11-1320082-000013-09 ISSN 1738-2963

2016 제2호

치안정책연구

The Journal of Police Policies

2016. 9 (제30권 제2호)

치안정책연구소
POLICE SCIENCE INSTITUTE

북한의 대남 사이버공작 대응 방안 연구*

- 법적·제도적 개선방안을 중심으로 -

A Study on Countermeasures to Deter North Korean Cyber Maneuvers against South Korea

- Focusing on Legal and Institutional Improvements -

김 윤 영**

차 례

● 국 문 요 약 ●

북한의 대남 사이버공작기관은 사용자의 비대면성과 익명성, 활용의 편리성, 대상의 광범위성, 통신의 쌍 방향성, 확산의 신속성, 정보 조작과 축적의 편리성, 경비의 저렴성, 보안유지의 용이성 등을 역이용해 국내 주요 국가 기관 전산망 해킹, 대남 선전·선동, 유언비어 살포 등을 통해 국론분열 조장, 역정보 누출, 정보교란 등의 대남 사이버공작을 수행하고 있다.

북한의 대남사이버 공작기관은 사이버공간을 더욱 지능화·고도화된 '사회주의 혁명의 해방구'로 악용하고 있는 현실에 우리가 어떻게 대응하느냐에 따라 국가의 안보가 좌우될 수 있다. 정보화의 발전은 국민들에게 편익을 제공하기도 하지만, 개인과 기관에 대한 사이버공격으로 국민생활과 국가안보에 직접적인 위협을 주고 있다.

북한의 대남 사이버공작에 대한 문제를 합리적으로 해결하기 위해서 북한 대남 사이버공작 사이트 삭제 및 접속차단, 북한 해커 자금제공 차단, 국가보안법 위반 사이트 일괄 처리 등에 대한 실질적인 법적 근거를 마련하기 위한 '사이버안보' 관련법 보완을 비롯한 제정을 더 이상 미루지 말아야 한다.

* 이 글은 치안정책연구소 2015 연구보고서(북한의 대남 사이버공작 실태 및 대응 방안) 내용 중 일부를 발췌해 수정·보완한 것임

** 경찰대학 치안정책연구소 연구관

북한의 사이버테러에 대한 적극적인 대응을 위해 정부 관련부처의 사이버보안 조직 증설, 정교한 방어 보안시스템의 개발, 사이버 전문 인력의 양성 등을 국가차원의 중장기적 전략 수립도 이루어져야 한다. 이러한 북한의 대남사이버 공작에 대한 완벽한 해결과 대응이 불가능할 수도 있지만, 국내외적 수사공조를 통해 그 가능성을 높아나가야 한다.

◈ 주제어 : 북한, 사이버 안보, 사이버 테러, 사이버 범죄, 사이버공작, 사이버 안보전략, 보안경찰

Ⅰ. 서 론

북한은 1997년 1월 13일 '조선통신'[1]을 해외에 개설한 이후, "인터넷은 항일무장투쟁시기 유격대의 '총'과 같은 무기이며, 극우 반통일 세력과의 투쟁 공간"으로 인식한 가운데, 사이버공간의 취약성을 악용해 국가기관·금융·민간 통신망 등을 대상으로 조직적인 사이버공격을 단행해 국내 안보환경을 무력화시키기 위한 대남공작 활동의 장으로 활용하고 있다.

북한이 대남 사이버공작 활동에 주목하는 이유는 '주체사상(김일성주의)과 선군사상(김정일 주의)을 지도사상'으로 받들어 '전 조선의 공산주의사회 건설' 즉, '남조선혁명(적화통일)'을 수행하는데 있기 때문이다. 이러한 대남혁명 전략 목표 달성을 위해 대남 사이버공작 기관은 '구국전선'과 '우리민족끼리' 등 직영 및 해외 친북 사이트를 개설해, 우리나라 대통령에 대한 원색적인 비난과 비방은 물론, 주한미군 철수, 「국가보안법」 철폐, 반미반전 투쟁, '친미극우보수세력 청산', 민족공조, 북한핵 합리화, 고려연방제통일, 선군정치 선전, 김정은 일가 우상화 및 3대 세습체제 정당화 등에 대한 사이버 공작 활동을 수행하고 있다.

최근 북한의 대남 사이버공작 부서는 청와대와 외교안보 부처, 국회를

1) '조선통신'은 2002년까지 '조선중앙통신'이라는 홈페이지 이름을 사용했다.

대상으로 대통령의 동선, 한미작전계획 등의 주요 정보를 획득하기 위해 해킹을 시도했던 것으로 드러났다.[2] 국정원은 2016년 3월 8일 "북한은 지난 2월말부터 3월초 사이에 정부 주요 인사 수십 명의 스마트폰을 공격, 해킹된 스마트폰에서 통화내역과 문자메시지, 음성통화 내용까지 절취했다"고 밝혔다. 대검찰청 사이버수사과는 지난 8월 1일 북한이 외교부와 방산업체, 대학, 포털 사이트로 위장한 '피싱' 사이트 27개를 개설한 뒤, '비밀번호가 유출되었으니 확인바란다'는 피싱 메일을 정부 외교·안보 부처 공무원과 전문가 등 90명에게 보내 56명의 계정 비밀번호 빼갔다고 밝혔다.[3]

이와 같이 오늘날 북한의 대남 사이버위협은 정부기관 망은 물론 개인 메일, SNS계정 등에 이르기까지 해킹을 시도하는 등 대남 사이버공작이 더 이상 무시할 수 없는 '총성 없는 사이버 전쟁'으로 진화되고 있지만, 우리는 북한의 사이버공작 활동에 대해 제대로 된 대응을 하지 못하고 사회적 혼란과 경제적 피해를[4] 당하고 있는 것이 현실이다.[5] 따라서 북한의 대남 사이버전략과 전략 수준을 정확히 파악해 선제적 대응

2) 국가정보원은 2015년 10월 20일 정보위 국정감사를 통해, 북한이 청와대와 외교안보 부처, 국회 내 컴퓨터에 대한 해킹을 시도했다고 밝혔다("사이버보안법 팽개쳐 北 해커에 문 열어준 국회의원들", 동아일보, 2015. 10. 22); 특히, 국회의 외교 안보 분야를 맡은 정보, 외교통일, 국방위원회 소속 국회의원을 대상으로 국가안보 관련 주요 정보를 노린 해킹 시도가 크게 늘어났다("'정보-외통-국방위 'PC 보안 이상' 2014년의 4배", 동아일보, 2015. 10. 23).

3) "북 추정 해킹조직, 외교안보 공무원 등 이메일 해킹 시도 … 56명 계정 비밀번호 유출", 전자신문, 2016. 8. 1.

4) 지난 10년간 한국에서 사이버공격으로 인한 연 평균 피해액은 3조6천억 원에 달했다(이영, "총성 없는 사이버 전쟁", 한국경제, 2016. 6. 2).

5) 북한의 대남공작기관이 사이버공간을 이용해 무차별적인 흑색선전(黑色宣傳)과 유언비어(流言蜚語) 유포 등 사이버심리전을 전개하고 있어 국민과 청소년들은 아무런 방어기재 없이 노출되고 있다.

전략을 세워 대남 사이버공격 징후를 사전에 파악하고 차단해 피해를 최소화할 수 있도록 준비하는 것이 무엇보다 중요하다.

그럼에도 북한의 대남 사이버공작에 대한 대비책과 관련한 연구는 자료 수집의 한계로 첩보나 정보 등에 근거한 단편적인 수준에 머물고 있다. 물론, 2000년 이후 북한의 정보기관과 IT부서에 근무했던 탈북민들의 증언에 의해 전문가들의 관심을 끌기도 했지만, 몇몇 연구 외에는 심층적인 분석과 대책을 제시하기 보다는 그들의 진술에 의존하는 경향을 보여주고 있다.[6)]

이러한 문제의식 하에 이글은 북한 대남공작기관의 대남사이버 공작 활동 실태 분석에 따른 문제점을 중심으로 법적·제도적 개선방안을 제언하고자 한다. 이를 위해 문헌연구와 행태적 접근방법은 물론, 공안기관 사이버 담당자들이 안보위해 사이트 관련 업무를 처리하는 과정에서 경험하는 각종 애로사항 등을 적극 반영해 대응 방안을 모색하고자 한다. 이러한 작업은 북한의 대남혁명 전략에 따라 수행되는 대남 사이버 공작 활동의 본질을 간파해 실무차원의 대응전략을 수립하는데 기초자료로 활용될 수 있을 것이다.

Ⅱ. 북한의 대남사이버공작 배경

1. 대남 사이버공작 요인과 방침

1) 대남 사이버공작 요인

최근 북한이 대남 사이버공작에 총력을 기울이는 주요 요인을 세 가

6) 김윤영, 북한의 대남 사이버투쟁에 관한 연구, 치안정책연구소 연구보고서, 2008, 3쪽 참조.

지 측면에서 찾을 수 있다. 첫째, 한국사회의 세계적 수준의 사이버 인프라를 역이용해 사이버심리전, 사이버해킹, 사이버테러 등을 통해 원하는 목표를 손쉽게 달성할 수 있기 때문이다. 우리나라 사이버 인프라 수준은 인터넷 속도, 전자정부지수, 인터넷 접속가구 비율, ICT 발전지수, 디지털 기회지수(Digital Opportunity Index)등은 세계적 수준에 있다. 우리국민의 인터넷 이용률은 전체 인구의 91.5%로 나타났다.[7] 북한은 세계 최고수준의 우리나라 사이버 인프라 수준을 '대남공작' 수행에 활용할 수 있는 최상의 공간으로 인식하고 있다.

〈표 1〉 한국의 IT 인프라 수준

지표 내용	순 위	평가 주관기관
인터넷 속도	1위	2014 글로벌 온라인 트렌드 조사 보고서(한국관광공사)
전자정부지수	1위	UN E-Government(전자정부) 2014(안전행정부)
인터넷 접속가구 비율	1위	2014 정보사회측정보고서 (국제전기통신연합: ITU, 2014. 11. 24 현재)[8]
세계정보통신기술(ICT: Information & Communication Technology) 발전지수(IDI, ICT-Development Index)	2위	
디지털 기회지수(DOI: Digital Opportunity Index)[9]	2위	

7) 2014 글로벌 온라인 트렌드 조사 보고서, 한국관광공사, 2015. 3, 11쪽.

8) ITU(국제전기통신연합)은 International Telecommunication Union의 약자이다.

9) 인터넷의 △인프라(보급률 등) 보급 △기회제공(소득대비 통신요금 비율 등) △활용정도(이용률 등) 등의 종합적인 분석을 통해 정보통신의 발전을 평가하는 지표다("[IT강국 한국] 한국, 디지털기회지수(DOI) 세계1위", 세계일보, 2005. 11. 17).

둘째, 북한의 대남 사이버공작을 통해 저비용으로 '남조선혁명'을 수행할 수 있기 때문이다. 북한이 남파간첩을 통한 지하당 구축, 각종 정보수집 등에는 많은 비용과 시간이 소요되고 남파 후 체포될 위험성이 따르지만, 현대사회에서 비대칭전략의 하나로 자리 잡은 사이버공작의 경우 저비용으로 주요 통신망에 실시간 접속해 각종 정보를 해킹하고 무력화시킬 수 있어 '남조선혁명'을 위한 최상의 수단이 되고 있다.

셋째, 북한의 대남 사이버공작은 익명이나 변조된 IP주소를 이용해 공격자와 공격지점을 은폐할 수 있어 비교적 노출위험이 적고 안전하다는 점이다. 북한의 대남 사이버공작은 중국 등 제3국의 서버를 이용하고 있어 공격자의 신분을 찾아내기 어렵고, IP 등을 추적해 사이버공격의 진원지를 찾아내도 북한이라는 증거를 입증하기 쉽지 않다.

2) 대남 사이버공작 방침

북한은 1990년대 들어 사이버공간의 전략적 중요성을 인식하기 시작했다. 미국이 1991년 걸프전에서 첨단장비를 이용한 정보전을 통해 승리하자 많은 국가들이 정보전에 대한 새로운 인식을 가지게 되었다. 북한은 이라크전쟁과 코소보전쟁에서 미국의 강화되는 정보전 수행능력이 공중작전이나 지상작전과 결합될 때 엄청난 파괴성과 효과성들을 실감한 후,[10] 김정일은 이라크 전쟁 이후 인민군 최고 수뇌부를 모아 놓고 정보력의 중요성에 대해 강조했다.[11]

---

10) 변상정, "북한의 사이버 위협 능력과 사이버 안보전략", 국가안보전략연구원 연구보고서, 2013. 8, 3쪽.

11) "지금까지 전쟁은 알(총탄 포탄 등) 전쟁, 기름 전쟁이었다면 21세기 전쟁은 정보전이다. 즉 누가 평소에 적의 군사기술정보들을 더 많이 장악하고 있는가, 그리고 전장에서 적의 군사지휘정보를 얼마나 강력하게 제어하고, 자기의

북한은 김정일의 지시에 의해 2000년대 중반 이후 DDoS 공격, 전산망 파괴, 해킹 등으로 사이버 능력을 강화하고, 공격 주체를 은폐하는 능력도 더욱 교묘해지고 있다. 최근에는 국가 주요 기반시설의 제어 시스템을 폐쇄망으로 운영함으로써 직접 해킹이 곤란해지자 유지·보수업체의 PC를 장악해 우회 공격을 시도하고 있다.[12)]

결국, 북한은 대남 사이버공작을 '남조선혁명' 목표 달성을 위한 핵심 전력으로 인식했다. 김정일, 김정은의 지시에 따라 북한 대남공작기구들은 대남 사이버공작 전담부서를 운영하며, 사이버공작을 지속화하고 있다. 김정일과 김정은은 대남 사이버공작의 중요성을 강조하고 있는데, 그 내용을 아래의 표와 같이 정리할 수 있다.

〈표 2〉 김정일·김정은 사이버 관련 교시 내용[13)]

구 분		교 시 내 용
김정일	사이버공간의 중요성 강조	· 인터넷은 국가보안법이 무력화되는 특별한 공간이다. · 남한당국이 통제할 수 없는 공간이다(2003. 7) · 남한 내 인터넷을 적극 활용하라
	사이버공격의 중요성 강조	· 사이버공격은 원자탄이고 인터넷은 총이다. · 21세기 전쟁은 정보전쟁이다. 현대전은 전자전이다. 전자전에 따라 현대전의 승패가 좌우된다.
	사이버전력의 강화 강조	· 더 많은 정보전사를 양성하라 · 사이버부대는 나의 별동대이자 작전 예비전력이다.
김정은	사이버공격의 중요성 강조	· 사이버전은 핵, 미사일과 함께 인민군대의 무자비한 타격능력을 담보하는 만능의 보검이다 (김정은 2013년 8월 정찰총국 군간부들에게)
	사이버전력의 중요성 강조	· 강력한 정보통신 기술, 정찰총국과 같은 용맹한(사이버) 전사들만 있으면 그 어떤 제재도 뚫을 수 있고, 강성국가 건설도 문제없다(김정은 2013년 4월 7일 정찰총국 해커부대 방문시)

정보력을 충분히 구사할 수 있는가에 따라 전쟁의 승패가 좌우된다."(김흥광, "북한의 사이버정보 실태", 북한, 2005년 5월호, 북한연구소, 32쪽 재인용)

12) 변상정, 앞의 글, 2쪽.

구 분		교 시 내 용
	사이버거점 장악과 무력화 지시	· 적들의 사이버 거점들을 일순에 장악하고 무력화 할 수 있는 만반의 준비를 갖추라(김정은 2014년 6월 28일 정찰총국 사이버부대인 121국 비공개 방문시)
	전략사이버사령부 창설 지시	· 김정은 2012년 북한군 총참모부 정찰총국 산하기구 110호 연구소를 방문해 '전략사이버사령부 창설' 지시 – 2014년 북한 사이버전력 최대 6000명: 이들은 직접적인 해킹을 기획하는 정찰총국 예하 병력 1200명, 기술지원 인력 1800명, 정찰총국 외 유관조직에 산재된 사이버 요원이 3000명 정도 – 사이버 영재는 중학교 시절 조기 발굴해 매년 300명씩 사이버 전사로 집중 양성
	사이버 인력 확보 지시	· 각 도의 제1중학교에서 유능한 컴퓨터 전문가를 양성하라 지시(2009. 10)

2. 대남 사이버공작 전술과 운영

1) 대남 사이버공작 전술

북한의 사이버 전략·전술과 관련한 공식자료는 알려진바 없다. 다만, 북한에서 사이버부대 및 IT관련 출신 탈북민들의 인터뷰나 언론사들이 이른바 '대북소식통'을 인용해 보도한 자료가 전부라 할 수 있다. 탈북민 김흥광(함흥컴퓨터기술대학 교수)에 따르면, 북한은 "인터넷은 제도적 기반과 정규군을 가진 일본군과 맞서 싸우던 항일빨치산의 투쟁무대"와 같다면서 "북한군의 정보 모략전, 해킹, 사이버심리전, 대남공작이 북한이 아닌 제3국에서 벌어지는 것으로 하여 적에게는 노출될 위험이 적고,

13) 임종인 외, "북한의 사이버전력 현황과 한국의 국가적 대응전략", 국방정책연구, 제29권 제4호, 2013년 겨울호, 14-15쪽 재정리.

반면에 적대국에서는 인터넷이 제도화되고 공개되어 있기 때문에 드러난 공격위험을 가지고 있는 더없이 유리한 작전공간으로 간주하고 있다"고 한다.[14]

북한 군부는 아프간전쟁(2001)과 이라크전쟁(2003)에서 미국이 '지휘통제자동화체제'를 이용해 소수의 군사력으로 승리하는 과정을 보고, 중국의 군사교리인 '점혈(點穴)전략'과 '사이버전법'을 벤치마킹하는 등 나름대로의 사이버 정보전을 발전시켜 왔다. 중국은 1990년대 중반부터 정규 군사력으로는 미국을 상대하기 힘들다는 판단 하에 비대칭전쟁인 '점혈(點穴·급소)전쟁' 방법을 채택한 바 있다.[15]

북한의 최근 대남 사이버공작 행태를 살펴볼 때, 북한의 사이버전술은 기습전술, 위장전술, 기만전술, 정보전술, 심리전술, 은폐전술, 파괴전술로 등 다양한 전술을 개발하고 사이버 교전규칙도 마련한 것으로 보인다.[16] 북한 사이버부대 출신 탈북민에 의하면, 북한의 교전규칙은 공격지점(북한 IP) 노출방지를 위해 북한 내부에서 사이버공작(공격작전)을 수행하지 않는 것이 원칙이라고 한다.[17]

2) 대남 사이버공작 운영체계

북한은 국방위원회 직속 정찰총국, 조선인민군 총참모부, 통일전선부

14) 김흥광, "북한의 사이버전 대응과 전략"(비공개발표문), 2004; 유동열, 사이버안보위해활동의 현황과 대책, 치안정책연구소, 2006, 24쪽 재인용.

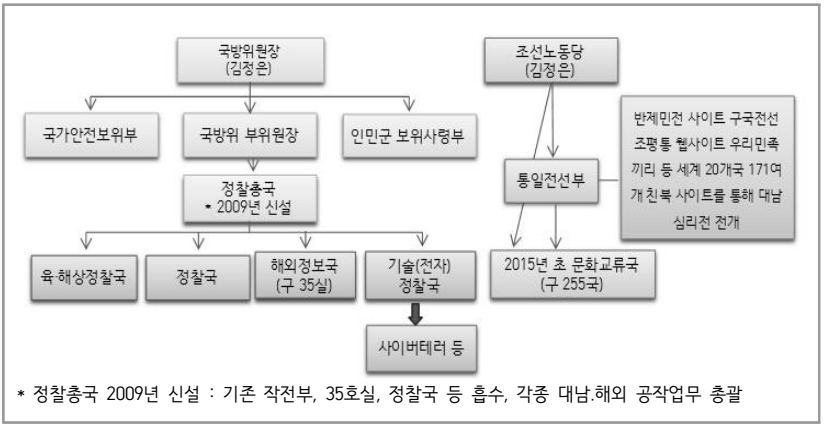
15) 김민석, "북한 사이버전법은 중국의 '점혈 전쟁술' 모방한 것", 중앙일보, 2009. 7. 10.

16) 길민권, "[6.25 해킹] 북한이 사용하고 있는 사이버전 전술은…", 데일리시큐(http://dailysecu.com/news_view.php?article_id=4601; 2015. 7. 20. 검색), 2013. 6. 26.

17) "북한 사이버 부대 귀순자, 3.20을 말하다", 전자신문, 2013. 5. 14.

등에 사이버공작 부서를 개설해 전산망 무력화와 공격을 비롯해 정보수집, 심리전, 해킹 등 대남 사이버공작을 주도하고 있다. 사이버전을 연구하는 국방위원회 산하의 국방과학연구원과 사이버전 전문가를 양성하는 총참모부 직할 김일 정치군사대학(구 지휘자동화대학) 등이 있다. 또한 조선로동당 산하에 사이버전 전담부서로 통일전선부 작전처 작전국과 해외정보국을 두고 있다. 북한의 대남 사이버공작 기구를 다음의 도표와 같이 정리할 수 있다.

〈그림 1〉 북한의 대남공작 기구[18]



첫째, 국방위원회 직속 정찰총국은[19] 기술국 100연구소, 작전국 414연

18) 유동열, "지금 사이버 공간이 대단히 위태롭다" (http://blog.naver.com/PostView.nhn?blogId=jkby1&logNo=220681629428 : 2016. 5. 10 검색), 참조 재구성

19) 북한은 2009년 초 조선노동당에서 수행했던 대남공작 기관을 국방위원회로 이관했다.

락소, 128연락소, 해외정보국의 기초자료 조사실 등 사이버전담부서를 운영하고 있다. 이들 부서는 대남 전략정보 수집, 국가공공망 디도스(Ddos)공격 등 사이버요원 해외 파견 및 거점을 통한 사이버테러와 사이버간첩 교신 등의 업무를 수행하고 있다. 실제, 2009년 7.7 사이버공격, 2011년 3.3 디도스공격 및 4월 농협전산망 해킹 등의 대남 사이버공작 활동을 실행한 바 있다.[20]

둘째, 조선인민군 총참모부에 지휘자동화국(31소, 32소, 57소 등)과 적공국 204소를 설치해 대남 사이버공작을 실시하고 있다. 이들 부서는 국가기관 망 해킹을 통한 정보 수집과 사이버심리전을 물론 군 지휘통신체계 교란과 무력화 등의 임무를 수행한다.

셋째, 조선노동당은 통일전선부 작전처 내에 사이버전담부서를 운영하고 있다. 이부서는 '구국전선'(반제민전 웹사이트)과 '우리민족끼리'(조평통 웹사이트) 등과 같은 170여개 친북사이트를 해외에 개설하여 안보위해세력과의 연계로 대남 사이버심리전 임무를 수행하고 있다. 특히, '댓글공작팀'이[21] 국내 네티즌들의 개인정보를 해킹한 자료를 이용하여 국내 포털사이트 회원으로 가입한 후, 유튜브(YouTube), 트위터(Twitter), 페이스북(Facebook) 등 SNS를 이용한 유언비어와 흑색선전 등을 유포하여 국론을 분열시키는 사이버심리전을 수행한다.

넷째, 외형적으로 내각 산하에 있지만, 통일전선부의 실제적인 지휘통제를 받는 225국(구 대외연락부)은 2012년 말경 통일전선부로 흡수 통합한 후, 2015년 초 문화교류국으로 개칭했다. 문화교류국은 사이버전담부서를 통해 사이버공간을 간첩교신 수단으로 이용하고 있다. 이를 위해

20) 이하 유동열, 사이버공간과 국가안보, 북앤피플・자유민주연구학회, 2012, 52-54쪽 참조해 재정리.

21) 유동열, "'사이버 安保수사' 法制 구축 서둘러야", 문화일보, 2015. 5. 16.

사이버드보크 개발 및 설치, 간첩 임무지령, 대북보고 지시 등의 임무를 수행한다.

이와 같이 북한의 대남공작부서는 별도의 사이버공작 전담부서를 운영하고 있다. 2015년 국정원 및 국군사이버사령부 평가에 의하면 6천여 명(사이버공작 작전 인력 1,700여 명 + 지원 및 기술 인력 4,300여 명)의 사이버 공작요원을 운용하고 있는 것으로 알려졌다.

Ⅲ. 북한의 대남사이버 공작 활동 실태

1. 북한의 대남 사이버공작 활동 양상

북한은 남조선혁명을 실현하기 위한 수단으로 '3대 혁명역량 강화노선'[22]을 채택하고 있다. 이중 북한이 대남 사이버투쟁을 전개하고 있는 것은 '남조선혁명 역량'을 강화하는데 있다. 이를 위해서 사이버공간을 이용해 '남한 내 반정부 및 좌익세력의 활동지원', '남한 민중의 의식화와 조직화', '지하당 및 통일전선 구축', '반혁명역량[23] 제거' 등에 주력하고 있다.[24] 결국, 북한과 그 추종세력들은 대남혁명 전략을 달성하고자 사이버공간을 이용해 사이버공작 활동을 전개하고 있다.[25]

첫째, 북한의 대남 사이버공작 부서는 직영 및 해외개설 사이트를 통

22) 북한은 1964년 2월 당 중앙위 4기 8차 전원회의에서 ①북조선 혁명역량 ②남조선 혁명역량 ③국제적 혁명역량을 강화라는 '3대 혁명역량 강화노선'을 채택하였다.

23) 북한이 규정한 반혁명역량이란 국군, 대공수사기관, 국가보안법 등을 의미한다.

24) 유동열, "북한 및 국내 좌파권의 사이버투쟁 실태", 자유민주연구 제2호, 2007, 41쪽.

25) 김윤영, 앞의 글, 68쪽.

해 대남혁명 전략전술 지침을 하달하고 있다. 반제민전은 구국전선 사이트를 통해 대남투쟁 3대 과제인 '자주·민주·통일'[26] 지침을 하달하고, 친북반한 세력들은 매시기 구국전선 사이트를 통해 '자주·민주·통일' 투쟁 지침을 하달 받아 활용하고 있다. 과거 범민련 및 범청학련 남측본부, 한총련 등은 홈페이지 자유게시판이나 원문 자료실 등에 구국전선이 발표하는 논평과 성명서 등을 실시간 다운로드 받아 게재한 바 있다.[27]

둘째, 북한의 대남 사이버공작 부서는 인터넷 웹사이트를 이용해 사이버 통일전선을 구축하고 있다. 최근 북한은 '민족'을 내세워 통일전선을 형성하고자 '우리민족끼리', '우리민족제일주의', '민족대단결', '민족공조' 등을 주장하고 있다. 전술한 바와 같이 2005년 3대 민족공조, 2006년 3대 애국역량, 2007년 3대 과업 등도 통일전선 차원의 선동구호이다. 이러한 통일전선 구호를 친북 사이트에 집중 게재하여 대남 통일전선을 강화하고 있다.[28]

셋째, 북한의 대남 사이버공작 부서는 사이버공간을 이용해 대미·대남 정보 수집을 하고 있다. 북한의 대남 사이버공작부서 요원들은 우리

26) 자주란 한국사회가 자주독립국가 아니라 '미제'의 강점 하에 있는 식민지사회이므로 '남조선 혁명'을 위해서는 먼저 '식민지 통치를 자행하고 있는 미제국주의 세력을 축출'하여 '민족해방'을 수행하고 민족자주권을 확립해야 한다는 것으로 '반미자주화투쟁'을 의미한다. 이에 따라 한민전(반제민전)과 국내 친북운동권 세력들은 '자주·민주·통일' 중 선차적 임무로 '미제' 타도를 위한 '반미자주화투쟁'을 주장하여 왔다. 민주란 한국사회가 민주주의사회가 아니라 '미제에 빌붙어 연명하면서 인민을 착취'하는 파쇼체제이므로 파쇼체제인 현 정권을 타도하고 '노동계급 중심의 인민민주주의 정권'을 구현하여 '인민(계급)'을 해방해야 한다는 '반파쇼민주화투쟁'을 의미한다. 통일이란 우리사회가 요구하고 있는 자유민주주의로의 통일이 아니라, 북한식 연방제에 의한 공산화통일을 지향하는 것으로 '조국해방'을 위한 '조국통일투쟁'을 의미한다.

27) 김윤영, 앞의 글, 68쪽.

28) 유동열, 사이버공간과 국가안보, 71쪽.

의 국가기관 망에 실시간 접속해 개인정보나 군사 및 산업정보를 비롯한 필요한 자료를 검색하고 해킹해 정보를 수집한다.

넷째, 최근 북한 대남공작부서는 사이버 드보크(Cyber Dvoke), 스테가노그래피(Steganograpy), 이 메일(E-mail) 등을 이용해 간첩과의 교신 수단으로 활용하고 있다.[29]

다섯째, 친북 사이트에 게재된 상징물(깃발・백두산・건축물)을 통해 상징 조작을 하고 있다. 친북 인터넷 사이트는 깃발, 건축물, 조형물, 백두산 등 인위적이고 자연적인 사물을 이용하여 강렬하고 명료한 상징체계를 보여주고 있는데, 이는 북한체제의 선전과 대남혁명을 선전선동하기 위해서 치밀하게 계산된 대남 사이버투쟁의 결과라 할 수 있다.[30]

여섯째, 북한의 대남 사이버공작 부서는 사이버공간을 이용해 시기별 '대남혁명 투쟁 구호'를 하달하고 있다. 2012년 19대 총선과 관련해 반제민전은 '구국전선'에 '총선투쟁 구호'('4.1 총선투쟁' 지침)를 하달해 특정후보 지원 및 특정정당 후보 낙선 투쟁 등을 선전 및 선동한 바 있다.[31] 이 같이 사이버공간을 통해 대남투쟁 구호를 하달해 남한사회의 국론분열과 사회혼란을 조성해 '남조선적화혁명'의 결정적 시기를 만들고 있다.

일곱째, 북한은 악성코드 유포, 서비스거부 공격 등의 방법을 동원해 공공기관 망, 언론 망, 민간 망 등을 대상으로 사이버테러를 전개하고 있다. 사이버테러 방식도 디도스(분산서비스거부)를 통한 서버장애로부

29) 김윤영, 앞의 글, 74쪽.

30) 위의 글, 76쪽.

31) 대표적인 선거투쟁 구호로는 "○○○당이 당선되면 핵전쟁터진다", "이번 총선에서 ○○○당 낙선시키고 평화옹호세력인 진보○○진영 후보를 대거 당선시키자", "각지에서 ○○○당 후보낙선운동을 강력히 전개하자!" 등이다

터 해킹을 통한 데이터 삭제, 하드디스크 파괴, 통신망 마비, 스마트폰 악성코드 유포 등의 행태로 고도화되고 있다. 이외에도 북한의 사이버 공작요원들은 해킹을 통해 우리의 국가기관 망, 공공 망, 상용 포탈 망 등에 실시간 접속해 각종 정보와 자료를 절취하고 있다. 북한의 사이버 요원들은 신종 악성코드 개발, 사이버공격 주체 은폐 기술을 비롯해 상당 수준의 정보수집과 해킹 프로그램 개발 능력을 보유하고 있다.[32]

여덟째, 사이버공작을 통해 외화벌이를 하고 있다. 북한의 대남공작부서는 중국 선양, 다롄, 베이징 등 세계 각국에 사이버전사(해커)를 파견해, 합법회사를 가장한 거점에서 사이버 공작은 물론 게임, 도박 프로그램 개발과 불법 사이버 도박회사를 운영해 연간 10억 달러 규모의 외화벌이 사업도 병행하는 것으로 알려졌다.[33] 이외에도 해커들을 동원해 국내 유명 온라인게임 서버를 해킹해 게임 아이템을 수집하고, 불법 프로그램을 제작·배포하기도 한다.

2. 대남 사이버공작이 국내 안보환경에 미치는 영향

안보위해세력들은 북한의 직영 및 해외 개설 인터넷 웹사이트에 게재된 북한체제 선전, 반미·반정부·반자본주의 투쟁 선전선동 등의 글들을 다양한 경로를 통해 다운받아 자체적으로 개설한 웹사이트 등에 여과 없이 게재하여 전파하고 있어 우리사회의 안보환경에 직접적인 악영향을 미치고 있다.

32) 김윤영, "Ⅲ, 북한의 대남 사이버공작활동 전망", 2015 치안전망, 치안정책연구소, 2014, 치안정책연구소, 300-301쪽 재정리.

33) 유동열, "북한의 사이버 위협 실태와 대책", 한반도 평화정착을 위한 우리의 과제 학술대회 자료집, 동의대학교 국가안전정책대학원, 2016. 6. 25, 60쪽.

첫째, 북한 사이버공작부서가 개설한 직영 및 친북해외 사이트에 대해, 우리정부 관계당국이 국내 접속을 차단했음에도 친북 네티즌들은 해외 프록시 서버 등을 이용해 접속한 후 자료를 다운 받아 국내 포털사이트나 카페, 블로그와 자유게시판, 자료실 등에 게재하고 댓글을 통해 전파하고 있다. 이외에도 웹사이트 간 상호 링크를 통해 북한 주장과 논조를 공유할 수 있도록 하고 있다. 경찰은 사이버안보사범을 색출해 사법처리하는 한편, 북한의 직영 및 해외 친북사이트의 접속차단과 인터넷 웹상에서 게재된 안보위해문건의 삭제, 불법 인터넷 카페 폐쇄 등의 업무를 수행하고 있다.

이러한 조치에도 불구하고 북한은 국내 특정 사이트와의 연결망 구축, 국내 특정 사이트 특정 방 접속 시 북한 개설 사이트와 자동연결 등의 다양한 방법을 동원해 사이버공작을 강화하고 있다. 여기에 SNS 선전선동 방식을 이용하고 있다. 특히, 북한의 대남 사이버 공작기관은 '댓글팀'을 가동해 남한 내 동조세력과 연대해 정권퇴진 등 반정부 여론 조성과 조작 등 국론 분열을 조성하고 있다.[34)]

둘째, 북한의 직영 및 친북해외 사이트의 주장과 논조 등을 안보위해세력들은 트위터, 페이스북, 유튜브 등 SNS를[35)] 통해 실시간 전파하고 있다. 이는 인터넷과 스마트폰의 급속한 확산에 따른 SNS의 보편화와 사용인구가 급증한데 따른 것이다. 2014년 현재 스마트폰의 국내 보급대수는 4,000만대를 넘어서 인구대비 스마트폰 보급률은 79.4%로 세계 1위 수준에 있다.[36)]

---

34) 치안전망 2014, 치안정책연구소, 2015, 248쪽.

35) 트위터 등 SNS는 가입절차가 간단하고 지연·학연을 초월한 쌍방향 커뮤니케이션으로 신속한 정보를 공유할 수 있는 장점도 있는 반면, 신분을 숨긴 채로 왜곡된 정보를 전파하는 등 정보를 조작할 수 있는 단점도 있다.

친북 SNS는 우리민족끼리, 로동신문 등의 주요 해외 친북사이트 게시물을 수많은 팔로워(follow)를 통해 친북정보를 실시간 전달하는 전파력을 가지고 있으며 그 파급력은 상상을 초월한다. 최근 사이버상에서 이루어지는 친북활동의 주요 수단들이 인터넷 카페, 블로그, 포털 등에서 전파력이 크고 신분 은닉이 용이한 트위터, 페이스북 등과 같은 SNS로 이동하고 있다. 이러한 SNS를 이용한 사례로 해외 친북 트위터 계정인 '우리민족끼리'를 리트윗한 사례도 있다.[37] 또한 종북카페 활동과 오프라인 활동을 주로 수행하면서 SNS를 보조수단으로 사용하는 경우도 다수인 것으로 알려졌다.

경찰청의 친북 SNS 등에 대한 차단 조치 결과에 대한 자료를 보면, 2010년 33건에서 2014년에는 960건으로 급증했다. 2015년 6월말 현재까지 564건을 차단하여 2014년 960건과 비교했을 때, 이미 58.8%에 이르고 있다. 특히, 동영상을 서로 주고받는 유튜브를 이용한 유포사례가 급증하는 특징을 보여주고 있다. 동영상의 주요 내용은 북한 주장을 인용·동조하거나 친북게시물을 이용한 반정부투쟁을 선전·선동하는 내용을 담고 있다. 당국의 친북 사이트, SNS 등에 대한 차단조치가 증가하고 있는 것은 역설적으로 북한의 대남투쟁 선전물이 증가하고 있다는 의미로 볼 수 있어 적극적인 대응책이 요구되고 있다.

---

36) 인터넷 동향보고서, 한국정보진흥원, 2014; "선생님들의 고민", 강원도민일보, 2015. 5. 15 재인용.

37) 박○○은 2010~2011년 북한 노동당 외곽 대남선전 기구인 조국평화통일위원회가 개설한 트위터 계정인 '우리민족끼리(@uriminzok)'를 팔로우한 뒤, 자신의 트위터 계정으로 리트윗해, 게시내용을 퍼뜨리거나 동영상 등 이적표현물을 링크한 혐의로 2012년 1월 구속 기소되었으나, 대법원은 2014년 8월 28일 무죄로 확정했다("'우리민족끼리' 리트윗 20대 국보법 위반 무죄 확정", 연합뉴스, 2014. 8. 28).

우리 관계 당국의 지속적이고 적극적인 접속차단 조치에도 불구하고 북한은 직영 및 해외에 서버를 둔 웹사이트 171여개 망과 기 구축된 SNS망 등의 진일보된 방법을 동원해 사이버공작을 더욱 강화하고 있다. 경찰이 2000년부터 2015년 6월말 현재까지 친북사이트 171개를 발견해 134개를 차단했던 사실에 잘 반영되어 있다. 또한 2010년부터 2015년 6월말까지 친북성향 SNS 계정 2,341건을 차단했다. 이러한 차단 조치에 대해 북한은 제2·제3의 대체 사이트를 구축해[38] 사이버공작을 강화하고 있다.

셋째, 안보위해세력은 사이버공간을 통해 북한의 대남공작 투쟁지침을 하달 받고 있다. 북한이 웹사이트를 통해 하달하는 대남혁명 지침을 안보위해세력들은 실시간 내려 받아 투쟁 지침으로 활용하고 있다.[39] 실제, 북한은 반제민전 웹사이트 '구국전선' 등을 통해 '민족해방민주주의혁명(NLDR)전략'·대남투쟁 3대과제(자주·민주·통일)·대남투쟁 3대목표(반미자주화, 반파쇼민주화, 조국통일투쟁)를 비롯해 통일방안인 '조국통일 3대헌장'[40]·'김정일 민족대단결 5대방침'[41]·'연방연합제 통일방안'(김정일의 연방제안, 낮은 단계 연방제) 등을 하달하고, 안보위해세력들은 이를 다운 받아 웹사이트에 게재해 전파하거나 투쟁 지침으로 받

38) 반제민전 홈페이지 '구국전선' 웹사이트를 차단하자 제2·제3의 대체 사이트를 개설하였다.

39) 김윤영, 앞의 글, 82쪽.

40) 북한의 조국통일 3대 헌장은 조국통일 3대원칙(자주, 평화통일, 민족대단결), 고려민주연방공화국창립방안, 전민족대단결 10대강령을 의미한다.

41) 민족대단결 5대방침은 김정일이 1998년 4월 18일 "온 민족이 대단결하여 조국의 자주적 평화통일을 이룩하자"라는 논설을 발표한 이후 통일강령으로 채택되었다. 민족대단결 5대방침은 ①민족자주원칙 견지, ②애국애족, 조국통일의 기치 밑에 대단결, ③남북관계 개선, ④외세·반통일 세력 반대, ⑤온민족의 접촉·대화와 연대·연합 강화 등이다.

들고 있다.

이외에도 해외 친북 사이트가 게시한 선전물들은 2011년 27,090건에서 2012년 41,373건으로 급증했다가 2013년에는 33,865건으로 다소 감소한 현상을 보여주었다. 2013년에 선전물이 감소한 이유는 김정은 후계체제 정착을 위해 내부결속에 주력했기 때문으로 보인다. 또한 김정일이라는 구심점이 사라짐으로 인해 친북세력 간 선명성 경쟁의 필요성이 감소한 것도 한 요인이라 할 수 있다. 이러한 사실은 2014년 해외친북 사이트에 게재된 선전물이 39,764건으로 증가한 사실에서 알 수 있다.[42]

최근 북한은 천안함 폭침(2010. 3. 26)과 연평도 폭격(2010. 11. 23), 3대 세습체제와 김정은의 공포정치 등으로 대중적 호응도가 낮은 '북한체제 찬양'에서 대중적 공감대의 형성이 가능한 '남한체제 비하'로 전술적 변화를 보여주고 있다. 이는 2011년 1월에서 10월까지 해외친북 사이트 선전물 중 북한 찬양·선전물이 64.6%로 반미·반정부 선전물 35.4%보다 29.5% 높게 나타났으나, 2011년 11월부터 2012년 3월까지의 경우를 보면 반미·반정부 선전물이 과반수가 넘는 51.2%로 급증했던 사실에서 찾을 수 있다.[43]

넷째, 남한사회에 대한 왜곡정보 및 역정보 등의 누출로 사회적 혼란을 조성하고 있다. 북한의 직영 및 해외 개설 웹사이트는 쌍방향적 교류를 허용하지 않거나 제한하고, 일방적인 자료만 제공해 북한에 대한 잘못된 환상과 반미·반정부 의식을 가지도록 하고 있다. 북한정보를 얻기 어려운 환경에서 네티즌들은 이들 사이트에 의존하게 되는데, 신뢰할 수 없는 과장된 정보를 그대로 수용할 위험성이 매우 크다. 실제로 안보위해 웹사이트 중에는 북한 선전선동 웹사이트에 게재된 각종 논평, 성명

42) 경찰청 자료, 2015. 6월 현재.

43) 경찰청 자료, 2012. 4월 현재.

등 북한의 주의 주장을 원문 그대로 복사 게시하고 있어 방송통신위원회 결정으로 삭제되고 있다.[44]

특히, 북한은 한국과 미국에 대한 왜곡된 허위정보를 사이버공간을 통해 안보위해세력들에게 투쟁 지침으로 제공해, 반미·반정부 투쟁의식을 고취시키고 있다. 북한은 그들이 자행한 천안함 폭침과 연평도 폭격을 한·미당국의 자작극으로 왜곡·날조한 선전물을 해외개설 웹사이트에 게재하고, 이러한 선전물을 안보위해세력들은 무차별적으로 다운받아 자신들이 개설한 웹사이트 등에 게재해 반미·반정부 의식을 고취시키고 있다. 천안함이 폭침된 지 5년이 되었지만, 북한과[45] 일부 세력들은[46] 남북대결 국면을 조성하기 위한 한국정부의 자작극이라 비방하고 있다.

다섯째, 북한 및 안보위해세력들은 사이버공간을 통해 국가안보를 위해하는「국가보안법」위반 불법정보를 무차별적으로 전파하고 있다. 방송통신심의위원회(이하 방심위)의「국가보안법」위반 친북·이적 사이트 시정요구(삭제·차단·폐쇄) 현황을 보면, 2008년부터 2015년 9월 18일 현재까지 8,997건에 이르고 있다. 이중 2015년 9월 18일 현재 1,274건은 2014년 한해 보다 12%(1,137건) 증가한 것이며, 삭제 또한 2014년

44) 김기영, "해외에 개설된 북한 선전사이트 활동실태 및 대응방안", 서강대학교 석사학위논문, 2012, 57쪽.

45) 북한 국방위원회는 2015년 5월 24일 정책국 성명을 통해 "5·24 조치는 날조된 천안호 침몰사건을 등대고 꾸며낸 대결조치이며 부당한 근거에 기초한 결과는 부당하기 마련"라고 날조했다.

46) 한○○ 목사는 천안함 폭침 사건으로 어떠한 방북도 허가되지 않는 상황임에도 밀입북하여 2010년 5월 22일 평양 인민문화궁전에서 북한 언론과 평양 주재 특파원을 상대로 기자회견을 열어 "천안함 침몰 사건은 이○○식 거짓말의 결정판"이라며 "6·15를 파탄 내고 한·미 군사훈련 등으로 긴장을 고조시켜 온 이○○이야말로 천안함의 희생자들을 낸 살인 원흉"이라고 주장했다(편집국, "천안함5주. 자작극괴담 종북세력 여전히...", 미디어펜(http://www.mediapen.com/news/articleView.html?idxno=69626), 2015. 3. 25).

한 해보다 182%(463건) 급증했다. 2015년 시정요구 요청 기관은 국정원 23건, 경찰청 1,251건으로 나타났다. 삭제된 사항을 보면 노동자단체 자유게시판 78%, 포털(블로그) 14%, 기타(일반) 사이트 8% 등 이다.[47]

그러나 삭제 시정요구 463건 중 61%인 281건은 방심위 시정 요구사항을 이행하지 않은 것으로 나타났다. 미이행 사이트는 진보넷, 방치된 사이트(또는 관리자 성향) 등이다. 접속차단은 해외 동영상 계정 63%, 북한 사이트 19%, 기타(블로그, SNS 등) 18%로 동일 계정(tonpomail, soffkj4y, willon200man) 동영상·블로그 등이 대부분이다. 이용해지는 대법원에 의해 인터넷신문등록 취소 확정판결(2015. 2. 13)된 인터넷 신문 '자주민보'(2015. 3. 26)이다. 이같이 최근 국가위반 불법정보가 급증하고 있다는 사실을 고려해 적극적인 대책이 요구되고 있다.

여덟째, 최근 북한 해커조직은 한국 범죄조직과 연계해 사이버공간을 외화벌이를 수단으로 활용하고 있다. 북한의 대남 사이버공작부서는 해커들을 동원해 국내 유명 온라인게임 서버를 해킹해 게임 아이템을 수집하고, 불법 프로그램을 제작·배포하기도 한다. 실제, 경찰은 중국에서 북한 노동당 39호실 소속 해커들과 수회 접촉하여 해킹에 필요한 노트북과 현금 등을 제공하고 DDos공격이 가능한 악성코드가 심어진 오토프로그램을[48] 전달받아 불특정다수의 네티즌에게 유포하여 개인정보 약 1억4천여만 건을 불법 취득한 후, 그 중 상당부분을 북한에 유출한 C씨(29세)를 체포해(2013. 3. 17) 구속 송치한 바 있다.[49]

47) 방송통신심의위원회, 2015. 9. 18 현재.

48) 컴퓨터에 깔아두면 자동으로 게임을 진행하여 아이템을 수집하는 '자동 사냥 프로그램'이다. 북한 IT조직의 대표적 외화벌이 수단이며 국내에서 인기 있는 리니지·디아블로 등에 대한 오토프로그램이 다수 유통 중에 있다.

49) "경찰, 국가안보 수호와 탈북민 정착지원에 앞장", 경찰청 브리핑, 2014. 2. 19.

Ⅳ. 북한의 대남 사이버공작에 대한 법적·제도적 개선 방안

1. 법적 개선

전술한 바와 같이, 북한의 대남 사이버공작 활동과 관련된 웹사이트에 대한 접속차단, 게시된 불법선전물의 삭제를 위해서는 「국가보안법」,[50] 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 정통망법) 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」(이하 시행령)에 따라 경찰청 등 관련 행정기관의 요청으로 방심위의 심의를 거쳐야 한다. 사이버상에서 이루어지는 대남 공작활동의 특성상 빠른 조치가 이루어져야 하나 심의의 절차적인 요건들에 의하여 그 시기가 오래 걸리는 경우가 많다. 이러한 문제점을 해결하기 위해서 법령의 개선이 조속히 이루어져야 하는 실정이다.

50) 「국가보안법」 제7조(찬양·고무 등)은 북한과 같은 반국가단체나 구성원의 활동을 찬양·고무·선전 또는 동조하는 행위, 국가변란을 선전·선동하는 행위, 불법선전물을 제작·반포하는 행위 등에 대해 처벌하도록 하고 있다. 즉, 제7조(찬양·고무 등) ① 국가의 존립·안전이나 자유민주적 기본질서를 위태롭게 한다는 정을 알면서 반국가단체나 그 구성원 또는 그 지령을 받은 자의 활동을 찬양·고무·선전 또는 이에 동조하거나 국가변란을 선전·선동한 자는 7년 이하의 징역에 처한다. … ⑤ 제1항·제3항 또는 제4항의 행위를 할 목적으로 문서·도화 기타의 표현물을 제작·수입·복사·소지·운반·반포·판매 또는 취득한 자는 그 각항에 정한 형에 처한다. ⑥ 제1항 또는 제3항 내지 제5항의 미수범은 처벌한다. ⑦ 제3항의 죄를 범할 목적으로 예비 또는 음모한 자는 5년 이하의 징역에 처한다.

1) 국가안보 위반 관련 사이트 우선 조치

북한의 대남 사이버공작을 차단하기 위해서는 방심위 심의 결과에 따라 친북 국내외 사이트나 불법정보 게시물에 대한 신속하고 즉각적인 시정요구(삭제·이용해지·접속차단)를 위해 심의 절차에 필요한 기간을 최소화하는 방안을 강구해야 한다.

법령상 명시된 불법정보 시정조치를 위한 소요기간을 최소화하기 위해, 정통망법에 긴급 차단·삭제를 위한 조항을 신설하는 것도 하나의 방법이 될 수 있다. 정식 절차에 의한 심의 결정을 기다릴 수 없는 긴급한 상황이 발생할 경우에는 선 시정조치, 후 심의 절차를 진행하는 방안이다. 긴급 조치의 필요조건은 '불법정보가 관계 법령을 위반했다'고 인정될 만큼 명백한 경우와 '긴급히 차단·삭제하지 않을 경우 회복하기 어려운 결과를 초래할 것으로 인정'되는 경우 등을 고려해 최소한도로 한정하는 방안을 검토해야 한다.[51]

〈표 3〉 불법정보 조치 단계별 소요기간

조치 단계	소요기간	관련 법률
심의 요청 (방송통신위 → 방송통신심의위)	7일 이내	정통망법
시정요구에 대한 이의신청 기간	15일	방송통신위원회의 설치 및 운영에 관한 법률
이의신청에 대한 재심의 및 재시정요구	15일	〃
삭제명령 전 의견제출 기회 부여 기간	최소 10일	행정절차법
삭제명령 이행 기간	10~15일	〃

출처: 김기영, 앞의 논문, 65쪽.

51) 김기영, 앞의 글, 67쪽.

이외에도 정통망법 내에 「국가보안법」 위반 사이트나 게시물, 방심위의 시정조치 문서 수령 거부와 소재지 불분명 운영자에 대해 관계기관의 요청이 있을 경우, 차단·삭제·폐쇄할 수 있는 조항신설을 검토하는 방안도 필요하다.

2) 「국가사이버안보법」 제정

「국가보안법」을 위반한 사이트나 게시물에 대한 긴급 삭제·차단을 위한 정통망법의 조항 신설이 어렵다면, 정부가 지난 9월 1일 입법 예고한 「국가사이버안보법」이[52] 하나의 대안이 될 수 있다.[53] 「국가사이버안보법」에는 「국가보안법」 위반 사이트와 불법게시물 즉, 불법정보에 대한 즉각적인 삭제·차단·폐쇄와 일관된 제재 조치를 위해 정통망법, 「전기통신기본법」, 「정보통신기반보호법」, 「지능형전력망의 구축 및 이용촉진에 관한 법률」, 「국방정보화 기반조성 및 국방정보자원관리에 관한 법률」 등을 포괄할 수 있는 근거 장치 등이 마련되어야 한다.

현재, 사이버테러 등 위기 발생시 대통령 훈령인 「국가 사이버 안전관리규정」에 근거해 상황전파 등에 주력하고 있어, 실질적 대응이 미흡하다. 당장 「국가사이버보안법」 신설이 어렵다면, 사이버상 유언비어와 흑색선전, 북한 등 반국가단체의 선전선동 문건 게시 행위, 사이버간첩교신 등을 규제할 수 있는 처벌조항을 「국가보안법」 내에 두거나 특별법을 신

52) 이 법안은 정부가 3년마다 사이버안보 기본계획을 수립·시행토록 하고, 사이버 위협 정보를 관리하는 핵심 기구인 '사이버위협정보공유센터'를 국무조정실장 소속으로 두도록 하고 있다("정부, '국정원 주도' 사이버 안보법 입법 예고", YTN, 2016. 9. 1).

53) 20대 국회에서 이철우 의원(국회 정보위원장)이 가칭 「'국가사이버안보에 관한 법률안」을 대표 발의한 바 있다.

설하는 방안도 검토할 수 있다.[54]

3)「국가보안법」위반 동일인·동일단체 사이트 일괄 처리

전술한바와 같이, 정통망법에 따라 방심위의 시정조치로 접속이 차단된 국내외 친북사이트 운영자가 주소·IP·사이트 이름 등을 변경해 운영할 경우, 이를 차단하기 위해서 새로운 심의절차가 진행되어야 한다. 따라서 동일한 친북 국내외 사이트의 경우 주소·IP 주소·사이트 이름 등을 변경해 재등록할 경우, 별도의 심의 절차 없이 기존 심의 결정에 따라 즉시 차단조치가 이루어지도록 관련 법령의 개선이 필요하다.[55] 즉,「국가보안법」위반 사이트를 다양한 방법을 통해 재개설할 경우, 유사성을 인정해 일괄적으로 시정조치를 할 수 있도록 관련 법령을 개정해야 한다.

또한 최근 언론 환경은 1인 미디어가 확산되는 것에 편승해 안보위해 인터넷 신문이 우후죽순처럼 번지고 있다.[56] 이를 고려해 인터넷 신문의 등록 요건을 강화하는 방안도 필요하다. 지난 9월 3일 문화체육관광부는 인터넷신문사의 상시인원을 5명 이상으로 하고, 증빙서류를 제출하지 않으면 등록을 불허하는 내용의 시행령 개정안을 입법예고한 후, 11월 19일부터 시행한다고 밝힌 것은 상당한 의미가 있다.

54) 유동열, 사이버공간과 국가안보, 164쪽.

55) 김기영, 앞의 글, 67-68쪽 재정리.

56) 문화체육관광부 자료에 의하면 인터넷 신문은 2014년 12월 31일 기준 2012년 3,914종, 2013년 4,916종, 2014년 5,950종으로 급속히 늘어나고 있다("사이비 언론 및 인터넷신문 현황", 연합뉴스, 2015. 7. 2 재인용).

2. 제도적 개선

1) SNS상 친북정보 차단

SNS를 통한 친북정보는 정통망법에 따라 관계기관의 요청 있을 경우, 방심위의 심의를 거쳐 「국가보안법」 위반 정보를 차단하고 있다. 그럼에도 북한 대남 사이버공작부서들은 https, 프록시서버 등의 접속 기술로 트위터 등 SNS를 통해 친북정보 및 친북 사이트 링크 등의 방법으로 대남혁명 수행 목적에 악용하고 있다. 이는 해외 위치 중계서버가 국내법을 적용받지 않고 있어 네티즌들이 쉽게 접근할 수 있기 때문이다.

해외 SNS의 계정(ID), https 포로토콜을 통한 트위터 접속은 현행 방식으로 불법정보를 유통할 경우, 다른 SNS와 달리 보안전송 기능을 제공하고 있어 근원적으로 차단하기 어렵다.[57] https 접속방식은 데이터를 암호화하여 정보를 주고받는 방식으로 URL 주소를 암호화하여 전송하고 있어 암호를 해독하기 전에는 차단이 불가능하다. 만약, https의 접속차단의 문제점과 프록시서버를 이용한 우회접속을 차단하기 위한 기술적 문제를 해결한다고 하더라도, 통신비밀보호법 위반과 국가 검열 및 표현의 자유 침해 논란에 대한 검토가 선행되어야 한다. 특히, 프록시서버를 이용한 우회접속을 방지하기 위해서는 이용자의 통신데이터 내용을 확인한 후, 불법정보 사이트의 유·무를 검토해야하는 문제점이 있다. 이 과정에서 개인정보의 도·감청 위배문제가 제기될 수 있다.

이와 같이 북한이 우회접속과 보안접속을 통해 게재하고 있는 불법정보를 차단하기 위해 필요한 고려 사항은 물론 선행적으로 해결해야할 문

57) 친북 계정 페이지를 URL(http://twitter.com/choicik)으로 차단하는 것은 가능하나, 'choicik'라는 계정(ID)을 차단하는 것은 불가능하다.

제점들이 많아 현실적으로 차단하기 어려운 것이 사실이다. 이를 극복할 대체 방안으로 2012년 트위터 측에서 '국가별 콘텐츠 제한정책'을[58] 통해 발표한 정책대안들을 활용하는 방안을 검토할 필요가 있다. 또한 트위터의 친북정보 차단의 실효성에 대한 문제 해결을 위해 방송통신위원회 등 관련기관이 트위터에 직접 업무협조를 통해 요청하는 방안도 검토할 수 있다. 그러나 트위터 측에서 불응하는 등의 비협조에 따른 국가 위상 추락, 정치적 논란 발생 등의 부담에 대한 고려도 필요하다.

2) 대남 사이버공작 대응 매뉴얼 활용

북한의 대남 사이버공작에 대한 별도의 대응 매뉴얼을 작성해 대응할 필요가 있다. 2009년 7월 청와대·국회·국방부 등 국가 주요기관 전산망이 북한의 사이버공격을 받아 일부 홈페이지가 중단되는 사태가 발생한 이후, 경찰청에서는 '사이버침해 대응 매뉴얼'을 만들어 배포한 바 있다. 이 대응 매뉴얼은 사이버침해 사고에 대비한 포괄적인 대응 매뉴얼로서, 북한의 대남 사이버공작에 대비한 구체적인 대응 매뉴얼이 미흡한 상태이다.

따라서 북한의 대남 사이버공작에 적극 대응할 수 있는 별도의 대응 매뉴얼을 제작해 활용할 필요가 있다. 대응 매뉴얼에는 기존 경찰청의 대응 매뉴얼을 참고해, 북한의 대남 사이버공작 부서, 역량, 사이버공작 형태, 해외 사이버공작 인력 등을 분석하고, 대남 사이버공작 형태에 따른 구체적인 대응절차 및 방안을 제시할 필요가 있다. 이외에도 북한의

58) 2012년 1월 26일 트위터 측은 본사 블로그를 통해 국가별 기준에 어긋나는 콘텐츠에 대해 해당국에서만 내용이 차단되도록 하는 국가별 콘텐츠 제한 정책을 발표한 바 있다.

대남 사이버공작 징후를 찾아 낼 수 있는 예방적 차원의 '보안사이버 점검목록'을 사안별·분야별로 작성해 활용하는 방안도 검토해야 한다.

3) 사이버 안보 관련국과의 공조 수사

전술한 바와 같이, 북한은 2015년 9월 현재 20여 국가에 서버를 두고 친북사이트를 운영하며 반미·반정부 투쟁을 선전·선동하는가하면, 안보위해세력에게 투쟁지침을 하달하고 있다. 우리 공안당국은 북한의 친북 인터넷 사이트를 발견해 삭제·접속차단 등을 하지만, 북한과 안보위해세력들은 IP변경이나 프록시 접속방법을 이용해 재접속하는 일이 반복되고 있다. 그럼에도 북한의 대남 사이버공작 활동 근거지로 이용되는 관련국가와 치안협력 체계를 구성해 어떠한 방식을 통해 해결해 나갈 것인가에 대한 구체적인 전략이나 프로그램이 심도 있게 논의되지 못하고 있다. 반면, 2007년 에스토니아 정부가 대규모 사이버공격을 받은 이후, 전 세계 120여 국가는 사이버 전쟁 능력을 발전시키고 있다.[59]

북한의 대남사이버공격을 추적해 원천적으로 차단하기 위해서는 국제협력의 필요성이 증대되고 있다. 북한이 서버를 둔 관련 국가와의 정보를 공유하고 네트워크를 구축해 대남 사이버공작 징후를 사전에 파악하여 신속한 대응체계가 이루어져야 한다. 그리고 대남 사이버공격이 발생하면 관련국가와의 공조체제를 통해 피해를 최소화하는 방안을 마련해야 한다. 특히, 북한 대남 사이버공작 해외거점 국가들인 중국, 미국, 일본, 동남아시아 등의 국가들과 사이버 안보 협력체계를 구축해 인터폴 사이버범죄 관련기구, 국제컴퓨터침해사고 대응협의회(FIRST), FBI컴퓨

59) 안유성, "사이버 안보 대응 역량 강화방안 연구", 정보보호학회지, 제24권 제6호, 한국정보보호학회, 2014. 12, 67쪽.

터 범죄회의 등과 정보공유는 물론 상시적인 협조체제가 가능하도록 해야 한다. 이들 국가의 인터폴 사이버범죄 관련기구와 양해각서를 체결해 세미나, 워크숍 등을 상호 개최하면서 실시간 정보를 공유하는 방안도 적극 검토할 필요가 있다.

Ⅴ. 결 론

북한의 대남 사이버공작기관은 사용자의 비대면성과 익명성, 활용의 편리성, 대상의 광범위성, 통신의 쌍 방향성, 확산의 신속성, 정보 조작과 축적의 편리성, 경비의 저렴성, 보안유지의 용이성 등을 역이용해 국내 주요 국가 기관 전산망 해킹, 대남 선전·선동, 유언비어 살포 등을 통해 국론분열 조장, 역정보 누출, 정보교란 등의 대남 사이버공작을 수행하고 있다.

북한의 대남사이버 공작기관이 사이버공간을 더욱 지능화·고도화된 '사회주의 혁명의 해방구'로 악용하는 현실에서 우리가 어떻게 대응하느냐에 따라 국가의 안보가 좌우될 수 있다. 정보화의 발전은 국민들에게 편익을 제공하기도 하지만, 개인과 기관에 대한 사이버공격으로 국민생활과 국가안보에 직접적인 위협을 주고 있다.

북한의 대남 사이버공작에 대한 문제를 합리적으로 해결하기 위해서 북한 대남 사이버공작 사이트 삭제 및 접속차단, 북한 해커 자금제공 차단, 「국가보안법」 위반 사이트 일괄 처리 등에 대한 실질적인 법적 근거를 마련하기 위한 사이버안보 관련법 보완을 비롯한 제정을 더 이상 미루지 말아야 한다.

그리고 북한의 대남 사이버공작에 적극적인 대응을 위해서 사이버보

안 엘리트 요원 양성, 첨단장비 확보와 보급, 예산 확보는 물론 국민과의 공감대를 조성시킬 수 있는 '사이버 대응 홍보팀' 신설도 필요하다. 북한의 대남 사이버공작의 주요 수단이 트위터, 페이스북, 유튜브(동영상), 플리커(사진) 등 SNS로 이동되고, 최근 첨단화·정교화되는 북한의 대남사이버 공작기법에 대응하는 '전문연구기관'(가칭 '사이버안보 연구소') 신설도 필요한 시점에 있다. 이외에도 북한의 사이버테러에 대한 적극적인 대응을 위해 정부 관련부처의 사이버보안 조직 증설, 정교한 방어 보안시스템의 개발, 사이버 전문 인력의 양성 등을 위한 국가차원의 중장기전략 수립도 이루어져야 한다. 이러한 북한의 대남사이버 공작에 대한 완벽한 해결과 대응이 불가능할 수도 있지만, 국내외적 수사공조를 통해 그 가능성을 높아나가야 한다.

〈논문 접수 : 2016. 8. 8, 심사 개시 : 2016. 8. 23, 게재 확정 : 2016. 9. 21〉

참 고 문 헌

Ⅰ. 국내문헌

1. 단행본

김윤영, 북한의 대남 사이버투쟁에 관한 연구, 치안정책연구소 연구보고서, 2008.

김정일선집(14), 조선로동당출판사, 2000.

양근원・장윤식, 사이버범죄 수사론, 경찰대학, 2008. 3, 3쪽.

유동열, 사이버 안보위해활동의 현황과 대책, 치안정책연구소, 2006.

_____, 사이버공간과 국가안보, 북앤피플・자유민주연구학회, 2012.

치안전망 2014, 치안정책연구소, 2015.

한국관광공사, 2014 글로벌 온라인 트렌드 조사 보고서, 한국관광공사, 2015.

한반도 평화정착을 위한 우리의 과제 학술대회 자료집, 동의대학교 국가안전정책대학원, 2016. 6.

2. 논문

김기영, “해외에 개설된 북한 선전사이트 활동실태 및 대응방안”, 서강대학교 석사학위논문, 2012.

김흥광, “북한의 사이버정보 실태”, 북한, 2005년 5월호, 북한연구소, 2005.

변상정, “북한의 사이버 위협 능력과 사이버 안보전략”, 국가안보전략연구원 연구보고서, 2013. 8.

안유성, “사이버 안보 대응 역량 강화방안 연구”, 정보보호학회지, 제24권 제6호, 한국정보보호학회, 2014.12.

유동열, “북한 및 국내 좌파권의 사이버투쟁 실태”, 자유민주연구 제2호, 2007.

이완수, “국가 사이버 안보 구축전략에 관한 연구”, 경기대 박사학위논문, 2014. 6.

임종인 · 권유중 · 장규현 · 백승조, “북한의 사이버전력 현황과 한국의 국가적 대응전략”, 국방정책연구, 제29권 제4호, 2013년 겨울호.

채재병, “안보환경의 변화와 사이버안보”, 정치 · 정보연구, 제16권 제2호, 2013.

한 희, “사이버 공간과 국가 안보”, 사이버공간과 국가안보, 2014년 국가전략연구소 학술회의 자료집, 국가안보전략연구소, 2014. 4. 17.

3. 기타

길민권, “[6.25 해킹] 북한이 사용하고 있는 사이버전 전술은…”, 데일리시큐(http://dailysecu.com/news_view.php?article_id=4601; 2015.7.20. 검색), 2013. 6. 26.

김정일, “혁명적군인정신을 따라 배울데 대하여”, 조선로동당 중앙위원회 책임일군들과 한담화, 1997년 3월 17일.

김필재, “임종석, 과거 北해커 양성 '김일성대학' 지원”, 뉴데일리, 2014. 10. 21.

김흥광, “북한의 사이버전 대응과 전략”(비공개발표문), 2004.

방송통신심의위원회, 2015. 9. 18. 현재 자료.

"북한 사이버 부대 귀순자, 3.20을 말하다", 전자신문, 2013. 5. 14.

"사이비 언론 및 인터넷신문 현황", 연합뉴스, 2015. 7. 2.

"선생님들의 고민", 강원도민일보, 2015. 5. 15.

유동열, "지금 사이버 공간이 대단히 위태롭다"
(http://blog.naver.com/PostView.nhn?blogId=jkby1&logNo=220681629428(2016. 5. 10. 검색)

이민재, "국가 사이버안보②] 제5의 공간, 사이버", 아이티비즈
(http://www.it-b.co.kr/news/articleView.html?idxno=3754), 2015. 6. 18. 재정리.

이영, "총성 없는 사이버 전쟁", 한국경제, 2016. 6. 2.

인터넷 동향보고서, 한국정보진흥원, 2014.

"정보-외통-국방위 'PC 보안 이상' 2014년의 4배", 동아일보, 2015. 10. 23.

편집국, "천안함5주. 자작극괴담 종북세력 여전히...", 미디어펜
(http://www.mediapen.com/news/articleView.html?idxno=69626), 2015. 3. 25.

< ABSTRACT >

A Study on Countermeasures to Deter North Korean Cyber Maneuvers against South Korea

– Focusing on Legal and Institutional Improvements –

Kim, Yun-Young

North Korean cyber maneuver institutions do actions such as promoting national schisms, the leakage of disinformation, and intelligence disturbance against South Korea through hacking the computer network of South Korean national institutions, anti-South Korea propaganda, and spreading rumors. These are accomplished by using the characteristics of cyber space including the non-face-to-face, the anonymity, the convenience of the usage, a wide range of subjects, the interactivity of communication, the rapidity of spread, the convenience of information manipulation and storage, the inexpensive cost, and the easiness of security.

The security of South Korea depends on our countermeasures against their actions because the North Korean cyber maneuver institutions distort cyber space into an area which is for a more intelligent and sophisticated socialist revolution. Development of ICT(information and communications technologies) provides benefits to citizens, but also directly threatens people's lives and national security from cyber attacks against individuals and institutions.

South Korea should not delay legislation of "Cyber Terrorism

Protection Law" or other laws that relate to cyber security to be substantial legal basis for the deletion and access blocking of the web-sites for North Korean cyber maneuvers, the blocking of North Korean hacker funding, and the batch process against the web-sites violating security law to rationally solve North Korean cyber maneuvers.

Long-term strategy at the national level for the expansion of cyber security organizations in relevant government ministries, the development of sophisticated defense security systems, and the nurturing of cyber experts should be established as an aggressive response to North Korean cyber terrorism. Although it may not be possible to fully resolve the North Korean cyber maneuver against South Korea, we should increase the possibility through national and international investigative cooperation.

◈ Key Words : North Korean, Cyber Security, Cyber Terrorism, Cyber Crime, Cyber Maneuver, Cyber Security Strategy, Security Police