사이버테러 대응방안에 관한 연구

김연준* · 김상진**

요 약

정보화 사회의 발달은 인간생활에 많은 편익을 제공하는 반면에, 새로운 유형의 위협을 증대시키고 있다. 특히 사이버테러는 컴퓨터체계와 정보통신망으로 구성된 네트워크상에서 발생하고 있으며 그 방법과 피해규모는 심각한 수준에 이르고 있다. 즉 사이버테러는 현실세계가 아니라 가상공간에서 발생하여 공격주체가 누구인지?(비가시성, 비정형성), 어디에서 공격을 하는 것인지?(초국가성) 등 그 실체파악이 대단히 어려운 실정이다. 사이버테러를 시행하는 해커는 개인 혹은 소규모단체의 수준임에도 불구하고, 국가의 안전을 위협할 수 있는 새로운 위협을 제시하면서 현재도 그 위협의 양상과 규모를 더욱 진화시키고 있다. 북한의 사이버테러 규모와 능력은 세계적 수준으로 평가되고 있다. 최근 북한은 사이버테러 역량강화에 주력하고 있다. 이에 한국 안보에 직접인 위협으로 부상하고 있는 사이버테러에 대한 대응체계 개선은 선택이 아니라 국가생존을 위한 필수적인 과제이다. 따라서 한국은 북한과 주변국가로부터 발생하는 사이버테러에 선제적으로 대응하기 위해서 국가차원의 통합된 컨트롤타워 기능을 수행할 수 있도록 법적•제도적 장치를 시급히 보완해야 한다.

Research on Cyber-terrorism preparation scheme

Kim Yeon Jun* · Kim Sang Jin**

ABSTRACT

While evolving information-oriented society provides a lot of benefits to the human life, new types of threats have been increasing. Particularly, cyber terrorism, happen on the network that is composed of a computer system and information communication network, and the mean and scale of damage has reached a serious level. In other words, it is hard to locate cyber terror since it occurs in the virtual space, not in the real world, so identifying “Who is attacking?” (Non-visibility, non-formulas), or “Where the attack takes place?” (trans-nation) are hard. Hackers, individuals or even a small group of people, who carried out the cyber terror are posing new threats that could intimidate national security and the pace and magnitude of threats keep evolving. Scale and capability of North Korea's cyber terrorism are assessed as world-class level. Recently, North Korea is focusing on strengthen their cyber terrorism force. So improving a response system for cyber terror is a key necessity as North Korea's has emerged as a direct threat to South Korean security. Therefore, Korea has to redeem both legal and institutional systems immediately to perform as a unified control tower for preemptive response to cyber terrors arise from North Korea and neighboring countries.

Key words : cyber-terrorism, non-visibility, non-formulas, trans-nation, preemptive-response.

접수일(2016년 5월 12일), 게재확정일(2016년 5월 30일)

* 용인대학교 군사학과
**용인대학교 학점은행제 경호비서전공(항공보안)

1. 서 론

정보화 사회가 고도화됨에 따라 정보통신기술로 인해 현대 사회는 편리해지기도 하였지만 보다 복잡한 양상을 보이고 있다. 컴퓨터체계와 정보통신망의 확산되면서 네트워크를 통한 사이버테러의 위협은 점차 증가하고 있으며, 그 피해규모도 더욱 커지고 있다. 현실세계가 아닌 가상공간에서 이루어지는 사이버테러는 공격주체가 누구인지?, 어디에서 공격을 하는 것인지? 등의 실체 파악이 곤란하며, 해커가 개인 혹은 소규모 단체수준임에도 불구하고 국가의 안전을 위협할 수 있는 새로운 위협을 제시하면서 현재도 그 위협의 양상과 규모는 더욱 진화하고 있는 실정이다.

우리는 북한이라는 실체적인 위협과 첨예하게 대치하고 있다. 그리고 최근 북한은 비대칭 전력 강화에 매진하고 있다. 그들의 비대칭 역량 중에서 사이버 전력의 규모와 수준은 상당한 것으로 파악되고 있다. 이에 우리 안보의 직접적인 위협으로 부상하고 있는 사이버테러에 대한 대응체계 개선은 반드시 필요한 핵심적인 과제이다.

이에 본고에서는 먼저 사이버테러에 대한 일반적인 이론을 고찰하고, 3장에서는 사례국가인 에스토니아와 그루지아, 미국 등에서 사이버테러의 사례와 대응체계를 고찰하고, 이를 토대로 한국에서 2009년 발생한 7·7 디도스(DDoS) 사건과 2013년 발생한 6·25 사이버테러 사건에 대한 사례분석을 통해 우리에 필요한 사이버테러의 함의를 도출하고자 한다. 이를 토대로 4장에서는 사이버테러에 대비한 개선방안을 제안하고자 한다. 따라서 본 논문은 사이버테러에 대한 일반적 이해를 도모하고, 이를 토대로 날로 진화하는 사이버테러에 효과적으로 대응하기 위한 정책적 대안을 모색하며, 사이버테러에 대한 국민과 전문가 그룹에 공감대 형성을 위해 시도하였다.

2. 사이버테러 주요이론 검토

2.1 사이버테러의 개념과 특징

현대 정보화시대의 핵심적인 수단인 컴퓨터체계와 정보통신망에 의한 가상의 공간인 사이버공간에서 발생하는 제반 문제들을 포괄하는 용어로 '사이버전쟁'(cyber-warfare) 혹은 '사이버범죄'(cyber-crime)등의 용어가 일상적으로 사용되고 있다. 사전적으로 '사이버테러'(cyber-terror)와는 그 범위와 수준에서 구분되어야 함에도 불구하고 그 의미가 혼용되어 사용되고 있다. 그러나 위 3가지 용어에는 공통점과 차이점이 존재하고 있으며, 이에 대한 구체적인 의미를 살펴보면 다음 <표 1>과 같다.

<표 1> 사이버 전쟁, 사이버 범죄, 사이버 테러의 분류기준

구 분	사이버전쟁	사이버범죄	사이버테러
행위자	국가	개인/ 단체	
공 간	국제성	무제한성	
시 간	무제한성	무제한성	
대 상	상대국가	개인/민간단체	공공/ 국가 기관
목 적	무차별성	경제성	정치•경제성
수 단	단순성-파괴성	단순성	공격성
피 해	경미-심각	경미	심각

※ 출처 : 조성권, '네트전쟁과 정보기관의 새로운 역할', 2001, p. 3-4.

'사이버전쟁'은 국가와 국가가 사이버 공간상에서 벌이는 일련의 전쟁과정이다. 자국의 특정한 이익을 위해 상대 국가를 대상으로 적대적 행위를 가하는 경우이다. 따라서 사이버 전쟁이 성립하려면 최소한 2개국 이상이 개입되어야 한다. 평상시 정보기관 사이의 사이버전쟁은 사이버 공간을 통해 공격수단이 파괴적이지 않더라도 산업스파이전처럼 그 피해가 클 경우도 있다. 그리고 사이버전쟁은 상개국가와의 물리적 충돌前·中의 과정에서 상대국가의 모든 요소들이 공격대상에 포함되는 무차별성을 추구하게 된다. '사이버범죄'는 개인 혹은 조직화된 단체가 사이버공간에서 시간과 장소에 관계없이 개인과 단체들에 대하여 정치성을 내포하지 않고 경제적 이익과 관련된 행위 혹은 반사회·문화적 행위를 범하는 경우를 의미한다. 그리고 그 행위의 수단, 피해가 단순하고 경미한 결과를 야기하는 특징이 있다.

반면에 '사이버테러'는 행위자, 장소와 시간 등이 '사이버범죄'와 유사하나, 사이버공간에서 해킹의 대상이 국가의 주요 공공기관과, 정부기관을 대상으로 하면서

정치적・경제적 목적을 추구하며, 해킹수단이 공격성을 띠며, 그 물리적 피해가 심각한 경우를 말한다. 그럼에도 불구하고 정치적 테러집단이 비록 공격수단이 단순하고 피해가 경미하더라도 국가의 주요 공공기관과 정부기관을 상대로 정치적 목적을 달성하기 위해 해킹하는 경우는 '사이버테러'로 규정해야 한다. 또한 사이버테러에 대한 개념은 국가와 학자마다 다양하게 규정하고 있는데 이에 대하여 대표적인 경우를 살펴보면 다음과 같다[3]. ① 해킹・바이어스유포・논리폭탄 전송・대량정보전송 및 서비스거부공격・고출력전자총 등 통신망에서 사용하는 컴퓨터시스템 운영 방해 행위 내지 정보통신망 침해행위 또는 전자적 침해행위에 의하여 국가적・사회적으로 공포심 내지 불안감을 조성하는 행위, ② 일반적으로 컴퓨터나 네트워크를 통해서 각국의 국방・치안 등과 관련되는 컴퓨터 시스템에 침입하여 데이터를 파괴하는 등의 수단으로 국가 또는 사회의 중요한 기반을 기능부전에 빠뜨리는 테러행위, ③ 법적으로 승인된 권한 없이 사이버시스템에 대하여 폭력, 파괴 또는 방해를 고의적으로 사용하거나 사용하겠다고 위협하는 행위, 그러한 사용이 사람이나 사람들의 사망이나 상해, 실제적인 재산에 대한 실질적 피해, 사회적인 혼란 또는 중대한 경제적 피해를 가져오는 경우가 수단되는 경우, ④ 컴퓨터와 네트워크를 대상으로 하고 사회적, 이념적, 종교적, 정치적 또는 유사한 목적을 해하거나 이루기 위한 또는 그러한 목적을 위해 사람에게 위협을 가하기 위한 계획된 방해성 행동 또는 위협 등으로 규정하고 있다.

'사이버테러'는 사이버 공간을 배경으로 폭력을 사용하여 적이나 상대편을 위협하거나 공포에 빠뜨리게 하는 행위로써 다음과 같은 특징이 있다[1]. ① 지구촌 어디든지 피해를 가할 수 있는 '탈영토성'의 특성을 들 수 있다. 즉 세계 전체가 하나로 연결된 정보공동체(one click society)이므로 사이버테러가 가능한 공간은 지구촌 어디든지 미칠 수 있다. ② 누가 공격을 했는지를 알 수 없는 '비가시성'을 특징으로 한다. 피해당사자는 가해자가 누구인지를 모르는 상태에서 보유하고 있는 정보를 유출・왜곡・파괴 등의 피해를 입게 된다. ③ 행위주체의 '비정형성'을 들 수 있다. 즉 소수의 숙련된 개인 혹은 집단 등이 장소에 구애를 받지 않고 상대방의 개인에서 집단수준까지 광범위한 피해를 강요할 수 있다. ④ 준비 면에서 '경제성'을 특징으로 한다. 사이버테러를 시행하기 위한 조직, 인력, 자금 등의 방대한 지원이 필요치 않다.

이상과 같이 '사이버테러'는 행위주체・공격대상・목적 면에서 '개인 혹은 단체가 주도하여, 주요 공공기관과 국가기관을 상대로 하며, 정치적・경제적 목적'을 추구한다. 또한 수단 면에서 '해킹, 컴퓨터바이러스 등 정보통신기술을 활용하여 컴퓨터시스템과 네트워크에 대한 공격을 가하는 행위' 이며, 결과 면에서 '국가・사회적인 혼란 등 중대한 피해를 야기하는 행위'라고 할 수 있다. 또한 '사이버테러'는 초국가적인 속성을 가지고 있고, 그 위협이 비가시적이며, 테러의 주체나 조직이 비정형적인 속성을 가지고 있다. 이는 기존의 테러리즘이 영토적인 제약을 가진다는 점, 조직의 형태에 있어서 네트워크적인 속성을 가지지만 테러 수행을 위해서는 일정 수준 이상의 조직체계를 갖추어야 한다는 점, 테러에 대한 위협이 가시적이라는 점과 대비된다.

2.2 사이버테러의 유형

정보통신 기술의 급속한 발전과 함께 사이버테러의 방식도 다양하게 진화하고 있다. 과거 단순한 호기심이나 약간의 금전적 이익을 얻기 위해 시도되었던 단순 해킹으로부터 현재는 정치적 이익을 얻기 위한 악의적인 공격까지 다양한 의도로 활용되어 왔다. 최근에는 사회공학적 해킹(social engineering hacking)이나 스턱스넷(stuxnet) 악성코드에 이르기까지 다양한 사이버테러 유형을 활용하고 있다. 최근까지 알려진 주요 사이버테러 공격 유형들은 다음과 같다.

첫째, 악성 프로그램이다. 인터넷에 연결되어 있던 컴퓨터가 많지 않았던 시절에는 컴퓨터 바이러스 유포의 비중이 높았지만, 이제는 악성 프로그램으로 통합되어 웜, 트로이잔 목마 등을 지칭하는 악성코드 비중이 높아졌다. 이러한 악성 프로그램은 사용자 몰래 자기 자신이나 자신과 유사한 변형을 복사하도록 만들어져 주변기기에 오작동을 초래하거나 파일의 손상시키는 등의 행위를 하는 컴퓨터 프로그램을 지칭한다. 악성 프로그램의 특징은 한번 생성되면 완전한 퇴치가 힘들며, 정보통신망이 확산됨에 따라 확산속도가 더욱 빨라지고 있다.

둘째, 해킹(hacking) 방식이다. 해킹은 개인용 컴퓨

터를 이용하여 타인의 컴퓨터 정보통신망에 불법적으로 침입하여 정보취득, 프로그램 조작, 네트워크 마비 또는 파괴 등의 방식으로 진행된다. 초창기에 발생했던 해킹은 단순 호기심이나 개인적인 성취 욕구 등이 주를 이루었으나, 점점 대상 시스템에 대한 파괴, 대량 정보 유출, 금전적 이득이나 사회혼란 등을 목적으로 하는 방식으로 변질되고 있다.[1] 해킹을 위한 수단으로 스팸메일 유포, 스니핑(sniffing), 스푸핑(spoofing) 기법 등이 있다.[2]

셋째, 분산서비스 거부(디도스) 공격이 있다. 분산서비스 거부 공격은 '서비스 거부'(Denial of Service; DoS) 공격이 진화한 형태이다.[3] 2000년대 들어 이런 DoS 공격방식은 기술발달과 함께 데이터 처리 용량이 급증하여 각 사이트의 트래픽 처리능력이 월등해짐에 따라 무력화되었는데, 디도스 공격은 이에 대비하여 여러pc에 몰래 특정 사이트에 접속을 시도하게끔 하는 명령어를 주입하여(좀비 pc), 좀비 pc로 공격하는 방식하다. 사이버테러 공격자는 많은 pc를 감염시킬수록 디도스 사이버테러 공격의 파괴력을 높일 수 있기 때문에, 공격전에 불특정 다수에게 이메일을 보내 악성코드를 실행하게끔 유도한다. 디도스 첫 피해 사례는 1999년 8월 미국 미네소타 대학 홈페이지에 대한 공격으로 보는 것이 일반적이다. 우리도 지난 2009년 7월에는 청와대를 비롯한 17개 사이트에 대한 디도스 대란(일명, 7·7 대란)이 발생하여 경제적으로 큰 피해를 입었는데 이 당시 사용된 좀비 pc는 약11만 5천여 대로 보고된다[10]. 최근 디도스 공격은 좀비 pc가 아니라 상위에 있는 서버를 이용한 디도스 공격이 발생하고 있으며, 이로 인한 피해는 더욱 확대될 전망이다.

넷째, 사회공학적 해킹(social engineering hacking)을 들 수 있다. 이는 시스템이 아니라 사람의 취약점을 공략하여 원하는 정보를 얻는 공격 방식을 사용한다. 즉 e-메일, 전화·우편물 등을 통해 전산관리자의 정보를 입수하고, 입수한 정보를 활용하여 전산망에 보통의 사용자처럼 자연스럽게 접근하기 때문에 피해자가 해킹을 당한 사실 자체를 인지하지 못하는 경우가 발생할 수 있다.

다섯째, 스턱스넷(stuxnet)이 있다. 스턱스넷은 원자력, 전기, 철강 등 주요 산업기반시설의 제어시스템에 침투하여 시스템을 모니터링하거나 이를 불법적으로 제어할 수 있도록 하여, 관련 시스템을 마비시킬 수 있는 악성코드로 독일 지멘스사의 산업자동화제어시스템을 공격목표로 제작되었다. 세계 최초의 정밀유도 사이버 무기로 평가되는 이 악성 웜바이러스는 이를 개발하였다고 주장하는 주체가 현재까지 밝혀지지 않고 있는 실정이다[12]. 스턱스넷은 악의적 공격자로 하여금 국가주요기반시설의 산업자동화제어시스템을 장악함으로써 시스템의 모터, 펌프 등 주요장비를 제어하거나 심지어 폭발시킬 수도 있도록 하는 강력한 파괴력을 지니고 있어 각국 정부와 보안전문가들이 깊은 우려를 보이고 있다. 이는 지난 2014년 12월에 자칭 '원전반대그룹'이라고 한 세력들이 한국수력원자력을 해킹하여 내부자료를 유출하고 이를 공개한 사태가 발생하면서 스턱스넷 관련 사이버테러가 현실화되고 있다는 우려를 사고 있다. 해킹세력에 의한 시설물 공격으로 한국수력원자력의 시설 가동이 중단된다면 국가적인 차원에서 전력수급에 심대한 문제를 초래할 수 있게 된다. 이러한 사실을 통해 스턱스넷을 앞세운 사이버테러 문제는 가시적인 현실 문제가 되고 있다.

마지막으로, 사이버테러에 의한 인명피해 가능성이다[2]. 2012년 뉴질랜드 출신의 화이트 해커인 버나비 잭(Barnaby Jack)은 인공췌장기의 보안상 결함을 지적하고 해커들이 90여m 거리에서 타인에게 삽입된 인공췌장기를 조작해 혈당량을 인체에 치명적인 수준으로 끌어올릴 수 있음을 증명했다. 이는 아직까지 사이버테러에 의해 직접적인 인명피해가 발생하기 않았지만, 사물인터넷이나 인공장기 등이 보편화될 경우에 사이버테러가 심각하고 폭력적인 범죄가 될 수 있음을 암시한다. 따라서 스턱스넷은 단순하게 경제적 피해를 유발하

---

1) 핵티비즘(hacktivism)을 그 예로 들 수 있음. 해커는 정치적 목적을 달성하기 위해 자신과 다른 성향의 정부, 기업·단체 등의 웹 사이트를 해킹하는 일체의 활동이나 주의를 지칭함.

2) 스니핑(sniffing)은 정보통신망에서 정보를 몰래 가로채는 기술을 의미하며, 스푸핑(spoofing)은 스스로 다른 시스템으로 가장하여, 다른 시스템으로 가야할 정보를 가로채는 기술을 의미함.

3) 서비스 거부 공격이란 시스템의 정상적인 운영을 방해하여 사용자에 대한 서비스의 제공을 거부하게 만드는 공격기술이다. 이는 컴퓨터 통신을 할 때 거쳐야 하는 '신호 송신→수신자응답→송신자 신호전송'의 인증과정에서 상대방의 신호를 받고도 의도적으로 신호전송을 거부하여 컴퓨터 시스템을 계속 신호대기 상태로 묶어놓아 시스템을 무력화시키는 방법임.

는 일반 사이버테러가 아니라 인간의 생명까지 위협할 수 있는 강력한 유형의 사이버테러 방식인 것이다.

이상과 같이 사이버테러의 유형은 단순한 해킹을 시작으로 급기야 인명살상을 할 수 있는 수준으로 진화하고 있다. 또한 해킹과 관련해서도 의도의 경계가 명확하지 않아 특정한 사이버테러가 단순한 목적을 가지고 행한 것인지 혹은 특정한 목적을 가지고 행해진 것인지, 그 경계가 모호한 경우가 많아지고 있다. 그리고 그 피해규모도 폭발적으로 증가되고 있는 실정이다. 지난 2009년 한국에서 발생한 7·7 디도스 대란에 의한 피해액수는 현대경제연구소 추산 363억 원에서 544억 원 수준으로 추산되며, 2013년 3·20 사이버 테러 피해액은 8,823억 원에 이르는 것으로 파악된다[5].

3. 사이버테러 사례와 대응 분석

3.1 NATO의 사례와 대응

3.1.1 에스토니아, 그루지아 사건

에스토니아와 그루지아는 1990년 구소련이 해체되면서 독립한 신생국가로서 나토의 회원국으로 가입하였다. 이후 위 신생국가는 과거 종주국이었던 러시아와 갈등을 겪으면서 사이버테러(공격)을 당하게 된다. 먼저, 에스토니아사건은 2007년 4월 27일 러시아 해커들에 의해 단순한 사이버공격을 받기 시작하였고, 30일에는 좀비 컴퓨터를 활용한 정교한 디도스(DDos) 공격을 당하였다. 당시 에스토니아에서는 구소련 시절에 세워졌던 소련군인의 동상을 철거하는 문제로 러시아계 시민들이 격렬한 시위를 벌이는 중이었고 유혈사태로 발전하였는데, 'E-stonia'로 불릴 정도로 인터넷 강국으로 알려진 에스토니아의 대통령궁, 행정부, 의회, 정당, 언론, 은행 등의 사이트와 전산망이 마비되는 사태가 발생하였다. 에스토니아에 대한 사이버테러는 많게는 8만 5천여 대의 컴퓨터가 동원되었고 3주간에 걸친 유례가 없는 장기간동안 지속되었다. 이러한 사이버테러의 여파로 에스토니아 58개 주요기관의 웹사이트가 마비되었으며, 에스토니아 최대은행은 이틀간에 걸쳐 온라인 서비스가 중단되는 최악의 상황이 초래되었다[12]. 이로 인하여 에스토니아 국민들은 일상생활에 심각한 어려움을 겪었으며 정부와 국가경제의 운영에도 막대한 피해가 발생하였다. 한편 에스토니아는 디도스 공격의 주체를 파악하는데 실패하였다. 러시아 정부가 배후에 있을 것이라는 심증이 있었지만, 당시 크렘린궁의 대변인은 '완벽한 허구'(completely untrue)라고 일축하였다. 또한 IP 주소 역시 변조되어 러시아 정부의 개입을 확증하는 증거를 확보하지 못했다[12].

다음으로, 그루지아 사건은 2008년 8월 러시아와 그루지아 간의 전쟁이 발생하였는데, 이때 사이버공격을 병행하였다. 당시 전쟁은 그루지아 남부지역에서 PKO 활동 중이던 러시아 군인 수십 명이 사망하는 사건에 대한 보복공격으로 러시아는 지상공격을 하기 전에 사이버공격을 한 후 공중폭격을 감행하였다. 당시 러시아는 그루지아 정부기관과, 방송국 등의 웹사이트에 디도스 공격을 한 달 동안이나 지속하였다고 한다[8]. 당시 그루지아는 인터넷 의존도가 높지 않았음에도 불구하고 정부 주요 공공기관·은행·언론 등의 사이트가 마비되어 국민생활과 국가운용에 큰 혼란을 초래하였다.

3.1.2 NATO의 대응조치

에스토니아와 그루지아에서 발생한 사이버테러는 피해당사자만의 노력으로 해결할 수 없는 탈영토적 속성과, 가상공간에서 발생하였음에도 불구하고 무력공격에 준하는 피해를 야기할 수 있음을 보여주는 상징적인 사건이었다. 이에 나토에서는 다음과 같은 조치를 취하는 계기가 되었다. 먼저, 나토차원에서 사이버방호센터를 설치하였고, 사이버 교전규칙을 발간하였다. 위 사이버공격이 계기가 되어 나토에서는 공동의 정보공유와 대처를 위한 '사이버방호센터'(CCDCOE)를 에스토니아의 수도인 탈린에 설치하고, 이후 3년간의 논의를 거쳐 사이버 교전수칙인 '탈린메뉴얼'(Tallinn Manual)을 출간하였다. 이 탈린메뉴얼은 국제사이버안보법(사이버공간에서 주권과 국가책임, 무력사용과 자위권 등)과 사이버무력충돌법(무력충돌, 교전규칙 등)로 구성되어 있어, 전시 사이버공격에 대한 교전규칙을 규정하는 국제적인 기준을 최초로 제시하였다[13]. 다음으로, 나토의 사이버방호센터 주관으로 2013년부터 매년 사이버 안보 컨퍼런스를 주최하고 있다. 이 컨퍼런스를 통해서 관련 정책, 전략, 법, 기술 등 다양한 분야의 연구과 주제발표로 효율적 대응방안을 모색하고 있다.

3.2 미국의 사례와 대응

3.2.1 소니사 해킹 사례

소니사 해킹은 2014년 6월 김정은의 암살 장면이 포함된 '인터뷰'라는 영화의 예고편을 공개하면서 발단이 되었다. 이에 북한 외무성과 유엔주재 북한대사는 위 '인터뷰'가 그들의 최고지도자를 모욕하였다고 주장하면서 영화 상영을 취소하라고 반발하였다. 이후 '평화의 수호자'(GOP)라는 정체불명의 해커가 2014년 11월 24일 소니사의 컴퓨터 시스템을 해킹해 내부 자료를 삭제하고, 유명배우 등 약 4만7천여 명의 개인정보를 유출시킨 사건이 발생하였다. 이어서 3일후에는 미개봉 영화를 포함한 불록버스터급 영화들이 온라인 사이트에 불법적으로 유포되어 100만 건 이상의 다운로드가 되었으며, 12월 5일부터는 위 GOP 해커로부터 소니사 직원들은 위 '인터뷰'상영을 중지하지 않으면 본인과 가족이 위협에 빠질 것이라는 협박성 이메일을 받았다. 결국 같은 해 12월 17일에 소니사는 이에 굴복하여 영화상영 중단을 발표하게 되었다.

그러나 미국정부는 소니사 해킹사건이 국가기반시설이 아닌 민간 기업이었음에도 불구하고, 헌법이 보장하는 표현의 자유를 침해하였고, 소니사 직원에 대한 물리적 테러를 위협했다는 이유로 연방수사국을 전격적으로 투입하여 조사에 착수하였다. 미국 연방수사국의 사이버테러 조사결과 북한의 소행임을 밝혀내고, 다양한 제제조치를 정부차원에서 부과하였음은 물론 위 '인터뷰'영화를 개봉하였다.[4)]

3.2.2 미국의 대응조치

불법해커(GOP)의 협박에 굴복하여 위 '인터뷰' 상영을 중단하겠다는 소니사의 발표에도 불구하고, 미국정부는 연방수사국을 전격적으로 투입하여 불과 이틀 후인 12월 19일 소니사 해킹사건의 배후로 북한을 지목했다. 이에 북한은 다음날인 12월 20일 소니사 사이버테러 사실을 부인하면서 미국에 대하여 공조수사를 제안하였으나, 미국은 이를 거부하면서 해커가 사용한 서버의 소재국인 중국에 수사협조를 요청하였다.[5)]

한편 미국의 오바마 대통령은 북한의 소니사 해킹사건에 대하여 '비례적으로 대응할 것이며, 가용한 대응수단으로 사이버 보복공격, 고강도 금융제재, 테러지원국 재지정과, 한국에 배치된 군사력 증강 등을 다양한 대응방안을 검토할 것'이라고 발표하였다[9]. 미국 대통령의 이러한 발표이후 북한 주요기관의 홈페이지가 다운되는 사건이 발생하였으며, 대북경제제재 행정명령(13687호)·고강도 금융제재 행정명령 발령 등 다양한 조치를 하였다.[6)]

이상과 같이 미국은 개별기업에 대한 사이버테러임에도 불구하고, 그 피해의 심각성을 고려하여 다양한 테러에 대비하기위한 확고한 법적인 기반 하에(애국법, 국토안보법, 연방정보보안관리법 등), 정부와 민간이 통합된 포괄적인 대응조치를 통해 사이버테러 위험으로부터 안전을 확보하고 있다.

3.3 한국의 사례와 대응

3.3.1 7·7 디도스/ 6·25 사이버테러 사건

먼저, 7·7 디도스(DDoS) 사이버테러 사건은 2009년 7월 7일부터 61개국 435대의 서버를 활용하여 한국과 미국의 주요기관 35개 웹사이트를 디도스 공격하여 피해를 입힌 사건이다. 이 공격은 이후 3일간이나 지속되었으며 공격이 종료됨과 동시에 감염된 pc를 파괴함으로써 종료되었다. 당시 디도스 공격은 국내 22개, 미국 13개의 정부·민간기관이 운용하는 웹사이트를 대상으로 이루어 졌으며, 국내의 경우 6개 정부기관과 16개의 민간기관의 홈페이지의 서비스가 마비되었다. 민간기관은 금융, 포털, 언론 등 각 분야의 대표적인 업체들의 웹사이트를 공격대상으로 하였다. 디도스 공격으로 인하여 해당기관에 접속장애 뿐만이 아니라 기업의

4) 미국 연방수사국은 ① 소니사 해킹사건에 사용된 악성코드가 한국에서 발생한 3·20(2013년, 방송·금융망 사이버테러)사건, 6·25(2013년, 69개 주요 정부기관·민간업체 사이버테러)사건 당시 사용된 악성코드와 유사한 점, ② 해킹에 사용된 악성코드와 북한 관련 IP가 교신한 점 등을 증거로 북한의 소행이라고 판단함.

5) 미국의 중국에 대한 수사협조에 대하여, 중국 외교부는 정례브리핑을 통해서 '미국과 북한 양자간의 해결을 강조하며' 원칙적인 입장만 고수함.

6) 미국이 북한의 소니사 해킹에 대한 주요 제재조치인, '대북경제제재 행정명령'은 해킹사건과 관련되는 것으로 추정되는 북한의 3개 단체와 개인 10명에 대한 제재를 명시하였고, '금융제재 행정명령'은 사이버테러를 시도한 개인 또는 단체의 금융거래에 대한 자산동결과 은행거래 정지 등을 포함하고 있음.

영업 손실, 국민 불편 초래와, 국가안보차원의 심각한 우려 증대 등 2차적인 피해를 초래하였다. 7·7 디도스 사이버테러로 인해 1,500여대의 컴퓨터가 악성코드에 감염되었으며, 10만대 이상의 좀비 pc가 공격에 동원된 것으로 추정되며, 이로 인한 피해액은 최소 350여억 원에서 최대 540여억 원 수준으로 추산되었다[4].

다음으로, 6·25 사이버테러 사건은 2013년 6월 25일부터 7월 1일까지 4회에 걸쳐 국내의 정부·언론·민간업체 등의 69개소의 서버가 공격을 받은 사건이다. 위 6·25 사이버테러 사건으로 주요기관의 홈페이지가 변조되었으며, 하드디스크 삭제, 디도스 공격과, 정부·민간기관의 294여만 명의 개인정보가 유출되었다.

3.3.2 우리의 대응조치

2009년 7·7 디도스(DDoS) 사건이 발생하자 우리 정부와 민간부분에서는 각자 독자적으로 사후조치를 강구하였다. 즉 정부차원에서는 행정자치부·방송통신위원회·금융감독원 등이 주체가 되어 소관부서에 대한 피해파악과 복구를 하였으며, 민간차원에서는 정보보안업체가 주축이 되어 백신프로그램을 무료 배포하여 피해복구에 주력하였다. 한편 국가정보원은 위 디도스 공격에 동원된 인터넷 IP주소가 북한 체신청이 사용해 온 IP이었다는 사실을 확인하였으며, 당시 한미 주요기관에 대한 사이버테러 공격 경로 추적을 통해 평양에 소재한 북한 해커조직들이 중국에서 동시 공격하여 우리 군의 인터넷망이 북한 해커부대 통제 하에 24시간 동안 무방비상태로 뚫려 국가기밀이 유출된 사실을 확인시켜 주었다[6].

이후 2013년에 발생한 6·25 사이버테러에 대하여 이전의 정부와 민간이 분리되어 사후조치 위주가 아니라, 사이버테러 발생 가능성을 사전에 예측하고 정부와 민간이 공조하여 이에 대응함으로써 그 피해를 최소화 할 수 있었다. 정부에서는 청와대에 컨트롤타워를 구축하고, 방송사 등을 포함한 주요기반시설을 망라하여 정보통신기반시설로 지정하고 담당책임자 임명, 보호조치 계획 수립·시행·복구 등에 관한 종합대책을 수립하고 시행함으로써 그 피해를 최소화 할 수 있었다. 한편 위 6·25 사이버테러에 사용된 인터넷 IP주소 등을 확인한 결과 북한의 소행으로 추정하였다.

북한은 과거 주로 바이러스 감염을 통해 해킹을 시도하였다. 그런데 2009년부터 북한은 단순한 바이러스를 통한 해킹이 아니라 대규모 서비스 거부 공격을 통해 전산망을 마비시키는 디도스 방식으로 진화하였다. 7·7 디도스 사건에 사용된 악성코드는 공격명령을 하달하는 숙주서버에 일정 주기로 접속하여 공격대상과 공격시간을 최신화하여 정해진 시간에 공격을 함으로써 감염 경로를 추적할 만한 증거를 제거하는 진화된 형태의 공격방식을 사용하였다. 그리고 그 이후인 2013년에 발생한 3·20 사이버테러 사건에서 북한은 디도스 공격에서 더욱 발전된 '사회공학적 해킹'(social engineering hacking) 방식으로 발전하였다. 위 사회공학적 해킹방식은 시스템이 아니라 사람의 취약점을 이용하여 원하는 정보를 얻는 방식이다. 즉 과거 해킹은 해커가 해킹도구를 이용하여 공격 대상이 되는 기관의 전산망에 침투하였으나, 이메일이나 전화·우편물 등을 통해 전산망 관리자의 정보를 도용하여 전산망에 침투하기 때문에 피해자가 해킹당한 사실조차도 인지하지 못하도록하는 방식으로 진화하였다. 그리고 2014년 12월부터 다음해 초까지 발생한 한수원 해킹 사건도 직장 내부의 임직원 이메일 계정을 도용한 사회공학적 해킹을 사용하였다. 당시 정체불명의 해커들은 이메일을 통해 악성코드에 감염된 한수원 임직원 pc를 공격하여 원전 관련 도면과 한수원의 임직원의 개인정보를 유출시키는 사건이 연이어 발생하는 등 해킹의 방식이 획기적으로 진화하고 있는 실정이다.

3.4 사이버테러의 진화와 함의

정보화 사회의 발달은 인간생활을 획기적으로 향상시키고 있다. 그럼에도 불구하고 에스토니아, 미국 등의 사이버테러 사례에서 살펴보았듯이 새로운 유형의 위협이 인간의 생활과 국가의 안전을 심각하게 위협하고 있다. 가상공간에서 발생하는 사이버테러는 행위주체의 비가시성, 공격대상의 비정형성과, 피해 과정과 범위의 탈영토성 등으로 인하여 그 피해규모와 영향은 엄청난 파장을 야기하고 있다. 즉 사이버테러는 해킹의 주범을 식별하는데 상당한 노력과 시간이 필요하며, 개인수준을 넘어서 국가 혹은 정부의 주요기관을 해킹함으로써 국가기능의 마비를 초래하고 있으며, 피해당사국가 외부에 소재한 전산망을 활용하여 해킹이 발생하며, 해킹의 흔적을 남기지 않는 등 창과 방패의 대결처

럼 더욱 교모하게 진화하고 있다.

해킹방식이 날로 진화하며 그 피해규모가 엄청난 수준으로 증가하고 있는 사이버테러에 대응하기 위해서는 단순히 사후에 대응수준이 아니라, 사태 발생前(정책수립과 예방 대책)과 사태 발생中·後(대응과 복구단계) 등의 全 과정에 대하여 관련기관의 역할과 기능이 통합되도록 해야 한다. 그런데 우리의 사이버테러에 대비한 대응체계는 대통령훈령 수준인 '국가사이버안전관리규정'을 근거로 국가의 모든 기관을 포함하는 것이 아니라 행정기관에 대한 역할과 의무만으로 한정되어 있는 실정이다. 위 '국가사이버안전관리규정'(대통령훈령 제267호)에 의거하여 국가·공공분야는 국정원이 담당을 하며, 민간분야는 미래창조과학부(한국인터넷진흥원)이 주관하고, 군사 분야는 사이버사령부와 기무사령부가 담당하는 등 분권화된 체계로 관련 정책을 준비하고 시행하게 되어있다.

반면에 미국의 소니사 해킹사건에 대한 사례분석에서 살펴보았듯이, 미국은 민간 기업에 대한 해킹임에도 사이버테러에 대한 통합된 법령체계 하에서 신속한 원인파악·해킹세력 식별과 병행하여 포괄적인 비례적 대응조치(자위권 행사) 등이 종합적으로 이루어져 사이버테러에 대한 엄정한 조치는 물론 향후 예상되는 테러에 대한 사전예방까지도 가능하도록 하고 있다.

이상과 같이 날로 진화하는 사이버테러의 방식과 피해규모를 고려하여, 이를 사전에 예방하고 대응하기 위해서는 국가적 차원의 통합된 컨트롤타워 기능을 유지하고 통합된 조치가 시행되도록 법적·제도적 장치가 시급하게 보완되어야 한다.

4. 사이버테러 대응 개선방안

최근 정보통신기술의 발달로 스마트폰, 태플릿 PC와, 다양한 형태와 기능의 USB, 사물인터넷 등 첨단 IT기술이 접목된 최첨단 장비가 다기능·초소형화·보편화됨에 따라 사이버테러에 대한 취약요소가 더욱 증대되고 있는 실정이다. 특히나 사이버테러에 대한 대응은 행위주체의 비가시성, 공격대상의 비정형성과, 피해과정과 범위의 탈영토성 등의 특징을 고려하여 국가 최상위차원에서 리더십 발휘가 가능하도록 컨트롤타워의 역할과 기능이 강화 되야 하며, 해킹수준의 발달을 고려하여 국가적 차원의 통합된 정보공유분석센터가 설치되어 운용되어야 한다. 이를 위한 법적·제도적 장치를 살펴보면 다음과 같다.

첫째, 분산되어있는 사이버테러 대응관련체계를 단일법령을 근거로 일원화하여 국가적 차원의 컨트롤타워를 명시화해야 한다. 현재 사이버테러 관련 법령은 정보통신기반보호법과 정보통신망이용촉진 및 정보보호 등에 관한 법률 등이 존재하고 있지만 각 법률의 적용대상과 목적을 달리하고 있기 때문에 이를 총괄할 수 있는 법령으로 단일화가 필요하다. 현재 우리의 국가사이버 위기관리 체계를 보면 법령이 아니라 대통령 훈령인 '국가사이버안전관리규정'을 근거로 대통령 직속으로 인터넷침해대응센터를 운용하고 있어 사전조치부터 피해복구단계까지 일원화된 정책수립과 시행이 제한되는 실정이다. 즉 사이버테러에 대하여 민간분야는 미래창조과학부(한국인터넷진흥원)가 담당하고, 공공·군사분야는 국가정보원과 국방부가 소관부서를 담당하게 되어있다. 그런데 사이버테러는 인터넷망이 연결되어 있는 경로를 따라 발생가능하기 때문에(공격대상의 비정형성), 통합된 리더십 발휘가 가능한 컨트롤타워의 존재가 필수적이다. 따라서 국가적 차원에서 임무수행이 가능하도록 기존의 '국가사이버안전관리규정' 수준이 아니라, '국가사이버안전관리법령(가칭)'으로 법제화하였을 때 현재의 컨트롤타워인 국가정보원은 공공분야만이 아니라 군사분야와 민간분야 등 국가의 인터넷망과 연결된 모든 기관을 통합하여 예방대책 수립부터 사후조치 단계까지 통합된 대응이 가능하다.

둘째, 날로 발전하는 해킹 방법·기술에 탄력적인 대응이 가능하도록 통합된 국가적 차원에서 정보공유분석센터를 설치하고 운용해야 한다. 현재 우리나라의 사이버 안보 대응기관으로 국가정보원의 국가사이버안전센터, 국방부의 국방정보전대응센터, 미래창조과학부의 인터넷침해사고대응지원센터, 대검찰청의 인터넷범죄수사센터, 경찰청의 사이버테러대응센터 등 다양한 대응센터가 유지되고 있다. 문제는 다양한 기관이 존재하고 있음에도 불구하고 실제로 사이버 위협과 테러가 발생했을 경우 각 기관의 책임과 역할이 불분명하고 강력한 리더십발휘가 법적으로 보장된 총괄전담기관이 없다는 점이다. 따라서 점증하고 있는 신종 기법의 해킹 방법과 기술에 관한 정보를 대내·외로부터 입수하

고 이를 최단 시간 내에 하부조직에 전파함으로써 사이버테러에 대한 대응역량을 보장할 수 있는 정보유통체계가 보다 적극적으로 개선 돼야 한다. 또한 국가적인 차원의 정보유통센터가 효율적으로 운용되기 위해서는 관련 전문 인력을 양성하며 센터운용의 효율성을 보장할 수 있도록 정책적인 노력이 병행되어야 한다.

마지막으로, 사이버테러의 탈영토성을 극복할 수 있도록 국제교류와 공조수사가 활성화돼야 한다[7]. 우리는 아시아태평양 경제협력체(APEC)과 국제전기통신연합(ITU) 등 국제기구의 회원국으로서 국제사이버안전을 위한 정보교류와 협력에 노력하고 있으며, 국제사고긴급대응팀(CERT)의 회원국으로 협력체계를 유지하고 있으나 우리나라의 발전된 ITC 수준을 고려할 때 국제적인 협력이 매우 미흡한 실이다. 유럽연합과 미국 등은 정례 사이버 사고 대응훈련을 정례적으로 시행하고 있으나 우리는 회원국가 연합한 사이버테러 대응 훈련 등 국제공조가 미흡한 실적이다. 또한 최근 발생하고 있는 해킹사건의 상당 부분이 해외에서 침입해온 것으로 파악되고 있다. 해외로부터 공격하는 해킹사건은 수사가 어려운 실정으로 예방이 최선의 방안이라 할 수 있다. 따라서 우리는 IT강국의 위상에 걸맞게 다양한 사이버관련 국제기구와 조약에 적극적으로 참여하고 활동함으로써 역할과 기능을 강화하고 인적교류를 강화해야 한다.

5. 결 론

사이버공격의 유형은 행위자, 공격 대상, 공격 목적 등에 따라서 사이버전쟁, 사이버테러와, 사이버 범죄 등으로 구분할 수 있다. 본고에서는 사이버테러를 중심으로 살펴보고자 한다. 사이버테러는 행위주체・공격대상・목적 면에서 '개인 혹은 단체가 주도하여, 주요 공공기관과 국가기관을 상대로 하며, 정치적・경제적 목적'을 추구한다. 또한 수단 면에서 '해킹, 컴퓨터바이러스 등 정보통신기술을 활용하여 컴퓨터시스템과 네트워크에 대한 공격을 가하는 행위' 이며, 결과 면에서 '국가・사회적인 혼란 등 중대한 피해를 야기하는 행위'라고 할 수 있다. 또한 '사이버테러'는 초국가적인 속성을 가지고 있고, 그 위협이 비가시적이며, 테러의 주체나 조직이 비정형적인 속성을 가지고 있다. 사이버테러의 유형은 단순한 해킹 수준이었던 것이 인명을 살상할 수 있는 수준으로 진화하고 있으며, 해킹과 관련해서도 의도의 경계가 명확하지 않아 특정한 사이버테러가 단순한 목적을 가지고 행한 것인지 혹은 특정한 목적을 가지고 행해진 것인지, 그 경계가 모호한 경우가 많아지고 있다. 그리고 그 피해규모도 폭발적으로 증가되고 있는 실정이다.

사이버테러의 사례에서 살펴본바와 같이, 해킹의 주범을 식별하는데 상당한 노력과 시간이 필요하며, 개인 수준을 넘어서 국가 혹은 정부의 주요기관을 해킹함으로써 국가기능의 마비를 초래하고 있으며, 피해당사국가 외부에 소재한 전산망을 활용하여 해킹이 발생하며, 해킹의 흔적을 남기지 않는 등 창과 방패의 대결처럼 더욱 교모하게 진화하고 있다. 특히나 북한의 사이버테러의 수준과 규모는 상당한 것으로 파악되고 있다.

북한과 주변국가로부터 발생하는 사이버테러에 대응하기 위해서는, 이를 사전에 예방하고 대응하기 위해서는 국가적 차원의 통합된 컨트롤타워 기능을 유지하고 통합된 조치가 시행되도록 법적・제도적 장치가 시급하게 보완되어야 한다. 이를 통해 사이버테러에 대한 국가적 차원의 컨트롤타워의 역할과 기능이 강화되어야 하며, 해킹의 기술수준을 압도할 수 있도록 관련 정보를 수집・분석・전파 할 수 있는 센터를 설치・운용하여 사전예방부터 사후조치 전 단계에 민간-공공기관이 통합된 조치가 가능하도록 보강되어야 한다. 또한 사이버테러의 탈영토성을 고려하여 관련 국제기구와 조약에 적극참여 하여 국제수사 공조체제를 강화하여 총체적인 대비능력 강화에 정책적 노력을 경주해야 한다.

참고문헌

[1] 권태영, "21세기 군사혁신과 미래전," 법문사, 2008, p. 224-225. 재정리

[2] 김배중, 2015. "사이버테러의 국제정치," 연세대학교 석사논문, pp. 27-28.

[3] 김흥석, 2010, "사이버 테러와 국가안보", 『저스티스』 121, p. 323-324.

[4] 디지털타임스, (2010. 7. 5자)
[5] 매일경제, 2013년 12월 24일자.
[6] 송봉선, “실패한 대남전략”, 북한문제연구소, 2009, pp. 51-52.
[7] 이완수, “국가사이버안보 구축전략에 관한 연구”, 경기대학교 박사논문, pp. 108-110.
[8] 오일석, 2014, “보안기관의 사이버보안활동 강화에 대한 법적고찰”, 과학기술법연구, 20(3), pp. 41-56.
[9] 연합뉴스, (2014. 12. 20)
[10] 조선비즈, 2011년 3월 4일.
[11] 장노순, 2005. “초국가적 행위자의 사이버공격과 핵공격에 관한 비교연구,” 『한국정치학회보』 39(5), pp. 263-281.
[12] 장노순, “사이버 무기와 국제안보”, 『JPI 정책포럼』 제13호, 2012, pp. 2. 11) 장노순, “사이버 무기와 국제안보”, 『JPI 정책포럼』 제13호, 2012, pp. 6.
[13] Schmitt, N. N., Tallinn manual on the International Law application to cyber warfare, Cambridge Press, 2013.

[저 자 소 개]

김 연 준 (Kim-Yeon Jun)

1983년 3월 문학사
1996년 11월 국방관리전공 석사
2012년 8월 경호학 박사
현재, 용인대학교 군사학과 교수

email : kyj23509@naver.com

김 상 진 (Kim-Sang Jin)

2001년 2월 용인대 경호학과 체육학사
2003년 2월 용인대 경호학과 경호학석사
2000년 2월 경기대 경호안전학과
경호안전학박사
현재, 용인대학교 학점은행제 경호비서전공(항공보안) 교수

email : ksj8004@naver.com