력중"』, 2018. 10. 22.
78) 보안뉴스, 『[단독] 하나투어 해킹 사건으로 대규모 사이버 공격 전모 밝혀지나 』, 2017. 11. 17.

2,800만 건에 대한 보상으로 99비트코인(약 6억 2,300만원)을 요구하는 협박 메시지를 보내기도 했다. 즉, 하나투어 고객정보 유출이 단순한 개인정보유출에 그치는 것이 아니라 직접적인 금전적 이득을 취하기 위한 목적의 개인정보 유출이었다는 점에서 기존 개인정보 유출과는 차별성을 가지고 있다.

사이버공격에 사용된 악성코드가 과거 북한이 주체로 지목된 공격에서 사용되었던 악성코드와 유사하다는 점 때문에 북한을 공격 주체로 추정하는 의견이 다수였으나, 행정안전부가 방송통신위원회 및 한국인터넷진흥원과 합동조사단을 구성하여 현장조사를 실시한 결과 구체적인 정황이 확인되지는 않았다.

• **암호화폐 거래소 공격(2017~2019)**

2017년 2월 북한의 해커조직이 대표적인 암호화폐 거래소인 빗썸에서 발생한 700만 달러 상당의 암호화폐 도난 사건에 연루되었을 가능성이 처음으로 보도되었다. 빗썸을 대상으로 수행된 북한의 사이버공격은 예전의 공격들과 동일하게 사회공학적인 기법을 활용하여 내부 직원의 개인 PC를 해킹하는 작업에서 출발하였다. 내부 직원이 자택에서 사용하던 개인 PC가 해킹되고 전체회원의 3% 수준인 3만 6,000여 이용자의 휴대전화와 이메일 주소 등 개인정보가 유출되면서, 북한 해커들에 의한 2차 공격이 진행되었다. 북한 해커들은 유출한 개인정보를 활용해 피해자들에게 전화를 걸어 빗썸 온라인 계좌가 해외에서 해킹을 시도하고 있음을 통보하며 일회용 패스워드(OTP) 번호를 바꿔야 하므로 현재 비밀번호를 알려달라는 방식으로 추가 정보를 탈취해 70억원 상당의 돈을 인출하였다.[79]

2017년 4월 22일에는 유빗이 보유한 자금 중 5분의 1에 해당하는 55억원을 탈취당하고, 2017년 12월 19일에는 두 번째 해킹을 통해 전체 자산의 17%를 탈취당하면서 파산 선언을 하게 된다. 미국 사이버보안업체 리코디드 퓨처는 2018년 1월 발표한 보고서를 통해 유빗 해킹의 배후로 라자루스 그룹을 지목하였다. 라자루스를 지목한 근거로는 사이버공격에 사용된 악성코드가 2014년 발생한 소니픽처스 해킹과 2017년의 워너크라이 사태에서 사용된 악성코드와 유사하다는 점을 들었다. 또한 한국의 범용 워드프로세서인 아래한글을 해킹 도구로 삼았다는 점도 북한을 공격주체로 확신하는데 크게 작용하였다.[80]

79) 매일경제, 『비트코인 거래소 `빗썸` 3만명 고객정보 털렸다』, 2017. 7. 3.; 연합뉴스, 『가상화폐거래소 빗썸 "개인정보유출 피해자 전원에 보상금"』, 2017. 7. 4.

유빗 해킹 사건 이후에도 암호화폐 거래소에 대한 사이버공격은 지속적으로 발생하면서, 상당한 규모의 금전적 피해가 발생했다. 2018년 6월에는 코인레일에서 약 4,000만 달러의 암호화폐가 도난당했고, 같은 기간 이미 한번 공격을 당했던 빗썸에서 약 250억원이 탈취되는 피해가 발생했다. 빗썸은 2019년 3월 세 번째 사이버공격을 당하면서 1,900만 달러를 탈취당했다. 2018년 10월에는 올스타빗도 사이버공격을 당해 가상화폐가 유출되었으나, 구체적인 피해금액은 확인되지 않았다.[81]

80) 연합뉴스, 『美보안업체 "유빗 해킹 배후, 북한 연계 라자루스 유력"』, 2018. 1. 17.
81) 보안뉴스, 『[2019 국감] 최근 3년 암호화폐 거래소 해킹사고 8건...약 1,266억 원 피해』, 2019. 9. 30.

4. 사이버위협 양상 변화의 전략적 의도와 정책적 함의

이라크전을 지켜보면서 최고지도자인 김정일 국방위원장이 정보전을 강조한 이후 북한은 사이버전 수행역량 확충을 위해 다각도의 노력을 전개하였고, 그 결과 현재는 전 세계가 인정하는 상당한 수준의 사이버전 수행역량을 갖추게 되었다. 비록 사이버 인프라는 열악하지만, 최고지도자의 강력한 추진 의지와 사이버전 전문가 양성을 위한 체계적인 교육체계, 해킹역량 확보를 장려하면서 전문가는 최대한 우대하고 성공에 대한 확실한 보상을 지급하는 내부 분위기는 북한을 전 세계가 두려워하는 최고의 사이버강국으로 나아가게 해주는 훌륭한 원동력이 되었다. 그에 더해 열악한 사이버 인프라는 방어적 측면에서 북한을 잃을 것이 없는 국가, 국가 마비나 파괴를 두려워하지 않고 오로지 공격에만 전념할 수 있는 국가로 나아갈 수 있는 더없이 좋은 기반이 되고 있다.

정보전과 사이버전의 중요성을 인식한 이후로 사이버역량의 사용은 북한에게 경제역량이 극도로 제한되는 상황 하에서도 가장 이상적이고 합리적인 군사적 선택을 제공해 왔다. 그리고 그러한 선택을 통해 북한은 이미 충분한 성공을 경험했기에 선택이 틀리지 않았음을 확신하고 있을 것이다. 따라서 향후 사이버전 수행역량은 미사일 또는 핵만큼이나 북한에게는 포기할 수 없는 전략적 자산이 될 것임은 자명하며, 운용의 범위나 규모, 빈도가 획기적으로 증가하게 될 것임을 충분히 예측 가능하다. 안보환경이 변화와 경제적 가치의 흐름전환에 발맞춰 북한은 최적의 사이버역량을 개발하고 적용해 나가기 위해 노력할 것이고, 우리는 그에 대한 대응방안을 선제적으로 마련해 나가야만 한다.

이에 본 장에서는 북한발 사이버위협 양상의 변화가 어떤 의도를 내포하고 있는지를 추정해보고 북한의 변화되는 전략적 의도에 능동적으로 대처하기 위해 참고할 수 있는 정책적 함의를 도출해 보고자 한다.

4.1 사이버위협 양상 변화에 따른 전략적 의도 변화

이상에서 살펴 본 북한發 사이버공격들을 시간순으로 나열하여 정리한 결과는 〈그림 2-3〉에서 보는 바와 같다. 그림에서는 본 연구에서 조사 대상에 포함시키지

는 않았으나, 북한이 명확한 공격주체로 지목된 단순 시도 형태의 사이버공격도 일부 포함되어 있다.

〈그림 4-1〉에서 확인할 수 있듯이, 2009년까지의 사이버공격은 7.7 DDoS 공격을 제외하고는 전부 정부기관 및 주요 기관 등을 대상으로 기밀정보 유출을 시도하는 공격이었다. 그리고 북한이 이라크전쟁을 계기로 전자전 및 정보전의 개념을 구현하기 위해 노력했던 시기이기 때문에, 전 세계를 대상으로 지금과 같은 대규모의 사이버위협을 가하기보다는 전문인력 양성과 기술개발을 통한 역량확보에 주력했을 것으로 짐작할 수 있다.

2016년도에 발표된 북한의 사이버작전 전략 분석 보고서[82]에 의하면, 1997년 조명래에 의해 개발된 'JML' 악성코드의 변종은 북한 내부의 독자 개발환경을 기반으로 개발된 것이 아니라 외부 소스를 통해 개발된 것으로 추정되고 있다. 즉 2000년대 초반은 자체 역량이 성숙되지 못한 상황에서 중국이나 러시아의 지원을 받아서 혹은 다른 해커집단이 사용하던 소스를 활용하여 사이버무기의 개발을 시도했던 단계로 볼 수 있다. 2014년 미국의 사이버보안업체 Novetta가 소니픽쳐스 해킹사건을 조사한 결과를 담아 발표한 보고서[83]에 의하면, 라자루스 그룹이 2007년 3월부터 향후 사이버공격에 사용하기 위한 1세대 악성코드를 개발하기 시작하였다고 한다. 이를 통해 짐작해 볼 있는 점은 북한이 전 세계를 대상으로 대규모의 사이버위협을 감행하기 이전인 2009년까지는 자체적으로 역량을 키워나가면서 대한민국을 대상으로 소규모의 사이버공격 수행을 통해 사이버무기의 적용 가능성을 시험해 보았을 것으로 판단된다.

82) Rowman & Littlefield,, "North Korea's Cyber Operations: Strategy and Responses", 2016.
83) Novetta, "Operation blockbuster; Unraveling the long thread of the Sony attack", 2016. 2.

〈그림 4-1〉 시간순으로 나열한 북한發 사이버공격 사례

〈표 4-1〉 사이버공격과 군사도발의 상관관계

시기	공격목표	형태	대응	주요 군사도발
2004. 6	국회, KIDA, 해경, 원자력연구원 등	악성코드에 의한 정보유출		
2004. 8	군 통신채널 침투	침투		단거리미사일 발사(5월)
2005				핵 보유 선언
2006				1차 핵실험(10월)
2007	논리폭탄 실험	논리폭탄	국제사회 경제제재	
2008	군 장교 대상 악성메일 유포	악성 이메일		박왕자씨 피살(7월)
2009. 3	3군사령부 및 화학 관련 기관	정보 유출		광명성 2호 발사(4월) & 2차 핵실험(5월)
2009. 7	청와대, 국방부, 언론매체, 금융권 등	DDoS	사이버사 창설	
2009. 12	연합사령부	정보유출		대청해전(11월)
2010				천안함 피격(3월) 연평도 포격 도발(11월)
2011. 3	정부기관/민간서비스	DDoS		
2011. 4	농협전산망	DoS		
2012. 6	중앙일보	해킹 시도		GPS 교란(4월) ICBM 시험 발사(4월)
2013. 3	57,000대 시스템	APT		3차 핵실험(2월)
2013. 6	정부기관/싱크탱크	APT		
2014. 12	한수원	정보 유출		
2015. 10	청와대 & 외교부	해킹 시도		
2016. 3	GPS 재밍 시도	GPS 재밍		미사일 발사(2월) 4차 핵실험(1월) 청와대 타격 위협(3월) 무수단 6발(4월~7월) SLBM 2발 발사(4,8월)
2016. 3	청와대/정부부처 인사 스마트폰 해킹	스마트폰 해킹		
2016. 7	인터파크 해킹 및 고객정보 유출	APT 정보유출		
2016. 9	국방망 해킹	APT 정보유출		
2017. 1	북한관련단체 사칭 악성메일 발송	해킹 시도		ICBM 개발완료 발표

2009년부터 북한은 본격적으로 전 세계를 위협하는 사이버공격을 감행하기 시작한다. 특히 북한이 수행한 최초의 전 세계 대상 사이버공격의 첫 번째 희생자가 미국이었다는 점을 고려하면, 북한의 사이버역량에 대해 충분한 자신감을 가지고 있었음이 분명하다. 핵 및 미사일에 버금가는 비대칭전력으로서 사이버역량을 활용할 수 있겠다는 자신감이 충만한 상황이었다 볼 수 있고, 체제의 건재함을 세계에 과시하기 위한 수단으로도 적극적으로 활용하였다.

2009년부터 본격적으로 진행된 북한의 사이버공격은 김정은의 후계 구도를 확고하게 굳히는데도 크게 기여하였다. 재래식 전력으로는 감히 넘볼 수 없는 미국을 대상으로 상당한 피해를 입혔던 7.7 DDoS 공격을 시작으로 2013년까지 이어진 대규모의 사이버공격은 국제사회와 대한민국에 김정은의 존재를 확실히 각인시켰다. 그리고 최고지도자로서의 집권이 시작된 2011년부터는 대한민국을 대상으로 한 사이버공격을 활발하게 전개하면서, 군사적 도발도 동시에 전개하기 시작한다. 〈표 4-1〉을 통해 확인할 수 있는 바와 같이, 2009년부터 2016년까지의 사이버공격은 대부분 군사적 도발과 병행하여 수행되었다. 대한민국이 연합훈련이나 UFG 등의 대규모 훈련을 실시했던 시기와도 교묘하게 겹쳐 있다. 사이버공격을 감행하기 1~2개월 전부터 방송이나 신문매체를 통해 대한민국의 전쟁연습은 북한체제를 위협하는 명백한 도발행위라고 규탄하며, 철저한 보복을 하겠다는 의지를 표명한다. 그리고 훈련기간을 전후로 사회불안을 조장할 수 있는 수준의 대규모 사이버공격을 감행하여 국민적 불안감을 증폭시켰다. 사이버공격이 감행된 이후에는 긴장감이 저하되는 것을 방지하기 위해 공해상으로 미사일을 발사하면서 기술력의 발전과 체제의 건재함을 과시하는 동시에 내부적으로는 결속을 강화하는 수단으로 활용하였다. 즉, 금강산 관광객의 피살 사건 이후 남북관계가 본격적으로 경색되기 시작한 2009년부터 군사적 긴장이 지속되었던 2016년까지 북한은 사이버역량을 군사적 긴장감을 고조시키는 보조수단이자 대한민국에 사회불안을 가중시키는 핵심 수단으로 활용하면서 국제 협상테이블에서 유리한 위치를 선점하기 위한 수단으로 활용하였다.

그러나 무리한 군사도발로 인해 국제사회의 제재가 강화되고 내부적으로는 심각한 경제난에 직면하게 되면서, 2016년도부터는 재화 마련을 위한 수단으로 사이버역량을 활용하기 시작한다. 사이버역량을 사용하여 SWIFT를 해킹하고 가상화폐 거래소를 해킹하여 데이터를 탈취하기만 하면, 수백만 달러에 달하는 재화를 너무

도 손쉽게 확보할 수 있었고, 워너크라이와 같은 랜섬웨어를 국제적으로 확산시키기만 하면 단기간에 북한이 원하는 수준의 재화를 마련할 수 있었기 때문에, 금융분야에 특화된 안다리엘과 같은 조직을 신설하면서까지 재화벌이에 집중했을 것이다. 작게는 개인정보 유출을 통해 가상화폐의 지불을 요구하기도 했고, 크게는 방글라데시 중앙은행과 미국 연방준비은행의 국제거래까지 해킹하면서 수천억 달러에 달하는 재화를 획득하였다.

2019년 3월 공개된 유엔 안전보장이사회 보고서에서는, 북한이 2015년부터 2018년까지 해킹 활동을 통해 약 6억 7,000만 달러를 확보한 것으로 명시했다. 그리고 8월에 발표한 대북제재위원회 보고서에서는 북한 해커들이 국제은행 및 암호화폐 거래소 해킹을 통해 20억 달러에 달하는 자금을 확보한 것으로 명시했는데, 이는 북한의 연간 GDP의 7%에 해당하는 금액이다. 그리고 사이버역량의 사용을 통해 확보한 자금은 대부분 대량살상무기(WMD) 개발에 사용된 것으로 보인다는 의견을 제시하였다.[84]

국제사회의 제재가 강화되기 시작한 2016년 이후부터의 사이버역량 사용의 주된 목적인 북한 내부의 만성적인 식량난, 경제제재로 인한 대외적 고립 및 경제위기 상황하에서의 재화 확보로 볼 수 있지만, 그 와중에도 대한민국의 사이버공간을 향해서는 크고 작은 사이버위협을 지속적으로 전개하였다. 표면적으로는 7.7 DDos나 농협 전산망 해킹사건과 3.20 사이버테러 같이 사회적 불안을 조장하고 막대한 경제적 피해를 유발할 수 있는 대규모의 사이버공격이 사라진 것처럼 보이기에, 국민의 입장에서는 사이버위협에 둔감해질 수밖에 없는 상황이다. 정부 차원에서도 2018년 이후 북한에 의한 직접적인 사이버위협이 확연하게 감소하였기에, 사이버보안에 대한 투자와 사이버안보 역량 강화를 위한 각종 사업들이 추진동력을 잃을 수도 있다는 우려의 목소리가 나오고 있다. 따라서 북한의 사이버위협이 다른 방향을 지향하고 있는 것이 아니라 현재의 안보상황에 맞도록 잠시 변화되었을 뿐이며, 언제든 상황이 변화되면 즉시 직면하게 될 상존 위협임을 명심해야만 할 것이다. 위협의 형태는 변할 수 있지만 그 본질은 변하지 않는다. 북한이 체제유지를 포기하지 않는 한 위협은 계속될 것이며, 우리는 항상 준비된 자세를 견지해야만 한다.

84) The Epoch Times, 『"맞을 짓 하지 말라"던 북한, 비트코인 해킹한 자금으로 미사일 제조』, 2019. 8. 10.

4.2 사이버위협 양상 변화에 대한 대처방안

대한민국의 연결성이 강화된 네트워크 환경과 개방된 인터넷, 그리고 ICT에 대한 심화된 의존성 및 복잡성은 북한이 자신의 사이버역량을 테스트하고 검증할 수 있는 최상의 공간이다. 그리고 대한민국은 북한의 사이버위협에 효율적으로 대응하고 발생한 위협을 최대한 빨리 완화시키거나 피해를 신속하게 복구하는데 집중해 왔기 때문에, 전술한 바와 같이 북한發 사이버위협에 대해서는 구체적인 대응조치를 취한 경우가 없다. 또한 사이버공간상에서의 위협을 규제할 수 있는 국제규범이 부재한 상황에서 전 세계 대부분의 국가들은 국가사이버안보전략의 개정을 통해 사이버위협에 대한 억지 또는 보복, 더 나아가서는 선제적 공격에 대한 의지를 천명하고 전략에 명문화하고 있다. 그러나 대한민국의 국가사이버안보전략은 그러한 개념을 포함하지 않고 있다. 이러한 상황이 향후에도 지속될 경우에는, 대한민국의 사이버공간은 북한이 보복을 두려워하지 않으면서 자신의 역량을 마음껏 펼쳐볼 수 있는 시험장의 위치를 벗어날 수가 없을 것이다. 따라서 향후 북한發 사이버위협의 양상이 안보환경 변화에 발맞춰 다변화되더라도 효율적으로 대응하기 위해서는 국가사이버안보전략 상에 사이버위협에 대한 적극적인 대응 의지를 담아낼 필요가 있다.

그리고 사이버위협이 초국경적 성격을 가지기 때문에 일개 국가 혼자서 효율적으로 대응하는 것은 불가능하며, 다른 국가와의 강력한 협력이 반드시 필요하다. 특히 제3국을 경유하면서 사이버공격을 수행하는 북한임을 고려하면 주변 국가와의 사이버분야 공조는 반드시 필요하고, 일반적인 공조보다는 국제규범의 틀 안에서 구속력을 가질 수 있는 공조체제로의 진입이 필요하다. 또한 대규모 사이버공격은 공조를 넘어서서 공동대응체계를 필요로 한다. 유럽연합의 경우 회원국이 사이버공격을 당하면, 회원국이 공동으로 외교적·경제를 가함으로써 잠재적 공격자에 대해서도 억지력을 가질 수 있는 공동대응체계를 구축하여 운영하고 있다. 따라서 우리도 기 구축된 공동대응체계의 틀 속에 합류하거나 혹은 협력 가능한 국가들과의 협약 체결을 통해 사이버위협에 대한 공동대응체계를 구축해 나갈 필요가 있다.

마지막으로 지난 2018년의 9.19 군사합의가 진행되었을 때 사이버전 분야는 제외된 바 있다. 현재 북한의 사이버능력 성숙 및 사용과 관련해 국제법상으로 어떠

한 부분도 금지되어 있지 않으며, 금지할 수도 없다. 사이버 역량의 확충 및 강화는 군비축소 대상도 아니다. 따라서 북한의 사이버역량 확충이나 사용을 제한하는 것은 대한민국이 압도적인 사이버역량을 구비하지 않는 한 불가능하다고 볼 수 있으며, 북한과의 양자대화를 통해 해결해 나가는 것이 필요하다. 즉, 누구보다 사이버역량을 전략적으로 활용하고 있는 북한이기에 사이버영역에서의 우발적 충돌 방지 및 상호 불가침에 대해 논의하고, 향후 군사합의사항들에 대한 재검토가 이루어질 기회가 마련된다면 해당 사항을 군사합의사항에 포함시키는 노력을 진행해 나가야만 할 것이다.

본 절에서는 국제규범의 틀 속에서 북한의 사이버위협을 간접적으로 완하하고 억지할 수 있는 방안으로서, 국제적 수준의 공동대응체계구축 및 사이버범죄협약 가입 방안에 대해서만 세부적인 내용을 기술하고자 한다.

가. 대규모 사이버위협에 대한 공동대응체계 구축

대규모 사이버위협에 대한 공동대응체계 구축의 첫걸음은 우선 한미 상호방위조약이 국가급 사이버공격에 대한 공동대응을 포함할 수 있도록 개정을 추진하는 것에서부터 시작할 필요가 있다. 일본은 2018년 12월 신 방위대강을 발표하면서, 자위대의 통합운영 범위를 우주·사이버·전자적 영역까지 확대하겠다는 의지를 천명하였고, 새롭게 추가되는 통합운영 영역에서의 대처능력 강화 방안도 구체적으로 명시한 바 있다. 한편으로는 2019년 4월 개최딘 미일안보협의위원회를 통해 일본에 대한 대규모 사이버공격에 대해서도 미국의 대일방위 의무를 규정한 미일안보조약 5조가 적용될 수 있음을 명시하면서, 미일동맹을 첨단 군사영역으로 확대 및 강화하고 있다.

대한민국도 한미상호방위조약을 사이버공간 등 첨단 군사영역으로 확대해야 할 필요성에 대해서는 공감하고 있다. 지난 2013년 북한의 사이버위협이 급증하고 심각한 피해를 유발했던 한미상호방위조약의 확대 및 강화에 대한 주장이 활발하게 제기되었다. 그러나 2018년 제50차 한미안보협의회의(SCM)에 이르기까지 관련 사항을 심도있게 논의한 적이 없다. 따라서 우리도 일본의 사례를 참고하여 한미상호방위조약의 틀 속에 대규모 사이버공격에 대한 상호 방위의무를 포함시켜 나가야만 한다.

공동대응체계을 구축하기 위해 참조할 수 있는 또 다른 모델은 유럽연합이 시행

하고 있는 'Cyber Diplomacy Toolbox' 이다. 그와 같은 공동대응체계를 구축하기 위해 우선은 ASEAN 국가들을 중심으로 사이버위협 대응을 위한 국가 간 상호협력 증진 및 우발적 상호 분쟁 사전 방지협약을 체결하면서 단계적인 공동대응체계 구축을 추진할 필요가 있다. 대한민국이 ASEAN에 직접적으로 속해있는 국가는 아니지만, ASEAN + 3[한국, 중국, 일본] 및 동아시아 정상회의, 아세안 지역포럼 등을 대화 및 협력 추진 창구로 활용하는 것은 가능하다. 그러나 ASEAN 국가들을 대상으로 사이버외교를 추진하고 공동대응체계 구축을 추진함에 있어서는 다음과 같은 사항들을 충분히 검토할 필요가 있다.

우선 일본이 ASEAN 내에서 차지하고 있는 입지이다. 일본은 이미 10년 전부터 ASEAN 국가들을 대상으로 활발한 역량강화 지원활동을 전개하면서 ASEAN 내에서의 입지를 강화한 상황이다. 따라서 한국이 ASEAN 국가들을 대상으로 사이버외교를 추진하고 공동대응체계 구축을 제안하기 위해서는 일본과의 협조가 반드시 선행되어야만 한다. 둘째, ASEAN 국가들의 관심사를 제대로 파악하고 접근해야만 한다. 베트남, 미얀마, 라오스, 캄보디아 등 1990년대 후반 ASEAN 가입국들은 비(非)서방주의 노선을 표방하며, 인터넷에 대한 강력한 국가통제를 주창하는 중국의 입장에 동조하고 있는 상황이다. 마지막으로 중국의 '디지털 실크로드' 구축 활동을 잘 지켜보아야 한다. 중국은 디지털 실크로드 구축이라는 명분하에 화웨이와 ZTE를 내세워 동남아에 대한 관여를 강화하고 있다. 그리고 ASEAN 후발 국가들은 자국의 사이버안보 역량강화를 지원해 주는 파트너로 중국을 더 선호하는 경향을 보이고 있다. 결론적으로 우리가 공동대응체계 구축을 추진할 수 있는 대상은 ASEAN 국가들이 최적이지만 반드시 넘어서거나 사전 협력을 추진해야 할 대상이 바로 중국과 일본임을 명심하고, 신중하게 접근할 필요가 있다. 그리고 후발 주자들보다는 ASEAN에서 사이버안보 선도국에 속해있는 말레이시아 및 싱가포르와의 양자협약을 우선적으로 추진하는 것도 현명한 선택이 될 것이다.

나. 유럽 사이버범죄협약 가입

경찰청에서 발표한 통계자료에 의하면, 대한민국에서는 최근 5년 동안 매년 10만 건 이상의 사이버범죄가 발생하고 있다. 그리고 발생하는 사이버범죄의 상당수는 대응을 위해 국제적인 공조를 필요로 한다. 현재 대한민국은 형사사법공조나 범죄인인도협약을 통해 국제공조를 진행하고 있으나, 국가적 사안이 아니면 협조가

제대로 진행되지 않고, 수사기관 간 공조가 진행된다 하더라도 그 수준이 낮아 사이버범죄 감소 효과는 미흡한 실정이다. 그리고 북한의 사이버위협이 중국 또는 제3국의 경유하여 수행되는 경우가 대부분임을 고려하면, 대응에 있어 국제공조는 필수적이다. 그런 면에서 가입국들에 대해 법적 구속력을 가지는 최초의 사이버공간 관련 국제협약이라고 할 수 있는 사이버범죄협약의 대한민국이 반드시 가입을 추진할 필요가 있는 국제협약이다.[85]

사이버범죄협약은 가입을 위해 국내법을 협약에서 요구하는 국제기준을 충족하는 방향으로 정비할 것을 요구한다. 대한민국이 사이버범죄협약 가입을 위해 필요한 법제도 개선 소요는 〈표 4-2〉에서 확인할 수 있다. 국내의 일부 법학자들은 국내법의 개정 없이도 협약 가입이 가능할 것이라는 주장을 펼치고 있지만, 협약에서 요구하는 조건은 의외로 엄격하여 이행입법이 필요한 상황이다. 그러나 이행입법을 추진하는 과정에서 필수적인 부분이 바로 수사기관의 권한 강화이기 때문에 그로 인해 발생할지도 모를 국민의 기본권 제한에 대해서도 신중하게 검토해야 할 것이다.

85) 2017년 수행된 연구에 의하면 사이버범죄협약 가입국은 사이버범죄 발생 비율이 감소하였으며, 대한민국과 같은 비가입국은 지속적으로 사이버범죄가 증가하고 있다고 한다.

〈표 4-2〉 사이버범죄협약 가입을 위한 국내 이행입법 소요

구 분	이행입법 필요 주장	이행입법 불필요 주장
제16조 (저장된 컴퓨터 데이터의 신속한 보전)	• 정당한 사용자가 저장한 데이터도 해당되어 압수수색과 차이가 있음 • 통신사실 확인자료는 통신이 되고 있는 데이터 의미	• 두가지 국내법으로 협약의 목적 일부를 달성 가능할 것으로 판단 ('유사한 조치'에 해당)
제17조 (트래픽 데이터의 신속한 보전 및 제출)	• 협약 요구 자료 중 통신사실 확인자료 요청제도의 제공자료 일부 미포함 (통신경로, 통신 크기, 서비스유형)	• 통신사실 확인자료 요청 제도의 자료 중 착/발신 통신번호, 로그기록, 위치 추적 자료 및 압수수색으로 관련내용 유추 가능
제18조 (컴퓨터 데이터 및 가입자 정보의 제출명령)	• 협약은 수사기관에 단독적인 제출 명령권을 부여하고 있으나, 한국은 법원의 권한	• 범죄혐의가 있는 컴퓨터만을 선별하여 제출명령을 시행해야 하는 것은 무의미
제19조 (컴퓨터 데이터의 수색과 압수) 2항(원격수색)	• 압수수색 과정 중 해당 컴퓨터가 다른 컴퓨터시스템, 웹하드, 클라우드 서비스 저장공간 이용시 원격수색을 허용하도록 요구 ※ 유사한 국내법 없음	-

5. 결 론

북한은 현존하는 국가 중에서 사이버역량을 가장 전략적으로 활용할 줄 아는 국가이다. 대한민국에 대한 최초의 사이버공격을 감행했던 2004년 이후 북한은 사이버역량을 한반도 안보상황과 국제정치 상황 변화에 맞춰 어떠한 상황에서도 전략적 우세를 달성할 수 있는 방향으로 활용해 왔다.

2004년부터 최근까지 발생했던 북한발 사이버공격의 분석을 기초로 사이버위협의 변화 양상을 분석해 본 결과, 크게 3가지 형태로 구분해 볼 수 있었다. 2004년부터 2009년까지는 사이버역량 확보의 전략적 중요성을 인식하고 내부적으로 역량 강화를 위한 다양한 노력을 전개하면서, 대한민국 정부기관과 주요기관들을 대상으로 한 기밀정보 수집을 지속적으로 시도하였다. 김정은의 후계구도가 거론되기 시작하고 사이버역량도 상당한 수준으로 성숙되었던 2009년부터는 한국을 비롯한 전 세계를 대상으로 사이버역량을 표출하면서 체제의 건재함과 우수성을 대외에 과시하고 내부적으로는 주민 결속 강화 및 체제안정을 도모하였다. 이 시기에는 국제사회의 제재가 본격화되기 시작한 2016년까지 핵실험 및 미사일 발사 등의 군사적 도발을 병행하면서, 군사적 긴장을 고조시키는 보조수단으로서 사이버역량을 활발하게 사용하였다. 그러다가 국제사회의 제재가 강화되기 시작한 2016년 이후부터는 경제제재를 교묘하게 회피하면서 재화를 확보하기 위한 수단으로 사이버역량을 적극 활용하였으며, 그 결과로 단기간에 북한 GDP의 7%에 해당하는 재화를 확보하였다.

북한에게 있어 사이버역량은 핵 및 미사일과 더불어 명확한 비대칭전력으로서의 역할을 확실하게 가지고 있는 상황이며, 안보상황 변화에 따라 다양한 목적으로 활용할 수 있는 수준으로 역량도 성숙하였다. 2018년 이후로 확연하게 줄어든 북한發 사이버위협으로 인해 대한민국의 사이버공간에도 평화가 찾아온 것처럼 오해할 수 있지만, 북한발 사이버위협은 잠시 형태를 전환했을 뿐이고 상황이 변하면 북한發 사이버위협은 언제든지 대한민국의 사이버공간을 향할 수 있음을 잊지 말아야 할 것이다. 위협의 형태는 변할 수 있을지 모르나 그 본질은 변하지 않는다. 북한의 위협이 다시 대한민국의 사이버공간을 향하게 될 때에는 지금보다 더 큰 위협으로 다가올 것이다. 따라서 갑작스럽게 찾아온 봄날에 취해있기 보다는 언제 다가올지 모르지만 상존하는 사이버위협에 보다 적극적으로 대비하는 노력도 기울

여 나가야만 한다.

이를 위해 우선적으로는 양자 협의 수준에서 사이버위협을 가장 빨리 완화할 수 있는 방안으로 북한과의 군사합의에 사이버공간에서 상호 충돌방지 및 불가침을 포함시킬 필요가 있으며, 다음으로는 한미상호방위조약을 사이버공간을 포함하는 수준으로 확대 및 강화시켜야 한다. 그리고 중국 및 일본이 ASEAN 국가들에게 미치는 영향력을 고려하면서 신중한 접근을 통해 ASEAN을 중심으로 한 사이버위협 공동대응체계의 구축을 추진해 나가는 노력이 필요하다. 마지막으로, 북한을 포함한 잠재적 위협국으로부터의 사이버위협에 효율적으로 대응하기 위해 국내법을 보완하면서 사이버범죄협약의 가입을 적극적으로 추진할 필요가 있다.

연구보고 2019

한반도 주변국의 과학기술과 안보위협 (무기체계를 중심으로)

마 정 목
(국방대학교 교수)

2019. 12.

국방대학교 산학협력단

목 차

그림목차

표 목 차

1. 연구개요

1.1 연구배경

우리 사회 모든 영역에 있어서 4차 산업혁명이라는 인간 삶의 근간을 뒤흔들 과학기술들이 이미 부분적으로 적용되거나 미래에 적용되어야 할 대상으로서 그 적용을 예고하고 있다. 산업혁명과 마찬가지로 군사 분야에서도 전쟁 양상의 변화에 대처하고 준비하기 위해 전쟁 개념과 전쟁 수행 방식의 혁신적 변화에 따라 전쟁의 세대(Generation of Warfare)를 구분하고 있으며, 많은 전문가들은 4차 산업혁명으로 대변되는 과학기술의 혁신적 발전이 다음 세대 전쟁의 특징을 규정지을 가능성이 높을 것으로 보고 있다. 특히, 전쟁 수행의 주요 수단인 무기체계는 과학기술의 영향을 직접적으로 받으며, 이미 개별 플랫폼 위주의 무기체계에서 벗어나 정밀성, 연결성, 자율성, 무인화 등을 강조하는 복합 무기체계 개발의 문턱에 들어서 있다. 우리 국방부도 새로운 과학기술들을 활용하여 사이버전, 지휘통제, 감시정찰, 군수, 인사, 의료 분야 등 각종 분야에서 스마트한 체계를 만들기 위한 현실적인 노력을 기울이고 있다. 이러한 환경에서 본 연구에서는 연구조사 시점에서 한반도 주변국인 미국, 중국, 일본, 러시아, 북한의 군사과학기술 및 무기체계 발전 동향을 체계적으로 분석해보고, 8대 무기체계 분류별로 기술발전 동향을 세부적으로 살펴봄으로써 우리가 앞으로 나아가야할 방향을 모색하고자 한다.

1.2 연구범위 및 목표

본 연구는 무기체계를 중심으로 한반도 주변국의 과학기술을 평가하고 세부적인 무기체계 발전 동향에 관련된 정보를 정리하여 제시하는 것을 목표로 하고 있다. 한반도 주변국으로는 미국, 중국, 일본, 러시아, 북한까지 역내 안보정세에 영향을 미치는 주요 5개국을 대상으로 삼았으며, 국가 수준에서의 무기체계 발전 동향의 파악을 첫 번째 단계로 보았다. 다음 방위사업법 시행령에 분류된 8대 무기체계의 분류에 따라 세부적인 무기체계 발전 동향을 체계적으로 분석하였다. 마지막으로 무기체계 발전 동향을 종합하고 우리가 지향해야할 방향을 도출해 보았다.

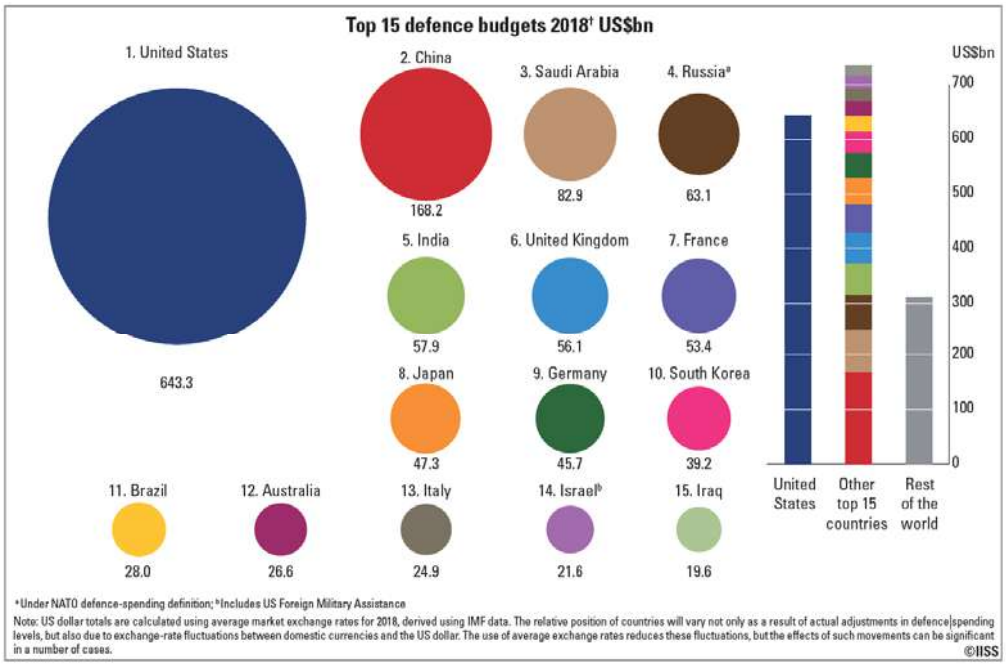
2. 국가별 무기체계 발전 동향

본장에서는 한반도 주변 주요 5개 국가인 미국, 중국, 일본, 러시아, 북한의 무기체계 발전 동향을 살펴본다. 아래 내용은 2018 국방백서, THE MILITARY BALANCE 2019 및 인터넷 공개 자료 등을 기초로 작성 및 재정리하였다.

2.1 미국의 무기체계

미국은 2017년 안보전략서(NSS: National Security Strategy)와 2018년 국방전략서(NDS: National Defense Strategy)에서 본토 보호, 자국의 번영 증진, 힘을 통한 평화 유지와 영향력 확대 등을 핵심 전략목표로 설정하고, 이를 힘으로 뒷받침하기 위한 군사적 우위 유지를 강조하고 있다.[1] 미국의 국방력은 군사적 우위를 달성하고 힘을 통한 평화를 달성하는데 필요한 핵심요소로서, 국방력 건설을 위해 투입되는 예산은 〈그림 2-1〉에 나타난 것처럼 세계 1위이다. 중국이 그 뒤를 따르고 있지만 미국 국방비는 2위 중국부터 11위 브라질까지의 국방비를 모두 합쳐야 미국의 국방비와 비슷한 수준에 이르는 막강한 수준을 유지하고 있다.

1) 국방부. “2018 국방백서”, 2018.



〈그림 2-1〉 국방비 상위15개 국가[2)]

그럼에도 불구하고, 2014년 11월 전 미 국방부 장관 척 헤이글은 지금까지는 미국이 우세한 기술력을 바탕으로 중국과 러시아보다 군사기술에서 우위를 차지하고 있었지만, 중국과 러시아의 군사기술이 급속도로 발전됨에 따라 미국의 군사기술 수준 우위가 보장받지 못할 수도 있다고 판단하였다. 이에 따라 미국은 빠르게 추격하고 있는 경쟁국에 대해 한 차원 높은 기술 혁신으로 군사적 우위를 유지하여 대응하는 제3차 상쇄전략(The Third Offset Strategy)을 현재까지 지속 추진하고 있으며 2017년 안보전략서(NSS)를 통해 그 내용을 확인할 수 있다. 제3차 상쇄전략은 미국의 군사과학기술 우세를 통해 군사적 우위를 지속적으로 유지해 나간다는 전략으로 〈그림 2-2〉와 같은 5가지 핵심 군사과학기술 분야를 제시한다.

2) IISS. "THE MILITARY BALANCE 2019", 2019.

〈그림 2-2〉 제3차 상쇄전략이 요구하는 핵심기술과 군사역량과의 관계도[3)]

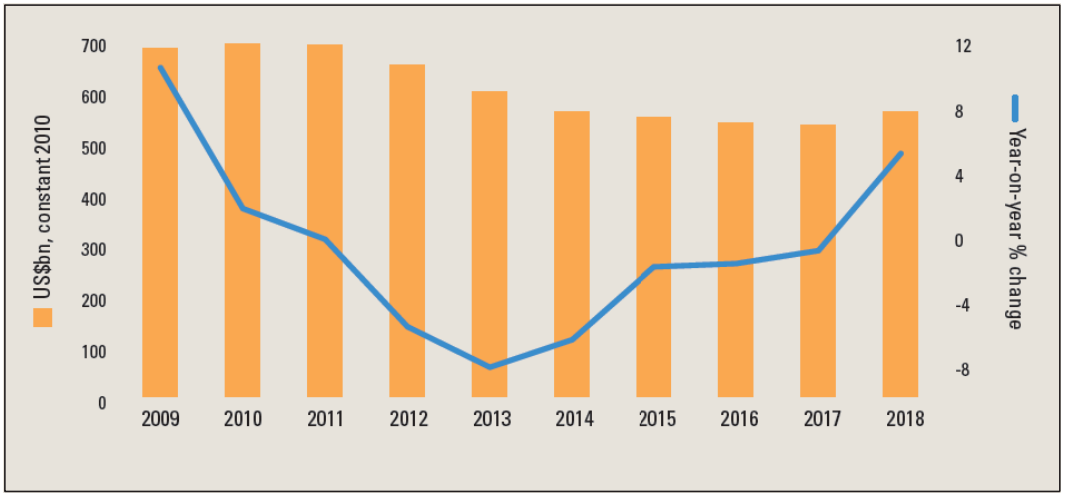
2017년 안보전략서(NSS)에서는 과학기술의 우세를 보유하고 유지하는 것이 국가 안보전략 중 하나라고 말한다.[4)] 과학기술의 우세는 국가 안보의 중요한 영역으로 국가 안보에 많은 영향을 미치며, 데이터과학(data science), 암호화(encryption), 자율화(Autonomous technology), 유전자 조작술(gene editing), 신소재(new materials), 나노기술(nanotechnology), 컴퓨팅기술(advanced computing technology), 인공지능(artificial intelligence) 분야가 앞으로 집중해야할 영역으로 판단하고 있다. 특히 자율주행차량에서부터 자율무기(autonomous weapons)까지 인공지능 분야가 급속하게 발전하고 있다고 언급한다.

이에 미 국방부는 안보전략서(NSS)의 국방분야 과제를 실현하기 위한 수단 중 하나로서 2018 국방전략서(NDS)에서 핵심능력의 현대화를 추진하고 있다. 그 중 첫 번째는 대륙간탄도미사일(ICBM: Inter-Continental Ballistic Missile), 잠수함발사탄도미사일(SLBM: Submarine-Launched Ballistic Missile), 전략폭격기 등 핵전력 3축 체계와 핵 관련 지휘/통제, 지원 기반시설을 현대화하는 것이다. 두 번째는 육상, 해상, 공중뿐만 아니라 우주, 사이버 영역을 군사작전이 이루어지는 전장으로 확대하여 우주 및 사이버 기술에 중점적으로 투자를 하는 것이다. 세 번째는 경쟁국들 보다 정보의 우위를 달성하기 위해 C4ISR(Command, Control, Communications, Computers and Intelligence, Surveillance, Reconnaissance)에 지속 투자하는 것이다. 네 번째는 전구미사일위협(Theater Missile Threats)과 북한 탄도미사일 위협에 대응하기 위해 다층적인 미사일 방어체계 구축을 추진하는

3) 산업연구원. "미국 新정부 국방획득정책 변화 및 대응전략 연구", 2018.
4) The White House. "National Security Strategy of the United States of America", 2017.

것이다. 끝으로 인공지능, 머신러닝, 자율화, 민간기술의 적용 등 첨단 자율 시스템을 군에 적용하기 위해 지속적인 노력을 기울인다는 것이다.

이를 뒷받침하듯 트럼프 대통령은 미국 국방예산을 확정짓는 2019 회계연도 국방수권법(NDAA: National Defense Authorization Act)에 서명함으로써, 〈그림 2-3〉과 같이 2016년부터 매년 국방비를 증액시켜 힘을 통한 평화를 지속 추진하기 위한 예산 토대를 마련하였다. 이번 국방수권법에는 잠재적 경쟁국(중국, 러시아)에 군사적 우위 유지를 위해 병력 증원, 핵 억제력 현대화, 대비태세 강화, 군별 현대화 계획, 동맹국 및 우방국 지원 등의 내용이 총체적으로 망라되어 있다.



〈그림 2-3〉 2009-2018 미국 국방비 지출 변화[5)]

미국의 국방비 중에서 무기체계 획득과 개발에 사용되는 예산을 통해 미국의 무기체계 발전방향에 대해 살펴볼 수 있다. 미국이 2018년 국방예산에서 추진하는 주요 무기체계 획득과 개발 예산 규모는 〈표 2-1〉과 같다.

5) IISS. "THE MILITARY BALANCE 2019", 2019.

〈표 2-1〉 2018 미국 예산 기준 상위 15개 무기체계 순위[6)]

순위	장 비	유 형	군	수 량	예산(US $)
1	Virginia class	핵잠수함	해군	2	7.29bn
2	F-35A Lightning II	전투기	공군	48	4.67bn
3	Columbia class	핵잠수함	해군	-	3.00bn
4	KC-46A Pegasus	공중급유기	공군	15	2.56bn
5	F-35B Lightning II	전투기	해병대	20	2.54bn
6	B-21 Raider	폭격기	공군	-	2.31bn
7	F/A-18E/F Super Hornet	전투기	해군	24	1.99bn
8	P-8A Poseidon	대잠초계기	해군	10	1.98bn
9	Gerald R. Ford	항공모함	해군	-	1.65bn
10	JLTV	합동경량전술차량	육군	3,390	1.32bn
11	F-35C Lightning II	전투기	해군	9	1.28bn
12	CH-53K	대형수송헬기	해병대	8	1.27bn
13	PAC-3MSE	지대공미사일	육군	240	1.13bn
14	UH-60M Black Hawk	중형수송헬기	육군	50	1.12bn
15	John Lewis class	보급지원함	해군	2	1.09bn

위 표에서 나타난 것처럼 해군은 버지니아급 잠수함 획득, 차세대 콜롬비아급 잠수함 개발, F/A-18E/F Super Hornet 전투기, P-8A Poseidon 대잠초계기, 항공모함 등의 전력 도입을 위해 예산을 편성하고 있다. 해병대도 F-35B 전투기, CH-53 대형수송헬기 도입을 추진한다. 공군은 F-35A 전투기, 구형의 KC-135 공중급유기를 퇴역시키고 15대의 신형 다목적 공중급유기 K-46 도입, 장거리 전략 폭격기 개발 등에 예산을 투입하고 있다.

육군은 CTCs(Combat Training Centers) 훈련시설을 향상시키고 무기체계의 현대화에 더욱 박차를 가하고 있다. 합동경전술차(Joint Light Tactical Vehicle)

6) IISS. "THE MILITARY BALANCE 2019", 2019.

구매, 항공전력 강화를 위해 AH-64(Apache) 헬기, UH-60(Black Hawk) 헬기 구매를 추진하고 있다. 〈표 2-2〉를 통해 육군이 추진하고 있는 무기체계 현대화 목록을 자세하게 살펴볼 수 있다.

〈표 2-2〉 2019 미 육군 무기체계 획득 및 성능개량 현황[7)]

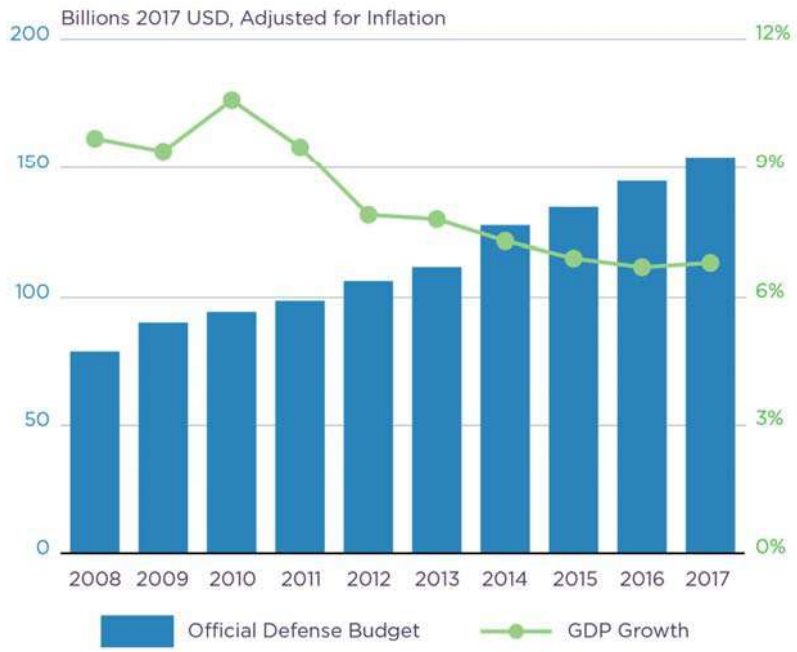
장 비	유 형		수 량	예산(US $)
AH-64E Apache	공격헬기	구매/성능개량	66	1.2bn
UH-60M/HH-60M Black Hawk	수송헬기	구매	55	1.1bn
MH-47G Chinook	수송헬기	성능개량	8	124m
M1A2C Abrams	주력전차	성능개량	135	1.5bn
Mobile Protected Firepower programme	경전차	개발	-	319m
M2A4/M7A4 Bradley	보병전투차량	성능개량	61	205m
M109A7 Paladin	자주포	성능개량	45	569m
Armoured Multi-purpose Vehicles (AMPV)	장갑차	구매	197	679m
Joint Light Tactical Vehicles (JLTV)	경량전술차량	구매	3,390	1.3bn

2.2 중국의 무기체계

시진핑 주석은 2017년 19차 당대회 업무 보고에서 중국의 부흥을 위해 2020년까지 군의 기계화와 정보화 실현, 2035년까지 국방과 군의 현대화 실현, 2050년에는 싸우면 이기는 세계 강군을 건설하는 목표를 제시했다. 중국은 세계 강군을 목표로 〈그림 2-4〉에 나타난 것처럼 2008년부터 2017년까지 국방비를 2배로 증가시켰고, 2010년 이후 지속해서 국방비 지출 세계 2위를 굳혀왔다. 또한 국방비

7) IISS. "THE MILITARY BALANCE 2019", 2019.

의 증가폭은 매년 평균 8%를 나타내고 있으며, 2018년에는 국방예산을 전년 대비 8.1% 증가한 약 1,682억 달러로 책정하여 무기체계 현대화와 군 개혁 추진을 가속화하고 있다.



〈그림 2-4〉 2008-2017 중국 국방예산[8)]

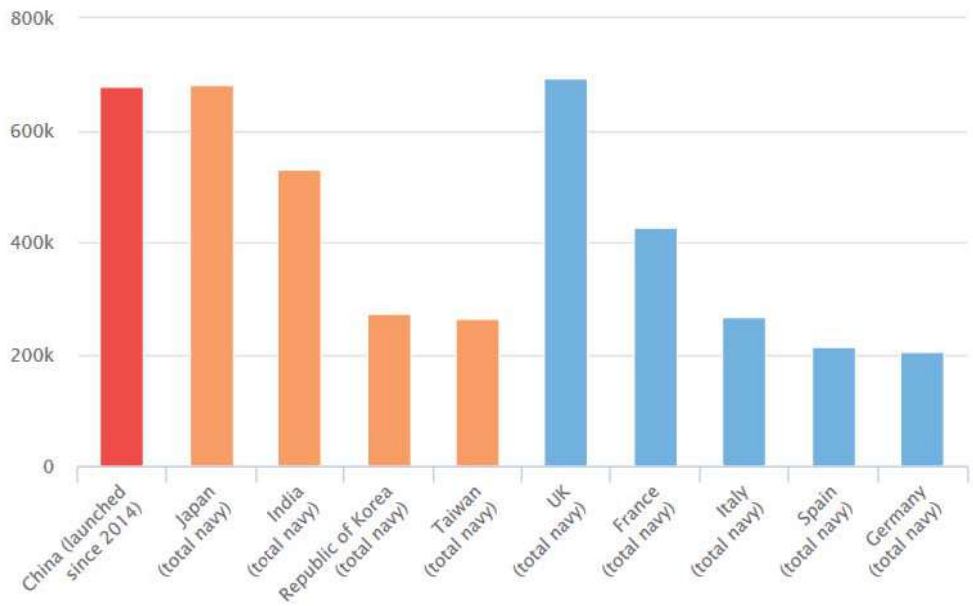
중국 군사전략문서에는 해상/정보영역의 중요성, 공세적 공중작전, 장거리작전, 우주 및 사이버작전 등 해외에서의 중국 국익을 확보할 수 있는 중국군의 능력건설을 강조하고 있다. 중국의 군사 현대화 계획에는 서태평양 내에 배치되는 적대세력에 대해 장거리 공격을 수행할 수 있는 능력 개발이 포함되어 있으며 태평양까지 해당 기능 강화를 목표로 하고 있다. 이러한 능력을 항공, 해양, 우주, 전자전 및 사이버 영역까지 확대시키고자 하고 있다.

육군은 현대화에 많은 투자를 하고 있으며, 병력을 신속하게 장거리 전개할 수 있는 능력에 중점을 두고 있다. 이를 위해 부대의 경량화와 기계화뿐만 아니라, 육군의 장갑, 방공, 항공, 전자전 능력 등을 향상시키는 현대화 노력에 초점을 맞춰

8) DOD. "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2018", 2018.

왔다. 또한, C4I 시스템을 현대화하여 상호운용성을 향상시키고 있다.

해군은 동아시아와 인도, 태평양을 넘어 점차적으로 작전 범위를 확장하여 운용할 수 있도록 발전하고 있다. 특히 해군은 2012년 랴오닝 항공모함 전력화에 이어 자국에서 생산한 항공모함 취역, 최신 구축함 건조 등 원거리 투사능력 향상에 집중하고 있다. 또한 〈그림 2-5〉와 같이 2014년 이후 프랑스, 독일, 인도, 이탈리아, 한국, 스페인, 대만 해군 전체의 톤수보다 더 큰 총 톤수로 해군 함정을 생산했다. 이는 중국의 해군 함정 생산량이 빠르게 가속화 되고 있는 것을 보여준다.



〈그림 2-5〉 국가별 해군 함정 톤수[9]

〈표 2-3〉은 중국 해군이 양적 향상을 위한 함정 생산뿐만 아니라 질적 향상을 위한 함정 현대화에도 집중하고 있는 것을 보여주고 있다.

9) https://www.iiss.org/blogs/military-balance/2018/05/china-naval-shipbuilding

〈표 2-3〉 연도별 중국 해군 함정 수 및 최신함정 비율[10)]

Ship type	2000	2005	2010	2015	2020
대 수					
디젤잠수함	60	51	54	57 - 62	59 - 64
핵잠수함	5	6	6	6 - 8	6 - 9
탄도미사일 잠수함	1	2	3	3 - 5	4 - 5
항공모함	0	0	0	1	1 - 2
구축함	21	21	25	28 - 32	30 - 34
호위함	37	43	49	52 - 56	54 - 58
초계함	0	0	0	20 - 25	24 - 30
상륙함	60	43	55	53 - 55	50 - 55
연안초계함	100	51	85	85	85
최신함정 비율					
디젤잠수함	7	40	50	70	75
핵잠수함	0	33	33	70	100
구축함	20	40	50	70	85
호위함	25	35	45	70	85

공군은 걸프전 및 코소보전 등 현대전의 영향을 받아 국토방공 위주 형태에서 공격과 방어를 겸비한 형태로 전략을 변경하였으며, 이로 인해 국토방공임무 전담 요격전투기는 감소한 반면 공격임무를 수행하는 폭격기와 전폭기는 급증하였다.[11)] 또한 중국 공군은 장거리까지 공군력을 투사할 수 있는 능력을 구축하기 위해, 공중조기경보통제기, 수송기, 공중급유기도 증가시키고 있으며, 신형 전투기 도입을 지속 추진하는 등 공군전력을 빠르게 현대화 시키고 있다. 특히 오랫동안 지속되어 온 미국의 주요 기술적 이점을 점차 약화시키고 있으며, 미 공군과의 격차를 좁히고 있다. 〈그림 2-6〉은 중국 공군 전력의 주요 특징들을 보여주고 있다.

10) Ronald O'Rourke , "China Naval Modernization: Implications for U.S. Navy Capabilities", Congressional Research Service, 2018.
11) 국방부. "2018 국방백서", 2018.

Chinese Manned Aircraft	U.S. Generation	Mission/Role	Status	AESA Radar	Long-Range A/A Missiles	Off-Bore-sight A/A Missiles	Precision-Guided Munitions	Speed
J-7	2nd	Fighter	Operational					Mach 2 class
J-8	3rd	Fighter	Operational		X			Mach 2 class
Su-30	4th	Multirole Fighter	Operational		X	X	X	Mach 2 class
J-10A	4th	Multirole Fighter	Operational				X	Mach 1.8 class
J-11B	4th	Multirole Fighter	Operational		X	X		Mach 2 class
J-10B	4th+	Multirole Fighter	Operational		X	X	X	Mach 1.8 class
J-10C	4th+	Multirole Fighter		X	X	X	X	Mach 1.8 class
J-16	4th+	Multirole Fighter		X	X	X	X	Mach 2 class
Su-35S	4th+	Multirole Fighter	Buying from Russia		X	X	X	Mach 2 class
J-20	5th	Multirole Fighter	Development	X	X	X	X	Mach 2 class
FC-31/J-31	5th	Multirole Fighter	Development	X	X	X	X	Mach 1.8 class
JH-7	N/A	Fighter-Bomber	Operational				X	Mach 1.7 class
H-6	N/A	Bomber	Operational				X	Subsonic
Tactical Bomber	Next Gen	Fighter-Bomber	Development	X	X		X	
Strategic Bomber	Next Gen	Long-Range Bomber	Development	X			X	
KJ-2000	N/A	AEW&C	Operational	X				Subsonic
KJ-200	N/A	AEW&C	Operational	X				Subsonic
KJ-500	N/A	AEW&C	Operational	X				Subsonic

+ Indicates a generation of aircraft has been partially upgraded with next-generation capabilities.

〈그림 2-6〉 중국 공군 항공기 특징[12)]

로켓군은 핵 및 재래식 미사일을 운용하는 군으로, 중국의 억제전략의 핵심요소로서 전략핵 반격 능력과 중·장거리 정밀타격능력 향상에 주력하고 있다. 차세대 중·장거리 탄도미사일인 DF-26은 괌까지 타격범위를 넓혔고 새로운 대륙간탄도미사일(ICBM)인 DF-41은 사정거리 15,000km로 중국 어디에서도 미국 전역을 타격 가능한 수준이다. 또한 최근 극초음속 비행체(HGV: Hypersonic Glide Vehicle)를 탄두에 탑재 가능한 신형 준중거리 탄도미사일(MRBM: Medium-Range Ballistic Missile)인 DF-17의 시험발사를 실시하는 등 미국의 미사일방어(MD)체계에 대응한 신형무기체계 개발을 추진 중인 것으로 알려져 있다.[13)]

12) DEFENSE INTELLIGENCE AGENCY. “CHINA MILITARY POWER", 2019.
13) 국방부. “2018 국방백서”, 2018.

〈그림 2-6〉은 로켓군에서 운용하고 있는 미사일에 대한 정보를 보여준다.

System	Type	Warheads	Propellant	Deployment Mode	Max Range km
CSS-3/DF-4	ICBM	Nuclear	Liquid	ROTL**	5,500+
CSS-4/DF-5	ICBM	Nuclear	Liquid	Silo	12,000-13,000
CSS-7/DF-11	SRBM	Conventional	Solid	Mobile	300-600
CSS-6/DF-15	SRBM	Conventional	Solid	Mobile	600-850+
CSS-11/DF-16	SRBM	Conventional	Solid	Mobile	800-1,000
CSS-5/DF-21	MRBM	Nuclear and Conventional Variants	Solid	Mobile	1,500-1,750+
CSS-5 Mod-5/DF-21D	ASBM	Conventional	Solid	Mobile	1,500+
DF-26	IRBM	Nuclear and Conventional Variants	Solid	Mobile	4,000
CSS-10/DF-31	ICBM	Nuclear	Solid	Mobile	7,200-11,200
CJ-10	GLCM	Conventional	Solid	Mobile	1500+

*This chart does not include systems in development.

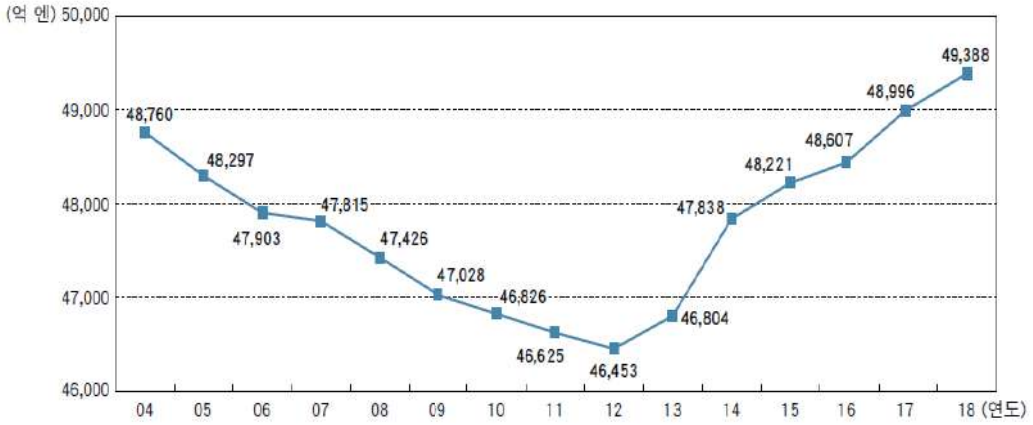
〈그림 2-7〉 중국 로켓군 운용 미사일[14)]

전략지원부대는 2015년 12월 31일에 창설되었으며 정보전, 전자전, 사이버전, 심리전, 우주전 등의 임무를 수행하는 것으로 알려져 있다. 특히, 미국의 위성과 우주자산에 대응하기 위해 우주 기술개발에 노력하고 있으며 레이저, 미사일, 전자전 등을 이용한 위성 공격용 무기 개발에도 집중하고 있다.

14) DEFENSE INTELLIGENCE AGENCY. "CHINA MILITARY POWER", 2019.

2.3 일본의 무기체계

일본은 2018년 12월 18일에 방위계획대강을 공식 발표했다. 방위계획대강은 일본의 국가이익과 안보를 위해 보유해야 하는 방위력의 목표수준을 규정하는 공식 문서로, 일본은 2018년 방위계획대강에서 북한의 핵미사일 위협과 중국의 군사력 증강 등 변화하는 안보환경 속에서 독자적 방위력 증대, 미·일 동맹 강화, 우방국과의 안보협력 강화를 강조하고 있다. 이를 뒷받침하기 위해 〈그림 2-8〉에서 보는 바와 같이 2018년도 국방비도 2017년 대비 0.8% 증가한 약 4조 9,388억 엔으로 증가시켰다.



〈그림 2-8〉 과거 15년간 일본 국방비 변화[15)]

일본은 방위력을 강화하기 위해 향후 5년간 27조 4,700억 엔의 국방비를 투입할 예정으로 이는 역대 최대 규모의 예산 투입이다. 2019년도 국방비는 5조 2,574억 엔으로 역대 최대 액수를 기록하였다. 이렇게 증가된 국방비를 이용해 2019년에 도입을 추진하는 무기체계 중 예산 기준 상위 10가지를 〈표 2-4〉를 통해 확인 가능하며, 지상기반 미사일 방어체계(Aegis Ashore)부터 육/해/공중전력, 미사일까지 다양한 무기체계를 확인할 수 있다.

15) MINISTRY OF DEFENSE. “일본 방위백서 2018”, 2018.

〈표 2-4〉 2019 일본 상위 10개 장비 순위[16)]

순위	장 비	유 형	수 량	예산(US $)
1	Aegis Ashore	지상기반 미사일 방어체계	2	2.13bn
2	30FF	호위함	2	906m
3	F-35A Lightning II	전투기	6	834m
4	SM-3 Block IIA SM-3 Block IB	함대공미사일	-	745m
5	Soryu class	디젤잠수함	1	647m
6	E-2D Hawkeye	조기경보기	2	495m
7	C-2	수송기	2	416m
8	Type-16	기동전투차	22	149m
9	Type-03	중거리 대공미사일	1company	126m
10	Type-12	대함미사일	1set	120m

2018년 일본 방위백서에서도 〈그림 2-9〉와 같이 지상기반 미사일 방어체계를 포함한 6가지 방위력 정비 주요사업을 명시하고 있으며, 이들 사업을 포함한 계획된 모든 방위력 정비를 지속적으로 실시할 것을 언급하고 있다.

〈그림 2-9〉 2018년도 방위력 정비 주요사업[17)]

16) IISS. "THE MILITARY BALANCE 2019", 2019.
17) MINISTRY OF DEFENSE. "일본 방위백서 2018", 2018.

일본은 방위계획대강에서 새로운 영역인 우주, 사이버, 전자전 영역과 전통적인 영역인 육상·해상·공중의 영역을 결합한 위협에 대응하는 것이 중요하다고 판단해서 다차원 통합 방위력 구축을 제시하고 있다. 이는 우주, 사이버, 전자파 영역을 포함한 모든 영역의 능력을 통합하는 대응태세를 갖추는 것을 의미한다. 이를 위해 육·해·공 자위대의 합동성을 더욱 강화하고 있으며, 우주·사이버·전자전 등 새로운 영역에서의 방위역량 증가를 목표로 하고 있다. 사이버전에 대비하기 위해 2014년 3월 육·해·공 자위대의 사이버전 기능을 통합하여 사이버 방위대를 창설하고 자위대 지휘통신시스템부대를 증원하였으며, 장기적으로 두 부대를 통합하여 2020년 '우주·사이버사령부'를 창설할 예정이다. 또한 2022년까지 우주 공간에서 각국 인공위성을 감시하는 시스템을 구축하고, 우주를 감시하는 전문부대를 창설할 예정이다.[18]

또한 일본은 군사과학기술의 발달로 전쟁의 성격이 급변함에 따라 일본의 과학기술력을 활용해 방위장비와 관련된 기술을 보강하는데 더욱 집중할 것이다. 인공지능과 다른 잠재적인 핵심 기술들에 선택과 집중을 통한 집중적인 투자를 할 뿐만 아니라 연구개발 프로세스와 절차를 간소화해 연구개발 일정을 대폭 단축하기 위해 노력할 예정이다.

육상자위대는 높은 기동력 및 경계·감시능력을 확보해 도서지역을 포함한 전 지역의 각종 비상사태에 대응하는 작전부대를 보유하고, 특수작전, 항공수송, 국제평화협력활동 등을 실시할 수 있는 전문기능을 갖춘 기동부대를 보유하려 한다. 또한, 도서지역에 대한 침공을 감시하고자 육상 배치형 이지스 시스템을 도입하고 가능한 해상 및 공중에서 저지하기 위해 지대함미사일과 지대공 미사일 도입에도 집중하고 있다.

해상자위대는 주변해역의 방위와 해상 교통로 및 해양 우세권 확보를 위해 함정 및 항공기를 증강하고, 무인잠수정(UUV: Unmanned Underwater Vehicle) 도입을 통한 수중작전 능력 강화뿐만 아니라 필요시 기존 함정이 단거리이륙·수직착륙(STOVL : Short Take-Off and Vertical Landing) 전투기를 탑재할 수 있는 능력을 갖추도록 할 예정이다.

항공자위대는 2023년까지 최신 전투기(F-35A) 도입 및 조기경보기, 공중급유기, 수송기 등을 전력화할 예정이다. 또한, 일본은 본토에서 떨어진 도서지역 방어를

18) 국방부. "2018 국방백서", 2018.

위해 장거리(Stand-off)미사일 능력 확보, 복합적인 공중 위협을 동시에 처리하기 위해 통합방공 미사일 체계 구축에도 중점을 둘 것이다.

2018년 12월 18일 발표된 중기방위력정비계획(2019-2023)은 5년을 단위로 방위력 정비의 구체적인 계획을 규정한 공식문서로 〈표 2-5〉에 나타난 것처럼 일본 자위대의 향후 무기체계 도입 장비와 수량을 확인할 수 있다.

〈표 2-5〉 2019-2023 중기방위력정비계획 무기체계 획득 수량[19)]

구 분	장 비	수 량
육상자위대	Mobile Combat Vehicles	134
	Armored Vehicles	29
	New Utility Helicopters	34
	Transport Helicopters (CH-47JA)	3
	Surface-to-Ship Guided Missiles	3 companies
	Mid-Range Surface-to-Air Guided Missiles	5 companies
	Land-based Aegis Systems(Aegis Ashore)	2
	Tanks	30
	Howitzers	40
해상자위대	Destroyers	10
	Submarines	5
	Patrol Vessels	4
	Other Ships	4
	Fixed-Wing Patrol Aircraft (P-1)	12
	Patrol Helicopters (SH-60K/K)	13
	Ship-Borne Unmanned Aerial Vehicles	3
	Minesweeping and Transport Helicopters (MCH-101)	1
항공자위대	Airborne Early Warning (Control) Aircraft (E-2D)	9
	Fighters (F-35A)	45
	Fighter Upgrade (F-15)	20
	Aerial Refueling/Transport Aircraft (KC-46A)	4
	Transport Aircraft (C-2)	5
	PAC-3 MSE	4 group
	Unmanned Aerial Vehicles (Global Hawk)	1

19) MINISTRY OF DEFENSE. “Medium Term Defense Program(FY2019 - FY2023)”, 2018.

2.4 러시아의 무기체계

2018년 3월 1일, 푸틴 대통령은 대통령연설에서 핵무기를 포함해 러시아의 군사장비를 현대화하는 방안을 거론하며 혁신적인 전략무기를 지속적으로 개발할 것이라고 언급했다. 러시아는 단거리 핵무기를 포함하는 경우, 핵보유국 중 가장 많은 핵무기를 보유하고 있으며, 2020년까지 약 280억 달러를 투자하여 현재 운용하고 있는 핵무기를 개량할 계획이다. 또한, 대륙 간 탄도 미사일과 단거리 탄도 미사일, 그리고 해상, 지상, 공중에서 핵을 투사할 수 있는 다양한 무기를 보유하고 있다.

또한, 푸틴 대통령은 2018년에 러시아의 새로운 장비 개발 및 무기체계 현대화에 3,660억 달러를 투자하는 2018-2027년 무기조달계획(SAP: State Armament Program)을 승인하였다. 이는 2027년까지 러시아의 무기체계 조달을 위한 우선순위의 기초를 형성하게 된다. 또한, 2011-2020년 무기조달계획에 따라 이루어진 발전을 바탕으로 러시아 군대를 더욱 강화하고 현대화할 것으로 예상된다. 〈표 2-6〉에서 알 수 있듯이 2013년에서 2017년까지 러시아 군의 무기체계 중 현대 장비의 점유율은 매년 증가하고 있으며, 새로운 무기조달계획에 의거하여 현대화는 지속 추진될 것으로 예상된다.

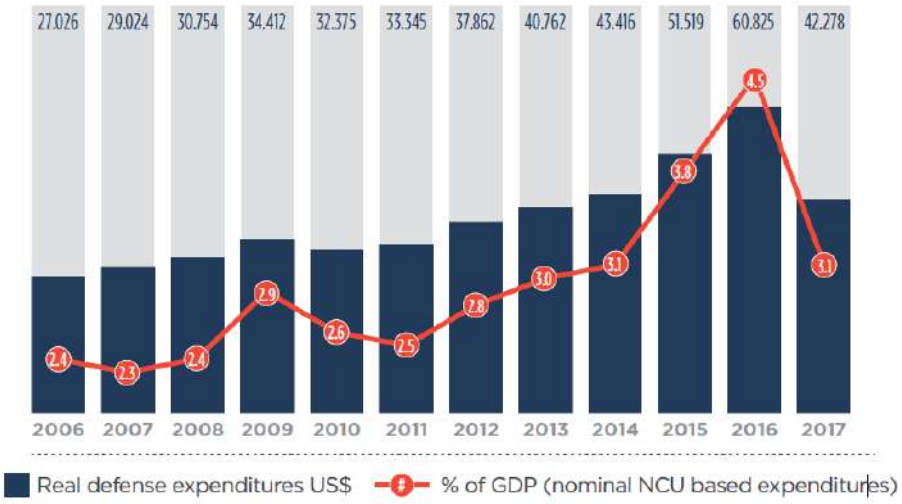
〈표 2-6〉 러시아의 현대화된 무기체계 비율(2013-17: 실제, 2020: 목표)[20]

무기체계	2013	2015	2017	2020
잠수함	47	51	59	71
수상함	41	44	54	71
고정익항공기	23	37	55	71
헬기	39	63	76	85
미사일시스템	27	64	100	100
포병	51	53	59	79
장갑차량	20	37	56	82
다목적차량	40	48	56	72

20) Royal Institute of International Affairs. “Russia’s New State Armament Programme Implications for the Russian Armed Forces and Military Capabilities to 2027”, 2018.

2018-2027년 무기조달계획의 초점은 극초음속 미사일을 포함해 육상/해상/공중 전투를 위한 초정밀 무기, 무인공격기, C4ISR 및 전자전 장비 조달에 있다. 뿐만 아니라 무인 차량과 로봇 기술의 개발에도 초점을 맞출 것으로 보이며, 2010년대부터 무기체계 조달은 대량 생산 논리에서 벗어나 양보다 질, 고품질, 성능개량, 현대화에 초점을 맞추고 있다.

이를 뒷받침하기 위한 러시아의 국방비 변화는 〈그림 2-10〉과 같다. 러시아 국방비는 지난 10년 동안 대체로 증가했고 2016년에 최고액을 달성했으며 특히, 무기조달계획이 2011년부터 2016년까지의 국방비 증액을 주도했다. 하지만 러시아 언론과 재무부 발표에 따르면 2017년부터 2019년까지 러시아 국방비는 명목상으로 동결되거나 감소할 것이라고 보고 있는데, 이는 러시아 정부의 세입 전망이 좋지 않고, GDP 성장률이 낮아지는 등 경제적으로 성장 한계에 직면했기 때문이다.



〈그림 2-10〉 2006-2017년 러시아 국방비[21]

육군은 최신 주력전차인 T-14 아르마타와 T-15 장갑차 132대를 2022년까지 도입 예정이다. 하지만, T-14 아르마타 전차의 비싼 단가로 인해 대량 조달에는 많은 예산이 소모되어 대규모 조달은 아닐 것으로 예상된다. 대신 T-72, T-80, T-90 전차 현대화에 초점을 두고 탱크 수량을 맞출 예정이다. 이에 따라 2017년

21) DEFENSE INTELLIGENCE AGENCY. "RUSSIA MILITARY POWER", 2017.

부터 육군은 향상된 엔진과 무장 시스템을 갖춘 개량형 T-72B 전차들을 인수하고 있고, 성능이 향상된 T-90M 전차는 2019년 시험평가 후 러시아 육군에 도입 예정이다. 또한, 기존의 낡은 보병전투장갑차(IFV, Infantry Fighting Vehicle)를 대체하기 위해 성능이 향상된 장갑차 BMP-2M을 도입하고 있다.

해군은 핵 3축의 필수 무기인 전략핵잠수함 10척을 운용하고 있으며 지속적으로 핵 억지력을 강화하기 위해 2020년까지 보레이급 핵 잠수함을 5척까지 보유할 계획이다. 또한, 킬로급 디젤잠수함을 개량하는 등 잠수함 건조와 현대화에 우선순위를 두고 있다. 수상함의 경우 신형 대형 선박 개발을 추진하는 대신 호위함, 초계함 등의 조달, 현대화, 수명 연장에 우선순위를 두고 있다. 해군은 〈표 2-7〉과 같이 2012년부터 2017년까지 수상함 12척, 잠수함 10척을 건조하였다. 이 함정들은 최신의 대함, 대지 장거리 미사일 시스템을 갖추었고, 이를 통해 원거리에서 지상 목표물도 타격할 수 있는 역량을 갖추게 되어 지상 작전을 효율적으로 실시할 수 있는 기반을 조성하였다.

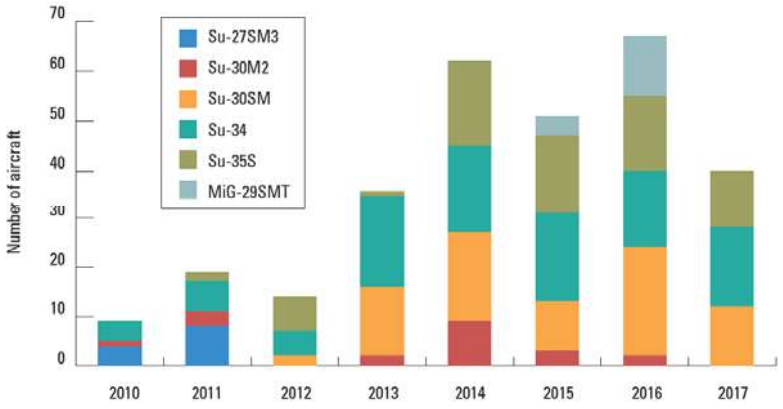
〈표 2-7〉 주요 수상전투함 및 잠수함 취역현황(2012-2017년)[22]

종류	급	취역년도	종류	급	취역년도
FFGM	Gepard	2012.11.28	FSGM	Buyan-M	2014.12.19
FSM	Buyan	2012.12.04	SSK	Varshavyanka	2014.12.26
SSBN	Borey	2012.12.29	SSK	Varshavyanka	2015.06.25
FFGHM	Steregushchiy	2013.05.16	SSK	Varshavyanka	2015.11.05
SSBN	Borey	2013.12.23	FSGM	Buyan-M	2015.12.12
SSGN	Yasen	2014.06.17	FSGM	Buyan-M	2015.12.12
FFGHM	Steregushchiy	2014.07.18	FFGHM	Grigorovich	2016.05.27
FSGM	Buyan-M	2014.07.27	FFGHM	Grigorovich	2016.06.07
FSGM	Buyan-M	2014.07.27	SSK	Varshavyanka	2016.10.26
SSK	Varshavyanka	2014.08.21	SSK	Varshavyanka	2016.11.24
SSBN	Borey	2014.12.10	FFGHM	Steregushchiy	2017.07.20

항공우주군의 2010년에서 2017년까지 전투기 도입 현황은 〈그림 2-11〉과 같으며, 기존의 4세대 전투기의 현대화와 5세대 스텔스 전투기의 도입에 노력을 집중하고 있다. 연간 12-18대의 비율로 Su-30SM 전투기를 현대화하여, 2027년까지 최소 186대로 늘릴 예정이고 200여대의 Su-35S 전투기도 도입 예정이다. 기존

22) IISS. "THE MILITARY BALANCE 2018", 2018.

Mig전투기를 대체하기 위해 항전장비, 레이더, 엔진 및 무장 등의 성능을 높인 차세대 다목적 전투기 Mig-35를 개발해 2018년부터 양산 및 전력화 중에 있다. 5세대 스텔스 전투기 Su-57은 2019년부터 12대가 도입될 예정이며, 핵 억지력 향상을 위해 기존 Tu-160 전략 핵 폭격기를 개량하여 신형 Tu-160M2 약 50대를 전력화 할 예정이다.



〈그림 2-11〉 2010-2017 러시아 전투기 도입 수[23]

방공체계 현대화를 위해서는 '러시아판 사드'로 불리는 지대공 미사일시스템 S-400을 지속 생산하여 전력화하고 있으며 2020년에는 차세대 지대공 미사일시스템 S-500과 중거리 지대공 미사일시스템 S-350을 도입할 예정이다.

전략미사일군의 핵과 미사일은 러시아에게 군사 강대국으로서의 위상 확립, 억지력 확보, 재래식 전력의 열세 보완, 외교 · 안보정책의 도구라는 측면에서 전력증강의 높은 우선순위를 유지하고 있다.[24] 이에 따라 다른 군과 비교했을 때 핵전력은 예산 삭감에 비교적 면책을 유지하고 있으며, 노후화된 핵무기 수를 줄이고 새로운 미사일의 신속한 획득과 개발에 집중한 결과 2018년 전략미사일군 무기체계의 79%가 현대화된 전력으로 분류되고 있다. 또한, 2018년 핵전력 야르스(SS-27 MOD2) 대륙간탄도미사일 3개 연대를 전력화하였으며, 차세대 대륙간탄도미사일 RS-28 사르마트를 개발하고 있다. 미국의 미사일방어망을 뚫을 수 있는 무기로 평가받는 야르스는 지하격납고식 발사대(Silo)나 이동식차량발사대(TEL)를 이용하

23) IISS. "THE MILITARY BALANCE 2019", 2019.
24) 한국전략문제연구소. "주변국 군사력 격차에 따른 적정 국방비 확보 방안", 2014.

며, 철로를 따라 이동하는 ICBM 탑재 핵 열차 개발은 예산의 문제로 연기될 것으로 보인다. 러시아에서 현재 운용하고 있는 ICBM은 〈표 2-8〉과 같다.

〈표 2-8〉 러시아 ICBM 체계[25)]

System	Number of Stages	Warheads	Propellant	Deployment Mode	Max Range km
SS-18 MOD 5	2 + PBV	10	LIQUID	SILO	10,000+
SS-19 MOD 3	2 +PBV	6	LIQUID	SILO	9,000+
SS-25	3 + PBV	1	SOLID	ROAD-MOBILE	11,000
SS-27 MOD 1	3 + PBV	1	SOLID	SILO and ROAD-MOBILE	11,000
SS-27 MOD 2	3 + PBV	Multiple	SOLID	SILO and ROAD-MOBILE	11,000

2.5 북한의 무기체계

북한의 군사전략은 크게 핵무기를 통한 전략적 억지력과 포탄, 다연장로켓을 포함한 광범위한 재래식 무기의 전진배치를 통한 재래식 억지력에 의존하고 있다. 북한 지상군의 약 70%와 해·공군의 약 50%가 비무장지대(DMZ)에서 60마일 이내에 배치되어 있으며, 재래식 군대의 질적 열세를 극복하기 위해 사이버전, 특수전부대, 탄도 미사일, 핵·WMD, 잠수함 등 비대칭 전력을 증강시켜왔다. 특히 미국에 도달할 수 있는 탄도미사일 개발과 잠수함발사 탄도미사일(SLBM) 개발에 초점을 맞추고 있다. 또한, 6,800여 명의 사이버전 인력을 운용하고 있으며, 전문인력 육성 및 최신기술에 대한 연구·개발을 지속하는 등 사이버전력의 증강을 위한 노력을 계속하고 있는 것으로 보인다.[26)] 이와 반대로 재래식 전력은 노후화된 장비에 의존하고 있으며 일부 재래식 무기 성능개량 외에 현대화를 위한 노력의 징후는 보이지 않는 등 전형적인 선택과 집중에 치중하는 모습이다.

25) DEFENSE INTELLIGENCE AGENCY. “RUSSIA MILITAR POWER”, 2017.
26) 국방부. “2018 국방백서”, 2018.

북한은 만성적인 경제난과 국제사회의 제제에도 불구하고 국방비가 차지하는 비율이 매우 높다. 미 국무부의 '2018년 세계 군비지출 및 무기이전 보고서[27]'에 따르면 북한은 2006년부터 2016년까지 11년 동안 연 평균 국내총생산(GDP)의 23.3%를 국방비로 지출했고, 이는 국내총생산(GDP) 대비 국방비 지출 분야에서 세계 1위였다. 또한, 군인의 수는 약 116만명으로 전체 인구 중 군인이 차지하는 비율이 4.8%로 세계 1위를 기록했다.

북한 육군은 약 110만명으로 중국, 미국, 인도 다음으로 세계에서 네 번째로 큰 병력을 보유하고 있으며 이는 러시아보다 더 크다. 더욱이 평양에서 원산으로 이어지는 이남지역에 병력의 70%가 전진 배치돼 있어 기습 공격에 작전상 큰 이점을 가지고 있다. 육군은 〈그림 2-12〉에 나타난바와 같이 주력 전차 및 경전차 4,300여 대, 장갑차 2,500여 대, 76mm 이상 자주포와 견인포 8,600여 문, 다연장로켓 발사체계(MRL : Multiple Rocket Launch systems) 5,500여 문 등으로 무장하고 있다. DMZ를 따라 전방에 배치되어 있는 240mm MRL과 170mm 자주포는 서울을 포함한 남한의 북부 지역을 위협하고 있다. 최근 개발이 완료되어 일부 배치된 300mm MRL(KN-09)은 사거리 최대 200km로 북한 포병의 위협 범위를 중부지역까지 확장시키고 있다.

〈그림 2-12〉 북한 육군 주요 보유장비[28]

1990년대 후반부터 북한은 제한된 자원을 비대칭 전력 개발에 집중했고, 그 결과 육군의 많은 무기체계가 노후화 되었다. 하지만 육군은 지난 20년 동안 경제적 어려움에도 불구하고, 노후화된 전력을 선별적으로 현대화하고 있다. T-62와 같은 구형 주력 전차를 천마, 선군호 등으로 교체하는 등 현대화를 지속하고 있으며, 장

27) Department of State. "World Military Expenditures and Arms Transfers, 2018 edition", 2018.
28) 국방부. "2018 국방백서", 2018.

거리 자주포, 240mm, 300mm 다연장로켓, 개선된 화력통제 시스템을 지속적으로 개발·생산 및 배치하고 있다.

해군은 수상 전력이 소형함정 위주로 편성되어 연안 방어에 적합하며 원거리 작전능력은 부족하다. 북한의 영해를 보호하고 남한에 특수전 부대를 침투시키는데 필요한 제한된 능력을 갖고 있다. 하지만 해군은 전력의 약 60%를 평양-원산선 이남에 전지 배치하여 경고 없이 기습 공격을 할 수 있다. 수상 전력은 초계함, 유도탄정, 소형경비정 등 대부분 소형 함정으로 구성되어 있으며, 대부분 수동식 재래식 무기를 탑재하고 있어 정밀공격 및 야간작전 능력에 한계가 있다. 제한적 현대화를 위해 지휘통제체계 개선, 초계함의 구형 무기체계를 새로운 개틀링 기관총으로 교체, 신형 중대형 함정과 고속특수선박(VSV : Very Slender Vessel)을 배치하는 등 수상전력 강화에 힘쓰고 있다.

공기부양정, 고속상륙정 등 250여 척으로 구성된 상륙전력은 대부분 소형함정이지만 특수전 부대의 후방 침투, 중요 상륙해안 확보 등의 임무를 지원할 것으로 예상된다. 수중전력은 로미오급, 상어급 잠수함과 잠수정 등 70여 척으로 구성되어 세계에서 가장 많은 척수를 보유하고 있다. 현대식 잠수함은 아니더라도 평시나 전시에 해상교통로 교란, 수상함 공격, 특수전 부대 침투지원 등의 임무를 충분히 수행할 것으로 판단된다. 최근에는 잠수함발사 탄도미사일(SLBM) 1발을 탑재할 수 있는 고래급 잠수함(2000톤급)을 건조하였을 뿐만 아니라 3000톤급 신형 잠수함도 건조 중인 것으로 판단된다. 더욱 커진 선체를 활용해 3000톤급 잠수함에는 잠수함발사 탄도미사일 3-4발을 탑재 가능할 것으로 추정된다.

〈그림 2-13〉 북한 해군 주요 보유함정[29)]

공군은 총 1,640여대의 항공기를 보유하고 있으며, 전투기는 810여 대 중 약

29) "2018 국방백서", 국방부, 2018.

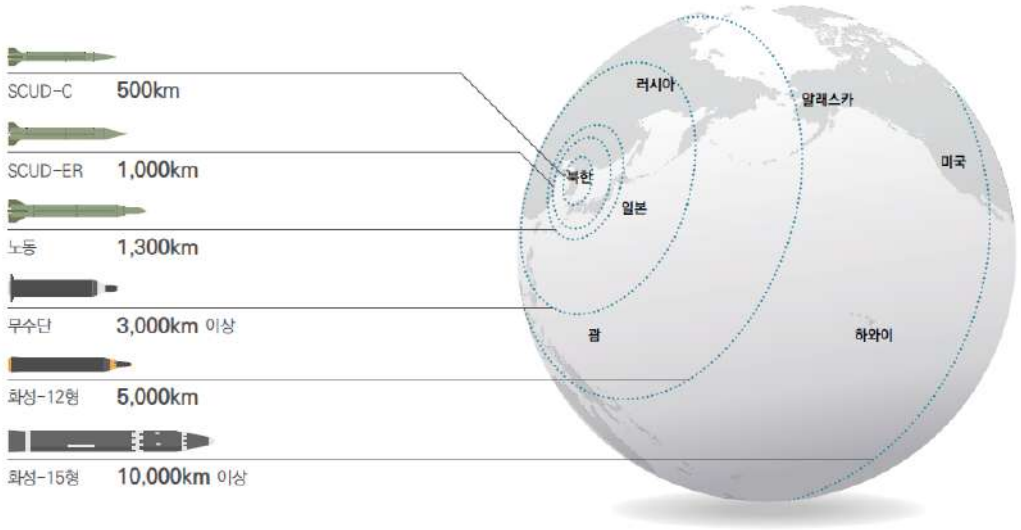
40%를 평양-원산선 이남에 전진 배치해 놓고 있다. 또한 AN-2기와 헬기를 이용한 대규모 특수전 부대의 침투능력을 갖추고 있으며, 정찰 및 공격용 무인기와 경항공기도 생산·배치하고 있다. 재고량 면에서 북한의 공군력은 한반도 내 한국 공군력이나 미 공군력보다 크지만 질적으로는 열세다. 1980년대 후반부터 국제사회의 제재로 현대식 신형 항공기를 구입할 수 없었다. 북한의 가장 최신 전투기는 MiG-29, MiG-23, Su-25 지상공격기 등으로 모두 1980년대 도입한 전투기다. 나머지 항공기는 구형이며, 성능이 떨어지는 MiG-15, MiG-17/J-5, MiG-19/J-6s, MiG-21/J-7 전투기, IL-28/H-5 경폭격기 등이 있다. 이로 인해 공군은 지상 기반 방공체계를 강화하는데 힘쓰고 있다. 공군은 구형의 SA-2, SA-3, SA-5 지대공 미사일을 이용하여 다중의 대공 방어망을 형성하고 있으며, 2010년 열병식에서 KN-06 미사일이 공개되면서 방공체계 현대화를 위한 노력에도 힘쓰고 있는 것을 알 수 있다. 뿐만 아니라 GPS 교란기를 포함한 다양한 전자교란 장비를 개발하여 함께 운용하고 있는 것으로 추정된다. 또한 다수의 중·소형 무인 항공기를 획득하거나 생산해 운용하고 있다.

〈그림 2-14〉 북한 공군 주요 항공기[30]

북한은 비대칭 능력의 핵심 요소인 핵, 탄도미사일을 지속적으로 개발하고 있다. 1980년대 핵물질 확보를 통해 2006년 이후 지속적인 핵실험 감행하였다. 또한, 1970년대 후반부터 다양한 탄도 미사일 개발 프로그램을 추진해 왔으며, 오늘날 미국 본토까지 위협할 수 있는 화성-14형과 15형을 시험 발사하는 등 핵 무장 ICBM, 잠수함 발사 탄도미사일(SLBM) 개발에 전념하고 있다. 북한이 현재 개발 또는 보유 중인 탄도미사일 종류와 사거리는 〈그림 2-15〉, 〈그림 2-16〉과 같다.

30) 국방부. "2018 국방백서", 2018.

〈그림 2-15〉 북한이 개발 또는 보유 중인 탄도미사일 종류[31]



〈그림 2-16〉 북한 미사일 도달 가능 거리[32]

31) 국방부. "2018 국방백서", 2018.
32) 국방부. "2018 국방백서", 2018.

3. 무기체계별 기술발전 동향

「방위사업법 시행령」제2조에 따라 무기체계 대분류는 지휘통제·통신무기체계, 감시·정찰무기체계, 기동무기체계, 함정무기체계, 항공무기체계, 화력무기체계, 방호무기체계, 그 밖의 무기체계로 분류할 수 있다. 아래에서는 8가지 무기체계별 기술발전 동향에 대해 살펴보고자 한다. 본장의 내용은 2014~2028 국방과학기술진흥정책서, 2018년도 국방과학기술진흥실행계획(안), 2018~2032 핵심기술기획서 일반본, 2016 국방과학기술조사서 등을 기초로 작성 및 재정리하였다.

3.1 지휘통제·통신 무기체계

지휘통제·통신 무기체계는 "네트워크를 구성하여 실시간으로 정확한 전장상황 파악 및 이해를 가능하게 하며 적시적절한 의사결정과 전장관리를 지원함으로써 합참, 작전사령부, 군단, 사단 등 지휘관의 작전지휘를 지원"[33]하는 체계로서, 전장인식을 지능화하고, 다차원 전장정보를 가시화하며, 지휘결심의 지능화, 전략급부터 전투급까지 종적 상호호환성 및 각 군간 횡적 상호호환성을 확보를 보장하는 방향으로 발전 중이다.

전장인식의 지능화를 위해서는 다양한 출처에서 수집되는 정보로부터 실시간 표적정보를 생성·추적·관리하는 실시간 전장정보 융합 기술과 전장상황을 인지·분석·예측·평가하는 지능형 전장상황 인식 및 평가 기술로 발전하고 있다. 전장정보 가시화를 위해 전장상황을 신속하게 공유할 수 있도록 음성, 동작, 생체 인식 기술들을 지휘통제체계에 접목하고 있다. 지휘결심 지능화를 위해서는 파악된 전장상황으로부터 적의 중심을 식별하고, 최대의 작전효과를 얻을 수 있는 최적의 방책을 식별·평가할 수 있는 지식 기반 방책수립 기술로 발전하고 있다. 또한, 선정된 방책에 대한 효과를 비교·분석할 수 있는 자율적응형 교전을 수행하는 수준으로 발전할 것이다.

이 분야 최고선진국인 미국은 집중적 투자를 통해 신속한 정보공유체계를 구축하고 복잡한 전장상황 속에서도 의사결정 지원을 가능하게 하는 체계를 정립하고

33) 국방기술품질원. "18~32 핵심기술기획서 일반본", 2018.

있으며, 감시정찰, 지휘통제, 정밀타격체계로 이어지는 사이클의 합동성 및 상호 운용성을 극대화하기 위해 C4ISR-PGM(C4I Surveillance Reconnaissance - Precision Guided Munitions)과 무기체계간 전술정보 공유를 위한 연결성을 강조하는 네트워크 중심 작전환경(NCOE: Network Centric Operational Environment)을 선도해 나가고 있다.

전술정보통신체계는 이동 중에도 자유롭게 통신할 수 있는 Full-OTM (On-The-Move) 통신기술과 유한한 전파 자원을 효율적으로 쓰고 주파수 자원 활용을 극대화한 CR(Cognitive Radio) 기술 등으로 발전이 예상된다. 군통신위성은 중·장기적으로 위성용 온보드 프로세서(On Board Processor)를 탑재 및 FDMA의 주파수 비효율성을 개선하고, TDMA자원할당 효율을 반영한 MF-TDMA(Multi Frequency-Time Division Multiple Access)기술과 항재밍/대용량 웨이브폼 기술을 적용할 것이며, IP 기반 스위칭 및 라우팅 기능을 탑재할 것으로 예상된다. 데이터링크는 영상 전송을 위한 고속 대용량화가 될 것이며 전술통신체계와의 연동을 위한 상호 운용성 요구가 강화될 것이다.

미국은 〈그림 3-1〉과 같이 WIN-T(Warfighter Information Network - Tactical)체계를 계발하는 등 이동 간 지휘통제와 초고속·대용량 통신을 보장하고 전투원 간의 통신을 제공할 수 있는 전술정보통신체계를 개발하였다. 또한 무전기 통신에 CR/DSA(Cognitive Radio/Dynamic Spectrum Access) 분야의 인공지능, 정보융합 등의 기술을 적용하여 새로운 개념의 기술을 개발하고 있다. 위성통신체계도 지속적으로 발전시키며, 차세대 미사일 감지센서 위성, 차세대 GPS 위성 및 군전용 기상관측위성을 전력화하여 운용중이며, 우주 분야의 최고선진국으로서의 위상을 가지고 있다.

WIN-T 체계[34)]

WIN-T Inc. 2 장착 스트라이커 전투여단[35)]

〈그림 3-1〉 WIN-T 체계

사이버무기체계는 적대 세력이 사이버 공간을 통하여 행하는 공격들에 대응하기 위해 사이버 방어 작전과 더불어 능동적 대응활동이 필요하며, 이를 위해 사이버 작전을 고도화하기 위한 정보융합 기술 확보와 사이버작전 가시화가 필요하다. 특히, 적 사이버 공격무기에 대응하기 위해 지능형 침입탐지 기술, 사이버 위험 분석 기술, 인공지능을 활용한 각종 사이버 방어기술의 필요성이 강조되고 있다. 또한, 평시 적군의 정보 교란 및 정보 절취 행위 발생 시 이를 추적하고 종적을 확보하기 위한 사이버 게놈 기술과 적의 침투 경로를 역추적하고 명령서버를 점유함으로써 추가적인 피해 방지를 위한 명령 제어서버 역추적 및 점거기술의 중요성도 강조되고 있다. 중·장기적으로는 유선망 연결이 불가능한 지역의 적 사이버 공간에서도 사이버 작전 전개가 가능한 사이버전자전 기술 확보가 필요하며, 컴퓨팅 능력 향상으로 다양한 의사난수를 이용하여 암호해독이 가능해짐에 따라 양자정보 기반 통신 등의 기술개발이 이루어질 전망이다.

이 분야 최고선진국인 미국은 2010년 Army Cyber Command를 설립한 후 사이버전 개념을 선도하는 동시에 관련 기술도 지속적으로 준비하여 세계 최고 수준의 핵심기술을 보유하고 있다. 특히, 군 예산이 감축되는 추세에도 불구하고 미국의 사이버안보 관련기관들에 투입되는 예산은 증가되는 추세이다. 중국은 미국의

34) DOD. "FY 2019 Program Acquisition Costs by Weapon System", 2018.
35) 국방기술품질원. "국방과학기술정보 제68호", 2018.

기술 주도권에서 벗어나기 위해 20년 전부터 운영체제를 비롯한 네트워크 장비의 국산화에 집중투자 하고 있으며, 중국의 사이버공격 실행 능력은 최고 수준으로 판단되고 있다. 사이버 공격과 방어에 대한 인력을 체계적으로 양성할 뿐만 아니라 국가적으로 양자컴퓨터 연구를 지원하고 있다. 러시아는 중국에 비해 사이버전 예산은 부족하나 여전히 강력한 국방 연구기관들을 보유하고 있으며, 이를 바탕으로 한 최고 수준의 사이버전 공격기술과 민간 차원에서 최고의 해킹 기술력을 가지고 있다.

지휘통제·통신 무기체계 기술발전 방향은 〈그림 3-2〉과 같다.

〈그림 3-2〉 지휘통제·통신 무기체계 기술발전 방향[36]

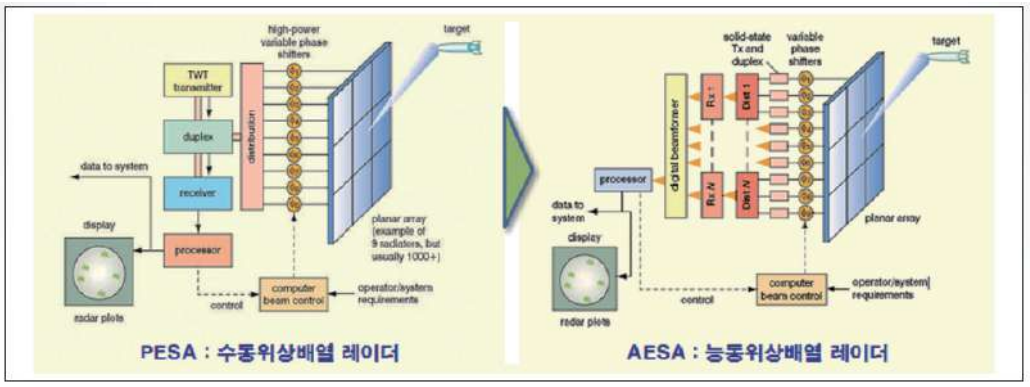
3.2 감시·정찰 무기체계

감시·정찰 무기체계는 "전자광학, 적외선, 레이더, SAR, 음향, 자기 등 각종 센서를 복합 운용하여 지상·해상·공중·수중·우주의 전략/전술 표적 및 전장 환경에 대한 영상, 신호(음향, 통신, 전자, 계기) 정보를 수집, 획득, 제공하는 무기체

36) 국방기술품질원. "18~32 핵심기술기획서 일반본", 2018.

계"[37]이다.

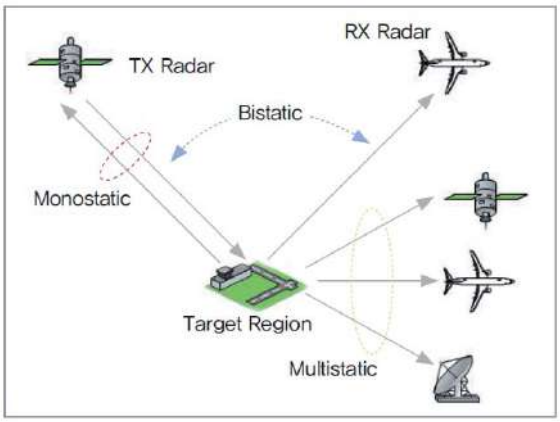
레이더체계는 단일 기능만을 수행하는 모습에서 여러 기능을 동시에 수행하는 다기능/다목적 레이더로 발전하고 있으며, 〈그림 3-3〉와 같이 튜브형 송신기를 사용하는 기계식 혹은 수동위상배열 레이더에서 반도체 송신기를 사용하는 능동위상배열 레이더로 발전하고 있다. 더불어 진보된 컴퓨팅 및 반도체기술에 의해 항공기에 사용 가능한 모듈화/소형화/경량화 및 고출력/고효율화 되어가고 있으며, 항공기 및 유도탄에 대한 정밀탐지/추적능력을 향상시키기 위하여 다중센서 융합, 자동표적인식 등 첨단 3차원 기법을 적용한 고성능 탐지기술이 개발되고 있다.



〈그림 3-3〉 수동위상배열과 능동위상배열 구조 비교[38]

SAR(Synthetic Aperture Radar, 합성개구면 레이더)는 표적에 대한 영상정보를 획득하는 레이더로 날씨에 무관하게 운용이 가능하다. 파장이 짧을수록 고해상도 영상을 구현하기가 상대적으로 쉽기 때문에 고해상도 SAR 영상의 수요에 맞추어 X밴드의 SAR가 운용이 되고 있으며, 30cm급 미만의 해상도를 확보하기 위해서 파장이 더 짧은 Ka밴드의 SAR도 운용되는 추세이다. 현재 운용중인 SAR 위성은 모노스태틱 레이더를 기반으로 하고 있는데 모노스태틱 레이더는 송신과 수신이 단일 레이더로 구성되어 표적에서 반사된 일부분의 신호만을 획득할 수 있는 단점이 있기 때문에 이를 극복하기 위해 송신용 레이더와 수신용 레이더를 분리시켜서 하나의 송신용 레이더와 여러 개의 수신용 레이더를 이용하는 바이스태틱 혹

37) 국방기술품질원. "18~32 핵심기술기획서 일반본", 2018.
38) 김진우, "레이더 발전추세 및 개발동향", 국방과 기술, 421:77-93, 2014.



〈그림 3-4〉 모노/바이/멀티스태틱 개념도

은 멀티스태틱 레이더 기술이 〈그림 3-4〉과 같이 개발되고 있다. 미국은 F-22, F-35 등의 최신 전투기 및 F-15, F-16 등의 기존 전투기에 대한 AESA 성능개량 사업을 통해 대부분 SAR 모드를 탑재하고 있으며, 최신 전투기종에 K밴드에서 동작하는 SAR/GMTI (Ground Moving Target Indicator)/MMTI(Maritime Moving Target Indicator)등 다양한 기능을 탑재 시도 중이다.

전자광학체계는 센서의 초소형 및 초경량화, 고분해능으로 점차 복합화 되고 지능화되고 있다. 전자광학체계의 해상도는 m급에서 cm급까지 고해상도로 발전되고 있고, 디지털 영상전송체계를 이용하여 고분해능 확보 및 장거리 관측을 위해 직경이 m급으로 대구경화 되고 있다. 미래에는 적응광학을 활용한 적외선 우주감시체계와 각 파장별 영상을 획득하여 표적을 식별하는 초분광 영상기술을 활용한 감시·정찰체계로 발전할 것으로 보인다.

〈그림 3-5〉 신형 전자전 전술차량

전자전은 작전지역이 점차 확장됨에 따라 적 통신망을 감청하고, 방향탐지, 위치탐지 등 신호정보 수집능력과 적 지휘통제 통신망 무력화를 위한 전자공격 능력 구비를 위한 무인항공기 탑재형 전자전 체계가 개발되고 있다. 이에 따라 항공기 탑재를 위한 소형화 기술이 발전하고 있다. 미국은 세계 최초의 디지털 조기경보기 AN/ALR-96A를 개발하였고 육군에서는 전투 여단급에 전자기 스펙트럼 내 위협 탐지 능력을 제공하기 위해 〈그림 3-5〉과 같이 신형 전자전 전술차량 (EWTV:Electronic Warfare Tactical Vehicle) 플랫폼을 시험하고 있다.

수중감시 체계는 더욱 저소음화 되어가는 적 수중위협에 대해 장거리·광역 표적 탐지가 가능한 저주파 능·수동 복합 음향탐지체계, 다기능 및 다중상태 탐지체계로 발전하고 있다. 또한, 다양한 수중위협에 대한 표적탐지 및 식별이 가능하도록 여러 종류의 센서를 복합적으로 운용하는 네트워크 기반 통합 감시체계가 개발되고 있다. 미국은 다중(Multi-static) 플랫폼 네트워크 기반의 수중감시체계 사업에 막대한 예산을 투자하여 개발 중에 있다.

감시·정찰 무기체계의 기술 발전 방향은 〈그림 3-6〉와 같다.

〈그림 3-6〉 감시·정찰 무기체계 기술발전 방향[39]

3.3 기동 무기체계

기동 무기체계는 "지상전 전투수행 및 전술적 운용을 위한 기동전투체계, 전장환경에서 전투원의 효과적인 임무수행을 위한 개인전투체계, 유인전투체계를 보완하기 위한 지상무인체계로 구성되며, 효과적인 지상전투를 수행하기 위한 주력 전력"[40]이다.

기동전투체계 중 전차는 기동 공세전력의 주력 장비이자 지상전투부대의 핵심이

39) 국방기술품질원. "18~32 핵심기술기획서 일반본", 2018.
40) 국방기술품질원. "18~32 핵심기술기획서 일반본", 2018.

며, 새로운 작전개념을 부합하고 효율성을 높이기 위해 플랫폼 융복합화 및 소형화, 스텔스화, 피탄 회피와 대응파괴 능력 강화, 하이브리드 추진 기술, 복합장갑과 반응장갑 기술 등이 필요하다. 고위력을 가지는 정밀 원거리 타격을 위해서 화력 증대 기술 및 자동화/지능화 추세에 따른 플랫폼 경량화와 무인 발사, 탄두내장형 탄약 발사시스템과 대구경 다기능 무장에 대한 기술개발이 이루어지고 있다. 신규생산이나 개발보다는 성능개량 위주의 전력 확보방안이 당분간 지속될 것으로 예상되어 체계의 중량과 공간소요를 감소하기 위한 부품 소형 경량화 및 부품 통합단순화 기술이 발전하고 있다.

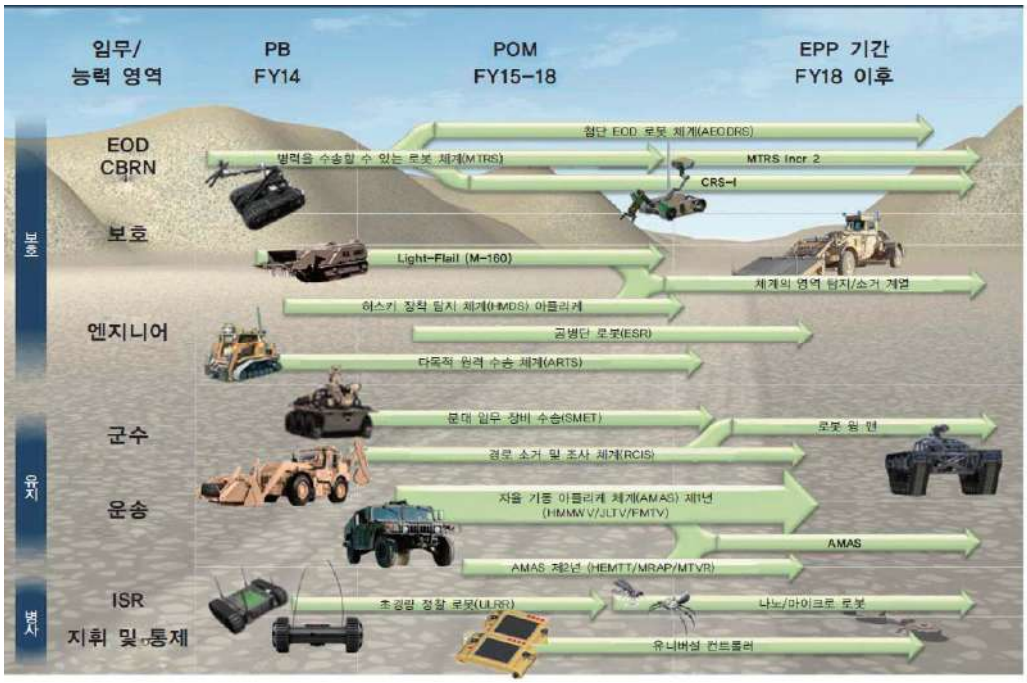
미국은 기존 M1A1/M1A2 전차를 지속적으로 성능개량하여 2040~2050년까지 운용하기 위해 신형 디젤엔진, 경량화 장갑, 자동장전장치, 생존성 개선 등이 반영된 M1A3 전차를 2020년까지 연구개발완료를 목표로 추진하고 있다. 또한, 노후된 병력수송장갑차 M113을 교체할 AMPV(Armored Multi-Purpose Vehicle) 사업을 추진하고 있다. 2017년을 기준으로 미국, 러시아, 중국의 주력전차 획득동향은 〈표 3-1〉과 같다.

〈표 3-1〉 미국, 러시아, 중국 주력전차 획득 동향[41]

미국	러시아	중국
- SEPv4 사업 개시를 위한 결심지점을 2020년으로 계획 - SEPv4 시제품 제작에 착수 - 2021년에 시제 7대 최초시험, 2022년에 양산 전환 예정	- 새로운 버전의 T-90, T-80, T-72 MBT 전력화 - T-14 아르마타의 무인로봇 버전 2018년까지 개발 계획	- 중국 기갑전력의 토대인 96식 주전차 주력화 - 96B식 엔진(1200hp 출력)·가벼운 새시·개선된 환기장치·현대화된 배기체계·현대식 전차
		
주력전차 M1A2 SEPv3	T-14 아르마타	주력전차 96B식

41) 국방기술품질원. "국방과학기술정보 제69호", 2018.

지상무인체계(UGS)는 전천후 환경에서 야지 및 험지 자율주행을 위한 지형 및 장애물의 여러 정보를 제공하는 근거리 센서 기술과 다중대역영상센서, 초분광센서를 활용한 자동탐지 및 식별처리 기술 등이 발전하고 있다. 또한, 단일체계의 상황처리 및 임무계획 수준에서 중장기적으로 그룹형태인 다수체계의 다중 운용 기술을 확보하는 추세로 발전할 것이며, 생존성 확보를 위한 특수형태 반응장갑 및 능동방호 시스템 적용기술, 피탐 확률 감소를 위한 다양한 전자파에 대한 흡수/반사/형상 설계 등에 관련된 기술 등을 개발하고, 지상무인체계의 운용시간을 연장시키기 위해 연료전지 기술과 고출력 하이브리드 기술 등을 확보하는 추세이다. 미국은 〈그림 3-7〉에서 보는 것처럼 2013년 무인체계 통합 로드맵(2013~2038)을 발표하여 적극적인 개발의지를 표명하였다. 또한, 이라크 등 전장에서의 운용경험을 바탕으로 상용화 및 성능입증을 수행하고 있으며 감시정찰, 폭발물 처리 등에 활용되는 UGV(Unmanned Ground Vehicle)기술은 최고의 수준을 자랑한다. 최근에는 생체모방 등의 분야에서 전력화에 근접한 수준을 달성해 생체모방로봇 LS3가 최종 점검 단계에 있다.



〈그림 3-7〉 미국의 임무/능력 영역별 UGS[42]

〈그림 3-8〉 전술통신헤드셋[43]

개인전투체계는 현용 장비를 개량하거나 신규 장비를 개발한 후 임무 및 기능에 따른 모듈통합형 체계 구축 후에 정보통신기술, 생명공학기술, 초정밀원자설계 기술의 융·복합을 통해 전체 시스템을 통합한 일체형 전투체계로 발전하고 있다. 착용자의 기동성과 생존성 향상을 위하여 인체 보행패턴 분석에 기반한 근력증강 메커니즘 최적화 설계와 신소재를 적용한 화생방 보호장비 등이 개발 중에 있다. 〈그림 3-8〉과 같이 미국은 미래전을 대비하여 Future Soldier 2030 Initiative 사업을 추진하고 있으며, 그 내용으로는 근력 강화장비, 주야간 전방향 입체 영상 전시, 전신 유연 소재 방탄 전투복, 생체 정보 모니터링 및 치료 등의 연구가 있다.

기동 무기체계의 기술 발전 방향은 〈그림 3-9〉와 같다.

〈그림 3-9〉 기동 무기체계 기술발전 방향[44]

42) 국방기술품질원. "18~32 핵심기술기획서 일반본", 2018.
43) 국방기술품질원. "국방과학기술정보 제67호", 2017.
44) 국방기술품질원. "18~32 핵심기술기획서 일반본", 2018.

3.4 함정 무기체계

함정 무기체계는 “군사적 목적에 사용되는 모든 선박을 지칭하며, 그 자체가 무기체계이면서 여러 종류의 센서와 무장이 탑재되는 대형·복합 무기체계(System of Systems)로 크게 수상함과 잠수함, 해양무인체계로 구분”[45]한다.

수상함은 통합마스트(IMM: Integrated Mast Module)를 적용하고, 종합적인 효과도가 체계적으로 분석될 수 있는 기술을 개발하는 방향으로 발전하고 있다. 수상함의 전투성능을 높이기 위해서 사격통제와 관련된 기술, 광역 다중표적 처리 기술 등이 연구되고 있으며, 네트워크 기반의 해상 협동교전이 가능한 체계의 구축이 궁극적인 방향이다. 추진체계는 소음을 줄여 탐지를 피하기 위한 제어기술과 전기추진체계 기술을 개발하여 전전기 함정(All Electric Ship)을 설계하는 방향으로 발전하고 있다. 또한, 함정 손상에 대비한 자동화된 손상통제 시스템을 개발하여 전투지속능력을 증대시키는 추세이다. 이 분야의 최고선진국인 미국은 전 함정을 설계·건조하면서도 차세대 전장에 대비하기 위한 전전기 함정 개념을 추진하고 있다. 통합전기추진체계 탑재를 통한 저소음화 유도 및 통합마스트 탑재를 통한 함 형상 스텔스 최대화 추진과 수상함 임무별 모듈화를 적용한 LCS(Littoral Combat Ship, 연안전투함)를 〈그림 3-10〉과 같이 운용중이다. 또한, 〈그림 3-11〉과 같이 DDG-1000 개발의 추진을 통해 스텔스를 통한 함정 생존성 극대화, 레일건 등의 신 무장 적용을 통한 전투성능 향상을 꾀하고 있다.

〈그림 3-10〉 연안전투함(LCS)[46]

〈그림 3-11〉 DDG-1000[47]

45) 국방기술품질원. “18~32 핵심기술기획서 일반본”, 2018.
46) 홍현수, “2012~2016 세계 함정 획득동향”, 국방기술품질원, 2016.

잠수함은 스텔스 성능을 결정하는 음향신호와 전자기 신호인 수중신호 감소를 위하여 수동제어와 함께 능동제어 기술을 잠수함에 적용하고 있다. 음향신호를 감소시키기 위하여 고성능 소음감소 기구, 저소음 기계류, 저소음 추진기, 능동·수동 음향 코팅재 등에 대한 연구가 이루어지 있다. 또한, 수중체류능력 극대화·고속화를 위하여 공기불요추진시스템(AIP)과 대용량 영구자석 추진 전동기 등을 적용하고, 고밀도 전력저장이 가능한 리튬전지 적용을 시도하고 있다. 미국은 건조 방법 효율화 및 모듈화 설계를 통해 생산 비용과 기간을 줄여가고 있으며, 무인잠수정을 발진 또는 회수할 수 있는 범용 발진 및 회수 모듈을 탑재하려 하고 있다. 또한, 버지니아급 추가 건조 사업을 통해 모듈화 설계기술, 스텔스 성능 증대를 꾸준히 추진시키고 있다.

무인 수상정에는 복합임무 수행이 가능한 플랫폼 설계 기술이 개발되고 있고 있다. 그리고 자율적으로 운항을 관제하고 경로를 생성하며, 임무에 기반한 운항제어가 가능하도록 하는 추세이며, 스스로 장애물을 탐지하고 고장발생시 자가 진단하여 대응하는 자율운용 개념을 적용하고 있다. 미국은 다목적용 (대수상함전, 대기뢰전, 대잠전 등) 무인수상정을 개발 중이며, 목적에 따라 크기에 변화를 주어 무인수상정을 개발 중이다.

무인 잠수정은 기뢰탐지 및 식별, 수중 정찰, 잠수함 탐지/공격 등을 목적으로 타 체계들과 유사하게 자율성이 강조된 자율운용 관련 기술이 개발되고 있다. 미국은 세계 최초로 버지니아급 잠수함에 수중 드론과 무인잠수정을 배치해 전략 요충지에서 다양한 수중 작전을 수행할 계획을 가지고 있다. 또한, 임무장비 교체만으로 대기뢰전, 감시정찰전, 대잠전 등을 선택적으로 수행할 수 있는 MRUUV(Mission Reconfigurable Unmanned Underwater Vehicle)를 개발 중에 있다. 미국의 해양무인체계 임무영역별 개요는 〈그림 3-12〉와 같다.

47) 홍현수, "2012~2016 세계 함정 획득동향", 국방기술품질원, 2016.

〈그림 3-12〉 미국의 임무 영역별 무인해양체계[48)]

함정 무기체계의 기술 발전 방향은 〈그림 3-13〉과 같다.

〈그림 3-13〉 함정 무기체계 기술발전 방향[49)]

48) 국방기술품질원. "18~32 핵심기술기획서 일반본", 2018.

3.5 항공 무기체계

항공 무기체계는 "평시 전략적 억제능력을 확보하고 유사시 공중우세 및 적 종심에 대한 정밀타격을 수행하는 무기체계로 고도의 전투능력 확보를 위해 탑재장비의 고성능화 및 소형화, 고고도 운용에 따른 실시간 정보전송, 높은 기동성 및 은밀성"[50]이 요구되고 있다.

고정익 항공기는 크게 RCS 및 IR 저감을 통한 스텔스 성능을 증대시키기 위해 형상 및 재료와 관련된 기술, 내부무장기술을 설계에 적용하는 방식이 사용되고 있으며, 통합화된 탑재장비 시스템 구현을 위해 IMA(Integrated Modular Avionics), HMD(Head Mounted Display)기술 등을 연구하고 있다. 고성능/경량화 소재를 개발하기 위해 티타늄 소재의 연구 및 가공기술에 대한 연구가 활발히 이루어지고 있으며, 스마트 기체구조를 통한 생존력 및 효율성 향상을 꾀하고 있다. 더불어 기동성 향상과 관련된 기술들과 전투수행 능력 향상을 위한 자동화된 표적 탐지, 추적, 처리 기술과 지능형 전자전 상황인식을 위한 연구가 진행되고 있는 추세이다. 현재 미국은 스텔스, 내부무장 기술, 추력편향을 적용한 5세대 전투기인 F-22〈그림 3-14〉를 운용 중이다. 나아가서 6세대 전투기 개발을 추진 중으로 광대역 스텔스 기술, 지향성 에너지무기, 자율화를 통한 유·무인 통합기술 등을 적용할 예정이다. 또한, P-8 Poseidon 해상초계기, E-8 Joint stars 조기경보기, EA-18 Growler 전자전기, KC-46 공중급유기 등을 개발하여 최신의 항공기를 보유하기 위해 노력하고 있다.

〈그림 3-14〉 F-22 전투기[51]

회전익 항공기는 고속 기동을 가능하게 하고 장거리 운용 능력을 확보하기 위해 고정익체계 특성을 혼합한 기술들이 적용되고 있다. 회전익은 로터라는 회전체를 갖고 있어

49) 국방기술품질원. “18~32 핵심기술기획서 일반본”, 2018.
50) 국방기술품질원. “18~32 핵심기술기획서 일반본”, 2018.
51) 국방기술품질원. “국방과학기술정보 제66호”, 2017.

근본적으로 높은 진동과 소음을 동반하므로 소음/진동 저감을 위한 능동 로터제어 기술이 발전하고 있다. 더불어 FBW(Fly-By-Wire) 기술과 같이 위험하고 고난이도의 제어기술을 요할 때 필요한 기술들이 개발되는 추세이다. 자율화와 더불어 생존성을 향상시키기 위한 능동형 생존체계 기술이 발전하고 있다.

〈그림 3-15〉 S-97 헬기[52)]

미국은 기존의 AH-64, AH-1 모델을 개량하여 AH-64D, AH-1Z로 개량 하는 등 최신 기술 확보에 주력하는 모습이다. 또한 무장과의 연동성을 증대시키기 위해 공격헬기에 AN/APG Longbow 밀리미터파 화력통제레이더를 장착하고, 편대공격을 위한 데이터 링크 탑재를 추진하였다. 그리고 동체의 대부분을 복합재료로 적용하고, ABC(Advancing Blade Concept) 로터를 적용한 복합헬기 S-97을 〈그림 3-15〉와 같이 개발 중이며, VTDP(Vectored Thrust Ducted Propeller) 방식을 적용한 헬기 개발도 추진하는 등 헬기에 대한 추자가 활발하다. 이 외에도 유무인 편대 비행기술, 진동제어기술, 지향성 적외선 대응장비 경량화, 진동 저감장치 개발 등을 지속적으로 추진하고 있다.

무인기체계는 필요시 장기간 체공하면서 실시간 고해상도 영상정보를 획득 및 전파할 수 있는 방향으로 나아가고 있다. 특히, 유인기와 협동하여 고위험지역에서 유인기의 생존성을 높이면서도 다양한 임무의 수행 성공률을 높이기 위한 연구가 진행 중이다. 또한 투척식 초소형 무인기 및 곤충을 모방한 신개념 플랫폼으로도 발전하고 있고, 저피탐성과 고속 기동 비행성능을 가지는 무인복합형헬기가 연구되고 있다.

미국은 정찰용 무인기 및 관련 분야에 있어 세계 최고의 기술력을 가지고 있다. 글로벌호크는 EO/IR, SAR/MTI 센서를 장착하여 주·야간은 물론 전천후 정찰임무가 가능하다. 또한, X-47B 무인 전투기 개발로 차세대 스텔스기술과 자율임무 기술을 확보하였다. 보잉에 의해 개발된 Phantom Ray는 스텔스 기능을 가진 UCAV(Unmanned Combat Aerial Vehicle)이며, 전투기급의 무장탑재를 목표로

52) 국방기술품질원. "국방과학기술정보 제73호", 2018.

하고 있다. MQ-8C Fire Scout은 다양한 감시·정찰 임무장비인 EO/IR, SAR, SIGINT(SIGnal INTelligence)등을 탑재하여 다목적 임무를 수행할 수 있다. 미 해군에서는 EO/IR, 해상레이더, ESM 센서를 탑재한 〈그림 3-16〉과 MQ-4C Triton을 개발하여 운용중에 있으며, 공군에서는 〈그림 3-17〉의 무인 공격기 MQ-9 리퍼를 운용하고 있다.

〈그림 3-16〉 MQ-4C Triton[53]

〈그림 3-17〉 MQ-9 리퍼[54]

미국의 무인항공체계 발전 방향은 〈그림 3-18〉과 같다.

53) Department of the Navy. "Naval Aviation Vision : 2016-2025", 2016
54) 국방기술품질원. "국방과학기술정보 제66호", 2017.

〈그림 3-18〉 미국의 무인항공체계 발전 방향[55]

우주 무기체계는 다수의 위성을 하나의 집단군으로 효율적으로 운용하고, 필요시 지상의 특정 위치 재확인 시간을 단축하는 등 위성의 운용 효율을 높이는 기술 개발이 진행되고 있다. 위성용 CMG(Control Moment Gyro)는 적은 용량의 반작용 휠을 이용하여 대용량의 토크를 생성할 수 있는 장치로서 최근 고기동성을 위한 소형위성에 탑재하여 효율성을 증가시킬 수 있는 방향으로 발전하고 있다. 또한, 단일 위성에 복잡한 다종의 센서를 장착하기 보다는 목적에 맞게 기능을 단순화 및 소형화하는 추세이며, 임무장비로부터 고해상도 영상을 획득할 수 있는 기술들이 개발 및 적용되는 방향으로 나아가고 있다.

미국은 〈표 3-2〉와 같이 DSP, SBIRS, STSS 등 감시정찰 위성을 개발하여 탄도미사일 추적은 물론 SAR영상을 통한 주요지역 상시감시가 가능하다. 더불어 협대역, 광대역, 보안위성을 모두 확보하여 운용중이며, GPS 위성을 통해 전 세계의 위치정보 전송이 가능하다. 발사체 분야에서도 벤처기업의 SpaceX, Virgin Galactic, Orbital Sciences Corporation 등 참여가 늘어나고 있으며, 1단 로켓

55) 국방기술품질원. "2013~2038 미국의 무인체계 통합 로드맵", 2014.

의 재사용이 가능한 발사체를 개발 중으로 성공 시 비용에 대한 절감을 달성할 것으로 보인다.

〈표 3-2〉 우주기반 센서[56]

구분	DSP	SBIRS	STSS
형상			
타입	정지궤도(GEO) 위성	정지궤도(GEO) 및 고타원궤도(HEO) 위성	저궤도(LEO) 위성
역할	전략 및 전술미사일 발사 탐지	• 미사일 탐지/경보 • 기술정보 수집 • 전장 인식	• 탄도미사일의 비행 전 단계 추적 및 식별 • 요격미사일에 항적정보제공
상태	• 3기 임무수행, 2기 백업 • SBIRS로 전환	• 2기의 GEO와 3기의 HEO 운용 중 • 추가로 GEO 3기, HEO 2기 발사가 계획됨	• 2기 운용 중
제조사	노드롭그루먼	록히드마틴	노드롭그루먼, 레이시온

항공 무기체계의 기술 발전 방향은 〈그림 3-19〉와 같다

〈그림 3-19〉 항공 무기체계 기술발전 방향[57]

56) 국방기술품질원. "18~32 핵심기술기획서 일반본", 2018.

3.6 화력 무기체계

화력 무기체계는 “적 종심 및 핵심표적을 타격하여 적의 전투수행 능력을 파괴 또는 마비시키고, 동시다발적 정밀타격에 의한 효과를 집중 시킬 수 있도록 네트워크에 의한 동시·통합 운용 개념이 적용되는 체계”[58]이다.

소화기는 기존의 핵심 성능인 사거리와 정확도 등을 향상시키면서도 필요시 주/야간 정밀 조준사격이 가능하도록 개발되고 있으며, 개인전투체계의 일부로서 정보공유가 이루어지도록 하고 있다. 최근 지상 무인화 기술 발전추세에 따라 RCWS(Remote Controlled Weapon Station)와 같은 원격이나 무인으로 운영이 가능한 무인 포탑 형태로 발전이 가속화되고 있다. 탄약은 정밀타격 능력을 향상시키기 위해 첨단 센서를 탑재하고, 사거리 향상을 위해 항력감소, 탄도수정, 복합추진 장치들을 탑재하여 개발되는 추세이다. 또한 관통성능을 향상시키고 폭발효과를 증대시키는 등 탄 자체의 성능을 개선하면서도 신관의 발전을 통한 지능화 및 소형화를 추진하고 있다. 이 분야 최고선진국인 미국은 정밀유도폭탄을 박격포탄 및 로켓탄약에도 적용하고 Excalibur를 전력화하는 등 정밀화를 높이는 방향으로 추진하고 있다. 더불어 재래식 탄약의 신관을 탄도수정신관인 PGK (Precision Guidance Kit)를 적용하여 〈그림 3-20〉과 같이 유도를 통한 정밀타격을 추진하고 있다.

〈그림 3-20〉 정밀유도키트(PGK)[59]

지상유도무기의 전술유도탄은 다양한 탄두를 고속으로 원하는 표적에 운송할 수 있는 무기체계로서 탄두의 다양화, 추진기관의 고성능화, 재

57) 국방기술품질원. “18~32 핵심기술기획서 일반본”, 2018.
58) 국방기술품질원. “18~32 핵심기술기획서 일반본”, 2018.
59) 국방기술품질원. “국방과학기술정보 제 63호”, 2017.

밍을 무력화할 수 있는 위성항법장치 등을 구현하는 방향으로 발전하고 있다. 대전차 유도무기의 경우 정밀한 유도조종이 가능하도록 정밀탐색기를 활용하고 탄두를 고성능화 시키고 있으며, 개인전투체계는 휴대성을 높이기 위한 초소형의 무장용 유도탄을 활용할 수 있으며 반대로 이를 탐지할 수 있는 스마트 탐지추적 기술이 개발되고 있는 추세이다.

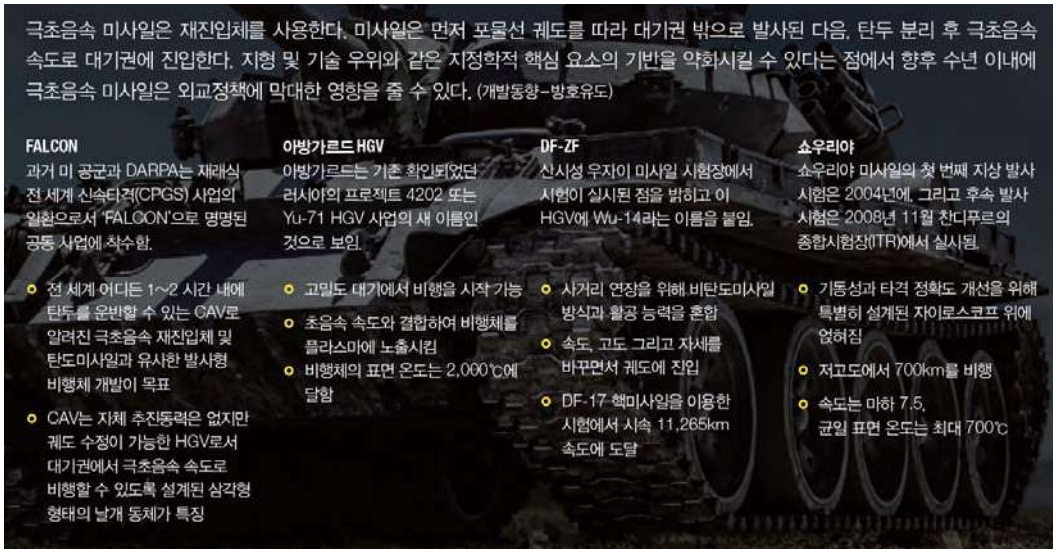
해상유도무기는 초음속 및 극초음속 유도무기를 위한 램제트 및 스크램제트 엔진을 개발하고 있으며, 양방향 데이터링크를 사용하여 실시간으로 비행중인 유도무기를 통제할 수 있도록 발전하고 있다. 지상표적에 대해서도 파괴력을 증대시키기 위해 침투탄두기술, 정밀항법기술, 다양한 탐지추적기술 등 관련 기술들을 개발하고 있다. 수중에서도 다른 공간의 표적을 유연하게 타격할 수 있도록 추진장치, 발사장치 및 표적 식별 추적장치 등을 개발하고 있다.

공중 유도무기는 발사체의 위협 범위 밖에서도 신속히 공격할 수 있도록 스텔스화, 고속 및 고기동, 장사정화를 달성할 수 있는 방향으로 발전하고 있다. 위협이 되는 발사체의 고속화 및 장거리화가 가속화됨에 따라 이를 정밀하게 탐색하고 고성능 추진장치 및 유도조종장치 등을 활용하여 방어할 수 있는 기술들의 개발이 이루어지고 있다.

미국은 지대지 유도무기인 MinutemanⅢ, 잠대지 유도무기인 Trident D5 등의 대륙간 탄도미사일을 정밀하게 타격할 수 있는 능력 보유를 위한 기술개발 및 성능개량을 지속적으로 추진하고 있다. 또한, AIM-9X, AIM 120과 같은 공대공 유도무기를 성능개량하고, 공대지/함대함(지)/대전차 유도무기 성능개량을 위한 기술개발도 추진 중이다. 나아가 FALCON, X-51A 〈그림 3-21〉과 같은 극초음속 유도무기 개발에도 집중하고 있으며, 극초음속 미사일 개발 동향은 〈그림 3-22〉와 같다.

〈그림 3-21〉 X-51A 극초음속 미사일[60]

60) 국방기술품질원. "국방과학기술정보 제 70호", 2018.



〈그림 3-22〉 극초음속 미사일 개발 동향[61]

수중유도무기는 잠수함 및 수상함의 주 공격수단인 어뢰에 대한 대항체계의 성능이 크게 향상됨에 따라 탐색 및 추적기술을 회피하기 위한 관련 기술들, 예를 들어 스텔스 기능, 장거리 및 고속 항주기술들이 발전하고 있다. 고속/장거리 주행을 위해서는 전동기추진방식 추진기술에 대한 연구가 이루어지고 있다. 또한, 초공동현상을 이용한 고속로켓어뢰 추진기술이 개발되고 있으며, 초고속어뢰의 종말 유도제어기술에 대한 필요성도 증대되고 있다. 기뢰는 자율성을 추가한 능동추적 파괴가 가능한 수중유도무기 수준으로 발전되고 있으며, 원격통제가 가능하면서도 정밀 복합감응이 가능한 기뢰로 발전되고 있다.

미국은 광대역 음향탐지기술 확보를 위해 각종 어뢰에 대한 음향탐지 성능을 지속적으로 개량하고 있다. 나아가 고속로켓 어뢰 SUPERCAP을 개발 중에 있으며, 초공동현상을 이용한 수중무기체계발을 활발히 진행해나가고 있다. 더불어, 어뢰 투발 수단의 다양화를 위해 원거리 비행이 가능한 날개킷트를 부착한 형태의 항공기 투하용 어뢰를 개발하고 있다.

레이저무기는 미국이 세계 최고 수준의 기술력을 가지고 있는 것으로 알려져 있으며 이와 더불어 집중적인 투자와 개발을 선도하고 있다. 〈표 3-3〉과 같이 다양한 플랫폼에 레이저기술을 적용하여 무기체계로서 운용가능성을 시험하고 있고 구

61) 국방기술품질원. "국방과학기술정보 제 74호", 2019.

체적인 전력화계획도 수립하고 있다. 물론 다른 군사선진국들도 레이저무기의 경제적, 군수적 강점을 이용하기 위한 많은 개발 노력을 기울이고 있으나 이를 군사적인 효용을 갖춘 무기체계로 개발하는 것에는 아직 제약 사항이 많으며, 안정적인 무기체계로서 사용까지는 시간이 걸릴 것으로 판단된다.

〈표 3-3〉 미국의 레이저 무기[62]

구분	HEL MD (High Energy Laser Mobile Demonstrator)	LaWS (Laser Weapon System)	HELLADS (High Energy Laser Air Defense System)
형상			
담당	미 육군	미 해군	DARPA
역할	로켓, 야포, 순항미사일 및 UAV 방어용	소형 공격보트, 헬리콥터, UAV 방어	전술항공기에 탑재하여 부스트 단계 탄도탄 파괴
현황	• '13년 박격포 및 UAV 등 150개 이상의 목표물 요격에 성공 • 악천우에서도 운용가능	• Phalanx 시스템에 의해 유도 • '14년 미 해군 폰스함에 탑재되어 시험평가 • 미래 대 탄도탄 방어함에 탑재 예정	• 150kW급 액체 레이저 • 현존 유사체계의 크기와 무게 대비 1/10수준 • '15년부터 야전시험 중

〈그림 3-23〉 레일건 탑재 개념도

전자력 추진무기(레일건)에 대한 연구는 고전력의 전원을 사용하고 단시간에 전력의 집중적인 소모를 기반으로 하기에 해군 전전기 전투함 운용계획과 병행하여 〈그림 3-23〉처럼 해군 무기체계에 대한 응용으로 연구 중이다. 미 해군은 1단계 목표로 해당하는 사거리 및 포구에너지, 분당 발사율이 가능한 시스템을 BAE사와

62) 국방기술품질원. "국방과학기술정보 제 62호", 2017.

GA-EMS사가 공동으로 개발하였고, 미 해군은 2012년에 GA-EMS사로부터 레일건을 인수하고 시제품으로 실시한 최초 사격시험을 성공한 것으로 알려져 있다.

고출력 전자파 무기는 비핵 EMP탄으로 대표되며, 미국은 90년대 중반에 수GW급의 고주파발생장치를 개발하였고 관련 교리를 발전시키고 있으며, 러시아도 90년대 초부터 자장압축발전기를 개발하고 이 분야를 선도해 나가고 있다. 영국과 독일도 미사일에 EMP탄두를 탑재할 수 있는 연구를 진행중이며, 일본은 2003년 고주파발생기를 개발한 것으로 알려져 있다.

유도 무기체계의 기술 발전 방향은 〈그림 3-24〉과 같다.

〈그림 3-24〉 유도 무기체계 기술발전 방향[63]

3.7 방호 무기체계

방호 무기체계는 "적 항공기, 유도탄, 화생방 무기로부터 인원, 무기, 장비, 주요시설 등을 보호하고 전투력을 보존하여 작전유지 능력을 극대화하는 체계"[64]이다.

공중위협은 항공기 위주에서 점차 확대되어 무인기 및 각종 유도탄으로 다양화되고 있으며, 스텔스화, 고속/소형화를 통해 요격이 어려워지는 상황에서 다양한 첨단기술을 적용하여 이를 극복하는 방향으로 발전하고 있다. 이에 따라 무인기,

63) 국방기술품질원. "18~32 핵심기술기획서 일반본", 2018.
64) 국방기술품질원. "18~32 핵심기술기획서 일반본", 2018.

탄도 등을 요격할 수 있는 기술 개발이 이루어지고 있으며, 다표적에 대한 동시 대응 능력을 향상시킬 수 있는 방향으로 진화하고 있다. 방공레이더는 탐지영역을 확장하고 다수의 표적을 동시에 탐지 및 추적할 수 있도록 발전되고 있으며, 동시 교전 능력도 함께 개발되고 있다.

미국은 전개된 미군의 인원 및 장비를 공격하는 유도탄을 요격하기 위하여 〈그림 3-25〉처럼 탄도미사일 방어시스템을 개발하여 운용하고 있으며, 발사단계, 중간비행단계, 종말단계의 3단계를 통하여 요격하는 시스템으로 이루어져있다.

〈그림 3-25〉 탄도미사일 방어시스템 구조[65]

방공유도무기는 미국과 러시아가 가장 높은 기술력을 보유하고 있으며, 양국의 방공무기는 〈표 3-4〉와 같다.

65) 국방기술품질원. "국방과학기술정보 제 62호",2017.

〈표 3-4〉 미국, 러시아 방공 유도무기[66]

미 국	러 시 아
패트리어트(Patriot)	부크
- 1970년대 실전 배치 - 개량형 버전인 PAC(Patriot Advanced Capability)-3를 전력화 - 1개 포대는 레이더 1기(PAC-3버전AN/MPQ-65 레이다)와 8개의 발사대로 이루어짐	- 항공기와 순항 미사일을 요격할 수 있는 러시아의 대표적인 유도탄 - 최신 버전은 buk-M3로 1개 포대는 발사대(TELER) 겸 레이더(9A317M) 2대 발사대(A9A316M) 1대로 구성 - 사거리 70km/요격고도 35km
사드(THAAD)	S-400
- 탄도탄이 100km 이상의 고고도 체공 중 요격하는 유도탄 - 사드 1개 포대 구성은 사격통제 레이더(AN/TPY-2)와 교전통제소, 6기의 발사대로 구성 - 최대사거리 200km/최대 요격고도 150km - 사격통제 레이더에는 최대 1200km의 물체 탐지	- 1개 포대에는 탐색레이더 1개, 추적레이더 1개와 8개의 발사대 등으로 구성 - 유도탄에 사용되는 고체추진 방식을 사용 - 탄두는 근접신관을 이용한 파편/폭풍 효과를 이용하는 폭발식 탄두 사용 - 사거리 400km/요격고도 30km
SM-3	S-500
- 함대공유도탄 SM-3 block 2A는 미국과 일본이 공동 개발한 무기체계 - 최대사거리/최대요격고도 2500km/1500km - 고체연료를 사용하는 추진체와 직격요격체로 구성	- 기존의 S-400을 개량한 최첨단 유도탄 - 1개 포대는 발사대 4대, 작전통제소 차량 1대, 전투통제 레이더 1대, 목표획득 레이더 1대, 다중모드 교전통제레이더 1대로 대략 8~10개의 차량으로 구성 - 사거리 600km/마하 20의 표적 요격 가능

화생방 무기체계는 시·공간적 광범위성과 막대한 피해를 불러오는 특성으로 인해 신속한 조기경보와 광대역감시체계 구축이 필요하며 원거리 탐지가 가능하도록 발

66) 국방기술품질원. “국방과학기술정보 제 73호”, 2018.
67) Office of the Assistant Secretary of the Army. “WEAPON SYSTEMS HANDBOOK 2018”, 2018.

〈그림 3-26〉 NBCRV Stryker[67]

전하고 있다. 탐지장비의 고도화와 더불어 무인화를 통한 인명피해 없이 탐지할 수 있는 기술이 개발되고 있다. 미국은 화생방 대응기술개발을 포함하여 군내 연구시설 및 연구능력은 다른 국가에 비하여 세계 최고 수준을 유지하고 있다. M31/M31A1 등 생물학 정찰차량을 보유하여 생물학 무기에 대한 위협에 대응하고 있고, M93A1, NBCRV Stryker(〈그림 3-26〉) 등 화생방 정찰차량도 보유하고 있다.

방호 무기체계의 기술 발전 방향은 〈그림 3-27〉과 같다.

〈그림 3-27〉 방호 무기체계 기술발전 방향[68]

68) 국방기술품질원. "18~32 핵심기술기획서 일반본", 2018.

3.7 기타 무기체계

기타 무기체계는 “과학적인 의사결정 및 사업 관리를 지원하는 국방M&S체계와 각종 무기체계에 포함되어 임무 달성을 위해 필요한 기능을 구현하는 국방SW체계로 구분하며, 각 무기체계의 기반기술 및 분석기술로 활용”[70]된다.

〈그림 3-28〉 증강현실훈련체계[69]

전장모의와 관련해서는 실제 전장을 현실감있게 모의할 수 있는 실시간 데이터 처리 및 재연 기술이 발전하고 있으며 다중 행위자기반모형(Multi Agent Based Model)이 이용되는 추세에 있다. 인공지능을 활용하여 자율화된 가상군을 운용하고 여러 전장 환경이 생동감있게 구축 및 모델링 될 수 있는 기술이 개발되고 있다. 미국은 M&S에 기반한 훈련, 실험, 획득을 동시에 가능하게 하기 위해 OneSAF(One Semi-Automated Forces)를 개발하였다. 또한, 〈그림 3-28〉과 같이 실제 전장환경 기반의 증강현실 모의 훈련장비를 육해공군의 가상훈련에 활용하고 있다.

국방 SW와 관련해서는 시스템 SW, SW 미들웨어, SW 플랫폼 기술 측면에서 급속한 발전이 진행되고 있으며, 〈표 3-5〉와 같이 각 무기체계별로 첨단기술 구현에 필요한 핵심 SW기술을 전망해 볼 수 있다.

69) 국방기술품질원. “국방과학기술정보 제 63호”, 2017.
70) 국방기술품질원. “18~32 핵심기술기획서 일반본”, 2018.

〈표 3-5〉 무기체계별 핵심 SW기술 발전 전망[71]

구 분	SW 기술 발전 전망
지휘통제·통신	인공지능 기술과 M&S 기반의 효과 검증기술, 상황 적응형 SW기술
감시·정찰	SW 기반 적응형 레이더와 디지털 빔 형성의 핵심인 재밍 및 간섭처리를 위한 적응빔 알고리즘, 클러터 처리 알고리즘, 최적 디지털 빔 형성 알고리즘 구현에 필요한 SW기술
기동무기	미래전에 효과적으로 대응하고, 생존성 향상, 자동항법장치 개발을 위한 시스템 자동화 SW 기술이 발전할 전망이며, 화력의 지능화와 생존성 향상 및 무인 로봇의 자율주행, 원격제어 등 새로운 유·무인 통합 전투체계를 위한 SW핵심 기술
함정무기	탑재되는 장비의 유사기능을 통합하여 중앙 통제할 수 있는 통합기능체계로 발전하고 있으며, 이를 위한 함정시스템 통합SW 기술개발
항공무기	무인전투기, 공중급유기 등 신개념 비행체에 대한 자율 비행제어 SW 기술과 전장상황 인식/판단을 통해 자율적으로 HW를 동작하기 위한 지능형SW 기술, 주변 환경이나 내부 상황 변화에 따라 스스로 판단하여 임무를 수행하는 기술인 자가 적응형 SW 기술
화력무기	사거리 증대, 고속/고기동, 정밀도 향상, 생존성 증대, 파괴력 증대, 전천후 운용 능력 및 기만체계에 대한 회피능력이 강화되는 방향으로 개발되고 있으며 이를 구현하기 위한 SW 기술
방호무기	모든 탐지장비가 디지털화 되고 C4I체계와 연동될 수 있도록 실시간 전장관리 SW기술이 발전할 전망이며, 화생방 탐지의 통합화, 소형화, 무인화 정찰체계로 발전이 가속화됨에 따라 이를 구현하기 위한 SW 기술

71) 국방기술품질원. “2016 국방과학기술조사서”, 2016.

기타 무기체계의 기술 발전 방향은 〈그림 3-29〉와 같다.

〈그림 3-29〉 기타 무기체계 기술발전 방향[72)]

72) 국방기술품질원. "18~32 핵심기술기획서 일반본", 2018.

4. 종 합

미국은 트럼프 대통령 취임과 더불어 자국우선주의를 내세우고 있으며, 국방비 증액으로 뒷받침되는 '힘을 통한 평화' 정책을 추진함에 따라 중국, 러시아와의 강대국 경쟁 시대로 재진입하는 모습을 보이고 있다. 이와 함께 중국도 강대국으로서의 지위확보를 위한 대전략하에 군의 작전투사능력을 획기적으로 증강하고 있으며, 일대일로 사업을 적극 추진하고 있다. 이처럼 미중의 영향력 경쟁이 심화되고 있고 그 여파로 다자주의가 약화되어 범지구적으로 불안정성이 증대되어가고 있다. 특히, 핵 군비 통제의 동력이 상실되어감에 따라 미국과 러시아는 자국의 핵전력을 현대화하고 있으며, 중국 또한 핵전력을 통한 억제력 증진에 힘을 쏟고 있다. SIPRI에서도 우려를 표명한 것처럼 재래식 군비경쟁도 최근 심화되어가고 있으며, 그 중심에는 4차 산업혁명 시대의 신기술을 활용한 군사혁신을 달성하려는 국가들 간의 경쟁이 있다.

급변하는 안보정세와 더욱 더 치열해진 국가별 국방과학기술 경쟁은 우리 군에게도 첨단·핵심무기체계 개발에 대한 요구를 한층 더 고조시킬 것이며, 이를 달성하기 위해서는 국방과학기술과 무기체계 개발의 국제적 동향을 이해하고, 그 이해를 바탕으로 핵심기술 연구 및 무기체계 개발을 장기적으로 기획하여, 미래의 국가 안보가 증강된 군 전력으로 뒷받침 될 수 있도록 끊임없는 도전과 혁신이 필요하리라 판단된다. 핵심기술 연구 및 무기체계 개발 기획을 위해 본 연구에서는 무기체계를 중심으로 한반도 주변국의 국방과학기술 동향을 살펴보았으며, 4차 산업혁명 시대 신기술의 적용과 맞물려 이미 무기체계의 자율화, 스마트화, 소형화, 정밀화, 초연결화, 은밀화가 획기적으로 증대되어가고 있음을 확인하였다.

먼저 지휘통제·통신 분야는 〈그림 4-1〉과 같이 실시간 전출처 정보들을 융합하여 처리하고, 지능화된 상황인식과 방책수립을 가능케하는 '초지능화', 상황인지 기반의 망을 자가 구성하고 네트워크 중심의 상호운용성을 고도화하는 '다계층 통합화', 초고주파 대역 통신 등을 통한 초고용량을 전송하고, 항재밍, 저피탐 강화 자가 방어 통신을 위한 '항재밍 초고속화'의 발전 추세를 보이고 있다.

〈그림 4-1〉 지휘통제·통신 분야 발전 추세[73]

감시정찰체계의 발전 추세는 〈그림 4-2〉와 같이 cm급 초해상도 및 고감도 센서를 탑재하고, 수 Gbps급 획득정보를 전송하기 위한 '고성능화', 실시간 표적 정보를 획득, 처리, 공유하기 위한 '실시간 징후감시', 다중센서와 AI기반의 표적식별, 탐지, 추적을 위한 '지능화'이다.

〈그림 4-2〉 감시정찰체계 발전 추세[74]

73) 김찬수. "선진국 및 국내 국방과학기술 개발 동향", 과학기술정책, 제232호, 2017.
74) 김찬수. "선진국 및 국내 국방과학기술 개발 동향", 과학기술정책, 제232호, 2017.

타격체계의 발전 추세는 〈그림 4-3〉과 같이 '초고속/장거리화', '고위력화', '초정밀화'로 대표될 수 있으며, 〈그림 4-4〉 및 〈그림 4-5〉와 같이 무인/플랫폼의 발전 추세는 '자율화', '초소형화', '전투효율 극대화' 및 '대형 고성능화'로 요약될 수 있다.

〈그림 4-3〉 타격체계 발전 추세[75]

〈그림 4-4〉 무인/플랫폼 발전 추세(지상/해양)[76]

75) 김찬수. "선진국 및 국내 국방과학기술 개발 동향", 과학기술정책, 제232호, 2017.
76) 김찬수. "선진국 및 국내 국방과학기술 개발 동향", 과학기술정책, 제232호, 2017.

〈그림 4-5〉 무인/플랫폼 발전 추세(공중)[77]

이러한 발전 추세를 바탕으로 분야별로 우리가 지향해야할 방향은 〈표 4-1〉과 같다. 지휘통제·통신 분야는 실시간 전출처의 정보들이 유기적으로 융합되도록 하고, 이를 바탕으로 자율적인 정보판단 체계를 구축하여야 한다. 또한 효율적이면서 안정적인 운영을 위해 초고용량, 항재밍, 저피탐 강화 자가 방어 통신체계를 개발하여야 한다. 감시·정찰체계 분야는 감시자산들의 정밀도, 해상도, 통신능력 등을 향상시킬 수 있는 고성능화에 집중하여야 하며, 지능화된 실시간 징후감시, 표적의 식별, 탐지, 추적 체계를 구축하여야 한다. 타격체계 분야는 초고속 및 장거리화 되어가는 타격체계 추세에 부합하는 기술 개발과 함께 이를 적절히 방어할 수 있는 방어체계가 함께 개발되어야 한다. 더불어 초정밀 타격능력을 위한 지능형 신관, 탄도비행 스마트화, 고기동 비행제어 기술 등을 개발해야 한다. 무인/플랫폼 분야는 소형 및 다양화되는 개발 속에서 유무인 협업을 통한 전투효율 극대화에 집중하여야 하며, 자율 의사결정 및 무인 체계간 협업을 위한 자율협업 능력의 획득도 필요하다.

77) 김찬수. "선진국 및 국내 국방과학기술 개발 동향", 과학기술정책, 제232호, 2017.