대북 사이버 안보역량 강화를 위한 방안: 사이버전 대비를 중심으로

김 호 중*, 김 종 하**

요 약

북한의 사이버 전력은 대부분 사회기반과 첨단무기체계 운용시스템이 네트워크로 구축되어 있는 한국에게는 심각한 안보적 위협이 되고 있다. 따라서 본 논문의 목적은 대북 사이버 안보역량 강화를 위해 한국정부가 무엇을 해야 하는지를 고찰하는 데 있다. 이를 위해 북한의 대남 사이버 공격 사례를 위협 유형과 목적으로 분류하여 분석하였다. 연구결과는 다음과 같다. 첫째, 적극적인 사이버 방호 및 공격능력을 갖추어야 한다. 둘째, 국가차원에서 총괄할 수 있는 통합적 사이버 안보 컨트롤타워를 구축하는 것이다. 셋째, 국내 사이버 관련 법제정이 필요하다. 넷째, 다자간·지역내 사이버협력 체제를 구축하는 것이다. 이런 연구결과의 시사점은 북한의 사이버 위협으로부터 평시 피해를 최소화하고 유사시 완전한 전쟁수행을 위해 한국은 사이버 안보역량을 강화할 필요가 있다는 것이다.

A Plan for Strengthening Cyber Security Capability toward North Korea: focusing on the Preparation of Cyber Warfare

Kim Ho Jung*, Kim Jong-ha**

ABSTRACT

North Korea's cyber warfare capability is becoming a serious security threat to Korea because most of the operational systems of social infrastructure and advanced weapons system are all networked. Therefore, the purpose of this article is to examine what the Korean government should do to strengthen cyber security capabilities toward North Korea. For this purpose, this article analyzed North Korea's cyber attack cases against Korea by categorizing according to threat type and purpose. The research findings are as follows. It is necessary first, to have aggressive cyber protection and attack capabilities; second, to establish an integrated cyber security control tower that can be overseen by the national government; third, to need to legislate domestic cyber- related laws; fourth, to build a multilateral & regional cyber cooperation system. The implication of these findings are that it needs to be strengthened the cyber security capability from the cyber threats of North Korea by minimizing the damage during the peacetime period and for the complete warfare in case of emergency.

Key words : cyber security, North Korea's cyber capacity and threat, preparation of cyber warfare

접수일(2018년 8월 8일), 게재확정일(2018년 9월 23일)

* 한남대학교/경영국방전략대학원

** 한남대학교/정치언론국방학과(교신저자)

1. 서 론

북한이 비대칭 군사적 수단으로 활용하고 있는 핵, 전략미사일, 생화학무기, 사이버전력 등은 한국 안보의 최대위협이다. 북한은 이들을 재래식 군사력과 연계하여 한국을 위협하고 있다. 특히 사이버전력은 세계 수준급으로 알려져 있다.

북한이 사이버 분야에 중점을 두는 이유는 정보화시대라는 흐름에 맞춰 대남적화혁명을 달성하기 위한 수단으로 활용하기 위해서이다. 사이버 위협은 특성상 전·평시 구분이 불분명하고 공격자에 대한 추적 및 식별 등이 어려우므로 공격목표 달성에 매우 유용하게 활용할 수 있다. 그러면, '한국의 대북 사이버 안보수준은 어느 정도인가.' 아쉽게도 한국의 사이버 안보에 대한 체계적인 시스템과 국민들의 인식 등은 그다지 높지 않다는 평가이다.

그동안 한국은 북한의 핵과 미사일 위협에 대응하기 위해 킬체인(Kill Chain), 한국형 대공미사일 방어(KAMD), 대량응징보복(KMPR) 등 3축 체계 작전개념을 구축해 왔다. 하지만 사이버 분야는 대비태세가 다소 취약한 실정에 있다. 일례로 북한의 사이버전에 대비해 사이버사령부를 창설하였으나 전략적 관점에서 볼 때, 아직까지 규모면에서 부족하고, 또 관련법 체계 등도 미비한 것을 들 수 있다.

따라서 한국은 북한의 핵, 미사일 도발과 사이버 공격 위협 억지를 위해 보다 적극적이고 실효성이 있는 안보역량을 강화할 필요가 있다. 이는 세계 최고 수준으로 운용되고 있는 북한의 사이버 능력에 대응하고 네트워크화 되어 있는 핵, 미사일 운용시스템과 의사결정체계 등을 파괴, 무력화시킬 수 있는 사이버 안보역량을 강화해야 함을 강조하는 것이다. 과거 미국과 이스라엘이 '스턱스넷(stuxnet)'을 이용해 이란의 핵개발 프로그램을 방해했던 것처럼 우리도 북핵, 미사일 등을 무력화 할 수 있는 사이버 공격 능력을 반드시 갖출 필요가 있는 것이다. 또한 전시는 물론 평시에도 사회적 혼란과 물리적 손해 등을 야기하는 북한의 사이버 공격으로부터 방호할 수 있는 사이버 역량을 확보해야 한다.

사실 한국은 사이버 네트워크 사회기반이 잘 구축되어 있을 뿐 아니라 대부분 첨단무기체계가 '네트워크 중심전'(NCW, Network-Centric Warfare)을 기반으로 발전되어 있기 때문에 북한의 사이버 위협으로부터 자유로울 수 없는 상황이다. 즉 정보통신기술(ICT, Information & Communication Technology) 인프라가 잘 발달되어 있는 국가이기 때문에 오히려 사이버 위협과 공격에 취약한 것이다[1].

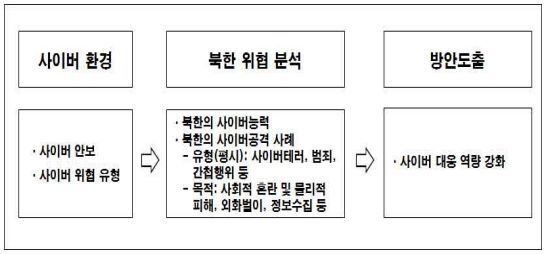
이러한 사이버 공간의 취약점을 잘 활용하고 있는 곳이 바로 북한이다. 북한은 한국과의 국력 격차에서 오는 군사적 열세를 극복하기 위하여 사이버 전력을 핵, 미사일 등과 함께 발전시켜 왔다. 실제로 북한은 한국을 대상으로 다양한 형태의 사이버 도발을 지속적으로 감행하고 있고, 이는 한국사회에 정치·경제·군사적 차원에서 심각한 안보 위협과 혼란을 야기하는 요인으로 작용하고 있다. 2009년 7월 7일 청와대, 국회 등에 분산서비스거부(DDoS, Distributed Denial of Service) 공격을 시작으로 지난 10여 년간 사이버 공격을 자행해 왔고, 최근에는 한반도 평화를 약속한 2018년 4월 27일 남북한 정상 간의 판문점 선언 이후에도 한국소비자원과 공정거래위원회 산하기관들을 해킹하는 등 한국을 대상으로 사이버활동을 감행하기도 하였다[2].

이처럼 북한은 사이버 도발을 가속화하고 있으나 우리는 북한의 사이버 위협을 국가 일부 영역에 국한된 문제로 인식할 뿐, 이것이 국가 생존과 발전에 관한 총체적인 문제, 즉 '포괄안보'의 관점까지는 생각하지 못하고 있다[3]. 이와 더불어 앞으로의 전쟁은 과거와 같이 재래식 무기체계를 전방에 사전 배진하는 방식이 아닌 전쟁 개시 직전 상대국 지휘통제 혹은 무기체계 운용시스템에 악성코드(malware)를 침투시켜 주요기반시설을 마비시키고 사회를 혼란에 빠뜨리면서 시작될 가능성이 있다. 영국의 국제전략연구소(IISS)는 2010년 군사균형(Military Balance)지에서 미래 사이버전쟁은 핵공포와 비슷한 수준의 전쟁양상이 될 것이라고 하였다[1]. 또한, 향후 사이버전은 사이버 기술의 발달과 함께 독자적인 전쟁수행의 형태로 물리적인 군사력과 완전히 통합된 전쟁이 수행될 것으로 전망된다[4]. 그 만큼 사이버 위협은 국가적으로 피해 위험성이 매우 크다고 할 수 있는 것이다.

바로 이러한 이유 때문에 미국을 중심으로 세계 주요국들은 사이버 위협으로부터 절대적 우세를 확보하

기 위해 첨단 사이버무기를 개발하고, 사이버 인력 강화와 함께 사이버부대를 증편·창설 등을 추진하고 있다. 또한 사이버전에 대한 억지력을 보유하기 위해서 공격과 방어기술이 적절한 균형을 이루어야 할 필요성을 인식하고. 이를 위한 기술개발을 대폭 강화해 나가고 있는 것이다[5].

이런 점을 적절히 인식, 우리나라도 북한의 직접적인 위협에 노출되어 있는 사이버 안보위협에 대해 적극적인 방호와 함께 공격능력을 갖출 수 있는 사이버 안보역량을 강화해 나갈 필요가 있는 것이다. 이에 본 연구에서는 사이버 안보와 사이버 위협 특성 등을 포함한 사이버 환경에 대해 이론적 차원에서 고찰해 보고, 이에 따른 북한의 사이버 능력 및 공격사례를 경험적 차원에서 분석하고, 이를 토대로 한국의 사이버 대응 역량 확립을 위한 방안을 제시하고자 한다. 즉 전시는 물론 평시에도 북한의 사이버전에 대비할 수 있는 사이버 역량을 갖추는데 필요한 방안을 제시하고자 한다. 연구를 위한 분석틀은 (그림 1)과 같다.



(그림 1) 분석틀

2. 사이버 안보와 사이버전 특성

2.1 사이버 안보

국가안보란 국가의 생존과 국가이익의 안전 확보를 위한 정책 및 전략이다. 전형적인 국가안보의 의미로는 외부적 위협으로부터 국가를 보호하는 군사적 안보의 개념이다. 하지만 20세기 후반에 급속하게 확장된 정보화·세계화로 인해 종래의 전통적 안보 개념에서 최근에는 사이버 분야가 포함된 다양한 형태와 위협의 범위가 확장된 포괄적 안보로 변경되어 왔다.

세계는 사물인터넷(IOT), 클라우딩 컴퓨터, 인공지능(AI) 등 신기술이 등장하는 등 정보통신기술이 급속하게 발전하면서 사이버 공간에 대한 의존도는 점점 높아지고 있다. 사이버 공간에서의 위협 역시 국가와 사회전반이 네트워크화 되면서 더욱 복잡하고 다양한 형태로 정교하게 진화하고 있다.

사이버 공간은 영토·영해·영공 등과 같은 기존 물리적 공간과 달리 공격을 받았을 경우 그 주체를 파악하기가 쉽지 않다. 따라서 상대적으로 사회혼란의 정도와 파장도 크다고 할 수 있다. 또한 사이버 공격을 통한 물리적 피해를 주므로 이는 실제적으로 존재하는 위협에 해당되어 국가안보의 위협 중 하나이다.

따라서 사이버 안보 역시 국가안보의 일부분으로 다양한 사이버 공간 상의 공격위협으로부터 국익을 보호하고 방어하려는 국가적 차원의 노력이 요구된다고 할 수 있는 것이다[6]. 특히, 많은 국가적 차원의 사회적 기반시스템이 정보통신망으로 구성되어 있기 때문에 사이버 안보에 대한 개념은 더욱 주목받고 있다.

사이버 영역은 기본적으로 무형의 정보 네트워크이다. 지리적 경계를 넘어서 놀랄만한 속도로 정보들을 전송하며, 원거리에서도 정보에 대한 접근이 가능하다. 이러한 사이버 공간을 통해 국가들은 스파이 행위를 저지를 수 있고, 산업 스파이들은 산업기술 비밀들을 훔칠 수 있고, 또 범죄자들은 돈을 훔칠 수 있다. 그리고 군대는 지휘통제 및 통신을 방해할 수도 있다[7].

사이버 위협은 사이버 공간이 갖는 근본적인 취약적 특성 때문에 테러, 보안, 해킹 등과 같은 위험요인이 상존하고 있다. 특히, 세계적 수준의 사이버 인력을 양성하고 있는 북한으로 부터 정치, 국방, 외교, 경제 등 제반 안보분야가 사이버 상 위협에 노출되어 있다. 한국은 DDoS 공격, 농협 전산망 해킹 등 사이버 공격으로부터 큰 혼란을 경험한 사례가 무수히 있다. 사이버 공간에서의 이러한 위협은 국가안보에 미치는 영향이 매우 크다. 따라서 사이버 공간을 안보적 관점에서 직시할 필요가 있는 것이다.

초기 사이버 공간에서의 침투 및 공격행위는 대체로 관심이 많은 일부 개인들의 일탈적 행위로 컴퓨터에 바이러스를 유포하고 해킹 등을 일으키는 정도였다. 그러나 시간이 지나면서 사이버 공격자들은 보다 조직화·전문화된 형태로 발전해왔으며, 이제는 사회적

혼란을 불러일으키는 목적에 초점을 두기 보다는 정치・경제적 등 상위의 목적을 실현하기 위한 수단으로 사이버공격을 주로 활용하고 있는 실정에 있다[8].

2.2 사이버전 특성과 위협 유형

최근 사이버 위협 중 중요한 특징은 '사이버공간의 군사화'이다[9]. 이것은 사이버 전쟁으로까지 확대될 수 있다. 사이버전은 사이버 안보의 하위개념으로서 지상전, 해상전, 공중전, 우주전에 이어 '제5의 전쟁'으로 인식되고 있다. 구체적으로 사이버전은 사이버 첩보전·테러전·기술전·심리전 그리고 정보작전이 복합된 개념으로서 공격자의 사이버 체계를 파괴하고 자국의 사이버 체계를 보호하는 일체의 활동이 포함되어 있다[5]. 사이버전은 군사적인 용어에 중점을 두고 있는 데, 이는 정보와 관련된 원칙에 따라 군사작전을 준비하고 실행하는 것을 의미한다. 즉 직접적인 군사 충돌이나 속임과 방해를 통한 간접적인 경쟁을 포함한 국가 수준에서의 사이버 충돌을 의미한다[10]. 미국은 2011년 5월 사이버 공격을 전쟁행위로 간주해 군사력을 사용할 수 있다는 '사이버 공간에서의 국제전략'을 발표하였다[4][11]. 미 합참교리에서는 사이버전을 정보작전과 밀접히 연계 시키고 있다. 즉 사이버전은 컴퓨터 및 컴퓨터 네트워크와 컴퓨터 및 네트워크 속에 내장된 정보를 공격하거나 방어하는 작전으로 비군사적 영역까지 포함하고 있다.

사이버전의 특성은 기존 전통적 전쟁과 달리 다음과 같은 특성을 가진다[5]. 먼저, 속도측면에서는 빛의 속도로 빠르게 일어나며, 비용 대 효과가 크다. 둘째, 전·평시 구분이 불분명하고 은밀히 진행되며, 공격자에 대한 은닉, 익명성 그리고 예측 불가능한 공격 특성을 가지고 있다. 셋째, 시공 제한 없이 전 세계적 컴퓨터, 서버 등 자원을 활용하여 상상을 초월한 파급력을 가지고 있다. 넷째, 피아 또는 민군 식별이 어려우며 현행 국제법상 적용이 곤란하다는 점이다.

또한 사이버 위협은 사이버 공간 상에서 이루어지므로 다음과 같은 특성을 갖는다. 첫째, 국가의 핵심적 기반시설이 정보통신망에 의해 구성되어 있기 때문에 사이버 공간상에서 발생하는 침해의 파급력은 상당하고 국가적 혼란을 초래하게 된다. 둘째, 사이버 공격은 저비용으로도 정보체계에 대한 전문지식만으로도 충분한 위협과 공격을 가할 수 있는 무기(바이러스 등)를 개발할 수 있다. 셋째, 사이버 위협은 특정한 목표물에 직접적인 피해를 줄 뿐만 아니라 정보통신 기술의 상호연계성을 활용하여 다른 지역 또는 시스템으로 그 피해를 확장할 수 있다. 즉 일반적으로 네트워크에 대한 방호 시스템이 상대적으로 약화되어 있는 전산망 시스템을 이용하여 우회하는 방식으로 공격을 수행한다[12][13]. 넷째, 전통적인 안보 위협 특성과 달리 사이버 위협에 대한 인지 및 조사가 어렵다는 것이다[13].

사이버의 위협을 유형별로 구분[10] 한다면, 국가 간의 사이버 테러, 사이버 범죄, 사이버 간첩행위 등으로 구분할 수 있다. 사이버 테러에 대해 미 국방부에서는 '일반적으로 정치, 종교, 사상적 목적을 위해 폭력적 방법의 수단을 이용해 정부 또는 사회를 위협하거나 공포심을 불러일으켜 어떤 행동을 강요하거나 또는 어떤 행동을 중단하게끔 강요하는 행위'라고 정의하였다. 사이버 범죄에 대해서는 구체적으로 정의하기는 어렵지만 정의를 할 때 주요하게 보는 부분은 범죄 시 컴퓨터를 사용해 스펨, 부정, 아동 포르노, 데이터 절취와 같은 행위가 있었는지 보는 것이다. 사이버 간첩행위는 정보 통신 시스템과 네트워크를 사용해서 다른 국가 또는 다른 회사의 기밀 정보나 민감한 정보를 정보 소유자의 허가 없이 불법으로 취득하는 것을 말한다.

이러한 사이버 위협 유형들의 목적을 살펴보면, 평시에는 사회적 혼란 및 물리적 피해를 주고, 획득한 정보를 이용하여 외화벌이도 하며, 국방・방산분야 등과 관련된 정보수집 등을 한다. 또한 전시에는 전쟁목표 달성을 위한 정보전쟁 수단으로 활용된다.

사실상 사이버 범죄, 사이버 테러 등의 유형을 구분하는 기준은 공격행태, 목적, 내용보다도 가해자의 성격과 의도 그리고 피해대상의 성격과 피해정도 등에 달려 있다[14][15]. 그러나 우리는 이러한 사이버 위협 형태가 비록 평시에 발생하더라도 북한과 같은 적대국으로부터 발생하기 때문에 사이버전쟁에 준하여 대응해야 할 것이다. 또한 사이버 공격은 주로 제3국 경로를 통하여 이용되며, 공격국가에 대한 추적 및 즉각 대응이 어렵고 사회적 혼란과 국민과 국가의 재산 손실 등 물리적 피해가 있기 때문에 평소부터 전

시에 준하여 대응역량을 위한 체계를 구축할 필요가 있겠다.

3. 북한의 사이버 능력과 공격사례 분석

3.1 북한의 사이버 능력

북한의 대남전략은 '전 한반도의 주체 사상화와 적화통일'이다. 북한은 이를 달성하기 위하여 핵, 미사일 등과 함께 사이버전력을 강화하고 있다.

북한은 1991년 걸프전에서 전자전이 가지는 중요성을 심각히 받아들여 사이버 공간에 관심을 갖게 되었다고 알려지고 있다. 국방위원장이었던 김정일은 "20세기 전쟁은 기름전쟁이고 알탄전쟁이라 한다면, 21세기 전쟁은 정보전쟁"이라고 언급[15] 하면서 사이버 능력을 강화하였다. 특히 김정은 시대 들어서 사이버 전력을 급속도로 강화하고 있다. 김정은은 2012년 8월 정찰총국 산하 사이버전 전력을 독립, 확대시켜 '전략사이버사령부'을 창설하였으며, 2013년 8월 "사이버 공격은 무자비한 타격력을 보장하는 만능의 보검"이라며 사이버전의 필요성을 역설하였다[1].

북한의 사이버 공격능력 수준에 대해서는 여러 견해가 있으나 대략 미국과 중국에 이어 세계 3위 수준으로 평가되어 지고 있다[1]. 북한은 6,800명 규모의 사이버 인력들을 운용하고 있다[16]. 이들은 20여 년의 경험 등을 통해 고난도 수준의 사이버 능력을 보유하고 있다[2]. 또한 북한은 어떤 장애환경에서도 군의 지휘통신을 보장하고 적의 지휘통신 시스템을 마비시키기 위한 장비들을 개발하고 있다.

북한의 사이버 능력은 다양한 공격을 야기할 수 있고 사이버전쟁을 수행할 수 있는 관련 기술을 고루 갖추고 있다. 북한의 사이버공격 능력은 단일적으로 실시하는 것이 아니라 전방위적으로 공격을 할 수 있는 능력을 가지고 있다. 즉 사이버 테러·범죄를 비롯한 사이버 심리전, 정보수집 그리고 물리적으로 EMP 공격 등을 이용하여 정보통신망 등을 공격하는 방법이다[17]. 이들의 주요 공격 무기체계로는 DDoS 공격, 지능형지속위협(APT) 도구, 악성코드와 논리폭탄 등 논리적 무기체계와 스피어피싱, 종북어플 등의 심리적 무기체계를 갖추고 있는 것으로 알려지고 있다.[25] 특히 북한은 사이버 위협 근거지로 중국 베이징, 칭다오, 광저우, 선양, 다련 등지에서 활동하고 있다.[26]

북한은 이미 한국을 대상으로 수차례 DDoS, 악성코드 등 사이버 공격도구를 이용해 국가기간망을 마비시키고 정보를 유출하는 등 한국을 내외적으로 혼란케 하고 있다.

3.2. 북한의 한국 사이버공격 사례 분석

북한이 지난 10년간 한국을 대상으로 사이버 공격한 주요 사례를 본 연구 제2장에서 분류한 사이버 위협 유형별로 구분하여 보면 다음과 같다.

사이버 테러행위로는, 북한은 2009년 7월 7일부터 9일까지 3일간 청와대 등 정부·금융·포털 35개 주요 홈페이지를 DDoS공격으로 마비시켰고, 2011년 3월에는 좀비 PC 10만여 대를 이용하여 국회·통일부 등 20개 정부 홈페이지를 비롯하여 증권사·은행·포털 등 20개 민간 홈페이지를 공격하였다. 또한 동년 4월에는 농협 협력업체 직원이 사용하는 노트북을 악성코드에 감염시켜 농협 전산센터 서버 273대 자료를 파괴하였다. 2012년 6월에는 'IsOne'이라는 별칭을 가진 공격자가 언론사 '중앙일보' 홈페이지를 변조 및 신문제작 시스템을 파괴하였다. 2013년 3월에는 방송국인 KBS·MBC·YTN과 금융사인 농협·신한은행 등의 전산망에 악성코드를 동시다발적으로 유포하여 서버·PC· ATM 등 총48,748대 데이터를 삭제하였다. 동년 6월에는 청와대·국무조종실 등 정부 홈페이지와 정당과 중소 언론기관 등에서 운영하고 있는 전산시스템에 사이버 공격을 동시다발적으로 실시하였다. 2014년 8월에는 국내 IT보안업체 제품의 취약점을 이용한 대학병원의 전산망에 침입하여 서버를 장악하고, 사이버 테러를 준비하였다. 2015년 11월에는 금융보안업체를 해킹하여 인증서를 유출하였고, 악성코드를 제작하여 10개 기관 19대 PC에 악성코드를 유포하였다. 2016년 1월에는 청와대 국가안보실 등 정부기관을 사칭하여 759명에게 이메일을 발송하였다.

또한 사이버 범죄행위로는, 2014년 12월에 한국수력원자력 조직도, 설계도면 등을 불상의 방법으로 6차례에 걸쳐 85건을 유출하였으며, 이를 네이버 등에

게시하고 금전을 요구하였다.

사이버 간첩행위로는, 2014년 7월부터 2015년 2월까지 대한항공 등 한진그룹 계열사 10곳과 SK네트웍스 등 SK그룹 계열사 17곳을 해킹하여 F-15의 날개 설계도면과 중고도 한국형 무인정찰기 관련 문서 등을 유출하였다. 2015년 8월에는 국방부 백신 납품업체를 해킹하여 군 인터넷망 서버 등에 악성코드를 유포하였다. 이 뿐만 아니라 한반도에 전쟁발생시 한·미 연합작전을 수행하는 '작전계획 5027'과 '작전계획 5015'까지 유출된 것으로 드러났다.

이처럼 북한은 군뿐만이 아니라 정부·방산업체 등에 사이버 공격을 자행하였다. 이를 본 논문 2장에서 설명한 것과 같이 사이버 위협 유형과 목적으로 분류해 보면 <표 1>과 같이 나타낼 수 있다.

<표 1> 최근 10년간 북한의 대남 사이버 주요 공격 유형 및 목적

구분		횟수	목적
사이버전 (평시)	사이버 테러	9	물리적 피해
	사이버 범죄	1	외화벌이
	사이버 간첩	2	국방 정보수집

이러한 북한의 사이버 위협과 공격은 정부·방송·금융분야 등 다양하였으며, 물리적 피해와 함께 국민들의 불안과 사회적 혼란을 야기하였다. 특히, 공격경로가 국내, 중국 등 여러 국가의 서버를 활용하여 복합적으로 침투함으로써 추적 및 대응에 상당한 기간이 소요되었다. 북한의 이러한 사이버 공격행위는 국가 안보에 상당한 피해와 혼란을 야기하므로 평시임에도 불구하고 북한이 적대국임을 고려할 때 사이버전에 준하여 관리 및 대응해야 한다.

북한이 사이버공격을 자행하는 이유는 상대적으로 물리적 전력이 한국보다 약한 측면이 있고 공간의 무제약성 특성을 가지는 사이버공간을 이용하는 것이 한국사회를 혼란케 하고 정치적 이익 달성에 효율적일 것이라는 판단으로 보여 진다[18]. 따라서 이를 대남 적화통일 목표달성을 위한 방법과 수단으로 활용하고 있는 것이다.

따라서 한국은 북한의 사이버 공격으로부터 적극적으로 대응하기 위해서는 북한의 사이버 능력을 분석하고 진화하는 유형을 예측하여 이에 대응할 수 있는 사이버 역량을 갖추어야 한다. 또한 이와 반대로 한국의 우수한 IT 기술력을 바탕으로 안보에 최대위협인 북한의 핵, 미사일, 생화학무기 시스템을 무력화할 수 있는 사이버 공격 능력도 갖출 필요가 있다. 즉 최근 심각한 위협이 되고 있는 북한의 핵, 미사일, 사이버 도발을 억지하고 전·평시 사이버전에 대비할 수 있는 사이버 안보 역량을 강화해야겠다.

4. 대북 사이버 안보역량 강화 방안

4.1 적극적 사이버 방호 및 공격능력 확보

북한은 오래전부터 해커 양성에 많은 노력을 기울여 왔다. 1986년에 사이버인력 양성기관인 김일 정치군사대학(미림대학)등에 전문 해커 양성과정을 개설하고 매년 100~110여 명 규모의 해커를 양성하고 있으며[4], 영국과 중국 등 선진국에 유학생을 파견하여 최신 전산 공격 기술 획득에도 많은 공을 들여왔다[1].

이밖에도 별도의 연구소를 설립해 해킹을 통한 정보절취, DDoS 공격을 통한 서버 무력화 또는 파괴, 악성코드와 바이러스를 이용한 시스템 파괴 등 다양한 사이버 공격 수단을 보유하고 발전시켜 나가고 있다[1].

따라서 적극적인 사이버 방호 능력을 구축해야한다. 여기에는 주요기관에 사이버 관련 전문 인력을 대폭 확충해야 한다. 즉 북한의 해커들이 한국의 주요기관 사이버 공간에 일체 침투하지 못하도록 하고, 혹시 침투하게 되더라도 피해가 최소화될 수 있도록 사이버 능력을 갖추어야 한다. 또한 국가 보안등급으로 지정되어 있는 중요시설과 사회적 혼란에 휩쓸릴 수 있는 금융기관 등에 대해서는 내부망과 외부망이 분리될 수 있도록 의무화하여 외부에서 악성코드가 유입되더라도 내부망에는 영향을 끼치지 못하도록 선제적으로 사이버 위협을 차단해야 한다.

그러나 아무리 방호체계를 잘 구축하였다 하더라도 사이버의 무제한성으로 인해 100% 방어를 보장할 수

는 없다. 따라서 사이버 공격을 받았을 경우에는 피해가 최소화 될 수 있도록 하고 즉각 복원할 수 있는 기술력을 갖추어야한다.

한편 북한은 세계 수준의 사이버 전력을 확충하고 있지만, 상대적으로 방어차원에서는 약점을 가지고 있다. 이는 북한의 사이버 인프라에 요구되는 ICT 기술력이 취약하기 때문이다. 물론 북한의 인터넷이 활성화되어 있지 않고, 국가차원에서 1차원적으로 운영하기 때문에 '역 사이버공격'을 취하기는 매우 제한적이다. 하지만, 이러한 북한의 사이버 기반이 허술하기 때문에 1회의 공격으로 큰 피해를 줄 수도 있다.

미국의 경우, 사이버 위협에 대비하여 방어기술과 함께 공격을 위한 기술도 개발 해왔다. 2014년 11월 북한이 미국 내 소니픽쳐스 엔터테인먼트 사이트를 공격하여 시스템을 파괴하고 영화파일 등을 유출하여 경제적 피해를 주었을 때, 미국 오바마 대통령은 비록 민간회사에 대한 공격이었지만, '비례적 대응'[19]을 천명하고 북한 내 주요 웹사이트를 마비시키는 보복공격을 강행하였다. 또한, 2015년 미사일 방어 분야의 최고 전문가들이 워싱턴에 있는 싱크탱크 국제전략연구소에 모였을 때, 해군 소장으로 예편한 아처 메이지 주니어 장군은 국방부가 성공적인 미사일 발사를 막는 법 뿐 아니라 발사된 미사일의 탄도나 방향을 교란하는 방법도 개발하고 있었다고 말했다[20]. 2015년 4월 미 국방부가 발표한 '국방사이버전략'에 의하면, 국방부 네트워크와 시스템, 정보의 보호와 방어하는 능력을 구축하는데 초점을 두고 있다[21][4]. 또한, 미국은 이스라엘과 함께 '스턱스넷'을 이용하여 이란의 핵시설 제어시스템을 공격해 마비시키는 사례가 있다. 한편 일본은 사이버 공격에 대한 대응태세를 단순방어가 아닌 사이버 반격 임무도 할 수 있도록 민간과 함께 사이버사령부 창설을 추진하고 있다.[27]

따라서 한국도 미국과 같이 북한을 공격할 수 있는 사이버 안보전략과 이를 실행할 수 있는 능력을 갖추어야한다. 북한의 ICT 취약기반을 이용하여 핵, 미사일 등 시스템을 유사시에는 즉각 무력화 할 수 있는 기술력과 능력을 확보해야한다.

한국은 세계에서 가장 우수한 인터넷이 구축되어 있다. 이러한 환경에 잘 체득되어 있는 젊은 세대들에게 조기 사이버전사로서 양성이 필요하다. 또한 이들이 장기간 직장이 보장되고 사이버전사로서 역할을 할 수 있도록 제도적 장치를 마련해야 한다.

사이버전사 못지않게 중요한 것이 사이버전에 사용가능한 사이버무기, 즉 '백신', '스턱스넷(stuxnet)'과 같은 소프트웨어의 개발이다. 이는 예방·감시·차단·복구뿐만 아니라 공격이 가능한 기능을 포함해야 한다. 따라서 정보통신기술의 발전추이를 예측하고 이보다 앞선 기술을 개발·확보해야 할 것이다.

현재 한국은 일부 대학에서 사이버 보안 전문인력들을 교육하고 있으며, 정부출연 연구기관 및 과학기술원 등 특화된 기관에서는 사이버 안보와 관련하여 기술연구를 수행하고 있다. 하지만, 방호와 공격능력을 갖춘 전문인력을 별도 양성하지는 않고 있다. 따라서 국가적 차원에서 사이버 인력 양성을 위한 로드맵을 구축하여 북한의 사이버테러, 범죄, 간첩행위와 나아가서는 사이버 전쟁에 대비할 수 있는 역량을 구축해야겠다. 이러한 사이버 능력을 갖추게 된다면 북한의 군사적 도발 억지력에 상당한 효과가 있을 것이다.

4.2 통합적 사이버 안보 컨트롤타워 확립

사이버 역량 강화를 위해서는 무엇보다도 국가적 차원 사이버 안보를 총체적으로 관리할 수 있는 컨트롤타워가 필요하다. 한국은 2004년 2월 사이버 안보 대응기관인 국가사이버안전센터(NCSC)를 설치하였고, 2009년에는 국정원을 중심으로 한국인터넷진흥원(KISA) 등 15개 관련기관이 모여 합동 사이버위협 대응팀을 운영하였으며, 2010년에 사이버전쟁을 전담하는 사이버사령부를 설립하는 등 사이버 위협에 대한 국가차원의 총괄 관리체계를 마련하였다. 이후 2013년 3.20 북한의 사이버테러가 발생하자 청와대가 사이버안보 컨트롤타워의 역할을 담당하기로 했다[4]. 하지만 청와대는 정치적 의사결정기관이지 계획하고 대응하는 실무적 기관이 아니다. 따라서 대북 사이버 위협으로부터 전·평시 구분 없이 실시간 총체적으로 상황을 관리할 수 있는 기관이 필요하다.

현재 국가 사이버 안보에 관한 업무는 국가정보원이 총괄하고 있고, 북한 사이버 부대에 대응하여 국방부에서는 사이버사령부를 운용하고 있다. 하지만, 이는 이원적인 관리체계라는 중복성이 있다.

본 연구 2장에서 사이버전을 사이버 테러, 사이버 범죄, 사이버 간첩행위 등 유형별로 구분하였듯이 위협 성격에 따라 주관기관이 다른 실정이다. 이 판단 기준에 의해 국정원, 국방부, 경찰청 등으로 분류하여 관리한다면 사이버 안보에 오히려 취약할 수 있다.

비록 위협의 정도나 대응과정에서 다소 차이는 있지만, 사이버 위협이 미치는 영향과 확대 가능성 등을 고려할 때 이러한 위협을 관리할 수 있는 중앙집권형인 기관이 필요하다. 미국의 경우 오바마 대통령은 취임 이후 사이버 안보에 강한 의지를 표명하고, 4성 장군이 이끄는 사이버 사령부를 창설하였다. 한국은 세계 수준의 사이버 인력을 운용하고 있는 북한과의 직접적 적대관계이며, 유사시에는 사이버전쟁이 발생할 가능성을 배제할 수 없다. 따라서 이를 예방, 대비, 대응을 통합 전담하는 전문 기관이 필요하다. 즉, 유사시 핵, 미사일 등 북한의 전략자산을 무력화 할 수 있는 역량을 갖추고 전·평시 구분 없이 북한의 사이버 안보위협을 실시간으로 관리하며, 사이버전을 수행할 수 있는 통합적 컨트롤타워가 필요하다고 하겠다.

4.3 국내 사이버 관련법 제정

사이버 안보는 사이버 공간의 특성상 적의 공격이 국가나 공공기관 뿐만 아니라 민간분야까지 미치기 때문에 이를 총괄하여 전문적으로 업무수행이 가능한 법적 근거가 필요하다. 하지만 현재 우리나라는 2005년 1월 대통령훈령으로 「국가사이버안전관리규정」을 제정한 수준에 머무르고 있다.

물론 정보통신기반보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 개인정보보호법 등이 있으나, 이는 국가적 차원에서 사이버 위협으로부터 보장을 위한 법률로서는 미약한 수준이다.

미국의 경우를 보면, 미국은 주요 기반시설에 대한 사이버공격에 대비한 「사이버안보보호법」, 사이버 전쟁에 대비한 민·관 협력을 규정한 「사이버안보강화법」 등의 관련 법률을 제정 및 시행하고 있다[4]. 또한, 최근 2018년 6월 26일에는 북한의 사이버 공격 등에 대비한 「사이버외교법안」이 미 상원 외교위원회를 통과하였다. 이 법안에 따르면, 국무부 산하에 설치되는 사이버 부서는 의회의 감독 하에 미국의 국제적인 사이버 정책 집행 등을 담당할 예정이다[22].

하지만, 한국은 「국가사이버안보에 관련한 법률안」이 정치적인 목적으로 악용될 우려가 있다하여 국회에 계류 중에 있는 상태이다. 국방부에서는 「국군사이버사령부령」을 운용[16]하고 있으나, 국가차원 사이버 안보를 위한 조치로는 역부족이다.

북한의 사이버 위협이 가속화되고 있고, 미국 등 선진국과 국제 공조에 맞추기 위해서도 사이버 안보와 관련된 법이 하루 빨리 제정되어야 할 것이다.

4.4 다자간・지역내 사이버 협력체제 구축

북한의 사이버 공격은 주로 위장을 위해 북한 내부가 아니라 중국, 동남아 국가 등 제3국 경로를 이용하여 자행하고 있다. 따라서 여러 관련국들과의 실효성 있는 사이버 안보 협력은 매우 중요하다.

한국은 북한의 소니픽처스사의 전산망 해킹사건 이후 미국과 사이버안보를 위한 공조를 강화해 오고 있다. 양국은 2013년부터 '한·미 정보통신기술(ICT) 정책포럼'을 개최하고 있으며, 2018년 6월 개최된 포럼에서는 양국 간 정책의 지속 공유·공조가 중요하다는 데 인식을 같이하고 사이버보안과 개인정보 보호에 대한 협력도 더욱 강화하기로 하였다[23].

또한, 한국은 이미 미국, 중국, 러시아, 인도 등 총 11개국과 양자·3자 사이버정책협의회를 개최하고 있으며, 2016년 10월 28일에는 서울 외교부 청사에서 일본과 '첫 사이버정책협의회' 열어 북한발 사이버 공격 등에 대한 공조 방안을 논의하였다[24].

따라서 정보통신기술의 발전과 함께 날로 진화되고 있는 북한의 사이버 위협에 적시에 대응하고 정보공유를 하기 위해서는 여러 국가들과 사이버 안보협력을 강화해야 할 것이다. 특히 한반도에 전쟁이 발발 시 북한의 핵, 미사일 등 무기체계와 지휘부 의사결정시스템을 한・미・일 간 공조하여 무력화 할 수 있는 강력한 사이버 협력체를 구축할 필요가 있다. 이는 북한의 군사적 도발 억지력에 전략적 가치가 매우 클 것이다.

5. 결 론

사이버 공간에서 발생하는 위협은 초공간·비선형적으로 이루어지는 속성 때문에 아무리 방어벽을 철저하게 쌓는다 하여도 빈틈이 생길 수밖에 없다.

이에 따라 세계 각국은 사이버 안보위협에 대한 대응방안을 마련하기 위해 고심하고 있다. 그만큼 사이버 안보위협은 전·평시 구분 없이 정치적 혹은 군사적으로 상당한 피해를 줄 수 있기 때문이다.

사이버 위협은 새로운 안보영역으로 부각되고 있으며 한국의 안정과 평화에 절대적으로 중요한 부분이다. 북한은 사이버 전력을 강화하고 있으며, 이는 핵, 미사일 등과 함께 한국의 3대 위협이다.

북한의 사이버 전력은 대미, 대남 억제력을 넘어 이미 도발을 위한 공격력 수준이라고 평가되고 있다. 즉 사실상 핵무기를 보유하고 있다고 추정되는 현시점에서 북한이 핵전략과 함께 사이버전을 결합하여 도발할 경우 이는 우리 안보에 매우 위협적이다.

북한은 한국을 대상으로 지난 10여 년간 다양한 방법으로 정부·방송·금융 분야 구분 없이 공격을 자행해 왔다. 그때 마다 정부에서는 많은 대책을 제시하였으나, 제대로 실현된 것은 없다.

본 논문에서는 대북 사이버 안보역량 강화를 위해 4가지 방안을 제시하였다. ① 적극적 사이버 방호 및 공격능력 확보이다. 한국은 '방호 능력'을 탈피하여 '공격 능력'을 확보할 수 있어야한다. 방호능력이란 적의 사이버 공격을 적시에 인지하고 피해를 최소화해야 하며, 피해사항에 대해서는 조기에 원상회복할 수 있는 능력이다. 또한, 공격능력이란 평시부터 북한의 사이버 취약요소를 식별하여 별도 관리하면서 즉각적인 공격 수행이 가능한 능력이다. 따라서 이를 위한 전문 인력을 양성해야 한다. ② 통합적 사이버 안보 컨트롤타워 확립이다. 북한의 사이버 공격은 지금까지 수차례 일어났으며, 한국사회의 정치·경제·군사적 분야 등에 손실과 함께 큰 혼란을 야기하였다. 이러한 북한의 사이버 위협은 앞으로도 전·평시 구분 없이 한국사회에 심각한 피해를 줄 것이다. 따라서 국가차원 총괄할 수 있는 통합적 컨트롤타워가 있어야겠다. ③ 국내 사이버 관련법 제정이다. 사이버 위협은 정보기술의 발전과 함께 매우 다양하게 진화하고 있으나, 아직까지 한국은 사이버 관련 기본법이 없는 현실이다. 사이버 안보 위협이 국민의 재산과 국가안보에 심각한 피해를 주는 만큼 이른 시일 내 관련법률 제정이 절실하게 필요하다고 하겠다. ④ 다자간・지역내 사이버 협력체제 구축이다. 북한은 주로 중국 등 제3국 서버 경로를 이용하여 사이버 공격을 자행해 왔다. 따라서 피해를 최소화하고 조기 추적 및 대응을 위해서는 관련국과의 절대적 협력이 필요하다. 또한, 해당국 범죄 집단으로부터 사이버 위협 행위를 차단하기 위해서도 지역내 여러 국가들과의 사이버 협력 체제를 구축할 필요가 있겠다.

한국은 인터넷과 과학기술의 발달로 정부, 기업, 개인 등 모든 시스템과 생활권이 사이버 공간에서 초연결화 되어 있으며, 정부기관, 은행 등 사회 기반 시설뿐만 아니라 국가 안보 의사결정 지휘체계와 전쟁 시에 운용되는 첨단무기체계도 유·무선 네트워크화로 연결되어 있다. 또한, 안보 위협은 기존 전통적 안보 위협에서 사이버 공간이 포함된 포괄적으로 다양화되고 있으며 위협수단과 방법이 첨단화되었을 뿐만 아니라 사이버 공간에서 발생하는 불특정 안보위협은 국가적·사회적으로 큰 혼란을 초래하고 있다.

북한은 대남적화혁명을 위한 수단으로 이러한 한국내 사이버 공간을 활용하고 있다. 또한, 앞으로의 전쟁은 물리전력과 사이버전력이 혼재되어 통합된 양상으로 전개될 것이다. 전쟁이 발발 전 또는 초기부터 사회기반시설이 마비되고 첨단무기체계의 불능으로 불용·무력화된다면 심리적 약화와 함께 상당한 피해를 보게 되고 국가적으로 감당하기 힘든 혼란이 야기될 것이다.

따라서 한국정부는 평시 북한의 사이버 공격 위협으로 부터 국민의 재산과 기본권을 보장하고 유사시 완전한 전쟁수행 보장을 위해 국격에 맞는 사이버 안보 역량을 강화해야 할 것이다.

참고문헌

[1] 마정미, “북한의 사이버 위협과 심리전에 대한 대응방안,” 국방대학교 국가안전보장문제연구소, pp.107 - 137, 2017

[2] 손영동. “사이버 안보와 국방 대응태세”. 군사논단, 제94호. pp.10-22. 2018.

[3] 김종하. “‘사이버 작전’ 독립 軍조직 필요하다”. 문화일보, 2016년 6월 15일.

[4] 조성렬, ‘전략공간의 국제정치: 핵, 우주, 사이버 군비경쟁과 국가안보’, 서강대학교 출판부, 2016.

[5] 유동열, ‘사이버공간과 국가안보’, 북앤피플, 2012.

[6] 허태희, 이상호, 길병옥, “위기관리이론과 사이버 안보 강화방안”, 국방연구, 제48권, 제1호, 국방대학교 안보문제 연구소, p.40, 2005,

[7] 정찬기, 이수진, ‘사이버 전쟁’, 국방대학교 국가안전보장문제연구소, p.432, 2014,

[8] 나용우. “초연결 융합시대와 사이버안보: 사이버 공간의 안보화와 한국의 사이버안보 강화 방안”. 공공정책연구소, p.39, 2017.

[9] 장노순, 한인택, “사이버안보의 쟁점과 연구경향”, 국제정치논총, 제53권, 제3호, pp.579-618. 2013.

[10] 김경곤 외 2(역), ‘사이버 보안과 국가 안보 전략’, 갑우문화사, p.534, 2015.

[11] The White House, “International Strategy for Cyberspace”, 2011.

[12] 박웅신, “복합적 위험사회에서 사이버 테러 규제 방안에 대한 연구”, 법제처 미래융합법제 연구보고서, 법제처, p.177, 2013.

[13] 정용기, “우리나라의 사이버 안보 위협현황과 대응 방안,” 경찰학연구소, 경찰학논총, 제11권, 제4호, pp.195-196, 2016.

[14] 김홍석, “사이버 테러와 국가안보”, 저스티스, 통권, 제121, pp. 319-356, 2010.

[15] 윤민우, “새로운 안보환경을 둘러싼 사이버테러의 위협과 대응방안”, 한국경호경비학회, 제40호, pp.118 -129, 2014.

[16] 국방부, ‘2016 국방백서’, 2016.

[17] 김승주. “세계 각국의 사이버전 수행능력과 국내 피해사례”. 군사논단, 제75호, pp.19-36, 2013.

[18] 신재헌, 김용현, “사이버 상의 안보위협에 대한 대응방안”, 한국경찰연구, 제15권, 제3호, pp.82-83. 2016.

[19] 연합뉴스, 2014년 12월 20일.

[20] David E. Sanger and William J. Broad, “U.S. Strategy to Hobble North Korea Was Hidden in Plain Sight”, New York Times, 2017.

[21] DoD, US Department of Defense Cyber Strategy, pp.2-8, 2015.

[22] NEWSIS, 2018년 6월 28일.

[23] 이데일리, 2018년 6월 22일.

[24] 연합뉴스, 2016년 10월 28일.

[25] 임종인 외 4, “북한의 사이버전력 현황과 한국의 국가적 대응전략”, 국방정책연구, 제29권, 제4호, p.23, 2013.

[26] 월간조선, 2015년 9월호.

[27] 중앙일보, 2018년 7월 16일.

[저 자 소 개]

김 호 중 (Ho Jung Kim)
1988 해군사관학교 학사
1994 목포대학교 경영행정대학원 석사
2017 한남대학교 대학원 박사
現 한남대학교 경영국방전략대학원 겸임교수
E-mail: ogoskim@hanmail.net

김 종 하 (Jong-ha Kim)
1989 울산대학교 학사
1993 경희대학교 평화복지대학원 석사
1997 영국 브리스톨대학교 정책대학원 박사
現 한남대학교 정치언론국방학과 교수
E-mail: jong-ha44@hanmail.net