북한 사이버공격에 대한 대응방안에 관한 연구

정영도* · 정기석**

요 약

북한이 우리 사회의 취약한 전산망에 대한 충분한 사이버 공격능력을 갖추고 있어 다양한 대규모의 사이버 공격을 시도할 것으로 예상된다. 북한의 사이버전 수준은 세계 최고수준으로 알려져 있다. 사이버 요원의 수도 지속적으로 증가하고 있다. 최근 북한의 사이버공격은 수법과 대상을 가리지 않는 전방위적으로 행해지고 있다. 그러나 지금까지의 북한 사이버공격은 실질적인 공격이라기보다는 탐색의 성격이 강하다. 남한이 얼마나 빨리 문제를 발견하고 복구하는지를 알아보기 위한 목적이었다고 볼 수 있다. 하지만 앞으로는 막대한 실질적 피해를 주는 사이버공격을 자행할 개연성이 높다. 주요 교통·금융·에너지시설 등의 국가기반시설에 대한 공격이 발생할 경우 그 피해규모는 상상을 초월할 것이므로 이에 대한 대책이 필요하다. 따라서 본 논문에서는 최근 북한 사이버공격의 특징을 살펴보고 대응 방안으로 사이버테러 방지법제정, 대응모의훈련실시, 민관협력체제 구축, 사이버보안 인프라 확대 등을 제시하고자 한다.

A Study on Countermeasures against North Korea's Cyber Attack

Jung Yeong Do* · Jeong Gi Seog**

ABSTRACT

As North Korea has a sufficient ability to attack our society's vulnerable computer network, various large-scale cyber attacks are expected to be tried. North Korea's cyber military strength is known a world-class level. The number of its cyber agents is increasing consistently. Recently North Korea's cyber attack has been made regardless of trick and target. But up to now North Korea's cyber attack is more of an exploration than a real attack. Its purpose was to check how fast Korea found a problem and recovered from it. In future, cyber attack that damages substantially is highly probable. In case of an attack against national infrastructure like traffic, financial and energy services, the extent of the damage will be great beyond imagination. In this paper, characteristics of recent North Korea's cyber attack is addressed in depth and countermeasures such as the enactment of cyber terror prevention law, simulation training enforcement, private and public cooperation system construction, cyber security infrastructure expansion, etc. are proposed.

Key words : North Korea, Cyber Attack, Countermeasures

접수일(2016년9월30일), 게재확정일(2016년10월18일)

* 유원대학교 정보통신보안학과
** 유원대학교 정보통신보안학과(교신저자)

1. 서 론

북한이 우리 사회의 취약한 전산망에 대한 충분한 사이버 공격능력을 갖추고 있어 다양한 대규모의 사이버공격을 시도할 것으로 예상된다. 북한은 수차례 우리사회 기간망들에 대한 공격을 통해 우리의 취약점을 속속들이 파악해 왔다. 사이버 테러를 자행할 때마다 공격목표를 바꾸고 기술적으로 다양한 기능을 추가하는 등 점점 더 정교해지고 있다.

북한의 사이버공격은 1998년 창설된 정찰총국이 총괄 하고 있으며 사이버요원은 6,000여명에 달하는 것으로 알려져 있다. 김정은 시대 들어서 사이버전력의 비중은 더욱 증가하여 사이버전을 주도하던 정찰총국 산하 전자정찰국과는 별도로 전력사이버사령부가 창설된 것으로 알려지고 있다. 이에 따라 사이버전 인력도 갈수록 증가할 것으로 보인다. 북한은 2009년 7·7 디도스(DDoS.분산서비스거부) 대란, 2011년 3·4 디도스 공격과 농협전산망 마비, 2012년 중앙일보 해킹에 이어 2013년 3월 20일 KBS 등 방송시설과 농협·신한은행 등 금융시설에 대한 공격을 자행했다. 최근에는 정부 외교·안보라인 공무원에 대한 스마트폰 해킹, 이메일 해킹 등 정부 주요인사를 타겟으로 정보를 탈취하려는 시도가 있었고, 또한 민간기업인 인터파크를 해킹해 개인정보를 유출하고 국민생활과 밀접한 보건·산업 시설에 대한 사이버공격을 하는 등 수법과 대상을 가리지 않는 전방위적인 공격이 행해지고 있다.

그러나 지금까지의 북한 사이버공격은 실질적인 공격이라기보다는 탐색의 성격이 강하다. 남한이 얼마나 빨리 문제를 발견하고 복구하는지를 알아보기 위한 목적이었다고 볼 수 있다. 하지만 앞으로는 막대한 실질적 피해를 주는 사이버공격을 자행할 개연성이 높다. 코레일과 같은 대중교통시설, 수차례 시도되었던 금융전산망과 한국수력원자력과 같은 주요 교통·금융·에너지시설 등 국가기간시설에 대한 공격이 발생할 경우 그 피해규모는 상상을 초월할 것이므로 이에 대한 대책이 필요하다. 따라서 본 논문에서는 최근 북한 사이버공격의 특징을 살펴보고 사이버공격에 대응할 수 있는 방안을 제시하고자 한다.

2. 북한 사이버공격 현황 및 특징

2.1 북한 사이버전력

북한의 사이버공격은 정찰총국이 전담하고 있는 것으로 알려져 있다. 1998년 창설된 정찰총국은 간첩 양성, 요인 암살, 테러, 사이버공격 등을 수행하는 대남 도발 총괄 조직이다. 정찰총국의 사이버 공작을 전담하는 부서는 110연구소로 종래 121소(일명 기술정찰조)와 100연구소를 통합한 부서다. 이 부서는 2009년 7·7 사이버 대란, 2011년 3·3 디도스 공격 및 농협 전산망 무력화, 2013년 3·20 사이버공격과 6·25 사이버공격, 2014년 한국수력원자력 해킹, 2016년 청와대 해킹메일 발송, 외교·안보라인 휴대폰 해킹 등을 자행한 것으로 알려져 있다[1].

김정은 시대 들어서 사이버전력의 비중은 더욱 증가한 것으로 알려지고 있다. 2012년 8월 김정은 위원장 지시로 기존의 사이버전을 주도하던 정찰총국 산하 전자정찰국과는 별도로 전력사이버사령부가 창설된 것으로 알려지고 있다. 이에 따라 사이버전 인력도 갈수록 증가하고 있다. 지난 2013년 당시 남재준 한국 국가정보원원장은 북한이 7개 해킹조직에 1,700여 명의 요원, 4,200여 명의 사이버전 지원조직을 갖추고 있다고 밝힌 바 있고 최근 한국 국방부가 자체 발간한 자료에는 북한의 사이버 요원이 6,000여명에 이르는 것으로 나타나 있다. 북한의 사이버 요원들은 어려서부터 컴퓨터 집중 교육을 받아온 사람들로 알려졌다. 이들은 주로 평양의 과학영재학교인 금성 1·2 중학교에서부터 컴퓨터 집중교육을 받는다. 그 뒤 미림대학이라고 불리는 총참모부 산하 지휘자동화대학이나 모란봉대학에서 3~5년간 교육을 받으면서 사이버 전사로 키워진다[2].

2.2 최근 북한 사이버공격 사례

2014년 8월에는 국내 정보기술(IT) 보안업체 제품의 취약성을 이용하여 대학병원 전산망에 침입해 서버를 장악하고 사이버공격을 준비한 정황이 밝혀졌다. 또 같은 해 12월에는 북한이 한국수력원자력 조직도와 계도면 등을 6차례에 걸쳐 85건을 탈취해 블로그 등에 올린 사건도 있었다. 또한 2015년 11월에

는 국내 한 금융보안업체를 해킹하여 인증서를 유출해 악성 코드를 제작한 뒤 10개 기관 PC 19대에 악성 코드를 유포한 바 있다.

<표1> 북한발 사이버공격 사건일지

일시	사건명	내용	공격근원지
2009. 7	7·7 디도스 사건	북한이 디도스 공격을 통해 한국·미국의 청와대, 백악관 등 정부기관·금융·포털 35개 주요 홈페이지 마비	북한 체신성
2011. 3.3.~5	3·4 디도스 사건	북한이 좀비PC 10만여대를 동원, 국회·행정안전부·통일부 등 20개 정부기관 홈페이지와 은행·증권사·포털 등 20개 민간 홈페이지에 대해 DDoS 공격을 감행	북한 체신성
2011. 4.12	농협 전산망 해킹	북한이 농협 협력업체 직원의 노트북을 악성코드에 감염시켜 농협 전산센터에서 운영중인 서버 273대에 대해 자료파괴로 업무마비	북한
2012. 6.9	중앙일보 신문제작 시스템 해킹	'IsOne'이라는 별칭을 쓰는 공격자가 '중앙일보' 홈페이지를 변조하고, 신문제작시스템을 파괴.	북한 체신성
2013. 3.20	3·20 방송·금융 전산망 해킹	KBS·MBC·YTN 및 농협·신한은행 등 주요 방송·금융기관의 전산망에 동시다발적으로 악성코드가 유포돼 서버·PC·ATM 등 총 4만8748대 데이터가 삭제됨.	평양 류경동
2013. 6.25	6·25 정부기관 등 해킹	청와대·국무조정실 등 홈페이지와 정당·중소 언론기관 등에서 운영하는 전산시스템에 동시다발적으로 사이버 공격을 감행	북한 체신성
2014. 8	대학병원 전산망 해킹	국내 IT보안업체 제품의 취약점을 이용, 대학병원의 전산망에 침입해 서버를 장악한 후 사이버테러를 준비	평양 류경동
2014. 12.15	한국수력원자력 문서 유출	불상의 방법으로 한국수력원자력 조직도, 설계도면 등 6차례에 걸쳐 85건을 유출해 네이버 블로그 등에 게시하고 금전을 요구	북한(중국요녕성)
2015. 11	정보보안업체 인증서 해킹	금융보안업체를 해킹, 인증서를 유출해 악성코드를 제작, 10개기관 19대 PC에 악성코드를 유포한 사건	평양 류경동
2016. 1.13 ~14	청와대 사칭 이메일 발송	'청와대 국가안보실' 등 정부기관을 사칭해 정부기관 및 포털을 사칭해 759명에게 이메일을 발송	북한(중국요녕성)

북한은 올 1월에는 청와대·외교부·통일부 등을 사칭한 해킹 메일을 정부 기관과 국책 연구기관 관계자들에게 보냈고[3], 3월에는 북한이 정부 및 국내 주요 인사들의 스마트폰을 해킹해 온 사실이 국가정보원 조사 결과 드러났다[4]. 5월에는 북한 해커 조직으로 추정되는 집단이 국내 방산업체와 무기 중개상들을 대상으로 방위사업청을 사칭한 해킹 이메일을 발송해 군 당국이 조사 중이다. 또 북한은 인터넷 쇼핑몰 인터파크를 해킹해 1030만 명의 회원 정보를 빼돌리고 유출사실을 공개하겠다고 협박하며 30억 원어치의 비트코인(가상화폐)을 요구했다. 6월에는 북한에서 제작한 것으로 추정되는 악성코드가 국내 대기업과 공공기관, 정부 부처 등 160여 곳에서 사용하는 PC 통합관리망을 뚫고 시스템에 침투하여 10만대이상의 PC 통제권과 42,608건의 각종 내부 문서를 탈취한 것으로 드러났다[5]. 8월에는 외교·안보의 핵심 정보를 가진 정부 고위관계자 90여명이 북한의 이메일 해킹 공격을 받았다[6]. 이번 공격은 가장 기본적인 해킹 수법으로 중요 정보를 다룰만한 위치에 있는 공무원의 이메일 등 개인정보를 사전에 파악한 뒤에 이메일 비밀번호를 탈취해 이메일에 저장된 안보 관련 중요 정보를 입수하는 식이다.

2.3 최근 북한 사이버공격의 특징

• 사이버공격의 주기 단축

북한의 핵실험 이후 뒤따르던 사이버공격 기간이 최대 두 달에서 일주일로 점차 줄어들고 있는 추세를 보이고 있다. 북한은 지난 2009년 5월말 2차 핵실험 이후 2개월여 만인 7월7일 디도스 공격으로 27만대의 PC를 마비시킨데 이어 청와대와 국회 등의 전산망도 마비시켰다. 2013년 2월초 이루어진 3차 핵실험 이후에는 한 달여 만에 금융사와 언론사 전산망을 공격하기도 했다. 올해 1월6일 감행된 4차 핵실험 이후에는 일주일 만에 청와대 등을 사칭한 스미싱, 이메일을 발송한 것으로 추정되는 등 다양한 사이버공격이 행해지고 있다. 지난 9월9일 5차 핵실험이 진행된 탓에 북한이 조만간 또 다른 형태의 사이버 공격을 전개할 것으로 전망된다.

• 스피어피싱공격

스피어피싱(spear phishig)은 표적 인물을 겨냥해 특정 인물이 가진 이메일 계정으로 취약점이 존재하는 한글문서(hwp) 파일이 첨부된 가짜 업무 메일을 발송해서 첨부 문서를 열어보도록 유도하는 공격이

다. 이러한 공격 유형은 불특정 다수를 노린 일반적인 사이버 범죄 유형과 달리 국가기관이나 주요 기업 내부의 기밀정보를 탈취하기 위한 고도화된 맞춤형 공격 수법으로 매우 은밀하게 악성 행위를 진행하는 특징이 있다. 지난 5월 북한 정찰총국 소속의 해커에 의해 발생한 인터파크 해킹 사태에 대한 미래창조과학부와 방송통신위원회의 조사결과, 해커는 지인 또는 거래처를 사칭하는 이메일을 보내 특정 직원 PC에 악성코드를 심는 스피어피싱 기법을 사용한 것으로 드러났다[7]. 또 8월에는 국내 연구기관이나 대북 통일 관련 분야 종사자를 대상으로 한 스피어피싱 공격 징후가 포착되기도 했다[8].

● 공격수법의 다양화

최근 북한은 수단과 방법을 가리지 않는 다양한 사이버공격을 자행하고 있다. 해킹메일이나 스마트폰 해킹, SNS를 이용한 공격이 시도되고 있다. 올 1월에는 청와대·외교부·통일부 등을 사칭해 정부 기관과 국책 연구기관 관계자들에게 해킹메일을 보냈고, 5월에는 북한 해커 조직으로 추정되는 집단이 국내 방산업체와 무기 중개상들을 대상으로 방위사업청을 사칭한 해킹 이메일을 발송해 군 당국이 조사 중에 있으며. 8월에는 외교·국방·통일부 공무원과 북한 정보를 다루는 교수와 무기 정보를 가지고 있는 방산업체 관계자를 타겟으로 하는 이메일 해킹 사건도 발생하였다, 3월에는 청와대와 정부 부처의 장관급 인사에 대한 휴대전화 해킹을 시도한 사실이 확인되는 등 공격수법이 대담해지는 경향을 보이고 있다. 또한 페이스북 등 SNS에 아름다운 여성 사진을 내걸고는 정부 부처 혹은 공공기관 직원에게 접근해 온라인 친구가 된 다음 내부 자료를 요구하는 북한의 사이버공격 수법도 최근 발견되고 있다[9].

● 대외관계상황을 고려한 계획된 공격

정보당국은 북한 정찰총국이 북한의 사이버공격 컨트롤타워 역할을 하는 것으로 파악하고 있다. 단순 해커조직이 각종 기관·시설에 대해 무계획적 사이버공격을 하는 것이 아니라, 대외관계상황 등을 고려해 정교한 계획 아래 사이버 도발을 한다고 판단하고 있다. 실제 2013년 방송사와 금융기관 등을 상대로 한 3·20 사이버공격은 북한이 장거리 로켓 발사에 이어 3차 핵실험을 한 직후 벌어져 무력 도발을 극대화하는 효과가 있었다. 같은 해 청와대 홈페이지를 해킹해 변조한 6·25 사이버공격은 남북 당국회담 무산에 대한 반발이었고 한국수력원자력 공격은 유엔의 북한 인권 의제 논의라는 국제사회 제재에 대응하는 수단으로 분석할 수 있다. 지난 8월 외교·안보 공무원 이메일 해킹 사건 역시 북한이 극도로 예민해 하는 우리 정부의 사드 배치 결정과 무관하지 않다.

● 아프리카 등 외국에서 공격

북한 외교관 출신인 고영환 국가안보전략연구원 부원장에 따르면 북한 사이버 공작 요원들이 아프리카 내 거점 국가로 가서 대남 사이버공격을 준비하고 있고 북한은 평양뿐 아니라 중국 동북3성과 동남아시아 등지에서도 사이버공격을 준비하고 있다[10], 아프리카는 이번에 처음 알려진 것으로 이는 해킹 흔적을 감추기 위한 목적으로 보인다. 지난 1월 청와대와 외교부, 통일부를 사칭해 북한의 제4차 핵실험과 관련한 의견을 개진해달라는 내용의 이메일은 중국 요녕성에서 발송된 것으로 확인되었다. 해당 IP가 중국 요녕성 구역의 것으로 이는 앞서 한국수력원자력 해킹에 관여한 것으로 보이는 IP와 같은 구역의 것이다[11].

● 민·관·군으로 영역 확대

정부·공공기관을 대상으로 시작된 사이버공격이 국방부·방산업체는 물론 민간 사기업으로까지 영역이 확대되고 있다. 지난 2009년 이후 정부부처·공공기관을 대상으로 공격이 지속 발생하였고 2011년 농협전산망 마비사건 이후부터는 2013년 3.20 사이버공격을 정점으로 해서 올 2월 금융기관 코드서명 해킹사건까지 지속적으로 금융기관에 대한 사이버 공격이 있어왔다. 이는 2009년 7·7 디도스 사태 이후 강화된 국가사이버안전관리규정의 국가전산망 보안관제의무화로 국가공공기관의 사이버 보안이 강화되었기 때문이다. 지난 4월에는 독도함을 건조한 한진중공업이 북한 정찰총국 산하 해커조직으로부터 해킹을 당한 정황이 뒤늦게 드러나 국군기무사령부측이 조사중에 있다[12]. 북한은 올 5월에는 인터넷 쇼핑몰업체 인터파

크 서버를 해킹해 1000만명이 넘는 개인정보를 탈취했고, 6월에는 국내 160여개사가 사용하는 전산망을 대상으로 대규모 해킹 공격을 시도하였으나 민관 협력 대응으로 사전에 차단되었다[13].

3. 대응 방안

3.1 사이버테러방지법 제정

우리나라의 사이버공간을 대상으로 한 북한의 사이버공격은 막대한 경제적 피해와 사회적 혼란을 유발할 수 있고, 공공과 민간을 가리지 않고 이루어지는 공격임에도 불구하고 우리의 국가적 대응활동은 공공·민간 부문이 제각각 분리, 독립적으로 대응하고 있어 광범위한 사이버공격 위협에 효율적 대처가 불가한 실정이다. 공공부문은 대통령훈령인 국가사이버안전관리규정에 근거하고 있어서 행정기관 이외 민간분야 및 입법·사법기관은 적용범위에서 제외되고, 민간 부문은 사이버공격 예방 및 대응을 위한 법률이 미흡하여 사이버공격 징후를 실시간 탐지·차단하거나 신속한 사고 대응에 한계가 있다. 따라서 정부와 민간이 함께 협력하여 국가차원의 체계적이고 일원화된 대응 체계를 구축하고 이를 통해 사이버공격을 사전에 탐지하여 사이버위기 발생가능성을 조기에 차단하며, 위기 발생 시 국가의 역량을 결집하여 신속히 대응할 수 있는 법률이 필요하다.

새누리당은 이철우의원 발의로 법안을 6월 국회에 제출하여 위원회심사가 진행중이고 정부도 국가정보원 주도의 법안을 지난 9월1일 입법예고하였다. 새누리당이 20대국회 중점법안으로 내놓은 사이버테러방지법안(국가 사이버안보에 관한 법률)은 사이버테러의 예방과 대응을 위해 국가사이버안전센터를 국가정보원장 소속으로 설치하고 책임기관들은 보안관제센터를 통해 사이버테러 정보와 정보통신망·소프트웨어의 취약점 등의 정보를 관계 중앙행정기관의 장 및 국가정보원장과 공유하도록 하는 내용을 골자로 한다. 또 국가정보원 주도의 국가사이버안보기본법은 국가사이버안전센터를 국가정보원장 소속으로 하는 사이버테러방지법과는 달리 국무조정실장 소속으로 사이버위협정보공유센터를 설치하자는 것이 골자다. 국가정보원의 과도한 권한 집중에 대한 우려를 반영해 국무총리실 산하로 전담기구를 두었지만 이 역시 국가정보원이 실질적으로 운영한다는 점에서 사이버테러방지법과 마찬가지로 국가정보원의 권한남용과 인권침해 소지로 법안 처리에 진통이 예상된다.

미국처럼 분기별로 관련 보고서 제출을 의무화해 정보기관의 실적을 유도하고 경각심을 갖도록 견제할 필요가 있고, 사이버테러방지법 등 인권침해 우려가 있는 법안은 영구법이 아닌 한시법으로 제정해 실적을 보고 폐지를 논의하는 방안도 고려할 만하다.

3.2 대응모의훈련 실시

모의 훈련은 최악의 보안 사고를 예방해 줄 가장 효과적인 준비다. 현장에서 진행하는 모의 보안 훈련은 실제 상황에서 발생할 수 있는 비상사태를 미리 분석할 수 있도록 해준다. 또한 참가자들은 기존의 작전 계획을 살펴보고 더 개선할 점은 없는지를 고민하며 보안에 대한 건설적인 논의를 할 수 있다. 이런 훈련은 정보 보안과 물리적 보안 모두에 있어 꼭 필요하다. 공격이 발생할 시 비상사태에 대한 계획, 준비, 그리고 협력의 장을 마련해 주기 때문이다. 보안 전문가들이 제시하는 모의 훈련 전략은 1.체계적이고 빈틈 없는 훈련 계획을 세운다. 2.기관, 회사 각 부처의 다양한 인원을 훈련에 참여시킨다. 3.참가자들에게 훈련의 기초 규칙들을 숙지시킨다. 4.산업과 정부 내부의 자원을 활용한다. 5.훈련 규모는 클수록 좋다. 6.최대한 현실적인 상황을 가정하고 훈련을 진행한다 등이다[14].

최근에 정부 주도로 모의 훈련이 이루어지고 있는데 그 예로는 미래창조과학부와 한국인터넷진흥원(KISA)이 6월29~30일 서울 송파구 KISA 상황관제실에서 민간분야 사이버 위기대응 모의훈련을 진행했다. 포털사이트·웹호스팅·컴퓨터 백신업체 등 기업 40여 곳, 4,300여명이 참여해 디도스 공격과 APT(지능형지속위협) 공격 상황을 가정한 훈련을 수행하였다. 또 인천해양경비안전서는 7월25일 북한의 사이버공격에 대비하기 위해 전 직원을 대상으로 모의 해킹 메일을 통한 대응훈련을 실시했다[15]. 그리고 지난 8월 22~25일 진행된 을지연습에서는 사이버테러 대응훈련이 확대 실시되었다.

3.3 수사기법의 선진화

살인, 유괴 등 강력사건 수사에 주로 활용되는 프로파일링 기법을 사이버공격 수사에도 적용할 필요가 있다. 프로파일링은 범죄 현장을 분석해 범인의 습관, 나이, 성격, 직업, 범행 수법 등을 추론하고 이를 바탕으로 범인을 찾아내는 수사 기법으로 경찰 내부에서 연쇄살인범 등 강력사건 수사에 많이 사용되고 있다. 경찰은 조속한 시일 내로 사이버공격 프로파일링 시스템을 구축하고 운영할 필요가 있다. 사이버공격과 관련된 인터넷주소(IP), 계정, 악성코드 정보, 사건 단서, 분석 내용, 사건 개요 등을 데이터베이스(DB)로 만들고 상관관계를 분석할 수 있는 시스템을 구축하여야 한다. 또 경찰은 정보의 민감성을 감안해 독립 서버, 독립 시스템 방식으로 시스템을 만들어야 한다. 해외에서는 이미 사이버공격 프로파일링 기법이 사용되고 있는 것으로 알려져 있다. 해외 수사기관, 글로벌 보안업체들이 해킹사건 발생 후 공격 근원지가 어디인지 추정하는데 프로파일링을 사용하고 있다[16].

3.4.보안관제 서비스의 활성화

보안관제란 사이버 공격에 선제적으로 맞서는 활동이다. 보안 시스템에 대한 운영과 관리, 공격 탐지·분석·대응, 예방 업무를 말한다. 2013년 발생한 3·20 사이버공격 이후 많은 기업·기관은 보안 위협에 대응하고 내부 보안을 강화하기 위한 다양한 보안 장비를 도입했다. 보안 장비가 생성하는 방대한 정보를 기반으로 기업·기관 정보를 노리는 공격 시도를 탐지하고 공격이 어떠한 경로로 들어왔는지, 어디까지 퍼졌는지를 빠르게 분석한다. 또 공격자가 침투할 만한 취약점은 없는지 찾아내는 것이 보안관제의 핵심이자 인력의 역할이다.

사이버 공격이 다양하고 정교한 형태로 진화함에 따라 이메일을 통한 APT 공격, 디도스 공격 대응, 모의 해킹 훈련 등 보안 담당자들이 수행해야 하는 업무는 많아지고 복잡해지고 있다. 그러나 모든 기업과 기관이 정보 수집부터 분석, 사고 대응, 보고, 후속 조치까지 실전 공격과 위기 상황에 원만하게 대응하는 전문 보안 인력을 보유하기는 어렵다. 상대적으로 투자 예산이나 여력이 없는 중소기업, 영세 사업자는 더욱 그렇다. 보안시스템을 도입, 운영해도 하루 24시간 1년 365일 실시간으로 보안시스템 이벤트를 보지 않으면 사고가 나기 전까지 알지 못한다. 특히 보안 담당자가 부재중일 때 사이버공격이 이루어진다면 대응에 문제가 발생할 수 있다. 이것이 전문 지식과 경험, 노하우를 바탕으로 하루 24시간 1년 365일 지켜보고 표준화된 관제 절차에 따라 정보보호시스템 운영과 관리를 대행하는 보안관제 서비스가 필요한 이유이다.

3.5 전문인력 양성 및 교육

사이버 안보에 필요한 전문인력 부족현상이 갈수록 심화되고 있다. 2017년까지 정보보호 분야 전문인력 공급이 예상 수요의 약 18.6%에 불과하다[17]. 사이버 안보를 지키기 위해서는 인력 기반이 뒷받침 되어야 하는데 현재 많이 부족하다. 해킹공격방어대회, 암호경진대회 등 사이버 영재를 발굴하기 위한 노력이 지속적으로 이루어져야 한다. 발굴된 영재는 사이버 보안에 특화된 고등 교육기관과 국가보안기술연구소의 사이버안전훈련센터와 같은 전문 훈련기관을 통해 체계적으로 육성해야 한다. 북한은 1990년대 초부터 사이버 전사를 체계적으로 양성하여 현재 6,000여 명의 사이버전 전문 인력을 운용하는 세계 최고 수준의 사이버전 역량을 보유하고 있다[18].

범부처 공동의 교육정책 발굴 및 표준화된 교육체계 개발을 위해 각기 축적한 교육 콘텐츠를 상호간 공유하고 정책실무 교육과정을 공동으로 개설하는 방안이 필요하고 사이버보안 인재양성을 위해서는 관련 기관들 간 협업을 통한 체계화된 교육 환경 조성이 필수이며, 협력을 통해 최고 수준의 교육 인프라 구축, 맞춤형 교육과정 개발 등이 이루어져야 한다.

3.6 민·관 협력체제 구축

공공기관들이 민간 분야와 긴밀한 공조체계를 구축하는 것은 사이버 보안 정책의 절대적인 명제다. 최근 사이버 공간에서의 공공과 민간 분야 간 연계성이 갈수록 증가하고 있어서 어느 한 지점의 피해도 인터넷 망을 통해 급속히 확산될 수 있기 때문이다.

한국인터넷진흥원이 지난 2014년부터 운영하고 있는 사이버위협정보 분석공유시스템인 C-TAS를 확대 운영할 필요가 있다. C-TAS는 해킹 정보 수집의 질적·양적 확대, 사고요인·연관성 분석 등을 위해 마련된 것으로 C-TAS에 참여하는 기관의 수는 지난해 100개에 달하였으나 부족하다[19]. 더 많은 기관참여가 필요하고 새로운 탐지·예방기술을 적용하여야 한다. 민간시스템을 대상으로 침해 시도가 지속적으로 증가하고 있고, 공격 내용이 지능화되어 감에 따라 선제적 예방 대응을 위해 공공·민간 관계기관 간 긴밀한 협력관계가 필요하다. 과거에는 보안사고 발생 시 공격형태 등을 파악하고 대응했지만 이제는 관계기관 간 정보공유를 통해 침해내용 및 위협사항을 미리 공유하고, 기관의 특성에 맞게 준비하는 등 사전 조치마련이 필요하다. 이에 따라 앞으로는 사이버사고 대응이 과거 수습위주 방식에서 정보를 공유함으로써 침해유형을 분석하고 위협사고를 예방 조치하는 사전 대응방식으로 전환되어야 한다.

3.7 사이버보안 인프라 확대

우리나라의 사이버보안 인프라는 취약한 것으로 조사되었다. 최근 경영컨설팅 전문업체 딜로이트컨설팅이 발표한 2016 딜로이트 아시아·태평양 국가보안 전망보고서(2016 Deloitte Asia Pacific Defense Outlook)에 따르면 한국의 사이버 리스크 점수는 1000점 만점 중 884점을 기록했다. 이는 아태지역 18개국 중 압도적 1위에 해당하는 수치로 2위 호주(582점)보다 300점 이상 높으며 아태지역 평균(201점)보다는 4배 이상 높다[20]. 사이버공격은 철저히 감시하고 대비해도 단 한번만 뚫리면 예측하기 힘든 엄청난 피해를 입을 수 있다. 이미 자연재해로 인한 연평균 피해 규모(1조7000억원)보다 사이버공격에 의한 피해 규모(3조6000억원)가 2배 이상 큰 것이 현실이다[21].

사이버 보안 인프라를 군은 물론 국가기관, 민간업체 등까지 확산시켜야 한다. 사이버공격이 발생하여도 소프트 타겟(테러리스트 공격에 취약한 민간 기관, 기업)의 인프라가 튼튼해야 군과 국가 단위의 사이버 안전도 보장될 수 있다. 최근 일어난 인터파크 회원 정보 유출 사고를 예로 들면 서버가 해킹당한 것만큼이나 해킹이 진행되는 동안 누구도 문제를 인식하지 못한 것 자체가 문제이며 민간 기업, 기관에서 사이버전에 버틸 수 있는 능력을 키울 수 있도록 인프라를 강화해야 한다.

4. 결 론

최근 북한의 사이버공격은 정부기관, 공기업, 방산업체, 민간기업 등을 가리지 않고 이루어지고 있다. 민·관·군의 협력이 절대적으로 필요하다. 북한의 사이버공격에 효과적으로 대응하기 위해서는 민·관·군이 협력해 법과 제도를 개선하고, 전문 인력을 양성·관리하며, 최신 정보보호 기술을 개발하는 등의 지속적인 노력이 필요하다. 또한 전문성과 신뢰성 있는 보안관제서비스, 모의해킹 서비스를 제공할 수 있는 환경이 조성되어야 한다. 향후에는 스마트폰이나 업무용 PC 등 엔드포인트 보안이슈가 많이 발생할 것으로 예상된다. 이에 대처하기 위해서는 기술적 보안 못지않게 정보보안 교육 등 보안의식 제고를 위한 관리적 보안과 보안 업데이트, 취약점 점검 등의 보안 점검이 더욱 중요해질 것으로 보인다. 그리고 지난9월 제5차 핵실험이후 이렇다 할 사이버공격의 징후가 보이지 않고 있는데 언제 가해올지 모르는 공격에 대비하여 철저한 준비태세가 필요하다.

참고문헌

[1] 유동열, “[긴급점검] 점증하는 북한 사이버테러 위협“, 미래한국, 2016.04.11.
[2] 박형주, “[뉴스인사이드] 북한의 사이버전 능력”, VOA, 2016.06.20.
[3] 손기은, “ 北, 안보 해킹부터 쇼핑몰 공격까지… 전방위 ‘사이버 테러 ”, 문화일보, 2016.08.01.
[4] 강준구, “ 北, 전방위 스마트폰 해킹 시도… 외교·안보라인 실무자급까지 주요 인사 20% 수준 수십명 해킹”, 국민일보, 2016.03.08.
[5] 임기창, “北, '3.20테러' 뛰어넘는 대규모 사이버 공격 준비했다 ”, 연합뉴스, 2016.06.13.
[6] 이예진, “北, ‘외교안보 핵심 관계자’ 90명 이메

일 해킹“, KBS 뉴스, 2016.08.02.
[7] 변동진, “인터파크 해킹, 특정 개인 겨냥한 '스피어피싱' 기법 사용”, BizFACT, 2016.08.31.
[8] 김학재, “ 북한발 사이버공격 주기 짧아졌다. 민간기업 대비 강화해야 ”, 파이낸셜뉴스, 2016.09.12.
[9] 유연수, “ 미모의 페친, 알고보니 간첩?…北 사이버테러, 정교하고 다양해졌다”, 아세아경제, 2016.07.20.
[10] 강정숙, “북한, 아프리카까지 진출해 대남 사이버테러 준비중”, 아주경제, 2016.06.14.
[11] 박지환, “청와대 사칭 핵실험 이메일, 중국 요녕성 IP로 발송“, 노컷뉴스, 2016.01.18.
[12] 박원형, “방위산업체도 당했나? 北 사이버공격 대상 전방위 확대 “, 보안뉴스, 2016.05.10.
[13] 송주영, “북한 추정 사이버테러 선제 대응…피해 막아 ”, ZDNet KOREA, 2016.06.15.
[14] Bob Violino, “효과적인 모의 보안 훈련을 위한 6가지 전략“, IT WORLD, 2014.10.30.
[15] 배종진 “ 인천해경, 북한 사이버테러 대비 전 직원 모의훈련 ”, 기호일보, 2016.07.26.
[16] 강진규, “사이버테러 수사에도 프로파일링 기법 적용한다”, 테크M, 2016.08.02.
[17] 이윤애, “눈에 보이지 않는 사이버 위협, 우리의 준비는“, 이투데이, 2015.04.29.
[18] 김영석, “기무사령관 “북한, 사이버 전사 6000명 양성””, 국민일보, 2016.07.07.
[19] 조양준, “[KISA, 사이버 보안 총력전] 탐지능력 고도화로 '파괴의 기술' 봉쇄“, 서울경제, 2016.02.28.
[20] 허주열, “기업들 사이버 보안 '구멍', 이유 있네”, Moneyweek, 426호, 2016.03.14.
[21] 정혜진, “박영선 두두아이티 연구소장 “사이버戰은 미개척지…개척자 되겠다””, 서울경제, 2016.08.16.

[저 자 소 개]

정 영 도 (Yeong-do Jung)

유원대학교
정보통신보안학과 3학년

email : wjddudeh0@naver.com

정 기 석 (Gi-seog Jeong)

1983년 2월 고려대학교
전자공학과 학사
1988년 8월 고려대학교
전자공학과 석사
1992년 8월 고려대학교
전자공학과 박사
현재 유원대학교
정보통신보안학과 교수

email : gsjeong@yd.ac.kr