한국과 미국의 사이버보안 단계별 법제도 비교 연구

박상돈* · 김인중*

요 약

기존 사이버보안 법제도 비교연구의 주된 경향은 비교하고자 하는 국가들의 관련 법령의 내용을 개별 법령별로 나열하여 소개한 후 종합적인 비교를 제시하는 형태를 나타냈다. 이러한 연구방법은 사이버보안 단계별로 적용할 한국의 법제도가 어떤 점이 미흡한지 파악하기 쉽지 않았기 때문에 보다 정밀하고 객관적인 법제도 비교 연구의 방법을 모색할 필요가 있다. 이에 본 논문에서는 사이버보안이 이루어지는 단계를 예방, 탐지, 대응, 복구로 설정하고 각 단계별로 한국과 미국의 사이버보안 법제도를 비교하여 한국 법제도의 문제점을 중심으로 차이점을 분석하였다. 그 결과 한국의 사이버보안 법제도에는 사이버보안의 모든 단계에서 규정의 부재, 명확성의 부족, 실효성의 부족, 규정간의 중복 등 여러 가지 미흡한 부분이 있음을 확인하였다. 그리고 문제점별로 개선방안을 제시하는 동시에 사이버보안 법제도 개선의 거시적인 방향도 함께 제시하였다.

Comparative Study on Legal System on Cybersecurity Stages in South Korea and the United States

Sangdon Park* · Injung Kim*

ABSTRACT

Existing comparative studies on legal system of cyber security just listed and introduced several laws of Korea and other countries and presented comprehensive comparison. These studies makes it difficult to know that which part of the cyber security activities has insufficient legal system from a practical standpoint because it is not easy to figure out. So cybersecurity stages are chosen as comparison criteria. And the legal system of United States are chosen as the target comparing one of South Korea. Then the legal system on cybersecurity stages in South Korea is compared with one of United States. Therethrough many problems of the legal system of South Korea is identified, for example, the absence of regulations, the lack of clarity, lack of effectiveness, and overlapping regulations, in prevention, detection, response, the recovery in cyber security. And many ways are suggested to improve the legal system for the resolution of such problems.

Key words : 사이버보안 법제도, 사이버보안 단계, Legal System on Cybersecurity Stages

접수일(2012년 8월 24일), 수정일(1차: 2012년 9월 14일), 게재확정일(2012년 9월 18일)

* 한국전자통신연구원 부설연구소

1. 서 론

기존 사이버보안 법제도 비교연구는[1][2] 비교하고자 하는 국가의 법령의 내용을 각 법령별로 나열하여 소개한 후 종합적인 비교를 제시하는 형태가 많았다. 이러한 연구방법은 각 법령별 내용을 확인하거나 비교대상 국가의 법제도를 전체적인 관점에서 파악하여 비교하기에는 용이하지만 사이버보안 단계별로 적용할 한국의 법제도가 어떤 점이 미흡하고 입법상의 공백이 무엇인지를 파악하기에는 어려운 점이 없지 않았다.

이러한 문제점을 극복하기 위하여 본 논문에서는 사이버보안의 단계를 비교항목으로 삼아서 보다 정밀한 비교를 시도하였다. 이에 따라 사이버보안 단계별로 법제도가 어떤 문제점이 있는지 보다 명료하게 확인할 수 있고, 그에 따른 대책 마련도 보다 수월할 것으로 기대된다. 비교 결과 나타난 한국과 미국의 차이점을 서술함에 있어서는 주로 한국이 취약한 부분을 중심으로 다루었다.

2. 비교대상 및 비교항목 설정

2.1 비교대상 설정

2011년 미국과 러시아의 연구기관이 공동으로 제시한 바에 의하면 사이버보안(cybersecurity)이란 '사이버공간이 지닌, 의도적・비의도적 위협에 대항하고, 대응・복구할 수 있는 속성'이다. 그리고 사이버공간(cyberspace)이란 '정보의 생성・전송・수신・저장・처리・삭제가 이루어지는 전자적 매체'이다[3]. 즉 이를 풀어서 사이버보안의 개념을 보다 명확히 제시하면 '정보의 생성・전송・수신・저장・처리・삭제가 이루어지는 전자적 매체가 지닌, 의도적・비의도적 위협에 대항하고, 대응・복구할 수 있는 속성'이라고 할 수 있다.

이에 기초하여 사이버공간이라는 전자적 매체의 보호를 다루는 법령을 비교대상으로 정하였으며, 개인정보보호법과 같이 그 영역을 사이버공간만으로 한정할 수 없거나 보호의 대상으로 전자적 매체를 주된 대상으로 염두에 두지 않은 경우는 보호 연구대상에서 배제하였다. 이러한 기준에 해당하는 한국과 미국의 법령을 식별하여 <표 1>과 같이 비교 대상 법령을 정하였다. 미국을 비교대상으로 정한 이유는 현재 미국이 세계를 주도하는 강국이면서 사이버보안에서도 그러한 면모를 보이고 있음을 부인할 수 없고, 전세계적으로 널리 사용되고 있는 IT 기술의 상당부분을 선도하고 있으며, 관련 입법활동도 비교적 상당히 활발하게 이루어지고 있기 때문이다.

<표 1> 비교 법령 목록

구분	법령명
한국	정보통신망 이용촉진 및 정보보호 등에 관한 법률, 정보통신기반 보호법, 전자정부법, 국가사이버안전관리규정
미국	컴퓨터 사기 및 오용에 관한 법률, 애국자법, 국토안보법(주요기반정보보호법, 사이버보안강화법 포함), 전자정부법(연방정보보안관리법 포함), 사이버보안 연구개발법

2.2 비교항목 설정

바람직한 법제도 비교는 구체적 항목별 비교를 통해 가능하다[4]. 적절하게 선정된 비교항목에 따른 법제도 비교는 비교결과의 가시성 및 객관성을 증대시킨다. 현재 비교적 객관성을 인정받을 수 있는 비교항목은 사이버보안의 단계를 기준으로 하여 설정하는 것이라고 본다. 사이버보안 침해사고 대응절차의 단계별 과정은 용어 표현상의 차이를 제외하면 일반적으로 예방・탐지・대응・복구 순으로 제시된다[5]. 용어상 대응절차를 구성하는 여러 단계 중 하나가 대응이라는 것은 논리적으로 맞지 않는다. 반대로 대응절차가 대응이라는 활동을 이루는 여러 구성요소 중 하나가 되어야 한다. 따라서 예방·탐지·대응·복구는 사이버보안 침해사고 대응절차의 단계가 아니며, 이보다 더 넓은 범위의 개념인 사이버보안의 단계로 보아야 한다.

예방・탐지・대응・복구라는 형태의 단계는 사이버공간과 대칭되는 물리적 공간의 재난에서도 유사한 경우를 찾을 수 있다. 현행 국내법상 재난관리의 단계는 '예방・대비・대응・복구'로 제시된다[6]. 재난관리와 사이버보안은 모두 재난이나 사이버공격이라는 위해요소로부터 사고를 방지하거나 피해를 최소화하는 것

을 의미한다. 따라서 사이버보안의 단계를 재난관리의 단계와 유사하게 설정하는 것은 타당하다. 다만 재난에서 대비에 해당하는 것이 사이버보안에서는 탐지이며, 나머지는 모두 동일하다.

예방이란 정보보호를 위한 평시 활동으로서, 침해사고 대응팀 구성 및 운영, 정보보호 교육을 통한 인식제고 등이 해당된다. 탐지란 정보자산 모니터링, 초기분석 등을 의미하며, 대응은 증거 데이터 수집 및 보호, 침입 유형별 긴급조치 등이 해당된다. 복구에는 재발방지 조치, 시스템 통제권 회복 후 재발방지 대책 수립 등이 해당된다[5]. 이러한 개념에 기초하여 사이버보안 단계에 기초한 비교항목과 항목별 주요 요소를 <표 2>와 같이 설정할 수 있다.

<표 2> 비교항목별 주요 요소

비교항목	주요 요소
예방	정책수립, 추진체계 수립, 사전점검 및 평가・인증, 연구개발 및 산업 진흥, 교육・훈련
탐지	정보수집 및 분석, 정보공유 및 협업, 경보발령
대응	긴급조치, 사고조사
복구	피해복구, 재발방지

사고 발생 시점을 기준으로 하면 예방과 탐지는 사고 발생 이전의 활동이며 대응과 복구는 사고 발생 이후의 활동이다. 복구 이후에는 재발방지 대책에 따라 사고의 재발을 예방하는 수순을 밟게 되어 다시 예방으로 돌아간다. 따라서 예방・탐지・대응・복구는 사이버보안 활동의 모든 과정을 포괄하며, 이러한 단계를 비교항목으로 하여 사이버보안 법제도를 비교하면 사이버보안이 이루어지는 과정 전체를 누락되는 부분이 없이 비교할 수 있게 된다. 비교 결과 다른 나라보다 법제도의 내용이 미흡한 부분이 있다면 보완이 필요한 사항이며, 법제도가 다루지 않는 부분이 있다면 입법상 공백으로 판단할 수 있다. 그리고 비교 결과 나타나는 그러한 차이점들이 바로 개선이 필요한 사항들이 된다.

3. 한국과 미국의 법제도상 차이점

3.1 예방단계

3.1.1 범국가적 사이버보안 원칙 부재

미국은 거시적 시각에서 정보혁명에 따른 기반보호의 중요성과 정책방향을 애국자법에 규정하고 있다. 이에 의하면 주요기반시설의 운영에 대한 어떠한 물리적 방해 또는 컴퓨터를 이용한 방해가 없어야 하고, 방해가 있더라도 최소한의 영향에 그쳐야 한다. 또한 기업 및 비정부 조직을 참여시키는 공공과 민간의 파트너십에 의해 주요기반시설 보호 정책, 모든 상황에서 연방정부의 본질적 기능을 지속시키는 종합적이고 효과적인 프로그램을 수립한다[7]. 반면에 한국은 정보통신기반보호법 등 관련 법령에 그러한 거시적 원칙을 정한 부분이 없다.

3.1.2 정책수립 관련 규정의 실효성 부족

미국은 정책수립 관련 규정의 절반 이상이 구체적으로 서술되어 담당자가 법령만으로도 어떤 정책을 수립해야 하는지 파악이 가능하다. 국토안보부장관은 주 및 지방 정부 조정실을 통해 주 정부 및 지방 정부, 민간기관과 적절한 계획, 준비, 훈련 및 연습 활동, 국토안보와 관련된 통신 및 통신 시스템, 경고 및 정보의 배포를 조정하고, 특별보좌관의 도움을 받아 민간부문 주요기반시설 보호를 위한 최선의 실행방법을 개발・촉진한다[8]. 또한 국토안보부의 정보분석 및 기반보호 담당차관은 주요 기반시설을 안전하게 하기 위한 포괄적 국가 계획을 수립하며, 그러한 국가 계획의 보호대상은 전력 생산, 발전 및 배전 시스템, 정보 기술 및 전기 통신 시스템(위성 포함), 전자 재정 및 재산 기록 저장소 및 전송 시스템, 비상 대비 통신 시스템, 그리고 이러한 시스템들을 지원하는 물리적 자산 및 기술 자산을 포함한 미국의 핵심 자원으로 한다[9]. 반면에 한국은 정책수립 관련 규정의 절반 이상이 구체성이 부족하여 어떤 정책을 수립해야 하는지 파악할 수 없다. 이를테면 '정보통신망의 안전성 및 신뢰성 제고' 등을 포함하여 '정보사회의 기반을 조성하기 위한 시책'을 마련하도록 정하고 있으나[10], 이것만으로는 어떤 정책을 수립하겠다는 것인지, 정책의 대상은 무엇인지

등 정책수립에 필요한 기본적인 사항에 대한 내용조차 알 수 없기 때문에 법조문만으로는 정책수립 담당자에게 실질적인 효력을 발휘하기 어렵다.

3.1.3 보안조치 추진체계의 구체성 미흡

미국은 보안대책 수립과 그에 따른 조치 실행을 구체적으로 규정한다. 국토안보부 정보분석 담당차관과 기반보호 담당차관은 핵심자원 및 주요 기반시설을 보호하기 위한 대책을 권고한다[9]. 백악관 관리예산처(OMB)는 정보보안 표준·지침을 개발하고 그 시행을 감독한다[11]. 반면에 한국은 보안대책 수립과 그에 따른 조치 실행의 구체적 내용이 부족한 부분이 일부 있다. 이를테면 중앙행정기관의 장은 소관 정보통신망에 대하여 안전성을 확보할 책임을 위하여 사이버안전업무를 전담하는 전문인력을 확보하는 등 필요한 조치를 강구하여야 한다고 정하고 있는데[12], 전문인력의 확보라는 예시만으로는 필요한 조치의 의미가 모호하여 실제 업무담당자에게 필요한 구체적 내용이 부족하다.

3.1.4 국회보고체계 부재

미국은 행정부의 사이버보안 주요 업무를 국회에 보고하여 권력 남용의 우려를 차단함으로써 입법부의 신뢰를 구축한다. 백악관 관리예산처는 연방 정보보안 실태를 의회에 보고하고[11], 국립과학재단(NSF)은 연구프로그램 및 장학금지원 검토 보고서를 의회에 제출한다[13]. 반면에 한국은 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 전자정부법 등 관련 법령에 별도의 국회보고체계가 전혀 없는 상태이다.

3.1.5 공공부문의 독자적 연례평가 부재

미국은 기관프로그램의 일환으로 정부기관의 독자적 연례평가에 관한 구체적 사항을 법률에 정하고 있다. 각 연방기관은 매년 소관 기관의 정보보안 프로그램 및 실무에 대해 프로그램과 실무의 효과를 판단하기 위해 독자적 평가를 수행한다. 평가결과는 매년 관리예산처장에게 제출되며, 중앙정보국(CIA) 및 국방부가 통제하는 시스템에 대한 평가는 별도로 의회의 소관 위원회에만 제출된다[14]. 반면에 한국은 전자정부법에서 보안조치의 안전성 확인을 추상적으로 규정하거나[15] 정보시스템 감리에 대한 내용만을 규정하고 있으며[16], 미국의 독자적 연례평가와 같이 지속적인 정기적 평가에 관한 상세한 내용을 별도로 정하지 않은 상태이다.

3.1.6 기반시설 위협 예측·평가 부족

미국은 국가기반시설 시뮬레이션·분석센터가 기반시설 구성 시스템 모델링·시뮬레이션·분석을 통해 예기치 못한 위해의 시사점, 재난 발생시 예상 반응 등을 도출한다[17]. 또한 국토안보연구소는 주요기반 취약성 감소를 위하여 배치된 시스템의 유효성 분석·모델링·시뮬레이션을 통해 발생가능한 위협을 사전에 예측한다[18]. 그리고 각 연방기관은 소관 업무 및 자산을 지원하는 정보 및 정보시스템의 무단접속, 사용, 공개, 방해, 수정 또는 파괴로 인해 야기될 수 있는 위해의 위험과 규모를 주기적으로 평가한다[19]. 반면에 한국은 발생가능한 위협을 적극적으로 예측하는 것은 법에 정하지 않고 취약점 분석·평가라는 표현을 사용하면서 추상적으로 규정하여[20], 법률상으로는 미래의 위험 예측에 대하여 적극적인 태도를 보이지 않고 현재의 취약점에 치중하는 듯한 모습을 보이고 있다.

3.1.7 연구개발 관련 규정의 추상성

미국은 연구개발에 관한 법률을 별도로 제정하여 사이버보안연구개발법에서 연구 지원 및 프로그램 운영 절차, 심사절차를 구체적으로 정한다[21]. 반면에 한국은 주로 해당기관의 임무로서 '시책을 마련'[10], '시책을 강구'[22] 등과 같이 선언적으로 표현하며, 구체적인 절차규정이 미흡하다.

3.1.8 민간연구기관 지원에 관한 구체적 규정 부재

미국은 사이버보안연구개발법에서 구체적인 지원대상과 지원프로그램 내용을 명시한다[23]. 반면에 한국은 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등 관련 법령에 민간연구기관 지원에 관한 별도의 구체적인 규정이 전혀 보이지 않는다.

3.1.9 고등교육기관 지원에 관한 구체적 규정 부재

미국은 고등교육기관에 제공되는 지원 프로그램을

구체적으로 규정한다[24]. 반면에 한국은 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등 관련 법령에 고등교육기관 지원에 관한 별도의 구체적인 규정이 전혀 보이지 않는다.

3.2 탐지단계

3.2.1 정보수집 지원 시책의 실효성 부족

미국은 탐지에 관하여 무엇을 개발하여 지원하는지 그 대상을 명시하여, 국가표준기술원이 탐지지침을 포함한 정보시스템 표준, 지침, 관련 방법, 기법을 개발한다고 정하고[25], 국토안보부 과학기술담당차관은 테러리스트 공격 탐지 관련 기술 및 시스템 연구・개발・시험・평가・조달을 담당한다고 구체적으로 명시한다[26]. 반면에 한국은 실효성을 확보하기 위한 구체적 내용이 부족하며, 정보통신기반시설의 경우 정보공유·분석센터의 구축을 장려하고 그에 대한 기술적 지원을 할 수 있다는 정도로만 정하여[27] 기술적 지원의 실체를 알기 어렵고, 정보수집 기술 연구개발에 관한 별도의 규정이 없다.

3.2.2 주요기반시설보호에 필요한 정보수집 및 정보공유 촉진 부족

미국은 자발적으로 제출된 기반시설보호 관련 정보를 특별히 보호하고, 제출되어 수집된 정보 이용에 관한 절차 수립 의무를 구체적으로 규정하여 정보공유를 촉진하고, 사고정보뿐만 아니라 보호에 필요한 다양한 종류의 정보를 포괄하여 규정한다[28]. 반면에 한국은 기반시설보호 관련 정보의 처리절차 규정이 구체적이지 않고 단지 정보공유·분석센터의 임무만 정하고 있으며[27], 전형적인 사고정보에 치우쳐 규정하고 있다.

3.2.3 국가보안시스템 보안사고 정보에 대한 별도의 공유규정 부재

미국은 국가보안시스템 운영・통제기관과 연방정보보안사고센터간 정보공유를 별도로 명시하여 국가보안시스템의 특성에 맞는 적정한 정보공유를 법제화하고 있다[29]. 반면에 한국은 국가사이버안전관리규정 등 관련 법령에 국가안보 담당기관에 특화된 정보공유 규정이 없는 상황이다.

3.2.4 정부가 직접 운용하는 주요정보통신기반시설 경보체계 부재

미국은 기반시설 경보를 정부가 직접 주도하여 전파한다[28]. 그러나 한국은 민간의 비중이 높은 정보공유・분석센터가 경보를 담당하도록 규정한다[27].

3.2.5 민간부문 경보발령 주체의 근거규정 중복

미국은 경보발령 주체에 관해 해석상 중복의 소지가 있는 규정이 없다. 그러나 한국은 민간부문 경보발령 주체가 방송통신위원회라는 점을 국가사이버안전관리규정과 정보통신망 이용촉진 및 정보보호 등에 관한 법률에서 각각 규정하여[30][31] 불필요한 중복규정으로 인한 혼란의 소지가 있다.

3.3 대응단계

3.3.1 지역사회와 긴밀한 관계의 사고대응 긴급조치 부재

미국은 지역전문가를 활용하여 지역사회 정보시스템 및 전기통신망 공격 대응을 전문적으로 지원하는 조직을 구성하도록 규정한다[32]. 반면에 한국은 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등 관련 법령에서 지역전문가를 활용하는 지역사회의 공격대응을 전혀 정한 바가 없다.

3.3.2 사이버공간에서의 공격행위를 가리키는 용어 정의 방법의 차이

미국은 공격행위의 정의규정을 별도로 사용하지 않고 관련 조문마다 개별적으로 표현하여 혼란의 소지를 없애는 안전한 방법을 택하였다. 반면에 한국은 공격행위의 정의규정을 별도로 사용하여 명확한 개념을 시도하고 있으나 유사한 의미의 용어를 사이버공격[33], 전자적 침해행위[34]로 다르게 나타내고 있어 오히려 부작용이 발생하였다.

3.4 복구단계

3.4.1 지역사회와 긴밀한 관계의 복구 지원 미흡

미국은 지역사회 정보시스템 및 전기통신망 공격으로 인한 피해복구를 지원하는 조직을 구성하도록 하고

있다[32]. 반면에 한국은 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등 관련 법령에서 지역전문가를 활용하는 지역사회의 복구를 전혀 정한 바가 없다.

3.4.2 사이버공격자에 대한 민사적 배상 불명확

미국은 사이버공격자의 민사적 배상 및 원상복구 청구권과 그 범위를 구체적으로 명시한다[35]. 반면에 한국은 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등 관련 법령에 별도의 규정이 없기 때문에 민법상의 일반규정으로 해결하여 배상 및 원상복구 범위 산정이 불명확하다.

3.4.3 신체적 손상 및 사망에 처벌규정 미비

미국은 사이버공격으로 인한 신체적 손상 및 사망의 경우를 상정하여 특별히 별도의 규정을 두고 있다[35]. 반면에 한국은 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등 처벌에 관한 내용을 정하고 있는 법령에 사이버공격으로 인한 신체적 손상 및 사망에 관한 별도의 처벌규정이 없다.

3.4.4 미수범 처벌 미비

미국은 미수범 처벌 규정을 정교하게 마련하고 있다[35]. 반면에 한국은 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등 처벌에 관한 내용을 정하고 있는 법령에 미수범 처벌 규정이 거의 없다.

4. 한국의 사이버보안 법제도 개선방안

4.1 예방단계

범국가적 사이버보안 원칙의 부재를 해결하기 위하여 사이버보안 정책의 거시적 원칙을 국가적 차원에서 정하고 이를 관련 법률에 정하는 것이 필요하다. 다만 현재로서는 개인정보보호와는 달리 사이버보안을 규율하는 일반법이 존재하지 않기 때문에 부문별 법률에 나누어 해당 부분의 원칙에 한하여 정할 수 밖에 없다.

정책수립 관련 규정의 실효성 부족을 해결하기 위하여 관련 조문의 내용을 구체적으로 정하는 것이 필요하다.

보안조치 추진체계의 구체성이 미흡한 문제를 해결하기 위하여 누가 어떤 종류의 조치를 취할지 구체적으로 정하고 이를 관계 법령의 조문에 명시하는 것이 필요하다.

또한 국회보고체계 신설로 입법부와 일반 국민들의 신뢰를 획득하는 것이 요구된다. 이는 사이버보안 강화에 대한 일각의 기우를 없애는 데 기여한다.

또한 공공부문 사이버보안 법률에 연례평가를 명시하고 관계기관 및 연구소 지원 하에 새로운 위험에 대한 예측까지 이루어지도록 법령을 개정하여 보다 적극적인 예방이 가능한 여건을 조성해야 한다.

이에 더하여 연구개발 시책의 주체, 대상, 종류를 명시하여 구체성을 부여하고 대학 등 고등교육기관에 대한 지원을 포함하여 민간연구기관 지원방법도 명확히 정할 필요가 있다.

4.2 탐지단계

정보수집 지원 시책의 실효성이 부족한 부분을 보완하여 구체적으로 지원 시책을 법률에 명시해야 한다.

또한 주요기반시설보호에 필요한 정보의 수집 및 처리 절차의 법적 근거를 신설하고, 이와 동시에 공유정보의 범위를 사고정보 외에 모든 관련 정보로 확대할 필요가 있다. 이를 통해 주요기반기설 보호를 위한 정보공유가 촉진될 수 있다.

한편 주요정보통신기반시설의 피해는 국가적인 재난이 될 수 있다는 점을 감안하면 주요정보통신기반시설 침해에 대한 경보체계를 국가가 직접 관장하는 것을 검토할 필요가 있다. 그리고 민간부문 정보통신망 침해사고에 대한 경보의 발령권자는 현재 동일한 내용을 중복해서 정하는 국가사이버안전관리규정과 정보통신망 이용촉진 및 정보보호 등에 관한 법률 중 택일하여 정하고 다른 하나에서는 삭제하는 것이 바람직하다.

4.3 대응단계

사고대응에 필요한 긴급조치는 시간적으로 급박하고 현장과 밀착되어 진행되어야 한다. 따라서 해당 지

역의 민간 전문가를 사고 초기부터 참여하는 체계를 구성하고 이를 법령에 정하는 것이 필요하다.

그리고 사이버공간에서의 공격행위를 가리키는 용어의 정비도 필요하다. 사실상 동일한 행위이면서 단지 부문별로 공격대상만 차이가 있을 뿐인데 그러한 행위를 가리키는 용어가 전혀 다른 것은 불필요한 혼란을 야기하기 때문에 개선이 필요하다.

4.4 복구단계

대응단계와 마찬가지로 복구단계에도 지역의 민간 전문가를 적극적으로 참여시키는 것을 검토할 필요가 있다. 또한 사이버공격자에 대한 배상책임을 명확히 하기 위하여 배상기준을 산정하고 이를 법령에 반영해야 한다.

사이버공격을 이용하는 범죄행위에 대한 처벌의 개선을 다각적으로 검토해야 한다. 신체적 손상이나 사망의 결과가 있는 경우 이에 대한 가중처벌 필요성을 검토하고, 미수범 처벌이 미비한 점을 보완하여 범죄예방효과를 높여야 한다.

5. 결 론

사이버보안을 다루는 실제적인 과정에 기초하여 정한 비교항목에 따라 한국과 미국의 사이버보안 법제도를 비교한 결과 한국의 법제도가 지닌 문제점이 다수 발견되었다. 그러한 문제점은 예방, 탐지, 대응, 복구 전 단계에 걸쳐 모두 존재하고 있으며, 향후 이를 해소하기 위한 법제도 개선이 요구된다.

본 논문에서 제시한 사이버보안 단계별 법제도 개선방안을 추진하기 위해서는 장기적으로는 사이버보안에 관한 일반법을 추진하고, 세부 부문별로 추가적인 입법이 필요하다면 특별법으로 보충하여 지금까지 나타난 문제점들을 보완하는 내용을 담아내는 것이 가장 이상적이라고 본다. 그러나 현실적으로 급히 개선이 필요하다면 우선 기존의 법제도 체계를 유지하는 선에서라도 법령 개정을 통하여 사이버보안 단계별로 나타나는 문제점들을 해결하여 시급한 문제점을 바로잡을 필요가 있다.

참고문헌

[1] 현대호, '정보보안 관련법제의 문제점과 개선방안', 한국법제연구원, 2007.

[2] 이창범 외 4인, '미국, 영국, 독일의 기반보호법 체계에 관한 연구', 한국인터넷진흥원, 2010.

[3] Karl Frederick Rauscher, Valery Yaschenko, Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations, EastWest institute, Information Security Institute of Moscow State University, 2011.

[4] John C. Reitz, 허순철 역, "비교법학 방법론(How To Do Comparative Law)", 경남법학, 제23집, pp. 147-167, 2008.

[5] http://www.ahnlab.com/kr/site/securityinfo/secun ews/ secuNewsView.do?menu_dist=2&seq=10897

[6] 재난 및 안전관리기본법 제3조

[7] 42 U.S.C. §5195(미국 애국자법)

[8] 6 U.S.C. §112(미국 국토안보법)

[9] 6 U.S.C. §121(미국 국토안보법)

[10] 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제4조

[11] 44 U.S.C. §3543(미국 전자정부법)

[12] 국가사이버안전관리규정 제4조

[13] 15 U.S.C. §7411(미국 사이버보안연구개발법)

[14] 44 U.S.C. §3545(미국 전자정부법)

[15] 전자정부법 제56조

[16] 전자정부법 제57조

[17] 42 U.S.C. §5195(미국 애국자법)

[18] 6 U.S.C. §192(미국 국토안보법)

[19] 44 U.S.C. §3544(미국 전자정부법)

[20] 정보통신기반 보호법 제9조

[21] 15 U.S.C. §7408(미국 사이버보안연구개발법)

[22] 정보통신기반보호법 제24조

[23] 15 U.S.C. §7403(미국 사이버보안연구개발법)

[24] 15 U.S.C. §7404(미국 사이버보안연구개발법)

[25] 15 U.S.C. §278g-3(미국 전자정부법)

[26] 6 U.S.C. §182(미국 국토안보법)

[27] 정보통신기반보호법 제16조

[28] 6 U.S.C. §133(미국 국토안보법)
[29] 44 U.S.C. §3546(미국 전자정부법)
[30] 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조의2
[31] 국가사이버안전관리규정 제11조
[32] 6 U.S.C. §144(미국 국토안보법)
[33] 국가사이버안전관리규정 제2조
[34] 정보통신기반보호법 제2조
[35] 18 U.S.C. §1030(미국 컴퓨터 사기 및 오용에 관한 법률)

[저 자 소 개]

박 상 돈 (Sangdon Park)

2002년 성균관대학교 법학과(학사)
2004년 성균관대학교 법학과(석사)
2010년 성균관대학교 법학과 박사과정 수료
2008년~현재 한국전자통신연구원 부설연구소 연구원

email : sdpark@ensec.re.kr

김 인 중 (Injung Kim)

1990년 충남대학교 전자공학과(학사)
1992년 충남대학교 전자공학과(석사)
2006년 성균관대학교 전기전자 및 컴퓨터공학부(박사)
1992년~1999년 국방과학연구소 선임연구원
2000년~현재 한국전자통신연구원 부설연구소 책임연구원 (실장)

email : cipher@ensec.re.kr