韓國컴퓨터情報學會 論文誌
第14卷 第6號, 2009. 6.

2009-14-6-5-4

사이버범죄에 대한 국가적 대응체계 구축의 이론적 함의 -사이버테러형 범죄를 중심으로-

김 영 환*

Theoretical Implication on Establishing the National Countermeasure System against Cyber Crime - Focusing on a Pattern of Cyber Terror -

Kim, Young Hwan*

요 약

20세기 후반부터 비약적으로 발전하기 시작한 정보통신기술과 이를 기반으로 한 인터넷의 세계적인 확산은 21세기의 새로운 정보사회로의 전환에 즈음하면서, 많은 역기능이 나타나기 시작했는데 그 중의 하나가 사이버범죄로서 사이버테러리즘이다. 사이버테러리즘은 자국 내 뿐만 아니라 국가안보적인 차원에서 심각성의 문제가 대두되고 있다. 이에 이 연구는 사이버테러리즘의 현황을 살펴보고 이에 따른 향후 전망을 하고, 사이버테러리즘 문제에 대응하고 있는 각국의 대응체계를 현실적으로 비교하였다. 이를 통하여 우리나라에서의 범국가적인 적극적 대응전략의 모색에 의한 효율적인 사이버테러리즘의 국가적 대응전략 방안을 모색하였다.

Abstract

From the late 20th century, rapidly progressing information communication technology and spreading Internet all over the world cause many reverse functions when there is a conversion into the new information society. One of them is cyber terrorism as cyber crime. Cyber terrorism gradually has had a serious problem in the national security as well as the domestic aspects. Therefore, this study looked into the present condition of cyber terrorism, discussed its prospect, and sought the efficient national countermeasure methods against cyber terrorism by comparing other countries' countermeasure systems currently.

▸ Keyword : 사이버범죄(Cyber Crime), 사이버테러(Cyber Terror), 정보보호시스템(Information Security System), 사이버공격(Cyberattack), 국제협력(International Cooperation)

• 제1저자 : 김영환
• 투고일 : 2009. 06. 14, 심사일 : 2009. 06. 14, 게재확정일 : 2009. 06. 26.
* 조선대학교 경찰행정학과 교수
※ 본 연구는 2008학년도 조선대학교 교내학술연구비 지원에 의해 연구되었음.

Ⅰ. 서 론

현대사회에 있어 네트워크를 통한 사이버공간의 확대와 컴퓨터 기술의 고도화, 지능화 등은 갈수록 그 사회적 영향력이 높아지고 있다. 이러한 고도 정보화 사회는 우리에게 많은 혜택을 주고 있음은 부인하지 못 할 사실이지만, 이에 못지않게 사이버범죄라는 부작용도 초래되고 있다. 이러한 경향은 향후에 더욱더 다양해지고 첨단화 될 것으로 예측되며, 더욱이 과학기술의 발전 양상에 비례하여 증가되리라 추정되고 있다.

현재 사이버범죄는 그 역기능에 따른 사회적 파장이 국가를 위태롭게 할 수도 있다는 점에서 매우 심각한 상황이지만, 그 광범위한 피해성과 기하급수적 발생률, 발생형태의 다양성 등으로 인하여 현실적인 대책마련이 힘들다는 것이 큰 문제점으로 지적되고 있다. 나아가 인터넷을 통한 사이버 공간상의 국가 간 접속이 용이해짐에 따라, 이로 인한 부정적 결과로서 국경을 초월하는 사이버범죄가 지속적으로 증가하고 있으며, 그 피해 지역 또한 국가의 벽을 넘고 있다. 예를 들어 물리적 국경을 초월하여 우리나라에 있는 정보시스템을 해킹하거나, 우리나라를 경유하여 다른 나라의 정보시스템을 해킹하는 경우, 고의로 컴퓨터를 비롯한 정보시스템의 작동을 방해하거나 운영을 못하게 하는 경우, 그 파급효과가 특정 프로그램을 사용하는 전 세계 모든 사용자에게 영향을 끼치는 컴퓨터 바이러스 등 국가의 영토적 한계에 구애받지 않고 피해를 주고 있다.[1]

즉 전 세계가 컴퓨터에 의해 상호 네트워크화 되고 또한 그에 심각히 의존되는 상황에서 발생할 가능성이 높은 사이버범죄에 노출되어 있는 것이다. 특히 사이버범죄의 한 유형으로써 사이버테러는 21세기 뉴테러리즘의 시대적 상황에 발맞춰 전통적 테러리즘에 극적인 변화를 주었고 또한 21세기 테러리즘의 새로운 모습으로 나타나고 있다.[2]

이에 전 세계 국가들은 사이버테러에 대비하기 위한 모든 조치들을 강구하고 있으며, 우리나라도 대응태세 구축을 위해 노력하고 있다. 그러나 정보기술의 발전 속도는 법과 제도가 따라가기에 너무 빠른 속도이므로, 대응체계의 낮은 탄력성은 곧바로 위협의 증대로 나타난다. 따라서 장기적인 관점에서 계속적으로 진화하는 기술과 이에 맞서 사이버테러의 대비에 적극적으로 참여함으로써, 위협을 예상하고 그에 맞춘 보호조치가 지속적으로 이루어져야 한다.[3]

이에 따라 이 연구는 사이버범죄로서의 사이버테러리즘과 관련하여 그 현황을 살펴보고 이에 따른 전망을 하였다. 그리고 현실적으로 사이버테러리즘 문제에 대응하고 있는 각국의 대응체계를 비교하고 이를 통하여 우리나라에서의 효율적인 사이버테러리즘의 대응전략 방안을 모색하는데 연구의 목적을 두었다.

Ⅱ. 이론적 배경

2.1. 사이버범죄의 의의

2.1.1. 사이버범죄의 개념

사이버범죄는 사이버공간에서 나타나는 제반 법·규범 위반행위라고 포괄적으로 말할 수 있지만 아직 명확하게 정의된 바는 없다.[4] 사이버범죄와 인터넷범죄의 용어사이에도 약간의 차이가 있을 수 있다. 사이버범죄가 인공적·가상적인 공간을 무대로 일어나는 행위라고 한다면, 인터넷범죄는 인터넷이라는 네트워크에 관련된 행위만을 의미한다고 볼 수 있기 때문이다. 하지만 사이버세계를 대표하는 연결망이 인터넷이라고 부를 수 있다는 점을 고려할 때 사이버범죄와 인터넷범죄는 같은 의미로 사용할 수 있다.[5] 사이버범죄는 국가를 초월하는 초국가적 특성을 띤다는 점에서 국가 간에도 적용될 수 있는 보다 포괄적이고 일반적인 의미로서의 정의가 필요하다. 따라서 사이버범죄는 컴퓨터나 IT기기가 범행대상이 되거나 혹은 그것이 도구로 이용되어 이루어지는 비합법적인 행위로 정의 되는 것이 일반적이며, 보다 포괄적으로는 기존의 컴퓨터 범죄를 포함하여 인터넷 및 사이버공간에서 행해지는 모든 유형의 범죄를 일컫는 것으로 정의된다.[6]

2.1.2. 사이버범죄의 유형

기존의 컴퓨터범죄로부터 그 논의의 무게중심이 사이버공간을 이용한 범죄들로 이동하면서, 사이버범죄에 대한 유형은 다양하게 제시되고 있다.[7]

표 1. 사이버범죄의 유형
Table 1. Types of Cyber Crime

학 자	사이버범죄의 유형
최영호 (1998)	컴퓨터해킹, 암호해독, 도청, 컴퓨터바이러스, 폰프리킹(phone phreaking)
양근원 (1999)	사이버스토킹, 사이버명예훼손, 통신사기, 음란·불법물 배포, 해킹, 바이러스유포, 음란사이트운영
조병인 외 (2000)	해킹과 관련-사이버테러나 개인정보유출/사이버성폭력, 언어폭력
김종섭 (2000)	사이버성폭력이나 스토킹, 사이버명예훼손, 전자상거래사기, 사이버도박, 해킹, 바이러스유포
원혜욱 (2000) 조두영 (1998)	인터넷도박, 인터넷몰에서의 사기판매행위, 인터넷을 통한 명예훼손, 저작권침해 및 사이버스토킹, 음란물의 판매·전시행위, 각종 위조·변조행위, 사이버테러, 아이디와 패스워드의 공개행위, 무차별적인 광고메일의 송신, 다른 사이트나 홈페이지의 무단복사행위
경찰청	사이버테러형 범죄-해킹, 일반사이버범죄-사기, 불법복제, 불법·유해사이트, 명예훼손, 개인정보침해, 사이버스토킹, 사이버성폭력, 협박·공갈

위의 〈표 1〉의 사이버범죄의 유형 중 경찰청 사이버테러대응센터[8]에서는 해킹, 바이러스 유포와 같이 고도의 기술적인 요소가 포함되어 정보통신망 자체에 대한 공격행위를 통해 이루어지는 범죄를 사이버테러형 범죄로 규정하고 있는데 이 연구에서의 연구대상도 사이버범죄 유형 중 사이버테러형 범죄로 한정하여 논의를 진행하고자 한다.

2.2. 사이버테러리즘의 의의

2.2.1.사이버테러리즘의 개념

테러리즘이라고 하면 복면의 사나이들, 폭탄, 자동소총, 인질 등을 연상하게 되나, 지금은 수천만대의 컴퓨터가 네트워크로 연결된 정보의 시대로, 테러리즘의 수단과 대상은 비트(Bit)로 운영되는 사이버 세계에서 이루어지고 있다. 수많은 컴퓨터를 연결하여 손쉽게 파일과 의사를 전달할 수 있는 수단인 인터넷은 목적을 가진 사람들에 의해 악용되면 무시무시한 전장으로 둔갑한다. 목적을 가진 사람들은 다름 아닌 사이버 테러리스트이다.[9]

이러한 사이버 테러리스트에 의해 저질러지는 사이버테러리즘에 대한 일반적인 개념은 "정보화시대의 산물로, 컴퓨터망을 이용하여 데이터베이스화되어 있는 군사·행정·인적자원 등 국가적인 주요 정보를 파괴하는 것을 말한다. 한편 사이버테러라는 용어는 그 대상이 개인인가 국가인가 불문하고 사이버 공간을 이용한 모든 공격행위 차체를 광의적인 개념으로 사용하는 경우도 있으며, 이러한 입장에서는 인터넷 사기, 사이버음란, 사이버폭력, 사이버 비밀침해 행위 등도 모두 사이버테러의 개념 속에 포함시키고 있다.[10]

2.2.2.사이버테러리즘의 유형과 특성

정보전이라고도 불리는 사이버테러리즘의 유형은 크게 3가지 유형으로 분류할 수 있다. 첫째, 단순히 개인적으로 활동하는 해커들에 의해 자행되는 것이고, 둘째, 네덜란드의 트라이던트 그리고 러시아의 지하 해킹마피아 등과 같이 범죄조직화된 집단에 의한 것이다. 셋째, 정치적·민족적·종교적인 목적을 달성하기 위해 조직된 단체나 혹은 주권국가에 의해 행해지는 것이다.[11]

이러한 유형을 반영한 사이버테러리즘의 특성을 살펴보면, 사이버테러는 보이지 않는 사이버 공간에서 해킹과 바이러스와 같은 수단으로 목적하는 대상의 정보시스템에 영향을 주어 목적하는 결과를 기대한다는 점에서 기존 사이버범죄와는 다른 여러 가지 새로운 특성을 갖고 있다.[12]

첫째, 전쟁과 테러 수행비용이 저렴하면서도 막대한 피해를 준다. 사이버테러(정보전)를 수행하는 데는 많은 비용이나 국가적 지원이 없어도 정보체계에 대한 전문지식만으로 사이버테러(정보전) 기술과 무기를 연구 개발할 수 있고, 네트워크를 통해 접근할 수만 있으면 개발된 정보전 무기를 사용하여 공격할 수 있다. 또한 정보체계들은 상호 의존성이 높기 때문에 어느 하나의 정보체계의 마비는 전체적으로 막대한 피해를 입게 된다.

둘째, 범행의 광역화와 익명성의 특징이다. 공격대상에 접근해야 될 필요가 없이 통신망이 연결된 곳이면 어디서나 공격이 가능하고, 증거 인멸이 쉬워 공격자와 공격 장소의 추적이 어렵다.

셋째, 사건예측의 불가능성이다. 은밀한 공간에서 컴퓨터 조작만으로 공격이 가능하고, 신속한 공격이 가능하여 공격받은 전산망이나 기간시설이 완전 무력화되거나 정보유출·조작 등이 이루어진 후에야 공격받은 사실을 감지할 수 있다.

넷째, 전통적인 전쟁과 범죄의 경계가 불분명하다. 사이버테러(정보전)는 위협과 공격행위의 근원지 파악이 어려워지며, 자국의 정보체계가 공격당하고 있을 때 그것이 범죄행위에 의한 것인지, 전쟁행위에 의한 것인지 구분하기 어렵다.

다섯째, 전후방과 전선의 구분이 따로 없다는 특징이 있다. 사이버테러(정보전)에서의 정보기술은 시간적·공간적 차이를 무의미하게 하므로 기존 전쟁과는 다르게 후방도 공격 대상이 된다. 국가의 모든 기반구조는 상호 연결되어 있고, 정보전 공격은 이들이 연결되어 있는 사이버 공간에서 수행되기 때문에 전방과 후방의 구분이 무의미해지고 네트워크를 통해 접근할 수 있는 곳이면 어디든지 잠재적인 전방이 될 수 있다.

III. 사이버 테러리즘의 현황과 전망

3.1. 사이버테러형 범죄발생현황

최근의 국가·공공부문과 민간부문의 사이버침해사고 발생현황(최근 5년 기준)과 사이버테러형 범죄발생 건수에 대하여 개괄적으로 살펴보면 〈표 2〉, 〈표 3〉과 같다.[13]

표 2. 최근의 사이버침해사고 발생 현황
Table 2. Occurrence status of recent cyber invasion accident

구 분	2003년	2004년	2005년	2006년	2007년
국가·공공부문	1,323	3,970	4,549	4,286	7,588
민간부문	26,179	24,297	49,726	34,597	27,728
합 계	27,502	28,267	54,275	38,883	35,316

2007년의 경우에 국가사이버안전센터에서 접수·처리한 침해사고를 분석한 결과, 공공부문 침해사고는 전년에 비하여 2배 가까이 늘었고 지방자치단체와 교육기관들의 보안 취약성은 오히려 악화된 것으로 나타났다. 지난해 공공부문 사이버침해사고 건수를 취합한 결과, 전체 공공기관에서 발생하는 사이버침해사고 건수는 총 7,588건으로 전년도의 4,286건에 비해 크게 증가한 것으로 나타났다.

표 3. 사이버테러형 범죄발생 건수
Table 3. Crime occurrence number as a pattern of cyber terror

연도	2003	2004	2005	2006	2007
전체 사이버범죄 건수	68,445	77,099	88,731	82,186	88,847
사이버테러 범죄 건수	14,241	15,390	21,389	20,186	17,671

출처: 경찰청 사이버테러대응센터.

지난 2003년, 전체 사이버범죄 66,445건 중 21.4%(14,241건)에 달하던 사이버테러형 범죄는, 컴퓨터와 인터넷의 대중화에 따라 전체 사이버범죄 발생 건수가 계속 늘어나는 것과 달리, 2005년 21,389건을 기록한 뒤 점차 줄어들어 2007년에는 17,671건이 발생하였고 차지하는 비중(19.9%)도 적어졌다.[14]

3.2. 사이버테러리즘의 전망

오늘날 사이버테러리즘 기술의 고도화·대규모화·악성화 추세로 그 위협은 첫째 해킹공격기술의 보편화로 국내 해킹사고가 매년 2-3배로 증가하고, 둘째 해킹 패러다임의 변화(파괴성+전염성)와 웜 바이러스 형태, 셋째 짧은 시간에 대규모 확산, 넷째 고도화된 정보통신인프라로 확산속도가 빠르고, 다섯째 전기·수도·항공관계시스템 마비, 주요 D/B 파괴 등 국가기간시설 공격 시 천문학적 피해, 여섯째 해킹 바이러스 공격의 지능화·고도화, 에이전트화·분산화·자동화·은닉화, 일곱째 다른 사이버범죄와 결합된 형태로 진화, 여덟째 해킹목적의 변화 등 위협이 증대되고 있다.[15]

특히 사이버테러리즘이 주목받는 이유는 물리적인 테러리즘보다 적은 비용으로 큰 효과를 노릴 수 있다는 데 있다. 폭탄을 설치하거나 인질을 납치하기 위해 목숨을 걸어야 하는 테러범들과는 달리, 사이버 테러리스트들은 전화선과 모뎀에 연결된 PC만 있다면 어디에서건 공격대상에 침투할 수 있다. 또한 고도 선진화된 사회일수록 전력과 금융, 통신 및 수송망 등의 사회기반이 네트워크로 연결되어 있는 만큼 정보망을 파괴했을 때의 파장은 예측하기 힘들다.

1999년 유고사태 와중에서 가상공간의 전쟁이라는 새로운 개념의 국지전이 실제로 벌어졌었는데 그 장소는 전장도, 민간인이 거주하는 지역도 아닌 비트세계 속이었다. 바로 미국과 나토의 유고 침공에 반대하는 개인과 단체들이 관련 기업이나 정부, 군사 등의 웹사이트를 공격해 서비스를 마비시킨 것이다. 이렇듯 사이버 테러리즘은 현실이며 세계 각국은 이에 대한 대응책 마련에 부심하고 있다.[16]

Ⅳ. 사이버테러리즘의 국가적 대응체계 구축방안

4.1. 외국의 국가안보관련 사이버안전체계

외국의 사이버테러리즘에 대한 대응체계에 대해서정리하여 보면 다음의 〈표 4〉와 같다.[17]

표 4. 외국의 사이버테러 대응체계
Table 4. Foreign countermeasure system against cyber terror

국 가	사이버테러 대응체계
미 국	사이버안보국, 국가정보체계국 등
영 국	M-15: 국가기반시설 보안조정기구 등
독 일	컴퓨터긴급대응팀-DFN-CERT 등
유럽연합	유럽네트워크정보보안청 등
일 본	정보보안부회, 방위청-사이버부대 등

4.2. 우리나라 국가안보관련 사이버안전체계

현 우리나라의 사이버안전체계는 국가정보원이 국가·공공부문, 국방부가 국방부문, 정보통신부가 민간부문을 담당하는 등 삼각체계를 유지하고 있는데 국가안보와 관련하여 사이버테러리즘에 대비하기 위한 범정부차원의 대표적인 기관을 살펴보면 다음과 같다.[18]

4.2.1. 국가사이버안전센터

국가정보원은 국가 사이버안전업무를 총괄하기 위해 2004년 2월 국가사이버안전센터를 개소하였으며, 2005년 1월 제정된 국가 사이버안전관리규정(대통령훈령 제141호)에 의거하여 국가차원의 종합적이고 체계적인 사이버공격 대응을 위

해 국가사이버안전 정책수립, 전략회의 및 대책회의 운영지원, 사이버위협 관련 정보의 수집·분석·전파, 국가정보통신망 안전성 확인 등의 업무를 수행하고 있다.

4.2.2. 국방정보전대응센터

국군기무사령부는 국방 분야 주요 정보통신 기반시설에 대한 정보보호 지원을 위해 1998년 대정보전팀을 창설하고 정보전대응 업무를 시작하였다. 첨단 정보보호기술과 컴퓨터 포렌식 전문인력으로 구성된 국방정보전대응센터는 정보전 대응분야와 IT기반 보호분야로 크게 분류되며, 정보전대응분야는 사이버안전기획과 사이버상황실, 침해사고 조사임무를 수행하고, IT기반분야는 취약점 분석과 사이버전 대응 및 모의훈련(정보작전방호태세), 보안측정 임무를 수행하고 있다.

4.2.3. 경찰청 사이버테러대응센터

경찰청은 사이버범죄의 위험성에 대한 범정부차원의 종합적 대응체제 필요성이 제기됨에 따라 2000년 7월 사이버공간의 선도적 치안을 담당할 사이버테러대응센터를 창설하였다. 이 센터의 산하에 전국 16개 지방경찰청에 사이버수사대가 있으며, 일선 235개 경찰서에 사이버 수사전담팀을 조직하여 운영하고 있다. 센터는 협력운영팀, 수사 1·2·3팀 및 기획수사팀, 기술지원팀으로 구성되어 있으며, 국내·외 사이버테러 사건추적·수사 및 초동조치, 사이버테러 수사기법 개발, 국제 경찰기구 등과의 협력체계 유지를 통해 사이버테러 대응 수사기관으로서의 역할을 담당하고 있다.

4.3. 사이버테러리즘의 사이버안전체계 구축방안

21세기 지식, 정보화 사회에서의 국가 경제, 사회 활동의 근간이 되는 통신, 금융, 전력, 국방, 행정 등 정보통신기반을 사이버위협으로부터 보호하여 국민들의 삶의 질을 향상시키고 국가경쟁력 및 국가안보 능력을 확보하기 위해서는 범국가차원의 사이버테러리즘 대응체제구축이 시급하다.

이에 사이버테러리즘에 대한 효과적인 국가 대응체제를 구축하기 위해서는 다음의 사항들이 우선적으로 고려되어야 한다.[19]

4.3.1. 사이버테러리즘 대응을 위한 법적· 제도적 기반 확보

날로 증가하는 사이버테러리즘의 위협에 효율적으로 대처하기 위해서는 법적, 제도적 장치가 우선적으로 마련되어야 한다. 이를 위해 국가 사회활동의 근간인 제반 시설에 대한 보호규정을 제정하여 우선 시행하고 향후 공공부문과 민간의 전 분야에 적용할 수 있는 법률을 제정하여 대처하는 것이 필요하다.

국가 공공기간의 사이버테러리즘에 대한 예방과 대응체제 구축을 위해 국가 정보원이 제정을 추진하고 있는 '국가정보기반보호규정(대통령훈령)' 내용을 살펴보면 국가정보 기반보호에 관한 부처 간의 의견을 수렴하고 이를 협의하기 위해, '국가정보기반보호실무협의회'를 설치 운영하고 또한 국가정보원장 소속 하에 '국가정보기반보호본부'를 설치하여, 국가정보기반보호계획 수립 시행, 국가정보기반별 취약성 평가 및 예방보응기술 개발 및 보급 등에 관한 업무를 총괄, 수행하도록 하고 있다. 특히 주요 국가정보기반은 통신, 금융, 에너지, 운송 등 분야별로 이를 보호대상으로 지정하여 중점보호 관리하면서, 사이버테러리즘을 조기에 탐지할 수 있는 탐지체계를 구축 운영토록 하여, 사이버테러리즘을 조기에 탐지하고 적절한 예방대책을 강구토록 지원하는 한편, 피해가 발생한 경우에는 신속한 복구기술을 지원하는 내용을 포함하고 있다.

4.3.2. 범정부 차원의 대응체제 구축과 대응체계의 기술적 능력 확보

사이버테러리즘에 대해 체계적이고 효율적으로 대처하기 위해서는 범 국 차원의 대응체제를 구축 운영하는 것이 필요하다, 이 대응기구를 통해서 지금까지 각 부처와 연구기관 등에서 분산 수행되어 온 대응전략 및 연구개발 기능을 유기적으로 통합 조정하는 한편 누가, 무엇을, 어떻게 책임 있게 수행해야 하는지 대해 충분한 검토와 협의가 이루어져야 한다. 이를 위해서 예방대책은 국가, 공공분야, 민간분야, 국방 분야로 나누어 대응체제를 구축 운영하는 것이 필요하며, 검찰과 경찰을 중심으로 사이버 범죄에 대한 수사기능을 확대하는 등 예방대책과 함께 사이버테러리스트에 대한 수사업의 강화 및 상호공조가 긴요하다. 이러한 대응체계를 통하여 정부기관과 민간기업 및 개인에게 국가사이버 안보정책을 설정하고 민·관·군 컴퓨터 침해사고 대응반 조직과 기능을 통합하여 체계적으로 조정할 수 있는 기능을 부여함으로써 사이버공격으로부터 실질적인 초기대응을 효과적으로 대응할 수 있는 기술적 능력의 확보도 필요하다.

4.3.3. 정보보호시스템 구축 및 보안관리 강화

사이버테러를 방지하기 위해서는 무엇보다 각 기관 및 업체의 주요 정보시스템에 대한 정보보호대 책이 강구되어야 하고 안전신뢰성을 보장할 수 있도록 보안관리가 철저하게 이행되어야 한다.

정보보호대책은 정보시스템에 대한 내외부 사용자의 접근제어, 인터넷 연결시 침입차단 및 탐지시스템, 해킹방지 및 안티바이러스 시스템 등 다양한 정보보호제품을 사용자 임무와 요구수준에 적합하도록 선택하여 설치하여야 한다. 또한

정보시스템의 안전한 보안 관리를 위해서는 최근 BS7799(영국 정보시스템 보안관리표준)에 준하는 평가인증을 받을 수 있도록 취약점을 보강하여야 한다.

4.3.4. 군의 사이버전 대응체계 구축

사회에서의 사이버테러는 군의 시각에서 사이버전과 밀접하게 관련된다. 우리 군은 장차전에서 승리할 수 있는 전력구축을 목표로 합동전장 운영개념 속에 정보전 수행을 명시하고 사이버전을 정보전의 일부로 인식하고 있다. 2001년 12월 국방부 정보화 기획실은 정보보호발전 기본계획을 수립하여 사이버전 대응체계 구축을 위한 국방부의 종합적인 계획을 제시하였다. 그러나 이 계획은 합참의 전력요소가 반영되지 않아 좀 더 정보작전차원의 구체적인 개념과 절차 및 교리연구가 필요하다. 또한 주변 환경을 고려하여 방어능력 뿐만 아니라 추적 응징능력, 즉 비상시 적극적인 공격능력까지 겸비한 사이버전 대응체계를 구축하여야 하며, 이를 위한 우선순위 확보를 위해서는 최고결정권자의 확고한 의지와 비전이 요망된다. 한편, 현재 합참 및 각 군에서 운용되고 있는 INFOCON(정보작전보호태세)도 사이버테러와 긴밀하게 연결되어 조치가 이루어질 수 있도록 하여야 한다.

4.3.5. 국가 간 국제협력의 강화

인터넷은 국경의 장벽 없이 전 세계적으로 연결되어 있으므로 외국사법 당국이나 국제기구와의 협조관계를 구축하여 인터넷 범죄에 공동대응 할 필요가 있으며, 외국의 입법동향 등을 충분히 파악하여 국제조약 체계 등에 대비하여야 할 것이다. 즉 인터넷 범죄발생으로 관련 사이트 및 이용자 수사시 외국의 사이트도 함께 수사해야 하므로 이에 대한 관할권 문제와 범죄인 체포활동 등 사이버범죄에 대한 효과적인 대응을 위해 외국과의 공조수사는 필수적이다. 그리고 이러한 문제점들을 인지하여 선진국들은 사이버범죄에 공동대응방안을 강구하고 있으므로 우리나라도 이에 대한 대책을 수립해야 할 것이다.

V. 결 론

전 세계적으로 인터넷 이용자의 급격한 확산은 사이버 공간에서 다양한 형태의 긍정적 측면과 부정적 측면을 동시에 드러냈다. 후자의 경우는 사이버 공간이 '21세기의 복음'이 아닌 '세기말의 판도라의 상자'라는 우려를 제시하였다. 인간의 지나친 컴퓨터 네트워크에 대한 의존은 범죄 및 테러단체들에게도 이용되어 결국은 인간의 자멸로 이어질 수 있다는 가능성을 제기하기도 한다. 염세주의자들은 인터넷상의 익명성과 초국가성은 물론 광범위한 전파성과 신속성 등이 사이버 포르노와 사이버매춘과 같은 사이버 펑크문화를 만들어내는 도구로 전락되고 있다고 주장한다. 또한 초국가적 범죄단체 및 정치적 테러단체들이 국제범죄 및 테러를 위한 수단으로 전개하여 궁극적으로 일국의 국가안보 내지는 국제안보에도 치명적인 타격을 줄 수 있다고 주장한다.[20]

이에 전 세계 국가들은 사이버테러에 대응하기 위한 모든 조치를 강구하고 있으며, 우리나라도 대응태세 구축을 위해 노력하고 있다. 그러나 정보기술의 발전 속도는 법과 제도가 따라가기에 너무 빠른 속도이므로 대응체계의 낮은 탄력성은 곧바로 위협의 증대로 나타난다. 따라서 장기적인 관점에서 볼 수 있는 시각으로 계속적으로 진화하는 기술과 이에 맞서 사이버테러에 대비에 적극적으로 참여함으로써, 위협을 예상하고 그에 맞춘 보호조치가 지속적으로 이루어져야 한다.[21]

이를 위해서는 사이버테러리즘 대응을 위한 법적·제도적 기반의 확보, 범정부 차원의 대응체제 구축과 대응체계의 기술적 능력 확보, 정보보호시스템 구축 및 보안관리 강화, 군의 사이버전 대응체계 구축, 그리고 사이버테러리즘에 대한 국가 간 국제협력의 강화 등을 위한 범국가적인 적극적 대응전략을 모색하여야 할 것이다.

참고문헌

[1] 한국전산원, 「국가정보화백서」, 106-107쪽, 2004.

[2] 조성권, "21세기 새로운 테러리즘과 한국의 대응방안," 「9.11 테러 이후 국제 안보환경의 변화와 우리의 대응」, 2001.

[3] 조광래, "정보환경시대의 사이버테러," 「제13회 한국경호경비학회 학술세미나 논문집」, 50쪽, 2004.

[4] 이성식, "사이버범죄와 시민의 역할," 「정보화정책」, 제13권 제3호, 70쪽, 2006.

[5] 백광훈, "인터넷범죄의 규제법규에 관한 연구," 36쪽, 2000.

[6] 이성식, EN(4), p.70.

[7] 정정일, "사이버범죄에 대한 국제적 대응방안," 「경호경비연구」, 제10호, 328-329쪽, 2005.; 이성식, EN(4), pp.70-71의 내용을 표로 재정리.

[8] 경찰청, 사이버테러대응 센터 (*http://www.ctrc.go.kr.*).

[9] 김두현, 「현대 테러리즘론」, 백산출판사, 151쪽, 2004.

[10] 최정호, "사이버테러리즘의 변천방향과 한국의 대응,"

「국방안보학술회의」, 158-159쪽, 2008.
〔11〕 김두현, EN(9), pp.144 -145.
〔12〕 남길현, "사이버테러와 국가안보," 「국방연구」, 제45권, 제1호, 168-170쪽, 2002.
〔13〕 국가사이버안전센터, "사이버침해 위협과 사례," 「2008 국가정보보호백서」, 16-20쪽 재인용, 2008.
〔14〕 최정호, "사이버테러리즘의 변천방향과 한국의 대응," 「국방안보학술회의」,160쪽, 2008.
〔15〕 김정구, "사이버테러리즘 대응인력 양성," 「제3회 사이버테러리즘 정보전 컨퍼런스 2003」, 사이버테러리즘 정보전학회, 155쪽, 2003.
〔16〕 김두현, EN(9), p.152, 2004.
〔17〕 김두현, EN(9), pp.153-155.; 남길현, EN(12), pp.176-181.
〔18〕 국가사이버안전센터, 「2006년도 사이버 침해사고 사례집」, 97-102쪽, 재인용, 2007.
〔19〕 김병준, 「신종범죄론」, 창조문화, 289-290쪽, 2006.; 김두현, EN(9), p.156.; 남길현, EN(12), pp.188-189.; 양종환, "테러형 사이버범죄 실태와 경찰의 대응방안에 관한 연구," 원광대학교 석사학위논문, 95-96쪽, 2007.; 한봉조, "사이버범죄 수사에 대한 국제적 협력문제," 「형사정책연구」, 제11권 제2호, 46-49쪽, 2000.
〔20〕 조성권, EN(2),
〔21〕 조광래, EN(3), p.50.

저자소개

김 영 환

2000년 8월: 조선대학교 행정학박사
2005년~현재: 조선대학교 사회과학대학 교수