주요국의 사이버테러 대응체계와 시사점 분석
– 미국·영국·독일 사례의 비교를 중심으로 –

권 오 국* · 석 재 왕**

〈요 약〉

사이버 영역에 대한 의존성이 심화와 현대사회의 상호연계성 강화로 인해 중요한 기반시설이나 조직에 대한 사이버 테러는 매우 치명적인 결과를 발생시킬 수 있다. 최근 한국의 국가기관을 비롯한 금융전산망에 대한 북한의 사이버공격이 시간이 지날수록 지능화·고도화되고 있는 상황이다. 핵심기반시설을 대상으로 한 북한의 사이버공격은 막대한 경제적 피해와 함께 사회혼란을 유발하고 있다. 본 논문은 미국, 영국 등 선진국들의 사이버테러 법률 및 조직체계를 중심으로 비교분석하여 우리에게 주는 시사점을 도출하는데 목적이 있다. 이들 국가들의 대테러 전략은 안보환경, 제도, 문화인 차이에도 불구하고 범정부차원의 대테러 업무 통합·협력 시스템 구축, 새로운 제도와 기관의 신설, 수사·정보활동 및 처벌 규정의 강화로 구체화된다. 한편, 우리의 경우 사이버 보안을 규율하는 일반법이 부재한 상황에서 개별 법률형태로 산재해있다. 따라서 우리는 선진국들의 사이버테러 대응 법적, 정책적 대응 동향을 검토·적용할 필요가 있다. 향후에는 사이버안보법 제정과 함께 사이버테러 사전 예방 및 복구 지원 등 위기관리 강화, 국가차원의 합동대응팀 운영, 민간 단체의 지원과 협조 필요성 등이 요구된다.

주제어 : 사이버테러, 대응체계, 법제현황, 사이버안보, 국가사이버안보기본법

* 경찰대 치안정책연구소연구관
** 건국대 안보재난관리학과 교수

목 차

Ⅰ. 서 론
Ⅱ. 이론적 배경: 사이버테러의 개념, 특징, 유형, 수단
Ⅲ. 미국, 영국, 독일의 사이버 안보 대응체계 비교
Ⅳ. 한국의 사이버 안보 대응체계 분석
Ⅴ. 결 론

Ⅰ. 서 론

정보화의 진전과 함께 해킹・사이버 테러와 같은 부작용이 발생함에 따라 국가사회와 개인에 대한 위협은 일상화되고 있다. 사이버 영역에 대한 의존성의 심화와 사회단위들의 상호연계의 강화로 인해 중요한 기반시설이나 조직에 대한 사이버 테러는 매우 치명적인 결과를 발생시킨다. 전시나 위기시에 주요 기반시설이나 지적 인프라에 대한 적대적 위협은 항상 존재해 왔다. 그러나 평화시 실제 세계에 대한 위협이 컴퓨터 해커로부터 비롯되고 있다는 점은 사이버 테러에 대한 대책 필요성을 말해준다.

탈냉전이후 국가간 대규모 전면전의 가능성은 현저하게 줄어든 반면, 사이버상의 갈등과 대립은 지속 확대되고 있다. 대표적으로 2007년 중국 해커부대의 미국 펜타곤 공격이나 2011년 G-mail계정의 해킹 발원지가 중국으로 밝혀짐에 따라 외교적, 군사적 마찰로 이어진 사례가 있다. 주요 선진국가의 사이버안보 체계를 분석해 보면 미국은 국토안보부, 영국・독일은 내무부, 프랑스는 국무총리실, 일본은 내각관방이 주무기관이 되어 관계기관들과 수평적 관계에서 협력체계를 이끌어 내고 있다. 이들 선진국가들 사이에서는 사이버테러가 국가안보 및 정보・통신・교통・전력 등 국가기간 산업에 지대한 영향을 미친다고 판단하여, 사이버테러와 관련된 법률체계를 정비 중에 있다. 미국은 '민・관 사이버보안 정보공유 촉진 행정명령'('15. 2. 13)

을 발표하여 국가사이버보안정보통합센터(NCCIC)의 기능 확대를 모색하고 있고, 일본은 「사이버보안기본법」('15. 7. 6) 개정안을 발의하였으며, 호주는 「통신법」('15. 10. 13)을 개정・발의한바 있다.

최근 한국의 국가기관을 비롯한 금융전산망에 대한 북한의 사이버공격이 시간이 지날수록 지능화・고도화되고 있다. 핵심기반시설을 대상으로 한 북한의 사이버공격은 막대한 경제적 피해와 함께 사회혼란을 유발하고 있다. 특히 국가・공공기관은 물론 농협('11), 금융・방송・신문사('13), 서울메트로・한수원('14. 12), 스마트폰('16) 해킹 등 상대적으로 보안이 취약한 민간 정보통신망에 대한 공격도 크게 늘어나는 추세이다. 본 논문은 미국, 영국 등 선진국들의 사이버테러 법률추진 및 조직체계를 중심으로 비교・분석하고 우리에게 주는 시사점을 도출하고자 한다. 이들 국가들은 안보환경, 제도, 문화적인 차이에도 불구하고 몇 가지 공통적인 특징을 보여주고 있다. 첫째는 대통령이나 수상 직속 또는 범 정부차원의 대테러 기능을 통합하거나 협력 시스템을 강화하고 있다. 둘째는 다양한 테러 위협 유형에 대응하여 이를 신속히 대응할 수 있는 제도와 기관을 신설하고 있다. 기존의 조직들은 관료제적 병리, 전문성의 부족, 조직의 관성 등으로 인해 사이버 테러위협을 예방하거나 조기 대응하는데 한계가 있을 수 있기 때문이다. 셋째, 민주주의 국가임에도 수사 및 정보활동을 강화하고 처벌규정을 강화하고 있다는 점이다. 이는 사이버테러 규정이 시민적 자유를 침해할 수도 있지만, 보다 큰 국가안보와 국민의 안전을 위해할 수 있다는 판단에 기인한 것이다.

한편, 우리나라의 경우 사이버 보안을 규율하는 일반법이 부재한 상황에서 개별 법률형태로 대응해 가고 있다. 따라서 이 같은 상황에서는 선진국들의 사이버테러 정책과 법제도의 장・단점, 운영실태를 면밀하게 검토하여 우리 실정에 맞게 선별 적용해 나갈 필요가 있다. 향후 사이버안보법이 제정될 경우 사이버테러의 사전예방 및 복구지원, 국가차원의 합동대응팀 구성・운영, 사이버 위협정보의 공유, 민간 단체의 지원・협조 체계구축 등이 입법 과정에서 심도 깊게 다뤄져야 할 핵심 의제가 될 것이다.

Ⅱ. 이론적 배경

1. 사이버 테러의 개념과 특징

사이버테러 용어에 대한 합의된 정의는 아직 없는 실정이나 “에너지, 교통, 정부 기관 등 주요 국가기반시설을 중단시키거나 정부 또는 시민들을 강제 또는 협박하기 위하여 컴퓨터 네트워크 도구를 이용하는 것”(CISI), “사이버상에서 개인, 국가의 전산망을 교란 또는 마비시키고 국가안보까지 위협하는 공격행위”(전웅, 2015: 318)로 정의될 수 있다.

사이버테러는 정보전쟁(information warfare), 사이버 범죄(cyber criminal) 등과도 혼동되기도 한다(Holt, 2012; 형사정책연구원 2012: 39-40). 그러나 사이버위협 행위자, 공격동기, 대상, 규모, 그리고 대응주체 등을 구분할 때, 일반 사이버 범죄와 사이버테러, 사이버전쟁의 개념규정은 달리 규정될 수 있다. <표 1>에서 보는 바와 같이 사이버 범죄가 단순 금전적 이득이나 개인적 보복에 동기가 있다면, 사이버테러는 정치적 목적을 의도한 테러조직이 국가급 주요시설을 공격 대상으로 삼는 행위이며, 사이버전쟁은 국가적 차원에서 정치・전략적 목적하에 국가전략 자산을 목적으로 가해지는 조직적 공격행위이라는 점에서 차이가 있다. 사이버전쟁은 사이버테러보다는 불확실하고 다소 논쟁적인 개념이다(Rid and McBurney, 2012: 7).

그러나 실제로는 사이버 공간[1]이라는 특수성으로 인해 ‘범죄와 테러, 전쟁’의 구별이 어려운 경우가 많이 발생한다.[2] 로저(Mike Rogers, 2013) 미 하원 정보위원회 위원장도 “대부분의 미 국민들도 이를 구별하지 못하고 있음”을 시인한 바 있으며, 린(William J. Lynn, 2013) 국방부 차관이 “사이버 공간을 제5의 전장(the Fifth domain of Warfare)로 규정”하고 있는 것도 구별의 어려움을 반영한 것이다.

1) 사이버공간은 정보가 생성되고, 전송되며, 저장・삭제되는 전자적 매개체로 정의할 수 있다. James B. Godwin(2014: 17).

2) 사이버공간에서의 각종 범죄나 테러 및 전쟁을 표현하는 용어는 결국 상대 국가의 네트워크를 무력화시키거나 파괴 또는 기능마비를 의도하는 포괄적 의미의 공격행위로 정의할 수 있다.Clay Wilson(2006: 7).

〈표 1〉 사이버범죄・테러・전쟁 유형분류

공격 유형	사이버범죄		사이버테러		사이버 전쟁
성격	일반 범죄자 개인이나 조직	↔	테러조직, 국가행위자	↔	국가행위자 또는 초국가적 테러 네트워크
동기	금전적 이득, 단순흥미, 개인적 보복	↔	정치적, 사회적, 종교적 목표	↔	국가 전략적 목표, 정치적 목표
대상	개인, 민간기업	↔	사회의 불특정 다수, 주요 국가기간시설, 교통, 전기, 수도, 금융, 방송 등 인프라, 정부기관, 국가급 주요민간 기업	↔	국가전체, 군사부문, 국가전략 기반시설
규모	개인이나 민간기업에 대한 심각한 침해	↔	사회전체 또는 사회의 불특정 다수, 국가의 일부 부문	↔	국가전역
대응 주체	검찰, 경찰 등의 일반 수사기관	↔	검찰청이나 경찰청 등의 중앙부서의 사이버 테러 전담기구, 국가정보원 등의 국가급 정보, 방첩기관	↔	대통령 지속의 국가안전보장회의, 국가안보실, 육・해・공군 등 국가 최고전쟁수행지도부

한편, 사이버 테러는 전통적인 테러와는 여러 가지 면에서 상이한 특징을 보여주고 있다(한희원, 2014: 337-338). 첫째는 수단적 측면에서 전통적인 테러가 폭탄 등 물리적 수단을 활용하는데 비해 사이버테러는 컴퓨터 바이러스, 전자우편, 해킹 등 비물질적인 도구를 사용한다. 둘째는 전통적인 테러의 경우 적군과 아군이 구분이 대체로 분명하고 물리적 공간에서 진행되는 반면, 사이버 테러의 경우 피아의 구분이 모호하며, 당연히 인터넷 공간에서 전쟁이 발생한다. 셋째는 전통적인 테러에 비해, 사이버 테러는 도발주체나 추적이 어려우며, 넷째는 전통적인 테러에 비해 상대적으로 비용이 저렴하다는 특징이 있다(전웅, 2015: 319).

2. 사이버 테러 유형과 수단

사이버 테러의 유형은 공격 수단 또는 피해를 중심으로 분류된다(형사정책연구원, 2012:59). '경찰청 사이버 테러대응센터'는 해킹, 바이러스유포, 메일폭탄, DOS공격 등 전자기적 침해장비를 이용하여 컴퓨터시스템과 정보통신망을 공격하는 행위를 사이버 테러형 범죄로 분류하고, 이를 해킹(단순침입, 사용자 도용, 파일등 삭제와 자료유출, 폭탄메일)과 악성프로그램으로 구분하고 있다.[3)]

또한, 사이버테러 공격의 파급효과와 영향력에 따라 일반적이고 효과가 낮은 수단들부터 구체적이고 강력한 효과를 보이고 있는 수단들로 구분하기도 한다.(Rid and McBurney, 2012: 7). 전자의 대표적인 것으로는 악성 소프트웨어(malware)가 있다. 이는 외부에서시스템에 부터 영향을 미칠 수는 있지만 기술적으로는 침투하여 직접적인 손실을 발생하지는 못한다. DDos는 원격조정 가능한 컴퓨터를 통해 특정 기관에 동시에 접속토록 하여 정보통신 서비스를 마비시키는 공격 수단이다. DDos는 실행과 방어가 다른 테러 수단에 비해 용이하며 초기에 공격 진원지 파악이 어렵고 재발가능성이 높아 상당히 위협적인 테러 수단이다.

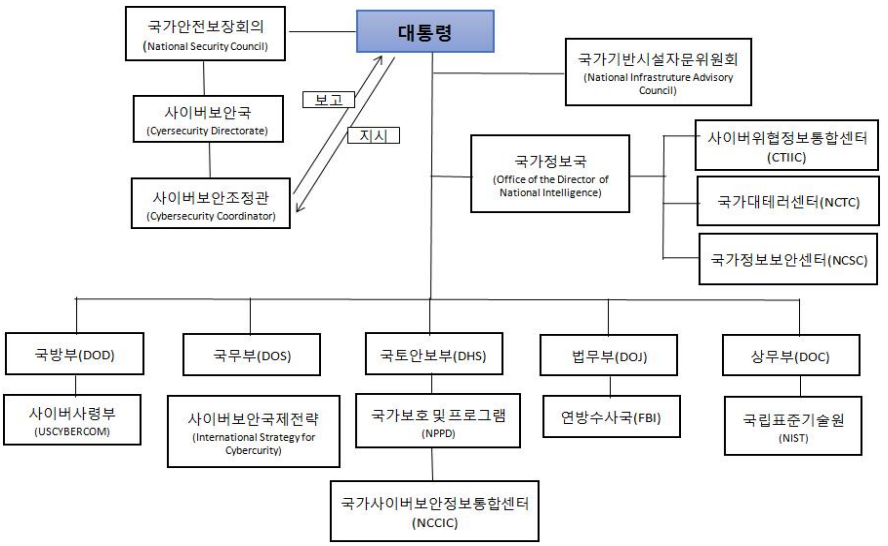
한편, 강력한 테러 효과를 보이고 있는 수단들 중에는 HARM(High-speed Anti-Radiation Missile)이 있다. 이는 상대방 목표 레이다를 추적, 탐지하여 파괴하거나 교란시키는 기능을 구비하고 있다. 이와 함께 객체이동가상 무기(Autonomous Mobile Cyber Weapons, AMCW)도 가장 강력한 파괴력을 보유한 테러 무기에 위치해 있다. AMCW는 공격목표 지점에 도달하여 적국의 기간통신이나 방공망 같은 주요 전산망을 교란시키거나 파괴하는 무기로 알려져 있다. 반면, 컴퓨터 하드웨어와 스프트 웨어 약점을 공격하는지 여부에 따라 구분할 수 있다(전웅, 2015: 320-321). 전자는 컴퓨터의 전자파를 수집해 컴퓨터 작업내용을 유출하는 TEMPEST(누설전자파), EMC(전자기 호환)등이 있다. 또한 후자의 대표적인 것으로는 전산망에 침투하여 바이러스를 삽입하거나 데이터 베이스를 파괴하는 해킹(Hacking), 시스템 내부 코드를 변경시키는 '논리폭탄'등이 있다.

3) 경찰청 사이버안전국(http://cyberbureau.police.go.kr, 검색일 2016. 11. 5).

Ⅲ. 주요국 사이버대응체계 비교

1. 미국

미국의 사이버안보 추진체계는 국가사이버보안조정관과 국가보안참모(National Security Staff) 內 사이버보안이사회(Cybrsecurity Directorate)에서 국가사이버안보 종합계획(International Strategy for Cyberspace, 2011)에 의거하여 추진되고 있다.



〈그림 1〉 미 사이버안보 추진체계

대통령 직속 국가사이버보안조정관이 국가안보회의에 상주하며, 사이버테러 및 침해사고시 총지휘관 역할을 수행하고, 국가안보국・국토안보부 등과 협력하여 대응한다. 이를 위해 국토안보부에 사이버공간에 대한 보안부서를 설치하고, 사이버 침해 예방・대비・대응・복구를 단계별로 관리・추진하며, 민간분야 보안업체 및 국내외 기관들과 파트너십을 구축하여 공동으로 사이버침해에 대응하는 동시에 국제협력에 주력하고 있다(한국과학기술원, 2011: 21). 주요한 업무로 연방네트워크 보

호강화, 국가안보통합센터(NCCIC) 구축, 사이버첩보계획 실현, 기밀 네트워크 보호, 행정부 안보체계 표준 실시간 감시 등을 목표로 하고 있다.

사이버보안 관련 연방법률은 약 50여개에 달하며, 주요법률은 9/11테러 이후 제정되었다. 그동안 기말사항이었던 「국토사이버보안종합계획」을 2009년 5월 '사이버공간정책리뷰(Cyber Policy Review)'를 통해 발표함으로써 체계적이며 일관된 정책을 추진 중이다(송은지・강원영, 2014: 5).

<표 2>는 미국의 사이버테러 관련 주요법적 근거, 정책기구, 주무기관, 정보통합기구, 수사기관 및 관련 기관을 정리한 것이다.

〈표 2〉 주요 법률적 근거 및 조직체계

구분 \ 법률		법률/조직체계	비고
법적 근거		컴퓨터보안법 (1987)	◆ 국립표준기술원에 보안표준 개발 책임부여 ◆ 상무부장관에게 보안기준 제정・고시 권한부여
		국가정보기반보호법 (1996)	◆ 국가정보기반 무단침입에 대한 형사처벌 규정 ◆ 데이터 장치 연결시스템 및 민간네워크 피해에 대한 형사처벌 규정
		국토안보법(2002)	◆ 사이버테러를 포함 국가적 위기 및 재해로부터 컨트롤타워 기능 및 권한부여
		전자정부법(2002)	◆ 연방정부기관의 사이버보안 책임 명확화 ◆ 연방보안사고센터 설립 ◆ 행정관리예산국 사이버보안 기준제정
		사이버보안강화법 (2010)	◆ 사이버보안 전문인력 양성 및 교육 ◆ 연방정부 R&D 우선순위 조정
		국가사이버보안보호법 (2014)	◆ 국가사이버 보안・통신 통합센터 설립(NCCIC 설치규정)
		사이버보안정보공유법 (2015)	◆ 사이버보안 위협에 대한 정보 민・관 정보공유 법적 근거마련 ◆ 정보공유자에 대한 면책규정
조직체계	정책기구	국가안전보장회의 사이버보안국	◆ 국가안보위원회 산하에 사이버보안국 신설 ◆ 국가사이버보안종합계획 입안・추진 ◆ 사이버보안조정관은 국가안보위원회의 위원과 대통령 특별보좌관 겸임 - 대통령에게 사이버보안정책 건의 - 州정부・민간부문과 긴밀한 업무협의 - 대규모 사이버침해 사고시 총지휘관 역할 수행(국방부・국무부・국토안보부・법무부・상무부와 협력)

조직체계	주무기관	국토안보부(DHS)	◆ 2002년 11월, 국가안보 및 치안유지에 필요한 22개 조직을 통합하여 설립 ◆ 사이버보안 관련 부서로 주요기반 시설 및 IT시스템은 국가보호프로그램단(National Protection and Programs Directorate, NPPD)이 담당 - 연방네트워크강화, 행정부 안보체계 실시간 감시 - 국가차원의 사이버테러 대응 훈련인 Cyber Storm을 격년제로 실시 ◆ 공유정보는 상무부, 국방부, 에너지부, 법무부, 재무부, 국가정보국과 자동화된 방식으로 실시간 공유
	테러정보통합기구	국토안보부 국가사이버보안정보통합센터(NCCIC) ⇩ (국가안전보장회의 활동지원) 국가정보국 국가사이버위협정보통합센터(CTIIC)	◆ 국가사이버보안정보센터는 2009년 11월 출범, 컴퓨터위기대응팀(US-CERT), 국가텔레커뮤니케이션조정센터(NCC), 국가사이버안보센터(National Cybercurity and Communications Integration Center, NCSC) 등의 조직을 흡수・통합 - 사이버보안위협지표 및 방어조치 정보, 사이버보안 위험과 사고 관련 정보공유 ◆ 2015년 3월 사이버위협에 효과적 대응 위해 국가정보국(DNI) 內 사이버위협정보통합센터(Cyger Threat Intelligence Integraton Center, CTIIC) 설치 - 사이버 안보 관련부처로부터 파견되는 약 50명의 직원으로 구성 ◆ 국가사이버보안정보통합센터(NCCIC), 국가사이버합동조사단, 사이버사령부 등의 업무를 지원
	수사기관	연방수사국(FBI) 사이버범죄수사부 법무부 컴퓨터범죄・지적재산과(CCIPS)	◆ 사이버범죄수사부(Cyber Division) - 운영지원과, 사이버범죄과, 컴퓨터침입범죄과, 특수기술응용과, 능력개발 및 대외협력과 등 5개과에 전국 주요 22개 도시에 테스크포스 별도 운영 ◆ 컴퓨터범죄・지적재산과 - 컴퓨터범죄와 지적재산권 침해에 대항 연방차원에서 전략 수립 - 사이버범죄 예방・수사・기소
	관련기관	연방수사국(FBI) 중앙정보국(CIA)	◆ FBI는 미국 법무부 산하의 수사 기관, 국내의 정보 수집 업무를 담당 ◆ CIA는 해외정보수집, 산하에 4개의 지역분석 그룹, 6개의 초국가적 그룹, 2개의 지원 부서 등을 운영
주요 사례		◆ 소니 픽처스 엔터테인먼트와 미군 해킹 사건으로부터 오바마 행정부는 사이버 보안강화를 위해 2015년 2월 13일 민・관 사이버보안 정보공유 촉진 행정명령(1369) 발동	

미국은 2010년 5월 사이버공간에서의 작전 능력을 강화하기 위해 사이버사령부(United States Cyber Command, USCYBERCOM)를 창설하고, 미군의 IT 인프라

공격에 대한 포괄적 대응방안 마련하였으며, 2015년 2월 「2015 국가안보전략」을 발표함으로써 사이버공간에서의 접근성 보장이란 안보계획을 제시하였다. 여기서 연방네트워크 보안강화, 민관과 협력하여 주요기반시설[4] 복원력 강화, 법률정비, 침해자 기소를 통한 벌금부과, 주변국가의 사이버 위협 대응지원, 글로벌 규범 제정 등을 적시하였다. 또한, '민・관 사이의 효과적이고 신속한 사이버위협 대응을 위한 사이버보안 정보공유 촉진 행정명령(13691)'발령하는 동시에 범정부 차원의 사이버위협 대응능력 제고를 위해 국가정보국(DNI) 내 사이버위협정보통합센터 설립하였다.

「사이버정보공유법」(2015)에 따라 연방기관, 구성기관(기업), 연방정부 요원 등은 범죄, 사기, 신분도용, 간첩, 검열, 거래비밀의 방지, 수사, 기소 목적에 한하여 정보를 공개・보유・이용할 수 있도록 규정하였으며,[5] 오바마 정부는 사이버보안 강화를 위해 2016년 예산을 전년 대비 12% 증가한 140억 달러로 책정하였다.

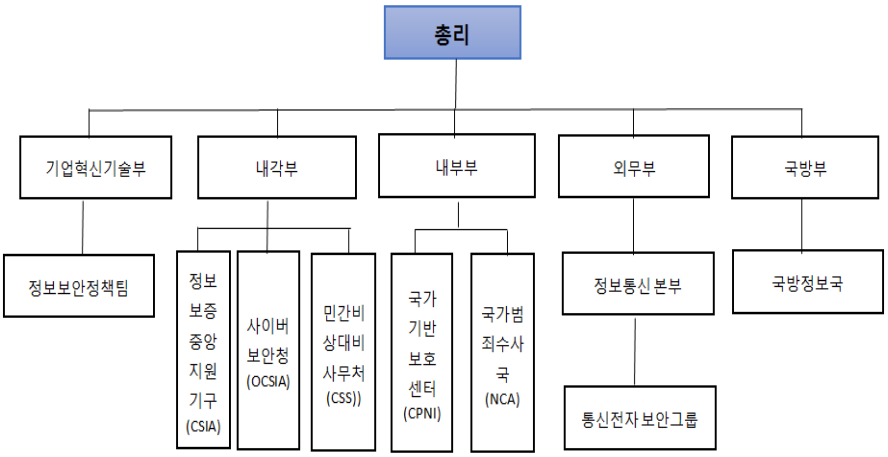
2. 영 국

영국의 사이버안보 추진체계는 사이버안보전략(Cyber Security Strategy of the United Kingdom, 2011)에 의거, 내각(Cabinet Office)이 주도하여 사이버보안의 전략적 목표와 정책실현을 위해 사이버보안・정보보호실(Office of Cyber Security & Information Assurance, OCSIA)과 사이버보안운영센터(Cyber Security Operation Center, CSOC)를 운영하고 있다(김재경, 2014: 26-28).

사이버안보・정보보호실은 20개 정부부처 및 공공기관에 대한 전략방향 설정, 사이버보안 프로그램 조정, 사이버보안 정보인증 등의 업무를 관할하며, 사이버안보운영센터는 외부의 사이버공격, 조직화된 사이버범죄 및 테러로부터 각 부처 및 기업들을 보호하며, 침해사고에 대한 효과적 대응 및 모니터링 실시하고 있다.

4) 미국의 주요기반시설은 화학, 상업시설, 통신, 제조, 댐, 응급서비스, IT, 원자력, 국방, 전력, 금융, 식품농업, 정부시설, 의료 및 복지, 교통, 수자원 등 16개 분야로 구성되어 있다(www.dhs.gov/critical–infrasture 검색일 2016. 7. 17).

5) 사이버공유법과 관련하여 원문은 www.congress.gov/bill/114th–congress/house–bill/2029/text, 검색일 2016. 6. 29.



〈그림 2〉 영국 사이버안보 추진체계[6)]

영국의 내각사무처는 급변하는 정보통신 환경변화를 반영, 범정부차원의 「사이버안보전략」(2009. 6. 25)을 발표하고, 사이버공간에서의 위험요소 감소를 통한 범죄대응 기회포착, 보안지식 및 대응력 제고, 의사결정 체계 강화 등을 제안하였다. 이에 따라 사이버안보실(OCS)과 사이버안보운영센터(CSOC)를 신설하였다. 사이버안보운영센터는 정보통신본부 산하에 설립되어 외부의 사이버 공격, 조직화된 사이버 범죄 및 테러로부터 각부처와 민간기업을 보호하고 침해사고에 대한 효과적인 대응과 모니터링 실시하고 있다.

2012년 12월부터 내각장관은 '사이버안보전략'에 대하여 의회에 서면보고서를 제출하도록 되어 있으며, 2013년 3월 산업체와 정부간에 정보 및 지식의 효율적 공유를 위해 '사이버안보 정보공유 파트너십(Cyber Security Information Sharing Partnership, CISP)을 발표한 바 있다.[7)] 주요 법률적 근거로는 「대테러 범죄 및 안전보장법(2001)」과 「수사권한규제법(2000)」이 있다. 2015년 11월에는 국가안보 및 중대범죄에 대처

6) 배병환・강원영・김정희(2014: 9).

7) 영국 사이버보안 전략(The UK Cyber Security Strategy)은 2015년까지 안심할 수 있는 사이버 공간 하에서 경제적·사회적 가치를 창출한다는 비전을 바탕으로 '사이버범죄 감소 및 안전한 사이버 공간 구축,' '사이버공격에 대한 복원력 강화와 사이버 상의 권익 보호,' '열린, 역동적, 안정적인 사이버 공간 구현,' '사이버보안 지식·기 술·능력 구축' 등의 네 가지 목표 하에 세부 실행과제 57개를 제시하였다(배병환・송은지, 2014: 7).

하기 위하여 법 집행기관 및 안보・정보기관에 인터넷 또는 통신에 대한 광범위한 수사권한을 부여하는 것을 주요 내용으로 한 「수사권 법률」 초안(Draft Investigatory Power Bill)을 공표하였으며, 통신 서비스 제공자에게 12개월간 시민들의 통신이용 데이터, 인터넷 접속기록을 저장하도록 요구하고 있으며, 판사의 영장 없이 감청을 광범위하게 허용하였다. 영국의 사이버안보 체계 및 법적 근거는 아래 <표 3>과 같다.

〈표 3〉 주요 법률적 근거 및 조직체계

구분	법률	법률 및 조직체계	비고
법적 근거		정보보호법(2005)	◆ 정보이용자와 컴퓨터 회사에 의한 등록제 실시
		수사권한 규제법 (2000)	◆ 우편, 전기통신 감청, 전자정보의 해독 및 접근 등 광범위한 수사 및 조사활동 기법에 법적 근거부여 ◆ 감시권한 사용 공공기관은 800곳에 달하고 전화, 이메일 기록 조회와 CCTV를 통한 감시 가능
		대테러, 범죄 및 안전보장법(2001)	◆ 테러리스트 자산 동결, 경찰권한, 항공기 보안, 데이터보안, 출입국 관리, 통신자료 취득 등을 규정
		컴퓨터부정사용 방지법(2006)	◆ 컴퓨터 소프트웨어 불법복제금지, 비인가자에 의한 컴퓨터 접속금지 규정(6개월 이하 징역 또는 벌금) ◆ 사기 및 도용 등 범죄 목적 비인가된 접속 금지(5년 이하의 징역 또는 벌금)
		수사권 법률 초안공표(2015.11)	◆ 2014년 제정된 '데이터 보유와 수사에 관한 법률'의 폐지(2016.12) 시한이 다가옴에 따라 대체 법률 제정 시도
조직체계	정책기구	총리실 소속, 사이버보안・정보보호실(OCSIA)	◆ 20개 정부부처 및 공공기관에 대한 전략방향 설정, 사이버보안 프로그램 조정, 사이버보안 정보인증 등의 업무관할
	주무기관	내각사무처 (Cabinet Office)	◆ 내각사무처는 정부기관의 정보보호 활동 및 업무 조정을 담당 - 정보보증중앙지원국(Central Sponsor for Informations Assurance, CSIA)은 중앙 및 지방정부, 민간부문에 걸쳐 정보시스템에 대한 보안문화 확산에 주력 - 사이버보안청(OCSIA)은 사이버보안전략 실행을 위한 재정지원프로그램의 관리와 조정을 담당 - 민간비상대비사무처(CSS)는 각종 비상사태에 대응하는 업무를 담당 ◆ 정보보호 기본정책, 정보보호 관련 정책 발표

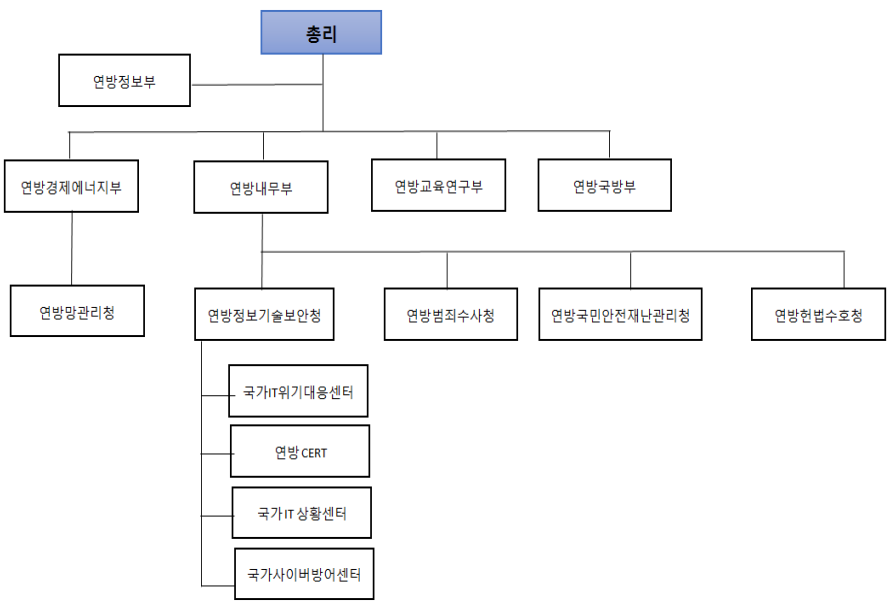
조직체계	테러정보통합기구	정보통신본부, 사이버안보운영센터(Cyber Security Operation Centre, CSOC)	◆ 외부의 사이버공격, 조직화된 사이버범죄 및 테러로부터 각 부처 및 기업들을 보호 - 사이버침해 사고에 대한 효과적 대응 및 모니터링 실시
	수사기관	내무부 소속, 국가범죄수사국(National Crime Agency, NCA)	◆ 2013년 국가범죄수사국 국가사이버범죄수사대(National Cyber Crime Unit, NCCU)를 설치・운영 - 런던경찰청의 사이버범죄단속반(PCeU)과 중대범죄수사국(SOCA)의 사이버 범죄 수사조직을 통합한 조직 - 국내외 사이버범죄에 대응하고, 국가・기업의 기반시설을 보호
	관련기관	내무부, 보안부(MI5)	◆ 보안부(Security Service, SS) - 테러정보 수집, 국가대테러정책 제시, 광범위한 정보활동 수행하나 체포권한 없음 ※ 런던 수도경찰청 내 대테러본부와 밀접한 관계
		정보통신본부(GCHQ)	◆ 정보통신본부(Government Communication Headquarters, GCHQ) - 내각과 군 지휘관들에게 국방과 외교, 경제정책과 관련된 광범위한 신호제공, 국가안보사항, 테러정보 수집 및 검증
		전자통신 보안그룹(CESG)	◆ 전자통신 보안그룹(Communications Electronics Security Group, CESG) - 정부, 공공기관, 군을 대상으로 정보보증 업무수행
주요 사례			◆ 2014년 민간 대기업과 중소기업의 보안사고 발생률이 각각 81%와 60%에 달하는 것으로 조사, 안전한 사이버공간에서 거대한 경제・사회적 가치를 구현한다는 비전아래 사이버안보 전략 전면 재검토

영국의 경찰서장 연합회(Association of Chief Police Officers)는 사이버 범죄 법집행전략에 따라 범죄자 및 테러리스트의 사이버 공간 활용 대처방안 마련하고 있다. 또한, 2001년 4월 컴퓨터 범죄수사를 목적으로 런던경찰청 하이테크범죄국 창설하고, 2005년에는 중대조직범죄수사청(Serious Organised Crime Agency, SOCA)을 창설하였으나, SOCA가 국가사무에 전념함으로써 민생 사이버범죄에 제대로 대응하지 못한다는 비판에 직면하여 2008년 중앙전자범죄대책단(Police Central e-crime Unit, PCeU)을 설립한 된 뒤, 2013년 국가범죄수사국 국가사이버범죄수사대로 통합시켰다.

3. 독일

독일의 사이버대응체계는 사이버안보전략(Cyber Security Strategy for Germany, 2011)에 의거 국가사이버보안위원회(Natinaler Cyber-Sicherheitsrat, Cyber-SR)가 사이버전략을 수립하고, 사이버공격을 받을 경우 연방정보기술안전청 산하 국가사이버대응센터(Nationales Cyber-Abwehrzentrum, Cyber-AZ)에서 공공 및 민간과 협력하여 정보공유(예방・방어적 보호정책)에 주력하고 있다.

위원회는 총리실, 내무부, 국방부,외무부, 경제기술부, 법무부, 제정부, 교육・연구부와 각 주 대표들로 구성되어 있으며, 민간부분에서는 산업계의 대표가 준회원으로 참여하고 있다. 또한 침해사고의 정책적인 사항은 내무부에서 수립・입안하고 있고, 세부적인 사항은 연방정보기술청(BSI)을 중심으로 여러 기관들이 유기적으로 협력・대응하고 있다. 여기에는 긴급대응팀(CERT-Bund), 국가사이버대응센터, 연방시민보호・재난구조청(BBK), 연방범죄수사청(BKA), 연방경찰(BPol), 관세범죄수사청(ZKA), 독일연방정보부(BND), 독일연방군(Bundeswehr) 등이 참여하고 있다.



〈그림 3〉 독일 사이버안보 추진체계

독일은 2005년 7월 IT보안에 대한 최초의 포괄적 종합전략인 「정보기반시설 보호를 위한 국가계획」을 마련하였으며, 상기 계획에 의거하여 2007년 4월 「주요기반시설 실행계획」이 실시되었다. 또한, 2011년 2월 「독일 사이버보안전략」을 수립하여 주요정보기반시설의 보호에 우선순위(10개 전략분야)를 부여하고, 국가사이버방어센터(Nationales Cyber-Abwehrzentrum)를 설치한 뒤 연방정보기술보안청(BSI)이 지휘하되, 연방헌법수호청과 연방재난방재청이 직접 참여할 수 있도록 하였다.

연방정보기술보안청은 주요기반시설의 사이버보안과 관련하여 관리·기술적 조치의 이행 및 침해신고 등을 의무화도록 규정하고 있다. 주요기반시설에는 "에너지, 정보기술 및 통신, 운송·교통, 건강, 물, 식품, 금융, 보험 등 공동체의 기능에 중요한 의미를 가지는 시설, 설비 또는 그 일부"로 규정하고 있다. <표 4>는 독일의 사이버 법률 및 대응체계를 정리한 것이다.

〈표 4〉 주요 법률적 근거 및 조직체계

구분	법률	법률 및 조직체계	비 고
법적 근거		연방정보기술안정청설치법(1991)	◆ 정보통신기술시스템의 연구·개발, 정보통신시스템 안전성 검사, 인증서 발급, 국가기관 및 민간기관에 대한 기술 지원 및 자문제공
		국제테러대책법(2002)	◆ 테러대책을 위한 재정확보, 효율적인 테러기관의 권한강화, 신원확인, 주요시설의 보안강화
		정보통신법(2004)	◆ 정부기관의 기밀누설 방지, 데이터의 안전성 확보, 네트워크 침해사고 방지, 정보요청시 인터넷 통신사업자의 정보통신 서비스 제공자 정보 제공
		에너지법(2011)	◆ 에너지공급망 운영을 위한 정보기술 보안 의무 부여
		원자력법(2015)	◆ 핵연료와 기술, 시설 운영자 보안의무 부여
		IT보안법(2015)	◆ 기업에서의 IT보안개선, 정보통신망을 통한 시민보호 강화, 연방정부의 IT보안 구축, 연방정보기술보안청(BSI)과 연방범죄수사청(BKA)의 역할 강화
조직체계	정책기구	총리실, 국가사이버안보위원회(Nationaler Cyber-Sicherheitsrat, Cyber-SR)	◆ 국가사이버위원회는 총리실, 내무부, 국방부, 외무부, 경제기술부, 법무부, 재정부, 교육·연구부와 각 주 대표로 구성

조직체계	주무기관	내무부, 연방정보기술보안청(BSI)	◆ 연방정보기술보안청은 정부조직상 연방내무부에 소속되나, 실질적으로 독립관청의 역할 수행 - 2015년 현재 사이버보안국을 비롯하여 5개국으로 구성(각 국에는 2개 과가 설치)되며, 600명의 직원이 근무 - 사이버보안 정책의 집행, 정부부처, 기관 및 민간에 대한 지원, 사이버보안 관련 인증 등의 역할 수행
	테러정보통합기구	내무부, 국가사이버대응센터(Nationalen Cyber-Abwehrzen trum)	◆ 2004년 연방테러대책합동본부(GTAZ)를 기초로 2011년 4월 국가사이버대응센터로 확대 개편 - 공공 및 민간과 협력하여 정보공유 (예방・방어적 보호정책에 주력) - 연방헌법수호청과 연방재난방재청이 참여
	수사기관	연방법죄수사청(BKA), 중대조직범죄국 사이버범죄과	◆ 사이버범죄과는 인터넷연구조사지원과, 조사1, 2, 3계 등 총 4개 係로 구성 - 컴퓨터업무방해죄(형법 제303b조)외에 주요기반시설과 관련한 각종 사이버범죄에 대한 수사권 보유 - 국제협력 활동과 실시간 국제공조 기능은 분리 운영 - 범죄정보 및 전략분석 등 사이버범죄에 대한 정보분석 기능 별도 운영
	관련기관	연방정보부(BND)	◆ 연방정보국은 자국산업과 정부기관을 사이버공격으로부터 보호하기 위해 130명(2013년 기준) 규모의 전담팀과 사이버전쟁에 대비한 전담부대 운영
		연방경제에너지부(BMIW)	◆ 사이버보안 사업 총괄 - 일반산업분야 및 원자력 분야의 산업육성과 보안 담당
		연방교육연구부(BMBF)	◆ 사이버보안 연구개발 총괄
		연방국방부(BW)	◆ 사이버보안 국방 총괄
주요 사례 ◆ 2015년 6월 연방하원의 정보시스템에 대한 사이버공격			

2015년 개정된 연방범죄수사청법에 따르면 컴퓨터업무방해죄(형법 제303b) 외에 주요기반시설과 관련한 각종 사이버범죄에 대한 수사권한을 확대 인정하였다.[8] 이외, 데이터탐지죄(제202a조), 데이터취득죄(제202b조), 데이터탐지 및 취득의 예비죄(제202c조), 컴퓨터사기죄(제263a조), 데이터손괴죄(제303a조)가 수사범위에 추가(연방수사청법 제4조 제1항 제1문 제5호 개정)되었다.

8) 연방범죄수사청법 개정 원문은 www.datenschutzzentrum.de/uploads/it/20141021-it-sicherheitsgesetz.pdf 참조, 검색일 2016. 8. 18.

4. 주요국 사이버 테러대응 시스템 비교

사이버테러 관련 경각심을 일깨워 준 사건은 미국의 9/11테러 사건이다. 그러나, 미 정부정책 차원에서 알카에다 테러사건보다 사이버전이 더 위험한 것으로 규정되기 시작한 것은 2013년 이후부터다(James R. Clapper, 2013).

〈표 5〉 주요국 사이버테러 관련 주요법률 및 조직체계 비교

	미국	영국	독일
법적근거	컴퓨터보안법 국가정보기반보호법 국토안보법 전자정부법 사이버보안강화법 국가사이버보안보호법 사이버보안정보공유법	정보보호법 수사권한 규제법 대테러, 범죄 및 안전보장법 컴퓨터부정사용방지법 수사권법률초안	연방정보기술안전청 국제테러대책법 정보통신법 에너지법 원자력법 IT보안법
정책기구	국가안전보장회의 사이버보안위원회	총리실 사이버보안・정보보호실 (OCSIA)	총리실 사이버안보위원회
주무기관	국토안보부(DHS)	내각사무처 (Cabinet Office)	내무부 연방정보기술안전청 (BSI)
테러정보 통합기구	국가사이버보안정보 통합센터(NCCIC) 국가사이버위협정보 통합센터(CTIIC)	사이버보안운영센터 (CSOC) 국가기반보호센터 (CPNI)	국가사이버대응센터 (NCA)
수사기관	연방수사국(FBI) 사이버범죄수사부 법무부 컴퓨터범죄・지적재산과 (CCIPS)	내무부 국가범죄수사국	연방범죄수사청 중대조직범죄국 사이버범죄과
관련기관	연방정보국(FBI) 중앙정보국(CIA)	보안부(MI5) 정보통신본부(GCHQ) 전자통신 보안그룹 (CESG)	연방정보부(BND) 연방경제에너지부 (BMIW) 연방교육연구부 (BMBF) 연방국방부(BW)

IT 기술발전에 힘입어 국경이 허물어지고, 간단한 장치와 조직만으로 개방된 인터넷 세계에서 마음 놓고 테러를 자행할 수 있다는 생각은 그 이전에는 미처 하지 못했기 때문이다.

국민과 영토와 주권을 보호한다는 전통적 의미에서 국가안보는 새로운 과학기술 문명의 발전과 괘를 같이하여 변화되고 있다. 정보혁명의 결과로 군사안보는 과거처럼 재래식 무기로 표현되는 단순한 화력의 총합이 아니라 사이버 전쟁수행 역량이 새롭게 검토되기 시작한 것이다. 이러한 국가안보 인식변화에 따라 각국은 사이버테러에 대비한 법・제도적 기구를 정비하고 있으며, 주무기관을 지정하고 그동안 산재되어 있던 각종 테러정보 기구를 통합하고 있다.

미국은 정책기구로 국가안전보장회의 내 사이버보안위원회를 설치운영하고 있고, 영국과 독일은 총리실 주관하에 사이버보안・정보보호실과 사이버보안위원회를 각각 운영하고 있다. 일본은 미국의 사례를 벤치마킹하여 국가안전보장회의를 신설하였으며, 내각관방 산하 사이버보안전략본부를 운영하고 있다.

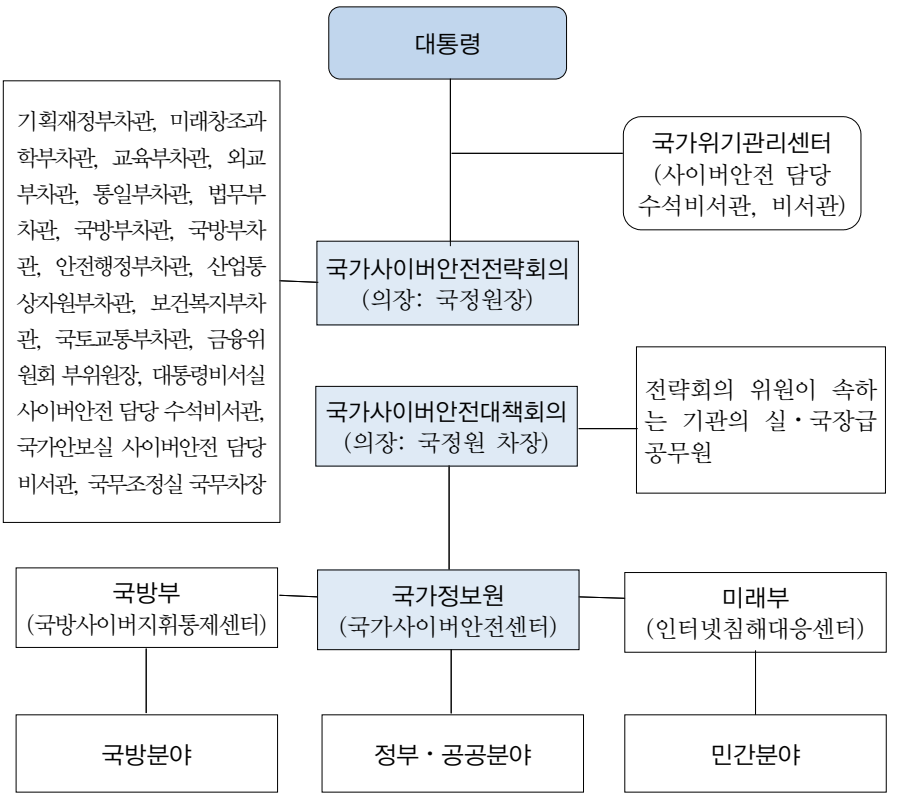
주요 선진국의 사이버테러 대응체계는 행정부 수반이 이끄는 정책기구뿐만 아니라, 각 정부기구에 흩어져 있던 정보기능을 통합함으로써 테러에 효율적으로 대응을 시도 중이다. 미국은 국가사이보보안정보통합센터와 국가사이버위협정보통합센터를 이원적으로 운영하고 있으며, 영국은 사이버보안운영센터와 국가기반보호센터를 각각 설치하고 있다. 독일과 일본은 국가사이버대응센터와 사이버보안센터를 신설하여 사이버테러에 대응하고 있다. 따라서, 우리나라도 향후 사이버테러 법률을 제정할 경우, 미국처럼 국가안보차원에서 총괄법으로 규정하고, 개인정보보호와 관련된 프라이버시 관련법은 특별으로 제정・통합될 필요가 있다.[9]

9) 우리나라의 경우는 국가안전보장을 위한 총괄법의 부재는 물론, 전자정부・사이버안전・주요기반보호・개인정보보호 등이 분야별, 기관별로 나뉘어 개별 법률로 제정하고 있고, 책임과 임무도 기관위주로 분산되어 있다.

Ⅳ. 한국의 사이버안보 대응체계 분석

1. 현 국가사이버안전 대응체계

우리나라 국가사이버안전관리체계는 2005년 1월 사이버위협에 따른 국가차원의 대응체계 구축을 위하여 「국가사이버안전관리규정」(대통령훈령 제141호)을 제정하고, 동년 10월 '국가사이버안전매뉴얼'을 개정함으로써 정비되기 시작했다(「국가사이바안전관리규정」(대통령훈령 제141호, 2005. 1. 31. 제정, '국가사이버안전매뉴얼', 2005. 10. 18).



〈그림 4〉 현 국가 사이버안전 관리체계

2008년 7월 행정안전부는 국가정보원과 지식경제부, 방송통신위원회, 한국정보보호진흥원과 합동으로 '정보보호 중기종합계획(2008～2012)'을 마련 한뒤, 2009년 7.7DDoS 공격을 계기로 '국가사이버안전전략회의'에서 국가사이버위기종합대책을 마련하였다.[10] 2011년 8월 관계부처 합동으로 국가차원의 사이버위협 대응체계를 정비하여 분야별 중점 추진과제 등이 포함된 '국가사이버안보 마스터플랜'을 마련하였고, '13년 7월 '국가사이버안보종합대책'을 수립하여 사이버안보강화를 위한 4대 전략[11]을 마련, 실시해 오고 있다(국회도서관, 2013: 20-21).

이에 따라 사이버안보 컨트롤타워는 청와대 국가안보실이 맡고, 실무총괄은 국정원이 담당하며, 미래부와 국방부 등 관계 중앙행정기관이 각기 소관분야를 담당하는 협업구조를 갖추었다. 따라서,「국가사이버안전관리규정(대통령훈령 제316호, 2013. 9. 2.)에 의거 국가정보원장을 의장으로 하는 '국가사이버안전전략회의'를 설치하고, 그 산하에 국가정보원 차장을 의장으로 하는 '국가사이버안전대책회의'를 두고 있다.[12]

한편, 국방부는 별도로 사이버사령부(국방사이버지휘통제센터)를 통해 국방분야의 사이버안전 업무를 담당하고 있으며, 미래창조과학부 산하 한국 인터넷진흥원 인터넷침해센터에서 민간분야의 사이버안전업무를 수행하고 있다. 국가정보원은 국가사이버안전센터를 통해 국가차원의 종합적이고 체계적인 대응업무를 수행중이다(강석구・이원상, 2014: 155).

사이버위기 경보단계는 각종 사이버공격의 파급영향, 피해규모 등을 고려하여 그 수준에 따라 관심 → 주의 → 경계 → 심각 등으로 구분하되, 국가정보원장, 미래부장관, 국방부장관은 경보 관련 정보를 발령전에 상호교환하고, 민간분야는 미래부장관, 국방분야는 국방부장관이 각각 발령하도록 하고 있다(강석구 외, 2010: 87-89).

반면, 미국 오바마 행정부는 '민・관 사이버보안 정보공유 촉진 행정명령'(2015. 2. 13) 발표하여 국가사이버보안정보통합센터(NCCIC)의 기능을 확대하고 있고, 일

10) 행정안전부 보도자료(2008. 7. 22.), 방송통신위원회 보도자료(2009. 9. 14) 참조.

11) 선진 사이버안보 강국실현을 목표로 '즉응성 강화(Prompt)', '협력체계 구축(Cooperative)', '견고성 보강(Robust)', '창조적 기반조성(Creative)' 등의 과제를 설정하였다.

12) 국가사이버안전대책회의는 국가정보원의 사이버안전업무를 담당하는 차장이 의장이 되며, 각 유관기관의 실・국장급 공무원이 위원이 된다. 주요 심의사항으로 국가사이버안전 관리 및 대책방안, 전략회의의 결정사항에 대한 시행방안, 전략회의로부터 위임받거나 전략회의의 의장으로부터 지시받은 사항, 그 밖에 대책회의의 의장이 부의하는 사항 등이다(대통령훈령 제316호, 2013. 9. 2., 일부개정).

본은 2014년 제정된 「사이버보안기본법」 개정안(2015. 8. 5)을 발의한 상태이며, 중국은 「네트워크안전법」 초안(2015. 7. 6)을 공표하였으며, 호주 또한 「통신법」(2015. 10. 13)을 개정하였다. 이렇듯 주요 선진국은 사이버테러가 국가안보 및 정보・통신・교통・전력 및 산업계에 지대한 영향을 미친다고 판단하여 법제를 정비 강화하는 추세이다.

2. 현행 법체계의 문제점

국제사회로부터 고립된 북한은 한국사회의 혼란을 초래하고자 국가핵심기반시설에 대한 사이버테러 가능성이 증대되는 추세이나, 국가사이버안전관리 규정은 국가・공공기관에만 적용되는 훈령에 근거하므로 민간영역 구속력이 미약한 상태다. 다시말해, 주요정보통신기반시설에 대해서는 주요정보통신기반시설법에 의거 국무총리실장에게 권한을 부여하고, 그 외의 공공기관이 운영하는 정보통신망에 대해서는 훈령에 따라 적용하므로 법적 부조화 발생하고 있는 것이다(박준석, 2015: 243).

〈표 6〉 사이버 테러관련 관련 법률

기관	역할	관련부서	근거법령
청와대	사이버보안컨트롤타워	사이버테러대응팀	
국가정보원	사이버보안 실무총괄	사이버안전센터	국가정보원법, 국가사이버안전관리규정, 정보통신기반보호법
국방부	국방분야 사이버보안	사이버사령부	정보통신기반보호법, 국군사이버사령부령
행정자치부	전자정부 분야 대국민서비스	정보기반보호과	정보통신기반보호법, 행정자치부와 그 소속기관 직제, 전자정부법
방송통신위원회	정보통신망법 적용 대상 관련 업무	개인정보보호윤리과	정보통신기반보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률
경찰청	사이버범죄 수사분야	사이버안전국	경찰청과 그 소속기관 직제
한국인터넷진흥원	민간분야 인터넷 진흥 및 정보보호	정보보호본부 인터넷침해본부	국가정보화기본법,정보통신기반보호법,정보통신망 이용촉진 및 정보보호 등에 관한 법률
미래창조과학부	정보보호 산업 육성, 보호법제 수립과 적용	정보보호정책과	정보통신망 이용촉진 및 정보보호 등에 관한 법률

결국, 우리나라의 사이버테러와 관련된 법제도는 목적에 따라 다양하게 존재하지만 사이버테러에 대한 포괄적인 기본법이 존재하지 않아 개별법 제도와의 통일성과 연계성을 갖지 못하는 한계를 지니고 있다(권양섭, 2014: 189). 또한, 「국가정보화기본법」, 「정보통신기반보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한법률」, 「전자정부법」, 「전자금융거래법」, 「개인정보보호법」, 「통신비밀보호법」, 「국가사이버안전관리규정」 등으로 산재하며, 사이버테러 행위의 형사처벌에 관해 구성요건적 행위의 유사성에도 불구하고 처벌에 관한 규정은 각 법률간 징역형에 있어서는 2배, 벌금형에 있어서는 4배의 격차가 발생하고 있다.

사이버공격에 대한 정부의 대응활동 역시 국가・공공기관에만 적용되는 「국가사이버안전관리규정」에 근거하고 있어 민간분야와의 정보공유는 물론 민간분야에서 발생하는 사이버테러 징후를 사전 탐지・차단하거나 대책을 강구・적용하는데 한계가 있다. 또한 민간기업은 보안취약점이 발견되더라도 비용부담과 기술부족 등으로 신속한 보호조치를 취하지 않아 피해가 반복되는 경향이 있다. 미국, 독일, 일본 등 주요 선진국들은 이러한 문제점을 인식하여 자국내 사이버 안보 관련 법률을 제정한 바 있다.[13] 따라서, 정부와 민간이 함께 협력하여 국가차원에서 체계적이고 일원화된 사이버테러 예방 및 사이버위기 대응업무를 수행하기 위해서는 체계화되고 일원화된 통합법 제정이 시급하다.

과거 북한 소행으로 밝혀진 3.20 디도스 공격사태시,[14] 관련 법률이 부재하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따라 '민관 합동조사팀'이 구성되어 조사가 진행되었다. 이 과정에서 통합법률의 미비로 인해 여러 난제가 존재하였음은 익히 알려져 있다.

13) 영국 「사이버안보법」('15.12), 독일 「IT-보안법」('15.6), 일본 「사이버시큐리티기본법」('14.11) 등이 그러한 사례이다.

14) 2013년 3월 20일 2시 10분경 KBS, MBC, YTN 3개 방송사와 신한은행, 농협, 제주은행 3개 은행의 전산망이 마비되어 막대한 경제적 피해를 입은 사건이다. 이날 피해 대상이었던 KBS, MBC, YTN 방송사와 신한은행, 농협, 제주은행 이렇게 총 6개 회사가 보유한 약 3만 2천 대의 PC가 일시에 오작동을 일으켰으며, 1만 6천여 대의 CD/ATM 기기가 손상됐다. 웹 서버도 피해를 입어 PC에 저장된 방송 데이터와 은행 데이터가 지워졌다. 이 모든 시스템이 정상 복구되는 데는 무려 1개월이 걸렸다.

Ⅳ. 결론

인터넷 보급 및 접속률이 지속 증가함에 따라 사이버테러의 위험이 날로 심화되고 있다. 이에 미국, 영국 등 주요 국가들은 사이버테러에 대한 법적, 정책적 대응책 마련에 부심하고 있다. 이들 국가들의 법 및 제도적인 특징을 살펴보면 다음과 같다.

첫째는 대통령이나 총리 등 산하에 사이버테러 기관이나 위원회를 설치하고 국가 차원의 통합적인 대응 노력을 기울이고 있다는 점이다. 미국의 경우 9/11이후 관련 법들을 정비하고 국토안보부 내 사이버안보국을 설립하는 등 제도적인 장치를 마련하였다. 영국 또한, 범정부적 차원에서 사이버 안보전략을 수립하고 사이버안보실(OCS)과 사이버안보운영센터(CSOC)를 신설하였다. 2012년 '사이버안보전략'에 대하여 의회에 서면보고서를 제출하도록 되어 있으며, 2013년에는 사이버 정보 공유를 위해 '사이버안보 정보공유 파트너십(Cyber Security Information Sharing Partnership, CISP)을 발표한 바 있다.

둘째는 수사권 확대, 정부의 사이버보안 책임 명확화, 형사처벌 규정 강화 등을 통해 사이버테러 사전 예방 및 사후 피해 최소화를 위한 노력에 집중하고 있다는 점이다. 사이버테러로 인해 대규모 피해가 발생하는데다 국민들의 안보불안감 조장 및 정부 국정운영 능력에 대한 불신까지 야기 시키고 있어 이에 대한 강력한 대응이 불가피한 것으로 판단하고 있다.

셋째는 행정부처, 정보기관, 법집행기관간의 정보공유와 공동수사를 통한 협업체계가 강화되고 있다. 이는 사이버테러가 특정 부처의 노력으로 만으로는 탐지가 어려운데다 범죄수사나 국가정보 활동 등 전통적인 영역과 달리 사이버테러는 이들 기관간 역할이 모호하여 협력에 의한 대응을 전개할 수 밖에 없다는 데 기인한다.

그렇다면 선진국(미・영・독)의 사례를 통해서 볼 때, 사이버 테러 대응과 관련하여 한국에 주는 시사점은 무엇인가?. 먼저, 사이버안보법 제정이 무엇보다 긴요하다. 현재 우리나라 사이버안보정책을 보면, 북한의 사이버공격에 따라 「국가사이버위기종합대책(2009)」, 「국가 사이버안보 마스터플랜(2011)」, 「국가사이버 안보종합대책(2013)」, 「국가사이버안보 강화방안(2015)」 등의 순으로 발전되어 왔다. 그러나 현행 법체계에서는 부문별, 목적별로 개별법이 존재하여 사이버공격에 탄력적으로 대응이 곤란한 상황이다. 따라서, 하루 빨리 통일적 대응체계를 갖는 법률제정이 시급하

다고 볼 것이다.

또한, 사이버테러 위협을 종합적으로 분석하고 대응할 수 있는 컨트롤 타워의 설치가 필요하다. 현 국가사이버안전관리규정에 의하면 사이버안보 컨트롤타워는 청와대 국가안보실이 맡고, 실무총괄은 국정원이 담당하며, 미래부와 국방부 등 관계 중앙행정기관이 각기 소관분야를 담당하는 협업구조를 갖고 있다. 「국민보호와 공공안전을 위한 테러방지법」에서는 국무총리실이 컨트롤 타워로 지정받았다. 사이버테러 관련 법률도 법체계의 일원화를 위해서는 국무총리실에 컨트롤 기능을 부여할 필요가 있다. 아울러 사이버 테러방지법 제정과 관련하여 정보기관의 정보독점에 대한 우려를 불식시키는 장치가 필요하다. 그렇지 않을 경우, 개인정보 감시라는 국민적 비판을 해소하기 어려울 것이다.

끝으로 정부 부처간 테러정보를 상시 공유할 체계를 반드시 설치・운영할 수 있도록 해야 한다. 각 부처, 민간에 산재돼 있는 정보기능들을 하나로 묶어 실시간으로 정보를 공유함으로써 사이버 테러에 즉각 대응할 수 있도록 해야 하고, 이 정보는 민간 기업에게도 동등하게 제공되어야 한다. 사이버 테러는 전통적 테러와 개념을 달리하는 새로운 종류의 전쟁이다. 특히 남북한이 대치한 상태에서 북한에 의해 저질러지고 있는 테러는 전쟁으로 보아도 무당하다. 그러한 점에서 사이버 테러 관련 법률체계는 하루 빨리 통합된 법률체계로 일원화될 필요가 있다.

참고문헌

1. 국내문헌

강석구 외(2010). 사이버안전체계 구축에 관한 연구. 한국형사정책연구원. 87-89.

강석구・이원상(2014). 사이버범죄 관련 법령정비 방안. 149-161.

국회도서관(2013). 사이버테러 한눈에 보기. 22-25.

김재경(2014). 국가사이버안보 전담기구「사이버보안청」설립필요(국정감사).

박준석(2015), 국가대테러체제의 구축 및 발전방안. 한국경호경비학회 42호.

방송통신위원회(2009. 9.14). 보도자료.

배병환・강원영・김정희(2014). 영국의 사이버보안 추진체계 및 전략분석. 4-24.

배병환・송은지(2014). 주요국 사이버보안 전략비교・분석 및 시사점. 정보통신정책연구원. 제26권 21호 통권 589호.

새정치연합 국회 정보위원회(2015). 테러방지법과 사이버테러방지법 무엇이 문제인가.

송은지・강원영(2014). 미국 오바마 정부 2기의 사이버보안 강화정책. INTERNET & SECURITY FOCUS September. 5-18.

오길영(2013). 사이버 '테러' 대응체제의 문제점과 개선방향. 민주법학 제54호. 463-482.

윤민우(2014). 새로운 안보환경을 둘러싼 사이버 테러의 위협과 대응방안: 쟁점들과 전략적 접근 틀에 대한 논의. 한국경호경비학회지 40호.

윤해성(2012). 사이버테러의 동향과 대응방안에 관한 연구. 한국형사정책연구원. 60-61.

이창범(2010). 미국, 영국, 독일의 기반보호법 체계에 관한 연구.

임종인(2016). 국가사이버보안 정책과 Think Tank의 역할.

정보위원회 수석전문위원(2013. 6). 국가사이버테러안전 관리에 관한법률안 검토보고서. 74.

전웅(2015), 현대 국가정보학, 서울:박영사

정육상(2014). 최근 테러양상의 변화에 따른 대응체제 개선방안. 한국치안행정논집. 11권 1호.

한국과학기술원(2011). 국가사이버보안 대응체계 혁신에 관한 연구.

한국인터넷진흥원(2011). 사이버보안법제 선진화방안 연구.

한희원(2014). 사이버안보에 대한 국가정보기구의 책무와 방향성에 대한 고찰. 한국경호경비학회지, 제39호, 323-253.

행정안전부(2008. 7. 22). 보도자료.

형사정책연구원(2012, 연구총서 12-B-03) 사이버 테러의 동향과 대응 방안에 관한 연구

2. 국외문헌

Cabinet Office(2013. 12. 12). The National Cyber Security Strategy: Our Forwad Plans. 1-14.

Clay Wilson(2006). Information Operation and Cyberwar: Capabilities and Related Policy Issues. Congressional Research Service - The Library of Congress(9.14).

Holt, T. J(2012), Exploring the intersections of technology, crime, and terror. Terrorism and Political Violence, 24.

James B. Godwin(2014). Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko(eds.) The Russia-US Bilateral on Cyberseurity- Critical Terminology Foundations. 16-22.

James R. Clapper(2013. 3. 12), Worldwide Threat Assessment of the US Intelligence Community(Statement for the Record, Senate Select Committee on Intelligence).

Mike Rogers(2013). Intelligence Chairman: U.S. Fighting Cyber War 'Every Day'. PJ Media, 29 July.

The White House(2011). International Strategy for Cyberspace(www.whitehouse.gov)

William J. Lynn(2013). Defending a New Domain: The Pentagon's Cyberstrategy. Foreign Affairs, Sept/Oct. 2010. 97–108.

3. 기 타

www.shugiin.go.jp, 검색일자 2016. 10. 13.

www.congress.gov/bill/114th-congress/house-bill/2029/text, 검색일자 2016. 10. 15.

www.dhs.gov/critical-infrasture, 검색일자 2016. 9. 18.

www.isaca.org/cyber/pages/cybersecuritylegislation.aspx, 검색일자, 2016. 10. 7.

【Abstract】

A study of the major countries cyber terrorism Response System and Implications

- Focusing on Analyzing the U.S., U.K. and Germany Cases -

Kwon, Oh-Kook · Seok, Jae-Wang

In the mordern society, the reliance on the cyber domain and the cyber connectivity has been increasingly strengthened. Due to this phenomenon, the cyberterror against critical infrastructures and state organs might lead to fatal consequences.

Lately, North Korea's cyberattacks against South Korea's national organizations and financial computer networks are becoming more and more intelligent and sophisticated. The cyberattacks against such critical infrastructures have caused enormous economic loss and social disorder.

This paper is designed to examine comparatively the cyberterror related laws and organizations of the advanced countries such as U.S. and U.K. and to draw implications. Although those countries are under different institutional and cultural backgrounds with varying security envrionments, they are identically pursuing measures by establishing government-wide counterterror system for coordination and cooperation. They are also commonly focusing upon creating new organizations equipped with new system and upon enhancing intelligence performance and devising punishment regulations.

Korea is lack of framework laws regulating cyber security, having only scattered individual laws. Since such legal base is far from efficient counterterror activities, it is necessary that the legal and policy response of the advanced countries should be closely studied for selective introduction. That will eventually lead to legislation of cyber security law. With such legislation on hand, it is subsequently required to strengthen crisis management

for prevention of cyberterror and to create joint response team, cooperating with private organizations.

Key words : Cyber Terror, Terror Response System, Cyber Security, National Cyber Security Basic Law