통일정책연구 제24권 1호 2015
pp. 117~148

북한 사이버전 수행능력의 평가와 전망

김 인 수* · KMARMA**

Ⅰ. 문제제기
Ⅱ. 기존 연구 검토
Ⅲ. 북한의 사이버전 교리와 조직
Ⅳ. 북한 사이버전의 가능성과 한계
Ⅴ. 결론 및 정책적 함의

국문요약

북한은 휴전 이후 적대행위를 지속하고 있으며, 최근에는 국가 중요시설의 전산망을 공격하는 사이버 위협을 확대하는 등 사이버전 관련 과학기술의 질적 변화를 추구하고 있다. 그러나 사이버전을 수행하기 위한 과학기술이 도입·발전하는 과정은 각국의 고유한 사회구조 또는 문화의 영향으로부터 자유로울 수 없다. 이러한 문제인식에 따라 본고에서는 북한의 정치·경제·사회·군사적 조건을 중심으로 북한의 사이버전 수행능력을 평가해보았다. 분석결과 북한의 대남공작기구들은 모두 사이버 심리전 수행조직을 편성하고 있어 사이버 심리전이 북한의 사이버전 수행체계에서 중요한 역할을 하는 것으로 나타났다. 그 이유는 북한의 대남혁명전략, 선전·선동 중시의 정치문화, 미비한 사이버 인프라, 통신기반시설의 중국 의존 등 북한 고유의 정치·경제·사회·군사적 조건이 사이버전 수행을 위한 새로운 기술시스템이 도입, 검증·시험, 공고화되는 과정에서 사이버전 교리 및 조직에 영향을 미쳤기 때문인 것으로 나타났다. 이러한 분석결과는 언론의 자유와 북한의 군사적 위협에 대응하기 위한 정부의 개입이 마치 양립할 수 없는 것처럼 불협화음을 만들어내는 우리 사회의 안보 현실을 고려할 때, 향후 대남 사이버 심리전에 효율적으로 대응하기 위한 방안 마련이 시급하다는 정책적 함의를 제공한다.

주제어: 북한, 군사혁신, 기술시스템론, 사이버전, 사이버 심리전

Ⅰ. 문제제기

인간 사회는 혁명적인 변화를 거치면서 끊임없이 변화해왔다. 토플러(Alvin Toffler)는 이러한 변화의 추세를 농업혁명, 산업혁명, 정보혁명이라는 개념을 통해 설명한다.[1] 혁명의 물결이 밀려오면 이전 시대와 구분되는 새로운 사회와 문화

* 육군사관학교 사회학 부교수, 교신저자.
** 육군사관학교 71기 군사혁신연구팀(김건일, 박상구, 박은석, 박주호, 이상언, 림피팀).
[1] 앨빈 토플러, 이상백 역, 『제3의 물결』(서울: 영광출판사, 1991), pp. 21~24.

가 형성된다. 전쟁 역시 이러한 변화의 물결을 거스를 수 없다. 토플러는 "제3 물결은…경제의 기반을 뒤흔들고, 정치체제를 마비시키고, 가치체제를 분쇄해서 모든 인간에게 영향을 미치게 한다"[2]고 강조한다. 사람들이 새로운 사회에서 생존하기 위해 변화하는 것처럼, 군대 역시 새로운 환경에 적응하기 위해 변화하지 않을 수 없다. 최근 북한은 "사이버전은 핵, 미사일과 함께 우리 인민군대의 무자비한 타격능력을 담보하는 만능의 보검"[3]이라며 사이버전의 중요성을 강조하고 있다. 실제로 2009년 7·7 DDoS 공격 이후 올해 발생한 한국수력원자력 해킹 공격에 이르기까지 북한의 사이버 공격은 우리의 국가안보를 심각하게 위협하고 있다. 이에 따라 미래 전장은 사이버전 양상으로 전개될 것이라는 전망과 북한의 사이버 위협에 대응하기 위한 무기체계 및 기술 개발에 앞장서야 한다는 주장이 힘을 얻고 있다. 그러나 북한의 무기체계 또는 군사과학기술을 표준화된 모델로 설정하고 이를 따라잡는 것이 마치 혁신인 것으로 평가하는 시각은 표준화와 선형화에 토대한 제2 물결 시대의 세계관으로 만들어진 진부한 사고방식이다.[4]

첨단 군사과학기술의 도입으로 인해 앞으로의 전쟁양상이 근본적으로 변화하게 될 것이라는 인식은 기술이 인간 사회의 변화양상을 결정한다는 기술결정론에 토대하고 있다. 그러나 지금까지의 역사를 돌이켜보면 군 고유의 전통 또는 문화와 충돌할 경우 군대는 효율성이 높은 새로운 군사기술의 도입을 반대하였다. 오늘날 핵심적인 무기체계로 자리 잡은 기관총과 탱크의 도입과정에 많은 반대가 존재했다는 사실이 좋은 예이다.[5] 사이버전을 수행하기 위해서는 사이버 전사(인원), 사이버 전장(컴퓨터 및 통신 네트워크), 사이버 무기체계(소프트웨어 또는 하드웨어 무기체계), 사이버 표적(적 정보 및 정보체계) 등이 필요하다. 이러한 요소들을 효율적으로 통합하여 전쟁을 수행할 수 있을지 여부는 각 국의 고유한 사회구조 또는 문화적 영향에 의해 달라질 수 있다.[6] 헌팅턴(Samuel P. Huntington)은 제2 물결 시대의 세계관에 사로잡힌 전투원으로는 제3 물결 시대의 전쟁을 효율적으로 수행할 수 없다고 강조한다. 그렇다면 북한의 사이버전 관련 군사과학기술이 북한의 정치·경제·사회·군사적 상황과 맞물려 어떠한 형태의 사이버전 수행체계로 발전해나갈 것인지를 살펴보는 것은 매우 중요한 연구 과제라고 할 수 있다.

---

[2] 토플러, 『제3의 물결』, p. 23.
[3] 『조선일보』, 2013년 11월 5일.
[4] 토플러, 『제3의 물결』, p. 113.
[5] 온만금·김인수, 『군대와 사회』 (서울: 육군사관학교 화랑대연구소, 2005), p. 204.
[6] 이에 대해서는 전략문화의 개념을 참조할 것. 로렌스 손드하우스, 이내주 역, 『전략문화와 세계 각국의 전쟁 수행 방식』 (서울: 육군사관학교 화랑대연구소, 2007), pp. 16~18.

본고의 핵심적인 주장은 북한의 사이버전 수행능력은 사이버전 무기체계뿐만 아니라 새로운 군사과학기술을 뒷받침하기 위해 필요한 정치·경제·사회·군사적 조건을 함께 검토하여 평가해야 한다는 것이다. 북한의 군사력 건설에 대한 우리의 관심은 온통 사이버전·전자전 등 북한의 첨단무기체계와 군사과학기술 도입에 국한되고 있다. 그러나 우리의 안보를 보다 실질적으로 위협하는 것은 SNS(Social Network Service) 등 일상적인 기술을 활용해 왜곡된 정보를 유포하고 군과 정부에 대한 신뢰를 무너뜨리는 북한의 사이버 심리전이다. 이러한 문제 인식에 따라 본고에서는 북한의 사이버전 수행조직이 사이버 심리전 중심으로 발전해나가는 과정을 북한의 정치·경제·사회·군사적 조건을 중심으로 검토해보았다. 본고는 다음과 같이 구성되었다. 먼저 기존 연구검토를 통해 기술결정론의 한계 및 이를 극복하기 위해 제시된 기술시스템론에 대해 살펴본 후, 북한의 사이버전 수행조직을 다른 국가의 사이버전 수행조직과 비교해보았다. 이후 이러한 차이가 발생한 원인을 북한 사이버전 기술시스템의 도입, 검증·시험, 공고화 과정을 통해 살펴본 후, 북한의 사이버전 수행능력의 한계를 평가해보았다. 마지막으로 주요 연구결과를 요약하고, 한국의 대응방향에 대한 정책적 함의를 제시하였다.

Ⅱ. 기존 연구 검토

1. 군사혁신과 기술결정론의 한계

기술결정론은 기술 변화와 사회 변화의 관계를 설명하는 이론 중 하나로 기술발전이 사회변동의 주요한 원인으로 작용한다고 설명한다. 예를 들어 맑스(Karl Marx)는 "손방아는 봉건 영주의 사회를 낳고 증기방아는 자본가의 사회를 낳는다"[7]고 설명하였는데, 여기에는 인간 사회가 생산력의 기반인 기술에 의해 전환된다는 시각이 내포되어 있다. 정보체계와 정밀타격 무기체계의 등장 등 군사기술의 혁신이 전쟁양상을 본질적으로 변화시킬 것이라는 주장 역시 군사기술을 사회 변화의 원인으로 파악한다는 점에서 기술결정론으로 평가할 수 있다. 이러한 시각은 근대국가의 형성과정에 관한 연구에서 흔히 나타난다. 통상 호전주의 학파(bellicose perspective)로 불리는 학자들은 전쟁을 수행하기 위한 중앙정부의 노

[7] Karl Marx, *The Poverty of Philosophy* (New York, NY: International Publisher, 1971), p. 109.

력이 오늘날과 같은 근대국가의 형성과정에 미친 영향을 집중적으로 탐구하였다. 전쟁에서 승리하기 위해서는 최신 군사기술에 토대한 군사력을 건설·유지해야 하고, 이를 위해서는 인적·물적 자원의 동원에 효율적인 중앙집권적 국가체제를 도입해야 했다. 이에 따라 이들은 영국과 프랑스에 각각 입헌군주제와 절대왕정이 형성된 이유에 대해 지정학적으로 바다로 둘러싸여 군사적 위협이 상대적으로 적었던 영국에는 입헌군주제가 형성되었고, 반대로 주변국과 끊임없이 전쟁을 수행해야했던 프랑스에는 강력한 중앙집권적 국가체제가 형성되었다고 설명한다.[8]

이에 주목한 로버트(Michael Robert)는 1968년 군사과학기술의 발전에 따른 군사전략, 전술, 무기체계의 변화와 이를 뒷받침하기 위해 수반된 정치·경제·사회적 변화 양상을 설명하기 위해 군사혁명(military revolution)이라는 개념을 제시하였다.[9] 군사혁명의 대표적인 사례로는 15세기의 '포병 혁명(Artillery Revolution)'을 들 수 있다. 당시의 전투 패러다임은 강력한 성벽을 쌓아올린 성을 기점으로 공성전을 벌이는 양상이었다. 그러나 화약의 개발로 성벽을 무너뜨릴 수 있는 거포가 개발되자, 방자의 이점이 사라지고 공자의 이점이 더욱 부각되었다.[10] 포병화기를 전장에서 효율적으로 활용하기 위해서는 새로운 전술, 군사교리, 훈련 방식이 요구되었고, 이는 상비군의 필요성으로 이어졌으며, 상비군을 유지하기 위한 재정적 압력은 관료제라는 근대적 정부 조직이 등장하는 계기가 되었다.

군사과학기술의 중요성은 1970년대 구(舊)소련의 연구자들에 의해 제시된 군사기술혁명(Military-Technology Revolution, MTR)이라는 개념에 의해서 다시 한 번 주목을 받게 되었다. 소련의 오가르코프(N. V. Ogarkov) 원수는 기존 정찰체계와 정밀·장거리 타격체계를 결합할 수 있는 군사기술의 발달로 군사적 능력을 획기적으로 강화시킬 수 있다는 사실을 강조하였다. 특히 미국의 군사력 건설 방향에 관심이 많았던 소련은 향후 정찰 및 정밀유도무기와 관련된 기술의 발전으로 무기의 양 보다 성능이 중요해질 것이며, 이로 인해 전쟁양상이 급변하게 될 것으로 전망하였다. 소련의 MTR 개념은 미국 총괄평가국(the Office of

---

[8] Thomas Ertman, "State Formation and State Building in Europe," Thomas Janoski, Robert Alford, Alexander Hicks, and Mildred A. Schwartz (eds.), *The Handbook of Political Sociology* (New York, NY: Cambridge University Press, 2005), p. 368.

[9] Michael Robert, *The Early Vasas: A History of Sweden, 1523-1611* (New York, NY: Cambridge University Press, 1968).

[10] Clifford J. Rogers, "Military Revolution and Revolutions in Military Affairs: A Historian Perspective," Thierry Gongora and Harald von Riekhoff (eds.), *Toward A Revolution in Military Affairs: Defense and Security at the Dawn of the Twenty-first Century* (Westport, CT: Greenwood Press, 2000), pp. 22~24.

Net Assessment) 국장인 마샬(Andrew Marshall)에 의해 미국 국방부로 도입되어 1990년대 중반 군사혁신(Revolutions in Military Affairs, RMA)이라는 개념으로 발전하였다.[11] 군사혁신과 관련된 가장 대표적인 사례는 2차 세계대전 당시 독일군이 적용한 전격전을 들 수 있다. 독일군은 무기체계와 조직, 전략을 기동중심으로 대폭 수정하여 방어 중심 패러다임에 사로잡힌 프랑스군을 격파하고 전장의 지배자로 등장하였다. 이에 따라 헌들리(Richard O. Hundley)는 군사혁신을 "정찰체계, C3I, 정밀무기가 신속하고 지속적인 통합작전과 정보전을 포함하는 새로운 작전개념으로 결합된 군사기술 혁명"[12]으로 정의한다.

<표 1> 군사혁명, 군사혁신, 군사기술혁명의 비교

이론적 수준	개념	영향의 대상
대전략	군사혁명(MR)	경제, 산업구조, 인구, 사회, 전략문화
전략	군사혁신(RMA)	육·해·공군, 군/군단, 시스템 복합체계
작전술·전술	군사기술혁명(MTR)	무기체계, 군수체계

출처: Bjørn Møller, "The Revolution in Military Affairs: Myth or Reality?" *COPRI Working Paper Series,* Vol. 15 (2002), p. 11.

군사기술혁명, 군사혁신, 군사혁명은 군사과학기술의 발전을 필요로 한다는 점에서 서로 유사하다. 그러나 군사혁신은 군대 조직과 군사 교리의 변화를 반드시 필요로 한다.[13] 따라서 군사기술의 진전 없이 이루어진 군사혁신은 존재하지만, 조직과 교리의 변화를 수반하지 않은 군사혁신은 존재할 수 없다. 예를 들어 오스테르리츠(Austerlitz) 전역에서 프랑스군은 대불 동맹군과 동일한 무기체계(hardware)로 무장했지만, 혁명정신, 리더십, 융통성 있는 전술과 같은 소프트웨

[11] Yves Boyer, "The American Revolution in Military Affairs: A French Perspective," Thierry Gongora and Harald von Riekhoff (eds.), *Toward A Revolution in Military Affairs: Defense and Security at the Dawn of the Twenty-first Century* (Westport, CT: Greenwood Press, 2000), p. 81.

[12] Richard O. Hundley, *Past Revolutions, Future Transformation* (Santa Monica, CA: National Defense Research Institute RAND, 1999), p. 8.

[13] *Ibid.*, p. 15.

어(software)를 적절하게 활용하여 적군을 궤멸시켰다.[14] 이러한 성과를 거둘 수 있었던 주요 원인은 시민혁명으로 탄생한 정치 이데올로기와 민족주의를 전장에 투영시켜 대규모 인원을 동원할 수 있었던 프랑스가 막대한 전·사상자 발생을 감내하면서 전투를 지속할 수 있었기 때문이다.[15] 이에 따라 군사혁신에서 기술적 우위를 지나치게 강조하는 시각에 대한 우려의 목소리가 제기되었다. 스티븐슨(Scott Stephenson)은 미국은 군사기술 혁신에 지나치게 민감하게 반응하고 있으며, 이로 인해 적의 무기체계 개발 노력에 집중된 위협 분석으로 전쟁의 본질적인 측면을 간과하고 있다고 지적한다.[16] 미 해군 제독 맥레인(Daniel McNeil) 역시 정보전, 사이버전 등 새로운 기술체계에 매료된 정책결정자들이 이들 무기체계를 전략적으로 운용할 수 있는 능력에 대해서는 주의를 기울이지 않는다고 비판한다.[17]

이처럼 새로운 기술을 개발하고 이를 이용하는 것은 인간이라는 점에 주목한다면 사회의 외부에 존재하는 기술이 사회를 변화시킨다는 기술결정론의 시각에서 벗어나 인간 사회와 군사과학기술이 상호작용하는 과정에 대한 검토가 필요하다. 기술결정론의 한계를 비판하는 논리는 사회구성론과 기술시스템론으로 구분된다. 먼저 사회구성론은 특정 기술이 사회에 도입된 것은 그 기술의 상대적 우위 때문이 아니라 이와 관련된 사회집단의 이해관계 때문인 것으로 파악한다. 예를 들어 앞바퀴가 큰 초기 형태의 자전거와 달리 오늘날과 같은 형태로 자전거가 발전하게 된 것은 기술적 효율성 때문이 아니라 여성 자전거 애호가들이 치마라는 복장 때문에 앞바퀴가 큰 자전거를 선호하지 않았기 때문이라는 것이다.[18] 반면 기술시스템론은 새롭게 도입된 기술과 이를 운용하기 위해 요구되는 다양한 사회적 요인들 간의 상호작용에 주목한다.[19] 이러한 시각에 따르면 최초 등장단계부터 사회에 지배적인 영향력을 행사할 수 있는 기술시스템은 존재하지 않는다. 한 사회에 보편적으로 적용되는 기술시스템은 기술의 혁신은 물론 정부의 정책에 의해서도

---

[14] Scott Stephenson, "The Revolution in Military Affairs: 12 Observations on an Out-of-Fashion Idea," *Military Review* (May-June 2010), p. 43.

[15] Williamson Murray, "Thinking about Revolutions in Military Affairs," *Joint Force Quarterly* (Summer, 1997), p. 71.

[16] Stephenson, "The Revolution in Military Affairs: 12 Observations on an Out-of-Fashion Idea," p. 43.

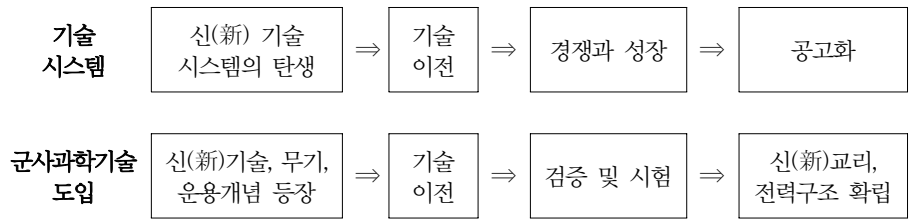
[17] Daniel McNeil, "Technology, History and the Revolution in Military Affairs," *Canadian Military Journal* (Winter, 2000/2001), p. 16.

[18] 홍현필·이용환, 『기술과 사회』 (서울: GS 인터비전, 2011), p. 85.

[19] 이장규·홍성욱, 『공학기술과 사회: 21세기 엔지니어를 위한 기술사회론 입문』 (서울: 지호, 2006), p. 109.

크게 변화할 수 있기 때문이다. 예를 들어, 유사한 전력 시스템을 도입한다고 하더라도 이를 유지하기 위해 소규모 발전소를 많이 건설하는 국가가 있는 반면, 소수의 대규모 발전소를 건설하는 국가도 존재할 수 있다. 이에 따라 새로운 기술시스템은 만들어진 이후 다른 지역으로의 이동, 경쟁 과정을 거치면서 상대적 우위를 점하게 되었을 때 비로소 모멘텀(momentum)을 확보하여 공고화된다.

<표 2> 기술시스템의 진화과정과 군사과학기술의 도입과정 비교



출처: 이장규·홍성욱, 『공학기술과 사회: 21세기 엔지니어를 위한 기술사회론 입문』 (서울: 지호, 2006), p. 114를 참고로 작성.

기술시스템론을 통상적인 군사과학기술의 도입 과정에 적용하면 <표 2>에 제시한 바와 같다. 군사과학기술이 최초 개발된 지역에서 다른 지역으로 이전되면, 광범위한 검증 및 시험을 거쳐 신(新) 교리와 새로운 전력구조로 정착된다. 그러나 과학기술적 요소들이 다른 지역으로 이전될 때에는 각 지역의 정치 체계, 지리적 조건, 규제 법령, 역사적 경험 등이 개입되어 새로운 형태로 변화할 수 있다. 군사과학기술의 활용을 제한할 수 있는 요인들은 정치·경제·사회·군사적 측면에서 검토해볼 수 있다.

2. 군사과학기술 활용의 제한 요인

가. 정치적 요인

전쟁의 승패는 군사기술의 우위가 아니라 인간의 관념에 의해 결정될 수 있다. 먼저 국가의 전쟁관을 결정하는 정치이념은 군사혁신을 제한하거나 촉진할 수 있다. 17~18세기의 절대왕정은 소규모 영토분쟁이나 왕위계승 문제를 두고 전쟁을 벌였다. 절대왕정의 목적은 체제를 유지하고 손실을 최소화하는 선에서 제한된 목표를 달성하는 것이었다. 이러한 이유로 당시의 국가는 전쟁을 최대한 기피하였으며, 대규모 병력의 충돌을 꺼렸다. 반면 혁명기의 프랑스에게 있어서 전쟁은 국

가의 존망이 걸린 중요한 문제였다. 유럽의 여러 나라들은 프랑스에서 일어난 혁명의 불길을 진압하기 위여 대불 동맹을 형성하고 프랑스와 전쟁을 벌였다. 국가의 존망이 달린 프랑스는 국민들의 혁명정신을 전쟁에 투사하여 국민 개병제라는 군사혁신을 일구어냈다. 나폴레옹은 대규모의 군대와 국민들의 혁명정신을 기반으로 한 산병전술을 바탕으로 압도적인 승리를 거두었다. 한편 19세기 중반 프로이센의 비스마르크를 비롯한 정치지도부는 '철혈정책'의 기조 아래 전쟁을 통하여 정치적 통일을 이룩해야 한다는 결정을 내렸다. 이는 프로이센의 사회뿐만 아니라 정계에서도 민족적 통합을 요구하는 목소리가 커졌기 때문이었다. 통일에 대한 정치적 요구는 새로운 군사기술의 도입으로 이어졌다. 빌헬름 1세는 1859년 당시 최신식 대포로 취급받았던 크룹(Krupp)사의 강철제 후장식 대포 300여 문을 도입하여, 보불전쟁에서 프랑스를 화력으로 압도할 수 있었고 결국 독일의 통일을 이룩하게 되었다.[20]

그러나 형이상학적 개념인 정치이념과 전쟁관이 제도와 기술의 실질적인 변화를 의미하는 군사혁신으로 직결되는 것은 아니다. 정치이념이 군사혁신의 걸림돌로 작용하는 경우도 있다. 오늘날 군사혁신의 개념은 소련에서 제시된 군사기술혁명 개념으로부터 발전하였다. 그러나 맑스의 이론에 따라 소련의 사회주의 국가가 사회 발전의 종착점이 될 것이라고 확신하였던 소련의 지도부는 군사기술혁명의 필요성에 대해 공감하지 못했다. 소련이 가지고 있는 군사전략 및 군사제도가 다른 국가에 뒤처진다는 평가는 사회주의 이념 자체를 부정하는 행위로 정치적 탄압의 대상이 될 수 있었기 때문이다.[21] 그 결과 소련의 군사기술혁명은 미국과 같은 군사혁신으로 이어질 수 없었다. 이처럼 국가의 정치이념·전쟁관과 군사혁신의 간극에는 정치지도자의 전략적 판단이 존재한다. 한국의 '국방개혁 2020'과 미군의 '변혁(transformation)'을 비교해보면, 각국의 지도자가 보이는 전략적 판단의 차이가 군사혁신의 성패에 얼마나 큰 영향을 끼치는지 알 수 있다. 미국의 럼스펠드 장관은 미군 수뇌부와 많은 갈등을 겪었지만, 변혁을 위하여 설정한 66개 목표 중 42개를 달성하였다.[22] 반면 미국과 달리 한국의 국방개혁은 실질적이고 구체적

[20] 윌리엄 맥닐, 신미원 역, 『전쟁의 세계사』 (서울: 이산, 2005), p. 331.

[21] acob W. Kipp, "The Labor of Sisyphus: Forecasting the Revolution in Military Affairs During Russia's Time of Trubles," Thierry Gongora and Harald von Riekhoff (eds.), *Toward A Revolution in Military Affairs: Defense and Security at the Dawn of the Twenty-first Century* (Westport, CT: Greenwood Press, 2000), pp. 90~91.

[22] Department of Defense, *Department of Defense Performance and Accountability Report FY 2006* (Washington D.C.: Department of Defense, 2006), p. 30.

인 변화를 이끌어내지 못했다. 확실한 계획을 수립한 후 점진적으로 변화시켜나가는 것을 개혁이라고 인식한 한국 국방부는 새로운 계획을 반복적으로 작성하는데 지나치게 비중을 많이 둔 나머지 계획을 실천으로 옮기는데 실패한 것이다.[23]

나. 사회적 요인

기술결정론의 입장에서는 향후 전쟁의 승패는 기존 무기체계에 비해 효율성이 뛰어난 첨단무기체계의 보유 여부에 따라 결정될 것이라고 전망한다. 그러나 무기체계를 새롭게 도입한다고 하더라도 이를 운용하기 위한 조직 및 작전운용 개념을 변경하는 것은 쉬운 일이 아니다. 이와 관련된 대표적인 사례는 병역제도의 역사적 발전과정에서 쉽게 찾아볼 수 있다. 17세기 스웨덴 국왕 구스타프 아돌프스(Gustavus Adolphus)는 소총과 대포의 경량화, 징병제에 토대한 상비군 운용, 보·포·기병의 통합전술을 구사해 군사적 승리를 거듭하였다.[24] 이러한 군사혁신을 가능하도록 한 것은 스웨덴의 특수한 사회구조였다. 소규모 자영농을 중심으로 구성된 스웨덴에서는 외적의 침입은 곧 토지의 상실을 의미했으므로 자신의 토지를 지키기 위한 명분으로 농민들을 국민군으로 징병할 수 있었다.[25] 반면 농노제에 토대한 유럽의 다른 지역에서는 전쟁이 여전히 지배자의 개인적인 업무에 불과했다. 프러시아에서도 농민들을 대상으로 징병을 실시하였지만, 농민들의 징병 회피 시도와 농민 감소로 인한 경제적 부담 등을 이유로 국민군대를 창설하는데 실패하였다.[26] 그 결과 용병제에 의존하지 않을 수 없었고, 이는 적용 가능한 전략과 전술을 크게 제한하였다. 용병에 토대한 유럽의 상비군 제도는 프랑스 혁명으로 이루어진 정치·사회적 개혁이 유럽의 다른 지역으로 확산되면서 붕괴되기 시작하였다. 징병으로 동원한 프랑스군의 대규모의 병력에 맞서기 위해서는 동일한 규모의 병력 동원해야 했고, 이를 위해서는 징병을 가능하게 할 정치·사회적 개혁이 반드시 필요했기 때문이다.

근대 국민군대를 만들어내기 위해 근대 시민이 필요했던 것처럼 미래 전쟁에서

---

[23] 박휘락, "국방개혁 2020과 미군 "변혁"(Transformation)의 비교와 교훈 : 변화방식을 중심으로," 『평화학연구』, 제13권 3집 (2012), pp. 167~168.

[24] 육군사관학교, 『세계전쟁사』 (서울: 일신사, 1995), pp. 72~73.

[25] 죤 하키트, 서석봉·이재효 역, 『專門職業軍』 (서울: 연경문화사, 1989), p. 62.

[26] 프러시아의 프레더릭 대왕(Frederick the Great)은 "우리 군의 연대는 반은 시민으로, 반은 용병으로 구성되어 있다. 용병들은 국가와는 어떤 이해관계도 없는 상태이므로 기회만 있으면 이탈한다"고 비판하였다. 위의 책, p. 89.

승리하기 위해서는 시대적 요구에 부합하는 전투원이 필요하다. 토플러, 드러커(Peter Drucker), 벨(Daniel Bell) 등의 미래학자들은 인간 사회가 농업사회, 산업사회를 거쳐 정보사회, 지식사회, 또는 후기 산업사회로 변화해나가고 있다고 설명한다. 대량생산, 대량소비, 표준화, 선형화 등으로 특징되는 산업사회와 달리 지식·정보 기반의 새로운 사회는 정보산업 또는 지식산업 종사자의 사회적 지위를 향상시킬 뿐만 아니라 체계적인 정보흐름을 가능하게 하는 네트워크화를 그 특징으로 한다. 군의 정보화 역시 개별 군인들에게 요구되는 기술 요건을 강화시켜 상호 교환이 불가능한 노동을 증가시킬 수 있다. 군대조직의 특성과 바람직한 군인 상 역시 이러한 사회 변화 방향에 따라 변화하지 않을 수 없다. 예를 들어 핵전쟁 시대의 도래와 함께 군인들에게 요구되는 전문지식과 기술적 수준이 함께 향상되었다는 사실에 주목한 자노위츠(Morris Janowitz)는 군대의 통솔이 권위에 의한 강압적 통제방식에서 설득과 동의에 의한 방식으로 변화하게 될 것이라고 설명한 바 있다.[27] 결국 미래 전장에서는 지식을 병력, 무기, 장비 등 유형 전투력 보다 지식기반의 군사전략과 전술, 군사훈련, 유연한 군 조직체계 등 무형 전투력의 중요성이 더 커지게 된다. 이러한 맥락에서 미국의 스태리 장군(Donn A. Starry)은 군사혁신을 위한 사회적 조건의 중요성을 다음과 같이 설명하였다.

> 군은 고치기가 매우 힘듭니다. 어쨌든 군도…제2 물결 제도니까요. 군도 공장인 셈입니다…우리의 산업시대 공장들이 무기를 계속 생산합니다. 군대는 군인들을 훈련공장에서 처리합니다. 그러고 나서 이 군인들과 무기들을 결합시키면 우리가 전쟁에서 이긴다는 겁니다. 접근방법 전체가 제2 물결적입니다. 이제는 그것을 제3 물결 세계에 끌어들여야 합니다.[28]

전투원이 새로운 기술에 동화될 수 있는 지 여부는 군사과학기술의 도입에 있어서 매우 중요하다. 기술적으로 효율적인 무기체계라고 할지라도 군대 조직에서 비효율적으로 사용될 수 있기 때문이다. 월남전 당시 M-16 소총 도입을 둘러싼 갈등이 좋은 사례가 될 수 있다. 민간 총기회사에서 제작된 M-16 소총은 미국 병기연구소에서 제작한 M-14 소총에 비해 기술적으로 우수했지만, 병기연구소에서 요구한 개선사항을 수용한 결과 심각한 기계적 결함을 갖게 되었다. 이에 따라 1967년 미국 의회는 군이 고의로 M-16 소총을 거부하기 위해서 문제점을 개선하

---

[27] Morris Janowitz, *The Professional Soldiers: A Social and Political Portrait* (New York, NY: The Free Press, 1970), p. xvii.

[28] 앨빈 토플러, 이계행 감역,『전쟁과 반전쟁』(서울: 한국경제신문사, 1994), p. 81.

기 위한 필요한 조치들을 취하지 않았다는 조사결과를 발표하였다.[29] 이처럼 군사변혁은 기술적 요인만으로는 완성될 수 없다. 새로운 무기체계를 개발·도입했다고 하더라도 기존의 편제, 교리의 개념이 그 무기체계의 효과를 발휘할 수 없는 구조로 되어있다면 그 무기체계는 무용지물이 될 것이다. 무기체계의 효과를 극대화하기 위한 지휘구조, 편제, 군사교리, 작전·전술적 개념은 그 시대의 사회적 조건에 영향을 받기 쉽다. 왜냐하면 사회적 요인들은 군사력 발달에 필수적인 전제가 되는 기술적 혁신을 제한할 수 있을 뿐만 아니라, 기술 혁신의 내용과 그것이 한 사회에 적용되는 방식을 결정하기 때문이다.

다. 경제적 요인

군사변혁을 추진하기 위해서는 경제적 조건을 고려하지 않을 수 없다. 모든 국가는 잠재적 적국의 군사변혁을 예의 주시하면서 이를 따라잡기 위해 노력한다. 그러나 이러한 노력은 심각한 경제적 부담을 초래하고 의도하지 않게 안보를 위협할 수 있다. 냉전시대에 미국과 소련은 공포의 균형에 의해서 평화를 유지하였기 때문에 군의 규모를 확장시키고 재래식 무기와 핵무기의 개발에 박차를 가하였다. 그러나 군비경쟁이 지속됨에 따라 소련은 막대한 경제적 부담을 떠안게 되었다. 이러한 상황은 통상 국방딜레마(defense dilemma)를 초래하게 된다. 국방딜레마란 국방을 위해 지나치게 많은 자원을 할당함으로써 국가의 생존에 필요한 다른 분야의 발전이 지체되어 결국 국가안보를 위협하게 되는 모순적인 상황을 말한다.[30] 이에 따라 경제적 부담을 완화시키기 위한 조치로 소련은 동구권의 위성국가와 아프가니스탄에 대한 군사적 개입을 철회하는 등 전략적 이탈(strategic exit)을 선택하게 되었다.[31] 이러한 정치적 상황이 소련의 대외적 영향력을 제한하는 가운데 고르바초프 시기의 개혁·개방정책이 추진되면서 소련은 결국 붕괴하게 되었다.

경제력의 한계로 인한 안보 위협은 군 내부에서도 발생할 수 있다. 군사변혁을 추진하는 국가는 제한된 예산을 각 군에 분배해야 하기 때문에 투자 대비 효과성을 고려하게 된다. 이로 인해 예산을 둘러싼 갈등이 발생할 수 있다. 핵폭탄의 투하로 2차 대전을 종전시킨 미 공군은 미국의 안보가 대규모 전략폭격기에 의해

---

[29] 온만금·김인수, 『군대와 사회』, pp. 205~206.
[30] 황진환 외, 『신국가안보론』, p. 269.
[31] Kipp, "The Labor of Sisyphus," pp. 90~91.

좌우될 것이며 해군과 육군은 공군을 보조하는 역할을 하게 될 것이라고 주장하여 해군과 육군의 반발을 초래하였다.[32] 오늘날의 군사변혁이 통상 공중, 우주, 해상에서의 탐지 및 정밀타격 능력을 확보하는데 초점을 맞추고 있고, 이를 위한 무기체계를 구입하기 위해 막대한 예산이 소요된다는 점을 고려하면 군사변혁을 추진하는 과정에서 군 내부의 갈등은 피할 수 없다. 이러한 갈등은 한국군 내부에서도 발견할 수 있다. 국방개혁 2020 계획은 최초 육·해·공군의 균형발전과 합참 기능의 강화를 목표로 설정하였다. 이에 따라 육군 병력을 54.8만에서 37.1만으로 감축할 것을 계획하였다.[33] 그러나 이명박 정부 들어 국방개혁 2020이 군 상부구조를 육군 중심으로 개편하는 국방개혁 307로 수정되면서 육·해·공군 간의 갈등이 불거졌다.[34]

라. 군사적 요인

군사기술의 우위를 무력화시킬 수 있는 요인으로는 군사적 조건도 있다. 군사적으로 열세에 있는 국가들은 이를 만회하기 위해 나름대로의 군사변혁을 추진한다. 독일이 1차 대전 당시 U-보트를 개발하거나 2차 대전 당시 기동을 중시하는 전격전을 개발하게 된 이유는 모두 경쟁국인 영국과 프랑스에 비해 병력이나 장비 수준에서 열세를 면할 수 없었기 때문이었다. 그러나 군사기술의 우위는 잠재적 적국의 노력에 의해 쉽게 추월당할 수 있다. 예를 들어 1940년 프랑스 침공 당시 독일의 전격전은 군사혁신의 대표적인 사례로 제시된다. 하지만 독일군은 1942년 후반부터 항복 전까지 우크라이나(Ukraine), 벨로루시(Byelorussia), 비스툴라(Vistula) 일대에서 소련 방식의 전격전에 맞서 싸워야 했다.[35] 또한 독일은 두헤(Giulio Douhet)과 미첼(Billy Michell) 같은 전략가들의 아이디어를 받아들여 후방의 민간인들을 표적으로 하는 전략폭력 능력을 발전시켰다. 이러한 시도 역시 독일 공군의 전략 폭격을 사전에 경고하고 대비하기 위해서 영국이 구축한 레이더, 공군기지, 지역 및 중앙통제소로 구성된 방어체계에 의해 무력화되었다.[36]

전략문화 역시 군사변혁에 영향을 미치는 요인이다. 전략문화는 "한 국가의 전통, 가치, 태도, 행동양식, 습관, 관습, 성취 및 환경에 적응하고 무력의 사용이나 위협

[32] Stephenson, "The Revolution in Military Affairs," p. 44.
[33] 국방부, 『Defense Reform 2020: 국민과 함께 미래를 향해』 (서울: 국방부, 2005), p. 12.
[34] 『한겨레』, 2011년 11월 4일.
[35] Stephenson, "The Revolution in Military Affairs," p. 40.
[36] *Ibid.*, p. 42.

과 관련하여 문제를 해결하는 특별한 방식," 또는 "한 국가의 전략적 공동체가 훈련이나 모방을 통해서 획득하는 습관적인 패턴의 총합"으로 정의된다.[37] 이러한 전략문화는 합리적 사고방식으로는 도저히 이해할 수 없는 특정 국가의 군사적 행위를 설명하기 위한 유용한 시각을 제공한다. 예를 들어 구소련의 경우 1970년대부터 MTR 개념에 기초한 군사혁신을 추진해야 한다는 요구가 제기되었다. 그러나 기갑 중심의 사고방식과 관료 문화에 사로잡힌 소련군 지휘부는 이러한 요구를 적극적으로 받아들이지 못했다.[38] 따라서 군사과학기술의 도입 과정을 이해하기 위해서는 해당 국가의 역사, 정치제도, 전략적 상황을 함께 고려해야 한다.

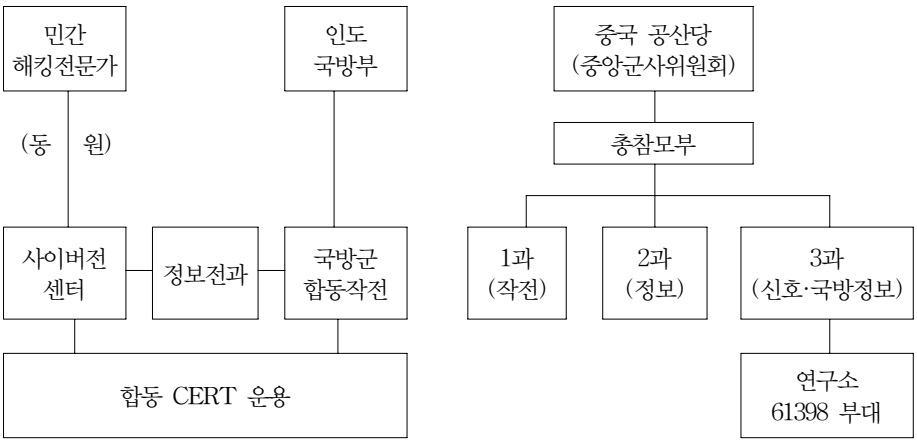
3. 사이버전 기술시스템의 국가별 차이

1990년대 후반부터 인터넷 사용이 세계적 규모로 확산되면서 개인, 인터넷, 사회를 연결하는 사이버 공간의 중요성이 커지고 있다. 모든 사람에게 접근을 허용하는 사이버 공간의 개방성은 한편으로 다양한 사회적 교류와 문화적 콘텐츠의 공유를 가능하도록 하는 장점이 있었다. 그러나 다른 한편으로는 사이버 공간의 익명성과 합쳐져 사이버 범죄에 취약한 약점을 드러냈다. 이처럼 데이터, 시스템, 정보통신망 등과 관련되어 발생하는 모든 불법적인 행위를 '해킹'이라고 한다. 해킹이란 용어 자체는 미국의 MIT 대학에서 자신의 기술을 과시하려는 학생들에 의해 처음 등장했지만, 점차 상대국의 군 정보 시스템뿐만 아니라 국가기반시설 전반에 걸친 사이버 공격으로 확대되고 있다. 또한 사이버 공간이 상대국의 취약점을 이용하여 도발을 억제하거나 또는 도발을 자행하는 전략적 수준의 전장으로 변화하게 되었다. 그 결과 "사이버 공간에서 일어나는 새로운 형태의 전쟁수단으로서, 컴퓨터 시스템 및 데이터 통신망 등을 교란, 마비 및 무력화함으로써 적의 사이버 체계를 파괴하고, 아군의 사이버 체계를 보호하는 것"을 의미하는 사이버전의 개념이 정립되었다.[39] 그러나 군사과학기술 도입에 영향을 미치는 정치·경제·사회·군사적 조건이 국가별로 상이하기 때문에 사이버전 기술시스템은 국가별로 다르게 발전하게 된다.

---

[37] 손드하우스, 『전략문화와 세계 각국의 전쟁 수행 방식』, pp. 16~18.
[38] Kipp, "The Labor of Sisyphus," p. 90.
[39] 엄정호·최성수·정태명, 『사이버전개론』 (서울: 홍릉과학출판사, 2012), p. 7.

<그림 1> 인도와 중국의 사이버전 지휘체계 비교



출처: Michael Aschmann, Joey Jansen van Buuren, Louise Leenen, "Cyber Armies: The Unseen Military in the Grid," The Proceedings of the 10th International Conference on Cyber Warfare and Security (24 February 2015), pp. 24~25.

<그림 1>은 중국과 인도의 사이버전 지휘체계를 비교한 결과를 보여준다. 인도와 중국은 사이버전 교리, 정보작전부대 운용 등에서 다른 국가들에 비해 기술적으로 앞서 있는 것으로 평가받고 있다.[40] 그러나 사이버전 수행방식에서는 큰 차이를 보인다. 인도는 민간 영역의 IT와 사이버 안보전문가를 화이트 해커(white hacker)로 동원하여 활용하는 구조를 발전시켰다.[41] 이는 군사적 목적의 독자적 기술 개발에 집중하기 보다는 민간 기술의 활용을 우선시 한다는 것을 의미한다. 중국은 1995년부터 정보전 능력을 발전시키기 위한 노력을 전개해왔으며, 1997년에는 서구 국가들의 지휘통제시스템을 공격하기 위해 넷포스(Netforce)로 알려진 사이버전 부대를 창설하였다.[42] 중국의 사이버전은 신호 및 국방정보를 총괄하는 총참모부의 3과가 주도하고 있으며, 3과는 13개의 연구소와 컴퓨터 네트워크 작전을 담당하는 61398부대를 운용하고 있는 것으로 알려졌다.[43] 민간 영역의 협력을 중시하는 인도와 달리 중국의 사이버전 조직 형태가 군 중심으로 발전

[40] 『연합뉴스』, 2013년 3월 21일.
[41] Michael Aschmann, Joey Jansen van Buuren, Louise Leenen, "Cyber Armies: The Unseen Military in the Grid," The Proceedings of the 10th International Conference on Cyber Warfare and Security (24 February 2015), p. 25.
[42] Desmond Ball, "China's Cyber Warfare Capabilities," *Security Challenges*, Vol. 7, No. 2 (Winter, 2011), p. 81.
[43] Michael Aschmann, Joey Jansen van Buuren, and Louise Leenen, "Cyber Armies: The Unseen Military in the Grid," p. 24.

한 이유는 중국이 체제 안정을 위해 민간 영역의 인터넷 사용을 강력하게 통제하고 있기 때문이다. 따라서 북한의 사이버전 교리와 조직 역시 북한 고유의 정치·경제·사회·군사적 상황 속에서 파악해야 한다.

Ⅲ. 북한의 사이버전 교리와 조직

1. 북한의 사이버전 교리

북한의 사이버전 교리는 외부로 공개된 자료가 없기 때문에 이를 정확히 파악하는 것은 쉽지 않다. 따라서 사이버전 교리의 군사적 특성을 파악하기 위해서는 먼저 중국과 러시아의 사이버전 교리를 살펴볼 필요가 있다. 북한의 사이버전 기술은 중국 및 러시아에 크게 의존하고 있기 때문이다. 첫째, 중국의 사이버전 교리는 2050년까지 적의 정보 기반시설(information infrastructure)을 붕괴시킬 수 있는 능력을 확보하여 전 세계적 범위에서 '전자적 우위(electronic dominance)'를 달성하는 것을 목표로 하고 있으며, 이를 위해 재래식 전쟁을 개시하기 전에 적의 금융 시스템, 민간 또는 군사통신 시스템을 파괴하는 전략을 채택하고 있다.[44] 둘째, 러시아는 대량살상무기를 이용한 재래식 군사 활동의 효과를 증폭시키기 위한 수단으로 사이버전을 활용한다는 교리를 채택하고 있다.[45] 그러나 북한의 사이버전 교리는 북한이 보유한 사이버전 기술에 의해서가 아니라 북한이 처한 상황에 따라 결정될 가능성이 크다. 이에 따라 북한의 정치·경제·사회·군사적 요인이 북한의 사이버전 수행목표 형성에 미칠 영향을 파악해보았다.

첫째, 북한의 사이버전 교리는 국가목표를 달성하기 위한 목적지향적 지침이 되어야 하기 때문에 정치적 맥락 속에서 파악해야 한다.[46] 북한은 조선로동당 규약 전문에 "조선로동당의 당면목적은 공화국 북반부에서 사회주의 강성대국을 건설하며 전국적 범위에서 민족해방, 민주주의 혁명의 과업을 수행하는데 있으며 최종목적은 온 사회를 주체사상화하여 인민대중의 자주성을 완전히 실현하는 데 있다"고 규정하고 있다.[47] 이러한 정치적 목표를 달성하기 위하여 북한은 다음과 같

---

[44] Ward Carroll, "China's Cyber Forces," <http://defensetech.org/2008/05/08/chinas-cyber-forces/> (검색일: 2015.6.9.).
[45] Ward Caroll, "Russia's Cyber Forces," <http://defensetech.org/2008/05/27/russias-cyber-forces/> (검색일: 2015.6.9.).
[46] 황진환 외, 『신국가안보론』 (서울: 박영사, 2014), p.
[47] 통일교육원, 『북한이해 2012』 (서울: 통일교육원, 2012), p. 87.

이 3대 혁명역량의 강화를 주장해왔다.

> 우리 조국의 통일, 즉 조선혁명의 전국적 승리는 결국 3대 역량의 준비에 있다고 말할 수 있다. 첫째로 공화국 북반부에서 사회주의 건설을 잘하여 우리의 혁명기지를 정치·경제·군사적으로 더욱 강화하는 것이며, 둘째로 남조선 인민들을 정치적으로 각성시키고 튼튼히 묶어 세움으로써 남조선의 혁명역량을 강화하는 것이며, 셋째로 조선인민과 국제혁명역량과의 단결을 강화하는 것이다.[48]

북한은 이러한 전략기조에 따라 1990년대 중반부터 "인민군대의 강화에 최대의 힘을 넣고 인민군대의 위력에 의거하여 혁명과 건설의 전반 사업을 힘 있게 밀고 나가는 특유의 정치"를 뜻하는 선군정치 이념체계 하에서 군을 최우선적으로 배려하고 있다.[49] 이에 따라 북한은 첫 번째 전략기조, 즉 북한 혁명역량 강화를 위해 대량살상무기 개발과 사이버전 능력 강화를 추진하고 있다. 그러나 북한은 두 번째 전략기조, 즉 남조선 혁명역량 강화를 위해서 사이버전 능력을 적극 활용할 것으로 예상된다. 그 이유로는 최근 사이버 공간이 남한 주민들의 정치적 행위에 미치는 영향이 커지고 있다는 사실을 무시할 수 없다. 남한의 사이버 공간은 경제·문화의 기반임과 동시에 여론이 형성되는 의사소통의 기반으로 작용하고 있다. 이는 북한이 사이버 공간을 장악할 경우 사회 모든 분야로 북한의 영향력을 확산시킬 수 있다는 것을 의미한다. 남조선 혁명역량이란 남한 내에 좌경세력과 체제에 불응하는 세력을 양성하여 남한의 사회체제를 흔들어 놓을 수 있는 능력을 말한다. 따라서 북한의 사이버전 교리는 인터넷을 통해 허위 정보를 유출하고 여론을 혼란시켜 친북세력을 형성·확대하는 것을 목표로 삼을 것으로 보인다.

둘째, 북한의 경제정책 역시 사이버전 교리에 영향을 미칠 수 있다. 북한은 "우리에게 간절한 문제는 현대적 과학기술에 튼튼히 의거 경제강국, 과학기술 대국을 세우는 것"[50]이라고 강조하고 있다. 이를 위해 북한은 IT 산업을 핵심으로 경제활성화를 추구하는 '단번 도약' 전략을 추진하고 있다. 북한이 IT 산업을 중시하는 이유는 군사강국 건설뿐만 아니라 경제구조의 개선을 위해서 반드시 필요하기 때문이다.[51] 이에 따라 북한 노동신문은 "정보기술인재 양성사업을 강화하는 것은

---

[48] 육군사관학교, 『북한학』 (서울: 황금알, 2004), p. 489.
[49] 통일교육원, 『북한이해 2012』, p. 88.
[50] 『노동신문』, 2002년 1월 23일.
[51] 김재호, 『김정일 강성대국 건설전략』 (평양출판사, 2000), pp. 31~37.

강성대국 건설의 지름길"[52]이라며 IT 기술의 중요성을 강조하고 있다. 그러나 경제적으로 낙후한 북한에서 단기간 내에 IT 산업 육성을 통한 성과를 기대하기는 힘들다. 이에 따라 북한은 대규모 자본투자 없이 기술 개발이 가능한 소프트웨어를 외화벌이를 위한 수단으로 활용할 수 있다. 김정은이 외화벌이 사업에 나선 "군대가 너무 돈에 맛을 들였다"고 질책했다는 사실 역시 군사과학기술이 경제적 목적으로 전용될 가능성을 보여준다.[53] 또한 국내 인터넷 게임 이용자가 북한 해커들에게 해킹 프로그램 개발을 의뢰하거나, 국내 도박꾼이 북한 정찰총국 소속 공작원에게 북한산 해킹 프로그램을 구입하는 사건이 잇따라 발생하고 있는 현실이 이를 뒷받침 한다.[54]

셋째, 북한은 "정치적으로는 수령중심의 일당독재, 경제적으로는 중앙집권적 계획경제, 사회적으로는 조직적 통제사회, 그리고 문화적으로는 주체사상의 유일사상화를 중심으로 하는 전체주의 사회"의 특성을 갖는다.[55] 북한과 같은 전체주의 사회가 안정적으로 유지되기 위해서는 폭력을 통한 강압과 정권의 정당성 강화를 위한 선전·선동이 병행되어야 한다. 폭력의 남용만으로는 체제에 대한 주민들의 자발적 복종을 얻어내기 어렵기 때문이다. 이로 인해 북한에서는 1960년대부터 주체사상을 통치 이데올로기로 제시하여 김일성에 대한 개인 우상화를 진행하였고, 통치자에 대한 우상화 시도는 현재까지 그대로 이어지고 있다. 이에 따라 북한의 학교 교육은 정치사상교육을 강조한다. 최근 북한 노동신문은 "모든 당원들은 우리 당 정책의 열렬한 지지자, 옹호자로서뿐 아니라 그 관철의 기수로서의 책임과 본분을 다해나가야 한다"[56]며 대중 선전·선동을 독려하고 있다. 이러한 북한의 정치문화를 고려할 때, 사이버전 기술은 체제선전을 위한 수단으로 활용될 가능성이 크다.

마지막으로 북한은 경제난의 지속으로 재래식 무기를 통한 군비경쟁에서 뒤처지고 있다. 컴퓨터 공학 교수 출신의 탈북자인 김흥광은 사이버전이 북한에게 다음과 같은 군사적 이점을 제공한다고 설명한다.[57] 첫째, 사이버전은 적은 비용으

---

[52] 『노동신문』, 2001년 5월 29일.

[53] 정성장, "'돈줄' 틀어쥐기 위해 군부 군기 잡기 나섰다," 『시사저널』, 1206호 (2012.11.29.), <http://www.sisapress.com/news/articleView.html?idxno=59345> (검색일: 2015.3.4).

[54] *YTN*, 2010년 5월 6일; 『연합뉴스』, 2014년 9월 10일.

[55] 통일교육원, 『북한이해 2012』, p. 224.

[56] 『노동신문』, 2014년 6월 23일.

[57] HP Security Research, "Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape," *HP Security Briefing Episode* 16 (August, 2014), p. 26.

로 군사적 도발을 가능하게 한다. 공격자가 분명하게 드러나는 통상적인 군사도발은 정치적 비난과 책임을 피할 수 없기 때문이다. 둘째, 사이버전은 포병 및 항공전력을 이용한 도발보다 실용적이다. 통상적인 군사도발을 위한 준비활동은 인공위성이나 기타 감시체계에 의해 신속하게 포착될 수 있기 때문이다. 셋째, 사이버전은 간첩 활동 및 심리전 수행을 위한 토대를 제공한다. 이에 따라 북한은 사이버전 기술을 이용한 군사적 도발을 지속할 것으로 보인다. 김정일은 죽기 전 "우리 인민군에 연유(연료)와 식량이 부족하지만 남조선 땅에만 가면 현지 조달이 가능하다. 남조선 땅만 밟으면 우리가 무조건 이긴다."[58]라고 밝힌 바 있다. 이는 북한이 남한의 국가 기반시설을 파괴의 대상이 아니라 이용 가능한 대상으로 파악하고 있음을 보여준다. 이에 따라 북한은 중국 및 러시아의 군사교리가 추구하는 것과 마찬가지로 북한은 대중교통, 전기, 통신망 등 국가 기반시설을 물리적으로 파괴하기 보다는 이들의 기능을 통합·관리하는 전산망의 마비를 목표로 사이버전을 수행할 것으로 예상할 수 있다.

<표 3> 북한의 사이버전 수행 목표

구분	북한 체제 특성	사이버전 수행목표
정치적 요인	3대혁명역량 강화	남한의 사회혼란 조성
경제적 요인	IT 산업 중심의 단번도약 전략	외화벌이
사회적 요인	선전선동 중시의 정치문화	체제선전
군사적 요인	재래식 군비경쟁의 열세	군사작전 방해, 국가기능 마비

북한 체제의 특성과 군사과학기술의 상호 작용을 고려할 때, 북한의 사이버전 수행목표는 <표 3>에 제시한 바와 같이 남한의 사회혼란 조성, 외화벌이, 체제선정, 군사작전 방해 및 국가기능 마비 등으로 요약할 수 있다.[59] 북한이 설정한 공격 목표와 지금까지 북한이 실시한 공격 양상을 고려할 때, 북한 사이버전의 기본 전략은 사이버 공간의 주요 특성인 광역성, 익명성, 비가시성을 중심으로 다음과 같이 추측해 볼 수 있다. 첫째, 광역성은 북한이 사이버 공간을 통해서 공격할 수 있는 대상이 매우 다양하고 한계가 없다는 의미이다. 이에 따라 북한은 인터넷을

[58] *Newdaily*, 2013년 11월 10일.
[59] 임종인 외, "북한의 사이버전력 현황과 한국의 국가적 대응전략," 『국방정책연구』, 제29권 4호 (2013), p. 15.

통해서 물리적 공간을 뛰어넘어 미국을 비롯한 남한의 주요 동맹국들에 대한 직접적인 공격을 가할 것으로 예상된다. 둘째, 익명성은 본인을 밝히지 않으면 사이버 공간의 활동 주체를 알아내기 힘들다는 특성을 말한다. 사이버전의 경우 공격의 주체를 은닉하기 용이하다. 따라서 북한은 자신들의 얼굴을 숨기고 남한과 주요 동맹국에 대한 체계적인 공격을 자행할 것으로 예상된다. 마지막으로 익명성이 국제적 비난에서 자유로워지는데 도움을 준다면 비가시성은 활동에서의 자유를 보장한다. 사이버 공격 또는 테러는 사전에 탐지가 거의 불가능하기 때문에 북한이 원하는 시간과 장소에서 도발을 일으킬 수 있다는 장점이 있다. 이에 따라 북한은 남한과 주요 동맹국의 취약점을 관찰하고 있다가 결정적인 시기에 공격을 가하는 지능형 지속가능 위협을 증가시킬 것으로 예상된다.

2. 북한의 사이버전 조직체계

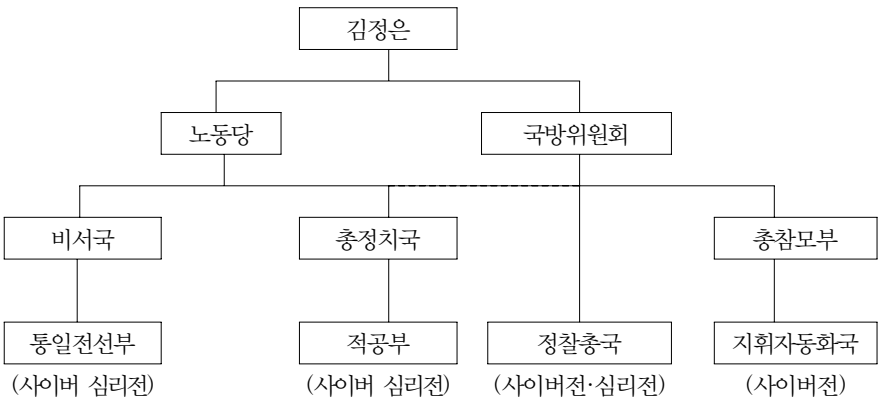
북한은 당이 다른 기관보다 우위에 있는 당 주도의 권력구조를 갖고 있다. 이에 따라 북한의 노동당 규약은 당 중앙군사위원회가 모든 군사사업을 조직·지도하는 것으로 명시하고 있다. 그러나 김정일 체제 출범 이후 국방위원회의 위상이 강화되고, 선군정치가 통치이념으로 제시됨에 따라 군부의 위상이 강화되고 있다. 특히 북한은 2009년 헌법 개정을 통해 국방위원회를 국가주권의 최고국방지도기관으로 규정하였다. 이러한 북한 체제의 특성은 북한의 사이버전 조직체계에도 영향을 미쳤다. 북한과 같이 당 주도의 국가체계를 갖고 있는 중국에서는 중국 공산당(중앙군사위원회) 직속의 총참모부가 사이버전 조직을 총괄하지만(<그림 1> 참조), 북한에서는 노동당과 국방위원회가 각각 사이버전 조직을 편성하고 있다.

북한의 사이버전 조직체계에 대한 분석은 연구자에 따라 일부 차이가 있지만 <그림 2>에 제시한 바와 같이 종합할 수 있다. 첫째, 노동당 비서국의 통일전선부는 대남사업의 핵심부서로 대남 심리전 및 통일전선 공작사업을 담당한다. 특히 통일전선부는 2012년 대남간첩공작 임무를 담당하는 225국을 흡수하여 '구국전선' 또는 '우리민족끼리'와 같은 웹사이트를 통해 북한 체제를 홍보하고 남한 사회 내에서 종북 세력을 확대하는 사이버 심리전을 담당하고 있다.[60] 둘째, 북한의 노

[60] 실제로 전직 공무원이 김정일에 충성을 맹세하는 글을 기고하고 '우리민족끼리'의 운영자와 연락을 주고받은 적도 있으며, 국제 해커집단인 어나니머스(Anonymous)는 2013년 '우리민족끼리'의 회원 9,000여 명의 신상을 공개하는 과정에서 1,800여 명이 국내 이메일 계정으로 가입했음을 밝히기도 하였다. 『조선일보』, 2014년 1월 7일; 『동아일보』, 2013년 4월 5일.

동당 규약은 “총청치국은 인민군 당 위원회의 집행부서로서 당 중앙위원회 부서와 같은 권능을 가지고 사업을 한다”[61]고 규정하고 있다. 총정치국 산하의 적군와 해공작부(적공부)는 적군의 전투의지를 무력화시키기 위한 선전, 선동, 삐라살포, 유인, 기만활동 등 사이버 심리전을 전담한다.[62] 김정은은 “적공일꾼들은 비가 오나 눈이 오나 사회주의 제도 옹위의 전초선을 믿음직하게 지켜가고 있다”고 격려하며 사이버 심리전의 중성을 강조한 바 있다.[63] 셋째, 국방위원회 직속의 정찰총국은 북한의 해외 공작활동을 총괄하는 기관이다. 정찰총국에는 일반 심리전을 담당하는 31·32소, 해커부대로 구성된 91소, 자료조사실, 기술정찰조, 110호 연구소 등 사이버전 조직이 편성되어 있다. 넷째, 총참모부 직속의 지휘자동화국은 해킹 및 통신 프로그램 개발을 담당한다.[64]

<그림 2> 북한의 사이버전 조직체계



북한 사이버전 지휘체계를 분석해보면 사이버 심리전과 관련된 기능이 중복적으로 편성되어 있다는 사실을 확인할 수 있다. 여기서 사이버 심리전이란, “사이버 공간에서 국가 정책의 효과적 달성을 목적으로 주체 측 외 모든 국가 및 집단

---

[61] 『조선노동당 규약(2010.9.28.)』, 49조.

[62] 연합뉴스는 임종인의 연구를 토대로 적공국은 총참모부 직속으로 파악하고 있다. 『연합뉴스』, 2013년 4월 10일 참고. 그러나 북한 원전에 따르면 적공국은 총정치국의 지휘를 받는다. 「조선로동당 중앙군사위원회지시 제002호’ 전시사업세칙을 내옴에 대하여」(2004년 4월 3일); 「조선로동당중앙위원회, 조선로동당군사위원회, 조선민주의 인민공화국 국방위원회, 조선인민군 최고사령부 공동명령 제002호」(2012년 9월, 보강된 전시사업세칙) 참고. 김성민, “무시무시한 조직... 북한 ‘적공국’을 아십니까,” 『조선 pub』, 2013년 11월 13일 재인용.

[63] 『노동신문』, 2013년 11월 12일.

[64] 『연합뉴스』, 2013년 4월 10일.

의 견해, 감정, 태도, 행동에 영향을 주는 선전 및 기타 모든 활동의 계획적 사용"[65]을 말한다. 적의 전투의지를 무력화하기 위한 심리전은 전쟁에서 빼놓을 수 없는 필수적인 요소이다. 그러나 통상 네트워크, 시스템, 정보자원 등을 공격 또는 방어의 대상으로 규정하는 사이버전의 정의에는 사이버 심리전이 포함되지 않는다. 그 이유는 무엇보다 대부분의 국가들이 잠재적 적국에 대한 실질적인 위협 수단으로 사이버 전력을 발전시켜왔기 때문인 것으로 보인다. 그러나 북한의 경우 남한에 대한 사이버 공격 외에도 남남(南南) 갈등을 조장하기 위한 수단으로 사이버 심리전의 중요성을 강조해왔다. 북한이 사이버전을 체계적이고 효율적으로 수행하기 위해 사이버전 관련 조직구조를 개편하면서 사이버 심리전을 강조하게 된 이유는 남한 사회의 혼란 조성과 체제선전을 사이버전 수행의 주요 목표로 설정하고 있기 때문인 것으로 보인다.

Ⅳ. 북한 사이버전의 가능성과 한계

1. 북한의 사이버전 수행능력

1990년대 이후 대부분의 국가에서 인터넷 이용자가 폭발적으로 늘어나고, 국가기반시설의 전산화가 이루어지면서 사이버전을 수행하기 위한 사이버 공간이 확대되었다. 이러한 현상을 잘 포착한 북한은 미래 전쟁에서 사이버전이 차지하는 중요성이 높아질 것이라고 예상하고, 사이버 전력을 강화하고 있다. 북한 노동신문은 "최첨단 과학기술 수단의 하나인 컴퓨터가 자본주의 나라에서 사람들에게 불안과 공포를 주는 파괴무기가 되고 있다"며[66] 사이버 위협을 강조하고 있다. 북한의 사이버전에 대한 관심은 1980년대부터 시작되었다. 특히 북한은 2003년 미군이 주도한 '사막의 폭풍작전' 이후 첨단 정보기술의 중요성을 인식하고, 사이버전 관련 기술을 본격적으로 개발하기 시작했으며, 사이버전 관련 기술 도입을 위해 중국, 러시아, 이란과 긴밀하게 협력하고 있다. 중국은 사이버전 기술 교육 외에도 서버, 라우터 등 하드웨어 제공을 통해 북한의 사이버전을 지원하고 있으며, 북한의 사이버전 부대인 전자정찰국(121국)이 심양(瀋陽)에서 임무를 수행할 수 있도록 협력하고 있다. 러시아는 프룬제 군사학교 출신 교수 25명을 파견하여 사

[65] 이상호, "북한 사이버 심리전의 실체와 대응방향," 『한국정치외교사논총』, 제33권 1집 (2011), p. 264.
[66] 『노동신문』, 2003년 4월 12일.

이버 전문가 양성교육을 지원하였고,[67] 전자파(EMP) 공격 기술과 인터넷 통제를 위한 기술 정보를 북한에 제공한 것으로 알려져 있다.[68] 이란은 2012년 북한과 기술교류협정을 체결하였으며, IT 기술 공유를 위한 학생 교환, 합동연구 등을 진행하고 있다.[69]

이러한 기술 도입을 토대로 북한의 사이버 공격은 점차 진화하는 모습을 보이고 있다. 사이버 공격의 유형은 이를 구현하기 위한 기술 수준에 따라 바이러스(virus)로부터 지능형 지속가능 위협(Advanced Persistent Threat, APT)으로 구분할 수 있다. 컴퓨터 바이러스와 웜(worms)은 다른 파일을 감염시키거나 변경하기 위하여 자기 자신을 복제하여 다른 컴퓨터에 전염시키는 프로그램을 말하고, 트로이 목마(trojans)는 감염된 PC를 원격 조정할 수 있어 분산서비스 거부 공격(Distributed Denial of Service, DDoS)을 가능하게 한다. 말웨어(Malware)는 시스템의 오작동 또는 마비 등을 목적으로 제작된 악성 소프트웨어(malicious software)를 말하고, 봇넷(botnets)은 말웨어에 감염되어 인터넷으로 연결되어 있는 PC를 말한다. 마지막으로 가장 높은 수준의 기술을 필요로 하는 APT 공격은 정부 또는 특정 기업의 정보를 취득할 목적으로 일련의 범죄 집단에 의해 이루어지는 지속적인 해킹 공격을 말한다. 북한은 바이러스, 인터넷 웜, 해킹, 디도스, 우회공격 및 역추적 방지기술, 해킹통신 암호화, 흔적삭제 등 발전된 소프트웨어를 보유하였으며, 하드웨어 측면에서도 GPS 전파 교란이 가능한 EMP(Electromagnetic Pulse) 무기 등을 개발하고 있다.[70]

<표 4> 북한 사이버 공격의 발전 추세

구분	Virus	Worms	Trojans	DDoS	Malware	Botnets	APT
기술수준	매우 낮음 ⬅			중 간	➡ 매우 높음		
대표적 공격사례	–	–	–	2009. 7. 7	2011. 4. 12	2009. 7. 7	2013. 3. 20

[67] 윤규식, "북한의 사이버전 능력과 위협 전망," 『군사논단』, 제68호 (2011), pp. 76~78.
[68] 『연합뉴스』, 2013년 10월 9일.
[69] 이에 대해서는 HP Security Research, "Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape," *HP Security Briefing Episode* 16 (August, 2014), pp. 42~44.
[70] 북한은 러시아로부터 GPS 전파교란 장비를 수입하여, 최근 3년 동안 세 차례에 걸친 GPS 전파 교란을 실시하였고, 그 결과 항공기 1,137대, 함정 4척, 선박 225척, 어선 36척 등 총 1,402대에 피해를 발생시킨 것으로 나타났다. 『연합뉴스』, 2014년 12월 24일.

2009년 기무사령부의 보고에 따르면 군 전산망에 대한 해킹 시도는 하루에 95,000여 건에 달하는 것으로 나타났으며, 이 가운데 바이러스 유포가 전체의 86%를 차지하여 가장 높은 비율을 나타냈다.[71] 그러나 최근 들어 북한의 사이버 공격 양상은 복합적인 형태로 전개되고 있다. 2009년 7월 7일에는 청와대, 백악관, 주요 포털 사이트를 대상으로 하여 DDoS 공격이 실시되었다. 하지만 DDoS 공격은 심각한 위협으로 간주되지 않는다.[72] 실제로 북한의 공격에 의한 피해는 홈페이지 접속이 일시 제한되고, 웜에 감염된 PC 중 일부에서 하드디스크가 파괴되는 정도에 불과했다.[73] 따라서 7·7 DDoS 공격의 주된 목적은 향후 추가적인 공격을 수행하기 위해 필요한 봇넷의 규모를 알아보기 위한 것이라는 주장이 제기되기도 하였다.[74] 반면 2013년 3월 20일에 발생한 APT 공격은 KBS 등 방송사와 농협 등 금융사의 내부 시스템 파괴를 목적으로 했다는 점에서 심각한 위협이 되었다. 2011년 4월 12일에는 은밀하게 악성 코드를 심어 놓은 PC를 통해 농협 전산망에 접근하여 서버를 파괴하는 공격이 발생하였다. 북한의 사이버 공격의 양상을 볼 때, 북한은 최고 기술 수준의 사이버 공격을 실행할 수 있는 다양한 전술을 개발하는데 성공했을 것으로 보인다. 그러나 이러한 기술적 성과에도 불구하고 북한의 사이버전 수행을 제한하는 다양한 요인들이 존재한다. 따라서 북한의 사이버전은 이러한 환경에 대응하면서 최적의 효과를 발휘할 수 있는 방향으로 발전할 것이다.

2. 사이버전 능력 제한요인과 사이버 심리전 위협

북한의 사이버전 수행을 제한하는 요인은 북한을 둘러싼 정치, 경제, 사회, 군사적 환경 속에서 찾아볼 수 있다. 첫째, 중국에 대한 북한의 의존성은 북한의 사이버전 수행을 제한하는 정치적 요인이다. 인터넷 기반시설이 부족한 북한은 사이버 전사들의 실제 훈련과 작전을 중국의 주요 도시에서 진행하고 있다. 중국을 경유한 북한의 사이버 공격은 익명성으로 인해 이에 대한 책임을 회피할 수 있다는 장점이 있다. 그러나 최근 자국 이익을 중심으로 재편되고 있는 북중 관계를 고려하면 중국은 국제사회의 비난을 자초하면서 북한의 사이버전을 지원하지 않을 것으로 보인다. 따라서 북한의 사이버 공격이 미국 또는 한국과의 관계를 악화시키

---

71 『SBS뉴스』, 2009년 6월 16일.
72 리처드 블라크·로버트 네이크, 이선미 역, 『해커 공화국』 (서울: 에이콘, 2013), p. 43.
73 『연합뉴스』, 2009년 7월 9일자.
74 블라크·네이크, 『해커 공화국』, p. 62.

거나 2014년 4월에 발생한 GPS 교란공격과 같이 불특정 다수 국가에게 피해를 발생시키는 결과를 초래한다면 중국은 자국 영토 내에서 이루어지는 북한의 사이버 공격을 묵인하지 않을 수도 있다. 한국 정부가 북한의 GPS 전파교란 공격에 대해 중국과 방지책을 논의한 사실이 이러한 전망을 뒷받침한다.[75]

둘째, 경제적으로 낙후한 북한에는 사이버 인프라가 거의 구축되지 않았다고 보아도 과언이 아니다. 인프라의 미비는 사이버 방어에 유리하기 때문에 북한의 사이버 전투력을 높게 평가하는 이유로 제시되기도 한다. 그러나 북한의 경제난은 사이버전 능력을 크게 제한할 수 있는 요인이다. 클라우제비츠(Karl V. Clausewitz)는 보편적 정신교양 수준이 높은 국민이 군사적 경향을 강하게 지닐 때 수준 높은 군사적 천재가 태어난다고 설명한다.[76] 대부분의 북한 주민들은 정권의 안정을 유지하기 위해 외부 사회와 차단된 채 살아간다. 따라서 북한에서는 사이버 공간에 대한 국민들의 보편적 이해가 형성될 수 없고, 사이버전을 주도할 군사적 천재도 태어날 수 없다. 세계 최고 수준의 사이버 공격 능력을 보유한 것으로 평가되는 중국에는 4억 5천 7백만 명 규모의 네티즌이 있으며, 이들 중 일부는 해커로 활동하면서 중국의 국익 또는 개인의 이익을 위한 사이버 공격에 자발적으로 가담하고 있다.[77]

셋째, 정부 주도의 북한 사이버전 교육체계는 사이버전의 효율적 수행을 저해할 수 있는 사회적 요인이다. 북한에서는 1995년 시·군·구역마다 영재학교를 설치하여 선발된 우수 학생들을 프로그래밍과 컴퓨터 하드웨어를 교육시키는 금성중학교 컴퓨터 영재반에 진학시키고, 졸업 후에는 평양의 지휘자동화대학에 진학시켜 네트워크 시스템 해킹 기술을 집중적으로 가르치는 것으로 알려졌다.[78] 외국 기술을 모방·추월을 목표로 하는 정부 주도의 기술발전 전략은 단기적으로 상당한 실력을 갖춘 사이버 전사를 양성하는데 효율적일 수 있으나, 민간 영역에서 신속하게 변화하는 다양한 기술발전의 추세를 따라잡을 수 없다. 따라서 북한의 사이버 전사들은 혁신적인 기술을 개발하기 보다는 기존 기술을 습득·운용하는데 치중할 가능성이 크기 때문에 북한은 사이버전 기술 경쟁에서 수세적 위치에 처하게 될 가능성이 크다. 북한이 사이버전 기술 도입을 위해 긴밀하게 협력하고 있는 중국의 사이버 방어능력이 현격하게 떨어진다는 점 역시 북한 사이버전 수행능력의

---

[75] *Daily NK*, 2012년 5월 18일.
[76] 클라우제비츠, 강창구 역, 『전쟁론 上』 (서울: 병학사, 1991), p. 74.
[77] Desmond Ball, "China's Cyber Warfare Capabilities," pp. 93~94.
[78] 블라크·네이크, 『해커 공화국』, p. 60.

한계로 작용할 수 있다. 중국은 세계적인 수준의 사이버전 능력을 갖추었지만, 다른 한편으로는 세계 최대의 해킹 피해국으로 알려져 있다. 2011년 중국의 정부 보고서에 따르면 2010년에 4,600개의 정부 관련 홈페이지의 내용이 해커에 의해서 무단으로 변경되었으며, 이는 이전에 비해 68% 증가한 수치이다.[79]

넷째, 사이버 방어능력 향상을 위한 한국의 지속적인 노력은 북한의 사이버전 능력을 약화시키는 군사적 요인이 될 수 있다. 한국 국방부는 2009년 7·7 DDoS 공격을 계기로 효율적인 사이버전 수행을 위해 2010년 국군 사이버 사령부를 창설하였고, 합참은 2014년 사이버작전과를 신설하여 사이버 침해 행위에 대한 관제 위주의 사이버 작전을 전투임무 위주로 전환하고, 공격·방어용 사이버 무기체계를 개발할 것이라고 밝혔다.[80] 또한 2014년부터 한미 국방 사이버정책실무 협의회를 개최하여 사이버 정책·전략·교리·인력·교육훈련 분야에서 다양한 협력을 강화하고 있다.[81] 북한의 전략문화 역시 북한의 사이버전 능력을 제한할 수 있다. 북한의 전략문화는 구소련 군사교리의 영향으로 조직 운용의 융통성이 떨어지는 문제를 안고 있다. 특히 중간급 장교들에게 권한을 부여하지 않기 때문에 이들은 스스로 판단하고 결심할 수 있는 자율성을 갖고 있지 못한 것으로 평가받고 있다.[82] 따라서 강력한 통제를 원칙으로 하는 북한군의 조직문화는 정보화 시대에 요구되는 수평적 협력문화를 만들어내지 못할 것으로 보인다.

북한의 사이버 심리전은 이러한 제약을 상대적으로 적게 받으면서 남한 사회를 위협할 수 있다. 첫째, 북한은 사이버전 기술시스템을 도입, 검증·시험, 공고화하는 과정에서 조선노동당과 국방위원회의 대남공작기구들에 사이버 심리전 임무를 중복 편성하고 있다. 이는 북한의 사이버전 수행체계에서 사이버 심리전이 매우 중요한 위치를 차지한다는 것을 의미한다. 둘째, 익명성이 보장되는 사이버 공간의 특성에도 불구하고, 북한이 사이버 공격의 배후에 있다는 사실이 밝혀지게 된다면 북한에 대한 국민적 경각심이 한층 높아지는 계기가 될 수 있다. 그러나 상대 국가의 국가기반시설에 직접적인 타격을 가하지 않는 사이버 심리전의 경우 사이버 공격과 달리 공격 행위자와 이를 방조한 국가에 대한 국제사회의 제재와 비난을 기대하기도 어렵다. 셋째, 북한의 사이버 심리전은 남한 정권의 정당성을

---

79 *Bloomberg*, March 10, 2011.
80 『연합뉴스』, 2014년 12월 23일.
81 위의 책, p. 54.
82 Axel Berkofsky, "North Korea's Military-What Do They Have, What Do They Want?" *ISPI Analysis*, No. 161 (March 2013), pp. 4~5.

직접적인 공격 목표로 삼고 남한 사회 내에서 정치적 혼란을 유발할 수 있다. 이를 위해 북한은 SNS, 블로그, 인터넷 카페 등을 통해 왜곡된 정보 또는 루머를 손쉽게 확산시킬 수 있다. 마지막으로 인터넷 통제의 필요성에 대한 일반 국민들의 동의를 얻기 힘들기 때문에 북한의 심리전 활동을 차단하는 것이 쉽지 않은 현실이다.

Ⅴ. 결론 및 정책적 함의

본고에서는 사이버전 수행능력을 중심으로 북한 군사변혁의 가능성과 한계를 검토해보았다. 북한은 재래식 군비경쟁의 열세를 만회하기 위해 대량살상무기 등을 활용한 비대칭 억지전략을 발전시켜왔다.[83] 특히 상대적으로 적은 경제적 부담으로 남한의 통신망, 금융망, 전력망 등 국가 기간시설에 심각한 피해와 혼란을 일으킬 수 있는 사이버전은 북한의 선택할 수 있는 매력적인 전쟁 수단이다. 그러나 이러한 장점에도 불구하고 북한의 정치·경제·사회·군사적 조건은 북한의 사이버전 수행능력에 일정 부분 제한을 가할 것으로 분석되었다. 첫째, 북한의 모든 사이버전 조직은 대남 심리전 업무를 중복 편성하고 있으며, 이러한 조직적 특성은 체계적이고 통합된 임무 수행을 제한할 수 있다.[84] 둘째, 심각한 경제난으로 인해 인터넷 인프라가 미비한 북한에서는 인터넷 활용 인구가 부족하여 혁신적인 사이버전 기술 개발이 제한될 것으로 보인다. 셋째, 정부 주도로 외국의 사이버 기술을 도입하는 교육정책으로 인해 북한은 사이버 방어 능력이 매우 취약한 중국의 문제를 답습하게 될 것으로 예상된다. 마지막으로 북한 사이버전 기술의 효율성은 한국의 사이버 방어능력 강화와 국제 공조 등을 통해 감소할 것으로 보인다.

본고의 분석결과는 북한의 사이버전에 대한 대응을 위해 다음과 같은 정책적 함의를 제공한다. 첫째, 북한의 사이버전 능력을 정확하게 파악하고 이에 대처하려는 노력이 필요하다. 중국 연구자들은 미국의 정치·군사적 필요에 의해서 중국의 사이버전 능력이 과대평가되는 경향이 있다고 주장한다.[85] 이러한 비판은 북한

[83] 통일교육원, 『북한이해 2012』, p. 100.
[84] 이에 대해서는 중국의 사례를 참고할 것, U.S.-China Economic and Security Review Commission (USCC), *2008 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington D.C.: U.S. Government Printing Office, 2008), p. 164.
[85] Magnus Hjortda, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *Journal of Strategic Security*, Vol. 4, No. 2 (Summer 2011), pp. 12~13.

에도 적용될 수 있다. 예를 들어 사이버 보안 문제를 다루는 미국의 테크놀릭틱스 연구소(Technolytics Institute)는 북한의 사이버 공격 능력을 세계 6위로 평가하였다.[86] 이러한 분석결과는 사이버전 기술의 선진국인 미국, 이스라엘, 중국, 러시아, 이란을 제외하고 북한이 세계 최고 수준의 사이버 공격 능력을 보유하고 있다는 것을 의미한다. 그러나 다른 전문가들은 사이버전 능력을 평가하기 위해서는 예산, 첨단 소프트웨어, 인력, 지원 시설이 종합적으로 고려되어야 하기 때문에 북한의 사이버 위협에 대한 평가는 과장되었다고 주장한다.[87] 미국의 오바마 대통령은 2015년 2월 17일 북한의 사이버전 능력이 매우 뛰어난 수준이 아니라고 평가하였다.[88] 실제로 오바마 대통령이 2014년 12월 23일 '소니 픽처스 엔터테인먼트' 해킹 사건의 배후로 북한을 지목하고, 비례적 대응방침을 밝힌 지 3일 만에 북한의 인터넷망이 마비되는 사태가 발생하였다.[89] 따라서 사이버사령부 등 새로운 조직의 창설과 유지, 예산 확보 등의 목적으로 북한의 사이버 전력을 지나치게 과장되는 것은 아닌지 엄밀하게 검토해볼 필요가 있다.

둘째, 북한 사이버전 능력의 한계를 효과적으로 활용하기 위한 대응책 마련이 필요하다. IT 인프라가 부족한 북한은 중국을 근거지로 사이버 공격을 감행하는 것으로 알려져 있다. 그러나 북한 외에도 많은 해커들이 중국을 경유한 사이버 공격을 시도함에 따라 중국은 국제사회로부터 사이버 공격의 온상으로 비난받고 있다.[90] 특히 국제사회에서는 사이버 공격을 방조한 국가에 대해서도 책임을 물어야 한다는 주장이 힘을 얻고 있다. 실제로 미국은 "당신 집 지하실에 방화범이 한 사람 있다. 그리고 그 사람이 매일 밤마다 밖으로 나와 이웃의 집에 불을 지르는데 당신이 이런 일을 알고 있다면 당신에게 책임이 없다는 주장을 할 수 없다"[91] 라는 논리를 제기하며 테러리스트의 활동을 묵인하는 외국 정부에 대해 책임을 물어야 한다고 주장하고 있다. 한국 정부는 사이버 위협에 대한 국제사회의 공동대응을 위해 2013년 10월 87개 국가, 18개 국제기구가 참가한 '세계 사이버스페이스 총회'를 개최하여 국제 공조체제를 강화하고 있다.[92] 따라서 중국이 해킹 방지를 위한 국제협력에 동참하도록 유도한다면 북한의 사이버 위협을 크게 약화시킬

---

[86] *The Science Times*, 2014년 5월 15일.
[87] *The Voice of America*, 2015년 2월 27일.
[88] 『연합뉴스』, 2015년 2월 18일.
[89] 『한겨레』, 2014년 12월 23일.
[90] Magnus Hjortda, "China's Use of Cyber Warfare," p. 12.
[91] 블라크·네이크, 『해커 공화국』, p. 333.
[92] 국방부, 『국방백서 2014』 (서울: 국방부, 2014), p. 11.

수 있다.

셋째, 모스코스(Charles C. Moskos)는 산업사회에서 탈근대사회로 사회 변화가 일어나면서 군인들에게는 기술자 또는 관리자로서의 자질 보다 정무(政務)적 감각이 중요해졌다고 설명한다.[93] 언론의 자유와 북한의 위협을 통제하기 위한 정부의 개입이 서로 양립할 수 없는 것처럼 불협화음을 일으키고 있는 남한 사회의 현실을 고려할 때, 군의 정치개입 의혹을 불식시키면서 북한의 심리전에 효율적으로 대응할 수 있는 방안이 모색되어야 한다. 사이버 심리전으로 인한 가장 큰 위협은 정부와 군의 정당성을 훼손시키는 왜곡된 정보의 확산이다. 북한 역시 이러한 위협을 잘 인식하고 있으며, 이에 따라 북한 노동신문은 "제국주의자들의 사상문화적 침투와 심리전에 경각성을 높이고 우리의 사상과 도덕, 생활양식을 견결히 지켜 나가야 한다"[94]고 강조한 바 있다. 기존 연구에 따르면 루머의 확산을 막기 위해서는 일반 국민들이 현재의 상황을 정확하게 알 수 있도록 적절한 정보를 제공하거나 제기된 의혹을 논리적 근거를 제시하며 적극적으로 반박해야 한다.[95] 고의로 루머를 확산하는 사람에 대한 처벌을 강화하는 것 역시 루머의 확산 방지에 효과적이다.[96] 이러한 연구결과를 고려하면 북한의 심리전에 대한 대응은 보다 적극적인 정보공개 정책과 루머 확산의 책임자에 대한 처벌 규정을 강화하는 방향으로 개선되어야 할 것으로 보인다.

마지막으로 본 연구의 한계를 지적하지 않을 수 없다. 본고는 과학기술 사회학의 주요 이론인 기술시스템론을 적용하여 북한이 새롭게 도입한 사이버전 기술이 북한 고유의 정치·사회·경제·군사적 조건과 맞물려 어떠한 형태로 공고화되었는지를 살펴보았다. 이러한 분석이 효과적으로 이루어지기 위해서는 북한의 사이버전 수행체계를 다른 국가의 사이버전 수행체계와 비교하는 연구가 진행되어야 한다. 그러나 폐쇄성을 특징으로 하는 북한 연구와 군사 연구의 특성상 신뢰성 있는 자료를 확보하는 것은 쉽지 않은 일이다. 이로 인해 북한의 정치·사회·경제·군사적 조건과 사이버전 기술이 상호작용하는 과정에 대한 비교 분석이 이루어지지 못했다는 점을 인정하지 않을 수 없다. 그러나 이러한 한계에도 불구하고, 북한

---

[93] Charles C. Moskos, "Toward a Postmodern Military: The United States as a Paradigm," Charles C. Moskos, John Allen Williams, and David R. Segal (eds.), *The Postmodern Military: Armed Forces after the Cold War* (New York, NY: Oxford University Press, 2000), p. 15.

[94] 『노동신문』, 2003년 6월 19일.

[95] 니콜라스 디폰조, 곽윤정 역, 『루머사회』 (서울: 흐름출판, 2012), p. 235.

[96] *Ibid.*, p. 248.

고유의 특성으로 인해 대남 사이버 심리전을 중시하는 형태의 사이버전 수행 교리와 조직체계가 형성되었다는 사실을 밝힌 것은 이 연구의 중요한 성과라고 할 수 있다.

■ 접수: 3월 4일 ■ 심사: 5월 13일 ■ 채택: 6월 17일

참고문헌

1. 단행본

국방부. 『Defense Reform 2020: 국민과 함께 미래를 향해』. 서울: 국방부, 2005.
_____. 『국방백서 2014』. 서울: 국방부, 2014.
김재호. 『김정일 강성대국 건설전략』. 평양: 평양출판사, 2000.
니콜라스 디폰조, 곽윤정 역. 『루머사회』. 서울: 흐름출판, 2012.
로렌스 손드하우스, 이내주 역. 『전략문화와 세계 각국의 전쟁 수행 방식』. 서울: 육군사관학교 화랑대연구소, 2007.
리처드 블라크·로버트 네이크, 이선미 역. 『해커 공화국』. 서울: 에이콘, 2013.
앨빈 토플러, 이상백 역. 『제3의 물결』. 서울: 영광출판사, 1991.
_____, 이계행 감역. 『전쟁과 반전쟁』. 서울: 한국경제신문사, 1994.
엄정호·최성수·정태명. 『사이버전개론』. 서울: 홍릉과학출판사, 2012.
온만금·김인수. 『군대와 사회』. 서울: 육군사관학교 화랑대연구소, 2005.
육군사관학교. 『세계전쟁사』. 서울, 일신사, 1995.
_____. 『북한학』. 서울: 황금알, 2004.
이장규·홍성욱. 『공학기술과 사회: 21세기 엔지니어를 위한 기술사회론 입문』. 서울: 지호, 2006.
윌리엄 맥닐, 신미원 역. 『전쟁의 세계사』. 서울: 이산, 2005.
죤 하키트, 서석봉·이재효 역. 『專門職業軍』. 서울: 연경문화사, 1989.
클라우제비츠, 강창구 역. 『전쟁론 上』. 서울: 병학사, 1991.
통일교육원. 『북한이해 2012』. 서울: 통일연구원, 2012.
홍현필·이용환. 『기술과 사회』. 서울: GS 인터비전, 2011.
황진환 외. 『신국가안보론』. 서울: 박영사, 2014.

Boyer, Yves. “The American Revolution in Military Affairs: A French Perspective.” Thierry Gongora and Harald von Riekhoff (eds.). *Toward A Revolution in Military Affairs: Defense and Security at the Dawn of the Twenty-first Century.* Westport, CT: Greenwood Press, 2000.

Department of Defense. *Department of Defense Performance and Accountability Report FY 2006.* Washington D.C.: U.S. Department of Defense, 2006.

Ertman, Thomas. "State Formation and State Building in Europe." Thomas Janoski, Robert Alford, Alexander Hicks, and Mildred A. Schwartz (eds.). *The Handbook of Political Sociology.* New York, NY: Cambridge University Press, 2005.

Hundley, Richard O.. *Past Revolutions, Future Transformation.* Santa Monica, CA: National Defense Research Institute RAND, 1999.

Janowitz, Morris. *The Professional Soldiers: A Social and Political Portrait.* New York, NY: The Free Press, 1970.

Kipp, Jacob W. "The Labor of Sisyphus: Forecasting the Revolution in Military Affairs During Russia's Time of Trubles." Thierry Gongora and Harald von Riekhoff(eds.). *Toward A Revolution in Military Affairs: Defense and Security at the Dawn of the Twenty-first Century.* Westport, CT: Greenwood Press, 2000.

Marx, Karl. *The Poverty of Philosophy*. NY: International Publisher, 1971.

Moskos, Charles C.. "Toward a Postmodern Military: The United States as a Paradigm." Charles C. Moskos, John Allen Williams, and David R. Segal (eds.). *The Postmodern Military: Armed Forces after the Cold War.* New York, NY: Oxford University Press, 2000.

Robert, Michael. *The Early Vasas: A History of Sweden, 1523-1611.* New York, NY: Cambridge University Press, 1968.

Rogers, Clifford J. "Military Revolution and Revolutions in Military Affairs: A Historian Perspective." Thierry Gongora and Harald von Riekhoff (eds.). *Toward A Revolution in Military Affairs: Defense and Security at the Dawn of the Twenty-first Century.* Westport, CT: Greenwood Press, 2000.

U.S.-China Economic and Security Review Commission (USCC), *2008 Report to Congress of the U.S.-China Economic and Security Review Commission,* Washington D.C.: U.S. Government Printing Office, 2008.

2. 논문

박휘락. "국방개혁 2020과 미군 "변혁"(Transformation)의 비교와 교훈: 변화방식을 중심으로."『평화학연구』. 제13권 3집 (2012), pp. 167~168.

윤규식. "북한의 사이버전 능력과 위협 전망."『군사논단』. 제68호 (2011년, 겨울).

이상호. "북한 사이버 심리전의 실체와 대응방향."『한국정치외교사논총』. 제33권 1집 (2011).

임종인 외. "북한의 사이버전력 현황과 한국의 국가적 대응전략."『국방정책연구』. 제29권 4호 (2013).

Aschmann, Michael, Joey Jansen van Buuren, and Louise Leenen. "Cyber Armies: The Unseen Military in the Grid." *The Proceedings of the 10th International Conference on Cyber Warfare and Security.* Vol. 24, Feb 2015.

Axel Berkofsky. "North Korea's Military-What Do They Have, What Do They Want?" *ISPI Analysis,* No. 161, March 2013.

Ball, Desmond. "China's Cyber Warfare Capabilities." *Security Challenges.* Vol. 7, No. 2, Winter 2011.

Hjortda, Magnus. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." *Journal of Strategic Security.* Vol. 4, No. 2, Summer 2011.

HP Security Research. "Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape." *HP Security Briefing Episode,* Vol. 16, August 2014.

McNeil, Daniel. "Technology, History and the Revolution in Military Affairs." *Canadian Military Journal.* Winter, 2000/2001.

Møller, Bjørn. "The Revolution in Military Affairs: Myth or Reality?" *COPRI Working Paper Series.* Vol. 15, 2002.

Murray, Williamson. "Thinking about Revolutions in Military Affairs." *Joint Force Quarterly.* Summer 1997.

Stephenson, Scott. "The Revolution in Military Affairs: 12 Observations on an Out-of-Fashion Idea." *Military Review.* May-June 2010.

3. 기타자료

『노동신문』.
『동아일보』.
『조선노동당 규약』.
『조선일보』.
『조선 pub』.
『연합뉴스』.
『한겨레』.
Daily NK.
Newdaily.
『SBS뉴스』.
The Science Times.
The Voice of America.
YTN.
Bloomberg.

Abstract

North Korea's Cyber Warfare Capabilities:
Assessment and Prospects

In-Soo Kim and KMARMA

North Korea is recently strengthening the cyber threat toward South Korea, praising the cyber warfare as an omnipotent precious sword. In order to respond to this threat effectively, it is essential to evaluate North Korea's cyber warfare capabilities. However, this is not a easy work because introducing new military technology is under influence of social structure and culture, which is peculiar to the North Korean society. On the basis of the technological system theory, we examine how cyber warfare technologies have been adapted to North Korea's political, social, economic, and military environment. Results show that North Korea's environments made North Korean military develop the technological system, which gave a priority to cyber-psychological warfare. At least, three factors—North Korea's strong emphasis on propaganda and agitation, retarded infra-structural development, and high level of technological dependence on China—could cause a direct or indirect effect on North Korea's cyber-warfare technology system in the middle of introducing, validating, testing, and consolidating new technologies of cyber warfare. If it is taken into account that there is a controversy over the surveillance of internet communication by South Korean government, findings imply that it is urgent to look for ways to counter North Korea's cyber-psychological warfare capabilities effectively.

Keyword: North Korea, RMA, Technological System Theory, Cyber Warfare Capability, Cyber-Psychological Warfare