< 훈련결과보고서 요약서 >

성 명	유 윤 근	소 속	경찰청
훈 련 국	독 일	훈련기간	2016. 2. 18. - 2018. 2. 17.
훈련기관	아우크스부르크 대학교 루트비히-막시밀리안대학교 형사법연구소	보고서매수	107 매
훈련과제	사이버테러 대응 체계 및 정책에 관한 연구		
보고서제목	독일의 사이버테러 대응 체계 및 정책		
내용요약	※ 붙임 참조		

요 약 문

(주제 – 독일의 사이버테러 대응 체계 및 정책)

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.

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 사이버공격으로 인한 국가와 국민들의 피해, 공포는 정보화의 역기능이자 '사이버테러'라는 새로운 유형의 테러라 할 수 있다.

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.

독일의 경우 '2009년 연방정부 연정계약'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 있

어서 취약한 인프라를 운영하는 기업)들과의 협업·지도 체계를 효율적으로 운영하고 있다. 특히 독일의 사이버테러 대응체제는 크리티스(KRITIS) 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 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, 이 글에서는 그 논의과정 및 구체적 내용에 대해 다루었으며, 이를 통해 대한민국의 사이버테러 대응 체제와 법률에 대한 개선방안을 제언하였다.

Ⅰ. 국내 사이버테러 대응 체계의 문제점

1. 초기 대응과 다양한 법규로 인한 대응체제 혼선

한국의 경우 체계화된 법률의 부재에 따른 문제점이 나타나고 있다. 한국은 사이버테러 범죄의 역기능에 대처하기 위한 방안으로 각 부처별로 상황에 따라 필요할 때마다 특별법을 제정하는 방법을 선택했다. 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. 이러한 정부의 대처방법은 각 법률 간 형벌의 불균형, 법체계상의 문제, 다수의 유사한 규정이 여러 법률에 산재되어 있는 문제점 등을 야기하였다.

다음은 초기 위협측정 체계 미흡의 문제로, 사이버공간의 위협은 시

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

마지막으로 사이버공격 초기 귀속의 한계에 따른 문제점으로, 사이버공간에서는 사이버공격의 실체를 확인하기 어려워 특정 공격이 어떤 침해행위에 속하는 것인지를 파악하기 힘들다는 문제점이 존재한다. 즉, 사건 발생 초기에는 사이버테러 주체가 개인인지, 조직인지, 국가인지 확인하는 것이 어렵다. 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.

2. 정보기관과의 협력 및 법집행기관의 참여 미흡의 한계

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 등에서

는 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 신설 필요성이 제기된다.

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

Ⅱ. 독일의 사이버테러 대응 체계

1. IT 안전법

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 예상되었고, 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.

IT 안전법의 계획은 이미 2013년 연정계약에서 논의되기 시작하였으며, 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. 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 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.

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 속하며, IT 안전법의 구성은 아래의 표와 같다.

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

이 글에서는 IT 안전법 중 가장 핵심적인 내용을 담고 있는 연방정보기술안전청법에서의 개정사항을 살펴보았다.

2. 사이버안전 관리체계

독일 사이버안전 관리체계의 핵심을 이루는 용어는 크리티스(KRITIS)이며, Kritische Infrastrukturen(취약한 인프라들)의 머릿글자를 따서 조합된 단어이다. 이는 그 손실이나 침해가 지속적 공급부족, 공공안전의 중대한 장애 또는 다른 심대한 결과를 야기하는, 국가공동체를 위해 중요한 의미를 가지는 조직 또는 기관들을 말하며, 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 Versicherungs-wesen), 영양(Ernährung), 국가와 행정(Staat und Verwaltung) 등 9개 하위 부문들로 구성되어 있다.

이어서 연방 수준의 사이버안전 정책의 성립 과정과 그 내용을 다루

었는데 그 내용은 다음과 같다.

- 2009년과 2013년 연정계약에서의 사이버보안
- 취약인프라 보호 정책으로서 취약인프라 보호를 위한 국가계획, 정보인프라 보호를 위한 국가계획의 KRITIS로의 전환계획, KRITIS 전략, KRITIS 실행계획(UP KRITIS), 연방 실행계획(UP Bund), 연방 실행계획 위원회(UP KRITIS-Rat), 독일의 사이버안전 전략, 독일의 디지털 아젠다, 연방과 주들의 IT 기획 위원회
- 사이버보안 영역에서의 정치기관으로서의 연방내무부, 연방정보기술안전청

Ⅲ. 결론 및 제언

1. 사이버위기관리법 제정

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.

또한 관리 대상으로서의 '취약인프라' 개념 도입이 필요하며, 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.

그리고 취약인프라 운영자의 의무에 대한 규정이 필요하며, 사이버

위기관리법 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.

2. 사이버안전 체계 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 초기대응을 할 수 있을 것이다.

그리고 실무 주도기관의 명확화가 필요한데, 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 과제이며, 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 「국가사이버안전관

리규정」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.