정 보 보 호 학 회 지
제24권 제6호, 2014. 12

# 사이버 안보 대응 역량 강화방안 연구

안 유 성*

요 약

최근 현실 공간에서의 물리적 공격(Hard Attack)이 가상공간을 통한 사회 공학적 공격 및 정보기반통신망 공격(Soft Attack)으로 변화하고 있다. 이에 따라 군사(방위산업) 및 국가 주요정책정보에 대해 정보통신망을 통한 각종 정보의 해킹 등 전자정부·사회간접시설 및 공공서비스의 기능에 대한 침해가 빈발하고 있다. 사이버공간에서의 국가안전보장을 위한 활동은 사후방어보다는 사전예방이 중요하며, 이를 위해서는 사이버공격 징후의 포착과 종국적인 책임기관에 의한 통합적 대비가 필요하다. 이러한 업무를 효율적으로 수행하기 위해서는 대통령실을 정점으로 국가안전보장을 종국적으로 책임지는 기관이 국가 사이버위기의 예방 및 방어 전략을 체계적·통합적 관리할 수 있도록 입법적 대응방안을 마련하는 것이 매우 시급한 과제이다.

## Ⅰ. 서 론

우리나라는 현재 인터넷 해킹사고·물리적 사고 등이 매우 빈번히 발생하고 있다. 이것은 우리나라의 초고속 인터넷 인프라가 우수하고 PC의 보급률도 높아 사이버 보안과 안보의 문제가 제기될 가능성이 높기 때문이다. 우리나라의 경우 다수의 무료 보안 백신이 서비스되고 있고, 쇼핑몰 및 은행 웹 사이트 접속 시 해킹 보안, 키보드 보안, 방화벽을 설치·실행해 주고 있음에도 불구하고 사이버 안보의 측면에서는 침해사고가 계속 발생하고 있다. 그 원인으로는 우선 다양한 프로그램들의 오·남용을 들 수 있기는 하지만, 기본적으로 바이러스에 감염되거나 부정 침입자의 원격 조종 소프트(백 도어)가 설치되었으나 PC사용자가 이를 인식하지 못하고 방치된 상태의 컴퓨터인 좀비PC가 다수 존재한다는 점을 고려해야 한다. 이들 좀비PC는 스팸 메일 발송, 해킹 공격, DDoS 공격 등에 악용되어 자신도 모르는 사이에 정보통신망 또는 정보통신 기반 시설을 공격하는 도구로 사용되고 있다. 스마트폰과 클라우드 컴퓨팅으로 대표되는 정보사회에 있어서 이러한 위험이 더욱 가중되고 있으므로 새로운 정보보안기술의 발전양태를 중심으로 보안기술의 현황과 관련 법제의 실태 등을 살펴보고 그 대안을 검토할 필요성이 있다. 당해 연구에서는 이러한 정보보안기술의 발전 양태를 고려하여 현재 진행되고 있는 국내·외의 사이버보안과 관련된 기술적·제도적 환경을 분석하고, 새로운 변화에 적극적으로 대응할 수 있는 근본적이고도 거시적·장기적인 해결책을 제시하며 사이버 침해에 대비한 발전방향을 제시하고자 한다.

## Ⅱ. 사이버 안보 침해 사고와 기술

### 2.1. 사이버보안 관련 용어의 다양성

2013년은 대한민국이 사이버위협의 공포에 시달린 한 해였다고 표현하여도 과언이 아닐 것이다. 2013년 3월 20일 KBS·MBC·YTN 등의 방송사와 농협·신한·제주은행·NH생명보험·NH손해보험 등 금융기관에 대한 사이버테러가 발생하였다. 그리고 상황을 정리하고 얼마지나지 않은 2013년 6월 25일 전쟁발발 63주년이자 정전 60주년에 해당하는 날, 북한의 소행으로 추정되는 대대적 해킹공격이 발생하여 청와대와 국무조정실의 홈페이지가 위·변조되고, 일부 언론사 홈페이지의 서버가 멈추거나 접속 불가상태에 빠지는 등 총 16개 기관에서 사이버공격을 받은 것으로 밝혀졌다.

#### 2.1.1. 사이버범죄

‘사이버범죄’라는 용어는 원래 1980년대 사이버펑크

* 성균관대학교 정보통신대학원 (dehan86@naver.com)

소설에서 처음 나타났는데, 이것은 사이버공간과 범죄를 조합한 개념으로 과거 현실 세계의 범죄가 단지 컴퓨터시스템을 통하여 사이버공간에서 이루어지는 형태를 '(일반)사이버범죄'라고 일컫는다. 이것은 인터넷과 같은 정보통신망으로 연결된 컴퓨터 시스템이나 이들을 매개로 한 사이버공간을 이용하여 공공복리를 저해하고, 건전한 사이버문화에 해를 끼치는 행위이며, 빠른 시간 안에 불특정 다수에게 광범위한 영향을 미치는 특성이 있다.

#### 2.1.2. 사이버공격

사이버테러와 구분하여 '사이버공격'(Cyber Attack)이라는 용어를 사용하기도 하는데, 사이버공격이란 인터넷을 통해 다른 컴퓨터에 불법접속하여 상대방 국가나 기업에 손상을 입히려는 행동으로서 실제로 실행하는 내용은 일반적 불법접속이지만 정치적인 의도로 불법접속을 하는 것을 지칭하며 우리나라의 국가사이버안전관리규정 제2조 제2호는'사이버공격'이라는 단어를 사용하고 있다. 사이버공격(Cyber Attacks)과 '사이버착취'(Cyber Exploitations)는 컴퓨터 시스템이나 네트워크를 상대로 적대적 행위를 한다는 점에서 공통점이 있다.

#### 2.1.3. 사이버테러

사이버공간의 위협은 여러 가지 방법으로 분류가 가능하다. 가장 일반적인 것 중 하나는 동기적 요소를 기초로 한 3가지 즉 사이버테러, 사이버공격, 사이버범죄의 분류방식이다. 그러나 공격하려는 동기에 대한 확신 또는 명확한 정의가 난해하여 '가해진 손해의 규모'만으로 분류하기도 한다. 사이버테러로 인한 손해는 컴퓨터 네트워크 사이의 높은 상호영향도와 정보기반시설에 연관된 서비스 상호의존 때문에 상당히 클 수밖에 없다. 예를 들어 한명의 서비스제공자 서버에 대한 공격은 관련 없는 기관의 정보시스템을 중단시킬 수 있고, 그것은 같은 제공자의 서비스를 사용하는 불특정 대다수에게 아마도 중요한 기반시설의 일부분일 것이다. 사이버테러(Cyber Terror)가 무엇인가에 대해서는 여러 가지 개념을 혼용하여 사용하고 있으며 국가마다 미묘한 차이가 있다. 먼저 사전적으로 사이버테러란 '정보통신망 자체를 공격 대상으로 하는 불법행위'를 말한다. 즉, 사이버테러는 해킹, 바이러스 유포, 메일 폭탄, 전자기적 침해 장비 등을 이용해 컴퓨터 통신망 및 인터넷 등의 사이버공간을 활용하여 불특정 다수에게 엄청난 피해를 입히는 일련의 행위로 컴퓨터시스템과 정보통신망 공격 등을 일컫는다.

## Ⅲ. 사이버 안보 침해 사고현황

### 3.1. 국내 사이버 침해 사고 사례

#### 3.1.1. 1 · 25대란

1·25대란은 호주, 미국 등에서 유입된 슬래머웜(Slammer Worm)이 MS의 데이터베이스 'SQL서버'를 공격하여 한국의 8,800대를 비롯하여 전 세계 75,000여 대를 다운시킨 사건이다. 한국의 경우, 국제회선 및 ISP의 주요 DNS 서버와 인터넷데이터베이스센터(IDC) 내부 망에 과부하 현상이 발생하였다. 당시 미국 FBI와 국제공조수사를 진행했지만, 범죄인지 테러인지에 대해 명확한 결론을 내리지 못했다. 그 후 이 사건은 어떤 특정 집단이 국내 인터넷망을 마비시키기 위해 시도한 공격이 아닌 국내 주요 도메인네임서비스를 제공하는 인터넷서비스제공업체(ISP: Internet Service Provider)에서 보안 패치를 제대로 설치하지 않아 발생한 사고로 판명되었으나, 이 사건은 웜 하나로 인터넷을 마비시킬 수 있다는 가상 시나리오를 현실세계에서 입증한 첫 번째 사례로 기록되었다.

#### 3.1.2. 북한 발 7·7 디도스 공격

7.7 DDoS 공격은 북한이 청와대 · 국방부 · 국정원 등 국가 중추기관과 언론사 · 은행 등 21개 사이트를 공격하여 시스템 운영을 방해한 사건이다. 이 사건은 북한의 공격이 대외적으로 공개된 최초의 사건이다. 공격자들은 악성코드를 설치하면서 원본 파일이 자동으로 소멸되도록 설계하였고, 악성코드를 그림파일로 위장하는 등 지능화된 수법을 사용하였다. 또한 악성코드에 감염된 11만 5천여대 좀비PC 공격으로 총 36개 사이트 접속 장애가 발생하였고, 하드디스크를 파괴함으로써 수사기관이 추적을 하지 못하도록 범행이 이루어졌기 때

문에 수사에 많은 어려움을 겪었다. 당시 사건을 살펴보면 2009년 7월 7일 18:00경부터 국내 정부기관, 정당, 포털 사이트, 언론, 인터넷 쇼핑몰, 금융기관, 백신업체 및 미국 정부에서 운영하는 홈페이지 등 35개 웹사이트가 동시다발적으로 DDoS공격을 당하였다. 공격은 7월 7일, 8일, 9일 3차례에 걸쳐 감행되었고, 10일 자정을 기해 DDoS 공격에 악용되었던 좀비PC가 파괴되면서 중단되었다. 이처럼 7·7 DDoS 사건은 기존 DDoS 사건과는 동일한 구조를 갖고 있으면서도 기존 방식과는 차원이 다르게 정교하게 구성되었고 다수의 서버가 동원된 점이 특징이다. 이 사건은 전 세계 61개국 435대 서버를 해킹하여 디도스 공격에 동원하는 등 글로벌한 공격 형태를 여실히 보여주었다. 당시의 경험에 비추어 부처 간 혼선을 예방하기 위해 범정부 차원의 '국가 사이버 위기 종합대책'을 마련하게 된 결정적인 계기가 되었다.

### 3.1.3. 북한 발 3·4 디도스 공격

북한이 좀비PC 10만대를 동원하여 국회・행정부 등 20개 정부기관 홈페이지와 은행・증권사・포털 등 20개 사이트에 대하여 DDoS공격을 감행한 사건이다. 이들은 해외 70개국에 746개의 공격명령 서버를 구축한 다음 실시간으로 좀비PC를 제어하면서 정부기관과 민간의 홈페이지를 마비시켰다. 당시 사건발생 직후 과거 7・7 디도스 공격과 같은 북한의 소행여부가 문제되었는데, 이에 경찰청은 파일공유 사이트를 통해 악성코드를 유포한 점, 디도스 공격체계와 방식이 동일하다는 점, 악성코드의 설계 및 통신방식이 일치하다는 점, 해외 공격 명령 서버 중 일부가 동일한 점 등을 종합하여 7・7 디도스 공격의 주체와 동일하다는 수사결과를 발표하였다.

### 3.1.4. 농협 전산망 해킹 사건

2011년 4월 12일 농협 전산망이 해킹되고 자료가 대규모로 훼손되어 수일에 걸쳐 전체 또는 일부 서비스 이용이 마비되었다. 서울 중앙지방검찰청의 수사결과, 농협 전산서버 유지보수업체 직원의 노트북이 웹하드 사이트를 통해 해킹되어 7개월 동안 노출되었고, 공격은 원격으로 인터넷을 통해 이루어졌다고 밝혔다. 이 사건은 7・7 디도스 공격 및 3・4 디도스 공격과 유사한 프로그래밍 방식을 사용하였고, 악성코드 유포 경로・방식의 유사성, 공격 명령 서버의 동일성 등을 근거로 공격주체가 북한이라고 밝혀졌다.

### 3.1.5. 2013년 사이버 침해 사례

우리나라는 올해 2013년 3월 20일 북한 정찰총국에 의한 막대한 사이버테러의 피해를 입었다. 일명 3·20 사이버테러로, KBS・MBC・YTN과 농협・신한은행 등 방송・금융 6개사 전산망 마비 사태가 발생한 사건을 말한다. 이후 4월 10일 민・관・군 사이버위협 합동 대응팀은 이번 사이버테러의 수법과 접속기록을 정밀 조사한 결과 북한 정찰총국의 소행인 것으로 결론 내렸다고 발표했다. 이에 따르면 주요 방송사(KBS・MBC・YTN)와 금융회사(신한은행・NH농협은행・제주은행) 전산망이 2013년 3월 20일 오후 2시경 악성코드에 감염, 총 3만 2000여 대에 달하는 컴퓨터가 일제히 마비되는 사상 초유의 정보보안 사고가 발생했다. KBS・MBC・YTN 등 방송사에서는 이날 직원들의 PC가 멈췄고, 신한은행・NH농협은행 등 금융기관에서는 인터넷 뱅킹과 영업점 창구업무, 자동화기기(ATM) 사용 등이 일시 중단되면서 관련 거래가 2시간 가량 중단됐다. 이날 미래부와 안행부, 국방부, 국정원 등 10개 관련 부처는 사이버위기평가회의를 열고 오후 3시 사이버위기 경보단계를 「관심」에서 「주의」로 격상시켰다. 또한 국방부도 군의 정보작전방호태세인 인포콘(INFOCON)을 4단계에서 3단계로 격상했다. 3개월 후인 2013년 6월 25일에는 청와대를 비롯한 다수의 기관을 대상으로 사이버테러가 발생하였다. 사이버테러를 감행한 해커집단은 새누리당원 250만 명, 군 장병 30만 명, 청와대 홈페이지 회원 10만 명, 주한미군 4만여 명의 개인정보를 탈취하는 범행을 감행하였다. 이날 오전 9시 10분경 청와대 홈페이지 및 주요 정부기관, 언론사 등에 웹 사이트 변조, 분산서비스거부(DDoS), 신상정보 유출 등의 공격이 수행되었다. 청와대 홈페이지 등에 접속하면 '위대한 김정은 수령', '통일대통령 김정은 장군님 만세! 우리의 요구조건이 실현될 때까지 공격은 계속될 것이다. 우리를 맞이하라. 위 아 어나니머스(We Are Anonymous)' 등의 문구와 박근혜 대통령의 사진이 나타났다. 이후 미래부는 7월 16일 6·25 사이버공격이 3·20 사이버테러 등 과거 북한의 해킹 수법과 일치한다

고 밝혔다. 해당 해커집단은 북한의 군 고위 간부 20여 명의 인적사항 공개와 함께 북한의 미사일, 무기 등 수만 건의 자료 공개를 예고한 바 있다.

### 3.2. 사이버 안보 침해 사고에 이용된 기술

개인·기업 또는 공공기관에서 추진하고 있는 다양한 스마트 단말 활용 분야 중 서비스별로 7가지의 보안 위협사안이 존재한다. 국가사이버안전센터의 스마트폰 보안규격에 따르면 스마트 단말서비스별 보안위협의 종류는 인터넷전화·모바일게시판·메신저·이메일·현장업무·업무보고 및 전자결재 등 총 7가지이다. 이에 대한 해킹사고의 주요 유형을 살펴보면 악성코드 유포·경유사이트를 통한 해킹, VPN(가상사설망)을 통한 해킹, 웹 어플리케이션 취약점 공격을 통한 해킹, DB연동 웹사이트 해킹, 악성코드 감염을 통한 해킹 등이 있다.

#### 3.2.1. 악성코드 유포·경유사이트·VPN을 통한 해킹

유포·경유사이트를 통한 악성코드 감염은 보통 기업의 보안관리 소홀로 발생한다. 악성코드를 유포하기 위해 공격자는 사전에 운영 중인 웹사이트의 서버를 해킹하여 웹 소스코드에 악성코드를 심어 놓고, 이를 알 수 없는 사용자는 자동으로 악성코드를 유포하는 사이트에 접속하게 되어 감염된다. 감염된 PC를 통해 개인정보유출, 분산서비스거부공격(DDoS), 스미싱 등의 이차적인 피해를 발생시키기 때문에 심각한 사회적 문제가 된다. 공격자에 의해 통제된 시스템은 키로거(Key Logger)나 사회 공학적 기법을 이용한 악성코드로 인해 사용자의 중요 정보가 유출되거나 막대한 금전적 피해를 야기할 수 있다. 특히 보이스 피싱이나 파밍 등의 기법이 정교하게 진화하고 피해액 또한 증가하고 있어 예방책이 시급하다.

#### 3.3.2. 웹 어플리케이션 취약점 공격

웹 어플리케이션(Web Application) 취약점을 이용하는 해킹 방식으로는 지속적으로 시스템에 접근하기 용이하게 백 도어를 설치하거나 파일업로드의 취약점을 악용한 웹 쉘(Web Shell) 업로드 등의 방법이 있다. 웹 어플리케이션의 취약점을 공격하면 홈페이지 변조뿐만 아니라 시스템에서 다양한 해킹을 수행하기 때문에 개인정보유출이나 좀비 PC 발생 등 지속적인 문제가 발생할 수 있다. 최근 스마트폰의 이용 증가로 안드로이드 운영체계의 취약점을 이용한 악성코드 공격도 활발하여 휴대폰에 저장된 전화번호 유출과 소액결제까지 보안 취약점에 대한 공격이 심각해지고 있다.

#### 3.3.3. 영향력이 확대된 자바의 취약점 공격

2014년에 사이버 범죄자는 자바 패칭(patching) 사례를 이용하여 가치가 높은 네트워크를 목표로 하기 위해 제로 데이 자바 취약점(zero-day Java exploits)을 이용한 공격할 것이며, 대부분이 자바의 구(舊)버전을 사용하기 때문에 이 취약점을 공략할 것이다.

## Ⅳ. 세계 각국의 침해사고 및 역량강화 현황

### 4.1 미국

사이버 안보에 대한 관심은 현 오바마(Obama) 행정부 뿐 아니라 부시(Bush) 대통령 재임 시절부터 ‘The National Strategy to secure Cyberspace' (2003.2) 등 사이버안보에 관련된 보고서를 발표하면서 선도적으로 정책과 법제를 완비하려는 노력을 계속해오고 있다. 보건·재산 그리고 안전을 사이버공격으로부터 보호하기 위해 미국은 대통령 훈령·행정명령·입법·정책들을 발표해왔다. 이를 위해 그동안 미국의 공군(USAF: United States Air Force)·첩보기관·연방수사국(FBI: Federal Bureau of Investigation)·국토안보부(DHS: Department of Homeland Security)·국토안보이사회·국방부(DOD: Department of Defense)·행정관리예산국(OMB: Office of Management and Budget) 등을 비롯한 다른 연방기관들은 사이버안보를 위한 대책마련에 전력을 기울였다. 이러한 노력의 결과 국제 라디오 또는 통신선 거래(Dealing With International Radio Or Wire Communications), 악의적 위성방해(Malicious Interference With Satellites), 텔레뱅킹을 이용한 유사 금융사기(Wire Fraud)에 대한 사이버공격의 문제들을 다룰 수 있는 법적 근거를 마련하였다. 나아가 오바마 대통령 취임 이후에는 보다 적극적인 태도로 임하여, 사이버안보를 국가안보의 중요한 일부분으로 간주하고 있으며

소극적인 방어에서 한 걸음 나아가 적극적인 대응체계로 변모하고 있다. 그 대표적인 사례로는 2009년 사이버안보 관련 보좌관 직위를 신설한 것과 사이버 사령부의 창설을 들 수 있다. 또한 기존의 사이버 정책을 점검하고, 새로운 정책 마련을 위해 2009년에는'사이버 정책 검토 보고서'(Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure)와 '사이버공간에 대한 국제 전략: 네트워크 세계에서의 번영, 안보 및 공개성'(ISC: International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World)이라는 보고서를 발표하였다. 이밖에도 인프라 소프트웨어나 시스템의 안전성을 평가·실험하는 기관의 설립과 국가정보 인프라를 통과하는 데이터를 검사하는 기술 연구의 필요성을 끊임없이 주장하고 있다.

### 4.2. 유럽

#### 4.2.1. 유럽연합

유럽연합은 사이버공격의 지능화, 다양화로 인해 기존의 기술적 대응만으로는 한계가 있음을 인식하고 새로운 유형의 악성코드 및 봇넷(Botnet), 피싱(Phishing)과 같은 사회 공학적 공격의 사전예방을 위해 사이버안보에 관한 인식제고를 위해 지속적인 노력 및 투자를 하고 있으며, 특히 최근 사이버안보 인식에 관한 실태조사 및 가이드라인 개발 등 활발한 연구를 수행하고 있다.

#### 4.2.2. 영국

영국은 국가안보를 위한 종합보고서라고 할 수 있는 'A Strong Britain in an Age of Uncertainty: The National Security Strategy'(2010)에서 사이버공격을 테러공격에 이어 두 번째 우선순위로 상정할 만큼 사이버안보에 대한 관심이 각별하다. 하지만 사이버공격의 위험성의 주안점을 현재까지는 주로 지적재산권의 도용이나 정보 유출에 두고 있는 것으로 인식하고 있는 한계가 있으며, 이는 미국의 인식과 차이를 보이는 점이다. 영국에서의 사이버안보에 대한 종합적인 내용은 총리실에서 작성한 'Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space(CSSUK)'(2009.6)을 통해 보다 구체적으로 알 수 있다. 당해 보고서는 ① 인권, 법의 지배, 정당하고 신뢰할 수 있는 정부, 정의, 자유, 관용 및 기회라는 핵심 가치에 기초해야 한다. ② 냉정하게 위험, 목표 및 능력을 평가해야 한다. ③ 가능한 한 안보적 도전과제를 조기에 해결해야 한다. ④ 국제적으로는 다자적 접근을 취해야 한다. ⑤ 국내적으로는 협력관계를 통해 접근해야 한다. ⑥ 정부 내에서는 보다 통합적인 접근방법을 개발해야 한다. ⑦ 강력하고 유연하면서도 균형 있는 능력을 보유해야 한다. ⑧ 안보를 강화하기 위해 계속해서 투자하고 학습하며 개선해야 한다는 등의 내용으로 구성되어 있다. 이 보고서에서는 위와 같은 원칙에 기초하여 ① 지식·능력 및 정책결정을 통해, ② 사이버공간에서의 위험을 줄이고, ③ 향후 사이버공간에서 영국의 이익을 확보해야 한다는 등 3가지 측면을 강조하였다. 이후 영국에서는 2011년 국무조정실에서 작성된 'The UK Cyber Security Strategy - Protecting and promoting the UK in a digital world(CSSUK)'를 통해 사이버안보전략을 한층 더 발전시킨 것으로 평가받고 있다. 2013년 초에는 정보기관과 민간 보안전문가로 구성된 사이버 보안통제센터를 설립하였는데, 여기에 금융·국방·에너지·통신·제약 등 5개 분야에서 160개 업체가 참여하여 사이버위협에 공동 대응하는 체계를 갖춘 바 있다.

#### 4.2.3. 독일

독일에서는 현재까지 테러 또는 사이버테러 예방이나 처벌을 위한 특별한 법률을 제정하고 있지는 않으나, 각 개별 형벌법규를 통하여 테러와 사이버테러 방지에 대비하기 위한 규정을 두고 있다. 그리고 「정보통신법」, 「통신서비스법」, 「연방데이터보호법」, 「정보통신서비스 정보보호법」, 「전자서명법」, 「통신법」, 「형법」, 「연방정보기술 안전청 설치에 관한 법률」, 「연방의 정보기술 보안강화를 위한 법률」 등 사이버안보와 관련된 법제의 정비를 통해 사이버 위기에 적극적으로 대응하고 있다. 독일 정보기관들의 임무와 권한의 특징은 국내안보에서는 군대의 역할이 배제되어 있고, 국내안보의 주요담당기관으로서 경찰의 지위가 확립되어 있고, 독자적인 헌법보호청을 설치함으로써 경찰의 정치화를 예방하고 있다. 향후 테러의 국제화·보편화와 더불어 연방경찰, 연방헌법

보호청, 연방정보기관(BND: Bundesnachrichtendienst), 군정보기관(MAD: Militärischer Ab- schirmdienst) 등 각급기관의 업무 관할이 불확실한 경우가 다수 발생할 수 있다. 이러한 상황에 대비하여 가령 연방헌법보호청의 경우 수집된 정보를 수사기관에 통보하도록 규정하는 등 독일 내 대테러 유관기관 간 협조체제의 유기적 구축을 통해 미묘한 문제를 해결하고 있다. 지난 2011년 2월 연방내무부는 'Cyber Security Strategy for Germany'(이하 CSSG)에서 사이버안보는 민간을 중심으로 이루어져야 한다고 하면서도, 이러한 민간의 조치는 동시에 군대(Bundeswehr)의 조치에 의해 보완될 수 있다고 밝힌바 있다. 더불어 사이버안보가 독일의 예방적(Preventive) 안보 전략의 일부에 속한다고 언급하고 있으며, ICT의 특성을 감안하여 국제적인 공조가 중요하다고 강조하고 있다.

#### 4.2.4. 에스토니아

에스토니아는 통신기술이 매우 발달한 국가 중 하나이므로 주요 정부 업무들은 2005년부터 이미 대부분 인터넷으로 이루어지고 있다. 각료회의도 온라인상으로 실시하였고, 서류에 대한 서명 또는 결제도 인터넷 서명을 통해 이루어졌다. 놀라운 점은 2007년 3월 이미 에스토니아 시민들은 온라인으로 투표를 진행하기도 했다는 것이다. 2007년 당시 인구의 60%가 온라인 은행 계좌를 갖고 있었고, 95%의 은행 거래가 온라인으로 이루어지고 있었다. 2007년 4월, 인터넷 의존도가 세계에서 가장 높은 나라 중의 하나인 에스토니아는 대규모의 사이버공격을 받았다. DDoS공격이 개시된 지 한 시간 내에 에스토니아의 은행, 신문 그리고 주요 정부 기관의 인터넷망이 마비되어 에스토니아는 사이버공간에 고립되었다. 에스토니아는 러시아가 공격의 배후에 있을 것이라고 추정하였지만 , 추후 다른 몇몇의 국가들이 진원인 것으로 밝혀졌고, DDoS공격 그 자체의 근원지는 추적할 수조차 없었다. 이후 이렇게 유럽국가 중 발전된 인터넷 망을 보유하고 있는 에스토니아는 사이버테러의 대상이 될 것을 우려하여 인터넷 보안체계의 정비를 서두르고 있다.

### 4.3. 중국

중국은 우주, 전자, 사이버공간에서의 국가안보이익 수호를 국방목표로 설정하고 있다. 중국은 현재 해커부대인 넷포스와 정보전시험센터·국방과학기술정보센터 등의 해커양성기관을 운영하고 있는 것으로 알려져 있으며, 유사시 사이버공간을 이용한 대규모공격을 실시하려고 시도하고 있는 것으로 파악되고 있다. 2007년에 이미 중국은 인터넷 사용자가 약 2억 1000만 명으로 인도사용자의 3배가 되었고, 2008년에는 인터넷 사용자가 미국을 넘어선 바 있다. 현재 100만 명 이상의 민간 애국해커(Patriot Hacker)가 활동 중이며, 이들은 사이버 예비군 역할을 하고 있다. 또한 국가 중앙군사위원회는 국가차원에서 사이버전에 대비하기 위해 조직을 정비중인 것으로 알려지고 있다.

### 4.4. 일본

일본은 사이버위기에 대응하기 위한 노력의 일환으로 법률은 물론이고, 각종 지침과 가이드라인을 통해 사전 예방, 사고발생시 피해확대를 방지하고, 사건에 대한 검토 등을 효율적으로 시행하도록 하고 있다. 물론 시간과 공간을 초월하고 그 징후를 알 수 없어 예측하기 어려운 사이버테러의 특성상 완벽한 사전예방이라는 것은 거의 불가능하지만 최대한 효과적으로 대응하기 위해서는 정부와 민간의 협업이 중요하다는 점이 강조되고 있다. 현재까지는 치명적인 사건이 발생하지 않았으나 향후 심각한 테러가 발생하는 상황을 상정하여, 사이버위기에 대비한 관련 법제를 정밀하게 검토하고 있는 것으로 알려지고 있다. 향후 일본은 궁극적으로 정보통신망 상의 위기와 아울러 사이버테러에 대한 전반적이고 종합적인 위기관리가 가능하도록 하는 제도를 준비하고 있다. 또한 하드웨어적인 정보처리장치나 정보통신망에 대한 관리·기술적 안전장치 및 하드웨어 시스템에 정통하면서도 사업자 간 또는 사업자와 행정부서간 보안대책을 연계할 수 있는 인재를 육성하고 사용자의 보안의식을 강화하는 방안을 마련하기 위해 전력할 것으로 보인다.

### 4.5. 호주

호주에서 사이버안보와 직접적으로 관련된 기관으로는 컴퓨터 긴급 대응팀(CERT Australia: Australia's national computer emergency response team)과 사이버 안보 운용 센터(CSOC: Cyber Security Operations

Centre)가 있으며, 기타 법무부·통신미디어국(ACMA)·안보정보국(ASIO) 등도 사이버안보와 관련된 정부 조직이다. 호주의 사이버안보 전략은 2009년 법무부 주관으로 작성된 'CYBER SECURITY STRATEGY'에 상세히 기술되어 있다. 이 보고서는 사이버안보를 '전자적 또는 유사수단에 의해 처리되고, 저장되며, 전파된 정보의 비밀성, 이용가능성 및 완전성에 관련된 조치'(Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means)라고 정의하고 있다. 한편 이 보고서에서는 목표와 전략적 우선사항을 제시하고 있는데, 주요목표(aim)는 호주의 국가안보를 뒷받침하고, 디지털 경제의 혜택을 극대화할 수 있도록 안전하고(secure), 복원가능하며(resilient), 신뢰받는(trusted) 전자적 운용 환경(Electronic Operating Environment)을 유지하는 것으로 보고 있다. 또한 사이버 정책도 '국가 전략 성명'(National Security Statement)의 내용과 조화를 이루어 국가 리더십(National Leadership), 책임 공유(Shared Responsibilities), 협력관계(partnerships), 국제적 차원의 적극적 관여(Active International Engagement), 위험관리(Risk Management), 호주의 가치 보호(Protecting Australian Values)라는 원칙들에 기초하고 있다.

## Ⅴ. 사이버안보 역량 강화를 위한 제도 개선

### 5.1. 해당 부처의 책임 강화

사이버 안보 기반시설 지정확대에 대해 최근까지 정부는 다소 소극적인 태도를 보여 왔다. 현재 우리나라는 세계적인 수준의 사이버공격 대응체계를 구비하고 있으나, 최근의 지능화된 사이버공격에 대한 대응 체계는 미흡한 실정이다. 따라서 이러한 사항을 개선하기 위해 지능형 사이버공격에 대한 민·관·군 유관 기관 간 즉각적인 정보 공유체계가 필요하다. 그러므로 기관 간 즉각적 정보 공유를 위해 해당 부처의 책임을 명확히 하는 것이 중요하며, 제도적으로는 각 부처의 세부계획 이행여부에 대한 정기검토를 통해 부서 평가 및 예산에 반영함으로써 해당 부처에 책임을 부여하는 방안도 필요하다.

### 5.2. 사이버사령부의 인력 강화

높은 비용과 지속적인 노력이 요구되는 보안인력양성 및 연구개발 등 중장기 과제들을 종합적으로 계획하고 조정할 수 있는 전문적인 능력을 갖춘 독립적인 사이버보안 담당부처의 설립이 필요하다. 구체적으로는 사이버안보 분야 인재 채용을 통한 국방부·각 군 CERT 팀 조직을 강화하고, 각 군 대학 및 국방대 내 사이버안보 전문 인력 양성 과정을 개설하는 방법을 활용할 수 있을 것이다. 국내에서는 이미 사이버국방학과를 설립하고 고급 인력들을 양성하고 있다. 또한 사이버사령관의 계급을 준장에서 소장으로 격상시키고 현재 500명 정도인 사이버사령부 인력을 2배 이상 늘리는 등 사이버 전력강화 의지를 밝힌 바 있다. 북한은 사이버 작전을 담당하는 정찰총국을 김정은이 직접 통제하고 있으며, 해킹과 사이버전 임무를 전담하는 인력만 해도 3,000명 이상이다. 또한 사이버전 전문 인력을 양성하기 위해 최고의 인력을 뽑아 최고의 교육 환경과 대우를 제공함으로써 높은 수준의 전문성과 실력을 보장하고 있다. 북한의 이러한 사이버 전력에 맞서 대내외적으로 사이버 국방 강화 의지를 보이고 실질적인 권한과 능력을 갖추기 위해선 위로는 사이버사령관을 중대장급으로 격상시키고, 아래로는 사이버국방병과를 신설하며 체계적인 사이버 국방인력 양성 로드맵과 교육 프로그램을 통해 인원을 확충하고 전문성을 강화해야 한다. 사이버 국방의 미래를 위해 우선 이들에게 최고 수준의 교육훈련과 최고 수준의 대우를 할 수 있도록 정책적 지원을 해야 한다. 장교들 중 사관학교 및 민간대학교 등에서 정보기술을 전공하였거나, 국방대학교에서 정보기술을 전공한 인원들을 일정 기간 교육 후 관련 부서에 근무토록 하는 것도 하나의 방법이다.

### 5.3. 사이버범죄의 국제화에 대한 적극적 대처

인터넷은 정부기능, 정보, 경제 등 다양한 분야에 영향을 끼쳤으며, 정치적 도구로도 이용되고 있다. 이러한 인터넷이 주는 혜택의 이면에는 인터넷은 전쟁의 무기로 사용될 수 있으며, 사이버공간은 전장이 될 수 있다는 위험성이 있다. 사이버스페이스의 특성대로 국경을 넘은 통신이 가능해지면서 사이버범죄도 국제화되고 있다. 또한 현재 정보 전쟁 시스템을 발전시키고 있는 나

라들은 전 세계 120개국에 이른다. 국제법에서 '공격'이라는 개념의 정확한 기준은 없으며, 실제로 사이버공격에 대한 기준은 사람이나 피해자의 재산이 침해되었는지 여부를 기준으로 결정된다. 그러나 2007년 거대한 규모의 사이버공격이 에스토니아 정부에 가해진 이래로 전기통신 사회기반시설·은행·온라인 미디어들은 사이버공격에 대한 인식을 대폭 수정하기 시작했다. 사이버범죄가 나타나기 시작하면서 OECD와 같은 국제기구들은 '컴퓨터 관련 범죄'를 '전자 프로세스 또는 데이터의 전파와 관련된 불법, 비윤리적 행위 또는 인정되지 않는 행위'로 정의했다. 그러나 사이버 범죄의 개념은 계속 확장되고 있고, 사이버 범죄를 넘어서 새로운 공격 상황에 대한 대처를 위해 정책과 법이 정비되어야 한다. 세계 각국은 이미 사이버 전쟁 능력을 발전시키고 있지만 사이버 안보에 대한 법제는 사이버공격에 대해 이미 한계를 드러내고 있다. 현재의 국제 규범을 사이버 전쟁에 직접 적용하기에는 직권의 문제, 사법적 문제 그리고 무력행사의 문제 등 3가지의 문제를 해결해야 한다. 하지만 이러한 문제는 근본적인 해결이 필요하기 때문에 사이버 전쟁의 경우에는 현존하는 체제와 국제법 구조로는 적절히 다룰 수 없다. 따라서 국제법이 직면하고 있는 현재의 이러한 어려움에 대한 관심을 높일 방안을 찾아야 하고, 사후약방문이 되지 않도록 국제적 차원의 조속한 조율 및 협상과 대안을 제시하여야 한다. 전자정보 네트워크가 확장되고, 국방과 산업 인프라 기반 시설들이 전자정보 네트워크에 의존하면서 사이버공격의 빈도와 규모는 점차 커질 가능성이 크다. 따라서 향후 UN 헌장과 법제는 새로운 사이버 범죄를 포괄할 수 있도록 사이버 범죄에 대한 정의를 진화시켜 나갈 것이다. 하지만 범죄에 대한 기준이 각국의 사회적 기준에 따라 내용과 적용환경이 다르므로 통합적인 형태의 국제조약은 불가능할 수 있다. 그러므로 향후 우리는 이러한 국제법적 한계의 문제를 고려하여 국내법을 정비하는 것이 필요하다.

### 5.4. 정보화책임관을 통한 사이버안보 업무체계 확립

사이버안보 위협이 일상화된 상황에서 국가적으로 중요한 의사결정과 대응이 신속히 이루어지기 위해서는 청와대에 정보화책임관을 두어 대통령에게 일상적으로 사이버안보 현황에 대해 보고하고 조치할 수 있는 체계를 갖출 필요가 있다. 사이버안보문제가 국가안보에서 차지하는 비중이 증대되고, 북한의 사이버공격 대처를 강화하기 위해 정보화책임관을 신설해야 한다. 정보화책임관은 사이버안보, 정보보호 분야에 대해 대통령을 보좌한다. 사이버범죄, 사이버테러와 같은 사이버전에 대해 국가의 이익을 보호하고 국가의 안보를 강화하는 역할을 수행한다. 향후 사이버공격에 대해 신속하고 체계적으로 대응하기 위해서는 해당 직무가 꼭 필요하며, 정보화책임관은 사이버공간 국제협력을 주도하고 기관간 역할을 조정하는 등 시너지 효과를 낼 수 있다.

## Ⅵ. 결 론

이상에서는 사이버 안보환경의 변화에 기초하여 다양한 정보보안침해사고의 유형과 내용을 분석하고, 국가안전을 수호하기 위한 침해 예방과 신속한 대응을 위한 법제 정비방안을 살펴보았다. 또한 구체적 개선안을 검토하여 국가의 사이버위기관리의 근본 체계와 정보통신기술의 발전 및 이용확산 추이를 감안한 국가정보보안 대책 마련을 위한 종합적인 정책방안도 제시하였다. 사이버공간에 대한 접근과 이용에는 경제적·기술적 제약이 없어야 하며, 개방적이고(open), 상호운용이 가능하며(interoperable), 안전하고(secure), 신뢰할 만한(reliable) 정보와 통신 기초시설을 증진시키기 위한 노력을 아끼지 말아야 할 것이다. 이렇게 정부는 정보화의 실현과 발전을 위해 지속적으로 노력해야 하며, 정보화로 인해 수많은 양의 디지털 데이터가 계속 팽창하면서 국민들에게 다양한 편익을 제공할 수 있다. 반면, 개인과 기관을 대상으로 한 사이버테러의 위험 역시 증가되고 있다. 최근에는 사이버테러에 의한 공격은 전방위적으로 진행되고 있어 국민생활 전반을 위협하고 있으며, 이에 대한 국민적 불안이 매우 높아지고 있다. 이러한 문제점을 해결하고 사이버 안보에 대한 위협으로부터 국민을 보호하기 위해서는 책임감과 국가수호에 대한 의지를 가지고 사이버안보 문제를 신속하고 합리적으로 해결하는 중심역할을 할 수 있는 기관과 우수한 인재가 필요하다. 따라서 눈에 보이지 않는 수많은 해커와 위협요소들에 대항할 수 있는 사이버안보 분야의 엘리트 인재들을 육성하는 정책이 지속적으로 시행되어야 한다. 향후에는 사이버안보 전문기술인력의 양성, 사이버안보 산업 육성의 근간으로서의 대학과 기업 간의 유대 조성,

사이버안보산업 육성, 사이버 안보코디네이터 역할 강화, 해당 부처의 책임강화 등의 정책을 통해 우리나라의 사이버 침해사고 대응 역량을 획기적으로 개선해 나가야 할 것이다. 사이버 안보 문제는 완벽한 문제해결이나 대응이 거의 불가능할 수도 있지만, 국민들의 지속적인 관심에 힘 입어 국내외적 협업과 노력을 기울여야 한다는 점을 깊이 명심해야 할 것이다.

## 참 고 문 헌


[1] 김귀남, “국가 사이버전 대비방안 연구”, 정보·보안논문지, 2006년

[2] 김은혜,이재일, “미 오바마 정부의 사이버보안 주요 정책 및 법안”, NET FOCUS, 2011년

[3] 남길현, “사이버테러와 국가안보,”, 국방연구 제45권 제1호, 2002년

[4] 박상돈, 김인중, “사이버안보 추진체계의 제도적 개선과제 연구”, 융합보안논문지, 2013년

[5] 부형욱, “사이버 안보의 주요 이슈와 정책방향”, 국방연구 제56권 제2호, 2013년

[6] 양근원, “사이버테러 대응과 현행 절차법 검토”, 인터넷법연구 제3권 제1호, 2004년

[7] 엄정호, “사이버안보를 위한 능동적 사이버전 억제전략”, 보안공학연구논문지 제10권 제4호, 2013년

[8] 김진, “사이버침해에 대한 효율적인 대응방안 연구”, 석사학위논문, 2011년

[9] 김진항, “포괄안보시대의 한국국가위기관리 시스템 구축에 관한 연구”, 석사학위논문, 2010년

[10] 하옥현, “국가 사이버안보체계 구출 전략”, 석사학위논문, 2005년

[11] 국정원, “국가정보보호백서”, 2013년

[12] 허태회 외, “위기관리이론과 사이버안보 강화방안”, 국방연구 제48권 제1호, 2005년

[13] 허태회 외, “세계 주요 강대국의 정보전 준비와 대응체계”, 국방연구 제49권 제1호, 2006년

[14] 노훈,이재욱 “사이버전의 출현과 영향, 그리고 대응방향”, 국방정책연구 제53호, 2001년

[15] 안종하, “국내 사이버보안 체계 진단 및 정책적 대응방안 연구”, 한국경찰연구, 2013년

[16] 유지용,이강규, “사이버안보 국제협력과 한국의 정책방향”, 주간국방논단 제1471호, 2013년

[17] 윤해성 외, “사이버안전체계 구축에 관한 연구”, 형사정책연구원 연구총서, 2013년

[18] 이강규, “세계 각국의 사이버 안보 전략과 우리의 정책 방향”, 정보통신정책연구 제23권 16호, 2011년

[19] 권장우, “IT 선도국가 도약을 위한 인재양성”, 정보통신산업진흥원, 2011년


## 〈저 자 소 개〉


**안 유 성 (Yoo-seong An)**
정회원

2014년 2월 : 성균관대학교 정보보호학과 석사
관심분야 : 사이버보안, 정보보호