북한의 대남 사이버공격 양상과 행태 : 사이버파워와 강압이론을 통한 분석

윤 태 영*, 우 정 민**

요 약

본 논문은 주요 국제정치이론을 바탕으로 2009년 들어 지속되어온 북한의 사이버 상에서 대남공격 행태를 분석하여 한국의 정책적 대응방안을 제시하는 것이 목적이다. 이를 위해 본 논문은 국제안보학계에서 최근 주목받는 '사이버파워'의 행동영역과 특성 및 '강압의 역동성' 모델을 적용하였다. 북한의 사이버공격 유형은 권력기반 잠식, 지도자 리더십 공격과 음해, 군사작전 방해, 사회불안과 혼란유도 유형으로 분류된다. 사이버파워 유형과 수단 면에서 북한의 GPS 교란, 국방부 서버해킹, EMP 등은 보복·위협성이 강한 하드파워이고, 사이버머니 현금화, 렌섬웨어 등은 소프트웨어를 볼모로 거액의 돈을 강탈하거나 요구하는 점에서 설득·유인의 행동 영역에서 힘으로 분석된다. 북한의 사이버공격은 2차 핵실험을 기점으로 현실적 제재에 따른 탈출구적 성격을 갖는다. 한국은 북한의 공세적 사이버파워가 방법과 능력에서 변화하고 있음을 명확히 인식하고, 북한의 행동이 이득보다 감당할 수 없는 손실이 훨씬 더 클 것이라는 결과를 갖게끔 만드는 것이 중요하다. 이를 위해서는 사이버심리전, EMP공격 대비, 해킹보안의 전문성 강화 등 제도적 보완과 신설을 통해 공격과 방어가 동시에 이루어지는 사이버보안과 역량을 강화할 필요가 있다.

North Korea's Cyber Attack Patterns and Behaviors : An Analysis Based on Cyber Power and Coercion Theory

Taeyoung Yoon*, Jeongmin Woo**

ABSTRACT

The purpose of this paper is to analyze the behavior of North Korea's cyber attack against South Korea since 2009 based on major international security theories and suggest South Korea's policy option. For this purpose, this paper applied the behavioral domain and characteristics of 'cyber power' and 'coercion dynamics' model, which are attracting attention in international security studies. The types of cyber attacks from North Korea are classified into the following categories: power-based incarceration, leadership attacks and intrusions, military operations interference, and social anxiety and confusion. In terms of types and means of cyber power, North Korean GPS disturbance, the Ministry of Defense server hacking and EMP are hard power with high retaliation and threat and cyber money cashing and ransomware are analyzed by force in the act of persuasion and incentive in the point of robbing or asking for a large amount of money with software pawns. North Korea 's cyber attack has the character of escape from realistic sanctions based on the second nuclear test. It is important for South Korea to clearly recognize that the aggressive cyberpower of North Korea is changing in its methods and capabilities, and to ensure that North Korea's actions result in far greater losses than can be achieved. To do this, it is necessary to strengthen the cyber security and competence to simultaneously attack and defend through institutional supplement and new establishment such as cyber psychological warfare, EMP attack preparation, and enhancement of security expertise against hacking.

Key words : Cyber Attack, Cyber Power, Hard Power, Soft Power, Coercion, North Korea

접수일(2018년 2월 19일), 게재확정일(2018년 3월 23일)

* 경남대학교 경호보안학과

** 한국외국어대학교 글로벌정치연구소

1. 서 론

정보화 후기 시대에 나타나는 여러 가지 현상 중에 사이버공간 의존도의 심화는 이제 더 이상 우리에게 새로운 현상이 아니다. 전 세계 국가들의 네트워크화가 진행되고 21세기 사회전반에 걸쳐 나타나는 혁신가치는 물리공간의 제약을 사이버공간의 특성을 활용하여 얻고자하는 접근으로부터 나오고 있다[1]. 사이버공간은 점증하는 위협과 능력에 새로운 전초기지가 되고 있지만 이에 대한 통제나 규제는 부족하다[2].

2010년대 들어 지구촌 네트워크가 본격화되면서 사이버분야는 시·공간적 확장을 통해 다양한 정보력과 기술혁명을 기반으로 생활의 편의를 제공하며 발전해 왔다. 하지만 사이버공간의 동향은 문명적 혜택과 발전 못지않게 중대한 위협에도 직면하고 있다. 이러한 위협들로는 악의적 목적을 가진 범죄자의 증가, 서비스거부 공격이나 중요한 데이터 탈취 등 네트워크상에서의 시스템을 악용하는 경우이다. 이른바 사이버 테러이다.

국제무대에서 진행되는 테러와 대테러의 변화된 움직임 속에서 주목되는 테러주체들 중에는 북한도 결코 예외일 수가 없다. 북한은 1980년대 미얀마 아웅산테러(1983. 10. 9), 대한항공(KAL) 858기 폭파사건(1987. 11. 29) 등 실제공간에서 정치적 공작으로 테러행위를 감행해 왔다. 그러나 2009년대를 기점으로 북한은 가상의 시·공간을 넘나들며 다양한 방법과 경로를 동원해 국제질서를 방해해 왔다. 청와대·백악관 등 35개 주요 정부기관 및 금융사를 겨냥한 디도스(DDoS) 공격(2009. 7. 7), 국회·행정안전부·통일부와 은행·증권사의 좀비PC 공격(2011. 3. 4) 및 농협 전산망 마비(2011. 4. 2), 중앙일보 신문제작시스템 파괴(2012. 6. 9) 등을 감행해 왔다.

2013년을 기점으로 북한의 사이버 상에서 테러행위는 국내외적으로 날로 증가되어 왔다. 국내적으로는 주요 방송사 및 금융기관 서버·PC 악성코드 유포(2013. 3. 20), 청와대·국무조정실·정당 전산망 공격(2013. 6. 25), 대학병원 전산망 서버장악(2014. 8) 및 한수원 조직·설계도 해킹(2014. 12. 15), 금융보안업체 인증서 해킹(2015. 11)이 있었다. 가장 최근에는 '인터파크' 대형쇼핑몰 해킹(2016. 7. 28), 청와대 국가안보실 및 방송사를 사칭해 대통령 음해 E-메일을 전파(2016. 1. 27 / 2. 18), 비트코인 거래소 계좌정보 탈취(2017. 4~12)한 이력이 있다. 이 외에도 국방·통신 분야의 해킹, GPS 공격 등 남한의 주요 핵심부처와 기간산업의 사이버 공격을 지속적으로 감행해오고 있다. 한편 대외적으로도 북한은 베트남은행 국제금융결제망(SWIFT) 해킹 미수사건(2015. 12), 미국 소니 픽처스(Sony Pictures) 영화사 해킹(2014. 11. 24) 및 연방준비은행(FRB) 내 방글라데시 중앙은행 해킹(2016. 2. 5) 등을 시도해 왔다.

이처럼 남북관계 갈등 속에서 북한의 사이버 공격은 정찰총국 산하 '121국'의 주도하에 감행된 것으로 판단되는 대표적 사례이다. 즉, 북한의 사이버테러는 네트워크화된 정치·경제·사회 영역에서 맞게 되는 심각한 안보위협이라 할 수 있다.

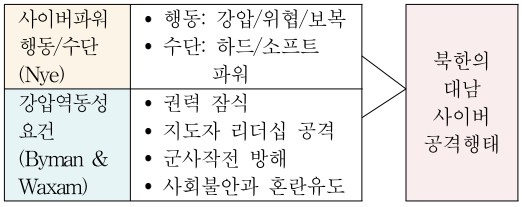
국가 상호간 대립 시 사이버 상에서 구사되는 강압은 실제공간에서의 강압보다 비교적 저비용·고효율로 상대국에 피해를 입힐 수 있다. 다시 말해 사이버 상에서 경성권력(hard power)으로서 힘을 말한다. 현실공간에서 '강압'의 전통적 형태들은 권력기반 침식, 지도자 리더십 공격, 군사작전 방해, 사회적 불안과 혼란 유도, 여론조작과 음해 등이었는데, 본 연구는 이러한 강압 방법들이 북한의 대남 사이버 공격에서도 유사한 형태를 보이고 있다는데 주목하고 있다. 사이버 공간에서 강압은 국가안보 차원의 보안해커의 수적 열세에 따른 상대적 비대칭성과 취약성, 익명성에 따른 서버추적의 어려움, 방어력의 불확실성 등에서 효과적인 수단이 되고 있다. 이는 적대국이 공세적 침투를 통해 사이버 상에서 전략적 우위를 점유하게 만드는 주요 요인이 된다.

이 연구는 사이버 공격의 행위를 강압이론에 따라 유형별로 분류하고, 분류된 유형들에 관한 대응이 어떻게 하면 가능할까라는 문제의식에서 출발한다. 그래서 적대적 관계에서 상대국 행동에 영향을 주는 강압이 사이버 공간에서도 21세기 새로운 형태의 힘으로써 효력과 기능을 할 수 있다는 것을 가설로 설정하였다. 이에 따라 사이버 상에서 북한의 강압을 역으로 강압하는 선제적 대응이 필요하다는 점을 주장한다.

이러한 배경에서 본 논문은 최근 남북관계 갈등 속에서 북한이 사이버 상에서 남한에 대한 공격방법을 강압이론의 유형을 가지고 분석하는데 일차적 목적이

있다. 나아가 대북 대응력으로서 우리정부가 사이버파워 역량을 제고하기 위한 정책적 시사점과 대응방안을 도출하는데 궁극적 목적이 있다.

연구방법은 국제정치학에서 21세기 현안으로 부각되고 있는 조지프 나이(Joseph S. Nye)의 '사이버파워'의 개념과 특성을 토대로, 바이먼(Daniel Byman)과 왁스먼(Matthew Waxman)이 제시한 강압이 역동성을 갖기 위한 주요 요건을 차용하여 분석의 틀로 적용하였다. 본 연구의 시·공간적 범위는 2차 북핵실험을 기준으로 2009~2016년까지이며 북한 김정은 정권의 남북관계로 제한한다.



(그림 1) 분석의 틀

2. 사이버파워(Cyber Power)와 강압이론 고찰 및 연계성

2.1 사이버파워: 개념과 특성

2.1.1 개념

사이버 상에서 적의 공격을 억제하기 위한 힘은 강압(coercion)의 방법이 되는 잠재적인 보복 또는 위협과 제재, 흥정(bargaining)의 방법이 되는 설득과 유인 중에 적절한 선택 또는 결합을 통해 이뤄진다. 이 때 힘은 명령을 내리는 것과 유인하는 행동으로 구별될 수 있다. 만약 힘이 자신이 원하는 결과를 얻기 위해서 다른 이에게 미치는 영향이라면, 보복과 위협 및 제재 또는 설득과 유인을 통해서 상대에게 영향을 줄 수 있다. 하드파워 행위는 보복과 위협 등 강압에 기반을 두고 있고, 소프트파워 행위는 행동지침 구상과 유인, 설득에 기반을 두고 있다. 다만, 하드파워는 대개 위협 내지 회유를 통해 자신의 의도를 따르도록 강제하는 직접적인 힘인 반면, 소프트파워는 상대가 나의 의도를 자발적으로 따르게끔 하는 힘으로 간접적 포섭력을 의미한다[3][4]. 즉 하드파워는 명령하는 힘이며, 소프트파워는 동조하게 만드는 힘으로 요약될 수 있다[3]. 이러한 행동영역(spectrum)은 다음과 같이 나타낼 수 있다[5].

Hard Power	Soft Power
명령(Command)	끌어들임/흡수(Co-opt)
Coerce/Threat/Pay/Sanction	Frame/Persuade/Attract
강압/위협/보복/제재	구상/설득/유인

(그림 2) 사이버파워의 행동영역[4][6]

하지만 사이버 공간에서는 하드파워를 갖춘 강대국도 그 영역과 경계가 모호하여 강제하거나 통제한다는 것이 사실상 어렵다. 사이버공간은 지리적 공간처럼 영역과 경계가 제한받지 않아 주권개념을 적용하기 힘들기 때문이다[1]. 즉 사이버 공간에서는 약소국이라도 세력을 키울 수 있는 환경이 조성됨에 따라 힘의 확산이 가능하며, 주권개념 또는 강대국의 기준을 매우 복잡하게 만든다. 이 맥락에서 보면 사이버파워를 이루는데 필요한 4가지 요건은 ① 작전의 기술적 진보, ② 속도의 빠른 확산과 범위의 무제한, ③ 주요 핵심시설의 통제와 관리, ④ 국가 동원력이 핵심이 된다[7]. 사이버파워는 "물리적 심리적 기술방법이 동원되어 가상의 사이버 공간을 통제하거나 제압할 수 있는 힘 또는 그러한 능력"으로 정의된다.

2.1.2 특성

사이버파워는 실제공간과 비교할 때 비교적 저비용·고효율의 비용편익과 주권적 통제가 어려운 환경과도 관련된다. 특히 사이버 공간 내부의 물리적 수단은 경제 네트워크 특성과 관할권 통제를 어렵게 만드는 정치적 성격을 지닌다[28]. 상대적으로 비용이 저렴한 정보의 영역은 많은 비용이 소요되는 물리적 외부 영역에 공격을 가할 수 있다. 반대로 물리적 영역의 통제는 정보의 영역 내외에서 모두 영향을 미칠 수 있다.

행태적 관점에서 사이버파워는 사이버공간에서 전산으로 상호 연결된 정보자원의 활용을 통해 자신이 의도한 결과를 얻을 수 있는 능력이다[9]. 또한 사이버

공간 안팎의 다른 영역들에서 자신의 의지대로 결과를 얻도록 사이버 수단을 활용할 수도 있다. 사이버 영역은 대규모의 참가인원, 접근의 용이성, 은폐의 기회 등 3가지를 특징으로 한다[9]. 복잡한 사이버 시스템에 의존하는 방식은 비국가행위자들(테러국가, 불량집단)에게 악용될 소지가 있기에 강대국들에 새로운 취약성을 유발한다. 사이버 공간에서 행위자들은 매우 다양하고 간혹 정체도 불명확하다.

사이버 공간에서는 물리적 거리가 큰 의미가 없고 한 두 차례의 가상공격에는 거의 비용도 들어가지 않는다. 또한 사이버 공간은 보안성보다 사용의 편의성 위주로 개발되었기 때문에 현재의 환경에서 방어는 공격에 비해 취약성을 갖는다. 적대국의 사이버 공격에 억제가 불가능한 것은 아니지만 공격원의 특성에 따라 차이가 나기도 한다. 따라서 사이버방어의 핵심적인 요소는 잉여성, 회복력, 신속한 재건능력이 된다[10]. 이와 같은 특성에 비추어 볼 때 사이버파워는 '사이버공간 내의 권력'과 '사이버공간 외의 권력' 범주로 구분되며 수단은 다음의 <표 1>과 같다.

<표 1> 사이버파워의 범주와 수단[6]

수단/유형	사이버 공간내의 파워	사이버 공간외의 파워
정보 수단	• 하드파워: 디도스 공격 • 소프트파워: 규범과 기준설정	• 하드파워: SCADA 시스템 공격 • 소프트파워: 여론 동요를 위한 민간 외교
물리적 수단	• 하드파워: 기업들의 정부통제 • 소프트파워: 인권 활동지원의 인프라	• 하드파워: 라우터 파괴나 케이블 절단 • 소프트파워: 사이버 공급자 공개와 반대시위

북한의 경우 만성적 경제난, 핵실험에 따른 국제사회의 제재로 이중고를 겪는 상황에서 사이버파워는 고립을 탈출하기 위한 수단이 되고 있다. 사이버머니의 현금화를 통한 통치자금 확보, 각종 해킹을 통한 국제사회 위협 등은 하나의 사례가 되고 있다. 가장 최근에는 4차례의 비트코인 해킹이 북한소행으로 밝혀지고 있다[11]. 비트코인 시스템은 추적이 어렵고 익명성이 보장되는 특징 때문이다.

이처럼 사이버 상에서 이뤄지는 공격은 북한의 새로운 강압수단이 되어 남한을 압박할 수 있음을 보여준다. 즉 북한의 사이버파워는 국제사회 제재, 경제난 등 이중고의 상황에서 "국제제재 탈피와 남한 압박"의 수단이 되는 힘(power)인 동시에 경제적 고립의 탈출구적 성격을 갖는다.

2.2 강압이론의 검토

국제관계에서 적대국에 대한 강압은 일반적으로 수사적(rhetoric) 발언이나 강경한 행동으로 전달된다[12]. 하지만 통념과는 다르게 항상 행동이 발언보다 더 강하게 취해지지는 않는다. 구두표현의 공갈(blackmail)이나 메시지(message) 등의 '신호 보내기'(signaling)는 군사적 또는 비군사적인 정치·외교적 행동보다 강하게 나타날 수 있으며, 종종 상황의 구조적 환경이나 위기 전개 양상에 따라 그 효력이 강화되거나 약화될 수 있다[12].

실제 공간에서 전통적 강압은 보편적으로 공습, 영통침공, 경제제재, 국제정치적 고립, 적대국 내의 반란세력 지원, 또는 이러한 방법들이 혼합되어 사용되어 왔다[13]. 이와 같은 방법들을 통해 강압이 성공하기 위해서는 크게 5가지의 조건을 전제로 한다. ① 정권과 지지자들 간의 관계를 괴리시켜 권력기반을 잠식하는 것(power base erosion), ② 정권에 대한 국민적 불만을 증폭시켜 정치적 불안을 조성하는 것(unrest), ③ 최고지도자의 안위를 위험에 처하게 하는 리더십마비 공격(leadership decapitation), ④ 국정 전반을 침체시키는 것(weakening state), ⑤ 전쟁에서 성공가능성을 부인하거나(denial), 군사적 수단을 통해 정치적 승리(political triumph)를 이루는 것이다[13]. 물론 이러한 분류는 이론상에서 분석의 용이성을 위한 것으로, 실제로는 독립적으로 나타날 수도 있고, 서로 혼합되어 나타나기도 한다. 예컨대 권력기반 잠식(①)과 지도자 리더십 공격(③)의 배합은 상대국 정권에 대한 국민적 불만(②)을 야기할 수 있을 뿐만 아니라, 국정 전반을 약화(④)시킬 수 있고, 사회적 불안과 동요를 가져오기도 한다[10].

이러한 논리에 입각하면 북한의 경우 다양한 방법의 기술적 진보(①), 남한의 주요부처와 민간 핵심시설마

비 목적의 해킹과 서버다운 행태(③), 국내외를 막론하고 동시다발로 감행되는 공격패턴(②), 정찰총국 등의 당·국가중심의 시스템(④)을 보임에 따라 앞서 제시한 사이버파워를 높이는 요건에 부합될 것으로 추정된다. 따라서 21세기 네트워크시대 북한의 사이버공격은 온라인상에서 대남 압박수단이 될 수 있으며, 새로운 유형의 강압으로 기능할 수 있다.

한편 사이버파워가 사이버 공간에서 또 하나의 강압이 되는 이점은 비용 효율성에 있다. 즉 강압하는 국가와 강압을 받는 국가 간에 비용편익(cost benefit) 문제와 관련된다. 현실공간에서 군사적 시위나 경제제재 등의 전통적 강압의 수단은 행위자의 비용편익 모델에 기반을 두고, 상대가 불응할 경우 감당할 수 없는 비용에 대한 영향력을 높이는데 중점을 두어왔다[14].

이는 가상의 사이버공간에서도 그대로 적용될 수 있다. 사이버공격에 필요한 자금이나 인력, 기술 등에 필요한 비용대비, 공격을 통해 얻을 수 있는 결과, 또는 그 잠재적 효과가 실제공간에서 강압으로 얻을 수 있는 비용편익보다 더 클 수 있다. 또한 사이버공격을 통해 상대국의 정보탈취 등의 이득과 함께 사회경제적 혼란을 야기할 수 있는 이차적 효과도 가능하다. 사이버공간을 통제나 제압을 통해 얻을 수 있는 타격효과는 반대로 통제나 제압당하는 국가의 경제적 부담과 비용을 높이는 것이기도 하다. 이러한 맥락에서 통제나 제압을 받는 국가의 사회적 비용을 증가하게 만들 수 있다. 이에 따라 적대국의 사이버공격이나 위협의 잦은 행동은 상대국의 '청중비용'(audience cost)을 높임으로써 저항보다는 순응을 예측하게 만들거나 자극할 수 있다[15].

2.3 사이버파워와 강압의 연계성

윌리엄스(Phil Williams)는 효과적 위기관리의 임무를 위기정책결정(decision making in crisis), 위기통제(crisis control), 강압흥정(coercive bargaining) 등 3가지 영역으로 설명하고 있다[16]. 이를 사이버파워와 연관지어보면, 사이버 테러나 해킹의 위협은 시급한 정책결정, 확산의 통제, 적절한 타협을 유도하지 못했을 때 위기의 파급력을 크게 만든다. 만약 사이버 상에서 조치가 보복(채찍) 또는 설득 (당근)중 하나를 선택했다면 상황에 따라 정치·외교적, 또는 경제적 파장을 불러오는 힘이 되거나 해결의 힘으로 작용한다[17]. 가령 사이버 상에서 적의 공격이 발생할 경우 보복이나 위협 등은 적을 제압해 타협을 만들어내는 명령하는 힘으로서의 '선택된' 사이버파워의 방법일 수 있다. 반면 널리 통용되는 규범과 규정을 적용해 국가나 개인이 동참토록 만드는 힘은 '자발적' 힘으로써 기능한다.

즉 사이버 공간에서의 명령하는 힘(하드파워)은 물리적으로 제압하는 '채찍'(stick)적 성격이 강하다. 반면에 동조하게 만드는 힘(소프트파워)은 규범과 여론조성, 외교의 힘을 빌려 자발적 실천을 유도하는 '당근'(carrot)으로써의 비물리적 성격을 갖는다.

이러한 맥락에서 명령하는 힘은 채찍이 되는 강압흥정으로, 동조하게 만드는 힘은 당근이 되는 위기통제로 이해된다. 즉 보복과 위협의 신뢰를 높여 적이 따르도록 만드는 강압흥정은 하드파워로, 위험수준이 확대되지 않도록 적절한 유인을 제시해 통제력을 높이는 위기통제는 소프트파워와 궤를 같이 한다. 결국 사이버파워가 특징으로 하는 명령하는 힘은 강압이론이 말하는 강압흥정으로, 동조하게 만드는 힘은 강압이론의 위기통제 측면으로 설명이 가능하기 때문에 연계가 깊다.

이상의 이론적 내용을 토대로 할 때 이 글은 북한이 실제공간에서 대남 도발행위 못지않게 사이버상의 행동도 하나의 강압이 되는 힘으로 작용하고 있음을 주장하려 한다. 본 논문은 이를 규명하기 위해 2009년 들어 감행된 사이버 상에서 북한의 대남 공격행태를 주요 강압의 유형으로 적용하여 분석하고자 한다.

3. 북한의 대남 사이버공격 유형별 분석

3.1 권력기반 잠식형

사이버파워는 우선 상대국가의 권력기반이나 국정운용 능력을 잠식하는 수단으로서 강압적인 기능을 한다. 특히 그 대상 국가가 적대관계에 있다면 더욱 그렇다. 북한의 권력기반 잠식을 위한 사이버파워 수법은 크게 국정핵심기관의 해킹과 난수방송의 재개이다. 2013년 6월 25일 오전 9시 30분경 대통령의 집무실인 청

와대가 홈페이지 해킹을 당하는 사상초유의 사태가 발생했다[18][19]. 이후 5시 30분경에는 정당과 중소언론기관의 전산시스템이 동시다발적으로 사이버공격을 받기도 했다. 당일 청와대를 포함해 홈페이지가 변조된 곳은 4곳이며 총131대 서버가 다운됐고 2곳은 분산서비스거부(디도스) 공격을 당했다. 특히 16개 시·도당 가운데 8곳이 해킹된 새누리당의 일부 홈페이지에서는 당원명부가 유출되기도 했다. 청와대가 홈페이지 해킹으로 마비된 것은 2009년 '7·7 디도스 공격'이후 4년여 만의 일이다. 이른바 북한의 '6·25 사이버테러'이다.

우리정부의 대응은 오전 10시 45분 미래창조과학부, 국정원 등 10개 부처 중심의 '사이버평가회의'를 열고 사이버위기 '관심' 경보를 발령한 뒤, 오후 3시 40분 '주의'로 경보단계를 격상했다. 북한의 청와대·국무조정실 홈페이지 공격은 국제해커그룹인 어나니머스(Anonymous)가 북한의 46개 주요 웹사이트를 해킹하겠다고 밝힌데 따른 보복성 메시지였다. 그리고 북한도 실제로 이날 정오부터 상당수의 웹사이트 접속이 차례로 차단됐다[19]. 실제 차단된 북한의 주요 웹사이트는 조선중앙통신, 노동신문, 내나라, 고려항공, 우리민족끼리 등으로 북한은 이날 실제 접속장애를 겪었다.

한편 가장 최근 북한의 대남 권력기반 잠식 행태는 공개적인 '난수지령'을 통한 방송매체의 활용이다. '난수'란 0-9까지 어지럽게 나열된 숫자를 문자와 연결하여 지령을 전달하는 암호화된 코드이다[18]. 북한이 대남공작을 위해 사용된 난수는 1980-90년대 주로 활용했으나, 2000년 6·15공동성명 이후 중단했다가 2016년 6월부터 본격적으로 재개되었다. 난수방송은 엄밀히 보면 사이버영역 밖에서 주로 라디오나 전파매체를 통해 이뤄지는 암호화된 숫자형태의 지령이다. 전달 매체나 난수 그 자체로만 보면 사실상 사이버공격 유형은 아니다.

하지만 난해한 숫자를 해독하여 이뤄지는 지령정보는 그 공격 대상들을 주로 인터넷을 매개로 사이버 상에서 진행 된다는데 있다. 난수지령으로 사이버 상에서 진행되는 대남공격 행위들은 군사기밀을 탈취하거나 정보당국을 교란시키는 행위에 관한 것들이다. 또한 그 대상 역시 국회, 국방부, 안보관련 국책기관 등 정치권을 대상으로 한다. 이는 정치권의 위정기반을 시험하고 정보당국을 교란시켜 국정의 힘을 마비시키려는 사이버 상에서의 기만전술이다. 따라서 난수지령은 권력기관을 잠식시켜 남한내부의 안보 공황을 유도하는 직간접적 전달수단으로 활용되고 있을 여지가 충분하고, 정치권의 압박수단으로 활용될 수 있다는 점에서 권력기반의 잠식의 유형중 하나로 본다. 이 밖에도 북한은 SNS 매체를 통해 친구 맺기를 통해 정부부처나 공공기관 직원을 상대로 내부 자료를 요구하는 사이버공격 수법도 전개되고 있다[20].또한 최근 한반도내 사드(THAAD) 배치와 2017년 대선 정국을 앞두고 온라인상에서 보복성 시위공격으로 분석된다. 특히 E-mail이나 동영상, 오디오 파일에 비밀지령을 숨겨 보내는 '스테가노그라피'(Steganography) 방식은 대남 권력기반과 국정운영을 마비시키는 북한의 새로운 사이버파워가 될 수 있다. 1968년 1월 청와대 기습사태와 같은 직접적 대남공작을 사이버 상에서 재개하고 있는 것이다.

북한은 고립된 상황이 여의치 않을 경우, 권력기반을 잠식하기 위한 사이버 공작은 향후 다양한 경로로 전개될 가능성도 배제할 수 없다. 따라서 부처 간 협력을 통해 네트워크의 이상 징후를 사전에 신속히 파악할 수 있는 통합컨트롤 체계를 갖추는 것이 필요하다.

3.2 지도자 리더십 공격 및 음해형

사이버파워가 되는 또 하나의 강압의 유형은 적대관계에 있는 최고 지도자의 정치적 리더십 공격과도 관련된다. 2016년 6월 8일 경찰청 사이버안전국은 1월 발생한 사이버공격 3건의 발생지를 추적한 결과, 전송에 사용된 경유서버·악성코드 제어서버 등이 평양 류경동 소재 인터넷 IP주소와 동일한 것으로 확인했다. 1월 27일 국내 방송사 2곳을 사칭해 보낸 E-mail에는 '박근혜 대통령의 거짓육성을 담은 동영상'이 편집되어 첨부됐다. 이 동영상 E-mail은 해외사이트를 거쳐 IP를 세탁한 뒤 국내 대량메일 발신서비스업체를 통해 38,988명에게 무작위로 전송되었다.

한편 2월 18일에는 현직 경찰청 사이버수사관을 사칭한 E-mail이 탈북자, 북한연구자 등 48명에게 발송됐다. 이 메일은 "대통령 음해 동영상에 대한 국가보안법 수사에 협조해 달라"는 내용과 함께 악성코드를 심은 파일이 첨부되었다. 또한 1월 11일에는 국내 대학의 북한관련학과 교수를 사칭한 E-mail이 언론사, 기자

등 83명에게 전송됐다. 여기에는 “북핵문제의 이성적 접근방식”이라는 문서명의 악성코드를 담은 파일도 첨부되었다. 우리 수사당국은 일련의 E-mail 공격이 2013년 3·30 사이버테러 당시 북한에서 접속한 대역과 일치하고, 몇 차례 국내 전산망 공격에 사용된 IP주소와 동일한 것으로 발표했다[21]. 또한 사회 주요 인사나 지식층을 대상으로 하는 ‘랜섬웨어’(ransom ware)도 북한의 새로운 사이버파워가 될 가능성을 높인다. ‘랜섬웨어’란 불특정인의 컴퓨터 화면에 잠금장치(lock)를 걸거나, 특정문서를 암호화하여 해독용 프로그램을 제공하는 빌미로 돈을 뜯어내는 수법이다[7]. 즉 온라인에서 범죄행위의 신종수법으로 Crimeware의 일종이다[8]. 이러한 사회 인사나 지식층에 대한 공격행위는 북한이 대규모 분산서비스거부(디도스) 공격을 하지 않는 평시에도 수시로 감행되고 있다.

사이버 상에서 대통령의 음해성 E-mail 유포는 대남 심리전의 일환이다. 또한 경찰당국과 사회지식층을 사칭한 E-mail 공격은 각각 공직기강 해이를 유도하고, 사회적 내분과 갈등을 만드는 정보탈취가 목적이다. 이는 북한이 남북 간 대립과 갈등에 따라 안으로는 체제단속을 위해 북한주민의 외부정보를 차단하고, 밖으로는 지도자의 리더십과 국정운영에 타격을 가함으로써 남한 내 국론분열을 통해 남북관계에서 정치적 우위를 점유하려는 의도로 분석된다.

이와 같은 전례를 종합할 때, 북한은 향후 IT매체를 통해 남한의 정치 지도자의 리더십을 훼손하는 방법의 연성권력(soft power)을 지속적으로 키울 가능성이 높다. 온·오프라인이 하나가 되는 사물인터넷(Internet of Things) 시대가 올 경우 초경량, 저 전력화에 따른 보안구축은 더 어려워질 수 있는 사이버 환경에 놓일 수 있다. 따라서 북한의 신뢰가 확보되지 않는 한, 한국의 정부당국은 온라인을 통해서도 리더십 공격에 선제적 대응을 해야 할 것이다. 실제 대북확성기 심리전 외에도 온라인상에서 대북 심리전의 추진은 북한의 강압(coercion)을 역으로 이용하는 하나의 방법으로 사이버파워가 될 수 있다.

3.3 군사작전 방해형

사이버파워는 각종 전파 교란과 통제에 관해서도 중요한 힘으로 기능한다. 이 중 대남 실제행동에 있고, 위협이 되는 것이 북한의 위성위치확인시스템(GPS) 교란과 전자기펄스(EMP) 마비 시도이다. 북한은 2016년 3월 31일~4월 5일까지 6일간 군사분계선(MDL) 북방의 해주, 연안, 평강, 금강, 개성 등 5곳에서 남방지역으로 무차별적인 GPS 교란 전파를 감행했다. 이에 따라 한국을 포함한 14개국 항공기 1,007대가 이·착륙으로 GPS 신호를 받는데 장애를 겪었다. 북한은 2010년과 2011년에도 GPS 교란을 시도한 전례를 갖고 있다. 1·2차 전파교란 당시 휴대전화가 전면 불통되는 피해가 컸고, 2016년에는 우리어선 280여 척의 조업이 중단되는 사태까지 발생했다. 이에 대해 한국정부는 그간 국제사회를 통해 공식적으로 문제제기를 지속해 왔다. 2012년과 2016년 5월 16일~6월 17일 한국은 국제민간항공기구(ICAO) 및 국제전파통신연합(ITU)을 통해 북한의 GPS 교란행위를 공식화하고 재발방지를 위해 국제적 조치를 요구했다. 그 결과, 북한 소행을 간접적으로 지칭하는 ‘북한지역’ 문구와 북한 책임론을 분명히 했다. 또한 중국과 러시아를 포함해 36개국 ICAO 이사국들의 동의를 얻는데 성공했다. 이는 향후 우려되는 북한의 GPS 교란 재발을 차단하기 위한 구체적인 첫 조치라는 점에서 대북 압박의 메시지로 효력을 갖는다. 즉 한국의 적극적·능동적 대응이 국제사회에서 북한의 ‘나쁜 행동’을 고립되게 만든 정치·외교적 성과로 평가된다.

<표 2> 북한의 GPS 신호교란과 정부대응 주요일지[19][22]

시기	대상	내용
2010-11	북한	GPS 신호교란용 전파발사
2012 4/5월	북한	GPS 신호교란용 전파발사
2012 6월	한국	ICAO, 북한행위 공식제소
2012 7월	ICAO	북 GPS교란방지 결의문채택
2016 3/4월	북한	GPS 교란전파 재시도
2016 5월	한국	ICAO, 북 교란문제 재차제기
2016 6월	ICAO	북 교란 ‘심각한 우려’ 경고
2016 8월	한국	을지·충무훈련, 교란 민관대응

2010~2016년 8월까지 북한의 대남 GPS 공격행태 추이를 보면 몇 가지 패턴으로 분석된다. ① 2-4년 주기로 감행시도, ② 신호체계 및 시스템교란 방식의 전파발사와 통신차단, ③ 민·관·군 합동훈련의 사전방해

로 안보공백의 유도가 목적인 것으로 판단된다.

한편 전자 네트워크에 또 다른 위협이 되는 것이 북한의 EMP(Electromagnetic Pulse) 공격 가능성이다. EMP는 다량의 방해 전자파를 사용해 상대 시스템을 일시에 마비시키는 일종의 사이버폭탄(Cyber Bomb)이다. 북한의 EMP 공격 가능성은 미 정보당국 전문가들의 진술로 주장의 논거를 뒷받침 한다. 미 상원 법사위원회 산하 EMP위원회 로렐 우드(Laurel Wood)에 따르면 북한의 대포동 2호보다 더 시급한 상황은 북한의 EMP 실전보유 위험성을 언급하였다. 이러한 우려 속에서 미 CIA 핵무기 전문가인 피터 빈센트 프라이(Peter Vincent Pry) 역시 러시아가 개발한 전자기(EMP)파 설계정보의 북한 유출을 진술한 바 있다[30].

하지만 북한의 EMP 사용을 제압하는 우리정부의 대응은 아직까지 취약한 면이 없지 않다. 북한의 EMP 사용이 현실화될 경우 첨단수준의 무기를 갖춘 우리군이 사이버 내외 공간에서 작전수행을 하는데 심각한 위협이 된다. 즉 EMP도 사이버전, GPS 교란 못지않게 북한이 저비용·고효율로 한·미 양국의 작전수행능력(Operational Performance Capability)을 무력화할 수 있는 사이버파워가 될 수 있다. 이를 위해서는 UN 산하 국제전기통신연합(ITU)을 통한 제재의 국제공조와 미국의 '방패법안(Shield Act)'과 같은 법률이 반드시 제정되어야 한다. 또한 EMP 위협에 대비하기 위한 국가기간시설에 대한 방호대책도 강구해야 한다.

미국의 경우, 대선후보인 트럼프(Donald Trump)의 2016년 공화당 정강정책을 보면 2012년과 비교할 때, 북한의 EMP를 실제적 위협으로 분명히 인식하고 있다. 2012년 대비 미 공화당의 2016년 정강정책에서 북한의 규정을 ① '노예국가(slave state)'로, ② 핵·미사일 능력에서 '보유 중'으로, ③ 무역정책에서 '더 나은 무역협정 필요'로, ④ 전자기펄스(EMP) 사용능력에 대해 '실제적 위협'으로 밝히고 있다[20]. 또한 2017년 미 국가안보전략보고서(NSS)는 본토 및 미국인 보호를 위해 북한의 사이버 테러를 위협 근원의 목표 중 하나로 규정하고, 디지털 네트워크 보안을 강화하는 내용을 담고 있다[16]. 이에 따라 한미연합 차원에서 한국은 북한의 EMP 공격 가능성을 열어놓고 통제 매뉴얼을 구체화해야 할 것이다. 결국 2010년대 4차례에 걸친 북한의 GPS 교란과 EMP 공격 가능성은 강압메커니즘이 요구하는 군사작전 방해의 한 유형으로 집약되며, 사이버파워가 되는 북한의 대남 교란과 통제 수단으로 기능할 수 있다. 따라서 한국은 온·오프라인에서 북한을 선제적으로 무력화할 수 있는 다양한 시나리오를 갖추고 대비해야만 한다.

3.4 사회불안과 혼란유도형

사이버 공간에서 사회적 불안을 조성하고 혼란을 유도하는 행위는 실제 공간에서보다 심각한 파급력을 갖는다. 가상공간에서의 파괴적 사회불안과 내부혼란의 유도는 적대국을 비교적 손쉽게 제압할 수 있는 사이버파워가 된다. 북한의 또 다른 사이버파워는 4차 핵실험 이후 전방위 제재와 압박에 따른 자금탈취 가능성과 연계된다. 즉 북한은 사이버파워를 가상공간에서 '현금 일탈화'와 '홍보심리전'을 이용해 대남 사회불안과 혼란을 유도하고 있다. 북한의 대남 공작기관들이 경제난과 외화난 해소를 위해 한국을 포함한 국제금융망을 대상으로 감행한 사이버공격은 세계 도처에서 발견되었다[23]. 2016년 2월 방글라데시 중앙은행의 8,100만 달러 탈취사건은 북한이 미국 소니 픽처스와 한국의 금융·언론기관 해킹 시 사용한 코드와 유사했다. 또한 북한은 최근 2000년대 초 남북합작으로 출범한 남북교역 사이트를 IT기술 홍보사이트로 개편한 것이 확인됐다[18]. 사실상 외화벌이 창구로써 북한의 IT기술을 동원한 사이트가 2016년 4월 대대적으로 개편되는 움직임을 보여 왔다. 같은 해 7월 5일 확인된 '조선엑스포'는 남북교류가 활발하던 2004년 남북이 합작해 설립한 '조선복권합영회사'의 무역전문 사이트였다. 하지만 우리정부가 남측사업자의 사업허가를 취소해 유명무실화되었고, 이후 북한이 독자적으로 운영해 온 것으로 현재 평가되고 있다[19]. 사이버공격을 위한 북한의 인적자원 역량은 정찰총국의 정찰대대와 사이버테러 요원, 특전사 11군단 '번개·우레' 등 10개 여단, 정규군단, 사단급 경보병부대와 정찰대대 및 통일선전부 산하 문화교류국 소속요원 등 20여만 명 규모로 추정·집계된다[23].

주목할 점은 북한의 이와 같은 행동들이 유엔안보리 대북제재 결의안 2270호와 미국 행정부의 대북제재법안 발효 등 대북압박 직후 본격화되고 있다는 점이다.

이는 북한이 2016년 1월 6일 4차 핵실험과 ICBM 시험발사 이후 대북제재로 자금조달이 여의치 않자, 사이버 공간에서 정보기술(IT)을 통해 제재국면의 돌파구를 만들려는 의도로 분석된다.

또한 북한은 외화난 해소와 경제난 탈피 목적으로 사이버해킹을 적극적으로 활용하고 있다. 일례로 국내외 각종 자본주의 게임 사이트를 해킹하여 가상의 사이버머니를 현금으로 바꾸는 이른바 '사이버머니의 현금화'이다. 이는 북한의 지하자원 등 주력 수출품이 핵개발에 따른 국제제재로 자원의 판로가 막히자 IT분야로 자금줄을 확보하려는 출구전략 의도로 판단된다. 결과적으로 북한의 일련의 행동은 시장주의 논리로 운용되는 경제적 사회불안을 조성하고, 자본주의 시스템의 혼란을 유도하기 위한 사이버공간에서 강압적 수단의 사이버파워가 되고 있다.

북한이 최근 공세적 IT기술홍보에 나선 것은 김정은 국무위원장의 '과학기술 강국건설'과 무관하지 않다. 김정은은 2016년 5월 제7차 당 대회에서 나노기술, 우주기술, 핵기술 등과 함께 정보기술 병진을 북한체제 유지를 위한 4대 주력핵심 분야로 꼽았다. 이처럼 북한의 대남 사이버행동은 공세적 방법으로 진화하고 있으며, 그 대상도 민·관·군 전 영역에 걸쳐 확대되고 있다. 북한당국과 군은 6개 이상 해킹조직에 1,700명 규모의 전문해커를 보유하고 있는 것으로 추정하고 있다. 또한 해킹지원세력은 17개 조직 5,100명에 이르는 것으로 파악하고 있다[24][25]. 국가정보원 및 미 국가정보국(DNI)은 북한의 해킹수준을 대량살상무기에 버금가는 위협과 세계 최고수준의 능력으로 평가하고 있다[25]. 따라서 북한의 사이버공격은 앞으로 복합전의 양상을 띨 가능성이 높다. 즉 동시다발적이고 온·오프라인 공격을 배합할 뿐만 아니라 국내 북한추종세력, 이슬람국가(IS) 등 해외 테러단체와 연계할 수 있는 여지도 배제할 수 없다.

이러한 정황에서 볼 때 한국은 정보화에 관한 한 세계적 수준을 갖지만 정보보안에 관해서는 취약한 면이 적지 않다. 특히 민·관 기관들은 해킹 피해에 대한 사회적 신뢰성저하 우려로 인해 상당부분 정보보호관련 투자와 협력에 소극적으로 대응해 왔다.

미래창조과학부가 2016년 상반기 발표한 기업 IT예산 정보부문 투자 통계수치이다. 최근 국내기업의 전체 IT예산 중 정보보호 부문이 차지하는 비중이 5% 이상인 기업은 1.4%에 불과하다. 역으로 보면 국내 IT예산 중 정보보호에 투자하는 비용이 5% 미만인 기업은 17.2%나 차지하는 것이 한국의 현실이다. 이 통계는 비록 민간 기업을 대상으로 하지만 정부나 군 당국의 대응 역시 이러한 통계로부터 자유로울 수 없다[11][22].

중요한 것은 북한의 사이버공격은 점점 고도화되고 있는 반면, 한국은 법적 제한과 규제 및 보안의 기술적 난해와 신뢰성저하 문제로 인해 민·관 기관의 조치는 사후대응에 그치고 있다는 것이다. 이는 북한의 전면적 사이버공격에 언제든 또다시 노출될 여지가 있음을 반증하는 것이다.

2013년 한수원 해킹은 핵심기반시설의 보안 취약성을 노출한 대표적 사건이었다. 따라서 북한의 기반기설 공격에 대비해 민·관 기관들 간의 정보공유와 정보보호에 적극적인 협력과 투자가 필요하다. 또한 선제적 대응의 국제공조 강화가 필수적이다. 군 당국이나 국가정보원은 타국과의 사이버안보 협력체를 능동적으로 주도할 필요가 있다. 종합해 볼 때, 북한의 대남 사이버파워 양상과 공격행태를 사이버파워와 강압의 이론화 내용으로 적용해 보면 <표 3>과 같은 결과로 정리된다.

<표 3> 북한의 대남 사이버공격 양상과 행태

수단/유형	사이버 공간내의 파워	사이버 공간외의 파워
정보수단	• 하드파워: 권력기반 잠식형 - 국정핵심기관 서버해킹과 난수방송	• 소프트파워: 지도자 리더십 공격과 음해형 - 대통령음해 E-mail 전파
물리적 수단	• 하드파워: 군사작전 방해형 - 국방·통신·GPS교란 및 EMP공격 - 기간산업·금융사 서버해킹	• 소프트파워: 사회불안과 혼란유도형 - 사이버머니 현금화와 홍보 심리전

4. 정책적 대응방안

북한의 대남 사이버파워 양상과 공격행태에 대한 한국의 대응은 다음과 같은 몇 가지 정책적 보완이 필요하다. 첫째, 국가안보 차원의 사이버보안 인력의 강화

이다. 현재 북한의 사이버 핵심전력은 정찰총국 산하 121국이 주도한다. 또한 조선노동당 휘하 부처일부에도 별도의 해커전담조직을 구성하고 있다. 북한은 총인구 대비 전투병력 890만 명 중에 사이버요원만 6천여 명에 이르는 것으로 파악되고 있다[21]. 예컨대 2015년 통계청 조사에 따르면 북한의 총인구는 현재 24,662,000명(2014년도 기준)으로, 전체인구 중에 36.1%는 군인이거나 언제든 전투동원이 가능한 가용력 있는 수치인 것으로 조사됐다. 특히 해킹 등 사이버전을 위해 북한 당국은 6,000여 명의 정예요원들을 현재 운영 중인 것으로 파악했다[26][31].

북한의 사이버 공작은 조직화된 해커들을 통해 국내외 상에서 대남교란을 가속화할 것으로 예측된다. 이에 대응하기 위한 몇 가지 대응을 주문하면 다음과 같다.

첫째, 안보관련 전문해커들을 국가차원에서 증원·양성하여 북한의 사이버 도발을 선제적으로 차단하는 역량이 필요하다. 국정원 직속 또는 유관부처 산하에 대북 해킹전담팀을 신설 또는 증원하여 대남교란을 사전에 차단하는 통제인력의 구축도 대안이 될 수 있다.

둘째, 익명성에 따른 서버 역추적의 국제공조와 협력이다. 현재 북한은 4차 핵실험 이후 미국주도의 국제사회로부터 자금줄 차단을 위한 전방위 경제제재를 받고 있다. 북한은 은닉자금줄 확보를 위해 대상국을 막론하고 사이버 상에서 금융해킹, 사이버머니의 현금화 등 수단과 방법을 가리지 않을 것이다. 또한 중국과 동남아는 불법게임 사이트를 개발하며 악성코드를 심는 북한 해커들의 거점으로 사이버 공격의 진원지가 되고 있다[27]. 2011년 8월~2016년 3월까지 북한의 악성코드 전파 진원지 및 게임·프로그램 주요사건 내역을 보면 중국의 선양, 다롄, 베이징, 칭다오는 불법게임 프로그램개발 하청지역으로, 태국 및 캄보디아는 도박 사이트를 개설한 외화벌이의 거점국가로 주목받고 있다. 따라서 북한의 사이버공격 자금줄을 차단하기 위해서는 국제금융결제망(SWIFT), 인터넷 등 국제간 대북 금융정보 교류와 네트워크를 통한 협력적 차단을 지속·강화시킬 필요가 있다.

셋째, 제도적 시스템의 보완과 개편 또는 신설이다. 현재 정부 차원의 대남 사이버 대응체계는 관계부처마다 역할과 기능이 분화되거나 중첩되어 있다. 따라서 사이버 공간상에서 테러나 해킹 위기 시 유기적 협력관리가 제한받아 효과적 대응을 어렵게 만든다. 한국은 2003년 1·25 인터넷대란 발생이후 2004년 국정원 산하 국가사이버센터를 설립해 사이버방어를 관리해왔다. 그리고 2015년 1월과 3월 각각 청와대 내 안보특별보좌관과 사이버안보비서관을 신설해 현재 운용하고 있다. 이를 위해서는 청와대 내 현존 사이버안보비서관을 '사이버안보실장'으로 격상하여 대통령직속 컨트롤타워의 효율적 통제와 관리의 강화가 무엇보다 필요하다. 그 밖에도 현재 국방부와 미래부가 논의 중에 있는 '사이버예비군' 창설과 함께 국방부 사이버전략사령부 내 '전술해커부대'(가칭) 추진도 하나의 제도적 대안으로 고려해 볼 수 있을 것이다.

북한의 GPS 교란에 관한 대처 역시 항재밍(anti jamming) 기술과 지휘체계의 통합적 통제시스템의 부재로 부처 간의 유기적인 협력과 대응을 어렵게 만든다. 미국의 경우 2015년 12월 통과된 '사이버보안법'(Cyber Security Act)을 강화하고, 2016년 2월 9일 미국민의 정보보호를 위한 '사이버안보 행동계획'(Cybersecurity National Action Plan)을 수립하였다. 또한 미 국가안보회의(NSC) 내 '사이버대테러전담부서'(CTC)를 별도 기구로 두고 상시 점검하는 실무적 대응력을 보여주고 있다.

국토안보부(DHS)도 국방부(DoD)와 국가안전보장국(NSA)을 통해 중요한 정부 네트워크를 보호하기 위한 노력을 강화시키는 중이다. 특히 국방부는 사이버전에 대비한 조직과 운용을 체계적으로 정비해 왔다. 2002년 변경된 통합군사령부 계획에 따라 정보작전의 책임을 전략사령부(STRATCOM)에 지정했다. 이에 따라 합동수행병력과 합동기능구성사령부 창설을 포함하는 광범위한 재편성을 실시했다.

전자가 군의 사이버 성능을 보호하고 방어하는 것이 주요임무라면, 후자는 네트워크공격 시 정보작전과 주요통제 임무를 담당한다. 일본 역시 2014년 11월 제정된 'Cyber-security' 기본법에 근거해 2015년 9월 사이버 안보전략을 수립하고 연차계획을 추진 중이며, 유럽도 2013년 유럽위원회 사이버보안전략(Cybersecurity Strategy of the European Union)을 마련한 바 있다.

정부는 대통령중심의 원톱(one-top) 시스템 대응체제 정비와 부처 간 네트워크의 실질적 강화를 통해 대북 사이버 방호에 시너지 효과와 힘을 높여야 한다. 이

와 함께 19대 국회에서 보류된 사이버테러방지법도 국가안보 차원에서 조속히 처리되어야 할 것이다.

5. 결 론

글로벌 시대 사이버 공간에서 테러는 개인이나 국가를 막론하고 대규모 피해를 입히는 위협의 능력으로 평가되고 있다. 이러한 사이버 공격의 중심에는 북한이 한몫을 차지하고 있다. 북한은 비대칭 전력인 핵무기와 함께 사이버 능력을 위협의 3대 수단의 하나로 간주하며 북한의 힘으로 적극 활용하고 있다. 북한의 대남 사이버 공격 양상과 행태는 다음과 같은 4가지의 목적과 의도의 결과로 분석된다.

첫째, 북한의 사이버 공격은 정부와 민간을 막론하고 남한 내 주요핵심 기능을 마비시켜 사회혼란을 유도하려는데 목적이 있다. 이 목적에 따라 북한은 현재 남한의 사이버방어태세 확인, 남남갈등을 유인하는 심리적 제압이나 탐색으로 사이버파워를 활용한다.

둘째, 북한의 사이버공격 행위는 근본적으로 남한과 국제사회를 위협해 각종 경제원조 협상 시 유리한 위치를 점유하기 위한 의도로 이해된다. 북한의 대남공격은 온·오프라인 상에서 동시 병행하는 행동에 근거한다.

북한은 2017년 6차 핵실험 이후 현재 국제사회의 전방위 대북제재 강화로 상당한 압박을 받으며 고립되어 왔는데, 사이버공격은 이에 따른 역강압(counter coercion)의 대체수단이 되고 있다.

셋째, 북한의 사이버공격은 고립탈출구적 성격을 갖는다. 가령 사이버머니의 현금화나 FRB내 방글라데시·베트남은행 해킹 미수는 북한이 대내외 경제적 위기탈피를 위한 전략적 출구가 되고 있다.

넷째, 사이버파워 유형과 수단 면에서 북한의 GPS 교란, 국방부 서버해킹, EMP 등은 보복·위협성이 강한 하드파워이고, 사이버머니 현금화, 렌섬웨어 등은 사이버 상에서 거액의 돈을 강탈하거나 요구하는 점에서 설득·유인의 소프트파워로 기능한다. 이는 남한내 사회시스템을 비용대비 쉽게 제압하는데 힘으로 작용한다.

집약하면 북한이 다양한 방식을 통해 구사하는 사이버 상에서 행동들은 결과적으로 권력기반 잠식, 지도자 리더십 공격과 음해, 군사작전 방해, 사회불안과 혼란 유도의 유형으로 분류된다.

이에 따라 한국은 북한의 공세적 사이버파워가 방법과 능력에서 변화하고 있음을 명확히 인식할 필요가 있다. 강압의 측면에서 북한이 핵을 포기하도록 하려면 핵을 보유하는 것이 견딜 수 없이 고통스럽거나, 북한정권의 생존을 심각하게 위협하는 상황이 와야 할 것이다[29].

이 연장선상에서 보면 북한의 사이버위협에 따른 행동은 이득보다 감당할 수 없는 손실이 훨씬 더 클 것이라는 결과를 갖게끔 만드는 것이 중요하다. 대북 사이버강압의 효력을 높이는 최선의 방법은 북한이 해킹을 통해서 얻는 이득보다 해킹을 하는데 드는 비용을 크게 만드는 것이다. 이를 위해서는 사이버 상에서 심리전, 현금 일탈화 방지 등 제도적 보완과 신설을 통해 공격과 방어가 동시에 이루어지는 사이버파워 역량을 강화할 필요가 있다. 이와 함께 한미동맹 수준에서 사이버 공조와 역량 강화도 필요하다.

무엇보다 중요한 것은 북한의 공세적 사이버행동에 따른 국민적 안보불안감과 남남갈등을 막는 것이다. 우리사회 일각은 북한의 사이버공격을 근거 없는 '북한 편들기' 자세로 보는 경향이 적지 않다. 2016년 3월 민주평화통일자문회의와 리서치앤리서치가 성인남녀 1,000명을 대상으로 한 우리국민 대북인식 여론조사에 의하면, 북한을 '협력대상'으로 보는 시각은 27.2%인데 반해, '경계대상'으로 보는 시각은 34.6%로 나타났다. 2015년 4분기 기준대비(협력 35.8% 경계 29.9%)로 각각 8.6% 하향과 4.7% 상승한 것으로 분석됐다[23].

이는 북한이 2009년 5월 2차 핵실험 이후 지속적으로 병행되어온 사이버테러에 따른 안보불안감과 사회적 남남갈등이 우리국민의 대북인식에 투영된 것으로 평가된다. 따라서 정부는 사이버 내외에 존재하는 안보무기력과 불안을 방지하기 위해 북한소행의 명확한 증거와 규명을 통해 국민이 의구심을 차단하고 일체감을 갖게 하는 국가리더십이 요구된다.

참고문헌

[1] 한희, “사이버공간과 국가안보”, 2014년 국가안보전략연구소 학술회의, pp. 3-18, 2014. 4. 17.
[2] Richard Haass, ‘A World in Disarray’, Penguin Books, 2018.
[3] 남궁영, ‘강대국 정치와 한반도’, 오름, 2016.
[4] Joseph S. Nye Jr., ‘The Future of Power’, Public Affairs, 2011.
[5]] Joseph S. Nye Jr., ‘Soft Power: The Means to Success in World Politics’, Public Affairs Press, 2004.
[6] Joseph S. Nye Jr., “Cyber Power”, https://projects.csail.mit.edu/ecir/wiki/images/d/da/Nye_Cyber_Powe1.pdf.
[7] Franklin D. Kramer, Stauare H. Starr and Larry K. Wentz(eds), ‘Cyberpower and National Security’, Potomac Books Inc, 2009.
[8] Markus Jakobsson and Ramzan Zulfikar, ‘Crimeware: Understanding New Attacks and Defenses’, Addison-Wesley Professional, 2008.
[9] 윤영호(역), ‘권력의 미래’, 세종서적, 2012.
[10] David E. A. Johnson and Pettit Steve, “Prinicples of the Defense for Cyber Networks”, Defense Concepts. Vol. 4. No. 2. January 2010.
[11] 한국경제, 2016년 6월 17일.
[12] Alexander L. George, ‘Forceful Persuasion: Coercive Diplomacy as an Alternative to War’, United States Institute of Peace Press, 1991.
[13] Daniel Byman and Matthew Waxman., ‘The Dynamics of Coercion: American Foreign Policy and the Limits of Military Mights’, Cambridge Univ. Press, 2002.
[14] 정하연, “사이버 공격을 통한 강압외교”, 2015 한국국제정치학회 연례학술대회, pp. 1-16, 2015. 2. 11.
[15] Gray Shaub Jr., “Compellence: Resuscitating the Concept”, in Lawrence Freedman(ed.) ‘Strategic Coercion’, Oxford University Press, 1998.
[16] Phil Williams, ‘Crisis Management: Confrontation and Diplomacy in the Nuclear Age’, Martin Robertson, 1976.
[17] 김경곤 외(역), ‘사이버 보안과 국가 안보 전략’, 에이콘출판부, 2015.
[18] 국민일보, 2016년 7월 6일.
[19] 동아일보, 2013년 6월 26일.
[20] 연합뉴스, 2016년 7월 20일.
[21] 중앙일보, 2016년 6월 14일.
[22] 미래창조과학부, ‘기업 IT 정보보호 부문평가’, 2015.
[23] 유동열, “북한의 테러위협과 우리의 대응전략”, 국가안보전략연구원·이스라엘 국제대테러연구소 공동 국제학술회의. pp.99-121, 2016. 6. 23.
[24] 조선일보, 2016년 7월 8일.
[25] 조선일보, 2017년 12월 16일.
[26] 민주평화통일자문회의 사무처, “민주평통 뉴스클리핑”, 2016년 6월 7일.
[27] 파이낸셜 뉴스, 2016년 6월 15일.
[28] Adam B. Lowther(ed.), ‘Deterrence: Rising Powers, Rogue Regimes, and Terrorism in the Twenty-First Century’, Palgrave Macmillan, 2012.
[29] 우정민. “한반도 군사적 현안에 관한 미중관계 고찰: 북핵. 사드. 한미동맹의 환경 하에서”, 융합보안논문지, 제17권, 3호. pp. 83-93, 2017.
[30] 이대성·신성식, “북한의 전자기파(EMP) 위협에 대한 검토” 한국테러학회보, 제6권, 1호. pp. 85-103, 2013.
[31] 통계청, ‘북한 총인구 통계현황’, 2014.

[저자소개]

윤 태 영 (Taeyoung Yoon)
1988년 2월 한국외국어대학교 학사
1992년 12월 뉴캐슬대학교 석사
1998년 5월 맨체스터 메트로폴리탄 대학교 박사
email : tyoon@kyungnam.ac.kr

우 정 민 (Jeongmin Woo)
2001년 2월 한국외국어대학교 학사
2004년 2월 한국외국어대 석사
2015년 2월 한국외국어대학교 정치학 박사
email : jmwoo72@daum.net