사이버공격 대응 분석을 통한 사이버안보 강화 방안 연구

윤오준* · 배광용* · 김재홍* · 서형준** · 신용태***

요 약

최근 한수원 원전자료 유출, 미국 소니픽쳐스사 해킹 등 사이버위협은 우리나라뿐만 아니라 선진국 모두에게 해결해야 할 큰 현안으로 대두되고 있다. 우리 정부는 그간 대형사고 발생 시마다 종합대책을 수립하여 시행해오고 있으며 사이버안보 강화에 대한 지속적인 투자와 개선 노력으로 과거에 비해 국가·사회 전반의 보안수준이 향상되었으나 여전히 미흡하다. 종합대책이 단기 위주로 그 실효성에 한계가 노출되었고 금융사기 등 사이버범죄가 교묘해지고 악성코드와 공격기술은 새로운 기법을 동원하여 지속적으로 출현하고 있기 때문이다. 또한 북한은 6,800여명의 해킹조직을 운영하면서 기반시설까지 해킹하여 심리전을 구사하고 있어 우리의 사이버안보에 직접적인 위협이 되고 있다. 본 논문에서는 2009년 이후 주요 사이버공격시 대두된 문제점 등 사고 사례를 분석해보고 그에 따른 종합대책의 수립·이행과정을 평가하여 궁극적으로는 우리나라의 사이버안보 관리체계 전반에 대한 수준을 제고하기 위한 방안을 제시하고자 한다.

A Study on Measures for Strengthening Cybersecurity through Analysis of Cyberattack Response

Yoon Oh Jun* · Bae Kwang Yong* · Kim Jae Hong* · Seo Hyung Jun** · Shin Yong Tae***

ABSTRACT

Recent cyberthreats are emerging as big issues that need to be addressed to both developed countries and South Korea. Our government has implemented and established comprehensive measures whenever major incidents were happened. It is still insufficient, even though the national and social level of cybersecurity are improved with continuous investments and efforts to strengthen the country than in the past. Comprehensive measures have been exposed to limit the effectiveness because they are focused on short-term measures. In this paper, we try to analyze the problems of incidents and assess the implementation process of establishing comprehensive measures in order to suggest ways ultimately to improve the country's overall level of cybersecurity.

Key words : Cybersecurity, Comprehensive measures, Cyberthreat, Cyberattack

접수일(2015년 5월 31일), 게재확정일(2015년 6월 15일)

* 숭실대학교 IT정책경영학과
** 한국전자통신연구원 부설연구소(책임저자)
*** 숭실대학교 컴퓨터학부(교신저자)

1. 서 론

우리나라는 유엔의 전자정부발전지수 1위 등 정보화 진전은 세계 어느 나라에 뒤지지 않는 선진국 수준에 도달해 있다. 반면 이를 악용하여 개인정보 등 중요자료를 유출하거나 금융 등 기간망에 침투하여 핵심기능을 마비시키는 등 각종 사이버공격이 2009년 이후 격년 단위로 자주 발생하고 있다. 대표적인 사례로는 7.7 및 3.4 DDoS공격, 농협 전산망 사이버테러, 3.20 방송 및 금융 사이버테러와 한수원 해킹 등이 있다. 최근 미국의 소니픽쳐스사, 영국의 BBC 해킹 등으로 판단해 보았을 때 정보유출이나 해킹 등 사이버 위협 문제는 우리나라 뿐 만아니라 선진국 모두에게 해결해야 할 큰 현안으로 대두되고 있다.

이에 정부에서는 그간 우리의 예방적 보안활동과 사고대응 과정에서의 미비한 점을 개선하기 위해 대형사고 발생 시마다 매번 종합적인 대책을 수립하여 시행해오고 있다. 또한 2015년 1월 외교안보부처 업무보고에서는 미사일, 핵, 테러 등 전통적인 안보사안과 더불어 사이버안보에 대한 중요성이 제기되고 정부차원의 실행의지도 표출되었다. 이를 계기로 대통령 안보특별보좌관이 신설되어 임명되었고, 국가안보실에 사이버안보비서관실이 설치되어 운영되면서 명실상부하게 사이버안보 컨트롤타워 역할을 수행하고 있다.

그러나 그간 정부의 사이버안보 강화에 대한 지속적인 투자와 개선 노력, 일련의 대응활동으로 과거에 비해 국가·사회 전반의 보안수준이 향상되었다고는 하나 국민들의 불안은 가시지 않고 있다. 우리나라는 사이버공격으로 인한 금전적·물질적·정신적 피해가 매년 증가하는 등 세계에서 가장 위험한 사이버공간에 존재함에도 정부의 종합대책은 단기적 위주의 대책으로 그 실효성에 한계가 노출되었고 민간영역은 사이버보안에 대한 인식과 투자가 매우 미흡한 실정이다. 금융사기 등 사이버범죄가 교묘해지고 악성코드와 공격기술은 새로운 기법을 동원하여 지속적으로 출현하고 있다. 또한 북한은 당 및 군 산하에 6개의 해킹조직으로 1,700여명의 핵심해커와 이들을 지원하는 5,100여명의 보조인력을 운영하면서 점차 기반시설까지 해킹하여 심리전을 구사하고 있어 우리의 사이버안보에 직접적인 위협이 되고 있다.

이에 본 논문에서는 2009년 이후 우리나라에서 발생한 주요 사이버공격 현황, 대두된 문제점 등 사고사례를 면밀히 분석해보고 그에 따른 정부의 종합대책 수립 이행과정을 평가하여 궁극적으로는 우리나라의 사이버안보 관리체계 전반에 대한 수준을 제고하기 위한 방안을 제시하고자 한다.

2. 관련 연구

2.1 국내 주요 사이버공격 사례 분석

국내에서 발생한 주요 사이버공격으로는 2009년 7.7DDoS공격, 2011년 3.4DDoS공격과 농협 전산망 테러, 2013년 3.20 방송·금융 사이버테러와 6.25사이버공격, 2014년 한수원 해킹 등이 있다. 이들 사이버공격의 유형을 보면 DDoS공격, APT(Advanced Persistent Threat)라는 지능형지속위협과 사이버심리전으로 크게 분류할 수 있다. 각 사고별 공격유형·대상, 피해규모(피해액) 등을 <표 1>과 같이 분석하였다.

<표 1> 주요 사이버공격 사례 분석

구 분	공격 유형	공격대상	피해규모 (피해액)
7.7DDoS	DDoS	국내외 36개 기관 웹서버	11만대 감염 PC 1,460대 파괴 (363~544억원)
3.4DDoS	DDoS	국내 40개 기관 웹서버	11만대 감염 PC 750대 파괴
농협 해킹	APT	내부 전산망 서버	서버 270대 파괴 (197억원)
3.20 사이버테러	APT	방송금융 6개사 PC / 서버	PC / 서버 48,800대 파괴 (8,672억원)
6.25 사이버공격	APT / DDoS	국내 69개 정부 기관, 언론사 PC / 서버	PC / 서버 150대 파괴
한수원 해킹	APT / 심리전	한수원 및 협력사 PC	PC 5대 파괴 문건 94건 공개

2.1.1 7.7DDoS공격

7.7DDoS공격은 2009년 7월7일부터 7월9일까지 DDoS공격으로 청와대 등 국내외 주요 정부기관과 민간기업 사이트가 마비된 사건이다. 대두된 문제점으로

첫째, 정부 부처별로 보도자료를 배포하여 혼선을 초래하였고 민-관간에도 악성코드 등 관련정보 공유가 부족하였으며 좀비PC의 신속한 확보체계 부재 등 DDoS 대응능력이 미흡이었다. 둘째, 사이버위협이 점차 현실적으로 다가오고 그 대응에 대한 중요성이 부각되면서 MB정부 출범이후 방통위·행안부·경찰 등 주요기관간 업무 충돌이 야기되었으며 이로 인해 기관간 유기적 협력이 부족하여 업무 컨트롤타워 부재 논란이 발생하였다.

2.1.2 3.4DDoS 공격 및 농협 전산망 테러

3.4DDoS공격은 2011년 3월4일부터 3월7일까지 발생한 DDoS공격으로 청와대·포털·금융사 등 국내 중요 사이트를 대상으로 진행되었으나 지난 7.7DDoS 공격에 대한 학습효과로 민-관이 긴밀한 협력을 통해 성공적으로 대응한 사례였다. 주요 문제점으로 웹하드 설치프로그램 변조를 통해 악성코드를 유포하는 방식에 대한 대응책이 미흡하였고 정부기관간 위기대응 역량이 분산되어 사이버위협에 효율적으로 대응하는데 한계가 있었다.

3.4DDoS공격이 발생한 후 한 달여 후인 4월12일에 7개월간 APT 공격으로 농협 내부 전산망 시스템 270대가 파괴되어 4월30일까지 농협 업무 일부가 마비된 사건이 발생했다. 이 사건은 단일기업 내부망에서 발생한 APT 침해사고와 관련하여 외주협력업체 보안관리에 대한 문제가 대두되었고, 금융기관 등 민간기업에 대한 보안관제를 실시하지 않아 사이버공격을 탐지하고 차단하는데 미흡하였다.

2.1.3 3.20 및 6.25 사이버테러

2013년 3월20일 KBS·MBC·YTN 등 국내 3개 방송사와 농협·신한은행·제주은행 등 금융권의 PC, 서버 등 시스템이 악성코드에 감염되어 48,800대가 파괴된 사건으로 그 피해액이 무려 8,672억원에 달하는 것으로 추정되었다[9]. 대두된 문제점으로 방송·금융기관은 개인정보 유출 우려와 신고의무가 없어 사고에 대한 상황전파가 지연되었고 사고조사를 위한 업무협조도 기피하였다. 또한 유관부처와 청와대간 직접적인 보고체계가 불명확하여 정부기관 내에서도 업무 혼선을 야기하였다.

3.20사이버테러 이후 대책을 수립하는 과정에서 3개월 후인 6월25일에 언론사 전산망 파괴, 청와대 등 정부기관 홈페이지 변조, 정부통합전산센터 DNS 대상 DDoS 공격으로 사회적 혼란이 야기된 사건이 발생했다. 대두된 문제점으로 첫째, 해커그룹 어나니머스가 6월25일 북한 전산망 공격을 예고하고 있는 상황에서 발생 가능한 위기대응에 미흡하였다는 것이다. 둘째, 3.4DDoS공격, 농협 전산망테러 계기로 수립한 기존의 '국가 사이버안보 마스터플랜'에서는 국정원이 대응을 총괄하도록 되어 있었으나, 전 부처를 아우르는 컨트롤타워의 필요성이 지속 대두되었다. 셋째, 이번 대응과정에서도 민·관·군 유관기관간 원활한 사이버위협 정보 공유체계가 미흡하였다.

2.1.4 한수원 해킹 공격

2014년 12월9일부터 12월12일 사이에 한수원 직원을 대상으로 악성코드가 포함된 이메일을 발송하여 시스템 파괴를 시도하였고 사전에 확보한 한수원의 원전관련 자료를 미끼로 협박을 한 최초의 사이버심리전 형태의 사이버공격이 발생하였다. 대두된 문제점으로 첫째, 주요 정보통신 기반시설 해킹사고에 대해서 사고대응 및 분석능력이 미흡하였다. 둘째, 해외 SNS 등을 통해 유출자료 공개·협박 등이 이루어지고 있는 상황에서 사이버심리전에 신속하게 대응하기 위한 체계가 미흡하였다.

2.2 사이버공격 계기로 수립한 종합대책

위에서 제시한 7.7DDoS공격, 3.4DDoS공격과 농협 전산망 사이버테러, 3.20사이버테러와 6.25사이버공격, 한수원 해킹 사건이후 정부에서는 대응과정에서의 문제점을 인식하고 이를 개선하기 위해 4차례에 걸쳐 국가 차원의 종합적인 대책을 수립하여 시행하게 되었으며 그 주요내용은 <표 2>와 같다.

<표 2> 주요 사이버공격별 정부의 종합대책

구 분	정부 대책 및 핵심내용
7.7DDoS	□ 범정부 사이버위기 종합대책 - 대국민 언론창구를 방통위로 일원화 - DDoS 대피소 구축 및 대응장비 설치

3.4DDoS/ 농협 테러	□ 국가 사이버안보 마스터플랜 - 민관군 사이버위협 합동대응팀 구축, 운영 - 업무망-인터넷망 분리 및 외주업체 보안강화
3.20/6.25 사이버테러	□ 국가 사이버안보 종합대책 - 청와대 중심 사이버안보 컨트롤타워 정립 (평시:미래전략수석, 위기시:국가안보실) - 상황발생시 청와대 및 국정원 동시 전파
한수원 해킹	□ 국가 사이버안보 태세 강화 대책 - 국가안보실로 사이버안보 컨트롤타워 일원화 (사이버안보비서관실 설치) - 주요 정보통신 기반시설 보호체계 강화

2.2.1 범정부 사이버위기 종합대책

7.7DDoS공격 사고 수습이후 2009년 9월에 '범정부 사이버위기 종합대책'이 발표되었는데 대책 일환으로 사고발생시 대국민 언론창구를 방통위로 일원화 하였고 정부에서 긴급 예산을 확보하여 주요 부처에 DDoS 대응장비를 설치하였다. 한국인터넷진흥원(KISA)에 중소기업을 위한 DDoS 대피소도 구축하게 되었으며 국민들의 좀비 PC를 치료하기 위한 사이버치료체계도 준비하기 시작하였다[3].

2.2.2 국가 사이버안보 마스터플랜

3.4DDoS공격, 농협 전산망테러 사고를 계기로 범정부 차원에서는 '국가 사이버안보 마스터플랜'을 발표하여 대응기구를 단일화하고 유관기관의 역할을 재정립하였다. 국가사이버안전센터에 민·관의 참여를 확대하여 사이버위협 합동대응팀을 구축하여 종합판단, 위협분석, 합동조사 등의 임무를 부여하고 2단계로 대응본부 신설을 추진키로 하였다. 민간분야의 사이버공격 탐지, 차단을 위해 웹하드·P2P 등을 대상으로 악성코드 유포 탐지체계를 마련하고 민간기업 대상 정보보호 관리체계(ISMS) 인증제도도 확대하며 외주협력업체의 보안관리를 강화하기 위해 기관 출입시 장비 반출입 통제 강화 및 입찰에서 용역사업 종료 시까지 단계별 보안대책을 수립, 시행토록 하였다[4]. 또한 금융위에서 업무망과 인터넷 분리를 철저히 이행하고 보험·카드사 등 여타 금융기관 대상 보안관제를 확대하는 등 금융회사 IT보안 강화대책을 발표하였다.

2.2.3 국가 사이버안보 종합대책

3.20 방송·금융 사이버테러와 6.25사이버공격 사고 이후 '국가 사이버안보 종합대책'이 마련되어 발표되었다. 컨트롤타워 변경이 이루어졌는데 청와대(평시에는 미래전략수석실, 위기시에는 국가안보실)를 컨트롤타워로 하고 국정원이 예방대책 수립, 사이버공격 대응 및 조사, 위협정보 수집·분석·배포 등 실무를 총괄하는 대응체계를 재정립하였다. 상황 발생시 국가안보실(위기관리센터)과 국정원에 동시 전파토록 하고 '주의' 경보 이상시 사이버위기 대책본부를 운영토록 하였다. 또한 청와대 홈페이지 변조 재발 방지를 위해 보안을 한층 강화한 홈페이지를 재구축 하였으며 주요 정보통신 기반시설의 지정을 확대하고 정보보호 인력을 점진적으로 양성하며 정보보호 산업의 경쟁력을 강화하기로 하였다[5].

2.2.4 국가 사이버안보 태세 강화 대책

한수원 해킹 사고이후 마련된 대책으로 범정부 차원에서 '국가 사이버안보 태세 역량강화 대책'이 발표되었다. 주요 내용으로 국가안보실로 사이버안보 컨트롤타워 기능을 통합하고 중앙부처·지자체 등에 사이버보안 전담조직을 확충해 나가며 주요국과 국제공조를 확대하고 사이버안보 관련 법령의 정비를 추진키로 하였다. 또한 주요기반시설 지정 확대, 보호대책 강화 등 관리체계를 개선키로 하였다[10].

2.3 사이버안보 강화 주요 동향

2.3.1 미국

미국은 「국토안보법(HSA)」에 의거 국토안보부(DHS)가 연방정부의 국가기반 보호 및 관련정책을 담당토록 하고 있다. 사이버안보도 국가기반으로서 보호토록 역할과 책임을 부여하여 공공 대중의 인식제고 뿐만 아니라 책임부서를 명확히 함으로써 사이버안보 업무에 관한 역할분담 및 업무 효율성을 높이고 있다. 또한 오바마 대통령은 백악관에 사이버안보 조정관(Cybersecurity Coordinator)을 두고 평시에는 관계부처 및 민간영역과의 협력과 조율을 담당하는 중요한 역할을 수행토록 하고 대규모 침해사고 발생 시에는 총괄적인 대응조정 등 지휘관 역할을 담당토록 하고

있어 미국에서 사이버테러 대응체계의 실질적인 컨트롤타워 역할을 수행한다고 할 수 있다[1].

또한 2009년 10월 국토안보부(DHS) 산하에 국가사이버안보 및 통신통합센터(NCCIC, National Cybersecurity and Communications Integration Center)를 설치하고 미국 정부를 상대로 한 각종 사이버위협 정보를 수집하여 대응하며 민간 및 공공의 기반시설 보호를 위해 위협정보를 신속하게 공유하고 있다. NCCIC에는 인터넷 침해사고에 대한 대응 및 예방업무를 수행하는 침해사고대응팀(US-CERT)과 국가 주요 기반시설의 산업제어시스템 침해사고에 대한 대응 및 예방업무를 수행하는 산업제어시스템 침해사고대응팀(ICS-CERT)을 운영하고 있다.

미국 소니 영화사가 김정은 암살을 다룬 영화 <더 인터뷰> 개봉을 앞두고 2014년 11월 '평화의 수호자'라는 해커조직으로부터 해킹공격을 받은 사건이 발생했는데 연방수사국(FBI)은 12월 해킹공격에 사용된 데이터 삭제용 악성코드가 과거 북한의 소행으로 의심됐던 해킹사건에 활용됐던 것들과 유사하고, 공격에 사용된 악성코드에서 북한 IP 주소의 흔적이 발견됐다는 점 등을 근거로 해킹 배후로 북한을 지목하였다. 이에 오바마 대통령은 소니를 해킹한 북한에 적절한 장소와 시간, 방법을 선택해 비례적 대응에 나설 것이라며 강도 높은 응징 조치는 물론, 나아가 북한을 테러지원국으로 재지정하는 방안도 검토하겠다고 밝혔다. 그리고 2015년 1월 대북제재를 강화하는 내용을 담은 행정명령을 발동하였다.

한·미 외교장관간 회담차 방한한 케리 미 국무부 장관은 2015년 5월18일 한 강연회에서 최근 미국을 겨냥해 사이버공격을 감행한 북한을 '사이버 불량행위자'로 지목하며 어느 국가도 온라인에서의 해킹 등을 통해 다른 나라의 핵심적인 인프라 산업에 피해를 주거나 산업활동을 방해해서는 안되며 사이버공간에서의 공격 행위는 절대로 용납할 수 없다고 하면서 국제사회가 사이버공간에서의 불량행위에 공동으로 대처해야 한다고 주장하였다.

2.3.2 영국

영국은 사이버공간에서 증대되고 있는 위협으로부터 자국민들을 보호하기 위해 2009년 6월 영국 최초로 사이버안보 전략을 발표하면서 사이버범죄에 대한 인식 확대와 민간 대응능력 제고 등을 목표로 제시하였다. 하지만 국가기반시설을 위협하는 사이버공격이 계속 증가하고 ICT 기술발전과 함께 사이버범죄도 증가하면서 2년 뒤인 2011년 11월에 새로운 사이버안보 전략을 수립하였다. 주요 목표는 사이버범죄 억제 및 안전한 사이버공간 구현, 사이버공격에 대한 복원력 강화와 사이버상의 권익보호, 사이버보안 지식·기술·능력 구축 등이다. 2013년 12월에는 사이버안보 전략 추진과정 검토와 함께 향후 전략 추진방향을 담고 있는 '국가 사이버안보 전략 계획'을 발표하였다[8].

2.3.3 북대서양조약기구(NATO)

2013년 3월 NATO는 에스토니아의 탈린에 위치한 나토 산하 사이버방어협력센터(CCDCOE)의 총괄 아래 20여명의 국제법 전문가들이 3년에 걸쳐 탈린매뉴얼을 완성하였다. 사이버테러에 관한 조항들을 성문화한 최초의 사이버교전 수칙으로 구속력은 없으나 사이버교전에서 국제적인 가이드라인 역할을 한다. 이 매뉴얼은 사이버테러의 심각성이 대두되자 사이버교전에서 최소한의 인도적 교전 규범이 필요하다는 인식에서 마련되었다. 이 수칙은 무장공격에 상응하는 사이버공격을 받은 국가는 자기방어권 행사 가능, 사이버공격의 피해 국가가 다수일 경우에는 집단적 자기방어권 행사 가능, 사이버공격에 직접적으로 가담한 민간인은 국제법상 공격으로부터 보호받지 못한다 등 총 95개의 사이버교전 수칙을 담고 있다.

3. 우리나라의 사이버안보 현주소

3.1 중장기적인 사이버안보 전략의 부재

위 사고사례 분석에서 보듯 우리나라는 북한의 사이버공격 등 계기시마다 사이버위기 또는 사이버안보에 관한 종합대책을 마련하여 추진해 왔는데 이는 대부분이 실행과제 중심의 중단기 계획에 불과하였다. 국가차원의 장기적이고 체계적인 사이버안보업무 수행을 위해서는 국가의 장기 비전과 목표 그리고 정책방향을 제시할 수 있는 사이버안보 전략의 수립이 필

요하다. 그러나 우리나라의 경우 그 필요성에 대해서는 꾸준히 제기되어 왔으나 현재까지도 사이버분야에 대한 국가차원의 포괄적인 안보전략이 수립되어 있지 않은 실정이다.

3.2 사이버보안 업무평가의 수행체계 미비

국가·공공기관의 자체 보안활동에 대한 이행여부 점검을 위해 '사이버보안 업무평가' 제도가 시행되고 있으나 여러 문제점을 내포하고 있는데 첫째, 「정부업무평가기본법」 또는 대통령령에 규정이 없어 법적 근거가 미흡한 실정이며 대통령훈령(제316호)인 「국가사이버안전관리규정」에 의하여 수행되고 있다. 또한 행자부의 '0000년 행정관리역량 평가계획', '0000년 지방자치단체 합동평가 실시계획' 및 기재부의 '공공기관 경영평가편람' 등에 의거 위임 수행일 뿐이다. 정부업무평가는 법률 또는 대통령령에 근거하지 아니하고는 다른 평가대상기관의 정책 등에 대하여 평가를 하여서는 아니된다는 조항(제3조)을 위배하고 있는 것이다. 둘째, 중앙행정기관, 지자체 및 공공기관의 평가에서 사이버보안 항목은 하위 소항목에 불과하고 반영비율 또한 현저히 낮은 편이다. 중앙행정기관은 행정관리역량-정보화분야, 지자체 합동평가는 중점과제분야, 공공기관은 경영관리-전략기획지표의 소항목에 포함되어 있다.

3.3 대응기관간 신속한 정보공유체계 미흡

사이버위협은 공공기관 및 민간기업 등 영역을 구분하지 않고 시간과 공간의 제약이 없이 동시다발적으로 발생하고 있으므로 위협요인을 조기에 파악하는 것이 중요하고 이를 차단하지 않을 경우 피해가 순식간에 확산될 수 있다. 특히 최근의 사이버테러는 보안관리를 강화하고 있는 공공기관 보다는 상대적으로 허술한 민간영역에서 대부분 발생하고 있으며 공공기관에 대한 위협도 취약한 민간기관을 경유하는 경우가 많아 두 영역간의 즉각적인 사이버위협정보 공유 없이는 공격차단, 피해예방, 긴급복구에 한계가 있을 수밖에 없으므로 대응기관간 위협정보 공유를 통한 공동 대응은 반드시 필요하다. 그러나 여러 차례의 사이버공격에 대한 대응 경험을 계기로 각급기관들이 정보공유의 중요성에 대해서 인식하고 많이 개선하여 왔지만 아직도 실시간으로 신속히 공유할 수 있는 정보시스템 구축 등 체계가 미흡한 상황이다.

4. 사이버안보 수준 제고 방안

위에서 주요 사이버공격 사고별 공격대상, 피해규모 등 사례분석을 통해 수립된 정부 차원의 대책을 고찰하였다. DDoS, APT, 사이버심리전을 통해 국민의 불편 초래, 사회혼란과 국가기능 마비를 획책한 사이버공격을 차단하고 대응하기 위해 민·관·군이 협업하여 국민들의 보안의식 제고에서부터 각급기관 보안시스템 보강, 업무수행체계 정비, 국가핵심 기반시설 보호 강화, 정보보호산업 육성 등 대책들을 시행하여 한층 더 보완된 보안수준을 유지하게 되었다.

그러나 지금까지의 대책들은 사고가 발생한 후 미흡한 사항들에 대한 단기과제 위주로 수립되어 근본적인 보안수준을 제고하기에는 한계가 있을 수밖에 없었다. 우리나라의 사이버안보 수준을 선진국 수준으로 격상시키고 장기적으로 강화하기 위한 국가 차원의 사이버안보 전략 수립, 각급기관 대상 사이버보안 평가의 내실화, 실시간 사이버위협 정보 공유 활성화에 대한 방안을 제시하고자 한다.

4.1 국가 차원의 사이버안보 전략 수립

지난 2014년 7월 국가안보실에서 발표한 '국가안보전략'에는 확고한 국방태세 확립과 미래지향적 방위역량 강화를 위해 범국가적 안보역량 통합을 제시하고 있다. 이를 위해 정부는 국가 사이버안보 전략을 수립하여 국가 차원의 통합 대응체계를 발전시키고 사이버안보 강국으로 도약할 수 있는 기반을 구축코자 한다며 사이버분야의 전문인력을 육성하고 최첨단 기술과 장비를 보강하여 대응능력을 제고하고 또한 우방국들과 사이버안보 협력을 강화하는 등 국제사회와의 다각적인 협력도 지속적으로 확대해 나갈 것이라고 천명했다[7].

우리의 국가 사이버안보 전략에 포함해야 할 내용으로는 첫째, 지금까지 우리나라는 외부로부터의 사이버테러, 정보절취를 위한 악성코드 유포, 사이버심리

전 등 다양한 사이버공격에 대해 일부 유감표명에 거치는 등 억지력 확보에 그다지 적극적으로 대응하지 못했다. 국가 중요시스템이나 국민 편의시설에 대한 심각한 사이버테러에 대해서는 정부차원의 맞대응 내지 공세적 대응역량을 확보해야 하고 이를 위해 대응수단(무기)이나 절차·방법을 마련하여 항시 준비하고 있어야 한다. 둘째, 국제공조를 강화해 나가야 한다. 물리적 공간과는 달리 사이버세상은 국경의 개념이 희박한데다 국경을 초월한 사고발생시 당사국의 협조가 없을 경우 적극적 대응에 한계가 있고 조사진행에도 차질이 발생할 수밖에 없다. 그렇기 때문에 사이버전장의 중심에 서 있는 우리나라로서는 국제사회가 공감할 수 있는 보편타당한 국제규범을 수립하는데 선도적으로 참여해야 하고 사이버우방국과 양자협력 및 국제기구내 다자협력에도 적극적으로 임해야 한다. 셋째, 핵심기반시설에 대한 보호대책도 포함되어야 한다. 고도화·지능화되는 사이버위협에 대비한 국가기능 유지와 국민안전을 확보하기 위해서는 기반시설에 대한 보호조치를 강구하여 생존성과 복원성을 갖추도록 해야 한다.

또한 수립된 전략(안)에 대해서는 미래부, 국방부, 국정원 등 관계부처 및 한국인터넷진흥원, 국방연구원 등 전문기관, 대학교수 및 업체 관계자의 다양한 의견을 수렴하여 반영함으로써 전 국민이 하나가 되는 전략을 마련해야 할 것이다.

4.2 사이버보안 평가의 법적 근거 확보

각급기관 특히 국가·공공기관의 사이버보안 수준을 제고하는데 효과적인 방법 중의 하나는 감독기관이 피감기관을 대상으로 자체 보안대책 이행여부를 객관적으로 점검하고 공정하게 평가에 반영하는 것이다. 이를 개선하기 위한 방안으로는 「정부업무평가기본법시행령」 제8조(평가총괄관련기관)에서 평가의 부문별 총괄 관련 중앙행정기관 즉, 주요정책부문은 국무조정실, 재정사업부문은 기획재정부, 조직·정보화부문은 행정자치부, 인사부문은 인사혁신처로 된 규정을 개정하여 '사이버보안 부문'을 신설하고 주무 중앙행정기관을 평가총괄관련기관으로 지정하면 된다. 또한 중앙행정기관, 지자체 및 공공기관의 평가항목에서 사이버보안 부분을 별도로 분리하고 반영비율 또한 높일 필요가 있다.

4.3 사이버위협정보 실시간 공유시스템 구축

나날이 교묘해지는 사이버공격을 선제적으로 차단하고 대응하기 위해서는 민간과 공공영역이 수집하는 위협정보를 상호간에 실시간으로 공유해야 한다. 먼저, 공공기관에서 수집, 처리되고 있는 위협정보가 민간영역까지 전파되어 유사시 효율적으로 활용될 수 있도록 해야 한다. 또한 반대급부로 민간기관들도 도처에 위치하고 있는 수집처를 가동하면 저인망식으로 다양한 위협정보를 생산해낼 수 있으므로 스스로 공공기관과 공유할 수 있는 체계를 만들어나가야 한다. 이를 위해 우선 관계부처 합동으로 가칭 '민-관 사이버위협정보 공유센터'를 만들어 사이버위협정보를 수집, 종합 분석, 배포 등 역할을 부여하고 운영해나가야 한다. 또한 민간기관과의 정보공유는 그 중요성의 우선순위에 따라 공유대상 수준을 판단하고 기관별 접근권한 차등 설정 등을 통해 순차적으로 시스템을 구축해 나가야 할 것이다. 한편 정보공유센터가 위협정보를 남용하지 않고 업무범위 내에서 건전하게 활용하도록 남용방지에 대한 대책도 마련해야 한다.

5. 결 론

본 논문에서는 우리나라에서 최근 발생한 DDoS공격, 기반시설 전산망 테러 등 주요 사이버공격 사례를 분석해보고 이를 토대로 수립되어 시행된 정부의 종합대책의 실효성에 대해 살펴보았다. 그간의 종합대책으로 국민들의 사이버안보에 대한 인식이 향상되었음은 물론 국가 전반의 보안수준도 증대되었다고 평가되고 있으나 기관별로 대책을 추진하는 과정에서 예산투자 및 인력확보 미흡 등 인프라 부족과 단기적인 성과위주의 대책 시행으로 일부 한계가 있을 수밖에 없었다. 향후 점차 고도화되는 사이버위협에 체계적으로 대응하기 위한 방안으로 국가 차원의 사이버안보 전략 수립, 각급기관에 대한 사이버보안 평가의 내실화, 사이버위협정보 실시간 공유시스템 구축 등을 제시하였다. 이를 통해 평시 예방적인 사이버보안 활동과 위기 발생시 대응활동을 상호 연계함으로써 각급기관의 사이

버보안 수준을 향상시켜 국민생활 전반에 대한 안전한 사이버공간의 구현과 궁극적으로는 국가 차원의 사이버안보를 확고히 하는 토대를 마련할 수 있을 것이다.

참고문헌

[1] 심우민, “최근 전산망 마비사태와 사이버테러 대응체계 개선방안”, 국회입법조사처 이슈와 논점, 제640호, 2013.4.18

[2] 강동원, “사이버테러의 실태와 과제 - 주요 사이버테러 현황과 향후 대응체계를 중심으로”, 2013년도 정기국회 정책자료집, 제1권, 2013.10

[3] 방통위, “정부, 국가사이버위기 종합대책 확정 발표”, 보도자료, 2009.9.14.

[4] 방통위, “정부, 국가 사이버안보 마스터플랜 수립”, 보도자료, 2011.8.8.

[5] 미래부, “정부, 국가 사이버안보 종합대책 수립”, 보도자료, 2013.7.4

[6] 금융위·미래부 등, “금융분야 개인정보 유출 재발방지 종합대책”, 보도자료, 2014.3.10.

[7] 국가안보실, ‘국가안보전략’, 2014.7

[8] 배병환, “영국 사이버보안 전략 분석 및 시사점”, 한국인터넷진흥원 주간기술동향, 2014.10.8

[9] 신영웅 외3, “국가 사이버보안 피해금액 분석과 대안”, 국가정보연구, 제6권, 1호, pp. 129-173, 2013.10.23

[10] 국무조정실 등, “국가 사이버안보 태세 역량 대폭 강화한다”, 보도자료, 2015.3.17

[저 자 소 개]

윤 오 준 (Oh-jun Yoon)

1990년 2월 서울대학교 학사
2013년 8월 건국대학교 정보통신 대학원 석사
2015년 3월 숭실대학교 IT정책경영학과 박사과정

email : ojyoon27271@naver.com

배 광 용 (Kwang-yong Bae)

1990년 2월 숭실대학교 전자공학과 학·석사
2004년 8월 건국대학교 전자정보통신공학과 박사수료
2015년 3월 숭실대학교 IT정책경영학과 박사과정
1990년~현재 KT 수석연구원

email : bky@kt.com

김 재 홍 (Jae-hong Kim)

1999년 2월 고려대학교 학사
2008년 2월 고려대학교 정보보호대학원 석사
2015년 3월 숭실대학교 IT정책경영학과 박사과정

email : jhkim295@naver.com

서 형 준 (Hyung-jun Seo)

1997년 2월 광운대학교 컴퓨터공학과 학·석사
2015년 2월 연세대학교 컴퓨터과학과 박사
2006년~현재 한국전자통신연구원 부설연구소 선임연구원

email : hjseo@ensec.re.kr

신 용 태 (Yong-tae Shin)

1985년 2월 한양대학교 학사
1994년 2월 美아이오아대학교대학원 컴퓨터공학과 석·박사
1994년 美미시간주립대 교수
1995년~현재 숭실대학교 컴퓨터학부 교수

email : shin@ssu.ac.kr