情 報 保 護 學 會 誌
第 12 券 第 6 號, 2002. 12

정보전(사이버전) 대비를 위한 제언

남 길 현*

요 약

인터넷 인구 2천 5백만, 초고속 전산망 가입자 1천만명을 돌파하고 사회전반의 정보시스템 의존도가 더욱 심화되고 있는 현시점에서 우리나라가 선진국 대열에 동참하기위해서는 정보화 역기능에 대한 대비책 마련이 필수적인 요소이다. 특히 국가안보와 관련된 정보전과 사이버전, 사이버테러에 대한 개념을 정립하고 군 뿐만아니라 범국가적 대응책을 마련하여야 한다. 전문인력 양성과 국민의식 홍보, 범국가적 협력체계 구축, 정보보호 시스템 구축 및 보안관리 강화등 기본적인 추진 방안을 제시하면서 이 분야 전문가 집단인 한국정보보호학회의 역할을 강조한다.

Ⅰ. 서 론

20세기 후반기에 개발되기 시작한 컴퓨터와 정보통신 기술은 과거 수 천년동안 인간이 이루었던 문명사적 진보를 훨씬 능가하는 과학기술 발전과 생활양식을 변화시키는 원동력이 되고 있으며 그 발전속도도 다른 어떤 기술이나 학문보다도 비교할 수 없을 만큼 빠르게 진전되고 있다. 정보통신기술을 기반으로 하는 인터넷의 세계적 확산은 전 세계를 한데 묶어 시·분·초를 다투는 단일 생활권으로 압축시키고 전자상거래의 열풍은 국경선을 뛰어넘어 새로운 국제경제 질서를 모색하고 있다.

인터넷 인구 2천 5백만을 넘어선 우리나라에서 컴퓨터와 정보통신은 경제·사회뿐만 아니라 국민 일상생활의 중요한 일부가 되고 있으며 선진국으로 도약하기 위한 국가경쟁력 확보를 위하여 정보기술(IT : Information Technology) 활성화는 정부가 주도하는 최우선 정책분야로 추진되고 있다. 이제 사회구성요소 모두의 정보시스템 의존도는 더욱 더 높아만 가고 있으며 국가전체가 네트워크화 되고 있기 때문에 어느 한 분야의 정보시스템 손상이나 마비는 사회적 파급효과가 연쇄적으로 온 국가에 확산되게 되어 있다.

다행스럽게도 우리나라의 초고속 정보통신망을 비롯한 정보기반구조 구축 성과는 선진국에 뒤떨어지지 않고 있다는 평가를 받고 있다. 그러나 정보화가 급진전됨에 따라 파생되는 정보화 역기능 즉, 정보의 변조, 도청, 오남용 및 개인 프라이버시 침해 등의 부작용이 심각한 문제점으로 지적되고 있으며, 특히 금융·전력·운송·공공기관 등 주요사회 기반시설의 정보시스템에 대한 사이버테러 위협은 국가안보적 차원에서 대비책을 강구해야하는 중요분야로 떠오르고 있다.

특히, 미국의 9·11테러이후 시간이 흐르면서 물리적 테러에 대한 경계심은 다소 늦춰지고 있는데 비해 사이버테러에 대한 경계심리가 한층 고조되고 있고, 미국 보안전문가들은 앞으로 이어질 테러는 미국의 상징적인 대기업들 뿐만 아니라 전력·운송과 같은 사회주요기반시설에 집중될 가능성이 높은 것으로 예상하고 있다.

정보전과 사이버전, 사이버테러에 대한 개념 구분은 아직도 명확치가 않다는 것이 현실이나 필자의 관점에서 볼 때, 사이버전은 국방 분야에서 정보우세를 목적으로 적의 정보시스템과 정보를 공격하고 아군의 정보시스템과 정보를 방어하는 정보전(정보작전)의 일부 분야로서, OSI 7계층 모델에서 2~7계층까지인 사이버 공간에서 바이러스나 해킹 등의 사이버 무기를 이용하는 군사작전이며 사이버테러는 민간차원에서 개인과 기업, 기타 민간 조직을 대상으로 한 사이버 위협으로 볼 수 있다. 본고에서는 사이버전과 사이버테러를 본질적으로 유사한 개념으로 간주한다. 따라서 사이버전 및 테러는 사이버공

* 국방대학교 (khnam@kndu.ac.kr)

간과 수단의 특수성을 고려할 때, 적과 아군의 구분이 모호하고, 국가간의 경계가 없으며, 전쟁과 테러를 수행하는 비용은 작지만 심각한 경우에는 핵무기와 같은 물리적 파괴무기 못지않는 엄청난 사회·경제적 파급효과를 가진다.

이미 미국·일본·중국·러시아 등 세계 주요 국가들이 사이버전 대응역량을 강화하고 있는 시점에서 우리나라도 사이버전 위협의 심각성을 재조명하고 국가 안보적 시각에서 대응책을 강구해야 할 필요성이 재기되고 있다. 미국은 튼튼한 사이버전 방어 기반위에 군사작전 수행 시 사이버 공격수단을 운용하는 전술을 개발 및 운용 중에 있고, 중국은 전자전 무기를 포함하는 사이버전 공격 무기를 개발하고 그 운용부대를 주기적인 훈련에 동참토록 하고 있으며, 일본은 중·장기 국방계획에 사이버전 전력 증강을 위한 집중적인 투자를 계획하고 있다.

우리나라도 국가정보원은 내년 상반기에 '국가 사이버테러 대응 종합계획'을 수립하여 현재 기관별로 독자적인 사이버테러 대응체계의 준비에 따른 업무 혼선, 예산 중복투자, 인력소모 등의 문제점 해결방법을 모색하고 있고 국정원에서 운영중인 보안 119를 중심으로 부문별로 운영되는 침해사고대응센터(CERT)와 정보공유분석센터(ISAC)를 연계해 '조기경보 및 침해사고대응종합센터'를 구축할 계획이다.

한편 국방부에서도 미래 전쟁양상으로 예상되는 정보전의 한 분야로서 사이버전의 위협을 대비하고 응징할 수 있는 사이버전 대응체계를 2010년까지는 선진국 수준으로 끌어올리기 위해 단계적인 계획을 수립하여 추진하고 있다

II. 제 언

정부 기관을 중심으로 사이버전(테러) 대응체계를 구축하기위해 많은 노력이 진행되고 있기는 하나 여전히 사이버범죄행위가 급증하는 것으로 보아서는 일반 기업이나 대학, 기관 등 사회 전반적으로 아직도 정보보호나 사이버전에 둔감하다는 결론을 내릴 수 밖에 없다. 따라서 먼저 사이버전 대응의 중요성을 인식토록하고, 이를 바탕으로 전문인력을 확충하고 조직을 정비하며, 관련 제도를 정비하고, 연관 조직 간의 협조체계를 구축하는 등의 기반체계 구축이 시급하게 선행되어야 한다.

본고에서는 사이버전 대응체계를 갖추기 위해 기본이 되면서도 우선적으로 수행되어야하는 대책들을 제안하고자 한다.

1. 전문인력 양성 및 국민의식 홍보

우리나라에서 사회적으로 정보보호에 관심을 갖기 시작한 것은 90년대 초반이라고 할 수 있으며 특히 해킹·바이러스에 의한 사이버테러 문제는 아주 최근에 이슈화 되었다. 따라서 대학이나 전문기관에서의 전문인력 양성은 소요에 대비하여 극히 부족하며, 국민전체의 중요성 인식도 아주 미흡한 실정이다. 산·학·관이 공동으로 대학 및 학회 또는 전문교육기관에 정보보호 교육프로그램을 개발하고, 교육을 활성화하기 위한 교육비 지원이나 장학제도를 확대할 수 있도록 하여야 한다. 최근 여러 대학 및 대학원에 정보보호 전공과정이 개설되고 정보통신부에서 각 학교에 있는 해커동아리 지원책을 마련하여 지도교수를 임명하고 연구결과 발표를 통한 해커양성화 방안은 매우 효과적인 전문인력 양성방안 중의 하나라고 할 수 있다. 특히 사이버전 기술의 핵심을 이루고 있는 해킹 바이러스 기술을 갖고 있는 해커들은 대부분 음성적으로 활동하기 때문에 이들에게 나쁜 사이버테러에 가담하지 않고 떳떳하게 기술 개발할 수 있는 환경을 마련해 준다면 이들이 사이버테러 대응기술을 연구 개발할 수 있는 전문 연구 인력으로 변모할 수 있을 것이다.

또한 사이버전을 비롯한 정보화 역기능의 폐해에 대한 심각성과 정보보호 대책의 중요성에 대한 국민의식 강화를 위한 홍보대책이 필요하다.

전문학회를 주축으로 하는 각종 정보보호 세미나와 학술대회를 통하여 전문기술과 지식을 전파할 뿐만 아니라 TV·신문 등 언론매체를 통한 광고 및 적극적인 홍보활동을 통하여 국민전체가 지식정보사회에서 사이버테러에 대한 경각심을 새롭게 하고 대응체계 구축에 적극적으로 동참할 수 있도록 하여야 한다.

2. 범정부적 차원 대응체계 구축 및 유관기관 협력체제 강화

사이버테러에 효율적으로 대응하기 위해서는 각 부처별로 흩어져 있는 임무와 기능을 통합하고 일관성 있는 정책수립과 시행을 위한 사이버테러 전담조직이 구성되고 산·학·관·군 협력 체제를 활성화 시켜야 한다.

국가 안보적 시각에서 중·장기적인 기획 및 예산을 담당하는 총괄기관이 선정되고 각 부처별로는 임무와 기능을 정확히 할당하여야 하며, 기술개발과 산학관군의 협력체제가 갖추어져야 한다.

사이버테러를 사전에 탐지·차단하는 예방대책 수립, 안전한 정보시스템 운영을 위한 관리시스템, 정보보호기술 연구개발 체계, 사고 발생시 검·경에 의한 수사 대응체계 등이 유기적으로 연동될 수 있는 범정부적 차원의 대응체계가 구축되어야 한다. 또한 해킹, 바이러스 대응을 위해서는 국제적인 긴밀한 공조체제도 강화해야 한다.

3. 사이버전 대응을 위한 법·제도적 기반 확보

사이버테러의 위협에 효율적으로 대처하기 위해서는 법·제도적인 장치가 우선적으로 마련되어야 한다. 현재 국가보안업무차원에서 제정된 보안업무규정이나 국가 정보통신 보안 기본지침에 의해 수행되고 있는 정부·공공분야에 대한 사이버테러 대응 업무를 더욱 강화할 수 있는 시행지침이 구체적으로 보완되어야 한다. 최근 시행령이 발효된 정보통신기반보호법도 주요 사회기반시설에 대한 사이버테러 방지를 위한 근간을 제공하고 있지만 각 기관별 업무분담과 사용자지침이 아직 충분치 못한 실정이다. 또한 사이버테러와 국방정보전의 사이버전과의 연계성도 더욱 명확하고 상호보완 할 수 있도록 하여야 한다.

4. 사이버테러 대응기술 연구개발 및 정보보호 산업 육성

사이버테러 대응기술과 관련된 정보보호 기술은 세계 각 국이 대부분 핵심부분에 대한 수출을 통제하고 있으며 상대방을 신뢰하기 어려운 보안의 특성 때문에 외국 제품을 수입하거나 복제하는 것은 원칙적으로 금지하고 있다. 따라서 정보보호 제품기술은 독자적으로 연구 개발하여야 한다는 현실적인 문제점을 안고 있다.

전문학회나 연구소를 중심으로 기초기반기술에 대한 연구를 지원함은 물론 정보보호 산업체들이 활성화 될 수 있도록 대책을 강구하여야 한다.

1998년도에 발족된 한국 정보보호산업 협의회에는 약 200여 개의 업체가 등록되어 있지만 종업원 수나 투자규모 면에서 거의 대부분 영세기업에 속하는 업체들이다. 이들 정보보호 산업체들이 국내외적으로 기술경쟁력을 확보할 수 있도록 한국정보보호진흥원과 전자통신연구원 및 국가보안기술연구소는 기술연구개발 및 제품 상용화를 지원하고, 정보통신부, 과학기술부, 산업 자원부는 연구 및 자금을 지원할 수 있는 방안을 마련하여야 한다.

사이버테러 대응기술은 정보시스템 취약성 분석기술, 침입차단/탐지·대응·복구기술, 안전/신뢰성 강화기술 등으로 분류할 수 있다. 이러한 기술은 필요한 경우에는 국가공공기관용과 민간부문으로 구분하여 연구 개발할 수 있으나 민군 겸용기술 개발로 중복투자를 최대한 억제하고 적절한 평가·인증절차를 거쳐 사용자 수준에 맞는 제품을 활용할 수 있도록 하여야 한다.

한편 한정된 국내시장에 국한하지 않고 세계시장으로 진출할 수 있도록 수출 지원책을 마련하고 이를 뒷받침하는 국제표준화 활동에도 적극 참여하여야 한다.

5. 정보보호 시스템 구축 및 보안관리 강화

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

정보보호 대책은 정보시스템에 대한 내·외부 사용자의 접근제어, 인터넷 연결 시 침입차단 및 탐지시스템, 해킹방지 및 안티 바이러스 시스템, PKI(공개키 기반)응용 인증 및 전자서명, VPN, 보안OS, 보안DBMS 등 다양한 정보보호 제품을 사용자 임무와 요구수준에 적합하도록 선택하여 설치하여야 한다.

또한 정보시스템의 안전한 보안관리를 위해서는 정보시스템 보안관리 표준을 제정하여 이에 준하는 평가인증을 받을 수 있도록 하고 이를 확대 시행하도록 하여야 한다.

지금까지 정보전(사이버전)에 대응하기위한 국가차원의 대응책을 몇 가지 서술하였다. 아직은 사이버전의 실체가 명확하게 제시되지 않은 시점에서 사이버테러와 복합된 사이버전은 군의 고유 업무라고 하기보다는 산학연관이 협력하여야 할 범국가적인 당면과제이며, 특히 정보보호분야 전문가들로 구성된 한국 정보보호학회는 사이버전 대응체계 구축의 길잡이 역할을 하여야 할 것으로 판단된다.

〈著 者 紹 介〉

남 길 현(Kil-Hyun Nam)
종신회원

1969년 : 육군사관학교 이학사
1973년 : 서울대학교 공과대학 토목 공학사
1979년 : 미 해군대학원 전산학 석사
1983년 : 미 위스콘신-메디슨 주립대 전산학 석사
1985년 : 루이지아나 주립대 전산학 박사
1973년~1977년 : 육군 사관학교 전임강사
1979년~1981년 : 육군 전산소 분석관
1985년~현재 : 국방대학교 교수
1996년~1997년 : 미 루이지아나 주립대 객원교수
1999.2 ~2001.2 : 한국통신정보보호학회 회장