**융합안보연구논총** | 2025년 제1권 제1호 | pp. 7~56

논문 1

# 북한 대남 사이버 공격 전술의 변화 발전과 대응*

김준섭**
(사단법인 통일안보융합연구원 원장)

**초록**

21세기는 새로운 안보환경의 중심으로 변화된 사이버공간(Cyber space)이 모든 국가의 절대적 안전보장의 필수 불가결한 영역으로 자리 잡았다. 이러한 사이버공간은 새로운 형태의 안보환경에 평시와 전시를 구분하지 않는 핵심 전장이 되었다.

본 연구는 북한 대남 사이버 전략과 전술의 지속성과 변화를 평가하고 분석하였다. 즉, 분단 이후 김정일·김정은 시기의 '대남 사이버 전술'의 공통점과 차이점 특히, 김정은 시대의 지능화된 사이버(Cyber) 활동 기반의 '하이브리드(Hybrid) 사이버전술'을 전통방식의 전술과 비교함으로써 북한의 대남 사이버 공작전술의 변화를 추적하였다.

해방 직후 조선공산당 지도자였던 김일성은 남조선 혁명에 있어서 '통일전선전술'의 중요성을 강조하고 체계화하였으며, 현재까지도 북한은 「조선로동당규약」을 통해서 전조선의 공산화 통일 혁명 달성의 목표를 견지하고 있음을 보여주고 있다.

김정일 시대 '대남 통일전선전술'은 2000년대 남한의 정보통신 발전과 인터넷 사이버 환경 급성장의 흐름에 편승 사이버공간을 활용한 사이버 공격 전술을 전개하였다. 특히, 2009년 2월 대남 및 해외 공작업무를 담당하던 노동당 35호실과 작전부를 당에서 분리하여 인민무력부의 정찰국과 통합하였다. 사이버 조직을 확대한 통합 무력 조직인 정찰총국을 출범하고 국방위원장이 직접 지휘하는 독립적인 대남 공작조직 체계를

* 이 논문은 2022년 국가정보학회(국가정보연구 제15권 2호) 학술지 게재 논문을 수정 편집한 논문임.

** 前) 동국대학교 북한학연구소 객원연구원, 現) 북한연구학회 이사, 現) 21C안보전략연구원(통일북한연구센터장), 現), 국민대학교 글로벌평화·통일대학원 겸임교수, (사)통일안보융합연구원 원장, iusc2024001@gmail.com

구축한 것이다.

김정은 시대의 대남 통일전선전술은 선대의 기조를 유지하면서 발전된 정보통신기술을 활용한 '하이브리드 사이버 전략 전술'을 보여주고 있다. 대남 하이브리드 사이버 전술은 사이버부대 등의 전담 조직을 확대하고 심리전·선전선동 웹사이트 운용, 사이버 해킹 공격, 인터넷(사이버) 공간의 사이버드보크, 스테가노그라피 간첩연락통신, 사이버 공간에서의 대남 공작활동 전개 등을 통해 지속적이고 확대된 공세적인 활동의 증가로 나타났다.

따라서 본 연구는 김정은 시대에 지능화·고도화 발전 추세에 있는 북한의 사이버 전략과 공작 전술을 시대적 발전 배경을 바탕으로 분석하여 그 특징을 고찰한 결과 북한의 사이버전 수행 능력과 예상되는 대남 사이버전 전략과 위협을 도출하였다는 것에 의미가 있으며, 우리의 효과적인 국가 사이버안보 전략과 정책 방안 마련의 방향을 제언하고자 한다.

**주제어 : 북한 사이버 전략, 북한 사이버 조직, 대남 사이버 공작전술, 사이버 심리전, 하이브리드 사이버 전술, 사이버 간첩 연락통신 기술**

## 목차

# Ⅰ. 서론

본 연구의 목적은 북한 사이버 전략과 전술의 탄생 배경과 지도자의 시기별 전개 내용에 차이가 있을 것임을 예상하며 그 지속과 변화가 어떤 특징을 가지는지 밝히고, 북한 사이버 전략의 태동과 시대적 전술 전개 내용의 주요 특징을 확인하여 김정은 시대의 사이버 전략 전술 지속과 변화의 한계와 실체를 확인하는데 주목적이 있다. 즉, 김정일·김정은 시기의 공산주의 대남 혁명전략 기조를 시작으로 전통 방식에서 사이버 방식으로의 변화한 대남 사이버 전술을 분석하는 것이다. 특히, 김정은 시대의 고도화된 사이버공간(Cyber Space) 활동 기반의 하이브리드(Hybrid)[1] 사이버 공작 전술을 전통 방식 전술과 비교함으로써 북한 사이버 공작 전술의 변화를 추적하였다.

남한과 북한은 한국전쟁 휴전 이후 69년 동안 정전 상태로 현재까지 대치 중이며 지상과 공중·해상을 이용한 도발과 무력 충돌이 지속되고 있다. 2012년 김정은 집권기 이후 북한은 사이버전(사이버 공격, 해킹, 테러, 사이버 심리전 등)의 전개를 강화하고 있다. 이러한 사이버 전술은 인터넷 공간의 비닉성을 활용하여 대한민국 정부 기관과 주요 기간산업의 전산시스템을 마비시켜 혼란 정국을 조성하려는 사이버 공작 전술로 비대칭 전략무기인 핵·미사일과 대등한 만능의 보검이라고 칭할 정도로 북한은 사이버 전력과 전술을 3대 핵심전략 전쟁 수단의 하나로 인식하고 빠른 속도로 발전시키고 있다.

특히, 북한은 사이버공간을 이용한 대남 사이버 공작전술 활동을 전개하여 한국의 국가안보를 심각하게 위협하고 있다. 북한의 이러한 사이버 공작전술 위협 강화전략은 대한민국이 컴퓨터 정보통신체계를 기반으로 하는 네트워크 사회시스템

1) "하이브리드(hybrid)"는 특정한 목표를 달성하기 위해 두 개 이상의 요소가 합친 개념으로 원래 이질적인 요소가 서로 섞인 것으로 이종(異種), 혼합, 혼성, 혼혈이라는 의미를 지닌다. 일반적으로 아날로그와 디지털을 합치면 '하이브리드'라고 일컫는다. 전통방식과 사이버기술융합 혼합방식의 북한 3세대 통일전선 전술의 의미로 "김정은 시대 공산주의 전통방식과 사이버 방식을 배합한 신(新) 개념의 통일전선 전술"을 총칭하는 용어로 연구자가 명명하였다.

기반이 조성되어 있기 때문이다. 이러한 사이버 환경은 새로운 전술 용어인 사이버 공격, 사이버전, 네트워크전, 사이버 정보전 등을 탄생시켰다.

사이버전(Cyber Warfare)은 적국의 컴퓨터 시스템에 침투시킨 바이러스를 통해 주요 전산망을 공격하여 무력화시키고, 내부에 탑재된 기밀정보를 탈취하며, 시스템을 장악하여 심리전을 펼치는 전술의 포괄 개념이다. 북한의 김정은 시대는 이러한 대남 사이버전을 수행하는 조직의 전력을 확대하고 전술을 광범위하게 전개하고 있다. 사이버테러나 사이버전은 더 이상 가상의 전장 상황이 아닌 현실에서 작용하고 있는 실체적인 안보 위협의 상황으로 상대 적국의 군사 지휘 체계와 정부 네트워크, 금융 네트워크, 통신네트워크 등 국가의 주요 기능을 무력화시키는 전쟁개념으로 발전되고 있다.

따라서 사이버전이 국가안보와 방위에 심각한 영향을 미치기 때문에 세계 주요 선진국들은 미래 사이버 전쟁에 대비한 전문인력의 양성과 사이버전을 지휘하는 시스템과 사이버전 전담 전략부대 창설과 확대를 통해 사이버전 수행 능력을 강화해 나가고 있다. 이 대목에서 대한민국의 사이버전을 대비한 국가 사이버안보의 전략과 정책은 선진국에 대비해 현재 초보적인 수준으로 미흡한 실정이다.

본 연구는 북한 사이버 전력의 실체를 확인하고 변화 발전된 대남 사이버 공작 전술의 위협과 방향을 도출한 결과를 토대로 국가 차원의 효율적인 대응 방안을 제시하고자 한다.

# Ⅱ. 현대의 사이버전

## 1. 사이버전의 개념

정보화가 진전됨에 따라 대부분의 인간 활동은 컴퓨터와 인터넷을 기반으로 사이버 공간에서의 활동으로 급속도로 전환 되었다. 이러한 환경의 변화는 삶의 질과 발

전 속도를 상승 시켰지만 그와 비례하여 여러 가지 피해를 양산하는 부작용도 급속도로 발생하고 있다.

사회의 모든 구성 요소들은 컴퓨터 네트워크를 기반으로 연결되게 되고 네트워크를 중심으로 유기적인 상호 관계가 가능하게 됨으로써 효율성의 가치가 증폭되었는데 이러한 환경은 역으로 상당한 기술력 통해 네트워크 체계를 악용하려는 세력에게는 상당히 매력을 주는 기회를 제공한다. 전산망 공격 및 파괴, 사이버 절도, 익명성을 이용한 개인과 기관에 대한 명예훼손, 불법 정보유출 행위 등은 이미 일반적으로 일어나고 있는 사이버공간에서의 심각한 범죄 행위이다.

그런데 이러한 범죄 행위들이 정치단체나 국가 등 권력기관에 의해 조직적이고 대규모로 자행될 때 타 국가의 사회, 경제에 미치는 영향은 심각할 것이다. 이는 곧 국가안보와 직결되는 문제로서 국가를 대상으로 안보에 영향을 주는 사이버상의 행위를 사이버상의 범죄와 구분하여 전쟁의 관점에서 '사이버戰'이라는 차별화된 용어를 사용한다. Aquilla와 Ronfeldt는 21세기는 사이버전 시대가 될 것이라고 강조 하면서 "사이버전은 정보 원칙에 따라 군사작전을 수행하는 것과 수행을 준비하는 것을 의미하고, 적을 알기 위해서 의존하는 정보와 정보체계를 와해시키는 것을 말한다"라고 정의한 바 있다.[2)]

사이버전 개념 자체가 정보화의 진전과 밀접한 관련이 있어 그 용어가 명확히 정의된 바는 없지만 광범위한 의미로는 "정보 혁명에 의해 출현한 새로운 형태의 전쟁 양상으로 정보의 우위를 달성하기 위하여 자국의 군사부문 및 민간부문의 정보체계를 보호하며, 적의 군사부문 및 민간부문의 정보체계를 교란, 파괴함으로써 적의 군사 분야뿐 아니라 이를 지원하는 민간 산업기반, 국가정보기반 구조를 무력화시키기 위한 광범위한 제반 활동"으로 정의 한다. 보다 세부적 관점에서는 컴퓨터와 관련된 기반 장비를 토대로 한 사이버공간에서 다양한 사이버 공격 수단을 사용하여 상대의 정보자산을 교란, 거부, 통제, 파괴하거나 이러한 공격 행위로부터

2) 엄정호 외 2명, 『제4차 산업시대의 사이버전 개론』, (서울 : 홍릉, 2020), pp. 27-28.

자신의 정보자산을 보호하는 행위로 정의하기도 한다. 또한 우리 군은 사이버전을 "사이버공간에서 일어나는 새로운 형태의 전쟁으로써 컴퓨터 시스템 및 데이터, 컴퓨터통신망 등을 교란 및 마비, 무력화함으로써 적의 사이버 네트워크 체계를 파괴하고, 아군의 사이버 체계를 방호하는 것"이라고 정의하고 있다.[3] 전쟁의 형태는 시대적 상황에 따라 변모해 왔다. 현대 전쟁의 특징은 〈표 2-1〉과 같다.

〈표 2-1〉 현대 전쟁의 특징

| 구 분 | 주요 특징 |
|---|---|
| 3세대 전쟁 | 첨단기술을 바탕으로 한 기동전<br>공지 합동전력 집중 활용<br>C4I 시설 및 군수 시설 파괴 중점 작전 구사 |
| 4세대 전쟁 | 네트워크 무력화를 통한 전쟁 수행 의지 굴복<br>사이버 공격 및 사이버 심리전 강화<br>비대칭 전력 중심의 작전<br>장기적인 정치투쟁의 심리전 / 선전선동 강화<br>군사적 승리보다 정치적 승리에 중점 |

출처 : 노보환 , "4세대 전쟁 양상과 대응전략", 『합참』 제49호(2011), pp. 93-97. 참고 재구성

4세대 전쟁으로 칭하는 현대 사이버전은 가용한 모든 네트워크 즉 사이버 수단을 활용하여 적의 전쟁 의지를 무력화시키기 위한 정기전이며, 비대칭 전력에 의존하는 장기적인 정치투쟁으로 군사적 승리보다 정치적 승리에 목적을 둔다.[4]

이러한 4세대 전쟁은 3세대 전쟁이 가장 절정에 달했던 1991년 걸프전에서 등장하였다. 당시 초강대국이었던 미국은 첨단무기, C4I 체계, 기동전과 배합전 "인사막의 폭풍" 작전을 통해 개전 2개월도 되지 않아서 이라크군을 격멸하고 쿠웨이트를 수복했다. 이를 계기로 첨단기술을 적용한 군사혁신(Revolution in Military Affair)만이 미래 전쟁의 열쇠가 될 것이라는 인식이 전 세계 안보관에 영향을 주었

3) 정기영, "국가방위를 위한 사이버전 대응체계에 관한 실증적 연구", (서울 : 숭실대학교 대학원 박사학위 논문, 2016), p. 30-31.
4) 노보환, 4세대 전쟁 양상과 대응전략", 『합참』 제49호(2011), pp. 92.

다. 이를 계기로 나타나기 시작한 신개념의 4세대 전쟁 수행 체계가 바로 네트워크 중심전 즉, 사이버전이다.

1998년 미국 해군저널(Proceedings of the Naval Institute)의 "Network Centric Warfare: its Origin and Future"을 통해서 처음 등장하였다. 3세대 전쟁에서 네트워크를 이용한 군사작전을 적용하는 새로운 전쟁 방법을 기술하였다.[5] 1931년 3세대 전쟁이었던 이라크전쟁 이후 코소보전에서 등장한 정보전(IOW) 용어와 함께 EBO(Effective Based Operation)가 부각 되었으며 이라크전쟁과 2001년 아프가니스탄 전쟁을 통해서 네트워크 중심전(Network Centric Warfare)이라는 용어로 통합되었다.[6]

## 2. 북한의 사이버전

북한이 사이버전에 본격적으로 관심을 갖게 된 것은 걸프 전쟁을 통해서이다. 1991년 걸프전에서 미국은 전자장비를 동원하여 이라크군의 방공망과 지휘 체계를 마비시키며 위력을 떨쳤다. 이에 김정일은 1996년 서해의 최전방부대를 시찰한 자리에서 "앞으로 모든 전쟁은 컴퓨터 전쟁이며 모든 인민군 지휘관들은 컴퓨터를 배워야 한다고 지시하며, 자신도 매일 한 시간 이상 컴퓨터를 사용한다."라고 말한 적이 있다.[7] 또한, 1999년 9월 25일에는 평양방송을 통해 걸프전 당시 미국이 4~6시간 전에 이라크 전선 전역에 걸쳐 종심 1,300km까지 영향을 미치는 강력한 전자 장애를 조성하여 이라크군의 지휘 체계를 마비시켰다고[8] 밝히며 전자전, 정보전의 중요성을 강조하였다.[9]

---

5) 노보환, 앞의 논문, (주 6), pp. 93.
6) 노보환, 앞의 논문, (주 6), pp. 94.
7) "위대한령도자 김정일동지께서 1996년 12월 15일 현지지도에서 제시하신 전투적 과업을 철저히 관철하자", 『로동신문』, 1996. 12. 26.
8) "걸프전 당시 미국이 이라크 전선 전역에…", 『평양방송』, 1999. 9. 25.
9) 남성욱, 『북한의 IT산업 발전전략과 강성대국 건설』, (서울 : 한울, 2002), p. 167.

또한, 북한 군부의 젊은 엘리트들이 사이버전에 대해 여러 차례 제안했었으나 채택되지 않았다가 최초의 사이버전인 1999년 코소보전쟁 이후 김정일이 사이버전에 대해 재평가하면서 북한은 사이버전을 국가전략으로 채택하게 되었다.[10] 코소보전쟁을 통해 초고속 통신망의 군사적 이용이 전쟁 수행에 미치는 중요성을 깨닫게 된 것이다. 2000년대에 들어와서는 남한의 컴퓨터의 보급이 확산되고 인터넷 사용이 본격적으로 활성화됨에 따라 북한은 이를 주시하여 사이버 전력을 대폭 적으로 증강하고자 하였다.

아프간전쟁(2001)과 이라크전쟁(2003)에서 미국의 강화되는 정보전 수행 능력이 공중 작전이나 지상 작전과 융합될 때 엄청난 파괴력의 효과를 발휘하는지 실감하였고, 이라크전쟁 이후 조선인민군부대 현지 지도때 마다 수뇌부를 모아놓고 정보전쟁의 중요성에 대해 강조하였다.[11] 특히 2003년 2차 이라크전쟁 이후 "김정일은 인민군 최고 수뇌부들을 모아놓고 지금까지의 전쟁이 물리적 전쟁, 기름 전쟁이었다면 21세기 전쟁은 정보전이며 누가 평소에 적의 군사기술 정보들을 더 많이 장악하고 있는가?, 그리고 전장에서 적의 군사지휘 정보를 얼마나 강력하게 제어하고, 자기의 정보력을 충분히 구사할 수 있는가? 에 따라 전쟁의 승패가 좌우된다"라고 역설하며 사이버전에 대한 능력 강화를 독려하였다.[12]

> "지금까지 전쟁은 알(총탄 포탄 등) 전쟁, 기름 전쟁이었다면 21세기 전쟁은 정보전이다. 즉 누가 평소에 적의 군사기술 정보들을 더 많이 장악하고 있는가, 그리고 전장에서 적의 군사지휘 정보를 얼마나 강력하게 제어하고, 자기의 정보력을 충분히 구사할 수 있는가에 따라 전쟁의 승패가 좌우된다."[13]

10) 변상정, "북한 과학기술정책 연구동향과 과제", 『현대북한연구』 제14권 제2호(2010), pp. 167-21
11) 김윤영, "북한의 대남사이버공작 대응방안 연구", 『치안정책연구』 제30권 제2호(2016), p. 246.
12) "조선인민군 최고사령관 김정일동지께서 조선인민군 제1353군부대(정찰총국 전자전부대)를 시찰하시였다", 『로동신문』, 2008. 8. 6.
13) 김흥광, "북한의 사이버정보 실태", 『북한』 제5호(2005), p. 32.

북한의 경제난 역시 사이버전에 집중하게 된 요인 중 하나로 작용하였다. 북한은 1980년대 중반부터 경제난으로 인해 기존의 재래식 전력 증강에 차질이 생겼고 이에 적은 비용으로 큰 효과를 낼 수 있는 사이버전 전력 강화에 집중하게 된 것이다.[14] 기존의 육·해·공군 전력과 같은 대칭 전력과 핵미사일 무기 등의 비대칭 전력들은 초기 구축 비용만 하더라도 상당한 자본이 소요되며, 구축 후 유지 보수에도 엄청난 비용이 필요하다. 또한, 인적자원의 보존과 훈련, 무기체계를 유지 개발하는 데에도 지속적인 비용이 추가되어야 한다. 반면 사이버전 전력은 두뇌집단에 컴퓨터와 통신장비, 사이버 능력 확충을 위한 훈련시설을 갖추면 기본적인 구축이 끝나며, 추가적인 유지 관리비용 또한 크지 않기 때문에 다른 전력에 비해 경제성이 좋다는 장점이 있다.

김정일의 지시에 의해 2000년대 중반 이후 D-DOS 공격, 전산망 파괴, 해킹, 남한 사회 국론분열 여론 조성 등을 실행하는 사이버 전력을 강화하고, 공격 주체를 은폐하는 능력을 발전시켰다.[15] 또한, 국가 주요 기반시설의 제어시스템이 폐쇄망으로 분리 운영되면서 직접적인 해킹이 어려워지자 유지보수 업체의 PC를 장악해 우회 침투와 공격을 시도하였다. 김정일은 대남 사이버 통일전선 공작 전술을 '남조선 혁명' 목표달성의 핵심 전력으로 인식하였다. 이후 김정일의 직접 지시에 의해 북한의 대남공작 기구들은 사이버 전담 부서를 강화하였고, 김정일은 대남 사이버 공작 전술의 중요성을 강조하기 시작하였는데 김정일 시대의 사이버 역량에 대한 강화된 교시 내용은 〈표 2-2〉와 같다.

14) 김필재, 『북한의 사이버 남침』, (파주 : 백년동안, 2014), p. 9.
15) "유능한 컴퓨터 전문가들을 양성하여야 한다.", 『로동신문』, 2003. 7. 15.

〈표 2-2〉 김정일 시대의 사이버역량 강화 교시 내용

| 구분 | | 교시 내용 |
|---|---|---|
| 김정일 교시 | - 사이버공간의 중요성 강조 | - 인터넷은 국가보안법이 무력화되는 특별한 공간임.<br>- 남한당국이 통제할 수 없는 공간임.<br>- 남한 내 인터넷을 적극 활용할 것. |
| | - 사이버전의 중요성 강조 | - 사이버 공격은 원자탄이고 인터넷은 총이다.<br>- 21세기 전쟁은 정보전쟁이다. 현대전은 전자전, 전자전에 따라 현대전의 승패가 좌우됨.[16] |
| | - 사이버 전력의 강화 강조 | - 더 많은 사이버 전사를 양성하라.<br>- 사이버 부대는 나의 별동대이자 작전 예비 전력임. |

출처 : 김윤영, "북한의 대남사이버공작 대응방안 연구", 『치안정책연구』 제30권 제2호(2016), pp. 241-276. 내용 참고 연구자 작성

결국, 김정일 시대의 대남혁명의 공작 전술은 두 가지의 형태로 나타났는데 한편으로는 반혁명 세력 규합과 폭력투쟁의 방법을 계승하는 소련과 중국의 공산주의 전통방식의 전술을 유지하였다. 또 다른 한편으로는 남한의 정보화시대 발전 환경 변화 흐름을 빠르게 인식한 사이버 공작 전술의 탄생과 시발점이 된 것이다.[17]

김정일이 본격적으로 사이버전에 나선 것은, 2009년 2월 정찰총국이 탄생하면서부터이다. 정찰총국은 간첩 혹은 사이버 전사를 양성하거나, 무력도발과 테러, 사이버 공격 등을 수행하는 온라인과 오프라인 환경에서의 대남공작 총괄조직이다.[18] 그 가운데에서 사이버 공격에 특화 되어있는 팀은 110연구소로 기존에 존재했던 121연구소와 100연구소를 통합하여 소프트웨어 개발을 하는 것으로 위장된 부서이다. 실질적인 정보전의 최전방 부서로, 해커 지휘부까지 설치된 것으로 알려졌

16) "현대전의 능수 진짜배기 싸움군들로…", 『로동신문』, 2016. 4. 24.

17) 김흥광, "북한의 정보전 전략과 사이버 전력: 돈 없는 북한의 최후 선택 사이버 전쟁", 『월간조선』 통권 제375호(2011), pp. 80-89.

18) "조선인민군 최고사령관 김정일동지께서 조선인민군창건 78돐에 즈음하여 조선인민군 제586군부대(정찰총국) 지휘부를 방문하시고 인민군장병들을 축하하시였다", 『로동신문』, 2010. 4. 26.

다.[19] 정찰총국은 2009년 7.7 사이버대란, 2011년 3.3 디도스 공격 및 농협 전산망 무력화, 2013년 3.20 사이버 공격과 6·25 사이버 공격, 2014년 한국수력원자력 해킹, 2016년 청와대 해킹 메일 발송, 외교, 안보라인 휴대폰 해킹 등을 자행한 것으로 알려져 있다.[20]

2000년대 들어 북한에 IT산업이 도입되었다. 그러나 우리가 알고 있는 바와 같이 북한의 인터넷 사정은 매우 열악하다.[21] 북한에서 운영하는 '광명'[22]이라는 인터넷 체계는 한국에서 말하는 인트라넷 수준에 불과하였다. 하지만 소프트웨어 개발을 담당할 IT 인력과 최신 IT 기술은 충분히 보유하고 있는 것으로 알려져 있다. 스마트폰과 같은 이동통신 서비스를 사용하고 있는 사람도 약 700만 명에 이르는 것으로 알려져 있다.[23]

# Ⅲ. 김정일 시대의 사이버 공작전술

## 1. 대량살상무기 개발과 「7·7 디도스」 사이버 도발

김정일 집권 초반에는 김일성 시대의 간첩침투와 국지도발 유형이 그대로 이어졌는데 2000년대에 들어서는 간첩의 직접 침투와 국지도발이 현저하게 줄어들었다. 김정일 집권기 중반부에 접어들면서부터 북한은 대량살상무기(WMD)를 활용한 도

19) "오중흡 7련대 칭호를 수여받은 조선인민군 제1313군부대관하 2중대 3대혁명 붉은기 조영호 영웅구분대를 시찰하시였다.", 『로동신문』, 2006. 12. 6.

20) 남기현, 안병두, "北 정찰총국 주도 드론 공격, 협박소포, 인사납치, 사이버테러 가능성", 『매일경제』, 2016. 2. 19.

21) 조우찬, "김정은 시대 북한 IT 산업의 패러다임 전환과 향후 남북 IT 교류협력, 사이버 전쟁(Cyber Warfare)의 시작과 남북 IT 교류협력을 중심으로", 『북한연구학회』 2016년 동계학술회의, 2016. 12. 23.

22) 이홍열, "북한의 인터넷과 국가도메인(kp) 승인", 『IT standard & test) TTA Journal』 통권 제118호 (2008), pp. 104-109.

23) 전영선, 『글과 사진으로 보는 북한의 사회와 문화』, (서울 : 경진, 2016), pp. 204-205.

발에 집중하며 도발유형의 변경을 꾀하기 시작하였다. 천안함 폭침과 연평도 포격 등의 국지도발이 김정일 집권 후반기에 벌어졌지만, 이 시기 북한의 도발은 WMD 개발에 집중되는 경향을 보였다. 북한은 2003년 핵확산금지조약(NPT)에서 탈퇴한 이후 2005년 2월 핵무기 보유를 선언하면서 핵무기 개발 의도를 본격적으로 내비치기 시작하였다. 이와 동시에 핵무기를 탑재할 수 있는 투발 수단인 장거리 미사일 개발실험에 박차를 가하면서 WMD 보유로 도발유형을 변화시켰다. 김정일 시대의 북한은 최초의 핵실험을 포함한 두 차례의 핵실험(2006년, 2009년)과 세 차례의 장거리 미사일 시험발사(1998년, 2006년, 2009년)를 감행하였다.

이 시기에 사이버테러라는 새로운 유형의 도발도 등장하였는데 저비용 고효율이라는 점에서 북한이 역량을 집중하고 있는 새로운 '사이버 도발'의 유형이 나타나기 시작하였다. 북한의 사이버 도발은 7.7일 디도스 공격(2009년)을 시작으로 농협 전산망 마비 사태(2011년) 등이 대표적인 사례이다.[24] 또한, 북한의 대외 매체와 제3국에 서버를 두고 운영하는 인터넷사이트를 활용한 대남 비방·비난과 선전선동 활동을 강화하기 시작하는 '사이버 공작전술'이 전격 등장하였다.

이와 동시에 인터넷 공간을 활용한 대남 비방과 선전선동 심리전 전개가 나타났는데 대표적인 사례로 '우리민족끼리', '구국전선' 등의 인터넷사이트를 활용한 남한 정부의 정책 비난과 유언비어 유포, 종북세력 확대 양산 등의 전방위적인 '사이버 공작전술'을 전개하였다.[25] 이러한 사이버 공작전술 전개는 이 시기의 남한 정부에 대한 반정부 투쟁 확산과 미제국주의 군대 철수, 한미동맹 조약 파기, 국가보안법 철폐 등을 요구하는 반정부 단체의 활동 증가에 영향을 주었다.

24) 정제혁, "검찰, 농협 해킹 전산망 마비 사건 북한 사이버테러소행 결론.『경향신문』, 2011. 5. 4.

25) 박순옥, "사이버상의 보안경찰 활동 연구", (광주 : 광주대학교 대학원 경찰행정학 석사논문, 2010), p. 44-46.

## 2. 대북 전단살포 조준 사격 위협과 「3·4 디도스」 공격 사이버전 전개

북한은 남한의 민간단체들이 주도하여 진행하는 대북전단 살포 행위에 대해 상당한 불만을 드러내다가 2011년 1월부터는 발원지를 직접 조준 사격하겠다고 협박하기 시작하였다. 2011년 3월 18일 북한은 탈북자 출신이 북한 민주화와 독재정권의 실상을 북한 주민에게 알리기 위해 남한의 설립한 대표적인 대북전단 살포 민간단체인 "북한민주화운동본부(대표 박상학)"을 포함하여 남한에서 대북 전단을 살포할 경우 원점을 직접 조준 사격하겠다는 "조선인민군 서부전선지구사령관"의 조선중앙통신 문답식 공개 발표를 통해 협박 심리전을 전개하였다. 이는 해당 지역 주민들에게 불안과 공포감으로 작용하여 주민들의 반발로 남한의 휴전선 지역에서 진행하던 대북 전단살포가 최초로 무산되었다.[26]

또한, 북한의 정찰총국 신설 직후 첫 대규모 사이버 공격은 2009년 7.7 디도스이였다. 이 공격으로 청와대와 국회, 미국 재무부와 국토안전부 등 한국과 미국의 주요기관 전산망이 마비되었다. 북한은 사이버 전술이 미치는 파급 효과와 성과를 직접 확인하는 계기가 되었다. 이후 2011년 공격 방법의 패턴을 바꾼 3.4 디도스 공격으로 국내의 40여 개 주요 사이트가 마비되고, 2013년 3월 20일에는 KBS와 MBC, YTN의 방송망이 동시에 공격을 받는 등의 사이버 공격을 감행하여 피해를 주었다.

경찰청 사이버테러 대응센터는 2011년 3월 4일 디도스 공격을 분석한 결과 "악성코드 유포 사이트와 국내 감염 좀비 PC, 외국 공격 명령 서버를 정밀 분석한 결과 공격 체계와 방식, 악성코드 설계 방식과 통신방식이 2009년 7월 7일 발생한 디도스 공격과 정확하게 일치한다"라며 북한의 소행으로 결론을 내렸다. 7.7 디도스 공격 당시 근원지는 중국에서 IP를 임차하고 있는 북한의 체신성이 사용 중인 IP로 확인된 바 있다.[27]

26) 백나리, "주민 저지로 대북전단 살포 첫 무산", 『연합뉴스』, 2011. 3. 14.
27) 양승식, "경찰 3월 4일 디도스 공격 북한소행", 『조선일보』, 2011. 4. 6.

## 3. 대남 사이버 공작 전술의 등장

2010년 적발된 직파 간첩 사건으로 한춘길과 강순정의 사건을 통해 북한의 대남 사이버 공작기법과 전술이 변화하였음이 확인되었다. 과거 직파 간첩이나 장기간 암약하는 고정간첩은 무전기나 무인포스트를 이용했지만 2010년부터는 북한의 대남 공작부서는 인터넷을 통해 보고나 지령을 간단히 받을 수 있게 되었다.

바로 '사이버드보크'[28]라는 신종 연락 수단이 대표적이다. 지령을 하달하는 북한 상부와 국내 암약 간첩이 제3국 이메일 계정을 개설해 아이디와 패스워드를 공유하고 암호화(Encryption)된 보고 내용과 지령을 탑재하여 공유하는 사이버 연락 방식을 말한다. 남파된 국내 암약 간첩이 수집한 자료를 상호 약정된 특정 웹사이트 내 자유게시판 등에 게시하여 교신하는 방법도 있다. 페이스북 같은 SNS 계정을 통해서도 활용할 수 있는 방식이다.

2010년 적발된 직파 간첩 한춘길과 강순정 사건이 사이버드보크 방식을 보여준 대표적 사례이다. 이때부터는 북한의 사이버 공작기술을 활용한 외화벌이 규모도 발전하게 되었다. 중국 등 제3국 지역에서 무역회사로 위장한 거점을 개설하고 사이버 공격과 함께 사이버 외화벌이 사업을 추진하였는데, 평소에는 사이버 도박, 게임 어플 프로그램을 개발하여 판매하거나 사이버 불법 도박사이트 운영 등을 통해 외화벌이를 하다가 상부의 지령이 하달되면 사이버 공격 작전을 실행하는 사이버 공작 전술이 나타기 시작했다.[29]

28) 무인포스트란 러시아어에서 유래된 두브크(dvoke)가 진화하여 사이버공간에서 이메일을 비밀 매설지로 활용하는 비밀공작 연락기술이다. 이메일을 보내지 않고 내가 보낸 메일함 또는 다른 메뉴 등에 숨겨놓고 약정된 사람이 방문하여 볼 수 있게 함으로써 전달되는 방식의 사이버드보크(Cyber dvoke) 이다.

29) 디지털기획, "북한의 사이버 공작요원 7,000여 명 연간 1조원 외화벌이", 『세계일보』, 2017. 11. 23.

# Ⅳ. 김정은 시대의 사이버 공작전술

김정은 시대 남한의 사이버 인터넷 환경은 고도화 발전되고 그 적용 범위가 급속하게 확대됨에 따라 친북인사와 연계한 사이버 통일전선의 은밀한 사이버 영역이 확보되어 사이버 간에서의 공작활동 노출의 은밀성과 기밀성이 유리해지고, 저비용 투자 대비 고효율 성과달성이라는 목적 실현의 조건이 유리하게 조성되면서 전통방식의 공작전술 전개와 사이버 영역의 공작 전술을 배합 추진하는 '하이브리드 사이버 공작전술'의 변화양상을 보이기 시작했다.

김정일 시대에는 공산주의 전통방식과 사이버 기술이 혼합된 2세대 혼합형 대남공작 전술을 시도하고 전개하였다면, 2012년 북한의 3세대 후계 체제로 출범한 김정은 정권에서는 김정일 집권기에 축적된 혼합형 대남공작 전술을 토대로 사이버 융합 기술을 접목한 3세대 배합형 '하이브리드 사이버 공작전술'을 고도화 발전시켜 전개하는 분명한 변화가 나타났다.[30]

북한이 김정은 시대에서 전개하는 사이버공간의 통일전선 전술과 선전 투쟁이 오프라인에서도 연대연합과 공동투쟁으로 작동하고 있으며,[31] 미국과의 협상과 한반도 비핵화를 주장하면서 핵과 미사일 개발을 지속 추진해오는 양상도 보이고 있다.[32] 그 이유는 기존의 김정일 시대의 대남 혼합형 공작전술 전개의 성과와 김정은 시대에 고도화 발전 중인 제3세대 '하이브리드 사이버 공작 전술을 배합 전개'[33]하여 일

30) 변상정, 『김정은 시대 과학기술정책 주요 내용과 평가』, (서울 : 국가안보전략연구원, 2021), pp. 3-13.

31) 이영종, "사이버전은 인민군의 무자비한 보검: 김정은, 핵·미사일과 함께 3대 전쟁 수단으로 규정", 『시사저널』 통권 제1315호(2014), pp. 24-25.

32) 김정은, 『신년사』, "조국수호정신 지니고 당과 수령, 조국과 인민을 목숨으로 옹호보위 하였으며 적들의 무모한 핵전쟁도발 책동과 반공화국대결소동을 걸음마다 짓부시고 공화국의 존엄과 위력을 높이 떨치였습니다", (평양 : 조선로동당출판사, 2014), pp. 3-4.

33) "전반적 무장력을 정치사상전으로 군사, 기술적으로 더욱 비약시키기 위한 군사적 대책 및 새로운 부대들을 조직 편성하여 위협적인 외부세력들에 대한 군사적 억제능력을 더욱 완비하기 위한 새로운 군사적 대체들에 관한 명령서들과 중요군사 교육기관, 책임역할을 높이기 위한 기구 개편 안 군사지휘체계를 개편할데 대하여", 『로동신문』, 2020. 5. 23.

정 부분에서 달성한 성과를 토대로 남한 내에 통일혁명 역량을 조성한다면 공산화 통일 실현이 충분히 가능할 것이라는 '남조선통일혁명 역량'에 대한 정세 판단을 굳게 인식하고 있기 때문이다.[34] 김정은 시대의 사이버 역량 강화 교시 내용은 〈표 4-1〉과 같다.

〈표 4-1〉 김정은 시대의 사이버 역량 강화 교시 내용

| 구분 | 지시 분야 | 주요 내용 |
|---|---|---|
| 1 | - 사이버공간의 중요성 강조 지시 | - 사이버전은 핵, 미사일과 함께 인민군대의 무자비한 타격 능력을 담보하는 만능의 보검이다. (김정은, 2013년 8월 정찰총국 간부들에게 교시) |
| 2 | - 사이버 전력의 중요성 강조 지시 | - 강력한 정보통신 기술, 정찰총국과 같은 용맹한 사이버 전사들만 있으며 그 어떤 제재도 뚫을 수 있고, 강성국가 건설도 문제없다. (김정은, 2013년 4월 7일 정찰총국 해커부대 방문시 교시) |
| 3 | - 사이버 거점 장악, 무력화 지시 | - 적들의 사이버 거점들을 일순에 장악하고 무력화할 수 있는 만반의 준비를 갖추라. (김정은 2014년 6월 28일 정찰총국 사이버 부대 121국 비공개 방문시 교시) |
| 4 | - 전략 사이버사령부 창설 지시 | - 김정은 2012년 북한군 정찰총국 산하 110호 연구소 방문시 전략 사이버사령부 창설 지시함. (사이버 영재는 중학교 시절 조기 발굴해 매년 300명씩 사이버 전사로 집중 양성) |
| 5 | - 사이버 인력 확보 지시 | - 각 도의 제1중학교에서 유능한 컴퓨터 인재 양성 지시함. (2009년 10월 평양 제1중학교 방문시 교시) |

출처 : 김윤영, "북한의 대남 사이버공작 대응방안 연구", 『치안정책연구』 제30권 제2호(2016), p. 248. 재구성

34) "당중앙위원회 제7기 16차 전원회의 '변화된 정세의 요구에 기초하여 새로운 투쟁로선과 전략전술적 방법들을 제시", 『조선중앙통신』, 2020. 8. 19.

또한, 북한 김정은 시대의 사이버 공작 전술은 "인터넷은 제도적 기반과 정규군을 가진 일본군과 맞서 싸우던 항일빨치산의 투쟁 무대"와 같다면서 북한군의 정보 모략전, 해킹, 사이버 심리전, 대남공작이 북한이 아닌 제3국에서 벌어지는 것으로 하여 적에게는 노출될 위험이 적고, 반면에 적대국에서는 인터넷이 제도화되고 공개되어 있기 때문에 드러난 공격위험을 가지고 있는 더없이 유리한 작전 공간으로 간주하고 있기 때문인 것으로 판단하고 있다.[35] 이러한 전략적 기반을 토대로 해외에 서버를 두고 운용하는 인터넷사이트 48개 중 대표적인 대남 선전용 웹사이트의 선전투쟁 내용과 북한 찬양 게시물이 국내 친북 인터넷사이트나 개인 블로그 등에 대체적으로 유사한 형태로 게시되고 있다.

김정은 시대에는 이러한 환경 기반을 바탕으로 북한의 체제선전을 위한 온라인과 웹 공간의 활동 역량을 강화하는데, 2010년 이후부터 페이스북이나 트위터, 개인 유튜브 방송 등의 계정을 개설해 체제선전과 대남 선동심리전을 위해 활용하기 시작하였고, 최근에는 딥페이크 기술을 활용한 사이버 모략심리전술 개발의 가능성도 대두되고 있다.[36]

북한의 전반적인 컴퓨터 시스템 관련 인프라가 열악하다고 하지만, 군사 분야나 소프트웨어 개발 분야에서는 고성능의 컴퓨터를 보유 및 활용하고 있다.37) 북한의 민간 컴퓨터 보급수준은 낮지만, 미사일 궤도안착 능력이나 전파수집 및 해독능력의 탁월함은 이러한 추론을 가능하게 한다. 또한, 북한의 IT 인력 인프라는 매우 잘 갖춰져 있는 상태인데, 해커 육성 대학으로 손꼽히는 '김일군사대학'(舊지휘자동화대학)이 건재하고, 노동당과 군부 차원에서 전문적인 해커 양성을 진행하고 있다. 북한의 사이버 전략과 위협은 김정은 집권 이전과 이후가 완전히 다르게 진행되고 있다.

35) 국방부, "북한은 약 6,800여 명의 사이버전 인력을 운영하며, 해킹, 디도스 공격 및 바이러스와 악성코드를 이용한 첩보수집 등 다양한 수단을 이용하여 국가 기반시설 마비와 금융기관 해킹 등 사이버전 도발을 감행하고 있다", 『2016 국방백서』, (서울 : 국방부, 2016), p. 236.

36) 김경윤, "평양 주민들도 트윗 하나?, 북한 개인명의 트위터 계정 등장", 『연합뉴스』, 2020. 11. 13.

37) 김학송, "조선인민군군사출판사 발간 〈전자전 참고자료〉로 본 북한의 전자전 능력과 우리 군의 대응 실태 분석", 『김학송 의원실』, (2011), pp. 9-11.

김정은 집권 이전과 이후 북한의 사이버 전략 및 컴퓨터 시스템 등의 여건 등을 고려해 봤을 때 경제적 기반이 약하다고 해서 능력 부분까지 평가 절하는 것은 그릇된 판단이다. 북한의 IT산업에서 사이버 전략, 그리고 이제는 사이버테러에 이르기까지 산업발전 자체뿐 아니라 체제유지와도 긴밀히 연결되어 있다.[38] 김정은 시대는 해킹을 포함한 사이버 공격을 통해 혼란과 분열을 유발하고, 소프트웨어기술 개발과 판매 등을 통해 외화벌이를 지속하며, IT인력 육성에 지속적인 노력을 기울이고 있다.[39] 특히 익명성이 보장된 사이버 활동(해킹 공격, 정보탈취, 금전탈취 등)의 경우, 목표에 대한 공격을 진행하면서도 그 배후를 철저히 숨길 수 있다는 점이 매우 매력적인 장점이며, 한국이나 미국 등 다른 나라들과의 정상적인 관계를 유지하면서도 공격목표에 대한 피해를 줄 수 있다는 점은 비(非)전쟁시대에 북한의 가장 큰 무기가 될 수 있는 부분이라 할 수 있다.[40] 북한의 대남 사이버전 수행조직 기구는 〈표 4-2〉와 같다.

38) 황지환, "북한의 사이버안보 전략과 한반도, North Korea's Cyber Security Strategy and the Korean Peninsula: 비대칭적, 비전통적 갈등의 확산", 『東亞硏究』 제29권 제1호(2017), pp. 139-159.

39) "실전을 반영할 수 없는 컴퓨터 모의 전쟁", 『로동신문』, 2013. 4. 20.

40) 김승주, "전 방위적으로 시도되는 북한 사이버테러 실상", 『북한』 통권 554호(2018), pp. 84-89.

〈표 4-2〉 북한의 대남 사이버전 수행조직

| 임무 기능 | 조직 부서 | | 수행 임무 |
|---|---|---|---|
| 사이버 요원 양성 | 김일성군사종합대학 | | - 1986년 개설, 5년제 전산과정 운영<br>- 1,000여명의 사이버전사 육성 |
| | 김일군사대학<br>(舊지휘자동화대학) | | - 1986년 지휘자동화대학(미림대학)<br>- 전자전 연구 및 사이버전사 양성 |
| | 김정은국방종합대학<br>(舊국방대학) | | - 1964년 국방대학으로 설립(2016년 6월 개칭)<br>- 군사작전 지휘체계 프로그램 전문가 양성 |
| | 모란봉대학<br>마동희군사대학<br>(舊압록강군사대학) | | - 1997년 작전부 산하 신설, 흡수통합<br>- 정찰총국 사이버해킹 전문가 양성 |
| 사이버 공작 실행 | 총참모부 | 지휘정보국 | - 군 지휘통신 교란 등 전자전 수행<br>- 31소, 32소, 56소 운영 |
| | 총정치국 | 적공국 204소 | - 한국군 대상 사이버심리작전 전개<br>- 역정보 및 허위정보 등 기만전술 |
| | 정찰총국 | 작전국 414연락소,<br>128연락소 | - 한국 및 해외정보 수집(해킹)<br>- 전담요원 해외파견, 사이버테러 수행 |
| | | 기술정보국<br>110연구소 | - 舊기술정찰조 확대 운용<br>- 한국 주요정보 수집(해킹)<br>- 사이버공격(테러) 수행 |
| | | 해외정보국<br>자료조사실 | - 한국 전략정보 수집(해킹)<br>- 사이버전담요원 해외파견 운용 |
| | 노동당 | 노동당중앙위원회<br>10국<br>(舊통일전선부) | - 대남 사이버심리전 수행<br>- 160여개 친북사이트 운용<br>- 트위터, 유튜브 등 SNS 심리공작 전개<br>- 여론조작 및 댓글팀 운용<br>- 남남갈등, 사회혼란 조성 |
| | | 문화교류국 | - 한국 전략정보 수집(해킹)<br>- 사이버 전담요원 해외파견 운용 |

출처 : 부형욱, 『최근 북한 사이버 활동의 변화와 함의』, (서울 : 한국국방연구원, 2018), pp. 1-6. 내용 참조 연구자 작성

## 1. 김정은 시대의 사이버 전사 양성

북한의 사이버 전사들은 약 7,000여 명으로, 이는 미국 사이버사령부에 배치된 약 5,000명의 사이버 요원들보다 많은 전력을 보유하였다.[41] 북한의 사이버 부대는 사이버 전사 육성을 병행하고 있는데 국가의 전폭적인 지원을 통해 육성되어 진다. 초기 북한의 사이버 전사들의 교육은 군사대학의 일부 비편제 인원으로 편성되어 육성되었으나, 점차 북한이 정책적으로 사이버 전사들을 키워내려는 움직임을 강화하며, 일반대학과 고등교육 과정에까지 해당 사이버 전사육성 교육을 진행하고 있다. 또한, 교육생의 일부는 중국과 인도, 그리고 러시아에서도 실무 훈련을 받는 것으로 알려져 있다.[42]

북한의 '김일성군사종합대학'은 북한의 대표적인 군 간부와 사이버 전문군관양성 기관이다.[43] 평양 만경대 구역에 있는 이 대학은 1956년 설립됐는데 인민군 총참모부 직속 기관으로 우리나라의 합동군사대학과 유사한 역할을 하는 북한 최고의 종합군사학교로 고급군관들을 양성하는 핵심이기도 하다. 김일성군사종합대학에서는 일반 병종의 부대에서부터 특수부대 병종에 이르기까지 중급 군관 이상을 양성하는 역할을 하고 있으며, 졸업자들은 북한 군대의 핵심부서 직책에 보직되어 군 수뇌부의 주요 역할을 하는 것으로 알려져 있다.[44] 이 대학은 본과 과정과 연구과정으로 나뉘어 있는데, 본과는 대위에서 중좌까지의 현역 군관들을 대상으로 교육을 담당하고 있다. 교육 기간은 병과에 따라 다르지만 일반적으로 3~4년 정도이며, 해당 교육과정을 완수한 후에는 김일성군사종합대학 경력이 자신의 군사경력으로 상당히 인정받기 때문에 큰 인사상의 큰 혜택을 볼 수 있다.

연구원 과정은 상좌 이상의 고급군관들을 대상으로 교육하는 과정으로 교육 기간

41) 박대광, "북한의 사이버전 능력과 우리의 대응 방향", 『합참』 제48호(2011), pp. 16-20.

42) 임종인, "북한의 사이버전력 현황과 한국의 국가적 대응전략", 『국방정책연구』 제2권 제4호 통권 제102호(2013), pp. 9-45.

43) "정보산업발전과 컴퓨터 인재양성을 중시하고 있는 조선", 『로동신문』, 2003. 11. 6.

44) 김지홍, "북한 사이버 공격 및 전력 연구," (서울 : 경기대학교 석사학위논문, 2017). pp. 21-30.

은 1년이다. 김일성 군사종합대학은 기존에 존재하고 있는 '강건종합군관학교', '김책공군대학' 등 초급지휘관을 육성하기 위한 군사학교들과는 달리 기존 지휘관으로 활동하고 있는 군관을 대상으로 고급지휘관을 양성하며, 이곳에 컴퓨터 과학대학이 설치되어 있다. 컴퓨터 과학대학에서는 기존 지휘관들에게 사이버 군사전략의 중요성에 대해 교육하는 역할을 하고 있으며, 실제 군사전략과 사이버 군사전략을 병행하여 수행하는 교육들이 진행되고 있다. 김일성군사종합대학은 사이버 전사양성을 위해 1986년 5년제의 전산과정을 신설한 이후 매년 약 수백 명의 사이버 전사를 배출하는 것으로 알려졌다.

'김일군사대학'은 대표적인 북한의 사이버 전사를 양성하는 전문군사대학 중 하나이다. 김일성군사종합대학이 전산과정을 신설하던 해에 김정일 국방위원장은 새로운 사이버 인력양성기관 설립을 지시하였다. 평양시 미림동에 설립되어 일명 '미림대학'으로 불리기도 하는데 최초 설립시 명칭은 '지휘자동화군사대학'이었다. 5년제 교육과정으로 설립된 이곳은 지난 2000년 '김일군사대학'으로 개칭되었으며, 3년제의 대학원 연구과정이 설치되어 있다.[45] 김일군사대학은 해마다 100여 명 이상의 졸업자를 배출하고 있으며 설립 초기부터 소련과의 협조를 통해 컴퓨터 전문가들을 초빙하여 사이버 전사들을 육성하는 핵심 사이버 군사교육기관으로 학생들은 졸업 후 정찰총국과 국방성 산하 인민군부대에 정보기술 군관으로 배치된다.[46]

또한, 김정은 시대에 들어와 사이버 전력 강화를 위해 개편된 평양에 위치한 '김정은국방종합대학'에도 컴퓨터 공학부가 설치되어 있다. 1964년 10월 '국방대학'으로 설립되었으나 2016년 6월 김정은의 지시에 따라 '김정은 국방종합대학'으로 개칭[47]하고 컴퓨터공학 특별반을 설치하여 전반적인 교육을 진행하며 컴퓨터 하드웨어기술, 소프트웨어기술, 무장 장비의 프로그램기술, 해킹 및 보안기술 등 사이버전에 필요한 모든 기술을 교육하고 있다. 학년마다 100~120명의 일반중대, 50명

45) 박준희, "86년 김정일 지시로 '미림대학' 설립, 사이버전사 체계적 양성", 『문화일보』, 2021. 8. 12.
46) 강철환, "北 해커부대 양성소는 미림대학", 『주간조선』 통권 제2156호(2011), pp. 38-40.
47) "경애하는 김정은동지께서 국방종합대학을 현지지도 하시였다", 『로동신문』, 2016년 6월 13일.

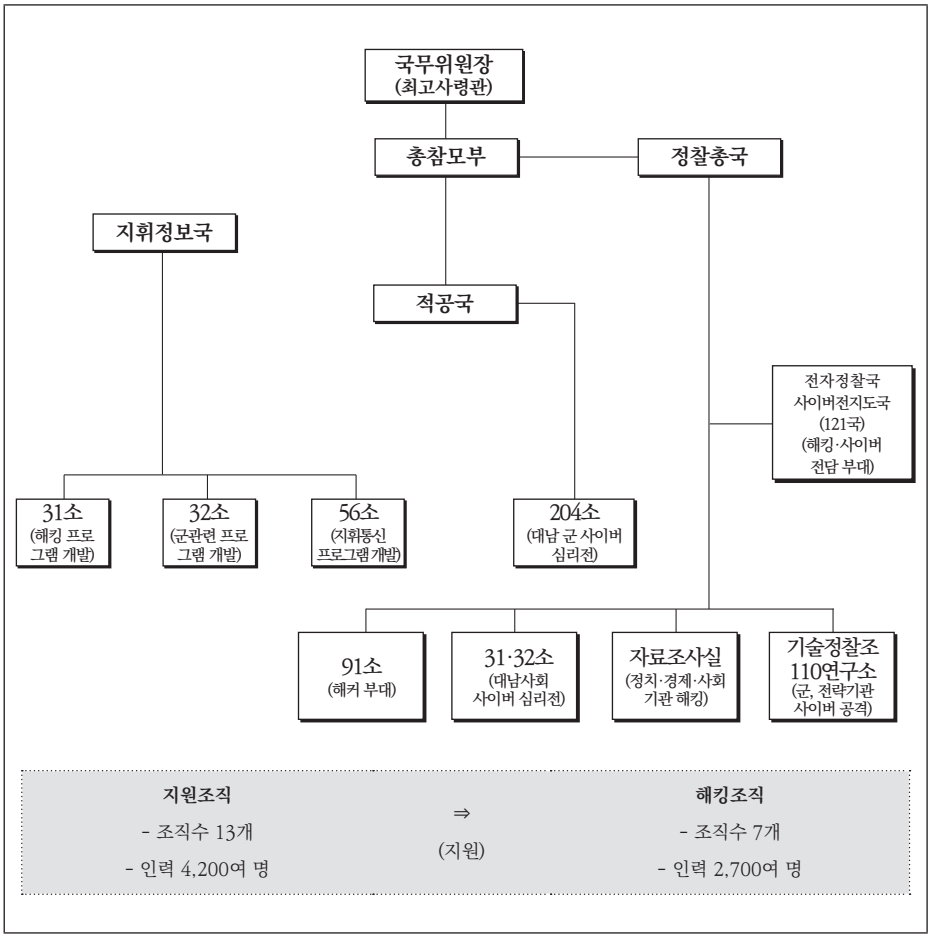
정도의 특수중대가 있으며, 졸업생은 인민군부대의 군사작전지휘체계 컴퓨터프로그램 전문가로 배치된다.

'모란봉대학'[48]은 김정일의 지시로 조선노동당이 1990년대 중반부터 컴퓨터 IT 분야가 세계적인 추세로 확산 발전되는 것에 주목하면서 노동당 작전부 산하에 컴퓨터 정보처리·암호해독·해킹 등의 전문가를 양성하는 모란봉대학을 1997년 최초 설립하였다. 신입생 선발 및 교과과정, 실습훈련 결과 등은 노동당 작전부장이 직접 지휘하는 체계를 유지하였던 만큼 중요하게 인식하였다. 2009년 2월 정찰총국이 신설되면서 작전부가 정찰총국으로 편입되어 지금은 정찰총국 소속의 사이버 전문 군관양성 대학으로 평양시 사동구역에 위치하고 있다. 이 대학의 목적은 사이버 심리전 작전요원과 사이버 첩보활동 요원 양성으로 외국어·전자통신 암호해독·해킹 등의 전문분야를 교육한다. 한 해 졸업생은 약 100여 명 정도로 해킹에 대한 전문 기술을 보유하고 있는 것으로 알려져 있다. 북한의 사이버 부대 규모와 지휘체계는 〈표 4-3〉과 같다.[49]

48) 모란봉대학 : 평양시 사동구역에 위치한 모란봉대학은 김정일의 지시로 1997년 노동당 작전부 산하에 설립되었다. 전자전 전문공작요원 양성을 목적으로 전산정보 처리, 암호해독, 해킹 등 사이버 공작 양성부서인 이곳은 매년 30여 명의 신입생을 선발하고 입학 당시부터 학생들에게 조선인민군 '중위'의 계급을 부여하고 있다. 2009년 2월 작전부가 정찰총국으로 편입되면서 현재는 국방성 정찰총국 산하 사이버전사 양성기관이다.

49) 김희수, "북한 사이버 위협의 심각성과 사이버전 수행 발전 방향", 『합참』 제59호(2014), pp. 71-176.

〈표 4-3〉 북한의 사이버 부대 규모 및 지휘체계




출처 : 임종인 외 4명, "북한의 사이버전력 현황과 한국의 국가적 대응전략, 『국방정책연구』 제29권 제4호 통권 102호(2013), pp. 9-45. 내용참조 연구자 작성

그 밖에도 북한은 사이버전사 육성을 위해 고등교육 과정에도 컴퓨터 전문학교를 설치하여 이를 통한 사이버전사 양성을 지속하고 있다. 특히, 제1 고급학교의 수재들을 융합한 특수학교를 중심으로 사이버 기초 기술, 하드웨어기술은 물론이고, 프로그램에 대한 지식과 폭넓은 컴퓨터 기반의 기본기술을 교육하고 있는 곳이 바로 평양금성중학교 이다.[50] 이곳에서는 교육을 중심으로 실습을 적절히 배치하여 실무

에 능한 컴퓨터 인재들을 키워내고 있으며, 실습 기간을 따로 마련하여 학생들에게 프로그램 개발의 기회를 부여하고 있다.

이들을 통해 국가 정보기술 전시회나 박람회 등에 여러 프로그램을 출품하고 있으며, 컴퓨터 하드웨어를 비롯하여 소프트웨어, OS 프로그램들을 교육하고 있다. 이들이 배우고 있는 자료구조와 알고리즘, 리눅스 프로그램 작성법, 인공지능 언어 등 상당 부분은 한국의 대학 과목으로 알려져 있다. 북한은 이렇게 교육한 IT 인재들 중에 우수한 인원들을 선발하여 김일성종합대학, 김책공업종합대학 등에서 다시 심화 교육을 실시하고 있다. 이렇게 모든 교육과정을 우수한 성적으로 마치고 발탁된 최우수 IT 인재들의 상당수가 '정찰총국 121국에 배치'[51]되어 사이버 공작활동 임무를 수행한다. 북한의 사이버 전사 양성기관과 교육 내용은 〈표 4-4〉와 같다.

〈표 4-4〉 북한의 사이버 전사 양성기관과 교육내용

| 양성 기관 | 교육 내용 |
|---|---|
| 김일성군사종합대학 | - 지휘관의 사이버전 주요 행동 전술 재교육 |
| 김일군사대학[52] | - 러시아와의 사이버전 기술교류 |
| 김정은국방종합대학[53] | - 컴퓨터 운용 및 사이버전 지휘체계 프로그램 설계 |
| 마동희군사대학<br>(舊 압록강군사대학)<br>모란봉대학 | - 전자정찰 전문 기술군관 육성<br>- 전자통신암호해독 / 해킹전문기술 군관 육성 |
| 중·고등과정 | - 컴퓨터 조기 교육을 통한 사이버 전사 육성 |
| **※ 사이버 전사 인원 약 7,000명 / 정찰총국 121국 · 110연구소 등 관리** | |

출처 : 주대준, "북한의 사이버 안보 위협 실태와 대응방안", 『국가안보전략』 통권 40호(2015), pp. 24-26. 내용 참조 연구자 작성

50) 최원우, "북 사이버 해킹에 올인". 『NK조선』, 2015. 2. 24.

51) 한영진, "북한 사이버테러 인력양성 모체, 제1중학교", 『북한』 통권 520호(2015), pp. 134-139.

52) 1986년 김정일의 지시로 북한군 총참모부 산하의 군 지휘자동화대학이 설립되었고 개편을 거쳐서 현재의 '김일군사대학'(舊지휘자동화대학)이 설립되었다. 이들 중에서도 선발된 엘리트들은 1년간 중국이나 러시아에서 해외 훈련을 받는다. 해외 훈련이 끝난 후에는 여러 해킹 부대에 배치돼 실전에 투입된다.

53) 1963년 6월 13일 설립. 2016년 현지 시찰 이후 김정은의 지시로 현재의 명칭으로 개명됨. 북한 평양시 용성구역 중이동에 위치 조선인민군의 핵무기, 대륙간탄도미사일, 잠수함발사탄도미사일 등

## 2. 온라인 공간의 대남 사이버 공작전술 전개

온라인과 웹 공간의 사이버 통일전선 구축을 위한 구체적인 전개 방법을 살펴보면, 북한은 그들의 선전선동 내용을 소위 1:9:90 법칙(90-9-1 rule)[54]이라는 전달 방식을 통해 남한의 인터넷상으로 순식간에 확산시켰다. 이는 북한의 "사이버 요원 1명이 남한의 인터넷에 선동 글을 게시하면, 핵심 북한 추종 세력 9명이 실시간으로 이를 옮겨 나르고, 90명이 보게 함으로써 일시에 선동 글이 퍼지도록 하는 방식"이다. 또한, 북한의 대남 사이버 공작요원들은 해킹을 통해 입수한 남한 국민들의 신분증 번호를 도용하여 인터넷 계정 ID를 생성하여 광우병 파동(2008. 5), 천안함 폭침(2010. 3), 연평도 포격(2010. 11) 등 남북한 간의 주요 사건의 발생 시기마다 마치 남한 국민들이 게시 글이나 댓글을 작성한 것처럼 위장하였다.[55] 북한의 댓글 공작팀은 "미국 수입 소를 먹으면 죽는다", "천안함 사건은 남한이 조작한 것", "연평도 포격은 남측의 책임" 등의 사실을 조작·왜곡하여 인터넷상에 집중적으로 게시하였다. 이들은 자신들이 작성한 댓글의 원점(原點)이 노출되지 않도록 북한식 표현을 남한 젊은이들 사이에 유행하는 최신 말투로 바꾸는 전문 한글 표기 검증팀인 '적구화(敵區化) 그루빠(그룹)'를 운영하여 마치 국내에서 댓글을 게시하는 것처럼 위장하였다.[56]

또한, 북한의 사이버 공작요원들은 국내에서 비합법적 방법으로 입수한 개인정보를 활용하여, 국내 주요 포털사이트의 영향력 있는 카페 등에 회원으로 가입하거나,

---

전략무기를 개발 및 연구 인재를 양성하는 곳으로 알려져 있다. 대외명칭은 제852군부대로 불린다. 8개 이상의 학부가 있고 전자공학부, 금속공학부, 화학 재료 공학부 등의 이름이 붙어 있지만, 외부에는 숫자만 공개된다. 가령 323조는 3학부 2학년 3반이란 뜻이다. 김정은의 이름이 붙기 전까지 3,000~4,000여 명의 재학생이 있었으며, 2021년 3월에 "극초음속 무기 학부"가 신설되었다.

54) Van Mierlo T, "The 1% Rule in Four Digital Health Social Networks: An Observational Study", (J Med Internet Res, 2014), p. 33.

55) 김호준, "北, 대남조직에 '댓글전담팀' 운영…사이버심리전 혈안", 『연합뉴스』, 2016. 10. 24.

56) 김흥광, "사이버 정보능력과 실태: 적대국(미국, 한국 등)에 대한 정보전, 대남공작 강화", 『북한』 통권 453호(2009), pp. 41-50.

공개 게시판·토론방·블로그 등을 직접 개설하고 조작된 정보와 유언비어, 흑색선전 등을 확산시켜 국론분열과 사회 혼란을 선동하였다. 또한, 북한은 트위터·페이스북·유튜브와 같은 북한 소유 SNS 계정 1,000여 개를 활용한 대남 사이버 심리전 공작 전술을 병행하고 있다.

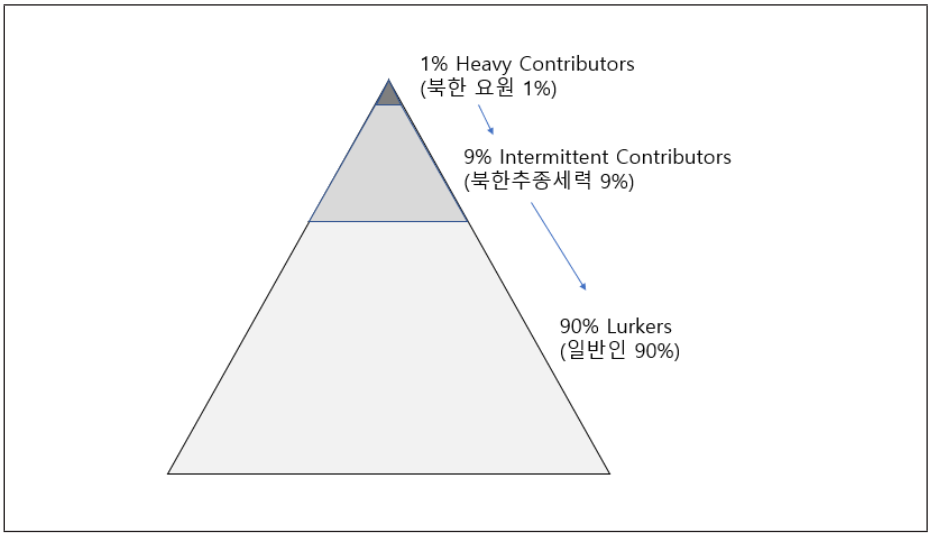
2021년 이후 북한은 세계적으로 유행중인 딥페이크 기술을 적용한 다양한 가짜 동영상을 제작 유포하여 정치·사회의 전 분야에서 혼란을 획책하고 우리 정부의 대북정책을 와해하려는 사이버 심리전의 시도와 얼굴과 목소리를 변형한 북한 해커가 국내 IT업체에 위장 취업을 시도하려는 활동도 포착되었다.[57] 친북 성향의 사이트·카페·블로그·페이스북 등과 연계하여 사이버 공간에서의 광범위한 '통일전선 지하조직 구축 공작 전술도 전개하고 있다.[58] 〈그림 4-1〉은 제이콥 닐슨의 '사이버 시장의 확장이론'[59]을 적용한 북한의 온라인과 웹 공간의 「1:9:90 법칙」 사이버 선동심리 공작전술 구축 법칙을 설명하였다.

57) 심재훈, "北 스파이, '딥페이크' 위장 취업 주의해야, 美 FBI 주의보 발령", 『자유아시아방송』, 2022. 7. 8.

58) 통일연구원 편저, "북한 사이버전 수행능력의 평가와 전망", 『통일정책연구』 제24권 1호(2015), pp. 117-148.

59) 제이콥 닐슨, 호아 로랭거 공저, "웹 사용성 중심의 웹사이트 제작론", (서울 : 도서출판 ITC, 2007), pp. 76-84.

〈그림 4-1〉 온라인과 웹 공간의 사이버 심리전 공작전술『1:9:90』법칙




출처 : Van Mierlo T, "The 1% Rule in Four Digital Health Social Networks: An Observational Study", (J Med Internet Res, 2014), p. 33. 재인용

## 3. 대남 간첩단 구축과 사이버 공작통신 기법의 등장

국내에 직파된 간첩과 장기간 암약하는 고정간첩들은 과거와 같이 무전기를 통한 대북 보고나 무인포스트에 의존하지 않고도, 진일보한 방법으로 인터넷을 통해 간단하게 대북 보고나 지령을 하달받을 수 있게 되었다.[60] 북한의 대남공작 부서에서는 이른바 '사이버드보크(Cyber Dvoke)'[61]란 신종 사이버 연락 수단으로 사이버공간 속에 드보크를 설치하여 간첩 간의 연락 수단으로 활용하였다.[62] 2010년 적발된 정찰총국 직파 간첩「한춘길·강순정 사건」에서 본격적으로 '사이버드보크'

60) 유동열, "사이버 공간이 위태롭다.",『미래한국』, 2016. 4. 6.

61) 간첩장비 비밀 매설지로 남파된 북한 공작원들이 고정간첩에게 줄 무기 등을 숨겨놓는 장소를 가리킴, 러시아어로 참나무를 뜻하는 '두푸'에서 변형된 말로, 간첩 장비 비밀 매설장소를 일컫는다.

62) 김정우, "北 독침 테러 사건의 전모: 박상학뿐 아니라, 김성민·이민복도 노렸다",『月刊朝鮮』통권 제380호(2011), pp. 140-153.

가 등장하였다.[63]

김정은 시대의 북한은 사이버 간첩 교신의 수단으로 첨단 스테가노그라피(Stegano graphy)[64]를 활용하고 있는데 '스테가노그라피'란 비밀 메시지를 이미지, 오디오, 비디오 또는 텍스트 등 커버라 불리는 다른 미디어에 은닉하여 전송하는 첨단 기법이다. 이 방식은 메시지를 숨기는 것은 물론 메시지 전송 자체를 흔적을 남지 않도록 하는 것에 목적이 있다. 2001년 알카에다가 9·11 테러 공격의 준비와 실행 간에 사용한 것으로 처음 알려졌는데, 2011년 7월 북한의 문화교류국(舊225국)의 지령을 받은 「왕재산 간첩단」 사건과 2013년 문화교류국의 지령을 받은 「전식렬 간첩」 사건에서 발견되었으며, 2022년 적발된 「충북동지회 간첩단」 사건에서는 진화된 스테가노그라피의 사이버 간첩 통신 기술을 사용한 것으로 밝혀졌다.[65]

## 4. 북한의 OGS와 해킹기술 고도화

북한의 해커 그룹인 Operation Ghost Secret은 미국을 포함한 17개국에 중대한 인프라(critical infrastructure), 통신시설(telecoms), 헬스케어 분야(health care), 그리고 연구(research) 등 다양하고 방대한 영역에 침투하여 정보를 탈취해 가는 것으로 알려져 있다. 미국 정보보안업체 '클라우드 스트라이크'의 연례 보고서에서는, 북한은 주요 국가들의 네트워크에 침입해 정보를 훔치거나 파괴한 뒤 빠져나가는 능력에서 러시아에 이어서 두 번째로 높은 능력을 보유한 것으로 보고하고 있다. 이 보고서는 북한이 경제제재를 극복하기 위하여 사이버 영역에서의 능력을 더욱 확충하고 있다고 적었다.

63) 서울중앙지방법원, 2010. 11. 7, 선고 2010고합1173 판결.

64) 사이버공간에서 진행하는 간첩연락 기법으로 영상이나 오디오 파일에 비밀 메시지를 감추어 그 정보의 존재 자체를 숨기는 보안기술로 메시지 또는 정보를 암호화시키지 않고 특정 물체 속에 숨겨 비밀통신을 위해 사용되기 시작하였으며 메시지를 숨긴다고 해서 정보 은닉술 이란 의미를 가진 스테가노그라피란 단어가 만들어졌다. 그리스어(헬라어)로 "덮다"라는 뜻의 스테가노스(Steganos) 와 "쓰다"라는 뜻의 그라페인(graphein)에서 나온 단어이다.

65) 서울중앙지방법원, 2011. 11. 31. 선고 2011고합1131 판결.

보고서에 따르면 정부 지원을 받는 러시아 전문 해커들은 18분 49초에 침투하고자 하는 네트워크를 뚫고 들어가 원하는 작업을 완료한 뒤 자취를 감출 수 있는 능력을 지니고 있다.[66] 이는 보안시스템이 해커를 발견해 강제로 해킹을 멈추기 전에 귀중한 자료를 빼낼 수 있음을 의미한다고 설명하였다. 러시아 해커들의 작업 능력은 다른 국가들의 해커들과는 비교가 되지 않을 정도로 신속한 수준이다. 한편, 북한 해커들은 러시아 다음으로 2위를 차지하고 있는데, 목표로 삼은 네트워크에 침입하여 작업한 뒤 빠져나가기까지 평균 2시간 20분이 걸리는 것으로 조사되었다. 북한 다음으로는 중국 해커들로 해킹에 보통 4시간 정도 걸렸다. 4위는 5시간 9분이 걸린 이란이 차지했다.

그 밖에 조직범죄 그룹은 해킹에 평균 9시간 42분이 걸리는 것으로 파악됐다. "사이버 보안에서 속도는 공격과 방어 양쪽 측면에서 모두 가장 중요하며, 해킹그룹의 순위는 목표 달성에 걸린 시간에 의해 결정이 된다"고 밝혔다. 미국 정부 관리들은 러시아, 북한, 중국, 이란과 같은 적대국의 사이버 공격 위험성에 대해 경고의 목소리를 높이고 있다.

북한은 현재도 유엔의 경제제재에도 불구하고, 사이버 공격(Cyber Attack)을 통해 무기제조에 필요한 물자와 기술 확보를 지속적으로 모색함으로써 핵무기와 탄도미사일을 현대화해 나가고 있다. 경제제재를 감시하는 전문가들은 유엔 안보리 상임이사 국가에 보낸 보고서를 통해 북한이 2019년부터 2020년 11월까지 가상자산 총 탈취 금액이 약 3억 1,640만 달러로 평가된다고 밝혔다. 조사위에 따르면 북한 연계 사이버 해커들이 2020년에도 금융기관과 가상화폐 거래소를 상대로 탈취한 자금으로 대량살상무기(WMD)와 탄도미사일 프로그램 지원을 계속한 것으로 조사되었다.

안보리 전문가들은 보고서에서 "북한과 이란이 장거리 미사일 개발 프로젝트에 대한 협력을 재개했다."라고 말하고 있는데, 이는 미사일 관련된 가장 최근의 선

66) 김인수 외 6명, "북한 사이버전 수행능력의 평가와 전망", 『통일정책연구』 제24권 제1호(2015), pp. 117-148.

적이 2020년에 이루어졌기 때문이다. 이란은 “전문가그룹이 우리에게 제공한 정보를 사전 검토하는 것은 패널 조사와 분석에 허위 정보와 조작된 데이터가 사용됐을 가능성을 시사한다.”라고 답변하였다. 북한 핵무기 개발에서 전문가들은 “김정은 정권도 핵무기 생산에 필수적인 핵분열 물질을 생산하고 핵시설을 유지해 왔다”고 보고 있다. 조선인민군 열병식에서 새로운 단거리, 중거리, 잠수함 발사 대륙간탄도미사일 시스템을 등장시키고 있는데, 신형 탄도미사일 탄두 시험 생산과 전술핵무기[67] 개발을 위한 준비를 발표하고 탄도미사일 인프라 역시 지속적으로 고도화하고 있다.

안보리는 2006년 첫 핵실험 이후 북한에 대해 점점 더 강력한 경제제재를 가하였다. 북한의 핵과 탄도미사일 프로그램을 포기하도록 북한을 압박하면서, 대부분의 수출을 금지하고 수입을 심각하게 제한하였다.[68] 그러나 이 보고서를 비롯한 주요 조사 결과에 의하면 북한이 경제제재를 회피하고 무기를 개발하며 정제된 석유를 불법 수입하고 국제은행 채널에 접속하며“악의적인 사이버 활동(malicious cyber activities)”을 수행해 오고 있다는 것을 알 수가 있다.

북한의 전략무기는 2017년 핵탄두 폭발 실험과 ICBM이 미국 본토 깊숙이 도달할 수 있음을 보여주는 비행시험이 포함된 이후 미국을 직접 위협하는 주요 위협으로 확대되었다.[69] 김정은은 한국과 도널드 트럼프 당시 미국 대통령과 2019년 핵무기 능력을 일부 포기하는 대가로 대규모 제재 완화를 요구하는 외교를 시작했으나 실패하였다.[70]

그리고 2020년에는 이미 타격을 입은 북한의 경제는 COVID-19로 인해 더욱 쇠

67) “김정은최고령도자 국가핵무력 완성을 특출한 성과로 강조, 핵단추가 사무실 책상 우에 놓여있다고 선언”, 『로동신문』, 2018. 1. 3.

68) “반공화국제재 해제와 미군철수를 주장”, 『로동신문』, 2019. 1. 19.

69) “조선로동당의 전략적핵무력의 일대 시위 대륙간탄도로케트 《화성-14》형 2차 시험발사에서 또다시 성공, 경애하는 최고령도자 김정은동지께서 대륙간탄도로케트《화성-14》형 2차 시험발사를 지도하시였다”, 『로동신문』, 2017. 7. 29.

70) “우리 당과 국가, 군대의 최고령도자 김정은동지께서 미합중국 대통령 도날드 제이. 트럼프와 또다시 상봉하시고 회담하시였다”, 『로동신문』, 2019. 3. 9.

락하였고, 이로 인해 김정은은 국경을 전면 폐쇄 하였다. 이러한 국경 폐쇄는 합법적인 것뿐만 아니라 불법적인 물품까지의 이전과 반입을 심각하게 제한하게 되었다.[71] 김정은은 2021년 1월 개최된 제8차 당대표자회의에서 북한 "내부의 경제기관이 수동적이고 자기 보호적인 성향을 갖고 있다"며 날카롭게 비판했다고 북한 관영매체가 보도하였다. 보도에서 김정은은 경제에 대한 국가 통제력 강화를 요구하는 동시에 북한이 미국에 대한 억제력으로 간주하고 있는 자신의 핵 프로그램을 활성화하기 위한 총력을 계속하겠다고 다짐하였다. 그러나 김정은의 외교 노력이 난항을 겪는 상황에서 트럼프 대통령과의 정상회담 결과를 비판했던 조 바이든(Joe Biden) 대통령의 임기가 끝나는 2025년 2월 또다시 트럼프 대통령과의 협상을 다시 시작해야 하는 상황을 맞이하였다.

# Ⅴ. 대남 사이버 전략 전술의 지속과 변화

## 1. 대남 사이버 전략 기조 유지

북한은 대남 사이버 심리전 외에 다양한 방식의 사이버 공작전술 활동을 통해 남한 사회의 혼란을 조성해 왔는데, 가장 심각한 형태 중의 하나가 사이버 공격(테러)이다. 사이버테러는 김정은의 직접 지시를 통해 전개되고 있는 것으로 알려져 있는데, 이는 우리 사회 내 혼란을 조성하면서 정부의 부실한 대응 태세에 대한 불만 확산과 함께 국민 생활에 직접적인 충격을 가함으로써 우리 국민의 심리적 공황 상태를 유발하기 위한 혼란 조성의 사이버 공작전술의 일환으로 볼 수 있다. 오늘날 우리 사회는 대부분의 일상이 인터넷과 모바일 장비를 통해 이루어진다고 할 정도로

71) 중앙비상방역지휘부, 『무역항들과 국경통과 지점들에서 봉쇄 및 검열대책을 철저히 세울데 대하여』, (평양 : 중앙비상방역지휘부, 2020). pp. 1-4; 『우리사람(화교포함)들에 대한 격리해제와 관련한 행동준칙』, (평양 : 중앙비상방역지휘부, 2020). pp. 1-3.

사이버에 대한 공생이 절대적임에도 사이버공간의 특성상 이를 보호할 수 있는 안전망이 제대로 구축되어 있지 않은 실정이다.

첫째, 체계적으로 양성된 해커부대(조직)을 동원한 사이버테러이다. 남한을 대상으로 한 북한의 사이버 공격 중 사회적 파장과 국가 안보적 중요성이 큰 사건들로는 북한의 한국군 고급장교를 목표로 한 트로이목마 메일 전파(2008), 7.7 디도스 공격(2009), 3.4 디도스 공격(2011), 3.20 사이버 공격(2013), 6·25 사이버 공격(2013), 국내 대기업 S사 전산망 공격(2013) 등으로 추정한다.[72] 이 가운데 3.20 사이버 공격은 2013년 3월 20일 KBS, MBC, YTN 등의 방송 3사와 농협은행, 신한은행, 제주은행 등 금융 3사의 전산망이 악성코드에 감염되어 총 32,000여 대의 컴퓨터가 일제히 마비된 사건이다.

이로 인해 방송사의 모든 컴퓨터와 금융기관의 인터넷 뱅킹, 영업점 창구업무, 자동화기기 사용 등이 약 2시간 동안 중단되었다. 이에 남한 정부의 민관군 합동 대응팀은 2013년 4월 10일 3.20 사이버 공격의 접속 기록을 조사한 결과 북한 정찰총국의 소행으로 발표하였다.[73] 3.20 사이버 공격은 주요 방송사를 목표로 하였다는 것이 심각한 사항이다. KBS는 공영방송으로 한반도의 유사시 국가의 정보를 제공하는 국영방송 매체이므로 이 사건은 주목할 만하다. 북한의 주요 대남 사이버테러의 사례는 〈표 5-1〉과 같다.

72) 김양현, "북한의 대남사이버테러 사례연구", 『한국테러학회보』 제7권 2호 통권16호(2014), pp. 5-21.

73) 김필재,『북한의 사이버 남침』, (파주 : 백년동안, 2014), pp. 88-103.

〈표 5-1〉 북한의 대남 사이버 공격(테러) 주요 사례

| 발생 시기 | 사이버 테러 내용 | 공격 주체 |
|---|---|---|
| 2009년 3월 | - 화학물질 사고대응정보시스템 CARIS 해킹 | 북한 소행 |
| 2009년 7월 | - 7·7 D-DoS 사태, 청와대, 국회, 포털 사이트 전산망 마비 | |
| 2011년 3월 | - D-DOS 공격 청와대, 국회, 외교부 등 정부기관 40곳 전산망 마비 | |
| 2011년 4월 | - 농협 전산망 해킹 사건 | |
| 2011년 5월 | - 육군사관학교 총동창회 홈페이지 해킹 | |
| 2013년 3월 | - 언론 / 금융사 내부시스템 파괴 목적 사이버 테러 감행 | |
| 2014년 12월 | - 한국수력원자력 원전 도면 유출 사태 | |
| 2016년 1월 | - 청와대, 외교부, 통일부 정부인사 460명 이메일, 문자 해킹 | |
| 2017년 4월 | - 국방 데이터센터 해킹, 작전계획 5027 등 군사비밀 탈취 | |
| 2021년 2월 | - 코로나19 백신기술 탈취 시도 | |
| 2021년 5월 | - 한국원자력연구원 해킹 | |
| 2021년 6월 | - 한국항공우주산업(KAI) 해킹 | |

출처 : 망라 기간에 발생된 北 사이버테러 관련 주요 언론 기사를 바탕으로 연구자 작성

둘째, 남한 주요기관 내부 기밀정보의 탈취이다. 대남 정보 탈취와 수집을 전담하는 전문 사이버 부대를 동원해 과거에는 남파간첩이나 고정간첩을 통해 획득할 수 있었던 정보를 평양의 대남 공작부서의 사무실 책상에 앉아서 주요 국가 기관망·공공망·상용망 등을 자유롭게 접속하여 필요한 정보와 자료를 입수하고 있는 것으로 알려졌다. 대표적인 사례로 화학물질 사고대응 정보시스템(CARIS) 해킹(2009), 군 작전계획5207 유출(2009), 농협전산망 해킹(2011), 중앙일보 해킹(2012), 한국수력원자력 조직도와 설계도면 등 6차례 걸쳐 85건 해킹(2013) 등이 있다.[74]

가장 최근에 일어난 해킹 사건은 2017년 한국군 국방망 해킹[75]과 2021년 한국

74) 백승구, "進化하는 북한 사이버테러 : 김정은 등장 이후 사이버테러 급증, 공격기술 高度化", 『月刊朝鮮』 통권 제426호(2015), pp. 102-111.

75) 김귀근, "군 검찰, 軍 국방망 해킹 北 해커 소행 결론,…中 선양지역 IP 식별, 『연합뉴스』, 2017. 5. 2.

수력원자력연구원 한국항공우주산업(KAI)을 해킹하여 자료가 유출된 사건으로 이는 해킹을 통해 확보된 자료를 공개하여 우리 정부의 안보 무능력 등에 대한 불신을 조장하여 내부 혼란을 조성하려는 전술을 전개한 것으로 볼 수 있다.[76] 국회 정보위의 하태경 의원에 의하면 원자력연구원은 2021년 5월에 12일 내부 컴퓨터망이 해킹되어 관계기관에 피해 신고를 하였다.[77] 또한 한국항공우주산업(KAI)도 해킹이 수일간 노출되었는지 조사 중이라고 밝혔다.[78] 국가정보원이 2021년 7월 8일 국회 정보위에서 밝힌 내용으로는 2021년 상반기 북한 해킹조직의 공격으로 인한 피해가 작년 하반기보다 9% 증가했다고 보고하였다.

이러한 북한의 해킹조직은 크게 네 군데로 추정되는데, 해외에 서버를 두고 있다. '라자루스'(Lazarus)는 주로 정부 기관, 금융과 방송 분야 등을 공격(D-DOS)하여 전산망을 무력화하고 사회적 혼란을 주요 목적으로 하고 있다. 라자루스는 2007년 조직되어 소니픽처스 해킹(2014), 방글라데시 중앙은행 해킹(2016), 워너크라임 랜섬웨어 공격(2017) 등을 수행하였다.[79] 미국 보안업체 '크라우드스트라이크'는 북한의 해커 집단 라자루스는 4개의 하부조직으로 이뤄져 있다고 조사한 내용을 공개하였다. 이 4개 하부조직 명칭은 '미로천리마'(APT37)[80], '침묵천리마', '별똥천리마', '물수제비천리마' 등인 것으로 추정하고 있다. 또 다른 조직인 '안다리엘'(Andariel)은 방산과 보안 솔루션업체에서 기술을 탈취하는 것이 주목적이다. 그리고 '블르노로프'(Bluenoroff)와 '킴수키'(Kimsuky)는 사이버상에서 금융 탈취를 전문으로 진행하는 것으 알려져 있다.[81] 북한의 사이버 전담 공작활동 조직은 〈표 5-2〉와 같다.

76) "국가 행사에 애국충정의 선물을 마련하는 것은 자랑스런 전통", 『로동신문』, 2015. 7. 14.

77) 고동욱, "원자력硏, 해킹에 12일간 노출…北 소행 추정", 『연합뉴스』, 2021. 7. 8.

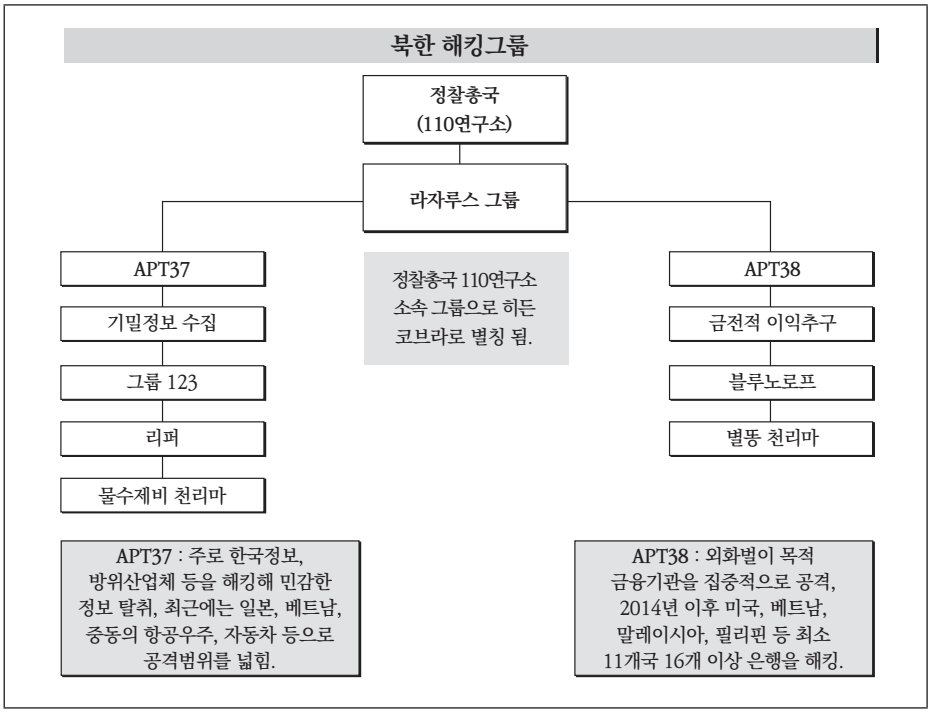
78) 하태경, "북한의 사이버테러 戰 능력 : 국가 차원에서 대대적으로 해커 양성, 한국의 정보망 드나들어", 『월간조선』 제30권 8호 통권 353호(2009), pp. 172-180.

79) 김상진, "北 해킹 전사들의 조직명은 '천리마'…하부조직 주특기 명확," 『중앙일보』, 2018. 2. 21.

80) APT37이라는 명칭은 지능형 지속 공격(Advanced Persistent Threat, APT) 해킹 기법을 쓰는 37번째 조직이란 뜻이다.

81) 방호엽, "북한은 해킹으로 얼마나 탈취했을까?", 『동아일보』, 2021. 7. 29.

〈표 5-2〉 북한의 대남 사이버 전담 공작활동 조직 체계




출처 : 조해수·유지만, "북한 해킹 그룹의 실체, 김수키·라자루스·스카크러프트·안다리엘 : 영재 교육받으며 키워진 북한 해커", 『시사저널』 통권 1653호(2021), pp. 18-20. 내용을 바탕으로 작성

셋째, 대남 사이버 심리전의 전개이다. 북한이 구사하는 전통적인 방법에 의한 통일전선전술의 전개는 ① 남북 당국 간의 협상과 대화 ② 범민련을 주축으로 하는 3자 연대 ② 전국연합을 주축으로 하는 비합법 통일전선전술 ③ 방북 인사를 대상으로 하는 연북연공 활동 ⑤ 공작원 등 전위조직을 활용한 방법 ⑥ 삐라, 대남방송, 시각 매체 자료를 이용한 선전선동 등으로 이루어진다. 북한은 "인터넷 사이버공간을 국가보안법이 무력화된 특별한 공간이며, 항일유격대가 다루던 총과 같은 무기"로 인식하고 활발한 활동을 전개하고 있다.[82)]

82) 최경환, "북한의 사이버선전 투쟁 분석", 『公安硏究』 제15권 제6호 통권 제81집(2003), pp. 3-24.

2017년 4월 국방부에서 국회에 제출한 자료에 의하면, 해외에 서버를 둔 친북 사이트는 162개 이상이며, SNS 계정은 1,622개 이상이다.[83] 이러한 북한의 선전 선동용 친북 인터넷사이트들은 국내 접속이 차단되어 있지만 인터넷 우회접속 프로그램(Proxy Server)을 사용할 경우 국내에서도 용이하게 접속이 가능하다. 특정 웹브라우저에 어플리케이션 하나를 설치하면 방송통신심의위원회의 북한 사이트 접속차단이 무력화되기 때문이다.[84] 이 같은 방식으로 마우스를 15회만 클릭하면 북한의 대남선전 사이트인 '구국전선' 등에 접속할 수 있고, 한글(워드) 문서로 게재된 북한이 게재한 전문(全文)을 다운로드 받을 수 있다. 현 수준의 인터넷 보안이라면 중·고등학생만 돼도 쉽게 접속하여 북한이 올려놓은 자료를 접할 수 있는 것이 현실이다. 이러한 사이버공간을 북한은 활용하여 기만 정보, 역정보 등을 유포하여 우리 사회의 남남갈등을 증폭시키고, 이념과 계파 간의 국론분열 조장의 원인이 되기도 한다. 북한이 제3국에서 운용 중인 인터넷 선전(심리전) 사이트 서버의 운용은 미국, 일본, 중국 등 13개 국가에서 약 90여 개에 이른다.[85]

## 2. 과학기술 발전에 따른 사이버 공작 전술의 변화

김정은 시대의 북한은 1990년대 김정일 시기의 고난의 행군과 같은 최악의 시기는 아니라 하여도 내외적인 여건이 매우 어려운 상황에 처해 있으며, 이는 곧 대남 혁명전략 수행에도 큰 영향을 미치고 있다. 북한의 대외적 악영향 요인은 소련과 동구권의 붕괴로 인해 체제에 대한 결정적인 타격을 입었으며, 이는 북한의 국제적 혁명역량에 심각한 손상을 입게 했다. 또한 계속되는 핵실험과 장거리 미사일 발사실험으로 유일한 사회주의 동맹국인 중국도 등을 돌리면서 국제사회의 질서를 교란

83) 문관현, "전문가, '北 160여개 친북사이트 활용해 대선 개입", 『연합뉴스』, 2017. 4. 17.

84) 한국인터넷진흥원, "더 파이러트 베이, 검열 방지용 웹브라우저 공개 : 접근 불가 웹사이트에 대한 우회접속 기능 제공", 『Internet & security weekly』(2013), pp. 1-2.

85) 통일부, 『제 303회 정기국회감사 요구자료(외교통상통일위원회), 친북 인터넷사이트 현황』, (서울 : 통일부, 2011), pp. 312-313.

하는 것에 대한 유엔 대북제재에 동참하는 상황을 만들어냈다.

북한은 1962년 4대 군사노선을 천명하고 경제와 국방건설 병진노선을 채택하여 국방력 강화에 최우선 투자를 전개해 왔다. 이는 김일성의 대남 무력통일 노선에 입각하여 김정일도 승계하여 노선을 견지하였다. 김정은도 동일한 노선을 계승하여 2013년 3월 조선노동당 중앙위원회 전원회의에서 "경제 건설과 핵무력 건설 병진로선"[86]을 채택하였다. 이것은 선대 유훈을 받드는 세습 정권의 특성상 함부로 바꿀 수 없는 속성을 지니고 있다. 이렇듯 북한의 경제는 침체를 거듭하고 있는 상황에서 경제와 병진노선에 맞게 핵개발과 국방력 유지에 국가 재정을 우선 배정하는 상황은 경제침체를 더욱 심화시킬 수밖에 없었다.

1980년대와 2000년대 초반의 남한의 정세는 민주화운동과 주사파의 친북세력이 정치적 세력을 형성하였다. 북한의 대남공작기관은 위험하고 어려운 지하당 조직을 구축하지 않아도 정치공작과 통일전선 심리전 전술을 통해 남남갈등을 조장하여 유리한 대남혁명 정세의 여건이 만들어진 것이었다. 때마침 이러한 상황에서 남한의 인터넷 환경발전은 선전선동 수단으로 대남 공작전술을 전개할 수 있는 새로운 전장의 토대가 갖추어진 것이었다.

남한은 세계 최고 수준의 인터넷 환경을 구축하였고, 당시 인터넷을 법적으로 단속하고 통제하는 수준 체계를 완벽하게 갖추지 못한 상태였기 때문에 인터넷을 활용한 사이버 대남공작전술의 전개는 최적의 조건이었다고 할 수 있다. 이 시기인 2000년대부터 북한은 남한의 인터넷을 대남 심리전(선전선동) 공작전술의 수단으로 활용한다는 방침을 세우고 기존의 '구국의 소리' 방송을 '구국전선'이라는 인터넷사이트로 전환하였다.[87] 또한, 이 시기부터 사이버 전사 양성을 강화하고 중국 등 제3국에 인터넷 사이버 거점을 구축하여 현재까지도 운용하고 있다. 사이버 인터

86) "당중앙위원회 2013년 3월 전원회의 정신을 높이 받들고 경제건설과 핵무력 건설 병진로선을 철저히 관철하자", 『로동신문』, 2013. 4. 1.; "조선로동당의 새로운 병진로선은 선군혁명승리의 로선", 『민주조선』, 2013. 5. 22.

87) 이정훈, "대남 심리戰 사이버공간서 활개 : 北, 효과 없어진 방송 중단 포기 후 전략 수정…구국전선 글 국내 사이트에 등장해 유포", 『주간동아』 통권 446호(2004), pp. 60-61.

넷 환경은 대남 사이버 심리전(선전선동) 공작전술 전개의 수단뿐만 아니라 사이버 드보크 등 간첩 통신의 안전한 수단으로도 활용되었다. 과거 단파 무전기와 단파 라디오를 활용하는 통신과 달리 이메일과 팝업 광고, 게시판, 메시지, 스테가노그라피 등과 같은 기술적인 사이버 은닉기법을 사용하는 안전한 지령 하달과 보고체계 구축에 매우 유리한 여건이 되었다. 또한, 남한의 친북인사와 세력에 대한 활동 방향과 투쟁 지침을 하달하는 공개 지령의 창구로도 활용되었다.[88)]

북한은 남한과의 경제적 열세로 군비경쟁에서는 승산이 없음을 인식하고 이미 비대칭 전력의 증강에 박차를 가해 왔다. 기존의 특수부대 전력과 은밀침투 수단인 잠수함 전력을 강화하고, 한·미연합군의 전략무기 자산에 대응하기 위한 핵무기와 미사일 개발에 주력해 온 것이다. 북한은 계속되는 국제사회의 대북제재 하에서도 교묘한 해외 불법무기밀매를 통해 통치자금을 확보해 왔고, 이를 통해 또다시 핵과 미사일을 지속 개발했고 이는 또다시 제재를 받는 악순환을 거듭하면서 오직 핵과 미사일만이 북한 체제를 유지 시켜줄 수 있는 유일한 수단이며, 대남혁명전략 측면에서도 남한과 미국을 타격 대상으로 삼는다는 대남혁명전략 논리의 정당성을 보장해주는 효과를 굳게 인식하고 있기 때문이다.[89)]

이렇듯 김정일 시기에 도입되고 김정은 시대에 비약적으로 발전하고 있는 북한의 사이버 능력은 비대칭 전력의 하나로 대남공격과 테러의 수단으로 이용되고 있다. 북한은 사이버 전사양성에 심혈을 기울여 오고 있는데[90)] 필요에 따라서 남한의 금융망, 국가기간망, 정부 주요기관 등에 침투하여 전산망을 마비시키고 기밀정보를 탈취하는 사회혼란 전술을 진행하는 이른바 저비용 고효율의 비대칭 전쟁의 성과를 거양하고 있는 것이다. 지금까지도 계속 연구하며 시도하고 있을 것으로 추정되는 가장 우려되는 활동으로 북한이 남한의 국방 전산망 침투에 성공한다면 남한

88) 김윤영, "북한 대남공작기관 실체와 대남공작 변화", 『북한』 통권 544호(2017), pp. 52-29.

89) 오일환, "핵·미사일 개발을 통한 북한의 체제 생존 전략 : 클린턴 행정부 시기 대미 관계를 중심으로", 『중소연구』 제 89호(2001), pp. 127-157.

90) "지하 막장의 미더운 전초병의 모습", 『로동신문』, 2019년 12월 28일; "당사상전선의 전초병들을 키우시는 위대한 손길", 『로동신문』, 2019. 3. 14.

의 국방전략자산을 장악 통제하는 엄청난 사태가 일어날 것이다. 이미 한국군의 통신 감청과 전자장비 교란 등을 통해 원활한 작전에 피해를 주었던 GPS 전파교란 사태의 사례를 통해 그 피해를 확인할 수 있다.

김정은은 2016년 5월 6일 개최된 조선노동당 제7차 대회에서 "전 민족적 합의에 기초한 연방제 방식의 통일"을 지향한다고 밝히면서 민족통일 3원칙(자주, 평화, 민족대단결)의 실행을 통해 조선의 평화적 통일을 위한 군사적 신뢰 분위기를 조성하고 남북 공동합의를 이해할 것을 남한에 제시하였다.[91] 이것은 김정일 시대의 대남 혁명전략 기조를 계승하여 추진하겠다는 의지를 보여준 것이며, 이는 2021년 1월에 제8차 노동당 대표자대회에서 개정된 '조선노동당규약' 서문을 통해서도 확인된 이후 현재까지 변화가 없다.

즉, 김정은 시대에도 북한은 대외적인 환경 변화가 불리하게 작용하더라도 선대의 혁명투쟁 정신으로 이를 극복하고 대남혁명 과업인 공산주의 국가 통일혁명을 계속 수행해나가는 전략을 견지하겠다는 것이다. 그러한 과정에서 선대 수령들이 전개했던 전통방식의 화전·강온 양면 전술인 무력도발, 간첩 직접 침투, 우회 침투, 국지전 도발, 핵무기 위협 전쟁 긴장 조성, 미사일 발사실험 등의 무력시위 전쟁 협박 등을 지속하면서 동시에 온라인과 웹 공간을 활용한 대남 통일전선 지하당 조직 구축과 남남갈등의 선동을 조장하고 사이버테러 감행을 통한 사회혼란 조성을 지속적으로 전개하고 있다. 이렇듯 김정은 시대의 대남 사이버 공작전술은 선대 수령들의 전략 기조를 유지한 채 공산주의 전통방식과 사이버 환경을 적극적으로 활용하는 사이버융합기술 배합 형태의 '하이브리드 사이버전략 전술'의 방향으로 빠르게 발전하였다.[92]

91) "경애하는 김정은동지께서 조선로동당 제7차대회 보고에서 제시하신 사상과 로선을 깊이 체득하고 철저히 관철하자", 『로동신문』, 2016. 6. 25.

92) 류병운, "국제법상 무력사용 금지와 새로운 안보위협 : 사이버전과 하이브리전을 중심으로", 『외법논집』 제44권 3호(2020), pp. 157-187.

# Ⅵ. 결론

북한의 김정일 시대에의 대남 공작전술은 '전조선 공산화통일'이라는 대남혁명전략 기조와 목표 유지 아래 비대칭 WMD 전략무기 개발에 중점이 맞추어져 있었다. 그러나 김정은 시대에는 비대칭 전략무기 개발의 완성과 함께 고도의 '하이브리드 사이버전략 전술'을 전개하고 있다. 과거 전통방식 공작전술에 온라인 및 웹 공간의 사이버기술을 결합한 새로운 유형의 대남 사이버 공작전술로 진화 발전하였다. 북한의 대남 사이버 공작전술은 김정일 시대에 등장하여 김정은 시대에 들어와서 지속되었으며 더욱 지능화되고 고도화 발전되었다. 남한의 인터넷 사이버 환경이 발전하면서 2000년 이후 세계 각 국가와 한국의 사이버공간을 사이버 전략과 기술의 돌파구로 활용하는 새로운 유형의 사이버 공작전술로 발전하였다.

특히, 김정일 집권 시기인 2009년 5월 10일 북한은 각종 대남·해외 공작업무를 하던 노동당 35호실과 작전부를 당에서 분리하고 인민무력부의 정찰국과 통합해 강력한 공작역량을 보유한 정찰총국을 출범시키고 개편된 정찰총국 조직 내 대남 사이버 조직 역량의 확대 발전에 총력을 기울였다. 여기에 김정은은 남한의 사이버 환경을 대남 공작전술 수행의 최적의 전장으로 인식하고 지능화 고도화된 사이버 발전기술을 융합한 형태로 '하이브리드 사이버 공작전술'의 활동 범위를 확장하였다.

김정은 시대의 사이버 전략과 통일전선전술의 지속은 변함이 없다. 공산주의 전통방식 대남혁명전략 기조가 사이버 기술과 융합하여 사이버공간을 이용한 통일전선 형성과 공작전술이 유지 전개되고 있기 때문이다. 2021년 개정된 조선로동당규약은 "공화국북반부에서 부강하고 문명한 사회주의 사회" 건설과 "전국적 범위"에서 "공산주의 사회 건설"을 위해 "전조선의 애국적 민주역량과의 통일전선"을 강화하는 공산주의 체제 조국 통일의 완성을 지향하고 있기 때문이다.

또한, 김정은 시대에는 경제적으로 효과적인 전술이 필요한 상황에서 급격하게 발전한 남한의 사이버 환경은 사이버 공작 전술의 변화를 가져왔다. 남한의 인터넷 환경을 활용한 대남 심리전(선전선동) 공작전술에 사이버융합 기술을 고도화 발전

시켜 '하이브리드 사이버 공작전술'을 전개하기 시작한 것이다. 김정은 시대의 하이브리드 사이버 공작 전술의 주요 특징은 다음과 같다. 첫째, 사이버 심리전·선전선동 전술이 강화되었다. 초기에는 '구국전선' 사이트를 통해 북한체제 선전 활동을 수행하다가 인터넷 기반이 확장되자 중국, 일본, 미국, 동남아 등지에 해외 선전사이트 거점을 개설했다. 선전사이트에는 체제 선전물을 개재했고, 제3의 인물이 선전물을 다시 남한의 인터넷사이트를 통해 재전파 확산하는 방법으로 사이버 선전선동 심리전 전술을 공세적으로 전개하는 방법이다.

둘째, 남한 내 지하당 구축과 간첩통신 기법이 안전한 연락기술 수단으로 발전하였다. 단파 무전기와 라디오를 활용하던 방식과는 달리 E-메일과 pop-up 광고, 게시판, 메시지 등 범용 메시지 전달방식의 '사이버드보크' 기법부터 '스테가노그라피(steganography)'의 사이버 은닉기법까지의 대남공작원과 간첩연락 통신의 사이버 기술이 다양하게 발전하였다.

셋째, 북한은 사이버 전력과 사이버 전사 양성에 심혈을 기울여 온 결과 대남 사이버 공격과 테러, 도발이 증가했다. 남한의 금융망, 국가망, 정부기관 등에 침투하여 전산 네트워크를 마비시키고 기밀정보를 탈취하는 등 저비용 고효율의 전술을 전개하고 있다. 사이버 기술을 활용한 군사정보 탈취 사례도 발견되었는데, 한국군 전산망에 사이버기술(해킹, 스미싱, 백도어, 웜바이러스, 악성 바이러스 유포 등)을 활용한 침투와 정보 탈취 시도가 보고되기도 했다. 김정은 시대의 대남 사이버 공작 전술은 사이버공간을 활용한 새로운 위협으로 부상하고 있다. 이러한 사이버공간에서 발생하는 국가안보에 대한 위협은 북한의 사이버 공작전술을 포함해서 국제테러, 경제정보 탈취 등 제3의 위협으로 확장되고 있으며, 과학기술이 발전하는 만큼 사이버 공간에서의 국가안보의 위협요인은 더욱더 증가할 수밖에 없다. 사이버공간에서 북한의 대남 공작전술에 대한 대응은 단순한 공안 대책의 차원을 넘어 포괄적이고 거시적인 사이버 안보정책의 수립과 사이버공간에서 발생하는 제3의 세력과 사이버 위협에 대한 대응이 동시에 이루어질 수 있는 역량과 체계를 갖추는 것이 시급한 이유이다.

따라서 본 연구를 통해 도출된 북한의 대남 사이버 전략과 공작전술에 대응하기 위한 국가안보전략 차원의 효율적인 대응 정책 방안을 제시한다. 첫째, 북한의 사이버 전력과 전술, 투쟁 활동체계에 대한 전담 연구기관의 설치이다. 국가 차원의 북한 사이버 전력과 체계 전술에 대한 대응력을 강화해야 한다. 이를 위한 북한 사이버조직과 전술체계 연구를 전담하는 연구기관 '가칭: 국가사이버안보연구원'을 설치하여 사이버 위협을 분석하고 파악된 약점을 평가하여 그 대응력을 높여나가야 한다.

둘째, 지속 발전 중인 북한의 사이버 안보공격 활동을 제어할 수 있는 국가 차원의 강력한 법령 제도 마련이 필요하다. 북한의 사이버 위협을 포함한 제3세력의 무차별적 사이버 공격과 위협에 포괄적으로 대응할 수 있는 강력한 법적 장치가 구축되어야 한다. 현재 사이버안보 관련 법령이 미비한 우리의 사이버 공간에서는 북한의 사이버 공작활동을 포함한 다양한 국가의 국가안보 위협에 대응할 수 있는 법령 제도가 부재한 상황으로 '가칭 : 국가사이버안보법 또는 국가사이버안전법'을 조속히 제정해야만 법령에 기반한 국가사이버 안보정책의 수립과 수사 활동이 가능하기 때문이다.

셋째. 사이버안보전담 수사기관 '가칭: 국가사이버안보수사청'과 군 수사기관 '가칭: 국군사이버안보사령부'의 설치이다. 앞에서 역설한 바와 같이 '가칭 : 국가사이버안보법' 법령이 제정되면 이를 적용한 적시적인 북한의 사이버 공작활동을 포함한 제3세력과 국내 안보 위해세력들을 적발하고 수사할 수 있는 활동의 기반이 뒷받침되어야 하기 때문이다.

넷째, 사이버안보 국제공조 협력체제의 구축이 필요하다. 북한의 사이버 공작활동 동향을 감시하고 위법 활동을 추적하여 신속하게 제압하기 위해서는 경계가 불분명한 영역의 광범위성과 은밀성이라는 사이버공간의 속성을 뛰어넘을 수 있도록 유관 국가의 사이버 수사기관과 공조 협력 체계가 구축되어야 한다. 북한은 전술상 자국이 아닌 제3국에 사이버 공작거점을 두고 국내에 침투하는 사이버 공작전술을 실행하고 있는데 이러한 사이버 공작을 추적하고 패퇴시키기 위해서는 관

련국 수사기관의 협조가 반드시 필요하다. 이를 위해 우리나라와 수교가 맺어진 국가를 우선 대상으로 국가 차원의 양해각서 또는 공조수사 협정체결 등의 사이버 안보 수사 공조 체제를 구축하여야 한다. 이러한 대응을 통해 우리는 김정은 시대에 더욱 고도화 발전 전개 중인 사이버 공작 전술과 안보 위협에 효율적으로 대응할 수 있을 것이다.

또한, 우리의 사이버 네트워크 환경의 발전으로 북한의 사이버 공격에 대한 피해는 우리 측의 피해가 심각한 것이 현실이지만, 북한 내부의 사이버 네트워크(붉은별 OS 체계 기반의 인트라넷) 체계의 환경도 점차 발전하고 있는바, 향후 북한 네트워크 체계 내부 공간에서의 사이버 작전 수행을 위한 북한 네트워크 체계에 대한 세밀한 분석과 작전전술 연구도 병행되어야 할 것이다.

# 〈참고 문헌 및 논문〉

국방부, 『2016 국방백서』, 서울 : 국방부, 2016.

김일성, 『김일성 선집 1』, 평양 : 조선로동당출판사, 1963.

김일기·김호홍, 『김정은 시대 북한의 정보기구』, 서울 : 국가안보전략연구원, 2021.

김필재, 『북한의 사이버 남침』, 파주 : 백년동안, 2014.

남성욱, 『북한의 IT산업 발전전략과 강성대국 건설』, 서울 : 한울, 2002.

부형욱, 『최근 북한 사이버 활동의 변화와 함의』, 서울 : 한국국방연구원, 2018.

변상정, 『김정은 시대 과학기술정책 주요 내용과 평가』, 서울 : 국가안보전략연구원, 2021.

엄정호 외 2명, 『제4차 산업시대의 사이버전 개론』, 서울 : 홍릉, 2020.

로동당출판사, "적들의 무모한 핵전쟁도발 책동과 반공화국대결소동을 걸음마다 짓부시고 공화국의 존엄과 위력을 높이 떨치였습니다", 평양 : 조선로동당출판사, 2014.

중앙비상방역지휘부, 『무역항들과 국경통과 지점들에서 봉쇄 및 검열대책을 철저히 세울데 대하여』, 평양 : 중앙비상방역지휘부, 2020.

_____, 『우리사람(화교포함)들에 대한 격리해제와 관련한 행동준칙』, 평양 : 중앙비상방역지휘부, 2020.

전영선, 『글과 사진으로 보는 북한의 사회와 문화』, 서울 : 경진, 2016.

한국인터넷진흥원, 『Internet & security weekly』, 서울 : 한국인터넷진흥원, 2013.

통일부, 『제 303회 정기 국회감사 요구자료(외교통상통일위원회), 친북 인터넷사이트 현황』, 서울 : 통일부, 2011.

강철환, "北 해커부대 양성소는 미림대학", 『주간조선』 통권 2156호(2011).

김윤영, "북한의 대남 사이버 공작 대응방안 연구", 『치안정책연구』 제30권 제2호(2016).

김승주, “전 방위적으로 시도되는 북한 사이버테러 실상”, 『북한』 통권 554호 (2018).

김정우, “北 독침 테러 사건의 전모 : 박상학뿐 아니라, 김성민·이민복도 노렸다”, 『月刊朝鮮』, 통권 제380호(2011).

김양현, “북한의 대남사이버테러 사례연구”,『한국테러학회보』 제7권 2호 통권 16호(2014).

김희수, “북한 사이버 위협의 심각성과 사이버전 수행 발전방향”, 『합참』 제59호 (2014).

김흥광, “사이버 정보 능력과 실태 : 적대국(미국, 한국 등)에 대한 정보전, 대남공작 강화”, 『북한』 통권 453호(2009).

김흥광, “북한의 사이버 정보실태”, 『북한』 제5호(2005).

_____, “북한의 정보전 전략과 사이버 전력: 돈 없는 북한의 최후 선택 사이버 전쟁”, 『월간조선』통권 제375호(2011).

_____, “북한 대남공작기관 실체와 대남공작 변화” 『북한』 통권 544호(2017).

김인수 외 6명, “북한 사이버전 수행능력의 평가와 전망”, 『통일정책연구』 제24권 제1호(2015).

김학송, “조선인민군군사출판사 발간 〈전자전 참고자료〉로 본 북한의 전자전 능력과 우리 군의 대응실태 분석”, 『김학송 의원실』(2011).

노보환, “4세대 전쟁 양상과 대응전략”, 『합참』 제49호 (2011).

류병운,“국제법상 무력사용 금지와 새로운 안보위협: 사이버전과 하이브리전을 중심으로” 『외법논집』 제44권 제3호(2020).

박대광, “북한의 사이버전 능력과 우리의 대응 방향”, 『합참』 제48호(2011).

변상정, “북한 과학기술정책 연구 동향과 과제”, 『현대북한연구』 제14권 제2호 (2010).

오일환, “핵·미사일 개발을 통한 북한의 체제생존 전략 : 클린턴 행정부 시기 대미 관계를 중심으로”, 『중소연구』 제89호(2001).

이영종, “사이버전은 인민군의 무자비한 보검 : 김정은, 핵·미사일과 함께 3대 전쟁 수단으로 규정”, 『시사저널』 통권 제1315호(2014).

이홍열, “북한의 인터넷과 국가도메인(kp) 승인”, 『IT standard & test) TTA Journal』 통권 제118호(2008).

임종인, “북한의 사이버 전력 현황과 한국의 국가적 대응전략”, 『국방정책연구』 제2권 제4호 통권 제102호(2013),

정기영, “국가방위를 위한 사이버전 대응체계에 관한 실증적 연구”, 숭실대학교 대학원 박사학위 논문, 2016. p. 30-31.

주대준, “북한의 사이버 안보위협 실태와 대응방안”, 『국가안보전략』 통권 40호(2015).

조우찬, “김정은 시대 북한 IT 산업의 패러다임 전환과 향후 남북 IT 교류협력, 사이버 전쟁(Cyber Warfare)의 시작과 남북 IT 교류협력을 중심으로”, 『북한연구학회』 2016년 동계학술회의(2016).

조해수·유지만, “북한 해킹 그룹의 실체, 김수키·라자루스·스카크러프트·안다리엘 : 영재 교육 받으며 키워진 북한 해커”, 『시사저널』 통권 1653호(2021).

하태경, “북한의 사이버 테러戰 능력 : 국가 차원에서 대대적으로 해커 양성, 한국의 정보망 드나들어", 『월간조선』 제30권 8호 통권 353호(2009).

한영진, “북한 사이버테러 인력양성 모체, 제1중학교”, 『북한』 통권 520호(2015),

황지환, “북한의 사이버안보 전략과 한반도, North Korea’s Cyber Security Strategy and the Korean Peninsula: 비대칭적, 비전통적 갈등의 확산”, 『東亞硏究』 제29권 제1호(2017).

최경환, “북한의 사이버선전 투쟁 분석”, 『公安硏究』 제15권 제6호 통권 제81집(2003).

통일연구원 편저, “북한 사이버전 수행능력의 평가와 전망”, 『통일정책연구』 제24권 1호(2015).

Van Mierlo T, “The 1% Rule in Four Digital Health Social Networks: An

Observational Study", (J Med Internet Res, 2014).
서울중앙지방법원, 2010. 11. 7, 선고 2010고합1173 판결.
서울중앙지방법원, 2011. 11. 31. 선고 2011고합1131 판결.
고동욱, "원자력硏, 해킹에 12일간 노출…北 소행 추정", 『연합뉴스』, 2021. 7. 8.
김경윤, "평양 주민들도 트윗하나, 북한 개인 명의 트윗계정 등장", 『연합뉴스』, 2020. 11. 13.
김귀근, "군 검찰, 軍 국방망 해킹 北 해커소행 결론, …中 선양지역 IP 식별", 『연합뉴스』, 2017. 5. 2.
김상진, "北 해킹 전사들의 조직명은 '천리마'…하부조직 주특기 명확," 『중앙일보』, 2018. 2. 21.
남기현, 안병두, "北 정찰총국 주도 드론 공격, 협박 소포, 인사납치, 사이버테러 가능성", 『매일경제』, 2016. 2. 19.
디지털기획, "북한의 사이버 공작요원 7,000여 명…연간 1조원 외화벌이", 『세계일보』, 2017. 11. 23.
문관현, "전문가 北 160여 개 친북 사이트 활용해 대선 개입", 『연합뉴스』, 2017. 4. 17.
백나리, "주민 저지로 대북 전단살포 첫 무산", 『연합뉴스』, 2011. 3. 14.
심재훈, "北 스파이 딥페이크 위장 취업 주의해야, 美 FBI 주의보 발령", 『자유아시아방송』, 2022. 7. 8.
조선중앙통신, "당중앙위원회 제7기 16차 전원회의 변화된 정세의 요구에 기초하여 새로운 투쟁로선과 전략전술적 방법들을 제시", 『조선중앙통신』, 2020. 8. 19.
양승식, "경찰 3월 4일 디도스 공격 북한소행", 『조선일보』, 2011. 4. 6.
이정훈, "대남 심리戰' 사이버공간서 활개 : 北, 효과 없어진 방송 중단 포기 후 전략 수정…구국전선 글 국내 사이트에 등장해 유포", 『주간동아』 통권 446호 (2004).

로동신문, “위대한령도자 김정일동지께서 1996년 12월 15일 현지지도에서 제시하신 전투적 과업을 철저히 관철하자”, 『로동신문』, 1996. 12. 26.

_____, “조선인민군 최고사령관 김정일동지께서 조선인민군 제1353군부대(정찰총국 전자전부대)를 시찰하시였다”, 『로동신문』, 2008. 8. 6.

_____, “유능한 컴퓨터 전문가들을 양성하여야 한다”, 『로동신문』, 2003. 7. 15.

_____, “현대전의 능수 진짜배기 싸움군들로”, 『로동신문』, 2016. 4. 24.

_____, “조선인민군 최고사령관 김정일동지께서 조선인민군창건 78돐에 즈음하여 조선인민군 제586군부대(정찰총국) 지휘부를 방문하시고 인민군장병들을 축하하시였다”, 『로동신문』, 2010. 4. 26.

_____, “오중흡 7련대 칭호를 수여받은 조선인민군 제1313군부대관하 2중대 3대혁명 붉은기 조영호 영웅구분대를 시찰하시였다.”, 『로동신문』, 2006. 12. 6.

_____, “실전을 반영할 수 없는 컴퓨터 모의 전쟁”, 『로동신문』, 2013. 4. 20.

_____, “정보산업발전과 컴퓨터 인재양성을 중시하고 있는 조선”, 『로동신문』, 2003. 11. 6.

_____, “경애하는 김정은동지께서 국방종합대학을 현지지도하시였다”, 『로동신문』, 2016년 6월 13일.

_____, “김정은최고령도자 국가 핵무력 완성을 특출한 성과로 강조, 핵 단추가 사무실 책상 우에 놓여있다고 선언”, 『로동신문』, 2018. 1. 3.

_____, “반공화국제재 해제와 미군철수를 주장”, 『로동신문』, 2019. 1. 19.

_____, “조선로동당의 전략적핵무력의 일대 시위 대륙간탄도로케트《화성-14》형 2차 시험발사에서 또다시 성공, 경애하는최고령도자 김정은동지께서 대륙간탄도로케트 《화성-14》형 2차 시험발사를 지도하시였다”, 『로동신문』, 2017. 7. 29.

_____, “우리 당과 국가, 군대의 최고령도자 김정은동지께서 미합중국 대통령 도날드 트럼프와 또다시 상봉하시고 회담하시였다”, 『로동신문』, 2019. 3. 9.

_____, “당중앙위원회 2013년 3월 전원회의 정신을 높이 받들고 경제건설과 핵무력 건설 병진로선을 철저히 관철하자”, 『로동신문』, 2013. 4. 1.

_____, “지하 막장의 미더운 전초병의 모습”, 『로동신문』, 2019년 12월 28일; “당사상전선의 전초병들을 키우시는 위대한 손길”, 『로동신문』, 2019. 3. 14.

로동신문, “경애하는 김정은동지께서 조선로동당 제7차대회 보고에서 제시하신 사상과 로선을 깊이 체득하고 철저히 관철하자”, 『로동신문』, 2016. 6. 25.

_____, “전반적 무장력을 정치사상전으로 군사, 기술적으로 더욱 비약시키기 위한 군사적 대책 및 새로운 부대들을 조직 편성하여 위협적인 외부세력들에 대한 군사적 억제능력을 더욱 완비하기 위한 새로운 군사적 대체들에 관한 명령서들과 중요군사 교육기관, 책임역할을 높이기 위한 기구 개편 안 군사지휘체계를 개편할데 대하여”, 『로동신문』, 2020. 5. 23.

_____, “국가 행사에 애국충정의 선물을 마련하는 것은 자랑스런 전통”, 『로동신문』, 2015. 7. 14.

민주조선, “조선로동당의 새로운 병진로선은 선군혁명 승리의 로선”, 『민주조선』, 2013. 5. 22.

박준희, “86년 김정일 지시 ‘미림대학’ 설립, 사이버 전사 체계적 양성”, 『문화일보』, 2021. 8. 12.

방호엽, “북한은 해킹으로 얼마나 탈취했을까?”, 『동아일보』, 2021. 7. 29.

정제혁, “검찰, 농협 해킹 전산망 마비 사건 북한 사이버테러소행 결론, 『경향신문』, 2011. 5. 4.

유동열, “사이버공간이 위태롭다.”, 『미래한국』, 2016. 4. 6.

평양방송, “걸프전 당시 미국이 이라크 전선 전역에…”, 『평양방송』, 1999. 9. 25.

Abstract

# Development and Response of Change in South Korea Cyber Attack Tactics in North Korea

Kim, June Seob
(Institute for Unification and Security Convergence)

In the 21st century, cyber space, which has changed as the center of the new security environment, has become an indispensable area of absolute security for all countries. This cyberspace has become a key battlefield that does not distinguish between peace and war in a new type of security environment. This study evaluated and analyzed the persistence and change of cyber tactics against North Korea. In other words, the changes in North Korea's cyber tactics were tracked by comparing the 'hybrid cyber tactics' based on cyber activities of the Kim Il-sung, Kim Jong-il, and Kim Jong-un periods after division. In the Kim Jong Il era, the "Unification Front Tactics for South Korea" developed cyber-craft tactics using cyberspace in the 2000s, riding on the development of information and communication in South Korea and the rapid growth of the Internet cyber environment. In particular, in February 2009, the Labor Party Room 35 and the Operations Department, which were in charge of public affairs in South Korea and abroad, were separated from the party and integrated with the reconnaissance bureau of the People's Armed Forces. It launched the Reconnaissance General Bureau, an organization that expanded cyber organizations, and established an independent anti-South Korean operational organization system directly led by the chairman of the National Defense Commission.