북한의 사이버전 위협에 대한 분석과 전망

이대성* · 안영규** · 김민수***

요 약

현대사회에서 정보통신기술의 발달은 인류에게 많은 기회를 제공하고 있지만, 그 이면에는 사이버 공격으로 인한 막대한 손해도 발생하고 있다. 최근 한국도 사이버 공격의 대상이 되었고, 그 위협의 범위도 점차 확대되고 있다. 특히 북한은 한국을 대상으로 한 적대행위를 지속적으로 자행하고 있으며, 최근에는 국가중요시설 등의 전산망을 공격하는 사이버 공격을 감행하고 있다. 이러한 북한의 사이버 공격 유형으로는 소프트웨어(Software) 측면에서 인터넷 내부를 파괴하거나 조정하는 컴퓨터 바이러스(Virus)와 웜(Worms), 트로이 목마(Trojan Horse), 분산서비스 거부공격(Distributed Denial of Service) 등이 있다. 이를 해결하기 위해 다음과 같은 제언을 하고자 한다. 첫째, 북한은 사이버 공격을 위하여 일원화된 조직체계를 갖추고 있으므로, 한국도 효과적인 대처를 위해 일원화된 대응조직체제로 전환할 필요성이 있다. 둘째, 소프트웨어 측면의 공격에 체계적으로 대응하기 위해서는 가칭 『사이버테러리즘방지법』의 제정을 적극 검토하여야 한다.

Analysis and prospect of North Korea's Cyber threat

Lee, Dae Sung* · Ahn, Young Kyu** · Minsu Kim***

ABSTRACT

In modern society, the development of Information and Communication Technology has given people a lot of opportunities. But on the other side cyber attack also gives enormous damage to people. Recently Korea has become the target of cyber attack. The threat of it is growing. Especially North Korea has committed hostile actions against South Korea. North Korea has recently attacked the computer networks of South Korea's important national facilities. The types of North Korea's cyber attacks include the followings. First, if we see it with the viewpoint of software, it tries to destroy or control the Internet, infects the networks with viruses, worms, Trojan Horse and Distributed Denial of Service. I suggest the following to solve the problem. First, South Korea should unify the organizations to respond to the attacks of North Korea, as North Korea has a unified organization for the cyber attack. Second, they should think about the establishment of 『Cyber Terrorism Prevention Act』 to systematically respond to the software attacks.

Key Words: Information and Communication Technology, Cyber Attack, Cyber Terrorism, Control Tower, Cyber Terrorism Prevention Act,

접수일(2016년 8월 22일), 게재확정일(2016년 9월 19일)

* 동의대학교 / 경찰행정학과
** 신경대학교 / 경찰행정학과
*** 경기대학교 / 융합보안학과

1. 문제의 제기

1950년 6월 25일 남침 이후, 북한이 한국을 대상으로 자행한 폭력적 통일전략전술로는 국지도발과 대남테러리즘 등이 있다. 북한의 국지도발행위를 살펴보면, 1960년대는 함정의 격침과 납치, DMZ에 무장공비 침투 등, 1970년대는 해안선과 도서산간(島嶼山間) 지역에 간첩 침투, 간첩선 남파 등, 1980년대는 GOP부대에 침투, 강(江)·만(灣) 등의 지역에 수중 침투 등, 1990년대는 해안 잠수정 침투, 도서지역에서의 해전 등, 2000년대는 북한 방문 관광객 피살, 도서지역 포격 등이 있다[1].

북한의 대남테러리즘을 고찰해보면, 1960년대는 항공기 납치, 국가기관 습격, 산간지역 양민 학살 등, 1970년대는 국가중요시설 폭파, 정부요인 암살, 유명인사 납치 등, 1980년대는 해외에서 국가정부요인을 대상으로 폭파, 항공기 폭파 등 1990년대는 해외에서 정부요인 암살, 탈북요인 암살 등, 2000년대는 중국의 동북3성에서 선교사와 목사 납치·살해, 탈북요인 암살 미수 등이 있다. 이를 통하여 2000년 이전(以前) 북한의 대남테러리즘 유형으로는 정치·군사적 측면의 정찰과 정보수집, 잠수정 등을 활용한 대남 간첩과 무장게릴라의 직접 침투, 한국 정부요인 및 유명인사의 납치와 암살, 해외에서 불특정 다수의 한국인을 대상으로 한 폭탄테러리즘 등이 있었다. 그리고 2000년 이후(以後) 북한은 한국과 중국 등의 지역에서 반북활동을 하는 탈북인과 선교사 등을 대상으로 한 납치와 암살 등에 주력하고 있으며, 이를 전담하는 기관으로는 정찰총국과 국가안전보위부 등이 있다[2].

이외에도 북한은 비대칭전력을 활용한 대남도발을 감행하고 있는데, 그 대표적 사례는 사이버전이다. 북한은 2009년부터 공격을 시작하여 2016년 현재까지 지속적인 사이버 공격을 하고 있다.

특히 한국은 세계적 수준의 인터넷망과 IT기술을 보유하고 있는데, 이러한 인터넷과 정보통신기술(ICT)은 국가기간산업 및 국가안보관련 시스템 등과도 밀접한 관련이 있기 때문에, 북한의 사이버 공격은 더욱 큰 위협이라고 할 수 있다. 이로 인하여 북한은 사이버전력 증강을 위한 핵심 기술 개발과 전문 인력 양성에 주력하고 있다[3][4].

이 연구에서는 북한의 사이버전 사례를 분석하고, 향후 발생 가능한 사이버전 공격을 전망하고자 한다. 또한 이를 통해 현행 대응시스템의 문제점을 고찰하여 그 개선방안을 모색하고자 한다.

2. 사이버전에 대한 이론적 검토

2.1. 사이버전 개념

사이버전(Cyber Warfare)은 관점에 따라 다의적 개념 정의가 이루어지고 있다. 국가기관, 연구소, 학자들의 견해는 다음과 같다. 우선, 합동참모본부는 사이버전을 컴퓨터에 의해 조성되는 가상 현실세계(Cyber space)와 가상인간의 영역과 같이 인공지능체계가 운용되는 공간에서의 전쟁 형태로 정의되고, 이는 정보화 사회의 과학기술 발전을 역이용하여 취약점을 공격함으로서 물리적인 군사시스템 파괴보다 훨씬 결정적인 손실을 강요할 수 있는 총체적인 가상공간에서의 정보마비전을 추구하는 전쟁수행방식으로 구체화하였다[5].

다음으로, RAND연구소는 다른 국가의 컴퓨터 또는 정보네트워크를 공격하거나 손상시키려는 국가 또는 국제조직의 행위를 사이버전이라고 하였다[6].

마지막으로, 윤규식은 사이버전을 전쟁 또는 전쟁에 준하는 의도를 갖고 정보통신망이나 정보통신 기반시설을 불법 침입하거나 교란 또는 마비시키고, 파괴하거나 정보를 절취·훼손하여 자국에게 유리한 상황을 조성하고자 하는 일체의 공격행위라고 규정하였다[7]. 이외에 리비키(Martin C. Libicki)는 사이버전을 정보전의 한 분야로서 사이버 공간에서 이루어지는 공격 형태이나 정보시스템 또는 그 속에 내재된 정보에 대한 내적인 공격이라고 정의하였다[8].

2.2. 사이버전 특징과 유형

사이버전은 네트워크가 연결된 곳이라면 언제·어디서나 공격이 용이하고, 정보 유출·왜곡·파괴가 가능하며, 국가 전체의 기능을 마비시킬 수도 있다. 또한 사이버전은 약소국이 강대국에 대응할 수 있는 비대칭 전력이라고 할 수 있고, 일반적으로 정보통신 인프라

(infrastructure)가 잘 구축되어 있는 국가일수록 사이버공격에 취약하며, 공격 기술의 융합으로 인한 진화와 변종으로 인하여 ·변종하기 때문에 탐지와 대응에 한계가 있다[9].

사이버전 유형은 다양한 형태로 구분할 수 있지만, 적용기술의 방식에 따라 해킹(Hacking), 전자우편 폭탄(E-mail Bomb), 논리폭탄(Logic Bomb), 분산서비스거부(Distributed Denial of Service: DDos) 등이 있다[10]. 우선, 해킹은 정보시스템의 취약점을 이용, 무단 접근하여 자료의 유출·위조·변조·삭제·시스템 장애 및 마비를 유발하는 행위로써 매우 다양한 기술이 개발되어 있고, 전자우편 폭탄은 상대 컴퓨터에 매우 크거나 다수의 전자우편을 발송하여 시스템을 마비시키는 수법으로 스팸(Spam)이라고도 한다.

다음으로, 논리폭탄은 날짜와 시간 등의 특정 조건을 충족시키거나 외부 입력 신호에 의해 상대 컴퓨터 내의 정보를 파괴하거나 정보의 사용을 방해하는 프로그램을 작동시킴으로써 상대시스템을 무력화하는 방식이고, 분산서비스거부(DDos)는 컴퓨터 통신을 거쳐야 하는 신호송신, 송신자응답, 송신자신호 전송의 인증과정에서 상대방의 신호를 받고서도 의도적으로 신호전송을 거부해 상대 컴퓨터를 계속 신호대기상태로 유지시킴으로써 시스템을 무력화하는 방법이다.

마지막으로, 스니핑(Sniffing)은 통신상에서 소프트웨어적 방법으로 접속하여 'ID'나 'Password' 등의 정보를 도청하는 방법이고, 객체이동 가상무기(Autonomous Mobile Cyber Weapon: AMCW)는 외부의 조작없이 스스로 네트워크를 따라 목표를 찾아 이동하면서 바이러스(Virus)와 유사한 방법으로 상대의 컴퓨터나 네트워크의 특정 목표만을 공격하여 마비시키거나 정보를 조작하는 무기이다.

3. 북한 사이버전에 대한 분석과 평가

3.1. 북한 사이버전 운영체계

북한은 1960년대부터 컴퓨터 개발을 시작하여 1974년에 1세대와 2세대 컴퓨터를 자체 개발하였고, 1975년부터 1982년까지 IT강국 추진정책을 통하여 3세대 소형(mini) 컴퓨터를 개발하였으나, 1983년부터 1998년까지 4세대 컴퓨터 개발에는 실패하였다. 1999년 이후부터 IT 강국으로의 도약을 위해 국가발전전략을 제시하여 조선노동당 군사공업부 산하 21국 주도로 5세대 컴퓨터 개발을 추진하였으나, 이 또한 실패하였다. 현재 북한 주민들의 컴퓨터 사용 인구는 전체 약 2,490만 중에 5% 정도이고, 국가기관은 30% 정도 보급되어 있는 것으로 추정하고 있다[11][12].

이러한 현실에도 불구하고 북한은 사이버전력을 증강하기 위한 다양한 방안을 모색하였다. 우선, 북한은 사이버 전문 인력 양성을 위해 중등교육부터 영재급 수재 선발을 통해 집중적인 교육을 실시하고 있다. 다음으로, 북한은 1986년 김정일의 지시로 미림대학(2000년 지휘자동화대학)에서 매년 100여명의 전문 인력을 배출하고 있다. 이외에도 북한은 1997년 이후부터 조선노동당 예하 모란봉대학에서 전문 해커(Hacker)를 양성하고 있다. 마지막으로, 현재 북한은 중국, 일본, 스위스 등의 다양한 국가의 인터넷 서버(Internet server)와 정보제공 사업자(Information provider)를 이용한 다양한 사이버전을 감행하고 있다[13][14].

북한의 대남 사이버전 조직과 기능은 국방위원회와 조선노동당로 구분하여 설명할 수 있다. 첫째, 국방위원회 총참모부는 ⅰ) 지휘자동화대학 등은 사이버전사 양성과 연구, ⅱ) 적공국 204소는 한국군 대상 사이버심리전 실행, ⅲ) 지휘자동화국은 한국군(軍)의 지휘통신 교란과 사이버전을 실행하고 있다. 둘째, 국방위원회 정찰총국은 ⅰ) 모란봉 대학은 사이버 요원 양상과 연구, ⅱ) 기술총국 110연구소와 414연락소 등은 대남정치·군사정보 해킹·사이버공작·전담요원해외파견·사이버테러리즘·사이버 외화벌이·대남심리전 등을 수행하고 있다. 셋째, 조선노동당 통일전선부는 ⅰ) 대남 사이버심리전 전담, ⅱ) 구국전선 등과 같은 160여개 웹사이트 운영, ⅲ) 트위터 등을 활용한 SNS 공작팀 운영, ⅳ) 대한민국의 여론조작을 위한 댓글팀 운영과 허위정보를 통한 사회교란 시도를 하고 있다. 넷째, 조선노동당 문화교류국은 ⅰ) 한국 내의 전략정보 수집, ⅱ) 한국 내의 간첩망을 활용한 흑색선전 등의 사이버심리전 병행, ⅲ) 사이버 드보크(Cyber Dvoke)와 사이버 간첩 교신을 하고 있다[15].

3.2. 북한 사이버전 사례분석

2009년 7월부터 2016년 현재까지 북한은 한국을 대상으로 11건의 사이버 공격을 감행하였다.

<표 1> 연도별 발생 건수

년도	2009	2010	2011	2012	2013	2014	2015	2016
공격 횟수	1	0	2	1	2	2	1	2

북한 사이버 공격 사례를 분석한 결과는 다음과 같다[16]. 우선, 북한의 사이버전은 소프트웨어(Software)적 측면의 공격으로 분류할 수 있다. ⅰ) 북한의 사이버전은 해킹(Hacking) 9건, 분산서비스거부(DDos) 2건이었고, ⅱ) IP 추적결과는 북한 평양시 8건, 중국 요령성 3건으로 밝혀졌다.

다음으로, 북한은 사이버전 수행을 위해 분산서비스거부(DDos)와 해킹(Hacking)을 활용하였다. ⅰ) 직접적인 DDos 공격 또는 좀비 PC를 활용하여 35개 국가기관, 금융사, 증권사, 포털사이트 등의 홈페이지를 마비시켰다. ⅱ) 악성코드를 유포하거나 감염시켜 KBS, MBC, 신한은행, 농협, 금융보안업체 등의 서버, PC, ATM 등의 기능을 마비시키거나 자료를 파괴하였다. ⅲ) 해커(Hacker)의 직접적인 공격을 통하여 청와대, 국무조정실, 정당, 언론사, 등의 전산시스템의 무력화를 시도하였으며, 한국수력원자력 설계도면과 조직도를 유출하였다. ⅳ) 해킹 조직으로 추정되는 단체가 외교부, 국방부 등에 근무하는 외교·안보 공무원 등의 E-mail에 접근하여 계정과 비밀번호를 유출하였다.

<표 2> 북한 사이버전 사례분석

유형	공격방법	공격대상	
사이버전	DDos	국가기관	안정행정부 청와대 통일부 외교부 국회 등
		국가기반시설[1]	금융사 등
		민간시설	인터넷 포털사이트 증권사 은행 등
	Hacking	국가기관	국무조정실 청와대 정당 등
		국가기반시설	한국수력원자력 KBS MBC YTN 등
		민간시설	금융보안업체 대학병원 신한은행 농협 등

3.3. 분석에 대한 평가

북한 김정은은 사이버전을 핵·미사일과 함께 우리 인민군대의 무자비한 타격능력을 담보하는 '만능의 보검'이라고 언급하면서, 사이버전을 핵·미사일과 함께 3대 전쟁수단으로 규정하였다[18]. 우선, 북한은 한국을 대상으로 지속적인 사이버전을 감행하고 있다. 이는 북한이 평화적 또는 비평화적 방법으로 한국을 통일하기 위한 수단으로 사이버전이 매우 유용하다는 것을 의미한다.

다음으로, 북한은 방법적 측면에서 좀비 PC의 동원, 악성코드의 감염·유포, 해커(Hacker)의 직접적인 공격 등을 활용한 분산서비스거부(DDos)와 해킹(Hacking)을 감행하였고, 공격대상도 국가기관, 국가기반시설, 민간시설로 그 범위도 확대되었다. 이는 북한이 한국의 사이버 인프라(infrastructure)의 취약성 등을 잘 파악하고 있는 것이고, 추후의 사이버공격을 실행하기 위한 준비, 보완, 완료하였다는 것을 의미한다.

마지막으로, 현재까지 공식적으로 밝혀진 북한의

1) 국민의 생명과 재산, 경제에 중대한 영향을 미칠 수 있어 지속적 관리가 필요하다고 인정되는 국가기반시설에는 9개 유형 19개 분야의 국가기반체계 내에 250여개소가 지정·관리되고 있다. 구체적으로 보면, 에너지 분야에 전력·가스·석유시설 37개소, 정보통신 분야에 통신망·전산망시설 24개소, 교통수송 분야에 철도·항공·화물·도로·지하철·항만시설 32개소, 금융 분야 관련시설 8개소, 보건의료 분야에 의료서비스·혈액시설 40개소, 원자력 분야에 관련시설 22개소, 환경 분야에 매립시설 5개소, 식용수 분야에 댐·정수장시설 79개소, 정부중요시설 분야에 정부청사 3개소가 지정되어 있다[17].

사이버 공격 유형은 분산서비스거부(DDos)와 해킹(Hacking) 공격이었다. 그러나 북한이 지속적으로 사이버전력을 강화한 것으로 볼 때, 위의 공격과 함께 전자우편 폭탄(E-mail Bomb), 논리폭탄(Logic Bomb), 십핑(Shipping) 등의 방법으로 한국의 국가기관, 국가기반시설, 민간시설 등을 대상으로 한 동시다발적인 사이버 공격의 가능성도 배제할 수 없다.

4. 제언 및 결론

현대사회에서 정보통신기술의 발달은 인류에게 많은 기회를 제공하고 있지만, 그 이면에는 사이버 공격으로 인한 피해도 발생하고 있다, 현재 한국도 사이버 공격의 대상이 되었고, 그 위협의 범위도 점차 확대되고 있다. 특히 북한은 한국을 대상으로 다양한 적대행위를 지속하였고, 최근에는 사이버 공격도 감행하고 있다. 이러한 공격은 정치・경제・사회적으로 피해규모가 막대하고, 파급 효과가 엄청나기 때문에 가칭『사이버테러리즘방지법』의 제정을 검토할 필요성이 있다. 물론, 현행 『정보통신망이용촉진및정보보호등에관한법률』,『정보통신기반보호법』 등으로 북한의 사이버 공격에 대처할 수 있다는 견해도 있지만, 동법들은 사전예방보다는 사후진압에 초점을 두고 있으므로, 북한의 조직적이고 선제적인 사이버 공격에 대처하기에 한계가 있다는 평가를 받고 있다. 만약, 사전예방 측면에 중점을 둔 가칭『사이버테러리즘방지법』이 제정된다면, 북한의 사이버 공격에 세부적이고 구체적으로 대처할 수 있는 '사이버 대(對)테러활동'의 법적 시스템이 구축되는 계기가 될 것으로 기대된다.

북한의 사이버 공격은 국가차원에서 국방위원회와 조선노동당으로 이원화된 체계로 운영되고 있다. 두 기관 모두 체계적이고 장기적인 계획 하에서 전자는 직접적인 공격을, 후자는 간접적인 심리전을 전담하고 있다. 또한 북한은 한국의 국가기관, 국가기반시설, 민간시설 등을 대상으로 무차별적인 사이버 공격을 감행하고 있다. 이에 대해 한국은 경찰청 사이버안전국, 대검찰청 사이버수사과, 국가정보원 국가사이버안전센터, 한국정보보호진흥원 인터넷침해사고대응지원센터 등에서 분산된 업무를 수행하고 있다. 이로 인하여 북한의 빈번한 사이버 공격에 체계적으로 대처하지 못한다는 평가를 받고 있다. 또한 실질적인 사이버 공격이 발생한 경우에도, 각 기관의 역할과 책임에 대한 명확한 규정이 불분명하여 관할권 문제가 발생하고 있다. 이에 북한의 사이버 공격에 체계적이고 효과적으로 대처할 수 있는 총괄전담기구(Control Tower)가 필요하다고 판단된다.

참고문헌

[1] 김광진, "북한의 대남테러 조직 및 테러전망", 국가안보전략연구원・이스라엘 국제대테러연구소 공동 국제학술회의 자료집, 75-98, 2016.

[2] 이대성, "북한의 대남테러리즘 분석과 향후전망: 김일성・김정일・김정은 집권기를 중심으로", 한국테러학회보, 5(1): 125-147, 2012.

[3] 김진무, "북한의 비대칭전력을 이용한 대남군사전략을 방관하지 말아야 할 때", 북한, 410: 84-92, 2006.

[4] 박창권, "안보를 위협하는 북한의 비대칭전력에 새로운 대응전력과 능력을 강화할 때", 북한, 411: 121-132, 2006.

[5] http://www.jcs.mil.kr: 2016. 2. 7.

[6] http://www.rand.org: 2016. 2. 8.

[7] 윤규식, "북한의 사이버전 능력과 위협 전망", 군사논단, 68: 64-95, 2011.

[8] Libicki, Martin C. *What Is Information Warfare?,* Washing, D. C.: National Defense University, 1995.

[9] 김기수, "북한의 사이버전 위협과 대비방안", 한국정책학회 학술대회 자료집, 2013, 293-311.

[10] 노훈・이재욱, "사이버전의 출현과 영향, 그리고 대응방향", 국방정책연구, 53: 177-201, 2001.

[11] 배달형, "국가군사전략급 수준에서 북한 사이버 위협과 한국군의 대응방향", 전략연구, 52: 147-174, 2011.

[12] 육군사관학교,「북한학」, 서울: 황금알, 2004.

[13] Lee Dae Sung, "A Study on the possibility of North Korean Cyber-Terrorism and its Counter

measures", Korean Terrorism Studies Review, 2 (2): 1-37, 2009.
[14] 임종인·권유중·장규현·백승조, "북한의 사이버전력 현황과 한국의 국가적 대응전략", 국방정책연구, 29(4): 9-45, 2013.
[15] 유동열, "북한의 사이버 위협 실태와 대책", 한국안보정책학회·한국테러학회·한국반테러정책연구원·국가안전정책학회 공동학술세미나 자료집, 47-78, 2016.
[16] www.yonhapnews.co.kr: 2016. 8.13.
[17] 행정자치부,「국가기반체계 보호전략 개발연구」, 경기도: 한국건설기술연구원, 2012.
[18] 김인수, "북한의 사이버전 수행능력의 평가와 전망", 통일정책연구, 24(1): 117-148, 2015.

[저 자 소 개]

이 대 성 (Lee, Dae Sung)

1997년 동국대학교 법학사
2000년 동국대학교 법학석사
2004년 동국대학교 형사학박사
現 동의대학교 경찰행정학과 부교수

email : dorian3145@daum.net

안 영 규 (Ahn, Young Kyu)

2001년 동국대학교 법학사
2008년 동국대학교 경찰학석사
2012년 동국대학교 경찰학박사
現 신경대학교 경찰행정학과 조교수

email : ayk93@hotmail.com

김 민 수 (Minsu Kim)

2004년 컴퓨터공학사
2012년 경호안전학석사
2015년 산업보안학박사
현 재 경기대학교 융합보안학과 초빙교수

email : fortcom@hanmail.net