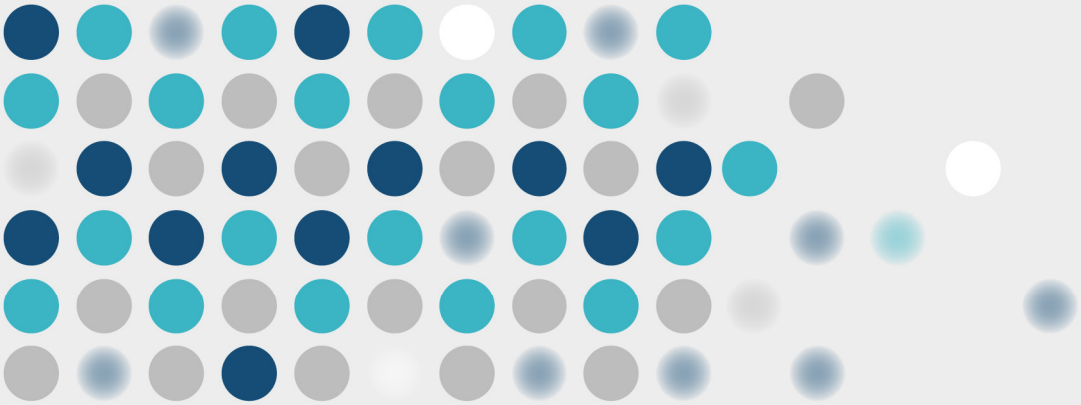
연구총서 15-B-05

동북아평화협력구상 실현을 위한 동북아지역 형사사법 협력방안연구 3

동북아 사이버범죄 및 보안 지역협력방안

김한균 | 고려대학교 사이버법센터



KIC 한국형사정책연구원
KOREAN INSTITUTE OF CRIMINOLOGY

발간사

본 보고서는 「동북아 평화협력 구상 실현을 위한 동북아지역 형사사법 협력방안 연구」 8가지 세부과제 중의 하나로 기획된 연구성과로서, 초국경적 성격을 갖는 사이버안전 및 사이버범죄 문제에 대응하기 위한 국가간 협력 대응체계를 마련하는데 목적이 있습니다.

우리 정부는 외교·안보정책의 한 축으로 「동북아 평화협력 구상(Northeast Asia Peace and Cooperation initiative)」을 제시하여, 동북아 지역의 대립과 갈등 구도를 다자간 대화와 협력의 질서로 전환함으로써 역내의 지속가능한 평화와 번영의 기반을 만들고자 노력하고 있습니다. 본 비교법적 연구를 통해 미국을 포함한 동북아시아 국가들의 협력을 통한 지역내 사이버안전을 위한 공동 대응에 기여할 것으로 기대합니다.

연구를 성실히 수행해준 고려대학교 사이버법센터장 박노형 교수와 정명현, 안민호 박사, 그리고 김한균 국제협력센터장의 노고에 감사드립니다.

2015년 12월

한국형사정책연구원

원장 김 진 환

목 차

표 차례

그림 차례

국문요약

1. 본 연구는 2015년도 「국제 범죄방지를 위한 UN·국제협력 및 연구 사업」의 세부과제로서, 정부의 동북아평화협력구상 실현을 위한 동북아 지역 형사사법 협력사업의 하나로 기획되었다. 한국형사정책연구원 국제협력사업의 일환으로 중국, 일본, 러시아 등 동북아 주요국가와의 형사사법분야 지역협력 연구사업을 본격화하면서, 향후 사이버안전분야에서 동북아지역 형사사법 협력방안을 발전적으로 제시하는데 목적이 있다.

2. 연구의 의의와 방법

사이버공간의 문제는 초국경적 성격을 갖기 때문에 사이버안전 및 사이버범죄 문제에 대응하기 위해서는 국가간 협력 대응체계를 마련하는 것이 중요하다. 현재 우리 정부는 미국을 포함한 동북아시아 국가들의 대화와 협력을 통한 신뢰 프로세스를 추진하고 있으며, 동북아 지역에서 공동 대응에 대한 인식이 공유될 필요가 있다. 그러나 동북아에서는 역내 국가간 경제·사회·문화적 상호의존성의 확대 동향에 비하여 정치·안보 협력은 이에 못 미치는 '아시아 패러독스' 현상이 지속되고 있으며, 국가간 분쟁을 다룰 다자협력체제도 형성되어 있지 않다.

향후 동북아 평화협력에서 한국이 선도적 역할을 하기 위해서는 동북아 협력을 위한 사이버안전 및 사이버범죄 대응협력방안에 대한 정책 분석과 대응방안을 모색할 필요가 있다. 본 연구에서는 미국, 중국, 러시아, 일본, 한국의 사이버안전 및 사이버범죄에 대한 최근의 정책기조에 대하여 검토하고, 해당 정책이 갖는 시사점을 통하여, 한국이 동북아 지역체제에 제시할 수 있는 협력대응방안을 도출하고자 한다.

3. 동북아 주요국가의 사이버안전 및 범죄정책 비교 연구 - 미국

미국은 2011년 '사이버공간에서의 국제전략'을 통하여 사이버공간에서의 적대행위

에 대응하여 필요한 경우에 국제법에 따라 최후의 수단으로서 군사력을 이용할 수 있음을 천명하고, 사이버정책을 발전시켜 왔다.

특히 2015년에는 악의적인 사이버 위협에 대한 대응을 구체화하고 국가안보전략, 대통령 행정명령, 국방부 사이버전략을 잇달아 발표하였다. 2015년 4월 미국 오바마 대통령의 행정명령에서는 국가 또는 민간을 불문하고 미국에 대한 사이버 위협이 개시된 출처에 대하여 적극적으로 대응하도록 촉구하였다. 또한 2015년 4월 국방부에서는 2011년 '사이버공간에서의 국방부 전략'을 개정·보완하여 새로운 '국방부 사이버 전략'을 발표하였다.

미국의 사이버행정명령은 사이버위협에 대한 적극적 대응을 강화시키는 정책의 일환으로서, 광범위한 용어를 사용하여 재무부장관에게 상당한 해석의 재량을 부여하고, 동 행정명령의 제재를 받는 자의 재산의 동결과 거래를 금지한다. 사이버행정명령은 해외에서 발생하는 유해 사이버-가능 활동과 같은 사이버 위협을 통제하려는 국가관행으로서 중요한 시도이다.

미국은 연방형법의 흠결을 보완하는 컴퓨터사기남용법을 통하여 인터넷과 컴퓨터 시스템에 대한 사이버범죄를 규율하고 있다. 특히 정부 컴퓨터 등 시설에 대한 침입과 훼손 행위 및 재범행위를 중하게 처벌하고, 사이버범죄에 대한 미수 또는 모의도 금지하여 광범위하게 처벌하고 있다. 또한 경찰뿐만 아니라 국토안보부 산하기관이 사이버범죄에 대한 조사권한을 가짐으로써, 관련 기관의 상호 협조 하에 신속한 대응이 이루어지도록 하고 있다.

4. 동북아 주요국가의 사이버안전 및 범죄정책 비교 연구 - 일본

일본은 사이버안전 분야의 기본법을 제정하여 국가가 추구하는 기본이념을 제시하고, 이를 바탕으로 범국가적인 사이버시큐리티 시책을 추진하기 위한 법적 근거를 마련하였다.

2015년 9월에 신 사이버시큐리티 전략에서는 급증하고 있는 인터넷뱅킹을 이용한 범죄, 대규모 정보유출사건 등 악의적인 사이버범죄의 실태를 파악하고, 신종 수법에 대처하기 위하여 범죄 대처능력과 수사능력 향상의 필요성, 정보수집 강화, 국제협력 체제 강화의 추진을 촉구하였다. 그리고 국제사회의 평화와 안정 실현을 위해서는

사이버공간에서의 다양한 가치관을 인정하고 자율성을 존중하며, 언론과 기업행동을 법치주의로 보장하여야 함을 강조하였다.

사이버범죄 대책을 위하여 경찰청에서는 2001년부터 '종합시큐리티대책회의'를 매년 개최하고 있다. 동 회의에서는 정보시큐리티에 관한 전문가, 전기통신사업자, 컨텐츠사업자, 컴퓨터 제조판매업자, 소프트웨어산업 등 각종 사업 관련자 및 법조계, 교육계, 방범단체 등 광범위한 분야에서 의견을 교환하여 추진과제를 제시하고 있다.

5. 동북아 주요국가의 사이버안전 및 범죄정책 비교 연구 - 중국

중국은 사이버안전에 대한 관리 강화를 목적으로, 국무원 및 관할 부서의 단독 행정관할에서 중국 공산당 중앙위원회와 국무원이 공동으로 관리하는 양자관할체제로 변경하였다. 또한 인터넷 보안정책과 법령의 발전을 함께 도모하여 전국인민대표회의와 중국공산당 대표대회 결의가 법률과 정책으로 추진되고 있다.

사이버범죄에 대응하여 형법에서는 사이버안전 운행을 침해하는 행위, 사이버를 이용하여 국가안전과 사회안정을 침해하는 행위, 사이버를 이용하여 사회주의 시장경제질서와 사회관리 질서를 파괴하는 행위, 사이버를 이용하여 개인·법인 및 기타 조직의 인신, 재산 등 합법적인 권리를 침해하는 행위를 규정하여 사이버범죄에 대응하고 있다.

중국이 현재 검토 중인 사이버안전법안은 네트워크 전반을 망라한 규제 법안으로서 네트워크에 대한 통제를 강화하는 한편, 사이버 공격을 방어하고, 중국의 이용자에 관한 정보를 보호하는 정부의 역량 강화를 목표로 하고 있다.

6. 동북아 주요국가의 사이버안전 및 범죄정책 비교 연구 - 러시아

러시아의 사이버 관련 정책은 정보 인프라에 대한 물리적인 보호와 함께 정보의 흐름을 관리·통제함으로써 사이버안전을 확보하는 데 초점을 맞추고 있다. 이와 같이 러시아가 사이버공간에 대한 공권력의 개입을 통하여 사이버안전을 추구하는 정책은 전반적으로 사이버 정보의 자유로운 흐름을 중시하는 서구와 가장 중요한 차이를 보여주는 특징이라 할 수 있겠다.

사이버범죄와 관련해서 러시아의 가장 두드러지는 특징은 정부당국이 법원의 허가

없이 자신의 재량에 따라 인터넷 자원을 폐쇄시킬 수 있는 권한을 갖고 있다는 점이다. 러시아는 국내외적으로 사이버범죄에 대한 기소 압력이 증가함에 따라 최근 들어 지적재산권을 침해하는 인터넷 공유자원에 대하여 단속하는 등 점차 처벌을 강화하고 있는 실정이다.

7. 동북아 주요국가의 사이버안전 및 범죄정책 비교 연구 - 한국

한국은 사이버전은 국방부가, 사이버테러는 국가정보원이, 민간분야의 사이버공격은 미래부가 관리하는 체계를 이루고 있으며, 전체적인 컨트롤타워의 역할은 사실상 국정원이 총괄하고 있다. 여기에 청와대에 사이버안보비서관실이 설치되면서 보다 실질적인 사이버안보 컨트롤 타워를 구축할 수 있는 조직을 만들었다.

법률적인 부분에서 한국은 기본법제가 아직 마련되지 않았고 지침에 의해 업무가 수행되고 있는 실정이다. 최근에 '국가사이버안보기본법'을 제정하기 위해서 노력하고 있으며, '사이버테러방지법'도 국회에 계류 중이다. 사이버안보에 대한 기본적인 방향과 사항들을 규정하는 국가사이버안보기본법의 우선 제정이 필요하다.

사이버안전에 필수적인 전문인력과 보안장비 면에서 한국은 상대적으로 다른 선진국들에 비해 부족한 실정이다. 사이버보안 전문인력의 경우에도 인력양성에 대한 필요성은 공감하고 있는 반면, 양성 방법 등에 대해서는 아직까지 뚜렷한 결과가 도출되고 있지 않다.

8. 2014년 동북아 평화협력포럼과 사이버범죄 지역협력 논의 동향

한국은 2014년 10월에 '평화와 협력의 동북아시아로 가는 길'이라는 주제 하에 '2014 동북아협력포럼'을 개최하였고, 포 사이버스페이스 분야에 대한 논의사항은 크게 개념 정의, 국제협력, 정보 공유 및 신뢰구축, 사이버범죄, 사이버역량 강화 및 교류로 나누어볼 수 있다.

사이버스페이스 분야의 협력을 위해서는 첫째, 포괄적이고 기능적이며 비배타적인 접근, 둘째, 대화와 협의의 다자적 플랫폼과 메커니즘, 셋째, 신뢰 구축과 역량 강화, 넷째, 국가적 접근과 함께 초국가적, 국제적, 글로벌 접근, 다섯째, 개인의 권리 보호와 보장 및 국가의 투명성, 여섯째, 새로운 법률체계와 인프라 구축을 위한 비국가 행위자

의 선도적 역할, 일곱째, 민관 협력을 통한 공동의 협력과 규제가 필요하다.

9. 동북아 평화협력구상과 사이버안전을 위한 지역협력 구축의 필요성

사이버스페이스에서의 국제협력을 위해서는 국가 간 합의된 원칙, 국가 간 이해 조정과 신뢰 구축, 역량 강화 및 협력 기반의 마련을 위한 협의체가 요구된다. 또한 상호 신뢰 구축을 위해서는, ① 모든 역내 국가가 참여하는 사이버 협력체 수립, ② 공동의 행동규범 창출, ③ 역내 국가 간 동질성 및 유사성 발견, ④ 역내 국가의 사이버 역량 강화 등이 필수적이다. 이러한 과정에서 동북아 국가들은 사이버 분야에서의 연성 이슈에 대해 우선 협력을 도모함으로써, 국가간 상호 신뢰의 기반을 확보해 나갈 수 있을 것이다.

10. 동북아 평화협력을 위한 정책적 제언

첫째, 사이버공간에 기존 국제법의 적용을 위해서는 동북아 협력 차원에서 국제법의 어떠한 내용이 어떻게 적용되어야 할 것인지에 대한 논의가 이루어져야 한다.

둘째, 사이버 위협에 대한 예방과 대응 차원에서 동북아 역내 국가간 대응체계에 대한 합의가 필요하다.

셋째, 군사적 차원에서 사이버무기에 대한 관리 규칙과 통제의 문제에 대해서도 지속적인 협력이 필요하다.

넷째, 동북아 역내 국가간의 디지털 무역 관련 규범체계에 대한 국가간 협력과 논의가 필요하다.

다섯째, 거버넌스 차원에서 사이버공간에 대한 제반 문제를 논의하고 협력하는 지역협력체 구축 및 관할기관에 대한 지속적인 협의가 필요하다.

여섯째, 사이버범죄협약에의 가입에 관한 역내 국가들의 공통의 이해관계에 대한 논의가 필요하다.

11. 한국의 정책 방향 및 국제적 대응방안

첫째, 동북아평화협력포럼은 정부기관간 논의인 Track 1 외교와 민간전문가간 논의인 Track 2 외교의 차원에서 적극 활용될 수 있다.

둘째, 동북아협력포럼은 지역 내 다자간 포럼이므로, 지역협력을 보완하기 위해서는 동북아평화협력포럼 내 양자간 협력 채널의 구축이 필요하다.

셋째, 사이버범죄 분야의 기본 국제조약인 유럽평의회의 사이버범죄조약에 대한 가입을 적극적으로 검토하여야 한다.

넷째, 사이버범죄 및 보안 분야의 국내 전문가 양성이 필요하다.

다섯째, 동북아 지역 내 사이버범죄 및 보안과 관련하여, 일반 시민, 기업, 그리고 정부를 대상으로 한 사이버범죄 및 보안에 대한 인식 제고가 필요하다.

여섯째, 국내적으로 법제도의 확립이 시급하다.

일곱째, 한국형사정책연구원 내 국제협력센터의 역량을 강화하여야 한다.

여덟째, 사이버보안과 사이버범죄 대응을 위해서는 기술적 우위를 점하여야 한다. 사이버보안과 사이버범죄 대응에 있어서 '거버먼트'에서 '거버넌스'로 옮겨가고 있는 국제적인 추세도 반영해야 할 것이다.

제1장

KOREAN INSTITUTE OF CRIMINOLOGY

연구의 의의와 방법

김 한 균

제1장

연구의 의의와 방법

본 연구는 2015년도 「국제 범죄방지를 위한 UN·국제협력 및 연구 사업」의 세부과제로서, 정부의 동북아평화협력구상 실현을 위한 동북아 지역 형사사법 협력사업의 하나로 기획되었다. 또한 유엔 범죄방지 및 형사사법 프로그램(UN Crime Prevention and Criminal Justice) 소속 연구기관으로서 14개국 34개 형사정책 연구기관 및 형사사법기관과 연구교류협력 사업을 진행하고 있는 한국형사정책연구원 국제협력사업의 일환으로 중국, 일본, 러시아 등 동북아 주요국가와의 형사사법분야 지역협력 연구사업을 본격화하면서, 향후 사이버안전분야에서 동북아지역 형사사법 협력방안을 발전적으로 제시하는데 목적이 있다.

제1절 연구의 배경 및 의의

현재 우리 정부는 앞으로 국제사회에서 아시아의 역할이 더욱 증대되고, 특히 동북아시아 지역 국가들의 영향력이 커지게 될 것으로 예상됨에 따라, 미국을 포함한 동북아 국가들이 환경, 재난구조, 원자력 안전, 테러 대응 등 연성 이슈부터 대화와 협력을 통해 신뢰를 쌓고, 이를 바탕으로 점차 다른 분야까지 협력의 범위를 넓혀가기 위한 동북아 다자간 대화 프로세스를 추진하고 있다.

세계화 시대에 재난 구호, 초국가적 조직범죄, 환경, 에너지 문제 등 새로운 이슈들이 국경을 초월하여 발생하고 있기 때문에 동북아 국가들이 이러한 문제를 다루는데 있어서 '공동 대응'이 필요하다는 인식이 공유될 필요가 있고, 이를 위해 상호 신뢰를 구축하는 것이 매우 중요하게 되었다. 이와 함께 유럽이 '하나된 유럽'이라는

비전을 공유함으로써 유럽의 화해와 통합을 이룬 것처럼 동북아에서도 바람직한 공동의 미래상에 대한 청사진을 만들고 공유하는 것이 필요하게 되었다.

그러나 동북아 지역에서의 경제, 사회, 문화적인 상호의존성이 확대되고 있는 것에 반해 정치·안보 협력은 이에 못 미치는 '아시아 패러독스' 현상이 지속되고 있으며, 동북아에는 국가 간의 분쟁을 다룰 다자협력체제(multilateral cooperation mechanisms)도 형성되어 있지 않은 것이 현실이다. 이에 논의의 의제를 에너지 안보, 원자력 안전, 재난구호, 환경, 사이버스페이스의 크게 다섯 분야로 나누어 각각의 분야에서 미국을 포함한 중국, 러시아, 일본, 몽골, 북한, 남한 등의 국가들이 공동목표를 설정하고, 서로간의 이해를 높이기 위한 노력을 기울이고자 한다.

이러한 노력의 일환으로 2014년에는 10월 한국에서 '2014 동북아 평화협력 포럼'을 개최하고, 미국을 포함한 중국, 러시아, 일본, 몽골, 한국(북한은 불참)의 전문가들이 참여하여 각 분야의 당면한 문제에 대해 논의하고 서로의 이해를 높이는 작업을 시작하게 되었다.

그런데 사이버스페이스 분야의 경우 한국의 종합적인 견해가 존재하지 않으며, 특히 사이버안전이나 사이버범죄와 관련해서 체계적인 국가적 견해가 마련되어 있지 않다는 한계에 직면하고 있다. 특히 사이버스페이스의 동북아 평화협력에 있어 한국이 주도권을 행사하기 위해서는 다른 국가들의 동북아 지역에 대한 사이버안전 및 사이버범죄에 대한 정책을 비롯하여 구체적이고 실질적인 정보가 요구되고, 한국의 각 정부기관들과 여타 기관들의 정책들을 면밀히 분석하여 자료로 제공하고, 한국의 견해를 피력하여야 함에도 불구하고 기본적이고 원론적인 내용을 전달할 수밖에 없는 한계를 갖게 되었다. 그러므로 앞으로 동북아 평화협력에서 한국이 주도권을 갖고 리더로서의 역할을 선도해 나아가기 위해서는 동북아 협력을 위한 사이버안전 및 사이버범죄 대응협력방안에 대한 정책 분석 및 대응방안을 모색할 필요가 있다.

최근 사이버스페이스는 사이버테러와 사이버범죄와 같은 악의적인 사이버 활동의 위협을 받고 있는 상황이다. 사이버테러의 경우 크게는 어나니머스, 이슬람국가(IS), 북한 등이 주요 사이버테러를 일으키는 원인이 되고 있으며, 사이버범죄는 피싱이나 스미싱과 같은 사기범죄 뿐 아니라 은행에 대한 해킹, 개인정보침해, 사이버머니 탈취 등 다양한 유형이 발생하고 있다. 이와 같은 사이버안전 및 사이버범죄 문제에 대응하

기 위해서는 한 국가의 개별적 대응으로는 부족하며 국가 간 협력하여 대응할 수 있는 체계를 마련하는 것이 매우 중요하게 된다.

사이버안전 및 사이버범죄에 대한 가장 대표적인 지역별 협력체계를 구축하고 있는 곳으로 유럽연합을 들 수 있다. 유럽연합은 사이버안전 및 사이버범죄에 대한 연합차원의 대응방안을 마련하고, 이를 각 회원국가들이 이행하도록 하여 단일한 대응정책으로 운영되고 있다. 따라서 우리 정부도 그와 같은 체계를 동북아 평화협력 체계에 도입할 것을 모색하고 있다.

이에 따라서 우선 동북아 평화협력 포럼에 참여하고 있는 국가 중 미국, 중국, 러시아, 일본, 한국의 사이버안전 및 사이버범죄에 대한 최근의 정책기조에 대해 파악하고, 해당 정책의 구체적 내용과 다른 나라에 대해 갖는 시사점을 살펴 보고, 한국이 동북아 국가들에게 제시할 수 있는 선도적인 협력대응방안을 모색하고자 한다.

제2절 연구의 방법

동 연구는 미국, 일본, 중국, 러시아, 한국의 국가별 사이버 분야에 대한 관련 최신 법제와 문헌연구 및 사례 조사를 통하여 1차적 자료 번역 및 분석을 수행하였다. 그리고, 국내외 사이버안전(보안) 및 사이버범죄 분야의 전문가 및 전문기관의 자문을 통하여 정책추진 방향 및 연구내용에 대한 검토를 수행하였다. 이 과정에서 미국 국제전략문제연구소, 일본 게이오대학교, 중국 화공이공대학교, 러시아 모스크바대학교 정보안보연구소 및 국내 유관기관과 긴밀하게 협력하였다.

조사 대상 국가는 2014년 동북아 평화협력포럼 참가국을 주요 국가로 선정하였다. 미국은 지역적으로 동북아시아에 속하지 않으나, 사이버 분야의 정책에 있어 전세계적으로 선도적 역할을 하고 있으므로, 미국의 사이버안전 및 범죄 정책은 동북아 지역에도 큰 영향을 미친다. 이러한 점에서 미국은 동북아 평화협력포럼에도 참여하게 되었고, 따라서 이를 검토하는 것은 동북아 지역의 사이버 정책에 대한 시사점이 클 것으로 보인다.

조사 대상 자료는 사이버안전과 사이버범죄 분야의 최근 정책기조를 반영하는 국가

전략, 명령, 법제도 등 공식적으로 채택된 자료를 선별하였다. 최근 국가별로 사이버정책에 관하여 1차 자료가 다수 발표되어, 동 자료에 대한 분석을 바탕으로 해당 국가의 사이버정책 일반, 사이버안전, 사이버범죄 분야의 최근 정책 동향을 검토하였다.

제2장

KOREAN INSTITUTE OF CRIMINOLOGY

동북아 주요국가의 사이버안전 및 범죄 정책 비교연구

박노형·정명현·안민호

제2장

동북아 주요국가의 사이버안전 및 범죄 정책 비교연구

제2장에서는 동북아평화협력포럼에 참여했던 주요 국가들을 대상으로 사이버정책 동향을 개관하고, 사이버안전 및 사이버범죄정책을 살펴보며, 한국에 대한 시사점을 검토하기로 한다.

제1절 미국

1. 미국의 사이버정책 동향 일반

미국은 2011년 '사이버공간에서의 국제전략'(International Strategy for Cyberspace)를 통하여 사이버공간에서의 적대행위에 대한 대응으로서 필요한 경우에 국제법에 따라 최후의 수단으로서 군사력을 이용할 수 있음을 천명하고, 사이버정책을 발전시켜 왔다. 특히 2015년에는 악의적인 사이버 위협에 대한 대응을 구체화하고 국가안보전략, 대통령 행정명령, 국방부 사이버전략을 잇달아 발표하여, 미국 사이버정책의 중흥기를 맞이하고 있다. 2015년 4월 1일에 발표된 미국 오바마 대통령의 행정명령에서는 국가 또는 민간을 불문하고 미국에 대한 사이버 위협이 개시된 출처에 대하여 적극적으로 대응하도록 촉구하였다. 또한 2015년 4월 23일에 국방부에서는 2011년 '사이버공간에서의 국방부 전략'(Department of Defense Strategy for Operating in Cyberspace)을 개정·보완하여 새로운 '국방부 사이버 전략'(Department of Defense Cyber Strategy)을 발표하고, 적국과의 무력충돌에서 '사이버전'(cyber warfare)의 사용을 처음으로 천명하였다.

2. 사이버안전정책: 사이버행정명령 중점 분석

가. 사이버행정명령

2015년 4월 1일 미국 오바마 대통령은 '중대하고 악의적인 사이버-가능 활동에 참여한 특정인의 재산 동결'(Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities)에 관한 행정명령 13694(Executive Order 13694, 이하 '사이버행정명령'이라 함)를 발동하였다.[1] 사이버행정명령은 미국의 국가안보, 외교정책 또는 경제적 건전 또는 재정적 안정에 대하여 상당한 위협을 야기하는 '중대하고 악의적인 사이버-가능 활동'(significant malicious cyber-enabled activities)에 참여한 개인과 단체(blocked persons)에 대하여 재무부장관이 재정 및 비자 발급에 관한 제재를 부과할 수 있는 권한을 부여한다. 오바마 대통령은 사이버행정명령을 통하여 해외에서의 악의적인 사이버-가능 활동으로 야기되는 중대한 위협을 다루기 위하여 국가비상사태(national emergency)를 선언한 것이다.

사이버행정명령은 미국 정부가 해외 해커와 해킹을 통한 영업비밀의 부정 유용에 관하여, 이를 알면서도 이익을 취하는 외국인에게 경제적 제재를 부과한 첫 사례가 된다. 사이버행정명령은 사이버 절도, 해커 및 그 후원자의 공급 측면은 물론 해킹을 통하여 탈취된 산업정보의 수령자 또는 수혜자의 수요 측면에 대하여 제재를 가한다. 이렇게 해킹 등 악의적인 사이버-가능 활동에 대하여 종래의 행위자에 대한 제재에 더하여 수요자 측면까지 제재를 부과하게 되어 이들 활동에 대하여 보다 치밀하게 대응할 수 있을 것으로 기대한다.

사이버행정명령에서 구체적인 사건이 인용되지는 않았지만, 오바마 대통령은 사이버행정명령이 미국의 핵심기반시설, 기업과 국민을 겨냥한 최근 몇 달에 걸친 미국 국외로부터의 사이버위협에 대한 대응이라고 밝혔다. 특히 오바마 대통령은 미국 은행에 대한 이란의 해킹, 소니 영화사에 대한 북한의 사이버공격 등을 거론하였다.[2]

---

1) The White House, Executive Order - "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"(2015.4.1.), 동 원문은 〈https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m〉 참조.

사이버행정명령은 악의적인 사이버 행위자가 기존의 미국 정부 권한의 범위를 벗어나 활동할 수 있는 상황에서 미국 정부에게 제재 권한을 부여한다. 여기서 기존의 권한은 외교적 활동, 무역정책적 수단과 법집행장치를 포함한다. 그럼에도 대부분의 경우에 미국은 해외에서의 사이버위협에 대처하기 위하여 먼저 외교적 및 법집행 수단을 사용할 것이라고 하였다.[3)]

사이버행정명령은 특정 국가군을 대상으로 하지 않고, 국외의 모든 출처로부터의 사이버 위협에 대응하도록 어느 곳이든 악의적인 사이버-가능 활동을 대상으로 한다. 예컨대, 오바마 대통령은 2015년 1월 북한에 대한 추가적 제재를 허가하는 행정명령을 발동하였다.[4)] 동 행정명령은 북한 정부의 지속적이고 도발적이며 불안정을 야기하고 강압적인 행동과 정책, 특히 2014년 11월과 12월의 파괴적이고 강압적인 사이버 관련 행동에 대한 대응이다.

사이버행정명령에 따라 외국의 해커를 제재하는 것은 국제법상 관할권 행사에 관한 객관적 영토관할권(objective territoriality jurisdiction)과 보호적 관할권(protective jurisdiction) 원칙에 따른 것으로 보인다. 즉, 사이버행정명령에 따라 제재를 받는 자는, 예컨대, 활동이 미국 밖에서 전체적으로 또는 상당부분 개시되거나 미국 밖에 소재한 자의 지시에 따른 사이버-가능 활동에 대한 책임이 있어야 하고, 이러한 사이버-가능 활동이 미국의 국가안보 등에 중대한 위협을 가져올 것이 합리적으로 예견되며, 또한 핵심기반시설 부문의 하나 이상 실체를 지원하는 컴퓨터나 컴퓨터 네트워크에 의한 서비스 제공을 해하는 목적이나 효과를 가져야 한다.

---

2) Barack Obama, "A New Tool Against Cyber Threats", 〈https://medium.com/@President Obama/a-new-tool-against-cyber-threats-1a30c188bc4〉.

3) Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator의 발언, The White House Office of the Press Secretary, "On-the-Record Press Call on the President's Executive Order, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"", April 1, 2015, 〈https://www.whitehouse.gov/the-press-office/2015/04/01/record-press-call-president-s-executive-order-blocking-property-certain-persons-engaging-significant-m〉.

4) The White House Office of the Press Secretary, "Executive Order-Imposing Additional Sanctions with Respect to North Korea", January 02, 2015, 〈https://www.whitehouse.gov/the-press-office/2015/01/02/executive-order-imposing-additional-sanctions-respect-north-korea〉.

나. 사이버행정명령의 제재

1) 제재 대상자

재무부장관이 법무장관과 국무장관과 협의하여 결정한 다음의 '자'(person)는 사이버행정명령의 대상이 된다.[5] 미국의 국가안보, 외교정책, 또는 경제적·재정적 안정에 대한 중대한 위협을 합리적으로 야기할 우려가 있거나 위협에 실질적으로 기여하고, 미국 밖에서 전부 또는 상당 부분 발생하거나, 미국 밖에 소재한 자가 지시한 사이버-가능 활동에 대하여 직접적 또는 간접적으로 책임이 있거나 관여 또는 참여한 자로서, 이러한 사이버-가능 활동은 다음의 목적이나 효과를 가져야 한다. (A) 핵심기반시설 부문에서 하나 이상의 실체를 지원하는 컴퓨터 또는 컴퓨터 네트워크에 의한 서비스 제공을 해하거나 달리 중대하게 손상하거나, (B) 핵심기반시설 부문에서 하나 이상의 실체에 의한 서비스 제공을 중대하게 손상하거나, (C) 컴퓨터 또는 컴퓨터 네트워크의 이용 가능성에 중대한 교란을 야기하거나, 또는 (D) 상업적 또는 경쟁적 이익 또는 사적 재정적 이익을 위하여 재정 또는 경제적 자산, 영업비밀, 개인적 신원식별자(personal identifier) 또는 금융정보의 중대한 유용을 야기하여야 한다.[6]

재무부장관이 법무장관과 국무장관과 협의하여 결정한 다음의 자도 사이버행정명령의 제재 대상이 된다.[7] (A) 미국 밖에서 사이버-가능 수단을 통하여 유용된 영업비밀을, 이러한 영업비밀이 유용된 것을 알고서, 상업적 또는 경쟁적 이익 또는 사적 재정적 이익을 위하여 수령 또는 이용에 대한 책임이 있거나 관여 또는 참여한 자로서, 이러한 영업비밀의 유용이 미국의 국가안보, 외교정책, 경제적·재정적 안정에 대한 중대한 위협을 합리적으로 야기할 것 같거나, 실질적으로 기여한 경우, (B) Sec.1(a)(i) 또는 Sec.1(a)(ii)(A)에서 기술된 활동이나 사이버행정명령에 따라 재산과 재산에 대한 이익이 동결된 자에 대한 재정적, 물리적 또는 기술적 지지, 또는 상품 또는 서비스를 실질적으로 지원 또는 후원하였거나 제공한 경우, (C) 사이버행정명령에 따라 재산과

---

5) Cyber Order, Sec. 1(a)(i). 사이버행정명령에서 '자'(person)는 '개인 또는 실체'(an individual or entity)를 의미한다. Cyber Order, Sec. 6(a). '실체'(entity)는 '합명/합자회사, 협회, 위탁사업체, 합작투자, 기업, 집단, 하위집단 또는 기타 조직'(a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization)을 의미한다. Cyber Order, Sec. 6(b).

6) Cyber Order, Sec. 1(a)(i)(A)-(D).

7) Cyber Order, Sec. 1(a)(ii).

재산에 대한 이익이 동결된 자에 의하여 직접적 또는 간접적으로 소유되거나 통제되거나, 또는 직접적 또는 간접적으로 이 자를 위하여 또는 대신하여 행동하였거나 행동하려고 한 경우; (D) Sec.1(a)(i)과 Sec.1(a)(ii)(A)-(C)에서 기술된 활동에 참여하려고 한 경우.[8]

여기서 중대한 해킹에 활용된 정상적인 암호 장치의 제공자도 이러한 '물리적 또는 기술적 지원'을 제공한 것으로 보아야 하는지 의문이 제기될 수 있다. 또한 중대한 해킹을 탐지하는 데 어려움을 줄 수 있는 프라이버시 보호 장치의 제공자도 이에 해당하는 것으로 볼 수 있는지에 대하여 의문이 제기될 수 있다. 특히 Sec.1(a)(ii)(A)가 '미국 밖'을 명시한 것과 달리 그렇지 않은 Sec.1(a)(ii)(B)의 경우, 동 행정명령의 대상이 미국 밖에 소재하여야 할 필요는 없는 것으로 보인다.

2) 제재 대상물

위의 제재 대상자의 자산으로서 미국에 소재하거나, 이후 미국으로 이전되거나, 미국인의 소유 또는 통제 하에 있거나 이후 받게 되는 '모든 재산과 재산에 대한 이익'(all property and interests in property)은 동결되고, 이전, 지불, 수출, 퇴거 또는 기타의 방법으로 처리되지 못한다.[9] 사이버행정명령에 따라 재산과 재산에 대한 이익이 동결되는 자에 의하거나, 이러한 자에게 주어지거나, 이러한 자를 위한 '자금, 상품 또는 서비스의 기여 또는 제공'(making of any contribution or provision of funds, goods, or services)과 이러한 자로부터 '자금, 상품 또는 서비스의 기여 또는 제공의 수령'(receipt of any contribution or provision of funds, goods, or services) 등이 금지된다.[10]

3) 악의적인 사이버-가능 활동

사이버행정명령의 대상이 되는 '악의적인 사이버-가능 활동'(malicious cyber-

8) Cyber Order, Sec. 1(a)(ii)(A)-(D).
9) Cyber Order, Sec. 1(a). '미국인'(United States person)은 '미국 시민, 영주외국인, 외국 사무소를 포함하여 미국법 또는 미국 내 관할권에 따라 구성된 실체, 또는 미국 내 소재하는 자'(any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States)를 의미한다. Cyber Order Sec. 6(c).
10) Cyber Order Sec. 3.

enabled activities)은 다음 세 가지 요소를 충족하여야 한다.[11] 첫째, 미국의 국가안보, 외교정책, 또는 경제적 건전 또는 재정적 안정에 대한 중대한 위협을 합리적으로 초래할 것 같거나 실질적으로 기여한 활동이다. 둘째, 미국 밖에서 전체로 또는 상당하게 부분적으로 개시되거나 미국 밖에 소재한 자의 지시를 받은 활동이다. 셋째, 이러한 사이버 - 가능 활동은 다음의 목적이나 효과를 가져야 한다. i) 핵심기반시설 부문에서 하나 이상의 실체를 지원하는 컴퓨터 또는 컴퓨터 네트워크에 의한 서비스 제공을 해치거나 달리 중대하게 손상하거나, ii) 핵심기반시설 부문에서 하나 이상의 실체에 의한 서비스 제공을 중대하게 손상하거나, iii) 컴퓨터 또는 컴퓨터 네트워크의 이용 가능성에 중대한 교란을 야기하거나, 또는 iv) 상업적 또는 경쟁적 이익 또는 사적 재정적 이익을 위하여 재정 또는 경제적 자산, 영업비밀, 개인적 신원식별자 또는 금융정보의 중대한 유용을 야기하여야 한다.

악의적인 사이버 - 가능 활동의 세 번째 요건에서 '컴퓨터 또는 컴퓨터 네트워크의 이용 가능성에 중대한 교란을 야기'하는 예는 '(분산) 서비스거부'(Distributed Denial of Service: DDoS) 공격이 될 것이다.[12] 또한, 세 번째 요건에서 '유용'(misappropriation)은 '부정한 수단으로 허가나 동의 없이 또는 허위로 얻는 것'(any taking or obtaining by improper means, without permission or consent, or under false pretenses)을 포함한다.[13]

따라서, 사이버행정명령은 모든 악의적인 사이버 - 가능 활동을 대상으로 하지 않고, 보다 구체적으로 동 행정명령에서 구체화된 해(harms)를 야기하는 활동만을 대상으로 한다. 이러한 활동은 미국 국가안보, 외교정책, 또는 경제적 건전 또는 재정적 안정에 영향을 줄 정도로 중대하여야 한다. 특히 오바마 대통령은 사이버위협이 미국에 대한 가장 심각한 경제적이고 국가안보의 도전 중의 하나라고 선언하고, 사이버행정명령이 '가장 심각한 유해 사이버 위협'(the most serious malicious cyber threats)을 근절하기 위하여 새로운 권한을 추가함으로써 미국 행정부의 광범위한 전략을 지지한다고 밝혔다.[14]

---

11) 이 세 가지 요소는 위의 제재 대상자에 관한 규정에서 확인할 수 있다. Cyber Order, Sec. 1(a)(i) 참조.
12) The White House Office of the Press Secretary, 앞의 주 4.
13) Cyber Order, Sec. 6(e).
14) The White House Office of the Press Secretary, 앞의 주 4.

그러나, 사이버행정명령은 '사이버 - 가능'(cyber-enabled) 용어에 대한 정의를 두고 있지 않다. 미국 재무부에 따르면, '사이버 - 가능' 활동이 주로 컴퓨터 또는 다른 전자적 장치를 통하여 완성되거나 이들에 의하여 촉진되는 행동을 포함하도록 정의하는 규정이 채택될 것이라고 한다.[15] 또한, 재무부에 따르면, 악의적인 사이버 - 가능 활동은 "원격 접속에 의한 것을 포함하여 컴퓨터시스템에 대한 허가받지 않은 접속을 통하여 완성된 의도적 활동; 방화벽의 우회를 포함하여 하나 이상의 보호조치를 우회함, 또는 공급망에서의 하드웨어 또는 소프트웨어의 안전을 손상함"을 포함한다고 한다.[16] 이들 악의적인 사이버 - 가능 활동은 핵심기반시설에 대한 손상, DDoS공격, 또는 영업비밀과 개인적 금융정보와 같은 민감정보의 대량 유실을 포함하여 종종 사이버행정명령에 열거된 구체적인 피해를 달성하는 수단이 된다.[17]

실제로 어떤 사이버 활동이 사이버행정명령에 따라 제재 대상이 될 것인지 결정하는 것은 쉽지 않을 것이다. 특히 '중대한'(significant)의 정도의 결정이 쉽지 않을 것이며, 예컨대, 사이버행정명령은 제재를 발동하는 데 충분한 경제적 피해 규모나 유용된 영업비밀 범주를 규정하지 않는다.

다. 사이버행정명령의 문제

1) 귀속의 어려움

사이버행정명령의 제재의 대상이 되는 악의적인 사이버 - 가능 활동의 귀속(attribution)은 그렇게 쉬운 사안이 아닐 것이다. 즉, 미국 밖에서 활동하는 해커가 누구인지 파악하는 것은 현실적으로 쉽지 않을 것이어서, 동 행정명령의 이행으로 제재를 받게 되는 대상자의 해당 국가와의 소위 진실게임과 같은 분쟁이 발생할 것이다.

---

15) U.S. Department of the Treasury, "447. What will significant malicious "cyber-enabled" activities mean for the purposes of Executive Order (E.O.) 13694?" in Cyber-related Sanctions: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities (Executive Order 13694), OFAC FAQs: Other Sanctions Programs, 〈http://www.treasury.gov/resource- center/faqs/Sanctions/Pages/faq_other.aspx#cyber〉.

16) 앞의 주.

17) 앞의 주.

2) 개념의 어려움

사이버행정명령이 보호하고자 하는 주된 대상은 미국의 핵심기반시설인데, 미국의 핵심기반시설은 그 자산, 시스템 및 네트워크가 미국에 필수적이어서 이의 무력화 또는 파괴가 안보, 국가경제안전, 국가공공보건 또는 안전 또는 이들의 결합을 약화하는 효과를 가지는 것이다.[18] 미국의 대통령정책지침 21(Presidential Policy Directive 21: PPD-21)은 "핵심기반시설안전과 회복"(Critical Infrastructure Security and Resilience)에 관한 것인데, 안전하고, 정상적이며 회복력 있는 핵심기반시설을 강화하고 유지하는 국가정책을 발전시키는 것을 목적으로 한다.[19] PPD-21은 관련 국토안전대통령지침 7(Homeland Security Presidential Directive 7)을 대체하며, 16개의 핵심기반시설 부문을 정하고 있다.[20] 미국의 핵심기반시설의 범위는 상당히 넓은데, 흥미롭게도 북한의 해킹을 받은 소니 영화사와 같은 영화촬영스튜디오, 카지노와 호텔도 보호되는 상업시설로서 핵심기반시설의 일부이다.

3) 준수의 어려움

사이버행정명령의 적용 범위는 상당히 넓기 때문에 동 행정명령의 제재를 받는 대상과 거래를 하는 미국 기업에게도 큰 부담이 될 수 있다.

4) 국제적 반발과 분쟁의 가능성

사이버행정명령은 영업비밀의 해킹 등을 이유로 미국의 비난을 받고 있는 중국 등의 특정 국가들로부터 강력한 반발을 받을 것이다.

---

18) U.S Department of Homeland Security, Critical Infrastructure Sectors, 〈http://www.dhs.gov/critical-infrastructure-sectors〉.

19) The White House Office of the Press Secretary, "Presidential Policy Directive-Critical Infrastructure Security and Resilience", 〈https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil〉.(2013.2.23.).

20) U.S Department of Homeland Security, Critical Infrastructure Sectors, 〈http://www.dhs.gov/critical-infrastructure-sectors〉.

3. 사이버범죄 정책

가. 컴퓨터사기남용법 개요

컴퓨터사기남용법(Computer Fraud and Abuse Act, 이하 'CFAA'라 함)은 컴퓨터 시스템을 대상으로 하는 범죄행위를 금지한다.[21] CFAA는 연방정부 컴퓨터, 은행 컴퓨터 및 인터넷에 연결된 컴퓨터를 보호하는 점에서 사이버안전법(cyber security law)이다.[22]

CFAA는 종합적이지 않지만, 연방 형법이 제공하는 보호에 있어 흠결을 보충하며, 컴퓨터를 다음과 같이 보호한다. 정부 컴퓨터의 해킹 등 컴퓨터 침입(computer trespassing)[23]. 특정 정부, 신용, 금융 또는 컴퓨터 저장 정보의 유출을 초래하는 해킹 등 컴퓨터 침입(computer trespassing)[24], 웜, 컴퓨터바이러스, 토로이 목마, 시한폭탄, 서비스거부공격, 기타 사이버공격, 사이버범죄 또는 사이버테러 등 정부 컴퓨터, 은행 컴퓨터 또는 주 간 또는 대외통상에서 이용되거나 이에 영향을 주는 컴퓨터의 훼손(damaging)[25], 정부 컴퓨터, 은행 컴퓨터, 또는 주 간 또는 대외통상에서 이용되거나 이에 영향을 주는 컴퓨터에 대한 불법적 접속을 수반하는 구성요소의 사기(committing fraud)[26], 정부 컴퓨터, 은행 컴퓨터, 또는 주 간 또는 대외통상에서 이용되거나 이에 영향을 주는 컴퓨터의 훼손 위협(threatening to damage)[27], 정부 컴퓨터의 비밀번호 탈취(trafficking in) 또는 동 탈취가 주 간 또는 대외통상에 영향을 주는 경우[28] 및 첩보 수행을 위한 컴퓨터 접속(accessing)[29].

이외에 CFAA에 의하면 위의 금지된 행위의 미수 또는 모의도 범죄가 된다.[30] 또한,

---

21) 18 U.S.C. 1030. 이하 내용은 주로 Charles Doyle, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report 97-1025, October 15, 2014(이하 'Cybercrime: an Overview'라 함)을 정리한 것이다.
22) Cybercrime: an Overview, Summary.
23) 18 U.S.C. 1030(a)(3).
24) 18 U.S.C. 1030(a)(2).
25) 18 U.S.C. 1030(a)(5).
26) 18 U.S.C. 1030(a)(4).
27) 18 U.S.C. 1030(a)(7).
28) 18 U.S.C. 1030(a)(6).
29) 18 U.S.C. 1030(a)(1).
30) 18 U.S.C. 1030(b).

단순한 사이버공간 침입에 대한 1년 이하의 징역부터 고의적 컴퓨터 훼손에 의한 살해에 대한 무기징역에 이르는 벌칙이 규정되어 있다.[31] 또한, 국토안보부 산하 비밀경호국(Secret Service)이 이들 사이버범죄에 대한 조사권한을 갖는다.[32] 또한 이들 범죄피해자는 민사소송을 제기할 수 있다.[33] 위의 범죄로 인하여 생성되거나 범죄를 위하여 이용된 재산은 몰수될 수 있다.[34]

나. 사이버범죄의 유형

1) 정부 사이버공간의 침입[35]

(1) 요건

연방정부가 배타적으로 사용하거나 연방정부가 접속을 공유하는 컴퓨터에 대한 해킹 등 불법적 침입은 금지되고 처벌된다.[36] 즉, 허가 없이 의도적으로 연방정부가 배타적으로 사용하는 정부 컴퓨터에 접속하거나, 최소한 부분적으로 연방정부에 의하거나 이를 위하여 사용되는 정부 컴퓨터에 접속하고, 동 접속이 연방정부에 의하거나 이를 위한 사용에 영향을 주는 것은 불법이다.

(2) 처벌

1년 이하의 징역 또는 재범의 경우 10년 이하의 징역 및/또는 제18장(Title 18)에 따른 벌금으로서 경범죄(misdemeanors)에 대한 10만달러/중죄(felonies)에 대한 25만달러와 해당 범죄로 야기된 손해나 이익의 두 배 중 보다 큰 금액의 처벌[37]을 받는다. 청소년이 범한 대부분의 연방범죄와 같이 이들 범죄는 주법원의 재판을 받는다.

---

31) 18 U.S.C. 1030(c).
32) 18 U.S.C. 1030(d).
33) 18 U.S.C. 1030(g).
34) 18 U.S.C. 1030(i) 및 (j).
35) 18 U.S.C. 1030(a)(3). 원문은 다음과 같다: "(a) Whoever … (3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States … shall be punished as provided in subsection (c) of this section."
36) 18 U.S.C. 1030(a)(3).
37) 18 U.S.C. 3571.

또한, 이들 범죄에 대하여 몰수, 반환(restitution), 돈 세탁(money laundering), 민사 책임, 및 공갈(racketeering)의 규정이 추가적으로 적용될 수 있다. 위의 범죄의 미수와 모의는 처벌된다.[38]

컴퓨터 시스템을 훼손하지 않거나 정부에 피해를 주지 않거나 해커가 이익을 얻지 않고 단순히 정부 컴퓨터에 대한 해킹을 하는 경우에는 '정보의 해킹과 획득'(hacking-and-acquiring-information) 금지의 위반이 된다.[39] 또한, 이는 '주 컴퓨터범죄'(state computer crime)가 될 수 있다.

2) 허가받지 않은 컴퓨터 접속에 의한 정보 획득[40]

(1) 요건

단순한 해킹 다음의 단계는 의도적으로 허가받지 않은 접속에 의하여 보호되는 정보를 획득하는 것이다. 이러한 정보에는 세 가지 유형이 있다. 연방정부의 정보, 소비자의 신용 또는 다른 금융정보, 및 보호되는 컴퓨터로부터 획득한 정보. 이러한 행위가 위법하기 위하여 다음의 네 가지 요소가 충족되어야 한다. 피의자가 첫째, 의도적으로, 둘째, 보호되는 컴퓨터를, 셋째, 허가 없이 접속하였거나 허가된 범위를 초월하여 접속하여, 넷째, 정보를 획득하였어야 한다.

다른 법규정에 따르면 신의성실의무(fiduciary obligation)를 준수하지 않거나 또는 재물을 얻거나 탈취하기 위하여 절취하는 경우에 처벌되지만, 허가받지 않은 컴퓨터 접속에 의하여 정보를 획득한 자의 처벌에는 절취 의도(larcenous intent)가 요구되지 않는다.[41]

---

38) 18 U.S.C. 1030(b). 원문은 다음과 같다: "(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section."

39) 18 U.S.C. 1030(a)(2).

40) 18 U.S.C. 1030(a)(2). 원문은 다음과 같다: "(a) Whoever … (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) [1] of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); (B) information from any department or agency of the United States; or (C) information from any protected computer;"

(2) 처벌

단순 위반의 경우 1년 이하의 징역 및/또는 제18장(Title 18)에 따른 벌금이 부과될 수 있고[42], 5천달러 이상의 이익 또는 이러한 금액을 수반하는 위반의 경우 5년 이하의 징역 및/또는 제18장에 따른 벌금이 부과될 수 있으며, 재범의 경우 10년 이하의 징역 및/또는 제18장에 따른 벌금이 부과될 수 있다.[43] 허가받지 않은 컴퓨터 접속에 의하여 정보를 획득한 자는 민사책임을 질 수 있다.[44]

다. 컴퓨터 훼손[45]

(1) 요건

웜 (worms)이나 바이러스를 촉발시키는 등 다음과 같은 컴퓨터 훼손은 금지된다. 첫째, 알면서도 보호되는 컴퓨터를 전염시켜 허가받지 않은 훼손을 의도적으로 초래하거나, 둘째, 보호되는 컴퓨터에 의도적으로 접속하여 무모하게 훼손을 초래하거나, 셋째, 보호되는 컴퓨터에 의도적으로 접속하여 훼손시킴으로써 손해를 초래하는 경우.

동 규정에 의하면 '보호되는 컴퓨터'가 훼손되는 경우에만 연방범죄가 된다. 이와 같이 보호되는 컴퓨터에는 다섯 가지 종류가 있다. 첫째, 미국 정부를 위하여 또는 미국 정부에 의하여 배타적으로 사용되는 컴퓨터, 둘째, 은행 또는 다른 금융기관을 위하여 또는 이에 의하여 배타적으로 사용되는 컴퓨터, 셋째, 부분적으로 미국 정부를 위하여 또는 이에 의하여 사용되는 경우, 이러한 컴퓨터 훼손이 정부의 사용 또는 정부를 위한 사용에 영향을 주는 컴퓨터, 넷째, 부분적으로 은행 또는 다른 금융기관을 위하여 또는 이에 의하여 사용되는 경우, 이러한 컴퓨터 훼손이 은행 등을 위하거나

41) 이 점에서 컴퓨터 사기의 범죄와도 구별된다. 18 U.S.C. 1030(a)(4) 참조.
42) 18 U.S.C. 1030(c)(2)(A).
43) 18 U.S.C. 1030(c).
44) 18 U.S.C. 1030(g).
45) 18 U.S.C. 1030(a)(5). 원문은 다음과 같다: "(a) Whoever … (5) (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss;"

또는 이에 의한 사용에 영향을 주는 컴퓨터, 다섯째, '주 간 또는 대외통상 또는 통신'(interstate or foreign commerce or communication)에서 사용되거나 이에 영향을 주는 컴퓨터로 분류된다.[46] 특히 다섯째 유형의 보호되는 컴퓨터에는 미국의 주 간 또는 대외통상이나 통신에 영향을 주는 방식으로 사용되는, 미국 국외에 소재하는 컴퓨터도 포함된다.[47]

(2) 처벌

상습적 범행과 무모하거나 의도적으로 심각하게 훼손하는 행위는, 초범 또는 의도적으로나 무모하지만 덜 심각하게 훼손하거나 반드시 심각하게 훼손할 의도가 없이 훼손하는 행위보다 중하게 처벌된다.[48] 즉, 심각한 훼손을 초래하지 않은 초범은 1년 이하의 징역으로 처벌될 수 있으나, 심각한 훼손을 초래하지 않았더라도 재범인 경우에는 10년 이하의 징역으로 처벌될 수 있다. 심각하지 않은 훼손을 의도적이거나 무모하게 초래한 재범은 20년 이하의 징역 또는/및 25만 달러 이하(기관의 경우 50만 달러 이하) 벌금으로 처벌될 수 있다. 그러나, 알면서도 보호되는 컴퓨터를 감염시켜 의도적으로 심각한 훼손을 초래한 초범은 10년 이하의 징역으로 처벌될 수 있지만, 재범은 20년 이하의 징역 또는/및 25만 달러 이하(기관의 경우 50만 달러 이하) 벌금으로 처벌될 수 있다. 허가받지 않은 접속이나 미수의 접속으로 무모하게 심각한 훼손을 초래한 초범은 5년 이하의 징역으로 처벌될 수 있지만, 재범은 20년 이하의 징역 또는/및 25만 달러 이하(기관의 경우 50만 달러 이하) 벌금으로 처벌될 수 있다. 알면서도 보호되는 컴퓨터에 의도적으로 감염을 초래하여 알면서 또는 무모하게 심각한 상해를 초래한 범행은 20년 이하의 징역 또는/및 25만 달러 이하(기관의 경우 50만 달러 이하) 벌금으로 처벌될 수 있지만, 사망을 초래한 범행은 무기징역 이하 또는/및 25만 달러 이하(기관의 경우 50만 달러 이하) 벌금으로 처벌될 수 있다.

다음과 같이 보다 심각한 유형의 훼손이 초래되면 초범이나 미수의 경우에도 보다 중한 처벌을 받을 수 있다. 첫째, 한 사람 이상에게 연간 5천달러를 초과하는 피해를 야기하는 경우, 둘째, 한 사람 이상의 의료서비스를 수정 또는 침해할 우려가 있는

46) 18 U.S.C. 1030(e)(2).
47) 18 U.S.C. 1030(e)(2)(B).
48) 18 U.S.C. 1030(c)(4).

경우, 셋째, 물리적 상해를 초래하는 경우, 넷째, 공공 보건 또는 안전을 위협하는 경우, 다섯째, 국방 또는 국가안보기관 컴퓨터에 영향을 주는 경우, 여섯째, 연간 10대 이상의 컴퓨터에 영향을 주는 경우.

컴퓨터 훼손에 대해서는 미수, 모의 및 공모에 관한 규정이 적용된다. 또한, 연방정부 자산, 금융기관 자산, 또는 주 간 또는 대외통상에서 사용되는 자산의 훼손이나 파손으로 연루될 수 있는 다른 연방법규정도 적용될 수 있다. 이러한 규정에는, 방화 또는 폭발에 의한 연방 자산의 파손[49], 미국 내 수목의 파손[50], 정부 기록의 파손[51], 연방 자산의 파손[52], 연방통신자산의 파손[53], 항공기 또는 항공기 시설의 파손[54], 자동차 또는 자동차 시설의 파손[55], 항행 시설의 파손[56], 기차 사고의 초래[57], 에너지 시설의 훼손[58]이 있다.

라. 컴퓨터 사기[59]

(1) 요건

컴퓨터 침입에 의한 사기, 즉 컴퓨터 사기(computer fraud)는 금지된다. 컴퓨터 사기는 다음의 세 가지 요소가 충족되어야 한다. 첫째, 알면서 및 사기의 의도를 가지고, 둘째, 허가 없이 또는 허가된 범위를 초월하여 보호되는 컴퓨터에 접속하며, 셋째, 기망하여 최소한 연간 5천달러 이상의 자산가치를 획득할 것.

---

49) 18 U.S.C. 844(f).
50) 18 U.S.C. 1853.
51) 18 U.S.C. 2071.
52) 18 U.S.C. 1361.
53) 18 U.S.C. 1362.
54) 18 U.S.C. 32.
55) 18 U.S.C. 33.
56) 18 U.S.C. 2280.
57) 18 U.S.C. 1992.
58) 18 U.S.C. 1367.
59) 18 U.S.C. 1030(a)(4). 원문은 다음과 같다: "(a) Whoever … (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;"

(2) 처벌

컴퓨터 사기는 5년 이하의 징역(재범인 경우 10년 이하의 징역) 및/또는 제18장(Title 18)에 따른 벌금으로 처벌될 수 있다.[60] 컴퓨터 사기의 피해자는 보상적 손해배상(compensatory damage) 및/또는 금지명령구제(injunctive relief)의 소를 제기할 수 있다.[61] 미수, 모의 및 공모도 처벌된다.

컴퓨터 사기와 관련하여 연루될 수 있는 다른 연방법규정은 다음과 같다. 전신사기(wire fraud)[62], 절취 자산의 주 간 운반(interstate transportation of stolen property)[63], 주 간 운송수단으로부터 절취(theft from interstate carriers)[64], 경제적 첩보(economic espionage)[65], 영업비밀의 절취[66](theft of trade secrets), 신용카드와 접속장비 수반 사기[67], 연방자산의 절취[68], 연방기관의 관할 사안에 관한 허위진술[69], 연방 보증 대출과 신용 청구에 관한 허위진술[70] HUD거래에 관한 허위진술[71], 미국에 대한 허위 청구[72], 은행 사기[73], 대부, 신용 및 보험기관 직원의 절취 또는 횡령[74], 은행 가입사기[75], 연방신용기관 가입사기[76]; 연방예금보험공사(Federal Deposit Insurance Corporation)에 영향을 주는 허위진술[77], 저작권 침해[78], 자금세탁[79], 공갈[80], 불법활동 수익금의 분배 등을 위한 주 간 또는 해외 여행의 금지.[81]

---

60) 18 U.S.C. 1030(c)(4).
61) 18 U.S.C. 1030(g).
62) 18 U.S.C. 1343.
63) 18 U.S.C. 2314.
64) 18 U.S.C. 659.
65) 18 U.S.C. 1832.
66) 18 U.S.C. 1832.
67) 18 U.S.C. 1029.
68) 18 U.S.C. 641.
69) 18 U.S.C. 1001.
70) 18 U.S.C. 1014.
71) 18 U.S.C. 1010, 1012.
72) 18 U.S.C. 287.
73) 18 U.S.C. 1344.
74) 18 U.S.C. 657.
75) 18 U.S.C. 1005.
76) 18 U.S.C. 1006.
77) 18 U.S.C. 1007.
78) 18 U.S.C. 2319.
79) 18 U.S.C. 1956, 1957.
80) 18 U.S.C. 1962.

마. 갈취 위협[82]

(1) 요건

주간 또는 대외통상에서 사람, 기업, 협회, 교육기관, 금융기관, 정부기관 또는 다른 법인에게서 돈이나 재물을 갈취할 의도를 가지고 보호되는 컴퓨터의 훼손을 초래하는 위협을 포함하는 통신을 주 간(interstate) 또는 대외통상에서 전송하는 것은 금지된다. 이러한 갈취 위협(extortionate threats)에서 '훼손'(damage)은 한 명 이상의 개인에게 1년 동안 최소한 5천 달러에 달하는 손해를 초래하거나, 한 명 이상의 사람의 의료 검사, 진단, 처치를 수정 또는 침해하거나, 수정 또는 침해할 우려가 있거나, 사람에게 물리적 상해를 초래하거나, 또는 공공 보건 또는 안전을 위협하는 데이터, 프로그램, 시스템 또는 정보의 완전성이나 이용가능성의 침해[83]를 가리킨다.

(2) 처벌

갈취 위협의 초범은 5년 이하의 징역 또는 재범은 10년 이하의 징역 및/또는 18장에 따른 벌금의 처벌을 받을 수 있다.[84] 피해자는 민사소송을 제기할 수 있다.[85] 미수, 모의 및 공모도 처벌된다.

갈취 위협은 다음과 같은 연방법규정의 위반이 될 수 있다. 통상에 영향을 주는 강탈(extortion)[86], 주 간 통상에서 전송되는 위협[87], 위협 내용의 우송[88], 외국에서 위협 내용의 우송[89], 갈취 수익의 수령 [90]

---

81) 18 U.S.C. 1952.
82) 18 U.S.C. 1030(a)(7). 원문은 다음과 같다: "(a) Whoever … (7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—
(A) threat to cause damage to a protected computer; (B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or (C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;"
83) 18 U.S.C. 1030(e)(8).
84) 18 U.S.C. 1030(c).
85) 18 U.S.C. 1030(g).
86) 18 U.S.C. 1951.
87) 18 U.S.C. 875.
88) 18 U.S.C. 876.
89) 18 U.S.C. 877.

바. 컴퓨터 접속에서의 거래[91]

(1) 요건

Section 1029의 접속장치의 금지와 유사한 컴퓨터 접속에서의 거래(trafficking in computer access)가 금지된다. 제한적이지만, 이러한 금지는 다음과 같은 특색을 가진다. 첫째, Section 1029의 경우보다 더 명확하게 정부 컴퓨터에 대한 암호에 적용된다. 둘째, Section 1029의 경우보다 더 많이 사전형량조정(plea bargaining)의 기회가 있다. 셋째, 불법행위가 지속되지 않는다면 심각한 처벌을 부과하지 않고 비밀 컴퓨터시스템에 대하여 공개적으로 접속하는 관행을 단절하는 수단을 제공한다. 넷째, 법원이 보다 적절하게 처리할 수 있도록 민사적 책임의 사적 집행이 가능하다.

컴퓨터 접속에서의 거래는 다음의 요소로 구성된다. 첫째, 알면서도 사기의 의도를 가지고, 둘째, 연방 컴퓨터나 주 간 또는 대외통상에 영향을 주는 방식으로, 셋째, 컴퓨터 암호 또는 유사한 컴퓨터 키를; 넷째, 거래하는 것이다. 여기서 거래(trafficking)는 전송 또는 처분할 의도를 가지고 전송, 도는 처분 또는 통제를 하는 행위를 가리킨다.[92]

(2) 처벌

컴퓨터 접속에서의 거래는 초범의 경우 1년 이하의 징역(재범의 경우 10년 이하의 징역) 및/또는 18장(Title 18)에 따른 벌금으로 처벌될 수 있다.[93] 피해자는 민사책임의 청구를 할 수 있다.[94] 미수, 모의 및 공모도 처벌된다. 컴퓨터 접속에서의 거래 금지는 신용카드 사기의 금지[95]와 전신사기의 금지[96]와 유사하다. 또한, 이들 금지되는 범행은 RICO[97]나 자금세탁[98]으로도 처벌될 수 있다.

---

90) 18 U.S.C. 880.
91) 18 U.S.C. 1030(a)(6). 원문은 다음과 같다: "(a) Whoever … (6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—
(A) such trafficking affects interstate or foreign commerce; or (B) such computer is used by or for the Government of the United States;"
92) 18 U.S.C. 1029(e)(5).
93) 18 U.S.C. 1030(c)(2).
94) 18 U.S.C. 1030(g).
95) 18 U.S.C. 1029(a)(2).
96) 18 U.S.C. 1343.

사. 컴퓨터 첩보[99]

(1) 요건

컴퓨터 첩보(computer espionage)의 금지는 미국 국방과 복지에 위해가 될 수 있는 정보의 공개 금지와 같은 스파이행위를 금지하는 연방첩보에 관한 법률과 기본적으로 유사하다.[100] 컴퓨터 첩보의 규정은 첩보와 컴퓨터 남용의 요소들의 결합으로 볼 수 있다. 컴퓨터 첩보는 다음의 행위를 금지한다. 첫째, 국방, 외교 또는 원자력에 관한 비밀정보를, 둘째, 이러한 정보가 미국을 해치는데 사용될 수 있거나, 외국에 이익이 되도록 사용될 수 있다고 믿을만한 이유가 있고, 셋째, 이러한 정보가 허가받지 않은 컴퓨터 접속으로 획득되고, 넷째, 이러한 정보를 고의로 공개, 고의로 공개 미수, 또는 고의로 반환하지 않는 행위.

(2) 처벌

컴퓨터 첩보는 초범의 경우 10년 이하의 징역(재범의 경우 20년 이하의 징역) 및/또는 제18장(Title 18)에 따른 벌금의 처벌을 받을 수 있다.[101] 미수, 모의 및 공모도 처벌된다. RICO[102]와 자금세탁[103]의 규정도 같이 적용될 수 있다.

---

97) 18 U.S.C. 1962. RICO(Racketeer Influenced and Corrupt Organizations Act)는 조직범죄 피해자의 보상을 규정한다.
98) 18 U.S.C. 1956, 1957.
99) 18 U.S.C. 1030(a)(1). 원문은 다음과 같다: "(a) Whoever—
(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;"
100) 18 U.S.C. 793, 794, 798 참조.
101) 18 U.S.C. 1030(c)(1).
102) 18 U.S.C. 1962.
103) 18 U.S.C. 1956, 1957.

4. 시사점

미국의 사이버행정명령은 사이버위협에 대한 적극적 대응을 강화시키는 정책의 일환으로서 동 사이버행정명령이 갖는 함의는 크다. 사이버행정명령은 광범위한 용어를 사용하여 재무부장관에게 상당한 해석의 재량을 부여함으로써, 동 행정명령의 제재를 받는 자의 재산의 동결은 물론 미국 시민의 이러한 자와의 거래를 일반적으로 금지하게 된다. 사이버행정명령은 해외에서 발생하는 악의적인 사이버 - 가능 활동과 같은 사이버 위협을 통제하려는 국가관행으로서 중요한 시도이다. 또한 미국의 국가안보와 외교정책은 물론 경제적 건전이나 재정적 안정에 대한 중대한 사이버위협을 국가비상사태로 인정한다. 특히 사이버행정명령은 UN헌장 제2(4)조의 무력사용이나 제51조의 무력공격의 기준의 아래에 있는 악의적인 사이버 - 가능 활동을 구체적으로 다루고 있는 점에 중요한 의의가 있다. 미국은 UN헌장 제51조에 따른 무력공격은 물론 '불법 무력사용'(illegal use of force)에 대하여 무력사용을 수반하는 자위권의 행사를 주창하고 있는데,[104] 사이버행정명령은 무력사용이 아닌 재정적 제한 및 비자의 발급 금지와 같은 제재를 부과함으로써 동 행정명령이 대상으로 하는 악의적인 사이버 - 가능 활동이 무력공격이나 무력사용에 해당하지 않는 것으로 이해될 수 있다.

특히 사이버행정명령의 대상과 제재는 오바마 대통령이 북한에 의한 소니 해킹을 '전쟁행위'가 아닌 '사이버 공공기물파손'(cyber vandalism)으로 이해하는 것과 일맥상통한다.[105] 사이버행정명령은 평화 시의 악의적인 사이버 - 가능 활동에 대하여 제재를 부과함으로써 최근 사이버 무력충돌에 지나치게 집중된 국제적 관심으로부터 벗어난 점에서 좋은 시도라고 볼 수 있다. 학계는 물론 국가들은 사이버 무력충돌의 가능성을 크게 주장하고 있음에도 실제로 국제인도주의법 또는 전쟁법의 적용을 받을 만한 사이버 무력충돌은 발생하고 있지 않다. 이러한 관점에서 사이버행정명령의 대상이 되는 악의적인 사이버 - 가능 활동은 사이버공간에서 및 사이버공간을 통한 무력

104) Harold Hongju Koh, Legal Advisor U.S. Department of State, "International Law in Cyberspace", USCYBERCOM Inter-Agency Legal Conference at Ft. Meade, MD, September 18, 2012, 〈http://www.state.gov/s/l/releases/remarks/197924.htm〉.

105) Sean Sullivan, "Obama: North Korea hack 'cyber-vandalism,' not 'act of war'", Washington Post, December 21, 2014, 〈http://www.washingtonpost.com/news/post-politics/wp/2014/12/21/obama-north-korea-hack-cyber-vandalism-not-act-of-war/〉.

사용과 무력공격에 이르지 않는 낮은 수준의 사이버 조작의 새로운 범주로서 간주될 수 있다. 다만, 추후 사이버행정명령의 대상이 되는 악의적인 사이버 - 가능 활동의 구체적 내용이 미국 재무부를 통하여 확인될 것인데, 이러한 내용의 당부에 관한 평가가 필요할 것이다.

사이버행정명령은 일반적인 행정명령과 달리 특정 국가나 특정 국가군을 대상으로 하지 않고 직접적으로 악의적인 사이버 - 가능 활동을 대상으로 한다. 이 점에서 사이버행정명령에서 구체적으로 확인되지는 않았지만 동 행정명령에서 규정된 악의적인 사이버 - 가능 활동을 하는 것으로 알려진 국가들에게는 상당한 수준의 억제(deterrence) 효과를 줄 것으로 기대된다. 또한, 동 행정명령에 따라 자칫 제재를 받게 될 여러 국가들이 집단으로 미국에 반발할 가능성도 있을 것이다. 반면에 미국과 같은 입장에 있는 서방국가들이 동지국(like-minded countries)으로서 미국을 지지하고 같은 행동을 취한다면 미국의 사이버행정명령의 일방적 성격이 점차 복수적 내지 다자적 성격을 가질 수 있을 것이다. 실제로 사이버행정명령은 이들 동지국들의 참여를 요청하고 있다.[106] 이와 관련하여 한국이 취할 수 있는 태도와 역할에도 주목해야 할 것이다.

한편, 사이버범죄 대응 정책으로 미국은 연방형법의 흠결을 보완하는 컴퓨터사기남용법을 통하여 인터넷과 컴퓨터시스템에 대한 사이버범죄를 규율하고자 하였다. 동법에서는 컴퓨터 침입 등 무단접속, 컴퓨터 훼손, 컴퓨터 불법접속과 사기, 첩보 수단으로서의 컴퓨터 접속 등의 사이버범죄를 금지하고 있다. 특히 정부 컴퓨터 등 시설에 대한 침입과 훼손 행위 및 재범행위를 중하게 처벌하고, 사이버범죄에 대한 미수 또는 모의도 금지하여 광범위하게 처벌하고 있다. 또한 경찰뿐만 아니라 국토안보부 산하기관이 사이버범죄에 대한 조사권한을 가짐으로써, 관련 기관의 상호 협조 하에 신속한 대응이 이루어지도록 하고 있다.

---

106) Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator 의 발언, The White House Office of the Press Secretary, "On-the-Record Press Call on the President's Executive Order, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"", April 1, 2015, 〈https://www.whitehouse.gov/the-press-office/2015/04/01/record-press-call-president-s-executive-order-blocking-property-certain-〉.

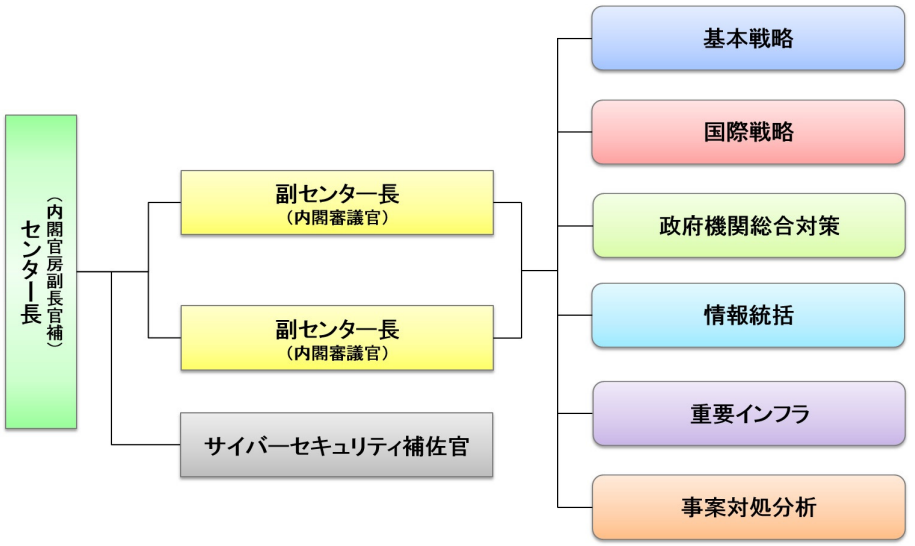
제2절 일본

1. 일본의 사이버정책 동향 일반

일본 사회에 정보통신기술(IT)의 급속한 발전과 보급에 따라, IT가 현재 모든 일상생활과 밀접하게 관련되어 있고, 사회 기반으로서 필수불가결한 것이 되었다. 이와 같이 IT의 중요성이 증대되는 반면, IT에 장애가 발생한 경우에는 국민생활과 경제활동에 큰 타격을 받을 수 있다. 2000년 2월, 인터넷의 급속한 이용 확대로 일본 사회와 국민생활의 IT화가 진전되는 과정에서, 부정엑세스 사안이 발생하고 컴퓨터 바이러스가 만연하는 등 정보시큐리티에[107] 관한 문제에 위기감이 고조되었고, 정보시큐리티 대책 추진에 관한 기획과 입안 및 종합적인 조정을 수행하기 위해 내각관방에 '정보시큐리티 대책추진실'이 설치되었다.[108] 2005년 4월에는 '정보시큐리티 문제에 대한 정부의 역할과 기능 개선방향'[109]에 근거하여, 정보시큐리티 대책추진실을 강화하고 발전시켜, 내각관방에 '정보시큐리티센터'가 설치되었다.[110] 정보시큐리티센터는 같은 시기에 IT전략본부 산하에 설립된 '정보시큐리티 정책회의'의 사무국으로서의 역할도 겸하였다. 2014년에는 관공서와 기업으로부터 정보유출이 발생하여 사이버안전의 확보가 시급한 과제가 되고 있는 상황에서 2014년 11월 '사이버시큐리티기본법'이 제정되었다. 사이버시큐리티기본법은 사이버시큐리티의 개념을 법적으로 정립하고, 국가와 지방공공단체 등 관계자의 책무를 명확히 함과 동시에 사이버시큐리티 정책에 관한 정부의 사령탑으로서 2015년 1월 내각에 '사이버시큐리티 전략본부'를 설치하고, 국가 행정기관에 대한 권고권한 등을 부여하였다.[111] 또한, 내각관방에 '내각사이버시큐리티센터'(National center of Incident readiness and Strategy for Cybersecurity, 이하 'NISC'라 함)'를 설치하였다.[112] 내각사이버시큐리티센터의 조직 구성은 다음과 같다.[113]

---

107) 일본은 'security'를 일본어로 'セキュリティ'(시큐리티)로 사용하고 있어서, 본 보고서에서는 해당 국가가 채택한 용어를 그대로 사용하기로 한다.
108) 内閣官房 情報セキュリティ對策推進室の設置について, 内閣總理大臣決定(2000.2.29).
109) 情報セキュリティ問題に取り組む政府の役割·機能の見直しに向けて, IT戰略本部決定(2004.12.7.).
110) 情報セキュリティセンターの設置に関する規則, 内閣總理大臣決定(2005.4.20.).
111) サイバーセキュリティ戰略, 内閣サイバーセキュリティセンター(2015.9.4.), p.1.
112) 内閣サイバーセキュリティセンター, 内閣サイバーセキュリティセンター(NISC)設置までの経緯, 〈http://www.nisc.go.jp/about/details.html〉.



[그림 2-2-1] 내각사이버시큐리티센터 조직체계

2. 사이버안전 정책

가. 사이버시큐리티 기본법

일본은 사이버시큐리티 기본법 제정 이전에 정보화 분야의 기본법인 '고도정보통신네트워크사회형성기본법'에 의거하여 정보시큐리티정책회의, 정보시큐리티센터 등 관련 기구들을 설치하고 관련 정책을 추진해 왔다. 그러나 사이버공간에서의 위협요소가 증가하고 복잡해졌으며, 국가안보 차원에서도 사이버안전의 강화와 사이버공간에서의 대응을 제시할 필요가 있었다. 이러한 기본법 제정의 필요성이 대두됨에 따라 사이버시큐리티 기본법은 2014년 6월 일본 국회에 법안이 제출되었으며, 같은 해 10월과 11월에 의회를 통과하여 공포·시행되었다. 동법은 총칙, 사이버시큐리티전략, 기본시책, 사이버시큐리티전략본부의 총 4개 장으로 구성되어 있으며, 35개 조문과 4개의 부칙으로 이루어져 있다.

113) 内閣サイバーセキュリティセンター, 内閣サイバーセキュリティセンター(NISC)の組織体制.

1) 목적

동법은 사이버시큐리티 관련 시책의 기본 이념을 정하고 국가 및 지방공공단체의 책무 등을 분명히 하며 사이버시큐리티 전략 수립, 기타 사이버시큐리티 관련 시책의 기본이 되는 사항을 정하고, 사이버시큐리티 전략본부 설치 등에 의하여 사이버시큐리티 관련 시책을 종합적·효과적으로 추진하고 경제사회의 활력 향상, 지속적 발전 및 국민이 안전하고 안심하고 살 수 있는 사회 실현을 도모하는 것과 동시에 국제사회의 평화와 안전 확보 및 일본의 안전 보장에 기여하는 것을 목적으로 한다.[114]

2) 정의

사이버시큐리티란, 전자적·자기적 방식 등 사람의 지각에 의해 인식될 수 없는 전자적 방식에 의하여 기록·발신·전송·수신되는 정보의 누설·멸실·훼손의 방지 및 기타 안전관리를 위한 조치, 정보시스템 및 정보통신네트워크의 안전성 및 신뢰성 확보를 위한 조치가 강구되고 그 상태가 적절하게 유지되는 것을 의미한다. 정보시스템 및 정보통신네트워크의 안전성 및 신뢰성 확보를 위한 조치에는, 정보통신망 또는 전자적 기록매체를 통하여 전자계산기에 대한 부정활동으로 인한 피해를 방지하기 위해 필요한 조치를 포함한다.[115]

3) 기본이념 및 책무

사이버시큐리티 관련 시책의 기본이념으로는, 사이버시큐리티 위협에 대하여 국가, 지방공공단체, 중요사업기반사업자 등 다양한 주체가 연계하여 적극 대응하도록 하고, 국민 개개인의 사이버시큐리티 관련 인식을 제고하고 자발적으로 대응하도록 하는 동시에, 피해 방지와 신속한 복구를 위한 체제를 구축하는 대책을 적극적으로 추진하여야 한다고 규정한다. 그 밖에 인터넷 및 기타 고도정보통신네트워크 정비와 정보통신기술 활용에 의한 활력있는 경제사회 구축 대책 추진, 사이버시큐리티 관련 국제질서의 형성과 발전에 선도적 역할 담당, 국민의 권리를 부당하게 침해하지 않을 것 등을 기본 이념으로 하고 있다.[116]

---

114) サイバーセキュリティ基本法(平成26年 法律第104號) 제1조.
115) サイバーセキュリティ基本法 제2조.
116) サイバーセキュリティ基本法 제3조.

또한, 동법에서는 국가, 지방공공단체, 중요사회기반사업자, 사이버 관련 사업자, 교육기관, 국민의 기본 책무를 각각 규정하고 있다. 국가는 사이버시큐리티 관련 시책의 기본 이념에 따라 종합적인 시책을 수립하고 실시하여야 하고, 지방공공단체는 기본이념에 따라 국가와 역할을 분담하여 사이버시큐리티에 관한 자율적 시책을 수립하고 실시할 책무를 갖는다. 사업자들은 적극적으로 사이버시큐리티 확보를 위해 노력하고 국가 및 지방공공단체의 시책에 협력하여야 한다.[117]

4) 사이버시큐리티 관련 사건 대응

국가는 사이버시큐리티 관련 범죄의 단속과 그 피해의 확대 방지를 위하여 필요한 시책을 강구한다. 또한 국가안전에 중대한 영향을 미칠 우려가 있는 사이버시큐리티 관련 사태에 대응하기 위하여 관계기관의 체제를 강화하고, 기관 간 상호협력 강화 및 역할 분담에 필요한 시책을 마련한다. 정부는 긴급사태에 상당하는 사이버시큐리티 관련 사건, 기타 정보통신망 또는 전자적 기록매체를 통한 전자계산기에 대한 부정활동으로 인하여 국민생활 및 경제활동의 기반이 되는 기능이 정지 또는 저하된 경우, 국민생활 및 경제활동에 중대한 영향의 발생을 방어하는 능력을 강화하기 위한 시책을 검토한다.[118]

5) 국제협력

국가는 산업진흥 및 국제경쟁력 강화를 위하여 사이버시큐리티 관련 첨단연구개발의 추진, 기술 고도화, 인재육성, 경영기반 강화 및 신규사업 개척, 기술의 안전성 및 신뢰성 관련 규격 등의 국제표준화 및 상호승인구조 참가 등 필요한 시책을 강구한다. 한편, 연구개발 발전을 위하여 사이버시큐리티 관련 연구체제 정비, 기초연구 및 기반적 기술의 연구개발 추진, 연구자 및 기술자 육성, 국가연구기관과 대학·민간 등의 연계 강화, 연구개발을 위한 국제협력 등 필요한 시책을 강구한다. 인재확보를 위하여 국가는 대학, 고등전문학교, 전수학교, 민간사업자 등과 협력을 도모하면서 사이버시큐리티 관련 사무종사자의 적절한 처우 확보, 자격제도 활용, 청년기술자 양성 등 필요한 시책을 강구한다. 일반 국민에 대해서는 사이버시큐리티 관련 교육

117) サイバーセキュリティ基本法 제4조-제9조.
118) サイバーセキュリティ基本法 제17조, 제18조 및 부칙 제3조.

및 학습 진흥, 지식보급 등 필요한 시책을 강구하며, 이러한 시책을 위한 행사 실시, 중점 교육기관 지정 등을 시행한다.[119] 또한, 국가는 사이버시큐리티 국제규범의 수립에 주체적으로 참여하고, 국가 간 신뢰구축 및 정보공유, 개발도상지역의 사이버시큐리티 역량구축 지원 등 국제적인 기술협력, 범죄 단속 및 기타 국제협력을 추진하고, 일본의 사이버시큐리티에 대하여 다른 국가들의 이해 증진을 위한 시책을 강구하여야 한다.[120]

6) 사이버시큐리티 전략 수립

정부는 사이버시큐리티에 관한 시책을 종합적이고 효과적으로 추진하기 위하여 사이버시큐리티 전략을 수립하고, 전략을 원활하게 실시하기 위하여 필요한 조치를 강구한다. 사이버시큐리티 전략에는 사이버시큐리티 관련 시책의 기본 방침, 국가행정기관 등의 사이버시큐리티 확보에 관한 사항, 중요사회기반사업자 및 지방공공단체의 사이버시큐리티 확보 촉진에 관한 사항, 기타 시책의 종합적이고 효과적인 추진에 필요한 사항을 정한다. 정부는 사이버시큐리티 전략 수립 시 지체없이 의회에 보고하고, 인터넷 또는 기타 적절한 방법으로 공표하여야 한다.[121]

7) 사이버시큐리티 전략본부 설치

사이버시큐리티에 관한 시책을 종합적·효과적으로 추진하기 위해 내각에 사이버시큐리티 전략본부를 설치한다. 사이버시큐리티 전략본부의 업무는 사이버시큐리티 전략 수립·실시, 국가행정기관 및 독립행정법인의 사이버시큐리티 관련 대책 기준 작성과 사이버시큐리티 관련 대책 기준에 따른 시책의 평가 등 해당 기준에 근거한 시책 실시·추진, 국가행정기관에서 발생한 사이버시큐리티 관련 중대사건에 대한 시책 평가, 기타 관련 시책의 중요 사항 기획에 관한 조사·심의, 시책 실시에 필요한 종합적 조정 등에 관한 사무를 주관한다.[122]

---

119) サイバーセキュリティ基本法 제19조-제22조.
120) サイバーセキュリティ基本法 제23조.
121) サイバーセキュリティ基本法 제12조.
122) サイバーセキュリティ基本法 제14조, 제15조.

나. 신 사이버시큐리티 전략

일본은 2013년 6월에 국가전략으로서 '사이버시큐리티 전략'을 공표하였고,[123] 2015년 9월 4일에 내각의회의 결정으로 IT환경의 발전과 법제 정비에 따른 새로운 '사이버시큐리티 전략'을 발표하였다.[124] NISC에서는 동 전략에 기초하여 사이버시큐리티 정책에 관한 종합적인 조정을 수행하고, '세계를 선도하는, 강력하고 활력있는' 사이버 공간의 구축을 위해 다양한 활동을 추진하고 있다. 일본의 사이버시큐리티에 관한 국가전략의 내용은 다음과 같다.

1) 목적

신 사이버시큐리티 전략은 사이버시큐리티 기본법에 기초하여 작성되었다.[125] 동 전략은 향후 약 3년간 기본적인 시책의 방향성을 제시하고 사이버공간에 대한 일본의 방침을 국내외에 명확하게 전달하며, 전략을 실천함으로써 '자유롭고, 공정하고 안전한 사이버공간'의 창출을 위해 적극 노력하고, '경제사회 활력 향상 및 지속적인 발전', '국민이 안전하게 안심하고 살아갈 수 있는 사회의 실현', '국제사회의 평화와 안정 및 일본의 안전 보장'에 기여하고자 한다.[126]

2) 기본 원칙

동 전략의 목적 달성을 위한 시책 수립 및 시행에 있어 다음의 기본원칙을 따르도록 하였다.[127]

(1) 정보의 자유로운 유통 확보

사이버 공간은 새로운 창의력과 발상의 장으로서, 자유로운 정보의 유통 확보가 그 발전의 기반이 된다. 이를 위해 일본은 사이버 공간에서 발신된 정보가 도중에 부당하게 검열되거나 부정하게 개·변조되지 않고, 의도한 수신인에게 도달하는 공간으로 창조되고 유지되도록 한다. 또한 사이버 공간에 적용되는 규범을 검토하는 경우

123) サイバーセキュリティ戦略, 情報セキュリティ政策会議決定(2013.6.10).
124) サイバーセキュリティ戦略(2015.9.4.).
125) サイバーセキュリティ基本法 제1조.
126) サイバーセキュリティ戦略(2015.9.4.), p.1.
127) サイバーセキュリティ戦略, pp.5-6.

에, 정보의 자유로운 유통을 최대한 존중하고, 프라이버시를 배려하며, 해당 규범과 프라이버시 확보의 적정한 균형에 대하여 충분히 고려하여야 한다.

⑵ 법치주의

사이버 공간을 실공간과 마찬가지로 모든 사람들에게 동등하게 개방되고, 안전하며 신뢰할 수 있는 공간으로 발전시키기 위해서는 사이버공간에서도 법치주의가 관철되어야 한다. 국내적으로는 사이버 공간에 법률과 시행령 등 규범이 적용되고 있으며, 마찬가지로 국제법을 비롯한 국제규범도 사이버공간에 적용되어 국제적인 법의 지배가 확립되어야 한다. 또한 사이버 공간이 확대되어 전세계 다양한 이용 주체가 참여하는 가운데, 국제사회의 평화와 안정을 위해서는 보편적 가치에 의거한 국제규범의 창설이 요구된다. 일본은 이러한 규범의 국제적 확립과 실천에 적극적으로 기여하고자 한다.

⑶ 개방성

사이버 공간은 일부에게 점유되어서는 안 되며, 참여를 원하는 모든 사람에게 상시 개방되어야 한다. 이러한 개방성 하에서 상호운용성을 확보함으로써 아이디어와 지식을 결부하여 새로운 가치를 창출할 수 있게 될 것이다.

⑷ 자율성

인터넷은 오랫동안 다양한 참여주체에 의한 자율적인 거버넌스를 통하여 발전해 왔다. 사이버 공간에서의 위협이 국가가 대처해야 하는 과제가 되었더라도, 사이버 공간의 질서유지를 국가가 전적으로 대체하는 것은 불가능하며 적절하지도 않다. 일본은 사이버 공간의 질서와 창조성의 공존을 실현하는 것을 목표로 하여, 인터넷의 자율성을 존중하고, 각자의 주체적인 행동에 의한 관리를 기조로 하여 사이버 공간을 둘러싼 다양한 사회 시스템이 각각 그 기능과 임무를 실현하고, 악의적인 행동을 억지해 나가는 자율적 메커니즘을 구축·운영하도록 추진한다.

⑸ 다양한 주체의 협력

사이버 공간은 모든 계층에서 다양한 주체가 활동하여 구축된 다차원적 세계이다. 때문에 정부에 한정되지 않고, 중요인프라사업자, 기업, 개인 등 사이버 공간에 관련된 모든 이해관계자가, 사이버시큐리티에 관한 비전을 공유하고, 각각의 역할과 책무를

다하며 노력하여야 한다. 그리고 정부는 이들 이해관계자의 실시간 정보공유 등 적절한 협력관계를 촉진하는 역할을 부담하여야 한다.

3) 추진 시책

사이버시큐리티 전략의 목적을 달성하기 위하여 상술한 5개 기본원칙에 기초하여, 전략이 기여하는 정책영역별로 향후 3년간 시행할 여러 시책의 목표와 실시 방침을 정한다. 이 때 각 시책은 사이버공간의 내재적 취약성을 고려하여 선제적 수단으로 필요한 정책을 마련하고, 민간부문이 주체적으로 구축해 온 공간이라는 점을 기반으로 민간이 자발적이고 주도적으로 대응할 수 있는 정책을 추진한다. 또한 실공간과 사이버공간의 융합이 심화되고 있어서 사이버공간에서의 현상이 사회에 영향을 미치는 점을 고려하여, 융합정보사회에로의 이행과정을 인식하고 그 변화를 파악하여 반영하는 정책을 도모한다.[128]

(1) 경제사회의 활력 향상 및 지속적인 발전

융합정보사회에서 네트워크를 활용한 사물인터넷(Internet of Things, 이하 'IoT'라 함)과 빅데이터를 활용한 새로운 서비스가 가능한 시스템이 보급됨에 따라 사이버공간과 실공간의 융합이 고도로 심화되고 있다. 이에 따라 안전한 품질을 확보한 IoT 시스템 창출, 시큐리티 마인드를 갖는 기업경영 추진, 시큐리티에 관한 비즈니스 환경 정비를 위하여 전략적인 시책을 추진한다. 이는 IoT 시스템의 시큐리티에 관한 체계 및 제도 정비와 더불어 기술개발과 신규사업을 진흥하고, 경영능력을 갖춘 사이버시큐리티 인재를 양성하며, 사이버시큐리티 관련 산업의 진흥과 더불어, 국내 관련 산업의 국제경쟁력 고취를 위한 데이터 시큐리티 확보와 서플라이체인 리스크(supply chain risk)에[129] 대한 대책도 추진하여야 한다.[130]

(2) 국민이 안전하게 안심하고 살 수 있는 사회 실현

국민의 개인정보와 재산을 비롯하여 실생활에 악영향을 미치는 사이버 공간의 위협

128) サイバーセキュリティ戦略, p.8.
129) IC칩을 포함한 기기와 시스템의 설계, 제조, 조달, 설치, 운용단계에 있어서의 리스크로서, 이들 단계에서 바이러스를 포함하는 악의적인 프로그램을 설치하는 등의 리스크를 포함한다. サイバーセキュリティ戦略, p.16.
130) サイバーセキュリティ戦略, pp.8-14.

에 대응하여, 국민이 안전하게 안심하고 살 수 있는 사회를 실현하기 위한 대책을 실시한다. 이에 따라 안전한 사이버공간 이용환경을 구축하고, 사이버공간 이용자의 인식을 제고하며, 인터넷뱅킹을 악용한 부정송금사건과 정보 절취 등 사이버범죄에 대한 대책을 강화한다. 또한 중요 사회기반시설의 보호를 위한 시책을 지속적으로 추진하고, 정부기관 등의 사이버시큐리티를 확보하여 기존의 위협은 물론 장래의 위협에 대해서도 유연하고 신속하게 대응할 수 있도록 정보시스템의 방어력을 강화하고 다각적인 대책을 추진한다.[131]

(3) 국제사회의 평화·안정 및 일본의 안전보장

사이버공간에서의 다양한 가치관을 인정하고 자율성을 존중하며, 언론과 기업행동을 법치주의로 보장하는 것이 국제사회의 평화와 안정을 실현하는 길이다. 이를 위하여 국내적으로는 사이버공격에 대한 대처 능력을 강화하고, 첨단기술을 안전보장에 활용하여 정부기관 및 사회 시스템을 방호하는 것이 필요하다. 한편 국제사회의 평화와 안정을 위해서는 사이버시큐리티의 확보와 정보의 자유로운 유통을 양립할 필요가 있고, 국제규범의 형성과 시행 및 국제사회의 신뢰구축, 사이버테러에 대한 적절한 대응, 각국의 역량 강화를 위하여 협력하여야 한다.[132] 이를 위한 추진시책에 관해서는 별도의 항목에서 상술하기로 한다.

(4) 횡단적 시책

위 세 가지 정책목표를 달성하기 위하여 연구개발 추진, 인재육성 및 확보 등 다방면에서의 횡단적이고 중장기적인 대책의 추진과 더불어, 민관 및 관계부처의 사업과 제도를 유연하게 활용하여 추진하도록 한다.[133]

4) 국제사회의 평화와 안정 및 일본의 안전보장을 위한 추진 시책

자유롭고 공정하며 안전한 사이버공간은 전세계적으로 커뮤니케이션이 가능한 글로벌 공통의 공간이며, 국제사회의 평화와 안정의 근간이 된다. 일본은 이러한 사이버공간에서의 다양한 가치관을 인식하고 자율성을 존중하며, 언론과 기업활동을 법에

131) サイバーセキュリティ戦略, pp.15-24.
132) サイバーセキュリティ戦略, pp.25-32.
133) サイバーセキュリティ戦略, pp.33-37.

의해 보장하는 것이 국제사회의 평화와 안정을 실현하고 번영으로 이끄는 길이라고 확신하고 있다. 현재 일본은 사이버공간을 활용함으로써, 평화롭고 안정적이며 지속적 발전이 가능한 경제 사회를 실현해 왔다. 반면에 국제적·국내적으로, 사이버공간에 대한 사회시스템의 의존도는 높아지고, 사이버공격의 수법과 영향이 심화됨에 따라 실공간 경제사회활동에 중대한 영향을 미치고 있다. 이에 사이버공격에 대하여 적절히 대처하고 사이버공간의 안전한 이용을 확보하는 것은, 국제사회의 평화와 안정 및 일본의 안전보장을 위하여 조속히 추진해야 할 중요한 과제이다. 이러한 과제에 대하여 국가 안전을 확보하기 위해서는 국가 전체의 대처능력을 근본적으로 강화하고, 동맹국과의 협력 및 연합과 국가간 신뢰 구축이 필요하다. 또한 정보의 독점, 통제, 검열, 절취, 파괴 및 테러리스트 등의 비국가주체에 의한 사이버공간의 악용 등 행위에 강력하게 대처하고, 국제협력의무에 근거한 '적극적 평화주의'로서 국제사회의 평화와 안정을 실현하고 국제 질서 유지에 적극적으로 공헌하면서 국내 안전보장을 확보하고자 한다. 이를 위하여 다음과 같은 전략적 접근을 추진한다.

(1) 국가 안전 확보

사이버공간과 실공간과의 융합이 진행되고 있고, 여러 조직이 사이버공간에 대한 의존도가 높아짐에 따라, 사이버공격에 의해 한 국가의 정치, 사회, 경제, 문화에 강한 타격을 줄 수 있게 되었다. 현재 사이버공간은 경제활동뿐만 아니라 안전보장과 인텔리젼스 활동의 장이 되어 국가 및 조직에 의한 사이버공격이 현실적인 위협이 되고 있다. 따라서 악의적인 사이버 활동으로부터 국가 안전 확보를 위하여 국내적으로 대응기관의 능력을 강화하고, 일본의 선도적 기술을 방호 활동에 활용하며, 정부기관과 사회시스템의 안전을 확보하여야 한다.

(2) 국제사회의 평화와 안정

국제사회의 평화와 안정을 위해서는 사이버시큐리티의 확보와 함께 글로벌 차원에서 정보의 자유로운 유통을 양립시켜야 한다. 이를 위해서는 사이버공간에 적용도는 국제적 규범을 확립하여 이를 이행할 수 있도록 적극적인 조직체계를 갖추어야 한다. 일본은 개별적, 구체적인 국제법의 사이버공간에의 적용에 대한 논의에 적극 참여하여 국제 규칙과 규범의 형성에 기여하고자 한다. 유엔을 비롯한 OECD, APEC 등

국제사회의 논의에서도, 경제사회적 측면과 인터넷 거버넌스에 역점을 둔 논의가 진행되고 있으며, 일본은 이러한 논의에서 국내외 각 주체와 협력하여 사이버공간의 개방성과 상호운용성, 자율성, 정보의 자유로운 유통을 확보하여 사회, 경제, 문화의 발전에 기여하기 위한 노력을 추진하고 있다. 이와 더불어 국제적인 신뢰구축 조치와 사이버분야의 역량강화에 대한 협력, 그리고 사이버공간을 악용한 국제 테러 조직활동에 대한 대책에 있어서도 필요한 정보 수집 및 분석 등 조치를 강화하도록 한다. 또한 사이버공간에 관한 기술적 지식을 보유하면서 각국의 상황과 국가안전보장, 국제협력 등에도 정통한 국제적인 인재를 정부 및 민간 차원에서 육성하고 증강시켜 나갈 것이다.

(3) 세계 각국과의 협력·연합

국제협력은 국가의 관여가 의심되는 고도의 사이버공격에 대한 국제적 대응력 강화를 위하여 필수적이다. 일본은 미 - 일 동맹을 기본 축으로 하여 각국과의 협력관계를 확대, 심화하는 한편, 사이버공격을 발단으로 하는 예측불가능한 사태의 발생을 방지하기 위하여 신뢰를 구축하고 광범위한 국제협력체제를 확립함으로써 사이버공간의 안전을 확보하고자 한다.

그 중에서 아시아·태평양 지역은 일본과의 역사적 관련성이 높고 국가간 투자의존성도 높다. 동 지역에서의 다양한 채널을 통하여 사이버분야에서의 국제협력과 역량강화에 협력하고, 정보의 수집과 소통을 강력하게 추진하도록 한다. 그리하여 사이버 관련 시책과 사이버공격에 관한 정보 공유 및 활용, 사이버공격에 대한 공동훈련 등 사이버분야에 있어서 전략적 파트너와의 협력관계를 심화시키고, 사이버공간에 관한 지역적 국제적 제문제에 대한 공동의 대응을 도모하도록 한다.

또한, 미주, 유럽, 중남미, 중동아프리카 지역에 대해서도 협력체제를 도모하고 강화하는 시책을 추진하고 있다.

5) 추진 체계

이 전략의 추진을 위하여 사이버시큐리티 전략본부가 사령탑 역할을 하고 NISC가 그 사무국으로서 여러 시책을 추진하기 위하여 주도적 역할을 담당하도록 한다. 이를 위하여 전략본부는 각 행정기관의 정보시스템에 대한 부정적인 활동 감시, 감사, 원인

규명 조사 등 사무를 수행하고, 국내외 사이버시큐리티 관련 정보 집약, 분석, 국제협력, 각 부처의 시큐리티 인재육성 등 정부의 사이버시큐리티 관련 능력을 증진시키는 기능을 담당한다. NISC는 사건 발생 시에 적절하게 정보가 집약되어, 정부의 적절한 대응이 이루어지도록 관계부처와의 신속한 정보공유체제를 구축하는 등 필요한 대책을 추진한다.

정부기관은 소관 사무를 수행하기 위하여 NISC와 협력하며, 사이버시큐리티에 필요한 대책을 실시하고, 소관 조직 및 사업자와의 정보공유와 필요한 권고를 적절히 행하는 책무를 담당한다. 위기관리 대응에 있어서는 사이버시큐리티 전략본부장에 의한 권고조치를 비롯하여 사이버공격 등 사건에 관하여 정부로서의 대처와 대책상황 확인 방법 등을 개선하고 한층 강화하도록 한다. 고도의 기술과 계획성을 동반하여, 국가의 관여가 의심되는 사이버공격이 최근 증가하고 있으며, 이러한 공격에의 대응은 일본의 위기관리, 안전보장에 있어서도 중요한 과제이다. 사이버시큐리티 전략본부는 필요에 따라 중대테러대책본부 등 위기관리체제와 정보를 공유하고 협력하며, 안전보장에 관한 문제에 대해서는 국가안전보장회의와 긴밀하게 협조하여 대응하도록 한다.[134]

3. 사이버범죄 정책

일본은 정보통신네트워크의 발전이 사회 경제활동의 근간을 이루는 중요한 시스템이라는 점을 인식하는 한편, 사이버범죄의 증가, 인터넷상 위법·유해정보의 범람, 컴퓨터 바이러스의 만연이 사회문제가 되면서 사이버공간에 대한 국민의 불안감이 고조되고 있으므로, 민관이 협력하여 효과적인 사이버안전 대책을 검토하고 실시할 필요성이 제기되고 있다.

이에 따라 일본은 2001년부터 정보시큐리티에 관한 산업계와 정부기관의 협력방안, 특히 경찰과의 협력방안에 관한 의견 교환을 목적으로 경찰청 생활안전국 주관하에 '종합시큐리티대책회의'를 개최하고 있다. 동 회의에서는 정보시큐리티에 관한 전문가, 전기통신사업자, 컨텐츠사업자, 컴퓨터 제조판매업자, 소프트웨어산업 등 각

134) サイバーセキュリティ戦略, pp.38-39.

종 사업 관련자 및 법조계, 교육계, 방범단체 등 광범위한 분야에서 의견 교환이 활발하게 이루어지고 있고, 매년 다양한 보고서를 발간해 왔다. 이러한 의견을 반영하여 2006년 인터넷 핫라인센터 운영 개시, 2008년 영화공유 소프트웨어를 악용하는 저작권침해대책협의회 발족, 2009년 6월 아동 포르노그래피 유통방지협의회 발족, 2012년 부정접속금지법 개정, 2014년 재단법인 일본사이버범죄대책센터 창설 등이 진행되어 왔다. 종합시큐리티대책회의 연간 주제는 다음과 같다.[135]

〈표 2-2-1〉 종합시큐리티대책회의 연간 주제

개최연도	주 제
2001	정보시큐리티 대책에 있어서 협력 추진
2002	정보시큐리티에 관한 위협의 실태파악·분석
2003	민관 정보시큐리티 관련 정보의 공유방안
2004	인터넷 일반이용자 보고 및 지적재산권 침해에 관한 민관 협력방안
2005	인터넷상 위법·유해정보에 대응하는 민관 협력방안
2006	인터넷 핫라인센터 운영방안 및 인터넷카페 등의 익명성 기타 문제과 대책
2007	Winny 등 파일공유 소프트웨어를 이용한 저작권침해문제와 대응방안
2008	인터넷상 아동 포르노그라피 유통에 관한 문제와 대책
2009	인터넷 경매에서의 도난품 유통방지대책
2010	안전하고 책임있는 사이버 시민사회 실현을 위한 대책 (1) 부정접속대책 (2) 위법·유해정보 대책 (3) 사이버방범자원봉사자육성
2011	사이버 범죄수사에서 사후추적가능성의 확보
2012	민관 협력의 위법·유해정보 대책의 새로운 추진방안 사이버 범죄수사의 과제와 대책
2013	사이버공간의 위협에 대처하기 위한 산관학 협력방안 — 일본판 NCFTA의 창설을 목표로 —
2014	민관 협력을 통한 사이버범죄에 대처하기 위한 인재육성 등

135) 警察廳, サイバー犯罪對策, 綜合セキュリティ對策會議, 〈http://www.npa.go.jp/cyber/csmeeting/index.html〉 참조.

가. 사이버범죄 관련 법제

일본이 사이버범죄에 대응하여 시행하고 있는 개별 법률에는 '부정접속행위금지등에 관한 법률', '형법', '인터넷 이성소개사업을 이용하여 아동을 유인하는 행위 규제 등에 관한 법률', '청소년이 안전하게 안심하고 인터넷을 이용할 수 있는 환경정비 등에 관한 법률'이 있다.

1) 부정접속행위금지등에 관한 법률

컴퓨터 및 정보통신상의 부정접속행위와 조장행위를 규제하기 위하여 '부정접속행위금지등에 관한 법률'이 1999년 8월 13일 법률 제128호로 제정, 2000년 2월 13일부터 시행되고 있다.

(1) 목적

부정접속행위금지등에 관한 법률[136]은 부정접속행위를 금지하고 재발 방지를 위해 부정접속행위를 관리하는 접속 관리자에 대하여 도도부현공안위원회(都道府縣公安委員會)의 지원 조치 등을 규정함으로써, 전기통신회선을 통하여 행해지는 전자계산기에 관한 범죄[137] 방지 및 접근제어기능에 의하여 실현되는 전기통신에 관한 질서의 유지를 도모하여, 고도정보통신사회의 건전한 발전에 기여하는 것으로 목적으로 한다.

(2) 기본 구성

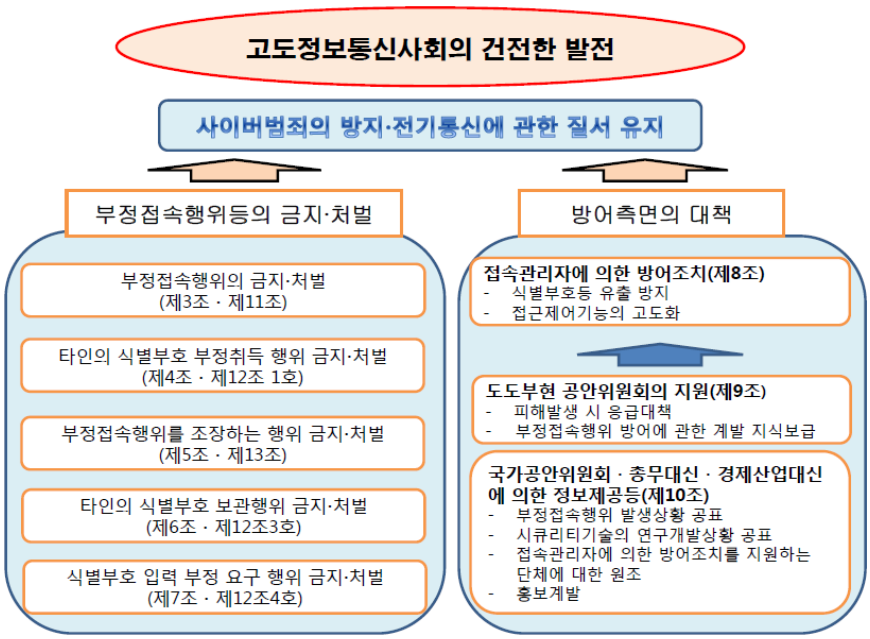
동법은 부정접속행위등의 금지·처벌과 같은 행위자에 대한 규제와, 부정접속행위의 대상이 되는 접속 관리자에게 방어조치를 요구하고 접속 관리자가 그 방어조치를 적절하게 강구할 수 있도록 행정적으로 지원하는 방어적 대책과 같은 두 가지 측면에서 부정접속행위의 방지를 도모하고자 한다. 부정접속행위 금지등에 관한 법률 개요는 다음과 같다.[138]

---

136) 不正アクセス行為の禁止等に関する法律.

137) '전기통신회선을 통하여 행해지는 전자계산기에 관한 범죄'라 함은, 전자계산기 사용사기, 전자계산기손괴등업무방해 등으로 컴퓨터 네트워크를 통하여 이에 접속한 컴퓨터를 대상으로 행해지는 범죄와, 컴퓨터 네트워크를 통하여 이에 접속한 컴퓨터를 이용해서 행하는 사기, 총기와 약물의 불법거래 등 범죄의 양자를 모두 가리킨다. 不正アクセス行為の禁止等に関する法律の解説, p.1.

138) 不正アクセス行為の禁止等に関する法律の解説, p.1.



[그림 2-2-2] 부정접속행위 금지등에 관한 법률 개요

(3) 주요 내용

동법은 부정접속행위, 타인의 식별부호를 부정하게 취득하는 행위, 부정접속행위를 조장하는 행위, 타인의 식별부호를 부정하게 보관하는 행위, 식별부호 입력을 부정하게 요구하는 행위의 금지 및 처벌을 규정하고 있다. 부정접속행위 금지를 위반한 자는 3년 이하 징역 또는 100만엔 이하 벌금에, 기타 행위 금지를 위반한 자는 1년 이하의 징역 또는 50만엔 이하의 벌금에 처하도록 하였다.[139]

부정접속행위란, 타인의 식별부호를 악용하거나, 컴퓨터 프로그램의 안전장치 미비를 이용하여 접속 권한이 없는 컴퓨터를 이용하는 행위를 말한다.[140] 동법상 부정접속행위는 '전기통신회선을 통하여' 행해지는 경우, 즉 컴퓨터 네트워크를 통하여 행하여지는 것에 한정되어 있다. 따라서 네트워크에 접속되지 않은 컴퓨터를 무단으로 사용하는 행위, 네트워크에 접속되어 접속제어기능에 의해 특정 이용이 제한되는 컴퓨터

139) 不正アクセス行為の禁止等に関する法律, 제3조-제7조, 제11조-제13조.
140) 不正アクセス行為の禁止等に関する法律の解説, p.6.

라도 당해 컴퓨터의 키보드를 직접 조작하여 무단으로 사용하는 행위는, '전기통신회선을 통하여' 행하는 것이 아니므로 부정접속행위에 해당하지 않는다.[141]

따라서 부정접속죄가 성립하기 위해서는 특정 전자계산기, 즉 컴퓨터 네트워크에 접속되어 있는 컴퓨터에 대한 것이어야 하고, 컴퓨터 네트워크를 통하여 특정 전자계산기에 접속이 이루어져야 하며, 타인의 식별부호 또는 접속제어기능에 의하여 특정이용을 제한할 수 있는 정보 또는 지령이 입력되고, 접속제어기능에 의하여 제한되어 있는 특정이용을 할 수 있는 상태로 만드는 행위가 필요하다.[142]

한편, 부정접속행위 금지에 대한 실효성을 확보하기 위하여 2012년 개정을 통해, 타인의 식별부호를 부정하게 취득하는 행위 금지 조항이 신설되었고, 부정접속을 조장하는 행위로서 규제되고 있는 타인의 식별부호의 제공범위를 확대하여, 어떤 특정 전자계산기의 특정이용에 관한 것인지가 불분명한 식별부호를 제공하는 행위를 금지하는 조항도 포함되었다. 또한 타인의 식별부호를 부정하게 취득하여, 부정접속행위 용도로 제공할 목적으로 보관하는 행위도 금지 대상으로 규정되었다.

동법은 식별부호의 입력을 부정하게 요구하는 행위, 즉 각종 피싱행위를 금지하는 규정을 두고 있다.[143] 여기에는 피싱사이트를 공개적으로 구축하여 정식 접속관리자가 공개한 웹사이트로 오인시키는 행위, 정식 접속관리자가 송신한 이메일로 오인시키는 이메일을 통하여 아이디와 비밀번호를 사취하는 행위가 포함되며, 금지되는 피싱행위에 해당하기 위해서는 이용자를 오인시키려는 의도를 갖고 행위하였을 것이 요구된다.

방어측면의 대책으로서 부정접속행위의 발생을 방지하기 위해서, 접속관리자가 방어조치를 구비하여 부정접속행위가 발생하기 어려운 환경을 정비하도록 하는 규정을 두고 있으며,[144] 접속관리자는 도도부현공안위원회에 지원을 요청하여 재발방지를 위한 자료 제공, 조언, 지도를 받을 수 있다.[145] 2012년 개정을 통하여 도도부현공안위원회는 부정접속행위의 방어에 관하여 계발 및 지식보급을 위해 노력하도록 규정되었다. 이는 이전부터 도도부현 경찰에서 수사를 통하여 축적한 지식 등을 활용하여

141) 不正アクセス行為の禁止等に関する法律の解説, p.7.
142) 不正アクセス行為の禁止等に関する法律の解説, pp.7-8.
143) 不正アクセス行為の禁止等に関する法律, 제7조.
144) 不正アクセス行為の禁止等に関する法律, 제8조.
145) 不正アクセス行為の禁止等に関する法律, 제9조.

부정접속행위를 비롯한 사이버범죄를 미연에 방지하고, 국민의 정보시큐리티에 관한 의식과 지식의 향상을 도모하기 위하여 계발 및 지식 보급 활동을 실시하여 왔으며, 이러한 지역경찰의 활동이 부정접속행위 방지에 미치는 역할의 중요성이 인정되어, 동법에서 지역공안위원회에 부정접속행위 방어에 관한 계발 및 지식보급을 도모할 책무가 있다고 명시하게 된 것이다.[146] 또한, 국가공안위원회 및 관련 부처에서 시큐리티사업자단체에게 필요한 정보를 제공하고, 그밖에 지원 조치를 하도록 규정하고 있다.[147]

2) 형법

(1) 목적

일본은 사이버범죄에 대하여 기존 형법 조항의 해석을 통하여 처벌해 왔으나, 증가하는 사이버범죄로 인한 국민의 재산과 프라이버시 침해에 대한 피해구제의 필요성과, 사이버범죄조약에의 가입에 따른 법제 정비의 필요에 따라 2011년에 형법에 사이버범죄를 다루는 조항을 추가하여 개정작업이 이루어졌다. 주요 내용으로는 전자적 기록 부정작출 및 공용을 통한 문서위조죄, 전자계산기 사용사기와 손괴 관련 업무방해죄 등이 있다. 동법상 '전자적 기록'이란 전자적 방식, 자기적 방식, 기타 사람의 지각으로는 인식할 수 없는 방식으로 작성된 기록으로, 전자계산기에 의한 정보처리 용도로 제공되는 것을 말한다.[148]

(2) 주요 내용

ⅰ) 전자적 기록 부정작출 및 공용죄

사람의 사무처리를 그르치게 할 목적으로 그 사무처리의 용도에 제공하는 권리, 의무 또는 사실증명에 관한 전자적 기록을 부정하게 작성한 자는, 5년 이하의 징역 또는 50만엔 이하의 벌금에 처한다. 이러한 범죄가 공공기관 또는 공무원에 의하여 작성되는 전자적 기록에 관련된 경우에는 10년 이하의 징역 또는 100만엔 이하의 벌금에 처한다. 권리, 의무 또는 사실증명에 관하여 부정하게 작성된 전자적 기록을

146) 不正アクセス行為の禁止等に関する法律の解説, p.16.
147) 不正アクセス行為の禁止等に関する法律. 제10조.
148) 형법 제7조의 2.

사무처리 용도로 제공한 경우에도, 해당 전자적 기록을 작성한 자와 동일한 형으로 처벌하며, 미수범에 대해서도 벌한다.[149]

ii) 지불용 카드 전자적 기록 부정작출죄

사람의 재산상 사무처리를 그르치게 할 목적으로, 해당 사무처리에 제공하는 전자적 기록으로서 신용카드 또는 기타 대금이나 요금 지불용 카드의 구성을 부정하게 작성한 자는, 10년 이하의 징역 또는 100만엔 이하의 벌금에 처한다. 예치금 인출용 카드를 구성하는 전자적 기록을 부정하게 작성한 자도 이와 같다. 이와 같이 부정하게 작성된 전자적 기록을 재산상 사무처리 용도로 제공한 자, 이러한 전자적 기록으로 구성한 카드를 양도, 대여, 매입한 자도 동일하게 처벌하며,[150] 미수범에 대한 처벌 규정도 두고 있다.[151] 한편, 부정하게 작성된 전자적 기록카드를 소지한 자는, 5년 이하의 징역 또는 50만엔 이하의 벌금에 처한다.[152]

iii) 전자계산기손괴 등 업무방해죄

사람의 업무에 사용하는 전자계산기 또는 그 용도로 제공하는 전자적 기록을 손괴하거나, 업무에 사용하는 전자계산기에 허위의 정보 또는 부정한 지령을 부여하거나, 기타 방법에 의하여 전자계산기에 사용 목적에 부합하는 작동을 시키지 않거나, 사용 목적에 반하는 작동을 시켜서 업무를 방해한 자는, 5년 이하의 징역 또는 100만엔 이하의 벌금에 처한다.[153]

iv) 전자계산기 사용사기죄

사람의 사무처리에 사용하는 전자계산기에 허위의 정보 또는 부정한 지령을 부여하여, 재산권의 득실 또는 변경에 관하여 부실한 전자적 기록을 작성하거나, 재산권의 득실 또는 변경에 관한 허위의 전자적 기록을 사무처리의 용도로 제공하여 재산상 불법의 이익을 취득하거나 타인에게 취득하도록 한 자는 10년 이하의 징역에 처한다.[154]

---

149) 형법 제161조의 2.
150) 형법 제163조의 2.
151) 형법 제163조의 5.
152) 형법 제163조의 3.
153) 형법 제234조의 2.
154) 형법 제246조의 2.

3) 인터넷 이성소개사업을 이용하여 아동을 유인하는 행위 규제등에 관한 법률

'인터넷 이성소개사업을 이용하여 아동을 유인하는 행위 규제등에 관한 법률'(이하 '인터넷만남사이트규제법'이라 함)은 2003년에 제정되었다. 이후 동 사이트의 이용에 따른 범죄가 다수 발생하게 되면서, 2008년 인터넷만남사이트사업자에 대한 규제 강화 등을 목적으로 동법의 일부가 개정되어 시행되고 있다.[155]

(1) 목적

동법은 인터넷만남사이트의 이용에서 발생하는 아동 매춘 및 기타 범죄로부터 아동을 보호하고, 아동의 건전한 육성을 도모하기 위한 것이다. 동법상 '아동'은 18세 미만의 청소년을 말하며. 인터넷만남사이트사업을 '인터넷이성소개사업'으로 규정하고 있다.

(2) 주요 내용

인터넷만남사이트 게시판에 아동을 상대로 하는 이성교제를 유인하는 게시물을 게시하는 행위는 금지된다.[156] 여기에는 아동을 성교의 상대로 하는 교제 요구, 아동을 상대로 금품을 목적으로 하는 이성교제를 요구하는 행위가 포함된다. 또한 아동이 인터넷만남사이트를 이용하는 것은 금지된다.[157]

인터넷만남사이트를 운영하는 자는, 사업신고의무, 이용자가 아동이 아니라는 사실의 확인의무,[158] 금지된 유인행위에 관한 게시물의 삭제 등의 의무가 있다.[159]

인터넷만남사이트 운영에 필요한 전기통신서비스를 제공하는 사업자는 필터링 서비스의 제공 등을 위해 노력하여야 하며, 아동의 보호자는 필터링서비스 이용 등을 위해 노력하여야 한다.[160]

---

155) インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律(이하 '出会い系サイト規制法'이라 함)の解説, 〈https://www.npa.go.jp/cyber/deai/law/index.html〉.
156) 出会い系サイト規制法 제6조.
157) 인터넷만남사이트에 아동의 이용금지를 명시하여야 한다. 이메일광고나 선전에서는 당해 이메일의 제목에 아동의 이용금지 취지를 표시하거나 '18금'으로 표시하도록 규정하고 있다. 出会い系サイト規制法施行規則 제3조.
158) 이용자가 아동이 아니라는 사실의 확인 방법에 대해서는 出会い系サイト規制法施行規則 제5조.
159) 出会い系サイト規制法 제3조, 제7조-제14조, 제16조.
160) 出会い系サイト規制法 제3조제2항, 제3항 및 제4조.

4. 시사점

일본은 사이버안전 분야의 기본법을 제정하여 국가가 추구하는 기본이념을 제시하고, 이를 바탕으로 범국가적인 사이버시큐리티 시책을 추진하기 위한 법적 근거를 마련하였다. 동법에서는 국가, 지방공공단체, 중요사회기반사업자, 사이버 관련 사업자, 교육기관, 국민 등 각 주체의 책무를 규정하고, 사이버위협에 대응과 함께 산업진흥, 연구개발, 인력양성, 국제협력 등 모든 관련 분야에서의 기본 시책을 규정하고 있다. 또한 사이버시큐리티 정책을 총괄하는 전략본부를 내각에 설치하여 총괄기구의 위상을 높이고, 국제규범 수립, 국가 간 신뢰구축 및 정보공유, 개발도상지역 지원 등 기술 협력, 범죄 단속과 같은 분야에서 국제협력 추진을 강화하도록 하였다.

2015년 9월에 발표된 신 사이버시큐리티 전략에서는 그 추진 시책의 하나로 사이버범죄에 대한 대책을 언급하고 있다. 급증하고 있는 인터넷뱅킹을 이용한 범죄, 대규모 정보유출사건 등 악의적인 사이버범죄의 실태를 파악하고, 신종 수법에 대처하기 위하여 범죄 대처능력과 수사능력 향상의 필요성, 정보수집 강화, 국제협력 체제 강화의 추진을 촉구하였다. 그리고 국제사회의 평화와 안정 실현을 위해서는 사이버공간에서의 다양한 가치관을 인정하고 자율성을 존중하며, 언론과 기업행동을 법치주의로 보장하여야 함을 강조하였다. 이를 위하여 국내적으로는 사이버공격에 대한 대처 능력을 강화하고, 첨단기술을 안전보장에 활용하여 정부기관 및 사회 시스템을 방호하는 것이 필요하며, 국제사회의 평화와 안정을 위해서는 사이버시큐리티의 확보와 정보의 자유로운 유통을 양립할 필요가 있고, 국제규범의 형성과 시행 및 국제사회의 신뢰구축, 사이버테러에 대한 적절한 대응, 각국의 역량 강화를 위하여 협력하는 시책을 추진하도록 하였다.

사이버범죄 대책을 위하여 경찰청에서는 2001년부터 '종합시큐리티대책회의'를 매년 개최하고 있다. 동 회의에서는 정보시큐리티에 관한 전문가, 전기통신사업자, 컨텐츠사업자, 컴퓨터 제조판매업자, 소프트웨어산업 등 각종 사업 관련자 및 법조계, 교육계, 방범단체 등 광범위한 분야에서 의견을 교환하여 추진과제를 제시하고 있으며, 이를 통하여 사이버범죄 관련 법제의 정비, 교육, 기관 설치 등을 시행하고 있다.

한국은 새로운 IT 환경에 대응하는 사이버 관련 기본법과 시책이 아직 체계화되지

않은 점, 총괄기구의 위상이 불명확한 점, 사고 발생 시 대응체계가 미흡한 점 등이 지적되고 있으며, 일본의 법제도 및 대응체제 정비와 국제협력 분야에 대한 폭넓은 추진 시책은 향후 한국의 관련 법령 개선과 체제 구축에 참고가 될 것으로 보인다.

제3절 중국

1. 중국의 사이버정책 동향 일반

가. 중국 사이버 정책 및 법제도 발전연혁

중국의 인터넷 관련 과학기술연구에 대한 첫 시도는 1986년 중국과학원 고능(高能) 물리연구소의 우웨이민(吴为民)이 IBM-PC에서 위성연결을 통하여 제네바 CERN에 있는 VXCERN의 왕쑤친(王淑琴) 계정으로 원격 등록하여 제네바의 Steinberger에게 이메일을 발송하면서부터 개시되었다. 1988년 3월에는 중국 내 여러 대학과 연구센터의 컴퓨터에 대하여 전세계적으로 컴퓨터 인터넷과의 접속을 목적으로 하는 중국컴퓨터과학기술인터넷(中国计算机科技网-CANET) 프로젝트가 개시되었고, 1993년 3월 12일, 당시 국무원 부총리를 역임한 주룽지(朱镕基)의 주최 하에 국가 공공경제정보통신네트워크(골든브릿지공정) 건설에 관한 회의를 개최하였다. 그해 12월 10일 국무원은 국가경제정보화연석회의(国家经济信息化联席会议) 기구의 설립을 허가하였으며, 당시 국무원 부총리인 쩌우쟈화(邹家华)가 주석을 역임하였다.[161]

1994년 2월 18일, 국무원령 제147호로 '중화인민공화국컴퓨정보시스템안전보호조례'(中华人民共和国计算机信息系统安全保护条例를 제정 및 시행하여 컴퓨터정보시스템의 안전을 보호하고 컴퓨터의 응용과 발전을 추진하고자 하였다. 1994년 4월 20일, 중국은 국제인터넷네트워크에 가입하여 77번째 회원국이 되었다. 1996년 1월 13일, 국가경제정보화연석회의는 국무원정보화사업영도소조판공실(国务院信息化工作领导小组办公室)로 변경되었으며 쩌유쟈화(邹家华) 부총리가 영도소조 조장을 담

161) 中国国家互联网信息办公室 , 1986년-1993년 인터넷대사기(互联网大事记), 〈http://www.cac.gov.cn/2009-04/10/c_126500533.htm〉, 2015년 8월 18일 검색.

당하였다. 1996년 2월 1일, 국무원 제195령으로 '중화인민공화국컴퓨터정보네트워크국제접속관리잠정규정'(中华人民共和国计算机网络国际联网管理暂行规定)을 제정 및 시행하여 국제인터넷접속에 대하여 처음으로 규정하였으며, 1997년 12월 30일, '컴퓨터정보네트워크국제접속안전보호관리법'(计算机信息网络国际联网安全保护管理办法)을 제정 및 시행하여 인터넷 국제네트워크을 이용하여 국가안전을 침해하고 국가비밀을 누설하는 불법행위를 규제하기 시작하였다. 1997년 4월, 전국 정보화사업 회의에서 '국가정보화95계획과 2000년비전목표'(国家信息化九五规划和2000年远景目标)를 논의, 통과시켰고, 중국인터넷네트워크를 국가정보기초시설건설에 포함시켰다. 1998년 3월, 우체부와 전자공업부를 합병하여 신식산업부(信息产业部)를 설립하였으며, 같은 해 8월에 공안부는 공공정보네트워크안전감사국(公安部公共信息网络安全监察局)을 설립하여 컴퓨터 네트워크 안전을 수호하고 사이버 범죄를 조사하도록 하였다. [162] 1999년 2월, 중국 국가정보안전검측평가인증센터(中国国家信息安全测评认证中心-CNISTEC)가 정식으로 운영을 시작하였으며, 1999년 12월 23일, 국가정보화사업영도소조판공실을 국가정보화추진사업판공실(国家信息化推进工作办公室)로 변경하고 당시 국무원 우빵궈(吴邦国) 부총리가 조장으로 부임하였다.[163]

2000년 1월 1일, '컴퓨터정보시스템국제접속비밀준수관리규정'을 시행하였고, 2000년 9월 25일, '전신조례'(电信条例)와 '인터넷정보서비스관리방법'(互联网信息服务管理办法)을 시행하게 되면서, 전신업무가 법제화 단계에 접어들게 되었다. 2000년 10월 11일, 중국공산당 제15기 제5차 전체회의에서는 '국민경제와 사회발전 관련 제10차 5년 계획 제정에 관한 중공중앙 건의'를 채택하고, "국민경제와 사회정보화를 적극 추진하는 것은 전면적인 현대화를 건설하는 전략적 조치이다. 정보화를 통하여 공업화를 이끌고 후발우세를 발휘하여 사회 생산력의 혁신적인 발전을 이룩할 것"을 제안하였다. 2000년 12월 28일, '인터넷안전 수호에 관한 전국인민대표대회상무위원회의 결정'(全国人民代表大会常务委员会关于维护互联网安全的决定)을 시행하고 인터넷 안전을 침해하는 행위에 대한 형사처벌 조치를 처음으로 규정하였다. 2001년

162) 中国国家互联网信息办公室 , 중국인터넷접속20년대사기(中国接入互联网20年大事记), 〈http://www.cac.gov.cn/2014-04/20/c_126417746.htm〉, 2015년 8월 18일 검색.
163) 中国国家互联网信息办公室, 1997년-1999년 인터넷대사기(互联网大事记), 〈http://www.cac.gov.cn/2009-04/12/c_126500441.htm〉, 2015년 8월 18일 검색.

8월 23일, 국가정보화영도소조가 다시 설치되면서, 당시 중앙정치국 상무위원이고 국무원 총리인 주룽지가 조장을 담임하였다. 2001년 9월 7일, '정보산10차5개년계획'(信息产业'十五'规划纲要)이 공표되었으며,[164] 2002년 7월 3일, '소프트웨어산업 진흥행동개요'(振兴软件产业行动纲要)가 공표되었다. 2004년 8월 28일, '전자서명법'(电子签名法)이 통과되어 2005년 4월 1일부터 시행에 들어갔다.[165] 2005년 11월 3일 '국가정보화발전전략(2006-2020)'(国家信息化发展战略2006-2020)이 통과되었으며,[166] 2007년 11월 1일 '정보안전기술 - 정보안전리스크평가규범'(信息安全技术 - 信息安全风险评估规范)(GB/T 20984-2007), '정보안전기술 - 홍채식별시스템기술요구'(信息安全技术 - 虹膜识别系统技术要求)(GB/T20979-2007), '정보안전기술 - 온라인은행시스템정보안전보장평가준칙'(信息安全技术 - 网上银行系统信息安全保障评估准则)(GB/T20983-2007), '정보기술 - 안전기술 - 정보안전사건관리지침'(信息技术 - 安全技术 - 信息安全事件管理指南)(GB/Z20985-2007), '정보안전기술 - 정보안전사건분류분급지침'(信息安全技术 - 信息安全事件分类分级指南)(GB/Z20986-2007), '정보안전기술 - 온라인증권거래시스템정보안전보장평가준칙'(信息安全技术-信息安全事件分类分级指南)(GB/T20987-2007)과 '정보안전기술 - 정보시스템재난회복규범'(信息安全技术 - 网上证券交易系统信息安全保障评估准则)(GB/T20988-2007) 등 7개 정보안전 관련 국가표준을 정식으로 실시하였다.[167]

2011년 5월 국가인터넷정보판공실(国家互联网信息办公室) 이 새롭게 설립되었으며, 중공중앙 선전부 부부장인 루워이(鲁炜)가 판공실 주임을 역임하였다. 동 기구의 설립 목적은 인터넷 구축 및 발전과 관리를 더 한층 강화하고 가상 사이버사회에 대한 관리수준을 향상하여, 국가차원에서 사이버를 한층 더 중시하는 경향을 보여주고 있다.[168] 2013년 11월, 중국공산당 제18기 제3차 회의에서는 "법에 의거하여 인터

164) 中国国家互联网信息办公室, 2000년-2001년 인터넷대사기(互联网大事记), 〈http://www.cac.gov.cn/2009-04/13/c_126500434.htm〉, 2015년 8월 18일 검색.
165) 中国国家互联网信息办公室, 2002년-2003년 인터넷대사기(互联网大事记), 〈http://www.cac.gov.cn/2009-04/14/c_126500426.htm〉 , 2015년 8월 18일 검색.
166) 中国国家互联网信息办公室, 2005년 인터넷대사기(互联网大事记), 〈http://www.cac.gov.cn/2009-06/04/c_126500390.htm〉, 2015년 8월 18일 검색.
167) 中国国家互联网信息办公室, 2007년 인터넷대사기(互联网大事记), 〈http://www.cac.gov.cn/2014-02/24/c_126182777.htm〉, 2015년 8월 18일 검색.
168) 中国国家互联网信息办公室, 2011년 인터넷대사기(互联网大事记), 〈http://www.cac.gov.cn/2014-02/24/c_126182823.htm〉, 2015년 8월 18일 검색.

넷에 대한 관리를 강화하고, 인터넷관리에 대한 영도체제를 신소과세 완비하여 기술로부터 콘텐츠, 일상적인 안전으로부터 범죄에 대한 처벌에 이르는 인터넷관리에 대한 역량을 형성·증진하고, 국가인터넷과 정보안전을 확보하여 국가안전과 사회안정을 수호하도록 한다."는 결의를 채택하였다.[169]

2014년 2월, 중앙인터넷안전과정보화영도소조(中央网络安全和信息化领导小组)가 설립되었으며, 시진핑(习近平) 총서기가 조장에 취임하였다. 2014년 3월에 개최된 전국인민대표대회 및 전국정치협상회의에서는 정부보고 중 처음으로 "인터넷안전수호"라는 내용이 포함되었다.[170]

2015년 6월, 제12기 전국인민대표대회 제15차 회의에서 '중화인민공화국인터넷안전법(초안)'(中华人民共和国网络安全法草案, 이하 '사이버안전법 초안'이라 함)을 심의하였으며, 2015년 8월 5일까지 개방하여 초안에 대한 의견을 수렴하였다.

현재까지 사이버 관련 법률은 주로 개인정보보호, 전자상거래, 시장접근 그리고 사이버 범죄와 관련된 법률 및 규범으로써 법률 3부, 행정법규 6부, 부문규장 30여부 및 사법해석 5부가 있다.[171]

나. 중국 사이버 관련 제도의 특징

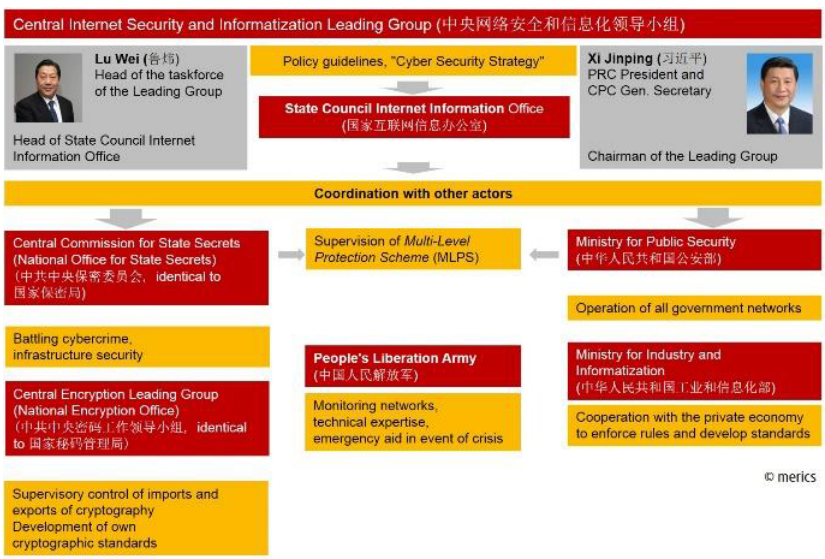
상술한 중국 사이버 관련 정책 및 법제도 형성 과정을 통하여 다음과 같은 2가지 특징을 확인할 수 있다.

첫째, 사이버 관리체제에서 있어서, 최고행정기관인 국무원 및 관할 부서의 단독 행정관할에서 중국공산당 중앙위원회와 국무원이 공동으로 관리하는 양자관할체제로 바뀜으로써 사이버 안전에 대한 관리를 강화하고 있다. 1993년 국가경제정보연석회의의 장이 국무원 부총리이었던 것으로부터 시작하여 2001년에는 국가정보화영도소조의 장이 국가 영도 서열 제5위이고 국가정치국 상무위원인 국무원 총리급으로 격상되었으며, 2014년에는 중국 영도서열 제1위인 시진핑 국가주석 및 중국공산당 총서기

169) 中国国家互联网信息办公室, 2013년 중국인터넷발전대사기(中国互联网发展大事记), 〈http://www.cac.gov.cn/2014-05/22/c_126535820.htm〉, 2015년 8월 18일 검색.
170) 中国国家互联网信息办公室, 중국인터넷20년 : 1994-2014(中国互联网之二十年 : 1994-2014), 〈http://www.cac.gov.cn/2014-11/16/c_1113265290.htm〉, 2015년 8월 18일 검색.
171) 工业和信息化部电信研究院政策与经济研究所, 腾讯互联网与社会研究院 〈中国互联网法律与政策研究报告〉, 电子工业出版社(2014.4).

가 중앙인터넷안전과정보화영도소조의 장을 맡음으로써 중국집권당과 정부가 사이버 안전에 대하여 고도로 중요시하고 있음을 엿볼 수 있다.

둘째, 정책과 법률의 제정 측면에서는, 인터넷 보안정책과 관련 법령이 어우러져 있으며, 서로 영향을 미치고 있다. 전국인민대표대회에서 의결한 결의는 일정한 기간 동안의 시행을 거쳐 법률로 승격되었으며, 중국공산당 대표대회에서 의결한 결의 역시 사이버 안보를 위한 정책으로 승격함으로써 서로 영향을 미치고 있다. 예를 들면 2000년 12월 28일, '인터넷안전을 수호할 것에 관한 전국인민대표대회상무위원회의 결정'(全国人民代表大会常务委员会关于维护互联网安全的决定)은 이후 형법 수정안에 반영되었으며, 2013년 11월, 중국공산당 제18기 제3차 회의 중 "법에 의거하여 인터넷에 대한 관리를 강화하고, 인터넷관리에 대한 영도체제를 신속하게 완비할 것"에 관한 결의는 2014년 2월, 중앙인터넷안전과정보화영도소조(中央网络安全和信息化领导小组)의 설립과 시진핑(习近平)국가주석이 직접 조장을 담당하도록 하는 결의안이 되었다. 다음은 중국 사이버안전 정책 관리 체제다.[172]



[그림 2-3-1] 중국 사이버안전 정책 관리 체제

172) Hauke Johannes Gierow, 'Cyber Security in China: New Political Leadership Focuses on Boosting National Security', China Monitor No.20, Mercator Institute for China Studies (2014.12). p.4.

2. 사이버안전 정책

가. 사이버 안전에 대한 정의

2015년 8월 현재 심의 중에 있는 '사이버안전법' 초안은 처음으로 "사이버 안전"에 대한 정의를 두고 있으며, "사이버 안전"이란 필요한 조치를 취하여 사이버에 대한 공격, 침입, 교란, 파괴와 불법사용 및 그 밖의 사고를 방지하여 사이버가 안정적으로 운행할 수 있는 상태를 유지하고, 사이버의 정보저장, 전송, 처리의 완전하고, 비밀보장적이고 사용가능한 역량을 보장할 수 있도록 하는 것을 말한다."고 규정하고 있다.[173]

나. 사이버공간에 대한 주권 주장

중국 정부는 2010년 6월에 발표한 '중국사이버상황백서'(中国互联网状况白皮书)에서 처음으로 사이버공간에 대한 주권을 주장하였는데, "인터넷은 국가의 중요한 기초시설로서 중국 역내의 인터넷은 중국 주권관할범위에 속하며, 중국의 인터넷 주권은 존중되고 보호받아야 한다."[174]고 언급하였다. 이러한 주장은 2015년 7월 1일부터 시행되고 있는 '국가안전법'(国家安全法) 제25조에도 반영되었다. 동 조항은 "국가는 사이버와 정보안전 보장체계를 구축하며, 사이버와 정보안전보호역량을 향상시키고 사이버와 정보기술의 창조연구와 개발응용을 강화하여 사이버와 정보 핵심기술, 관건이 되는 기초시설과 중요한 분야의 정보 및 데이터가 안전하고 통제 가능하도록 한다. 사이버에 대한 관리를 강화하고, 사이버 공격, 사이버 침입, 사이버 비밀 절도, 불법 그리고 유해한 정보의 살포 등 사이버 불법 범죄행위를 예방하고, 제지하며, 법에 따라 처벌하고 국가의 사이버 공간주권, 안전과 발전이익을 수호한다."고 규정하고 있다.

'사이버안전법' 초안은 상술한 내용을 반영하여 사이버 주권과 국가안전수호를 입법취지로 하고 있는 바, "중화인민공화국 역내에서 인터넷을 설치, 운영, 유지보수 및 사용하거나 사이버 안전에 대한 감독 관리에는 동 법을 적용한다."고 규정하고 있다.[175] 즉 사이버주권은 주권의 사이버 공간에서의 연장과 표현이라고 하며, 사이버

173) 사이버안전법 초안 제65조 제1항.
174) 중화인민공화국 국무원신문판공실, 중국사이버상황백서(中国互联网状况白皮书)(2010.6).

주권원칙은 국가안전과 이익을 수호하고 사이버 국제관리와 협력에 있어서 시종일관 견지하는 중요한 원칙이라고 주장한다.

다. 사이버 산업발전과 안전보장의 병행

전술한 사이버 정책과 법제도 연혁에서 보는 바와 같이, 사이버 및 정보 산업 육성은 중국 경제발전 계획 중의 핵심이다. 이와 동시에 사이버안전의 보장은 사이버 산업 발전을 위한 보증임과 동시에 국가안전 보호라는 측면에서 병행하여 진행하고 있으며, 이러한 내용은 사이버안전법 초안에서도 재차 확인되고 있다. 즉 사이버 안전보장과 사이버 산업발전이라는 두 마리 토끼를 동시에 다스린다는 원칙하에 "사이버 기초시설 건설을 추진하고 사이버 기술혁신과 응용을 장려함과 동시에 사이버 안전보장체계를 확립하고 사이버 안전보호 역량을 향상시키도록 하고 있으며",[176] 이를 위하여 사이버 안전전략의 수립, 안전표준체계의 확립, 사이버 안전기술 및 산업에 대한 지원, 관련 지적재산권 보호와 기술혁신에 대한 지원을 명시하고, 사이버 안전에 대한 교육, 홍보 및 인재양성에 대하여 원칙적인 규정을 두고 있다.[177]

라. 사이버 안전에 대한 분류

사이버 안전에 대하여 인터넷 관련 상품 및 서비스 안전, 사이버 운행 안전 및 사이버 정보안전 등 크게 3가지 부류로 나누고 있다.

첫째, 인터넷 관련 상품과 서비스 안전에 관련하여, "상품과 서비스" 뿐만 아니라 "인터넷 관련 중요 시설 및 사이버 안전을 위한 상품"을 포괄하는 총체적 개념이며; 안전에 관하여서는 "국가 및 산업 표준에 부합"될 것을 요구하고 있으며, 상품 및 서비스 제공자에 대하여서는 "악의적인 프로그램을 설치할 수 없으며, 사용자의 정보를 수집하는 기능이 있을 경우 이를 사용자에게 명백히 고시하고 그 동의를 취득하여야 하며, 안전에 결함 등 리스크가 있을 경우 이를 위한 구제조치를 취하여야 하며 안전유지 조치를 취하여야 하며, 사이버 안전을 위협하는 활동을 하거나 사이버 안전

175) 사이버안전법 초안 제2조.
176) 사이버안전법 초안 제3조.
177) 사이버안전법 초안 제11조-제16조.

을 위협하는 활동을 위하여 기술적 지원, 홍보, 지불결산 등 방조행위를 하여서도 아니된다."는 등 여러 가지 의무를 부여하고 있다.[178]

둘째, 사이버 운행 안전과 관련하여 공중통신, 라디오TV전송 등 기초 정보네트워크, 에너지, 교통, 수리시설, 금융 등 중요한 산업과 전력, 수도, 가스 등 공급과 의료위생, 사회보장 등 공중서비스 분야의 정보시스템, 군사 관련 인터넷 네트워크, 시(市) 단위 이상 정부기관의 인터넷과 사용자가 많은 "인터넷과 시스템"을 "관건적 정보기초시설"로 확정하여 중점 보호를 한다. "관건적 정보기초시설"의 안전운행에 관해서는 특별규정을 두고 있는데, 국무원 산하 관련 부서는 안전운행의 지도와 감독의 의무가 있고, 관건적 정보기초시설 운영자에게는 안전관리전문직 설치, 안전관리인원 교육, 중요한 데이터에 대한 보존 등 의무를 부여하고 있으며, 국가안전에 위협을 미칠 수 있는 상품 및 서비스의 구매와 관련하여 안전심사를 받도록 하고 있다.[179]

셋째, 사이버정보안전과 관련하여 주로 개인정보, 프라이버시와 영업비밀에 대한 보호를 규정하고 있다. 여기서 개인정보는 "전신업무 경영자와 인터넷정보서비스 제공자가 서비스를 제공하는 과정에서 수집한 사용자의 성명, 출생연월일, 신분증번호, 주소지, 전화번호, 계좌 및 비밀번호 등 단독으로 또는 기타 정보와 결합하여 사용자의 정보 및 사용자의 서비스 사용시간, 지점 등 정보"를 지칭하고 있는 바[180] 개인정보에 대한 범주가 비교적 좁다. 개인의 프라이버시와 영업비밀과 달리 개인정보는 적법성, 적정성, 필요성의 원칙하에 개인의 동의를 받은 후 수집 및 사용할 수 있으나 수집한 정보에 대하여 비밀을 준수하여야 하며, 누설, 왜곡, 훼손 또는 타인에게 불법으로 제공하거나 또는 판매하여서는 아니되며, 인터넷 운영자는 적절한 조치를 취하여 개인정보의 안전을 확보할 의무가 있다.[181]

마. 사이버 안전보장 책임 및 주체의 세분화

상술한 사이버 안전의 분류에 따라 안전보장의무 이행의 주체를 국가, 정부 및 각 부처, 산업협회, 그리고 법인과 자연인 등 4가지 부류로 나누고, 각각의 의무를

178) 사이버안전법 초안 제17조-제24조.
179) 사이버안전법 초안 제25조-제33조.
180) 전신과인터넷사용자개인정보보호규정(电信和互联网用户个人信息保护规定)(2013.6.28.), 제4조
181) 사이버안전법 초안 제34조-제36조.

규정하고 있다. 첫째, 국가의 사이버 안전보장 의무. 국가는 사이버 공간에 대한 관리를 적극적으로 전개하고, 사이버 기술연구 및 개발과 표준을 적극 제정하여야 하며, 사이버 범죄행위에 대한 징벌하는 등 국제교류와 협력을 추진하여야 한다. 둘째, 정부 각 부서의 안전감독 관리의 의무. 국가인터넷정보판공실(国家互联网信息办公室) 및 중공중앙인터넷안전과정보화영도소조판공실(中共中央网络安全和信息化领导小组办公室)은 전국적으로 인터네정보안전과 콘텐츠 관리를 하는 최고 기관이며, 국무원 공업과정보화부(工业和信息化部), 공안부(公安部), 문화부 그리고 상술한 관건정보기초시설 관리 중앙부서, 그리고 각 현급(县级) 이상 정부는 직책 범위 내에서 사이버 안전과 감독관리의 의무가 있다. 셋째, 사이버 운영자 또는 서비스 제공자, 그리고 관련 산업협회는 법률, 법규의 규정, 국가표준, 협회표준 등 강제적 요구에 따라 사이버 안전을 예방하고 보장할 의무와 자율적 관리의 의무가 있다. 넷째, 법인 및 자연인의 법규범 준수의무. 여하한 개인 또는 조직은 사이버안전을 침해하거나 사이버를 이용하여 국가안전을 침해하고 테러리즘, 극단주의, 민족차별, 음란정보를 살포하거나 타인에 대한 비방, 사회질서 교란, 공공이익 침해, 타인의 지재권침해 및 기타 합법적 권익 침해하는 행위를 하여서는 안 된다.[182]

바. 사이버 안전점검과 조기경보 및 응급조치

국가는 사이버 안전에 대한 점검과 조기경보제도를 확립하고 응급대응 시스템을 마련하며, 관건정보기초시설의 안전 담당 부서는 해당 산업 및 분야의 사이버 안전응급대응조치방안을 마련하고 정기적으로 모의훈련을 하여야 한다.[183] 중국국가인터넷정보판공실은 주별, 월별, 연별로 웹사이트에 인터넷안전정보와 동태보고를 공개하고 있으며,[184] 안전허점공고는 국가인터넷정보판공실 산하 국가정보안전허점공공네크워크(国家信息安全漏洞共享平台)와[185] 중국국가정보안전허점데이터베이스(中国国家信息安全漏洞库)[186]에서 책임지고 정기적으로 업데이트하여 공개하고 있다.

---

182) 사이버안전법 초안 제5조-제9조.
183) 사이버안전법 초안 제44조-제49조.
184) http://www.cac.gov.cn/aqbg.htm 참조.
185) http://www.cnvd.org.cn/webinfo/list?type=14 참조.
186) http://www.cnnvd.org.cn/ 참조.

그 밖에 공업과정보화부에서 공표한 '인터넷네트워크안전응급예안'(互联网网络安全应急预案)은 응급조치 관련 조직체계와 직책을 명시하였을 뿐만 아니라 예방체제도 규정하고 있다. 동 응급예안에 따르면 사이버안전 사건은 위해성과 긴급정도에 따라 "4급/일반", "3급/예경", "2급/경보", "1급/긴급" 등 4가지 등급으로 나뉘며, 각각 "남색" "황색" "오렌지색" "적색" 등 4가지 색상으로 표기하고 있다.

"4급/일반" 급의 안전사력은 사이버 운영회사와 국가컴퓨터네트워크응급기술처리조화센터(国家计算机网络应急技术处理协调中心, CNCERT/CC)의 정보 교류를 통하여 자체적으로 처리하나, 기타 급별의 안전사고가 발생하였을 경우 국가통신보장응급영도소조에 보고한 후 각 사이버운영회사 및 CNCERT/CC에 응급방안을 개시하도록 지시할 수 있다. 각 사이버 운영회사는 사이버 관리, 운행정비 등 부서로 응급인원을 구성하고 사이버응급사건처리업무를 전담하도록 하여야 하며, 응급에 필요한 설비를 마련하여야 한다.

사. 사이버 국제협력

중국은 사이버 국제협력과 관련하여 다음과 같은 방침을 제시하고 있다.[187]

첫째, 국제 사이버 관리와 관련하여 유엔 산하에 민주적인 절차를 통하여 형성된 권위적이고 공정한 사이버국제관리기구의 설립을 주장하고 있으며 유엔이 동 분야에서의 역할을 할 것을 주장하고 있다.

둘째, 사이버기초자원은 사이버 발전과 안전과 직결됨으로써 각국은 국제 사이버 기초자원 관리에 참여할 평등한 권리를 갖는다고 주장함과 동시에 기존의 관리모델을 기반으로 다자적이고 투명한 국제사이버 자원의 배분체계를 확립하고, 사이버 기초자원을 합리적으로 배분하여 글로벌 사이버공간의 균형적인 발전을 추진할 것을 주장한다.

셋째, 국가간 국제협력과 관련하여 호혜평등의 기초 위에 다양한 형식, 다양한 경로 및 다양한 분야의 교류와 협력을 진행할 것을 주장하고 있다. 여기에는 양자간 교류체제 확립, 사이버 산업 간 국제교류협력, 그리고 과학과 윤리분야 및 과학기술교류가

187) 중화인민공화국 국무원신문판공실, 중국사이버상황백서(2010.6).

포함된다. 또한 사이버 국제범죄에 대응하기 위하여 각국 사법기관은 사이버 범죄를 예방하고 대치함에 있어서 조사에 협력하고 다자간 및 양자간 협력체제를 확립할 것을 주장하고 있다.

넷째, 사이버 시장 개방과 관련하여 중국 정부는 세계무역기구에 규정한 회원국의 의무 및 가입의정서에 약속한 의무를 엄격히 준수할 것이고, 각국 기업들이 〈외상투자전신기업관리규정〉에 근거하여 중국 사이버 시장에 투자하는 것을 환영하며, 법에 의거하여 외국인투자기업들의 합법적 권익을 보호하고, 우호적인 사이버 경영환경을 적극적으로 조성할 것임을 밝혔다.

사이버 국제협력과 관련하여 '사이버안전법(초안)'은 제5조에서 간략하게 "국가는 사이버 스페이스의 관리, 사이버 기술연구 및 개발과 표준의 제정, 사이버 불법범죄 등 분야의 국제교류와 협력을 적극적으로 추진하며, 평화적이고 안전하고 개방적이고 협력적인 사이버 스페이스의 구축을 추진한다"고 규정하고 있고, 구체적인 계획과 조치를 명시하고 있지는 않다.

3. 사이버범죄 정책

가. 사이버범죄 대응 정책

중국은 2015년 9월 미국을 방문한 시진핑 국가주석의 미 대통령과의 정상회담과 UN 연설을 통하여, 사이버공간을 안전하게 보장하기 위한 중국의 사이버범죄 대응정책과 국제협력을 선언하였다. 이러한 전략적 협력 정책의 목적은 중국에 대한 국제사회에서의 신뢰를 구축하고 긴장 관계와 의혹을 완화시키고자 한 것이다. 동 발표에서 중국은 사이버안보 위반행위 문제와 관련하여 "고위급, 공동 대화 체제"(high-level, joint-dialogue mechanism)를 수립할 준비가 되어 있다고 언급하였다.[188]

중국은 2013년 에드워드 스노든이 미국 국가안보국(NSA)의 불법 도청 및 감청에 대해 폭로한 이후, 사이버 보안을 국가안보 차원의 중요 과제로 선정하는 한편, 네트워크 관련 정책의 최우선 순위로 두어 왔다. 이를 위해 2014년 11월에는 중국 내에서

188) "Xi offers Cybercrime Dialogue in Bid to Defuse U.S. Tensions",(2015.9.23.) 〈http://www.bloomberg.com/news/articles/2015-09-23/china-ready-for-deal-with-u-s-on-cybercrime-xi-says-in-seattle〉.

통신, 인터넷 서비스를 제공하는 기업은 정부가 데이터에 접속할 수 있는 장치를 마련하고 암호키를 제공하도록 한 '반테러리즘법'(反恐怖主义法) 법 초안을 발표하였으며, 2015년 7월 1일에는 사이버안보를 국가안보의 영역에 포함시킨 새로운 '국가안전법'이 통과되었다. 이어서 7월 6일에는 사이버공간의 관리와 통제를 종합적으로 체계화한 '사이버안전법' 초안을 발표하였다. 법안의 소관부처는 공업정보화부와 공안부 등이다.[189] 동법은 사이버공간과 자국의 데이터에 관한 정부의 관리 및 통제를 강화하기 위한 것으로서, 중국 내 인터넷서비스사업자는 물론 많은 외국계 기업에도 크게 영향을 미칠 가능성이 있어서 주목을 받고 있다.

나. 사이버범죄 관련 법제

중국의 사이버 관련 범죄는 그 범죄 대상에 따라 크게 4가지 부류로 나눌 수 있다.

1) 사이버 운행 안전을 침해하는 행위

첫째, 국가사무, 국방건설, 첨단과학기술분야의 컴퓨터정보시스템에 침입하는 행위가 범죄를 구성할 경우 형법 제285조에 규정한 (가) 컴퓨터정보시스템불법침입죄, (나) 컴퓨터정보시스템데이터불법취득죄, 컴퓨터정보시스템불법통제죄, (다) 컴퓨터정보시스템침입 및 불법통제에 프로그램 또는 도구 제공죄에 해당한다.

컴퓨터정보시스템불법침입죄에 해당하는 경우 3년 이하 유기징역 또는 6개월 이하 단기징역에 부과되며, 컴퓨터정보시스템데이터불법취득죄와 컴퓨터정보시스템불법통제죄에 해당하는 경우 3년 이하 유기지역 또는 6개월 이하 단기징역과 벌금형을 병행 부과하며, 사정이 특별히 심각할 경우는 3년이상 7년 이하 유기징역에 벌금형을 병행 부과하며; 컴퓨터정보시스템침입 및 불법통제에 프로그램 또는 도구 제공죄의 경우 컴퓨터정보시스템데이터불법취득죄와 컴퓨터정보시스템불법통제죄를 참조하여 형사처벌을 부과한다.

둘째, 국가규정을 위반하여 컴퓨트네트워크 또는 통신서비스를 임의로 중단시켜 컴퓨터네트워크 또는 통신시스템이 정상적으로 운행되지 못하도록 하는 경우 형법

189) 김유향, '중국 네트워크안전법(안)의 주요 내용과 함의', 이슈와 논점 제1083호, 국회입법조사처(2015.11.)

제286조 제1항에 규정한 컴퓨터정보시스템파괴죄에 해당하며, 손해결과가 심각할 경우 5년 이하의 유기징역 또는 6개월 이하의 단기징역에 부과하며, 손해결과가 특별히 심각할 경우 5년 이상의 유기징역을 부과한다.

셋째, 고의로 컴퓨터 바이러스 등 파괴성 프로그램을 제작 및 전파하고, 컴퓨터시스템 및 통신 네트워크를 공격하여 컴퓨터시스템 및 통신 네트워크가 피해를 받을 경우 형법 제286조 제3항에 규정한 컴퓨터정보시스템파괴죄에 해당한다. 손해결과가 심각할 경우 5년 이하의 유기징역 또는 6개월 이하의 단기징역을 부과하며, 손해결과가 특별히 심각할 경우 5년 이상의 유기징역을 부과한다.

2) 사이버를 이용하여 국가안전과 사회안정을 침해하는 행위

첫째, 사이버를 이용하여 요언을 날조하거나 비방하거나 또는 기타 해로운 정보를 발표, 전파하거나, 국가정권 전복을 선동하고, 사회주의 제도를 전복하고 또는 국가분열을 선동하고 국가통일을 파괴하는 경우, (가) 형법 제103조의 국가분열죄, 국가분열선동죄, (나) 형법 제105조의 국가정권전복죄, 국가정권전복을 선동한 죄에 해당한다.

국가분열죄와 국가분열선동죄의 경우, 국가분열, 국가통일파괴를 조직, 계획 및 실시한 주요 범죄자 또는 죄행이 심각할 경우 무기징역 또는 10년 이상 유기징역을 부과하며, 적극 가담한 자에 대하여서는 3년 이상 10년 이하 유기징역을 부과하고, 기타 참여자에 대하여서는 3년 이하 유기징역, 6개월 이하 단기징역, 관제(管制) 또는 정치권리 박탈 형을 부과한다. 국가분열을 선동하고 국가통일을 파괴한 자에 대하여서는 5년 이하의 유기징역, 6개월 이하 단기징역, 관제 또는 정치권리 박탈형을 부과하며, 주요 범죄자 또는 죄행이 심각한 자는 5년 이상의 유기징역을 부과한다.

국가정권전복죄, 국가정권전복을 선동한 죄의 경우, 국가정권 전복, 사회주의 제도 전복을 조직, 계획 및 실시한 주요 범죄자 또는 죄행이 심각할 경우 무기징역 또는 10년 이상 유기징역을 부과하며, 적극 가담한 자에 대하여서는 3년 이상 10년 이하 유기징역을 부과하고, 기타 참여자에 대하여서는 3년 이하 유기징역, 6개월 이하 단기징역, 관제(管制)또는 정치권리 박탈 형을 부과한다. 요언날조, 비방 또는 기타의 방식으로 국가정권 전복, 사회주의제도 전복을 선동한 자에 대하여서는 5년 이하의 유기징역, 6개월 이하 단기징역, 관제 또는 정치권리 박탈형을 부과하며, 주요 범죄자 또는

죄행이 심각한 자는 5년 이상의 유기징역을 부과한다.

둘째, 사이버를 이용하여 국가비밀, 정보 또는 군사비밀을 절취, 누설하는 경우, (가) 형법 제398조의 국가비밀고의누설죄 또는 국가비밀과실누설죄, 또는 (나) 군사비밀불법취득죄, 해외를 위하여 군사비밀을 절취, 정탐, 매수, 불법제공죄, 또는 (다) 군사비밀고의누설죄, 군사비밀과실누설죄에 해당한다.

국가비밀고의누설죄 또는 국가비밀과실누설죄의 경우, 국가공무원이 국가비밀보수법의 규정을 위반하여 국가비밀을 고의 또는 과실로 누설하여 사정이 심각할 경우 3년 이하의 유기징역 또는 6개월 이하 단기징역을 부과하며, 사정이 특별히 심각할 경우 3년 이상 또는 7년 이하의 유기징역형을 부과한다. 비국가공무원이 상기 조항의 범죄를 행하였을 경우 위 규정에 비추어 처벌한다.

군사비밀불법취득죄, 해외를 위하여 군사비밀을 절취, 정탐, 매수, 불법제공죄의 경우, 절취, 정탐, 매수하는 방법으로 군사비밀을 불법적으로 취득할 경우 5년 이하의 유기징역형에 부과하며, 사정이 심각할 경우 5년 이상 10년 이하의 유기징역형을 부과하고, 사정이 특별히 심각할 경우 10년 이상의 유기징역형을 부과한다. 해외의 기구, 조직, 인원을 위하여 군사비밀을 절취, 정탐, 매수, 불법 제공할 경우 10년 이상의 유기징역, 무기징역 또는 사형을 부과한다.

군사비밀고의누설죄, 군사비밀과실누설죄의 경우, 국가비밀보수법을 위반하여 군사비밀을 고의 또는 과실로 누설하여 사정이 심각할 경우 5년 이하의 유기징역 또는 6개월 이하 단기징역에 부과하며, 사정이 특별히 심각할 경우 5년 이상 10년 이하의 유기징역에 부과한다. 전쟁 중에 상술한 범죄를 행하였을 경우 5년 이상 10년 이하의 유기징역에 부과하고, 사정이 특별히 심각할 경우 10년 이상 유기징역 또는 무기징역에 부과한다.

셋째, 사이버를 이용하여 민족원한, 민족차별을 선동하고 민족단결을 파괴할 경우, 형법 제249조의 민족원한 선동, 민족차별죄에 해당하는 바 사정이 심각한 경우 3년 이하 유기징역, 6개월 이하 단기징역, 관제 또는 정치권리 박탈 등 형을 부과하고, 사정이 특별히 심각할 경우 3년 이상 10년 이하 유기징역에 부과한다.

넷째, 사이버를 이용하여 사이비조직을 구성하고, 사이비조직 구성원간에 연락하는 등으로, 국가법률, 행정법규를 위반하는 경우 형법 제300조 제1항의 비밀결사조직

구성, 또는 비밀결사조직을 이용하여, 또는 미신을 이용하여 법률을 위반한 죄에 해당하는 바 3년 이상 7년 이하의 유기징역을 부과하며, 사정이 특별히 심각할 경우 7년 이상의 유기징역을 부과한다.

3) 사이버를 이용하여 사회주의 시장경제질서와 사회관리 질서를 파괴하는 행위

첫째, 사이버를 이용하여 위조 상품을 판매하거나 또는 상품과 서비스에 대하여 허위 홍보를 진행할 경우 형법 (가) 제140조의 위조상품 생산 및 판매죄, 또는 (나) 형법 제222조의 허위광고죄에 해당한다.

위조상품 생산 및 판매죄는, 생산자 또는 판매자가 제품 중 다른 상품 또는 가짜 상품을 섞어 넣어 품질이 저급한 제품으로 좋은 제품을 충당하거나 또는 불합격 제품으로 합격제품을 충당하는 행위가 이에 해당한다. 판매금액이 5만위엔 이상 20만 위엔 이하인 경우 2년 이하 유기징역 또는 6개월 이하 단기징역을 부과하고 동시에 판매금액의 50%이상 2배 이하의 벌금을 병행 부과 또는 단독 부과할 수 있다. 판매금액이 20만 위엔 이상 50만 위엔 이하인 경우 2년 이상 7년 이하의 유기징역을 부과하고, 동시에 판매금액의 50%이상 2배 이하의 벌금을 병행 부과하며; 판매금액이 50만 위엔 이상 200만 위엔 이하 일 경우 7년 이상의 유기징역에 부과하고, 동시에 판매금액의 50%이상 2배 이하의 벌금을 병행 부과하며; 판매금액이 200만 위엔 이상일 경우 15년 유기징역 또는 무기징역에 부과하고, 동시에 판매금액의 50%이상 2배 이하의 벌금을 병행 부과하거나 또는 재산을 몰수한다.

허위광고죄의 경우, 광고주, 광고경영자, 광고발행자가 국가규정을 위반하고 광고를 이용하여 상품 및 서비스에 대하여 허위광고를 진행하거나 기타 심각한 사정이 있는 경우 2년 이하의 유기징역 또는 6개월 이하의 단기징역을 부과하며 병행하여 또는 단독으로 벌금을 부과할 수 있다.

둘째, 사이버를 이용하여 타인의 상업신용과 상품명성을 침해할 경우 형법 제221조의 상업신용, 상품명성 훼손죄에 해당하는 바 허위사실을 날조 및 살포하여 타인의 상업신용, 상품명성을 침해하고 타인에게 중대한 손실을 입히거나 또는 기타 심각한 사정이 있을 경우 2년 이하의 유기징역 또는 6개월 이하의 단기징역형을 부과하며, 병행하여 또는 단독으로 벌금형을 부과할 수 있다.

셋째, 사이버를 이용하여 타인의 지적재산권을 침해할 경우 (가) 형법 제214조의 허위등록상표 상품을 판매한 죄, (나) 형법 제217조의 저작권 침해죄, (다) 형법 제218조의 권리침해복제품 판매죄, (라) 형법 제219조의 영업비밀침해죄에 해당한다.

허위등록상표 상품을 판매한 죄의 경우, 판매금액의 수준에 따라 판매금액이 비교적 많은 경우 3년 이하의 유기징역 또는 6개월 이하의 단기징역에 부과하며, 동시에 또는 단독으로 벌금형을 부과하고, 판매금액이 상당한 경우 3년 이상 7년 이하의 유기징역형에 벌금형을 병행하여 부과한다.

저작권 침해죄의 경우, 불법소득이 비교적 크거나 또는 기타 심각한 사정이 있는 경우 3년 이하의 유기징역 또는 6개월 이하의 단기징역에 부과하며, 동시에 또는 단독으로 벌금형을 부과하고, 불법소득 액수가 상당하고 또는 기타 특별히 심각한 사정이 있을 경우 3년 이상 7년 이하의 유기징역형에 벌금을 병행하여 부과한다.

권리침해복제품 판매죄의 경우, 영리를 목적으로 형법 제217조의 권리침해복제품임을 알면서 판매하여 불법소득이 상당한 경우 3년 이하의 유기징역 또는 6개월 이하의 단기징역형에 벌금형을 병행부과 또는 단독 부과한다.

영업비밀침해죄의 경우, 영업비밀 권리자에게 심각한 피해를 초래하였을 경우 3년 이하의 유기징역 또는 6개월 이하의 단기징역을 부과하며, 특별히 심각한 결과를 초래하였을 경우 3년 이상 7년 이하의 유기징역에 벌금을 병행 부과한다.

넷째, 사이버를 이용하여 증권, 선물거래 또는 기타 금융시장 질서를 교란하는 정보를 날조 및 전파하는 행위의 경우 (가) 형법 제180조의 내부거래, 내부정보누설죄, 미공개정보를 이용하여 거래한 죄, (나) 형법 제181조의 증권, 선물거래 허위정보 날조 및 전파죄, 투자자를 유인 기만하여 증권을 매매하고 선물계약을 하는 죄에 해당한다.

내부거래, 내부정보누설죄, 미공개정보를 이용하여 거래한 죄의 경우, 사정이 심각한 경우 5년 이하 유기징역 또는 6개월 이하의 단기징역을 부과하고 불법소득의 1배 이상 5배 이하의 벌금을 병행부과 또는 단독 부과하며, 사정이 특별히 심각한 경우 5년 이상 10년 이하의 유기징역을 부과하고, 불법소득의 1배 이상 5배 이하의 벌금을 병행 부과한다.

증권, 선물거래 허위정보 날조 및 전파죄, 투자자를 유인 기만하여 증권을 매매하고 선물계약을 하는 죄의 경우, 일반인이 위 죄를 행하여 심각한 결과를 초래하는 경우

5년 이하의 유기징역 또는 6개월 이하의 단기징역형과 1만 위엔 이상 10만 위엔 이하의 벌금을 병행 또는 단독 부과한다. 증권거래소, 선물거래소 등 전문 인원이 고의로 허위정보를 제공하는 등 행위를 통하여 투자자를 유인, 기만하여 증권을 매매, 또는 선물계약을 체결하여 심각한 결과를 초래하는 경우, 5년 이하의 유기징역 또는 6개월 이하의 단기징역을 부과하며, 1만 위엔 이상 10만 위엔 이하의 벌금형을 병행부과 또는 단독 부과하한다. 사정이 특별히 심각한 경우 5년 이상 10년 이하의 유기징역과 2만 위엔 이상 20만 위엔 이하의 벌금형을 부과한다.

다섯째, 사이버 상 음란웹사이트, 웹페이지를 개설하고, 음란물 접속서비스를 제공하거나 또는 음란서적, 영화, 동영상, 사진을 전파할 경우 (가) 형법 제363조 제1항의 음란물 제작, 복제, 출판, 판매, 전파로 인한 이익 취득죄, (나) 형법 제364조의 음란물 품전파죄, 음란영상물조직방영죄에 해당한다.

음란물 제작, 복제, 출판, 판매, 전파로 인한 이익 취득죄의 경우, 3년 이하의 유기징역, 6개월 이하의 단기징역 또는 관제에 부과하며 동시에 벌금을 병행 부과하며; 사정이 심각한 경우 3년 이상 10년 이하의 유기징역과 벌금을 병행 부과하며; 사정이 특별히 심각한 경우 10년 이상의 유기징역 또는 무기징역에 부과하며, 동시에 벌금형을 부과하거나 또는 재산을 몰수한다.

음란물품전파죄, 음란영상물제작방영죄의 경우, 음란물 전파행위에 대하여 사정이 심각한 경우 2년 이하의 유기징역, 6개월 이하의 단기징역 또는 관제에 부과한다. 음란영상물을 제작하여 방영하는 경우 3년 이하 유기징역, 6개월 이하의 단기징역 또는 관제에 부과하며, 동시에 벌금형을 병행 부과하고, 사정이 심각한 경우 3년 이상 10년 이하의 유기징역형과 동시에 벌금형을 부과한다.

4) 사이버를 이용하여 개인, 법인 및 기타 조직의 인신, 재산 등 합법적 권리를 침해하는 경우

첫째, 사이버를 이용하여 타인을 모독하거나 또는 사실을 날조하여 타인을 비방하는 경우 형법 제246조의 모독죄, 비방죄에 해당하며, 사정이 심각한 경우 3년 이하의 유기징역, 6개월 이하의 단기징역, 관제 또는 정치권리 박탈 등 형을 부과한다. 단, 사회질서와 국가이익을 심각히 침해하는 경우를 제외하고 상술한 행위는 피해자의

고소를 요하는 친고죄이다.

둘째, 타인의 전자메일 또는 기타 데이터 자료를 불법적으로 가로채거나 수정하거나 또는 삭제하여 시민의 통신자유와 통신비밀을 침해하는 경우 (가) 형법 제252조의 통신자유침해죄, (나) 형법 제253조의 공민개인정보 판매, 불법제공죄 및 불법취득죄에 해당한다.

통신자유침해죄의 경우, 사정이 심각하면 1년 이하 유기징역 또는 6개월 이하의 유기징역을 부과한다.

공민개인정보 판매, 불법제공죄 및 불법취득죄에 대하여, 국가기관 또는 금융, 전신, 교통, 교육, 의료기관 등의 근무자가, 국가규정을 위반하여 직무이행 또는 서비스 제공 중 취득한 일반대중의 개인정보를 타인에게 판매 또는 불법적으로 제공하는 경우, 사정이 심각한 경우에는 3년 이하 유기징역 또는 6개월 이하 단기징역을 부과하며 벌금형을 병행부과 또는 단독 부과한다.

셋째, 사이버를 이용하여 절도, 사기, 협박하여 재물갈취를 하는 경우 (가) 형법 제264조의 절도죄, (나) 형법 제266조의 사기죄, (다) 형법 제274조의 협박하여 재물갈취죄에 해당한다.

절도죄의 경우, 액수가 비교적 크고 또는 여러 차례 절도하였을 경우 3년 이하의 유기징역, 6개월 이하 단기징역 또는 관제에 부과하며, 벌금형을 단독 또는 병행 부과하고; 액수가 과다하거나 또는 사정이 특별이 심각한 경우 3년 이상 10년 이하의 유기징역을 부과하며, 벌금형을 병행 부과하고; 액수가 특별히 과다하거나 또는 기타 특별히 심각한 사정이 있는 경우 10년 이상의 유기징역 또는 무기징역에 부과하며, 벌금형을 병행 부과하거나 또는 재산을 몰수한다.

사기죄의 경우 액수가 비교적 큰 경우 3년 이하의 유기징역, 6개월 이하 단기징역 또는 관제에 부과하며, 벌금형을 단독 또는 병행 부과하고; 액수가 과다하거나 또는 사정이 특별이 심각한 경우 3년 이상 10년 이하의 유기징역에 부과하며, 벌금형을 병행 부과하고; 액수가 특별히 과다하거나 또는 기타 특별히 심각한 사정이 있는 경우 10년 이상의 유기징역 또는 무기징역을 부과하며, 벌금형을 병행 부과하거나 또는 재산을 몰수한다.

재물갈취죄의 경우, 액수가 비교적 큰 경우 3년 이하의 유기징역, 6개월 이하의

단기징역 또는 관제를 부과하며, 액수가 과다하거나 또는 기타 심각한 사정이 있는 경우 3년 이상 10년 이하의 유기징역을 부과한다.

그 밖에 사이버를 이용한 테러행위에 대하여 현재 심의 중에 있는 형법 제9차 수정안은 제120조 제2항에서 테러행동 조직, 영도 및 가담죄로 규정하여, "자료제작, 자료배포, 정보발송, 직접 강의 등 방식 또는 음성, 동영상, 정보네트워크 등을 통하여 테러주의, 극단주의를 선양하거나 또는 폭력, 테러활동의 실행을 선동한 경우 5년 이하의 유기징역, 6개월 이하의 단기징역, 관제형 또는 정치권리박탈형을 부과하며, 동시에 벌금형을 부과하고; 사정이 심각할 경우 5년 이상의 유기징역과 벌금형을 병행 부과하거나 또는 재산을 몰수한다." 제120조 제4항은 "테러주의, 극단주의를 선양하는 물품, 도서, 음성 및 영상자료를 소지하고 그 사정이 심각한 경우 3년 이하의 유기징역, 6개월 이하의 단기징역 또는 관제형을 부과하며, 벌금형을 병행 또는 단독으로 부과한다."고 규정하고 있다.

4. 시사점

중국은 사이버안전에 대한 관리 강화를 목적으로, 국무원 및 관할 부서의 단독 행정관할에서 중국 공산당 중앙위원회와 국무원이 공동으로 관리하는 양자관할체제로 변경하였다. 또한 중앙인터넷관리기관의 장을 국가주석이 겸하게 함으로써 사이버안전에 대한 정부의 인식이 강화된 것을 볼 수 있다. 또한 인터넷 보안정책과 법령의 발전을 함께 도모하여 전국인민대표회의와 중국공산당 대표대회 결의가 법률과 정책으로 추진되고 있다.

사이버안전의 주체와 관련하여 중국은 정부, 산업협회, 기업 및 개인의 책임을 규정하여 이를 세분화하고, 사이버안전에 대한 예방, 경고 및 비상대처조치를 제도화 하고 있다. 사이버안전의 확보와 함께 사이버 및 정보산업 육성에도 힘쓰고 있으며, 사이버안전에 대한 점검을 정기적으로 진행함으로써 이를 현실화하고자 한다. 금년 7월부터 시행되고 있는 국가안전법을 통하여 중국의 인터넷 주권과 역내관할권을 명시하였으며, 현재 심의 중인 사이버안전법 초안에서도 사이버안전에 대한 정의 규정과 함께 중국 역내 사이버안전에 대한 감독 관리를 명시하여 사이버주권원칙을 명확히 하고 있다.

한편, 형법에서는 사이버안전 운행을 침해하는 행위, 사이버를 이용하여 국가안전과 사회안정을 침해하는 행위, 사이버를 이용하여 사회주의 시장경제질서와 사회관리질서를 파괴하는 행위, 사이버를 이용하여 개인·법인 및 기타 조직의 인신, 재산 등 합법적인 권리를 침해하는 행위를 규정하여 사이버범죄에 대응하고 있다. 사이버를 이용한 테러에 대한 범죄행위 처벌에 대해서도 법적 근거를 마련하고 있는 중이며, 사이버 관련 중요한 기반시설에 대한 안전 확보에 특히 중점을 두고 있다.

또한, 중국은 외국의 소프트웨어가 국가안보에 잠재적인 위협이 될 수 있다는 점을 고려하고 있다. 이에 중국 기업들은, 이를 대체하는 중국 소프트웨어가 제대로 기능하지 않고 서구 상품만큼 안전성이 확보되지 않더라도, 국내 소프트웨어를 사용하도록 권장되고 있다. 이와 같이 중국은 인터넷 시큐리티에 관하여 가능하면 통일되고 종합적인 방법으로 규정하고자 한다.[190]

중국의 사이버안전법 초안이 시행되는 경우, 국내외에 갖는 시사점은 크다. 동 법안은 네트워크 전반을 망라한 규제 법안으로서 네트워크에 대한 통제를 강화하는 한편, 사이버 공격을 방어하고, 중국의 이용자에 관한 정보를 보호하는 정부의 역량 강화를 목표로 하고 있다. 국내정치 및 국가안보에서부터, 네트워크 환경, 해외사업자에까지 적용되는 이 법안의 의미는 크게 세 가지로 요약할 수 있다.

첫째, 대외적 차원에서 법안은 중국의 사이버안보에 대한 높은 관심과 전략방향을 잘 보여주고 있다. 제정 목적에는 사이버 주권과 국가안보, 사회공공이익을 수호하기 위해 사이버 보안을 강화함을 밝히고 있다. 해킹을 둘러싼 미국과의 갈등이 계속되는 가운데 발생한 스노든 사태는 중국 정부의 사이버안보에 대한 대응을 본격화하는데 영향을 미쳤다. 이 법안과 함께 '반테러리즘법', '국가안전법' 등 일련의 법률들의 정비는 사이버안보에 대한 중국정부의 대응방향을 잘 보여주는 것이라 할 수 있다.

둘째, 대내적 차원에서 동 법안은 중국의 사이버 보안체계를 종합적으로 정비하기 위한 것이다. 이를 위해 법안에서는 사이버 보안전략의 제정, 안전등급 보호제도의 시행, 네트워크 핵심 장비 및 보안 전용 제품에 대한 안전 인증 및 검사제도 시행 그리고 핵심 정보인프라 지정·보호를 위한 방법이 자세히 규정되어 있다.

---

190) Hauke Johannes Gierow, 'Cyber Security in China: New Political Leadership Focuses on Boosting National Security', China Monitor No.20, Mercator Institute for China Studies (2014.12). p.6.

셋째, 현재 국제적으로 쟁점이 되고 있는 국가간 정보 이전 및 저장과 관련한 중국정부의 입장이 잘 드러나고 있다. 법안에는 자국민 개인정보를 처리하는 기업은 수집한 데이터를 중국영토 내에 보관해야 하며, 비즈니스 목적으로 해외에 저장한 데이터는 중국정부의 승인이 필요하도록 함으로써 자국데이터에 대한 통제의도를 명확히 밝히고 있다.[191]

중국의 법제도와 정치적 환경은 우리와 다르지만, 한국 ICT 기업들이 다수 중국에 진출해 있고, 향후 사이버안전법안이 채택되어 발효된다면 직접적으로 법의 적용대상이 될 수 있으므로 한국은 동 법안의 진행과정을 예의주시하며 대응책을 강구할 필요가 있다.

제4절 러시아

러시아 인구는 2012년 12월 기준 약 1억4천3백만 명으로, 이 중 61.4%가 인터넷을 이용하고 있다.[192] 이러한 러시아는 사이버공간의 본질과 잠재력, 이용 등에 대하여 서구와는 다른 관점을 갖고 있다.[193] 마찬가지로 사이버안전(보안)에 관한 개념 또한 상당한 차이를 보여주고 있다는 평가를 받는다.[194] 특히 러시아는 사이버공간에서의 자유로운 정보교환원칙과 사이버공간에서 국경이 갖는 한계 내지 제한성에 대하여 깊이 우려하고 있으며, 국가 또는 사회에 위협이 될 수 있는 정보의 유통과 인터넷상의 주권 문제, 즉 정보공간에 대한 통제능력에 주된 관심을 갖고 있는 것으로 파악된다.

---

191) 앞의 주.

192) United Nations Statistics Division, 2012.12; International Telecommunication Union (ITU) Statistics, (2013.12).

193) Keir Giles, "Russia's Rublic Stance on Cyberspace Issues" in C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), *2012 4th International Conference on Cyber Conflict*, NATO CCD COE Publications, 2012, p.63.

194) 미국으로 대표되는 서구의 경우 정보는 자유롭게 이동할 수 있어야한다는 입장인 반면, 러시아는 사이버공간에서도 국경의 원칙이 적용되어야 한다는, 즉 주권을 중시하는 입장이다. Keir Giles, "Russian Cyber Security: Concepts and Current Activity", RFP Round-table Summary, Chatham House, 2012, p.2.

1. 러시아의 사이버정책 동향 일반

러시아의 사이버정책은 크게 '국가안보전략'과 '국가사이버안전전략' 두 가지로 나누어 접근해볼 수 있다. 전자는 사이버 분야를 포함하는 국가 전반의 안보 및 국방에 관련된 전략이고, 후자는 사이버공간의 특수성이 고려된 보다 구체적인 전략이다.

가. 국가안보전략

먼저 러시아의 국가안보전략(national security and defence strategies)을 파악함에 있어 가장 중심이 되는 정책문건은 '국가안보개념'이다. 1997년 12월과[195] 2000년 1월에 각각 국가안보개념 문서들이 발표되었는데, 2000년 '국가안보개념'[196](Концепция Национальной Безопасности Российской Федерации)은 러시아의 국익을 개인, 사회, 국가의 수준에서 국내정치, 경제, 사회는 물론 국제, 정보, 군사, 국경, 환경 등 다양한 분야에서 구현되어야 하는 이익의 총체로 규정하고 있다. 이에 따라 러시아의 안보개념 역시 단순한 군사적 안보뿐만 아니라 경제, 사회 등 기타 분야를 모두 포함하는 '포괄적 안보'(comprehensive security) 개념에 입각하여 제시되고 있으며, 그에 따라 각 세부분야에서 러시아 정부가 취해야 하는 정책을 설명하고 있다. 또한 러시아의 국익이 지속가능한 경제 발전을 통해서만 실현될 것이라고 지적하면서 경제적 기반 확충의 중요성을 강조하고 있다.[197]

2009년 5월에는 '국가안보전략 2020'[198](Стратегия национальной безопасности Российской Федерации до 2020 года)이 새롭게 발표되어 상기 2000년 '국가안보개념'을 대체하였다. '2000년 국가안

---

195) Концепция национальной безопасности Российской Федерации, (1997.12.17.).

196) 대통령령 제24호, (2000.1.10.), 〈http://archive.mid.ru//bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/36aba64ac09f737fc32575d9002bbf31!OpenDocument〉.

197) 신범식, "러시아 신(新)동방정책과 동북아 지역정치: 지역 세력망구도 변화와 러시아의 가능성 및 한계", EAI 국가안보패널 보고서: 동북아 데탕트-탈냉전 국가대외전략 비교연구, 동아시아 연구원, 2014, p.4.

198) 대통령령 제537호, (2009.5.12.), 〈http://www.scrf.gov.ru/documents/99.html〉.

보개념'에서 제시하였던 안보개념과 주요 정책방향은 '국가안보전략 2020'에서도 상당 부분 그대로 유지되고 있으나, 기존의 '포괄적 안보' 개념이 보다 구체화되었다. 국가안보의 주요 구성요소로는 국방, 국가와 공공의 안보, 러시아 국민들의 삶의 질 개선, 경제성장, 과학·기술·교육의 강화, 보건의료 강화, 문화창달, 생태계 보존, 전략적 안전성과 전략적 동반자와의 평등한 관계 등 순으로 그 내용이 구체적으로 제시되고 있다.[199]

한편, 각각 2000년, 2008년, 2013년에 발표된 '외교정책개념'(Концепция Внешней Политики Российской Федерации)은 러시아의 기본적 국제정치관, 외교정책 목표와 각 지역별 정책방향 등을 보여주는 문서로[200] 국가안보전략의 일부를 구성하고 있다.[201] 이에 따르면 러시아의 주요 관심사가 기존 냉전시기 군사적 대립과 핵무기에서 경제, 정치, 과학, 기술과 같은 비군사적 영역으로 변화하고 있음을 알 수 있다. 또한 테러리즘, 조직범죄와 같은 비전통 안보영역에서의 위협과 도전들이 대두하고 있음을 주목하고 있으며, 국제사회에서 국제법과 안전보장이사회 등 UN의 역할이 중요함과 이에 대한 존중 역시 지속적으로 강조하고 있다.

나. 국가사이버안전전략

국가사이버안전전략(national cyber security strategy)과 관련해서는 2000년 '정보안전정책'[202](Information Security Doctrine of the Russian Federation)이 발표되었다. 이후 2011년 '정보공간에서 러시아군의 활동 개념'[203](Conceptual Views

---

199) 신범식, 전게서.

200) Концепция внешней политики Российской Федерации, 2000.6.28.; 2008.7.15.; 2013.2.12., 〈http://archive.mid.ru//brp_4.nsf/0/6D84DDEDEDBF7DA644257B160051BF7F; http://archive.mid.ru//brp_4.nsf/0/76389FEC168189 ED44257B2E0039B16D〉.

201) Cyber Security Strategy Documents-Russia, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 〈https://ccdcoe.org/strategies-policies.html〉.

202) Information Security Doctrine of the Russian Federation (2000.9.9.), 〈http://archive.mid.ru//bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument〉.

203) Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space, 〈https://ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf〉.

Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space)이 수립되었으며, 2013년에는 '2020년까지의 국제정보안전분야 국가정책기본원칙'[204](Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020, '이하 국제정보안전기본원칙'이라 함)이 발표되었다. 현재 '국가사이버안전전략개념'[205](Concept of Russia's Cyber Security Strategy)의 초안이 작성되고 있는데, 발표될 경우 향후 러시아의 사이버안전전략의 추진에 중요한 영향을 미칠 것으로 예상된다.

국제정보안전기본원칙은 국제정보안전 분야에서 주요 위협과 러시아 국가정책의 목표, 목적과 우선순위 및 그 이행을 위한 메커니즘을 확인하였다.[206] 기본원칙의 법체계는 러시아연방헌법, 국제정보안전분야에서 러시아연방이 체결한 국제조약과 협정, 연방법, 러시아대통령과 연방정부의 시행령, 기타 법적문서를 포함한다. 기본원칙은 2020년을 향한 러시아연방의 국가안보전략 규정, 러시아의 정보안전독트린과 러시아외교정책의 개념, 기타 전략문서를 자세히 다루고 있다.

이들 기본원칙은 첫째, 법적, 제도적 지원을 포함하여 국제정보안전체계를 수립하는 러시아 이니셔티브를 국제적으로 증진하고, 둘째, 국제정보안전 분야에서 러시아 및 관련 국가들과 정부간 타깃 프로그램을 발전시키고, 셋째, 러시아 국가정책 이행을 위한 유관기관간 협력을 구축하고, 넷째, 실물경제에서 ICT이용을 증대시킴으로써 세계 주요 강국들과의 기술적 동등성을 성취하고 이를 유지하는 것이다.

동 원칙에서 '국제정보안전'이라 함은 정보 영역에서 개인, 사회 및 국가의 권리 침해 가능성을 방지하고, 국가중요정보기반시설에 대한 파괴적, 불법적 영향을 방지하는 글로벌 정보공간을 위한 조건으로 정의된다. 그리고 이러한 국제정보안전에 대한 주요위협으로 다음의 네 가지를 들고 있다. 첫째, ICT를 국제법에 위반하여 군사적,

---

204) Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года, PR-1753, (2013.7.24.), 〈http://www.scrf.gov.ru/documents/6/114.html〉; 〈https://ccdcoe.org/sites/default/files/ strategy/RU_state-policy.pdf〉.

205) Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года, 〈http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf〉.

206) 국제정보안보기본원칙, para.2.

정치적 목적의 정보 무기로 사용하는 것이다. 여기에는 국가의 주권과 영토를 침해할 목적으로 하는 적대행위나 공격적 행동, 국제평화와 안전 및 전략적 안정성을 위협하는 행위가 포함된다. 둘째, ICT를 테러 목적으로 이용하는 것이다. 주요 정보기반시설에 파괴적인 영향을 주거나 테러리스트를 옹호하고 테러행위자를 모집하는 것 등이 포함된다. 셋째, ICT를 주권국가의 내정을 간섭하거나, 공공질서 위배 등 사회적 차별과 혼란을 야기할 목적으로 이용하는 것이다. 넷째, ICT를 범죄 목적으로 이용하는 것이다. 여기에는 컴퓨터 정보에 무단으로 접속하거나, 악의적인 컴퓨터 소프트웨어를 제작, 사용하고 배포하는 행위를 포함한다.

동 국가정책의 목표는 국제정보안전 시스템 설립을 목적으로 하는 국제규범체제를 증진하는 것이다. 따라서 러시아가 양자, 다자, 지역 및 글로벌 수준의 국제정보안전시스템 설립을 목적으로 이러한 시스템 구축 과정에 참여하는 것, ICT를 국가 주권과 영토 침해 및 국제 평화와 안전을 위협할 목적으로 하는 적대행위에 이용할 위험을 감소시키고자 노력하는 것 등을 포함하여 국제규범체제 증진을 위한 러시아의 정책 수립에 대하여 구체적인 방향을 제시하고 있다.

국제사회에 있어서는 러시아는 사이버공간에 대한 불간섭을 중요시하는 한편, 사이버공간에 관한 새로운 국제협약의 채택을 촉구하고 있다. 중국, 타지키스탄 및 우즈베키스탄과 같은 국가들이 이러한 러시아의 입장을 지지하고 있으며, 상하이협력기구(Shanghai Cooperation Organization, SCO) 회원국들은 국제사이버안전을 위한 러시아의 제안과 매우 유사한 내용에 합의한 바 있다. 그밖에 러시아는 앞서 언급한대로 입장 차이를 갖고 있는 서구국가들과도 다양한 논의의 장에서 국제사이버안전에 관한 대화를 하고 있으나 광범위한 수준에서의 협상에 그치고 있는 한계를 나타내고 있다.

2. 사이버안전 정책

가. 주요 입법

러시아의 사이버안전과 관련된 대표적인 입법으로는 '개인정보보호에 관한 연방법 제152호'[207](Federal Law 152 on Personal Data Protection, 이하 '개인정보보호

법')와 '블랙리스트 등재 및 ISP 통제에 관한 연방법 제139호'[208](Federal Law 139 on Blacklisting and ISP Control, 이하 '인터넷규제법')가 있다.

먼저 연방법 제152호, 즉 개인정보보호법은 2006년 제정되어 2007년부터 시행되고 있다. 동 법은 연방정부기관, 주(州)정부기관 등 국가기관과 지방자치단체의 개인정보 처리(processing)와 관련된 활동을 규제하기 위한 것으로,[209] 총 6개 장(Chapter) 25개 조문으로 구성되어 있다. 제1장은 일반조항(Genreal Provision)으로 법률의 적용범위와 목적, 주요 용어에 대한 정의, 그리고 입법근거를 밝히고 있다. 제2장은 개인정보처리에 관한 원칙과 요건을 규율하며, 제3장은 개인정보주체의 권리를, 제4장은 운영자(operator)의 의무를 규정하고 있다. 제5장은 개인정보처리의 통제, 감독 및 법률 위반의 책임에 대하여 규율하며, 제6장은 최종조항을 담고 있다.

입법목적은 프라이버시권, 개인 및 가족의 비밀에 대한 권리를 포함하는 개인정보를 처리하는 동안 그 개인의 권리와 자유를 보장하는데 있다.[210] 동 법은 개인정보를 '특정 또는 식별된 개인'[211]에 직접 또는 간접적으로 관련되는 모든 정보로 정의하고 있다. 이러한 정의는 대체로 개인정보에 대한 일반적인 정의에 따른다고 할 수 있다.

다음으로 연방법 제139호, 즉 인터넷규제법은 2012년 7월 개정되었는데 위 각주에서 밝혔듯이 "보건, 발전 및 러시아 연방의 활동에 유해한 정보로부터 아동을 보호하기 위한 연방법 개정"이라는 매우 긴 명칭을 갖고 있다. 그 실질적인 내용은 법률명에서 밝히고 있는 목적을 달성하기 위하여 인터넷을 제한(restriction)할 수 있음을 담고 있다.

---

207) Федеральный закон от 26.07.2006 №. 152-ФЗ О персональных данных; Federal Law of 27 July 2006 N 152-FZ on Personal Data. 자세한 법조문은 러시아 '연방통신·정보기술·매스컴감독원'(Roscomnadzor) 홈페이지 영문 번역본 참조, http://pd.rkn.gov.ru/authority/p146/p164/,

208) Федеральный закон Российской Федерации от 28 июля 2012 г. N 139-ФЗ "О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации". Российская газета, 30/07/2012; Federal law No. 139-FZ "On Amendments to Federal Law On Protecting Children from Information Harmful to Their Health and Development and Certain Legislative Acts of the Russian Federation", July 28, 2012.

209) 개인정보보호법 제1조.

210) 개인정보보호법 제2조.

211) a particular or identified individual, 정의 조항 이후 "개인정보주체"(personal data subject)로 표기하고 있음.

동 법에 따르면 정부는 사법적 감독을 위한 별도의 기제 없이 차단해야 하는 인터넷 서비스제공자(ISP) 웹사이트의 목록을 작성할 수 있다. 근본적인 취지는 아동 포르노, 마약 관련 재료 또는 극단적인 내용을 포함하는 불법 콘텐츠와 사이트에 대한 접근을 제한하기 위한 것이나, 합법적인 사이트 또한 동 법에 따라 차단되고 있다는 NGO 등의 비판을 받고 있다.[212]

상기 두 법의 시행은 모두 통신·매스미디어부(Ministry of Telecom and Mass Communications)와 연방정부의 통제 하에 '연방통신·정보기술·매스컴감독원'(Roscomnadzor)이 담당한다.[213] 동 기관은 특히 인터넷규제법이 시행됨으로써 막강한 권한을 갖게 되었다. 즉, 어떤 사이트가 법이 제한하는 내용을 포함하고 있는지 여부에 기반하여 해당 사이트의 차단 여부를 결정할 수 있는 권한을 보유하게 된 것인데, 이러한 결정은 법원의 사전 승인을 필요로 하지 않는다. 결과적으로 Roscomnadzor는 인터넷상의 정보를 걸러내고 통제하는 분야에서 독보적인 주체가 되고 있는 실정이다.

나. 기타 관련 제도

러시아는 이상에서 살펴본 주요 입법 외에도 사이버안전을 추구하기 위하여 다음의 표에서 확인할 수 있듯이 중요 인프라 보호, 암호화, 기밀 데이터 보호, 정보보호 솔루션 감사 등의 다양한 제도를 운영하고 있다. 참고로 각 기관은 모두 보안 솔루션 및 데이터 보호를 위한 자체적인 인증(certification) 방식과 요건을 갖추고 있다. 그러한 인증방식과 요건이 서로 매우 유사하지만, 인증 절차는 상이하며 이에 대한 통제 또한 각 기관별로 이루어진다. 러시아의 사이버안전 관련 제도 현황은 다음과 같다.[214]

---

212) 예컨대 미국의 국제인권단체인 Freedom House가 정기적으로 발행하는 보고서에 따르면 동 법이 합법적인 온라인 활동에 부정적인 영향을 주지 않으면서 시행되기 어렵고, 직접적으로 온라인 콘텐츠를 검열하는데 사용될 수 있다는 것을 경고하는 비판의 목소리가 있다는 점을 밝히고 있다. Freedom on the Net 2013-Russia, Key Developments: May 2012-April 2013, https://freedomhouse.org/report/freedom-net/2013/russia.

213) Федеральная служба по надзору в сфере массовых коммуникаций и связи (Роскомнадзор); The Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor).

〈표 2-4-1〉 러시아의 사이버안전 관련 제도 현황

사이버안전 관련 제도	담당 기관
개인정보보호(Personal Data Protection)	연방통신·정보기술·매스컴감독원 (Roscomnadzor)(연방법 제152호)
인터넷규제(Blacklist & ISP Control)	연방통신·정보기술·매스컴감독원 (Roscomnadzor)(연방법 제139호)
중요 인프라 보호 (Critical Infrastructure Protection: CIP)	연방기술·수출통제원(FSTEC)[215] 연방보안국(FSB)[216]
암호화(Cryptography)	연방보안국(FSB)
정보보안(Information Security) – 정부 부문(in Gov't sector)	연방보안국(FSB) 연방기술·수출통제원(FSTEC) 연방경호국(FSO)[217]
정보보안- 해외소재 정부기관 부문	해외정보국(SVR)[218]
정보보안 – 국방부(Ministry of Defence, 'MoD')	국방부(MoD)[219] 연방보안국(FSB)
정보보안 – 기밀 데이터 보호 (confidential data protection)	연방기술·수출통제원(FSTEC)
정보보안 솔루션(소프트웨어 및 하드웨어) 감사 (Information Security solutions compliance)	연방기술·수출통제원(FSTEC)
사이버범죄수사(Cybercrimes investigations)	내무부(MoI)[220]

214) Global Cybersecurity Index & Cyberwellness Profiles, ABI Research, International Telecommunication Union (ITU), 2015, p.25.

215) Федеральная служба по техническому и экспортному контролю; Federal Service for Technical and Export Control of Russian Federation (**FSTEC**). 중요 인프라 보호는 기밀에 해당하며, 허가 받은 기업과 산업에만 배포됨.

216) Федеральная служба безопасности Российской Федерации (Federal'naya Sluzhba Bezopasnosti: **FSB**); Federal Security Service of the Russian Federation. 연방보안국은 중요 인프라 보호 전략을 수립, 발표함.

217) Федеральная служба охраны (Federalnaya Sluzhba Okhrany: **FSO**); Federal Guard Service of the Russian Federation 또는 Federal Protective Service.

218) Слу́жба вне́шней разве́дки (Sluzhba Vneshney Razvedki: **SVR**); Foreign Intelligence Service of the Russian Federation.

219) Министерство обороны Российской Федерации; Ministry of Defence of the Russian Federation (**MoD**).

220) Министерство внутренних дел; Ministry of the Interior of the Russian Federation (**MOI**).

기술적 수단으로서 사이버안전의 한 축을 담당하는 컴퓨터사고 대응조직(Computer Incident Response Team: CIRT)으로는 러시아 정부의 공식 CERT[221](GOV-CERT), 조인트 정부 프로젝트 CIRT[222](RU-CERT), 그리고 기업들의 사고대응사업 CIRT[223](CERT-GIB) 등을 운용하고 있다. 한편 국제적으로 인정된 사이버안전기준을 이행하기 위한 국가 차원의 공식 표준은 없는 상태이며, 사이버안전과 관련하여 정부기관이나 공공 전문가들을 인증하기 위한 자격증 제도 또한 보유하고 있지 않다.[224]

3. 사이버범죄 정책

가. 형법

러시아연방 형법(Criminal Code of the Russian Federation)은 1996년 5월 하원에서 채택되어 동년 6월 연방의회에서 승인된 후 대통령에 의해 서명, 공포되었다. 동법은 구소련의 1960년 형법을 대체한 것으로 1997년 1월 1일부터 시행되어 현재에 이르고 있다.[225]

구소련 형법에는 사이버범죄 관련 규정이 부재하였기 때문에 명백하게 공공에 위협이 되는 컴퓨터범죄일지라도 형사 관할대상 범죄에 해당하지 않아 불법이 아니었다. 그러나 이러한 상황은 1997년 새로운 형법이 도입되면서 바뀌게 되었다. 즉, 동법 제28장이 '컴퓨터 정보 범죄'(computer information crimes)를 새로운 범죄유형으로 규정함으로써 사이버범죄가 비로소 러시아 형법의 관할 대상으로 등장하게 된 것이다.

제28장은 3개 조항으로 이루어져 있다. 제272조는 컴퓨터 정보에 대한 불법 접근, 제273조는 전산정보 처리가공시설에 유해한 프로그램의 작성·사용 및 유포, 제274조는 전산정보 처리가공시설, 그 시스템 또는 네트워크 사용규칙 위반을 규율한다. 이하에서 각 조항에 대하여 간단히 살펴본다.

---

221) http://gov-cert.ru.
222) http://www.cert.ru/ru/about.shtml.
223) http://cert-gib.com.
224) Global Cybersecurity Index & Cyberwellness Profiles, ABI Research, International Telecommunication Union (ITU), 2015, p.389.
225) 한종만·김용욱·김정훈, 러시아연방헌법, 한국형사정책연구원, 2010, p.13.

1) 컴퓨터 정보에 대한 불법접근

제272조는 컴퓨터 및 컴퓨터 네트워크를 포함하는 컴퓨터 시스템의 소유자의 권리를 보호하기 위한 규정이다. 보호대상인 컴퓨터 정보에 불법적으로 접근했을 경우(예컨대 정보를 파괴하거나 비밀번호를 무단으로 사용하거나 관리자 명의를 도용하는 등) 처벌 대상이 된다. 동 조항에서는 이와 같은 불법접근으로 인하여 발생하는 정보의 멸실, 차단, 수정 또는 정보의 복사, 전산정보 처리가공시설 업무와 시스템 또는 네트워크의 파괴 등의 결과 간의 인과관계가 중요하다. 따라서 의도하지 않은 단순한 우연, 실수, 또는 오류에 의해 불법접근이 이루어졌을 경우에는 형사책임이 수반되지 않는다.

제272조 컴퓨터 정보에 대한 불법 접근[226)]

① 법률상 보호되는 컴퓨터 정보, 즉 기계소유자, 전산정보 처리가공시설, 전산정보 처리가공시스템 또는 그 네트워크의 정보에 대한 불법 접근을 통하여 정보의 멸실, 차단, 수정 또는 정보의 복사, 전산정보 처리가공시설 업무와 시스템 또는 네트워크의 파괴를 발생하게 한 자는 200,000루블 이하 또는 18월 이하의 임금 또는 기타 수입에 해당하는 벌금, 또는 6월 이상 1년 이하의 교화노동, 또는 2년 이하의 자유박탈에 처한다.

② 위의 죄를 사전공모에 따라 집단적으로 범하거나, 조직집단에 의하여 범하거나, 또는 자신의 공적지위를 이용하여 범하거나, 전산정보 처리가공시설 또는 전산정보 처리가공시스템 또는 그 네트워크에 접속이 가능한 자가 범한 때에는 100,000루블 이상 300,000루블 이하 또는 1년 이상 2년 이하의 임금 또는 기타 수입에 해당하는 벌금, 또는 6월 이상 2년 이하의 교화노동, 또는 3월 이상 6월 이하의 구류, 또는 5년 이하의 자유박탈에 처한다.

---

226) Article 272. Illegal Accessing of Computer Information

1. Illegal accessing of legally-protected computer information, that is, information on machine-readable media, in computers, computer systems, and their networks, if this deed has involved the destruction, blocking, modification, or copying of information, or the disruption of the work of the computers, computer systems, or their networks, shall be punishable by a fine in the amount up to 200 thousand roubles, or in the amount of the wage or salary, or any other income of the convicted person for a period up to 18 months, or by corrective labour for a term of six to twelve months, or by deprivation of liberty for a term of up to two years.
2. The same deed, committed by a group of persons in a preliminary conspiracy or by an organized group, or by a person through his official position, and likewise by a person who has access to computers, computer systems, or their networks, shall be punishable by a fine in the amount of 100 thousand to 300

2) 유해컴퓨터프로그램의 생산, 사용 및 유포

제273조는 컴퓨터 프로그램을 만들거나 기존 프로그램을 변경하는 등의 행의를 통하여 정보시스템에 위해를 끼치는 경우를 규율함으로써 컴퓨터 시스템의 소유자와 시스템에 포함된 정보의 소유자의 권리를 보호하기 위한 규정이다. 가장 대표적인 예로 바이러스 프로그램을 제작하여 특정 시스템을 감염시키는 경우를 들 수 있다. 동 조항에 따라 형사 책임을 부담함에 있어 정보 소유자에게 부정적인 결과가 초래될 것을 요구하지 않는다. 부정적인 결과를 초래하는 것으로 알려진 프로그램을 제작하거나 기존 프로그램을 수정했다는 사실 자체만으로도 동 조항의 관할대상 범죄가 되는 것이다.

제273조 전산정보 처리가공시설에 유해한 프로그램의 작성·사용 및 유포[227]

① 정보의 비합법적인 소멸·차단·수정·복사 또는 전산정보 처리가공시설의 작업이나 전산정보 처리가공시설의 시스템 및 그 네트워크의 파괴 등을 고의적으로 실행하기 위하여, 전산정보 처리가공시설의 프로그램을 작성하거나, 그 주요 프로그램을 변경하거나, 이러한 프로그램 또는 프로그램 매체를 사용하거나 확산시킨 자는 3년 이하의 자유박탈에 처하되 200,000루블 이하 또는 18월 이하의 임금 또는 기타 수입에 해당하는 벌금을 병과한다.
② 위 행위가 과실로 인하여 중대한 결과를 발생하게 한 때에는 3년 이상 7년 이하의 자유박탈에 처한다.

---

thousand roubles, or in the amount of the wage or salary, or any other income of the convicted person for a period of one to two years, or by corrective labour for a term of one to two years, or by deprivation of liberty for a term of up to five years.

※ 영문조문은 UN마약범죄사무소(UNODC) 사이트에서 제공하는 자료를 이용함. 이하 동일.〈https://www.unodc.org/tldb/showDocument.do?documentUid=8546〉.

227) Article 273. Creation, Use, and Dissemination of Harmful Computer Viruses

1. Creation of computer viruses for the introduction of changes to existing programmes, which knowingly leads to the unsanctioned destruction, blocking, modification, or copying of information, the disruption of the work of computers, computer systems, or their networks, and also the use or dissemination of such viruses or machine-readable media with such viruses, shall be punishable by deprivation of liberty for a term of up to three years, with a fine in the amount up to 200 thousand roubles, or in the amount of the wage or salary, or any other income of the convicted person for a period up to 18 months.
2. The same acts, which have involved by negligence grave consequences, shall be punishable by deprivation of liberty for a term of three to seven years.

3) 컴퓨터, 시스템 혹은 네트워크 운영규칙의 위반

제274조는 컴퓨터, 시스템, 네트워크 등에 접근 권한을 가진 자가 사용규칙을 침해하여 법적으로 보호되는 정보를 파괴하거나 수정하는 등의 행위를 통하여 중대한 피해를 끼쳤을 경우 그러한 자에게 형사책임을 부여하는 규정으로, 시스템이 안전하게 유지될 수 있어야 하는 소유자의 권리를 보호하데 그 목적이 있다. 제274조는 앞서 살펴본 제272조와 상당히 유사한 범죄요건을 갖고 있는 바, 그 차이는 권한 있는 자의 불법접근인지 권한 없는 자의 불법접근인지에 달려있다.

제274조 전산정보 처리가공시설, 그 시스템 또는 네트워크 사용규칙 위반[228]

① 전산정보 처리가공시설, 그 시스템 또는 네트워크에 접속할 수 있는 자가 전산정보 처리가공시설, 그 시스템 또는 네트워크의 사용규칙에 위반하는 행위를 통하여 법률상 보호된 전산정보 처리가공시설의 정보의 멸실, 차단 또는 변경을 발생하게 한 때에는 5년 이하의 기간 동안 일정한 공직 또는 활동에 종사할 권리를 박탈하거나, 180시간 이상 240시간 이하의 강제노동, 또는 2년 이하의 자유제한에 처한다.
② 위 행위가 과실로 인하여 중대한 결과를 발생하게 한 때에는 4년 이하의 자유박탈에 처한다.

4. 시사점

러시아의 사이버정책 동향과 사이버안전 및 사이버범죄정책에 대하여 살펴본 결과, 아래 표에서도 볼 수 있듯이 다양한 분야에서 체계가 잘 정비되어 있다고 평가할 수 있다.

러시아의 사이버 관련 정책은 정보 인프라에 대한 물리적인 보호와 함께 무엇보다

228) Article 274. Violation of Rules for the Operation of Computers, Computer Systems, or Their Networks
1. Violation of rules for the operation of computers, computer systems, or their networks by a person who has access to computers, computer systems, or their networks, which has involved the destruction, blocking, or modification of legally-protected computer information, if this act has inflicted substantial damage, shall be punishable by disqualification to hold specified offices or to engage in specified activities for a term of up to five years, or by compulsory works for a term of 180 to 240 hours, or by restraint of liberty for a term of up to two years.
2. The same act, which has involved by negligence grave consequences, shall be punishable by deprivation of liberty for a term of up to four years.

정보의 흐름을 관리·통제함으로써 사이버안전을 확보하는데 초점을 맞추고 있는 것으로 판단된다. 러시아가 이와 같이 사이버공간에 대한 공권력의 개입을 통하여 사이버안전을 추구하는 정책은 전반적으로 사이버 정보의 자유로운 흐름을 중시하는 서구와 가장 중요한 차이를 보여주는 특징이라 할 수 있겠다.

〈표 2-4-2〉 러시아 사이버안전정책의 체계

국가안보 및 국방전략		국가안보개념(2000)
		국가안보전략 2009-2020(2008)
		외교정책개념(2013)
국가사이버 안전전략	정책	정보보안정책(2000)
		정보공간에서 러시아군의 활동개념(2011)
		국제정보보안분야 국가정책 기본원칙(2013)
		국가사이버안전전략개념(초안 검토중)
	법	형법(사이버범죄 대응)
		개인정보보호법(2006)
		인터넷규제법(2012)
	기술	GOV-CERT, RU-CERT, CERT-GIB
	역량구축	표준개발: ITU-T Study Group Question 17
	협력	국가간: CET-GIB
		기관간: FSB, MoD, MVD 등

사이버범죄와 관련해서 러시아는 사이버 공간에서의 포괄적인 증거 수집능력이 매우 높은 수준인 것으로 알려져 있으며, 사이버범죄에 대한 소프트웨어와 기술 개발에 있어 세계를 선도하고 있다. 무엇보다 가장 두드러지는 특징은 정부당국이 법원의 허가 없이 자신의 재량에 따라 인터넷 자원을 폐쇄시킬 수 있는 권한을 갖고 있다는 점이다. 또한 최근까지 러시아의 사이버범죄자들은 러시아 국민을 대상으로 저지른 사이버범죄가 아닌 경우 사실상 처벌받지 않았다. 러시아는 국내외적으로 사이버범죄에 대한 기소 압력이 증가함에 따라 최근 들어 지적재산권을 침해하는 인터넷 공유자원에 대하여 단속하는 등 점차 처벌을 강화하고 있는 실정이다.

제5절 한국

1. 한국의 사이버정책 동향 일반

한국은 지정학적으로 중국과 러시아, 일본과 미국의 중간에 위치해 있다. 따라서 중국의 입장에서는 태평양으로 뻗어 나가기 위한 중요한 거점이 되고, 미국과 일본의 입장에서는 대륙으로 진출하기 위한 교두보가 된다. 그러므로 한국은 과거에도 그랬듯이 여전히 열강들의 틈바구니에서 힘겨운 지위를 지켜내고 있다. 또한 한국은 아직까지 전쟁이 끝나지 않은 휴전상황이다. 그래서 우리의 북쪽에는 항상 북한과 대치하고 있다. 비록 우리는 지금 마치 종전이 된 것과 같이 평화를 누리는 것처럼 보이지만, 언제 다시 전쟁이 재발할지 예측하기 어려운 상황이다. 그런 상황에서 한국은 국방에 수많은 예산을 투입하고 있으며,[229] 발발할지도 모르는 전쟁에 대비하기 위해 젊은이들은 국방의 의무를 지고 군복무를 하고 있으며, 군복무 뒤에도 예비군이나 민방위에 편성되어 국가를 지키고 있다.

이처럼 가시적으로 눈에 보이는 국가의 안보에 대해서는 우리 국민들이 문제의식이나 위기감을 가지고 있다고 할 수 있다. 하지만 우리가 상시 위협받고 있고 대치하고 있는 사이버안보와 관련해서는 그 중대성과 치명성에도 불구하고 아직까지도 위기의식을 제대로 갖지 못하고 낮은 수준의 막연한 인식에 그치고 있는 실정이다. 그러나 사이버안보를 제쳐두고 국가안보를 논하는 것은 어불성설이라고 할 수 있다. 미국의 경우 오바마 행정부는 사이버안보에 대해 그 중대성을 높이 평가하여 그 시작과 함께 사이버담당 보좌관을 두었고, 올 해 발표된 '2015년 국가안보전략'(National Security Strategy)에서도 다시금 그 중요성을 역설하였다.[230] 그와 같은 오바마 행정부의 입장은 최근 한국을 방문하여 고려대학교에서 강연을 한 존 캐리 미 국무장관의 강연문에

---

229) 한국의 국방예산은 344억달러(약 38조700억원)로서 439억 달라인 독일에 이어 세계 10위 규모라고 한다. 1위는 5,810억 달러인 미국이고, 2위는 1,294억 달러의 중국이며, 그 뒤를 이어 808억 달러의 사우디아라비아, 700억 달러의 러시아, 618억 달러의 영국이 많은 규모의 국방예산을 지출하는 것으로 나타나고 있다. 세계 7위 규모인 일본은 477억 달러(55조 7,800억원)를 지출하여 한국에 비하여 매우 많은 것으로 나타났다; 〈http://daily.hankooki.com/lpage/politics/201502/dh20150212102716137530.htm〉, 2015.10.31. 방문.

230) 2015년 국가안보전략에 따르면 오바마 행정부는 중국의 사이버공격에 대한 우려와 북한의 사이버테러에 대한 위험에 대해서 경계를 하면서 자국의 사이버안보에 보다 역점을 둘 것을 표명하고 있다; 백악관, 국가안보전략(2015.2), 7면 이하.

서도 그대로 드러나고 있다.[231]

하지만 한국은 3.4디도스 공격, 7.7디도스 공격 뿐 아니라 수많은 사이버공격 등으로 인해 사이버안보가 위협받고 있는 상황에서도 아직까지 대응체계나 대응능력이 충분하다고는 할 수 없는 상황에 처해 있다. 정부는 사이버공격 이후 다양한 정책을 발표하였지만 해당 정책이 제대로 수행되고 있는지는 여전히 미지수이며, 사이버안보를 지탱해 줄 수 있는 근거 법률은 여전히 국회를 통과하고 있지 못하고 있다. 경찰청은 조직 개편으로 사이버테러대응센터를 사이버안전국으로 승격하였고, 컨트롤 타워가 없다는 지적에 청와대에서는 청와대가 컨트롤 타워를 맡기로 하고 사이버안보비서관을 신설하기도 하였다. 그러나 해당 조직들이 사이버안보에 어떻게 효율적으로 동작할 수 있을지에 대해 여전히 의구심이 표출되고 있다.

그런 상황에서 우리는 현재 한국의 사이버안보 및 사이버범죄와 관련된 상황을 좀 더 객관적으로 살펴볼 필요가 있다. 그리고 그를 바탕으로 해외 주요국들의 상황과 비교분석해 보고, 개선점을 도출하여 신속히 적용할 필요가 있다. 따라서 아래에서는 한국의 전체적인 사이버위기 대응체계에 대해서 살펴보고, 다시금 민간부문, 국방부문, 사이버범죄 부분으로 나누어서 관련 법령과 조직체계 등을 좀 더 구체적으로 살펴보아 이후에 진행될 비교분석 과정의 근거로 삼고자 한다.

가. 주요 사이버안보 정책 추진 경과

1) 2011년 국가 사이버안보 마스터플랜

점차로 고도화 및 지능화 되고 있는 한국의 사이버위협 상황에서 보다 효율적으로 대응하기 위해 정부는 2011년 8월 2일 관계부처 합동으로 '국가 사이버안보 마스터플랜(이하 '마스터플랜'이라고 함)'을 발표한다. 마스터플랜의 수립 과정을 보면 2011년 5월 11일 '국가 사이버안전 전략회의'에서 마스터플랜을 수립할 것을 결정하고, 동년 5월 13일~7월 5일에 걸쳐 관련기관이 함께 초안을 마련하여 전문가 자문을 받고, 동년 7월 6일~18일 걸쳐 '국가 사이버안전 대책회의'의 심의·의결을 받은 후, 동년

231) 강연에서 존 캐리는 사이버상의 표현의 자유와 함께 북한의 사이버테러에 대한 문제점을 부각하였다; 〈http://www.yonhapnews.co.kr/bulletin/2015/05/18/0200000000AKR20150518162000004.HTML?input=1195m〉, 2015.10.31. 방문.

8월 2일 50개 세부추진과제를 도출해 내었다.[232]

주요 내용을 보면 5대 추진전략으로 ① 민·관·군 합동 대응체계 정립, ② 핵심시설·기밀보호 강화, ③ 범국가적 사이버공격 탐지·차단, ④ 국제공조를 통한 억지력 확보, ⑤ 사이버안전 기반 조성 등을 제시하고 있다.[233] 우선 대응체계 정비 및 부처간 역할 정립을 위해서 사이버위협에 대한 정보를 공유하고, 공조 등 합동성을 강화하기 위해서 국가사이버안전센터에 민·관·군이 참여하는 "국가 사이버위협 합동대응팀"을 구축하도록 하고 있다. 이 합동대응팀은 종합판단, 합동상황, 합동분석 및 합동조사 분야로 구성되어 2012년 1월부터 본격적으로 가동하도록 되어 있었다. 또한 국정원이 평시와 위기시에 국가 사이버안보에 관한 제반사항들을 총괄하고, 방송통신위원회가 방송과 통신 등과 관련된 사이버안보 관련 업무를 수행하며, 행정안전부가 전자정부 대민서비스, 통합전산센터, 지자체 등과 관련된 업무를 수행하는 등 유관부처들을 역할을 확정하고 정립하게 되었다.[234]

이를 바탕으로 마스터플랜에서는 크게 다섯 가지의 중점 추진사항을 강조하였다. 첫째로, 사이버공격을 조기 탐지하고 그에 대해 신속히 대응할 수 있는 체계를 확립하는 것이다.[235] 사이버공격을 조기 탐지하고 차단하기 위해서 "국제관문국 - 인터넷서비스업체 - 기관 및 개인"을 하나로 연결하는 소위 "3선 방어체계"를 정립하도록 하였다. 특히 금융기관의 보안시스템을 보강하고 보험사 및 카드사 등으로 보안관제를 확대하는 등의 조치를 통해 금융분야에서의 대응체계를 강화시켰다. 그와 함께 좀비 PC에 대해서 신속한 치료를 할 수 있도록 전용 백신을 개발하고 배포하는 것에 노력을 기울이기 위해 민·관의 협력을 강화하여 사이버치료체계를 보강하고 DDoS 긴급대피소를 확대하기도 하였다.

둘째로, 중요자료나 핵심시설의 보안관리 수준을 매우 높은 수준에서 유지하도록 하였다.[236] 국가기밀 보호를 위해서는 비밀관리시스템을 확대 구축하고 암호체계를 개선하여 보안 수준을 한 단계 업그레이드 하였다. 그리고 전력이나 교통 등과 같은 핵심시설에 대한 정보통신시스템 보안대책을 강화하며, 관련 기관과 협력하여 합동으

232) 2011 국가사이버안보 마스터플랜, 1/3면.
233) 앞의 주.
234) 2011 국가사이버안보 마스터플랜, 2/3면.
235) 앞의 주.
236) 앞의 주.

로 기동점검 체계를 구축하기로 하였다. 무엇보다 보안문제가 조직 내부보다는 외부의 부주의로 인한 경우가 많기 때문에 외주 용역사업 보안관리를 강화함과 동시에 책임범위를 명확화 하고, 정부가 사용하는 소프트웨어의 보안 취약점에 대해 진단하는 것을 의무화 하도록 하는 제도를 도입하기로 하였다.

셋째로, 사이버안보강화 기본을 조성하기 위해 법령, 인력, 예산에 집중하였다.[237] 그래서 대통령훈령인 "국가사이버안전관리규정"을 개정하고 신규 관련 법규를 제정하여 법적 근거를 마련하고, 정부 소관 분야별 사이버보안 전담조직과 인력보강 및 인력양성에 노력을 기울이며, 정보보호제품의 수출을 지원하고, 정보보호 R&D예산을 5%에서 10%로 확대하기로 하였다.

넷째로, 사이버도발 억지력을 확보하고 국제공조를 강화하고자 하였다.[238] 사이버안보와 관련된 주요국가 및 국제기구 등과 양자 및 다자간 정보공유체계를 구축함과 동시에 사이버분야에 있어서 협력확대를 모색하였다. 그리고 사이버공격의 주체와 그 의도를 알아내고, 국민의 의혹해소와 공신력을 확보하기 위해서 '민간 검증단'을 운영하기로 하였고, 사이버위기 상황에서 적절하게 대응하기 위해 유관기관과 협력하여 통합훈련을 실시하여 사이버안보의 내실화와 활성화를 도모하도록 하였다.

다섯째로, 사이버안보에 대한 마인드가 사회전반으로 확산될 수 있도록 노력을 기울이기로 하였다.[239] 그를 위해 대국민 사이버보안 인식제고와 저변확대를 위해서 범정부 차원에서 법정기념일인 "정보보호의 날"을 제정하기로 하였고, 개인정보를 보호하고 좀비PC의 양산을 방지하기 위해서 '클린인터넷 운동'을 민간분야에서 활성화 시키며, 초중고를 대상으로 정보보호 교육을 강화하기로 하였다.

2) 2013년 국가 사이버안보 종합대책

2013년 정부는 방송사 및 금융기관을 대상으로 한 3.20테러 및 6.25 사이버공격이 발생하면서 다시금 "국가 사이버안보 종합대책"을 수립하고 사이버안보 강화를 위한 4대 전략(PCRC)를 발표하였다.[240]

첫째로, 사이버위협에 대해 즉각적인 대응방안을 높이기 위해서는 반드시 컨트롤타

237) 2011 국가사이버안보 마스터플랜, 3/3면.
238) 앞의 주.
239) 앞의 주.
240) 2013년 7월 4일 미래창조과학부 보도자료 참조(http://www.msip.go.kr, 2015.10.31. 방문).

워가 필요한데 그 컨트롤타워를 청와대가 담당하고, 국정원이 실무담당, 미래부 및 국방부 등 유관 기관이 각자의 임무를 수행하도록 하였다. 따라서 청와대를 비롯해서 각각의 대응기관들이 사이버상황에 대해서 즉각적으로 인지하고, 판단하여 대처할 수 있도록 '동시 상황전파 체계'를 구축한다고 하였다. 그와 함께 중대한 사이버 공격에 대해서는'민·관·군 합동대응팀'을 구축하여 상호협력과 함께 공조를 강화한다고 하였다.

둘째로, 이제까지 사이버위기에 처하여 유관기관들간의 정보공유가 원활하지 못하였기 때문에 그를 해결하기 위해 2014년까지 국가차원의 '사이버위협정보 공유시스템'을 구축하기로 하였고, 민간과의 정보공유 및 협력강화를 추진한다고 하였다.

셋째로, 사이버공간상의 보호대책을 보다 강화하기 위해 2017년까지 주요정보통신기반시설을 209개에서 400개로 확대한다고 하였다. 그와 함께 주요 국가기반시설의 경우 시스템을 인터넷망에서 분리하여 운영하도록 하였으며, 주요 시설의 특징에 따라 특화된 위기대응훈련을 실시한다고 하였다. 특히 주요 민간기업의 경우 정보보호관리체계(ISMS)의 인증 대상을 150개에서 500개로 확대하며, 중소기업에 대해서는 보안취약점 점검, 교육지원 등을 제공한다고 하였다.

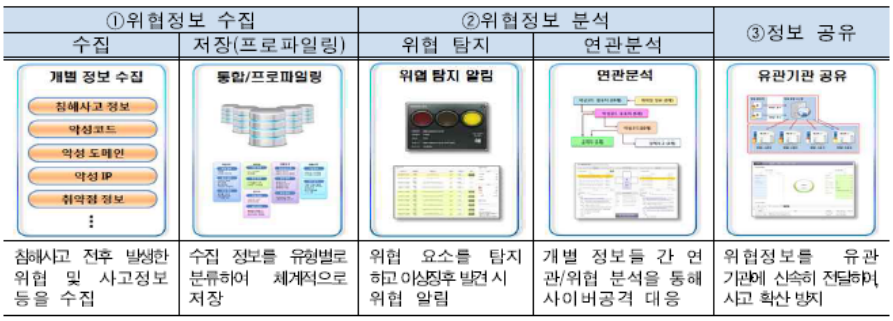
넷째로, 2017년까지 적어도 사이버 전문인력 5,000명을 양성하기 위해서 양성사업을 확대하고, 영재교육원 등을 설립하고, 암호 · 인증 · 인식 · 감시 · 탐지 등과 같은 5대 기반분야, 스마트폰 · IoT/M2M · 클라우드 · ITS · 사회기반 등과 같은 5대 신성장 분야 등에 집중적인 연구개발을 통해 기술 경쟁력을 강화한다고 하였다.

이제까지 사이버안보와 관련된 정책이 여러 차례 발표되었지만 해당 대책의 성과에 대해서 보다 구체적으로 밝힌 적은 흔하지 않았다. 하지만 2013년 발표된 대책에 대해서 미래부는 2014년에 구체화된 성과들에 대해 브리핑을 하였다.[241]

첫째로, 정부는 청와대를 컨트롤타워로 하여 민·관·군이 유기적으로 협력할 수 있는 대응체계를 마련하였다고 하였다. 무엇보다 사이버위협 정보를 수집 및 검토하여 관계기관들이 관련 정보를 신속하게 공유할 수 있는 시스템인 "사이버위협 정보분석·공유시스템(C-TAS: Cyber Threats Analysis System)"을 구축하여 2014년 8월에

241) 미래창조과학부 보도자료, 국가 사이버안보 종합대책 성과, (2014.11.17.) 참조(http://www.msip.go.kr, 2015.10.31. 방문).

본격적으로 가동하였고, 그를 통해 종전에는 6시간 걸리던 작업이 30분으로 단축되었다고 하였다. 그와 함께 행정기관 및 공공기관에 대해 행해지는 지능화된 사이버공격 방지와 해킹방어 능력을 향상시키기 위해서 빅데이터 분석기술을 적용한 "범정부 로그분석시스템(nSIMS: National Security and Information Management System)"을 구축하였다고 한다.[242]



※출처: 미래창조과학부 보도자료

[그림 2-5-1] C-TAS

둘째로, 국가 핵심시설에 대해 행해지는 침해사고를 예방하고, 보안인프라를 보강하였다고 한다. 그를 위해 정부는 2013년 209개였던 주요 정보통신기반시설 지정을 292개로 늘렸으며, 2014년 9월부터는 모바일 전자정부 서비스에 프로그램의 개발단계에서부터 소프트웨어의 보안상 취약을 파악하여 사전에 차단하는 "시큐어 코딩(Secure Coding)"기법을 확대 적용한다고 했다.[243] 그뿐 아니라 2014년 6월에는 공무원의 직류에 "정보보호"를 신설하였고, 동년 10월에는 "사이버안전 훈련센터"개소하고 "디도스 대피소"의 방어용량을 40기가에서 100기가로 확대하였으며, 동년 11월에는 민간영역에서 "정보보호 최고책임자 지정·신고제도"를 시행하기도 하였다. 그리고 금융권에 대해서는 2014년 1월 침해하고 대응 전담반을 운영하고, 동년 9월에는 겸직을 금지한 전임 정보보호최고책임자(CISO)를 두도록 하였으며, 2015년에는 금융보안 전담기구를 신설할 것이라고 하였다.[244]

---

242) 2014년 11월 17일 미래창조과학부 보도자료 2면.
243) 2014년 11월 17일 미래창조과학부 보도자료 2~3면.
244) 2014년 11월 17일 미래창조과학부 보도자료 3면.

셋째로, 정보보호 인재를 육성하기 위해 캐리어 패스(Career-Path)체계를 확립하였다고 한다. 그를 위해 중고등학생을 대상으로 하는 "정보보호 영재교육원" 4개를 지정하고, 대덕전자기계고를 마이스터고로 신설하였으며, 정보보호 경력단절을 방지하기 위해서 2014년 2월부터 민·군 연계 프로그램을 추진하였다고 한다. 그리고 BK21 사업에 정보보호 사업을 추가하여 4개 대학을 선정하였고, "고용계약형 정보보호 석사과정"도 8개로 확대하였다고 한다. 그와 함께 차세대 보안리더(BOB:Best-of-Best)과정과 최정예 사이버 보안인력 양성(K-Shield) 과정을 신설하고, 해킹방어대회인 화이트햇 콘테스트나 코드게이트(Codegate)와 같은 행사를 개최하여 숨겨진 정보보호 인재를 발굴하기도 했다고 한다.[245]

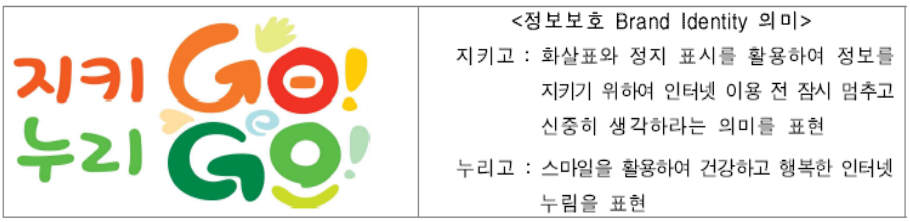
넷째로, 민간 기업이 자율적으로 정보보호를 수행할 수 있도록 하고, 정보보호 분야에 투자를 촉진할 수 있도록 2014년 7월에 "정보보호 투자 활성화 대책"을 수립하였다고 한다. 그에 따르면 정보보호에 투자를 한 경우 조세감면 혜택을 2014년 7%에서 2015년 10%로 확대하고, 연구나 기술자문 투자와 같은 정보보호 서비스에 대한 조세감면도 25%를 적용하며, 중소기업이 정보보호 인력을 신규채용 시 1인당 최대 월90만원까지 보조해 주기로 했다고 한다. 그와 함께 10대 일류 정보보호 제품을 선정하여 추진할 계획이라고도 했다.[246]

※ 출처: 미래창조과학부 보도자료

[그림 2-5-2] 정보보호 투자확대와 산업육성의 선순환 생태계 구축

245) 2014년 11월 17일 미래창조과학부 보도자료 4면.
246) 2014년 11월 17일 미래창조과학부 보도자료 5면.

다섯째로, 국민들의 정보보호에 대한 의식을 고취시키고 자발적인 실천을 위해서 “지키Go! 누리Go!”라는 캠페인을 전개함과 동시에 2014년 7월 “제3회 정보보호의 날”행사를 개최하기도 하였다.[247]



※ 출처: 미래창조과학부 보도자료

[그림 2-5-3] 정보보호 Brand Identity 의미

3) 2015년 K-ICT 시큐리티 발전 전략

2015년 4월 미래창조과학부에서는 정보보호와 창조경제를 위한 새로운 전략을 발표하였다. 그처럼 새로운 전략을 다시금 추진하게 된 이유는 사이버공간의 확대로 인한 경제활동 의존도가 증가하고, 사이버안보가 국민의 생명 및 국가안보와 직결되어 있으며, 사이버보안 전략은 세계적인 추세이자 산업의 경향이 되고 있고, 보안기술 확보와 인력양성이 매우 중요하며, 중·장기를 고려한 정보보호 전략이 필요했기 때문이었다.[248]

따라서 정보보호 패러다임을 크게 전환하여 크게 비전을 “정보보호가 기본이 되는 사회, 창조경제 먹거리 산업화”로 삼고, 5대 목표를 정보보호투자강화, R&D수준향상, 보안인재양성, 침해대응, 정보공유 등으로 설정하였다.[249] 그리고 그를 위한 추진과제로 정보보호 산업 기반강화, 글로벌 원천 보안기술 개발, 최고 보안인재 양성 및 정보보호 실천문화조성, 사이버보안 복원력 제고 등으로 잡았다. 그를 통해서 예상되는 기대효과로는 ICT 산업에서 정보보호 산업의 비중을 2019년까지 현행 5%에서 8%까지 끌어 올릴 수 있으며, 시장규모도 7.6조까지 커질 수 있을 것이라고 하였다. 또한 수출에 있어서도 현행 매출액 대비 수출액이 20%인데 반하여 2019년 까지는

247) 앞의 주.
248) 미래창조과학부, K-ICT 시큐리티 발전 전략, 2015.4, 3~4면.
249) 미래창조과학부, K-ICT 시큐리티 발전 전략, 2015.4, 21면.

30%까지 증가하고, 융합보안 신시장을 창출하여 연평균 성장률도 15%까지 올릴 수 있다고 한다. 그로 인해 일자리도 현행 36,000명 수준에서 2019년에는 1.7배인 55,000명 수준까지 늘어날 것으로 예상하였고, 선진국과의 기술격차도 현행 1.6년에서 2019년에는 0.3년으로 단축될 것이라고 하였다.[250]

※출처: 미래창조과학부 보고서

[그림 2-5-4] 새로운 패러다임의 비젼 및 목표

250) 미래창조과학부, K-ICT 시큐리티 발전 전략, 2015.4, 80면.

나. 국가사이버안전을 위한 대응

1) 사전적 대응방안

사이버안전을 위해서는 기술과 인력확보가 매우 중요하다. 특히 사이버안전을 담보할 수 있는 관련 기술의 연구개발을 위해 노력하여야 하는 것은 선택이 아니라 필수이다. 그래서 국가정보원장은 국가사이버안전을 위한 기술개발 및 기술향상 시책을 추진할 수 있다(제15조 제1항).[251] 또한 중앙행정기관장은 공공분야의 기술 확보를 위해 국가보안기술연구소를 통해 연구를 수행토록 할 수 있다(동조 제2항).[252] 하지만 기술 못지 않게 중요한 것으로 사이버안전을 위한 인력양성이라고 할 수 있는데 그를 위해 관계 중앙행정기관장은 사이버안전 관련 전문기술인력의 확보 및 양성, 사이버안전 교육프로그램의 개발 및 투자, 그 밖에 전문인력 양성, 교육 및 홍보 등에 관하여 필요한 사항 등을 강구하여야 하고(제16조 제1항), 국가정보원장은 관계 중앙행정기관장의 요청이 있는 경우 그를 지원할 수 있다(동조 제2항).

또한 사이버안전의 문제는 사이버공격에 대한 정보를 사전에 파악하는 것이 매우 중요하다. 그에 따라 방지 대책이나 방어 대책 등을 세울 수 있기 때문이다. 그래서 중앙행정기관장, 지방자치단체장 및 공공기관장이 국가 사이버안전을 위협할 수 있는 사이버공격에 대한 관련 정보를 알게 되었다면 국가정보원장에게 지체없이 통보하여야 한다(제10조 제1항). 그러면 국가정보원장은 그에 필요한 대책을 강구하고 그 결과를 해당기관의 장에게 통지하도록 하고 있다(동조 제2항).

사이버안전은 사고 후에는 달성할 수 없기 때문에 늘 만전을 기해야 하지만, 사이버위기 상황이 발생하였을 경우에는 체계적인 대응을 통해서 필해를 최소화 시켜야 한다. 그것이 입증된 것이 이번 메르스 사태라고 할 수 있다. 전염병에 대한 허약한 예방 및 대응체계의 민낯이 가감없이 드러나게 되었기 때문이다. 이는 사이버안전의 경우에도 동일하게 발생할 수 있다. 따라서 중앙행정기관장, 지방자치단체장 및 공공기관장에게 자신이 관리하는 정보통신망에 대해 매년 정기적인 사이버위기 대응 훈련 실시를 의무화 하고 있다(제9조의2 제1항). 더 나아가 국가정보원장은 경우에 따라

---

251) 국가사이버안전관리규정(대통령훈령 제316호, 2013.9.2.) 이하의 설명은 동 규정에 따른다.
252) 연구개발과 관련된 세부사항은 국가정보원장이 정하도록 하고 있다(제15조 제3항).

전체를 대상으로 사이버위기 대응 통합훈련을 실시할 수 있고(동조 제2항), 그 결과에 따라 각 소관 기관장에게 시정조치를 요청하도록 하고 있다(동조 제3항).

그런데 사이버안전을 위해 중요한 것은 사이버공격에 대한 상황을 관련 기관이나 시민들에게 빠르게 전파하고 그에 따른 조치를 취할 수 있도록 대응 준비를 시키는 것이다. 따라서 국가정보원장은 사이버공격에 대한 분석이 후 그 파급영향이나 피해규모 등을 고려하여 관심 · 주의 · 경계 · 심각 등 수준별 경보를 발령하도록 하고 있다(제11조 제1항).[253]

국정원장은 관계 중앙행정기관장에게 경보와 관련된 정보를 요청할 수 있고(동조 제4항), 경보를 발령한 경우 각 관계 중앙행정기관장은 공공기관장 및 지방자치단체장에게 그를 신속히 전파한 뒤 적절한 조치를 취하여야 한다(동조 제2항). 만일 사이버공격이 국가안보에 중대한 위해를 초래할 것으로 판단되는 경우 국가정보원장은 국가안보실장과 협의하여 심각 수준의 경보를 발령할 수 있다(동조 제3항)

2) 사후적 대응방안

사이버공격이 발생한 이후에는 신속히 발생한 피해를 복구하고, 그 원인을 파악하여 이 후의 공격에 대비하는 것이 중요하다. 그러므로 사이버공격이후 중앙행정기관장은 피해를 최소화시킴과 동시에 관련 사실을 국가정보원장에게 통보하여야 한다(제12조 제1항). 또한 공공기관장 및 지방자치단체장의 경우에는 관련 사실을 관계 중앙행정기관장에게 통보하고, 관계 중앙행정기관장은 국가정보원장에게 통보하여야 한다(동조 제2항). 그럴 경우 국가정보원장은 관계 중앙행정기관장에게 사고복구 및 피해의 확산방지를 위한 조치 및 협조를 요청할 수 있다(동조 제3항)

사이버공격 이후 국가정보원장은 그 원인 분석을 위한 조사를 실시할 수 있는데, 경미한 경우에는 해당 기관장으로 하여금 조사하여 통보토록 하고 있다(제13조 제1항). 만일 조사결과 범죄혐의가 발견되면 국가정보원장은 해당 기관장과 협의하여 수사기관장에게 관련 내용을 통보할 수 있다(동조 제2항). 그런데 만일 사이버공격으로 인한 피해가 심각한 수준에 이른 경우 국가정보원장은 관계 중앙행정기관장과 협의 후 '사이버위기 대책본부'를 구성 및 운영할 수 있으며(동조 제3항), 구체적인

253) 그러나 민간분야는 미래창조과학부장관이 국가정보원장과의 관련 정보교환 후 경보를 발령하도록 하고 있다(제11조 제1항 단서).

대응을 위해 그 아래 합동조사팀 등 하부기구를 둘 수 있다(동조 제4항). 그리고 그에 필요한 인력, 장비 및 관련 자료 등을 요청할 수 있다(동조 제5항).

※ 출처: 국가사이버안전센터 홈페이지

[그림 2-5-5] 국정원의 사이버공격 수준별 경보

2. 사이버안전 정책

가. 사이버안전 대응체계

한국의 경우 인터넷의 하드웨어적인 인프라가 과히 세계 제일이라고 할 수 있다. 이미 2000년 초반에 초고속인터넷이 각 가정까지 연결되었고, SK나 KT, LG 등의 지속적인 투자로 인해 인터넷 접속속도는 세계의 최고 수준을 유지하고 있다.[254] 하지만 그에 비해 사이버보안에 대한 수준은 상대적으로 낙후되어 있기 때문에 해커들의 공격과 공격을 위한 경유지의 역할을 한다는 비판도 받고 있다.[255] 무엇보다 한국은 북한이라는 적이 사이버공간을 통한 공격을 수시로 하고 있는 특수한 환경에 처해 있다. 그러므로 한국의 사이버공격에 대한 대응체계는 단순히 사이버범죄를 방지하기 위한 수준에 머물러서는 안 되며 국가안보를 지켜낼 높은 수준을 유지해야 한다. 따라서 한국은 이제까지 사이버공간의 위기에 대해 대응하기 위한 다양한 정책들을 마련해 왔다.

한국의 사이버위기의 대응체계의 정점에는 '국가사이버안전센터(NCSC: National Cyber Security Center)'가 있다고 할 수 있다. 그러므로 사이버안전과 관련된 정책이나 예방활동, 탐지활동 및 사후 조사 및 복구지원 등의 활동은 NCSC를 중심으로 이루어지게 되는 것이다. 그를 바탕으로 미래창조과학부나 행정자치부, 국방부 등과 같은 유관 부처들과 한국인터넷진흥원, 방송통신위원회, 검찰청, 경찰청 등 유관 기관들이 유기적인 협력과정을 통해 사이버위기에 효과적으로 대응할 수 있게 된다. 그를 뒷받침 해줄 정책이나 법령도 매우 중요하다고 할 수 있다. 특히 법령을 통해 담당기관에게 예산이나 인력을 제공해 주고, 권한을 설정해 주어 사이버위기에 적극적이고 실효적으로 대응할 수 있도록 근거를 마련해 주어야 한다.

그러나 최근 발생하는 사이버공격에 대해서 NCSC가 적절한 역할을 수행하지 못한

---

254) 인터넷 시장조사업체인 Akamai가 2015년 134개국을 대상으로 조사하여 발표한 인터넷 평균 속도에서 한국은 평균 속도가 23.5Mbps로 세계 평균 속도인 5.0Mbps의 네 배 이상을 나타내며 1위를 차지하였다; 〈http://www.akamai.co.kr/html/about/press/releases/2015/press-062415.html〉, 2015.10.31. 방문.

255) 한국경제, '해커 먹잇감' '액티브X' 천지 … 한국은 인터넷 보안 후진국, (2014.6.6.), 〈http://www.hankyung.com/news/app/newsview.php?aid=2014060620471〉, 2015.10.31. 방문.

다는 지적과 함께 실질적 컨트롤 타워가 부족하다는 지적이 계속되어 왔다. 그로인해 청와대가 컨트롤 타워 역할을 수행해야 한다는 요구들이 계속되어 왔고, 그러한 요구들에 따라 최근 사이버위기에 대해 청와대가 컨트롤 타워 역할을 수행하는 체계로 바뀌게 되었다.

국가사이버안전관리체계는 크게 국가사이버안전전략회의와 국가사이버안전대책회의, 그리고 국가사이버안전실무회의로 구성된다. 다만 모든 국가사이버안전 업무를 국가정보원이 모두 수행하는 것은 아니다. 국가정보원은 국가사이버안전센터를 통해 국가차원의 총괄적이고 체계적인 업무와 함께 국가 및 공공분야의 사이버안전 업무담당하게 된다. 따라서 민간부문의 사이버안전 업무는 미래창조과학부가 담당하게 되는데, 사실상 그 산하의 한국인터넷진흥원에서 관련 업무를 수행하게 되고, 국방분야의 사이버안전 업무는 국방부의 사이버사령부(국방사이버지휘통제센터)를 통해 수행된다.[256]

※ 출처: 한국인터넷진흥원

[그림 2-5-6] 국가사이버안전관리체계

256) 강석구/이원상, 사이버범죄 관련 법령정비 방안, 한국형사정책연구원, 2013, 155면.

그러나 이처럼 형식상으로는 국가정보원이 컨트롤타워 역할을 하는 것처럼 보이지만 사실 실질적인 컨트롤타워는 존재하는지에 대해서는 여전히 의구심이 들었다. 그 이유는 먼저 사이버공격에 대한 조사의 과정이 매끄럽지 못했기 때문이다. 예를 들어, 지난 3.20 사이버공격의 경우를 살펴보면, 사이버공격초기 민·관·군 합동조사단은 언론을 통해 사이버공격의 근원지에 대해 우왕좌왕하는 모습을 그대로 보여주기도 하였다. 유관 기관들이 조사 과정에서 서로 다른 견해들을 보이기도 하며, 통일되지 못한 자료들을 내어 놓기도 하였다. 결국 최종적으로는 북한의 소행이라는 것이 밝혀지긴 하였지만,[257] 조사 초기 허둥대는 모습은 국민의 신뢰감을 반감시키기 충분하였고, 그 결과 최종 결과에도 불구하고 의혹이 충분히 해소되지 못하는 문제점이 나타나게 되었다.[258]

또한 3.20 사이버공격에서도 마찬가지 이지만 사이버공격이 있는 경우 대개 국가정보원이 주도하여 민·관·군 합동조사단이 조직된다. 이는 앞서 살펴본 훈령에서 잘 나타나고 있는데, 사이버공격으로 인한 피해가 심각한 수준에 이른 경우 국가정보원장은 관계 중앙행정기관장과 협의 후 '사이버위기 대책본부'를 구성 및 운영할 수 있으며(제13조 제3항), 구체적인 대응을 위해 그 아래 합동조사팀 등 하부기구를 둘 수 있기 때문이다. 하지만 3.20 사이버공격의 경우는 주로 민간부문의 공격이었으므로 정통망법 제48조의4에 규정되어 있는 민·관 합동조사팀이 조사를 했어야 한다는 비판도 제기되고 있다.[259] 이제까지 수차례 민간에 대한 사이버공격이 있었지만, 한번도 미래창조과학부 주관의 민·관 합동조사팀이 조사를 한 적은 없으며, 모두 국가정보원주도의 민·관·군 합동조사단에 의해 조사가 이루어졌다. 이는 현행 법규가 국가사이버위기에 대한 적절한 통합적 규정을 하지 못하고 있기 때문인데, 민·관·군 합동조사단에 대한 규정은 대통령 훈령으로 규정되어 있고, 민·관 합동조사단에 대한 규정은 정통망법에 있으며, 사이버전에 대한 사항은 국군사이버사령부령에 매우 추상적으로 규정되어 있는 상황이다.

---

257) The Verge, 'South Korea blames North Korea for last month's major cyber-attack', (2013.4.10.), 〈http://www.theverge.com/2013/4/10/4207980/south-korea-says-north-is-responsible-for-march-hack?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+google%2FDTsn+(ICT)〉, 2015.10.31. 방문.
258) 강석구/이원상, 앞의 글, 156면.
259) 강석구/이원상, 앞의 글, 157면.

이제 청와대가 사이버안보에 대한 실질적인 컨트롤 타워를 할 것을 선언하고 직제를 개편해서 비서실장을 추가하였다. 그러나 실제적인 업무는 지금과 같이 주로 국가정보원의 주도하에 수행될 것이다. 이번 메르스 사태를 겪으면서 사이버위기의 경우에도 국가의 대응체계도 적절하게 작동하지 못할 것이 매우 염려되는 상황이다. 그러므로 청와대가 형식적으로는 컨트롤 타워의 모양새를 갖추었지만, 실질적으로도 컨트롤 타워가 될 수 있도록 인적, 물적, 제도적 보완이 필요하다고 사료된다.

나. 사이버안전 주요 기관

1) NCSC

앞서 언급한 바와 같이 한국의 사이버안보 정점에는 실질적으로 국가정보원이 있다. 그리고 관련 지침 하에서 사이버안전에 대해 체계적인 예방 및 방지대책, 조사 등의 업무를 수행하는 기관으로 국가사이버안전센터(이하 '안전센터'라고 함)가 있다. 안전센터는 2003년 1월 25일 있었던 슬래머 웜으로 인한 대규모 피해를 경험한 이후 국가차원의 종합적·체계적인 대응전략을 수립·총괄하기 위해 2004년 2월 20일에 설립되었다.[260] 안전센터의 주요업무를 보면 크게 국가사이버안전 정책 총괄, 사이버위기 예방활동, 사이버공격 탐지활동, 사고조사 및 복구지원 활동 등을 수행하고 있다.

국가사이버안전 정책과 관련해서는 국가사이버안전정책을 기획하고, 유관 기관들과 관련 사항을 조율하며, 민관군이 사이버안전과 관련된 정보를 공유할 수 있도록 노력하고 있다. 그리고 사이버위기가 발생하기 이전에 차단하기 위해서 예방활동에 힘을 쓰고 있는데, 각급 기관의 정보보안 관리 실태를 살펴보기도 하고, 사이버위기 대응 훈련을 수행하기도 한다. 대표적으로 사이버안전 여부를 점검할 수 있는 소프트웨어를 보급하여 매월 자신의 컴퓨터의 보안실태를 점검하도록 하고 있기도 하다. 또한 사이버안전을 위해서는 탐지활동이 필요한데, 그를 위해 24시간 365일 각급 기관에 대한 보안관제를 하기도 하며, 사이버위기가 발생하는 경우 그에 해당하는 경보를 발령하기도 한다. 또한 새로운 해킹에 의한 공격을 탐지하기 위한 기술을 개발하기도 한다. 마지막으로 사이버공격이 발생한 경우에는 민관군 합동조사단을

260) 국가사이버안전센터 소개, 〈http://service1.nis.go.kr/intro/business.jsp〉, 2015.10.31. 방문.

운영하여 사고조사 및 원인규명을 하고, 국내 유관기관 및 해외 유관 기관들과 협력하여 신속히 사고에서 회복될 수 있도록 노력을 기울이고 있기도 하다.

[그림 2-5-7] 국가사이버안전센터 주요업무

2) 사이버 안보비서관실

사이버안보에 대한 컨트롤 타워의 부재 문제가 부각되고, 모든 부처를 총괄하는 것을 국가정보원이 수행하는 것 보다는 청와대가 수행해야 한다는 주장이 거세지게 되었다. 따라서 청와대는 국가안보실에 '사이버 안보비서관실'이 신설되었다. 그 전단계로 2015년 1월23일 안보 특보를 임명하여 사이버안보와 관련된 사안들에 대해 청와대가 전문적으로 접근할 수 있는 기반을 마련하기도 하였다.[261] 이처럼 사이버 안보비서관실을 신설한 가장 큰 이유는 청와대가 사이버영토를 수호해야 할 필요성을 인식했기 때문이며, 최근 소리 없이 벌어지고 있는 사이버 공간에서의 분쟁에 대해 보다 적극적으로 대처하기 위한 단호한 결단이 표출된 것이라고 할 수 있다.[262]

사이버 안보비서관실 신설을 위해 '국가안보실 직제 일부개정령안'이 상정되어 개정되었다.[263] 그에 따르면 "제4조 제3항,[264] 제5조 제1항 및 제2항[265] 중 "정보융합비

261) http://news.mk.co.kr/newsRead.php?year=2015&no=302422, 2015.10.31. 방문.
262) http://news.inews24.com/php/news_view.php?g_serial=890616&g_menu=020200, 2015.10.31. 방문.

서관"을 각각 "정보융합비서관·사이버안보비서관"으로 한다."되어 있다. 그에 따라 국가안보실 비서관은 정책조정비서관(국가안전보장회의 사무차장을 겸함), 안보전략비서관, 정보융합비서관, 위기관리센터장 그리고 사이버안보비서관으로 5명이 되었다. 특히 사이버안보비서관실에는 위기관리센터장 산하의 사이버위기대응팀이 흡수되어 사이버안보에 전문성을 갖춘 실무진으로 구성된 것으로 알려져 있다.[266]

다. 민간부문의 사이버안전 대응체계

사이버위기의 문제는 비단 한 분야나 부문에만 국한되지는 않는다. 따라서 국가의 사이버위기가 발생하게 되면 모든 부처와 공공기관, 단체, 기업 등이 함께 대응할 필요가 있다. 그러나 국가적인 위기와는 다소 거리가 있고, 사이버공격이 민간부문을 중심으로 이루어지게 되는 경우에는 미래창조과학부가 담당을 하도록 되어있다. 그러나 사이버공격이 국가사이버위기와 관련이 있다고 판단하게 되면 다시금 국가정보원이 담당을 하게 된다.

민간부문에서는 한국인터넷진흥원에 의해서 많은 부분이 수행되고 있다. 정보통신망법 제52조에 따르면 "정부는 정보통신망의 고도화와 안전한 이용 촉진 및 방송통신과 관련한 국제협력·국외진출 지원을 효율적으로 추진하기 위하여 한국인터넷진흥원을 설립"하도록 하고 있다(제1항). 그리고 인터넷진흥원은 "① 정보통신망의 이용 및 보호, 방송통신과 관련한 국제협력·국외진출 등을 위한 법·정책 및 제도의 조사·연구, ② 정보통신망의 이용 및 보호와 관련한 통계의 조사·분석, ③ 정보통신망의 이용에 따른 역기능 분석 및 대책 연구, ④ 정보통신망의 이용 및 보호를 위한 홍보 및 교육·훈련, ⑤ 정보통신망의 정보보호 및 인터넷주소자원 관련 기술 개발 및 표준화, ⑥ 정보

263) http://www.law.go.kr/lsInfoP.do?lsiSeq=170042&lsId=&efYd=20150403&chrClsCd=010202&urlMode=lsEfInfoR&viewCls=lsRvsDocInfoR#0000, 2015.10.31. 방문.

264) 제4조(차장) ③ 제1차장은 정책조정비서관·안보전략비서관·정보융합비서관·사이버안보비서관 및 위기관리센터의 소관 업무에 관하여 국가안보실장을 보좌하고, 제2차장은 외교·국방 및 통일 업무 중 국가안보에 관하여 국가안보실장을 보좌한다.

265) 제5조(비서관 등) ① 제1차장 밑에 정책조정비서관·안보전략비서관·정보융합비서관·사이버안보비서관 및 위기관리센터장 각 1명을 둔다. ② 정책조정비서관·안보전략비서관·정보융합비서관·사이버안보비서관 및 위기관리센터장은 고위공무원단에 속하는 일반직 또는 별정직 공무원으로 보한다.

266) http://news.inews24.com/php/news_view.php?g_serial=890616&g_menu=020200, 2015.10.31. 방문; 다만, 조직에 대한 구체적인 자료는 확보할 수 없었다.

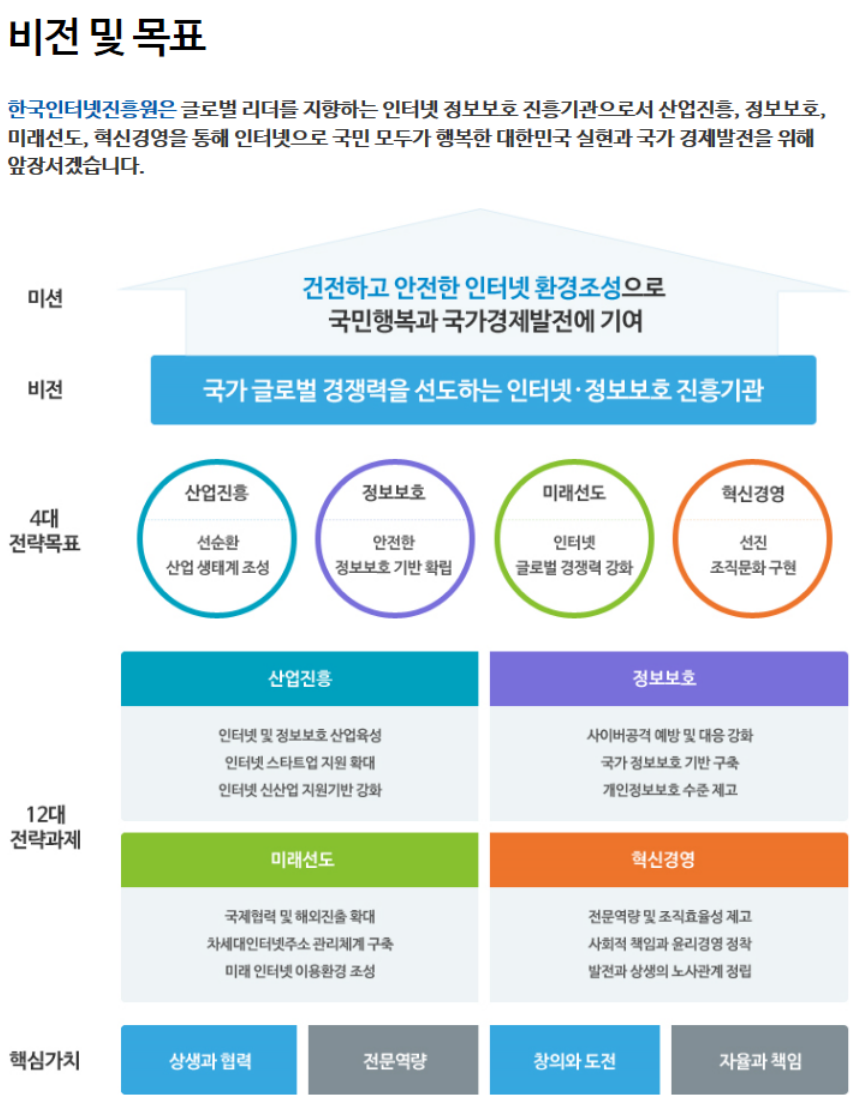
보호산업 정책 지원 및 관련 기술 개발과 인력양성, ⑦ 정보보호 관리체계의 인증, 정보보호시스템 평가·인증 등 정보보호 인증·평가 등의 실시 및 지원, ⑧ 개인정보보호를 위한 대책의 연구 및 보호기술의 개발·보급 지원, ⑨ 분쟁조정위원회의 운영 지원과 개인정보침해 신고센터의 운영, ⑩ 광고성 정보 전송 및 인터넷광고와 관련한 고충의 상담·처리, ⑪ 정보통신망 침해사고의 처리·원인분석 및 대응체계 운영, ⑫ 「전자서명법」 제25조제1항에 따른 전자서명인증관리, ⑬ 인터넷의 효율적 운영과 이용활성화를 위한 지원, ⑭ 인터넷 이용자의 저장 정보 보호 지원, ⑮ 인터넷 관련 서비스정책 지원, ⑯ 인터넷상에서의 이용자 보호 및 건전 정보 유통 확산 지원, ⑰ 「인터넷주소자원에 관한 법률」에 따른 인터넷주소자원의 관리에 관한 업무, ⑱ 「인터넷주소자원에 관한 법률」 제16조에 따른 인터넷주소분쟁조정위원회의 운영 지원, ⑲ 「정보보호산업의 진흥에 관한 법률」 제25조제7항에 따른 조정위원회의 운영지원, ⑳ 방송통신과 관련한 국제협력·국외진출 및 국외홍보 지원, ㉑ 제1호부터 제20호까지의 사업에 부수되는 사업, ㉒ 그 밖에 이 법 또는 다른 법령에 따라 인터넷진흥원의 업무로 정하거나 위탁한 사업이나 미래창조과학부장관·행정자치부장관·방송통신위원회 또는 다른 행정기관의 장으로부터 위탁받은 사업"으로 되어 있다(동조 제3항).

한국정보화진흥원의 연혁을 살펴보면,[267] 2009년 7월 한국정보보호진흥원(KISA)와 한국인터넷진흥원(NIDA), 정보통신국제협력진흥원(KIICA)가 통합되어 한국인터넷진흥원(KISA)이 창립되었다. 이후 같은 해 8월 주민등록번호클린세터가 개소하였고, 11월에는 개인정보 노출대응 상황실이 개소하였다. 2010년 1월에는 118 상담센터가 개소하였고, 동년 12월에는 인터넷침해대응센터 종합상황관제실이 개소하였다. 2011년 5월에는 한국도메인 서비스를 개시하였으며, 동년 10에는 개인정보보호 기술지원센터가 개소하였다. 2013년 1월에는 피싱대응센터가 개소하였고, 같은 해 6월에는 인터넷윤리체험관이 개소하였다. 그리고 2014년 1월에는 ICANN(국제인터넷주소관리기구) 서울사무소가 개소하였고, 5월에는 IoT 혁신센터가, 7월에는 인천정보보호지원센터가 개소하여 지금의 조직에 이르고 있다.

---

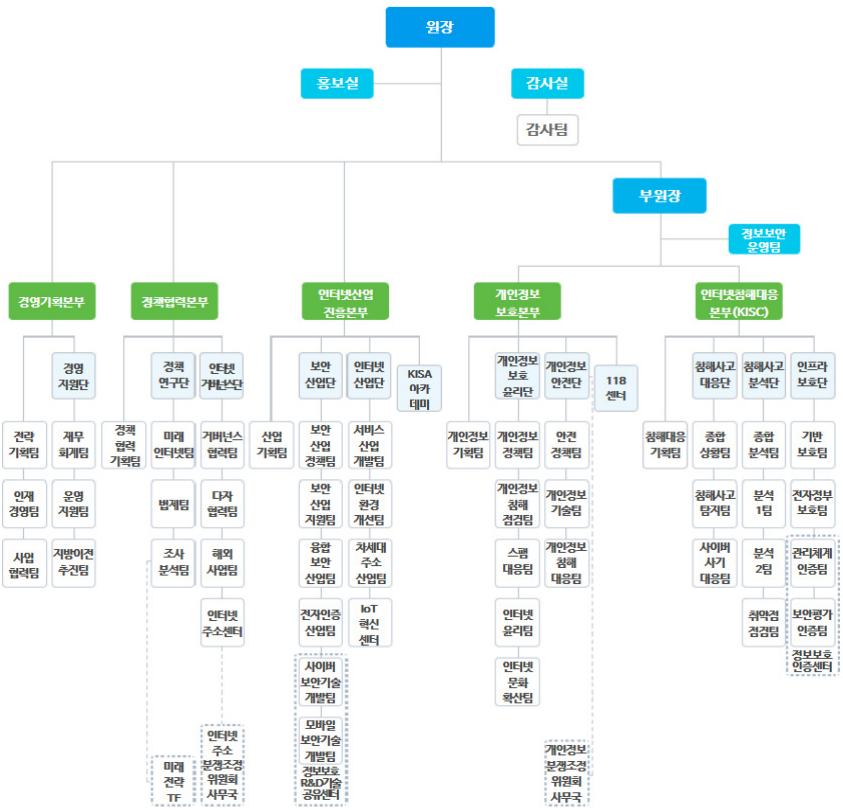
267) http://www.kisa.or.kr/intro/history.jsp, 2015.10.31. 방문.

한국인터넷진흥원이 제시하고 있는 비전을 보면 다음과 같다.



[그림 2-5-8] 한국인터넷진흥원 제시 비전

그리고 현재 한국인터넷진흥원의 조직체계는 다음과 같다.



※ 출처: 한국인터넷진흥원 홈페이지

[그림 2-5-9] KISA 조직도

민간부문에서의 사이버조사는 민·관 합동조사단에 의해서 이루어진다. 민·관 합동조사단의 경우 그 설치 목적은 "정보통신망 침해사고가 발생할 시 피해확산 방지, 사고대응, 복구 및 재발방지를 위하여 정보보호의 전문가들이 그 원인을 조사"하는 것이다.[268] 그런데 민·관 합동조사단이 그 설치목적에 따라 제대로 운영되고 있는지는 일단 의문이다. 그 이유는 민·관 합동조사단이 가지고 있는 구조적인 문제 때문이라고 할 수 있다.

268) 강석구/이원상, 앞의 글, 159면.

먼저 앞서 살펴본 바와 같이 “국가사이버안전관리규정” 제11조에서는 민간분야의 경보발령은 미래창조과학부장관이 경보를 발령하되 국가차원의 효율적인 경보 업무수행을 위해 발령 전에 국가정보원장과 관련정보를 상호 교환하도록 하고 있다(제1항). 만일 경보상황이 경계 단계에 이르게 된다면 그 때 부터는 정보통신망법이 적용되고, 정보통신망법 제48조의 4에서는 민·관 합동조사단에 대한 법적근거가 규정되어 있다. 그에 따라 미래창조과학부 장관은 정보통신망에 중대한 침해사고가 발생하면 ‘피해 확산 방지, 사고대응, 복구 및 재발 방지’를 위하여 민관합동조사단을 구성하여 조사활동을 진행할 수 있다(동조 제2항). 그리고 민·관 합동조사단에 대한 제반규정은 “민·관 합동조사단 구성 및 운영에 관한 규정”에 두고 있다. 그에 따라 한국인터넷진흥원에서는 전문가 풀(Pool)을 구성하여 전문가그룹을 관리하고 있다. 해당 내용은 규정 제6조와 제7조에 있는데, 전문가 풀은 ‘사이버보안전문단’이라는 명칭으로 관리된다. 사이버보안전문단의 구성원은 ① 정보보호 관련 분야 5년 이상의 실무 경험이 있는 자, ② 국내·외 해킹방어대회 입상자, ③ 정부의 정보보호전문가양성 프로그램 수료자, ④ 그 밖의 정보통신망 침해사고와 관련한 기술적, 관리적, 물리적 조치사항에 대한 전문지식 있는 자 등의 자격요건을 요구하며(제6조 제1항), 임기는 2년이다(동조 제2항). 사이버보안전문단은 평상시에는 ① 정보보호 관련 기술세미나 및 워크숍 활동, ② 사이버침해 위협 동향 및 신규 위협 연구 활동, ③ 정보보호 인식제고를 위한 홍보 및 캠페인 활동, 그리고 ④ 그 밖에 정보보호와 관련하여 필요한 활동을 수행하다가 미래창조과학부 장관이 조사단을 구성하여 소집하면 민·관합동 조사단으로 활동하게 된다.

조사단은 사이버보안전문단원 중 20명 내외로 지명되며(제8조 제2항), 단장은 미래창조과학부 정보보호 관련 공무원 또는 한국인터넷진흥원 인터넷침해대응센터의 보직자 중에서 임명된다(동조 제1항). 조사단은 원인조사반과 검증분석반 등으로 구성되며(제9조 제1항), 조사단의 기능은 ① 원인조사반은 중대한 침해사고 발생 시 관계인의 사업장에 출입하여 침해사고 원인 조사, ② 검증분석반은 침해사고의 원인 분석 및 대책 등 조사결과 보고서를 작성하여 운영위원회에 상정, 그리고 ③ 그 밖에 해당 피해사고와 관련하여 조사단장이 지시하는 사항 등이다(제11조 제1항). 조사단은 조사활동이 끝나면 미래창조과학부장관에게 최종결과보고서를 제출하고 그 활동을 종료한다(제17조).

라. 국방부문의 사이버안전 대응체계

앞서 살펴본 바와 같이 한국의 사이버안보와 관련해서 국방과 관련된 부분은 국방부가 담당하고 있으며, 주로 사이버사령부가 주업무기관이라고 할 수 있을 것이다. 국방 분야에서의 사이버안보가 중요하다는 것은 이미 주요 선진국들의 정책에서도 잘 나타나고 있다. 특히 미국과 중국이 매우 적극적이라고 할 수 있는데, 미국은 사이버전쟁에 대응하기 위해 민간 IT전문가들로 구성된 총 40개 팀의 '사이버 공격부대'를 신설하기로 하였으며, 13개 팀은 국가 방어팀 그리고 27개 팀은 사이버공격 지원업무를 수행할 예정이라고 하였다.[269] 또한 중국은 이미 2010년 7월에 인민해방군 총참모부 직속으로 사이버 사령부 산하에 사이버전을 수행하기 위한 '61398'를 창설하여 미국과 대립하고 있으며, 이스라엘도 국방부 직속 정보부대은 '8200'부대를 운영하고 있으며, 영국도 2012년 12월에 외인부대 성격의 '사이버 예비군'을 창설하였다.[270] 한국 사이버 사령부의 인력은 2013년 당시 400명 수준이었으며, 향후 1,000명 이상으로 확대할 계획이라고 하였다.[271] 다만, 사이버부대와 관련된 사안들은 비밀인 것이 많기 때문에 정확한 사항을 알 수는 없지만 최근 언론에 이해 보도된 내용에 따르면 한국의 사이버사령부는 500명의 병력을 보유하고 있으며, 화이트 해커 1,000명을 양성할 계획으로 알려져 있고, 북한은 6,000여명의 정보전사를 가지고 있으며, 중국은 30만명의 화이트 해커와 18만명의 사이버 부대가 있는 것으로 추정되고, 미국은 매년 50억 달러를 투입해 사이버 전쟁 훈련을 수행하며 사이버사령부에 8만명, 6,000명의 전문요원을 보유하고 있는 것으로 나타났고, 일본도 사이버 방위대 예산으로 약2000억원을 지출하고 있는 것으로 나타났다.[272]

---

269) Internet&Security Weekly, 한국인터넷진흥원, 2013년 3월 4주, 21면.
270) 위와 동일.
271) Internet&Security Weekly, 22면.
272) http://news.chosun.com/site/data/html_dir/2015/07/24/2015072400370.html, 2015. 10.31. 방문.

세계 주요 사이버戰 사례

시기	내용
2015년	중국, 미국 인사관리처 해킹해 연방공무원 2150만명 신상 정보 유출
2014년	러시아, 미국 백악관 전산망 침입해 오바마 대통령 일정 정보 등에 접근
2014년	북한, 소니픽처스 엔터테인먼트 사이트 공격·정보 유출 미국, 노동신문 등 주요 웹사이트 마비시키는 보복 조치
2013년	북한, 한국 방송사·금융기관 등 주요 사이트 사이버 테러(3.20, 6.25 공격)
2012년	이란, 미국 금융회사와 이스라엘 정부 사이버 공격
2011년	북한, 한국군·이통사 통신 장비 교란 및 NH농협 전산망 마비
2010년	미국·이스라엘, 악성 코드 이용해 이란 핵 시설 파괴
2007년	러시아, 에스토니아 전체 인터넷 2주간 마비

※ 출처: 조선일보

[그림 2-5-10] 주요국의 사이버부대 상황

그런데 문제는 최근 선거와 관련해서 사이버 사령부가 개입한 사실이 나타나면서 사이버 사령부의 지위에 문제점이 발생하게 되었다. 사이버 사령부가 정치에 개입한 사건이 발생하였고, 그에 대한 관련자들에 대한 유죄가 선고되면서[273] 사이버 사령부에 대한 지위가 흔들리고 있기 때문이다. 북한은 군 전체 예산의 10~20%를 사이버전에 투입하며, 사이버전을 준비하고 있는데 비해[274] 한국 사이버사령부는 국가정보원에의해 예산배정을 받으며,[275] 정치적인 문제에 발목이 잡혀 상시적으로 모니터링을 받아야 하는 처지에 있다.[276] 더욱이 군사정보활동 등 특수활동비의 경우 2011년에는

273) http://www.hankookilbo.com/v/53779e5994c745faba60cfc80bbba552, 2015.10.31. 방문.
274) http://www.newsis.com/ar_detail/view.html?ar_id=NISX20150529_0013694598&cID=10102&pID=10100, 2015.10.31. 방문.
275) http://the300.mt.co.kr/newsView.html?no=2014111010327624725, 2015.10.31. 방문.

30억이었고, 2012년 42억, 2013년 55억, 2014년 60억으로 지속적으로 증가하던 예산도 2015년에는 41억으로 축소한 상황이다.[277]

그러나 국방을 위한 사이버안보는 아무리 강조해도 지나치지 않다. 따라서 국방분야에서의 사이버안보에 대해 살펴보기 위해서 우선 관련 법령체계를 살펴보고, 상세히는 알 수 없지만 그 조직체계에 대해 살펴보며, 사이버안보를 위한 국방 전략 등에 대해 살펴보고자 한다.

사이버사령부와 관련된 대표적인 법령으로는 대통령령 제26101호인 '국군사이버사령부령'이 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 ① 국방 사이버전의 기획 및 계획 수립, ② 국방 사이버전의 시행, ③ 국방 사이버전 전문인력의 육성과 기술 개발, ④ 국방 사이버전을 대비한 부대 훈련, ⑤ 국방 사이버전 유관기관 사이의 정보 공유 및 협조체계 구축, 그리고 ⑥ 그밖에 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 국방부장관이 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·감독해야 하기 때문이다(제7조).

국군사이버사령부는 필요한 참모 부서를 두며, 국군사이버사령부 예하에 기능별

276) http://www.segye.com/content/html/2015/03/24/20150324004928.html?OutUrl=naver, 2015.10.31. 방문.

277) http://www.asiae.co.kr/news/view.htm?idxno=2014110907201462079, 2015.10.31. 방문.

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

국방부의 사이버전 관련 조직에 대한 정확한 정보는 그리 많지 않다. 다만, 일부 문헌이나 언론을 통해 공개된 것에 따르면 사이버전과 관련해서는 사이버사령부가 주요 업무를 수행하고, 국방부는 전체적인 총괄 지휘를 하며, 원활한 지휘를 위해 합동참모본부에 사이버방어과를 설치할 계획이라고 한다.[278] 하지만 국방부의 전체적인 사이버전 대응 체계를 보면 사이버방호정책팀(국방정보보호 정책 및 기획, 계획 담당), 사이버사령부(사이버전과 관련된 기획이나 계획, 시행, 부대훈련 등을 담당), 국군기무사령부의 정보보호부대(국방정보 통신체계 보호를 위한 예방활동과 교육 등을 담당), 국방부조사본부의 사이버수사팀, 그리고 각 군 정보보호 부서 및 CERT팀 등이 체계적인 형태로 구축되어 있다.[279]

※ 출처: 엄정호, 앞의 논문, 179면

[그림 2-5-11] 사이버사령부 조직체계

사이버사령부는 31센터(연구개발 담당), 510단(사이버전 담당), 530단(대북 심리전 담당) 그리고 590단(교육훈련 담당)으로 구성되어 있다. 처음에는 200여 명으로 출발하였으며 2013년에는 453명이며, 앞으로 1000명으로 증원할 것이라고 한다. 특히 지난 대선에서 문제가 되었던 대북 심리전을 담당하고 있는 530단은 기획·정보·작

278) 엄정호, "사이버전 전력 강화를 위한 사이버 전문인력 인증평가 모델", 보안공학연구논문지, 제11권 제2호, 2014, 179면.
279) 앞의 주.

전·미디어·해외홍보 등 5개 팀으로 구성되어 있으며, 2013년 당시 전체 453명 가운데 200여 명이 530단에 속해 있었다고 한다.[280]

그러나 독립부대로 편제된 이후에도 독립건물이 없어서 기무사령부, 777부대 등으로 전전하고, 국방부 내 빈사무실 및 경기도 일대 31곳에 나누어져 근무를 하다가 2014년에 전자기폭탄(EMP) 방어능력을 갖춘 지휘센터를 건립하게 되었다.[281]

3. 사이버범죄 정책

가. 개관

사이버안보에 있어서 사이버전과 사이버테러가 주로 대외에서 국내 사이버영토를 공격하는 행위라고 한다면 주로 국내에서 발생하는 사이버영토 위협행위는 사이버범죄에 속한다고 할 수 있다. 그래서 현재 사이버안전국으로 승격한 이전의 사이버테러대응센터는 사이버범죄를 사이버테러형범죄와 일반사이버범죄로 구분하고, 전자에는 해킹이나 악성코드 유포 등의 행위를 포함시켰고, 그 외에 기존의 범죄가 디지털화된 경우는 후자에 포함시키기도 하였다. 그와 같은 분류가 적절하였는지는 차치하고 전자는 전형적으로 사이버공간과 함께 태생한 범죄유형이라고 할 수 있으며, 후자는 기존의 범죄가 사이버공간에 적응한 형태라고 할 수 있을 것이다. 따라서 두 유형에 대한 대응방법은 다소 다르게 접근할 필요가 있을 것이다.

먼저 전자는 좀 더 포괄적으로 표현해서 사이버공격과 관련된 행위라고 할 수 있을 것이다. 사이버공격은 크게 사이버전을 위한 공격, 사이버테러를 위한 공격[282], 사이버범죄를 위한 공격으로 나누어 볼 수 있을 것이다. 사이버전과 사이버테러의 경우 사실상 범죄의 영역에서 다루기는 쉽지 않다. 물론 일부 사이버테러는 사이버범죄 영역에서 다루어 질 수 있을 것이다. 그러므로 사이버범죄에서 다룰 수 있는 사이버공격은 개인의 이익을 위한 사이버공격이라고 할 수 있다.[283]

---

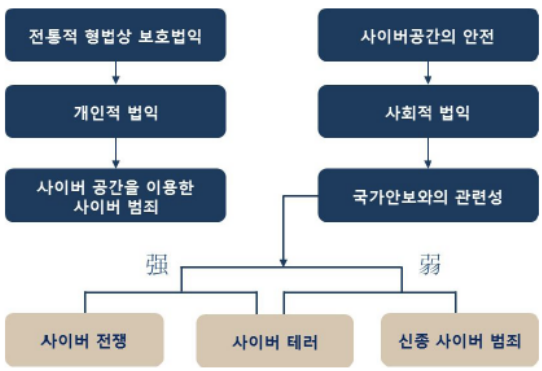
280) http://www.sisainlive.com/news/articleView.html?idxno=18596, 2015.10.31. 방문.
281) http://www.asiae.co.kr/news/view.htm?idxno=2014110907201462079, 2015.10.31. 방문.
282) 사이버 테러는 "정부나 시민을 위협하려는 목적으로 사이버 툴(tool)을 이용해 에너지, 수송, 공공시설 등의 주요 국가 기반시설을 중지시키려고 하는 행위"라고 정의되기도 한다; 윤해성, 사이버 테러의 동향과 대응 방안에 관한 연구, 한국형사정책연구원 연구총서, 2012, 38면.
283) 강석구/이원상, 사이버범죄 관련 법령정비 방안연구, 한국형사정책연구원, 2013, 26면 이하.

〈표 2-5-1〉 사이버공격의 분류

해결방법	정치·군사적 해결	정치·군사적 해결 / 형사사법적 해결	형사사법적 해결
관련영역	사이버 전쟁	사이버 테러	사이버범죄로서의 해킹
예시	미국과 중국간의 사이버 전쟁	알카에다의 사이버 공격/ 어나너머스의 공격	어나너머스의 공격/ 일반적인 사이버공격

※ 출처: 강석구/이원상, 29면

이를 다시금 보호법익을 기준으로 하여 전통적 형법의 보호법익 가운데 그 침해수단이 컴퓨터나 인터넷을 수단으로 하는 경우는 사이버범죄로 보아 한 축을 이루고(엄밀히 말하면 이는 '사이버화 범죄'라고 할 수 있다), 사이버공간의 안전이라는 사회적 법익을 침해하는 행위 가운데 국가안보와의 관련성을 고려하여 그것이 강하면 사이버전쟁, 그 다음이면 사이버테러, 그리고 그것이 약할 경우 신종 사이버범죄로 구분하는 견해도 있다(이것이 '사이버범죄'라고 할 것이다).[284] 그에 따라 범죄와 연결되어 있지 않은 경우는 '사이버사고'로 규정하여 안전한 시스템 구축을 통해 해결하고, 사이버전쟁은 국제법적 조치로, 사이버가 지원된 범죄는 일반범죄와 같은 처분을, 신종 사이버범죄 및 테러는 새로운 국가적 대응전략이 필요하다고도 한다.[285]



※ 출처: 강수진, 앞의 글, 106면

[그림 2-5-12] 보호법익을 기준으로 한 유형화

284) 강수진, 국가 사이버범죄 대응전략 설계, 경찰청, 2013, 106면.
285) 강수진, 앞의 글, 107면.

사이버범죄와 관련된 통계를 제공하고 있는 나라는 거의 없다. 물론 경우에 따라 단편적인 통계를 제공하고 있지만, 한국 경찰청에서처럼 사이버범죄에 대해 별도로 정보를 제공해 주는 국가를 찾기는 쉽지 않다. 그처럼 경찰청에서 사이버범죄에 대한 통계를 제공하고 있다는 것은 사이버범죄에 대한 관심을 기울이며 대응하고 있다는 것을 나타내는 것이라고 할 수 있다. 특히 그동안 수사국에 속해 있던 사이버테러대응센터를 사이버안전국으로 승격시킨 것을 통해서도 사이버범죄에 대한 경찰청의 의지를 알 수 있다.

우선 사이버범죄에 대한 대략적인 통계수치를 살펴보면 지난 10년간 다소간의 수치의 등락이 존재하고 있지만, 사이버범죄의 발생총수는 꾸준히 증가하고 있는 추세라고 할 수 있다. 2004년 총 발생건수가 77,099건이었던 것이 2013년에는 155,366건으로 두배 가량 증가하였다. 검거 건수를 보면 2004년에는 82%, 2009년에는 89%이었지만, 2012년에는 78%, 2013년에는 55%로 오히려 점차 낮아지고 있는 추세이다. 그 원인이 무엇인지는 살펴보아야 할 것이지만, 사이버범죄는 날로 발전하고 있는데 수사기관의 수사체계와 능력, 무엇보다 법률은 그에 뒤따라가지 못하는 점이 작용한 것일 수도 있다.

사이버안전

사이버범죄 발생 검거현황 | 사이버범죄 범죄통계(유형별) | 사이버범죄 범죄통계(연령별)

구 분	총 계			사이버테러형 범죄			일반사이버 범죄		
	발 생	검거		발생	검거		발생	검거	
		건수	인원		건수	인원		건수	인원
2004	77,099	63,384	70,143	15,390	10,993	11,892	61,709	52,391	58,251
2005	88,731	72,421	81,338	21,389	15,874	17,371	67,342	56,547	63,967
2006	82,186	70,545	89,248	20,186	15,979	17,498	62,000	54,566	71,750
2007	88,847	78,890	88,549	17,671	14,037	15,302	71,176	64,853	73,247
2008	136,819	122,227	128,635	20,077	16,953	17,649	116,742	105,274	110,986
2009	164,536	147,069	160,656	16,601	13,152	13,619	147,935	133,917	147,037
2010	122,902	103,809	111,772	18,287	14,874	16,777	104,615	88,935	94,995
2011	116,961	91,496	95,795	13,396	10,299	11,399	103,565	81,197	84,396
2012	108,223	84,932	86,513	9,607	6,371	7,239	98,616	78,561	79,274
2013	155,366	86,105	92,621	10,407	4,532	5,514	144,959	81,573	87,107

※ 출처: 경찰청 사이버안전국

[그림 2-5-13] 사이버범죄 발생 검거현황

다음으로 사이버범죄의 유형별 분류를 살펴보면 해킹 및 바이러스와 같은 사이버테러형 범죄는 매년 만 여건 정도 발생하는데, 전체적인 사이버범죄의 증가를 고려하면 오히려 상대적으로 줄어들고 있다. 하지만 그 강도는 매우 세어지고 있기 때문에 단순히 수치가 줄었다고 해서 안심할 수 있는 것은 아니다. 인터넷 사기나 사이버폭력 등도 꾸준한 수치를 보이고 있으며, 눈에 띄는 것은 기타의 범죄가 꾸준히 늘어나고 있다는 것이다. 즉, 사이버범죄의 유형이 분화되고 있다고 볼 수 있는 대목이다.

사이버범죄 발생 검거현황 | **사이버범죄 범죄통계(유형별)** | 사이버범죄 범죄통계(연령별)

구분	총계	해킹 바이러스	인터넷 사기	사이버 폭력	불법 사이트운영	불법복제 판매	기 타
2004	63,384	10,993	30,288	5,816	2,410	1,244	12,633
2005	72,421	15,874	33,112	9,227	1,850	1,233	11,125
2006	70,545	15,979	26,711	9,436	7,322	2,284	8,813
2007	78,890	14,037	28,081	12,905	5,505	8,167	10,195
2008	122,227	16,953	29,290	13,819	8,056	32,084	22,025
2009	147,069	13,152	31,814	10,936	31,101	34,575	25,491
2010	103,809	14,874	35,104	8,638	8,611	17,885	18,697
2011	91,496	10,299	32,803	10,354	6,678	15,087	16,275
2012	84,932	6,371	33,093	9,055	3,551	15,111	17,751
2013	86,105	4,532	39,282	7,873	2,953	13,567	17,898

※ 출처: 경찰청 사이버안전국

[그림 2-5-14] 사이버범죄 유형별 범죄통계

그리고 사이버범죄의 연령별 통계를 보면 2008년에는 10대와 20대의 비중이 높았는데 해가 지나갈수록 연령대가 높아지고 있는 것을 볼 수 있다. 이는 초기 사이버공간을 이용하던 세대가 나이를 먹어감에 따라 연령별 통계치도 함께 이동하기 때문이라고 할 수 있다. 따라서 2013년에는 20대와 30대가 주요 계층이 되고 있으며, 그와 같은 추세는 계속해서 나타나게 되어 사이버범죄의 연령도 높아질 것으로 예상된다.

사이버범죄 발생 검거현황	사이버범죄 범죄통계(유형별)	사이버범죄 범죄통계(연령별)

구분	계	10대	20대	30대	40대이상	기타
2008	100	26.6	38.9	21.8	11.8	0.9
2009	100	19.4	34.0	29.6	16.5	0.5
2010	100	19.5	39.5	25.4	14.4	1.2
2011	100	17.4	40.1	27.1	14.6	0.8
2012	100	19.9	40.9	24.5	12.9	1.8
2013	100	16.4	41.6	25.9	9.5	6.6

※ 출처: 경찰청 사이버안전국

[그림 2-5-15] 사이버범죄 연령별 범죄통계

그런데 사이버범죄와 관련해서 우리 수사기관의 조직적, 기술적, 인적 대응 방안이 적절한지에 대해서는 여전히 의문을 제기하는 견해가 많다. 그 이유는 사이버범죄는 끊임없이 발전하고 진화해 나가고 있는 반면 수사기관은 여전히 아날로그식 법제하에서 관련 수사를 진행해야 하고, 사이버범죄에 대응하기 위한 조직적, 기술적, 인적자원의 확보는 그리 수월하지 않기 때문이다. 특히 그와 관련된 예산은 여전히 요원하기만 하다. 그럼에도 불구하고 사이버범죄에 대한 대응은 지금 이 순간에도 계속되고 있다. 따라서 사이버범죄와 관련된 법령과 조직체계와 관련된 사안을 파악해 보고, 이 후 개선점을 고찰해 볼 필요가 있다.

나. 검찰의 정책

검찰의 사이버범죄를 위한 조직과 관련된 법령은 대통령령 제23105호인 '검찰청 사무기구에 관한 규정'이라고 할 수 있다. 검찰은 지난 수 년간 해당 법령을 개정하면서 사이버범죄에 대응하기 위한 조직체계를 갖추어 가고 있다. 먼저 2011년 8월 29일 일부개정에서는 대검찰청에서 사용되는 디지털수사망과 관련된 장비 및 설비의 관리·운영을 위해 필요한 인력 4명의 정원(6급 1명, 7급 1명, 8급 2명)을 증원하였다. 2012년 4월 10일 일부개정에서도 동일한 이유로 인력 13명(5급 2명, 6급 2명, 7급 5명, 8급 3명, 연구사 1명)의 정원을 증원하였다.

2012년 9월 21일 일부개정에서는 점점 더 지능화·첨단화되는 범죄에 효율인 대응

을 위해 서울중앙지방검찰청에 공공형사수사부를 신설했고, 대검찰청에서 디지털증거 분석·자금추적 업무 등을 담당할 실무인력 8명(5급 1명, 6급 2명, 7급 3명, 8급 2명)과 지방검찰청에 실무인력 10명(7급 5명, 8급 5명)을 증원하였으며, 2014년 8월 27일 일부개정에서는 사이버 범죄의 대응 및 과학적 증거 분석의 강화 등을 위하여 필요한 인력 15명(5급 1명, 6급 2명, 7급 6명, 8급 4명, 보건연구사 2명)을 대검찰청에 증원하고, 효율적인 형사사건처리 시스템의 구축과 기록물 관리 수요의 증대에 대응하기 위하여 필요한 인력 14명(5급 5명, 기록연구사 9명)을 지방검찰청에 증원하기도 하였다.

2015년 2월 11일 일부개정에서는 대검찰청에 과학수사부를 신설하게 되었다. 따라서 제9조의2에서는 "대검찰청 과학수사부에 과학수사1과·과학수사2과·디지털수사과 및 사이버수사과를 두고, 과학수사부장 밑에 과학수사기획관 1명"을 두도록 하였다(제1항). 여기서 과학수사기획관은 ① 과학수사업무의 기획 및 종합계획의 수립에 관한 사항, ② 연구개발 및 교육에 관한 총괄 지도 및 관리에 관한 사항, ③ 과학수사 관련 행정에 관한 사항, ④ 과학수사업무 관련기관 협조에 관한 사항, ⑤ 부내 과별 업무의 조정에 관한 사항, ⑥ 그 밖에 검찰총장이 명하는 사항 등의 업무를 수행하면서 과학수사부장을 보좌하도록 하고 있다(제6항)

각 과들의 업무수행내용을 살펴보면, 먼저 과학수사1과는 ① 과학적 조사기법의 개발 및 운영에 관한 사항, ② 범죄 수사와 관련된 감정 및 감식에 관한 사항, ③ 과학수사장비의 확보·개발 및 운영에 관한 사항, ④「디엔에이신원확인정보의 이용 및 보호에 관한 법률 시행령」 제4조에 따른 디엔에이인적관리자의 업무에 관한 사항, ⑤ 제1호부터 제4호까지의 업무와 관련된 지도·교육에 관한 사항, ⑥ 그 밖에 부내 다른 과의 주관에 속하지 아니하는 사항 등의 사무를 수행하도록 하고 있다(제2항). 그리고 과학수사2과는 ① 디엔에이 및 법생화학 감식시료의 분석과 데이터베이스의 관리에 관한 사항, ② 디엔에이 및 법생화학 감식기법과 관련 수사기법의 연구·개발에 관한 사항, ③ 디엔에이 및 법생화학 감식장비의 확보·개발과 운영에 관한 사항, ④ 그 밖에 법생화학 감정·감식과 관련된 사항, ⑤ 제1호부터 제4호까지의 업무와 관련된 지도·교육에 관한 사항 등 주로 디엔이이 및 법생화학과 관련된 업무를 담당하도록 하였다(제3항).

또한 디지털수사과는 ① 전자적 증거의 분석에 관한 사항, ② 전자적 증거의 분석기법에 대한 연구·개발에 관한 사항, ③ 전자적 과학수사기법의 연구·개발에 관한 사항, ④ 과학수사를 위한 컴퓨터프로그램의 연구·개발에 관한 사항, ⑤ 제1호부터 제4호까지의 업무와 관련된 지도·교육에 관한 사항 등의 사무를 수행하는 등 주로 증거분석과 관련된 업무들을 수행한다. 그리고 사이버수사과는 ① 사이버범죄 사건의 수사지원에 관한 사항, ② 검찰총장이 명하는 사이버범죄 사건의 지휘에 관한 사항, ③ 사이버범죄 수사기법의 연구·개발에 관한 사항, ④ 사이버범죄 장비의 확보·개발 및 운영에 관한 사항, ⑤ 제1호부터 제4호까지와 관련된 국제수사공조 등 국제협력업무에 관한 사항, ⑥ 제1호부터 제5호까지의 업무와 관련된 지도·교육·지원에 관한 사항 등 주로 사이버범죄의 수사와 관련된 업무들을 관장하도록 하고 있다(제4항).

대검찰청 뿐 아니라 서울중앙지방검찰청에도 첨단범죄수사제1부와 첨단범죄수사제2부를 두어 사이버범죄에 대응하고 있다(제13조 제1항). 이 때, 두 부서는 ① 검사장이 지정하는 첨단범죄사건의 수사 및 처리에 관한 사항, ② 제1호의 사건에 관련된 정보 및 자료의 수집·정비에 관한 사항, ③ 컴퓨터 등 정보처리장치 및 정보통신매체와 관련된 증거자료에 대한 압수·수색 및 분석에 관한 사항, 그리고 ④ 제1호 내지 제3호에 관련된 사항 등과 관련된 업무를 수행하며, 검사장이 각 부장간 사무분담을 하도록 하고 있다(제11항)

사이버범죄에 대한 검찰의 조직을 보면 대검찰청 내에 범죄수사 증거물과 관련된 과학수사부와 사이버수사와 관련된 사이버 수사과의 두 조직이 눈에 띈다. 먼저 과학수사부는 "범죄수사 증거물의 신속·정확한 감정(분석), 사이버범죄에 체계적인 대응으로 일선 검찰청 수사를 지원하여, 국민 안전과 인권 보장에 앞장서고 있다. 또한 과학수사장비의 첨단화, 감정 기법 연구, 전문수사관 양성을 통해 과학수사 역량을 강화함으로써 과학수사 메카로서의 위상을 정립"하는 것을 목적으로 삼고 있다고 밝히고 있다.[286] 2015년 2월에 과학수사부를 신설하고, 과학수사담당관실을 과학수사1과로, 디엔에이수사담당관실을 과학수사2과로, 디지털수사담당관실을 디지털수사과로, 그리고 사이버범죄 수사단을 사이버수사과로 개편하였다.[287] 과학수사부의 주요역할은 수사력의 강화 실체적 진실을 발견이 매우 중요하고, 인권보장과 증거의

286) http://www.spo.go.kr/spo/major/forensics/forensics01.jsp, 2015.10.31. 방문.
287) 위와 동일.

신뢰성의 중요성이 높아지고 있으며, 그를 위해 보편적 과학지식의 필요성이 증대하고 있는 현실에 발맞추어 일선의 각종 수사업무 지원과 각종 디지털 분석 도구 및 기법개발, 그리고 전문가 교육을 통해 능력향상을 꾀하여 적시성과 정확성, 신뢰성을 함양하는 것이라고 할 수 있다.[288]

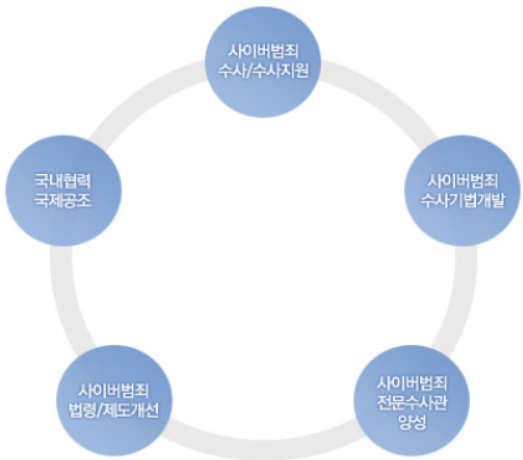
※ 출처: 대검찰청 홈페이지

[그림 2-5-16] 과학수사부의 역할

과학수사부에는 사이버범죄를 위한 사이버수사과를 두고 있다. 사이버수사과의 연혁을 살펴보면 검찰은 1995년에 서울지검에 "정보범죄수사센터" 발족하였고, 그 후 2001년에는 대검찰청에 "인터넷범죄수사센터"를 설치하여 사이버범죄를 담당하게 하였다. 그러다가 2010년에는 대검찰청 디지털수사담당관실내에 "사이버팀"을 신설하였고, 이는 다시금 2011년 5월에 "사이버통제팀"으로 개칭된다. 그리고 나서 2011년 11월 사이버통제팀을 "사이버범죄수사단"으로 통합 개편하였고, 2015년 2월에 대검찰청 과학수사부 사이버수사과로 정식 직제 개편 하였다.[289]

288) http://www.spo.go.kr/spo/major/forensics/act/forensics02.jsp, 2015.10.31. 방문.
289) http://www.spo.go.kr/spo/major/disclosure2/disclosure01.jsp. 2015.10.31. 방문.

사이버수사과의 주요 업무로는 사이버범죄 사용도구 분석 등을 통한 사이버범죄 수사지원, 네트워크 분석이나 빅데이터 분석을 통한 대용량 데이터 분석, 사이버범죄 수사인력 관리 및 교육, 신종 사이버범죄에 대응을 위한 수사기법 및 도구 개발, 그리고 유관기관 협력 및 사이버범죄 24시간 국제공조 네트워크(G8 Network for 24hour High Tech Crime) 등을 통한 국제공조 등이 있다.[290]



※ 출처: 대검찰청 홈페이지

[그림 2-5-17] 대검찰청 사이버수사과의 주요활동내역

다. 경찰의 정책

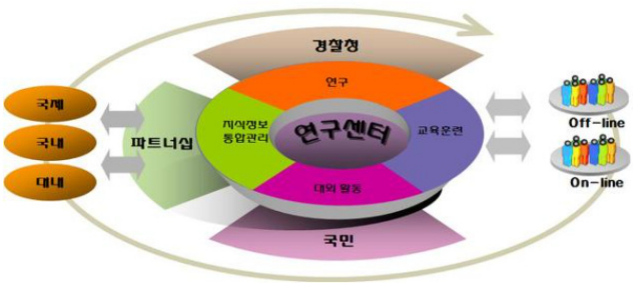
사이버범죄와 관련된 경찰의 임무와 조직에 관한 근거 법령으로는 경찰법, 경찰관직무집행법 그리고 경찰청과 그 소속기관 직제 등이 있다.[291] 그 가운데 사이버범죄와 관련된 검찰 조직과 관련된 규정으로는 경찰청과 그 소속기관 직제(대통령령 제22459호)라고 할 수 있다. 해당 규정은 2014년 3월 11일 개정을 통해 계속해서 증가하는 사이버범죄에 대응하기 위해 경찰청 본부에 사이버안전국을 신설하였다. 그리고 그를 위해 인력 50명(경무관 1명, 총경 2명, 경정 9명, 경감 24명, 경위 6명, 연구관 3명, 연구사 5명)을 증원하게 되었다. 해당 규정 제12조의2에 따르면 사이버안전국장은

290) http://www.spo.go.kr/spo/major/disclosure2/act/disclosure02.jsp, 2015.10.31. 방문.
291) 강석구외 6인, 사이버안전체계 구축에 관한 연구, 한국형사정책연구원, 2010, 127면.

치안감 또는 경무관으로 보하도록 하고 있으며(제1항), 사이버안전국의 주요업무로는 ① 사이버범죄 정보의 수집·분석, ② 사이버범죄 신고·상담, ③ 사이버범죄 수사에 관한 사항, ④ 사이버범죄 예방에 관한 사항, ⑤ 사이버범죄 관련 국제경찰기구 등과의 협력 그리고 ⑥ 전자적 증거분석 및 분석기법 연구·개발에 관한 사항 등이다.

그런데 경찰의 사이버범죄 대응에 있어 중요한 부분 중에 하나가 국제협력이라고 할 수 있다. 사이버범죄는 국경을 초월하는 범죄이기 때문에 국제협력 없이는 제대로 된 수사를 수행할 수 없기 때문이다. 따라서 경찰관 직무집행법에서는 기존에 경찰의 국제협력에 관한 부분이 명시적인 직무범위에 포함되지 않았었다. 그러다가 2014년 5월 20일 일부개정을 통해 해당 법령 제2조 제6호에 "외국 정부기관 및 국제기구와의 국제협력"을 경찰의 직무범위에 포함시키게 되었다.[292]

또한 사이버범죄에 대응하기 위해서는 사이버범죄에 대한 연구도 매우 중요하다고 할 것이다. 그래서 경찰대학은 2012년 9월 18일 그 산하에 "국제 사이버범죄 연구센터(ICRC)"를 개소하였다.[293] 센터는 사이버범죄 관련 연구 뿐 아니라 연구모임, 교육, 사이버범죄 관련 국제회의 등을 통해 경찰청의 사이버치안의 씽크탱크의 역할을 수행하고 있기도 하다.



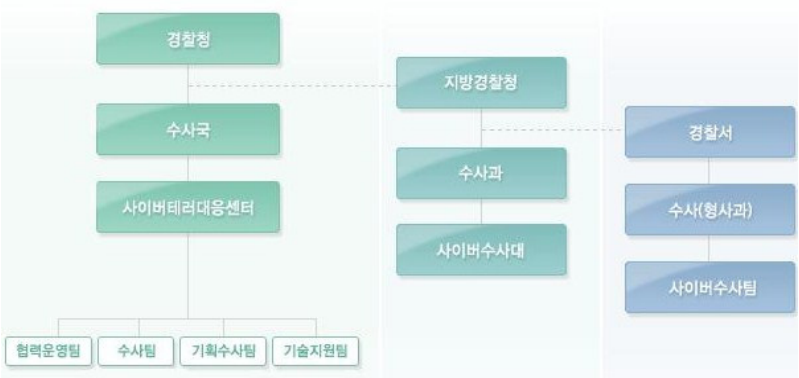
※ 출처: 경찰대학 공식블로그 '폴라리스'

[그림 2-5-18] 국제 사이버범죄 연구센터의 개념도

292) 개정이유서에서는 "수사 및 재판과 관련한 국제협력에 대해서는 「국제형사사법공조법」에 구체적인 규정이 마련되어 있으나, 그 이외의 위험방지 또는 예방경찰 작용에 있어서의 국제협력에 대해서는 근거 규정이 마련되어 있지 않아 경찰의 업무수행에 어려움이 있고, "대테러 작전" 역시 국가경찰작용으로 수행하고 있으나 법문상 이에 대한 명확한 근거 조항이 없으므로 대테러 작전 수행 및 국제협력 관련 규정을 경찰관의 직무범위에 추가하고, 국제협력을 위한 개별적 수권조항을 마련하는 등 현행 경찰작용의 법적 근거를 명확히 하는 한편 … "이라고 밝히고 있다.

293) http://www.police.ac.kr/open/photo_news.jsp?SEQ=33305&BoardMode=view, 2015. 10.31. 방문.

경찰청의 사이버범죄 대응조직은 최근에 사이버안전국이 설치되면서 그 형태에 변경이 있었다. 따라서 비교를 위해 먼저 이전 조직체계를 먼저 살펴보고자 한다. 기존의 사이버수사조직을 살펴보면 경찰청을 필두로 수사국이 있고, 수사국 내에 사이버테러대응센터가 설치되어 있었다. 사이버테러대응센터 조직은 크게 협력운영팀, 수사팀, 기획수사팀, 기술지원팀으로 구분되어 운영되었다. 그러나 사이버수사조직은 단지 경찰청에만 설치되어 있는 것은 아니었다. 각 지방경찰청과 경찰서에도 사이버수사대 및 사이버수사팀을 설치하여 사이버범죄에 대응하도록 하였다. 따라서 경찰청은 사이버수사대가 설치되어 있는 16개 지청들과 사이버범죄수사팀이 설치되어 있는 236개 경찰서가 사이버테러대응센터와 함께 협력하는 구조를 띠고 있었다.



※ 출처: 구 사이버테러대응센터 홈페이지

[그림 2-5-19] 구 경찰청 사이버범죄 대응조직구조

경찰청은 2014년 6월 경찰청 내에 사이버안전국을 설치하면서 사이버대응을 위한 조직의 지위를 체계 내에서 보다 높게 설정하였다. 사이버안전국은 "사이버공간의 치안을 확보하여 국민이 안심하고 이용할 수 있고 기업이 활동하기에 안전한 환경 조성"을 비전으로 하고, "민간·유관기관·외국과의 긴밀한 협력을 바탕으로 선제적 사이버범죄 예방 정책을 발굴·시행하여 국민·기업·국가의 피해 최소화", "지속적인 연구개발로 인적·물적 자원과 기술의 전문성을 높이고, 선택과 집중을 통해 효율적으로 주요 범죄를 제압하여 사이버치안 확보"를 사명으로 삼고 있다.[294] 그리고 존중, 봉사, 투명, 협력, 전문, 효율의 6가지를 지향 가치로 삼아 ① 예방 중심의 사이버안전

서비스 제공,[295] ② 범죄 정보 조기 분석을 통한 선제적 대응,[296] ③ 수사역량 강화를 통해 사이버범죄 강력 단속,[297] ④ 국내외 협력 강화를 통한 사이버 치안역량 제고,[298] ⑤ 전담요원과 업무시스템의 전문성 고도화,[299] ⑥ 조직 개편 및 연구 개발(R&D)로 변화에 능동적 대처[300] 등 6대 정책방향을 설정하고 있다.[301]

이를 위해 경찰청은 사이버안전국을 신설하고, 사이버안전국 내에는 사이버안전과, 사이버범죄대응과, 그리괴 디지털 포렌식 센터를 두고 있다. 다시 사이버안전과에는 사이버안전기획팀, 사이버안전서비스팀, 사이버위협분석팀, 사이버국제협력팀을 두고, 사이버범죄대응과에는 사이버수사기획팀, IT수사전략팀, 사이버테러수사팀, IT금융범죄수사팀을 두며, 디지털 포렌식 센터에는 포렌식기획팀, 첨단기법개발팀, 모바일포렌식팀, 그리고 컴퓨터포렌식팀을 두고 있다.[302]

---

294) 경찰청, 사이버안전 확보 기본 계획, 2014, 6면.

295) 여기에는 "사이버공간에서의 경찰 안전활동을 위한 법제 정비, 국민·학계·기업 등 민간과의 협력안전활동 강화, 대국민 사이버범죄 피해 예방 강화 정책 추진, 사이버범죄 피해 최소화 및 피해자 등 보호활동 전개" 등의 세부 활동이 있다; 경찰청, 앞의 글, 7면.

296) 이에는 "협업과 시스템을 통한 범죄 정보 조기 분석, 활용, 분석 결과 지속 관리 및 공유로 위협 대응 역량 강화, 분석 결과에 따른 선제적 기획수사 및 제도 개선 추진" 등의 세부 활동이 있다; 경찰청, 앞의 글, 8면.

297) "경찰청·지방청·경찰서간 사이버범죄 효율적 대응 체계 정비, 사이버 불법행위 조성 환경에 대해 강력히 대응, 수사역량 강화를 위한 인프라 개선" 등의 세부 계획이 있다; 경찰청, 앞의 글, 8면 이하.

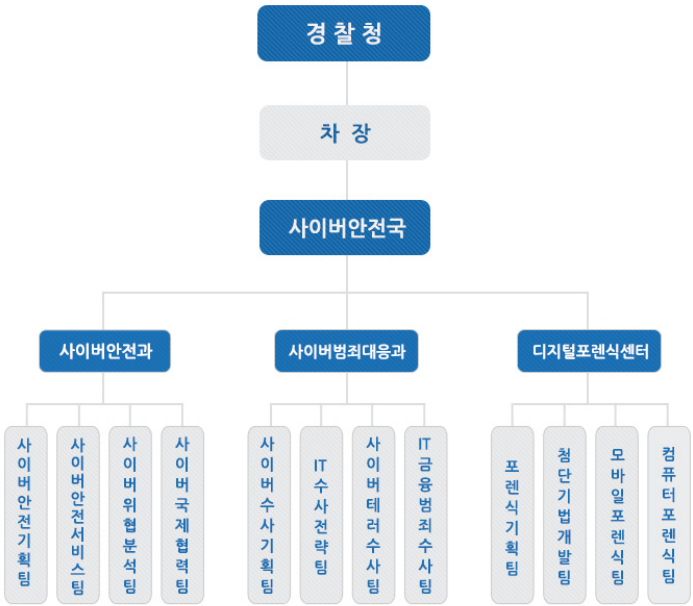
298) 이를 위해 "민간·유관기관과의 실질적 협력체계 강화, 국제 교류 협력 확대, 기술·인력 교류 등 국제적 협업 내실화" 등의 계획이 있다; 경찰청, 앞의 글, 9면.

299) 이를 위해 "사이버범죄 대응 요원의 전문성 강화, 전문시스템 구축을 통한 업무처리 효율화, 디지털증거분석 절차 개선, 분석결과의 공정성·신뢰도 제고" 등이 수행된다; 경찰청, 앞의 글, 10면.

300) 여기에는 "사이버안전활동 대응 인력·조직 확충·정비, 발전적 조직 개편 연차 추진, 사이버안전 연구·개발(R&D) 전담조직 운영, 중장기 정책과제 체계적 연구·개발" 등의 계획이 있다; 경찰청, 앞의 글, 11면.

301) http://cyberbureau.police.go.kr/bureau/sub2.jsp?mid=040200, 2015.10.31. 방문.

302) http://cyberbureau.police.go.kr/bureau/sub4.jsp?mid=040401, 2015.10.31. 방문.



※ 출처: 사이버안전국 홈페이지

[그림 2-5-20] 경찰청 사이버범죄 대응조직구조

4. 시사점

한국의 사이버안전 및 사이버범죄정책의 시사점을 살펴보면 크게 세 가지로 구분해 볼 수 있을 것이다.

첫째로, 조직에 관한 부분이다. 한국은 사이버전은 국방부가, 사이버테러는 국정원이, 민간분야의 사이버공격은 미래부가 관리하는 체계를 이루고 있으며, 전체적인 컨트롤타워의 역할은 사실상 국정원이 총괄하고 있다. 여기에 이번에 청와대에 사이버안보비서관실이 설치되면서 보다 실질적인 사이버안보 컨트롤 타워를 구축할 수 있는 조직을 만들었다. 현재 한국이 취하고 있는 이와 같은 조직 형태는 매우 바람직하다고 할 수 있다. 사이버안보에 있어서 미국과 같이 국토안보부가 막강한 권한을 가지고 있는 경우 효율성 면에서는 우수할 수 있지만, 사이버권력을 견제할 수 있는 방안이 쉽지 않다. 그러므로 한국과 같이 사이버 권력을 국방과 대북, 민간으로 구분하여 분산시키는 것은 사이버권력의 분배와 견제의 측면에서 적절하다고 할 것이다.

다만, 그와 같은 사이버권력의 분배를 적절히 조합하고 적용하기 위해서는 컨트롤 타워의 역할이 매우 중요하게 된다. 앞서 언급한 바와 같이 국정원이 실질적인 컨트롤 타워의 역할을 수행하고 있고, 청와대가 조직 개편을 통해 사실상 컨트롤 타워는 구축되어 있지만 컨트롤 타워가 제대로 동작하기 위해서는 앞으로도 구축해야할 시스템이 남아 있다. 결국 한국의 사이버안보와 관련해서는 컨트롤 타워의 위상과 역할을 제대로 설정하고, 실질적으로 동작할 수 있는 시스템을 구축하는 과제가 있다고 하겠다.

또한 사이버범죄와 관련해서는 경찰청의 사이버안전국이 큰 역할을 수행하고 있다. 기존의 컴퓨터 수사대가 사이버범죄수사대로, 다시 사이버테러대응센터로 조직이 확대되었고, 2014년에는 사이버안전국으로 승격하게 된 것이다. 조직이 커짐에 따라 과거처럼 기동력 있고 유연한 대응은 다소 떨어질 수 있지만, 체계적이고 계획적이며 장기적인 대응이 가능하게 된 것이다. 다만, 조직이 좀 더 다져지기 위해서는 시간이 좀 더 필요할 것으로 사료된다.

둘째로, 법률적인 부분이다. 이 부분은 한국이 가장 취약한 부분이라고 할 수 있다. 외국의 경우를 보면 사이버안전과 관련된 조직, 인력, 예산 등과 관련된 법률들이 제정되어 사이버안전을 법률적으로 지지해 주고 있다. 하지만 한국의 경우 법률적인 지원이 부족한 측면이 있다. 사이버안전과 관련해서 아직까지도 지침에 의해 업무가 수행되고 있는 실정이다. 최근 국회의 해킹사건과 관련해서도 법률적으로 명확한 규정이 없기 때문에 국회는 사실상 해킹의 사각지대에 놓이게 된 셈이다. 그러므로 하루속히 사이버안전과 관련된 법률이 마련되어야 할 것이다. 최근의 동향을 보면 올 연말에 '국가사이버안보기본법'을 제정하기 위해서 노력하고 있는 것으로 나타나고 있다.[303] 아직까지 국회에 계류되고 있는 '사이버테러방지법'도 중요하지만 우선 사이버안보에 대한 기본적인 방향과 사항들을 규정하는 것이 보다 바람직하다고 생각되므로 국가사이버안보기본법의 제정이 기대되는 바이다.

셋째로, 전문인력 및 보안장비이다. 사이버안전을 위해서는 전문인력과 보안장비가 필수라고 할 수 있다. 그런데 한국의 전문인력과 보안장비의 경우, 상대적으로 다른 선진국들에 비해 부족한 실정이다. 보안장비의 특성상 본 보고서에서 보안장비에 대한 내용을 상세히 다루지는 못하였지만, 한국의 보안장비의 자체 생산 현황도 그리

303) http://news1.kr/articles/?2466961, 2015.10.31. 방문.

좋은 편은 아니며, 결국 해외의 보안장비를 구입해서 사용할 수 밖에 없는 실정이다. 이와 같은 상황에서 우리의 보안정책이 해외로 유출될 수 있는 위험이 발생하게 된다. 그러므로 보안장비의 국산화가 시급한 실정이다. 또한 사이버보안 전문인력의 경우에도 인력양성에 대한 필요성은 공감하고 있는 반면, 양성의 방법 등에 대해서는 아직까지 뚜렷한 결과가 도출되고 있지 않다. 다만, 전문인력 양성을 위해서는 사이버안전 관련 시장이 보다 폭넓게 형성되어야 하고, 사이버안전인력에 대한 대우도 향상될 필요가 있다. 단순히 국가의 하향식 인력양성 구조로는 충분한 사이버안전인력이 양성되기 쉽지 않기 때문이다. 국가에서는 사이버안전 관련 시장이 폭넓게 형성될 수 있도록 직·간접적인 노력을 기울여야 할 것이다.

제3장

KOREAN INSTITUTE OF CRIMINOLOGY

2014년 동북아 평화협력포럼과 사이버범죄 지역협력 논의 동향

정명현·안민호

제3장

2014년 동북아 평화협력포럼과 사이버범죄 지역협력 논의 동향

제3장에서는 2014년에 미국을 포함하여 동북아 주요국가들의 참여 하에 한국 정부의 주도로 개최된 동북아 평화협력포럼에서 사이버스페이스 분야의 논의사항을 살펴보고,[304] 향후 논의 의제의 발전 방향과 한국 정책에 대한 시사점을 도출하고자 한다.

제1절 2014년 동북아 평화협력포럼 논의사항 분석

1. 동북아 평화협력포럼 개최 배경 및 의의

동북아 지역은 역내 경제적 상호의존성이 확대되고 있음에도 그동안 정치·안보 분야의 협력은 미약하였다. 최근에는 역사 및 영토 문제 등을 둘러싼 역내 국가간 갈등이 고조되는 등 동북아 지역의 전략적 환경이 악화되고 있다. 이는 동북아 지역 단위의 다자협력체제가 갖추어지지 않고 있어, 역내 갈등 요소 및 새로운 공동 위협 요인에 대하여 효과적인 대응이 미흡하였기 때문인 것으로 분석되고 있다. 이에 따라 동북아 지역 내 다자협력을 통한 신뢰 구축으로 역내 국가들에게 우호적인 환경 조성이 필요하게 되었다.[305]

한국 정부는 2013년부터 동북아 평화협력을 주요 외교과제로 추진해 왔다. 동 협력은 비전통 안보분야에서부터 대화와 협력의 관행을 축적하고 신뢰를 구축하여 평화와 협력의 동북아시아를 만들고자 하는 정책 이니셔티브이다. 이러한 의미있는 협력을

304) 2014 동북아 평화협력포럼은 원자력 안전, 에너지 안보, 사이버스페이스, 환경·재난 구호의 4개 분과로 나누어 워킹그룹을 구성하였다. 동북아 평화협력포럼의 논의에 관해서는 포럼에서 사용한 '사이버스페이스' 용어를 그대로 사용하기로 한다.

305) 외교부, 보도자료, 동북아평화협력구상 개황(2015.6.17.)

지속적으로 만들어가는 과정(process)에 초점을 두고, 이를 통해 역내 국가들의 점진적인 인식 변화를 유도하고 다자안보협력에 대한 공감대를 형성하고자 한다.

협력과 신뢰구축 방법으로는, 비교적 덜 민감하고 참여부담이 적은 연성안보 분야에서의 대화와 협력을 통하여 각국 정부의 정치적 의지 결집을 촉진하는 상향식(bottom-up) 접근법과 함께, 정부 간 고위급 대화를 정례화함으로써 기능별·의제별협력을 촉진하는 하향식(top-down) 접근법을 병행하고 있다. 이러한 접근방식을 통하여 기능적·정치적 분야에서 협력이 지속될 수 있는 쌍방향적 효과를 기대하고, 지역 내 분열요소를 다자적 틀에서 관리하며, 국가별 비전이 상호 조화를 이루어 동북아 지역의 지속가능한 평화와 번영을 창출하는 데 기여하고자 한다.

2. 참여대상 및 의제

동북아 평화협력포럼은 동북아 지역의 주요 국가들과의 협력을 심화하고 지역 외 국가·기구들과의 파트너십을 확대하고 있다. 역내 주요국으로는 미국, 중국, 일본, 러시아, 몽골이 참여하고 있으며, UN, EU, NATO, OSCE 등 국제적·지역적 평화체제 수립에 주요 역할을 담당하는 지역협력체 및 다자기구와의 협력적 관계를 구축하고 있다. 향후 협력대상을 ASEAN 등 기타 지역협력기구로 확대해 나갈 예정이다.

[그림 3-1-1] 동북아 평화협력포럼 협력국가 및 국제기구

동 포럼에서는 동북아 지역의 공통적인 위협 요소로서 작용하는 연성안보 의제를 논의하기로 하였다. 해당 의제는 원자력 안전, 에너지 안보, 기후변화와 환경, 재난관리, 사이버스페이스, 마약 및 보건 분야에서의 협력이다. 이들 의제를 중심으로 연성안보 분야의 협력을 진행하면서 참여국가들 간에 공감대를 형성하고, 향후 경성안보 분야에로 논의를 점차 확대해 나갈 예정이다.

3. 사이버스페이스 분야 논의사항

2014년에 한국은 미국, 중국, 일본 등 주요국에서 동북아 평화협력포럼에 대한 현지 설명회를 개최하여 국제사회의 이해를 제고하고, 미·중·일·러·몽골 등 주변국가와 독일, 프랑스, 영국, 캐나다, 호주, 인도네시아, 베트남 및 UN, EU, ASEAN, NATO 등 국제기구와 지역협력체들로부터 지지와 협력의사를 받았다. 한편 국내에서는 정부-민간 합동 국제회의를 수차례 개최하여 민간전문가들의 포럼에 대한 공감대를 높이고, 협력 분야 및 추진 방향에 대한 의견을 수렴하였다. 2014년 10월에는 '평화와 협력의 동북아시아로 가는 길'이라는 주제 하에 '2014 동북아협력포럼'을 개최하였고,[306] 포럼기간 중에 제1차 동북아 평화협력 정부간 회의를 개최하여 미·중·일·러·몽골이 공식 참여국으로, UN·EU·NATO가 대화 파트너(dialogue partner)로 참여하였다. 2014년 포럼에서의 사이버스페이스 분야에 대한 논의사항은 크게 개념 정의, 국제협력, 정보 공유 및 신뢰구축, 사이버범죄, 사이버역량 강화 및 교류로 나누어볼 수 있다. 이 중에서 사이버범죄와 사이버역량 강화 및 교류는 절을 바꾸어 상술하기로 한다.

가. 개념 정의

사이버스페이스 분야에서는 동 분야에서 사용되고 있는 용어들에 대한 국가별 이해가 상이하다는 점에 의견을 같이 하였다. 특히 '사이버스페이스'에 대한 공동의 정의가 없고, '사이버' 이슈의 광범위한 성격으로 인해 지역적·국제적 차원의 합의가 이루어

306) 2014 동북아평화협력포럼은 공개 본회의와 비공개 워킹그룹회의로 진행되었으며, 워킹그룹에서는 각 분야별 전문가가 2일간 논의를 거쳐 최종 결정문의 형태로 그룹 보고서를 제출하도록 하였다.

지기 어려운 점 등 다양한 협력의 장애 요소를 극복할 방안을 모색하는 것이 필요하다는 의견이 제시되었다. 이에 따라 공동의 개념 정의와 함께 국제적인 행동규범(Code of Conduct)을 마련하고, 정보 공유를 통하여 국가간 신뢰를 구축해 나갈 필요성이 강조되고 있다.[307]

나. 국제협력

사이버스페이스 이슈는 다른 의제들과는 달리 새로운 영역이자 새로운 프론티어(frontier)이므로 동북아평화협력구상을 통해 역내 상호 신뢰의 기반 위에 협력의 기초를 다지는 것이 중요하다. 특히 사이버스페이스 문제는 초국경적인 국가안보 문제이므로, 국가 간 협력이 필수적이며, 동북아 평화협력포럼을 계기로 역내 국가들이 다 같이 참여하는 정기적, 제도적인 대화의 장을 마련하여 지역 내 다자간 협력 체제를 창설할 필요가 있다. 특히 사이버스페이스의 초국경적인 성격으로 인하여 관할권의 문제, 개인정보 보호 문제 등이 발생하므로, 국가들의 국내법 집행에 있어서도 국가간 협력이 필요하다. 한편, 개인정보보호, 사이버안전, 전자상거래 등 최근 대두되고 있는 이슈에 대해서는 국가들이 준수하여야 할 공동의 행동규범 마련 등 공동의 대응을 통한 해결책 모색이 필요하다.

사이버공간의 초국경적 성격과 관련하여, 사이버 이슈를 다루는 데에 국내법 체제와 국제법 체제로 이원화하는 것은 정보 사회, 특히 고도의 기술사회에 적합하지 않다는 견해도 제시되었다.[308] 이에 의하면, 새로운 정보 질서를 수립하기 위해서는 국가 및 국제적 노력으로 글로벌 원칙을 설정하는 것이 필요하며, 각 국가별로 상이한 법제도 및 환경에도 불구하고, 합의 가능한 수준에서 조화된 규칙의 표준화가 요구된다는 것이다. 예컨대, 개인정보의 국외 이전이나, ICT 기반시설의 설립 및 협력 분야에서는 국가별로 상이한 법제를 조화시키기 위한 글로벌 표준이 절실하다. 또한, 사이버공간에서는 개인이 정책 결정에 중대한 역할을 담당한다. 이러한 관점에서는 새로운 인터넷 거버넌스는 ICANN이나 다국적기업과 같은 비국가행위자들이 보다 큰 역할을

307) 외교부, 동북아 협력구상(2015), p.24.
308) Kim Il-Hwan, 'State in Cyberspace: the Roles and Functions', 2014 Northeast Asia Peace and Cooperation Initiative Forum, p.37.

할 수 있도록 국제적인(international) 접근보다는 초국경적인(transnational) 접근이 더 적합하다고 본다. 이와 같이 국가간 격차가 큰 아시아 지역에서는 비국가행위자의 역할이 크며, 한국과 같이 고도의 숙달된 기술을 가진 비국가행위자들을 다수 보유한 국가에서, 사이버공간의 새로운 글로벌 거버넌스 수립에 앞장서야 한다는 논의가 제기되었다.[309] 이와 관련하여 공동의 역사적 경험 및 협력 유인을 전제로 한 '유럽 모델'보다는 정기적 협의와 개인정보보호를 특징으로 하는 '브레튼우즈 체제 모델'을 참조하는 것이 더 적합할 것이라는 의견도 개진되었다.

그러나 한편으로, 사이버안전의 문제는 여전히 국경이 존재하며, 민간부문에서는 안전(security)과 공공안전(public safety) 등의 문제를 해결할 수 없다는 견해도 제시되었다.[310] 동 견해에 의하면 사이버안전의 진정한 이슈는 국가가 지원한 첩보행위와 범죄, 공격적 군사역량의 성장으로 인한 사이버 무력 충돌 및 정치적·사회적 영향이라는 것이다. 따라서 사이버안전은 사이버공간을 안정적이고 안전하게 만들 수 있도록 궁극적으로는 전략, 규범, 그리고 조직의 구성을 요구하게 되며, 이는 국가에게 요구되는 역할이다.

다. 정보공유 및 신뢰 구축

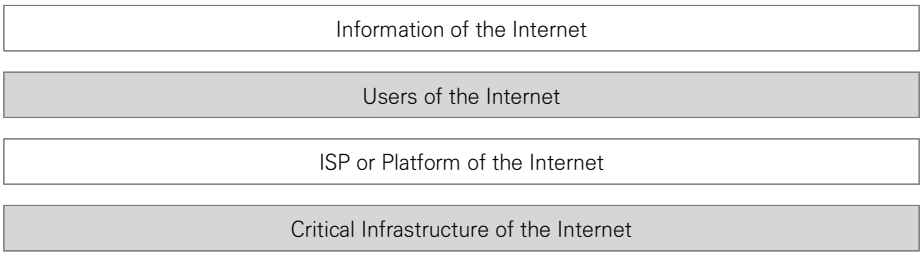
사이버스페이스에서는 개별국가들의 행위 의도를 오인할 가능성이 높고 국가별 보유 역량이 상이하므로, 신뢰 구축이 필수적이며, 남북간에도 사이버 부문의 오해가 긴장 국면으로 확대될 수 있다는 점에 유의하여, 남북 간 정보 공유 등을 통해 신뢰를 구축해 나가야 한다. 따라서 사이버스페이스에서 국가간 협력을 위해서는 각국의 정보와 지식 공유를 통한 신뢰 구축이 필요하며, 역내 국가들 간에 존재하는 언어, 관할권 등의 장벽을 초월할 수 있는 방안이 모색되어야 한다. 정보와 지식 공유를 위해서는 공동의 웹사이트를 구축하는 방안을 고려할 수 있고, 국가별 법령 및 사이버 관련 사례 정보가 역내 국가 상호간에 공유되기 위해서는 역내 국가가 사용하는 모든 언어로 접근이 가능하여야 한다.

---

309) Kim Il-Hwan, 'State in Cyberspace: the Roles and Functions', 2014 Northeast Asia Peace and Cooperation Initiative Forum, p.39.

310) James A. Lewis, 'Talking Points on Cybersecurity', 2014 Northeast Asia Peace and Cooperation Initiative Forum, pp.40-43.

중국은 사이버안전을 위하여 국내법은 인터넷의 성격에 맞게, 그리고 사이버 위협의 문제에 효과적으로 대응할 수 있도록 균형잡힌 구조를 갖추어야 한다는 견해를 제시하였다.[311] 그 구조를 그림으로 나타내면 다음과 같다.



[그림 3-1-2] 사이버 분야에 적용되는 국내법의 구조

위 그림에서 각각의 그룹이 갖는 성격과 고유한 위협은 모두 다르다. 따라서 정부의 법제는 그러한 차이에 기초하여 단계별로 상이한 위협에 대응할 필요가 있다. 일반법과 인터넷 관련 특별법의 관계도 마찬가지이다. 정부 입법은 모든 위협에 종합적으로 대응할 수 있도록 균형있는 접근을 하여야 한다. 이 때 균형이라 함은, 권리와 의무, 공공 이익과 개인의 자유, 개발과 안전, 정부 규제의 수준과 규제의 대안 등 모든 관계를 적절하게 유지하는 것을 말한다. 따라서, 국가들은 이러한 서로 다른 구분과 대응을 이해하기 위한 정보 공유와 교류가 더욱 필요하게 된다.

제2절 사이버범죄

사이버스페이스에서 안보 및 범죄 이슈는 국제법, 국제인권, UN과 같은 국제기구를 포함하므로, 더 이상 기술적 영역에 국한되지 않으며 정치적인 이슈가 된다. 즉 사이버스페이스 이슈는 다층적이고 복합적이므로 국제사회에 보편적 규범을 확립할 필요가 더욱 절실해진다. 현재는 국가 및 지역, 그리고 다변적 국제기구 간에 사이버범죄를 포함한 안보 이슈에 다양한 이견이 존재하나, 보편적 규범의 확립과 다자적

311) Zhou Hanhua, 'Cyberspace and its Governance', 2014 Northeast Asia Peace and Cooperation Initiative Forum, p.50.

메커니즘이 필요한 시점이다. 국제사회가 동일한 행동규범을 따르기 위해서는 법적인 규정의 통일화가 시급하며, 차후 단계로 역량 강화(capacity building)이 이루어져야 할 것이다. 특히 사이버 무기의 유출과 사이버 인적 자원의 운용을 위해서는 남북한이 신뢰를 기반으로 하여 상호 협력하여야 한다.

사이버범죄 분야는 사이버공간에서 비교적 일찍 법제가 발전되어 온 분야이다. 사이버범죄는 초기에는 주로 컴퓨터 네트워크의 기술적 수단을 이용하여 부당하게 이익을 취득하고자 하는 사인에 의하여 행하여져 왔으나, IT 기술의 발달과 함께 새로운 타입의 범죄유형이 증가하고 그 행위의 결과가 국경을 초월하여 막대한 영향을 미치게 됨에 따라 유럽평의회에서는 2001년에 '사이버범죄협약'(Convention on Cybercrime)을 채택하였고, 2004년 7월에 발효되었다.[312] 미국과 일본은 유럽평의회 회원국은 아니나, 동 협약에 서명, 비준하여 참여하고 있으며, 호주에 이어 최근에는 캐나다도 비준국가가 되었다.

사이버범죄는 그 행위의 성격과 주체에 따라 사이버 무력공격, 사이버 테러리즘, 사이버첩보, 또는 사이버 사고 등으로 분류될 수 있으나, 현재는 사이버공간의 사용주체가 정부인지 민간부문인지에 대한 명확한 경계를 설정하기 어려우므로 사이버범죄도 국제협력의 관점에서 논의되어야 한다.[313] 범죄 수사에 있어 신속한 상호 공조와 국제협력이 보다 강조되는 사이버범죄 분야에서 유일하게 구속력 있는 국제문서인 사이버범죄협약은 그 중요성이 더욱 증대되고 있다.[314]

제3절 사이버역량 강화 및 교류

사이버스페이스 분야의 협력을 위해서는 세 가지의 핵심 요소들, 즉 합의된 원칙, 합의된 원칙에 대한 이해와 동의, 그리고 협력 메커니즘이라는 요소가 중요하다. 이를

312) 2015년 9월 현재 47개국이 사이버범죄협약을 비준하였다. 〈http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG〉.

313) Yoo Joonkoo, 'Cyberspace Governance and Regional Cooperation: Challenges and Opportunities', 2014 Northeast Asia Peace and Cooperation Initiative Forum, p.47.

314) Hiroshi Miyashita, 'Rebuild a Culture of Privacy and Trust in Cyberspace: Lessons from Japan', 2014 Northeast Asia Peace and Cooperation Initiative Forum, p.46.

위해서는 첫째, 포괄적이고 기능적이며 비배타적인 접근, 둘째, 대화와 협의의 다자적 플랫폼과 메커니즘, 셋째, 신뢰 구축과 역량 강화, 넷째, 국가적 접근과 함께 초국가적, 국제적, 글로벌 접근, 다섯째, 개인의 권리 보호와 보장 및 국가의 투명성, 여섯째, 새로운 법률체계와 인프라 구축을 위한 비국가 행위자의 선도적 역할, 일곱째, 민관 협력(Public-Private Partnership)을 통한 공동의 협력과 규제가 필요하다.

그리고 정보기술에 의한 통제 및 국내법 체계만으로는 초국경적인 문제에 대응할 수 없으므로 국제적 합의를 이끌어내고 적극적으로 수용하여 각국의 국내법을 일치시켜 나가거나, 최소한 국내법의 차이를 공유하고 이를 조정해나가기 위한 협의가 필요하다.

또한, 국가간 협력 방안의 하나로 인적자원의 개발과 교류를 통하여 역량을 강화하고 상호 이해를 촉진하는 방안이 제시되었다. 인적자원 개발과 교류를 위한 기금 제도나 교류 프로그램을 마련함으로써 국가간 우호 증진과 협력 촉진을 기대할 수 있을 것이다. 또한 지속적인 연구 프로젝트를 통하여 인적자원을 개발하고 국가간 정보를 공유하는 방안도 논의되고 있다. 이러한 협력기반 마련을 위한 협의체가 필요하다는 의견에는 대다수의 포럼 참가자들이 의견을 같이하였다.

제4절 동북아 평화협력구상과 사이버안전을 위한 지역협력 구축의 필요성

동북아평화협력포럼은 점진적·단계적 협력을 지향함에 따라, 참여 가능한 국가간에 협력이 용이한 분야부터, 참여국이 합의하는 방식으로 대화와 협력을 모색함으로써, 국가간 협력의 가치와 상호 이해를 증진하고, 지역 내 불신과 대립의 구도를 해소하고자 한다. 또한 기존의 한·중·일 3국 협력, 6자회담, 아시아지역포럼 등 지역 협의체와 협력·보완 관계를 모색함으로써 상호 호혜적인 효과를 창출하고, 이슈를 지속적으로 발굴하고 상호연계성을 확대하고자 한다. 개방적인 포럼으로서 다층적인 논의체제를 병행하여 발전시키고, 동시에 민간전문가 차원의 협력과 정부간 협력의 시너지 효과를 창출하고자 한다. 이와 같이 동북아 지역 내 국가들이 공동으로 주도하는

참여체제 속에서 한국은 참여국들이 논의를 주도할 수 있는 환경을 조성하는 촉진자 역할을 수행할 것으로 기대되고 있다.

2014년 동북아 평화협력포럼을 통하여, 사이버스페이스에서 발생하는 제반 이슈들에 대하여 역내 상호 신뢰의 기반 위에 협력의 기초를 다지는 것이 중요하다는 점이 강조되었다. 이에 따라 동북아 평화협력구상은 기술적 협력을 넘어서 정치적 협력의 차원에서 지역적 기반 위에 중요한 역할을 할 수 있을 것으로 보인다. 즉, 국제사회에 보편적 규범 확립을 위하여 국제사회에 적용될 수 있는 행동규범이 필요한데, 초기 단계부터 전 세계의 통일된 규범에 합의하기는 어려우므로, 동북아 지역과 같이 지리적 인접성 및 공통의 이해관계를 갖는 국가들부터 협의체를 구성하여 국가간 합의와 조정을 지속시켜 나가는 것이 필요하다.

사이버스페이스에서의 국제협력을 위해서는 국가 간 합의된 원칙, 국가 간 이해조정과 신뢰 구축, 역량 강화 및 협력 기반의 마련을 위한 협의체가 요구된다. 또한 상호 신뢰 구축을 위해서는, ① 모든 역내 국가가 참여하는 사이버 협력체 수립, ② 공동의 행동규범 창출, ③ 역내 국가 간 동질성 및 유사성 발견, ④ 역내 국가의 사이버 역량 강화 등이 필수적이다. 다만, 사이버 문제는 안보와도 직결된 문제이므로 협력 기반을 마련하기까지는 장기적으로 단계적이고 체계적인 접근이 필요할 것으로 보인다. 이러한 과정에서 동북아 국가들은 사이버 분야에서의 연성 이슈에 대해 우선 협력을 도모함으로써, 국가간 상호 신뢰의 기반을 확보해 나갈 수 있을 것이다. 특히 구속력 있는 규범에의 합의를 서두르기보다 상대적으로 합의가 용의한 가이드라인 또는 프레임워크 형태로 국가간 합의를 이끌어내고, 공동의 이해를 갖는 특정 분야에 대하여 우선적으로 논의하고 합의하는 방안도 고려될 수 있다.

동북아 역내 주요 국가들의 관심 분야가 신뢰 구축과 역량 강화에 집중되고 있으므로 이 두 분야를 연결할 수 있는 협력 방안으로서, 정보 공유 정책의 시행이 우선적으로 요구된다. 정보 공유를 위하여 역내 국가들 간에 존재하는 언어, 관할권 등의 장벽을 초월할 수 있는 방안이 모색되어야 하고, 공동의 웹사이트를 구축하여 국가별 법령 및 사이버 관련 사례 정보를 역내 국가 상호간에 공유하는 방안도 고려할 수 있다.

이러한 신뢰 구축과 역량 강화를 비롯한 국제협력방안은 동북아 지역에서 사이버스

페이스에 관한 지역협력 메커니즘의 창설을 통하여 추진할 수 있다. 이러한 메커니즘을 창설하는 경우에도 참여국가의 범위, 참여 주체를 국가 행위자에 한정시킬 것인지에 대한 논의가 선행되어야 할 것이다. 특히, 역내 모든 국가의 참여 여부와 관련하여 북한의 참여 문제, 국가별 사이버 규제 내용에 대한 견해 차이, 국내법 체계의 차이 등 문제가 대두될 수 있다. 참여 주체를 역내 국가로 한정하는 경우, 동북아 지역에서의 사이버스페이스에 관한 첫 번째 지역협력 메커니즘이 될 수 있다. 다만 사이버 분야의 신뢰 구축과 국제적 합의를 위한 협력의 목적에 비추어, 타 지역 국가의 참여에 대해서도 개방적으로 운영하는 것이 보다 바람직할 것이다.

제4장

KOREAN INSTITUTE OF CRIMINOLOGY

동북아 평화협력을 위한 정책적 제언

김한균·정명현

제4장

동북아 평화협력을 위한 정책적 제언

동북아 지역은 세계 경제의 약 20% 이상을 차지하고 있는 지역임에도 불구하고, 지역별 다자협력체 부재로 인한 '아시아 패러독스[315]'현상이 심화되고 있다. 이러한 점에서, 현 정부의 동북아평화협력구상은 구체적인 실천을 통해 점진적으로 신뢰를 쌓아 나가고 마음을 열어 동북아지역의 평화와 협력을 실현해 나가기 위해 추진되고 있다. 이를 통해 다자간의 작지만 의미 있는 노력과 협력이 동북아지역의 어떠한 변화를 가지고 올 것이라는 관점에서, 주변 국가들의 적극적인 참여를 유도할 방안을 모색하는데 초점을 맞추고 있다. 따라서 동북아평화협력구상의 틀 안에서 비전통·연성안보 의제인 원자력 안전, 에너지 안보, 사이버스페이스, 재난구호와 환경·기후변화에 공동 대응할 방침이 필요하다는 인식이 동북아 국가들 간에 공유되어야 할 것이다. 향후 공감대 형성을 통해 전통안보로 협력의제를 확장하여 동북아 미래에 대한 공통된 비전을 설립하고 있다.

동북아 국가들이 이해와 협력의 관행을 쌓아 신뢰를 축적하고, 지역 간의 협력체제를 구축하기 위한 기획의 첫 단계는 우선적으로 미국, 중국, 일본, 러시아, 몽골 그리고 남·북한 등 역내 모든 이해당사국을 중심으로 시작 될 것이며, 지역안전 의제를 다룬 대화와 협력 관행지연을 방지하기 위하여 개방적 정책(open door policy)의 방식을 취하에 될 것이다. 역내 협력의 필요성은 높으나 정치적 이견의 소지는 적은 비전통 연성안보 의제인 사이버스페이스 내지 초국가적 범죄 문제야 말로 지속적인 지역협력의 틀을 만들어나가는 효과적인 계기를 제공하게 될 것이다.

---

315) "'아시아 패러독스'라는 표현은 박근혜 대통령 취임 이전인 2012년 10월 한·중·일 협력 사무국이 주최한 국제포럼에서 처음 사용한 것으로 동아시아에서 경제 분야의 복합적 상호의존이 심화되고 있는 상황과 반대로, 정치·안보 분야의 갈등이 증가하는 현상을 지적한 것이다." 동북아역사재단 공식 블로그(http://blog.naver.com/correctasia/220311729023) 참조.

제1절 지속적 지역협력을 위한 논의 과제

사이버범죄, 테러 및 무력충돌 등 다층적이고 복잡한 사이버공간에서의 불법행위의 심각성에도 불구하고, 현재 사이버 문제를 구체적으로 다루는 국제법은 존재하지 않으며, 대다수 국가들이 사이버 시대 이전의 국제법에 의존하고 있는 것이 현실이다. 이는 사이버공간에서의 불법행위가 특정 국가의 노력만으로 해결될 수는 없으며, 국가뿐만 아니라 비국가 행위주체를 포함하여 전 세계적 차원의 협력을 필요로 하지만, 국가간 정치적 이해관계의 대립이 심각하기 때문이다. 전문가들은 사이버공간에서 발행하는 행위, 예컨대 사이버 무력공격, 사이버범죄 등의 정의 및 성격에 대한 국가간 동의가 부족하고, 사이버공간에 대한 국가별 인식과 정치적 이해관계가 상이하기 때문에 사이버공간에서의 행위 규제를 위한 국제 규범이 당장 마련되기는 쉽지 않을 것으로 전망하고 있다. 다만, 2015년 제4차 UN 정보안보에 관한 정부전문가그룹(UN Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security)의 보고서 채택, 사이버전에 적용가능한 국제법에 관한 탈린 매뉴얼 개정, 상하이협력기구(Shanghai Cooperation Organization), 브릭스(BRICs) 정상회의에서 정보안보협약(Information Security Convention) 채택 등 여러 국제기구에서 사이버공간을 규율하는 국제규범 및 원칙들이 제시될 예정이므로, 이러한 국제적 규범 동향에 주목할 필요가 있다.

동북아 지역에서 사이버범죄, 테러, 무력충돌을 금지하는 법적 프레임워크 및 가이드라인이 필요하나, 현재 동북아의 역내 협력은 국가별 인식 및 정책 방향성의 차이, 제도적 리더십 부내, 상호 신뢰 부족 등의 이유로 타 지역에 비해 미약하다고 볼 수 있다. 이에 보다 효과적인 사이버 분야의 지역협력을 위해서는 ASEAN, SCO, APEC 등 기존의 다양한 협력 메커니즘 간 공조 방안 및 UN 등의 국제적 접근과 지역적 접근을 연결하는 다층적 협력 프레임워크를 마련하는 방안에 대하여 고려하여야 한다.

향후 사이버 분야에서 동북아 지역의 지속적 협력을 위해서는, 다음과 같은 실체적 논의 사항과 절차적·체제적 논의 사항을 함께 추진해 나가야 한다.

첫째, 사이버공간에 기존 국제법의 적용을 위해서는 사이버공간의 주권적 요소와 글로벌 공용재로서의 특성의 양면을 고려하여 적절히 유추하여 적용하는 것이 필요하다. 동북아 협력 차원에서 국제법의 어떠한 내용이 어떻게 적용되어야 할 것인지에 대한 논의가 이루어져야 한다. 이 문제는 사이버공간에서의 국가 주권의 범위 문제와도 밀접한 관련이 있다.

둘째, 사이버 위협에 대한 예방과 대응 차원에서 동북아 역내 국가간 대응체계에 대한 합의가 필요하다. 사이버 위협의 사후적 대응을 위해서는 개별 국가의 기술적 한계 및 국가 간 공조의 제약 등이 있으므로, 국제법 및 국제인도법 적용 시 사이버 공격을 예방하는 차원의 접근이 필요하고, 이를 위한 사전 정보 공유와 신뢰 구축 및 역량 강화를 위한 협력이 요구된다.

셋째, 군사적 차원에서 신무기에 대한 관리 규칙과 통제의 문제에 대해서도 지속적인 협력이 필요하다. 사이버 무기의 경우, 피해의 효과 측면에서 실체적 내용과 목적 및 수단이라는 요소를 모두 고려해야 하는 만큼, 사이버 기술의 특성상 군축보다는 사이버공간에서의 군사적 이용 금지에 초점을 두고 규제하는 것이 바람직하다는 의견이 대두되고 있다.

넷째, 디지털 환경에서 발생하는 국제 통상의 제반 문제에 대한 논의도 필요하다. 전자상거래의 활성화를 넘어 디지털 환경에서는 상품 거래뿐만 아니라, 디지털 컨텐츠의 국경간 이동과 사이버공간에서 금융, 의료, 교육 서비스 등의 제공이 가능해짐에 따라서 지식재산권의 보호 문제, 개인정보의 제3자 제공 및 위탁에 따른 보호 문제 등이 발생하고 있다. 동북아 역내 국가간의 디지털 무역 활성화를 위해서는 이에 대한 규범체계에 대한 국가간 협력과 논의가 필수적으로 요구된다.

다섯째, 거버넌스 차원에서 사이버공간에 대한 제반 문제를 논의하고 협력하는 지역협력체 구축 및 관할기관에 대한 지속적인 협의가 필요하다. 사이버협력은 비전통 안보 분야로서 상대적으로 지역적 차원의 협력이 용이한 분야로 간주되고 있다. 그러나 현재 동북아 지역에서의 사이버 분야의 지역적 협력은 미주나 유럽 지역에 비하여 미비하므로, 기존의 다양한 역내 협력 기구 및 논의 기제들을 효과적으로 활용하는 방안도 고려할 수 있다.

여섯째, 사이버범죄협약에의 가입에 관한 역내 국가들의 공통의 이해관계에 대한

논의가 필요하다. 사이버범죄협약은 유럽평의회의 회원국을 중심으로 발전되어 왔으나, 최근 미국, 일본, 호주, 캐나다 등 비회원국의 가입과 비준이 이루어지고 있는 경향에 따라, 동북아 역내 국가들의 범죄 수사에 있어 신속한 상호 공조와 국제협력 차원에서 동 협약에의 가입에 대한 검토 및 공동의 대안을 모색할 수 있을 것이다.[316]

사이버범죄는 그 행위의 성격과 주체에 따라 사이버 무력공격, 사이버 테러리즘, 사이버첩보, 또는 사이버 사고 등으로 분류될 수 있다. 사이버범죄에 대해서는 국가들이 기존의 형법 개정 또는 개별 행위에 대한 특별법 제정을 통하여 어느 정도 규제 방안을 마련해 오고 있으나, 현재는 사이버공간의 사용 주체가 정부인지 민간부문인지에 대한 명확한 경계를 설정하기 어려우므로 사이버범죄도 국제협력의 관점에서 논의되어야 한다.

제2절 한국의 정책 방향 및 국제적 대응방안

1. 사이버보안 정책의 방향과 과제

사이버스페이스 또한 현재 국제사회가 직면한 안보 위협에 노출되어 있다. 개인정보 침해와 개인의 사이버 범죄를 넘어 최근 연쇄적인 국제 사이버 공격에서 보듯 국가 간의 사이버 전쟁의 위험성까지 보여주고 있다. 사이버스페이스의 평화와 번영을 어떻게 유지할 것인가?

한국은 사이버공격, 사이버테러 및 사이버범죄의 상시적 피해를 입고 있는 국가로서 사이버 문제의 국제적 논의 추세를 예의주시하고 면밀하게 검토할 필요가 있다. 한국의 사이버안보 체계는 청와대가 컨트롤 타워 역할을 수행하고 있으며 실질적인 업무는 국가정보원이 수행하는 형태로 이루어져 있다. 그 중에서도 국가정보원은 실질적으로 사이버테러와 관련된 사이버안보업무를 수행하고 있으며, 민간과 관련된 사안은 미래창조과학부가 담당하고, 국방과 관련된 업무는 국방부가 담당하고 있다.

이와 같은 관계 속에서 일각에서는 국가정보원이 실질적인 컨트롤 타워로서 모든

316) 유럽평의회 사이버범죄협약의 국내 연관성검토에 관하여는 김한균·이승현·김성은, 사이버범죄방지를 위한 국제공조방안연구, 대검찰청, 2009 참조.

정보의 수집과 배분에 관한 권한을 갖게 되면, 사이버 분야에서의 권한이 하나의 기관에 지나치게 집중된다는 우려의 견해도 제기되고 있다. 때문에 야당은 국가정보원이 사이버안보의 컨트롤 타워 역할을 수행할 수 있도록 해 주는 근거가 되는 법률의 제정에 반대를 하고 있고, 그로 인해 사이버안보와 관련된 중요한 체계가 대통령 훈령에 의해 운영되고 있는 불합리한 상황이 지속되고 있다.

하지만 앞서 언급한 바와 같이 구조적으로 한국의 경우 사이버공간의 권력을 적절히 배분하도록 구성하고 있는 것에서 일단 조직적으로는 견제와 균형이 작용할 수 있는 체제를 갖추고 있다. 따라서 관건은 그러한 구조가 실질적으로 작동할 수 있도록 구체적인 시스템을 마련하는 것이다. 그러기 위해서는 하루 속히 법령을 통해 구체적인 기획을 실현하여야 하며, 현재 한국의 사이버안전이 법령의 미비로 인해 발목을 잡히는 일이 있어서는 안 될 것이다. 그런 가운데 올해 내에 입법이 추진되고 있는 '국가 사이버안보기본법'이 충실히 제정될 수 있도록 최선의 노력을 기울여야 할 것이다.

또한 사이버범죄에 있어서도 다양한 노력이 필요하다고 하겠다. 경찰청은 기존의 사이버테러대응센터를 사이버안보국으로 승격하여 사이버범죄에 보다 강력하게 대응하기 위한 노력을 기울이고 있다. 그러나, 특히 사이버범죄는 경찰청 외에 민간전문가의 도움이 절실한 분야이다. 그러므로 단순히 거버먼트(Government)의 차원에서 접근하기 보다는 거버넌스(Governance)차원에서 접근할 필요가 있다. 즉, 사이버안보국 뿐 아니라 보안 관련 기업들, 개인 전문가들, 보안 관련 대학, 보안 관련 연구소 등이 사이버범죄의 문제에 함께 대응할 필요가 있는 것이다. 물론 그와 같은 원리는 앞서 언급한 사이버안전에서도 적용될 수 있을 것이다. 이는 사이버안전과 사이버범죄의 경우 단순히 국가만의 문제가 아니라 모든 사회의 문제라는 인식이 저변이 있기 때문이다.

제2장에서 동북아 주요국가의 사이버안전 및 범죄 대응정책을 통하여 살펴보았듯이, 주요국들은 사이버공간에서의 시큐리티 문제를 국가안전보장뿐만 아니라 국제평화 및 안정의 실현을 위해서 필수적이고 절실한 것으로 인식하고 있다. 국내적으로는 사이버안전 확보를 위한 법제도 마련, 대응체제 구축, 각종 설비와 시스템의 안전 확보 및 유지, 전문인력 양성 등을 주요 정책과제로 삼고 있으며, 대외적으로는 국가간 상호 신뢰구축과 정보 공유, 역량 강화를 위한 협력, 국제적 논의를 수렴해 나가기

위한 협력체 구성, 그리고 국제규칙 및 규범의 마련이 필요하다고 강조하고 있다. 이러한 기조에서 미국의 사이버행정명령과 국방부 사이버전략, 일본의 사이버시큐리티 기본법과 신 사이버시큐리티 전략, 중국의 국가안전법과 사이버안전법 초안, 러시아의 국제정보안전기본원칙과 국가사이버안전전략개념과 같은 사이버안전 및 범죄대책의 기본 정책들이 채택되고 추진되는 과정은, 한국의 향후 사이버 정책 추진과 방향에 갖는 시사점이 매우 크다고 하겠다.

또한 주요 국가들은 사이버공간에 대한 지역적 협력의 용이성을 인식하고 미주지역, 유럽지역의 협의체와 같이 동북아 지역 내 국제협의체의 구성과, 지역협의체 내에서의 자국의 역할 및 기여방식에 많은 관심을 갖고 있다. 효과적인 사이버 분야의 지역협력을 위해서 ASEAN, SCO, APEC 등 기존의 다양한 협력 메커니즘 간 공조방안 및 UN 등의 국제적 접근과 지역적 접근을 연결하는 다층적 협력 프레임워크를 마련하는 방안을 함께 고려하여, 한국의 사이버분야 국제협력에 대한 추진 방향과 역할에 대해서도 바람직한 방향이 설정되어야 한다. 국제협력 분야에서 한국은 그동안 우리가 경험했던 여러 사건과 사례를 바탕으로 정보를 공유하고, 사건 대응에 대한 방향성을 제시하면서 신뢰를 구축함과 동시에, 우수한 IT 기술 보유국으로서 필요로 하는 국가에 대하여 기술교육과 이전 등 역량강화에 앞장설 수 있을 것이다.

2. 사이버범죄 및 보안 분야 지역 협력의 시사점

가. 한국 - 중국 - 일본의 협력

2014년 10월 21일에 북경에서 개최된 제1차 한·일·중 사이버정책 협의회에서는 사이버 이슈에 관한 각국의 전략과 정책을 소개하고 최근 동향을 논의하였다. 또한 UN 정보안보 정부전문가그룹(UNGGE)과 아세안 지역포럼(ARF) 등 국제적 절차를 통한 사이버 관련 노력에 관하여 의견을 교환하였다. 2015년 10월 15일 서울에서 개최된 제2차 한·일·중 사이버정책 협의회에서는 최근 사이버위협을 포함한 사이버 안보환경, 각국 사이버 전략 및 정책, 사이버공간의 국제규범 및 신뢰구축 조치, 지역적·국제적 사이버 협력, 사이버범죄 및 사이버테러 등 의제가 논의되었다.

이와 같이 3개국 사이버정책 협의회는 각국의 사이버 정책 및 경험 등 정보 공유를

통하여 상호신뢰를 증진하고, 구체적인 협력방안을 모색하는 계기가 되고 있다. 한-중-일 3국의 정책협의체는 동북아지역의 사이버보안 지역협력체계의 핵심기반이 될 것으로 기대된다.

나. 국제적인 사이버스페이스 관련 의제의 주도

2013년 10월에는 2011년 런던, 2012년 부다페스트에 이어 사이버 관련 이슈를 종합적으로 논의하는 국제 포럼인 서울 사이버스페이스 총회를 개최하였다. 특히 '개방되고 안전한 사이버공간을 통한 글로벌 번영'(Global Prosperity through an Open and Secure Cyberspace)이라는 주제를 선정하여, 안보뿐만 아니라 경제성장, 사회문화적 혜택, 사이버보안, 사이버범죄, 역량개발 등 상호 연관되어 있는 다양한 이슈들을 논의하였으며, 정부 대표뿐만 아니라 관련 업계, 학계, 비정부기구, 시민사회 등이 함께 참여하여 사이버 이슈 관련 최대 규모의 종합 포럼으로 자리매김하는 계기가 되었다.

이를 통해 사이버공간 관련 제반 이슈에 대한 논의방향을 제시함으로써 의제 주도국(Agenda-Setter)로서의 한국의 위상을 다지는 계기를 마련할 것으로 기대된다.

다. 동북아 평화협력과 사이버보안 정책

2015년 11월 1일 한·일·중 3국은 '동북아평화협력을 위한 공동선언문'을 통하여 '악성 사이버행위, 테러리즘, 폭력적 극단주의가 국제안보에 심각한 위협이 되고 있음을 인식하고, 공동대응을 위해 긴밀히 협력해 나갈 것이며, 이러한 차원에서 2015년 5월 제3차 3국 대테러협의회와 10월 제2차 3국 사이버정책협의회가 개최된 것을 환영한다'고 밝혔다.[317] 또한 분야별로 '경제통상분야에 관한 공동 성명'을 통해 '전자상거래, 빅데이터 등을 포함한 창조경제 분야에서 협력을 강화하기로 하고, 새로운 경제적 가치의 창출에서 전자상거래의 중요성을 감안하여, 역내 차원의 디지털 단일시장을 만드는 것이 3국 모두에게 혜택이 된다는 시각을 공유하였다.'[318]

---

317) 동북아 평화협력을 위한 공동선언문, 청와대 보도자료(2015.11.1.) 〈http://www1.president.go.kr/news/newsList.php?srh%5Bview_mode%5D=detail&srh%5Bseq%5D=12808〉 (접속날자: 2015년 11월 2일)

이처럼 사이버보안 정책을 동북아평화협력구상의 틀 안에 위치지움으로써 지속적인 지역협력 기반을 다지는 계기가 될 것으로 기대된다.

3. 동북아 지역 사이버보안 협력방안

사이버범죄 및 보안 분야의 동북아평화협력을 위한 지역협력방안으로서 한국이 수립하여야 하는 정책은 다음과 같이 제시할 수 있다.

가. 정부-민간 협력

동북아평화협력포럼은 정부기관간 논의인 Track 1 외교와 민간전문가간 논의인 Track 2 외교의 차원에서 적극 활용될 수 있다. 예컨대, 한·일·중 사이버정책 협의회가 외교부를 중심으로 하는 Track 1 차원에서 2014년부터 개최되고 있는데, 사이버범죄 및 보안 분야에서는 법무부와 경찰청, 그리고 국정원이 Track 1을 담당할 수 있고, 실무적으로 법무부와 경찰청이 Track 1에 적극 참여할 필요가 있다. Track 1에서는 사이버범죄의 적극적 근절 및 보안 강화를 협력의 직접적인 목적으로 하므로, 정보공유 및 교환·교류, 국제공조가 논의의 핵심이 될 것이다. Track 2 차원에서는 사이버 분야 이슈 발굴, 협력 체제 모델 및 규범과 원칙을 논의하기 위하여 학계와 전문가 그룹에서 참여하게 된다. 예컨대 경제첩보(economic espionage)의 문제는 사인이 범죄목적으로 행하는 경우에는 사이버해킹이 되고, 국가가 주도적으로 하는 경우에는 첩보행위가 된다. 동북아평화협력포럼의 Track 1과 Track 2 채널을 활용하여 국제모델을 도출하는 경우, 사이버해킹행위의 방지 및 처벌에 관한 국제공조 논의와 함께, 국가는 자국의 기업 이익을 위하여 다른 국가의 기밀을 탈취하지 않도록 합의를 이끌어내는 것이 필요하다.

나. 양자협력 채널 구축

동북아협력포럼은 지역 내 다자간 포럼이므로, 지역협력을 보완하기 위해서는 동북아평화협력포럼 내 양자간 협력 채널의 구축이 필요하다. 한국은 기존에 미국, 러시아,

318) 동북아 평화협력을 위한 공동선언문, 경제통상 협력에 관한 공동선언. 외교부(2015.11.1.).

EU, 호주 및 인도와 양자 사이버정책 협의회를 개최해 왔다. 사이버범죄의 문제는 아직 국가 내 정치적 이념의 문제와 밀접하게 관련되어 있으므로, 국제협력 시 동지국 간 접근이 필요하다. 따라서 이와 관련하여 한·미·일간 먼저 양자 또는 3국간 협력을 논의하고 이를 바탕으로 다자간 협력으로 확대해 나갈 수 있을 것이다. 또한 향후 중국, 러시아, 몽골에 대해서 협력 채널을 확대하기 위해서는 별도의 추가적인 연구가 진행될 필요가 있다. 이와 같이 양자 내지 삼자간 협력 채널을 구축하고 확대해 나간다면, 동북아평화협력포럼은 한·미·일, 러·중·몽의 협력을 아우르는 지역협력체제로 발전할 가능성이 있다. UNGGE의 논의과정에서 볼 수 있듯이 사이버 분야의 논의는 미국 중심의 서방 국가들과 러시아 중심의 사회주의 국가들이 대립하고 있는데, 동북아지역협력체제가 성공적으로 이루어진다면 사이버범죄 및 보안 분야에서 국제협력의 좋은 사례로서 시금석이 될 수 있을 것이다.

다. 국제 사이버범죄조약 가입검토

사이버범죄 분야의 기본 국제조약인 유럽평의회의 사이버범죄조약에 대한 가입을 다각적으로 검토하여야 한다. 미국과 일본은 이미 동 조약에 가입하여 시행하고 있으며, 한국도 한·미·일 동지국(like-minded) 차원에서 이에 대한 가입의 타당성 여부를 신중하게 검토할 필요가 있다. 이를 위해서는 통신비밀보호법 개정을 통하여 범죄수사를 위한 실시간 통신감청이 이루어질 수 있도록 해야 하고, 외국과의 사이버범죄 정보 교류가 이루어질 수 있도록 법제도를 보완하여야 한다.

라. 전문가 양성

사이버범죄 및 보안 분야의 국내 전문가 양성이 필요하다. 이 분야에서는 기술분야 전문가와 법분야 전문가가 모두 필요한데, 한국은 IT 강국으로서 기술 전문가는 다수 배출되고 있는 반면, 법 전문가는 종래 4년제 법학교육이 3년제 석사과정의 로스쿨로 전환되는 현 시점에서 학문후속세대의 양성이 어려움에 봉착하고 있다. 따라서 동 분야의 법 전문가를 육성하기 위한 제도 마련이 시급하다. 법 전문가 육성을 위해서 동 분야의 선도 국가인 미국, 독일 등지에서의 박사 후 과정, 신진학자 및 교수 연수

등이 필요하고, Track 2 차원의 논의에 참여하기 위한 전문가 양성을 위해서도 이러한 지원은 필요하다. 보다 체계적인 인력양성 계획을 수립하고, 실질적으로 사이버전문가가 양성될 수 있는 곳에 예산이 투입될 수 있도록 노력을 기울여야 할 것이다.

마. 국민적 인식제고

동북아 지역 내 사이버범죄 및 보안과 관련하여, 일반 시민, 기업, 그리고 정부를 대상으로 한 사이버범죄 및 보안에 대한 인식 제고가 필요하다. 사이버 분야의 어려움은 이슈가 매우 광범위하고, 국가마다 정치·경제·사회·문화적 배경에 따라 체감하는 이슈에 대한 문제의식이 다르게 나타난다는 점이다. 모든 이슈를 동시에 논하기는 어렵겠지만, 경제첩보와 같은 특정 주요 이슈에 대한 합의가 우선 이루어진다면 UN과 같은 국제사회에서 동지국으로서의 역량을 키워나갈 수 있을 것이다.

바. 국내법제도 정비

국내적으로 법제도의 확립이 시급하다. 앞서 살펴보았듯이 사이버범죄 및 보완과 관련하여 미국은 필요시마다 행정명령 등을 발표함으로써 법제도 마련과 선행 사례 축적에 힘쓰고 있으며, 일본 및 중국도 새로운 법제를 마련하고 있다. 러시아도 동 분야 개념 정의부터 시작하여 구체적인 제도 마련을 추진 중이다. 한국이 현재 대외적으로 공식적으로 갖고 있는 사이버 분야의 정책은 2011년에 발표한 국가사이버안보 마스터플랜이다. 다른 국가들과의 국제협력을 추진하기 위해서는 국내적으로 관련 법 및 국가전략이 채택되고 공개되어 개선된 협력방안을 도출하여야 한다. 한편 이렇게 도출된 국제협력방안을 한국 사이버국가전략에 다시 반영할 수 있을 것이다. 그리고 현재 구축되어 있는 한국의 사이버안전 체계가 실질적으로 작동할 수 있도록 법률적 기반을 마련해야 한다. 이를 위해 우선 관련 법률이 통과되어야 한다. 한국의 사이버안전이 달려있는 중대한 사안이므로 빠른 시일 내에 합의를 통해 관련 법률을 통과시켜야 할 것이다. 그리고 각 기관들이 실질적으로 협력을 할 수 있도록 청와대에서도 컨트롤 타워의 역할을 수행할 수 있는 체계를 완비하여야 할 것이다.

사. 국제협력 역량강화

한국형사정책연구원 내 국제협력센터의 역량을 강화하여야 한다. 사이버범죄 및 보안의 문제는 네트워크를 매개로 하므로 그 자체로 초국경적이며 국제적 현안이다. 한국을 대표하는 유일한 형사정책 분야의 국책연구기관으로서 한국형사정책연구원 내의 기존 우수한 연구원들이 사이버 문제에 대한 관심을 제고하고 신진 전문인력을 양성함으로써, 사이버범죄 및 보안 분야의 전문가 그룹을 형성한다면, 동 분야의 민간 전문가 그룹으로 지역협력 및 국제협력의 한 축을 담당할 수 있을 것이다. 즉, 한국형사정책연구원은 Track 2를 통하여 적극적인 논의에 참여하면서 사이버범죄 및 보안 전문가 양성을 통하여 전문가그룹을 형성하며, Track 1에서의 논의를 위하여 법무부 또는 경찰청을 지원하는 전문연구기관의 역할을 해야 할 것이다.

아. 기술역량 강화

사이버보안과 사이버범죄 대응을 위해서는 기술적 우위를 점하여야 한다. 한국의 경우 사이버공간을 이루는 인프라에서는 매우 우수한 평가를 받지만 정작 보안장비 등과 관련해서는 여전히 선진국에 뒤쳐져 있는 상황이다. 지금과 같은 상황이라면 우리의 사이버안보를 해외의 기술에 의존해야 하고, 결국 윈도우 사태에서 보는 것과 같이 선진국의 논리에 좌지우지 되는 모양새를 띠게 된다. 그러므로 국가주도의 기술개발도 중요하겠지만 민간부문에서 활발한 기술개발이 가능하도록 국가가 간접적인 지원방안에도 최선의 노력을 다 해야 할 것이다. 국가주도의 기술개발은 장점도 있지만 민간주도의 기술발전 속도를 따라갈 수 없는 측면도 있다. 그러므로 사이버보안과 사이버범죄 대응에 있어서 앞서 언급한 바와 같이 '거버먼트'에서 '거버넌스'로 옮겨가고 있는 국제적인 추세도 반영해야 할 것이다.

4. 전망과 향후 과제

남북 분단이라는 한국의 특수한 상황에서 북한은 우리의 사이버안전을 실질적으로 위협하고 있다. 따라서 우리는 하루 빨리 굳건한 사이버안전 체계를 건설해야 한다.

사이버안전 및 범죄 대응을 위해서는 정치적인 논리보다는 실질적인 논리가 적용되어야 할 것이다. 이 점에서 이번 메르스로 인해 한 순간에 붕괴되었던 보건의료 시스템을 반면교사로 삼을 필요가 있다. 형식적으로 시스템이 잘 갖추어져 있더라도, 실질적인 문제에 당면해서 한 순간에 시스템이 무력화 될 수 있기 때문이다. 그러므로 평소에 사이버안전을 위한 훈련에 힘을 쓸 필요가 있으며, 현재 우리의 사이버안전 및 사이버범죄 체계에 대한 문제점을 신속히 개선하여야 한다. 이를 위해 해외의 사례와 한국의 사례를 면밀히 비교 분석하여 장단점을 파악하고, 한국의 실태에 적합한 실질적인 시스템을 갖추기 위하여 지속적으로 사례 연구를 수행해 나갈 필요가 있다.

한국은 사이버스페이스를 동북아 평화협력 구상의 맥락에서 다각적인 협력의 중요한 영역으로 제시하는 선도적인 역할을 해왔다. 사이버보안 내지 사이버안전 의제를 설정하고 관련 지역협력을 지도하며, 지속적인 지역협력기반을 만들어 나가야 할 것이다. 그 주요 과제는 다음과 같이 제시할 수 있다.

첫째, 사이버스페이스 정책 정보 공유체계의 구축.

둘째, 사이버스페이스 관리통제 규정의 제정.

셋째, 사이버스페이스 분야 신뢰구축 방안 제시.

넷째, 모범 사례(best practice)의 공유와 확산.

다섯째, 사이버스페이스 문제대응 역량 강화.

여섯째, 사이버스페이스 관련 지역협력 프로그램 개발.

참고문헌

〈국내자료〉

김유향, '중국 네트워크안전법(안)의 주요 내용과 함의', 이슈와 논점 제1083호, 국회 입법조사처, 2015.11

신범식, '러시아 신(新)동방정책과 동북아 지역정치: 지역 세력망구도 변화와 러시아의 가능성 및 한계', EAI 국가안보패널 보고서: 동북아 데탕트-탈냉전 국가대외전략 비교연구, 동아시아 연구원, 2014

엄정호, '사이버전 전력 강화를 위한 사이버 전문인력 인증평가 모델', 보안공학연구논문지, 제11권 제2호, 2014

강수진, 국가 사이버범죄 대응전략 설계, 경찰청, 2013

강석구/이원상, 사이버범죄 관련 법령정비 방안, 한국형사정책연구원, 2013

윤해성, 사이버 테러의 동향과 대응 방안에 관한 연구, 한국형사정책연구원 연구총서, 2012

한종만·김용욱·김정훈, 러시아연방헌법, 한국형사정책연구원, 2010

강석구외 6인, 사이버안전체계 구축에 관한 연구, 한국형사정책연구원, 2010

Kim Il-Hwan, 'State in Cyberspace: the Roles and Functions', 2014 Northeast Asia Peace and Cooperation Initiative Forum, 2014.10

James A. Lewis, 'Talking Points on Cybersecurity', 2014 Northeast Asia Peace and Cooperation Initiative Forum, 2014.10

Zhou Hanhua, 'Cyberspace and its Governance', 2014 Northeast Asia Peace and Cooperation Initiative Forum, 2014.10

Yoo Joonkoo, 'Cyberspace Governance and Regional Cooperation: Challenges and Opportunities', 2014 Northeast Asia Peace and Cooperation Initiative Forum, 2014.10

Hiroshi Miyashita, 'Rebuild a Culture of Privacy and Trust in Cyberspace: Lessons from Japan', 2014 Northeast Asia Peace and Cooperation Initiative Forum, 2014.10

외교부, 동북아 협력구상, 2015
외교부 보도자료, 동북아평화협력구상 개황, 2015.6.17
미래창조과학부, K-ICT 시큐리티 발전 전략, 2015.4
미래창조과학부 보도자료, 국가 사이버안보 종합대책 성과, 2014.11.17
경찰청, 사이버안전 확보 기본 계획, 2014
국가 사이버안보 마스터플랜, 2011
국가사이버안전관리규정(대통령훈령 제316호)
국군사이버사령부령(대통령령 제26101호)
검찰청 사무기구에 관한 규정(대통령령 제23105호)
정보통신망 이용촉진 및 정보보호 등에 관한 법률(법률 제13014호)

〈국외자료〉

The White House, Executive Order-"Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities", 2015.4.1

The White House Office of the Press Secretary, "On-the-Record Press Call on the President's Executive Order, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"", 2015.4.1

The White House Office of the Press Secretary, "Executive Order-Imposing Additional Sanctions with Respect to North Korea", 2015.1.2.

U.S. Department of the Treasury, "447. What will significant malicious "cyber-enabled" activities mean for the purposes of Executive Order (E.O.) 13694?" in Cyber-related Sanctions: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities (Executive Order 13694)

Sean Sullivan, "Obama: North Korea hack 'cyber-vandalism,' not 'act of war'", Washington Post, 2014.12.21.

Charles Doyle, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report 97-1025, 2014.10.15

The White House Office of the Press Secretary, "Presidential Policy Directive-Critical Infrastructure Security and Resilience", 2013.2.23

Harold Hongju Koh, Legal Advisor U.S. Department of State, "International Law in Cyberspace", USCYBERCOM Inter-Agency Legal Conference at Ft. Meade, MD, 2012.9.18.

Hauke Johannes Gierow, 'Cyber Security in China: New Political Leadership Focuses on Boosting National Security', China Monitor No.20, Mercator Institute for China Studies, 2014.12

サイバーセキュリティ戦略, 内閣サイバーセキュリティセンター, 2015.9.4

サイバーセキュリティ戦略, 情報セキュリティ政策会議決定, 2013.6.10

情報セキュリティ問題に取り組む政府の役割・機能の見直しに向けて, IT戦略本部決定 2004.12.7

内閣官房 情報セキュリティ對策推進室の設置について, 內閣總理大臣決定, 2000.2.29

警察廳, サイバー犯罪對策, 綜合セキュリティ對策會議

サイバーセキュリティ基本法 (平成26年 法律第104號)

不正アクセス行為の禁止等に関する法律

不正アクセス行為の禁止等に関する法律の解說

インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律(出会い系サイト規制法)

出会い系サイト規制法施行規則

出会い系サイト規制法の解說

日本刑法

中国国家互联网信息办公室, 1986-2013 互联网大事记

中国国家互联网信息办公室, 中国互联网之二十年：1994-2014

工业和信息化部电信研究院政策与经济研究所, 腾讯互联网与社会研究院 〈中国互联网法律与政策研究报告〉, 电子工业出版社, 2014.4

中华人民共和国 国務院信息办公室, 中国互联网状况白皮书, 2010.6

中华人民共和国网络安全法草案, 2015.6

电信和互联网用户个人信息保护规定, 2013.6

Keir Giles, "Russia's Rublic Stance on Cyberspace Issues" in C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), 2012 4th International Conference on Cyber Conflict, NATO CCD COE Publications, 2012

Keir Giles, "Russian Cyber Security: Concepts and Current Activity", RFP Roundtable Summary, Chatham House, 2012

Cyber Security Strategy Documents-Russia, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

Концепция внешней политики Российской Федерации, 2000.6.28.; 2008.7.15.; 2013.2.12

Концепция национальной безопасности Российской Федерации, 1997.12.17

Information Security Doctrine of the Russian Federation, 2000.9.9

Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space

Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года, PR-1753, 2013.7.24

Федеральный закон от 26.07.2006 №. 152-ФЗ О персональных данных; Federal Law of 27 July 2006 N 152-FZ on Personal Data

Федеральный закон Российской Федерации от 28 июля 2012 г. N 139-ФЗ "О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации". Российская газета; Federal law No. 139-FZ "On Amendments to Federal Law On Protecting Children from Information Harmful to Their Health and Development and Certain Legislative Acts of the Russian Federation", 2012.7.28

Федеральная служба по надзору в сфере массовых коммуникаций и связи (Роскомнадзор); The Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor)

Global Cybersecurity Index & Cyberwellness Profiles, ABI Research, International Telecommunication Union (ITU), 2015

Abstract

UN·International Cooperation and Research for Crime Prevention (XI): Studies in Criminal Justice Policy for Northeast Asia Peace and Cooperation Innitiative III

Northeast Asia Regional Cooperantion in Cyber Security Policy

Kim Han-kyun · Park Rho-hyung,
Chung Myung-hyun · Ahn Min-ho

Chapter 1. The Objectives and Methods of the Study

Cyberspace is under threat of malicious cyber activities, such as cyber-terrorism and cyber crime. Malicious cyber activities are becoming diverse in size and type and the impact is very significant. Since the cyberspace issues are transboundary in nature, it is important to establish the national cooperation response system to respond to cyber-security and cyber-crime issues. Currently, South Korea is promoting trust process through the national dialogue and cooperation among the Northeast Asia region including United States. In the Northeast Asia, however, a regional cross-border political and security cooperation has continued short of interdependence as compared to economic, social and cultural interdependence trends, so called "Asian Paradox" phenomenon, and a multilateral partnership mechanism is not formed to deal with disputes between states.

In 2014, South Korea held "2014 Northeast Asia Peace and Cooperation

Forum" and experts from United States, China, Russia, Japan, Mongolia, and Korea participated to discuss the current issues of the energy security, nuclear safety, and the cyberspace and worked to improve mutual understanding. However, in the field of cyberspace, South Korea does not have a systematic view about the national cybersecurity and cybercrime. Therefore it is necessary to explore policy analysis and responses to cybersecurity and cybercrime for cooperation in Northeast Asia. This study will review of the recent policy stance on cybersecurity and cybercrime in the United States, China, Russia, Japan, and South Korea, and draw cooperative response measure through the implications of those policies which South Korea may suggest in the Northeast Asia region.

Chapter 2. Comparative Study on Cybersecurity and Cybercrime Policy in Northeast Asia Countries

I. The United States

The United States has developed cyber policy through 'international strategy in cyberspace' in 2011, and affirmed that the use of military force as a last resort in accordance with international law when necessary in response to hostile acts in cyberspace. In particular, the U.S. has embodied the response to malicious cyber threats and released national security strategy, President executive order, and the Department of Defense cyber strategy in 2015. The executive order of U.S. President Barack Obama announced on April 1, 2015 urged to respond actively about the source disclosed the cyber threat to the United States, regardless of the state or private sector. In addition, the Department of Defense amended 'DoD strategy in cyberspace' in 2011 and released a new 'DoD Cyber Strategy' on April 23, 2015.

US policy to respond to cybercrime on the internet and computer systems

is governed through the Computer Fraud Abuse Act to supplement the deficiency of the federal criminal law. In addition, by having the investigation authority to the Department of Homeland Security agencies, as well as cybercrime police, prompt response is to be done by mutual cooperation of the relevant authorities.

II. Japan

Japan enacted the Basic Law of the cyber security in 2014, presented a basic principle within the law, and provided legal basis for promoting a national cybersecurity initiatives. The law provides the responsibilities of each entity, such as local governments, critical infrastructure operators, cyber-related businesses, educational institutions, public, and specifies basic policy applicable to industrial development, research and development, human resource development, international cooperation, including all relevant sectors. In addition, by establishment of the Strategy Headquarters to oversee cybersecurity policy to the Cabinet, it is expected to strengthen international cooperation, cross-border confidence-building and information sharing, developing countries support, including technical cooperation and criminal enforcement.

Japan also released new "Cybersecurity Strategy" in September 2015 to promote international cooperation to secure in cyberspace, free flow of information, establishment of international norms, confidence building, including response to the cybercrime and cyber terror.

III. China

For the purpose of strengthening the governance of cyber security, China has changed the competent authorities to the joint governance system with the State Council and the Central Committee of the Communist Party of China. China expressly provided China's Internet sovereignty and jurisdiction over the

region through national security law in force since July 2015, The draft of Cybersecurity Act also provides the definition of cybersecurity and principle of cyber sovereignty. On the other hand, in the Criminal Code responds to cybercrime and defines the acts violating the human trafficking, such as legitimate property rights of individuals, corporations and other organizations, response to the criminal acts that infringe upon the cybersecurity operation using a cyber, acts that infringe upon national security and social stability using a cyber, acts that destroy socialist market economic and social management order.

The draft Cybersecurity Act currently under review is to strengthen the control over the whole network, defense and cyber attacks, and aims to capacity building of the government to protect Chinese users' information. This Act will apply from domestic politics and national security to foreign operators, and reflect recent trend of Chinese government policy.

IV. Russia

Russian cyber related policies focuses to ensure cybersecurity by governing and controlling the flow of information with a physical protection of the information infrastructure. The main differences of Russia policy with the West that focuses on the free flow of information is pursuit of cybersecurity through the intervention of public authorities to cyberspace. With regard to cybercrime, Russia is known to be a very high level in comprehensive evidence gathering capabilities in cyber space, and has been leading country in the software and technology for cyber crime.

The most prominent feature is that it has the authority to shut down Internet resources according to their own discretion, without the permission of the court authorities. In addition, until the recent cases Russian cyber criminals were not de fact punishment if they did not committed by targeting the Russian

nationals. Russia is a situation that gradually increases penalties for enforcement, such as a shared resource on the Internet that infringes the intellectual property rights since recently increased pressure on the prosecution in national and international cybercrime.

V. South Korea

In South Korea, cyberwarfare is governed by the Ministry of Defence, cyber terrorism is by National Intelligence Service, and the cyber attacks in the private sector is governed by the Ministry of Science, ICT, and Future Planning.

In addition,as presidential secretary for cyber security was established, it made the organization more practical to build a cyber security control tower. Regarding cybercrime, Cyber Bureau of Korea National Police Agency is the main competent authority since 2014.

On the other hand Korea has not yet established legal mechanism in response to cybersecurity and cybercrime except for the guidelines under the competent authority. In this regards, it is urgent to enact a cybersecurity basic law which defines basic principles and concepts. Also it is necessary to establish a mechanism for educating capable cybersecurity experts in this field.

Chapter 3. Issues and Developments of 2014 Northeast Asia Peace Cooperation Forum and Regional Cooperation in Cybercrime

I. Discussions in 2014 Northeast Asia Peace Cooperation Forum

The need to gradually build trust among countries by establishing a common definition and international norms for “cyber space” and “sharing of information” has been emphasized. In this regard, the ROK Government will first exert efforts to expand cooperation with the newly launched ROK-China-Japan Cyber Policy Consultation held in October 2014 as a basis, and to make use

of the opportunities presented by such occasions.

A considerable number of international seminars have been held bringing together representatives from the governmental and nongovernmental sector, such as the ROK-NATO NAPCI(Northeast Asia Peace Cooperation Initiative) Seminar on July 9, 2014; the Joint ROK-EU Seminar held on September 18-19; and the Northeast Asia Peace and Cooperation Forum held on October 28-30. These have served to further foster consensus on NAPCI among experts and to gather opinions on feasible areas of cooperation and the future direction for NAPCI. In 2015 also through the holding of joint seminars with NATO, the EU, the OSCE, and ASEAN, the ROK Government will seek to deepen cooperation with these organizations and to garner wisdom with regard to the full pursuit of projects for cooperation on various issues in the context of NAPCI.

The first High-level Intergovernmental Meeting was held on October 28, 2014 with the US, China, Japan, Russia, and Mongolia attending as official participants and the UN, the EU, and NATO attending as dialogue partners.

Welcoming the efforts by the ROK Government to overcome the Asian Paradox through functional cooperation, the participants shared the view that such efforts should also address the following matters: how to complement existing mechanisms for cooperation (such as the ARF and the EAS); how to encourage the participation of North Korea; how to improve ROK-China-Japan relations; how to identify issues of common interest; and how to bridge such efforts with cooperation in hard security areas.

II. Northeast Asia Peace Cooperation Initiative and The Need of Regional Cooperative Mechanism for Cybersecurity

There is a need to make concerted efforts to effectively respond to transnational cyber threats. Transnational threats, which respect no national or

regional boundaries, are ones that cannot be tackled by the efforts of a single country alone. It is desirable to seek to effectively deal with such issues through cooperative efforts. There is a need to address such issues as transboundary an increase in malicious cyber activities and cybercrime, through information sharing and the effective use of human and material technological resources. To deal with unforeseen crises resulting from natural or human disasters, it is important to prepare in advance by building a mechanism for multinational and pan-governmental cooperation so that the countries in the region can promptly respond to and minimize the impact of crisis situations.

Chapter 4. Policy Suggestions for Peace and Cooperation in Northeast Asia

The issues arising in cyberspace including illegal and malicious cyber activities require the collaboration of international dimension not only among states but non-state actors. In this process, it is necessary to note that international norms and principles suggested by several international organizations to govern cyberspace including the adoption of the report of the fourth UN Group of Government Experts in the field of Information Security, revision of Tallinn Manual on international law applicable to the cyber warfare, Code of Conduct of Shanghai Cooperation Organization, and Information Security Convention adopted in BRICs.

The agenda for the future discussion are as following. First, which part of the international law is applicable to cyberspace in what form. Second, it is necessary to have agreed response mechanism against the cyber threats in Northeast Asia. Third. governing rules and control system regarding to cyber weapons. Fourth, international cooperation and discussion about the legal mechanism of digital trade issues. Fifth, establishment of regional cooperative

mechanism and competent authorities in the governance view point. Sixth, common understanding and discussion about accession to the Cyber Crime Convention under the discussion of mutual assistance and cooperation.

연구총서 15-B-05

동북아 사이버범죄 및 보안 지역협력방안

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 | 고려씨엔피 (02)2277-1508
I S B N | 978-89-7366-671-3 93330