https://doi.org/10.33778/kcsa.2020.20.1.015

국가 사이버테러대응 미래 발전전략 수립에 관한 연구

김 민 수*, 양 정 모**

요 약

사이버터러나 사이버전(cyber warfare)은 더 이상 가상적 상황이 아닌 현실적이며, 실체적인 안보상황으로 상대국의 군사지휘체계는 물론 통신, 에너지, 금융, 수송체계 등 국가 주요기능 무력화의 전쟁 개념의 확대로 재인식과 국가적 차원에서의 사이버보안 미래전략 수립이 필요하다. 각 국의 사이버戰 동향 분석 및 국내 사이버戰 현황 분석을 통해 사이버보안 기술개발과 산업육성, 그리고 인력양성 전략 마련과 기존의 정보보호 정책과 법·제도을 바탕으로 신규 정책수요에 대한 체계적 발굴과 이를 통해 지속적 발생 가능한 국가적 위기를 효율적으로 관리하고, 효과적이며 능동적으로 사이버戰에 대응할 수 있는 중·장기적 사이버보안 미래전략 수립에 대하여 제안한다.

A Study on Establishing of the Future Development Strategy for National Cyber Terror Response

MinSu Kim*, Jeongmo Yang**

ABSTRACT

Cyber terror and cyberwarfare are no longer virtual, but real, and as an actual security situation, it is necessary to have new understanding through expanding the concept of war to neutralize not only the other country's military command system, but also the country's main functions such as telecommunications, energy, finance, and transport systems, and it also needs to establish the future development strategy of cyber terror response at the national level.

Through analysis of cyberwarfare trends in each country and current status of cyberwarfare in Korea, it will systematically explore the demand of new policy based on laws and systems, including the strategies of cyber security technology development, industry promotion, and manpower training and existing information protection policies. through this, it effectively manages a sustainable national crisis, and it suggests to establish a future strategy for the medium and long term cyber security that can effectively and actively respond to cyberwarfare.

Key words : Cyber Terrorism, Security Threat, ICT, National Cyber Security, Security R&D

접수일(2020년 02월 29일), 1차 수정일(2020년 03월 16일), 게재확정일(2020년 03월 30일)

* 중부대학교 정보보호학과(주저자)
** 중부대학교 정보보호학과(교신저자)

1. 서 론

지식정보사회에 대한 인식이 보편화되면서 정치・경제・문화 등 사회 전반에 걸쳐 그 특징들이 급속하게 변화하고 있다. 과거 하나의 정보는 하나의 수단으로만 사용되었다면 지식정보사회로 변화하면서 단일 수단으로만 사용되었던 하나의 정보가 다양한 조합과 분류를 통하여, 각 기술 및 영역간의 경계를 뛰어 넘는 기술혁신으로 새로운 형태의 정보로 재탄생되고 있다.

이러한 지식정보사회로의 가장 큰 원인은 정보통신의 발전이 있었기에 가능하였고, 정보통신의 기술적 혁명은 전 세계를 하나의 네트워크로 연결하여 시공간을 초월한 '사이버 공간'에서의 정보공유가 가능하게 되면서, 정보의 양은 빠른 속도로 증가하는 반면 정보의 가공・처리의 시간과 비용은 오히려 감소되는 등 지식기반산업 발전의 토대가 되었다.

그러나 지식정보사회의 순기능과 역행하여 ICT (Information and Communication Technology) 기술을 활용한 새로운 유형의 위협이 급격하게 증가하고 있다. 특히 사이버공간에서 목적・의도를 감추고 활동하는 것이 가능하기 때문에 세계 각국은 물론 테러・범죄조직・산업스파이 등의 주요 활동무대가 되어가고 있다. 이와 같은 사이버테러 공격은 기술적 발전과 사회공학적 기법 등의 활용과 그 실체적 중심점을 파악하기가 쉽지 않으며, 피해 범위도 국가적 측면에서 국가기간시설 마비, 국가 핵심기술 유출 등과 사회·경제적 측면에서 국민 생활에 혼란을 야기하는 위협에 이르기까지 광범위하게 발생하고 있다는 점에서 국가안보에 지대한 영향을 미칠 뿐만 아니라 더 나아가 글로벌 위협 요인으로 대두되고 있는 실정이다.

이에 따라 국가 안보 차원에서 사이버공격에 대한 대응 역량 강화와 국제 협력 및 대응 공조에 대한 국가 사이버테러 대응 미래 발전전략 수립이 필요해졌다. 따라서 본 연구에서는 현 시점을 기준으로 국가 사이버테러대응을 위한 미래 발전전략 수립을 위한 사이버보안 관련 법·제도, 사이버보안 기술 개발 및 산업 육선 전략, 사이버보안 인력양성 전략에 대한 방안을 제안한다.

2. 관련 연구

2.1 사이버 안보와 위협의 개념

2.1.1 사이버 안보의 개념

사이버 안보는 사이버 공간을 이용하여 프런트 앤드(front-end)와 백앤드(back-end)에서의 시스템 운영방해 및 침해행위를 통해 진행되는 다양한 공격이나 위협이 없는 상태[1]로, 정보시스템 및 정보보호의 일반적인 의미인 사이버 보안과는 다르게 사이버 공간에서 가해지는 다양한 공격들로부터 국가의 안전[2]을 최우선으로 대응하며 단순한 경제적 피해가 아닌 사회적인 혼란 등을 야기하는 보안 위협으로부터 공공 및 민간을 아우르는 대응체계를 구축하고 보안 컨트롤타워를 중심으로 역할을 수행하는 특징을 가지고 있다[3].

2.1.2 사이버 위협의 개념

사이버 위협은 네트워크를 통해 방대한 정보가 융합되어 다양한 상호작용이 가능한 사이버 공간[4]에서 익명성, 쌍방향성, 공간의 무제약성, 즉흥성과 동시성, 대칭성, 낮은 진입 비용[5] 등으로 인해 해킹(hacking), 바이러스(virus), 웜(worm), 서비스 거부 등의 공격을 통하여 국가, 기업 등 주요 시스템의 정보 절취, 훼손, 서비스 마비시키고 있다[6][7]. 또한 사이버 공격은 사회공학적 기법 등을 활용과 그 실체적 중심점을 파악하기 쉽지 않으며, 공격 시점 또한 특정화 하지 않고 지속적으로 수많은 공격자들에 의해 수행되고 있는 특징을 가지고 있다[8].

2.2 사이버보안 환경 분석

2.2.1 사이버 공격의 유형

사이버공격은 공격 주체에 따라 랜선웨어(Ransomware)와 같은 개인적 침해 위협, 기업의 전산망 마비를 통한 손실을 일으키는 디도스(DDoS, Distributed Denial of Service Attack) 공격을 포함하는 조직적 침해 위협, 개인적 침해 위협과 조직적 침해 위협의 공격수단을 포함하여, 나라간 진행되는 사이버전으로 인한 국가적 침해 위협으로 구분할 수 있다.

<표 1> 사이버 공격의 유형

구분	개인적 침해 위협	조직적 침해 위협	국가적 침해 위협
주체	· 해커 · 컴퓨터 범죄자	· 산업스파이 · 테러리스트 · 조직화된 범죄집단	· 국가 정보기관 · 사이버 전사
목적	· 금전획득 · 영웅심 발휘 · 명성획득	· 범죄조직의 이익달성 · 정치적 목적달성 · 사회·경제적 혼란 야기	· 국가기능 마비 · 국가방위 능력 마비
대상	· 민간사설망 · 공중통신망 · 개인용 컴퓨터	· 기업망 · 금융, 항공, 교통 등 정보통신망	· 국방, 외교, 공안망 등
공격방법	· 컴퓨터 바이러스 · 서비스 거부공격 · 해킹, 메일 폭탄, 홈페이지 변조, 패스워드 유출, 개인 신분 위장, 트로이목마 등	· 개인적 공격방법 포함 · 유·무선 도청 · 정보통신망 스니퍼 · 통신망 교환 시스템 동작마비 공격	· 개인, 조직적 공격 포함 · 첨단도청 및 암호해독 · 전자공격 무기, 고에너지 전파무기, 전자기파 폭탄 등 · 기타, Chipping/초미세형 로봇/전자적 미생물

2.2.2 사이버 공격기법

사이버 위협의 공격기법 유형을 넓은 의미에서 해석하면 대상 시스템의 서비스를 비활성화하거나, 해당 시스템에 접근하여 관리자 권한을 얻어 소기의 목적을 달성하는데 있다.

이와 같이 시스템 운영을 불가능하게 하거나 접속권한을 얻기 위한 다양한 공격 기법을 일반화하면 <표 1>과 같다.

<표 2> 사이버 공격기법의 유형[9]

사이버 공격기법 유형
1. 악성코드(Malware)
2. 피싱(Phishing)
3. 랜섬웨어(Ransomware)
4. 서비스 거부(DoS, Denial of Service)
5. 중간자(Man in the middle)
6. 크립토재킹(Cryptojacking)
7. SQL 인젝션(injection)
8. 제로데이 익스플로잇(Zero-day exploits)

2.2.3 사이버 공격의 양상

최근 사이버 공격은 디지털 전환으로 인한 공격 면의 확대와 더불어 통합된 인공지능(AI, Artificial Intelligence)과 스웜(swarm) 기술로 인한 파급 효과와 공격 속도가 지속적으로 높아지고 있으며, 공격의 형태가 더욱 정교해지고 있는 실정이다.

<표 3>은 해킹사고 통계로 홈페이지 변조의 경우 '16년~'17년까지 핵티비즘 목적의 공격으로 탐지 건수가 증가하였고, '18년에는 중소기업 웹취약점 점검 및 보안조치 강화 등으로 탐지 건수가 전년대비 67.1% 감소하였다. '19년에는 동일 IP에서 운영되는 다수 홈페이지 변조 등으로 증가하였다. 침해사고의 경우 해킹 공격기법의 지능화·다양화로 인한 침대사고 발생 증가에 따라 침해사고 신고 건수도 지속적으로 증가하고 있다. 악성코드 은닉사이트 탐지현황은 취약점을 복합적으로 악용하여 악성코드를 유포시키는 방법이 지속될 것으로 전망된다.

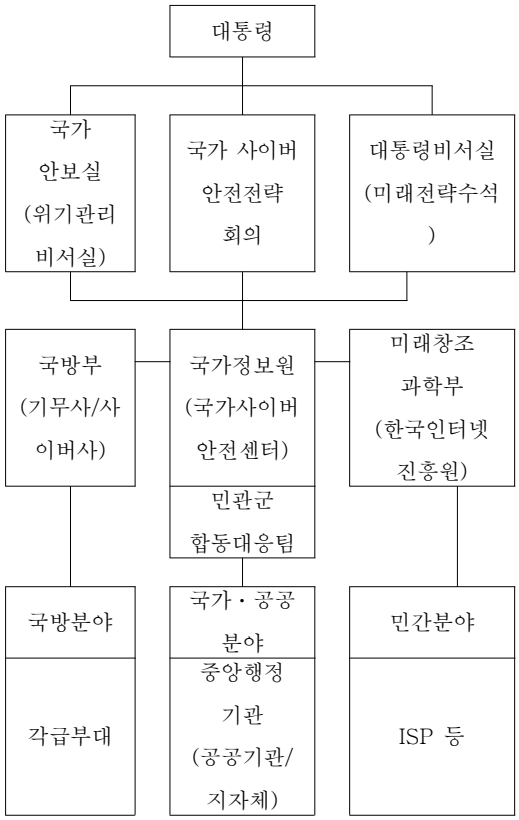
<표 3> 해킹사고 통계[10]

구분	홈페이지 변조	침해사고 신고접수	악성코드 은닉사이트 탐지
2016년	1,056	247	11,044
2017년	1,724	287	13,347
2018년	567	500	14,754
2019년	707	419	8,299

3. 기존 사이버보안 대응체계 분석

3.1 국가 사이버체계 현황

사이버보안체계는「국가사이버안전관리규정」(대통령훈령 제316호)[11]과 '사이버 분야 위기관리 표준매뉴얼'에 반영하여 시행하고 있으나, 법적 근거가 여전히 미흡함에 따라 국가의 역량을 결집하여 추진하는데 한계가 있어 보인다.



[그림 1] 국가사이버안보 관리체계

3.2 국가 사이버보안업무 수행체계

사이버보안업무 수행은 관계법령에 따라 크게 사이버안전관리 수행체계와 정보통신기반보호체계 등으로 구분해 볼 수 있다.

국가사이버안전관리체계는 2011년 농협전산망 해킹사태 등을 계기로 '국가 사이버보안 마스터플랜'을 수립하여 민·관·군 대응 기구를 구축하였고, 2013년 3.20 사이버테러와 6.25 사이버공격이 연이어 발생하자 '국가사이버보안 종합대책'을 수립·시행하고 있다.

정보통신기반보호체계는 국가·사회적으로 중요한 정보통신망을 주요 정보통신기반시설로 지정하여 중점 관리하고 전자적 침해행위에 효과적으로 대응하기 위하여 2001년「정보통신기반보호법」[12]제정 후 2019년 일부개정을 하였다.

정보통신기반보호체계는 관계 중앙행정기관과 관리기관 중심의 예방활동이 중심으로 침해사고 발생 시 사고조사를 실시하고 피해확산을 방지하는 사후 대응으로는 부족하다. 사례로 주요정보통신기반시설에 대하여 침해사고가 광범위하게 발생한 경우 정보통신기반보호위원회 위원장이 그에 필요한 응급대책, 기술지원 및 피해복구 등을 수행하기 위한 기간을 정하여 위원회에 정보통신기반 침해사고대책본부를 둘 수 있도록 하고 있다.

그러나, 사이버 특성상 사고 발생 후 대책본부를 구성하여 가동하는 것은 현실적으로 무의미해 보인다.

3.3 사이버보안 관련 법·제도 분석

3.3.1 정보통신망 이용촉진 및 정보보호 등에 관한 법률[13]

정보통신망법의 경우 사전 예방적 조치에 대하여 마련되어 있으나, 지식정보사회에서의 다양한 사이버공격에 대응하기는 미흡한 실정이다. 사전 예방적 조치로 개인정보 보호조치, 정보통신망의 안전성 확보, 정보통신시설의 보호 및 정보보호 관리체계의 인증, 이용자에 대한 보호조치로 되어 있으나 세부적인 관리지침이 마련되어야 한다.

또한 사이버침해사고에 대하여 백신소프트웨어 제공 및 이용자의 PC에 대한 취약점 점검 등 이용자에 대한 보호조치를 위한 법적 근거를 마련하여야 한다.

3.3.2 정보통신기반 보호법[12]

정보통신기반 보호법은 미래창조과학부, 국가정보원, 국방부를 컨트롤타워로 공공 분야, 민간 분야, 국방 분야를 구분하여 주요정보통신기반시설 보호대책 및 주요정보통신기반시설보호계획의 지

침에 대한 수립을 협의하여 정하도록 하고 있다.

하지만 현재의 사이버위협은 특히 공공 및 민간 분야를 구분하지 않고, 또한 침해사고 발생 시 어느 한 분야의 피해가 아닌 국가적 피해로 야기될 수 있기 때문에 2원화된 체계 유지에 대하여 고려하여야 한다. 국방 분야를 제외한 공공 및 민간 분야에 대한 범 국가적인 컨트롤 타워의 일원화가 필요한 실정이다.

또한 주요정보통신기반시설의 경우 정보통신 및 미디어, 금융기관, 교통수송, 에너지, 원자력, 식품의약품관리, 보건복지, 사회안전시설 등을 중심으로 지정되고 있다. 지식정보사회에서 IT와의 융합을 통한 신생산업이 개발 및 발전되고 있기 때문에 그 범위를 확대하여 지정하여야 한다.

그리고 주요정보통신기반시설에 대한 취약점 분석 및 평가에 있어 국가 중요정보를 취급하여야 하는 보안업무 특성상 보안 컨설팅에 있어 신중한 접근이 필요하다.

3.3.3 전자정부법[14]

전자정부법의 경우 주무부처가 행정자치부로 안전한 대민서비스를 위한 보안대책 수립 및 시행으로, 국가정보화기본법과 비교해 볼 때, 그 차이점을 뚜렷하지 않다. 유사 법안에 대한 법률 이원화로 인한 권한과 책임의 문제점이 있을 수 있기 때문에 법률의 통합적 검토가 다시 이루어져야 한다.

3.3.4 국가사이버안전관리규정[11]

국가사이버안전관리규정의 경우 '정보통신기반보호법'과 '정보통신망법'에서 규정하고 있는 침해대응과 관련하여 규제적 중복이 있기 때문에, 규정에 대한 통합적 검토가 다시 이루어져야 한다.

3.3.5 국가정보화기본법[15]

국가정보화기본법의 경우 주무부처가 미래창조과학부로 안전한 대민서비스를 위한 보안대책 수립 및 시행으로, 전자정부법과 비교해 볼 때, 그 차이점을 뚜렷하지 않다. 유사 법안에 대한 법률 이원화로 인한 권한과 책임의 문제점이 있을 수 있기 때문에 법률의 통합적 검토가 다시 이루어져야 한다.

3.3.6 전자금융거래법[16]

전자금융거래법에서 배상 책임에 있어 각 호에 해당하는 사로로 인하여 이용자에게 손해가 발생한 경우로 규정하고 있다.

하지만, 각호에 대한 개념과 범위가 불분명하고 침해사고에 대한 구분이 분명하지 않기 때문에 명확한 개념적 검토가 필요하다.

4. 국가 사이버테러 대응 발전전략

4.1 국가 사이버보안 관련 제도 개선방안

4.1.1 사이버보안 컨트롤 타워 구축

사이버보안 컨트롤타워의 주된 역할은 국가의 사이버보안정책·전략을 종합·조정하고 국가적 중요 안건을 심의하는 회의기구를 운영하며, 국가적 위기발생시 신속하고 정확한 상황판단 및 위기관리를 주도하는 것이다. 구체적인 역할로는 사이버보안 정책 조정, 중앙 행정부처간 업무협력 조율, 실무총괄기관의 감시·통제 등을 둘 수 있다. 또한 컨트롤 타워는 민·관·군 영역 전반에 대해 예방·점검, 사고조사·복구 등의 모든 집행업무를 수행하는 것이 아니라, 각 영역별로 기능과 효율을 최대한 발휘할 수 있도록 조화와 균형을 이루는 조정자 내지는 중재자 역할을 수행해야 한다. 이와 관련하여 현재 「국가사이버테러방지법안」등 관계법령 제·개정이 추진 중에 있다. 그렇다면 법령이 제정될 경우 '컨트롤 타워' 역할은 청와대가 담당할 필요가 있고 「국가사이버안전관리규정」에 따라 국가·공공기관에 대해 기존에 사이버보안업무를 총괄·수행해 왔던 국가정보원이 '실무총괄' 역할을 수행함으로써 컨트롤타워의 역할을 지원토록 사이버보안체계를 구축하는 것이 바람직하다.

4.1.2 사이버보안 업무에 대한 통제

· 개인 프라이버시 침해

국가사이버보안 법률안이 제정되면 국가정보원이 민간영역까지 개입하게 되는 빌미를 제공할 수 있다는 우려가 많다. 국가정보원이 사이버보안이라는 미명아래 개인 프라이버시를 침해하고 민간

인을 사찰할 수 있다는 우려가 있다. 주요 근거로는 국가정보원이 전산망 보안관제 및 사이버위협정보 공유를 통해 합법적으로 개인 프라이버시 침해가 일상화되고 국가정보원의 정치적 편향성으로 인해 정치적 목적으로 악용될 수 있다. 무엇보다도 정보는 신뢰에 기반하여 공유되고 통제 가능해야 하므로 비밀정보기관인 국가정보원이 개인정보에 접근하는 것은 적합하지 않다는 것이다.

그러나, 국가정보원이 정보통신망 운영기관과 공유하고자 하는 위협정보는 개인 신상이나 소유자료 또는 개인 간의 일반적인 통신내용이 아니라 각 기관이 자체 사용하는 침입차단시스템・침입탐지시스템 등 상용 정보보호시스템에서 해킹・DDoS공격 등을 알려주는 일반 정보로 알려져 있다. 이 정보는 개인 프라이버시와는 무관하며 사이버공격을 사전 탐지하여 대응하기 위해 필요한 정보이다. 만약, 국가정보원이 사이버공격 정보를 통해 개인 프라이버시를 침해할 수 있다면 정보통신망 운용기관이나 기업체의 정보보호 업무를 대행하고 있는 전문업체도 마찬가지이다. 다만, 정보공유 과정에서 개인 프라이버시 침해 우려가 있는 만큼 정보공유 절차에 대한 신뢰성을 확보하고 정보에 대한 통제를 강화하는 방향으로 법제화할 필요가 있다.

・정보 독점

각급기관이 사이버공격 관련 정보를 국가정보원에 제공토록 함으로써 국가정보원이 정보를 독점할 우려가 있다는 지적이 있다. 사이버공격 정보를 제공하는 목적은 한 기관에 발생한 공격기법이나 악성코드가 다른 기관에도 재차 사용되어 피해가 확산되는 것을 방지하기 위한 것이다. 백신업체가 개인PC의 위협정보를 수집하여 보안 패치를 제작하고 있는 것과 마찬가지이다. 즉, 위협정보를 수집하여 국가차원에서 사이버공간에 대한 위협동향을 분석하고 관련 대책을 지원하는 것이므로 모든 정보를 가져가서 되돌려주지 않는 '정보독점'과는 다른 개념이다.

전문가들은 우리나라의 경우 민간・공공간 사이버위협정보가 원활히 공유되지 않고 있다고 지적하고 오히려 정보공유 활성화를 요구하고 있다. 민간과 공공의 정보 활용의 어려움 때문에 실질적인 공격 예방과 대응을 어렵게 한다는 평가이다. 국가정보원이 정보수집과 분석을 주 업무로 하고 있는 정보 전문기관이므로 다른 어느 부처보다 업무를 잘 할 수 있을 것으로 보인다. 다만, 국가정보원이 작성한 분석정보가 각급기관에 원활히 공유토록 하여 사이버공격을 사전 예방하고 대응할 수 있도록 제도화할 필요가 있다.

・권한 강화

국가정보원이 민간영역까지 권한을 갖게 되고 사이버공간에 대한 통제력이 강화된다는 주장이 많다. 하지만, 정보보안업무 특성상 일정부분 권한과 함께 책임을 부여하는 것은 불가피해 보인다. 다른 기관에 총괄기관의 역할을 부여할 경우에도 동일한 권한 강화 우려가 있을 수 있다. 그러므로 법률 제정과정에서 정보보안 전문가 및 시민단체 등 각계각층의 의견을 적극 수렴함으로써 최적의 균형점을 찾는 것이 중요하기 때문에 여・야간의 원만한 합의가 도출되어 민주적 정당성이 담보된 법률안을 제정하여야 한다. 오히려 법제화를 통해 국가정보원에 대한 통제 효과를 높이는 방향으로 접근해 볼 필요가 있다. 이러한 해법으로 과도한 권한집중으로 이러한 우려를 불식시키기 위해 견제와 감시 장치가 반드시 필요하고 국회에 보고의무를 규정하는 법안 제정을 해야 한다.

・보안관제에 의한 민간사찰

보안관제는 시스템 인입부에서 외부로부터 들어오는 해킹・바이러스 공격 등 유해 트래픽을 탐지하는 것으로, 기술적 측면에서 보안관제 대상 시스템 내부의 저장 자료나 이메일 등에 대해서는 접근 자체는 불가능하다. 시스템에 저장된 정보를 열람하기 위해서는 해당기관이 관리하는 비밀번호・인증키 등 접근권한을 별도로 부여받아야만 가능하다. 관제시스템은 해킹 등의 사이버공격을 사전 탐지・대응하기 위한 기본 구성요소로 국내는 물론 세계 각국이 동일한 시스템을 사용 중이다.

이 시스템은 관제 대상기관에 설치되어 기관 자체적으로 보안관제를 실시하고 있으며, 필요한 경우 다른 기관과 탐지정보만을 공유하고 있어 악용 자체는 크지 않다. 다만, 악용될 개연성이 있는 만큼 사용 목적을 명확히 하고 위반 시 처벌 조항을 규정할 필요가 있어 보인다. 또한, 양 법률안은

책임기관이 사이버공격 정보를 탐지·대응할 수 있는 보안관제센터를 구축하거나 전문기관에 관제를 위탁하도록 하고 있다.

국가정보원이 민간분야를 관제토록 하겠다는 것이 아니라 중요 전산망 보호를 위해 해당 책임기관이 보안관제를 하도록 하자는 것이 법조문의 성격이다. 이 또한 책임기관이 재정상 이유 등으로 보안관제센터 설립·운영이 어려운 경우 기존에 운영되고 있는 국가정보원 등에 보안관제를 위탁토록 하고 있으나, 민간인 사찰에 대한 우려가 있으므로 대체 법안 마련 시 국가정보원의 민간기관에 대한 직접 보안관제를 제한토록 법제화할 필요가 있다.

· 사고조사 과정에서의 개인정보침해 등

사고조사는 사고원인을 파악하여 재발방지대책을 마련하기 위한 기본 업무이다. 개인정보 침해에 대해서는 지나치게 우려할 필요는 없어 보인다. 왜냐하면, 현재 시행되고 있는 통신비밀보호법은 세계적인 유례가 없을 정도로 개인의 사생활 보호라는 측면에서 엄격한 통제를 가하고 있어 만약 사고의 원인을 분석하기 위한 정보가 '통신사실확인자료'에 해당되는 경우 「통신비밀보호법」에 의거 통신사실확인자료 제공의 요건과 절차를 준수해야 하기 때문이다.

「개인정보보호법」도 개인정보의 수집·이용 절차에 대해 엄격히 규정하고 있기 때문에 국가정보원이 개인정보를 불법 수집·관리·이용한 경우에는 관련법에 의거하여 법적 처벌이 가능하다. 다만, 사고조사에 대해 우려하는 시각이 있는 만큼 모든 경우에 사고조사를 할 수 있도록 하는 것이 아니라 국가보안 및 이익에 중대한 영향을 미칠 수 있는 경우에 한해 정부합동조사가 가능하도록 법제화해야 한다.

4.2 사이버보안 기술 개발 및 산업 육성 전략 방안

4.2.1 사이버보안 R&D 협력체계 강화

국가적 과제인 사이버보안 R&D의 체계적 추진과 활용성을 높이기 위해, 미래창조과학부, 국방부, 국정원 등 각 부처 간 협력과 연계를 강화해야 한다. 이를 위해 「사이버보안 R&D 조정 협의체」를 구성하고 운영하여 R&D 결과물에 대한 원천기술 및 사업화 성공률을 제고하여야 한다.

협의체는 사이버보안 R&D 컨트롤타워(정부기관)를 중심으로 각 연구기관 및 외부전문위원회 그리고 정부산하기관과의 신규과제 발굴, 기획, 결과물 사업화를 위한 지속적인 협력체계를 구성하여야 한다.

4.2.2 정보공유 및 성과확산 강화

사이버보안 R&D 조정 협의체를 중심으로 기술수요조사서를 통해 개발 사업의 추진 방향을 설정하게 되고, 이를 통해 개발된 연구 성과물의 기술이전 및 사업화가 이루어지도록 개발 완료될 기술들의 사전 공개를 통해 수요처 및 기관이 조기 기술이전 및 사업화를 효율적으로 추진할 수 있도록 성과확산 활동을 강화하여야 한다.

4.2.3 글로벌 국제협력 강화

사이버보안 R&D 사업에 있어 해외 연구자 및 기업의 참여기회를 확대하고 국가 간, 기업 간 컨소시엄을 통해 다자간 R&D 협력 연구사업을 추진해야 한다.

이를 위해 미국 DHS는 BAA(Broad Agency Announcement) 프로그램을 통해 전 세계 연구자를 대상으로 연구책임자를 공모하여 운영하고 있다. 또한 글로벌 사이버보안 R&D 경쟁력 강화를 위한 국제공동연구를 확대 지원하여야 한다.

4.2.4 사이버보안 R&D 특화센터 구축

사이버보안 R&D를 통해 기술 사업화의 성공률 제고를 위해 연구개발 시제품의 성능평가용 특화센터를 구축해야 한다. 사이버위협에 대한 공격 시나리오 및 실험 데이터 등을 통해 개발 중인 제품의 보안성 검증, 평가 수행을 통해 상용화에 인프라 지원을 하게 된다.

미국의 경우 6개의 국립 테스트 랩(INL, SNL, PNNL, ORNL, ANL, LANL)을 중심으로 분산형 테스트 랩 운영과 활동결과를 공유하여 보안성을 제고하고 있다.

4.2.5 사이버보안 R&D 벤처 및 창업지원

사이버보안 R&D를 위한 통합적인 벤처 및 창업지원 정책 추진체계를 마련할 필요가 있다. 미국 등

의 주요국은 R&D 재원을 중심으로 벤처 및 창원지원(인프라, 자금)을 연계하는 통합 추진체계를 운영하고 있다.

또한 기존 벤처 및 창원 지원 사업에서 재도전 기업인의 참여를 확대하여 재창업 기업에게 참여기회를 부여 및 정책적 금융 지원을 위한 제도적 보완이 필요하다.

4.3 사이버보안 인력양성 전략 방안

4.3.1 사이버보안 전문인력 적용을 위한 직업 분류의 체계화

각 산업별로 구축되어 있는 IT 시스템 및 사이버 생태계, 보안 우선순위, 대표적인 위협 요인 등의 차이가 있고, 특정 산업에 대한 이해가 수반되어야만 실질적인 보안 업무 수행이 가능하게 된다.

따라서 향후 사이버보안 전문인력 양성을 더욱 가속화하기 위해서는 직업 분류 체계화 작업과 함께, 기업의 보안인력 확충을 위한 정책적 지원이 뒷받침 되어야 한다.

4.3.2 미래 네트워크 인프라 확장에 따른 보안인재 양성체계 구축

사이버보안 전문인력 양성을 위한 직업 분류 체계화 작업과 함께, 미래 네트워크 인프라 확장에 따라 일원화된 교육 프로그램이나 특정 역량만을 부양하는 인력양성 정책보다는 포괄적인 관점에서 사이버보안 인재를 키울 수 있는 교육 인프라를 구축하여야 한다.

4.3.3 사이버보안 전문인력 양성을 위한 협의체 구성

사이버보안 인력 수요 및 보안 이슈에 대한 파악은 전문 기술과 노하우를 보유한 기업들이기 때문에 사이버보안 인력난에 신속히 대응할 수 있는 실무 중심의 적합한 교육과정 개발에 있어, 교육기관의 연계를 통해 이들의 기술력과 노하우를 교육 커리큘럼을 개발하고 정부 주도하에 전문인력 양산을 체계화할 수 있다.

이를 위해 산·학 연계를 촉진하기 위한 수단으로 사이버보안 전문인력 양산을 위한 협의체 구성이 필요하며, 협의체를 통해 사이버보안 전문 교원 확보, 파트너십 지원 프로그램, 기술 상용화 촉진 정책 등을 개발 및 특화할 수 있으며, 사이버보안에 관심이 있는 이들을 모으고 기회를 제공하는 포털로서의 역할도 수행이 가능하다.

4.3.4 전주기 사이버보안 전문인력 양성체계 구축

우수한 보안영재 발굴과 특성화 대학의 지원 등 체계적인 육성을 위한 기반을 구축하기 위해 중고등 및 영재교육원에 대한 지원을 통해, 사이버보안 전문인력 양성을 위한 기초를 다지고 보안 예비 인력에 대한 체계적인 육성 및 전문성 강화를 위한 생애 주기형 양성체계를 구축하여야 한다.

4.3.5 해외 인력수출 기회 모색

급격히 증가하는 사이버보안 수요에 따라 업계는 전 세계적으로 사이버보안 전문가 수급에 심각한 어려움을 겪고 있다. IT전문 취업전문기업 Experis 조사에 따르면, 2019년까지 사이버보안 전문가 수요는 전 세계적으로 6백만 명에 달하나, 150만 명 이상의 인력 부족이 발생할 것으로 전망하고 있다.

또한 Symantec 前CEO, 마이클 브라운은 인재확보가 기업의 최우선 과제라고 밝히는 등, 미국 내 글로벌 기업들은 앞 다투어 사이버보안 분야 인재 확보 경쟁에 뛰어들고 있는 상황이다. 미국 내 글로벌 기업들은 H-1B 비자(전문 인력을 채용을 위한 비 이민 비자) 스폰서를 통해 이스라엘, 인도 등으로부터 IT전문가 영입에 노력 중에 있다.

따라서, 차세대 사이버보안산업 분야에 국내 인재들이 해외 기업에 취업할 수 있게 정부는 국가간 협력체계를 구축과 지원을 통해 사이버보안 전문 인력에 대한 동기부여 및 활성화에 노력을 기울여야 한다.

5. 결론

지식정보사회에서의 활동 공간인 사이버공간에서의 역기능인 사이버 위협에 대한 보안 문제점을 해소하기 위한 국가 사이버테러 대응 미래 발전전략 수립이 필요한 실정이다.

이를 위해, 사이버보안 환경 분석과 함께 기존 사이버보안 대응 체계에 대한 선행 연구를 바탕으로 국내외 사이버보안 관련 법·제도와 정책을 비교 분석하고 사이버보안 관련 법령 개선방안과 사이버보안 기술 개발 및 산업 육성 전략 도출 그리고 사이버보안 전문인력양성 전략에 대한 발전전략 수립 방안을 제안하였다.

국가 사이버테러 대응 전략으로는 첫째, 국가 사이버보안 관련 제도 개선방안 둘째, 사이버보안 기술 개발 및 산업 육성 전략방안 셋째, 사이버보안 인력 양성 전략 방안을 제시하였다.

국가 사이버보안 관련 제도 개선방안은 사이버보안 컨트롤 타워 구축과 사이버보안 업무에 대한 통제에 대한 필요성을 강조하였고, 사이버보안 기술 개발 및 산업 육성 전략으로 사이버보안 R&D 협력체계 강화, 정보공유 및 성과확산 강화, 글로벌 국제협력 강화, 사이버보안 R&D 특화센터 구축, 사이버보안 R&D 벤처 및 창업지원과 관련된 방안을 제시하였다. 또한 사이버 보안 인력양성 전략으로 사이버보안 전문인력 적용을 위한 직업분류의 체계화, 미래 네트워크 인프라 확장에 따른 보안인재 양성체계 구축, 사이버보안 전문인력 양성을 위한 협의체 구성, 전주기 사이버보안 전문인력 양성체계 구축, 해외 인력수출 기회 모색을 제시하였다.

마지막으로 차세대 사이버보안산업 분야에 국내 인재들이 해외 기업에 취업할 수 있게 정부는 국가 간 협력체계를 구축과 지원을 통해 사이버보안 전문 인력에 대한 동기부여 및 활성화에 노력을 기울여야 한다.

참 고 문 헌

[1] 조화순, “사이버안보의 국제정치와 미래전략”, 한국의 중장기 미래전략, 2015.

[2] 조화순, “한국과 미국의 사이버안보 거버넌스 사이버위협의 안보화 관전에서의 비교”, 한국정보사회학회, 2017.

[3] 홍준호, “사이버보안 컨트롤타워 필요성에 관한 연구”, 한국법학회, 2019.

[4] Cavelty, Myriam Dunn. “Cyber-Security.” in Alan Collins (ed.), *Contemporary Security Studies,* Fourth Edition. Oxford: Oxford University Press, 2016.

[5] 박성용, “SWOT 분석을 통한 한국의 사이버 안보 위협 전략적 대응 방향성”, 한국동북아논총, 2019.

[6] 이성민, “국가 사이버 안보전략 연구: 주요국 양상과 한국적 상황 분석”, 경기대학교 박사학위논문, 2016.

[7] 김동희 외, “사이버 위협정보 공유체계 구축방안에 관한 연구-미국 사례를 중심으로-”, 한국융합보안학회, Vol.17, No.2, 2017.

[8] 김익환 외, “위협간 연관분석을 위한 사이버위협인텔리전스 데이터 모델 제안”, 한국통신학회, 2019.

[9] http://www.itworld.co.kr/news/145522

[10] http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1363

[11] 국가사이버안전관리규정(대통령훈령 제316호)

[12] 정보통신기반 보호법(법률 제16758호)

[13] 정보통신망 이용촉진 및 정보보호 등에 관한 법률(법률 제16021호)

[14] 전자정부법(법률 제14914호)

[15] 국가정보화 기본법(법률 제15369호)

[16] 전자금융거래법(법률 제14828호)

〔저자소개〕

김 민 수 (Minsu Kim)

2004년 컴퓨터공학사
2012년 경호안전학석사
2015년 산업보안학박사
현 재 중부대학교 정보보호학과 조교수

email : mskim@joongbu.ac.kr

양 정 모 (Jeongmo Yang)

1984년 2월 동국대학교 사범대학 수학과 학사
1989년 2월 동국대학교 대학원 수학과 이학석사
1997년 2월 단국대학교 대학원 수학과 이학박사
1995년 3월~ 중부대학교 정보보호학과 교수

email : jmyang@joongbu.ac.kr