독일의 사이버테러 대응 체계 및 정책

2018년 2월

경 찰 청

유 윤 근

국외훈련개요

1. 훈련국 : 독일

2. 훈련기관명 : 루트비히-막시밀리안 대학교 부설 형사법연구소

(Institut für die gesamten Straf-rechtswissenschaften und Rechtsinformatik)

3. 훈련분야 : 사이버테러 대응

4. 훈련기간 : 2016. 2. 18. - 2018. 2. 17.

훈련기관 개요

<table>
<tr><td>명 칭</td><td colspan="4">뮌헨 루트비히-막시밀리안대학교 형사법연구소 (Institut für die gesamten Strafrechts- wissen- schaften, Rechtsphilosophie und Rechtsinformatik)</td></tr>
<tr><td>소 재 지</td><td colspan="4">Prof.-Huber-platz 2, 80539 Muenchen</td></tr>
<tr><td>홈페이지</td><td colspan="4">http://www.jura.uni-muenchen.de/fakultaet/institute/strafrecht/index.html</td></tr>
<tr><td>설립목적</td><td colspan="4">○ 형사법 전 분야, 법철학 및 법적 인포마틱의 이론과 실제에 관한 연구와 그 성과의 발표, 보급 및 해외교류를 통하여 법률 교육 및 문화 발전에 기여</td></tr>
<tr><td>조 직</td><td colspan="4">○ 형사법, 법철학, 법이론 분과</td></tr>
<tr><td>주요기능 및 연구분야</td><td colspan="4">○ 형사법 : 독일형법과 외국형법, 형사소송절차, 비교형법 등
○ 범죄학 : 비행, 범죄교정, 형사제제, 피해자학 등
○ 법철학 : 법해석학, 법사회학 등
○ 법적 인포마틱 : 법정보학, 정보통신 관련법</td></tr>
<tr><td>주요인사 인적사항</td><td colspan="4">○ Prof. Dr. jur. Satzger, Helmut
▪ EU 의회 ‘EU 범죄정책 전문가 그룹’ 독일 책임자
▪ 독일 의회 상설 ‘법학분과위원회’ 구성원
▪ ‘형사법의 EU화 문제’, ‘국제 및 EU 형사법 비교’ 등 다수 저작</td></tr>
<tr><td rowspan="3">교섭창구</td><td colspan="4">Lena Hartung, Sekretariat Prof. Satzger</td></tr>
<tr><td>전화</td><td>+49-89-2180-2734</td><td>FAX</td><td>+49-89-2180-2782</td></tr>
<tr><td>E-mail</td><td colspan="3">office.satzge@jura.uni-muenchen.de</td></tr>
</table>

< 목 차 >

제1장 서 론

오늘날 세계 각국은 정보통신 기술의 비약적인 발전을 통해 인터넷을 기반으로 한 정보화를 빠르게 확산시키면서 각종 정보와 자원을 활용하여 과거와 비교할 수 없을 정도의 높은 생산성과 편리함을 누리고 있다. 또한 사이버공간은 언어와 민족은 물론 국경과 종교의 장벽을 초월한 인류의 보편적 의사소통 수단으로 자리매김하고 있고, 정보를 양방향으로 신속하게 소통시킴으로써 정치·사회·문화·경제 전반에 다양한 가치의 생산과 교류를 촉진시키고 있다.[1)]

사이버공간이라는 곳에서는 인터넷을 통한 간단한 자료의 전달은 물론이고, 사이버쇼핑이나 사이버증권거래 등과 같이 인류 생활에 주는 이점 못지않게 각종 범죄현상도 늘어나고 있으며, 특정 목적 달성을 위한 테러의 수단으로도 사이버공간이 이용되고 있다. 최근에는 금융망, 교통망, 행정망 등 국가의 중요한 기간 전산망을 인터넷과 연동시키려는 시도가 이루어지게 되면서 이에 대한 사이버 공격은 곧 국가중추신경망의 마비로 이어지게 되고, 그로 인한 파장과 손실은 상상할 수 없이 커지게 될 우려를 낳고 있다.[2)]

이처럼 인터넷이라는 사이버공간(Cyberspace)은 우리 생활에 없어서는 안되는 필수 생활공간이 되었지만, 인터넷 환경을 이용한 해킹, 바이러스 유포, 분산서비스 거부(DDos, 디도스)공격 등과 같은 사이버 공격으로 인한 국가와 국민들의 피해, 공포는 정보화의 역기능이자 '사이버테러'라는 새로운 유형의 테러라 할 수 있다.

실제로 국내의 사이버테러 피해는 2003년 「1·25 인터넷 대란」 때 1,675억 원(한국정보보호진흥원 추정), 2009년 「7·7 DDos 대란」 때 363~544억 원(현대경제연구원 추정)으로 집계되었고, 다수의 국내외 사이트가 동시다발적인 접속 장애를 일으키거나 악성코드로 인해 시스템이 파

1) 박지형, "국가 사이버안전체계 개선에 관한 연구", 경기대학교 대학원 석사학위 논문, 2005, p.1.
2) 정재영, "사이버 테러에 대한 국가별 대응실태 연구", 국민대학교 정치대학원 석사학위 논문, 2010, p.2.

괴되었으며, 2011년 「농협 전산망 마비 사태」 때는 농협 전산망에 있는 자료가 대규모로 손상되어 수일에 걸쳐 서비스 이용이 마비되는 등 국가 재난적 피해를 발생시켰다.

특히 2011년 「농협 전산망 마비 사태」는 관공서 등 다수기관 홈페이지 운영을 일시적으로 방해하는 기존 분산서비스거부(DDos) 공격과 달리 금융기관 시스템 자체를 파괴하기 위한 1개 기관에 대한 집중 공격으로서, 새로운 형태의 사이버테러라고 할 수 있다.[3)]

이처럼 지능화·대규모화 되어가는 사이버테러에 대응하는 해결책을 찾기 위해 그동안 정부와 민간부문에서 많은 노력을 기울여 왔다. 하지만 날로 발전적인 양상을 보이고 있는 사이버테러의 위협에 비해 국내 사이버테러 대응체계는 사이버위기를 체계적으로 관리할 수 있는 제도와 구체적 방법·절차가 확립되어 있지 않아 사이버위기 발생 시 국가안보와 국익에 중대한 위험과 막대한 손해를 끼칠 우려가 있다. 그러므로 정부와 민간이 참여하는 국가 차원의 종합적인 대응체계를 구축하도록 하고 이를 통하여 사이버 공격을 사전에 탐지하여 사이버 위기 발생 가능성을 조기에 차단하며, 위기 발생 시 국가의 역량을 결집하여 신속히 대응할 수 있는 태세를 갖추어야 한다.[4)]

독일의 경우 '2009년 연방정부 연정계약[5)]'에서부터 사이버안전이라는 주제와 관련한 심도 깊은 논의를 통해 사이버테러 대응 체계를 발전시켜 왔으며, 연방내무부 소속 연방정보기술안전청(Bundesamt für Sicherheit in der Informationstechnik, BSI)을 중심으로 하는 연방 및 각 주(州)의 유관부처들과의 협업 및 민간기업(특히 사이버안전에 있어서 취약한 인프라를 운영하는 기업)들과의 협업·지도 체계를 효율적으로 운영하고

3) 김연준, 옥정석, "국가위기관리를 위한 사이버테러 대응체계 구축방안", 인문사회과학연구 제18호, 2011, p.43.

4) 이필재, "유비쿼터스 환경과 국가사이버위기관리 법제도의 문제점 및 개선방안" (국가위기관리학회보, 2009), p.124.

5) 연정(聯政)이란 연합정권의 줄임말로서, 의원내각제 국가에서 다수당이 과반수 의석을 확보하지 못했을 때 다른 정당과 함께 과반수를 채워 구성한 정부를 이르며, 성향이나 이념이 다른 2개 이상의 정당이 연립정권을 구성하는 만큼, 독일의 경우 방대하고 세밀한 연정계약서를 통한 향후 추진 정책에 대한 사전조율을 전제로 하고 있음.

있다. 특히 독일의 사이버테러 대응체제는 크리티스(KRITIS)[6] 전략 및 실행계획 등 사이버공격으로부터 취약한 인프라(취약인프라)에 초점을 맞추어 발전되어 왔는데, 그 발달 과정과 현재의 체제는 우리에게 시사하는 바가 크다.

한편 법률적 측면에서 독일은 2005년 IT 안전법[7] 제정을 통해 사이버안전 분야에서의 연방내무부 소속 연방정보기술안전청의 선도적 임무와 권한을 명확히 하여 사이버테러 대응에 있어서의 효율성, 통일성, 즉응성의 기반을 마련하고 있다. 또한 IT 안전법의 또 다른 중요한 의의는 취약인프라 운영자에 대해 사이버테러를 포함하는 사이버안전 사고에 대한 보고의무를 규정하고 있다는 점인 바, 그 논의 과정 및 구체적 내용에 대해서도 다루고자 하며, 이를 통해 대한민국의 사이버테러 대응 체제와 법률에 대한 개선방안을 제언하고자 한다.

제2장 사이버테러의 정의 및 특성

제 1 절 사이버테러의 정의

테러라는 용어는 라틴어의 'Terree'에서 유래하였으며, '커다란 공포'를 뜻하는 말이다. 최초로 사용된 시기는 1793년 프랑스 혁명시기에 공화당 혁명정부를 이끌었던 로베스피에르가 반대파인 왕당파 숙청을 위해 자행했던 공포의 시대(The reign of Terror)에서 시작되었다.

우리가 흔히 사용하는 테러라는 용어는 테러리즘을 의미하는 것으로서 다소 그 개념의 차이는 있으나 일반적으로 구별 없이 사용하는 경우가

6) Kritische Infrastrukturen(취약한 인프라들)의 머릿글자를 따서 조합된 단어로, 그 손실이나 침해가 지속적 공급부족, 공공안전의 중대한 장애 또는 다른 심대한 결과를 야기하는, 국가 공동체를 위해 중요한 의미를 가지는 조직 또는 기관들을 말하며, 독일 사이버안전 관리체계의 핵심을 이루는 용어임.

7) Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme(정보기술 시스템들의 안전 고양을 위한 법), 약칭 IT Sicherheitsgesetz(IT 안전법)

많다. 학자들에 의하면 테러란 '특정한 위협이나 공포로 인해 모든 인간들이 심적으로 느끼게 되는 극단적인 두려움의 근원이 되는 것'으로 정의하고, 주관적이며 가치중립적인 자연현상이라고 평한다.[8)]

사이버테러리즘 혹은 사이버테러는 최근에 등장한 개념으로 사이버 공간을 통해 사이버 수단을 이용, 테러목적을 달성하려는 것으로서 "최첨단 정보통신 기술을 이용해 사회중추신경인 전산망을 파괴하거나 해킹으로 획득한 자료를 불순한 목적에 이용하는 행위",[9)] 첨단 정보통신 기술을 이용해 물리적 세계가 가상의 세계로 전환되어 있는 공간을 무차별적으로 공격하는 행위", "해킹, 바이러스 등 정보통신망 자체에 대한 공격행위로서 국가 또는 사회적 혼란 또는 불안을 야기하는 행위"[10)] 등과 같이 학자 간에 다양하게 정의되어지고 있으며, 야후 인터넷용어 백과사전에 의하면 사이버테러(Cyber terror)라 함은 "주요기관의 정보시스템을 파괴하여 국가기능을 마비시키는 신종테러"라고 용어정의를 하고 있으나, 사이버테러라는 용어 자체는 우리나라 법령에 사용된 예가 없으며 국가대테러활동지침(대통령훈령 제4호) 제2조1호에서 "컴퓨터 통신망을 이용한 정보조작 및 전산망 파괴"를 테러의 유형 중 하나로 규정하고 있다.

그러나 이러한 사이버테러가 개인으로부터 집단·국가에 이르기까지 다양한 주체로부터 행해질 수가 있고 그 결과가 국가기반시설에 초점이 맞추어질 경우 엄청난 피해를 야기한다는 사실에는 모두 공감하고 있으며 그에 따른 준비의 필요성도 절감하고 있다.

제2절 현행법상 사이버테러의 의미

사이버테러에 대해 「정보통신기반보호법」(법률 제14839호)에서는 '전자적 침해행위'(제2조2항)로 규정하고 있는데, "정보통신기반시설을 대상

8) 최진태, "테러리즘의 이론과 실제", 대영문화사, 2006, p.9.
9) 조병인, "사이버경찰에 관한 연구", 한국형사정책연구원, 2000, p.227.
10) 양근원, "사이버테러의 실태와 법적대응에 관한 연구", 경희대학교 대학원 석사학위논문, 2004, p.183.

으로 해킹, 컴퓨터바이러스, 논리·메일폭탄·서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위"라고 정의하고 있다. 또한 「국가사이버안전관리규정 」(대통령훈령 제316호)에서는 '사이버공격'이라고 규정(제2조 제2항)하고 있는데, "해킹·컴퓨터바이러스, 논리폭탄·메일폭탄, 서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위"라고 정의하고 있다.

이러한 관점에서 볼 때, 사이버테러란 공격주체가 공격대상의 국가, 공공, 민간의 정보통신망을 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 등에 의하여 정보통신 기반시설을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위라고 규정할 수 있다.

제3절 사이버테러의 특성

사이버테러는 전 세계에 그물망처럼 연계된 인터넷 망을 통해 빛의 속도로 전개되며 소요시간도 그동안에 있었던 일반적인 테러와는 달리 수분 이내에 끝나면서도 피해규모 또한 일반인이 상상할 수 없을 만큼 국가의 안보에 심각한 위협으로 나타날 수 있다.

따라서 사이버테러는 그동안 우리 인류에 커다란 위협이 되어 왔던 일반적인 테러와는 그 본질을 달리하는 것으로 볼 수 있는데, 통상의 테러와는 다른 사이버테러의 특징을 살펴보면 다음과 같다.

1. 광역성 및 다양성

일반적으로 사이버테러는 테러리스트가 목표로 정한 공격 지점에 직접 접속하여 공격하는 것이 아니라 네트워크가 연결된 곳이라면 세계 어느 곳이든 공격을 감행할 수가 있다. 특히 네트워크망에 대한 보안시스템이 잘

완비되고 국민들의 보안의식이 높은 선진국보다는 보안시스템이 취약한 지역·국가에서부터 출발하여 여러 단계를 거친 다음 목표하는 전산망에 접근하여 필요한 정보를 빼내가는 우회적인 방법을 선택하는 것이 일반적인 방법이다.

따라서 사이버 공간에 대한 범죄가 발생했을 경우 피해를 당한 전산망에 대한 조사권만 가지고 조사하는 것에는 한계가 있으며, 그것이 국제적 테러조직에 의한 범죄일 경우 국제적인 협력이 없다면 조사 자체가 불가능해지는 상황까지 발생한다.

또한 사이버테러를 대비하기 위해서는 과거처럼 경찰이나 군 등이 책임지역이나 건물을 가지고 독자적으로 업무를 수행할 수 있는 것이 아니고 네트워크에 연계된 각 기관들이 공동으로 상호 유기적인 협조 체제를 구축하지 않고서는 적절한 대비가 어렵기 때문에 미래 사회의 위협이 될 사이버테러는 국제적인 협력관계 구축은 물론 관련 기관간의 유기적인 협조체제가 구축되도록 노력해야 한다.

2. 최소한의 인원으로 최대의 피해 가능성

컴퓨터 네트워크를 이용하여 적의 정보통신망에 침투하기 위한 최소한의 기술자만 있으면 사이버테러리즘은 가능하다. 물리적인 테러가 대규모 혹은 소규모라도 다수의 인원을 필요로 하는 것에 비해, 목표 대상에 따라 필요 인원이 증가할 수는 있겠지만 사이버테러를 위한 인원은 다른 어떤 물리적인 테러를 수행하기 위한 인원에 비해 적다. 하지만 이러한 경우에도 타격 대상이 되는 정보통신시스템을 파괴 또는 마비시키는 것에 따를 경제적·사회적 파급 효과는 정보통신기반시설이 더욱 선진화되고 의존도가 높은 국가일수록 비례하여 커진다.

또한 컴퓨터 범죄행위는 반복 가능성, 영속성의 속성이 있으므로 한 번의 범죄행위는 그 규모나 피해가 작을지라도 계속적으로 자동적인 프로

그램의 실행, 확산을 통해 피해액이 계속 증가할 가능성이 높다. 하지만 물리적 테러리즘보다 극적인 요소가 덜해 테러리스트들이 사이버테러리즘을 그리 선호하지 않을 것이라는 의견도 있다.

3. 증거의 은닉성과 비가시성

테러리스트들은 물리적 공간이 아닌 사이버 공간의 특수성을 활용하여 수사기관의 추적으로 따돌리고 증거를 변조하거나 삭제하고 있다. 이와 같이 원본과 복사본 구별이 어렵고 수사가 곤란한 디지털 증거에 법적 증거능력을 갖게 하는 방법인 컴퓨터 포렌식(Computer forensics) 기법은 최근 들어 크게 발전하고 있다.

수사 및 법적인 관점에서 디지털 자료는 눈에 보이지 않는 비가시성에 바탕을 두고 잠재성과 다양성·대량성 등의 특징을 가지고 있어 사법처리를 위한 증거 자료를 확보하는 것에 특별한 방법과 절차를 요구하고 있다. 범죄의 혐의가 있을 때 범죄 사실과 증거를 수사하여야 하는 것은 컴퓨터 관련 범죄에서도 다른 범죄와 마찬가지이나, 컴퓨터와 관련된 증거를 수집함에 있어서는 전통적 증거 수집과 달리 증거 수집 절차에 있어서 새로운 문제가 야기된다. 예를 들어 컴퓨터에 의하여 처리되고 저장된 데이터 또는 프로그램 등이 저장되어 있는 자기테이프나 디스크는 유체물이기 때문에 압수 대상이 되지만, 데이터나 프로그램 그 자체로는 유체물이 아니기 때문에 형사소송법상 압수수색 대상이 될 수 있는가의 문제가 생긴다.

또한 사이버 범죄의 주요 유형 중 하나인 해킹 기술이 발전할수록 보안기술도 함께 발전해 왔다고 할 수 있지만, 알려지지 않는 행위나 새로운 공격기법에 대하여 방어하기에는 역부족이고, 해킹을 당했는지조차 알지 못하며 체계적인 대응방안을 세우는 데에도 익숙하지 못해 피해 복구에 대한 전문적인 기술개발이나 체계적인 연구가 진행되지 못하고 있다.

4. 저가의 테러수행 비용

사이버테러를 수행하는 데는 많은 비용과 국가적 지원이 없어도 정보체계에 대한 지식만으로 사이버기술과 무기를 연구개발 할 수 있고, 네트워크를 통해 접근만 할 수 있으면 개발된 사이버무기를 사용하여 공격할 수 있다. 또한 정보체계들은 상호의존성이 높기 때문에 어느 하나의 정보체계 마비는 전체적으로 막대한 피해를 입히게 된다.

제3장 사이버테러의 주요 사례와 국가위기관리와의 상관관계

제1절 국내 주요 사이버테러 피해현황

1. 1·25 인터넷 대란(2003년)

1·25 대란은 호주, 미국 등에서 유입된 슬래머 웜(Slmmer worm)이 MS의 데이터서비스 'SQL서버'를 공격하여 한국의 8,800대를 비롯하여 전세계 75,000여대를 다운시킨 사건이다. 한국의 경우 국제회선 및 ISP의 주요 DNS 서버와 인터넷데이터베이스센터(IDC) 내부망에 과부하 현상이 발생하였다. 당시 미국 FBI와 국제공조수사를 진행했지만 범죄인지, 테러인지, 전쟁인지에 대해서 결론을 내리지는 못했다. 이 사건은 웜 하나로 인터넷을 마비시킬 수 있다는 가상 시나리오를 현실세계에서 입증한 첫 번째 사례로 기록되었다.

2. 국가기관 해킹사건(2004년)

국가기관 해킹사건은 중국의 해커조직에 의해 한국의 국회, 국방연구

원, 원자력연구소 등 10개 국가기관 222대의 시스템이 공격을 당한 사건으로 한국에서 발생한 국가안보 관련 사이버테러 중에서 가장 피해가 컸던 사건으로 기록되고 있다. 이 사건은 약 6개월 동안 국가안보와 관련된 중요 기관의 시스템에 침입하여 중요 기밀이 유출되었다. 당시 경찰청에서는 중국 해커를 용의자로 특정하고 국제공조를 요청하였으나 중국 측의 비협조로 검거하지는 못했다. 이 사건은 당시 국가정보원의 '국가사이버안전센터' 창설과 「국가사이버안전관리규정」을 제정하는데 기여하였다.

3. 7·7 디도스(DDos) 대란(2009년)

7·7 디도스 공격은 북한이 청와대·국방부·국정원 등 국가 중추기관과 언론사·은행 등 21개 사이트를 공격하여 시스템 운영을 방해한 사건으로, 북한의 공격이 대외적으로 공개된 최초의 사건이다. 공격자들은 악성코드를 설치하면서 원본 파일이 자동으로 소멸되도록 설계하였고, 악성코드를 그림파일로 위장하는 등 지능화된 수법을 사용하였다. 또한 감염된 좀비PC의 하드디스크가 파괴되어 수사기관이 추적을 하지 못하여 수사의 많은 어려움을 자아냈다. 이 사건은 전 세계 61개국 435대 서버를 해킹하여 디도스 공격에 동원하는 등 글로벌한 공격 형태를 여실히 보여주었다. 당시 국정원, 방통위가 공격을 사전에 탐지하지 못했고, 공격 대응에 있어서 부처 간 혼선이 발생하면서 7·7 디도스 공격은 범정부 차원의 '국가사이버위기종합대책'을 마련하게 된 결정적인 계기가 되었다.

4. 3·4 디도스 사건(2011년)

북한이 좀비PC 10만대를 동원하여 국회·행정안전부·통일부 등 20개 정부기관 홈페이지와 은행·증권사·포털 등 20개 사이트에 대하여 디도스 공격을 감행한 사건이다. 이들은 해외 70개국에 746개의 공격명령 서버를 구

축한 다음 실시간으로 좀비PC를 제어하면서 정부기관과 민간의 홈페이지를 마비시켰다.

당시 사건발생 직후 과거 7·7 디도스 공격과 같은 북한의 소행여부가 문제되었는데, 이에 경찰청은 파일공유 사이트를 통해 악성코드를 유포한 점, 디도스 공격체계와 방식이 동일하다는 점, 악성코드의 설계 및 통신방식이 일치한다는 점, 해외 공격명령서버 중 일부가 동일한 점 등을 종합하여 2009년의 7·7 디도스 공격의 주체와 동일하다는 수사결과를 발표하였다.

5. 농협 전산망 해킹(2011년)

2011년 4월 12일 농협 전산망이 해킹되고 자료가 대규모로 훼손되어 수일에 걸쳐 전체 또는 일부 서비스 이용이 마비되었다. 이에 서울중앙지방검찰청의 수사결과 농협 전산서버 유지보수업체 직원의 노트북이 웹하드 사이트를 통해 해킹되어 7개월 동안 노출되었고, 공격은 원격에서 인터넷을 통해 이루어졌다고 밝혔다. 이 사건은 7·7 디도스 공격 및 3·4 디도스 공격과 유사한 프로그래밍 방식을 사용하였고, 악성코드 유포 경로·방식의 유사성, 공격명령서버의 동일성 등을 근거로 공격주체를 북한으로 발표하였다.

6. 중앙선관위 사이버테러 사건(2011년)

2011년 10월 26일 서울시장 보궐선거일에 중앙선거관리위원회와 박원순 후보 홈페이지에 디도스 공격을 감행하여 유권자들의 투표소 검색 기능을 마비시킨 선거방해 사건이다. 이 사건은 디도스 공격이 정치적 목적을 가지고 선거에 영향을 미친 최초의 사건으로 평가되고 있다. 당시 경찰은 한나라당 국회의원 보좌관을 포함한 피의자 5명을 검거·구속하였지만, 정치권·언론 일각에선 사건 배후 수사가 미흡하다는 의혹을 제기함에 따라 특검

까지 실시하게 되었다.

7. 중앙일보 신문제작 시스템 해킹(2012년)

‘IsOne’이라는 별칭을 쓰는 공격자가 중앙일보 홈페이지를 변조하고, 신문제작 시스템을 파괴한 사건이다. 북한 체신성 인터넷 프로토콜(IP)을 통해 중앙일보 사이트에 집중적인 접속이 시작된 시점은 4월 21일로, 북한이 대규모 대남 규탄집회를 열고 일부 언론사 등에 특별행동을 감행하겠다고 한 시기와 일치한다.

8. 3·20 방송·금융전산망 해킹(2013년)

KBS·MBC·YTN 및 농협·신한은행 등 주요 방송·금융기관의 전산망에 동시다발적으로 악성코드가 유포돼, 서버·PC·ATM 등 총 4만8748대 기기의 데이터가 삭제되었다. 민·관·군 합동대응팀은 공격 경로 추적·분석 결과 북한 정찰총국 소행으로 추정하였으며, 해당 공격에서 북한 내부 IP가 사용된 점이 확인되었고, 해커가 접속 흔적을 제거하려고 노력했지만 남아 있는 원격 터미널 접속 로그를 통해 이를 확인했다고 설명하였다.

9. 6·25 정부기관 등 해킹(2013년)

청와대·국무조정실 등 홈페이지와 정당 및 중소 언론기관 등에서 운영하는 전산시스템에 동시다발적인 사이버공격이 감행되었다. 해킹 공격을 위해 사용한 인터넷프로토콜(IP)에서 북한이 사용한 IP가 발견되었고, 서버를 다운시키기 위해 사용된 방법, 이용된 악성코드 문자열 등이 위 3·20 해킹사건에서 사용된 방법과 거의 유사한 점 등에서 북한의 소행으로 추정되었다.

10. 한국수력원자력 문서유출(2014년)

자칭 'Who Am I', 일명 원전반대그룹이라는 해킹조직이 2014년 12월 15일부터 2015년 1월 12일까지 모두 6회에 걸쳐 한수원 관련 자료를 공개하며 원전 가동을 중단하라고 협박하였다. 본격적인 협박 이전인 2014년 12월 9일부터 나흘간 한수원 직원 3,571명에게 5,986통의 악성코드(파괴형) 이메일을 발송해 PC 디스크 등의 파괴를 시도하기도 했으나, 공격을 받은 PC 중 한수원 PC 8대만 감염되고, 그 중 5대의 하드디스크가 초기화되는 정도에 그쳐 원전 운용이나 안전에는 이상이 없었다. 특정 권한을 가진 내부자가 결탁되면 아무리 강력한 기술적 보호조치가 있다 해도 해킹을 막을 수 없다는 사실을 잘 보여준 사례이다.

11. 청와대 사칭 이메일 발송(2016년)

청와대 국가안보실 등 정부기관을 사칭해 759명에게 북한의 4차 핵실험에 대한 의견을 수렴하는 내용의 이메일을 발송한 사건으로, 이에는 악성코드가 포함되어 있었다. 이메일 발신지가 위 한수원 문서유출 사건과 동일한 중국 랴오닝성 소재 IP 주소지와 일치하고, 악성코드 간 유사점 등을 근거로 북한의 소행으로 추정되었다.

제2절 진화하는 북한의 사이버공격 위협

1. 북한의 사이버공격의 전략적 특징

북한의 사이버공격은 정보기술 연결에 취약한 다른 우월한 적들에

대한 비대칭전력으로서의 성격을 가진다. 따라서 즉각적인 무력 대응을 유발할 가능성도 낮다. 북한이 출처라는 사실이 밝혀질 즈음이면 이미 사이버 공격의 흔적은 사라질 수밖에 없다.

최근 북한의 대남도발 양상은 중국 공산당의 군사교리를 모방한 점혈전략(點穴戰略)인데, 인간으로 치면 인체의 급소가 되는 '점'을 공략해 상대방을 무력화시키는 전략이다. 가장 많이 적용되고 있는 분야는 역시 사이버전이라 할 수 있다. 정보시스템의 약점과 급소 부위의 혈을 눌러 전체를 마비시킴으로써 최대의 효과를 추구하는 것이다.

북한의 사이버공격은 핵, 미사일과 함께 3대 보검 전략의 하나이기 때문에 김정은이 북한의 사이버부대 창설과 운영에 깊이 관여하고 있다는 점과 사이버전이 비대칭 전력으로서 필수불가결하다는 인식을 가지고 있다는 점 및 대남혁명전략의 일환으로 사이버공격을 활용한다는 점에 유의할 필요가 있다. 김정은은 2013년 8월 군 간부에게 "사이버공격은 핵, 미사일과 함께 우리 군의 만능의 보검"이라며 사이버공격 능력 강화를 주문했고, 2014년에는 정찰총국 산하 121국을 방문해 "적들의 사이버 거점을 일순간에 장악하고 무력화할 준비를 갖추라"고 지시했다. 이 지시에 따라 인민군과 노동당 산하 기관들은 ,사이버 충성경쟁'에 돌입해 경쟁적으로 사이버 조직을 만들고 사이버 전사들을 확충하는 데 주력하고 있는 것으로 파악됐다.

2. 북한의 사이버전력

북한의 사이버전 능력은 세계 최고수준인 미국에 버금간다는 평가를 받고 있다. 1990년대부터 사이버전 역량을 축적해왔고, 경제난으로 재래식 전력 증강에 어려움을 겪자 적은 비용으로 큰 효과를 낼 수 있는 사이버 전력 강화에 박차를 가했다. 2003년 이라크 전쟁 당시 미국이 지휘통제자동화시스템을 통해 소수 인력으로 이라크군 전체를 무력화시키자, 북한은 더 심혈을 기울여 사이버전 능력 배양에 집중하고 있는 것으로 알려지고

있다.

북한의 사이버공격은 상당히 세분화된 조직들에 의해 체계적으로 이뤄지고 있다. 가장 주도적인 조직은 정찰총국 산하 다양한 작전국들이다. 육·해상 정찰국, 해외정보국(구 35실), 기술정찰국 등이 있다. 또 별도 조직으로 사이버전지도국(121국), 11군단이 있다. 총참모부 내 사이버 전담부서, 노동당 내 통일전선부와 문화교류국은 다양한 사이버심리전을 병행한다. 이들은 주요 대상국인 미국과 한국의 인터넷이 상당히 발달돼 많은 정보가 있다는 특징을 악용해 저비용 고효율인 사이버 집중공격을 벌이고 있다.

121국은 주중 선양, 베이징 등에 위치한 무역회사로 위장해 사이버공격을 감행하고 있다. 11군단에는 10개 직할 여단 4만 여명의 후방 테러, 게릴라전 수행 가능 인력이 있고, 문화교류국은 수백 개의 간첩망을 확보하고 있는 것으로 알려졌다. 북한에서 사이버공격을 담당하는 인원이 점점 증가해 현재 6,800 여명에 이르는 것으로 알려졌다. 자유민주연구원의 분석 결과에 따르면 북한의 사이버공격 담당 인력 중 단순기술 인력이 아닌 실제 작전에 투입되는 정예요원만 1,700 여명에 달한다. 고급인력을 사이버공격 쪽으로 더 투입하다 보니 점점 더 고강도의 공격이 시도되고 있다.

또 북한은 '공격 전용 네트워크'를 인터넷에서 분리 구축하고 있는 것으로 나타났다. 이에 따라 북한의 사이버전에 대한 의지는 러시아에 이어 중국·미국과 같은 2위이며, 공격 능력은 6위, 사이버정보 평가능력은 7위로 평가되고 있다.[11)]

제3절 사이버테러와 국가위기관리의 상관관계

1. 국가위기관리의 개념

11) 아시아경제 2016년 6월 26일자 ""사이버공격, 핵·미사일 등과 3대 전쟁수단"…김정은, 사이버 전사 육성 직접 지시" 기사 참조

"위기(crisis)"라는 단어는 사전의 일반적 의미 외에 접근 방식에 따라 다양한 정의가 존재하고 있다. 웹스터 사전(Webster´s New Dictionary of Synonyms)에 의하면 위기는 "더 좋게 되거나 더 나쁘게 되는 갈림길"이라고 정의하였고, 위기를 "중요한 변화가 절박하게 요구되는 불완전한 상태이거나 혹은 하나의 사건 또는 행동과정이 계속 진행되어야 하는지 아니면 수정 또는 종결되어야 하는지의 여부가 결정되는 순간으로의 전환점"으로 정의하기도 한다.

그러나 일반적으로 위기라는 단어는 "위험한 고비나 시기"라는 의미로 나쁜 상황을 초래할 수 있는 위급한 상황을 가리키는 경우가 더 많다. 실제로 위기라는 단어는 태풍·폭설·홍수 등의 자연재해, 폭발·교통사고·붕괴 등 인적·기술적 재난, 테러리스트들의 공격, 북한 및 외교관계의 실패, 각종 정책의 실패, 기업·가계·국가의 경제적 어려움, 범죄·질병의 확산, 각종 스캔들 등 다양한 상황에서 포괄적인 위험상황을 의미하곤 한다.[12)]

「국가위기관리기본지침」에서는 위기를 "내재된 위험이 표출되어 조직의 핵심 요소나 가치, 존립에 중대한 위해가 가해질 가능성이 있거나 가해지고 있는 상태"로 정의하고 이에 따른 국가위기의 영역을 전통적 안보, 재난, 국가핵심기반 분야로 구분하여 33개의 위기유형을 선정하였다. 전통적 안보(Conventional Security) 위기는 통일, 외교, 군사 등의 분야에서 전쟁이나 외침 등에 의해 영토와 주권이 위협받을 수 있는 국가 위기로 우리나라의 경우는 북한으로부터의 위기와 주변국 등 외부로부터의 위기로 구분할 수 있다. 재난(Disaster) 위기는 전쟁이나 외침의 우려가 없는 대내적 위기이지만 국민의 생명과 재산 및 건강을 심각하게 손상시키거나 파괴할 수 있는 국가위기이다. 핵심기반(Critical Infrastructure) 위기는 국가의 운용 기반으로서 정치·경제·사회·문화의 생명력의 기반이 되는 핵심기반시설, 시스템, 기능 가치를 위협하는 국가위기이다.

12) 장기범, "국가종합위기관리"(법문사), 2009, p.17.

<표 1> 국가위기관리표준매뉴얼 상 33개 위기유형

구 분	위기 유형
전통적 안보(13)	서해 NLL 우발사태, 대통령 권한 공백, 재외국민 보호, 소요·폭동, 파병부대, 우발사태, 테러, 비군사적 해상분쟁 등
재난(11)	풍수해, 지진, 산불, 고속철도 대형사고, 다중밀집시설 대형사고, 대규모 환경오염, 화학물질 유출사고, 지하철 대형사고, 공동구 화재사고, 전염병, 가축질병
국가핵심기반(9)	사이버 안전, 전력, 원유수급, 원전 안전, 금융전산, 육상화물운송, 식·용·수, 보건의료, 정보통신

출처: 장기범, "국가종합위기관리"(법문사), 2009, p.24.

위기관리에 대해서는 그 적용 범위에 따라 그 개념이 다양하나 국가적 차원으로 보았을 때, 위기관리는 재난관리에서 관리의 대상인 자연재난과 인위적 재난 같은 재난 위험뿐만 아니라, 전쟁이나 테러 등 안보의 위협도 고려해야 하는 폭넓은 개념으로 인식된다. 국가적 차원의 위기관리는 "위기로부터 국민의 생명과 재산을 보호해 주고 위험을 극복하기 위한 사업계획을 집행하는 일상화된 과정"으로 정의할 수 있고, 우리나라의 국가위기관리기본지침(대통령훈령 제124호)에서는 국가위기관리를 "국가위기를 사전에 예방하고 발생에 대비하며 위기 발생 시에는 효과적인 대응 및 복구를 통하여 그 피해와 영향을 최소화함으로써 조기에 위기 이전상태로 복귀시키고자 하는 제반활동"으로 정의하고 있다.[13)]

이러한 국가위기관리의 정의는 다음과 같은 요소로 구성된다.

첫째, 국가위기관리의 주체는 국가로서 중앙행정기관은 물론 각급 지방자치단체 등의 위기관리 주관기관, 유관기관, 실무기관을 포함한다. 그리고 국가위기관리에 있어서 국가는 민간부문의 기업과 시민사회단체와의 거버넌스 구축을 통해 협력적 연계활동을 전개한다.

13) 장기범, "국가종합위기관리" (법문사), 2009, pp.33-34.

둘째, 국가위기관리 효과성 확보를 위하여 국가위기를 사전에 발생하지 않도록 예방하고 대비하며 위기발생 시 신속하고 효율적으로 대응하고 복귀함으로써 피해를 최소화, 회복시키는 것을 목표로 설정한다.

셋째, 국가위기관리를 위한 자원으로는 인적자원과 물적자원, 그리고 정보자원·문화자원 등 국가 내·외부에서 가용한 무형자원들을 모두 의미한다.

넷째, 국가위기관리를 위해 국가는 각급 조직들로 하여금 수준별, 기능별, 지역별 특성에 맞는 계획을 수립하게 할 수 있다.

다섯째, 국가위기관리의 조직화는 국가위기관리의 집행계획을 구체적으로 추진하기 위하여 권위의 배분과 작업의 분할을 통하여 업무수행이 잘 조정되도록 공식기구를 설치·조정·개편할 수 있다. 여섯째, 국가위기관리의 효율성 확보를 위해 국가는 각급 기관 및 조직의 성과를 측정하고 평가함으로써 통제할 수 있다.

2. 국가기반시설에 대한 사이버테러 위협

경제협력개발기구가(OECD) 2011년 발간한 '글로벌 미래 쇼크' 보고서에 따르면 지구인의 미래를 위협할 다섯 가지의 글로벌 쇼크[14] 중 하나가 중요한 기반 시설에 대한 사이버 공격이다. 그리고 시장조사업체인 가트너(Gartner)는 "가까운 장래에 G20국가의 주요 핵심 인프라는 온라인 공격으로 파괴되고 피해를 입을 것"이라는 예측을 내놓았고, 저명한 독일의 사회학자 울리히 벡(Ulich Beck)도 "현대사회는 위험사회(Risk Society)로, 위험은 단순한 재앙이 아닌 예견된 잠재적 위험이며 급속한 과학기술 발전, 산업화 등에 주로 기인한다."고 경고했다.

현대 사회는 발달된 정보통신기술로 인해 전 세계 전산망이 서로 연결돼 있어 '디도스(DDos)' 공격과 같은 사이버테러에 취약하고 사이버테러

14) 글로벌 경제에 있어 파괴적인 쇼크(충격)가 앞으로 좀 더 빈번해지고, 더 큰 경제적이고 사회적인 어려움을 가져올 수 있다며 그 요인으로 전염병 대유행, 중요한 기반시설에 대한 사이버 공격, 금융위기, 지구 자기장 폭풍, 사회·경제적인 불안을 꼽았다.

는 자칫 잘못 대응할 경우 전산망 마비 등과 같은 치명적 피해를 입게 되는데, 지난 2007년 개봉한 영화「다이하드 4.0」에서는 고도의 해킹 기술을 이용해 교통, 통신, 금융 등 기반시설을 송두리째 마비시켜 사회를 혼란에 빠지게 만드는 사이버테러를 현실감 있게 보여주고 있다.

최근 사이버테러의 양상이 과거 단순 해킹이나 경제적 이득을 위한 사이버 공격에서 공공기관이나 국가기반시설 등에 대한 타겟형 공격으로 변화되어 가고 있는데, 2010년 이란 부셰르(Bushehr) 원자력발전소에서 발생한 사이버테러가 대표적인 예라고 할 수 있다.

이란 부셰르 원자력발전소 시스템에 '스턱스넷(Stuxnet)'[15]이라는 악성 바이러스가 침투해 우라늄 농축 프로그램을 교란시켜 원심분리기 1,000여대를 고장냈다. 이 바이러스는 부셰르 핵발전소 가동을 앞두고 시설 준공을 맡은 러시아 전문가의 USB메모리를 통해 감염됐다고 한다. 이를 두고 보안 전문가들은 '스턱스넷(Stuxnet)'이 이란 핵발전소를 겨냥해 국가 차원에서 만들어진 고도의 사이버 무기가 틀림없다고 분석했으나, 그 배후에 대해서는 사이버테러의 특성상 추정만 할 뿐 정확하게 밝혀진 사실이 없어 사이버테러가 국가차원의 전략 무기가 될 수 있음을 잘 보여 준다.

사이버테러에 의한 피해 규모는 아래 <표 2>와 같이 자연(인재)재해 규모를 능가하고 국가·공공기관 및 민간기관에 대한 공격뿐만 아니라, 교통, 전기, 수도, 발전소, 공장생산시설과 같은 국가기반의 제어 시스템(PCS, Process Control System)을 감염시켜 오작동을 유발하게 하는 등 심각한 피해를 발생시킨다. 실제 국내에서 2009년도에 발생한 '7·7 DDos 공격'으로 입은 피해는 현대경제연구원 추산으로 최소 363억 원에서 최대 544억 원에 이를 것으로 분석되었는데, 이는 국내 연간 풍수해 피해액과 맞먹는 수준이다.

15) 국가주요 기반 시설을 공격하는 신종 악성코드로, 독일 지멘스사의 산업자동화 제어 시스템을 공격목표로 제작되어 바이러스 코드 안에 'Stuxnet'으로 시작하는 파일 이름이 많아서 '스턱스넷'으로 불리게 되었다.

<표 2> 사이버테러 피해 규모

구 분	사이버테러		인재 및 자연재해		
	1·23 인터넷 대란(2003년)	에스토니아(2007년)	대구 지하철 화재(2003년)	강원도 양양산불(2005년)	연간 풍수해(2008년)
피해액	10억 달러(전 세계)	수천만 달러	614억 원	230억 원	579억 원

출처: 이완석, "주요정보통신기반시설 사이버 위협 및 대응", 한국인터넷진흥원(2010)

따라서 사이버테러는 피해 발생 시 경제적인 피해뿐만 아니라 국가기반시설의 마비 등과 같은 국가적 재난으로 이어질 수 있기 때문에 국가위기관리의 측면에서 논의되어야 할 필요성이 있다.

제4장 국내 사이버테러 대응체계

제1절 사이버테러 대응 법체계

1. 형법상 사이버 테러 관련 처벌규정

형법상 구성요건을 검토해 보면 정보통신망 교란·파괴 및 사이버전쟁과 관련하여 사이버상의 행위에 적용될 수 있는 구성요건은 "손상·은닉·기타 방법으로 효용 해함", "손괴·불통·기타방법으로 방해", "전복·매몰·추락·파괴", "손괴·허위정보입력·부정명령입력·기타방법으로 정보처리에 장애를 발생", "허위정보입력·부정명령입력·무권한정보입력·변경하여 정보처리를 하게 함" 등으로 분류할 수 있다. 이러한 구성요건은 사이버공간 상에서 이루어져 많은 피해양상을 나타낼 수도 있는데, 이 행위로 인하여 국가기관의 기능을

정지하게 하거나(형법 제87조), 교량을 손괴 또는 불통하게 하거나 기타 방법으로 교통을 방해(형법 제185조), 손괴하거나 기타 방법으로 자동차·선박 또는 항공기 등의 교통방해(형법 제186조), 자동차·항공기 등을 전복·매몰·추락·파괴(형법 제187조), 컴퓨터등 정보처리장치 또는 전자기록등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리장치에 장애를 발생하게 하여 사람의 업무방해(형법 제314조 제2항), 전자기록 등 특수매체기록을 취거·은닉 또는 손괴하여 타인의 권리행사 방해(형법 제323조), 전자기록등 특수매체기록을 손괴 또는 은닉 기타 방법으로 기효용을 해함(형법 제366조) 등이 있다.

이러한 행위태양은 국가적 법익, 사회적 법익, 개인적 법익을 침해하는 경우로 나눌 수 있다. 이처럼 형법 상에서는 주요 정보통신망을 교란 및 손괴하여 주요 기반시설을 파괴하거나 장애를 발생하는 등의 행위 유형을 구성요건화 하고 있지만 이를 사이버공간 상에서 명확하게 적용할 수 있는 법규로는 공무소사용 서류 또는 전자기록 및 특수매체기록을 손상·은닉·기타 방법으로 효용을 해함(형법 제141조 제1항), 컴퓨터등 정보처리장치 또는 전자기록 등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해(형법 제314조 제2항), 전자기록 등 특수매체기록을 취거·은닉 또는 손괴하여 타인의 권리행사를 방해(형법 제323조), 컴퓨터등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 권한 없이 정보를 입력·변경하여 정보처리를 하게 함으로써 재산상 이익취득하거나 제3자로 취득(형법 제347조의2), 전자기록등 특수매체기록을 손괴 또는 은닉 기타 방법으로 기 효용을 해함(형법 제366조) 등의 구성요건에 불과하다. 이 가운데 형법상 정보통신망 교란 및 파괴와 관련된 직접적인 조항은 형법 제141조 제1항, 형법 제366조 뿐이다.

또한 사이버공간 상에서 국가의 의사와 관계없이 외국과 전투행위를 벌이고 이것이 무력에 의한 조직적 공격이라면 외국사전행위(형법 제111조)가 성립될 수 있으며, 사이버테러 또는 사이버전쟁을 위하여 특정·다수인

이 계속적인 의사연락 하에 단체를 조직하거나 이에 가입하였다면 범죄단체조직·가입죄(형법 제114조)가 성립될 수 있다. 이러한 사이버상의 테러나 전투를 침해주체로 유형분류하면 국가적 침해 내지 조직적 침해로 구분할 수 있다.[16)]

2. 특별법상 사이버테러 관련 주요 처벌규정 분석

가. 정보통신기반보호법

1) 개 요

정보통신기반보호법은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다(동법 제1조).

이 법에서의 '정보통신기반시설'이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 제1항 제1호의 규정에 의한 정보통신망을 말하며, '전자적 침해행위'라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위이며, 여기서의 '침해사고'란 전자적 침해행위로 인하여 발생한 사태를 말한다(동법 제2조). 정보통신기반보호법은 주요정보통신기반시설의 보호에 관한 심의를 위하여 국무총리 소속 하에 정보통신기반보호위원회를 두고 있으며(동법 제3조), 주요정보통신기반시설의 보호 및 침해사고에 대응하기 위하여 벌칙조항을

16) 윤해성, "사이버침해 유형에 관한 형사법적 검토", 법무연구 제2권, 대한법무사협회 법제연구소, 2011, pp. 244-246.

마련하고 있다.

2) 행위유형과 법정형

정보통신기반보호법의 벌칙조항을 통하여 사이버침해에 대한 행위유형을 도출해 보면, i) 접근권한을 가지지 아니하는 자가 주요정보통신기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위, ii) 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신시설의 운영을 방해할 목적으로 컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위, iii) 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위 등이 있다(동법 제 12 조 참조). 이러한 행위유형은 주요정보통신기반시설을 교란·마비 또는 파괴한 자에 대하여 10 년 이하의 징역 또는 1 억원 이하의 벌금에 처하고 있으며(동법 제 28 조 제 1 항), 미수범도 처벌하고 있다(동법 제 28 조 제 2 항).

3) 검토

정보통신기반보호법에서 '전자적 침해행위'라고 하여 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위라고 정의하고 있는데, 벌칙조항을 검토해 보면 i)의 경우, 주요정보통신기반시설에 접근권한을 가지지 아니하는 자(무권한자)와 접근권한을 가진 자(권한자)가 권한을 초과하여 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위이다. 무권한자(외부자)와 권한자(내부자)로 구분하며, 이들이 데이터를 조작·파괴·은닉 또는 유출하여 정보통신기반시설을 교란·마비 또는 파괴하는 행위에 대하여

처벌하고 있다. 외부자에 의한 대표적인 것이 해킹행위이며, 내부자에 의한 대표적인 것이 조작·파괴·은닉 또는 유출이다. 양자 모두 주요정보통신기반시설의 데이터를 조작·파괴·은닉 또는 유출하려고 행하였다면 고의범이다. ii)의 경우 컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위이고, 이때 데이터를 파괴하거나 운영을 방해할 목적으로 행하였다면 목적범이다. iii)의 경우, 일시에 대향의 신호를 보내거나 부정한 명령을 처리하도록 하여 정보처리에 오류를 발생하는 행위이고, 이때 운영을 방해할 목적으로 행하였다면 목적범이다.

따라서 이를 정리해보면 정보통신기반보호법에서 말하는 전자적 침해행위의 정의 속에 해킹은 i)의 행위이고, 컴퓨터바이러스 및 논리·메일폭탄은 ii)의 행위이며, 서비스거부 또는 고출력 전자기파 등은 iii)의 행위로 대칭될 수 있으며, 해킹은 '고의'가 존재해야 하고, 그밖에 사이버 공격에 대해서는 초과주관적 구성요건인 '목적'을 요하고 있다. 그러나 법정형은 동일하게 규정되어 있는 것을 알 수 있다.

나. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

1) 개 요

동법은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다(동법 제1조). 이 법에서의 '정보통신망'이란 전기통신사업법 제2조 제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집, 가공, 저장, 검색, 송신 또는 수신하는 정보통신체제를 말하며, '개인정보'란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·

문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다. 그리고 '침해사고'란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다(동법 제2조)고 규정하고 있다.

2) 행위유형과 법정형

정보통신기반보호법의 벌칙조항을 통하여 사이버침해에 대한 행위유형을 도출해 보면, i) 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 사실을 드러내어 다른 사람의 명예를 훼손한 행위에 대해서는 3년 이하의 징역이나 금고 또는 2천만 원 이하의 벌금에 처하고 있으며(동법 제70조 제1항), 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 다른 사람의 명예를 훼손한 행위에 대해서는 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만 원 이하의 벌금에 처하고 있다(동법 제70조 제2항 참조).

ii) 개인정보의 수집·이용에 있어 이용자의 동의를 받지 아니하고 개인정보를 수집한 행위(동법 제7조 제1호), 이용자의 동의를 받지 아니하고 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집한 행위(동법 제71조 제2호), 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 행위(동법 제71조 제3호), 이용자의 동의를 받지 아니하고 개인정보 취급위탁을 한 행위(동법 제71조 제4호), 이용자의 개인정보를 취급하고 있거나 취급하였던 자가 이용자의 개인정보를 훼손·침해 또는 누설하는 행위(동법 제71조 제5호), 개인정보가 누설된 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 행위(동법 제71조 제6호),

정보통신서비스 제공자 등은 오류정정의 요구를 받으면 지체 없이 오류를 정정하거나 정정하지 못하는 사유를 이용자에게 알려야 하는데, 이를 위반하여 필요한 조치를 하지 아니하고 개인정보를 제공하거나 이용한 행위(동법 제 71 조 제 7 호), 법정대리인의 동의를 받지 아니하고 만 14 세 미만인 아동의 개인정보를 수집하는 행위(동법 제 71 조 제 8 호), 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 악성프로그램을 전달 또는 유포하는 행위(동법 제 71 조 제 9 호), 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애를 발생하게 하는 행위(동법 제 71 조 제 10)호, 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비민을 침해·도용 또는 누설하는 행위 등은 5 년 이하의 징역 또는 5 천만 원 이하의 벌금에 처하고 있다(동법 제 71 조 제 11 호).

iii) 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하는 행위와 미수범은 처벌하며(동법 제 72 조 제 1 항 제 1 호, 제 2 항), 기망하여 다른 사람의 정보를 수집하거나 다른 사람이 정보를 제공하도록 유인하여 다른 사람의 개인정보를 수집하는 행위(동법 제 72 조 제 1 항 제 2 호), 직무상 알게 된 비밀을 타인에게 누설하거나 직무 외의 목적으로 사용하는 행위(동법 제 72 조 제 1 항 제 5 호) 등은 3 년 이하의 징역 또는 3 천만 원 이하의 벌금에 처하고 있다(동법 제 72 조 참조)

iv) 정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영, 접속기록의 위조·변조 방지를 위한 조치, 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치, 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치 등 기술적·관리적 조치를 하여야 하는데, 이에 따른 기술적·관리적 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·누출·변조 또는 훼손하는 행위(동법 제 73 조 제 1 호), 청소년유

해매체물임을 표시하지 아니하고 영리를 목적으로 제공하거나(동법 제 73 조 제 2 호), 청소년유해매체물을 광고하는 내용의 정보를 청소년에게 전송하거나 청소년 접근을 제한하는 조치 없이 공개적으로 전시하는 행위(동법 제 73 조 제 3 호), 방송통신위원회는 침해사고의 원인을 분석하기 위하여 필요하다고 인정하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 정보통신망의 접속기록 등 관련 자료의 보전을 명할 수 있는데 이에 따른 명령을 위반하여 관련 자료를 보전하지 아니한 행위(동법 제 73 조 제 4 호 및 제 5 호), 정보통신망을 통하여 속이는 행위로 다른 사람의 정보를 수집하거나 다른 사람이 정보를 제공하도록 유인하여서는 아니 되는데, 이를 위반하고 개인정보의 제공을 유인하는 행위(동법 제 73 조 참조)

v) 정보통신망을 통하여 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시하는 내용의 정보를 유통하는 행위(동법 제 74 조 제 1 항 제 2 호), 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하게 하는 행위이며, 이 행위는 피해자가 구체적으로 밝힌 의사에 반하여 공소를 제기할 수 없다(동법 제 74 조 제 1 항 제 3 호 및 제 2 항). 또한 인터넷 홈페이지 운영자 또는 관리자의 사전 동의 없이 인터넷 홈페이지에서 자동으로 전자우편주소를 수집하는 프로그램이나 그 밖의 기술적 장치를 이용하여 전자우편주소를 수집·판매·유통하거나 정보 전송에 이용하는 행위(동법 제 74 조 제 1 항 제 5 호), 불법행위를 위한 광고성 정보 전송금지행위(동법 제 74 조 제 1 항 제 6 호) 등에 대해서 1 년 이하의 징역 또는 1 천만 원 이하의 벌금에 처하고 있다(동법 제 74 조 참조)

3) 검 토

동법에서는 '개인정보'를 보호하고 정보통신망을 보호하기 위한 여러 가지의 대책을 담고 있다. 개인정보와 관련해서는 사람을 비방할 목적으로

정보통신망을 이용하여 진실한 사실 및 허위의 사실을 통하여 명예를 훼손하는 행위에 대하여 처벌하고 있으며, 형법과 달리 반의사불법죄로 규정하고 있다. 또한 부정한 방법으로 개인정보를 수집하거나(동법 제 71 조 제 1 호, 제 2 호, 제 8 호, 제 72 조 제 1 항 제 2 호), 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받거나(동법 제 71 조 제 3 호, 제 6 호) 제공한 행위(동법 제 71 조 제 7 호, 제 73 조 제 2 호), 제공을 유인하는 행위(동법 제 73 조 제 7 호)가 있다. 그리고 타인(이용자)의 개인정보를 훼손(도용)·침해 또는 누설하는 행위(동법 제 71 조 제 5 호 및 제 11 호, 동법 제 72 조 제 1 항 제 5 호)와 개인정보를 분실·도난·누출·변조 또는 훼손하는 행위(동법 제 73 조 제 1 호)가 있으며, 유해정보 및 전자우편주소, 광고성 정보 등을 전송 또는 공개적으로 전시하는 행위(동법 제 73 조 제 3 호, 제 74 조 제 1 항 제 1 호 및 제 5 호, 제 6 호)를 규제하는 규정이 있다.

‘침해사고’에 대해서는 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태라고 정의하고 있다(동법 제 2 조 제 1 항 제 7 호). 벌칙조항 가운데 이와 관련된 규정을 검토해 보면, i) 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 악성프로그램을 전달 또는 유포하는 행위(동법 제 71 조 제 9 호), ii) 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애를 발생하게 하는 행위(동법 제 71 조 제 10 호), iii) 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하는 행위가 있으며 이때 미수범은 처벌규정이 있다(동법 제 72 조 제 1 항 제 1 호, 제 2 항).

따라서 이를 검토해 보면 정보통신망 이용촉진 및 정보보호 등에 관한 법률에서 말하는 ‘침해사고’의 정의 속에 해킹은 iii)의 행위로 대칭될 수 있고, 해킹은 ‘고의’가 존재해야 하며, 동법에 의하면 미수범은 처벌하게 된다. 그리고 컴퓨터바이러스, 논리폭탄, 메일폭탄은 i)의 행위이며, 서비스거

부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 정보시스템을 공격하는 행위는 ii)의 행위로 대칭할 수 있다. 그러나 법정형은 동일하게 규정되어 있지 않은 것을 알 수 있다. 따라서 이 법에 의하면 해킹은 미수범 규정이 있음에도 가장 적은 법정형으로 규정되어 있는 반면, 악성프로그램 전달·유포와 정보통신망에 장애를 발생한 행위는 높게 처벌하고 있는 것을 알 수 있다.

다. 사이버테러 관련 특별법 규정 검토

특별법 상의 처벌규정은 정보통신망 보호(국가의 안전, 국민경제의 발전 및 생활안전보장 포함) 관련 규제와 개인정보보호 관련 규제, 그리고 양자 모두 규제하는 법률로 분류할 수 있다. 먼저 정보통신망 보호 관련 특별법으로는 「정보통신기반보호법」, 그리고 정보통신망 보호와 개인정보보호 관련 특별법으로는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등이 있다.

행위유형 가운데 정보통신망 보호와 관련하여 정보통신망 보호와 관련하여 정보통신망 교란 및 파괴 등의 행위로는 “접근권한을 가지지 아니하는 자가 주요정보통신기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위(해킹 행위)”, “주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신시설의 운영을 방해할 목적으로 컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위”, “주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위(서비스 거부 또는 고출력 전자기파)”, “정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 악성프로그램을 전달 도는 유포하는 행위(컴퓨터바이러스, 논리폭탄, 메일폭탄)”, “정보통신망의 안정적 운영을 방해할

목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애를 발생하게 하는 행위(서비스거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 정보시스템을 공격)", "정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하는 행위(해킹)", "신용정보전산시스템의 정보를 변경·삭제하거나 그밖의 방법으로 이용할 수 없게 하거나 권한 없이 신용정보를 검색·복제하거나 그밖의 방법으로 이용한 행위" 등이 있다.

주관적 구성요건과 관련하여 보면 해킹의 경우 고의를, 컴퓨터바이러스, 논리·메일폭탄과 서비스거부 또는 전자기파 등은 목적으로 요구하는 법규정 형식을 볼 수 있었다. 특히 목적과 관련해서 보면 "주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신시설의 운영을 방해할 목적", "주요정보통신기반시설의 운영을 방해할 목적", "외국에서 사용하거나 사용되게 할 목적", "행정정보의 처리업무를 방해할 목적", "공공기관의 개인정보처리업무를 방해할 목적", "정보통신망의 안정적 운영을 방해할 목적" 등이 있다.

특별법상에 나타난 각각의 개념을 정보통신망과 관련하여 살펴보면, '정보통신기반시설'이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 제1항 제1호의 규정에 의한 정보통신망을 말하며, '전자적 침해행위'라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위이며, 여기서의 '침해사고'란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다(정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조). '정보통신망'이란 전기통신기본법 제2조제2호에 따른 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터 이용기술을 활용하여 정보를 수집·가공·검색·송신 또는 수신하는 정보통신체제를 말하며, '정보시스

템'이란 정보의 수집·가공·저장·검색·송신·수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계를 말한다(동법 제2조).

라. 소 결

한국의 경우, 사이버테러 범죄의 역기능에 대처하기 위한 방안으로 각 부처별로 상황에 따라 필요할 때마다 특별법을 제정하는 방법을 선택했다.[17] 그 이유는 그간 정책입안자 및 입법자가 사회현실의 변화에 따라 새로이 등장하는 범죄현상에 대해 충분한 형법이론적·형사정책적 고민 없이 진압위주의 강경한 법정책 기조 위에 임기응변식으로 손쉽게 법을 만들어 적용해온 데에 있다.[18] 이러한 정부의 대처방법은 각 법률 간 형벌의 불균형, 법체계상의 문제, 다수의 유사한 규정이 여러 법률에 산재되어 있는 문제점 등을 야기하였다.[19]

실무적으로는 해킹, 디도스, 피싱, 악성프로그램 유포와 관련된 범죄는 모두 정보통신망법, 정보통신기반보호법으로 처벌하고 있으므로, 사이버테러와 관련하여 특별법을 제정할 경우에는 오프라인 범죄체계와 균형, 첨단기술의 특성을 고려한 법절차적 조항 신설, 온라인서비스제공자의 책임조항 신설, ISP에 대한 정보통신망에 대한 기술적 대응장치 의무화, 보호관찰·사회봉사명령·수강명령 제도 도입 등을 고려해야 할 것이다.[20]

아울러 보호법익과 법정형 및 용어에 있어 기존 형벌법규와의 체계성을 잃지 않는 선에서 법제를 마련하는 것이 중요하다.[21]

제2절 국가 사이버안전 관리체계

17) 유석준, "사이버범죄에 대한 외국의 입법례", 영산법률논집 제5권 제1호, 2008, p.1.
18) 서보학, "인터넷상의 정보유포와 형사책임", 형사정책연구 제12권 제3호, 2001, p.10.
19) 유석준, "사이버범죄에 대한 외국의 입법례", 영산법률논집 제5권 제1호, 2008. p.2.
20) 곽병선, "사이버범죄 예방을 위한 법제도적 해결방안 - 가칭 '사이버범죄 특별법' 제정논의를 중심으로 -", 법학연구 제24집 제3호, 원광대학교 법학연구소, 2008, pp.132-136.
21) 강동범, "정보통신망법상 사이버범죄처벌규정의 검토", 인터넷법률 제39호, 법무부, 2007, p.50.

1. 사이버테러 관련 법적 근거

사이버테러와 관련하여 한국은 2001년 정보통신기반보호법이 제정되면서 정보통신기반시설[22]에 대한 침해사고 대응체계가 처음으로 구축되었고, 2001년 초 (구)한국정보보호진흥원(KISA)의 인터넷침해사고 대응지원센터와 국가정보원의 국가사이버안전센터, 국방부의 정보전대응센터 등 사이버안전 기관들을 설립하여 국가안보회의(NSC) 중심의 대비체계를 마련하였다.[23]

이후 2004년 국가기관 해킹사건을 계기로 2005년에 국가사이버안전관리규정이 대통령 훈령으로 제정되면서 우리나라에 사이버테러 대응에 관한 규정이 처음으로 법제화되었다. 2006년 당시 「사이버위기 예방 및 대응에 관한 법률안」이 발의되었으나, 특정기관에 대한 과도한 권한집중, 시민단체의 반발, 부처 간 합의 실패 등의 이유로 입법화되지 못하고 국회 회기 종료와 함께 폐기되었다.

반면, 군의 경우에는 2009년 북한발 「7.7 DDos 사건」 등의 영향으로 2010년 1월 국회에서 「국방정보화 기반조성 및 국방정보자원 관리에 관한 법률」을 제정하였고, 국방정보본부에 '사이버사령부'를 신설하여 정보사령부, 제777부대 등과 함께 배속하는 등 입법화를 완료하였다.[24]

2. 사이버테러 대응 체계

한국의 국가 사이버테러 관련 대응 체계는 한국인터넷진흥원의 '인터

22) 정보통신기반보호법 제2조 제1호에 의하면 "국가안전보장.행정.금융.치안.통신.운송.에너지 등의 업무와 관련된 전자적 제어.관리시스템 및 정보통신망이용촉진및정보보호등에관한법률 제2조제1항제1호의 규정에 의한 정보통신망을 말한다."고 정의되어 있다.

23) 윤해성, 강석구, 박영우, 김민호, 권헌영, 김도승, 김기범, "사이버안전체계 구축에 관한 연구", 형사정책연구원 연구총서 10-07, 2010, p.67.

24) "2010 국가정보화백서", 2010, p.171.

넷침해대응센터'가 민간분야를 담당하고, 국가정보원 소속의 '국가사이버안전센터'가 공공분야를 담당하며, 국방정보본부 산하의 '사이버사령부'가 군 분야를 담당하는 민·관·군 종합 대응체계이다.[25] 이와 별도로 경찰청과 대검찰청은 사이버 테러에 대한 범죄수사를 전담하고 있다.

경찰청 사이버수사 조직은 2000년 수사국 소속 '사이버테러대응센터'로, 2014년에는 '사이버안전국'으로 확대되어 오늘에 이르고 있다. 지방경찰청은 2000년에 전국적으로 사이버범죄수사대를 창설하였고, 2007년에 전국 경찰서 1급지에 사이버범죄수사팀을 설치하여 전국적인 수사체제를 구축하였다. 또한 경찰청에서는 중앙 단위에 별도의 수사조직을 운영하고 있는데, 주로 사이버테러 대응, 국제공조수사를 하고 있고, 지방경찰청은 개인정보 유출, 음란·도박사이트 단속 등 인지수사를 하고 있으며, 경찰서는 인터넷 사기, 사이버명예훼손, 디지털 저작권 침해, 음란물 유포 등을 수사하고 있다.[26]

3. 국가 사이버안보 마스터플랜

2011년에 북한에 의해 정부기관 및 민간의 홈페이지가 마비(3·4 디도스 공격)되고, 농협 전산망이 해킹을 당해 전산망이 마비되는 사건을 경험하면서 국가정보원을 중심으로 "국가 사이버안보 마스터플랜"을 새롭게 수립하게 되었다. 마스터플랜에는 각종 사이버위협에 총력 대응할 수 있도록 '국가사이버안전센터'를 중심으로 관계 부처 간 협력공조와 민간전문가 참여를 확대해 나가는 한편, 국정원의 컨트롤타워 기능과 부처별 역할을 명확히 하여 기관간의 업무 혼선 및 중복을 최소화하도록 노력하였다. 사이버공간을 영토·영공·영해에 이어 국가가 수호할 또 하나의 영역으로 선언하고, 이를 위해 5대 분야(예방, 탐지, 대응, 제도, 기반)의 중점 전략과제를 선정

25) 윤해성, 강석구, 박영우, 김민호, 권헌영, 김도승, 김기범, "사이버안전체계 구축에 관한 연구", 형사정책연구원 연구총서 10-07, 2010, p.79.
26) 윤해성, 강성구, 박영우, 김민호, 권헌영, 김도승, 김기범, "사이버안전체계 구축에 관한 연구", 형사정책연구원 연구총서 10-07, 2010, p.130.

하였다.

4. 기능과 역할 재정립

사이버테러에 관해서는 정보통신망법, 정보보호기반보호법, 전자정부법, 국가사이버안전관리규정(대통령령) 등 다수의 법률이 규제하면서 기관간 임무가 중첩되는 경우가 발생하기도 한다. 따라서 다양한 기관이 존재하고 있음에도 실제 사이버위기가 발생하였을 경우 각 기관의 책임과 역할이 불분명하다.[27] 특히 사이버 테러는 정치·사회적 동기가 파악되어야 하고, 사이버전은 공격을 감행하는 국가가 특정되어야 하는데, 추적과 조사를 선행하지 않고는 알아낼 수 없다. 그러나 경찰은 범죄의 의심이 있다면 국가적인 문제인지, 사적인 문제인지, 혹은 테러공격인지, 금전적 이익 목적인지, 심지어 국가정보를 탈취하기 위한 것인지 등에 관계없이 개입이 정당화되기 때문에 사고대응에 있어 정당성을 가질 수 있다.[28]

이에 경찰은 사건 초기에 적극적으로 참여하여 사실관계를 정확히 밝히는 노력을 하고, 밝혀진 사실을 유관부서에게 적시에 통보하여 필요한 조치를 취할 수 있도록 긴밀한 협력 체제를 구축해야 한다.

제3절 사이버테러 대응체계의 문제점

1. 초기 대응과 다양한 법규로 인한 대응체제 혼선

가. 체계화된 법률의 부재

27) 김도승, “사이버위기 대응을 위한 법적 과제: 미국의 사이버위기 대응체계 현황과 시사점을 중심으로”, 방송통신정책 제21권 제17호, 정보통신정책연구원, 2009, 참조

28) 이동희 외, “국제 사이버범죄 아카데미 모델 개발”, 경찰청, 2010, p.19.

사이버 테러의 특징 상 발생 초기에는 개인인지, 조직인지, 국가인지 확인이 되지 않는다. 따라서 군이나 정보기관이 초기에 나서는 것은 부담스럽다고 한다. 이러한 면모는「 3·3 디도스공격」, 「7·7 디도스공격」이 모두 북한의 소행이었어도 군의 수사가 아닌 수사기관이 수사를 진행해야 한다는 모순에 직면한다. 당시 언론에서는 사이버사령부는 북한의 공격이 있음에도 역할을 못하고 있다는 비난이 있었다.

아울러 이러한 초기 대응의 문제점과 관련하여 현행 사이버테러 대응에 관한 법제는 정보통신망법, 정보통신기반보호법, 국가사이버안전관리규정(대통령 훈령) 등에 산재되어 있는 실정이다. 이러한 체계 하에서는 정보통신망법은 민간, 정보통신기반보호법은 정보통신기반시설, 국가사이버안전관리규정은 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망을 관리 대상으로 규정하면서 체계적인 대응을 어렵게 하고 있다. 또한 국가사이버안전관리규정 제3조에 의하면 “이 훈령은 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망에 대하여 이를 적용한다. 단, 정보통신기반보호법 제8조의 규정에 의하여 지정된 주요정보통신기반시설에 대해서는 적용하지 아니한다.”고 규정하고 있다. 이러한 한국의 사이버테러 대응체계는 대통령 훈령으로 규정되어 있어서 유관부처 간 역할과 책임이 불분명하고 구속력이 약할 뿐만 아니라 상위 법률과 충돌이 발생하면서 많은 한계를 드러내고 있다.

나. 초기 위협측정 체계 미흡

사이버공간의 위협은 시각적으로 측정되지 않고, 국가가 민간 시스템에 접근하는 것도 어려워 측정하는데 어려움이 있다. 또한 각종 법률에 사이버공격 및 침해사고가 발생하였을 때 국가정보원이나 방송통신위원회 등에 신고하도록 규정되어 있으나, 이러한 신고들이 수사기관으로 전달되지 않고 사장됨에 따라 사이버위협이 제대로 측정되고 있지 않다. 이러한 침해

사고 및 사이버공격을 접수하는 부처에서 예방조치만 취함에 따라 위협 상황이 제거되지 못하고 잠재되어 있는 실정이다.

다. 사이버공격 초기 귀속의 한계

사이버공간에서는 사이버공격의 실체를 확인하기 어려워 특정 공격이 어떤 침해행위에 속하는 것인지를 파악하기 힘들다는 문제점이 존재한다.[29] 즉, 사건 발생 초기에는 사이버테러 주체가 개인인지, 조직인지, 국가인지 확인하는 것이 어렵다.[30] 따라서 사이버테러의 주체가 적국으로 확인되지 않는 상황에서 군이나 정보기관이 나서는 것은 부담스러울 수밖에 없다. 반면 수사기관은 공격주체가 누구이든 상관없이 개입할 수 있다는 장점이 있다. 실제 2009년 「7·7 디도스 공격」이나 2009년 「3·3 디도스 공격」 역시 모두 북한의 소행이었지만 군 또는 정보기관이 아니라 수사기관이 추적, 수사하여 확정 발표한 사례를 보면 알 수 있다.

이러한 점에 비추어 사이버테러 대응에 관한 법령 및 종합대책에는 국정원과 방통위 등의 역할이 중심적으로 기술되어 있을 뿐, 수사기관의 역할에 대해 구체적으로 기술되어 있지 않다. 반면 2003년 발표된 미국의 '사이버공간 보안 국가전략(The Natioanl Strategy to Secure Cyberspace)'에 의하면 법집행기관과 국가안보 공동체는 사이버스페이스의 공격을 예방하는데 중요한 역할을 수행하는데, 법집행기관은 형사법적 권한을 집행함으로써 공격의 귀속에 중심 역할을 하는 등 법집행기관의 역할을 중요시하고 있다.[31]

2. 정보기관과의 협력 및 법집행기관의 참여 미흡의 한계

29) 김기범, 장윤식, "사이버범죄수사론", 경찰대학, 2012, p.89.

30) 귀속이 어려운 이유는 기술적인 측면에서 공격자의 추적의 어려움, 위장이나 우회의 용이함, 인터넷정보의 신뢰성 부족 등이 있고, 기술외적인 문제로는 국외정보 추적의 법적 어려움이나 자발적 협조나 획득의 곤란성 등이 있다. 김기범, 장윤식, "사이버범죄수사론", 경찰대학, 2012, p.89.

31) 김기범, 장윤식, "사이버범죄수사론", 경찰대학, 2012, p.89.

사이버테러의 문제는 결국 사이버안전 문제와 직결된다. 그러나 우리나라의 경우 정보기관이 정책집행에 참여하고 있는데, 이는 i) 부처와 정책경쟁 발생, ii) 정보기관의 특성상 정보공유 한계, iii) 정보기관 활동의 법률적 근거 미흡, iv) 국제협력 역량의 한계가 지적될 수 있다. 따라서 수사기관에 범죄첩보 제공 등의 원활한 협력관계를 구축하지 않는 한 여러 가지 문제점과 한계가 지적될 수밖에 없다.

아울러 외국의 국가 사이버범죄 대응정책, 사이버안전 정책 등에서는 법집행기관이 중요한 핵심 포스트 역할을 수행하고 있다. 하지만 우리나라의 사이버안보 마스터플랜에서는 경찰의 역할이 거의 규정되어 있지 않다. 이러한 문제점은 자칫 사이버안전 대응에 있어서 추적·검거라는 한 축이 사실상 누락되어 있기 때문에 입체적인 대응체제에 한계가 있을 수 있다.

3. 공공·민간·군 기능별 대응체제로 신속대응 한계

사이버공격 대상은 국가·공공, 민간, 국방을 가리지 않는다. 사이버테러는 영역을 불문하고 발생하고 있으나 기능별로 대응하고 있어서 신속대응에 한계가 있다. 이에 대하여 컨트롤 타워(Control Tower)에 대한 주장이 제기되었고, 대통령실에 비서관이 신설되기도 하였지만 정책 조정에는 한계가 있다. 별도의 사이버안전청, 사이버보안청 등과 같은 부서의 신설도 고려해야 할 것으로 보인다.

아울러 국가가 정책을 주도하면서 민간은 소극적 참여자로 전락하고 있다. 민간 스스로가 주도적으로 사이버테러를 방지하고 사이버안전을 확보할 수 있는 사회적 동력이 부족한 실정이다. 오프라인 범죄예방은 주로 경찰관과 순찰차의 몫이며, 법률로 규제한다. 반면 최근 카카오톡·포스단말기·메신저 피싱 등과 같은 경우를 보면, 온라인 범죄예방은 특정기업의 시스템을 개편함으로써 즉시 범죄예방의 성과를 낼 수 있다. 다시 말해서 사이버

테러는 인터넷망 위에서 이루어지는 것이고 이러한 망을 관리하는 기업이나 민간이 협력해 준다면 많은 부분 사이버테러 범죄 예방이 용이해질 수 있다.

제5장 독일의 사이버테러 대응체계

제1절 독일에서 이해하는 사이버공간에서의 사이버위협과 사이버보안

독일은 사이버전쟁, 사이버범죄 또는 사이버테러에 대한 새로운 도전에 직면해 있는 고도의 네트워크화 된 사회이며, 이러한 위협은 사이버공간의 존재로부터 유래한다. 이러한 위협들로부터의 보호를 위해서는 사이버보안이 핵심적 역할을 수행하는 바, 독일에서 이해되는 이러한 개념들에 대한 정의, 설명을 알아보기로 한다.

1. 사이버공간

사이버공간이라는 개념은 이미 1980년대 윌리엄 깁슨(William Gibson)의 공상과학소설에서부터 존재하였다. 이후로 그 개념은 세계적인 컴퓨터 네트워크의 결합으로 생성된 상호작용 공간을 칭하기 위해 저널리스트들이나 학자들에게 전수되었고, 오늘날에는 매우 광범위하게 사용된다.

일반적으로 독일에서는 사이버공간이란 “정보기술(ICT, information and communication technology) 시스템, 네트워크 그리고 온·오프라인을 불문하고 이러한 시스템이나 네트워크에 포함된 정보”라고 이해된다.[32] 정보기술은 자신의 능률적이고 이용 창출적인 능력 안에서 지속적으로 발전됨으로써 거의 모든 기술적 시스템이 통합되고, 디지털화를 가속화하는 중

32) Tessier-Stall, “The future of cybersecurity”, The Hague Centre for Strategic Studies and TNO, 2011, p.9.

요한 요인이 되는 것을 말한다.[33] 사이버공간이란 정보를 네트워크화 된 정보시스템에 저장하거나 교환하기 위하여 신호교환 목적의 전기 및 전자기적 스펙트럼의 이용으로 특정되는 영역을 말한다. 여기서 네트워크화 된 정보시스템은 물리적인 인프라를 필요로 한다. 네트워크는 공공성을 띄는지, 또는 사적으로 운용되는 것인지를 불문하고 유리섬유나 무선통신을 통해 구성되며, 이를 통해 형성되는 사이버공간은 전 지구적 상호작용 공간이라고 할 수 있다.[34]

2. 사이버위협

정보기술과 통신기술을 통해 공공부문 및 사부문 이용자들의 사이버 상호의존성이 발생하며, 이러한 기술의 이용은 전 세계적으로 증가되어 왔고, 사회에서 핵심적인 의미를 가지게 되었다. 이를 통해 정보통신기술 시스템은 파괴를 목표로 하는 사이버공격의 매력적인 목표물이 될 수밖에 없다. 이러한 시스템에 대한 사이버공격은 사회의 안전에 심각한 손해를 끼칠 수 있기 때문에, 사이버 상호의존성에 기반한 취약한 정보통신시스템은 중대한 위기로 인식된다. 사이버 상호의존성은 향후 더 가속될 것이며, 이에 따라 사이버공격 또한 증가할 것으로 전망된다. 사이버공격은 국가적 차원의 대상뿐만 아니라 비국가적 차원의 대상 또한 목표로 삼는다. 이러한 공격이 항상 목표지향적인 것은 아니며, 그 영향력은 지속적으로 확대될 것으로 전망된다.[35] 결과적으로 사이버공격은 그 방법에 있어서 어떤 목적을 추구하고, 그 공격을 통해 어떤 작용을 미칠 것인가에 따라 달라지게 될 것이다. 사이버공격은 이를 실행하는 그룹이나 개인 등의 실행주체에 따라 그 양상이 달라지며 사이버 행동가, 사이버 테러리스트, 사이버 범죄 또는 해

33) Das Lage der IT-Sicherheit in Deutschland 2014, Bundesamt fur Sicherheit in der Informationstechnik, 2015, p.7.
34) Hansel, M, “Interantioanle Beziehungen im Cyberspace. Macht, Institutionen und Wahrnehmung”, 2013, p.34.
35) Das Lage der IT-Sicherheit in Deutschland 2014, Bundesamt fur Sicherheit in der Informationstechnik, 2015, p.15.

외 정보기관 등이 이와 결부될 수 있다. 결과적으로 사이버공격의 내용과 효과는 개별 사안에 따라 다양하게 나타날 수 있으며, 기업들의 경쟁력을 장기적으로 약화시키고 이로써 사회 전체가 악영향을 받을 수밖에 없는 '기업들에 대한 해외 정보기관의 사이버스파이'일 수도 있고, 또는 전체 사회에는 별 영향이 없는 것, 예를 들자면 사적인 개인 신용카드 정보에 관계된 것일 수도 있다.

사이버공격이란 IT 안전을 파괴하기 위해 하나 또는 많은 다른 IT 시스템을 목표로 갖는 사이버공간에서의 IT 공격이라고 정의할 수 있다. 사이버스파이, 사이버범죄, 사이버사보타지, 사이버테러리즘 그리고 사이버 전쟁은 사이버공간에서 심대한 손해를 초래할 수 있는 사이버위협에 속한다. 이에 반해 사이버행동주의와 사이버반달리즘은 그 손해 가능성이 상대적으로 낮다고 볼 수 있다.[36] 사이버위협의 종류는 다음과 같이 분류할 수 있다.

가. 사이버범죄

사이버범죄는 인터넷, 데이터네트워크, 정보기술시스템 또는 그 데이터를 목표로 삼아, 이러한 정보기술을 통해 행해지는 범죄행위를 말한다. 근래에는 기업들을 목표로 삼는 사이버범죄 산업마저 나타나고 있는 실정이다.[37] 2014년 독일에서는 10개 중 4개의 기업이 사이버범죄 피해를 입은 것으로 파악되며, 이러한 해커공격들은 조직적인 범죄, 경쟁기업들, 그리고 해외정보기관의 소행이라고 여겨진다.[38]

나. 사이버스파이

36) Kullik, J, "Vernetzte (Un-)Sicherheit? Eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik", 2014, pp.43-69.
37) Sievers, U, "BSI: Der Cyberraum ist ein großes Haifischbecken", 2013, Ingenieur.de
38) Corporate Trust Business Risk & Crisis Management GmbH, "Studie: Industriespionage 2014, 2015, p.3.

IT 시스템의 신뢰성을 타겟으로 하는 사이버공격이 알려지지 않은 정보기관으로부터 수행된 경우, 이를 사이버스파이 또는 사이버엿보기(Cyber-Ausspähung)라고 한다. 2015년 6월 독일연방의회에 대한 대규모 사이버공격이 감행되었으며, 이를 통해 상당히 민감한 정보들이 유출되었다. 이 사건 조사 과정 중 미디어에서는 이것이 러시아 정보기관 FSB에 의한 사이버스파이인 것으로 보도하였는데, 미디어의 이러한 추정은 아직까지 공식적으로 확인되지 않고 있으며, 공개적인 증거 또한 없는 상태이다.

사이버스파이는 독일 경제와 매우 밀접하게 관련된 문제이다. 이는 독일 산업의 혁신적 우위를 위협하는 결과를 야기한다.[39] 선도적 산업국인 독일로서는 산업의 혁신성이라는 가치를 결코 포기할 수 없는데. 이를 통해 성장, 복지 그리고 일자리를 보장할 수 있기 때문이다. 근래 독일 기업들은 이미 산업스파이로 인해 수백 만 유로의 손실에 시달리고 있다.[40]

다. 사이버사보타지

IT 시스템의 무결성과 이용가능성에 대한 사이버공격을 사이버사보타지라고 하며, 이는 취약인프라에 대한 공격과 이를 통해 나타나는 사회의 심각한 위험을 전제로 한다. 사이버스파이와 사이버사보타지는 대체로 서로 연관되어 있으며, 테러리스트들이 IT 공격을 범하기 위해 사용할 가능성이 있다.[41]

라. 사이버전쟁

39) Schnaas, D, “Die Angst vor der Innovationsperipherie. Wirtschaftsspionage ganz neuer Qualitat gefahrdet den Vorsprung des Westens”, Internationale Politik, 2014, p.8.

40) Heeg, T, “Cyberkriminalitat. Deutsche Firmen erleiden Milliardenschaden”, Frankfruter Allgemeine, 2015.

41) Kullik, J, “Vernetzte (Un-)Sicherheit? Eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik“, 2014, p.67.

사이버전쟁에 대한 명확하고 통용되는 정의는 아직 없는 상태이며, 사이버범죄와의 구분 또한 모호한 경우가 많다. 미디어에서는 사이버전쟁을 종종 컴퓨터, 컴퓨터 기술 그리고 인터넷이 이용되는 모든 종류의 사건들이라는 개념으로 설명하고 있으며, 아직 현실에서는 발생한 적이 없지만 '사이버 수단'을 통한 전쟁의 상태를 설명한다는 점에서만 오직 사이버범죄와 명확히 구분될 뿐이다.[42] Tassilo Singer에 따르면 그 개념은 더 나아가 사이버작전(Cyberoperation)을 포함하는 사이버전투(Cyberwarfare)로 이해되어야 하며, 이는 사이버공간 내부뿐만 아니라 외부 또한 특정 목적을 달성하기 위하여 이용하는 하는 것을 말한다. 이 경우에 있어서는 전쟁수행 관련 국제법이 적용되어야 한다. 그러나, 사이버전쟁이 시민권(Völkerrecht)을 기초로 한 무장 충돌이라고 평가되기 위하여, 또한 이에 대해 어떻게 법적으로 규율되어야 하는지를 판단하기 위해서는 어떠한 기준에 따라 사이버전쟁을 정의해야 할 것인지에 관한 다툼의 여지가 있다.[43] 독일연방의회는 2011년 "사이버 공격이란 오직 그것이 그 효과에 있어 이미 무장충돌의 수준이라고 볼 수 있고, 전통적인 무기와 비견될 수 있는 경우에 한하여 시민권적 의미에서의 무장공격으로 분류할 수 있다"고 설명하였다.[44] 그러나 이 정의 또한 어떻게 그 효과가 측정될 수 있으며, 어떠한 방법으로 전통적인 무기와 비교할 수 있는지에 대한 의문을 남긴다. 2015년 미디어를 통해 알려진 연방의회에 대한 사이버공격의 과정에서, 그 사건이 NATO동맹의 자동군사개입의무를 발생시키는지 여부에 관해 의문을 제기하는 보도들이 있었다. 이러한 사실은 그러한 새로운 종류의 현상들

42) Singer, T, "Cyberwarfare? Damoklesschwert fur das Volkerrecht?", Sicherheit & Frieden, 2014, p.17.

43) Bendiek, A, und Ulmer, K, "Cybersicherheit - eine facettenreiche politische Herausforderung. Aus internationale Zeitschriften 2012/2013". SWP-Aktuell 3. Stiftung Wissenschaft und Politik. 2013, p.1.

44) Deutscher Bundestag, "Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Agnes Malczak, Omid Nouripour, Tom Koenigs, weiterer Abgeordneter und der Fraktion BUNDNIS 90/DIE GRUNEN - Drucksache 17/6802", 2011, p.4. http://dipbt.bundestag.de/doc/btd/17/069/1706971.pdf

에 알맞은 정의와 평가가 필요하다는 점을 명확히 해 주고 있다. 어쨌건 그러는 사이에 사이버공간이 영토, 영공, 바다 그리고 우주에 이어 제5의 영역이라는 새로운 입지를 구축한 것만은 확실해 보인다.

사이버공격으로 인한 군사적 방어라는 실제적인 사건은 아직은 일어나지 않았지만, 독일 또한 사이버전쟁이라는 위협의 형태에 직면해 있는 상황이며, 만약 실제로 그런 사건이 발생한다면 독일군이 그 방어를 관할하게 될 것이다. 여기에는 사이버방어의 능력을 보유하고 있는 전략지휘소(KSA, Kommando Strategische Aufklärung), 그리고 독일 정보기관 중 하나이며 독일군 내에서 사이버공격 방어를 관장하는 군사방어청(MAD, Militärischen Abschirmdienst)이 있다.

마. 사이버테러리즘

사이버테러리즘이란 사이버공간에서의 테러 그룹에 의한 스파이나 사보타지를 통한 사이버공격을 말한다. 테러리스트들에게는 아직까지는 사이버공간에서 심각한 결과를 일으키는 테러공격을 수행하기 위해 필요한 재정적, 기술적 수단 및 필수 노하우가 부족한 것으로 보인다. 더 나아가 필수 자원과 전문지식 교환은 테러리스트들에게는 자신의 신원을 발각되게 하는 위험요인이 된다. 그럼에도 불구하고 사이버공격의 위험은 테러 그룹들의 공격력 강화와 연합을 통해 증가될 수 있다. 더 나아가 테러 그룹들의 사이버능력이 강화되는 것을 상정해 볼 수 있는데, 테러리즘이 만일 사이버공간으로 전이되게 된다면 많은 국가들과 심각한 관련성을 가지게 되며, 사이버공간에서의 또 하나의 911테러마저 우려되는 실정이다.[45]

국제적 암시장에서는 이른바 사이버전사들이 이미 높은 몸값을 가지고 있으며, 본격적인 훈련장에서 테러 해커를 교육시키고 있을 가능성도 존재한다. 따라서 사이버테러리즘은 장차 한 국가의 IT 시스템이나 취약 인프

45) Kullik, J, “Vernetzte (Un-)Sicherheit? Eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik“, 2014, pp.67-68.

라에 대한 사이버공격과 연관될 수 있다. 독일 국방정책에서는 독일을 사이버테러리스트들의 잠재적 공격목표로 간주하고 있으며, 사이버테러리즘 또한 국제적 수준에서 효과적으로 대응할 수 있기 때문에 이에 대한 국제적 대응 협력의 필요성 또한 커지고 있다.

바. 사이버행동주의

사이버행동주의는 아직까지 학문분야에서 충분히 연구되지는 않았으나, 지금까지 이에 대해 일반적으로 1) 순기능적 의도, 2) 역기능적 의도, 3) 불명확한 의도라는 세 범주로 분류한다. 모든 사이버행동주의 그룹들은 폭넓은 IT 전문지식을 갖추고 있으며, 사이버행동주의자들은 대체로는 정치적 동기를 지니고, 부분적으로는 자유주의와 이상주의를 추구한다.[46] 예를 들자면 그들은 "인터넷에서의 개인의 발언과 정보의 자유를 목표로 하기도 하고, 더 나아가 국수주의적 사이버행동주의자도 존재한다.

시리아 내전에서는 아사드 반대파가 서방 네트워크행동주의자들과 함께 국제 정보와 프로파간다 확산을 막으려고 하는 데 반해, 그 추종자들은 이를 확산시키고자 노력하는 것을 관찰할 수 있다. 여기서 중요한 문제는 시리아에서의 웹사이트와 정보에 대한 접근권이다.

지속적인 미국 정보기관 NSA의 도청 스캔들 과정에서 독일에서는 정치적 의사결정권자들에 대해 압박하는 네트워크 행동주의자들의 활동 또한 증가하고 있다. 이러한 점에서는 네트워크 행동주의가 정치인이나 안전기관로서는 증가하는 위협으로 인식되고 있다. Jakob Kullik의 견해에 따르면 평화적이든 또는 공격적인 방법이든 간에 사이버행동주의가 향후 중요한 역할을 하게 될 것이라고 한다.[47]

---

46) Kullik, J, "Vernetzte (Un-)Sicherheit? Eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik", 2014, p.44.

47) Kullik, J, "Vernetzte (Un-)Sicherheit? Eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik", 2014, pp.43-45.

사. 사이버반달리즘

사이버반달리즘은 단순한 정치적 저항 뿐만이 아니라 무분별한 웹 컨텐츠 파괴까지도 포괄한다. 범인은 보통 스크립트 키디즈(Skript Kiddies)라고 불리는 청소년들이다. 범인들은 IT 시스템 사용자들의 불충분한 안전의식과 시스템의 약점을 악용하여 IT 시스템을 바이러스에 감염시키고 파괴할 수 있다.[48]

3. 사이버보안

사이버보안이라는 테마는 새로운 것은 아니며, 지난 40 여 년 간의 경험을 통해 정보통신기술 시스템의 발전은 항상 새로운 안전문제를 일으켜왔다는 사실이 충분히 인식되고 있다. 근래의 급속한 디지털화는 정보통신기술에서의 더 많은 안전공백을 야기하고 있다.[49] 안전이라는 것은 상대적인 개념이라는 것을 생각해 볼 때, 사이버 보안은 국가적 또는 국제적 수준에서 전 세계적 사이버공간의 위험을 수인 가능한 정도로 낮추는 IT 안전의 정도에 도달하고자 노력하는 상태를 말한다.[50] 이로써 사이버 보안은 IT 시스템의 기능이 제한받지 않는 상태를 실현한다. 이 점에서 사이버보안은 IT 시스템의 안전공백을 해소하고 사이버공격으로부터 방어하는 것을 목적으로 한다. 이것은 정보통신기술 시스템이 최대한 방해받지 않고, 완전파괴의 위험 없이 작동할 수 있는 가능성이 실현되어야 한다는 것을 의미한다.

48) Kullik, J, “Vernetzte (Un-)Sicherheit? Eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik“, 2014, pp.46-47.
49) Luiijf, E, “New and emerging threats of cyber crime and terrorism. In Akhgar, Babak/Staniforth, Andrew/Bosco, Francesca”, Cyber crime and cyberterrorism investigator's handbook, 2014, pp.19-20.
50) Bundesministerium des Innern, “Cyber-Sicherheitsstrategie fur Deutschland”, 2011, p.15.

사이버보안의 요구를 해결하기 위한 다양한 조치들이 존재하며, 여기에는 예방에 기여하는 기술적·제도적 수단들이 속한다. 제도적인 수단들은 무엇보다도 사이버위협에 대한 민감도 강화나 국제적 협력 강화를 들 수 있다. 학계에서 이미 자주 논의된 바와 같이 “사이버 군비경쟁을 불러일으키지 않기 위해서는 방어적 사이버 보안조치와 공격적 조치의 밸런스를 어떻게 맞출 수 있는가?”하는 질문은 미래를 위한 국가 정책에 있어 중요한 문제이다. Sandro Gaycken 같은 작가들은 그 군비경쟁이 이미 오래전에 시작되었다는 견해를 가지고 있다.[51]

제2절 IT 안전법

1. 도입 배경

2013년 독일에서 발생한 NSA 스캔들로 인해 독일의 미국에 대한 여론이 악화되었으며, 독일 정부는 첩보행위를 한 것으로 알려진 미국 중앙정보국(CIA) 베를린 주재 책임자를 추방하기에 이르렀다. 독일이 북대서양조약기구(NATO) 내 최대 우방인 미국에 이 같은 조치를 취한 것은 극히 이례적인 결정이다. 이 사건은 또한 독일 내 IT 안전에 대한 심각한 우려를 공론화하는 계기가 되었으며, 이는 2015년의 IT 안전법 제정으로 이어지게 되었다.

IT 안전법의 주요 목표는 취약인프라에 대한 해킹으로부터의 보호 강화, 취약인프라 운영자들의 보안사고 신고의무 도입 및 독일 내 데이터에 대한 외국 스파이로부터 보호 등이다.

취약인프라에 대한 침해사고가 매번 신고될 경우 연간 약 240만 건의 사이버 공격 신고가 이뤄지며, 절차 비용도 대거 발생할 것으로 예상되

51) Gaycken, S, “Cyberwar. Das Wettrusten hat langst begonnen. Vom digitalen Angriff zum realen Ausnahmezustand”, Wilhelm Goldmann Verlag, 2012.

었고, 컨설팅 기업 KPMG 조사에 따르면 IT 안전법 내 관료적 절차에 따른 비용 또한 연간 약 10억 유로(약 1조4,000억 원)에 달할 것으로 예상되었음에도 당시 산업계 역시 이를 환영하는 입장이었다.

2. 제정 논의 및 과정

IT 안전법의 계획은 이미 2013년 연정계약에서 논의되기 시작하였으며,[52] 2015년 6월 12일 독일연방의회는 IT 안전법 초안을 의결하였다. 해당 법의 관할권은 연방내무부에 주어졌으며, 2015년 6월 25일에는 IT 안전법이 발효되기에 이르렀다.

당시 IT 안전법의 시급성은 무엇보다도 지속 증대되고 있는 국가, 경제 그리고 사회의 IT 시스템 이용, 그리고 이에 동반되는 디지털화와 네트워크화에 기초하고 있었다.[53] 이를 위해 해당 법률을 통해 취약인프라에 대한 안전 강화가 무엇보다도 중요한 것으로 지목되었다. 따라서 해당 법 시행에 따라 취약인프라 운영자들은 IT 안전에 있어 최소 기준을 충족해야 하며, 사이버 공격 시 연방정보기술안전청(BSI)에 보고해야 한다.

2015년 6월 해당 법 의결 당시에는 오직 원자력발전소와 통신기업들만이 사이버공격 보고의무를 가졌다. 이후 발효 시까지 IT 안전법은 시행령에서 취약인프라와 그의 하위부문에 대해 명확히 정의를 내려야 했다. 그렇지 않으면 어떤 인프라가 취약인프라로서 그 규정에 관련이 되는지 해당 법을 통해서 파악하기가 어려웠기 때문이다.

사이버공격 시 취약인프라 운영자의 보고의무는 유럽연한(EU)이 이미 2013년에 역내 가입국들을 대상으로 그 도입을 촉구한 바 있으나, 이후로는 그러한 보고의무가 유럽연합 가입국들의 정치권과 경제계에서 호응을

52) Deutscher Bundestag, “Koalitionsvertrag zwischen CDU, CSU und SPD (2013). Deutschlands Zukunft gestalten, 18. Legislaturperiode”, 2013, p.147

53) Bundesministerium des Innern, “Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)”, 2015, p.12.

받지 못하였다. 이를 위해 유럽연합은 가입국들에게 보고의무 규정과 관련한 조치도입을 위한 마스터플랜을 제시하였다. 그 마스터플랜을 통해 '유럽 및 국제적 디지털 위치정책'이 확립되었고, 애초에 독일은 이를 위해 2014년 12월에 IT 안전법 초안을 마련하게 된 것이다.

당시까지 독일 경제계의 몇몇 기업들은 사이버공격을 신고하지 않았으나, IT 안전법으로 인해 그러한 사이버공격에 관한 신고가 의무화되었다. 기업 관계자들에 따르면 이전까지 사이버공격이 제대로 보고되지 않은 이유는 이러한 신고와 함께 기업들이 사이버공격 정보에 대한 통제권을 넘겨주게 되고, 그 정보의 계속적인 전파에 관해 아무런 영향력이나 신뢰성 있는 지식을 가질 수 없게 된다는 것을 우려했기 때문이라고 한다.

IT 안전법 도입 시 취약인프라 운영자들에게는 요구된 아이티 최소기준을 이행하기 위해 2년의 유예기간이 주어졌으며, 보고의무에도 마찬가지로 2년간의 유예가 주어졌다.

3. 내 용

가. 구 성

IT 안전법이 하나의 특별법으로서 해당 법 자체에 새로운 정의 및 규율내용을 담고 있는 것은 아니며, 연방정보기술안전청법·원자력법·에너지산업법·텔레미디어법·텔레커뮤니케이션법·연방급여법·연방형사청법 등의 기존 조항을 개정하는 것을 내용으로 하고 있으며, 이러한 법형식은 독일에서는 새로운 법 제정 시 일반적인 형태에 속한다.

IT 안전법의 구성은 아래의 표와 같다.

< 표 3 >

조 항	내 용
제1조	연방정보기술안전청법의 개정
제2조	원자력법의 개정
제3조	에너지산업법의 개정
제4조	텔레미디어법의 개정
제5조	텔레커뮤니케이션법의 개정
제6조	연방급여법의 개정
제7조	연방형사청법의 개정
제8조	연방정보기술안전청법의 다른 개정
제9조	연방 비용징수구조 개혁법의 개정
제10조	사후보완
제11조	발효

나. 연방정보기술안전청법의 개정내용

여기서는 IT 안전법 중 가장 핵심적인 내용을 담고 있는 연방정보기술안전청법에서의 개정사항을 살펴보기로 한다.

- 제1조 (정보기술에서의 안전을 위한 연방관청)

	기 존	개 정
원문	Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik als Bundesoberbehörde. Es untersteht dem Bundesministerium des Innern.	Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) als Bundesoberbehörde. Das Bundesamt istzuständig für die Informationssicherheit auf nationaler Ebene. Es untersteht dem Bundesministerium des Innern.

번역	연방은 정보기술에서의 안전을 위한 연방관청을 연방상급기구로서 둔다. 이는 연방내무부 밑에 있다.	연방은 연방정보기술안전청을 연방상급기구로서 둔다. 그 연방관청은 국가적 수준에서의 정보안전에 관할권이 있다. 이는 연방내무부 밑에 있다.

- 제2조 (정의)

	기 존	개 정
원문		(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die 1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und 2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt.
번역		(10) 이 법에서 말하는 취약인프라는 조직, 시설 또는 분야들 중 1. 에너지, 정보기술 그리고 원격통신, 운송 그리고 교통, 건강, 물, 식품 및 경제와 보험분야에 속하고,

		2. 그 부족이나 침해로 인해 중대한 공급부족 또는 공공의 안전에 위협이 발생할 수 있기 때문에 공동사회의 기능에 큰 의미를 갖는 것을 말한다. 이 법에서 말하는 취약인프라는 제10조 제1항에서 상세히 규정한다.

- 제3조 (연방정보기술안전청의 임무) 제1항

	기 존	개 정
원문	2. Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen und Zurverfügungstellung der gewonnenen Erkenntnisse für andere Stellen, soweit dies zur Erfüllung ihrer Aufgaben oder zur Wahrung ihrer Sicherheitsinteressen erforderlich ist;	2. Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen und Zurverfügungstellung der gewonnenen Erkenntnisse für andere Stellen, soweit dies zur Erfüllung ihrer Aufgaben oder erforderlichist,sowiefürDritte,soweitdies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist;
번역	안전위험과 안전대비 정보들의 수집과 평가, 그리고 획득한 지식이 다른 기관들의 임무를 완수시키거나 다른 기관들의 안전이익 유지를 위해 필요한 경우 이를 제공	안전위험과 안전대비 정보들의 수집과 평가, 그리고 획득한 지식이 다른 기관들의 임무를 완수시키거나, 다른 기관들 및 제3자의 안전이익유지를 위해 필요한 경우 이를 제공

	기 존	개 정
원문	15. Aufbau geeigneter Kommunikationsstrukturen zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung sowie Koordinierung der Zusammenarbeit zum Schutz der ~~kritischenInformationsinfrastrukturen~~ im Verbund mit der ~~Privatwirtschaft.~~	15. Aufbau geeigneter Kommunikationsstrukturen zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung sowie Koordinierung der Zusammenarbeit zum Schutz der SicherheitinderInformationstechnikKritischerInfrastrukturen im Verbund mit der Privatwirtschaft; 16. Aufgaben als zentrale Stelle im Bereich der Sicherheit in der

		Informationstechnik im Hinblick auf die Zusammenarbeit mit den zuständigen Stellen im Ausland, unbeschadet besonderer Zuständigkeiten anderer Stellen; 17. Aufgaben nach den §§ 8a und 8b als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen.
번역	위기조기인식, 위기대응 그리고 위기극복을 위한 적합한 커뮤니케이션구조 구축 및 사경제와의 결합에서의 취약한 정보인프라를 보호하기 위한 협업의 조정	15. 위기조기인식, 위기대응 그리고 위기극복을 위한 적합한 커뮤니케이션 구조 구축 및 사경제와 결합에서의 취약인프라에 대한 정보기술에서 안전을 보호하기 위한 협업의 조정 16. 다른 기관의 특정한 관할권에 상관없이 외국에서의 관할권 있는 기관들과의 협업과 관련하여 정보기술에서의 안전 영역에서 중앙기관으로서의 임무 17. 제8a조 및 제8b조에 따른 취약인프라의 정보기술에서의 안전을 위한 중앙기구로서의 과제

	기 존	개 정
원문		(3) Das Bundesamt kann Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen.
번역		연방정보기술안전청은 취약인프라 운영자들의 요청에 따라 그들의 안전기술의 안전에 있어서 조언 및 지원하거나, 또는 자격 있는 안전서비스제공자를 지정할 수 있다.

- 제4조

	기 존	개 정
원문	§ 4 Zentrale Meldestelle für die Sicherheit in der Informationstechnik	§ 4 Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes
번역	제4조 정보기술에서의 안전을 위한 중앙 신고기관	제4조 연방의 정보기술에서의 안전을 위한 중앙 신고기관

- 제5조 (연방의 통신기술을 위한 손상프로그램과 위험으로부터의 방어)

	기 존	개 정
원문	Sofern nicht die nachfolgenden Absätze eine weitere Verwendung gestatten, muss die automatisierte Auswertung dieser Daten unverzüglich erfolgen und müssen diese nach erfolgtem Abgleich sofort und spurenlos gelöscht werden. Die Verwendungsbeschränkungen gelten nicht für Protokolldaten, sofern diese weder personenbezogene noch dem Fernmeldegeheimnis unterliegende Daten beinhalten. ~~Behördeninterne~~ Protokolldaten dürfen nur ~~im~~ Einvernehmen ~~mit der jeweils betroffenen Behörde~~ erhoben werden.	Sofern nicht die nachfolgenden Absätze eine weitere Verwendung gestatten, muss die automatisierte Auswertung dieser Daten unverzüglich erfolgen und müssen diese nach erfolgtem Abgleich sofort und spurenlos gelöscht werden. Die Verwendungsbeschränkungen gelten nicht für Protokolldaten, sofern diese weder personenbezogene noch dem Fernmeldegeheimnis unterliegende Daten beinhalten. Die Bundesbehörden sind verpflichtet, das Bundesamt bei Maßnahmen nach Satz1 zu unterstützen und hierbei den Zugang des Bundesamtes zu behördeninternen Protokolldaten nach Satz1 Nummer1 sowie Schnittstellendaten nach Satz1 Nummer2 sicher zu stellen. Protokolldaten der Bundesgerichte dürfen nur in deren Einvernehmen erhoben werden.
번역	다음 항이 추가적인 사용을 허용하지 않는 한, 이 데이터의 자동화된	다음 항이 추가적인 사용을 허용하지 않는 한, 이 데이터의 자동화된

	평가는 지체 없이 행해져야 하고, 조정이 이루어진 후에는 즉시 그리고 흔적 없이 삭제되어야 한다. 프로토콜데이터가 개인신상과 관련된 정보나 통신비밀에 해당하는 정보를 포함하고 있지 않은 경우에 한하여 그 사용의 제한은 적용되지 않는다. 기구내부의 프로토콜데이터는 오직 각각의 관련된 기구와의 협의 하에 조사될 수 있다.	평가는 지체 없이 행해져야 하고, 조정이 이루어진 후에는 즉시 그리고 흔적 없이 삭제되어야 한다. 프로토콜데이터가 개인신상과 관련된 정보나 통신비밀에 해당하는 정보를 포함하고 있지 않은 경우에 한하여 그 사용의 제한은 적용되지 않는다. 기구내부의 프로토콜데이터는 오직 각각의 관련된 기구와의 협의 하에 조사될 수 있다. 연방기구들은 제1항에 따른 조치의 경우에 연방정보기술안전청을 지원하고, 이 경우 제1항 1호에 따른 기구 내부의 프로토콜데이터 그리고 제1항 2호에 따른 인터페이스 데이터에 대한 접근을 보장해야 할 의무가 있다. 연방법원의 프로토콜데이터는 오직 연방법원과의 협의 하에 조사될 수 있다.

- 제7조 (경고)

	기 존	개 정
원문	(1) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 kann das Bundesamt Warnungen vor Sicherheitslücken in informationstechnischen Produkten und ~~Dienstenund~~ vor Schadprogrammen ~~andiebetroffenenKreise~~ oder ~~dieÖffentlichkeitweitergebenoder~~ Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen. Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung von diese Produkte betreffenden Warnungen zu informieren, sofern hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks	(1) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 kann das Bundesamt 1. die folgenden Warnungen an die Öffentlichkeit oder an die betroffenen Kreise richten: a) Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten, b) Warnungen vor Schadprogrammen und c) Warnungen im Falle eines Verlustes von oder eines unerlaubten Zugriffs auf Daten;

	nicht gefährdet wird. Soweit entdeckte Sicherheitslücken oder Schadprogramme nicht allgemein bekannt werden sollen, um eine Weiterverbreitung oder rechtswidrige Ausnutzung zu verhindern oder weil das Bundesamt gegenüber Dritten zur Vertraulichkeit verpflichtet ist, kann es den Kreis der zu warnenden Personen anhand sachlicher Kriterien einschränken; sachliche Kriterien können insbesondere die besondere Gefährdung bestimmter Einrichtungen oder die besondere Zuverlässigkeit des Empfängers sein.	2. Sicherheitsmaßnahmen sowie den Einsatzbestimmter Sicherheitsprodukte empfehlen. Das Bundesamt kann zur Wahrnehmung der Aufgaben nach Satz 1 Dritte einbeziehen, wenn dies für eine wirksame und rechtzeitige Warnung erforderlich ist. Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung von diese Produkte betreffenden Warnungen zu informieren, sofern hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks nicht gefährdet wird. Soweit entdeckte Sicherheitslücken oder Schadprogramme nicht allgemein bekannt werden sollen, um eine Weiterverbreitung oder rechtswidrige Ausnutzung zu verhindern oder weil das Bundesamt gegenüber Dritten zur Vertraulichkeit verpflichtet ist, kann es den Kreis der zu warnenden Personen anhand sachlicher Kriterien einschränken; sachliche Kriterien können insbesondere die besondere Gefährdung bestimmter Einrichtungen oder die besondere Zuverlässigkeit des Empfängers sein.
번역	제3조제1항 14호에 따른 임무의 완성을 위하여 연방정보기술안전청은 정보기술 제품과 서비스의 안전결함에 대한, 그리고 관계된 그룹이나 공공에 대한 Schad프로그램에 대한 경고를 발령하거나, 안전조치 및 특정 안전제품의 투입을 권장할 수 있다. 그 조치와 함께 추구되는 목적의 성취가 위협받지 않는 한, 관련된 제품의 생산자는 이 제품들의 공개 전에 관련된 경고를 알려야 한다.발견된 안전결함이나 해악프로그램이 일반적으로 알려진 것이 아니라면, 그	제3조제1항 14호에 따른 임무의 완성을 위하여 연방정보기술안전청은 1.다음의 경고들을 공공이나 관련 그룹에 발령할 수 있다 a)정보기술 제품과 서비스에서의 안전결함에 대한 경고 1. 해악프로그램에 대한 경고 2. 데이터 손실 또는 허가받지 않은 데이터 접근의 경우에 경고

	전파나 불법적 악용을 막기 위하여 또는 연방정보기술안전청이 제3자에 대하여 신뢰성의 의무가 있기 때문에, 연방정보기술안전청은 물적 기준에 의해서 경고를 받는 사람들의 그룹을 제한할 수 있다; 물적 기준은 특히 특정 시설의 특별한 위협 또는 수취인의 특별한 신뢰성이 될 수 있다.	연방정보기술안전청은 효과적이고 적시성 있는 경고를 위해 필요한 경우, 제1호에 따른 임무의 실현을 위하여 제3자를 포함시킬 수 있다. 그 조치와 함께 추구되는 목적의 성취가 위협받지 않는 한, 관련된 제품의 생산자는 이 제품들의 공개 전에 관련된 경고를 알려야 한다. 발견된 안전결함이나 해악프로그램이 일반적으로 알려진 것이 아니라면, 그 전파나 불법적 악용을 막기 위하여 또는 연방정보기술안전청이 제3자에 대하여 신뢰성의 의무가 있기 때문에, 연방정보기술안전청은 물적 기준에 의해서 경고를 받는 사람들의 그룹을 제한할 수 있다; 물적 기준은 특히 특정 시설의 특별한 위협 또는 수취인의 특별한 신뢰성이 될 수 있다.

- 제7조a (정보기술에서의 안전의 조사)

	기 존	개 정
원문		(1) Das Bundesamt kann zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14 und 17 auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen. Es kann sich hierbei der Unterstützung Dritter bedienen, soweit berechtigte Interessen des Herstellers der betroffenen Produkte und Systeme dem nicht entgegenstehen. (2) Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14 und 17 genutzt werden. Das Bundesamt darf seine Erkenntnisse weitergeben und

		veröffentlichen, soweit dies zur Erfüllung dieser Aufgaben erforderlich ist. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben.
번역		(1) 연방정보기술안전청은 제3조제1항 1호, 14호와 17호에 따른 임무 완성을 위해 시중에 공급된 또는 공급 예정인 정보기술 제품 또는 시스템에 대해 조사할 수 있다. 이 경우 관련 제품이나 시스템의 생산자의 정당한 이익이 대립되지 않는 한 제3자의 지원을 받을 수 있다. (2) 그 조사를 통해 획득된 지식은 오직 제3조제1항 1호, 14호와 17호에 따른 임무의 완수을 위해서만 사용될 수 있다. 연방정보기술안전청은 이러한 임무의 완수를 위해 필요한 경우에 한하여 자신의 지식을 전달하고 공개할 수 있다. 그 이전에 관련 제품과 시스템의 생산자에게 적당한 기한과 함께 입장표명의 기회가 주어져야 한다.

- 제8조 (연방정보기술안전청의 목표)

	기 존	개 정
원문	(1) Das Bundesamt ~~kann~~ Mindeststandards für die ~~Sicherung~~ der Informationstechnik des ~~Bundesfestlegen.~~ Das Bundesministerium des Innern kann ~~nachZustimmungdesRatsderIT-Beauftragtender Bundesregierungdienach Satz1festgelegtenAnforderungen~~ ganz oder teilweise als allgemeine Verwaltungsvorschriften für alle Stellen des Bundes erlassen.	(1) Das Bundesamt erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes. Das Bundesministerium des Innern kann imBenehmenmitdemIT-RatdieseMindeststandards ganz oder teilweise als allgemeine Verwaltungsvorschriften für alle Stellen des Bundes erlassen.

	~~SoweitineinerallgemeinenVerwaltungsvorschriftSicherheitsvorgabendesBundesamtesfürressortübergreifendeNetzesowie die fürdenSchutzbedarf des jeweiligenNetzesnotwendigen und vondenNutzerndesNetzesumzusetzendenSicherheitsanforderungenenthaltensind,werdendieseInhalteimBenehmenmitdemRat der IT-BeauftragtenderBundesregierungfestgelegt.~~ Für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach diesem Absatz empfehlenden Charakter.	DasBundesamtberät die Stellen des BundesaufErsuchenbeiderUmsetzung und Einhaltung der Mindeststandards. Für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach diesem Absatz empfehlenden Charakter.
번역	연방정보기술안전청은 연방의 정보기술 안전을 위하여 최소요구기준을 설정할 수 있다. 연방내무부는 연방정부의 아이티전문가위원회의 동의에 따라 1째 문장에 따라 설정된 요구 전부 또는 일부를 연방의 모든 기관들을 위한 일반행정규정으로 공포할 수 있다. 일반행정규정에서 여러 부서가 관련된 네트워크를 위한 연방정보기술안전청의 안전목표, 각각의 네트워크에 대한 보호 필요성이 있고 네트워크의 이용자들로부터 실행되어야 하는 안전요구가 포함되어 있는 경우, 이 내용들은 아이티전문가위원회와의 협의 하에 설정된다. 제2조제3장 2번째문장에서 언급된 법원과 헌법기관들을 위하여 이 규정은 이에 따라 권고의 성격을 가진다.	연방정보기술안전청은 연방의 정보기술 안전을 위한 최소요구기준을 작성한다. 연방내무부는 아이티위원회와의 협의 하에 이 최소요구기준 전부 또는 일부를 연방의 모든 기관들을 위한 일반행정규정으로 공포한다. 연방정보기술안전청은 연방 기관들에게 최소요구기준 실행과 준수에서의 요청에 따라 조언한다. 제2조제3장 2번째 문장에서 언급된 법원과 헌법기관들을 위하여 이 규정은 이에 따라 권고의 성격을 가진다.

- 제8조a (취약인프라 정보기술에서의 안전)

	기 존	개 정
원문		(1) Betreiber Kritischer Infrastrukturen sind verpflichtet,

		spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht. (2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die Feststellung erfolgt 1. im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde. (3) Die Betreiber Kritischer Infrastrukturen haben mindestens

		alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann bei Sicherheitsmängeln verlangen: 1. die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und 2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel. (4) Das Bundesamt kann zur Ausgestaltung des Verfahrens der Sicherheitsaudits, Prüfungen und Zertifizierungen nach Absatz 3 Anforderungen an die Art und Weise der Durchführung, an die hierüber auszustellenden Nachweise sowie fachliche und organisatorische Anforderungen an die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber und der betroffenen Wirtschaftsverbände festlegen.
번역		취약인프라 운영자들은 늦어도 제10조제1항에 따른 규정의 발효 2년 이내에, 그들이 운영하는 취약인프라의 정상적 기능에 중대한 영향을 미치는 사용 장애를 피하고, 정보기술 시스템의 무결성과 신뢰성을 확보하기 위한 적절한 조직적, 기술적 대비,

		그리고 구성요소와 절차들을 갖추어야 할 의무를 진다. 이때 기술의 수준은 준수되어야 한다. 조직적, 기술적 대비는 이를 위한 비용이 관계된 취약인프라의 사고나 침해의 결과를 현저히 벗이나지 않는 경우 적합한 것으로 판단한다. (2) 취약인프라 운영자와 그들의 산업협회는 1항에 따른 요구의 보장을 위한 산업부문에 특별한 안전표준을 제안할 수 있다. 연방정보기술안전청은 그것이 제1조에 따른 요구를 보장하는 데 적합한 것인지 신청에 따라 확정한다. 그 확정은 1. 시민보호 및 재난원조청과의 협의 2. 연방의 관할권 있는 감독기구와의 합의 또는 기타 관할권 있는 감독기구와의 협의로 행해진다. (3) 취약인프라 운영자는 최소 2년마다 제1항에 따른 요구의 충족을 적절한 방법으로 증명해야 한다. 그 증명은 안전감사, 시험 또는 인증을 통해 이루어진다. 운영자들은 수행된 감사, 시험 또는 인증의 목록을 거기서 발견된 안전결함을 포함하여 연방정보기술안전청에 제공해야 한다. 연방정보기술안전청은 안전에 결함이 있는 경우 다음을 요구할 수 있다: 1. 모든 감사, 시험 또는 인증결과들의 제출 2. 연방의 권한있는 감독기구와의 합의 또는 기타 권한 있는 감독기구와의 협의에 따라 안전결함의 제거 (4) 연방정보기술안전청은 제3항에 따른 안전감사, 시험 그리고 인증 절차 구성을 위해, 증명의 발행을 위한 수행의 종류와 방법에 대한 요구 및 관련된 운영자와 경제연합의 대표들로부터의 청문 후 시험 대상들에

		대한 기술적 및 조직적인 요구를 확정할 수 있다.

제8조b (취약인프라 정보기술에서의 안전을 위한 중앙 기구)

	기 존	개 정
원문		(1) Das Bundesamt ist die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik. (2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe 1. die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen Informationen zu sammeln und auszuwerten, insbesondere Informationen zu Sicherheitslücken, zu Schadprogrammen, zu erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und zu der dabei beobachteten Vorgehensweise, 2. deren potentielle Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe zu analysieren, 3. das Lagebild bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen kontinuierlich zu aktualisieren und 4. unverzüglich

		a) die Betreiber Kritischer Infrastrukturen über sie betreffende Informationen nach den Nummern 1 bis 3, b) die zuständigen Aufsichtsbehörden und die sonst zuständigen Behörden des Bundes über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen nach den Nummern 1 bis 3 sowie c) die zuständigen Aufsichtsbehörden der Länder oder die zu diesem Zweck dem Bundesamt von den Ländern als zentrale Kontaktstellen benannten Behörden über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen nach den Nummern 1 bis 3 zu unterrichten. (3) Die Betreiber Kritischer Infrastrukturen haben dem Bundesamt binnen sechs Monaten nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 eine Kontaktstelle für die Kommunikationsstrukturen nach § 3 Absatz 1 Satz 2 Nummer 15 zu benennen. Die Betreiber haben sicherzustellen, dass sie hierüber jederzeit erreichbar sind. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Kontaktstelle. (4) Betreiber Kritischer Infrastrukturen haben erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen

		1. führen können oder 2. geführt haben, über die Kontaktstelle unverzüglich an das Bundesamt zu melden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur Branche des Betreibers enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat. (5) Zusätzlich zu ihrer Kontaktstelle nach Absatz 3 können Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, eine gemeinsame übergeordnete Ansprechstelle benennen. Wurde eine solche benannt, erfolgt der Informationsaustausch zwischen den Kontaktstellen und dem Bundesamt in der Regel über die gemeinsame Ansprechstelle. (6) Soweit erforderlich kann das Bundesamt vom Hersteller der betroffenen informationstechnischen Produkte und Systeme die Mitwirkung an der Beseitigung oder Vermeidung einer Störung nach Absatz 4 verlangen. Satz 1 gilt für Störungen bei Betreibern und Genehmigungsinhabern im Sinne von § 8c Absatz 3 entsprechend. (7) Soweit im Rahmen dieser Vorschrift personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ist eine

		über die vorstehenden Absätze hinausgehende Verarbeitung und Nutzung zu anderen Zwecken unzulässig. § 5 Absatz 7 Satz 3 bis 8 ist entsprechend anzuwenden. Im Übrigen sind die Regelungen des Bundesdatenschutzgesetzes anzuwenden.
번역		(1) 연방정보기술안전청은 정보기술에서의 안전과 관련된 업무에서 취약인프라 운영자를 위한 중앙 신고처이다. (2) 연방정보기술안전청은 이 과제의 수행을 위해 1. 정보기술에서 안전 위험 방어를 위한 중요정보 수집과 평가, 특히 안전결함, 해악프로그램, 정보기술에서의 안전에 대한 성공한 혹은 시도된 공격, 그리고 거기서 관찰된 대응방법에 대한 정보 2. 관할권 있는 감독기구들과 시민보호 및 시민보호와 재난도움청과의 협업에서 취약인프라의 유효성에 대한 잠재적 효과 분석 3. 취약인프라의 정보기술에서의 안전과 관련한 상황보고를 지속적으로 업데이트 4. 지체없이 다음을 보고 a) 취약인프라 운영자에게 1호 내지 3호에 따른 그들과 관련된 정보 b) 관할권 있는 감독관청과 기타 연방의 관할권 있는 기구들에게 1호 내지 3호에 따른 그들의 임무 수행에 필요한 정보 c) 주정부의 관할권 있는 감독기구 또는 이러한 목적 하에 주정부로부터 연방정보기술안전청에게 중앙 연락소로 임명된 기구들에 1호 내지 3호에 따른 그들의 임무 수행에 필요한 정보 (3) 취약인프라 운영자들은 연방정보기술안전청에게 규정 발효 6개월

		이내에 제10조 제1항에 따른 커뮤니케이션구조를 위한 연락소를 제3조제1항 15호에 따라 임명하여야 한다. 취약인프라 운영자는 이곳으로 언제나 연락이 닿는다는 것을 보증하여야 한다. 제2항 제4호에 따른 연방정보기술안전청을 통한 정보 전달은 이 연락소를 통해 이루어진다. (4) 취약인프라 운영자는 그들이 운영하는 취약인프라에 손실 또는 기능에 침해가 1. 발생할 수 있거나 2. 발생한 그들의 정보통신시스템, 구성요소 또는 절차에 대한 중대한 가용성, 무결성, 신뢰성의 장애를 그 연락소를 통해 즉시 연방정보기술안전청에 신고하여야 한다. 이 보고는 장애와 기술적 조건, 특히 추정적 또는 확정적 원인, 관계되는 정보기술, 관계되는 조직이나 시설의 종류 그리고 운영자의 부문에 대한 진술이 포함되어야 한다. 운영자에 대한 명명은 그 장애가 실제로 손실이나 취약인프라의 기능 침해가 발생된 경우에 한하여 필요하다. (5) 제3항에 따른 연락소 외에 같은 분야에 속하는 취약인프라 운영자들은 공통의 상위 연락창구를 지명할 수 있다. 이러한 것이 지명된 경우, 연락소와 연방정보기술안전청 간의 정보교환은 보통 그 공통의 연락창구를 통해 이루어진다. (6) 필요한 경우 연방정보기술안전청은 관계되는 정보기술 제품과 시스템의 생산자들에게 제4조에 따라 장애 제거 또는 회피에 대한 협력을 요구할 수 있다. 1번째 문장은 제8c조 제3항에 해당하는 운영자와 허가권소유자에서의 장애에 유효하다. (7) 이 규정의 범위 내에서 개인 정보가 수집, 처리 또는 사용되는 한, 전항을 벗어나는 다른 목적으로 위한 처리와

		사용은 허용되지 않는다. 제5조 제7항 3번내지 8번문장은 상응하게 적용되어야 한다(해당하는 경우면 이게 사용된다는 뜻 같음). 기타의 경우에는 연방데이터보호법의 규정이 적용된다.

- 제8조c (적용영역)

	기 존	개 정
원문		(1) Die §§ 8a und 8b sind nicht anzuwenden auf Kleinstunternehmen im Sinne der Empfehlung 2003/361/EC der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36). Artikel 3 Absatz 4 der Empfehlung ist nicht anzuwenden. (2) § 8a ist nicht anzuwenden auf 1. Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen, 2. Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 3 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324) geändert worden ist, in der jeweils geltenden Fassung, 3. Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), das

		zuletzt durch Artikel 2 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324) geändert worden ist, in der jeweils geltenden Fassung für den Geltungsbereich der Genehmigung sowie 4. sonstige Betreiber Kritischer Infrastrukturen, soweit sie auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8a vergleichbar oder weitergehend sind. (3) § 8b Absatz 3 bis 5 ist nicht anzuwenden auf 1. Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen, 2. Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes, 3. Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes für den Geltungsbereich der Genehmigung sowie 4. sonstige Betreiber Kritischer Infrastrukturen, die auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8b Absatz 3 bis 5 vergleichbar oder weitergehend sind.
번역		(1) 제8a조와 제8b조는 2003년 5월 6일의 영세기업 및 중소기업의 정의와 관련된 위원회의 2003/361/EC 권고에서 말하는 영세기업에는 적용되지 않는다. 해당 권고의 제3조

		제4항은 적용되지 않는다. (2) 제8a조는 다음의 경우 적용되지 않는다. 1. 취약인프라 운영자가 공공 텔레커뮤니케이션망을 운영하거나 공개적으로 이용가능한 통신서비스를 제공하는 경우 2. 2015년 7월 17일 개정된 에너지경제법에서 말하는 에너지공급망 또는 에너지시설 운영자 3. 2015년 7월 17일 개정된 원자력법 제7조제1항에 따른 허가권소유자 4. 제8a조에 따른 요구와 비교할 만하거나 더 초과하는 법규에 따른 요구를 충족시켜야만 하는 기타 취약인프라 운영자 (3) 제8b조 제3항 내지 제5항은 다음 경우에는 적용되지 않는다. 1. 취약인프라 운영자가 공공 텔레커뮤니케이션망을 운영하거나 공개적으로 이용가능한 통신서비스를 제공하는 경우 2. 에너지경제법에서 말하는 에너지공급망 또는 에너지시설 운영자 3. 원자력법 제7조제1항에 따른 허가권자 4. 제8a조 제3항 내지 제5항에 따른 요구와 비교할 만하거나 더 초과하는 법규에 따른 요구를 충족시켜야만 하는 기타 취약인프라 운영자

- 제8d조

	기 존	개 정
원문		(1) Das Bundesamt kann Dritten auf Antrag Auskunft zu den im Rahmen von § 8a Absatz 2 und 3 erhaltenen Informationen sowie zu den Meldungen nach § 8b Absatz 4 nur erteilen, wenn schutzwürdige Interessen des betroffenen Betreibers Kritischer Infrastrukturen dem nicht entgegenstehen und durch die Auskunft keine Beeinträchtigung wesentlicher Sicherheitsinteressen zu erwarten ist. Zugang zu personenbezogenen Daten wird nicht gewährt. (2) Zugang zu den Akten des Bundesamtes in Angelegenheiten nach den §§ 8a und 8b wird nur Verfahrensbeteiligten gewährt und dies nach Maßgabe von § 29 des Verwaltungsverfahrensgesetzes.
번역		(1) 연방정보기술안전청은 제8a조 제2항과 제3항의 범위 내에서획득된 정보와 제8b조 제4항에 따른 보고를, 관계되는 취약인프라 운영자의 보호가치 있는 이익이 제3자와 충돌하지 않고, 그 통지를 통해 현저한 안전이익의 침해가 예상되지 않는 경우에 한하여 신청에 따라 이를 제3자에게 통지할 수 있다. (2) 제8a조와 제8b조에 따른 업무에 있어서의 연방정보기술안전청의 서류에 대한 접근은 오직 절차당사자에게만 허용되며, 행정절차법 제29조에 따라 허용된다.

- 제10조 (법령 공포 권한)

	기 존	개 정

현행없음	(1) Das Bundesministerium des Innern bestimmt nach Anhörung der betroffenen Wirtschaftsverbände und im Einvernehmen mit dem Bundesministerium für Wirtschaft und ~~Technologie~~ durch ~~Rechtsverordnung~~ das Nähere über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen nach § 9 und deren Inhalt. ~~(2)~~ Für individuell zurechenbare öffentliche Leistungen nach diesem Gesetz und nach den zur Durchführung dieses Gesetzes erlassenen Rechtsverordnungen werden Gebühren und Auslagen erhoben. Die Höhe der Gebühren richtet sich nach dem mit den Leistungen verbundenen Verwaltungsaufwand. Das Bundesministerium des Innern bestimmt im Einvernehmen mit dem Bundesministerium der Finanzen durch ~~Rechtsverordnung~~ die gebührenpflichtigen Tatbestände, die Gebührensätze und die Auslagen.	(1) Das Bundesministerium des Innern bestimmt durchRechtsverordnung,dienichtderZustimmungdesBundesratesbedarf, nach Anhörung vonVertretern der Wissenschaft,der betroffenen Betreiberundderbetroffenen Wirtschaftsverbände imEinvernehmenmitdemBundesministeriumfürWirtschaft und Energie,demBundesministeriumderJustizundfürVerbraucherschutz,demBundesministeriumderFinanzen,demBundesministeriumfürArbeitundSoziales,demBundesministeriumfürErnährungundLandwirtschaft,demBundesministeriumfürGesundheit,demBundesministeriumfürVerkehrunddigitaleInfrastruktur,demBundesministeriumderVerteidigungunddemBundesministeriumfürUmwelt,Naturschutz,BauundReaktorsicherheitunterFestlegungderindenjeweiligenSektoren im Hinblickauf§2Absatz10Satz1Nummer2wegenihrerBedeutungalskritischanzusehenden Dienstleistungenundderenalsbedeutendanzusehenden Versorgungsgrads,welcheEinrichtungen,AnlagenoderTeiledavonalsKritischeInfrastrukturenimSinnediesesGesetzesgelten.DernachSatz1alsbedeutendanzusehendeVersorgungsgradistanhandvonbranchenspezifischenSchwellenwertenfürjedewegenihrerBedeutungalskritischanzusehendeDienstleistungimjeweiligenSektorzubestimmen.ZugangzuAkten,diedieErstellungoderÄnderungdieserVerordnungbetreffen,wirdnicht gewährt. (2) Das Bundesministerium des Innern bestimmt nach Anhörung der betroffenen Wirtschaftsverbände und im EinvernehmenmitdemBundesministeriumfürWirtschaftund Energie durch Rechtsverordnung,dienichtderZustimmungdesBundesratesbedarf, das Nähere über das Verfahren der Erteilung von Sicherheitszertifikaten und

		Anerkennungen nach § 9 und deren Inhalt. (3) Für individuell zurechenbare öffentliche Leistungen nach diesem Gesetz und nach den zur Durchführung dieses Gesetzes erlassenen Rechtsverordnungen werden Gebühren und Auslagen erhoben. Die Höhe der Gebühren richtet sich nach dem mit den Leistungen verbundenen Verwaltungsaufwand. Das Bundesministerium des Innern bestimmt im Einvernehmen mit dem Bundesministerium der Finanzen durch Rechtsverordnung,dienichtderZustimmung desBundesratesbedarf, die gebührenpflichtigen Tatbestände, die Gebührensätze und die Auslagen.
번역	(1)연방내무부는 관계되는 경제단체의 청문 후 경제와 기술 연방부처와의 합의 하에 법령을 통해 제9조와 그 내용에 따른 안전증명서와 승인 발급의 절차에 대한 상세한 사항을 규정한다. 3. 이 법과 이 법의 실행으로써 공포되는 법령에 따라 개별적으로 귀속되는 공공 서비스를 위해서는 비용과 경비가 징수된다. 비용의 액수는 그 서비스와 결부된 행정비용에 따라 결정된다. 연방내무부는 연방재무부와의 합의로 법령에 따라 비용지불 대상이 되는 구성요건, 요율과 경비를 결정한다.	(1)연방내무부는 연방의회의 동의를 요하지 않는 법령을 통하여 경제계, 관련되는 운영자들과 관련되는 경제단체의 대표들의 청문 후, 연방경제에너지부, 연방 사법소비자보호부, 연방 재무부, 연방 노동사회부, 연방 영양농업부, 연방보건부, 연방 교통디지털인프라부, 연방국방부 및 연방 환경자연보호건축원전안전부와의 합의 하에 각각의 부문에서 제2조 제10항 2호와 관련하여 그 중대성 때문에 취약한 것으로 보이는 서비스와 중요한 것으로 보이는 공급등급 확정에 따라, 어떤 기관, 시설 또는 그들의 부분이 이 법에서 말하는 취약인프라로 간주되는지 결정한다. 1번째 문장에 따라 중요한 것으로 간주되는 공급등급은 각각의 부문에서 그 중요성 때문에 취약한 것으로 보이는 서비스를 위한 분야 전문적인 임계값에 의해 결정된다. 그 지침의 신설 또는 개정에 관계되는 문서에 대한 접근은 허용되지 않는다. (2) 연방내무부는 관계되는 경제단체의 청문과 연방경제에너지부와의 합의 하에 연방의회의 동의가 필요 없는 법령을

		통하여 안전증명과 승인 부여의 절차에 관한 상세한 사항을 제9조와 그 내용에 따라 규정한다. (3) 이 법과 이 법의 실행으로써 공포되는 법령에 따라 개별적으로 귀속되는 공공 서비스를 위해서는 비용과 경비가 징수된다. 비용의 액수는 그 서비스와 결부된 행정비용에 따라 결정된다. 연방내무부는 연방재무부와의 합의로 연방의회의 동의를 요하지 않는 법령에 따라 비용지불 대상이 되는 구성요건, 요율과 경비를 결정한다.

- 제13조 (보고의무)

	기 존	개 정
원문		(1) Das Bundesamt unterrichtet das Bundesministerium des Innern über seine Tätigkeit. (2) Die Unterrichtung nach Absatz 1 dient auch der Aufklärung der Öffentlichkeit durch das Bundesministerium des Innern über Gefahren für die Sicherheit in der Informationstechnik, die mindestens einmal jährlich in einem zusammenfassenden Bericht erfolgt. § 7 Absatz 1 Satz 3 und 4 ist entsprechend anzuwenden.
번역		(1) 연방정보기술안전청은 연방내무부에 자신의 활동을 보고한다. (2) 제1항에 의한 보고는 연방내무부를 통해 최소 연 1회 총괄보고서로 발간되는, 정보기술에서의 안전과 관련된 위험에 대한 대중 설명에 이바지한다. 제7조 제1항 3번째와 4번째 문장은 상응하게 적용된다.

- 제14조 (벌금규정)

	기 존	개 정
원문		(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig 1. entgegen § 8a Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine dort genannte Vorkehrung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig trifft, 2. einer vollziehbaren Anordnung nach § 8a Absatz 3 Satz 4 a) Nummer 1 oder b) Nummer 2 zuwiderhandelt, 3. entgegen § 8b Absatz 3 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine Kontaktstelle nicht oder nicht rechtzeitig benennt oder 4. entgegen § 8b Absatz 4 Satz 1 Nummer 2 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht. (2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 2 Buchstabe b mit einer Geldbuße bis zu hunderttausend Euro, in den übrigen Fällen des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden. (3) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes

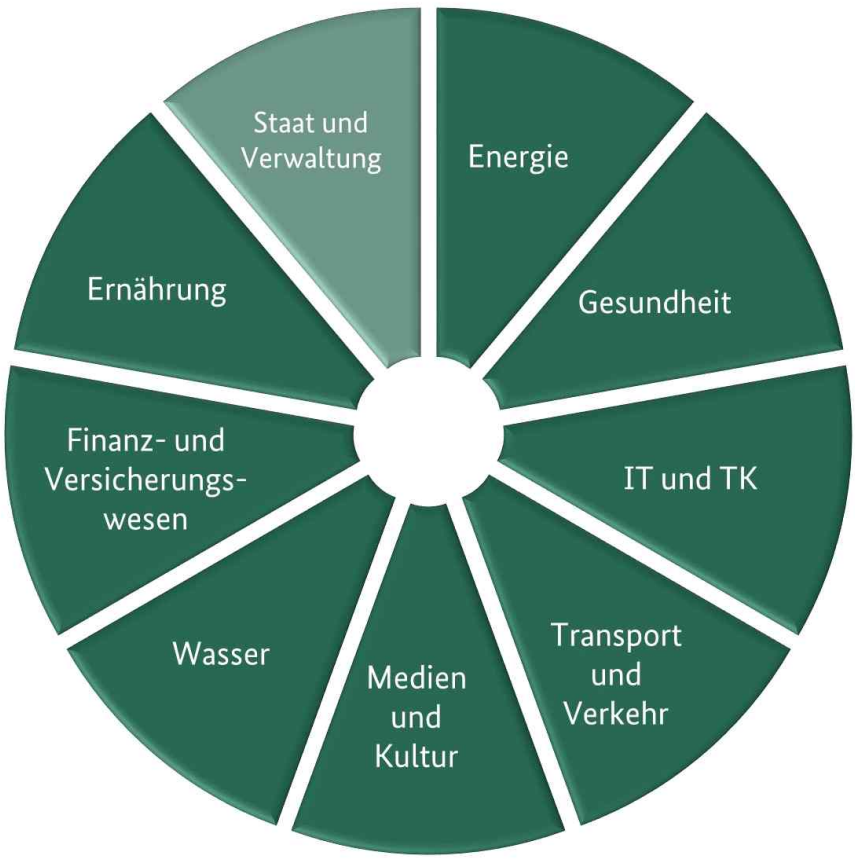
		über Ordnungswidrigkeiten ist das Bundesamt.
번역		(1) 고의 또는 과실로 다음의 행위를 한 자는 규정을 위반한 것이다. 1. 제8a조 제1항 1번째 문장에 반하여 제10조 제1항 1번째 문장에 따른 법령과 결부되어 거기에서 지정된 예방책을 준수하지 않거나, 올바르게 하지 않거나, 완전히 하지 않거나, 적시에 하지 않은 경우 2. 제8a조 제3항 4번 문장에 따른 집행 가능한 명령에 a) 제1호 또는 b) 제2호에 위반한 경우 3. 제8b조 제3항에 반하여 제10조 제1항 1번째 문장에 따른 법령과 결부되어 연락처를 지정하지 않거나 제때에 지정하지 않은 경우 4. 제8b조 제4항 2호에 반하여 통지를 하지 않거나, 올바르게 하지 않거나, 완전히 하지 않거나 또는 적시에 하지 않은 경우 (2) 제1항 2호 b의 경우 10만 유로 이내의 벌금, 제1항의 나머지 경우는 5만 유로 이내의 벌금에 처한다. (3) 이 법 제36조 제1항 1호에서 말하는 규정위반에 대한 행정관청은 연방정보기술안전청이다.

제3절 사이버안전 관리체계

1. 크리티스(KRITIS)

크리티스란 Kritische Infrastrukturen(취약한 인프라들)의 머릿글자를 따서 조합된 단어로, 독일 사이버안전 관리체계의 핵심을 이루는 용어이다. 이는 그 손실이나 침해가 지속적 공급부족, 공공안전의 중대한 장애 또는 다른 심대한 결과를 야기하는, 국가 공동체를 위해 중요한 의미를 가지는 조직 또는 기관들을 말하며, 다음의 9개 하위 부문들로 구성되어 있다.

< 그림 1 >



출처 : 독일연방내무부
https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/sektoren_node.html

이는 에너지(Energie), 건강(Gesundheit), 정보기술과 통신(IT und TK), 운송과 교통(Tranport und Verkehr), 미디어와 문화(Medien und Kultur), 물(Wasser), 경제와 보험 분야(Finanz- und Versicherungswesen), 영양(Ernährung), 국가와 행정(Staat und Verwaltung) 등 9개 분야이다.

이러한 취약인프라 운영자들은 그들이 사경제 분야에 속하는지, 공공기업으로 조직되었는지를 불문하고 시민 생활을 위해 필수불가결한 서비스를 높은 품질과 안정성 하에 공급한다.

2. 연방 수준의 사이버안전정책

사이버테러를 통한 위협은 안전정책 분야 중 비교적 최근에야 나타난 새로운 분야이며, 따라서 새로운 해결 컨셉트를 필요로 한다.[54] 사이버안전이 이에 따라 대외정책 및 안전정책의 새로운 분야로 나타났으며, 해당 정책분야의 '다면적인 정책적 도전'이 되었다. 사이버안전은 정책분야에서 독일은 물론이고 국제적 수준에서도 중요성이 점점 강조되어 왔다.

독일에서의 사이버보안 영역은 연방내무부(BMI)의 관할에 속하며, 연방내무부는 지속적으로 '더욱 강력한 사전조치'를 촉구하고 있다. 한편 사이버보안의 관할권은 오로지 연방내무부에만 주어져 있는 것은 아니며, 연방정부 또한 예를 들어 사이버대외정책을 통해 사이버공간에서의 국가들 간 책임감 있는 협력을 가능케 하기 위한 '국제적 규범 강화'를 위해 노력하고 있다.

미국에서는 사이버안전이 대체로 군사 영역으로 귀결된다. 이는 사이버전쟁 능력이 국가 간 분쟁에서의 전략적 무기로 성장해 왔기 때문이다.[55] 독일은 선진 산업국가, 경제 대국으로서 기업에 대한 사이버공격 위

54) Tschersich, T, "Zur Notwendigkeit eines Umdenkens beim Thema Cybersicherheit", Datenschutz und Datensicherheit, 2011, p.408

55) Bendiek, A, und Ulmer, K, "Cybersicherheit - eine facettenreiche politische

협을 우선적으로 받고 있는 반면, 미국은 실질적 패권국가로서 군사적 조직에 대한 사이버 공격 위협이 더욱 크다는 점에서 그 차이를 찾을 수 있다.

사이버 보안이라는 테마는 독일에서는 2009과 2013년에서야 연방정부에 의한 연정계약에서 다루어졌다. 위협에 취약한 인프라(Kritischen Infrastrukturen)의 보호를 위해 2009년에는 'KRITIS 전략'이 의결되었고, 이어서 2011년에 '사이버안전 전략', 2014년에 '디지털 아젠더 2014'가 의결되었다. 2013년의 연정계약에서는 특히 IT 안전과 산업스파이에 대해 다루어졌다.[56] 연방정부는 2013의 연정계약을 통해 IT 안전이라는 테마를 아젠다로 설정한 이후로 디지털정책의 원칙 수립을 통해 방향을 제시하고 있다. 연방정부는 그 원칙에서 "디지털 변화는 경제, 학문, 사회 그리고 정책을 위한 핵심 과제가 되었다"고 설명하고 있다. 이어서 개별 연정계약, 전략, 계획에 대해 다루기로 한다.

가. 2009년과 2013년 연정계약에서의 사이버보안

사이버보안이라는 테마는 2009년의 CDU(기독민주당), CSU(기독사회당) 그리고 FDP(자유민주당) 간의 연정계약서 중 '혁신과 교육'의 장에서 주목을 받았다. 2009년의 연정계약에서 인식 변화가 있었고 그것은 "독일이 오래 전에 정보사회에 도달했다"는 것이다. 이러한 이유로 모든 사람들이 인터넷 접근권을 가져야 한다는 목표가 설정되었으며, 이를 위해서는 고성능의 브로드밴드 공급이 필수적이었다. 더 나아가 "권리와 법은 인터넷에서 이미 오늘날, 그리고 미래에도 다른 어느 곳과도 동일하게 적용된다"고 강조되었다. 여기서 사이버범죄의 문제가 나타나게 되며, 무엇보다도 데이터보호법률의 개선으로 대응해야 하는 데이터 악용의 문제가 부각된다. 결과적으로 연정계약서에는 "데이터 악용의 방지를 위해서는 자기 자신의 정

Herausforderung. Aus internationale Zeitschriften 2012/2013". SWP-Aktuell 3. Stiftung Wissenschaft und Politik. 2013, pp.1-2.

56) Deutscher Bundestag, "Koalitionsvertrag zwischen CDU, CSU und SPD (2013). Deutschlands Zukunft gestalten, 18. Legislaturperiode", 2013, p.140.

보에 대한 보호의 민감도 강화를 통해 스스로의 정보보호를 용이하게 해야 한다."고 확정되었다.[57]

사이버범죄와의 싸움(특히 사기와 신상정보 절취)의 확대에 대비하여 형사 소추에 관한 사항들이 주정부들과의 협력 하에 기술됨에 따라, IT 전문가들과 특별 훈련된 인력들이 안전 관련 기구에서 형사소추 개선에 기여하게 되었으며, 더 나아가 통신에서의 안전성 강화가 주목을 받았다. 이러한 요구를 더욱 잘 처리하기 위하여 사이버범죄에의 대응을 위한 국제적 협력 또한 강화되었다.

IT 안전(사이버보안)은 공개적 영역 및 비공개적 영역을 불문하고 강화되었으며, 특히 특별한 보호가 요구되는 취약인프라의 IT 시스템이 강조되었는데, 이를 위해 연방정보기술안전청의 권한이 강화되었다. 사이버공격에 대한 방어를 위하여 연방정부 정보기술 분야 전권위원회가 강화되었고, 연방정보기술안전청은 이 부분에서 지원역할을 수행하며, 무엇보다도 사이버공격에 대한 방어에 있어서 협력·조정자로서의 기능을 위해 폭넓은 지원을 할 수 있도록 '중앙 사이버안전 기구'로서 폭넓게 개편되었다.[58]

2013년의 CDU, CSU und SPD(사회민주당) 간 연정계약에서도 사이버보안 또는 IT 안전의 테마가 새로운 견지에서 상세하게 재차 다루어졌다. 디지털 안전과 데이터 보호의 장에서 이러한 주제가 이전의 연정계약에 비해 더욱 구체적으로 다루어졌으며, 사이버범죄, IT 인프라, 디지털 데이터 보호 등이 집중적으로 다루어졌다.[59] 여기서는 또한 관련 법령의 상황이 다루어지고, 법령 정비의 시급성이 부각되었다.

더 나아가 새로운 연정계약에서는 IT 안전법의 당위성이 명확히 확정되었으며, IT 인프라와 디지털 데이터 보호의 측면에서 그 필요성이 상세히 다루어졌다. IT 안전법은 취약인프라 운영자를 통한 취약인프라의 IT

57) Deutscher Bundestag, "Koalitionsvertrag zwischen CDU, CSU und FDP (2009). Wachstum. Bildung. Zusammenhalt, 17. Legislaturperiode", pp.100-101.
58) Deutscher Bundestag, "Koalitionsvertrag zwischen CDU, CSU und FDP (2009). Wachstum. Bildung. Zusammenhalt, 17. Legislaturperiode", pp.101-103.
59) Kullik, J, "Vernetzte (Un-)Sicherheit? Eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik", 2014, p.84.

안전에 대한 구속적인 최소 요구기준과 중요 IT 안전사고에 대한 보고의무를 규정한다.

당시 EU 수준에서는 기술주권의 회복을 위한 조치와 함께 유럽 사이버안전 전략이 추구되었으며, EU 데이터보호 기본규정 개선안 마련을 서두르고 있었다. 제도적 수준에서 연방정보기술안전청과 사이버방어센터(Cyber-Abwehrzentrum, Cyber-AZ) 그리고 독일 안전기관들의 더 나은 IT 장비 도입이 계획되었다.

2013년의 NSA 스캔들 관련 내용은 연정계약에서 “스파이로부터의 보호를 위한 법적 구속력 있는 정당 간 합의”를 목표로 하나의 개별 장에서 주제로 다루어졌다. 사이버보안이라는 테마의 영역에서 더욱 언급할 가치가 있는 부분은 독일을 위한 ”디지털 아젠다(Digitalen Agenda)“이다. 디지털 아젠다를 통해 강력한 경제, 평등한 교육 그리고 자유롭고 안전한 인터넷의 실현가능성이 강화되었다. 또한 독일을 유럽의 디지털 성장 1등 국가(digitalen Wachstumsland Nr. 1 in Europa로 만든다는 목표가 구체화되었다.

나. 취약인프라 보호

이 장에서는 취약인프라 보호를 위한 정책의 전략과 계획을 다룬다. 취약인프라 보호라는 주제가 지속적으로 연정계약에서 다루어진 후에, 2005년 정보인프라 보호를 위한 국가계획(NPSI) 이 성립되었고, 2007년 정보인프라 보호를 위한 국가계획의 KRITIS로의 전환 계획, 2009년 KRITIS 전략, 그리고 2014년 KRITIS 실행계획(UP KRITIS)이 뒤를 이었다. KRITIS 실행계획의 틀 안에서 정치권과 경제계, 그리고 연방 실행계획(UP Bund)의 대표자들과 함께 연방 실행계획 협의회가 설립되었다.

취약인프라에 대한 사이버 위협으로부터의 보호는 연정계약들에서 점차 중요성이 커져갔다. 처음에는 그 테마가 연방내무부의 의뢰로 실무 그

룹에 의해 체계화되고, 1997년 보고서가 발행되었다. 이 보고서에는 IT를 통해 운용되는 시설에서 발생 가능한 사고들 및 이러한 사고들의 잠재적 결과들이 조사되었으며, IT 안전은 향후 상당한 중대성을 갖게 될 것이라는 점이 확인되었다.[60]

1) 정보인프라 보호를 위한 국가계획(Nationaler Plan zum Schutz der Informationsinfrasturukturen, NPSI)

정보인프라 보호를 위한 전략적 계획은 2005년에서야 연방내무부, 정보인프라 보호를 위한 국가계획 공동으로 제시되었다. 여기에 비로소 IT 안전이라는 개념이 독일의 정책에서 다음의 구체적인 정의를 갖추고 다루어지기 시작했다. "IT안전이란 IT 정보의 이용가능성, 무결성, 연결성 그리고 신뢰성이 보장되는 상태이다.".[61]

정보인프라 보호를 위한 국가계획에서 정보인프라는 한 국가의 신경망이라고 표현되었다. 정보인프라에 대한 사이버위협은 그 근원이 국가적 차원뿐만 아니라 국제적 차원에 또한 이를 수 있다.

결과적으로 예방전략계획의 대부분은 취약인프라 보호를 위한 예방에 초점을 맞추고 있다. 연방내무부에는 기업들을 위하여 IT 시스템과 생산물에 대해 그 안전성을 공인하는 역할이 주어졌다. 여기에는 안전한 통신을 위해 제작된 신뢰성 있는 암호화제품의 이용가능성 또한 포함된다. 특히 산업스파이와 관련해서는 독일의 암호화 관련 절차가 핵심적인 것으로 파악되었다.

취약인프라들은 종종 사기업에 의해 운영되기 때문에, 당시 연방정부는 경제계와의 협력이 필수적이라고 판단했다. 정보인프라 보호를 위한 국

60) Kullik, J, "Vernetzte (Un-)Sicherheit? Eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik", 2014, pp.86-88.
61) Bundesministerium des Innern, "Nationaler Plan zum Schutz der Informations-infrastrukturen(NPSI)", 2005, pp.7-8.

가계획에서는 KRITIS 실행계획이 기업 및 경제계 대표들과 함께 마련되어져야 한다고 주장되었다. 이후로 연방정보기술안전청은 기업들에게 사이버 보안에 있어서 행동 권장 형태로 지원하게 된다[62]

2) 정보인프라 보호를 위한 국가계획의 KRITIS로의 전환계획 (Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen)

정보인프라 보호를 위한 국가계획에 이어 2007년에는 정보인프라 보호를 위한 국가계획의 KRITIS로의 전환계획이 뒤따르게 된다. 이 새로운 계획은 정보인프라뿐만 아니라 광범위한 취약인프라를 아우르며, IT위기로부터의 보호를 위한 '예방', '반응','지속'을 통한 전략적 대응이 채택되었다. IT 위기는 정보인프라 보호를 위한 국가계획의 KRITIS로의 전환계획에 다음과 같이 정의되었다. "정보인프라 보호를 위한 국가계획의 KRITIS로의 전환계획 상의 IT 위기란, 어떠한 조직이나 단체로부터 IT와 결부되어 국가공공조직에 대해 지속되는 공급 애로, 공공안전의 현저한 장애나 다른 중대한 결과가 나타나는 손실 또는 침해가 발생하거나 예상되는 경우를 말한다."[63]

이 경우 정보인프라 보호를 위한 국가계획의 KRITIS로의 전환계획에서는 취약인프라 보호 외에도 장애 발생의 경우 해당 인프라에서 실행되어야 하는 메커니즘과 IT 위기대응이 수행된다.[64]

3) KRITIS 전략(KRITIS-Strategie)

---

62) Bundesministerium des Innern, "Nationaler Plan zum Schutz der Informations-infrastrukturen(NPSI)", 2005, pp.7-8

63) Bundesministerium des Innern, "Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen", 2007, p.21.

64) Bundesministerium des Innern, "Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen", 2007, pp.21-22.

2007년의 정보인프라 보호를 위한 국가계획의 KRITIS로의 전환계획에 이어 2009년에는 취약인프라에 대한 국가, 경제 그리고 사회의 중요성과 책임이 다시 한 번 강조된 KRITIS 전략이 뒤따르게 된다. 취약인프라의 개별부문은 표 4와 같이 기술적 기초인프라와 사회경제적 서비스인프라의 하위 부문으로 나눠지게 된다.

< 표 4 >

기술적 기초인프라	사회경제 서비스인프라
전기공급	공중보건, 영양
정보- 통신기술	응급- 구조, 재난보호
운송과 교통	의회, 정부, 공공행정, 헌법기관
식수공급과 하수처리	재정- 보험
	미디어와 문화예술

서비스인프라와 기초인프라 간 상호적인 독립성은 중요한 의미를 지닌다. 예를 들자면 에너지공급은 사회경제적 서비스 유지에 필수적이며, 또한 에너지공급의 안정성은 제대로 작동하는 법률시스템에 기반한다. 이러한 상호적인 독립성을 통해 하나의 손실에 다수의 인프라들이 연관될 수 있다. 결과적으로 하나의 개별 요소가 여러 영역에서 심대한 장해를 야기할 수 있는 취약인프라 네트워크가 전제되어야만 한다.

다만, KRITIS 전략에서는 취약인프라에 대한 구체적 정의가 결여되어 있다는 비판이 존재하며, 특히 운송과 물류 분야에서는 예를 들어 특정 유통회사의 물류 분야가가 취약인프라로 평가되는지에 대한 불명확성이 존재한다. 계획들과 전략들을 취약인프라에 편입시킬 수 있도록, 명확히 상호간에 경계가 지어진 정의가 필요하다는 요구가 독일 내에서 상존한다.

4) KRITIS 실행계획(UP KRITIS)

2014년에 정보인프라 보호를 위한 국가계획의 KRITIS로의 전환계획을 대체하는 ‘KRITIS 실행계획’이 의결되었다. KRITIS 실행계획은 취약 인프라 운영자, 그들의 협회와 관할권 있는 국가기관들 간의 공공 및 사적 협력체이다.

KRITIS 실행계획은 취약인프라 9개 부문 중 8개 부문을 대상으로 하며, ‘국가와 행정’ 부문은 ‘연방 실행계획(UP Bund)’에서 다뤄진다. 이 협력체의 최종 목표는 독일에서의 취약인프라 서비스 공급을 유지하는 것이며, 다음의 하위 목표들이 있다.

- 취약 프로세스에서의 정보통신 구성요소의 견고성 강화
- 현행 사건에 대한 의견교환
- 사이버안전 상황에 대한 공동의 사정 및 평가
- 공동의 문서들과 지위에 관한 처리
- 위기관리체계의 수립 및 재편
- 위기 대응 및 관리에서의 협력
- 응급·위기 연습 수행
- 제3자에 대한 공동 행동

KRITIS 실행계획은 연방정부의 정보인프라 보호를 위한 국가계획에서 설정된 ‘예방, 대응 그리고 유지’라는 목표를 취약인프라 영역에서의 구체적인 조치와 조언을 통해 구성하고자 마련되었다. 발전과정에서 정보인프라 보호를 위한 국가계획은 ‘사이버안전 전략’으로 대체되었으며, 이는 연방정보기술안전청을 통해 관리 운영된다.

‘KRITIS 실행계획 위원회’로부터 ‘취약인프라 보호를 위한 공공-사

적 파트너십'이라는 원칙과 목표가 의결되었다.[65] 그 원칙과 목표에서 잘 작동하는 취약인프라가 국가, 경제 그리고 사회를 위해 포기할 수 없는 것이라는 점이 다시 한 번 강조되었다. 위 그림 1에서 살펴본 바와 같이 이것은 에너지, 건강, 정보기술과 통신, 운송과 교통, 미디어와 문화, 물, 경제와 보험 분야, 영양, 국가와 행정 등 9가지 분야이다.

5) 연방 실행계획(UP Bund)

국가와 행정 부문은 KRITIS 실행계획의 관할권 영역에 속하지 않으며, 이를 위해 연방 실행계획이 의결되었다. 연방 실행계획으로부터 연방행정의 정보인프라 보호를 위한 통일적인 최소요구사항이 마련되었다. 연방행정은 매년 대략 3백만 유로를 정보 및 통신인프라 확대에 사용하고 있기 때문에, 그 최소요구사항은 필수적이다. 이로써 IT 시스템에 더 높은 수준의 보호가 요구될수록 더 많은 공격가능성이 발생하게 된다.[66]

연방 실행계획으로부터의 조치들과 관련하여, 연방부처들은 잘 보호되고 있으나 행정관청들은 충분히 보호되지 못한다는 평가가 있으며, 이 점에서 행정관청이 수장들이 종종 충분치 못한 문제의식을 보이고 있다고 비판받는다. 정치권이 기업들에게 어떠한 조치들을 요구하여 실행시키기 이전에 자신들의 기관에서 좋은 선례들과 함께 발전시켜 나갈 필요성이 있으며, 이 점에서 또한 각각의 관청들을 위한 IT 안전개념의 정립 필요성이 제기된다.

6) KRITIS 실행계획 위원회(UP KRITIS-Rat)

65) Bundesamt für Sicherheit in der Informationstechnik und Bundesamt für Bevolkerungsschutz und Katastrophenhilfe, "Zusammenarbeit im Rahmen des UP KRITIS", 2011

66) KPMG, "IT-Sicherheit in Deutschland Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes", p.6.

KRITIS 실행계획에서는 취약인프라 운영자들이 정치권과의 협업에 대해서 소극적이라는 평가가 있어왔다. 한편 그러한 협업이 KRITIS 실행계획 위원회에서는 잘 발전되었으나, 그럼에도 불구하고 더 나은 협업체계를 구성함으로써 IT 안전법에 기여할 필요성 또한 크다고 할 수 있다.[67] 지금까지는 보험과 은행 그리고 통신과 에너지 분야의 운영자들은 잘 조직되어져 왔으며, 독일에서는 IT 안전법을 통해 그간 언급되지 않았던 부문까지 아우르게 되었으며, 법적인 수단을 통해 협업을 규정하게 되었다. KRITIS 실행계획의 도입 이래로 독일 정치권과 기업들에서 사이버보안과 관련하여 이미 많은 토론과 주목이 있었다는 것은 일반적으로 주지의 사실이다.

몇몇 연방부처들과 연방관청들은 취약인프라 운영자들과의 더 나은 협업을 원하며, 한편으론 취약인프라 운영자들 또한 이러한 희망을 표출한다. KRITIS 전략, KRITIS로의 전환계획, KRITIS 실행계획 그리고 정보인프라 보호를 위한 국가계획(NPSI)에서는 정치권이 취약인프라 운영자의 사이버보안을 위한 책임 또한 강하게 지는 한 취약인프라 보호의 책임이 항상 국가, 경제계, 그리고 사회에 있는 것으로 간주한다.[68]

다. 독일의 사이버안전 전략(Cyber-Sicherheitsstrategie)

독일 사이버안전 전략은 2011년 연방의회에서 의결되었고 크리티스 실행계획과 2005년의 정보인프라 보호를 위한 국가계획으로부터 한층 발전된 것으로 간주되었다.[69] 이는 사이버범죄나 사이버테러리즘처럼 사이버보안에 있어 높은 중대성을 가지는 안전정책의 많은 분야를 포괄한다.

독일의 사이버안전 전략의 형성은 그것이 유럽 안전전략과 기준들에

67) Dominika, Zendler, “Zur strategischen Planung vonCyber Security in Deutschland”, AIPA 2 Lehrstuhl Internationale Politik Universitat zu Koln, 2016, p.31.
68) Bundesministerium des Innern, “Cyber-Sicherheitsstrategie fur Deutschland”, 2011, P.3.
69) Kullik, J, “Vernetzte (Un-)Sicherheit? Eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik“, 2014, p.92.

초첨을 맞추고 있음을 알 수 있으며, 특히 2003년의 유럽 안전전략과의 공통점들을 많이 찾아볼 수 있다. 하지만 2010년이 되어서야 유럽 정치권의 안전전략은 당시까지 에스토니아, 영국 그리고 슬로바키아에만이 가지고 있었던 국가 사이버안전 전략을 다른 많은 구성국들이 발전시키도록 이끌었다.[70] 몇몇 EU 구성국들이 이미 사이버안전 전략을 보유하고 있기는 하였으나, 2013년에야 공통의 유럽전략이 의결되었다. 독일의 사이버안전 전략은 모두 열 개의 전략적인 목표와 조치를 포괄한다.[71]

1. 취약인프라 보호
2. 독일 내 시민들과 중소기업의 IT 시스템과 관련된 안전
3. 공공행정에서의 IT 안전 강화
4. 국가 사이버방어 사령부(Cyber-Abwehrzentrum) 설치
5. 국가 사이버안전 위원회(Nationaler Cyber-Sicherheitsrat) 설치
6. 사이버범죄에 대한 효과적인 투쟁
7. 유럽 및 세계 사이버안전을 위한 효과적인 협력
8. 신뢰성 있는 정보기술 투입
9. 연방기구들의 인력개발
10. 사이버공간에서의 공격을 방어하기 위한, 권한 있는 국가기관으로부터 결정되고 온전한 기구

여기서는 취약인프라 보호에 초점이 맞추어졌으며, 이는 해당 분야 및 필요 기술들이 고려되어야 한다. 정치권 내에서 그리고 경제계와 함께 협업을 성공적으로 이끌기 위하여, 안전한 IT 시스템들과 공공행정에서 높

70) Berger, c, “Zwischen Strafverfolgung und nachrichtendienstlicher Analyse”, Konsequenzen aus der Europaisierung der Cybersicherheitspolitik fur Deutschland. Vierteljahreszeitschrift des Instituts fur Europaische Politik in Zusammenarbeit mit dem Arbeitskreis Europaische Integration (4). p.321.

71) Bundesministerium des Innern, “Cyber-Sicherheitsstrategie fur Deutschland”, 2011, pp.6-12.

은 수준의 IT 안전을 폭넓게 정착시키는 것뿐만 아니라 사이버방어 사령부(Cyber-AZ)와 사이버안전 위원회(Cyber-SR) 또한 설치되었다.

사이버안전 위원회는 제도적 수준에서 연방정부 내의 더 나은 협업을 위해 존재하지만, 또한 제휴 동맹자로서 경제계 대표단들과 관련이 되며, 이 점에서 사이버안전 위원회는 국가와 경제계 간 조정자라고 볼 수 있다.

위 6번(사이버범죄에 대한 효과적인 투쟁)과 관련하여, 사이버안전 전략에 있어서 사이버범죄와의 싸움은 국가적 뿐만 아니라 국제적으로도 '점증하는 도전'이라고 묘사되었다.[72] 유럽 수준에서 이것은 사이버범죄 영역에서의 형사법의 통일성 유지를 의미한다. 국제적 사이버범죄를 저지하기 위해서는 국제적 수준의 형법 상 조화가 필요하며, 유럽 수준에서 이는 컴퓨터범죄 영역에서 형법의 일치를 의미한다.

위 7번(유럽 및 세계 사이버안전을 위한 효과적인 협력)은 '세계적으로 안전한 사이버공간'이라는 목표 도달에 있어서 포기할 수 없는 요소인 국제적 협력과 연결되는 문제이다. 여기에는 유럽 수준에서의 협업 외에도 유엔이나 북대서양조약기구(NATO)와 같은 국제동맹과의 협력 또한 해당된다.

마지막 세 항목(8번부터 10번)에서는 신뢰성 있는 IT 시스템, 특히 취약인프라를 위한 연구의 필요성이 언급되었다. IT 시스템의 발전은 국가적 그리고 유럽적 수준에서 연합 구성원들, 파트너들과 함께 강화되어야 한다. 국가적 수준에서는 연방기구들의 권한과 자원, 특히 인력 영역에서의 점검이 초점이며, 거기에 추가로 연방과 주 수준에서의 국가적 기구 간, 그리고 경제기업과의 협력 필요성이 강조되었다. 이러한 협력은 사이버공격과의 싸움을 위한 수단으로 이해된다.[73]

---

72) Bundesministerium des Innern, "Cyber-Sicherheitsstrategie fur Deutschland", 2011, p.10.

73) Bundesministerium des Innern, "Cyber-Sicherheitsstrategie fur Deutschland", 2011, p.12.

라. 독일의 디지털 아젠다(Digitale Agenda)

18대 연방의회의 연정계약에서 2014년 9월 의결된 디지털 아젠다에 대한 계획이 확정되었다. 이는 디지털 변화를 촉진하기 위한 '네트워크 개편, 사이버안전 그리고 디지털 경제의 촉진'의 실행을 위해 성립되었다. 디지털 아젠다는 무엇보다도 독일의 혁신을 촉진하고, 고속통신망의 폭넓은 재편을 가속화하며, 시민 모두의 정보인프라 접근을 가능하게 하고, IT 시스템들의 안전을 높이는 것을 목표로 했다.

디지털 아젠다는 7개의 활동영역에서 구축되었으며, 이를 통해 연방내무부가 특히 '혁신적 국가', '디지털 사회' 그리고 '사회와 경제를 위한 안전, 보호 및 신뢰'의 영역에 관할권이 있음이 명시되었고, 독일 산업의 특별한 강점으로는 산업기술과 생산기술이 특정되었다.[74] '인더스트리 4.0'으로 표방되는 지능적·맞춤형 생산과 물류를 더욱 발전시키고, 이를 통해 지능적 서비스를 확대하며, 이로써 지속적인 성장 및 꾸준히 높은 취업률을 유지한다는 청사진이 제시되었다.[75] 인더스트리 4.0과 함께 구조조정이 불가피하고 이를 통해 일자리가 줄어들겠지만, 그럼에도 불구하고 여기서도 또한 새로운 고용이 창출되고 독일 산업의 경쟁력을 높이는 새로운 사업의 기회와 성장 영역들의 출현이 전망되었다.

인더스트리 4.0과 더불어 사이버보안 영역에서의 경제적인 기회들을 필연적으로 동반하는 제4차 산업혁명이 독일 내 연구들에서 추론되었다. 네트워크화 된 생산시스템들이 등장으로 인해 IKT(Informations- und Kommunikationstechnologien, 정보통신기술) 시스템들은 더 이상 경제분야에서 서로 분리되어 있지 않으며, 이로써 기업들 내부적으로 뿐만 아니라 하청 기업체(그들의 사이버 보안은 원청 기업에게도 중요한 의미를 가진다.)와도 모든 영역에서 네트워크화 된다. 망 연결에 따라 더 많은 사이버 공격의 기회가 발생하기 때문에, 월등히 높은 안전 요구기준이 필수적이다.

74) Die Bundesregierung, "Digitale Agenda 2014-2017", 2014, p.2.
75) Die Bundesregierung, "Digitale Agenda 2014-2017", 2014, p.2.

이로써 IT 서비스에서 예를 들어 클라우드 컴퓨팅과 같은 전혀 새로운 가치 창조 분야들이 생겨난다. 기업들의 생산과 관련된 정보들 같은 고(高)민감정보는 점증하는 사이버 공격에도 불구하고 반드시 보호되어야 한다.[76]

그러는 사이에 세계는 시민의 사생활의 영역이든지, 경제 또는 정치 영역이든지 간에 많은 영역들에서 네트워크화 되었으며, 이는 디지털 인프라의 개편을 요구한다.

디지털 아젠다에서는 경제분야에서 실행되어야 하는 몇몇 다른 조치들과 더불어 독일 디지털 안전산업의 강화가 강조되었고, '사회와 경제를 위한 안전, 보호 그리고 신뢰의 장(章)'에서 다시 한 번 사이버보안이라는 테마가 디지털 인프라의 안전, 시민 보호, 정보 보호, 사용자 보호 그리고 사이버공간에서의 안전에 초점을 두고 중점적으로 다루어졌다.[77]

디지털 아젠다는 데이터 보호에서부터 혁신 촉진까지 폭넓은 영역을 그 과제로 포괄하고 있으며, 따라서 향후 디지털화 과정의 진행에 방향성을 제시할 수 있도록 연방부처들의 활동이 망라되어 아젠다로 이행되게 되었다. 그 계획을 실행할 수 있기 위해서는 안전기구들의 기술적 관점 및 인력적 관점에서의 더 나은 준비 등과 같은 사이버안전 구조의 전략적인 새 기준이 필요하게 되었다.

마. 연방과 주들의 IT 기획 위원회(IT-Planungsrat von Bund und Ländern)

'연방과 주들의 IT 기획 위원회'의 설립을 위한 계약 및 이와 결부된 요구사항들이 2010년 4월 1일 발효되었다. 연방정부의 정보기술 전권위원들과 각 주들의 정보기술 책임자들이 그 구성원으로 편성되었다. 더 나아가 경제계와 정치계에서 더 많은 대리인들이 고문으로 참여할 수 있다.

---

76) Fraunhofer, "Strategie und Positionspapier Cyber-Sicherheit 2020", Herausforderungen fur die IT-Sicherheitsforschung, p.13.

77) Die Bundesregierung, "Digitale Agenda 2014-2017", 2014, pp.30-33.

독일을 위한 사이버안전 전략에서는 “효과적인 IT 안전은 연방행정의 모든 기구들을 대상으로 한 강력한 구조와 체계를 필요로 한다.”고 명시하고 있다. 이러한 과제는 연방과 각 주들의 독일을 위한 사이버안전 전략에 맡겨졌다. 기구들은 데이터 안전에서 모범적 선례를 채택하고, 이를 바탕으로 통일적으로 행동하게 되며, 이를 위해 가용 자원들이 적정하게 분배되고 투입된다.

IT 국가계약에서는 무엇보다도 전자정부프로젝트(E-Government-Projekte)가 행정 분야에서의 정보기술 발전과제로서 진행된다. 연방과 주들의 IT 기획 위원회는 구상된 프로젝트와 그로부터 도출되는 연방과 주정부들 간 협업의 실행에 권한이 있다. 더 나아가 연방과 주들의 IT 기획 위원회는 연방과 주정부들을 대상으로 IT 안전 표준에 관한 문제들을 다룬다. 이를 위해서는 연방과 주정부들 간 협업이 필수적이며, 그 협업의 책임은 연방과 주들의 IT 기획 위원회에 귀속된다.

정보안전의 영역에서 아이티 기획 위원회는 현재까지 ‘공공행정에서의 정보안전을 위한 기본 노선’ 그리고 이에 속하는 실행계획을 의결하였다. 그 계획은 공공행정의 정보 경영을 지향한다. 2015년 이래로 베를린은 내부에 국가비서와 함께 IT 기획위원회 위원장을 두고 있다. 그 위원장은 온라인 거래의 재편과 수기양식 요구의 철폐를 통한 전자화에 중점을 두고 있다. 독일 연방의회에 대한 사이버공격 가능성의 관점에서 보면, 독일 연방의회의 IT 시스템들에 대한 사이버보안이 아직까지도 개선의 여지가 큰 상황이며, 지금까지 연방의회행정을 포함하는 연방행정을 위해 취해진 조치들이 아직까지 충분하지 않은 것으로 평가된다.[78]

3. 사이버보안 영역에서의 정치 기관들

독일에서 사이버보안이라는 과제는 다양한 연방부처와 연방관청들에

78) Bewarder, M, “Verfassungsschutz verfolgt Spur nach Russland”, Die Welt, 2015.

게 나누어져 있다. 사이버보안을 위한 과제들은 독일 내부의 안전을 위한 책임에 속한다는 점에서 연방내무부에 속하는 것이 당연시 된다.[79] 또한 연방내무부의 업무범위에는 사이버보안 영역에서 과제를 담당하는 대부분의 연방관청들이 속한다. 여기에는 연방정보기술안전청(BSI), 연방범죄수사청(BKA) 그리고 연방헌법보호첨(BfV)이 속한다. 추가로 연방경제에너지부(BMWi), BMVg(연방국방부), 연방교통디지털인프라부(BMVi) 그리고 외무청(AA)이 사이버보안의 영역에서 과제를 담당한다. 사이버방어 분야에서는 연방국방부가 최고위 업무관서이며, 위에서 거명된 나머지 연방부처들은 연방국방부를 지원하도록 되어 있다.

연방정보기술안전청은 연방내무부 소속 하에 설치되어있다. 이 두 기관은 독일에서의 사이버보안에 중요한 의미를 가지는 바, 이 두 기관에 관해서 중점적으로 다루기로 한다.

가. 연방내무부(BMI, Bundesministerium des Innern)

연방내무부는 다양한 내부정책 과제를 담당한다. 연방내무부가 주도적으로 이끄는 독일연방공화국 내부의 안전은 매우 중요한 영역이다. 취약인프라의 안전을 위한 연방내무부의 관할권은 이미 2009년 크리티스 전략에서 “취약인프라 보호를 위한 중앙적·국가적 조치는 연방내무부 관할부문으로 조정된다.”고 확립되었다.[80] 연방내무부는 다른 연방기구들로부터 취약인프라 보호에 있어 분석, 위험 평가 그리고 보호 컨셉트 등의 형태로 지원을 받는다. 연방내무부는 2005년 취약인프라 보호를 위한 국가계획을 시작으로, 2007년 크리티스 실행계획, 2009년 크리티스 전략, 2011년 사이버안전 전략, 그리고 2014년 디지털 아젠다 등 사이버안전 정책의 모든 중요한 전략과 계획들을 이끌어 왔으며, 입법 특히 IT 안전법 입안에서 중대

79) Dominika, Zendler, “Zur strategischen Planung vonCyber Security in Deutschland”, AIPA 2 Lehrstuhl Internationale Politik Universitat zu Koln, 2016, p.44.

80) Bundesministerium des Innern, “Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS Strategie)”, 2009, p.3.

한 영향력을 행사하였다.

국가사이버방어사령부(Cyber-AZ)를 통한 연방기구들 간의 빈틈없는 맞물림 덕분에 사이버 보안의 영역에서의 과제 분배로 인한 정보손실은 거의 없다고 평가되지만, 그럼에도 불구하고 여기에서 또한 개선의 여지는 있어 왔다.[81] 사이버안전 과제 관련 정보의 분산으로 인한 연방부처들과 연방관청들에의 단편화가 야기하는 협업과 정보손실의 문제점은 조직으로 인한 것이 아니라 오히려 인간 요소에 의존하는 경우가 많다.

나. 연방정보기술안전청(Bundesamt für Sicherheit in der Informationstechnik, BSI)

연방정보기술안전청은 1991년에 설립되었으며, 연방내무부의 업무영역에 속한다. 연방정보기술안전청은 정보사회의 IT 안전 관련 문제를 위한 독립적이고 중립적인 기구이며, 연방의 IT 안전을 관할한다.

연방정보기술안전청은 약 600명의 종사자를 거느린 독일의 사이버보안을 위한 국립 안전기구며, 종사자들은 법률가, 정치학자 그리고 기술정보 영역 출신들이 대부분이다. 사이버보안 테마의 현행성과 전문가 부족으로 인해 이 영역에 추가적인 종사자를 찾는 데 애로를 갖고 있는 것으로 알려져 있다.

연방정보기술안전청은 사이버방어사령부에서의 연방 선도적 역할을 맡고 있으며, 연방행정의 IT 보안에 대해서도 관할권을 갖는다.

그 소속 위원회에서 경제 분야 대표단들과의 교류가 이루어지는데, 사이버안전 연합(Allianz für Cybersicherheit), 또는 2014년 의결된 크리티스 실행계획에 따라 설립된 KRITIS 실행계획 위원회 등이 그 예이다. 연방정보기술안전청은 지식산업, 통신 및 뉴미디어 관련 연방연합인 비트콤

81) Dominika, Zendler, “Zur strategischen Planung vonCyber Security in Deutschland”, AIPA 2 Lehrstuhl Internationale Politik Universitat zu Koln, 2016, p.47.

(BITKOM)과 함께 사이버안전 연합도 설립하였다. 사이버안전 연합은 그 구성원들을 위하여 지식과 경험의 교류를 제공하며, 현재 1,283개 기관들을 구성원으로 두고 있다. 그 구성원들은 사경제의 기업들뿐만 아니라 공공분야까지 망라하며, 거기에 참여하는 모든 기관들은 상담파트너를 두고 있다.

연방정보기술안전청은 기업들과 시민들을 위해 수많은 조언, 표준 및 현황 정보를 제공하고 있다. 대상 그룹은 1)연방, 2)경제계 그리고 3)시민들이며, 이 업무분야에 있어서 연방정보기술안전청의 구체적 임무는 예방, 감지 그리고 대응이다.

연방정보기술안전청은 IT 안전법 초안 마련에 있어서 연방내무부에 적극 협력하였다. IT 안전법을 통해 보고의무가 도입되었는데, 연방정보기술안전청은 이미 이전부터 IT 안전 사건들에 대해 이미 보고를 받고 있었으나, 보고된 사건들은 실제 사건들의 숫자에 현저히 미치지 못하는 수준이었다. 그러나 연방정보기술안전청은 그 업무에서 사건의 범인을 찾아내고, 기업들에 더 나은 조언이 될 수 있는 정보를 기업에 제공해야 했으며, 따라서 기업들과의 더 나은 협업이 요구되었다.

IT 안전법을 통해 연방정보기술안전청에 주어진 과제는 더 많은 인력 배치를 통해서만 이루어질 수 있는 것들이며, 연방정보기술안전청은 그 과제에 따라 수많은 중요 연방기구 및 기업들과의 협업을 이끈다. 다만, 사이버보안의 영역에서 다양한 연방기구의 과제들을 하나로 합병하는 것이 별 의미가 없으며, 개별 연방기구들이 사이버공격을 스스로 방어할 수 있도록 강화되어야 한다는 일부 의견 또한 있어 왔다.[82] 그러한 취지에서 연방정보기술안전청의 직원들이 기업들의 안전사건으로부터 교훈을 얻고, 기업들의 사이버보안 대응능력을 강화하기 위해 직접 기업들로 진출하는 방안도 추진된 적이 있으나, 그로 인한 중립성 훼손에 따른 부작용 우려로 인해 실제로 진행되지는 않았다.

82) Dominika, Zendler, “Zur strategischen Planung vonCyber Security in Deutschland”, AIPA 2 Lehrstuhl Internationale Politik Universitat zu Koln, 2016, p50.

국제적 수준에서 연방정보기술안전청은 외무청(AA)와의 협업 또한 유지한다. 더 나아가 연방정보기술안전청은 유럽연합(EU)와 북대서양조약기구(NATO) 수준의 활동그룹과 위원회들에 있어서 독일연방을 대표한다. 다만 그러한 국제적 수준의 협업은 전 세계를 아우르고 있다고 보기는 어려우며, 유럽의 수준에 놓여있다. 프랑스의 관할권 있는 연방기구가 독일의 연방정보기술안전청과 유사하게 조직되어 있기 때문에 특히 프랑스와의 협업이 원활히 이루어지고 있다.

연방정보기술안전청의 트렌드 관찰과 기술적 모니터링은 IT 안전에 있어서는 진보적이라고 평가된다. 비록 이러한 관찰과 모니터링을 통한 예측이 정확성을 보장하지는 않지만, 이 분야에 있어서는 지속적 발전이 관찰되고 있다. 이로써 연방정보기술안전청은 기술 발전의 속도와 이에 동반해 나타나는 범인들의 공격방법들을 통해 새로운 요구사항을 제시한다. 이 요구사항들에 대응하기 위하여 전통적인 커뮤니케이션 구조 대신에 자동화된 구조를 더 발전시키고, 정적인 보호조치들이 역동적인 보호조치로 전환되고 있다.[83]

미래를 위해 연방정보기술안전청은 IT 기본보호(IT-Grundschutz)를 개량할 것을 계획하고 있다. IT 기본보호와 함께 연방정보기술안전청은 '정보안전을 위한 기초'를 달성할 수 있는 정보와 표준을 제공한다.[84] 특히 중소기업들에게는 이를 통해 개선된 IT 안전에의 진입 문턱이 더 낮아지게 된다. 그러나 기술발전의 빠른 속도로 인해 IT 기본보호는 잦은 갱신이 필요한 반면, IT 기본보호의 작업은 사용자들과의 협업으로만 성취되는 사항이기 때문에 결코 쉽지 않은 과정이다. 이러한 작업과 연방정보기술안전청의 다른 과제들의 실행에 있어서 사이버안전 분야 연구를 통한 기여는 매우 중요한데, 연방정보기술안전청이 직접 사이버안전을 연구하지는 않기 때문이다.

---

83) Dominika, Zendler, "Zur strategischen Planung vonCyber Security in Deutschland", AIPA 2 Lehrstuhl Internationale Politik Universitat zu Koln, 2016, p51.

84) Bundesamt für Sicherheit in der Informationstechnik, "IT-Grundschutz", 2015.

제6장 결 론

제1절 사이버위기관리법 제정

가. 사이버위기관리법 제정의 필요성

산재해 있는 사이버테러 대응 및 위기관리 법제를 정비하여 국가 차원의 사이버위기를 예방하고 위기 발생 시 일원화된 종합적인 사이버테러 대응 및 위기관리체계를 구축하기 위하여 조속히 국가 사이버위기 관리법을 제정할 필요가 있다. 현재 우리나라는 국가 사이버위기 관리에 관한 개별 법률들이 산재되어 체계화되어 있지 못하며, 법률 간의 협력이나 연계가 미흡한 실정이다. 따라서 전통적 안보 차원, 국가핵심기반 차원, 국민생활 안전 차원 등에서의 국가 사이버위기를 포괄할 수 있는 기준이 되는 법률의 제정을 통하여 국가 사이버위기 관리와 관련된 법률을 체계화하는 것이 요구된다.

이와 함께 지금까지는 각 기관 간 역할이나 국가차원의 대응체계를 고려하지 않고 소관부처 중심으로 업무수행이 이루어져 정보공유와 업무협조에 있어서도 소극적일 수밖에 없었고, 사이버테러로 인한 침해사고와 관련한 민간기업의 정보 제공, 정보보호 안전진단 등 침해사고의 최소화 방안이 미흡하였다. 이러한 문제점들을 개선하며 실질적인 대응업무를 마련하고 정착시키기 위해서는 관련 법령들의 개선이 필요하다.

그리고 현재까지 사이버위기 관리를 위한 국내의 독립적인 법률의 부재로 인하여 국가 핵심기반시설이나 시스템에 대한 국내외 사이버공격을 예방하고 대비하며 실제로 사이버위기가 발생하는 경우 공격에 대응하는 시스템이 미흡한 상태이다. 특히 민간기업 및 개인에 대한 사이버위기는 물론 국가사회적으로 중요한 기능을 수행하는 핵심기반 마비와 관련된 사이버위기 관리를 위한 체계 구축이 필요하다.

나. 관리 대상으로서의 ‘취약인프라’ 개념 도입

제정되는 사이버위기관리법은 취약인프라 관리의 법적 근거가 되어야 하며, 취약인프라에 대해 명확한 정의를 통해 어떤 조직이나 기업이 이에 해당하는 지에 관한 혼선이 없도록 해야 할 것이다.

취약인프라와 관련하여 독일 「IT 안전법」은 “에너지, 정보기술 그리고 원격통신, 운송 그리고 교통, 건강, 물, 식품 및 경제와 보험분야에 속하고, 그 부족이나 침해로 인해 중대한 공급부족 또는 공공의 안전에 위협이 발생할 수 있기 때문에 공동사회의 기능에 큰 의미를 갖는 것을 말한다.”라고 정의하고 있다.

다. 취약인프라 운영자의 의무

현재 국내의 산재된 법률체계 하에서는 사이버테러로 인한 침해사고와 관련한 민간기업의 정보 제공, 정보보호 안전진단 등 침해사고의 최소화 방안이 미흡한 실정이다. 사이버위기관리법 제정을 통해 취약인프라 운영자들을 대상으로 ‘침해사고를 예방하기 위한 IT 안전의 최소요구기준 준수의 의무’, 그리고 ‘침해사고 발생 시 피해 확산 방지와 신속한 범인 검거를 위한 보고의무’를 명시함으로써 취약인프라 보호의 목적을 달성할 수 있도록 하여야 할 것이다.

제2절 사이버안전 체계 구축

사이버테러에 대한 범국가적 차원에서의 대응태세 확립을 위해 국가안전보장회의(NSC)를 중심으로 ‘국가사이버안전센터’는 국가 공공분야, ‘국방정보전대응센터’는 국방분야, ‘인터넷침해사고대응지원센터’는 민간분야, ‘국가보안기술연구소’는 교육분야, ‘정보공유분석센터’는 통신·금융분야, ‘사이버범죄수사기구’는 사이버범죄행위에 대한 수사활동의 대응업무를 각각

지원하면서 사이버테러 정보분석을 통한 경보를 발령하고 또한 상호 간에 전파하고 있다. 그러나 핵심적인 조정역할을 담당하고 있는 국가안전보장회의 내에는 정보보안문제를 총괄하고 조정할 수 있는 전문가 그룹이 부족한 것이 현실이고, 각 기관별 대응센터간 정보공유 및 협조체제 역시 미미할 뿐만 아니라 실무 주도기관이 부재한 실정이다.

가. 범 국가차원의 대응체계 구축

사이버테러에 대해 체계적이고 효율적으로 대처하기 위해서는 범 국가차원의 대응체계를 구축하고 이 대응기구를 통해서 지금까지 각 부처와 연구기관 등에서 분산 수행되어 온 대응전략 및 연구개발 기능을 유기적으로 통합·조정하여야 한다. 이를 위해서는 예방대책은 국가, 공공분야, 민간분야, 국방분야로 나누어 대응체계를 구축·운영하는 것이 필요하며, 이러한 대응체계를 통하여 정부기관과 민간기업 및 개인에게 국가 사이버안보 정책을 설정하고, 민·관·군 사이버테러 대응조직과 기능을 통합하여 체계적으로 조정할 수 있는 기능을 부여함으로써 사이버테러로부터 효과적인 초기 대응을 할 수 있을 것이다.

나. 실무 주도기관 명확화

사이버테러에 관해서는 정보통신망법, 정보보호기반보호법, 전자정부법, 국가사이버안전관리규정(대통령령) 등 다수의 법령이 규제하면서 기관 간 임무가 중첩 및 실제 사이버위기가 발생 시 각 기관의 책임과 역할이 불분명의 문제가 있다. 게다가 한국의 사이버테러 대응체계는 대통령 훈령으로 규정되어 있어서 유관부처 간 역할과 책임이 불분명하고 구속력이 약할 뿐만 아니라 상위 법률과 충돌이 발생하면서 많은 한계를 드러내고 있다. 따라서 법적 근거 마련을 통한 실무 주도기관의 명확화가 시급한 과제

이며, 또한 실무 주도기관은 정책기능 뿐만 아니라 자체 연구개발 인력 보유를 통해 기술적 표준이나 IT 최소요구 기준 마련 등 연구개발 분야도 망라하는 것이 효과적인 사이버테러 대응에 중요한 요소이다.

한국의 실무 주도기관 설정과 관련해서는 그간 「국가사이버안전관리규정」을 통해 사실상 공공분야의 사이버안전 정책 개발 및 실무를 주도하고 있는 국가정보원의 '국가사이버안전센터'를 확대하는 방안이나 행정안전부 소속 하에 새로운 기관을 창설하는 방안 등이 그간 각계에서 논의되어 왔다. 그러나 정보기관의 정책집행 참여에 따른 부처와의 정책경쟁 발생, 정보기관의 특성에 기인하는 정보공유 한계, 정보기관 활동의 법률적 근거 미흡, 국제협력 역량의 한계 등의 문제점을 고려할 때 IT 안전과 사이버테러 대응을 전담하는 새로운 기구의 창설이 더욱 적합해 보이며, 따라서 IT 안전 과제를 연방내무부 소관사항으로 명시하고, 그 산하에 연방정보기술안전청을 설치하여 정책 집행, 민간분야와의 협력 및 지도·관리, 국제적 수준의 협력, 연구개발 등을 담당하며 실무 주도기관으로서의 입지를 명확히 하고 있는 독일의 사례는 참조할 만한 가치가 있다.

[참고문헌]

Ⅰ. 국내문헌

강동범, “정보통신망법상 사이버범죄처벌규정의 검토”, 인터넷법률 제39호, 법무부, 2007.

곽병선, “사이버범죄 예방을 위한 법제도적 해결방안 - 가칭 ‘사이버범죄 특별법’ 제정논의를 중심으로 -“, 법학연구 제24집 제3호, 원광대학교 법학연구소, 2008.

김기범, 장윤식, “사이버범죄수사론”, 경찰대학, 2012.

김도승, “사이버위기 대응을 위한 법적 과제: 미국의 사이버위기 대응체계 현황과 시사점을 중심으로”, 방송통신정책 제21권 제17호, 정보통신정책연구원, 2009.

김연준, 옥정석, “국가위기관리를 위한 사이버테러 대응체계 구축방안”, 인문사회과학연구 제18호, 2011.

박지형, “국가 사이버안전체계 개선에 관한 연구”, 경기대학교 대학원 석사학위 논문, 2005.

서보학, “인터넷상의 정보유포와 형사책임”, 형사정책연구 제12권 제3호, 2001.

양근원, “사이버테러의 실태와 법적대응에 관한 연구”, 경희대학교 대학원 석사학위논문, 2004.

유석준, “사이버범죄에 대한 외국의 입법례”, 영산법률논집 제5권 제1호, 2008.

윤해성, “사이버침해 유형에 관한 형사법적 검토”, 법무연구 제2권, 대한법무

사협회 법제연구소, 2011.
윤해성, 강석구, 박영우, 김민호, 권헌영, 김도승, 김기범, “사이버안전체계 구축에 관한 연구”, 형사정책연구원 연구총서 10-07, 2010.

이동희 외, “국제 사이버범죄 아카데미 모델 개발”, 경찰청, 2010.

이필재, “유비쿼터스 환경과 국가사이버위기관리 법제도의 문제점 및 개선방안” (국가위기관리학회보), 2009.

장기범, “국가종합위기관리”(법문사), 2009.
정재영, “사이버 테러에 대한 국가별 대응실태 연구”, 국민대학교 정치대학원 석사학위 논문, 2010.

조병인, “사이버경찰에 관한 연구”, 한국형사정책연구원, 2000.

최진태, “테러리즘의 이론과 실제”, 대영문화사, 2006.

“2010 국가정보화백서”, 2010, p.171.

Ⅱ. 외국문헌

Bendiek A, und Ulmer, K, “Cybersicherheit - eine facettenreiche politische Herausforderung. Aus internationale Zeitschriften 2012/2013”. SWP-Aktuell 3. Stiftung Wissenschaft und Politik. 2013.

Berger c, “Zwischen Strafverfolgung und nachrichtendienstlicher Analyse”, Konsequenzen aus der Europaisierung der Cybersicherheitspolitik fur Deutschland. Vierteljahreszeitschrift des Instituts fur Europaische Politik in Zusammenarbeit mit dem Arbeitskreis Europaische Integration (4), 2013.

Bewarder M, “Verfassungsschutz verfolgt Spur nach Russland”, Die Welt, 2015.

Bundesamt fur Sicherheit in der Informationstechnik, “Das Lage der IT-Sicherheit in Deutschland 2014”, 2015.

Bundesamt für Sicherheit in der Informationstechnik, “IT-Grundschutz”, 2015.

Bundesamt für Sicherheit in der Informationstechnik und Bundesamt für Bevolkerungsschutz und Katastrophenhilfe, “Zusammenarbeit im Rahmen des UP KRITIS”, 2011

Bundesministerium des Innern, “Cyber-Sicherheitsstrategie fur Deutschland”, 2011.

Bundesministerium des Innern, “Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)”, 2015.

Bundesministerium des Innern, “Nationaler Plan zum Schutz der Informations- infrastrukturen(NPSI)”, 2005.

Bundesministerium des Innern, “Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS Strategie)”, 2009.

Bundesministerium des Innern, “Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen”, 2007.

Corporate Trust Business Risk & Crisis Management GmbH, “Studie: Industriespionage 2014, 2015.

Deutscher Bundestag, “Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Agnes Malczak, Omid Nouripour, Tom Koenigs, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN - Drucksache 17/6802”, 2011.

Deutscher Bundestag, “Koalitionsvertrag zwischen CDU, CSU und

FDP. Wachstum. Bildung. Zusammenhalt, 17. Legislaturperiode", 2009.

Deutscher Bundestag, "Koalitionsvertrag zwischen CDU, CSU und SPD (2013). Deutschlands Zukunft gestalten, 18. Legislaturperiode", 2013.

Die Bundesregierung, "Digitale Agenda 2014-2017", 2014.

Dominika, Zendler, "Zur strategischen Planung von Cyber Security in Deutschland", AIPA 2 Lehrstuhl Internationale Politik Universitat zu Koln, 2016.

Fraunhofer, "Strategie und Positionspapier Cyber-Sicherheit 2020", Herausforderungen fur die IT-Sicherheitsforschung, 2014.

Gaycken S, "Cyberwar. Das Wettrusten hat langst begonnen. Vom digitalen Angriff zum realen Ausnahmezustand", Wilhelm Goldmann Verlag, 2012.

Hansel M, "Interantioanle Beziehungen im Cyberspace. Macht, Institutionen und Wahrnehmung", 2013.

Heeg T, "Cyberkriminalitat. Deutsche Firmen erleiden Milliardenschaden", Frankfruter Allgemeine, 2015.

KPMG, "IT-Sicherheit in Deutschland Handlungsempfehlungen fur eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes", 2014.

Kullik J, "Vernetzte (Un-)Sicherheit? Eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik", 2014.

Luiijf E, "New and emerging threats of cyber crime and terrorism. In Akhgar, Babak/Staniforth, Andrew/Bosco, Francesca", Cyber crime and cyberterrorism investigator's handbook, 2014.

Schnaas D, "Die Angst vor der Innovationsperipherie. Wirtschaftsspionage ganz neuer Qualitat gefahrdet den Vorsprung des Westens", Internationale Politik, 2014.

Sievers U, "BSI: Der Cyberraum ist ein großes Haifischbecken", 2013.
Singer T, “Cyberwarfare? Damoklesschwert fur das Volkerrecht?”, Sicherheit & Frieden, 2014.
Tessier Stall, “The future of cybersecurity”, The Hague Centre for Strategic Studies and TNO, 2011.
Tschersich T, “Zur Notwendigkeit eines Umdenkens beim Thema Cybersicherheit”, Datenschutz und Datensicherheit, 2011.