국가 사이버안보 시스템 관련 법률안 분석과 연구

남원희* · 박대우**

*호서대학교 벤처전문대학원

Mobile Auto questions and scoring system

Won-Hee Nam* · Dea-Woo Park**

*Hoseo Graduate School of Venture

E-mail : dlbongmt@na.go.kr · prof_pdw@naver.com

요 약

스마트폰에서 인터넷뱅킹, 전자상거래, 업무의 처리 등 국민의 정치, 경제, 사회 실생활의 업무는 사이버 공간에서도 처리된다. 사이버 공간과 실제 공간의 경계가 모호해짐에 따라, 국가의 인프라 시설 관리 및 운영에서도 사이버 테러가 발생하고, 국가 안보위협의 가능성이 높아지고 있다. 국가의 주요 인프라 및 정부 서비스가 정보통신 시스템과 시설로 연계되어 있다. 사이버 테러와 국가 사이버안보에 관한 중대한 위협에 대처하기 위한 법과 제도적 장치로서, 국가사이버안보시스템에 관한 법률체계의 정립이 필요하다. 이를 위해 현재 국회에 계류 중인 사이버안보 관련법을 중심으로 분석과 현행 우리나라의 사이버 관련 법체계와 대별하여 분석하고, 국가사이버안보 컨트롤타워 문제와 국가사이버안보 인력 및 산업육성이 논의되어져야 하며, 사이버테러 대응 체계를 분석하여, 국가 사이버안보 시스템 관련 법률제정의 필요성을 연구한다.

ABSTRACT

Internet baking, e-commerce, business processing, etc on smartphone handing could be possible in present days. Ambiguity between cyber and real life has made vulnerability on infrastructure, Gov’t Service and National security by cyber terrorism. Especially, Lots of Infrastructure and Gov’t Service based on Information Technology were exposed by Cyber terror. Legal system should be improved to keep from these threats. This paper proposed needs of cyber legal system by analyzing proposed cyber related code on Korean National Assembly, issue on Cyber Control Tower, National Cyber Security Industry and Human resource.

키워드

사이버, 사이버보안, 법률, 국가사이버안보

Key word

Cyber, CyberSecurity, Law, National CyberSecurity

Ⅰ. 서 론

현대는 전철과 버스의 교통카드사용, 전력사용, 전자사이버경제, 사이버안보 등 사이버와 연계되는 국민생활이 이루어지고 있다. 하지만 스마트폰을 통한 스미싱[1], 파망, 해킹 등 공격과 안전한 국민생활을 위한 사이버 네트워크가 안정적[2]으로 방해 없이 작동하는 것이 매우 중요하다. 사이버 공간과 실제 공간 간의 경계가 모호해짐에 따라 사이버 테러 등의 가능성과 그 파급 효과가 날로 커지고 있으며 특히, 국가의 주요 인프라 및 서비스가 정보통신시설로 연계되어 사이버 테러는 국가안보에 중대한 위협이 되고 있다.

국가사이버안보 법률체계는 첫째, 국가사이버안보 컨트롤타워 문제와 둘째, 국가사이버안보 인력 및 산업육성이 동시에 논의되어져야 한다.

본 논문에서는 현 사이버안보 관련법을 중심으

로 살펴보고, 현행 우리나라의 사이버 관련 법체계 대별 사이버테러 대응체계, 이를 위한 법률제정 필요성과 찬성 및 반대의 입장[3]에서 국가사이버안보법 제정 검토 방향을 연구한다.

Ⅱ. 관련연구

2.1 사이버안보 관련 법체계

1) 정보통신망·정보시스템보호 관련법 : 정보통신망법, 정보통신기반보호법, 전자정부법, 국가사이버안전관리규정

2) 개인정보·사생활 보호 관련법 : 개인정보 보호법, 정보통신망법, 위치정보법, 신용정보법, 통신비밀 보호법

3) 사이버안전 인력·산업 육성 관련법 : 정보통신산업진흥법, 정보통신망법, 국가정보화기본법, 산업기술보호법, 국가사이버안전관리규정

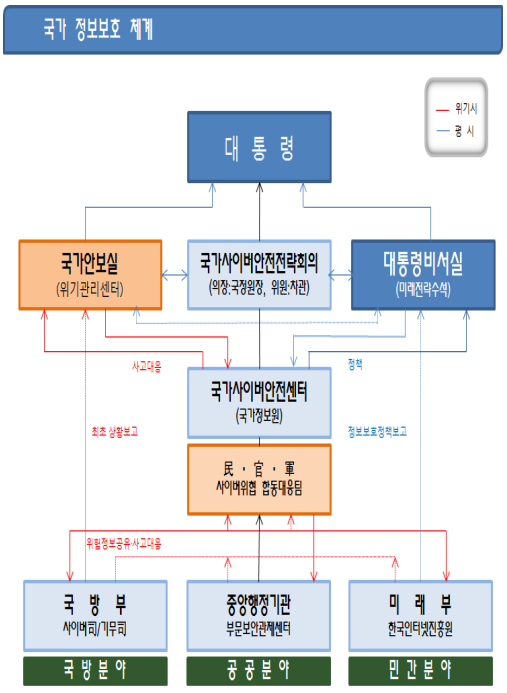

그림 1. 2014년 현재 국가정보체계

Ⅲ. 사이버테러(위협) 대응 시스템

3.1 사이버위기관리 체계(실제)

일상적 상황에서는 분산관리 방식을 적용하여 민(방송통신위원회)·관(국가정보원)·군(국방부) 분야별로 역할을 분산, 국가안보 사안에 대해서는 국가정보원이 총괄하는 중앙통제방식 적용한다. 최근에는 국가정보원·미래부·방송통신위원회·국방부·안전행정부·금융위원회 등 관계부처가 참여하고 국가정보원 중심으로 민·관·군 합동대응체계로 대응하고 있다.

국가사이버안보 마스터플랜의 주요 내용은 다음과 같다.

외부로부터의 사이버공격이 국민의 재산과 국가안보를 위협하는 상황 인식 공유.

'국가사이버안전센터'를 중심으로 관계 부처간 협력·공조와 민간 전문가 참여 확대.

국가정보원의 컨트롤타워 기능과 부처별 역할을 명확히 하여 기관간의 업무 혼선·중복 및 사각지대 발생의 문제점 해소 추진.

3.2. 사이버관련 법령 대응체계

사이버위협 대응에서 현재 국가정보원의 컨트롤타워 기능 수행의 주요 규범으로서 작용할 '국가사이버안전관리규정'은 법률이 아닌 대통령훈령으로서, 그 범위가 공공부문에 한정되고 행정기관에만 효력이 있다. 관계부처들이 합동으로 국가사이버안보 마스터플랜을 마련하면서, 사이버위협 대응을 보다 효율화하기 위해 관련 법령의 정비를 추진하기로 하였으나 답보 상태이다. 관련 법령의 정비가 미진함에 따라 집행력이 미약하고 대국민 효력 발휘에 한계가 있다.

현재 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「정보통신기반보호법」, 「국가사이버안전관리규정」 등에 의해서 국가사이버전략회의, 국가사이버안전대책회의, 국가사이버안전센터 등 국가기관의 사이버안보 및 위기관리체계 마련, 시행하고 있다. 하지만 사이버위협에 대한 대응하기 위해 추진체계의 법적 근거가 명확하고, 민간기업에 대한 행정지도 및 관련자 처벌 등 대국민 효력에 필요한 근거 마련이 필요하다.

Ⅳ. 사이버안보 법률안 필요성과 논점

4.1 사이버 위협 및 법률 제정 필요성

북한의 국방위 정찰총국 중심 사이버공격 전문조직 가동 국가안보 위협하고 있어, 사이버 위협이 가중되고 있으며, 중국의 국가기밀, 첨단산업기밀, 개인정보에 대한 해킹 공격이 이루어지고 있다.

2009년 7.7 DDos공격, 2011년 3.4DDos공격, 4.12농협전산망 파괴, 2013년 방송·금융사 전산망 마비 3.20 사이버테러, 6.25사이버공격 등에 노출 되고 있다.

우리나라는 사이버안보 관련 업무가 소관부처별로 이루어지고 각 부처의 업무범위는 정보자산과 기반시설에 대한 침해사고 대응 및 복구에 한정, 현재 「국가사이버안전관리규정」은 국가 및 공공기관에만 적용되는 대통령훈령으로서 종합적이고 체계적인 근거 법령 미흡하다.

따라서 국가사이버안전 확보, 국가사이버위기관리 기구 상설화, 민관 간 정보 공유로 사이버공격에 대응할 수 있는 중심조직과 법적지위 확보 위한 근거법 제정 필요성 있다.

4.2 사이버테러(위협) 및 법률 제정 찬성 측면

국회 정보위원회에 계류 중인 법률안과 같이 국가의 사이버테러(위협)을 관리를 총괄할 수 있는 체계를 두는 법률 제정에 찬성하는 입장이다.

우리의 경우 국가차원의 사이버테러(위협) 관리 등을 위한 법제가 시급하다는 점과 현재 국가사이버안보마스터플랜과 훈령에 따라 국정원이 실제 컨트롤타워 역할을 수행하고 있는 부분을 법률에 규정 그 기능을 강화해야 한다.

국가정보원은 국내에서 사이버공격 등에 대한 분석 및 대응에 있어 최고의 기술력과 노하우가 있다는 점 등을 강조한다.

4.3 사이버테러(위협) 및 법률 제정 반성 측면

정보기관에 의한 정보독점 폐해를 우려하며 사이버안보법의 제정을 반대하는 입장이다.

국가국정원의 사이버 공간에 대한 통제력 과도로 위험소지가 있으며, 국가국정원의 활동이 민간영역까지 개입 빌미 제공여지가 있다.

또한 민간과 공공 간의 정보공유 과정에서 개인정보 유출, 프라이버시 침해가 있을 수 있다.

4.4 국가사이버컨트롤타워 필요성 및 감시체계

향후 사이버테러로 인한 국가 안보를 위협하는 상황 등을 미연에 방지하기 위해서는 국가 전체의 사이버위기관리를 총괄할 수 있는 법률 체계를 구축할 필요성이 있다고 보이며, 그러한 경우에도 특히 컨트롤타워 기관에 대한 민주적인 감시와 통제 가능한 장치 필요하다.

Ⅴ. 결 론

본 논문에서는 국가사이버안보 법률체계에서 현재 사이버안보 관련법을 중심으로 살펴보고, 현행 우리나라의 사이버 관련 법체계 대별 사이버테러 대응체계, 이를 위한 법률제정 필요성을 연구하였다.

향 후 연구로는 국가사이버안보법률 제정에 대한 방향을 연구한다.

참고문헌

[1] “In-Woo Park, Dea-Woo Park, “A Study on the Analysis and Security Measures for Smishing Hacking Attacks”, International Conference on Computing and Convergence Technology, Oct, Korea, 2013.

[2] Dea-woo Park, “Guideline for Countermeasures against Smishing Incident“, CJK IT Standards Meeting, April, Korea, 2014.

[3] 남원희, 국가사이버안보정책포럼 위크숍, 국가사이버법률 필요성 및 법률안 현황, 2014. 7.18.