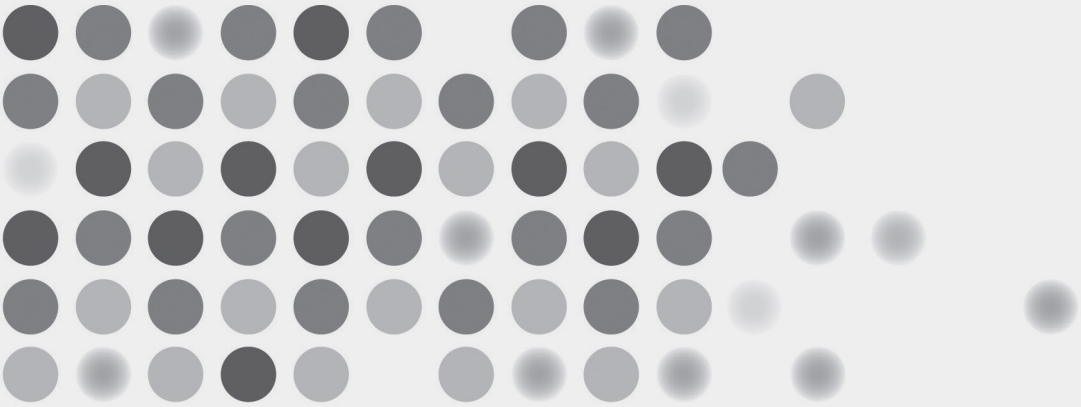
연구총서 15-B-11

한 · 미 사이버테러 대응정책 협력방안 연구

김한균 | 조민정 | 박소영 | 안수정



KIC 한국형사정책연구원
KOREAN INSTITUTE OF CRIMINOLOGY

발간사

본 보고서는 한국형사정책연구원 국제협력사업 중에서 사이버범죄 및 보안 분야 연구와 기술적 지원협력 사업 추진성과를 기반으로, 사이버범죄와 더 포괄적인 사이버안보의 측면에서 특히 중국, 북한 등 사이버테러 관련국 및 그 실태에 대한 기초적인 논의자료를 제공하는데 목적이 있습니다.

향후 안보협력의 가장 중요한 동반자인 한국과 미국 간의 사이버안보 정책협력의 기반구축을 위해 양국 주요 형사정책 연구기관들의 공동연구를 위한 틀을 제시하는데 기여할 것으로 기대합니다.

연구를 성실히 수행해준 김한균 국제협력센터장과 조민정, 박소영, 안수정 연구원의 노고에 감사드립니다.

2015년 12월

한국형사정책연구원

원장 김 진 환

목 차

표 차례

그림 차례

국문요약

1. 본 연구는 한국형사정책연구원 국제협력사업인 사이버범죄 및 보안 분야 연구와 기술적 지원(technical assistance)협력 사업 추진성과를 기반으로, 미국 내 주요 연구협력기관과의 공동연구협력사업을 통해 향후 과제를 발전적으로 제시하는데 목적이 있다.

2. 본 연구의 배경은 현 정부의 「동북아 평화협력 구상」이다. 특히 사이버 공간에서의 협력증진은 동북아평화협력구상의 중요한 의제이기도 하면서, 동북아 지역의 주요이해관계자인 미국과의 공동관심사이기도 하다.

3. 본 연구는 사이버범죄와 더 포괄적인 사이버안보의 측면에서 특히 중국, 북한 등 사이버테러 관련국 및 그 실태에 대한 기초적인 논의자료를 제공하고, 향후 안보협력의 가장 중요한 동반자인 한국과 미국 간의 사이버안보 정책협력의 기반구축을 위해 양국 주요 형사정책 연구기관들의 공동연구를 위한 틀을 제시해보고자 한다.

4. 테러의 개념에는 전쟁의 개념과 범죄의 개념이 중첩적으로 나타나기 때문에 현실공간에서도 그들을 명백히 구분하는 것이 쉽지 않다. 사이버공간에서도 마찬가지이다. 사이버전쟁은 정치나 군사적으로 해결해야 하고, 사이버범죄는 형사사법에 의해 해결을 해야 하는 반면 사이버테러는 일부는 정치나 군사적으로, 일부는 형사 사법적으로 해결해야 할 필요성이 생긴다.

5. 2003년 국가안전보장회의(NSC)의 주도로 “국가 사이버 테러 대응 체계 구축 기본 계획”이 수립되었고, 그에 따라 국가 사이버안전업무 체계가 만들어지게 되었다. 현재 우리나라의 사이버안전과 관련된 체계는 2013년 ‘국가사이버안전관리규정(대통령훈령 제310호)’에 근거한다.

6. 2015년 4월부터 시행되고 있는 사이버안보태세 강화 종합대책에 따르면 청와대의 국가안보실 중심의 사이버컨트롤타워 기능을 강화하고, 그를 중심으로 각급 기관들이 체계적으로 사이버안전 업무를 수행하도록 하고 있다.

7. 현재는 사이버안전과 관련된 근거법률이 미비하다. 훈령에 종합적인 내용들을 담고 있고, 법률들은 단편적인 내용을 담고 있는 기이한 구성을 하고 있다. 그러므로 사이버안전과 관련된 종합적인 법률이 하루 속히 마련되어야 할 것이다.

8. 사이버테러와 관련된 법률규정은 형법을 비롯해서 정보통신기반보호법, 정보통신망법, 국가정보화기본법 등 다양한 개별 법률들 속에 부분적으로 규정되어 있다. 현행 사이버테러 관련 법령체계는 관련 기본법을 중심으로 관련 법령들이 만들어지기 보다는 소관 부처별로 필요에 의해서 개별법이 만들어지고 있다.

9. 사이버테러 대응 법체계 정비방안을 고려해 볼 때, 독립된 통합법체계를 구축해야 한다. 사이버테러에 대한 대응은 거버넌스(Governance)의한 것이다. 사이버테러에 대한 대응방안이 앞으로는 국가조직과 함께 기업이나 단체, 개인 등도 참여할 수 있는 구조를 가져야 한다. 이를 반영한 사이버테러 관련 법령 제개정이 필요하다.

10. 아직까지 관련 법률은 현실의 상황을 제대로 반영하지 못하고 있는 실정이다. 국회에 제출된 사이버테러방지법은 여전히 계류 중에 있으며, 제출된 법률안들이 지금의 현실을 제대로 반영하지 못하고 있다. 사이버테러방지법에서 제외되었던 강력한 사이버보호조치가 요구된다. 특히 사이버테러에 대한 정책에 있어서도 세밀한 정책이 필요하며, 법률에 있어서도 보다 면밀한 검토가 필요하다.

11. 사이버테러는 국제적인 문제이므로 국제적인 협력도 사이버테러 관련 정책의 한축을 형성하여야 할 것이다. 따라서 사이버테러와 관련된 국제협약이나 양자간 협약 등에도 보다 많은 노력을 기울일 필요가 있다.

12. 미국 오바마 행정부는 대통령 사이버보안 위원회, 2011년 안전한 사이버 미래를 위한 청사진: 국토안보체계를 위한 사이버보안 전략, 대통령의 행정명령 13636, 4개년 국가안보점검 등을 통하여 사이버보안 정책을 펼치고 있다.

13. 미국의 사이버안보 우선순위는 첫째, 사이버 위협으로부터 미국의 가장 중요한 정보 시스템인 핵심기반시설을 보호한다. 둘째, 사이버 사건을 식별하고 신고하기 위한 역량을 제고하여 신속하게 대처하도록 한다. 셋째, 사이버 공간상의 자유를 장려하고 개방적이고, 상호운용적이며, 안전하고, 믿을 수 있는 사이버 공간을 구축하기 위한 국제적 동반자들과의 협력한다. 넷째, 명확한 안보 세부목표 설정과 유관 기관들이 그 세부목표의 달성을 위해 책임의식을 갖게 함으로써 연방 네트워크를 방호한다. 다섯째, 인터넷에 능통한 인력 구성과 민간부문과 강한 연대를 형성한다.

14. 사이버 안보를 강화를 원칙은 정부 통합적(whole-of-government) 접근방식, 네트워크 방호 우선원칙, 사생활 및 시민의 자유 보호, 정부-민간 협력, 국제 협력 및 참여이다.

15. 미국의 국가 사이버 보안 종합 계획(CNCI)은 첫째, 오늘날의 즉각적 위협에 대항한 최전 방호선 구축, 둘째, 위협의 전(全)영역에 대한 방호, 셋째, 미래 사이버보안 환경 강화를 달성할 수 있도록 설계된 활동들로 구성된다.

16. 국가기반시설에 관한 행정명령 제13636 호는 첫째, 기술 중립적이고, 자율적인 사이버보안 프레임워크 개발, 둘째, 사이버보안 관행의 도입을 촉진하고 보상금으로 장려, 셋째, 사이버 위협 정보 공유에 관한 양, 속도, 질의 향상, 셋째, 국가기반시설의 보안을 위한 모든 계획에서 사생활 및 시민자유의 엄격한 보장, 넷째, 사이버보안 촉진을 위한 기존법률 활용방안 연구를 목적으로 한다.

17. 2008년 대통령 사이버보안 위원회의 최종보고서에 따르면, ① 사이버보안은 오늘날 미국의 주요 국가안보문제 중 하나이다. ② 그 결정사항과 활동은

사생활과 시민적 자유를 준수해야만 한다. ③ 사이버보안의 국내적 및 국제적 측면 모두를 아우르는 포괄적 국가 안보 전략만이 미국을 더욱 안전하게 한다.

18. 사이버보안을 위한 미국의 정책은 '포괄적'이라고 표현할 수 있다. 미국의 사이버보안정책은 민간부문과의 긴밀한 협력뿐만 아니라 다양한 정부 기관들 간의 정보공유 또한 그 해결책으로 제시한다. 미국 유관 정부기관 간 정보공유 기제는 DHS의 사이버 커뮤니티 C^3 원 프로그램(Critical Infrastructure Cyber Community Voluntary Program, the C^3 Voluntary Program)과 FBI의 사이버 방호 연합(Cyber Shield Alliance, CSA)을 들 수 있다.

19. 이른바 중국 발(發) 사이버공격의 특징은 정부 주도적이라는 점과 경제적 이익을 추구한다는데 있다. 중국 발 사이버공격은 다년간 이어져 오고 있으며, 그 표적 분야의 범위 확대뿐만 아니라 영향력도 커져가고 있다. 미국은 중국의 이러한 적극적 움직임에 대하여 법 당국의 대응전략 개선 및 더욱 강경한 벌금 및 형벌규정으로 맞서고 있다.

20. FBI는 중국의 사이버 위협에 맞서 전략 파트너십 조정관(strategic partnership coordinators, SPCs) 네트워크를 활용하고 있다. 또한 미연방의회는 미양형위원회를 통해 관련 범죄에 관한 양향기준을 2단계 상승시킬 것을 승인했다.

21. 중국의 2015년 전국인민대표대회는 네트워크 및 사이버공간 관련 사항에 관한 종합적인 법률인 중화인민공화국 네트워크안전법(中华人民共和国网络安全法 혹은 사이버보안법, Cyber Security Law)의 초안을 논의 하였다. 이는 네트워크와 정보기술 등에 대한 통제를 포함하는 국가안전법을 2015년 시행한 데 이어 별도로 발표된 네트워크 관련 보안법이다.

22. 중국의 2015년 네트워크안전법(안)은 사이버범죄나 사이버테러 외에 개인정보보호, 지적재산권 보호 등 컴퓨터 및 인터넷과 관련된 다양한 기술적인 문제점을 보완하고, 관련 법제를 포함한다. 정부와 민간에 발생할 수 있는 네트워크 공격 위협에 대하여 보안 책임자를 설정하는 방식으로 사이버테러를 방지 및 대응하고자 한다.

23. 2014년 미국 법무부는 사이버안보와 관련하여 사이버보안과(Cybersecurity Unit)를 신설함으로써 사이버범죄 조사 및 예방 활동을 강화했다 사이버보안과는 법적 집행력과 대응력을 보강하기 위하여, 전자감시규정에 관한 법적 가이드라인과 전문적인 자문을 제공하는 중앙 허브로서의 역핼을 수행하고 국내 및 해외 법률 조직에서 사이버범죄 가해자들을 감시 및 처벌하기 위한 효과적인 법적 집행도구에 대한 정보를 제공한다.

24. 미국 국립사법연구원 (National Institute of Justice, NIJ)의 연구 분야는 테러리즘, 성폭력, 아동학대, DNA수사, 인터넷범죄, 사이버범죄 및 수사, 디지털 증거, 물리적 증거 등을 광범위하게 포함하며 최근 5년-10년간 새로운 중점연구 분야로 떠오른 분야는 컴퓨터 관련 기술을 포함한 범죄와 수사이다.

25. NIJ가 관장하고 있는 컴퓨터 및 인터넷을 포함한 범죄관련 연구 분야에는 신상정보 절도(Identity theft), 아동 및 청소년 대상 사이버 범죄, 도용된 데이터(Stolen data) 관련 범죄, 국제 조직범죄(International Organised Crime, IOC)와 사이버 범죄의 연관성, 전자범죄 관련 기술, 수사방법 및 법 집행 그리고 디지털 범죄 수사 및 증거 등이 있다.

26. 미국 뉴욕법학대학원 안보 법 센터(Center on Law and Security)의 사이버 안보 프로그램은 부단히 발생하는 새로운 종류의 위협요소에 대응하는 새로운 협력모델과 공공-민간부분의 협력에 초점을 맞춰 개발되었다. 특히 정부와 기업들 간의 효과적인 협력방안을 제시하고 있다.

27. 2003년 대통령 국가 사이버공간 보안 전략에서도 미국 법무부와 FBI가 사이버범죄 수사 및 기소를 위한 노력을 주도함을 명시했다. 이에 따라 FBI는 미국 내에서 국내 정보기관 협력조정, 미국 국토안보부 지원, 미국 법 집행 기관과 대응 노력을 주도하고 있으며, 국외에서는 미 대사관 등을 통해 기타 국가와의 협력 및 상호사법공조 강화의 노력을 기울인다 FBI는 대응 체제를 갖추기 위해 2002년 사이버국(Cyber Division)을 신설하였다.

28. 동북아지역에서 한국과 미국의 공동현안으로서 사이버테러는 특히 중요한 의미를 가진다. 왜냐하면 동북아 평화협력구상 실현의 대상인 중국과 북한이 오히려 사이버테러의 진원지로서 지목받고 있기 때문이다. 따라서 미국과 한국은 동북아지역내 사이버공간을 넘어 국가들간의 정치경제적 공간에서 사이버 안전과 사이버안보를 위협하는 요소를 최소화하면서 위협요인을 평화요인으로 바꾸어 나가기 위해 공동의 노력을 경주해야 한다.

29. 미국 연방법무부, 미국사법정책연구원, 미국 뉴욕대 안보법센터 등의 기관은 향후 한국형사정책연구원의 한미 사이버테러 대응정책 협력방안 연구에서 주요한 협력기관이 될 것으로 기대된다. 상호협력관계를 기반으로 향후 한국과 미국 형사정책 연구기관간 사이버보안 분야 공동연구를 강화해나갈 계획이다.

제1장

KOREAN INSTITUTE OF CRIMINOLOGY

서 론

김 한 균

제1장

서 론

본 연구는 2015년도 「국제 범죄방지를 위한 UN·국제협력 및 연구 사업」의 세부 과제 하나로 기획되었다. 또한 유엔 범죄방지 및 형사사법 프로그램 (UN Crime Prevention and Criminal Justice) 소속 연구기관으로서 14개국 34개 형사정책 연구기관 및 형사사법기관과 연구교류협력을 진행하고 있는 한국형사정책연구원 국제협력사업 중에서도 사이버범죄 및 보안 분야 연구와 기술적 지원(technical assistance) 협력 사업 추진성과를 기반으로, 미국 내 주요 연구협력기관과의 공동연구협력사업을 통해 향후 과제를 발전적으로 제시하는데 목적이 있다.

제1절 연구의 의의와 목적

본 연구의 배경에는 현 정부의 「동북아 평화협력 구상」이 있다. 즉 동북아평화협력 구상은 점진적이고 단계적인 접근방식을 통해 민간과 정부가 다 함께 참여하는 다차원적 협력을 지향하는 가운데, 비전통 연성 안보 의제 (원자력 안전, 에너지 안보, 환경·기후변화, 재난 구호, 사이버 스페이스 등 5대 중점분야)에서부터 협력사업을 활성화하고자 하는 기획이다. 또한 동북아 지역 다양한 현안에서 형사사법공조와 인권보장의 증진을 목표로 다자간 협력 문화정착과 협력 메카니즘 제도화 방안을 선도적으로 제시하고 있다. 특히 사이버공간에서의 협력증진은 동북아평화협력구상의 중요한 의제이기도 하면서, 동북아 지역의 주요이해관계자인 미국과의 공동관심사이기도 하다.

이에 본 연구는 사이버범죄와 더 포괄적인 사이버안보의 측면에서 특히 중국, 북한 등 사이버테러 관련국 및 그 실태에 대한 기초적인 논의자료를 제공하는데 목적이

있다. 나아가 향후 안보협력의 가장 중요한 동반자인 한국과 미국 간의 사이버안보 정책협력의 기반구축을 위해 양국 주요 형사정책 연구기관들의 공동연구를 위한 틀을 제시해보고자 한다.

제2절 연구의 대상과 체계

1. 연구 대상

본 연구의 대상은 한국, 미국의 사이버테러 관련 형사사법 정책이다. 구체적으로는 중국과 북한의 사이버테러 위협에 대하여 한미 양국의 사이버테러 대응 협력방안을 살펴본다. 이러한 협력방안 연구는 향후 한국과 미국의 공동연구 협력사업으로 체계적으로 지속해 나갈 계획이며, 본 연구는 그 기초자료가 될 것이다.

특히 북한 배후 추정 주요 사이버테러는 지난 2003년을 시작으로 2009년 DDoS 공격, 2011년 농협 전산망 마비 사건, 2013년 방송사·금융기관 전산망 마비 등이 일어났고, 피해액 추정치만도 무려 1조원이 넘게 발생하고 있는 실정이다. 더구나 갈수록 북한의 사이버테러 공격 수준도 고도화되고 있다. 2014년 발생한 원전자료 유출 사건 당시, 한수원 퇴직자 및 협력업체 직원 등의 피싱메일을 통해 원전 자료가 유출되었다. 즉, 북한 해커들이 주요 기간 시설의 내부망 해킹이 어려워지면 자연스럽게 협력업체 직원을 통해 우회 공격하는 수법까지 동원하고 있는 셈이다. 따라서 사이버테러의 초국가적 특성과 전문 기법을 고려할 때 안보협력의 핵심 파트너인 한국과 미국의 공동대응 방안에 대한 연구가 필수적이다.

2. 연구 체계

본 연구의 제2장에서는 한국의 사이버테러관련 형사사법정책을 분석한다. 여기서는 현행 사이버테러 대응법제와 체계, 그리고 사이버테러 대응입법동향을 다룬다. 이어서 제3장에서는 미국의 사이버테러 관련 형사사법정책을 분석한다. 먼저 미국의 사이버안보정책을 개관하고 현 오바마 행정부의 사이버안보정책에 초점을 맞춘다. 그리고 미국의 대 중국 사이버안보정책을 분석한다. 특히 미국 연방법무부, 미국사법

정책연구원, 미국 뉴욕대 안보법센터의 사이버안보 관련 정책과 연구동향을 분석한다. 이들 기관은 향후 한국형사정책연구원의 한미 사이버테러 대응정책 협력방안 연구에서 주요한 협력기관이 될 것으로 기대된다.

제4장에서는 북한의 사이버테러 위협 실제사례와 대응정책을 분석한다. 북한의 소행으로 추정되는 역대 사이버테러 사건의 내용과 그 수사결과를 정리한다. 이어서 북한 사이버테러 위협에 대한 한국과 미국의 공동대응정책을 고찰한다.

제2장

KOREAN INSTITUTE OF CRIMINOLOGY

한국의 사이버테러 관련 형사사법정책

이 원 상

제2장

한국의 사이버테러 관련 형사사법정책[1)]

제1절 사이버테러 대응 법제 및 체계

1. 사이버테러 개관

테러(terror)는 라틴어(terrorem)에 그 기원을 두고 있는데 "거대한 공포·경악·무서움" 등을 의미한다.[2)] 테러의 사전적 정의를 보면 일반적으로 "어떤 정치적 목적을 달성하기 위하여 직접적인 공포 수단을 이용하는 주의나 정책"을 의미한다.[3)] 좀 더 구체적으로 "주권 국가 또는 특정 단체가 정치, 사회, 종교, 민족주의적인 목표를 달성하기 위하여 조직적이고 지속적으로 폭력을 사용하거나 폭력의 사용을 협박함으로써 특정 개인, 단체, 공동체 사회, 그리고 정부의 인식 변화와 정책의 변화를 유도하는 상징적, 심리적 폭력 행위의 총칭"[4)]이라고 하기도 한다.

그런데 그와 같은 테러가 사이버공간(cyberspace)에서도 발생하고 있다. 이는 사이버라는 개념이 인공이나 가상, 인터넷상의 등과 같은 개념으로 사용되고 있지만,[5)] 사이버테러에서의 사이버의 의미는 사이버공간이라는 공간적인 개념이라고 할 수 있다. 따라서 사이버테러는 기본적으로 '사이버공간에서 발생하는 테러'인 것이다. 그런데 문제는 테러의 개념에는 전쟁의 개념과 범죄의 개념이 중첩적으로 나타나기

---

1) 본 장은 본 연구사업의 전문가 자문위원인 이원상 교수(조선대학교 법학과)가 집필하였음.
2) http://www.etymonline.com/index.php?term=terror, 2015.11.10 방문.
3) http://terms.naver.com/entry.nhn?docId=1152766&cid=40942&categoryId=31645, 2015.11.10 방문.
4) http://terms.naver.com/entry.nhn?docId=2764283&cid=50307&categoryId=50307, 2015.11.10 방문.
5) 이원상, "'사이버'개념을 통한 사이버 모욕죄의 고찰과 대안", 형사정책 제20권 제2호, 2008, 256쪽.

때문에 현실공간에서도 그들을 명백히 구분하는 것이 쉽지 않다.[6] 그것은 사이버공간에서도 마찬가지이다. 예를 들어, 사이버공간에서의 가장 대표적인 침해행위라고 할 수 있는 사이버공격의 경우에도 그것이 사이버전쟁인지, 사이버테러인지, 사이버범죄인지를 판단하는 것은 공격이 발생하고 그 사실이 규명될 경우에 비로소 가능하게 될 것이다. 하지만 사이버공격의 성격이 규명된다고 하더라도 그 해결 방법은 다르게 나타난다. 사이버전쟁은 정치나 군사적으로 해결해야 하고, 사이버범죄는 형사사법에 의해 해결을 해야 하는 반면 사이버테러는 일부는 정치나 군사적으로, 일부는 형사사법적으로 해결해야 할 필요성이 생기기 때문이다.[7]

〈표 2-1〉 사이버공격의 분류

해결 방법	정치·군사적 해결	정치·군사적 해결 / 형사사법적 해결	형사사법적 해결
관련 영역	사이버 전쟁	사이버 테러	사이버범죄로서의 해킹
예시	미국과 중국간의 사이버 전쟁	알카에다의 사이버 공격/ 어나너머스의 공격	어나너머스의 공격/일반적인 사이버공격

(출처: 강석구/이원상, 29면)

일부에서는 보호법익을 기준으로 사이버공간에서의 안전을 사회적 법익으로 보고 국가안보와의 관련성을 침해하는 행위가운데 침해 정도가 강하면 사이버전쟁으로 규명하고, 그보다 다소 약한 경우를 사이버테러라고 하며, 가장 약한 경우를 신종 사이버범죄라고 규명하기도 한다.[8] 그에 따른 대응에 있어서도 앞서 구분한 것에 속하지 않는 경우는 '사이버사고'로 분류하여 사이버 안전한 시스템을 통해 해결하고, 사이버전쟁에 속하는 경우에는 국제법을 통해서 해결하며, 사이버범죄 및 테러는 그에 적합한 새로운 국가적 대응이 필요하다고 한다.[9]

하지만 그와 같은 방법으로 사이버공격을 분류하고 대응하는 것은 너무 뒤늦은

6) 윤해성, 사이버 테러의 동향과 대응 방안에 관한 연구, 한국형사정책연구원, 2012, 35쪽.
7) 강석구/이원상, 사이버범죄 관련 법령정비 방안연구, 한국형사정책연구원, 2013, 26쪽.
8) 강수진, 국가 사이버범죄 대응전략 설계, 경찰청 연구용역, 2013, 106쪽.
9) 강수진, 앞의 글, 107쪽.

감이 있다. 그 이유는 앞서 언급한 바와 같이 사이버공격 당시에는 구분이 불가능한 것이며, 사이버공격에 대한 규명이 있은 후에야 가능한 방법이기 때문이다. 따라서 사이버공격에 대한 구분을 정보보호의 3요소(CIA Triad) 가운데 어떤 요소를 공격 하는가로 구분을 하고자 하는 견해가 있다. 정보보호의 3요소는 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)이다. 기밀성은 정보의 유출을 보장하는 것이고, 무결성은 데이터를 무단으로 변경하거나 삽입, 삭제하는 등을 방지하는 것이며, 가용성은 데이터를 최대한 활용할 수 있도록 해 주는 것이다.[10] 기밀성의 침해정도는 유출된 정보의 종류에 따라 다르기 때문에 개인신용정보의 경우에는 사이버범죄가, 국가 기밀일 경우에는 사이버테러나 사이버전쟁에 해당할 수 있다.[11] 가용성의 침해는 DDoS공격이 대표적인데, 어떤 서버를 공격하는지에 따라 구분할 수 있을 것이다.[12] 그리고 무결성의 경우 데이터를 변경하거나 삭제하는 행위라고 할 수 있는데, 그 데이터가 국가의 전략과 관련된 것인지, 아니면 일반적인 데이터 인지에 따라 대응이 달라질 수 있게 된다.[13] 물론 CIA만을 가지고 판단하는 것은 쉽지 않다. 다만, CIA가 사이버전쟁과 사이버테러, 사이버범죄를 구분하기 위해 사용되는 종합적인 사고의 한 부분을 차지할 수 있을 것이다.

이처럼 사이버테러를 구분하여 그에 합당한 대응을 하는 것은 사실 쉽지 않다. 그럼에도 불구하고 사이버테러를 구분하고, 그에 대한 대응을 하려는 노력은 계속되어야 한다. 그 이유는 우리 사회가 고도의 정보화 사회로 진입하게 될수록 사이버테러는 테러범들이 사용할 수 있는 가장 적절한 수단이 될 수 있기 때문이다. 더욱이 우리나라는 북한을 머리위에 두고 있으며, 실재로 북한은 우리에게 사이버테러를 가하고 있기 때문이다. 하지만 엄밀히 말해서 북한의 사이버부대가 우리나라에 대해 행하는 사이버공격은 사이버전쟁이라고 해야 할 것이다. 현재 우리나라는 휴전상태이며, 사이버 공격을 행하는 주체가 군대라는 점, 그들이 공격하는 것이 국가의 주요 전산망이라는 점을 고려해야하기 때문이다.

---

10) 김광진, 해킹 패턴과 윈도우 보안 전략, 한빛미디어, 2003, 378쪽.
11) P.W. 싱어, 알란 프리드만, 사이버 보안과 사이버 전쟁 - 모두가 알아야 할 것들, 프리렉, 2014, 93쪽.
12) P.W. 싱어, 알란 프리드만, 사이버 보안과 사이버 전쟁 - 모두가 알아야 할 것들, 프리렉, 2014, 93쪽.
13) P.W. 싱어, 알란 프리드만, 앞의 책, 94쪽.

2. 사이버테러 대응 체계

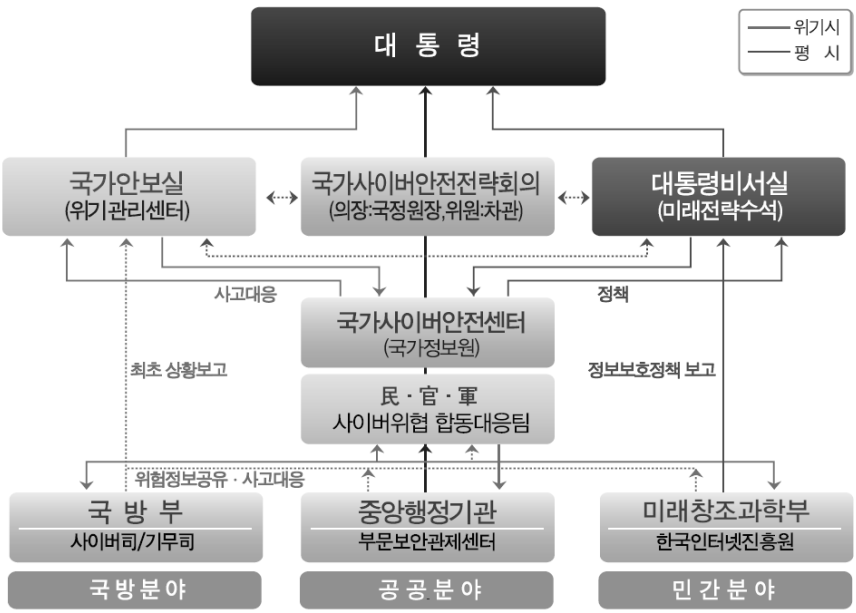
가. 국가사이버안전관리 업무 개관

2003년 1월 25일에 있었던 인터넷 대란으로 인해 국가의 사이버안전을 위한 체계가 구축될 필요성을 인식하게 되었다. 그에 따라 국가안전보장회의(NSC)의 주도로 "국가 사이버 테러 대응 체계 구축 기본 계획"이 수립되었고, 그에 따라 국가 사이버안전업무 체계가 만들어지게 되었다.[14] 현재 우리나라의 사이버안전과 관련된 체계는 2013년 5월 24일에 시행된 '국가사이버안전관리규정(대통령훈령 제310호)'에 의하고 있다. 이 훈령은 "이 훈령은 국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적"으로 제정되었다(동법 제1조). 다만, 문제점은 국가의 중대한 사이버안전에 대한 규정이 법률이 아닌 훈령으로 제정되어 있다는 것이다. 나중에 언급하도록 하겠지만 해당 규정이 훈령으로 규정되어 있기 때문에 다른 법률에 규정이 있으면 후순위로 밀릴 수밖에 없는 상황이 발생하게 된다. 그리고 동 훈령의 적용범위는 중앙행정기관이나 지방자치단체, 또한 공공기관의 정보통신망이 포함된다. 다만, '정보통신기반보호법'에 따른 주요정보통신기반시설의 경우에는 본 훈령보다 '정보통신기반보호법'이 우선 적용된다(제3조).

현행 훈령에 의한 체계에서는 국가사이버안전정책 및 관리의 중심에 국가정보원이 있다. 따라서 주요 업무는 국가정보원에서 관계 중앙행정기관장과의 협의를 통해 총괄 및 조정하도록 하고 있다(제5조 제1항). 그러므로 그를 위해 국가정보원장은 관계 중앙행정기관장과 협의하여 국가사이버안전 기본계획을 수립하고 시행하여야 하고(동조 제2항), 그를 위해 관계 기관에 예산 반영 등에 관한 협조요청을 할 수도 있다(동조 제3항). 하지만 사이버안전 확보를 위해서 각 중앙행정기관장은 소관 정보통신망의 안전성 확보에 대한 책임을 지며, 그에 필요한 조치를 강구해야 하며(제4조 제1항), 자신의 소관 공공기관장 및 지방자치단체장에게도 필요한 조치를 강구하도록 하여야 한다(동조 제2항). 또한 각 중앙행정기관장은 소관 정보통신망 보호를 위해 사이버안전대책을 수립 및 시행하며 지도·감독하여야 하며(제9조 제1항), 소관 공공기관장

14) 안성진/이경호/박원형, 보안관제학, 이한미디어, 2014, 38쪽.

및 지방자치단체장에게도 동일하게 하도록 하여야 한다(동조 제2항). 물론 그를 위해 국가정보원장은 미리 관계 중앙행정기관장과 협의하여 그를 지원해 주기 위한 국가사이버안전매뉴얼이나 관련 지침을 작성하여 배포할 수 있으며(동조 제3항), 특히 국가정보원장은 각 중앙행정기관의 사이버안전대책 이행여부를 진단 및 평가하여 필요한 경우 해당 중앙행정기관장에게 시정 등의 조치를 권고할 수 있고, 그 소관 지방자치단체 및 공공기관에 관한 사항은 중앙행정기관장과 협의하여 수행하도록 하고 있다(동조 제4항).

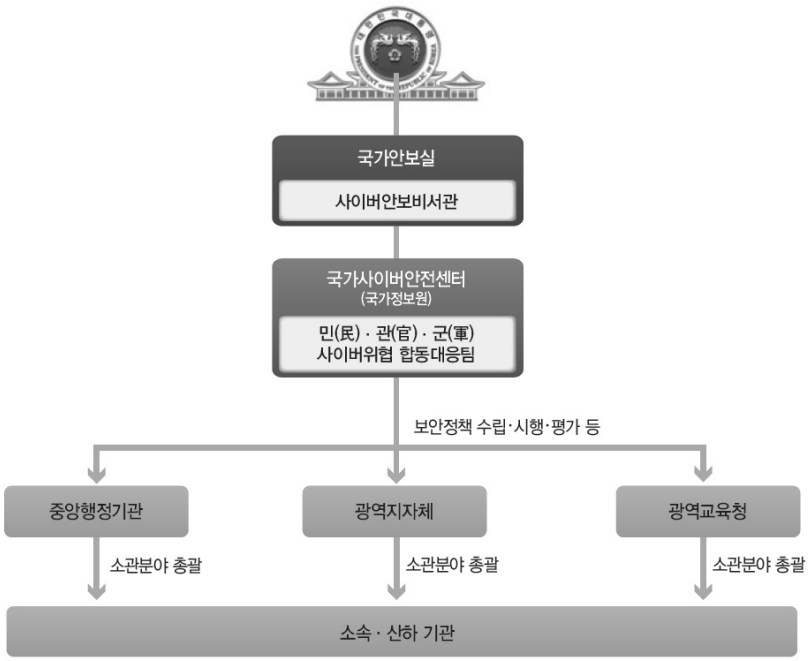


[그림 2-1] 우리나라 사이버안전을 위한 대응체계[15]

하지만 청와대의 국가안보실 산하에 사이버안보 비서관실이 신설되었기 때문에[16] 사이버안보와 관련해서는 국가안보실의 역할이 보다 강화되었다. 따라서 2015년 4월부터 시행되고 있는 사이버안보태세 강화 종합대책에 따르면 청와대의 국가안보실 중심의 사이버컨트롤타워 기능을 강화하고, 그를 중심으로 각급 기관들이 체계적으로

15) 2015년 국가정보보호백서 11쪽.
16) http://www.zdnet.co.kr/news/news_view.asp?artice_id=20150331092432&type=det&re=, 2015.11.10. 방문.

사이버안전 업무를 수행하도록 하고 있다.[17] 특히 지방자치단체의 주요기반시설 강화도 포함한 것과 사이버안보 정책에 대한 의사결정을 일원화 한 것이 특징이라고 할 수 있다.[18]



[그림 2-2] 개선된 사이버안전을 위한 대응체계[19]

다만, 이와 같은 개선체계가 제대로 작동하기 위해서는 근거법률이 필요하다. 현재는 사이버안전과 관련된 근거법률이 미비하다고 할 수 있다. 앞서 언급한 훈령에 의한 것과 정보통신망법 등 일부 법률들이 있는데, 훈령에 종합적인 내용들을 담고 있고, 법률들은 단편적인 내용을 담고 있는 기이한 구성을 하고 있다. 그러므로 사이버안전과 관련된 종합적인 법률이 하루 속히 마련되어야 할 것이다. 최근 국회 해킹과 관련해서 사이버안전에 대한 문제가 다시 부각되고 있는 상황에서 다시금 법률의 중요성이 대두되고 있는데, 그에 따라 청와대 국가안보실이 '사이버안보기본법'제정

17) 2015년 국가정보보호백서 12쪽.
18) 2015년 국가정보보호백서 13쪽.
19) 2015년 국가정보보호백서 12쪽.

을 추진하고 있다.[20]

나. 국가사이버안전을 위한 조직

국가사이버안전을 위한 조직은 크게 네 가지 조직으로 나누어 볼 수 있다. 먼저 국가사이버안전에 관한 중요사항을 심의하기 위한 조직으로 국가정보원장 소속하에 국가정보원장을 의장으로 하는(제6조 제2항) 국가사이버안전전략회의를 두도록 하고 있다(동조 제1항). 그리고 그 위원은 관계 중앙행정기관의 차관급 공무원이 된다(차관 또는 차관급 공무원이 2명 이상인 기관은 사이버 안전 업무를 담당하는 차관 또는 차관급 공무원이 위원이 됨)(동조 제3항).[21] 국가사이버안전전략회의의 주요 심의 사항은 국가사이버안전체계의 수립 및 개선에 관한 사항, 국가사이버안전 관련 정책 및 기관 간 역할조정에 관한 사항, 국가사이버안전 관련 대통령 지시사항에 대한 조치방안, 그리고 그 밖에 전략회의 의장이 부의하는 사항 등이다(동조 제4항). 그 밖에 구성이나 운영 등을 위한 필요사항은 의장이 정하도록 하고 있으며(동조 제6항), 심의된 사항가운데 중요한 사항은 대통령과 국무총리에게 보고하도록 하고 있다(동조 제5항).

전략회의의 효율적인 운영을 위하여 전략회의에 국가사이버안전대책회의를 두고 있으며(제7조 제1항), 그 의장은 국가정보원의 사이버안전업무를 담당하는 차장이 맡게 되며, 위원은 전략회의의 위원이 속하는 기관의 실·국장급 공무원이 맡는다(동조 제2항). 국가사이버안전대책회의의 심의 사항은 국가사이버안전 관리 및 대책방안, 전략회의의 결정사항에 대한 시행방안, 전략회의로부터 위임받거나 전략회의의 의장으로부터 지시받은 사항, 그리고 그 밖에 대책회의의 의장이 부의하는 사항 등이다(동조 제3항). 국가사이버안전대책회의의 구성 및 운영 등에 관한 사항은 의장이 정하도록 하고 있다(동조 제4항).

---

20) http://news.inews24.com/php/news_view.php?g_serial=925363&g_menu=050210&rrf=nv, 2015.11.10. 방문.

21) 그에 따라서 해당 위원들의 구성은 ①기획재정부차관, ②미래창조과학부차관, ③교육부차관, ④외교부차관, ⑤통일부차관, ⑥법무부차관, ⑦국방부차관, ⑧안전행정부차관, ⑨산업통상자원부차관, ⑩보건복지부차관, ⑪국토교통부차관, ⑫금융위원회 부위원장, ⑬국가안보실 사이버안전 담당 비서관, ⑭국무조정실 국무차장 등이다.

그를 수행하기 위한 조직으로 국가정보원장 소속하에 국가사이버안전센터를 두도록 하고 있다(제8조 제1항). 국가사이버안전센터는 국가사이버안전정책의 수립, 국가사이버안전전략회의 및 국가사이버안전대책회의의 운영에 대한 지원, 사이버위협 관련 정보의 수집·분석·전파, 국가정보통신망의 안전성 확인, 국가사이버안전매뉴얼의 작성·배표, 사이버공격으로 인하여 발생한 사고의 조사 및 복구 지원, 외국과의 사이버위협 관련 정보의 협력 등이다(동조 제2항). 국가정보원장은 국가 차원의 사이버위협에 대한 종합판단, 상황관제, 위협요인 분석 및 합동조사 등을 위해 사이버안전센터에 민·관·군 합동대응반을 설치·운영할 수 있으며(동조 제3항), 그를 위해 관계 중앙행정기관장, 지방자치단체장 및 공공기관장에게 소속 공무원 및 직원의 파견을 요청할 수 있다(동조 제4항).

중앙행정기관장, 지방자치단체장 및 공공기관장은 사이버공격 정보를 탐지·분석하여 즉시 대응 조치를 할 수 있는 "보안관제센터"를 설치 및 운영해야 하고, 보안관제센터를 두지 못하는 경우에는 그것을 운영하고 있는 다른 기관에 업무를 위탁할 수 있다(제10조의2 제1항). 각 보안관제센터에는 전담직원이 상시 배치되어야 하며(동조 제3항) 수집된 정보는 국가정보원장 및 관계 기관장에게 제공하여야 한다(동조 제2항). 보안관제센터의 설치·운영, 사이버공격 정보의 제공 범위, 절차 및 방법 등 세부사항은 국가정보원장이 관계 중앙행정기관장과 협의하여 정하도록 하고 있다(동조 제5항). 각 보안관제센터는 미래창조과학부장관이 지정하는 보안관제 전문업체의 인원을 파견 받아 보안관제업무를 수행하도록 할 수 있으며, 그에 관한 사항은 미래창조과학부장관이 국가정보원장과 협의하여 정하도록 하고 있다(동조 제4항).

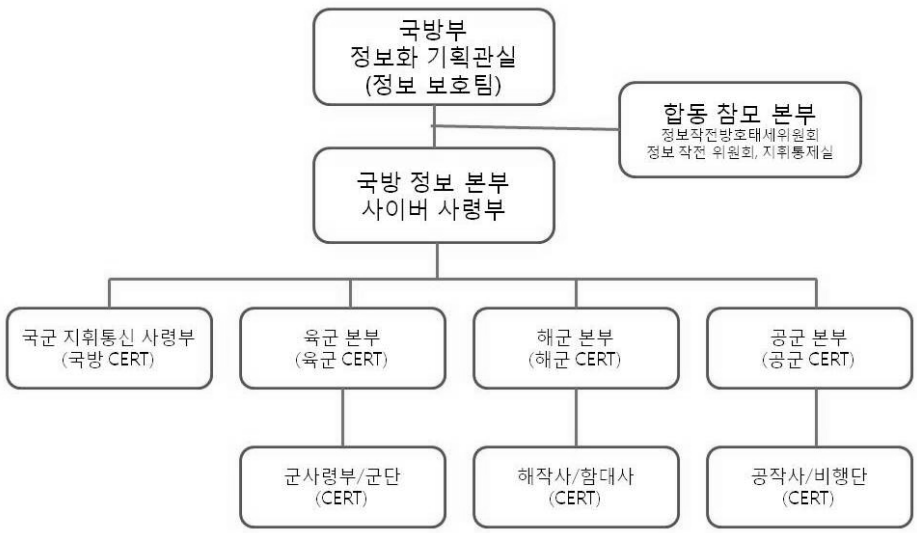
또한 사이버안전업무를 전담하는 전문기구를 운영하는 기관은 사이버위협 관련 정보의 탐지 및 정보공유체계의 구축·운영, 사이버안전 관련 정보의 분석·전파, 사이버안전 위해 요소에 대한 조치방안, 공격기법 분석 및 공격차단 등 대응방안, 그 밖에 경보의 수준별 세부 대응조치 등 필요한 사항 등에 긴밀히 협조하여야 한다(제14조 제1항). 그리고 사이버안전센터장은 그를 위해 관계전문가 회의를 소집할 수 있다(동조 제2항).

〈표 2-2〉 기관별 보안관제센터 운영현황[22)]

부문	담당기관	관제센터
행정	행정자치부	정부통합전산센터(대전)
		정부통합전산센터(광주)
		사이버침해대응센터(G-CERT)
국방	국방부	사이버사령부
외교	외교부	외교 사이버안전센터
국토교통	국토교통부	국토교통 사이버안전센터
보건·의료	보건복지부	보건의료 사이버안전센터
교육	교육부	교육 사이버안전센터
에너지	산업통상자원부	산업통상 사이버안전센터
통신과학	미래창조과학부	미래창조과학 사이버안전센터
		KISA 인터넷침해대응센터
		과학기술 정보보호센터
금융	금융위원회	금융ISAC(금융결제원)·
		금융ISAC(KOSCOM)
치안	경찰청	경찰 전산보호센터
특허	특허청	특허 관제센터
관세	관세청	관세 관제센터
국세	국세청	국세 관제센터
방위산업	방위사업청	방위사업 관제센터
재정	기획재정부	재정 관제센터
문화	문화체육관광부	문화체육관광 관제센터
기상	기상청	기상 관제센터
노동	고용노동부	노동 관제센터
공공	국가보안기술연구소	보안관제 기술지원센터
환경	환경부	환경 관제센터
법무	법무부	법무 관제센터
통일	통일부	통일 관제센터
농식품	농림축산식품부	농식품부 사이버안전센터
검찰	대검찰청	대검 사이버안전센터
병무	병무청	병무청 사이버안전센터
해양	해양수산부	해양수산 사이버안전센터
중소기업	중소기업청	중기청 사이버안전센터
공정위	공정거래위원회	공정위 사이버안전센터

22) 2015년 국가정보보호백서 67쪽.

그러나 국방과 관련해서는 특례를 두고 있다. "국가 사이버 안전 관리 규정" 제18조에 따르면 제9조(사이버안전대책의 수립·시행 등), 제12조(사고통보 및 복구) 및 제13조(사고조사 및 처리) 규정과 관련해서 국방 분야와 관련해서는 국방부장관이 안전성 확인, 사고통보, 사고조사 등의 업무를 수행하고(제1항), 해당 업무를 수행함에 있어 국가안보에 필요한 경우에만 국가정보원장에게 관련 내용을 통보하도록 하고 있다(제2항). 그에 따라 국방부는 자체적으로 사이버위협에 대한 보안관제 시스템을 구축하고 있다.



[그림 2-3] 국방부문 사이버안전체계[23]

기존에는 국방부 및 각 군의 CERT, 국군기무사의 정보전 대응센터가 사이버안전을 위한 시스템을 구축하고 있었는데, 사이버전을 대비하여 사이버 사령부를 중심으로 새로운 시스템을 구축하였다. 다만, 잦은 인사이동으로 인해 전문성 확보가 어렵기 때문에 사이버안전을 위한 노하우가 축적되지 못하는 한계가 드러나고 있기도 하다.[24]

---

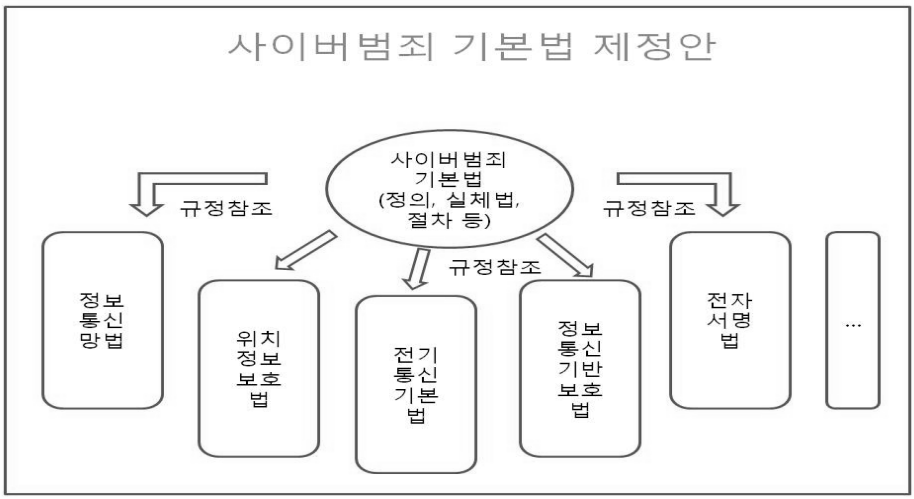
23) 안성진/이경호/박원형, 앞의 책, 45쪽.
24) 안성진/이경호/박원형, 앞의 책, 46쪽.

다. 사이버테러 대응 법제

사이버테러와 관련된 법률규정은 여러 곳에 흩어져 있다. 형법을 비롯해서 정보통신기반보호법, 정보통신망법, 국가정보화기본법 등 다양한 개별 법률들 속에 부분적으로 규정되어 있다.[25] 그런데 우리나라의 사이버테러 관련 법령체계는 관련 기본법을 중심으로 관련 법령들이 만들어지기 보다는 소관 부처별로 필요에 의해서 개별법이 만들어지고 있다. 사실 가장 바람직 한 방법은 기본법에서 사이버테러에 대한 기본방침과 방향성, 주요 규정들을 설정하고 그를 바탕으로 개별 법률들이 규정될 수 있도록 실질적인 대응 법률 체계를 구축하는 것이다. 그런데 문제는 우리나라의 경우 기본법이 사실상 헌법과 일반적인 법률의 중간단계에 위치할 어떤 근거도 없기 때문에 사실상 기본법은 일반 법률과 동등한 위치에 존재한다.[26] 따라서 기본법이 제정된다고 하더라도 기본법과 상충되는 법률이 제정되거나 개정되는 경우에는 신법우선원칙이나 특별법우선원칙이 적용되어 기본법은 배재된다. 따라서 기본법을 중심으로 사이버테러의 하부체계를 구성하는 법률체계가 구축되기 위해서는 입법자들이 스스로 기본법에 기속될 필요가 있다. 그 예로 일본을 들 수 있다. 일본의 경우에는 개별법률 등이 실질적으로 기본법체계 하에서 만들어지고, 입법자들도 그와 같은 체계를 지키고자 노력하는 것으로 보인다.[27] 따라서 관련 하부체계는 기본법을 중심으로 개별법이 기본법의 테두리 내에서 규정하게 된다. 그러나 우리나라의 입법동향을 보면 그와는 동떨어져 보인다. 그럼에도 불구하고 적어도 형식적으로라도 사이버범죄 기본법이 제정될 필요성이 있다는 주장이 제기되고 있다.[28] 그 이유는 지금과 같은 상화에서는 관련 법률들이 충돌하는 경우를 해결하기가 어렵기 때문에 적어도 그 해석의 근거가 될 만한 규정이 요구되고 있기 때문이다. 그와 같은 체계를 도표로 표시하면 다음과 같다.

---

25) 정완, "한·미 사이버보안 법제 동향에 관한 고찰", 경희법학 제48권 제3호, 2013, 219쪽.
26) 강석구/이원상, 앞의 글, 181쪽.
27) 강석구/이원상, 앞의 글, 52쪽.
28) 강석구/이원상, 앞의 글, 185쪽.



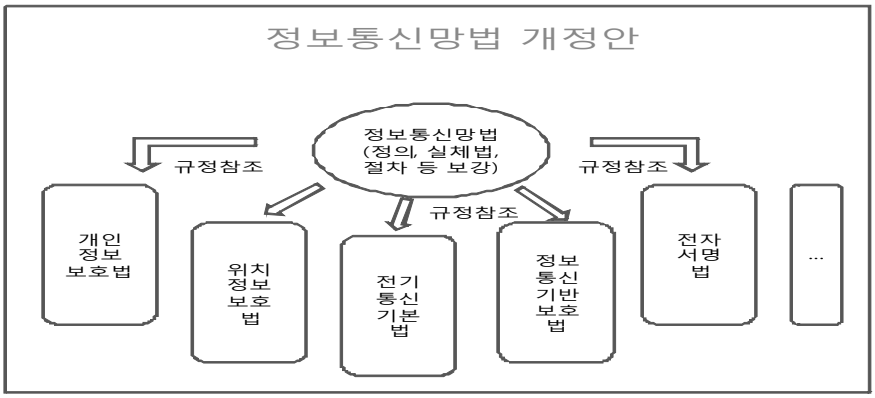
[그림 2-4] 사이버범죄 기본법 제정안

(출처:강석구/이원상, 앞의 글, 186면)

그런데 기본법이 제정되더라도 문제가 될 수 있는 것은 사이버테러에 대한 처벌규정이 있음에도 실제로 그 적용을 받는 수범자들은 해당 법률이 있는지 조차 모르고 있는 실정이다. 그러므로 가급적 처벌규정들은 수범자들이 쉽게 살펴볼 수 있도록 통합되는 것이 적절하다고 생각된다. 그런 역할을 수행해야 하는 것이 바로 형법일 것이다. 그런데 우리나라는 1995년 형법이 개정된 이 후 사이버범죄 등과 관련해서는 거의 규정의 변화가 없는 실정이다. 따라서 사이버범죄와 관련해서 형법이 적용되는 경우는 거의 없다고 할 수 있다. 그렇다면 사이버범죄 등을 규정하는 법 규정들은 과연 어디에 위치하고 있는 것일까? 바로 정보통신망법이 사이버범죄에 있어서는 사실상 기본법의 역할을 수행하고 있다.[29] 따라서 사이버범죄 등과 관련해서 처벌할 필요성이 발생하게 되면 정보통신망법에 규정되는 경향을 보이고 있다. 그런데 사이버테러와 관련된 규정에서도 처벌규정들이 존재하고 있다. 나중에 살펴볼 입법안들에서도 처벌규정을 두고 있다. 하지만 사이버테러가 일부는 사이버범죄로 처리될 수 있기 때문에 그와 관련된 처벌규정들은 각 개별규정에 산재하기 보다는 한 법률에 집중해서 규정하는 것이 적절할 것이다. 가장 좋은 방법은 형법에 규정하는 것이다.

29) 강석구/이원상, 앞의 글, 125쪽.

그러나 형법의 규정이 매우 어려운 우리나라의 입법현실을 고려해 보면, 정보통신망법을 이용하는 것도 적절할 것으로 사료된다.



[그림 2-5] 정보통신망법의 개정안

(출처:강석구/이원상, 앞의 글, 187면)

현행 사이버범죄 등과 관련된 대략의 규정들만 나열해도 다음과 같다.

형법

정보통신망 이용촉진 및 정보보호 등에 관한 법률

개인정보보호법

저작권법

통신비밀보호법

주민등록법

신용정보의 이용 및 보호에 관한 법률

전기통신기본법

성폭력범죄의 처벌 및 피해자보호등에 관한 법률

전파법

게임산업진흥에 관한 법률

정보통신기반 보호법

전자서명법

전기통신사업법
사행행위등 규제 및 처벌특례법
청소년보호법
위치정보의 보호 및 이용 등에 관한 법률
그 외 다수

그 가운데 형법에서의 관련 규정을 살펴보면 다음과 같다.

〈표 2-3〉 형법에서의 관련 규정

1	제140조 제3항	공무상 비밀장치된 전자기록 등 탐지
2	제141조 제1항	공용 전자기록 등 손상 · 은닉 등
3	제227조의 2	공무소 · 공무원의 전자기록 등 위변작
4	제228조	공전자기록 등 불실 기재 · 기록
5	제229조	위변작 등 공전자기록 행사
6	제232조의 2	타인 전자기록 등 위변작
7	제234조	위변작 타인 전자기록 등 행사
8	제246조	(상습)도박
9	제247조	영리목적 도박개장
10	제248조	무허가 복표 발매 · 중개 · 취득
11	제309조	출판물에 의한 명예훼손
12	제314조 제2항	컴퓨터 등 장애(손괴)업무방해
13	제316조 제2항	비밀 장치한 전자기록 등을 기술이용 탐지
14	제323조	권리행사방해(전자기록 취거 · 은닉 · 손괴)
15	제347조	사 기
16	제347조의 2	컴퓨터 등 사용사기
17	제366조	재물손괴(타인 전자기록 손괴)

그리고 정보통신망법의 내용을 요약하면 다음과 같다.

〈표 2-4〉 정보통신망법

1	제70조 제1항	사이버 명예훼손(사실 유포)
2	제70조 제2항	사이버 명예훼손(허위사실 유포)
3	제71조 제1호	이용자 개인정보 수집
4	제71조 제3호	개인정보 목적외 이용 및 제 3자 제공
5	제71조 제5호	이용자 개인정보 훼손 · 침해 · 누설
6	제71조 제9호	악성프로그램(바이러스)유포
7	제71조 제10호	정보통신망 장애발생
8	제71조 제11호	타인정보 훼손 및 타인비밀 침해 · 도용 · 누설
9	제72조 제1항 제1호	정보통신망 침입
10	제72조 제1항 제5호	직무상 비밀 누설 및 목적외 사용
11	제72조 제1항 제2호	속이는 행위에 의한 개인정보수집
12	제73조 제1호	정보통신 서비스 제공자등의 기술적 · 관리적 조치 미이행
13	제73조 제2호	영리목적 청소년유해매체물 미표시
14	제73조 제3호	청소년유해매체물 광고 청소년에게 전송
15	제74조 제1항 제1호	인증기관 인증표시 무단 표시 · 판매 · 진열
16	제74조 제1항 제2호	음란문언 · 음향 · 영상 등 배포 · 판매 · 전시
17	제74조 제1항 제3호	사이버 스토킹(공포불안 말 · 음향 등 반복 행위)
18	제74조 제1항 제4호	스펨메일 수신거부 회피 관련 기술조치 행위
19	제74조 제1항 제5호	전자우편주소 무단 수집 · 판매 · 유통 · 정보전송에 이용
20	제74조 제1항 제6호	불법행위를 위한 광고성 정보 전송

3. 국방부 관련 법제

사이버사령부와 관련된 대표적인 법령으로는 대통령령 제26101호인 "국군사이버사령부령"과 "국가 사이버 안전관리 규정", "국방정보보호훈령", "국방 사이버기강 통합관리 훈령" 등이 있다. 국가 사이버 안전관리 규정에서는 앞서 언급한 바와 같이

국방부분에 있어서는 안전대책이나 사고조사 등에 있어서 국방부의 독자적인 업무수행을 규정해 놓고 있으며, 업무 수행에 필요한 부분에 있어서 국가정보원장에게 통보하도록 하고 있다(제18조). 또한 국방정보보호훈령에서는 정보통신기반법이나 개인정보보호법, 전자정부법 등에서 위임된 사항 및 국방정보체계를 위한 규정들이 포함되어 있다. 그에 따라 정보보호 추진목표(제4조), 정보보호 추진원칙(제5조), 정보보호 업무범위(제6조) 등이 규정되어 있으며, 업무분장(제7조), 국방정보보호위원회(제8조), 정보대책 및 관리(제12조~제49조), 정보보호평가(제50조~52조), 그리고 사이버침해사고 예방 및 대응(제53~제62조), 정보보호 업무발전 및 인력양성(제63조~제67조) 등에 대한 내용이 있다.

국방 사이버기강 통합관리 훈령에서는 군에 복무하는 모든 자들이 사이버 공간을 사용함에 있어서 군 기강을 확립하기 위한 목적으로 제정되었으며, 그에 따라 업무분장(제4조), 건전한 사이버문화 조성 활동J(제5조), 사이버 근무기강 확립(제6조), 사이버윤리 교육(제7조) 등에 대한 내용과 함께 웹사이트 관리(제8조~제10조), 시스템·기술적 통제 및 관리(제11조~제14조), 예방관리 활동(제15조~제19조), 그리고 위반자에 대한 제재(제20조~제21조)를 규정해 놓고 있다.

국군사이버사령부령에서는 사이버사령부의 조직과 소관 사무 등에 대한 규정을 두고 있다. 그에 따르면 국군사이버사령부의 설치 목적은 "국방 사이버전(戰)의 기획, 계획, 시행, 연구·개발 및 부대 훈련에 관한 사항을 관장"하는 것이고, 그에 따라 국방부장관 소속하에 국군사이버사령부를 설치하도록 하고 있다(제1조). 그와 같은 설치목적 하에서 국군사이버사령부는 ①국방 사이버전의 기획 및 계획 수립, ②국방 사이버전의 시행, ③국방 사이버전 전문 인력의 육성과 기술 개발, ④국방 사이버전을 대비한 부대 훈련, ⑤국방 사이버전 유관기관 사이의 정보 공유 및 협조체계 구축, 그리고 ⑥그 밖에 국방 사이버전과 관련된 사항에 대한 임무를 수행하도록 하고 있다(제2조)

국군사이버사령부의 조직체계를 보면 수뇌부로 장관급 장교인 사령관 1명과 영관급 장교인 참모장 1명을 두도록 되어 있다(제3조). 사령관은 국방부장관의 명에 따라서 국군사이버사령부와 관련된 업무일체를 총괄하고, 예하 부대를 지휘·감독하는데(제4조 제1항) 만일 사령관이 부득이한 사유로 직무를 수행할 수 없을 때에는 국방부

장관이 정하는 사람이 그 직무를 대행하도록 하고 있다(동조 제3항). 참모장은 사령관을 보좌하고, 참모 업무를 조정·통제하며(동조 제2항), 예하 부대장은 사령관의 명을 받아 소관 업무를 처리하며, 소속 부대원을 지휘·감독하여야 한다(동조 제4항). 그러나 사이버전과 관련해서 국군사이버사령부는 합동참모의장의 지도·감독 하에 있게 되는데, 합동참모의장은 국방부장관의 명을 받아 국군사이버사령부가 국방 사이버전에서 사이버작전을 원활하게 수행할 수 있도록 지도·감독해야하기 때문이다(제7조).

국군사이버사령부는 필요한 참모 부서를 두며, 국군사이버사령부 예하에 기능별 임무 수행 부대를 두며(제5조 제1항), 해당 참모부서 및 예하 부대의 조직과 사무분장에 관한 사항은 국방부장관이 하도록 하고 있다(동조 제2항). 그리고 국방부장관이 정하는 범위 내에서 군인과 군무원을 배치한다(제6조).

4. 민간부문의 대응 법제

가. 일상의 정보보호 조치

민간부문에서는 정보통신망법 제52조에 의해서 한국인터넷진흥원(KISA)이 관련업무를 수행하고 있다. 특히 KISA는 사이버안전업무를 수행하기 위해 인터넷 침해 대응센터(KISC)를 설치하여 운영하고 있는데, 이 기관은 민간부문의 사이버위협에 대응하고, 국제 침해사고의 창구역할을 수행하고 있다.[30] 그와 함께 은행이나 증권 등 금융기관에 있어서는 금융 결제원 금융 정보보호센터(FISeC)가 사이버위협의 예방업무를 수행하고 있고, 그 외에도 안철수 연구소 등 여러 민간 업체들이 민간 부문의 사이버안전 업무를 수행하고 있다.[31]

사이버안전과 관련해서 민간부문의 대응에 대한 근거규정으로는 정보통신망법 제6장이라고 할 수 있다. 그에 따르면 미래창조과학부장관은 정보보호조치에 관한 지침을 고시하여야 하고(제45조 제2항), 정보통신서비스 제공자는 그에 따라 보호조치에 만전을 기해야 한다(동조 제1항).[32] 그를 위해 미래창저과학부장관은 대통령령에 따

30) 안성진/이경호/박원형, 앞의 책, 47쪽.
31) 안성진/이경호/박원형, 앞의 책, 48쪽~49쪽.
32) 보호조치 내용에는 "①정당한 권한이 없는 자가 정보통신망에 접근·침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치·운영 등 기술적·물리적 보호조치, ②정보의 불법 유출·변조·삭제 등을 방지하기 위한 기술적 보호조치, ③정보통신망의 지속적인 이용이 가능한 상

른 정보보호 사전점검기준에 따로 정보통신서비스 제공자들이 지키도록 하여야 하며(제45조의2 제2항), 정보통신서비스 제공자는 해당 사항을 고려하여 정보통신망 구축 및 서비스 등의 계획 및 설계 등에 반영하여야 한다(동조 제1항). 특히 최근 정보보호의 중요성에도 불구하고 최고책임자를 두고 있지 않은 경우가 많아서 사이버공격에 대한 적절한 대응을 하지 못하는 경우가 많았다. 따라서 정보통신서비스 제공자는 임원급의 정보보호 최고책임자를 지정할 수 있고(제45조의3 제1항),[33] 침해사고에 대응하여 정보보호 최고책임자를 구성원으로 하는 정보보호 최고책임자 협의회를 구성 및 운영할 수 있으며(동조 제4항), 종업원 수가 1천명 이상인 경우 등에는 미래창조과학부장관에게 신고토록 하고 있다(동시행령 제36조의6).

그러나 정보보호에 대해서는 각 기업들이 서로 다른 기준에 의해서 수행할 수 있기 때문에 정보보호 관리체계를 어느 정도 표준화 시킬 필요가 있다. 따라서 미래창조과학부장관으로 하여금 정보보호 관리체계를 수립 및 운영하고 있는 경우 한국인터넷진흥원이나 기타 정보보호 관리체계 인증기관을 통해(제47조 제5항) 인증을 할 수 있도록 하였다(동조 제1항). 정보보호 관리체계 인증에 대해서는 고시하도록 하였으며(동조 제3항), 인증의 유효기간은 3년으로 하였다(동조 제4항).

또한 국가안전보장과 관련된 정보들이 외부로 유출되는 것도 큰 문제가 되고 있다. 최근 한수원을 해킹한 해커들이 원전설계도도면으로 추정되는 파일이나 계획 문서 등을 인터넷에 공개하여 많은 논란이 되고 있다.[34] 이처럼 국내의 중요 기밀문서들이 해커들에 의해 해킹당하여 해외로 유출되거나 인터넷에 공개되는 것은 매우 큰 문제라고 할 수 있다. 따라서 정부는 "국가안전보장과 관련된 보안정보 및 주요 정책에 관한 정보", "국내에서 개발된 첨단과학 기술 또는 기기의 내용에 관한 정보" 등이 망을 통해 국외로 유출되는 것을 막기 위해 정보통신서비스 제공자나 이용자에게

태를 확보하기 위한 기술적·물리적 보호조치, ④정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치" 등에 관한 내용이 있어야 한다(동조 제3항).

33) 정보보호 최고책임자는 "①정보보호관리체계의 수립 및 관리·운영, ②정보보호 취약점 분석·평가 및 개선, ③침해사고의 예방 및 대응, ④사전 정보보호대책 마련 및 보안조치 설계·구현 등, ⑤정보보호 사전 보안성 검토, ⑥중요 정보의 암호화 및 보안서버 적합성 검토, ⑦그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행" 등이다(동조 제3항).

34) http://www.zdnet.co.kr/news/news_view.asp?artice_id=20150713170352&type=det&re=, 2015.11.10. 방문.

“정보통신망의 부당한 이용을 방지할 수 있는 제도적·기술적 장치의 설정”, “정보의 불법파괴 또는 불법조작을 방지할 수 있는 제도적·기술적 조치”, “정보통신서비스 제공자가 취급 중 알게 된 중요 정보의 누출을 방지할 수 있는 조치” 등 필요한 조치를 하도록 할 수 있다(제51조).

나. 침해사고 발생 시의 보호조치

사이버공격에 의한 침해사고가 발행하는 경우를 대비해서 미래창조과학부장관은 ①침해사고에 관한 정보의 수집·전파, ②침해사고의 예보·경보, ③침해사고에 대한 긴급조치, ④그 밖에 대통령령으로 정하는 침해사고 대응조치 등을 마련해야 한다(제48조의2 제1항). 그를 위해 정보통신서비스 제공자 등은 “침해사고의 유형별 통계, 해당 정보통신망의 소통량 통계 및 접속경로별 이용 통계 등 침해사고 관련 정보”를 미래창조과학부장관 또는 한국인터넷진흥원에 제공하여야 하고(동조 제2항), 한국인터넷진흥원은 그를 분석하여 미래창조과학부장관에게 보고 하여야 한다(동조 제3항). 만일 정보통신서비스 제공자 등이 정보제공 거부나 거지 정보 제공시 미래창조과학부장관은 시정을 명할 수 있으며(동조 제4항), 침해사고 대응을 위해 그들에게 필요한 인력지원을 요청할 수 있다(동조 제6항). 다만, 제공받은 정보는 침해사고 대응을 위해서만 사용할 수 있다(동조 제5항).

정보통신서비스 제공자 등은 침해사고가 발생하면 반드시 그 사실을 미래창조과학부장관이나 한국인터넷진흥원에 신고하여야 하고(제48조의3 제1항), 미래창조과학부장관이나 한국인터넷진흥원은 그에 대한 조치를 취해야 한다(동조 제2항). 이 때, 정보통신서비스 제공자 등은 침해사고의 원인 분석과 피해확산 방지하여야 한다(제48조의4 제1항). 그리고 미래창조과학부장관은 전문가들로 구성된 민·관합동조사단을 구성하여 침해사고의 원인 분석을 할 수 있다(동조 제2항). 그를 위해 정보통신서비스 제공자 등에게 관련 자료의 보전을 명할 수도 있으며(동조 제3항), 침해사고 관련 자료 제출을 요구할 수 있고, 민·관합동조사단에게 관련 사업장에 출입하여 원인을 조사토록 할 수도 있다(동조 제4항). 이 때, 제출받은 자료와 정보 등은 오직 침해사고 원인 분석 및 대책 마련을 위해서만 사용할 수 있다(동조 제5항).

또한 사이버공격으로 인한 침해사고가 발행한 경우 가장 중요한 조치중 하나는 이용자가 침해사고를 인지하고 방어조치를 취할 수 있도록 하는 것이다. 그러므로 정보통신서비스 제공자는 사이버공격으로 인한 침해사고가 발생한 경우 이용자에게 보호조치를 취하도록 요청하고, 그에 응하지 않으면 일시적으로 망접속을 제한할 수 있다.(제47조의4 제2항).

다. 사이버공격에 대한 처벌 근거

민간부문에 대한 사이버공격은 주로 사이버범죄에 해당하는 경우가 많으며 경우에 따라서는 사이버테러에 속하기도 한다. 따라서 사이버공격이나 사이버테러를 처벌하기 위한 근거규정이 요구된다. 그러므로 정보통신망법 제48조 제1항에서는 사이버공격이나 사이버테러의 수단이 되는 해킹죄를 처벌하고 있으며, "누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다."고 규정하고 있으며, 그를 위반하는 경우 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하고 있다(제72조 제1항 제1호). 그리고 동조 제2항에서는 "정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램을 전달 또는 유포"한 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처해지며(제72조 제9호), "정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애가 발생하게"한 경우에도 동일하게 처벌된다(동조 제10호).

라. 사이버테러 대응 법체계 정비방안

사이버테러 대응 법체계 정비방안을 고려해 볼 때, 다양한 견해들이 제시되고 있다. 그 가운데 우선적으로 제기되고 있는 것이 독립된 통합법체계를 구축해야 한다는 것이다. 이는 앞서 살펴본 바와 같이 현생 사이버테러와 관련된 법률체계는 가장 중요한 내용은 지침에 의존하고 있으며, 나머지 사항들은 개별법률 등에 단편적으로 규정되는 형국을 띄고 있다. 이와 같은 체계는 사실상 사이버테러가 발생하는 경우 그에 대해 효과적으로 대응하지 못하는 모습을 보이고 있다.[35] 따라서 그에 대한

대응방안으로 사이버테러의 경우에도 국가적 재난에 준하여 대응할 필요가 있고, 국가재난에 대해서는 '재난 및 안전관리 기본법'이 있기 때문에 그를 확대하여 통합을 하는 경우 보다 효과적이라는 견해도 있다.[36] 하지만 기존의 재난과 사이버테러를 물리적 재난과 전자적 침해로 구분하여 재난과 관련된 법령체계는 사이버테러의 특성을 충분히 고려하지 못한 것이기 때문에 독립된 법령을 제정해야 한다는 반대 견해도 존재한다.[37]

그와 사이버테러 대응 법체계에 있어서 현행의 시스템이 반영될 필요가 있다. 앞서 설명한 바와 같이 현행 체계는 기존의 체계가 개선되어 청와대의 국가안보실의 사이버안버비서관이 컨트롤 타워의 정점에 있고, 그 아래에 국방부, 국가정보원, 미래창조과학부가 민·관·군의 사이버안전 문제를 담당하며, 중앙행정기관 이외에도 지방자치단체, 지방교육청 등도 사이버안전체계에 포함되어 있는 상황이다. 다만, 문제는 청와대가 컨트롤 타워의 역할을 수행한다고 하더라도 결국 총괄적인 업무를 수행해야 하는 기관을 필요하게 된다. 기존에는 국가정보원이 그와 같은 업무를 수행하고 있으며, 지금도 실질적으로 해당 업무를 수행하고 있기 때문에 국가정보원이 총괄기구를 맡아야 한다는 견해들이 있다.[38] 그러나 그와 같은 국가정보원의 활동의 신뢰성에 대해 의구심이 제기되고 있기 때문에 국가정보원의 활동을 통제하기 위한 감시 장치를 두는 것을 전제조건으로 할 필요가 있다고도 한다.[39] 하지만 국가정보원이 총괄기관을 담당하는 것에 대한 우려를 표하면서 국무총리산하에 사이버안전중앙위원회를 두고, 그 아래 중앙사이버안전대책본부를 두는 것이 보다 적절하다는 견해도 있다.[40]

또 하나 쟁점이 될 수 있는 것은 사이버테러에 대한 대응은 거버먼트(Government)에 의해 달성될 수 있는 것이 아니라 거버넌스(Governance)의한 것이라는 견해가 대두되고 있다.[41] 거버넌스란 "...정부·준정부를 비롯하여 반관반민(半官半民)·비영

35) 오길영, "'사이버테러'대응체계의 문제점과 개선방향", 민주법학 제54호, 2014, 473쪽.
36) 윤해성, 앞의 글, 67쪽.
37) 곽병선, 사이버테러 대응을 위한 법체계 검토, 법학연구, 제59호, 2015, 16쪽.
38) 김도승, "사이버위기 대응을 위한 법적 과제 - 미국의 사이버위기 대응체계 현황과 시사점을 중심으로", 방송통신정책 제21권 제17호, 2009, 53쪽.
39) 임종인, "3.20 대란과 국가사이버 위기관리법의 과제", 국가사이버위기 관리제정을 위한 공청회 자료집, 2013, 19쪽.
40) 곽병선, 앞의 글, 17쪽.
41) 임종인, 앞의 글, 4쪽.

리·자원봉사 등의 조직이 수행하는 공공활동, 즉 공공서비스의 공급체계를 구성하는 다원적 조직체계 내지 조직 네트워크의 상호작용 패턴으로서 인간의 집단적 활동...” 이라고 할 수 있다.[42] 즉, 사이버테러에 대한 대응방안이 현재는 국가조직을 바탕으로 구축되어 있는데 반하여 앞으로는 국가조직과 함께 기업이나 단체, 개인 등도 참여할 수 있는 구조를 가져야 한다는 것이다. 그러므로 사이버테러 관련 법령을 구축함에 있어 그와 같은 부분들이 구체적으로 반영될 수 있도록 해야 할 것이다. 따라서 민간과 민간의 협력방안, 법집행기관과 민간의 협력방안, 국가간 협력 방안 및 국제조직과의 협력방안 등이 구체적으로 명시될 필요가 있다.[43]

제2절 사이버테러 대응 입법 동향

앞서 살펴본 바와 같이 현행 사이버테러 관련 법률은 현재의 대응체계를 제대로 반영하고 있지 못할뿐더러 지침이 법령보다 우선 적용되는 문제점이 존재하고 있다. 따라서 사이버테러에 대응하기 위한 법률을 제정하는 것은 매우 시급한 문제라고 할 것이다. 그런데 그와 같은 문제의 발목을 잡고 있는 것이 그 대응 주체를 국가정보원으로 하는 것에 대한 야당의 반발이 있기 때문이다.[44] 그러나 이제는 청와대가 직접적인 컨트롤 타워를 맡을 수 있는 조직을 두었기 때문에 그와 같은 문제는 일단 해결된 것으로 보아야 할 것이다. 따라서 현재 개선된 사이버안전 체계를 반영할 법률이 제정될 필요가 있다. 그런데 이제까지 발의된 하태경 의원안이나 서상기 의원안 등은 이전의 논의가 반영된 것이기 때문에 현실의 상황을 100% 반영하고 있지는 못한 것으로 보인다. 하지만 기본적인 내용들은 현실과 부합할 수 있기 때문에 사이버테러와 관련된 입법동향을 살펴보기 위해서 이제까지 국회에 제출된 입법안들을 검토해 보고자 한다.

---

42) http://terms.naver.com/entry.nhn?docId=75398&cid=42152&categoryId=42152, 2015.11.10. 방문.
43) 윤해성/윤민우/Joshua Freilich/Steven Chermak/Robert G. Morris/김일수, 사이버 테러의 동향과 대응 방안에 관한 연구, 한국형사정책연구원, 2012, 277쪽~281쪽.
44) http://www.fnnews.com/news/201510261550578209, 2015.11.10. 방문.

1. 하태경 의원안

하태경은 '국가 사이버안전 관리에 관한 법률안'을 발의하였다.[45] 해당 법률안은 총 16개 조문으로 구성되어 있다. 주요 내용을 보면 국회와 법원, 헌법재판소, 중앙선거관리위원회 뿐 아니라 중앙행정기관이나 지방자치단체 및 공공기관의 장은 사이버안전을 위해 노력을 하도록 하고 있다(제4조), 그와 같이 국가 사이버안전에 관한 정책을 체계적으로 관리하기 위해 국가정보원장과 각 부처가 협의를 거치도록 하고 있다(제5조).

그런데 본 법률안에서 눈에 띄는 것은 사이버안전에 대한 중요사안을 심의하기 위해서 국무총리 소속으로 '국가사이버안전전략회의'를 두도록 하고 있으며, 전략회의의 의장을 국무총리로, 부의장을 (구)행정안전부장관, 국가정보원장 및 방송통신위원회 위원장으로 하고 있다는 것이다(제6조). 이와 같이 국가사이버안전전략회의를 국무총리 산하에 두도록 한 조치는 컨트롤 타워의 역할을 국무총리가 하도록 하기 위함이다. 이는 현행처럼 청와대가 컨트롤 타워를 하기 이전에 국가정보원이 컨트롤 타워의 역할을 수행하는 것에 대한 대안이라고 할 수 있다. 사실 현재는 청와대가 컨트롤 타워 역할을 수행할 수 있기 때문에 현재는 큰 의미가 없다고 하겠다. 다만, 사이버안전대책의 수립이나 사이버위기 대응 훈련, 사이버경보 발령, 사고통보 및 복구, 사고처리 등은 국가정보원장과 협의 하에 수행하도록 하여 사실상 국가정보원이 관련 업무를 수행하도록 하고 있다.

그런데 인력양성과 교육홍보 등은 관계 중앙행정기관의 장이 강구하도록 하고 있다(제15조). 현재 우리나라의 전문 인력 확보 정도나 예산, 교육프로그램, 교육전문요원 등을 고려해 볼 때, 그와 같은 것을 각 기관이 각자 수행하는 것은 다소 어려운 점이 있을 것으로 예상된다. 그리고 국방 분야와 관련해서는 국방부에 우선권을 주고 있다(제16조). 이는 사이버테러가 사이버전쟁의 성격을 가지고 있을 경우에는 국방부가 대응해야 할 필요성이 있기 때문이다.

다만, 본 법률안의 경우 주로 중앙행정기관 등에 제한하여 규정하고 있기 때문에 국가 사이버위기가 발생하는 경우 민간분야까지 체계적으로 관리할 수 있을 지에

45) 국가 사이버안전 관리에 관한 법률안(1904286).

대해 의구심을 보이기도 한다.[46] 그리고 해당 규정에는 처벌규정을 두고 있기 때문에 사이버안전에 대한 책무를 강제할 수 있는 방안에 한계가 보이기도 한다.

2. 서상기 의원안

서상기 의원은 '국가 사이버테러 방지에 관한 법률안'으로 발의하였다.[47] 서상기 의원안은 제1장 총칙, 제2장 국가 사이버테러 방지 및 위기관리 추진체계, 제3장 사이버테러 방지 및 위기관리 활동, 제4장 연구개발 및 지원 등, 그리고 제5장 벌칙으로 구성되어 있다.

본 안에서는 사이버테러를 방지하기 위해 국가정보원장 소속하에 '국가사이버안전전략회의'를 두도록 하고 있다(제6조). 하태경 의원이 국무총리 산하에 두고 있는 것과 대비된다고 하겠다. 따라서 전략회의의 의장은 국가정보원장이 된다. 그런데 본 조문에서 보면 중앙행정기관의 장은 소관 책임기관에 대하여 사이버테러와 관련된 실태를 점검하고 평가하되, 국가정보원장이 그 모든 결과를 취합하여 국회에 보고하도록 하고 있다(제8조 제2항). 그런데 국회와 법원, 헌법재판소, 중앙선거관리위원회에 대한 점검과 평가는 관련 기관의 사무총장 또는 사무처장이 요구하는 경우에만 가능하도록 하고 있다(제2항 단서). 이는 문제점이 발생하는데 그에 대해서는 아래의 법률안에서 이야기하고자 한다.

국가정보원정은 국가사이버안전센터를 설치하고, 그 운영을 위해 민·관·군 합동대응팀을 설치 및 운영할 수 있도록 하고 있으며, 중앙행정기관 및 지원기관의 장에게 그를 위한 인력과 장비의 지원을 요청할 수 있도록 하고 있다(제9조 제3항, 제4항). 이는 현행 훈령으로 되어 있는 조직을 법률에 명시하는 것이다. 현재 정보통신망법에서는 민·관 합동조사단에 대한 근거규정을 두고 있으나, 사이버테러가 발생하는 경우에는 훈령에 따른 민·관·군 합동조사단이 운영되는 문제점을 법률로 해결하는 것이 된다.

---

46) 허영호, 검토보고서, 2014, 71~72쪽(http://likms.assembly.go.kr/bill/jsp/BillDetail.jsp?bill_id=PRC_P1D3O0N3T2Y6A1K7D5A5E5J8Q2M5Q3, 2015.11.10. 방문).

47) 국가 사이버테러 방지에 관한 법률안(1904459).

각 기관의 장은 국가정보원장과의 협의하에 사이버테러 방지대책을 수립하고 시행해야 한다(제10조). 그리고 악성프로그램의 확산을 차단하고(제11조), 보안관제센터 등을 설치하며(제12조), 사고조사를 수행하여 보고하고(제13조), 사이버테러 대응 훈련도 시행하도록 한다(제14조).

국가정보원장은 사이버위기경보의 발령에 대한 권한을 가지고 있는데, 이는 현재도 운영되고 있으며, 그를 명문화 하는 것이라고 하겠다(제15조). 만일 사이버위기가 발생하여 경계단계 이상이 된 경우에는 국가정보원장을 대책본부장으로 하는 사이버위기대책본부가 구성되어 대응을 하도록 하고 있다(제16조).

하태경 의원안에서는 각 중앙부처가 인력양성 및 교육홍보를 수행하도록 하고 있는 것에 비해 서상기 의원안에서는 정부가 연구개발(제19조)이나 산업육성(제20조), 인력양성 및 교육홍보(제21조), 국제협력(제22조)을 하도록 규정하고 있다. 또한 사이버테러와 관련된 포상 규정을 두고 있으며(제24조), 하태경 의원안과 달리 처벌규정(제25조)과 과태료 규정(제26조)도 두고 있다.

서상기 의원안에 대해서는 책임기관, 중앙행정기관, 관계행정기관, 관계기관 등 각 기관들의 업무와 역할, 관계 등에 대해 명확한 구분이 미약함과 동시에 현행 규정인 '국가사이버안전관리규정'에서는 국방 분야의 특수성을 고려하여 특례를 규정하고 있는 반면, 동 법률안에서는 그와 같은 것이 적용되지 못하고 있다는 견해가 있다.[48]

3. 이철우 의원안

이철우 의원은 '사이버위협정보 공유에 관한 법률안'을 발의하였다.[49] 동 법률안은 사이버위협의 특성을 고려하여 민간과 공공이 사이버위협정보를 공유하고 함께 분석할 수 있도록 하여 사이버위협을 조기에 탐지하고 전파하는 체계를 구축하는 것을 그 목적으로 삼고 있다.[50] 다른 법률안들은 사이버테러에 대한 조직과 임무 등 사이버

48) 허영호, 검토보고서, 2014, 72~73쪽(http://likms.assembly.go.kr/bill/jsp/BillDetail.jsp?bill_id=PRC_P1D3O0N3T2Y6A1K7D5A5E5J8Q2M5Q3, 2015.11.10. 방문).
49) 사이버위협정보 공유에 관한 법률안(의안번호 15185).
50) http://likms.assembly.go.kr/bill/jsp/BillDetail.jsp?bill_id=PRC_V1F5Z0J5U1L9T1X3E4S1B4T2L1F7W7, 2015.11.10 방문.

테러에 대한 전반적인 내용을 규율하고 있는 것에 반하여 동 법률안은 사이버위협정보의 원할한 공유에 그 초점을 맞추고 있다.

동 법률안은 총 12개 조문으로 구성되어 있다. 제1조에서는 본 법률안의 목적을 정의하고 있고, 제2조에서는 관련 용어들의 정의를 하고 있다. 정의의 내용들은 여타 사이버테러 관련 법률안과 큰 차이점이 없다. 제4조에서는 사이버위협정보의 공유체계 구축에 대해서 규정하고 있는데, 그 주체는 국가정보원장이며, 국가안보실장, 미래창조과학부장관 및 금융위원회위원장 등과 협의하여 관련 절차를 마련하도록 하고 있다(제1항). 사이버위협정보 공유기관에는 헌법, 정부조직법, 국가정보화 기본법에 규정된 공공기관, 정보통신기반 보호법상의 주요정보통신기반시설 관리 기관, 정보통신망법에서의 주요정보통신서비스 제공자, 전자금융거래법상의 기관·단체·사업자, 그리고 산업기술의 유출방지 및 보호에 관한 법률에서의 기업체나 연구기관이다(제2항).

국가정보원장은 사이버위협 공유를 위해 사이버위협정보 공유센터를 설치하여 운영할 수 있고(제5조 제1항), 관련 기관이나 업체에서 파견된 전문 인력으로 구성하여 운영하도록 하고 있다(제2항). 그에 따라 사이버위협정보 공유센터장은 사이버위협정보를 종합하고 분석하여 관련 정보를 분배하고, 필요한 조치를 취하도록 해야 한다(제6조). 하지만 사이버위협정보에는 중요한 내용들이 포함되어 있다. 따라서 국가정보원장은 법무부장관, 행정자치부장관, 미래창조과학부장관, 금융위원회 위원장 및 민간 전문가가 참여하는 협의회를 구성하여 관련 대책을 수립하여야 한다(제7조).

눈에 띄는 규정은 제8조인데, 사이버위협정보의 보유자 또는 악성코드 감염자는 공유센터장에게 신고할 수 있고(제1항), 또는 공유센터장이 그들에게 국가의 안전보장을 위한 목적으로 관련 정보를 요구할 수도 있다(제2항). 공유센터 장은 국회에 사이버위협정보 공유 활동의 결과를 평가하고 보고해야한다(제9조). 제11조에서는 사이버위협정보 공유와 관련해서 알게된 비밀을 누설하는 경우를 처벌하고 있으며, 제12조에서는 각 기관의 장이 알게된 정보를 누설하는 경우 과태료를 부과하도록 하고 있다.

사실 동 법률안의 효과는 매우 지협적이라고 할 수 있다. 사이버테러 관련 법률안들이 사이버테러와 관련된 전체적인 체계와 임부, 수행방법 등에 대해 폭넓게 규정하고

있는 것에 비해 동 법률안은 사이버위협정보와 관련된 내용만을 규정하고 있기 때문이다. 그리고 주요 규정들은 대통령령에 위임하고 있기 때문에 전체적인 규정이 어떤 모습을 보일지도 법률안으로만은 알 수 없다. 다만, 사이버위협정보를 공유해야 한다는 의식을 고취시키는 점에 있어서는 의미가 있다고 하겠다.

4. 이노근 의원안

이노근 의원안은 서상기 의원안과 구조적으로 유사성을 띄고 있다.[51] 따라서 법률안은 크게 제1장 총칙, 제2장 사이버테러 방지 및 위기관리 추진체계, 제3장 사이버테러 방지 및 위기관리 활동, 제4장 연구개발 및 지원 등, 그리고 제5장 벌칙으로 구성되어 있다. 먼저 제1장에서는 본 법률안의 목적과 정의, 다른 법률과의 관계, 책임기관의 책무, 책임기관 소속 공무원 등의 책무, 민·관 협력 등을 규정하고 있다. 특히 제5조에서는 책임기관의 소속공무원을 특사경으로 지정하도록 하고 있다(제5조 제2항).

제2장에서는 사이버테러 방지 및 대응에 대한 주요 내용들을 심의하는 기관으로 국가정보원장 산하에 사이버안전전략회의를 두도록 하고 있다(제7조 제1항). 그리고 효율적인 운영을 위해 사이버안전전략회의에 사이버안전대책회의를 둘 수 있다(제5항). 각 중앙행정기관은 매년 사이버안전계획의 이행여부를 매년 확인하고, 국가정보원장은 그들을 종합하여 매년 국회에 보고하도록 하고 있다(제9조 제2항). 그런데 국회·법원·헌법재판소·중앙선거관리위원회에 대한 점검·평가는 국회사무총장·법원행정처장·헌법재판소 사무처장 및 중앙선거관리위원회 사무총장이 요청한 경우에만 실태를 점검하고 평가하도록 하고 있다. 동 법률안의 가장 큰 문제점이 이 부분이라고 할 수 있다. 이번 국회 해킹 사건에서 볼 수 있는 바와 같이[52] 사이버테러는 국회나 법원, 헌법재판소, 중앙선거관리위원회 등 어느 기관도 가리지 않고 발생할 수 있으며, 특히 그와 같은 기관들은 사이버테러의 대상이 되기 싶다. 무엇보다 사이버테러 대응에 대해서는 절대로 예외가 있어서는 안 된다. 그 예외가 바로 공격의 대상이 될 수 있기 때문이다. 그럼에도 요청이 있는 경우에만 사이버안전 실태를 점검하고 평가

51) 사이버테러 방지 및 대응에 관한 법률안(15777).
52) http://news.jtbc.joins.com/html/670/NB11072670.html, 2015.11.10. 방문.

하도록 한 것은 본 법률안의 허점이라고 할 수 있다. 그리고 제10조에서는 사이버안전센터를 설치하도록 하고 있는데, 이는 현행 사이버안전센터에 대한 규정을 확인한 것이라고 할 수 있다.

제3장에서는 각급 기관들이 사이버테러를 방지하기 위한 대책을 수립하고 시행하는 것과 관련된 내용들 규정하고 있다. 그런데 여기서도 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관은 해당 기관의 장이 필요하다고 인정하는 경우에만 적용하도록 하고 있다. 이는 앞서 말한 바와 같이 사이버안전에 대한 흠결이라고 할 수 있다. 만일 국가정보원이 관리하는 것에 대한 부담으로 인한 것이라면 점검 및 평가하는 기관을 제3의 독립된 기관에 의할지라도 점검과 평가가 필요하다고 할 수 있다. 그리고 국가정보원장은 사이버테러 방지를 위한 매뉴얼 개발과(제12조), 악성프로그램 차단(제13조)을 위해 노력해야 하고, 책임기관의 장은 보안관제센터를 설치 및 운영하도록 하고 있다(제14조). 그와 함께 사이버테러에 대한 사고조사와(제15조), 대응훈련(제16조), 사이버위기경보의 발령(제17조), 대책본부구성(제18조) 및 기술지원(제19조)에 대한 규정을 두고 있는데, 이는 현행의 실무를 그대로 적용한 것이라고 할 수 있다.

제4장에서는 책임 기관에 대한 지원(제20조)과 사이버테러 방지를 위한 연구개발(제21조), 산업양성(제22조), 인력양성(제23조), 국제협력(제24조)에 대한 원칙들을 규정하고 있다. 다만, 본 장의 내용들이 제대로 수행되기 위해서는 국가정보원의 노력으로는 불가능 하고 다른 기관들의 협력이 필요하게 된다. 예를 들어, 관련 산업을 양성하는 것에 대한 부분은 시장이 작동해야 하는 부분이기도 하다. 따라서 본 규정은 원칙만을 선언한 것이라고 할 수 있다.

그리고 제5장에서는 벌칙 규정을 두고 있는데, 보안관제센터 설치 및 운영, 사고조사, 비밀엄수와 관련해서 위반한 경우에는 5년 이하 5천 만원 이하의 벌금에 처하도록 하고 있다(제27조 제1항). 업무상 과실의 경우에도 처벌하고 있다(제2항). 또한 제3항에서는 과태료 처분도 규정하고 있다. 다만, 염려되는 것은 사이버테러의 경우 내부의 완벽한 대응이 거의 불가능하고, 그로 인해 보안담당자들은 언제나 처벌의 위험에 처하게 된다. 그러므로 벌칙 규정에 대해서는 좀 더 고민을 해 보아야 할 것이다.

5. 사이버테러 관련 법률안 검토

앞서 살펴본 사이버테러 대응 법체계 정비방안에서는 몇몇 주요 견해들이 제시되었다. 그를 중심으로 제출된 법률안들의 내용을 살펴볼 필요가 있다.

먼저, 정비방안에서는 독립된 통합법체계를 구축해야 한다고 하였다. 이는 현행 법률체계가 주가 되는 내용은 훈령에 있고, 단편적인 내용들이 법률로 규정되어 있기 때문이다. 그런 측면에서 보면 제출된 법률안들은 현행 훈령의 내용을 법률의 단계로 승격시키고 있기 때문에 적절하다고 하겠다. 다만, 이철우 의원안은 사이버위협정보의 공유에 주안점을 두고 있기 때문에 독립된 통합법체계와는 다소 거리가 있다고 할 수 있다. 물론 이철우 의원안도 대통령령을 통해 다른 법률안에서의 내용들이 어느 정도 규정될 수 있지만, 법령명에서 볼 수 있듯이 사이버위협정보의 공유라는 한계를 가질 수밖에 없다.

다음으로 사이버테러 대응 법체계가 현실을 제대로 반영할 필요가 있다는 지적이 있었다. 현행 체계는 앞서 언급한 것처럼 청와대의 국가안보실에 사이버안버비서관이 신설되어 사이버안전을 위한 컨트롤 타워 역할을 수행하고, 그를 정점으로 국가정보원과 국방부, 미래창조과학부가 각각 민·관·군의 사이버안전 문제를 주관하도록 하고 있다. 그와 함께 지방자치단체, 지방교육청 등도 사이버안전체계에 포섭되어 국가사이버안전체계망을 구축하도록 하고 있다. 하지만 제출된 법률안은 이전의 국가정보원 중심의 체계를 염두에 두고 있기 때문에 지금의 현실을 적절히 반영하고 있지는 못한 것으로 보인다. 이전 체계에서는 국가정보원이 훈령에 따른 컨트롤타워 역할을 수행하고, 국가정보원을 정점으로 사이버안전체계가 형성되었지만, 현행 시스템은 청와대가 컨트롤 타워가 되는 구조를 가지고 있기 때문이다. 이는 국무총리를 그 주체로 하는 하태경 의원안 보다도 더욱 강력한 결집력을 발휘할 수 있는 구조라고 할 수 있다. 하지만 제출된 법률안에서는 그와 같은 내용이 적절히 반영되고 있지 못하다.

그리고 정비방안에서는 사이버안전의 문제는 기존의 국가기관 중심의 체계로는 해결이 거의 불가능하기 때문에 민간이나 개인까지도 통합하여 규정할 필요가 있다고 하였다. 그러므로 사이버안전체계의 형상이 거버먼트(Government)에서 거버넌스

(Governance)로 이전하여 기업이나 단체, 개인 등도 국가의 사이버안전을 위해서 체계 내에 포섭될 필요가 있다고 하였다. 하지만 제출된 법률안에서는 여전히 국가기관이 사이버안전의 주요 담당자로 자리 잡고 있으며, 기업이나 민간단체, 개인 등은 국가의 지시를 받는 객체로만 규정되어 있을 따름이다. 그와 같은 체계구축은 현실의 사이버위협에 대한 대응방안을 적절히 제시하고 있는 것이라고 보기 어렵다. 그러므로 법령이 거버넌스의 개념을 포섭하여 제시될 필요가 있다고 사료된다.

제3절 소결

사이버테러에 있어 한국은 최근에 발생한 국회의 해킹 사태를 포함하여 이제까지 여러 차례에 걸쳐 다양한 상황들을 경험하였다. 그에 따라 관련 정책이 개발되어 발전되기도 하였고, 각 부문의 법률들에도 사이버테러와 관련된 내용들이 포함되기도 하였다. 이제까지 사이버테러가 발생하면 적절한 대응을 하지 못한 이유가 컨트롤 타워의 부재라는 견해가 제기되었고, 그로 인해 2015년에는 청와대가 적극적으로 사이버위협에 대한 컨트롤 타워 역할을 수행할 수 있는 조직도 만들어지게 되었다. 그럼에도 불구하고 아직까지 관련 법률은 현실의 상황을 제대로 반영하지 못하고 있는 실정이다. 국회에 제출된 사이버테러방지법은 여전히 계류 중에 있으며, 제출된 법률안들이 지금의 현실을 제대로 반영하지 못하고 있는 부분도 어느 정도 존재하고 있다. 이와 같은 상황에서 최근 발생 국회의 해킹 사태는 다시금 새로운 시각을 제시해 주기도 한다. 사이버테러방지법에서 제외되었던 국회에 대해서도 강력한 사이버보호 조치가 요구된다는 것이다. 그럼에도 불구하고 여전히 국회에서는 필요성에 대한 논의에서 쉽게 벗어나지 못하고 있는 상황이다.[53]

우리나라의 사이버안전의 문제에서 사이버테러리스트와 우리나라는 소위 "제로섬 게임"을 하고 있다.[54] 특히 사이버공간에서의 보안은 99%가 완벽하다고 하더라도 1%만 뚫리게 되면 모두 뚫리는 것과 같다. 그러므로 사이버안전에 있어서는 예외가 존재하면 안 된다. 그러므로 사이버테러에 대한 정책에 있어서도 세밀한 정책이 필요

53) http://www.fnnews.com/news/201510261550578209, 2015.11.10 방문.
54) 제로섬게임이란 게임에 참여하는 두 사람이 있는 경우 승자가 되는 사람의 이득과 패자가 되는 사람의 이득을 합할 경우 그 총합이 0(zero)가 된다는 이론이다.

하며, 법률에 있어서도 보다 면밀한 검토가 필요하다. 그러기 위해서는 일부만이 정책이나 법률 제정과정에 참여하여서는 안 되며, 보다 많은 전문가들과 기관, 기구, 단체 등이 참여하는 '멀티스테이크홀더(multistakeholder)'의 모습을 보여야 할 것이다. 그와 함께 국가 중심의 거버먼트에서 다수가 참여하는 거버넌스 형태로의 변경도 요구된다. 이는 사이버위협이 더 이상 국가만의 문제가 아니라는 것이며, 국가만의 힘으로는 해결할 수 없다는 것도 의미한다.

더 나아가 비록 본 장에서는 한국 내의 정책에 국한되어 살펴보았지만, 사이버테러는 국제적인 문제라고 할 수 있다. 그러므로 국제적인 협력도 사이버테러 관련 정책의 한축을 형성하여야 할 것이다. 따라서 사이버테러와 관련된 국제협약이나 양자간 협약 등에도 보다 많은 노력을 기울일 필요가 있다.

제3장

KOREAN INSTITUTE OF CRIMINOLOGY

미국의 사이버테러 관련 형사사법정책

김한균·박소영·안수정

제3장

미국의 사이버테러 관련 형사사법정책

제1절 사이버안보정책 개관

2001년 9월 11일 종교적 무장 테러범들에 의한 미국본토 공격[55] 이후 선포된 테러리즘과의 전쟁을 시작으로, 미국은 주요기반시설 방호를 위한 노력을 경주해 오고 있다. 9/11 테러가 일어난 2001년과 그 이후 사이버안보정책의 산물들을 살펴보면 다음과 같다.

부시(George W. Bush) 행정부 시절에는 미국 국토안보부(Department of Homeland Security, DHS) 설립,[56] 주요기반시설보호위원회(Critical Infrastructure Protection Board) 설립[57], 미국연방 정부 정보시스템의 보안을 위한 연방정보보안관리법(the Federal Information Security Management Act, FISMA) 제정[58], 국가 사이버 보안 종합 기획(the Comprehensive National Cybersecurity Initiative, CNCI)[59] 등이 시행되었다.

---

55) '9/11 공격'은 알-카에다(al-Qaeda) 이슬람 테러리스트들이 2001년 9월 11일 아침 동부 네 개 도시에서 캘리포니아로 향하는 4대의 비행기를 납치하여 뉴욕 세계무역센터의 쌍둥이 타워와 워싱턴 D.C, 미 국방부 청사에 충돌시킨 사건이다. 이에 대한 자세한 내용은 다음에서 확인 가능하다. http://www.911memorial.org/faq-about-911

56) 2001년 10월 행정명령 13228(*국토안보부실 및 국토안보위원 설립(Establishing the Office of Homeland Security and the Homeland Security Council)*)과 2002년 11월 의회를 통과한 국토안보법(Homeland Security Act)에 의해 설립되었다. 미 국토안보부 (DHS)의 설립에 대한 세부정보는 다음에서 확인 가능하다. http://www.dhs.gov/creation-department-homeland-security

57) 동 위원회는 부시 대통령의 행정명령 13231(*정보화 시대의 주요기반시설 보호(Critical Infrastructure Protection in the Information Age)*)으로 설립되었다. https://www.dhs.gov/xlibrary/assets/executive-order-13231-dated-2001-10-16-initial.pdf

58) http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

59) 동 이니셔티브는 부시 행정부에서 오바마 행정부로 계승되었으며, 이에 대한 자세한 내용은 다음에서 확인 가능하다. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

1. 오바마 행정부 시기 관련정책

오바마(Barack Obama) 행정부는 대통령 사이버보안 위원회(Commission on Cybersecurity for the 44th Presidency), 2011년에 발표된 DHS의 안전한 사이버 미래를 위한 청사진: 국토안보체계를 위한 사이버보안 전략(Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise), 대통령의 행정명령 13636(Executive Order No. 13636, E.O. 13636), 대통령 정책지침(President Policy Directive, PPD) 21: 주요기반시설 보안 및 회복성(resilience), 미국표준기술연구소(National Institute of Standards and Technology, NIST)의 국가기반시설의 사이버보안 개선을 위한 프레임워크, 4개년 국가안보점검(the Quadrennial Homeland Security Review), SANS 연구소의 핵심보안통제, NIST가 진행 중인 특정 기획 등을 통하여 사이버보안 정책을 펼치고 있다.

2. 관련 법제개혁 성과

가. 2001년 애국법

부시 행정부 시기, 2001년에 제정된 미국 애국법(USA PATRIOT Act)은 주요기반시설(critical infrastructure)에 대한 정의를 제시하며, 그 정의는 아래 〈표3-1〉과 같다.

그리고 E.O. 13228 Section 3의 (c)보호(protection)[60]는 미국을 테러 공격으로부터 보호하고자 국토안보실(Office of Homeland Security)을 창설한다. 뿐만 아니라 다음과 같은 국가기반시설에 대한 보호를 규정한다. 해당 주요기반시설에는 에너지 생산, 전달, 배포 서비스 및 핵심 시설, 그 밖의 수도, 전기, 가스 등 공익시설, 전기통신(telecommunications), 핵물질취급시설, 그 밖의 국가 기반 서비스 및 핵심 시설이 포함된다.

60) 동 행정명령에 대한 자세한 내용은 다음에서 확인 가능. http://www.gpo.gov/fdsys/pkg/WCPD-2001-10-15/pdf/WCPD-2001-10-15-Pg1434.pdf

〈표 3-1〉 주요기반시설(critical infrastructure)에 대한 정의

"Critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. -USA PATRIOT ACT Section 1016. (e)	"주요기반시설"이란 유형 또는 가상의 시스템이나 자산이 미합중국에 있어 매우 중요하여 그러한 시스템이나 자산의 불능이나 파괴가 안보, 국가 경제 안보, 국가 공중 보건 및 안전, 또는 이러한 사안들의 조합에 대하여 악영향을 미치는 것을 일컫는다. -미국애국법 Section 1016, (e)

나. 2002년 연방정보 보안관리법

2002년에 제정된 연방정보 보안관리법(FISMA)는 동 법률 제3541로 (목적(Purposes))에서 밝히듯 정보보안의 효율성을 보장하는 통합적 기본 틀을 제공하여 연방 활동 및 자산을 지원하는 정보를 통제한다. FISMA에 따라 관리예산처(Office of Management and Budget, OMB)는 정보보안에 관한 정책, 원칙, 기준, 지침을 개발하고 감독한다. 또한 이를 위한 체계성을 보장하고자 미국표준기술연구소(NIST)으로 하여금 연방 정보 시스템에 관한 기준과 지침을 마련하도록 한다. 동 법률은 "각각의 연방 기관들로 하여금 기관 수준의(agency-wide) 프로그램을 개발, 기록, 이행하여 정보 및 정보 시스템을 위한 정보보안을 제공할 것을 요청하며, 이를 통해 해당 타 기관, 도급업자, 또는 다른 방식으로 제공 또는 관리되는 기관의 활동 및 자산을 지원한다."[61]

다. 2014년 개정 연방정보 보안관리법

FISMA는 2014년 12월 18일 개정[62]되었다 (이하 FISMA 2014). 다음과 같이 연방정부의 사이버보안 관행이 개편되었다. 아래 내용은 해당 업데이트에 관해 DHS에 안내된 것이다.

첫째, 기술적 지원 제공 및 기술의 효율적 사용을 포함하는 비(非)국가적 보안 연방행정부 시스템을 위한 정보보안정책의 이행을 관리하는데 있어 DHS의 권한이 성문화되었다. (Codifying DHS authority to administer the implementation of

61) 미국표준기술연구소(NIST), 자세한 개괄(Detailed Overview), http://csrc.nist.gov/groups/SMA/fisma/overview.html 2015.11.15.방문.
62) https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

information security policies for non-national security Federal Executive Branch systems, including providing technical assistance and deploying technologies to such systems.)[63]

둘째, 연방기관의 정보 보안 관행에 관한 OMB의 감독 권한이 개정 및 명료화 되었다. (Amending and clarifying the OMB's oversight authority over federal agency information security practices.)[64]

셋째, OMB가 OMB A-130 (연방정보자원의 관리)를 "비효율적이고 낭비적인 보고 제거"로 개정 또는 수정하도록 요청 하였다. (Requiring OMB to amend or revise OMB A-130 to "eliminate inefficient and wasteful reporting")[65]

라. 국가 사이버보안 종합계획

부시 대통령은 2008년 대통령령을 통해 국가 사이버 보안 종합 계획(CNCI)을 수립하였으며, 오바마 대통령은 동 계획을 계승하여 사이버보안 정책의 핵심 요소로 삼고 있다. 동 계획은 DHS와 국가안보국(National Security Agency, NSA)가 공동 주관하며, 미국 사이버보안의 프레임워크를 구성하는 총 12개 항목이 있다. 이에 대한 자세한 내용은 이후 제2절에서 다루기로 한다.

제2절 現 오바마 정부의 사이버안보 정책

정부 출범 초기부터 오바마 대통령은 사이버안보의 중요성을 인식하고 이에 대한 국가적 대응방안을 적극적으로 모색해왔다. 정부는 사이버 방호 향상, 대응 역량 증진, 돌발 상황 관리 도구 개선을 위해 국내·외적으로 폭넓은 정책을 시행한 바 있다.[66]

사이버 위협이 그 강도와 기법 면에서 지속적으로 고조됨에 따라 행정부의 노력

63) 미국 국토안보부(DHS), 연방정보보안관리법(FISMA), http://www.dhs.gov/fisma, 2015. 11.15.방문.
64) 미국 국토안보부(DHS), 연방정보보안관리법(FISMA), http://www.dhs.gov/fisma, 2015. 11.15.방문.
65) 미국 국토안보부(DHS), 연방정보보안관리법(FISMA), http://www.dhs.gov/fisma, 2015. 11.15.방문.
66) 미국 국토안보부(DHS), 연방정보보안관리법(FISMA), http://www.dhs.gov/fisma, 2015. 11.15.방문.

또한 강화되고 있다. 사이버 보안은 특성상 고립된 단일적 조치만으로는 그 위기를 적절히 관리할 수 없기 때문에 행정부는 사이버안보에 관한 기획을 장기적, 포괄적으로 진행하고 있다. 오바마 정부의 사이버안보 정책은 다음 영역에 중점을 두고 펼쳐진다.

주요기반시설 보호, 연방 네트워크 안보 개선, 돌발 상황에 대한 대처 및 관리 역량 제도, 국제적 연합체 구축, 미래의 안전한 사이버 공간 형성이 그것이다.

오바마 정부는 사이버안보 위협에 대한 접근방식을 강화하는데 있어 다섯 가지 우선순위를 제시한다. 사이버안보 우선순위는 다음과 같다.

(1) 사이버 위협으로부터 미국의 가장 중요한 정보 시스템인 핵심기반시설을 보호한다. (Protecting the country's critical infrastructure-our most important information systems-from cyber threats.)[67]

(2) 사이버 사건을 식별하고 신고하기 위한 역량을 제고하여 신속하게 대처하도록 한다. (Improving our ability to identify and report cyber incidents so that we can respond in a timely manner.)[68]

(3) 사이버 공간상의 자유를 장려하고 개방적이고, 상호운용적(interoperable)이며, 안전하고, 믿을 수 있는 사이버 공간을 구축하기 위한 국제적 동반자들과의 협력한다. (Engaging with international partners to promote internet freedom and build support for an open, interoperable, secure, and reliable cyberspace.)[69]

(4) 명확한 안보 세부목표 설정과 유관 기관들이 그 세부목표의 달성을 위해 책임의식을 갖게 함으로써 연방 네트워크를 방호한다. (Securing federal networks by setting clear security targets and holding agencies accountable for meeting those targets.)[70]

(5) 인터넷에 능통한 인력 구성과 민간부문과 강한 연대를 형성한다. (Shaping a cyber-savvy workforce and moving beyond passwords in partnership with the private sector.)[71]

---

67) https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/summit
68) https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/summit
69) https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/summit
70) https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/summit
71) https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/summit

위의 우선순위를 실행해 옮기고 사이버 안보를 강화하기 위해 오바마 정부는 다음의 다섯 가지 원칙을 준수한다. 해당 원칙은 정부 통합적(whole-of-government) 접근방식, 네트워크 방호 우선원칙, 사생활 및 시민의 자유 보호, 정부-민간 협력, 국제 협력 및 참여이다.

1. 국가 사이버 보안 종합 계획 및 행정명령 제13636 호

가. 국가 사이버보안 종합 계획 (The Comprehensive National Cybersecurity Initiative, CNCI)

부시 대통령은 2008년 1월 국가안보 대통령령 제54호/국토안보 대통령령 제23호(NSPD-54/HSPD-23)을 통하여 국가 사이버 보안 종합 계획(CNCI)을 출범했다.[72] 오바마 대통령은 동 CNCI를 계승하였다. 이에 대하여 백안관의 외교정책을 소개하는 사이트에서 설명하고 있다.[73] 이에 따르면, 오바마 대통령은 CNCI와 그 유관 활동들이 더욱 폭넓고, 향상된 미합중국 사이버보안 전략의 핵심 요소로서 발달시켜나갈 것을 결정했다. 또한 CNCI는 사이버 공간상 미국이 다음의 세 가지 주요 목표를 달성할 수 있도록 설계된 활동들로 구성된다.[74]

(1) 오늘날의 즉각적 위협에 대항한 최전 방호선 구축

연방 정부 내 네트워크 취약점, 위협, 사건에 대한 상황인식의 공유를 형성 또는 증대한다. 현존하는 취약점 감소 및 침임 방지를 위해 빠르게 대응하는 능력의 형성 또는 향상도 필요하다. 이는 궁극적으로 주, 지방정부 및 민간부문 파트너를 포괄한다.

(2) 위협의 전(全)영역에 대한 방호

미국의 방첩 능력의 개선 및 핵심 정보 기술 관련 공급망의 보안을 향상한다.

---

72) 미국 백악관(the White House), 국가 사이버 보안 종합 계획(the Comprehensive National Cybersecurity Initiative), https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative, 2015.11.15.방문.

73) 미국 백악관(the White House), 국가 사이버 보안 종합 계획(the Comprehensive National Cybersecurity Initiative), https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative, 2015.11.15.방문.

74) 미국 백악관(the White House), 국가 사이버 보안 종합 계획(the Comprehensive National Cybersecurity Initiative), https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative, 2015.11.15.방문.

(3) 미래 사이버보안 환경 강화

사이버 교육 확대, 연구 및 개발을 조정 및 재수립을 위한 전(全) 연방정부기관의 노력, 사이버공간 상 적대적 및 악의적 활동을 저해하기 위한 전략을 인식하고 개발을 위해 노력한다.

"To establish a front line of defense against today's immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threat, and events with the Federal Government-and ultimately with state, local, and tribal governments and private sector partners-and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions."[75]

"To defend against the full spectrum of threats by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies."[76]

"To strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the Federal Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace."[77]

CNCI에 따르면[78], 동 계획을 수립하는데 있어 정부 내 특정 핵심 전략적 기반역량을 강화가 필수적이다. 따라서 CNCI는 다음을 포함하게 되었다. 첫째, 범죄수사 등 핵심 기능을 개선하기 위한 연방 법 집행, 첩보, 방어 공동체를 위한 재원지원, 둘째, 정보의 수집, 처리, 분석, 셋째, 국가적 사이버보안 노력을 가능케 하는데 필수적인 정보 보증이 그것이다.

---

75) 미국 백악관(the White House), 국가 사이버 보안 종합 계획(the Comprehensive National Cybersecurity Initiative), https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative, 2015.11.15.방문.

76) 미국 백악관(the White House), 국가 사이버 보안 종합 계획(the Comprehensive National Cybersecurity Initiative), https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative, 2015.11.15.방문.

77) 미국 백악관(the White House), 국가 사이버 보안 종합 계획(the Comprehensive National Cybersecurity Initiative), https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative, 2015.11.15.방문.

78) 미국 백악관(the White House), 국가 사이버 보안 종합 계획(the Comprehensive National Cybersecurity Initiative), https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative, 2015.11.15.방문.

CNCI는 정부 전반에 걸쳐서 민간 전문가들과의 긴밀한 협의를 통해 사생활과 시민 자유 충족을 위해 많은 노력과 주의를 기울여 개발되었으나, 시민적 자유와 사생활권 보호는 CNCI의 이행에서 기본적 목적으로 유지된다.[79] 오바마 대통령이 표명한 투명성(transparency) 시책에 따라 사이버공간 정책 점검(Cyberspace Policy Review)는 정보 공유 향상을 효과적인 사이버보안의 핵심요소로 꼽았다.[80] 이러한 연방정부의 노력에 대한 대중의 이해를 증진시키기 위하여 사이버보안 조정관(Cybersecurity Coordinator)은 다음과 같이 CNCI의 주요내용을 공개하였다. 여기서는 CNCI의 12개 세부항목(initiatives)만 대략적으로 소개하도록 한다.

〈표 3-2〉 CNCI의 12개 세부항목(initiatives)

Initiative #1	연방정부의 네트워크를 신뢰할 수 있는 인터넷 접속(Trusted Internet Connections, TIC)를 활용한 단일 네트워크로 관리 (Manage the Federal Enterprise Netwo가 as a single network enterprise with Trusted Internet Connections.)
Initiative #2	연방 네트워크 전역에 침입탐지시스템 배치 (Deploy an intrusion detection system of sensors across the Federal enterprise.)
Initiative #3	연방 네트워크 전역에 침입방지시스템 배치 (Pursue deployment of intrusion prevention systems across the Federal enterprise.)
Initiative #4	연구개발(R&D) 노력의 조정 및 재수립 (Coordinate and redirect research and development (R&D) efforts.)
Initiative #5	상황인식 제고를 위한 기존 사이버운영센터의 연계 (Connect current cyber ops centers to enhance situational awareness.)
Initiative #6	정부 차원의 사이버 방첩활동 계획의 개발 및 이행 (Develop and implement a government-wide cyber counterintelligence (CI) plan.)
Initiative #7	기밀 네트워크의 보안 강화 (Increase the security of our classified networks.)
Initiative #8	사이버교육 확대 (Expand cyber education.)
Initiative #9	미래로 도약하기 위한 기술, 전략, 프로그램의 확립 및 개발 (Define and develop enduring "leap-ahead" technology, strategies, and programs.)
Initiative #10	지속적 억지 전략 및 프로그램 확립 및 개발 (Define and develop enduring deterrence strategies and programs.)
Initiative #11	국제적 공급네트워크의 위험관리를 위한 다차원 접근방식 개발 (Develop a multi-pronged approach for global supply chain risk.)
Initiative #12	주요기반시설 도메인 내 사이버보안 확대를 위한 연방정부의 역할 규정 (Define the Federal role for extending cybersecurity into critical infrastructure domains.)

79) 미국 백악관(the White House), 국가 사이버 보안 종합 계획(the Comprehensive National Cybersecurity Initiative), https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative, 2015.11.15.방문.

80) 미국 백악관(the White House), 국가 사이버 보안 종합 계획(the Comprehensive National Cybersecurity Initiative), https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative, 2015.11.15.방문.

나. 국가기반시설에 관한 행정명령 제13636 호[81] 및 대통령 정책지침-21[82]

E.O. 13636은 다년간 진행된 사이버안보 관련 연방정부의 역할에 관한 논의에도 불구하고 제정 법률안의 부재상황을 해결하기 위해 2013년 2월 공표되었다. 2월 12일에는 동 행정명령과 함께 대통령 정책지침(PPD)-21도 공표했다. 양 EO와 PPD는 모두 국가기반시설에 관하며, 민관협력(PPP)의 중요성을 명확히 밝히는 가운데 각각 아래와 같은 목표를 두고 있다.

1) E.O. 13636

국가기반시설 사이버보안 개선에 관한 E.O. 13636는 행정부에게 다음과 같이 지시한다.[83] 첫째, 기술 중립적이고, 자율적인 사이버보안 프레임워크 개발, 둘째, 사이버보안 관행의 도입을 촉진하고 보상금으로 장려, 셋째, 사이버 위협 정보 공유에 관한 양, 속도, 질의 향상, 셋째, 국가기반시설의 보안을 위한 모든 계획에서 사생활 및 시민자유의 엄격한 보장, 넷째, 사이버보안 촉진을 위한 기존법률 활용방안 연구가 그것이다. 그 중 기술 중립적이고, 자율적인 사이버보안 프레임워크 개발(사이버보안 프레임워크(Cybersecurity Framework))와 사이버 위협 정보 공유에 관한 양, 속도, 질의 향상(향상된 사이버보안 서비스(Enhanced Cybersecurity Services, ECS))는 PPP를 통해서 사이버보안 문제를 다루게 된다.

2) PPD-21

PPD-21은 국토보안 대통령령(Homeland Security Presidential Directive)-7(2003년 공표)을 대체하며, 다음과 같이 지시한다.[84] 첫째, 근 실시간으로 운영되는

---

81) 2014년 2월 12일자 동 행정명령은 국가기반시설에의 잦은 침입에 대한 사이버보안 개선의 필요성을 해결하고자한다. improving-critical-infrastructure-cybersecurity

82) 2014년 2월 12일에 행정명령 13636을 보완하고자 공표되었다. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

83) DHS, 행정명령 13636 및 대통령 정책지침 21(Executive Order (EO) 13636 국가기반시설 사이버보안 개선, Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience), https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf, 2015.11.15.방문.

84) DHS, 행정명령 13636 및 대통령 정책지침 21(Executive Order (EO) 13636 국가기반시설 사이버보안 개선, Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience), https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf, 2015.11.15.방문.

기반시설의 물리적 및 사이버 측면을 다루는 상황인지역량 개발, 둘째, 기반시설 실패의 연쇄적 결과에 대한 이해, 셋째, 민관협력 파트너십에 대한 평가 및 발달, 넷째, 국가기반시설보호계획 업데이트, 다섯째, 포괄적 연구 및 개발 계획 개발이 그것이다. PPD-21의 공표는 E.O. 13636과 함께 새로운 위험 환경과 터득한 중요 교훈에 적응하고, 적극적으로 역량 향상을 도모하기 위함이다.

2. 민간부문과의 협력을 통한 대응

미국 국제전략문제연구소(Center for Strategic and International Studies, CSIS)[85]는 2008년동안 대통령 사이버보안 위원회(Commission on Cybersercurity for the 44th Presidency)를 설립하였으며, 최종 보고서인 대통령 사이버공간 보안 정책(Securing Cyberspace in the 44th Presidency)[86]을 제출했다. 동 위원회의 최종보고서에 따르면, 동 위원회는 정부와 사이버보안, 두 영역에서의 경험을 갖고 있는 개인들로 구성되어 있으며, 그 목적은 오바마 행정부가 국가 사이버보안 관련 뚜렷한 개선을 신속히 이뤄내기 위한 권고사항을 제시하는데 있다. 또한 미국의 향후 사이버 목표에 있어 핵심적인 장기적 권고사항을 제시하게 된다.

동 위원회의 세 가지 주요 결론은 다음과 같다. ① 사이버보안은 오늘날 미국의 주요 국가안보문제 중 하나이다. ② 그 결정사항과 활동은 사생활과 시민적 자유를 준수해야만 한다. ③ 사이버보안의 국내적 및 국제적 측면 모두를 아우르는 포괄적 국가 안보 전략만이 미국을 더욱 안전하게 한다.

가. 주요 권고내용

동 위원회는 다음과 같이 10가지 권고사항을 제시하였다.[87]

(1) 사이버공간을 위한 포괄적인 국가안보전략 수립(Create a comprehensive national security strategy for cyberspace.)

---

85) 동 연구소는 미국 워싱턴 D.C.에 본부를 둔 미국을 대표하는 무당파·비영리 싱크탱크 중 하나로 미국 대외정책 및 국제전략적 이슈를 연구한다. www.csis.org

86) 국제전략문제연구소(Center for Strategic and International Studies, CSIS), 제44대 대통령 임기 간 사이버공간 보안(Securing Cyberspace in the 44th Presidency), http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf, 2015.11.15.방문.

87) 국제전략문제연구소(Center for Strategic and International Studies, CSIS), 제44대 대통령 임기 간 사이버공간 보안(Securing Cyberspace in the 44th Presidency), http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf, 2015.11.15.방문. 1-2쪽.

(2) 백악관의 선도적 역할(Lead from the White House.)
(3) 민관협력 파트너십(Public-Private Partnership, PPP)의 재조명(Reinvent the public-private partnership.)
(4) 사이버공간 규제(Regulate cyberspace.)
(5) 디지털 신분 인증(Authenticate digital identities.)
(6) 유관 당국의 현대화(Modernize authorities.)
(7) 보안 개선을 위한 인수정책(acquisitions policy) 활용(Use acquisitions policy to improve security.)
(8) 역량 증진(Build capabilities.)
(9) 기존 성과를 출발점으로 삼을 것(부시 행정부의 CNCI에서 시작할 것) (Do not start over.)

나. 민관협력 파트너십의 중요성

동 위원회가 강조하는 사항 중 하나인 PPP의 재조명은 사이버공간 보호를 위해서는 정부와 민간부문이 함께 일할 때에만 가능하다는 사실에서 기인한다. 이는 민간부문이 미국의 주요기반시설의 대부분을 설계, 배치, 유지하고 있기 때문이다.[88] 동 위원회의 최종보고서도 인정하듯이, 국가보안의 다른 특정 요소들과는 달리, 사이버공간은 정부 홀로는 지킬 수 없으며, 따라서 이러한 가상의 공간에 대하여 정부와 민간부문이 그 책임과 통제를 나눠 갖게 되는 것이다.

동 최종보고서에 따르면, 미국정부는 그 사이버보안 노력을 에너지, 금융, 정보통신기술(ICT), 주정부 및 시행정부를 포함하는 정부 서비스의 네 가지 핵심 가상기반시설에 집중할 필요가 있다. 정부와 회사간부 간 신뢰 구축과 사이버공간 관련 진정 핵심적인 것에 노력을 모을 것을 강조하는 권고가 제시되었다. 민관 신뢰 구축을 위해서는 정보공유를 도구로 인식하며, 기존의 복잡하고 비효율적인 구조를 단순화하여 실천중심적(action-oriented) 관계 형성을 권고했다.[89]

---

88) 국제전략문제연구소(Center for Strategic and International Studies, CSIS), 제44대 대통령 임기 간 사이버공간 보안(Securing Cyberspace in the 44th Presidency), http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf, 2015.11.15.방문. 43쪽.
89) 국제전략문제연구소(Center for Strategic and International Studies, CSIS), 제44대 대통령 임기 간 사이버공간 보안(Securing Cyberspace in the 44th Presidency), http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf, 2015.11.15.방문.

사이버보안을 위한 PPP의 중요성은 널리 알려진 바이며, 미국 사이버보안을 담당하는 해당기관뿐만 아니라 유관분야 전문가들 또한 그 중요성을 공식적으로 인정하고 있다. DHS는 그 연장선상에서 민관협력을 통한 회복성제고 컨퍼런스(Building Resilience through Public Private Partnership Conference)를 지속적으로 열어오고 있으며, 2015년 12월 10-11일 제5차 컨퍼런스가 열릴 예정이다.[90]

다. 국가사이버보안 협의회와 민관협력 파트너쉽

국가사이버보안협의회(National Cyber Security Alliance, NCSA)의 임무 이행을 위해서도 PPP는 필수적이다.[91] NCSA는 강한 민관파트너십을 구축하여 인터넷 사용자들의 사이버보안에 관한 인식을 제고하고, 사이버 위협으로부터 스스로를 보호할 수 있는 교육을 제공하여 사이버보안문화를 장려하는 기관이다.[92] 동 기관의 이사회는 Microsoft, AT&T Services, Inc., Google, PayPal, Intel, Symantec Corporation, Visa 등 세계유수기업들의 대표들을 포함한다. 그리고 동 기관은 매년 10월을 국제 사이버보안 이해의 달(National Cyber Security Awareness Month, NCSAM)로 선정하여 미국정부와 민간기업 간 공동노력을 강화하기 위한 지속적인 노력을 경주한다.[93] 2015년은 12번째 NCSAM의 해이며 백악관 또한 강한 지지를 보이고 있다. 2015년 9월 30일 오바마 대통령은 NCSAM을 지지하는 성명서를 발표한 바 있다.[94]

라. 사이버보안서비스의 강화

사이버보안을 위한 PPP의 다른 예는 DHS의 향상된 사이버보안 서비스(ECS)이다.

---

90) 제5차 민관협력을 통한 회복력제고 연례 컨퍼런스(Fifth Annual Building Resilience through Public-Private Partenership Conference)는 2015년 12월 10-11일 양일간 미국, 로스앤젤레스(LA)에서 개최될 예정이다.. http://www.dhs.gov/event/public-private-partnerships-conference 2014년에 열린 동 컨퍼런스에 대한 정보는 다음에서 확인 가능하다. http://www.dhs.gov/blog/2014/10/15/2014-building-resilience-through-public-private-partnerships-conference-blog

91) 미국 국가사이버보안협의회(NCSA), NCSA 소개(About NCSA), https://www.staysafeonline.org/about-us/, 2015.11.15.방문.

92) 미국 국가사이버보안협의회(NCSA), NCSA 소개(About NCSA), https://www.staysafeonline.org/about-us/, 2015.11.15.방문.

93) 미국 국가사이버보안협의회(NCSA), 국제 사이버보안 인식의 달(National Cyber Security Awareness Month), https://www.staysafeonline.org/ncsam/about, 2015.11.15.방문.

94) https://www.staysafeonline.org/ncsam/about

본 프로그램은 자율적 정보 공유 프로그램으로 E.O. 13636을 통해 "국가기반기설"로 분류되는 주체들뿐만 아니라 미국에 기반을 둔 이해관계있는 모든 공공 및 민간 조직을 포함하도록 확장되었다. ECS의 임무는 미국정부에 의해 민감 정보로 분류되어 공유가 어려운 정보들을 공공 및 민간 이행당사주체들과 공유케 함으로써 이들이 사이버위협으로부터 그들 스스로 뿐만 아니라 그들의 고객들까지도 지킬 수 있도록 돕는 것이다. 동 프로그램에 참여하기 위해선 적격심사를 거친 후 DHS와 양해각서(Memorandum of Agreement)를 채결해야 한다. 동 프로그램은 다음과 같은 방식으로 작동된다. 즉 ECS는 정부가 검열한 기밀의 민감한 사이버 위협 정보를 적격한 온라인 서비스 제공자(Commercial Service Provides, CSPs) 및 운영 책임자(Opertional Implementers, OIs)과 공유하고, CSP는 이 정보를 고객보호에, OI는 그 내부 네트워크를 보호하는데 활용하게 된다.[95]

3. 유관기관 간 협력을 통한 대응

사이버보안을 위한 미국의 정책은 '포괄적'이라고 표현할 수 있다. 앞서 살펴본 것과 같이 미국의 사이버보안정책은 기술발달에 따라 미국의 핵심기반시설이 사이버상 시스템에 의존하고 있다는 점과 그에 따라 국가기반시설이 공격의 대상이 되고 있음을 명확히 인지하고 있다. 또한 미국의 사이버보안정책은 민간부문과의 긴밀한 협력뿐만 아니라 다양한 정부 기관들 간의 정보공유 또한 그 해결책으로 제시한다. 미국 유관 정부기관 간 정보공유 기제는 DHS의 사이버 커뮤니티 C^3 원 프로그램(Critical Infrastructure Cyber Community Voluntary Program, the C^3 Voluntary Program)과 FBI의 사이버 방호 연합(Cyber Shield Alliance, CSA)을 들 수 있다.

가. C^3 자원 프로그램

E.O. 13636을 통해 설립된 사이버 커뮤니티 C^3 원 프로그램(the C^3 Voluntary Program)은 "핵심기반시설 사이버보안 향상을 지원하고 "표준기술연구소(NIST)의

95) DHS, 사이버보안 서비스의 강화(Enhanced Cybersecurity Services), http://www.dhs.gov/sites/default/files/publications/ECS%20Fact%20Sheet%2007.30.15.pdf, 2015.11.15.방문.

사이버보안 기본 틀(Cybersecurity Framework)의 도입을 장려하기 위함이다".[96] 사이버보안 기본 틀의 수립은 동 행정명령의 주요 부분 중 하나였으며, 동 기본 틀의 최종안의 공표에 맞추어 사이버 커뮤니티 C^3 원 프로그램이 2014년 2월에 출범했다. 동 기본 틀은 사이버보안 위험을 관리를 돕기 위해 고안된 일련의 산업기준 및 우수사례이며, 정부와 민간부문의 협의를 통해 탄성되었다. 세계적으로 인정받는 최신 사이버보안 기준을 차용함으로써, 조직의 규모, 사이버보안 위험 정도, 사이버보안 기술과는 무관하게 다양한 기관들이 동 기본 틀이 제공하는 원칙과 우수사례를 적용할 수 있도록 하였다. 동 기본 틀의 개략적 설명은 다음과 같다.[97]

> "본 기본 틀은 기업관계자들이 사이버보안 활동의 지침으로 활용할 수 있도록 그리고 해당 기관의 위험관리의 일부로 사이버보안 위험을 고려할 수 있도록 하는 것에 중점을 둔다. 사이버보안 기본 틀은 핵심(the Framework Core), 프로파일(the Framework Profile), 실행 단계(the Framework Implementation Tiers)로 구성된다. 프레임워크 핵심은 국가기반시설 유관 부문들 전반에 공통적인 일련의 사이버보안 활동, 결과, 참조정보이며, 각 기관별 프로파일을 만드는 세부 지침을 제공한다. 이러한 프로파일을 통해서 본 기본 틀은 해당 기관이 그 사이버보안 활동과 그 기관의 기업 요건, 위험감수도, 자원을 일치시킬 수 있도록 지원한다. 프레임워크 실행 단계는 사이버보안 위험을 관리하는 기관들의 접근방식 특성을 확인하고 이해할 수 있는 기제를 제공한다."[98]

---

96) DHS, 사이버 커뮤니티 C^3 원 프로그램(Critical Infrastructure Cyber Community Voluntary Program), https://www.us-cert.gov/ccubedvp, 2015.11.15.방문.

97) NIST, 국가기반시설의 사이버보안 개선을 위한 프레임워크(Framework for Improving Critical Infrastructure Cybersecurity), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf2015.11.15.방문.

98) NIST, 국가기반시설의 사이버보안 개선을 위한 프레임워크(Framework for Improving Critical Infrastructure Cybersecurity), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf2015.11.15.방문. 박스 내 내용의 원문은 다음과 같다. "The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management. The Framework consists of three parts: the Framework Core, the Framework Profile, the Framework Implementation Tiers. the Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk."

동 사이버보안 틀의 확대를 위하여 사이버 커뮤니티 C^3 원 프로그램은 사이버 커뮤니티 C^3 원 프로그램 확장 및 메시지 킷(the C^3 Voluntary Program Outreach and Messaging Kit)을 개발하여 해당 프로그램 이해당사자들을 교육하게 된다. 그리고 동 프로그램을 통해 사이버보안 프레임워크를 도입하고자 하는 부문이나 기관들이 DHS, 타 미국정부기관, 민간부문이 제공하는 사이버 위험 관리 역량에 맞게 연결될 수 있도록 돕는다.

나. 사이버 방호연합

FBI의 사이버 방호 연합(Cyber Shield Alliance, CSA)은 "법 집행 네트워크 및 핵심 기술에 대해 선제적으로 사이버위협을 방어하고 대응하기 위한 FBI 사이버 보안 파트너십 기획으로서 법 당국을 위해 법 당국이 개발했다."[99] CSA는 다양한 법 집행 당국의 참여를 장려할 뿐만 아니라 해당 법 당국의 네트워크를 보호하고 최적화할 시킬 수 있도록 필요한 교육과 훈련도 제공한다. CSA는 주, 지역, 영토, 부족(State, local, territorial, and tribal, SLTT)기관들이 미국 시민들을 위험으로부터 지킬 수 있는 최전선이라는 점을 직시하고, SLTT기관들과 단일한 최전방 방호선 체계를 구축하고자 노력한다.

제3절 중국관련 사이버안보 정책

1. 중국 發 사이버공격의 특징

이른바 중국 발(發) 사이버공격의 특징은 정부 주도적이라는 점과 경제적 이익을 추구한다는데 있다. 중국 발 사이버공격은 다년간 이어져 오고 있으며, 그 표적 분야의 범위 확대뿐만 아니라 영향력도 커져가고 있다. 이에 대하여 미국·중국 경제안보검토위원회(the U.S.-China Economic and Security Review Commission, UCESRC)는 2014년도 의회 보고서에서 다음과 같이 밝히고 있다.[100]

---

99) 법집행사이버센터(Law Enforcement Cyber Center), FBI의 사이버 방호 연합(FBI Cyber Shield Alliance), http://www.iacpcybercenter.org/resource-center/fbi-cyber-shield-alliance/, 2015.11.15.방문.

100) 미국·중국 경제안보검토위원회(UCESRC), 2014년도 의회 보고서, 2쪽, 34쪽, http://origin.www.uscc.gov/sites/default/files/annual_reports/Complete%20Report.PDF 2015.11.15.방문.

"2014년 미국과 중국 사이의 무역 갈등은 세계무역기구(World Trade Organization, WTO)에 핵심 사건들이 상정되거나 결론이 남에 따라 고조되었다. 중국인민해방군 소속의 다섯 명의 군인들이 상업적 재물 국가지원을 받아 인터넷을 통해 절도한 혐의로 미국법무부(DOJ)에 의해 기소되었다. WTO의 분쟁해결패널(Dispute Resolution Panel)은 미국의 주장을 받아들여, 중국이 미국을 상대로 희토(稀土, rare earths), 반덤핑(antidumping), 상계관세(countervailing duties)에 관한 불법적인 수출제한을 가하는 것으로 인정했다. 그러나 중국을 상대로 한 수많은 무역 분쟁이 여전히 해결되지 못하거나 아예 다뤄지지도 못하고 있다. 이는 중국이 보조금에 관하여 WTO에 보고하지 않는 것, 미국의 기술을 중국에 이전하도록 강제하는 현지화요건(localization requirements), 다양한 산업영역에 대한 시장접근 저해 등 이 포함된다. [중략]

중국의 경제 스파이 행위를 밝혀내기 위한 미국의 결연한 노력에도 불구하고, 2014년에도 중국의 경제 스파이 행위는 감소하지지 않았다. 2014년 5월에는 미국 연방법무부는 다섯 명의 중국해방인민군을 5 개의 미국 회사 및 1개 국제노동조합을 상대로 사이버절도(cyber-theft)를 저지른 혐의로 기소하였다. 중국은 미국의 이와 같은 주장에 맞서 사이버보안에 관한 미국과의 양자회담을 중단하고 미국의 컴퓨터 소프트웨어 및 하드웨어 회사들에게 보복조치를 취했다. 중국이 이러한 활동을 지속해 나갈 경제적 유인은 매우 크기 때문에 미국의 소극적 대응으로는 그 활동양상을 바꾸기 어려울 것으로 판단된다."[101]

101) 미국·중국 경제안보검토위원회(UCESRC), 2014년도 의회 보고서, 2쪽, 34쪽, http://origin.www.uscc.gov/sites/default/files/annual_reports/Complete%20Report.PDF 2015.11.15.방문. 동 부분에 대한 원문은 다음과 같다. "Trade tensions between the United States and China escalated in 2014 as key World Trade Organization (WTO) cases advanced or were concluded and the U.S. Department of Justice filed indictments against five Chinese People's Liberation Army (PLA) soldiers for engaging in state-sponsored, cyber-enabled theft of commercial property. The WTO Dispute Resolution Panel ruled in favor of U.S. automobile imports. However, several trade disputes with China remain to report subsidies to the WTO, localization requirements that force the transfer of U.S. technology to Chinese firms, and restricted market access in several industries. [...]China's cyber espionage continued unabated in 2014, despite a concerted U.S. effort since 2013 to expose and stigmatize Chinese economic espionage. In May, the U.S. Justice Department charged five Chinese military officers with cyber-theft from five U.S.-based corporations and a major international labor union. China responded to the allegaions by suspending its participation in a bilateral dialogue on cyber security and by retaliating against U.S. based computer software and hardware firms. China's material incentives for continuing this activity are immense and unlikely to be altered by small-scale U.S. actions."

중국의 이러한 사이버공간을 활용한 적극적 움직임은 정보화 시대 이전에는 접근할 수 없었던 다양한 통로를 인터넷이 제공하고 있기 때문이며, 중국의 사이버 활동은 국가안보뿐만 아니라 국가 경제 개발을 위해서도 활발하게 활용되고 있다. 미국은 중국의 이러한 적극적 움직임에 대하여 법 당국의 대응전략 개선 및 더욱 강경한 벌금 및 형벌규정으로 맞서고 있다. 미국 연방수사국(Federal Bureau of Investigation, FBI)에 따르면, 미정부는 지적재산권절도)에 대응하는 더욱 큰 규모의 작전의 일부로 경제 스파이 활동에 대항하는 포괄적인 전략을 추구한다.[102]

DOJ는 2010년 2월에 지적재산권 전담반을 꾸렸고, 동 전담반은 대통령비서실(Executive Office of the President) 소속 지식재산집행조정관실(Office of the Intellectual Property Enforcement Coordinator, IPEC)[103]과 함께 일한다. IPEC는 2011년 3월 경제 스파이의 법정 최고형량을 20년 이상으로 상향 조정해야 한다는 권고내용을 제시했고, 이와 함께 피고의 범죄행위에 기초한 양형 강화방법을 통해 처벌을 확대할 수 있도록 미국 양형위원회(U.S. Sentencing Commission)에 지시할 것을 의회에 권고한 바 있다.[104]

또한 FBI는 중국의 사이버 위협에 맞서 전략 파트너십 조정관(strategic partnership coordinators, SPCs) 네트워크를 활용하고 있다. SPC는 미국 전역에 (2013년 기준으로) 15,000개가 넘는 연락망을 유지하고 있으며, 이 연락망은 지역 기업, 교육기관, 방위업체 등으로 구성되어 있다. FBI는 SPC를 활용하여 다른 정부기관이나 민간기업과 협력하여 기업 내부 위협 및 사이버 침임에 적절히 대응하기 위해 함께 노력한다.

---

102) Christopher Munsey, 미국 연방수사국(FBI), 경제스파이: 산업기밀 절취를 통한 무역 분야에서의 경쟁(Economic Espionage: Competing For Trade By Stealing Industrial Secrets), https://leb.fbi.gov/2013/october-november/economic-espionage-competing-for-trade-by-stealing-industrial-secrets, 2015.11.15.방문.

103) 지식재산집행조정관실(IPEC)은 미국 경제에 중요한 지적재산의 보호를 위해 노력하며, 미연방정부의 업무를 조정하여 불법적이고 해악을 끼치는 지식재산권절도를 막는 것을 그 임무로 한다. https://www.whitehouse.gov/omb/intellectualproperty/ipec

104) 지식재산집행조정관실(IPEC), 2011 지식재산집행에 관한 미국 지식재산집행조정관 연례보고서(2011 U.S. Intellectual Property Enforcement Coordinator Annual Report on Intellectual Property Enforcement), 10쪽, https://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_2011_report.pdf, 2015.11.15.방문.

미연방의회는 이같이 증가하는 위협에 대하여 2012년 입법[105]을 통하여 경제 스파이 행동에 책임 있는 자에게 기존의 최대 500,000 USD에서 500만 USD으로 벌금형 상한을 가중했다. 나아가 경제 스파이 행위를 저지른 조직도 기존의 최고 100만 USD의 벌금에서 이제는 절취한 영업비밀 가치의 세 배까지로 그 상한을 올렸다. 그리고 의회는 미양형위원회가 경제 스파이 및 영업비밀 절도에 대한 양형기준을 검토하도록 지시하였고, 이에 따라 2013년 초 동 위원회는 이러한 범죄에 관한 양향기준을 2단계 상승시킬 것을 승인했다.[106]

2. United States of America v. Wang Dong, Sun Kailing, Wen Xinyu, Huang Zhenyu, Gu Chunhui 사건 (2014년)

2014년 United States of America v. Wang Dong, Sun Kailing, Wen Xinyu, Huang Zhenyu, Gu Chunhui 사건은 해킹(hacking)과 관련하여 알려진 정부 행위자를 상대로는 처음 이루어진 형사고발이라는 점에 의의가 있다. Wang Dong 외 4인은 중국인민해방군 군인으로 2006년부터 2014년 사이의 기간 동안 Westinghouse Electrc Co., SolarWorld AG, △United Stated Steel Corp., Allegheny Technologies Inc., the United Steal, Paper, and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union, Alcoa, Inc.의 원자력, 금속 및 태양광 제품 회사와 노동조합을 상대로 한 컴퓨터 해킹, 경제 스파이 등의 혐의로 기소되었다.

본 사건에 대한 DOJ의 2014년 5월 19일자 성명서는 다음과 같다.[107]

---

105) 지식재산집행조정관실(IPEC), 2011 지식재산집행에 관한 미국 지식재산집행조정관 연례보고서(2011 U.S. Intellectual Property Enforcement Coordinator Annual Report on Intellectual Property Enforcement), 10쪽, https://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_2011_report.pdf, 2015.11.15.방문.

106) 지식재산집행조정관실(IPEC), 2011 지식재산집행에 관한 미국 지식재산집행조정관 연례보고서(2011 U.S. Intellectual Property Enforcement Coordinator Annual Report on Intellectual Property Enforcement), 10쪽, https://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_2011_report.pdf, 2015.11.15.방문.

107) DOJ, 상업적 이득을 위해 미국 기업 및 노동조합을 상대로 사이버 스파이 행위를 한 5인의 중국군 해커 기소(U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage), http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor, 2015.11.15.방문.

문건 기소는 피고들이 미국국적의 기관들에 대한 해킹을 공모한 혐의를 든다. 이는 피해자들의 컴퓨터에 불법적 접근을 유지하고 정보를 절취하여 피해 기업들의 중국 경쟁사를 이롭게 하기 위함이며 그 중국 경쟁사에는 중국의 국유기업(SOE)들도 포함된다.[중략]

미연방 검찰총장 Eric Holder는 다음과 같이 말했다. "이번 사건에서 절취된 영업비밀 및 타 민간 기업 정보의 범주는 광범하며 매우 적극적인 대응을 요구한다. 세계 시장에서의 성공은 한 기업의 혁신과 경쟁 역량에만 기반을 둬야하며 영업비밀을 탐지, 절취하는 행위를 후원하는 정부의 역량에 따르는 것이 아니다. 현 정부는 미국 기업들을 대상으로 한 불법적 방해 공작과 자유로운 시장의 운영에 관한 공정 경쟁의 완결성을 저해하려는 어떤 국가의 활동도 용인하지 않을 것이다."

FBI 국장 James B. Comey는 다음과 같이 말했다. "중국정부는 너무 오랫동안 노골적으로 사이버 스파이 행위를 통하여 중국 국유 기업의 경제적 이익을 추구해 왔다. 문건 기소는 중요하지만, 여전히 많은 피해자와 과제들이 산적해있다. 미국의 개별 형사사법 및 국가 안보 당국들과 함께 FBI는 사용 가능한 모든 법적 수단을 활용하여 사이버 스파이에 대처할 것이다."[108]

108) DOJ, 상업적 이득을 위해 미국 기업 및 노동조합을 상대로 사이버 스파이 행위를 한 5인의 중국군 해커 기소(U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage), http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor, 2015.11.15.방문. 동 부분에 대한 원문은 다음과 같다. The indictment alleges that the defendants conspired to hack into American entities, to maintain unauthorized access to their computers and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises (SOEs). [...] U.S. Attorney General Eric Holder said[,] "[t]he range of trade secrets and other sensitive business information stolen in this case is significant and demands an aggressive response. Success in the global market place should be based solely on a company's ability to innovate and compete, not on a sponsor government's ability to spy and steal business secrets. This administration will not tolerate actions by any nations that seeks to illegally sabotage American companies and undermine the integrity of fair competition in the operation of the free market." "For too long, the Chinese government has blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries," said FBI Director James B. Comey. "The indictment announced today is an important step. But there are many more victims, and there is much more to be done. With our unique criminal and national security authorities, we will continue to use all legal tools at our disposal to counter cyber espionage from all sources."

이처럼 미국 정부는 사이버 스파이 행위를 통한 사이버 보안망의 침해가 국가안보와 경제안보에 미치는 악영향을 명확히 인식하고 있으며, 이에 적극적으로 대처하기 위하여 사이버 보안과 관계된 다양한 당사자들을 포섭하여 전략적이고 강경한 대책을 수립하고 법적 수단을 이용하여 대처하고 있다.

3. 중국의 사이버안보 정책: 네트워크안전법(안)

가. 네트워크안전법(안)

1) 입법 정보 및 배경

중국의 전국인민대표대회(이하 전인대)[109]는 지난 7월 6일 네트워크 및 사이버공간 관련 사항에 관한 종합적인 법률인 중화인민공화국 네트워크안전법(中华人民共和国网络安全法 혹은 사이버보안법, Cyber Security Law)의 초안[110]을 내놓았다.

이는 네트워크와 정보기술 등에 대한 통제를 포함하는 국가안전법을 2015년 7월 1일부터 시행한 데 이어 별도로 발표된 네트워크 관련 보안법인 샘이다.[111]

중국의 네트워크 및 정보 관련 법안의 강화가 본격적으로 시작된 시기는 2013년 미국 국가안보국(NSA) 소속 에드워드 스노든(Edward Joseph Snowden)의 폭로 이후다.[112]

이후 반터러리즘법 초안(中华人民共和国反恐怖主义法(草案)[113]이 발표되었고, 국가안전법(中华人民共和国国家安全法)[114]이 통과되었다.

2) 네트워크안전법(안) 주요 내용

네트워크안전법(안)은 사이버범죄나 사이버테러 외에 개인정보보호, 지적재산권 보호 등 컴퓨터 및 인터넷과 관련된 다양한 기술적인 문제점을 보완하고, 관련 법제를

---

109) 중국의 국회격이라 볼 수 있으며 형식상 중국 최고 권련기관이다. http://terms.naver.com/entry.nhn?docId=1687331&cid=43792&categoryId=43793

110) 网络安全法(草案)」, 〈http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm〉

111) 보안뉴스, http://www.boannews.com/media/view.asp?idx=47184&kind=3

112) 김유향, 중국 「네트워크안전법(안)의 주요 내용과 함의」, 이슈와 논점 제1083호, 국회입법조사처, 1쪽.

113) 「中华人民共和国反恐怖主义法(草案)」 〈http://www.npc.gov.cn/npc/lfzt/rlys/2014-11/03/content_1885073.htm〉

114) 「中华人民共和国国家安全法」, 〈http://www.npc.gov.cn/npc/xinwen/2015-07/07/content_1941161.htm〉

포함한다. 초안은 총칙, 네트워크 보안 전략·기획·촉진, 네트워크 운행보안, 네트워크 정보보안, 모니터링 경보와 응급처치, 법률 책임, 부칙 총 7장 68개 조항으로 구성되어 있다.[115] 또한 내용은 크게 네트워크 보안과 안전, 개인정보보호, 불법정보규제 부문으로 나뉘어진다.[116]

그 중에서도 사이버범죄 혹은 사이버테러와 가장 관련이 높은 부문은 네트워크 보안과 안전에 해당하는 조항이다. 「중국 네트워크안전법(안)의 주요 내용과 함의」에서는 관련 내용을 이렇게 정리한다.

> 네트워크 보안 및 안전과 관련해서는 네트워크를 이용한 안보위협 및 각종 금지된 활동에 대해 적시하며(제9조), 네트워크 보안에 해를 가하는 행위에 대한 신고의무를 부과하고 있다(제10조). 국가는 네트워크 보안전략을 제정하고 안전하게 관리·유지할 의무가 있으며(제11조), 통신, 방송, 에너지, 교통, 수리(水利)), 금융 등의 주무부처와 기타 유관부처는 국가의 네트워크 보안전략에 따라 네트워크 보안 계획을 작성하고 시행해야 한다(제12조). 국가는 네트워크 안전등급 보호제도를 시행하며 네트워크 사업자는 안전등급 보호제도의 기준에 따라 내부 보안 관리제도와 운영규정을 제정하고, 보안책임자를 지정하며, 네트워크 침해를 방지할 기술조치를 취하는 등의 의무를 이행해야한다(제17조).
>
> 네트워크 핵심장비 및 보안 전용제품에 대한 안전 인증 및 검사제도 시행에 대해서도 규정하고 있는데(제19조), 국가 업계 표준의 요구사항이 포함된 안전 인증이나 안전 검사에 합격한 제품 목록은 국무원이 제정하고 발표한다. 또한 네트워크의 안전을 위해 그 이용에 있어서 실명인증을 의무화하고 있다(제20조). 네트워크 사업자는 통신망 가입 수속이나 정보공개 서비스의 제공을 위해 이용자의 실제 신분정보 제공을 요구해야 한다.
>
> 또한 국가는 공공통신, 방송 등 기초정보 네트워크, 에너지, 교통, 수리 금융 등 중요산업, 전력, 수도, 의료보건 등 공공서비스분야의 주요 정보시스템, 군사 네트워크, 지급(地級)이상 국가의 정무 네트워크, 이용자가 많은 네트워크 서비스 공급자가 소유·관리하는 네트워크를 핵심 정보인프라로 지정하고 중점 보호하여야 한다(제25조). 이들 핵심 정보인프라의 보안방법은 국무원에서 정하며, 이들 시설들은 안전 보호 의무 이행, 네트워크 제품 및 서비스 구매 시 보안 심사, 매년 안전 평가 및 보고 등의 규제를 받아야 한다.[117]

---

115) 보안뉴스, http://www.boannews.com/media/view.asp?idx=47184&kind=3
116) 김유향, 중국 「네트워크안전법(안)의 주요 내용과 함의」, 이슈와 논점 제1083호, 국회입법조사처, 2쪽.

이처럼 중국의 새로운 네트워크보안법은 정부와 민간에 발생할 수 있는 네트워크 공격 위협에 대하여 보안 책임자를 설정하는 방식으로 사이버테러를 방지 및 대응하고자 한다.

네트워크로 서로 연결되어 있는 사이버공간의 특성상 개인정보보호 및 불법정보규제 부문에 관한 조항에서도 사이버테러와 관련된 기본적인 입장을 찾아볼 수 있다. 즉 중국 정부는 개인정보보호 등을 통해 데이터를 통제할 의도를 밝히고 있다.[118]

> 개인정보보호와 관련하여 네트워크 사업자는 개인정보 보호제도를 마련해야하며 개인정보를 수집하고 이용할 때는 법을 준수하고 목적·방식·범위 등을 명시하며 사용자 동의를 받도록 규정하고 있다(제34~39조). 이때 네트워크 사업자는 제공하는 서비스와 무관한 개인정보를 수집하거나 법에 어긋나는 개인정보를 수집 또는 사용할 수 없으며(제35조), 이용자는 약정에 어긋난 본인 정보에 대한 삭제 및 본인정보의 오류에 대해 정정을 요구할 권리가 있다(제37조). 네트워크 사업자는 물론 누구든지 개인정보를 불법으로 취득하거나 판매할 수 없다(제38조).
>
> 여기서 주목할 것은 핵심정보인프라 사업자가 개인정보를 저장 할 경우 반드시 중국내에 보관(제31조)하도록 의무화하고 있다는 점이다. 핵심 정보인프라사업자는 관련 제품 및 서비스 구매 시 국가의 보안심사에 통과해야하며, 수집된 개인정보 등 중요한 데이터는 저장해야하며, 해외에 저장할 경우나 해외 기관 또는 개인에게 제공할 경우 정부의 보안평가에 따라야한다.
>
> 불법정보와 관련한 내용으로는, 네트워크 사업자에게 불법 정보의 차단 및 보고(제40조)를 의무화하는 한편, 전자정보 발송자가 발송하는 전자정보와 SW 제공자가 제공하는 SW는 악의적인 프로그램을 포함하거나 불법 정보를 발표하거나 전달해서는 아니되며(제41조), 국가는 법에 의해 금지된 정보에 대해 네트워크 사업자에게 전송중단 및 제거 등을 요구할 수 있다(제43조). 이를 어기면 최고 50만 위안의 벌금이 부과되며 사업 면허가 해지될 수도 있다. 법안에 따르면 네트워크 사업자는 불법정보를 발견하면, 전송 중단, 제거, 확산 방지, 기록 보관 등의 조치를 수행하고 유관기관에 보고하여야 한다.
>
> 나아가 국가안보 및 사회공공질서 수호를 위해 국무원 또는 성, 자치구, 직할시 인민 정부는 국무원의 승인을 받는다면 일부 지역에서 네트워크 통신에 대한 임시 조치를 취할 수 있도록 하였다(제50조).

117) 김유향, 중국 「네트워크안전법(안)의 주요 내용과 함의」, 이슈와 논점 제1083호, 국회입법조사처, 2쪽.

118) 김유향, 중국 「네트워크안전법(안)의 주요 내용과 함의」, 이슈와 논점 제1083호, 국회입법조사처, 4쪽.

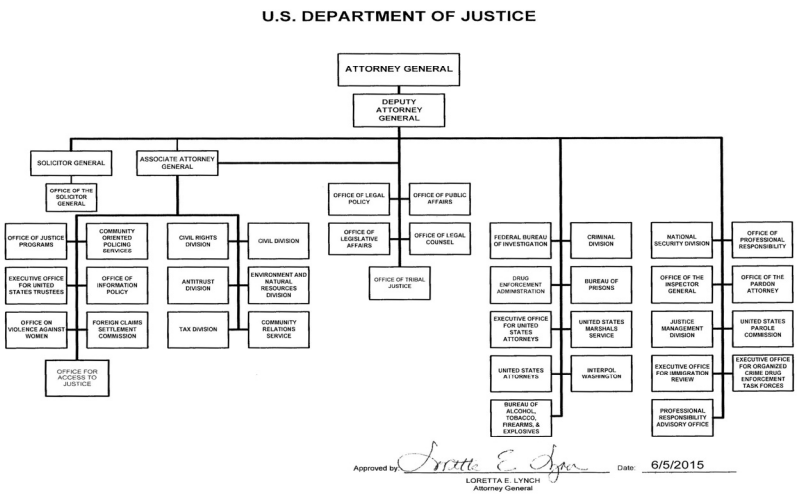
마지막으로 이 법안에서는 중국내 네트워크 운영 및 관리에 대한 중국정부의 통제와 개입을 명문화하고 있다. 즉 중국정부가 중국내의 온라인 데이터에 억세스하고 정보를 입수할 권한, 국내법에 위반되는 사적 정보의 확산을 저지할 권한을 강화하는 것을 목적으로 하고 있다(제43조~50조). 특히 법안에서 주목할 것은 제43조로서 여기에서는 중국 외부로 부터의 정보에 대해 차단과 전송저지를 할 수 있는 권한을 기재하고 있는데, 이는 지금까지 중국정부가 암묵적으로 실시해왔던 것을 처음으로 법률차원에서 명확히 제시한 것이다.

제4절 미국 법무부의 사이버안보 정책

1. 연방 법무부(Department of Justice) 개관

미연방 법무장관(Attorney General)직은 1789년 법원조직법(the Judiciary Act of 1789)에 의해 창설됐다. 이어서 연방 법무부가 1870년 법무부 설치에 관한 법률(the Act to Establish the Department of Justice)을 통해 설립됐다.

미연방 법무부는 법 집행, 주(state) 및 지역(local) 지원, 국가법무 및 자문, 출입국 관리 부서, 형행 부서, 관리 및 감독 등의 업무를 분장하는 총 39개의 조직으로 구성되어 있다. 그 조직체계는 다음과 같다.



[그림 3-1] 美 연방법무부의 조직도(DOJ Organizational Chart)[119]

연방법무부의 39개의 조직기구의 구성을 좀 더 살펴보면 다음과 같다.

〈표 3-3〉 美 연방법무부의 조직기구(The Department of Justice Components)[120]

고위직	
법무장관실 (Office of The Attorney General, AG)	법무부장관실 (Office of The Associate Attorney General, ASG)
법무차관실 (Office of The Deputy Attorney General, DAG)	송무차관실 (Office of the Solicitor General, OSG)
직속청	
사법 서비스청 (Office for Access to Justice, ATJ)	대외협력청 (Office of Public Affairs, PAO)
법률정책청 (Office of Legal Policy, OLP)	소수민족 사법청 (Office of Tribal Justice, OTJ)
입법업무청 (Office of Legislative Affairs, OLA)	
법 집행기관	
연방수사국 (Federal Bureau of Investigation, FBI)	인터폴 워싱턴 (INTERPOL Washington – United States National Central Bureau)
연방마약수사국 (Drug Enforcement Administration, DEA)	형사국 (Criminal Division, CRM)
연방검찰사무국 (Executive Office for United States Attorneys, EOUSA)	마약범죄조직특별단속팀 사무국 (Executive Office for Organized Crime Drug Enforcement Task Forces, OCDETF)
연방보안관 (United States Marshals Service, USMS)	연방주류·담배·화기단속국 (Bureau of Alcohol, Tobacco, Firearms and Explosives, ATF)
주(state) 및 지역(local) 지원부서	
사법제도실 (Office of Justice Programs, OJP)	지역 사회 지원 서비스 (Community Relations Service, CRS)
지역사회 담당경찰청 (Office of Community Oriental Policing Services, COPS)	여성폭력방지청 (Office on Violence Against Women, OVW)
법률 대변 및 자문부서	
법률자문국 (Office of Legal Counsel, OLC)	송무국 (Civil Division, CIV)
조세국 (Tax Division, TAX)	인권국 (Civil Rights Division, CRT)

119) 미연방법무부, 조직구성 http://www.justice.gov/sites/default/files/doj/pages/attachments/2015/04/27/doj_june_2015_2.pdf

120) 미연방법무부, 조직구성, 임무, 그리고 역할 매뉴얼(Organization, Mission & Functions Manual), http://www.justice.gov/jmd/organization-mission-and-functions-manual

법률 대변 및 자문부서	
환경·자원국 (Environment and Natural Resources Division, ENRD)	국가안보국 (National Security Division, NSD)
반독점국 (Antitrust Division, ATR)	연방관재국 (Executive Office for United States Trustees, EOUST)
출입국 부서	
출입국심사사무소 (Executive Office for Immigration Review, EOIR)	
행형 부서	
연방교정국 (Federal Bureau of Prisons, BOP)	사면국 (Office of the Pardon Attorney, OPA)
미국가석방위원회 (United States Parole Commission, USPC)	
관리 및 감독 부서	
사법관리과 (Justice Management Division, JMD)	직무감찰 담당관실 (Office of Professional Responsibility, OPR)
감찰국 (Office of the Inspector General, OIG)	감찰자문실 (Professional Responsibility Advisory Office, RPAO)
기타	
대외청구권해결위원회 (Foreign Claims Settlement Commission, FCSC)	정보담당관실 (Office of Information Policy, OIP)

법무장관실(Office of the Attorney General)의 임무는 연방법무부의 행정 및 운영을 감독하고 지시하는 것이다. 여기에는 연방수사국(Federal Bureau of Investigation), 연방마약수사국(Drug Enforcement Administration), 연방주류·담배·화기 단속국(Bureau of Alcohol, Tabacco, Firearms and Explosives), 연방교정국(Bureau of Prisons), 사법제도실(Office of Justice Programs), 연방검사 및 연방보안관 서비스(U.S. Attorneys and U.S. Marshals Service)와 같은 연방법무부 조직기구들이 포함된다.[121]

121) 미연방법무부, 조직구성, 임무, 그리고 역할 매뉴얼: 법무장관, 법무차관, 법무 부장관 (Organization, Mission & Functions Manual: Attorney General, Deputy, and Associate), http://www.justice.gov/jmd/organization-mission-and-functions-manual-attorney-general#asg

법무차관실(Office of the Deputy Attorney General)은 1950년에 창설되었다. 법무차관은 연방법무부에서 두 번째로 높은 직위이며, 법무장관에게 조언을 제공하고 그 업무를 지원한다. 그 범위는 연방법무부 정책 및 프로그램의 수립 및 이행 그리고 모든 연방법무부 내 조직기구들에 대한 전반적인 감독과 지시에 관한다.[122]

법무 부장관실(Office of the Associate Attorney General)은 1977년 법무장관 명령으로 창설되었으며, 법무 부장관은 연방법무부에서 세 번째로 높은 직위이다. 법무 부장관은 법무장관의 고위급관리침의 일원으로서 법무장관과 법무차관을 보좌한다.[123]

2. 법무부의 사이버안보관련 정책

2014년 12월, 미국 법무부는 사이버안보와 관련하여 사이버보안과(Cybersecurity Unit)를 신설함으로써 사이버범죄 조사 및 예방 활동을 강화했다.[124] 사이버보안과는 기존의 컴퓨터범죄 및 지적재산부(Computer Crime and Intellectual Property Section, CCIPS) 산하에 편성됐다. 사이버보안과는 법적 집행력과 대응력을 보강하기 위하여, "전자감시규정에 관한 법적 가이드라인과 전문적인 자문을 제공하는 중앙 허브로서의 역할을 수행"[125]하고 "미국 국내 및 해외 법률 조직에서 사이버범죄 가해자들을 감시 및 처벌하기 위한 효과적인 법적 집행도구에 대한 정보를 제공할 방침"[126]이다.

---

122) 미연방법무부, 조직구성, 임무, 그리고 역할 매뉴얼: 법무장관, 법무차관, 법무 부장관 (Organization, Mission & Functions Manual: Attorney General, Deputy, and Associate), http://www.justice.gov/jmd/organization-mission-and-functions-manual-attorney-general#asg

123) 미연방법무부, 조직구성, 임무, 그리고 역할 매뉴얼: 법무장관, 법무차관, 법무 부장관 (Organization, Mission & Functions Manual: Attorney General, Deputy, and Associate), http://www.justice.gov/jmd/organization-mission-and-functions-manual-attorney-general#asg

124) 한국인터넷진흥원, Bimonthly-5호, 미국 법무부(DoJ), 사이버범죄 소탕 및 보안 강화를 위한 조사팀 신설, http://www.kisa.or.kr/uploadfile/201412/201412301110107707.pdf, 2011.11.15.방문.

125) 한국인터넷진흥원, Bimonthly-5호, 미국 법무부(DoJ), 사이버범죄 소탕 및 보안 강화를 위한 조사팀 신설, http://www.kisa.or.kr/uploadfile/201412/201412301110107707.pdf, 2011.11.15.방문.

126) 한국인터넷진흥원, Bimonthly-5호, 미국 법무부(DoJ), 사이버범죄 소탕 및 보안 강화를 위한 조사팀 신설, http://www.kisa.or.kr/uploadfile/201412/201412301110107707.pdf, 2011.11.15.방문.

가. 피해자대응 및 사이버사고 신고에 관한 우수사례 버전 1.0

사이버보안과는 법률 자문 지원뿐만 아니라 사이버범죄의 효과적 대응을 위한 민관협력 및 정보공유 체계의 확립을 위해 노력한다. 민관협력과 정보공유의 노력은 민간기업의 합법적인 사이버보안 관행을 장려하고 사이버범죄 피해 구제에 도움을 주기 위해서이다. 이에 대한 최근의 성과로는 2015년 4월에 출판한 피해자대응 및 사이버사고 신고에 관한 우수사례 제1판 (Best Practices for Victim Response and Reporting of Cyber Incidents Version 1.0)이 있다.

동 보고서는 사이버 사고 발생 시 신속하고, 효율적인 대응이 사고로 인한 피해와 그 피해복구에 걸리는 시간을 단축하는데 핵심적 요소라는 점을 인정한다. 그 목표는 다양한 기관들이 사이버 사고 시의 대응 계획 수립하도록 돕고 대비시키는 것이다. 그리고 이러한 내용을 요약한 사이버사고 준비 체크리스트를 사이버 공격이나 침입 이전, 공격 및 침입 중, 그 이후로 나누어 보기 쉽게 제공하기도 한다.

나. 국제전략문제연구소(CSIS)/법무부 사이버 방호 전문가 라운드테이블 (2015년 3월 10일)[127]

2015년 3월, 국제전략문제연구소(CSIS)와 법무부(DOJ)는 '적극적 사이버 방호'와 관련 사이버보안 민간 실무가들이 참여하는 라운드테이블을 개최했다. 동 회의는 "사이버보안 유닛의 계속되어온 노력의 일환인 사이버 위험이 고조된 환경에서 네트워크를 보호하기 위해 민간 부문이 사용하는(그리고 사용하지 않는) 기술에 관한 정보를 수집"[128]도 그 목적으로 한다.

사이버보안과의 주최로 열린 동 라운드테이블에서 논의된 사안은 대략적으로 다음과 같다. 사이버 방호의 범주, 사이버 방호 활동을 통한 사이버 정보 수집, 법적 명확성의 부재, 세계 환경에서 방어적인 사이버 활동 수행, 역(逆)해킹(hacking back), 효과적인 사이버 방호 활동이 그것이다.

---

127) 법무부, 국제전략문제연구소(CSIS)/법무부 사이버 방호 전문가 라운드테이블(CSLS/DOJ Active Cyber Defense Experts Roundtable), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/05/18/CSIS%20Roundtable%205-18-15.pdf, 2011.11.15.방문.

128) 법무부, 국제전략문제연구소(CSIS)/법무부 사이버 방호 전문가 라운드테이블(CSLS/DOJ Active Cyber Defense Experts Roundtable), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/05/18/CSIS%20Roundtable%205-18-15.pdf, 2011.11.15.방문. 1쪽.

제5절 미국 국립사법연구원의 사이버보안 관련연구

1. 미국 국립사법연구원(National Institute of Justice) 개관

미국 국립사법연구원 (National Institute of Justice, NIJ)는 미국 법무부 산하 연구소로서 과학적 접근으로 범죄 및 사법에 관련된 현안을 연구하여 범죄에 대한 인식을 높이고 범죄를 예방하는 방안을 제시하는 역할을 담당한다.

대통령이 원장을 임명하고 미국 연방법무부(Department of Justice) 사법정책청(Office of Justice Programs)의 주요과제를 설정하고 수행한다. 연구과제는 피해자와 사회 구성원들 그리고 범죄학 전문가들의 현실적 필요에 의해 결정되며 관련 정부기관, 공공 및 민간단체 그리고 국제사회와의 협력으로 연구를 진행한다.

가. 전략적 목표

국립사법연구원의 다섯 개의 전략적 목표는 다음과 같다.[129)]

1) **과학기반의 형사사법 실행 장려**(Fostering Science-based criminal justice practice) : 가정, 이웃과 사회의 안전을 위한 과학적 연구 지원

2) **지식의 실무로의 전환**(Translating knowledge to practice) : 형사사법 전문가들의 연구과제 참여를 통한 범죄방지와 감소방안 제시

3) **기술발전** (Advancing technology) : 기술발전을 통해 더욱 효과적이고 공평한 형사사법시스템 개발

4) **학제적 연구** (Working across disciplines) : 물리적, 과학 수사적, 사회 과학적 분야를 통한 정의구현

5) **국제적 관점 수용** (Adopting a global perspective) : 미국 국내의 사회적 맥락과 국제적 맥락 이해

---

129) http://www.nij.gov/about/Pages/welcome.aspx, 2015.11.15.방문.

NIJ의 중점목표는 연구와 정책을 실생활에 적용시켜 범죄에 대응하고 정의를 구현하는, 지식의 실무적 활용이다.[130] 즉, 연구자들이 발견한 필요사항을 연구과제에 반영하고 연구의 결과물을 평가해 정책에 반영함으로써 범죄방지에 기여하는 것이다.

나. 주요연구 분야

NIJ의 연구 분야는 테러리즘, 성폭력, 아동학대, DNA수사, 인터넷범죄, 사이버범죄 및 수사, 디지털 증거, 물리적 증거 등을 광범위하게 포함하며 최근 5년-10년간 새로운 중점연구 분야로 떠오른 분야는 컴퓨터 관련 기술을 포함한 범죄와 수사이다. 이 분야는 과학 및 기술실(The Office of Science and Technology)의 중점분야로서 연구과제 선택에는 기술자문그룹(Technology Working Groups, TWG)의 역할이 부각된다.[131]

TWG는 법집행 및 교정기술센터(National Law Enforcement and Corrections Technology Center)의 지원을 받아 수행과제와 기술평가 기준을 개발하고 부단히 발전하는 새로운 기술에 보조를 맞추기 위해 NIJ의 연구에 있어 최첨단 기술도입을 위해 노력한다. 또한 이를 바탕으로 ①연구과제 제안서를 동료연구자의 검토를 통해 평가하고 ②진행되고 있는 연구 및 프로젝트의 과정과 상태를 검토하며 ③프로그램 및 프로젝트의 성공여부를 평가하고 ④다른 기관들과 협력하여 새로 개발된 기술을 증명하고 시험한다.[132]

2. 미국 국립사법연구원의 연구과제

NIJ가 관장하고 있는 컴퓨터 및 인터넷을 포함한 범죄관련 연구 분야에는 신상정보 절도(Identity theft), 아동 및 청소년 대상 사이버 범죄, 도용된 데이터(Stolen data) 관련 범죄, 국제 조직범죄(International Organised Crime, IOC)와 사이버 범죄의 연관성, 전자범죄 관련 기술, 수사방법 및 법 집행 그리고 디지털 범죄 수사 및 증거 등이 있다.

---

130) http://www.nij.gov/about/Pages/welcome.aspx, 2015.11.15.방문.
131) 형사사법의 최우선 과제: 기술적 필요사항 (High Priority Criminal Justice: Technology Needs), 6쪽, https://www.ncjrs.gov/pdffiles1/nij/225375.pdf, 2015.11.15. 방문.
132) http://www.nij.gov/topics/technology/pages/working-groups.aspx, 2015.11.15.방문.

가. 신상정보 절도 (Identity theft)범죄 연구

NIJ는 신상정보 절도에 관하여 사회적 경제적 지위를 불문하고 모든 사람이 취약한 범죄라 규정하고 타인의 신상을 인터넷상에서 도용하거나 타인의 신상으로 등록된 은행관련 사기, 신용카드 및 체크카드, 휴대폰 심카드 도용 등 관련범죄를 연구했다.

1) **신상정보절도 연구 분석**("Identity Theft Research Review"[133]) 보고서에서는 이제까지 불분명했던 신상정보절도의 정의, 패턴과 범위, 종류, 범죄자들이 사용하는 신원정보 추출방법, 범죄의 단계, 신고, 그리고 신상정보절도 범죄 관련 법률제정 등을 검토하고 연구했다.

2) **신상정보절도 범죄자의 전략과 위험 인지**("Identity Theft: Assessing Offenders' Strategies and Perceptions of Risk"[134]) 보고서는 신상정보절도 범죄자들의 범행수단, 기법 및 범행 동기 등을 심도 있게 분석하고 온라인 경제활동에 미치는 영향을 분석하여 실현가능한 예방 방안과 대처방안을 제시했다.

나. 아동 및 청소년대상 사이버 범죄(Cyber-bullying and Internet crime against children)

NIJ는 미국 내 십대들의 인터넷과 스마트폰 그리고 소셜 네트워크의 사용량이 급속도로 많아지면서 그에 따르는 범죄 유형에 대한 연구의 필요성에 따라 관련 연구를 진행했다.

1) **인터넷 네트워크와 십대들의 데이트 폭력, 남용 그리고 따돌림의 관계**(Technology, Teen Dating Violence and Abuse and Bullying[135]) 보고서는 기술사용에 따라 십대들이 겪는 폭력유형과 십대들의 교우관계에 미치는 영향에 대한 연구내용을 제시하고 있다. 특히 소셜 네트워크 사이트(페이스북, 트위터, 마이스페이스 등),

133) 신상정보절도- 연구 리뷰(Identity theft- A Resesarch Review) 2007, https://www.ncjrs.gov/pdffiles1/nij/218778.pdf, 2015.11.15. 방문.
134) Identity Theft: Assessing Offenders' Strategies and Perceptions of Risk 2007, https://www.ncjrs.gov/pdffiles1/nij/grants/219122.pdf 2015.11.15.방문
135) 인터넷 네트워크와 십대들의 데이트 폭력, 남용 그리고 따돌림의 관계 (Technology, Teen Dating Violence and Abuse,and Bullying) 2013, https://www.ncjrs.gov/pdffiles1/nij/grants/243296.pdf, 2015.11.15.방문.

문자 메시지를 통해 이루어지는 따돌림과 폭력경험을 조사해 인터넷의 사용과 사이버상의 범죄, 그리고 십대들이 겪는 피해상황을 알리고 오프라인에서도 지속되는 피해상황을 조사했다. 그에 따른 대응방안으로 학교의 주도적 역할과 인터넷상 신고시스템 개발방안 등을 제시했다.

2) **아동상대 인터넷 범죄 관련 중앙 및 주 정부 법원 판례요약**(Internet Crimes Against Children: A Matrix and Summary of Major Federal and Select State Case Law)[136]을 통해 아동 포르노그래피, 성적 착취, 아동들의 의사와 관계없이 접하는 디지털 성인물 그리고 온라인 상 괴롭힘과 따돌림 등에 관한 판례와 법률 제정을 정리했고, 아동 대상 인터넷 범죄의 동향과 발전하는 기술에 대응하는 새로운 방안의 필요성을 제시하였다.

다. 국제 조직범죄(International Organised Crime, IOC)와 사이버 범죄의 연관성

NIJ의 전문가 전담반(Expert Working Group, EWG)에서는 John T. Picarelli 사회과학부 분석가 주도로 국제 조직범죄에 대한 보고서("Expert Working Group Report on International Organized Crime"[137])를 발간했다. 본 연구에서는 현재 국제조직범죄를 연구하는 전문가들이 정보를 공유하고 IOC와 사이버 범죄의 비례관계의 실태와 영향력을 평가했다. 본 보고서의 사이버 범죄 관련 주요내용은 다음과 같다.

IOC의 사이버 범죄행위는 지적 재산권 절도, 사이버 무기로서 악성 소프트웨어 개발, 해킹 그리고 온라인을 이용한 자금세탁 등을 포함하고, 그로 인한 손해액은 측정 할 수 없을 정도이다. 특히, 범죄자들은 지적 재산권 절도로 마개한 경제적 이득을 취하고, 그로 인한 미국 내 2009년 한 해의 대략 손해액은 1조 달러에 달했다. 하지만 인터넷의 특성상 법적 통제 대상이 되기 어렵고 정보흐름의 특성상 범죄자들을 추적하기 어려운 점이 해결방안 마련에 장애요인이 되고 있다.[138] 또한 IOC는

---

136) 아동상대 인터넷 범죄 관련 중앙 및 주 정부의 판례요약 (Internet Crimes Against Children: A Matrix and Summary of Major Federal and Select State Case Law) 2009, https://www.ncjrs.gov/pdffiles1/nij/grants/228814.pdf, 2015.11.15.방문.

137) 국제 조직범죄에 대한 보고서("Expert Working Group Report on International Organized Crime" 2010, https://www.ncjrs.gov/pdffiles1/nij/230846.pdf, 2015.11.15.방문.

138) 국제 조직범죄에 대한 보고서("Expert Working Group Report on International Organized

테러리스트 단체와 마약밀매 등 분야에서 연계를 맺어 범죄를 저지르는 경향이 크고 그 과정에서 사이버 공간은 물리적 접촉 없이 범죄를 저지를 수 있는, 위험한 장소가 된다.[139] EWG는 정부기관들과 연구기관 간의 지속적 협력이 IOC의 범죄활동을 억제할 수 있는 방법이라 결론지었다.[140]

라. 형사사법상 전자범죄 기법 (Criminal Justice Electronic Crime Technology)[141] 연구

전자범죄가 복잡한 디지털 기술을 이용하고 그에 대응하는 수사방법 또한 고도의 기술을 필요로 함으로써 NIJ는 전자범죄를 전문적으로 처리하는 전자범죄과 (Electronic crime unit) 개설을 목적으로 연구를 기획하였다. 본 연구의 중점사항은 아래와 같다.

1) 형사사법기관의 전자범죄 처리 및 분석 역량개발
2) 전자범죄와 디지털 증거에 관한 훈련프로그램 평가
3) 디지털 증거 수사유닛의 수행능력 평가 프로그램 개발
4) NIJ의 디지털 범죄와 수사관련 기술적 해결책에 대한 형사 사법적 절차 관련발간물 지속적 갱신

마. 사이버 수사와 디지털 증거관련 연구

사이버 범죄 수사는 기술의 발전에 상응하여 지속적으로 개발되어야 한다는 점, 수사기법의 법률적 근거가 미비되어 있어 수사에 어려움을 겪는다. 이에 대처하기 위해 NIJ는 연구를 통해 사이버 범죄 수사 방법 및 디지털 증거의 추출 및 보관에 관한 가이드라인을 제시했다.

Crime" 2010, https://www.ncjrs.gov/pdffiles1/nij/230846.pdf, 2015.11.15.방문., 3쪽

139) 국제 조직범죄에 대한 보고서("Expert Working Group Report on International Organized Crime" 2010, https://www.ncjrs.gov/pdffiles1/nij/230846.pdf, 2015.11.15.방문. 17쪽

140) 국제 조직범죄에 대한 보고서("Expert Working Group Report on International Organized Crime" 2010, https://www.ncjrs.gov/pdffiles1/nij/230846.pdf, 2015.11.15.방문. 3쪽

141) 전자범죄와 형사사법제도 (Criminal Justice Electronic Crime Technology) 2009, https://www.ncjrs.gov/pdffiles1/nij/sl000874.pdf 2015.11.15.방문.

1) **법정에서의 디지털 증거제시**: 법집행기관과 검사들을 위한 가이드라인 (Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors)[142] NIJ는 검사와 수사관이 사이버 범죄 수사와 압수수색 시 주의해야 할 사항과 법정에서의 디지털 증거 제시방법, 그리고 수사와 사생활 권리 간의 관계를 주의 깊게 명시했다. https://www.ncjrs.gov/pdffiles1/nij/211314.pdf 2015.11.15.방문

2) **전자범죄 현장 수사 시 최초 대응자를 위한 지침서** (Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition)[143]

NIJ는 디지털 증거와 증거능력의 안전한 확보를 위해 전자 기기의 종류, 컴퓨터 시스템, 저장기기, 휴대용 기기의 종류, 디지털 증거를 포함할 가능성이 있는 모든 종류의 기기와 시스템에 관한 지침서를 발간했다. 본 지침서는 디지털 증거 추출을 위한 수사도구와 장비, 현장 수사 시 증거 추출방법, 증거의 수송 및 보관 절차, 그리고 범죄 유형에 따른 전자범죄 수사 및 증거획득 방법을 상세히 제시한다.

3) **디지털 증거의 과학적 수사: 인터넷과 컴퓨터 네트워크가 연관된 범죄의 수사** (Forensic Examination of Digital Evidence: A Guide for Law Enforcement Investigations Involving the Internet and Computer Networks)[144]

수사 과정상 그 대상에 인터넷과 컴퓨터 네트워크를 포함할 때, 그리고 범죄에 고도의 기법이 사용되었을 때의 수사 과정과 관련된 정책을 제시한다. 증거 획득, 증거의 실효성과 증거능력에 관한 가이드라인을 제시하고 개인의 사생활 보호와 수사 간 균형의 법적 쟁점을 검토한다.

---

142) 법정에서의 디지털 증거제시: 법집행기관과 검사들을 위한 가이드라인 (Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors), 2007, https://www.ncjrs.gov/pdffiles1/nij/211314.pdf 2015.11.15.방문.

143) 전자범죄 현장 수사 시 최초 대응자를 위한 지침서 (Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition) 2008, https://www.ncjrs.gov/pdffiles1/nij/219941.pdf 2015.11.15.방문.

144) 디지털 증거의 과학적 수사에 관한 법 집행: 인터넷과 컴퓨터 네트워크가 연관된 범죄의 수사 (Forensic Examination of Digital Evidence: A Guide for Law Enforcement Investigations Involving the Internet and Computer Networks) 2004, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf 2015.11.15.방문.

4) 디지털 증거와 미국의 형사사법체계 (Digital Evidence and the U.S Criminal Justice System)[145]

본 연구는 디지털 증거를 효과적으로 추출하고 사용하기 위해 필요한 사항을 검토하고, 판례를 통한 디지털 증거의 실효성, 휴대폰 압수수색 시 영장을 발부받도록 하여 판례의 판도를 바꾼 Riley v. California 사건의 의의와 영향력을 제시하며 디지털 증거 관련 법률적 쟁점(전문법칙, 플레인뷰 법칙의 적용) 및 사생활 보호법 (수정헌법 제4조, 전자커뮤니케이션 프라이버시 법[146] 등)과 관련된 사이버 수사 쟁점을 연구했다. 또한 법률적 쟁점에 관한 해결책을 제시한다.

바. 향후 연구과제

NIJ는 2014년 데이터 형상화, DNA수사, 성 범죄자에 대한 정보공유 시스템, 범죄피해 조사, 청년층 데이트 폭력 등의 분야 연구를 지원했고[147], 2015년 현재 형사사법 제도에 있어 과학적 수사의 역할, 총기 안전의 기술적 도전과제, 사회적 및 행동학적 과학 분야의 연구를 지원하고 있으며[148] 2016년에는 크게 과학수사 분야(Forensic Science), 사회 및 행동학적 과학(Social and Behavioral Science) 분야의 연구를 지원할 예정이다.[149]

NIJ에 따르면 2040년까지 중점적으로 수행할 연구과제가 크게 세 가지로 분류된다.

1) 양국간 정보전달(Bilateral transfer of information between countries)[150]

국가 간의 효과적인 정보전달과 공유는 한 나라의 형사사법 제도를 바꿀 수 있다.[151] 예를 들면, 미국 국제개발 기관의 사절단이 중국에서 처벌제도에 관한 정보를

---

145) 디지털 증거와 미국의 형사사법 구조 (Digital Evidence and the U.S Criminal Justice System) 2015, https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf, 2015.11.15. 방문.
146) 전자커뮤니케이션 프라이버시 법 (Electronic Communications Privacy Act), http://www.it.ojp.gov/PrivacyLiberty/authorities/statutes/1285,2015.11.15.방문
147) http://nij.gov/funding/pages/expired.aspx?status=expired&fiscalyear=2014, 2015.11.15.방문.
148) http://nij.gov/funding/Pages/current.aspx, 2015.11.15.방문.
149) http://nij.gov/funding/Pages/forthcoming.aspx, 2015.11.15.방문.
150) http://nij.gov/journals/255/pages/2040.aspx, 2015.11.15.방문.
151) http://nij.gov/journals/255/pages/2040.aspx, 2015.11.15.방문.

공유 했고, 그 후 중국이 독일과 호주와 그 정보를 공유했다면 중국은 세 나라의 시스템을 혼합한 요소를 제도에 반영할 수 있다. 그 결과 아시아의 다른 나라들에도 영향력을 미칠 수 있으므로 건설적인 정보전달 시스템이 필요하다.[152]

2) 다방향의 개혁(Multilateral innovation)[153]

국제형사재판소의 수석검사가 한국계 미국인이라 가정했을 때, 세계 각 국의 동료들과 업무를 진행하며 서로의 영향을 받아 형사사법 시스템의 새로운 방법 및 규범을 개혁해 나갈 수 있다. 이는 각각 자국의 국내 사법 제도에 긍정적 영향을 줄 수 있으므로 다방향의 개혁이 권장되어야 한다.[154]

3) 사법정책의 국제적 보급(Global dissemination of justice products)[155]

법정관리 컴퓨터 시스템, 컨설팅 서비스, 교도소 설계의 타국에 대한 보급은 형사사법 제도를 변화시킬 것이다.[156] 예를 들면, 유럽형 법정 시스템이 남아프리카에서 성공적으로 마케팅 된 사례[157]가 있다.

제6절 미국의 사이버보안을 위한 유관기관의 노력(뉴욕대 안보 법 센터)

1. 안보 법 센터(Center on Law and Security, CLS) 개관

미국 뉴욕법학대학원 안보 법 센터(the Center on Law and Security)는 미국 국가안보전략과 국가안보 법 관련 프로그램을 개발 및 연구 하고 있다. 본 센터는 선도적 전문가 초빙과 함께 긴급 국가안보 현안에 관한 해결책을 찾고자 노력해왔다. 본 센터가 다루고 있는 핵심영역은 다음과 같다.[158]

152) http://nij.gov/journals/255/pages/2040.aspx, 2015.11.15.방문.
153) http://nij.gov/journals/255/pages/2040.aspx, 2015.11.15.방문.
154) http://nij.gov/journals/255/pages/2040.aspx, 2015.11.15.방문.
155) http://nij.gov/journals/255/pages/2040.aspx, 2015.11.15.방문.
156) http://nij.gov/journals/255/pages/2040.aspx, 2015.11.15.방문.
157) http://nij.gov/journals/255/pages/2040.aspx, 2015.11.15.방문.
158) http://www.lawandsecurity.org/Programs, 2015.11.15.방문.

1) 정보기관 감독 (Intelligence Oversight)

2) 경제적 제재 및 경제 국정운영 (Financial Sanctions and Economic Statecraft)

3) 국가안보 공공-민간 협력: 사이버안보 (Public-Private Partnerships in National Security: Cybersecurity)

4) 억지방안에 관한 법적 전략 (Law and Strategy: Navigating Deterrence)

5) 안보연구 세미나 (Security Research Seminar)

6) 교육 (Teaching)

CLS의 사이버 안보 프로그램은 부단히 발생하는 새로운 종류의 위협요소에 대응하는 새로운 협력모델과 공공-민간부분의 협력에 초점을 맞춰 개발되었다. 특히 아래 세 가지 요인이 연구개발의 바탕이 되어 정부와 기업들 간의 효과적인 협력방안을 제시하고 있다.

첫째, 국가의 핵심 사이버 인프라 대부분이 민간소유이며 민간소유 네트워크는 취약성이 크다. 하지만 대부분 보안 조치는 민간부분에서 실행되어야 한다.

둘째, 민간소유의 전략적 지적 재산권이 국가와 관련된 사이버 절도의 목표물이 된다.

셋째, 사이버 안보위협을 완화하기 위해 정부가 필요로 하는 정보를 대부분 민간기업이 보유하고 있다.

CLS는 뉴욕 법학대학원 내 글로벌 연구기관으로 자리매김 하며 사이버 안보 전문가와 학자들의 최신 동향의 연구를 선도하여 정부기관과 기업들이 당면한 시급한 문제해결에 기여하고 있다. 또한 컴퓨터공학 및 엔지니어링 부서, 미디어와 커뮤니케이션 부서와 협력하여 안보연구 세미나를 매주 개최해 기술, 안보, 법에 관한 연구를 해오고 있다. 2013-14년도에는 디지털 시대의 안보, 정보시스템과 소프트웨어, 컴퓨터 네트워크와 사이버 물리시스템(cyberphysical system)에 초점을 맞추어 사이버 안보관련 법과 정책의 최첨단 이슈에 관한 연구를 진행했다.[159]

159) http://www.lawandsecurity.org/Programs, 2015.11.15. 방문.

가. 사이버 안보 전담반 (Cyber-security Task Force)

CLS는 도전적 과제들의 본질을 깊이 있게 이해하고 사이버 안보관련 공공-민간부분 협력에 있어서 직면한 시급한 문제점들에 대한 해결책을 제시하기 위해 사이버 안보 전담반을 설립하였다. 전담반은 전직 정부 공무원과 민간부분의 저명한 전자통신, 기술 및 금융서비스 회사 그리고 법률사무소 구성원들로 이루어져 있다. 구성원들은 2013-14년, 세 번의 라운드테이블 토론을 주최해 아래 사항들에 관한 논의를 진행했다.

1) 새로운 안보환경 고찰을 위한 정부와 민간부분의 적절한 역할 및 효과적 정보공유 방안

2) 진화하는 규제와 법적 책임 영역

3) 사이버 안보 위협에 대한 국제적 협력 상 직면한 도전과제

나. 라운드테이블 및 회의 (Roundtables and Conferences)

CLS는 라운드테이블, 국제회의, 공공 토론세션 등을 센터의 주요사업으로 보고 있다. 이 과정에서 얻은 결과물을 바탕으로 효과적인 정부와 민간의 협력을 저해하는 요소들을 분석하고 해결방안을 권고하는 출판물들을 발간해왔다. 다음은 2014, 2015년 CLS에서 진행된 사이버 안보 회의의 예이다.

1) 정부의 클라우드 데이터 접근에 관한 심포지엄 (Symposium on Government Access to Data in the Cloud)[160], 2015:

마이크로소프트사와 협력하여 클라우드 저장 정보 접근에 대한 정부의 접근방식에 관련된 국내, 국제적 법적 관점을 주제로 토론을 진행하였다.

2) 사이버 윤리관련 부각되고 있는 쟁점과 발전하는 법률 (Cyber-Ethics: Emerging Issues and Evolving Laws)[161], 2014:

---

160) http://www.lawandsecurity.org/May-26-27-2015, 2015.11.14.방문.
161) http://www.lawandsecurity.org/December-4-2014, 2015.11.14.방문.

정부기관, 기업 운영진 및 법률 고문이 다루어야 하는 사이버 범죄관련 윤리적 현안, 정부와 기업 간 정보공유, 기업의 사이버 위협 대응책 관련 패널 토론을 진행하였다.

3) 사이버안보 법에 관한 종합적 접근 (The Law of Cybersecurity: A Multidisciplinary Perspective)[162]:

사이버안보와 민간부분, 사이버안보 수사, 사이버 분쟁관련 법과 전략, 사이버안보 분야의 미래지향적 변화에 관한 패널 토론을 진행하였다.

2. 센터의 연구 성과

CLS의 연구는 대부분 테러리즘과 사이버 안보에 관련된다.

CLS의 대표적인 연구물은 *테러리스트 대응에 관한 성적표(Terrorist Trial Report Card, TTRC)*[163]가 있다. 국가기반시설에 대한 안보가 2001년의 9/11 테러 이후 사회적 이슈화된 점을 고려한다면 CLS의 동 연구가 학계에서 환영받는 이유를 잘 알 수 있다. 동 연구는 9/11 공격 이후의 시대를 규정짓는 법적 및 안보 쟁점들에 대한 이해를 제고하고자 하며 지금까지 총12개의 TTRC 연구물이 출판되었다. TTRC에 따르면 동 보고서의 목표는 입법자, 판사, 정책결정자 등이 테러리즘의 위험 감소를 위해 노력해온 미국 법 시스템의 방식에 대한 평가를 돕기 위함이다.[164]

그 밖의 CLS의 연구는 *CLS 사이버보안 연구(CLS Cybersecurity Research), NYU 법과 안보에 관한 검토(the NYU Review of Law and Security), 안보 법 소식(the Bulletin on Law and Security), 기록상으로(For the Record), 사건 절차(Event Proceedings)* 등이 있다. 이 중 CLS 사이버보안 연구는 지금까지 세 개의 출판물이 관련 웹사이트에 게재되어 있다.[165] 가장 최근 출판물은 *군사작전실에서 이사회실로? 최전선에 참가하지 않고 사이버 위험 관리하기(From the War Room to the Board*

162) http://www.lawandsecurity.org/September-19-2014, 2015.11.14.방문.
163) http://www.lawandsecurity.org/Publications/Terrorism-Trial-Report-Card
164) 안보 법 센터(CLS), 테러리스트 대응에 관한 성적표(Terrorist Trial Report Card: U.S. Edition), http://www.lawandsecurity.org/Portals/0/documents/09_TTRCComplete.pdf, 2015.11.15.방문.
165) http://www.lawandsecurity.org/Publications/CLS-Originals

*Room? Effectively Managing Cyber Risk without Joining the Front Lines)*로 2015년 6월에 출판되었으며, 2014년에는 *침입 이후: 사이버보안 위험책임(After the Breach: Cybersecurity Liability Risk)*과 *사이버보안 파트너십: 민관협력의 새 시대(Cybersecurity Partnership: A New Era of Public-Private Collaboration)*가 있다. 이 세 개의 출판물에 관해서는 이후에 하나씩 살펴보도록 하겠다.

이 외에도 동 센터 연구진들의 연구결과물, 행사 등은 40여개의 미국 국내 및 국외 미디어를 통해 배포되고 있으며, 해당 미디어는 세계 유수의 매체인 The New York Times, The Wall Street Journal, The Economist, The Financial Times, Foreign Policy 등을 포함한다.

가. 군사작전실에서 이사회실로? 최전선에 참가하지 않고 사이버 위험 관리하기(2015년)[166]

본 보고서의 저자들은 사이버안보에 있어서 민간부문의 중요성을 인식하면서도 결국 민간 기업들은 그들 스스로를 지켜야만 한다고 주장한다. 사이버 침해의 많은 부분이 상업적인 이익을 얻기 위해서이기 때문에 사실상 모든 상업적 주체들이 사이버 위험에 노출되어 있다. 그리고 이러한 사이버 공격은 때로는 정부의 지원 하에 이뤄지기도 하며, 그 대표적인 예가 United States of America v. Wand Dong, et all.사건[167]이다. 게다가 공격의 대상이 되는 사이버 기발시설의 대부분을 민간 기업이 소유하고 있기 때문에 정부가 민간 부문을 지키기 위해 움직일 수 있는 폭이 제한된다.

---

166) Randal Milch 및 Zachary Goldman, 법과안보센터(CLS), 군사작전실에서 이사회실로? 최전선에 참가하지 않고 사이버 위험 관리하기(From the War Room to the Board Room? Effectively Managing Cyber Risk without Joining the Front Lines), 2015년 6월, http://www.lawandsecurity.org/Portals/0/Documents/whitepaper_final.pdf(마지막 방문일: 2015년 11월 15일)

167) DOJ, 상업적 이득을 위해 미국 기업 및 노동조합을 상채로 사이버 스파이를 한 5인의 중국군 해커 기소(U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage), http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor, 2015.11.15.방문.

두 저자는 이러한 문제를 해결하기 위해서는 민간 기업들이 그들이 처해있는 사이버 환경의 비대칭적 자원분배 상태를 명확히 인식해야 한다고 말한다. 앞서 설명한 중국이나 북한과 같이 정부가 사이버 공격을 주도하는 경우 하나의 민간 기업이 이를 막기 위해 유용 가능한 자원은 당연히 상대적 열세에 놓일 수밖에 없기 때문이다. 따라서 민간 기업들은 스스로가 사이버 전쟁의 최전선에서 싸우기 보다는 사이버 위험을 기업 위험관리의 하나로 인식하고 해당 쟁점을 이사회실로 들여와야 한다는 것이다.

나. 침입 이후: 사이버보안 위험책임(2014년)[168]

사이버 공격의 위험은 공격 후에 드러나지만 민간 기업들은 사이버 침입이 발생하기 전에 이에 대해 고민하고 선제적인 대응방책을 준비해야한다. 이러한 필요성은 사이버보안에 대한 법제적 및 법적 책임의 환경이 계속해서 변화하고 있기 때문에 더욱 절실해 진다. 이와 같은 배경으로 인해 기업들은 사이버 위협에 대항하는데 있어서 법적 모호성을 겪고 있는 것이다. 이는 기업들로 하여금 다음과 같은 해결과제를 안겨준다. ①보안 장치의 설치 및 감시, ②사이버 사고에 대응하는 정책 및 절차 이행, ③위협, 취약점, 사고 정보의 공개, ④정부와의 협력 시기, 협력 여부, 당국에게 사고보고 방식의 결정, ⑤앞서 설명한 해결과제의 해결방안, ⑥해당 결정들이 소송에 미치는 영향이 그것이다.

여기에 민간 부분이 국가기반시설을 운용하는 인터넷 시스템 및 네트워크를 상당부분 소유하고 있다는 사실을 더하면 해당 문제의 심각성은 그 무게를 더할 수밖에 없다. 이를 해결하기 위해선 민간 기업들이 사이버 위험에 대비하는 방책 수립에 있어서 고려요소들에 대한 이해가 선행되어야 한다. 국가 보호라는 정부의 전통적 역할이 점점 더 민간부문으로 옮겨 가고 있다는 현실도 직시해야만 한다.

---

168) Judith H. Germano 및 Zachary K. Goldman, 안보 법 센터(CLS), 침입 후: 사이버보안 위험책임(After the Breach: Cybersecurity Liability Risk), http://www.lawandsecurity.org/Portals/0/Documents/CLS%20After%20the%20Breach%20Final.pdf2015.11.15. 방문.

다. 사이버보안 파트너십: 민관협력의 새 시대(2014년)[169]

국가적 사이버 문제 해결을 위한 민관협력의 필요성은 이미 널리 받아들여졌지만, 민관협력 관계에 대한 상황, 본질, 범위에 대한 논의는 여전히 진행될 필요가 있다. 그리고 민관협력을 저해하는 요소들도 여전히 산적해 있으며, 그 대표적인 요소는 민사상 법적책임에 관한 소송의 위험이다. 여기에 사이버 문제의 국제적인 측면과 그 빠르게 변화하는 기술이 더해진다면, 국가 수준에서 이 문제를 해결하기 위한 정부의 노력과 민관협력관계는 더욱 복잡해지게 된다.

사이버 문제 해결에 있어 민관협력에 대한 이해를 제고하기 위하여 본 보고서는 사이버보안에 관한 전략적 접근방식을 도입하는데 필수적인 다음의 네 가지 핵심 영역을 살펴본다.

첫째, 사이버보안은 다른 위협과는 왜 다르며, 사이버보안의 문제를 해결하는데 왜 민간협력이 특히 중요한가?

둘째, 효과적인 민관협력에는 어떤 장애물이 존재하며, 어떠한 장애물이 모호성을 더하고 사이버 공격의 피해 기관에게 해가 되는가?

셋째, 이러한 장애물들과 현재의 가용 민간 부문의 자원을 고려할 때 기업들은 사이버 문제를 해결하기 위해 자조(self-help)적이 되어야 하는가? 정부의 도움 없이 민간 기업들은 언제 그리고 어느 정도까지 사이버 공격에 스스로 대항할 수 있는가?

넷째, 전통적인 거버넌스 모델보다 더 성공적인 민간협력 방식에는 무엇이 있는가? 그리고 포괄적인 사이버보안 전략에 있어 다양한 정부 주체가 맡아야만 하는 역할에는 무엇이 있는가?

---

169) Judith H. Germano, 안보 법 센터(CLS), 사이버보안 파트너십: 민관협력의 새 시대(Cybersecurity Partnership: A New Era of Public-Private Collaboration), http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf, 2015.11.15.방문.

제4장

KOREAN INSTITUTE OF CRIMINOLOGY

북한의 사이버테러 위협과 대응정책

김한균·조민정

제4장

북한의 사이버테러 위협과 대응정책

제1절 북한 추정 사이버테러 분석 및 수사결과

1. 사건별 사이버테러 유형과 범행 수법

가. 2014년 11월 미국 소니 픽처스 엔터테인먼트 해킹

1) 사건 정보 및 배경

2014년 11월 소니 픽처스 엔터테인먼트(Sony Pictures Entertainment, 이하 SPE)[170]의 기밀 정보가 유출되는 사건이 발생했다. 유출 피해를 입은 SPE의 정보에는 직원 및 직원 가족의 이메일, 회사 경영진 연봉, SPE가 보유한 미개봉 영화 파일 등이 포함되었다. SPE는 공식 공지문(Sony Pictures Notice Letter)[171]을 통해 자세한 피해 내역과 발생 경위 등을 발표했다. 그 상세 내용을 정리하면 다음과 같다.

SPE의 전산에 심각한 손해가 발생한 시기는 2014년 11월 24일이며 이 사실을 인지한 날은 2014년 12월 1일이다. SPE가 파악한 개인정보 유출 내역으로는 이름, 주소뿐만 아니라 출장비용을 결제한 신용카드, 보수, 고용 관련 정보 등이 포함되었다.

SPE가 북한 추정 해킹의 대상이 된 이유는 북한의 김정은 국방위원회 제1위원장을 희화화한 영화 더 인터뷰(The Interview)의 제작 및 유통을 담당하였기 때문이다.[172] SPE의 공식 공지문상으로 전산 장애 및 개인정보 유출의 원인을 사이버공격

---

170) 일본의 다국적 기술 및 미디어 기업인 소니 코퍼레이션(Sony Corporation)의 계열사다. 소니 픽처스 엔터테인먼트는 1991년 설립되었으며 현재는 미국 기업이다. 소니 픽처스 엔터테인먼트 홈페이지 참조.
http://www.sonypictures.com/

171) 캘리포니아주 법무부 법무장관실을 통해 공개되었다. http://oag.ca.gov/system/files/12%2008%2014%20letter_0.pdf

이라고 언급했다.

2) 범행 수법

SPE에 대한 공격은 이른바 평화의 수호자(Guardians of Peace, 이하 GOP)라는 해커에 의한 것으로 밝혀졌다. 해킹이 처음 시작된 시기에 대해서는 알려진 바가 없다. SEP의 전산 관리자들은 침입을 통제하기 위해 해킹 사실을 알게 된 이후 전 세계 네트워크를 종료하고 VPN 연결과 와이파이 연결을 차단했다.[173] 그러나 여전히 어떠한 방식으로 해킹이 일어났는지는 정확히 파악되지 않은 상황이다.

FBI의 발표 자료에 따르면 해커들은 데이터를 삭제하는 파괴적인 멀웨어(destructive malware)[174]를 사용했다.[175] 공격자인 GOP는 수개월 전 SPE 직원 컴퓨터에 멀웨어를 심은 다음 정보를 빼냈고, 11월 21일에는 임원진에게 "God'sApstls"라는 이름으로 또한 금전적 요구를 하거나 SPE를 폭격하겠다는 협박성 메일을 보내기도 했고, 11월 24일에는 직원들의 컴퓨터 화면에 경고 메세지를 띄우기도 했다.[176]

나. 2014년 12월 한국수력원자력 해킹

1) 사건 정보 및 배경

한국수력원자력(이하 한수원)의 해킹은 2014년 12월 9일부터 2015년 3월 12일까지 총 6회에 걸쳐 발생하였다. 개인정보범죄 정부합동수사단(이하 합수단)의 보도자료에 따르면 1차로 한수원 직원 이메일에 대한 공격, 2차 한수원 자료공개 및 협박이

---

172) CNN, New York Times 등 주요 미국 언론과 BBC 등 세계 각국의 언론이 일제히 보도하였다. 다음의 기사 참조.
http://money.cnn.com/2014/12/24/technology/security/sony-hack-facts/
http://www.nytimes.com/2014/12/15/world/sonys-international-incident-making-kims-head-explode.html?_r=1

173) http://www.wired.com/2014/12/sony-hack-what-we-know/

174) 멀웨어는 악성 소프트웨어의 줄임말이다. 파괴적인 멀웨어는 멀웨어 중 감염된 컴퓨터를 파괴시킬 수 있을 정도의 강력한 멀웨어를 일컫는다. 예를 들어 데스토버 공격이 있다. 시만텍은 소니 해킹 멀웨어에서 과거 한국 표적 공격과 연관성이 높은 멀웨어를 발견했다고 밝히면서 데스토버 샘플을 공개했다. http://www.symantec.com/ko/kr/about/news/release/article.jsp?prid=20141208_01

175) FBI의 공식 언론보도자료 참조.
https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

176) http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg

있었다. 아래는 합수단의 보도자료를 정리한 것이다.[177]

1차 이메일 공격은 한수원 직원 이메일 계정으로 악성코드 이메일을 발송하는 것으로 시작되었다. 2014년 12월 9일 발송인 211명 이메일 계정으로부터 한수원 직원 3,571명을 수신으로 하여 악성코드가 첨부된 이메일 총 5,986통이 발송되었다. 구체적으로 9일 5,980건, 10일 3건, 11일 1건, 12일 2건이 발송되었다.

2차 자료 공개 및 협박은 12월 15일부터 시작되었다. 네이버에 '우리는 원전반대그룹! 끝나지 않은 싸움'이라는 글을 게시하며 한수원 임직원 주소록 파일 등이 공개되었고 이후 18일(2차) / 19일(3차) / 21일(4차) / 23일(5차) 트위터 등에 '크리스마스 때까지 원전 가동을 중지하고 100억 달러를 주지 않으면 보유한 (원전)자료를 계속 공개하겠다'는 취지의 글을 게시하였다. 이후 2015년 3월 12일(6차)에는 '돈이 필요하다'는 글과 함께 한수원의 원전 도면 증을 게시하였다.

공개된 한수원 자료의 내용은 임직원 주소록, 전화번호부, 원전관련 도면 등 파일 94개로 드러났다. 다만 한수원 자체점검 결과 6차에 걸쳐 공개된 자료들은 원전 운용과 관련한 핵심자료가 아니며 교육용 등 일반문서가 대부분이고, 원전관리에 위험을 초래하거나 원전수출 등 국가적 원전정책에 영향을 미칠 수 있는 중요정보의 유출은 없었다.[178]

2) 범행수법

한수원 사이버테러 사건에 사용된 수법은 피싱(phishing)[179]으로, 이메일에 첨부된 악성코드를 통한 PC 디스크 파괴다. 합수단 보고자료에 따르면 PC중 8대만 감염되고 그중 5대의 하드 디스크가 초기화되는 정도에 그쳐 원전 운용이나 안전에는 이상이

177) 2015년 3월 17일 합수단 보도자료.
http://www.spo.go.kr/_custom/spo/_common/board/download.jsp?attach_no=154704

178) 2015년 3월 17일 합수단 보도자료.
http://www.spo.go.kr/_custom/spo/_common/board/download.jsp?attach_no=154704

179) 개인정보(Private data)와 낚시(Fishing)의 합성어로 개인정보를 낚는다는 의미. 금융기관 또는 공공기관을 가장해 전화나 이메일로 인터넷 사이트에서 보안카드 일련번호와 코드번호 일부 또는 전체를 입력하도록 요구해 금융 정보를 몰래 빼가는 수법을 의미한다. 사이버경찰청 홈페이지 참조.
http://www.police.go.kr/portal/main/contents.do?menuNo=200289

없었다. 범인(조직)은 이메일에 피싱 메일을 보내 한수원 관계자들의 이메일 비밀번호를 수집한 후 그 이메일 계정에서 자료들을 수집하는 등 범행을 사전에 준비하였다. 공격 이메일에는 한글(hwp) 파일이 첨부되었는데, 이를 실행하면 악성코드가 실행되어 파일실행 장애, 하드디스크 초기화, 네트워크 장애 유발 등의 문제가 발생한다. 다만 자료유출의 기능은 없는 것으로 확인되었다.[180]

다. 2013년 3월 주요 방송사 및 금융사 전산망 마비

1) 사건 정보 및 배경

2013년 3월 20일 오후 2시께 한국의 주요 방송사 및 금융사의 전산망이 마비되고 다수의 컴퓨터가 악송코드에 감염되어 피해를 입은 사건이 발생하였다. 피해 기관으로는 MBC·YTN·신한은행 등 언론 및 금융사가 포함되었다. 직원들의 컴퓨터 전원이 일제히 꺼지고 '재부팅 하라'는 메시지가 떴다. 피해 규모는 6개사, PC 및 서버 3만 2천 여 대에 달했다.[181]

민관군 사이버위협 합동대응팀(이하 합동대응팀)에 따르면 국가공공기관은 피해가 없었으며, 국내에서만 발생한 것으로 파악되었다.[182]

2) 범행 수법

한국인터넷진흥원에 따르면 3월 20일 전산망 마비에 사용된 범행 수법은 지능형 타깃 지속 공격(Advanced Persistent Threat, 이하 APT)[183]다. 최소 9개월 이상의

---

180) 해당 악성 코드 등에 관한 자세한 내용은 합수단 보도자료 참조. http://www.spo.go.kr/_custom/spo/_common/board/download.jsp?attach_no=154704

181) http://www.kisa.or.kr/uploadfile/201312/20131204144304798 4.pdf

182) 사이버 위협 합동 대응자료 참조. http://www.kcc.go.kr/user.do?mode=view&page=A05030000&dc=K00000001&boardId=1113&boardSeq=36096

183) 다양한 보안 위협으로 정부 기관이나 산업시설, 기업, 금융기관 등의 컴퓨터를 지속적으로 공격하는 것. 통신망을 타고 들어가 내부 시스템으로 침투한 뒤 한동안 이를 숨겨놓았다가 시간이 지나 한꺼번에 동작시켜 주요 정보를 유출하거나 시스테믕ㄹ 무력화하는데 쓰인다. 기존의 안티바이러스 프로그램에 탐지되지 않도록 악성코드를 제작할 수 있고, 자체 전파하는 바이러스와 달리 다량의 트래픽을 발생시키는 것도 아니어서 네트워크 관리자의 감시도 쉽게 피할 수 있다. 대표적 기법으로는 스턱스넷(Stuxnet)과 오퍼레이션 오로라(Operation Aurora), 나이트 드래곤(Night Dragon), EMC/RSA 공격 등을 들 수있다. 2011년 SK커뮤니케이션즈 3500만명과 넥슨 1320만명의 개인정보 유출, 농협 전산망 마비 사건의 주범이 바로 PT였다. 또한 2014년 12월 발생한 한국수력원자력 해킹에도 APT 공격이 활용됐다.

공격 준비기간을 거쳐 사전 계획된 목표 서버해킹으로 내부망에 연결된 PC를 공격해 48,700여대의 하드디스크를 손상시켰다.

라. 2013년 6월 사이버테러 사건

1) 사건 정보 및 배경

2013년 6월 25일 청와대, 국무조정실, 새누리당, 연합뉴스, 조선일보 등의 홈페이지가 해킹되고 주요 정부기관 총69개와 민간기업의 서버가 마비되는 사태가 발생하였다. 청와대는 홈페이지에 '통일대통령 김정은 장군님 만세!'라는 문구가 뜨는 등 홈페이지 일부가 변조되어도 개인정보가 유출되었으며[184], 새누리당과 군장병, 주한미군의 개인정보가 공개되기도 하였다.[185]

2) 범행 수법

해당 공격에 사용된 범행 수법은 크게 세 가지로 구분할 수 있다. 웹 사이트 변조 공격, 신상정보 탈취 공격, 그리고 시스템을 마비시킨 분산서비스거부(DDoS)공격이 그것이다.[186] 정부합동대응단은 '6.25 사이버공격 준비는 3월 20일 이전인 최소 6개월 전부터'라고 밝혔다.[187]

마. 2011년 4월 농협 해킹사건

1) 사건 정보 및 배경

2011년 4월 12일 국내 농협전산망 전체가 이용불가상황에 빠진 초유의 사건이 발생했다. 농협의 전산마비 사고는 단순 시스템 오류가 아닌 계획적인 의도를 가지고 내부 시스템에 접근해 서버가 파괴된 사건이었다. 농협은 시스템 파일 삭제 명령이 실행되고 있음을 감지하고 고객 개인정보와 금융거래 원장을 보호하기 위해 주요

한경 경제용어사전, http://dic.hankyung.com/apps/economy.view?seq=10195

184) 청와대 공지사항, http://www1.president.go.kr/news/noticeList.php?srh%5Bpage%5D=5&srh%5Bview_mode%5D=detail&srh%5Bseq%5D=659

185) 《6·25 사이버 테러 분석 보고서》 NSHC, 2013

186) 국가기록원, http://www.archives.go.kr/next/search/listSubjectDescription.do?id=009375

187) 박재문 미래부 정보화전략국장 정부합동대응팀 브리핑, http://news.mt.co.kr/mtview.php?no=2013071616161216589

업무 시스템의 거래를 모두 차단해 대고객 거래가 전면 중단되었다. 또한 백업센터마자 파일 삭제 명령의 영향을 받아 장애 복구가 지연되었으며, 일부 거래내역이 손실되기도 했다.[188] 또한 자료 대규모 자료 손상으로 18일이 지난 4월 30일에야 정상업무가 가능했다.[189]

2) 범행수법

농협 전산망 사건에는 프로그램 삭제 명령이 포함된 악성코드가 사용되었다. 2010년 9월 범인들이 한 웹하드 사이트를 통해 사이트 업데이트 프로그램을 가장한 악성코드를 유포했고, 농협의 협력업체 직원 노트북이 해당 악성코드에 감염되면서 문제가 발생했다. 발견된 악성코드만 81개에 달했다. 또한 범인들이 해당 노트북을 7개월 이상 집중적으로 관리하고 도청프로그램까지 사용해 공격대상의 IP와 최고관리자 비밀번호 등도 노출되었다.[190]

바. 2011년 3월 DDoS 공격

1) 사건 정보 및 배경

2011년 3월 DDoS 공격은 흔히 3.4 DDoS 공격이라고도 한다. 2011년 3월 3일 오후 5시경 최초로 국내 포털 사이트 및 공공기관의 웹 사이트에 대한 공격 징후가 발생하였고, 이후 4일 오전 10시와 오후 6시 30분 사이 국방, 은행, 인터넷 포털, 공공기관 등 총 40개의 웹사이트를 대상으로 디도스 공격이 발생하였다.[191]

2) 범행 수법

2011년 3월 DDoS 공격은 2009년 7월 공격보다 진화된 공격이다. 우선 3.4 DDoS 공격에는 좀비PC의 Host 파일을 변조하여 악성코드 치료를 위한 백신의 업데이트와 설치를 방지했고, 동일한 악성코드 파일로 다수의 공격을 수행한 2009년 7월 공격과

---

188) 한국과학기술단체총연합회, 〈과학과 기술 2011.06〉, p.48. http://kofst.or.kr/kofst/PDF/2011/n6s505/GGDCBE_2011_n6s505_44.pdf
189) 국가기록원, http://www.archives.go.kr/next/search/listSubjectDescription.do?id=009375
190) 한국과학기술단체총연합회, 〈과학과 기술 2011.06〉, p.49. http://kofst.or.kr/kofst/PDF/2011/n6s505/GGDCBE_2011_n6s505_44.pdf
191) 신종환, Internet & Security Focus, 2013 9월호, 44쪽.

는 달리 공격 시마다 악성코드 파일이 달라지고 여러 가지 악성코드가 유기적으로 동작하며 공격을 진행하였다.

공통점은 악성코드를 배포한 배포지가 웹하드 업체였다는 점과 국가기관 및 공공기관, 금융기관 또는 포털사이트를 공격대상으로 삼았다는 점, 공격 종료시점에 좀비 PC의 파일과 하드디스크를 검색해 파괴 후 공격을 종료하는 점 등이다.[192]

사. 2009년 7월 DDoS 대란

1) 사건 정보 및 배경

2009년 7월 7일 DDoS 공격으로 인한 전산망 장애 등이 발생한 사건이다. 북한의 공격이 대외적으로 공개된 최초의 사건이기도 하다.[193] 2009년 7월 DDoS 공격을 흔히 7.7 DDoS 대란이라고 하기도 한다.

2009년 7월 7일에 대규모 DDoS 공격이 국내 12개 주요 정부기관 및 금융, 포털 사이트를 대상으로 발생했으며, 이어 8, 9일 주요 기관에 대한 2차, 3차 DDoS 공격 발생 후 7월 10일 공격이 종료되었다.[194] 이 사건의 주요 특징은 2009년 7월 5일 미국을 시작으로 며칠간에 걸친 공격에서 한국이 목표가 되면서 진행되었다는 점이다.

2009년 Cisco Systems Korea의 분석 자료에 따르면 1차 DDoS 공격(2009년 7월 5-6일)에서는 미국 21개 주요 정부기관, 금융, 인터넷 포털 사이트가 공격 대상이 되었고 2차 공격(2009년 7월 7-8일)에서는 국내 12개와 미국 14개의 주요 정부기관, 금융, 인터넷 포털 사이트가, 3차 공격(2009년 7월 8-9일)에는 국내 15개 및 미국 1개 정부기관, 금융, 인터넷 포털사이트가, 4차 공격(2009년 7월 9-10일)에는 국내 7개 주요 정부기관, 금융, 인터넷 포털 사이트가 대상이 되었다.[195]

---

192) DDos 지속공격 비교 분석 및 대응방안 연구, 〈방송통신기술 이슈&전망〉 2013년 제 23호, 한국방송통신전파진흥원, 5쪽.

193) 윤해성, 윤민우, 사이버 테러의 동향과 대응 방안에 관한 연구, 한국형사정책연구원 (2012), 244쪽.

194) DDos 지속공격 비교 분석 및 대응방안 연구, 〈방송통신기술 이슈&전망〉 2013년 제 23호, 한국방송통신전파진흥원, 3쪽.

195) 〈DDoS 공격 비상, 어떻게 대처할 것인가? - 7.7 DDoS 공격 유형 분석 및 대응방안〉, Cisco Systems Korea, 2009
https://www.cisco.com/web/KR/learning/events/down/July_DDoS_Websemi

2) 범행 수법

해당 사건에서도 DDoS 공격 수법이 사용되었다. 한국인터넷진흥원이 제시한 자료에 따르면 해당 DDoS 공격에는 10만대 이상의 좀비PC가 사용되어 공격대상과 공격시간을 명령하였다.[196]

7.7 디도스 사건은 기존의 디도스 공격과는 다른 양상을 보였다. 즉 기존의 디도스 공격에서는 좀비 PC를 실시간으로 단순 조정하여 공격하였으나 7.7디도스의 경우에는 악성코드의 기능 및 공격대상을 업데이트 할 수 있는 숙주서버에 특정시간에 일정주기로 접속해 공격대상 및 공격 스케줄링 명령을 받게 하여 공격대상과 공격시간을 명령받은 10만대 이상의 좀비PC가 이미 정해진 명령에 따라 공격대상 웹사이트를 동시에 공격하였다. 또한 공격에 사용된 좀비 PC의 악성코드는 감염 경로를 추적할 만한 정보를 모두 제거한 진화된 형태로의 공격이 이루어졌다. 한편 기존 디도스 공격이 금전적 목적으로 이루어진대 반해 7.7 디도스는 정부, 금융, 포털 등 사회적 혼란을 야기할 목적으로 수행된 것으로 추정되어 향후 디도스 공격의 변화양상을 엿볼 수 있는 사건이라 평가된다.[197]

2. 수사 결과 및 북한 소행 추정 근거

가. 미국 소니 픽처스 엔터테인먼트 해킹

미 FBI 공개 자료에 따르면 미국이 소니 픽처스 엔터테인먼트의 해킹을 북한 소행으로 추정한 근거는 다음과 같다.

> 수사 노력과 미 정부 부처 및 기관의 협력의 결과 FBI는 북한 정부가 해당 행위에 책임이 있다고 결론지을 수 있는 충분한 정보를 보유하고 있다. 민감한 정보원 및 수법을 보호할 필요에 의하여 모든 정보를 공유할 수는 없지만 다음의 근거로 결론을 내렸다: 해당 공격에 사용된 데이터 삭제 멀웨어 기술 분석 결과 북한 정부

---

nar.pdf

196) 한국인터넷진흥원, http://www.kisa.or.kr/uploadfile/201310/201310071957453995.pdf

197) 신종환, Internet & Security Focus 2013 9월호, 43-44쪽.

가 이전에 개발한 다른 멀웨어와의 연관성이 드러났다. 예를 들어 코드의 특정 라인, 암호화 알고리즘, 데이터 삭제 방식, 네트워크 손상 등이다. FBI는 또한 해당 공격에 사용된 인프라와 기타 미국 정부가 북한으로 부터 직접적인 연결성을 발견한 악성 사이버행위가 상당부분 동일함을 발견했다. 예를 들어 FBI 조사결과에 따르면 북한 소유로 알려진 일부 인터넷 프로토콜(IP) 주소가 해당 공격의 데이터 삭제 멀웨어로 코딩된 IP 주소와 통신한 기록이 있었다. 이와는 별개로 SPE 공격에 사용된 수단은 북한의 2013년 3월 한국의 은행 및 언론사 사이버 공격과 유사함을 보였다.[198]

나. 2014년 12월 한국수력원자력 해킹

합수단이 한수원의 해킹을 북한 소행으로 추정하는 이유도 FBI의 근거과 유사하다. 합수단은 수사를 통해 해당 사건에 대한 IP 주소와 악성코드 등을 분석하였다. 그 결과 발표내용은 다음과 같다.

① 본건 이메일 공격에 사용된 악성코드는 북한 해커 조직이 사용하는 것으로 알려진 'kimsuky(김수키)' 계열 악성코드[199]와 그 구성 및 동작방식이 거의 같고, ② 본건

198) As a result of our investigation, and in close collaboration with other U.S. government departments and agencies, the FBI now has enough information to conclude that the North Korean government is responsible for these actions. While the need to protect sensitive sources and methods precludes us from sharing all of this information, our conclusion is based, in part, on the following: Technical analysis of the data deletion malware used in this attack revealed links to other malware that the FBI knows North Korean actors previously developed. For example, there were similarities in specific lines of code, encryption algorithms, data deletion methods, and compromised networks. The FBI also observed significant overlap between the infrastructure used in this attack and other malicious cyber activity the U.S. government has previously linked directly to North Korea. For example, the FBI discovered that several Internet protocol (IP) addresses associated with known North Korean infrastructure communicated with IP addresses that were hardcoded into the data deletion malware used in this attack. Separately, the tools used in the SPE attack have similarities to a cyber attack in March of last year against South Korean banks and media outlets, which was carried out by North Korea. FBI의 공식 언론보도자료 참조.
https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

199) 'kimsuky(김수키)' 악성코드: 2013년 세계적인 러시아 보안회사인 카스퍼스키가 북한에서

악성코드에 이용된 '흔글 프로그램' 버그(취약점)가 'kimsuky' 계열 악성코드에 이용된 버그와 동일하며, ③ 'kimsuky' 계열 악성코드들의 IP 일부가 본건 협박글 게시에 사용된 중국 선양 IP 대역들과 12자리 중 9자리까지 일치하고, ④ 범인이 본건 자료 탈취/이메일 공격/협박글 게시 루트로 도용한 국내 ㈜H사 VPN 업체와 관련하여, 동 회사가 관리하는 다른 접속 IP 중에서, '14.'12. 하순 북한 IP 주소 25개, 북한 체신성 산하 통신회사 KPTC에 할당된 IP주소 5개가 접속한 흔적이 발견되었으며, ⑤ 본건 범행은 국민안전과 직결되는 국가 인프라 시설인 원전을 대상으로 전 국민에게 지속적이고 공개적으로 협박을 하여 사회불안을 야기하고 국민들의 불안 심리를 자극한 사건임이다.[200]

또한 합수단의 수사 결과는 범인들의 범행동기와 목적을 금전 등 실질적 이익에 두지 않고 국민을 불안 심리를 자극한 것에 방점을 두었다. 그 대표적인 근거로 ① 국민안전과 직결되는 국가인프라 시설인 원전을 대상으로 하여 사회불안 야기, ② 한수원 이메일 공격이 실패하자 피싱으로 수집한 정보로 불안심리 자극, ③ 실제 돈을 받아내기 위함이 아닌 다른 목적을 희석하기 위한 불분명한 금전요구, ④ 국민안전이나 금전적 목적과 무관한 국가정책 현안으로 협박을 지적하였다.[201]

다. 2013년 3월 주요 방송사 및 금융사 전산망 마비

2013년 3월 20일 사이버테러에 대하여 정부는 민관군 합동대응팀을 꾸려 접속기록과 악성코드를 분석해 북한과의 연관성을 검토했다. 그리고 〈3.20 사이버 테러에 대한 중간 조사결과 발표〉를 통해 북한 정찰총국에서 사용하는 해킹 방법과 유사한 방법이 해당 공격에 사용되었음이 드러났다고 밝혔다.

브리핑에서 북한과의 연관성에 대해서는 다음과 같이 언급했다.[202]

만들어졌다고 추정한 악성코드로서, 이후 다수 유사 악성코드가 발견되었다. 2015년 3월 17일 합수단 보도자료.
http://www.spo.go.kr/_custom/spo/_common/board/download.jsp?attach_no=154704

200) 2015년 3월 17일 합수단 보도자료.
http://www.spo.go.kr/_custom/spo/_common/board/download.jsp?attach_no=154704

201) 위의 자료.

202) 대한민국정책포털, 3.20 사이버테러 중간 조사결과발표,
http://ebrief.korea.kr/open.brf.EBSB0021.selectBriefPopup.laf?brpId=36483

"실제 북한 내부 PC 6대에서 직접 접속하거나 또는 해외를 거쳐서 1,590회를 접속한 흔적이 있었고, 그 중에서 13번은 북한에서 직접 접속한 그런 IP가 발견되었습니다. 실제 북한 내부 PC에서 해외를 거쳐서 금융사에 유포한 악성 코드 3종을 업로드 했습니다. (...중략...) 또한, 북한과 연관성이 있는 관련 증거들은 지금까지 파악된 국내 공격 경유지, 보통 일반적으로 말하는 명령조정서버, C&C라고 말하기도 하는데, 그런 C&C, 그리고 로그 분석해서 나온 공격경유지 중 총 49개가 발견되었는데, 그 중 22개가 과거에 사용했던 경유지, 과거에 사용했다는 의미는 국정원이나 군 기무사 사이버 사령부에서 대남에 관한 해킹에 대한 정보를 수집하고 있습니다. 그 부분에 대해서는 사실 자세히 말씀드릴 수 없겠지만, 확인된 결과에 의하면, 과거에 사용되었던 경유지와 동일한 경유지가 22개나 겹칩니다."

라. 2013년 6월 사이버테러 사건

2013년 6월 사이버테러 사건을 다루기 위해 민관군 합동대응팀을 이루어 로그 기록, IP 주소, 기존 북한의 대 남한 해킹 자료 등을 비교하여 분석하였다. 그 결과 3월 20일 사이버테러 사건과 동일 수법으로 추정된다는 내용의 〈'6.25 사이버공격 조사 결과' 발표〉를 통해 다음과 같이 그 이유를 설명하였다.[203]

"첫째, 6월 25일 서버 파괴 공격을 위해 활용한 국내 경유지 서버와 7월 1일 피해기관 홈페이지 서버에서 북한의 IP가 발견되었고, 둘째, 서버를 다운시키기 위한 시스템 부팅역역 파괴, 시스템의 주요 파일 삭제, 해킹 결과를 전달하기 위한 상황 모니터링 방법과 악성코드 문자열 등이 3.20 사이버테러와 동일하였습니다."

203) 대한민국정책포털, 6.25 사이버공격 조사결과 발표, http://ebrief.korea.kr/open.brf.EBSB0021.selectBriefPopup.laf?brpId=37730

마. 2011년 4월 농협 해킹사건

2011년 농협 해킹사건에 대해서도 북한이 공격자로 추정된다고 발표되었다. 다만 이에 대한 회의적인 시각도 많았다.[204] 해당 사건에서 검찰은 IP주소와 악성코드 등을 살폈다. 검찰의 브리핑 자료[205]에 따르면 삭제 대상 파일 확장자를 비교한 결과 2009년 7.7 DDoS 공격 및 2011년 3.4 DDoS공격과 유사한 특성이 발견되었다. 특히 7.7 DDoS와는 29개가 93%일치하였고, 3.4 DDoS와는 31개가 100% 일치하였다. 또한 3.4 DDoS와 농협 해킹사건에 발생한 암호키도 A로 시작하는 45자의 암호키가 동일하였다. 악성코드 감염경로, 악성코드 유포수법, 공격구조는 7.7 DDoS 공격 및 3.4DDoS 공격과 같은 것으로 드러났고, 프로그램의 유사성도 발견되었다.[206]

바. 2011년 3.4 DDoS 공격

경찰청 사이버테러대응센터는 보도자료를 통해 3.4 DDoS 공격 역시 2009년 7월 7일 발생한 공격과 동일범이라고 밝혔다.[207] '북한'을 명시하지는 않았지만 사실상 북한 소행이라 발표한 것이다.[208]

경찰이 제시한 근거는 다음과 같다. 7.7 DDoS 공격자와 동일범임을 판단하는 근거로 파일공유사이트를 통해 악성코드를 유포하고 여러 단계의 해외 공격명령서버(C&C: Command & Control)를 이용하여 공격을 시도하는 등 디도스 공격체계 및

---

204) 연합뉴스, http://www.yonhapnews.co.kr/economy/2011/05/03/0301000000AKR20110503096700017.HTML; 경향신문, http://news.khan.co.kr/kh_news/art_print.html?artid=201105032151525

205) 서울중앙지방검찰청 첨단범죄수사제2부 농협 전산망 장애사건 수사결과, 2011, http://www.slideserve.com/cahil/5682386

206) 서울중앙지방검찰청 첨단범죄수사제2부 농협 전산망 장애사건 수사결과, 2011, http://www.slideserve.com/cahil/5682386

207) 경찰청 사이버테러대응센터 보도자료, 2011년 4월 6일 〈3.4 DDoS 사건의 공격자는 7.7 DDoS와 동일범〉, http://www.police.go.kr/portal/bbs/view.do?nttId=7968&bbsId=B0000011&searchCnd=1&searchWrd=&section=&sdate=2011-03-01&edate=2011-04-10&useAt=&replyAt=&menuNo=200067&viewType=&delCode=0&option1=&deptId=&pageIndex=1

208) 경찰청 사이버테러대응센터 보도자료, 2011년 4월 6일 〈3.4 DDoS 사건의 공격자는 7.7 DDoS와 동일범〉, http://www.police.go.kr/portal/bbs/view.do?nttId=7968&bbsId=B0000011&searchCnd=1&searchWrd=&section=&sdate=2011-03-01&edate=2011-04-10&useAt=&replyAt=&menuNo=200067&viewType=&delCode=0&option1=&deptId=&pageIndex=1

방식이 동일하다는 점, 악성코드의 설계방식 및 통신방식이 정확하게 일치하는 등 동일 프로그래머에 작성된 것으로 입증된 점 특히 3.4 DDoS 공격과 7.7 DDoS 공격 시 활용된 해외 공격명령서버 일부가 동일한 점 등을 결정적 증거로 제시하였다.[209] 또한 이에 덧붙여 전 세계 IP 주소는 42억개 이상으로 공개되지 않은 7.7 DDoS의 C&C 서버와 동일한 IP를 사용했다는 사실에 비추어 동일범이 아니면 불가능하다.[210]

사. 2009년 7.7 DDoS 대란

7.7 DDoS 대란에 대해서는 국가기관이 공개적으로 북한발 공격을 인정하는 자료는 없다. 사건 발생 당시 언론이 일제히 북한발 공격이라고 보도하였는데 이에 대하여 국가정보원은 2009년 7월 다음과 같이 공지했다.[211]

> 국정원은 일부 언론이 11일 정보위發로 "북한 해커조직의 IP〈인터넷 접속위치〉를 확인했다고 단정적으로 보도한 것은 앞서나간 것"이라며 신중 보도를 당부했다.
>
> 이와 관련 국정원은 이번 「7.7 사이버공격」의 배후가 북한이라는 여러 가지 증거를 가지고 정밀 추적과 조사가 진행 중인 상황이며, 아직 북한의 소행임을 최종 확인한 것은 아니라고 밝히면서 그럼에도 일부 언론이 마치 확인된 것처럼 단정해서 보도한데 대해 유감을 표명했다.
>
> 국정원은 또한 非公開로 진행된 국회 정보위 간담회(7.10) 보고내용이 언론에 유출되어 보도된데 대해서도 우려를 전했다.

---

209) 경찰청 사이버테러대응센터 보도자료, 2011년 4월 6일 〈3.4 DDoS 사건의 공격자는 7.7 DDoS와 동일범〉, http://www.police.go.kr/portal/bbs/view.do?nttId=7968&bbsId=B0000011&searchCnd=1&searchWrd=&section=&sdate=2011-03-01&edate=2011-04-10&useAt=&replyAt=&menuNo=200067&viewType=&delCode=0&option1=&deptId=&pageIndex=1

210) 경찰청 사이버테러대응센터 보도자료, 2011년 4월 6일 〈3.4 DDoS 사건의 공격자는 7.7 DDoS와 동일범〉, http://www.police.go.kr/portal/bbs/view.do?nttId=7968&bbsId=B0000011&searchCnd=1&searchWrd=&section=&sdate=2011-03-01&edate=2011-04-10&useAt=&replyAt=&menuNo=200067&viewType=&delCode=0&option1=&deptId=&pageIndex=1

211) 국가정보원 보도자료, http://www.nis.go.kr/jsp/board/notice.do?method=view&cmid=11510&content_number=7855&page=5

국가정보원이 해당 사건이 북한의 소행이라고 인정한 것은 2009년 10월 29일 비공개 국회 정보위 국정감사에서였다. 이에 대해 국내 주요 언론[212] 및 북한 전략센터[213]에서는 당시 국정원장의 발언 등을 인용해 "공격경로를 추적한 결과 중국에서 선을 임차해 쓰는 북한 체신성 IP가 확인[214]"되었으며, "구체적으로 답변하는 것은 국가적 전략을 노출하는 것[215]"이라며 신중한 태도를 취했다고 보도했다.

제2절 한국 및 미국의 사이버테러 대응정책

1. 한·미 사이버테러 대응: 수사

가. 미국의 사이버테러 수사 기관

1) 미국 연방수사국(FBI)

FBI는 미국 주요 수사기관으로서 사이버보안에 대한 위협 제지를 FBI의 주요 임무로 인식하고 있다.[216] 또한 2003년 대통령 국가 사이버공간 보안 전략에서도 미국 법무부와 FBI가 사이버범죄 수사 및 기소를 위한 노력을 주도함[217]을 명시했다.[218]

이에 따라 FBI는 미국 내에서 국내 정보기관 협력조정, 미국 국토안보부 지원, 미국 법 집행기관과 대응 노력을 주도하고 있으며, 국외에서는 미 대사관 등을 통해 기타 국가와의 협력 및 상호사법공조 강화의 노력을 기울인다.[219] 협력 중인 국내 정보기관으로는 미국정보공동체(U.S. Intelligence Community, USIC), 국가사이버수사공동

212) 서울신문, http://www.seoul.co.kr/news/newsView.php?id=20091031006015; 뉴스코리아, http://www.newskorea.info/news/articleView.html?idxno=4303; 아이뉴스24, https://news.inews24.com/php/news_view.php?g_serial=454146&g_menu=020200 등.
213) 북한전략센터, NKSC뉴스, http://www.nksc.co.kr/bbs/board_view.php?bbs_code=bbsIdx2&num=5573&page=137&keycode=&keyword=&c1=&c2=&sub_code=
214) 서울신문, http://www.seoul.co.kr/news/newsView.php?id=20091031006015
215) 뉴스코리아, http://www.newskorea.info/news/articleView.html?idxno=4303
216) FBI 웹사이트, https://www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity-1
217) The Department of Justice and the FBI lead the national effort to investigate and prosecute cybercrime.
218) The National Strategy to Secure Cyberspace, February 2003, 16쪽. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf
219) FBI 웹사이트, https://www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity-1

대응팀(National Cyber Investigative Joint Task Force, NCIJTF) 등이 있다.

또한 FBI는 대응 체제를 갖추기 위해 2002년 사이버국(Cyber Division)을 신설하였다.[220]

2) 미국 국토교통부 (DHS)

미국 국토교통부는 사이버안보관련 다음과 같은 대응체계를 갖추고 있다. 즉 사이버사건 발생 시 국토교통부는 피해 기관에 대한 지원, 주요 사회기반시설에 대한 잠재 영향 분석, 법집행 협력기관과 책임자 수사, 중대한 사이버사건에 대한 국가대응 체제 조정을 담당한다.[221]

또한 국토교통부는 사이버 및 통신 통합의 가교 역할을 하는 국가사이버안보 및 통신 통합센터(National Cybersecurity and Communications Integration Center, NCCIC)를 통해 24시간 실시간 감시, 사건 대응을 담당하고 있다. 뿐만 아니라 NCCIC의 미국 컴퓨터비상태세팀(United States Computer Emergency Readiness Team, US-CERT)에서 국가 네트워크를 대상으로 하는 범죄를 저지하기 위한 최신 네트워크 및 디지털 미디어 분석 전문지식을 갖추고 있다.[222]

3) 미국 대통령경호실(Secret Services)

미국 대통령경호실도 사이버범죄 관련 수사를 담당하고 있다. 비밀 검찰국은 이를 컴퓨터 기반 범죄(computer-based crimes)로 정의하고, 온라인 뱅킹 등 금융 분야부터 초국가 조직범죄에 이르는 부문을 관장하고 있다.

특히 사이버 작전과(Cyber Operations)[223]를 두고 있다. 사이버 작전부에 대해서는 다음과 같이 설명하고 있다.[224]

---

220) FBI 웹사이트, https://www.fbi.gov/news/testimony/responding-to-the-cyber-threat

221) When cyber incidents occur, the Department of Homeland Security (DHS) provides assistance to potentially impacted entities, analyzes the potential impact across critical infrastructure, investigates those responsible in conjunction with law enforcement partners, and coordinates the national response to significant cyber incidents. DHS 웹사이트, http://www.dhs.gov/cyber-incident-response

222) DHS 웹사이트, http://www.dhs.gov/cyber-incident-response

223) 대통령경호실 웹사이트, http://www.secretservice.gov/investigation/

224) 대통령경호실 웹사이트, http://www.secretservice.gov/investigation/

선진기술과 인터넷의 결합으로 미국 금융기관 및 주요 사회기반시설을 대상으로 한 사이버범죄가 늘고 정교해졌다. 오늘날 범죄 동향은 이메일 피싱, 계정 탈취, 멀웨어, 해킹 공격 및 네트워크 침입 등으로 인한 중대한 데이터 손상을 포함한다. 국가의 금융 인프라를 사이버 및 금융 범죄로부터 보호하기 위하여 비밀감찰국은 다음을 포함하는 다각화된 전략을 취한다:

전자범죄특수요원프로그램(Electronic Crimes Special Agent Program, 이하 ECSAP)을 통한 선진 컴퓨터 포렌식 및 네트워크 침입 수사 훈련 진행으로 특수요원 역량강화; 해외지부 및 ECSAP 요원의 국제기구 파견을 통한 국제 법집행기관 체결국과 협력관계 극대화;휴대전화, 사기 기기, GPS 기기 등을 포함하는 모바일 기기로부터의 증거 추출을 위한 최신 기술과 관련된 교육훈련, 시험 및 연구 제공; 컴퓨터포렌식기관(National Computer Forensics Institute)에서 협력 국가 및 지역 법집행기관 대상 컴퓨터 기반 훈련 제공을 통한 수사역량 강화; 46개 금융 범죄 대응팀 및 39개 전자 범죄 대응팀과의 네트워크를 통한 협력.[225]

나. 한국의 사이버테러 수사 기관

1) 2014년 12월 한국수력원자력 해킹 합동수사단

한국수력원자력 해킹 사건 발생 후 정부는 합동수사단을 만들어 수사를 착수했다. 합수단 보도자료에 따르면 합수단은 국가정보원, 대검 과학수사부·국제협력단, 경찰

225) As a result of the amalgamation of advanced technology and the Internet, both the quantity and sophistication of cybercrimes targeting U.S. financial institutions and critical infrastructure have increased. Today, criminal trends show an increased use of phishing emails, account takeovers, malicious software, hacking attacks and network intrusions resulting in significant data breaches. To protect the nation's financial infrastructure from cyber and financial criminals, the Secret Service has adopted a multipronged approach that includes: Providing advanced computer forensics and network intrusion investigation training to enhance the skills of special agents through the Electronic Crimes Special Agent Program (ECSAP); Maximizing partnerships with international law enforcement counterparts through overseas field offices and by forward deploying ECSAP agents to international working groups; Providing training, examination services and research into cutting edge processes to extract potential evidence from mobile devices to include cellular phones, skimming devices and GPS units; Providing computer-based training to state and local law enforcement partners to enhance their investigative skills at the National Computer Forensics Institute; Collaborating through an established network of 46 Financial Crimes Task Forces and 39 Electronic Crimes Task Forces

청 사이버안전국, 방송통신위원회, 한국인터넷진흥원, 안랩(AhnLab) 등과 공조하여 수사를 진행하였고, 경유지 IP 서버 소재지 국가들(미국·중국·일본·태국·네덜란드 등)과도 국제수사공조를 통해 범인을 추적[226]했다.

2) 2013년 3월 주요 방송사 및 금융사 전산망 마비 합동대응팀

2013년 3월 20일 전산망 장애 사건에서는 민·관·군 합동대응팀이 구성되었다. 또한 3월 20일 방송통신위원회, 행정안전부, 국방부, 국가정보원 등 10개 부처가 '사이버위기 평가회의'를 개최하여 사이버위기 주의경보를 발령하였으며, 정부합동조사팀이 방송사, 신한은행 및 LG U+를 방문하여 현장조사를 진행[227]하였다.

또한 사이버 공격과 관련한 대응체계에 컨트롤 타워 부재 문제를 지적하는 기사[228]에 대하여 국가 사이버 위기 대응체계의 구축·운용 중임을 밝혔다. 다음은 그 해명 내용이다.[229]

> 정부는 DDoS 및 해킹 등 사이버 공격에 의한 침해사고가 발생할 경우, 국가사이버 안전관리규정[230]에 따라 "범정부 사이버 위기 대책본부"를 구성하여 체계적으로 대처하고 있습니다. 이번 3.20일 전산망 마비 사고의 경우에도 정부는 초기부터 국정원과 방통위를 중심으로 대책본부를 구성하고 민·관·군 합동 조사반을 현장에 급파하는 등 긴급 대응하고 있으므로, 사이버 침해사고 콘트롤 타워가 없어 대처방안이 부재하다는 보도 내용은 사실과 다름을 알려드립니다.

---

226) 2015년 3월 17일 합수단 보도자료. http://www.spo.go.kr/_custom/spo/_common/board/download.jsp?attach_no=154704

227) 방송통신위원회 보도자료, http://www.kcc.go.kr/user.do?mode=view&page=A05030000&dc=K05030000&boardId=1113&cp=72&boardSeq=36093

228) 아시아경제, http://www.asiae.co.kr/news/view.htm?idxno=2013032111110012208; 헤럴드경제, http://biz.heraldcorp.com/common_prog/newsprint.php?ud=20130321000487

229) 방송통신위원회 보도자료, http://www.kcc.go.kr/user.do?mode=view&page=A05030000&dc=K05030000&boardId=1113&cp=72&boardSeq=36100

230) 이 훈령은 국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적으로 한다. 국가사이버안전관리규정, 대통령훈령 제 316호, 2013.9.2., 일부개정, http://www.law.go.kr/admRulSc.do?menuId=1&query=%EA%B5%AD%EA%B0%80%EC%82%AC%EC%9D%B4%EB%B2%84#liBgcolor0

3) 2013년 6월 사이버테러 사건 합동대응팀

2013년 3월 20일 언론 및 금융사 전산망 마비를 뒤따라 6월 25일 발생한 사이버 공격도 민관군 합동대응팀[231]이 구성되어 수사가 진행되었다. 2013년 7월 16일 '6.25 사이버공격 조사 결과' 발표 자료에 따르면 민관군 합동대응팀은 악성코드의 조기 발견 및 백신 보급으로 피해 확산을 방지하였고, 사이버 대피소 가동 등을 확대하여 서버 복구를 긴급 지원하는 등 피해를 최소화하였다.[232]

또한 대응체계에 관해서는 7월 4일 마련한 국가사이버안보종합대책[233]을 바탕으로 컨트롤 타워인 청와대를 중심으로 국정원과 미래부 등 정부부처 간 위협정보 적시 공유 등 사이버위협 대응체계를 확립하고, 사이버 공격에 대한 대응 기술 연구 및 전문인력 확충 등 사이버 안보기반을 지속적으로 확충해 나갈 예정임을 밝혔다.[234]

4) 2011년 4월 농협 해킹사건 수사공조

2011년 4월 농협 해킹과 관련해서는 금융사에 발생한 사건인 만큼 금융당국도 관여했다. 방송통신위는 제46차위원회회의 결과 브리핑 자리에서 해당 사건에 대한 대응으로 국가 사이버안보 마스터플랜[235] 수립을 밝혔다. 또한 2011년 5월 11일 15개 관계부처가 참석한 국가사이버안전 전략회의를 진행하여 대응하였음을 밝혔다.[236]

---

231) 합동대응팀은 미래·국방·안행·법무(검찰)부, 금융위, 국정원, 경찰청, 국내보안업체(안랩·하우리·이글루시큐리티·윈스테크넷·KT 등) 및 한국인터넷진흥원(KISA) 등 18개 기관 전문가로 구성. 미래창조과학부 웹사이트, http://www.msip.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1212563

232) '6.25 사이버공격 조사 결과' 발표, 대한민국정책포털, http://ebrief.korea.kr/open.brf.EBSB0021.selectBriefPopup.laf?brpId=37730

233) 사이버안보 강화를 위해 1. 사이버위협 대응체계 즉응성 강화 (Prompt), 2. 유관기관 스마트 협력체계 구축 (Cooperative), 3. 사이버공간 보호대책 견고성 보강 (Robust), 4. 사이버안보 창조적 기반조성 (Creative)를 골자로 하는 박근혜 정부의 사이버안보 마스터 플랜. 대한민국정책포털, http://www.msip.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1212488

234) '6.25 사이버공격 조사 결과' 발표, 대한민국정책포털, http://ebrief.korea.kr/open.brf.EBSB0021.selectBriefPopup.laf?brpId=37730

235) 국가사이버안전센터, service1.nis.go.kr/safe/120802_masterplan_kr.pdf

236) 방송통신위원회, http://www.kcc.go.kr/user.do?mode=view&page=A05030000&dc=K05030000&boardId=1113&cp=176&boardSeq=31663

5) 2011년 3월 DDoS 공격 수사공조

2011년 3.4 DDoS 수사는 경찰청이 유관기관의 협조를 통해 진행하였다. 또한 국정원이 국가 사이버테러대응센터를 가지고 있으므로 정부 및 공공부문에서는 국정원이 필요한 IP 주소 확인을, 그 주소를 가지고 한국인터넷진흥원이 IP 차단을 하는 방식으로 공격을 줄였다. 추가 감염을 막을 수 있는 백신을 보급하고, 개인 사용자들에게 피해 방지를 할 수 있는 방법을 알렸다.[237]

6) 2009년 7월 DDoS 대란 합동대응팀

2009년 7.7 DDoS 대란에 대해서는 국정원의 언로 보도자료를 통해 정부가 합동대응팀을 구성하였으며, 정보보호진흥원과 협조하였음을 알 수 있었다. 또한 대응 노력으로는 사이버 위기경보 단계 상향조정, 민간부문인 안철수 연구소와 하우리 등 민간 전문업체에 악성프로그램의 샘플 및 분석결과를 공유하는 것 등 공조 체제를 가동한 것을 확인할 수 있다.[238]

또한 국가정보원의 보도자료[239]에 따르면 정부는 7월 8일 국정원 주관으로 청와대, 총리실, 방통위, 국방, 외교부, 금융위 등 12개 기관으로 구성된 '사이버 안전실무회의'를 소집하여 DDoS 사고 개요와 피해실태 및 조치사항을 설명하고 비상대비태세를 점검하고 재발방지대책을 논의 하였으며, 미국 수사기관과 협력을 통해 국정원의 악성 프로그램 샘플과 분석자료를 제공하는 등 우방국과의 공조를 강화하였음을 알 수 있다.

---

237) 대한민국정책포털,
http://ebrief.korea.kr/open.brf.EBSB0021.selectBriefPopup.laf?brpId=26225

238) 국가정보원,
http://www.nis.go.kr/jsp/board/notice.do?method=view&cmid=11510&content_number=7853&page=5

239) 국가정보원,
http://www.nis.go.kr/jsp/board/notice.do?method=view&cmid=11510&content_number=7853&page=5

제5장

KOREAN INSTITUTE OF CRIMINOLOGY

결 론

김 한 균

제5장

결 론

2015년의 세계는 지구상 어느 한 나라도 테러에서 자유로울 수 없는 유비쿼터스 테러(ubiquitous terror)의 시대를 맞고 있다. 도처에서 때와 장소를 가리지 않고 테러 공격이 벌어지고 있는 것이다. 현실 세계뿐만 아니라 사이버공간에서는 이미 유비쿼터스 테러가 이루어 지고 있다. 따라서 사이버테러의 문제는 국가적 대책 뿐만 아니라 국제적 지역적 협력체계를 통한 통제와 방지가 대단히 중요한 의미를 가진다.

1. 한·미 사이버테러 대응정책의 의미

현 정부의 「동북아 평화협력 구상」은 이른바 비전통 연성 안보 의제로서 원자력 안전, 에너지 안보, 환경·기후변화, 재난 구호, 사이버 스페이스를 제시하고 있다. 이러한 5대 중점분야외에도 다양한 협력사업의제를 발굴하고 그 기획을 활성화하고자 하는데 실천적 의미가 있다.

따라서 일차적 의제에 한정될 것이 아니라, 동북아 지역 다양한 현안에 있어서 다자간 협력 문화정착과 협력 메카니즘 제도화 방안을 구상하는 중요한 계기로 삼아야 것이다. 특히 사이버공간에서의 평화와 협력의 증진은 동북아평화협력구상의 중요한 의제이기도 하면서, 동북아 지역국가는 아니지만 주요이해관계국의 하나인 미국과 한국의 공동관심사이기도 하다.

사이버공간에서의 평화와 협력이라는 연성안보의제는 사이버테러의 영역, 즉 형사정책의 영역에서는 진성안보의제가 된다. 특히 동북아지역에서 한국과 미국의 공동현안으로서 사이버테러는 특히 중요한 의미를 가진다. 왜냐하면 동북아 평화협력구상 실현의 대상인 중국과 북한이 오히려 사이버테러의 진원지로서 지목받고 있기 때문

이다. 따라서 미국과 한국은 동북아지역내 사이버공간을 너머 국가들간의 정치경제적 공간에서 사이버안전과 사이버안보를 위협하는 요소를 최소화하면서 위협요인을 평화요인으로 바꾸어 나가기 위해 공동의 노력을 경주해야 하는 과제를 함께 짊어지고 있는 실정이다.

이에 본 연구는 사이버범죄와 더 포괄적인 사이버안보의 측면에서 동북아지역내 사이버테러 관련국 및 그 실태에 대한 논의기반을 제공하고자 수행되었다.

2. 사이버테러 대응정책 협력의 전망과 과제

본 연구는 한국과 미국의 사이버테러 관련 형사사법 정책관련 문헌자료와 확보가능한 북한의 사이버테러 위협과 대응정책에 대한 기초자료를 통하여 한국과 미국의 사이버테러 관련 형사사법정책을 분석하였다.

이는 향후 안보협력의 가장 중요한 동반자인 한국과 미국 간의 사이버안보 정책협력의 기반구축을 위해 양국 주요 형사정책 연구기관들의 공동연구를 위한 틀을 제시하기 위함이다. 또한 미국 연방법무부, 미국사법정책연구원, 미국 뉴욕대 안보법센터의 사이버안보 관련 정책과 연구동향을 정리 분석하였다. 이들 기관은 향후 한국형사정책연구원의 한미 사이버테러 대응정책 협력방안 연구에서 주요한 협력기관이 될 것으로 기대되기 때문이다.

특히 미국 국립사법정책연구원은 한국형사정책연구원과 함께 유엔범죄방지및형사사법 프로그램 네트워크 소속기관으로서 2015년 제13차 유엔범죄방지 및 형사사법총회에서 공동으로 사이버범죄 워크숍을 주관한 바 있다.[240] 또한 2015년 11월 미국범죄학회(2015 American Society of Criminology Meeting in Washington, DC.)에서 사이버보안을 주제로 공동 특별세션 (A Comparative Look at Cybercrime)을 기획했었다. 이러한 협력관계를 기초로 삼아 향후 한국과 미국 형사정책 연구기관간 사이버보안 분야 공동연구를 강화해나갈 계획이다.

---

240) UNODC, Background paper on the Workshop on strengthening crime prevention and criminal justice responses to evolving forms of crime such as cybercrime and trafficking in cultural property, including lessons learned and international cooperation, A/CONF.222/12, 2015

참고문헌

1. 국내문헌

김일수, 윤해성, 윤민우, Freilich Joshua, Chermak Steven and Morris G. Robert (2012), 사이버 테러의 동향과 대응 방안에 관한 연구, 한국형사정책연구원

김도승 (2009), 사이버위기 대응을 위한 법적 과제 - 미국의 사이버위기 대응체계 현황과 시사점을 중심으로, 방송통신정책 제21권 제17호

강석구, 이원상 (2013), 사이버범죄 관련 법령정비 방안연구, 한국형사정책연구원

강수진 (2013), 국가 사이버범죄 대응전략 설계, 경찰청 연구용역

김광진 (2003), 해킹 패턴과 윈도우 보안 전략, 한빛미디어

김유향(2015). 중국「네트워크안전법(안)의 주용 내용과 함의」. 이슈와 논점 제1083호. 국회입법조사처

강은영, 이성식 (2010), 약물남용 실태 및 의식에 관한 연구, 한국형사정책연구원

국가 사이버안전 관리에 관한 법률안(1904286).

국가 사이버테러 방지에 관한 법률안(1904459).

국가정보원(2009). 국정원, 언론에「7.7 사이버공격」관련 신중보도 당부. http://www.nis.go.kr/jsp/board/notice.do?method=view&cmid=11510&content_number=7855&page=5. 2015.11.15.방문.

곽병선 (2015), 사이버테러 대응을 위한 법체계 검토, 법학연구 제59호

권덕근 (2008). 마약 등 약물사범에 대한 치료보호제도 연구. 행정안전부 교육훈련정보센터.

대한민국정책포털. 6.25 사이버공격 조사결과 발표. http://ebrief.korea.kr/open.brf.EBSB0021.selectBriefPopup.laf?brpId=37730. 2015.11.15.방문.

배소진(2013). [일문일답] "北, 6.25사이버공격 통해 개인정보 유출 추정". 머니투데이. http://news.mt.co.kr/mtview.php?no=2013071616161216589. 2011.11.15.방문.

박대한(2011). 보안업계 “농협 北 사이버테러 근거 약하다”. 연합뉴스. http://www.yonhapnews.co.kr/economy/2011/05/03/0301000000AKR20110503096700017.HTML. 2011.11.15.방문.

보안뉴스(2015). [中 ‘사이버 보안법’ 뭘 담았나 ①] 네트워크·인터넷 보안 총망라. http://www.boannews.com/media/view.asp?idx=47184&kind=3. 2011.11.15.방문.

북한전략센터(2009). 청와대·국방부 ‘DDos 테러’ 진원지는 북한 체신성. http://www.nksc.co.kr/bbs/board_view.php?bbs_code=bbsIdx2&num=5573&page=137&keycode=&keyword=&c1=&c2=&sub_code. 2015.11.15.방문.

정완 (2013), 한·미 사이버보안 법제 동향에 관한 고찰, 경희법학 제48권 제3호

사이버센터(2011). 3.4 DDos 사건의 공격자는 7.7 DDos와 동일범. 사이버경찰청. http://www.police.go.kr/portal/bbs/view.do?nttId=7968&bbsId=B0000011&searchCnd=1&searchWrd=&section=&sdate=2011-03-01&edate=2011-04-10&useAt=&replyAt=&menuNo=200067&viewType=&delCode=0&option1=&deptId=&pageIndex=1. 2015.11.15.방문.

사이버위협정보 공유에 관한 법률안(의안번호 15185).

사이버테러 방지 및 대응에 관한 법률안(15777).

서울중앙지방검찰청 첨단범죄수사 제2부(2011). 치밀하게 준비된 사이버 테러. http://www.slideserve.com/cahil/5682386. 2015.11.15.방문.

신종환(2013). Internet & Security Focus. 2013년 9월호.

안성진, 이경호, 박원형 (2014), 보안관제학, 이한미디어.

임종인 (2013). 3.20 대란과 국가사이버 위기관리법의 과제. 국가사이버위기 관리제정을 위한 공청회 자료집.

오길영 (2014), ‘사이버테러’대응체계의 문제점과 개선방향, 민주법학 제54호

이원상 (2008), ‘사이버’개념을 통한 사이버 모욕죄의 고찰과 대안, 한국형사정책연구원

윤해성 (2012), 사이버 테러의 동향과 대응 방안에 관한 연구, 한국형사정책연구원

한국과학기술단체총연합회(2011). 과학과 기술. http://kofst.or.kr/kofst/PDF/2011/n6s505/GGDCBE_2011_n6s505_44.pdf. 2015.11.15.방문.

한국방송통신전파진흥원(2013). DDos 지속공경 비교 분석 및 대응방안 연구. 방송통신기술 이슈&전망. 2013년 제23호.

한국수력원자력(2015). 한수원 사이버테러 사건 중간수사결과. http://www.spo.go.kr/_custom/spo/_common/board/download.jsp?attach_no=154704

한국인터넷진흥원. Bimonthly-5호. 미국 법무부(DoJ), 사이버범죄 소탕 및 보안 강화를 위한 조사팀 신설. http://www.kisa.or.kr/uploadfile/201412/201412301110107707.pdf. 2015.11.15.방문.

한국인터넷진흥원. 해킹방지원크샵 2013년 주요 침해사고 사례와 대응. http://www.kisa.or.kr/uploadfile/201312/201312041443047984.pdf. 2011.11.15.방문.

허영호, 검토보고서, 2014, 71~72쪽(http://likms.assembly.go.kr/bill/jsp/BillDetail.jsp?bill_id=PRC_P1D3O0N3T2Y6A1K7D5A5E5J8Q2M5Q3, 2015.11.10. 방문).

2015년 국가정보보호백서

2. 국외문헌

Alexander Moens, Syechelle Cushing and Alan W. Dowd(2015). Cybersecurity Challenges. Fraser Institute.

Alberto R. Gonzales R. Alberto, Schofield B. Regina and Hagy W. David(2007). Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors. U.S. Department of Justice Office of Justice Programs.

Ashcroft John, Daniels J. Deborah and Hart V. Sarah(2004). Forensic Examination of Digital Evidence: A Guide for Law Enforcement Investigations Involving the Internet and Computer Networks. U.S. Department of Justice Office of Justice Programs.

CISCO(2009). DDos 공격 비상, 어떻게 대처할 것인가? https://www.cisco.com/web/KR/learning/events/down/July_DDoS_Webseminar.pdf. 2011.11.15.방문.

Christopher Munsey(2013). Economic Espionage: Competing For Trade By Stealing Industrial Secrets. FBI Law Enforcement Bulletin. https://leb.fbi.gov/2013/october-november/economic-espionage-competing-for-trade-by-stealing-industrial-secrets. 2015.11.15.방문.

Center for Strategic and International Studies(2015). CSIS/DOJ Active Cyber Defense Experts Roundtable. http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/05/18/CSIS%20Roundtable%205-18-15.pdf. 2015.11.15.방문.

Copes Heith, Vieraitis Lynne(2007). Identity Theft: Assessing Offenders' Strategies and Perceptions of Risk. National Institute of Justice.

Department of Homeland Security. The Investigative Mission. http://www.secretservice.gov/investigation/. 2015.11.15.방문.

FBI Nationl Press Office(2014). Undate on Sony Investigation. https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation. 2015.11.15.방문.

FBI. Addressing Threats to the Nation's Cybersecurity. https://www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity-1. 2015.11.15.방문.

Goodison E. Sean, Davis C. Robert and Jackson A. Brian(2015). Digital Evidence and the U.S Criminal Justice System. The RAND Corporation.

Goodison E. Sean, Davis C. Robert and Jackson A. Brian(2015). Digital Evidence and the U.S Criminal Justice System. The RAND Corporation.

Holder H. Eric, Robinson O. Laurie and Rose, Kristina(2009). High Priority Criminal Justice: Technology Needs. U.S. Department of Justice Office of Justice Programs.

Homeland Security(2015). Cyber Incident Response. http://www.dhs.gov/cyber-incident-response. 2015.11.15.방문.

Homeland Security. Enhanced Cybersecurity Services. http://www.dhs.gov/sites/default/files/publications/ECS%20Fact%20Sheet%2007.30.15.pdf. 2015.11.15.방문.

Homeland Security(2013). Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity & Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience. https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf. 2015.11.15.방문.

James Andrew Lewis(2008). Securing Cyberspace for the 44th Presidency. the CSIS Commission on Cybersecurity for the 44th Presidency.

Jose Pagliery(2014). What caused Sony hack: What we know now. CNN. http://money.cnn.com/2014/12/24/technology/security/sony-hack-facts/. 2015.11.15.방문.

Joseph M.. Demarest(2013). FBI Testimony. Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism. https://www.fbi.gov/news/testimony/responding-to-the-cyber-threat. 2015.11.15.방문.

Judith H. Germano and Zachary K. Goldman(2014). After the Breach: Cybersecurity Liability Risk. http://www.lawandsecurity.org/Portals/0/Documents/CLS%20After%20the%20Breach%20Final.pdf. 2015.11.15.방문.

Judith H. Germano(2014). Cybersecurity Partnership: A New Era of Public-Private Collaboration. http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf, 2015.11.15.방문.

Kim Zetter(2014). SONY got hacked hard: What we know and don't know so far. Wired. http://www.wired.com/2014/12/sony-hack-what-we-know/. 2015.11.15.방문.

Law Enforcement Cyber Center. FBI Cyber Shield Alliance. http://www.iacpcybercenter.org/resource-center/fbi-cyber-shield-alliance/. 2015.11.15. 방문.

Lewis Marieke, Miller Patrick and Buchalter R. Alice(2009). Internet Crimes Against Children: A Matrix and Summary of Major Federal and Select State Case Law. National Institute of Justice.

Mark Seal(2015). An Exclusive Look at Sony's Hacking Saga. Vanity Fair. http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg. 2015.11.15.방문.

Martin Fackler, Brooks Barnes and David E. Sanger(2014). Sony's International Incident: Making King Jong-un's Head Explode. The New York Times. http://www.nytimes.com/2014/12/15/world/sonys-international-incident-making-kims-head-explode.html?_r=2. 2015.11.15.방문.

Mukasey B. Michael, Sedgwick L. Jeffrey and Hagy W. David(2008). Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition. U.S. Department of Justice Office of Justice Programs.

National Institute of Standards and Technology(2002). Detailed Overview. http://csrc.nist.gov/groups/SMA/fisma/overview.html. 2015.11.15.방문.

National Institute of Standards and Technology(2014). Framework for Improving Ctirical Infrastructure Cybersecurity Version 1.0. NIST 2014.

Newman R. Graeme and McNally M. Megan(2007). Identity Theft-A Research Review. National Institute of Justice

Office of the US Intellectual Property Enforcement Coordinator(2013). 2011 U.S. Intellectual Property Enforcement Coordinator Annual Report on Intellectual Property Enforcement.

Office of Public Affairs of the Department of Justice(2014). U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commerical Advantage. http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hack

ers-cyber-espionage-against-us-corporations-and-labor. 2015.11.15. 방문.

Picarelli T. John(2010). Expert Working Group Report on International Organized Crime. National Institute of Justice. http://www.lawandsecurity.org/Portals/0/Documents/whitepaper_final.pdf. 2015.11.15.방문.

Randal Milch and Zachary Goldman(2015). From the War Room to the Board Room? Effectively Managing Cyber Risk without Joining the Front Lines.

StaySafeOnline. About NCSA. https://www.staysafeonline.org/about-us/. 2015. 11.15.방문.

StaySafeOnline. National Cyber Security Awareness Month. https://www.staysafeonline.org/ncsam/about. 2015.11.15.방문.

SONY Pictures(2014). http://oag.ca.gov/system/files/12%2008%2014%20letter_0.pdf. 2015.11.15.방문.

The Center on Law and Security. Terrorist Trial Report Card: U.S. Edition. http://www.lawandsecurity.org/Portals/0/documents/09_TTRCComplete.pdf. 2015.11.15.방문.

US-CERT United States Computer Emergency Readiness Team. Critical Infrastructure Cyber Community Voluntary Program. https://www.us-cert.gov/ccubedvp. 2015.11.15.방문.

U.S. Government Printing Office(2014). 2014 Report to Congress of the U.S.-China Economic And Security Review Commission.

U.S. Department of Justice(2009). Solicitation: Criminal Justice Electronic Crime Technology Center of Excellence 2009.

United Nationa Office on Drugs and Crime(2015). Background paper on the Workshop on strengthening crime prevention and criminal justice reponses to evolving forms of crime such as cybersrime and trafficking in cultural property, including lessons learned and international cooperation 2015, A/CONF.222/12.

White House. Foreign Policy; Cybersecurity. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity. 2015.11.15.방문.

White House. Foreign Policy; The Comprehensive National Cybersecurity Initiative. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative. 2015.15.방문.

White House(2003). The National Strategy to Secure Cyberspace. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf. 2015.11.15.방문.

Zweig M. Janine, Dank Meredith, Lachman Pamela and Yahner Jennifer(2013). Technology, Teen Dating Violence and Abuse, and Bullying. National Institute of Justice.

Department of Justice(2014). Organization, Mission & Functions Manual: Attorney General, Deputy, and Associate. http://www.justice.gov/jmd/organization-mission-and-functions-manual-attorney-general#asg. 2015.11.15.방문.

Abstract

UN·International Cooperation and Research for Crime Prevention (XI)

Criminal Justice Policy against Cyber-Terrorism in Korea and the US

Kim, Han-kyun · Cho, Min-jeong,
Pak, So-young · An, Su-jung

This research is based on the achievements of Korean Institute of Criminology's international cooperation projects in the field of cybercrime, cyber security and technological cooperation, and aims to provide fundamental discussion resources on cybercrime and comprehensive aspects of cyber security, especially on the relevant countries such as China and North Korea. Furthermore, it attempts to suggest the framework of joint projects that the criminal policy research institutes in Korea and the U.S could conduct in order to establish the ground for cooperative cyber security policies in the two countries that are significant partners in security cooperation.

Chapter II analyzes Korean criminal justice policies on cyber terror and addresses current legal system and countermeasures on cyber terrorism and the legislature trend. Chapter III includes analysis of the current U.S criminal justice policies on cyber terror and the cyber security policies against China. Also, the Department of Justice, National Institute of Justice and the Center on Law and Security at New York University's research trends and relevant policies will be analyzed.

In Chapter IV, the actual cases of North Korean cyber terror threats as well as countermeasures against the threat will be presented and analyzed. This includes the description of cyber terror attacks that were allegedly committed by North Korea and the result of investigations. In addition, considerations on cooperative countermeasures that Korea and the U.S could take against North Korean cyber security threats will be indicated

연구총서 15-B-11

한·미 사이버테러 대응정책 협력방안 연구

발 행 | 2015년 12월
발 행 처 | 한국형사정책연구원
발 행 인 | 김 진 환
등 록 | 1990. 3. 20. 제21-143호
주 소 | 서울특별시 서초구 태봉로 114
전 화 | (02)575-5282
홈 페 이 지 | www.kic.re.kr
정 가 | 7,000원
인 쇄 | 삼신인쇄 (02)2285-6478
I S B N | 978-89-7366-938-7 93360