주요국 사이버보안 전략 비교·분석 및 시사점 – 미국, EU, 영국의 사이버보안 전략을 중심으로 –

배병환* · 송은지**

미국, EU, 영국은 사이버보안 전략을 체계적으로 수립 및 추진하고 있는 대표적 국가들이다. 미국은 백악관을 사이버보안 컨트롤 타워로 지정, 사이버보안조정관 직위를 신설하여 국가 차원의 사이버보안 전략을 총괄, 지원하고 있으며, EU의 경우, 유럽 전체를 포괄하는 사이버보안 전략을 마련해 회원국들 간의 협력을 촉구하고 있다. 영국 역시 사이버보안 선진국으로 사이버보안 전략 발표 이후, 매년 추진사항에 대한 검토를 진행하는 등 체계적인 추진의 모범 국가 중 하나다. 미국, EU, 영국 등 주요국의 사이버보안 전략의 수립 과정과 추진 현황은 추진체계와 복원력 강화, 산업 육성, 인력 양성, 인식제고, 국제협력 등 6개 부문으로 구분해 분석할 수 있었으며, 다양한 전략적 요소를 고려한 정책을 추진하고 있는 것으로 확인할 수 있었다. 이에 따라 우리나라도 사이버보안 정책 추진시 복원력 강화를 위한 담당 기관 간 및 민간·공공 간 협업 강화를 비롯해 사이버보안 산업 육성, 인력 양성 등 다양한 부문을 고려한 사이버보안 정책 추진이 필요하다는 결론을 도출하였다.

목 차

* 한국인터넷진흥원 정책기획팀 주임연구원, (02)405-6343, bbh0113@kisa.or.kr
** 한국인터넷진흥원 정책기획팀 주임연구원, (02)405-6324, songeunji@kisa.or.kr

Ⅰ. 서 론

최근 전 세계를 대상으로 하는 사이버위협의 피해규모가 계속해서 증가함에 따라 국가차원의 효과적인 사이버위협 대응을 위한 사이버보안 전략을 수립·시행 중에 있다.[1] 특히 미국과 유럽, 영국 등 사이버 침해사고가 상대적으로 많이 발생하고 비교적 국가 체계가 안정된 국가를 중심으로 사이버보안 전담 부처 또는 기관을 설립하여 대응하고 있으며, 더불어 사이버위협 대응 전문 인력 수요 급증에 따른 인력양성 전략을 별도로 수립하는 등 효과적인 사이버위협 대응을 위한 정책을 추진하고 있다.

미국은 9.11 테러 발발이후 사이버공간 내 보안을 전담할 부처인 국토안보부(DHS)를 설립하며, 전 세계 사이버위협 대응 체계의 본보기가 되고 있는 사이버보안 선진국가이다. 이미 오바마 정부에서 사이버공간 보호 등을 기반으로 한 IT 생태계 구축과 활용을 통해 경제 성장과 혁신 촉진 의지를 표명함에 따라 백악관을 필두로 사이버보안을 총괄·관리하고 있다.[2] 또한, 유럽연합(EU)은 지난 2013년 2월 범 유럽 차원의 사이버보안 전략을 수립하는 등 EU 회원국 간의 사이버 보안 협력 증대를 위한 공통된 규범과 기본 가치를 전파하기 위해 노력 중에 있으며, 영국 역시 EU 국가 내에서도 사이버보안 선진 국가로 사이버보안 전략에 따른 추진과정 및 성과를 검토한 보고서를 매년 출간하는 등 사이버보안 강화 정책의 실효성을 제고하기 위해 노력하고 있다.

이러한 배경을 바탕으로 본고는 사이버보안 정책을 주요 국정과제로 삼아 추진하고 있는 국가인 미국, EU, 영국들의 정책 추진 현황과 전략들을 상세히 살펴보고자 한다. 먼저 사이버보안 전략의 수립 과정과 추진 현황을 알아보고 사이버보안 전략을 상세히 알아보기 위해 추진체계와 복원력 강화,[3] 산업 육성, 인력 양성, 인식제고, 국제협

1) 시만텍이 발표한 2013 노턴 보고서에 따르면, 1인당 사이버범죄로 인한 금전적 피해는 2012년 197달러에서 2013년 298달러로 약 50%가 증가하였으며, 전세계 사이버범죄 피해비용 역시 2012년 1,110억 달러에서 2013년 1,130억 달러로 증가하고 있다는 보고서를 발표하였음.

2) 미국 경기회복 투자법(American Recovery and Investment Act of 2009, ARRA)를 통해 의료 IT, 스마트그리드, 연방기관 정보시스템 등에 정보보호 강화를 추진 중.

력 등 6개 부문으로 나누어 해당 내용을 비교·분석해보려고 한다. 사이버보안 전략과 체계를 세분화된 주제로 비교·분석하는 작업을 통해 궁극적으로 국내 사이버보안 정책 수립에 참고할 수 있는 시사점을 도출해보려고 한다.

Ⅱ. 주요국 사이버보안 전략 추진 현황

1. 미국

미국은 다른 국가에 비해 사이버공격의 표적이 되는 경우가 빈번해 이른 시기부터 국가 사이버안보에 관심을 가지게 된다. 특히 미국 정부는 사회적 혼란 및 국가 안정성과 관련되는 주요 기반시설의 사이버보안 강화에 집중하며, 이를 주요 국정과제로 삼고 정책적인 노력을 기울이는 특징이 있다. 사이버보안을 강화하기 위한 정책들은 법체계 정비에서 출발하게 되는데, 그 시작은 1980년대 중반의 컴퓨터 범죄 또는 사이버안보에 관한 법 제정[4]이다. 이 시기에 국가 주요기반 시설 보호를 위해 중앙정부를 중심으로 전략 개발이 이루어지기 시작하였으며, 1998년 5월 대통령령(Presidential Decision Directive, PDD) 63호 공표를 통해 주요기반 시설에 대한 범정부적 보호체계를 처음으로 마련하는데 이른다.[5]

클린턴 정부에 이어 2001년 출범한 부시 정부는 국방부 펜타곤이 공격을 받고 세계무역센터 빌딩이 무너지는 9.11 테러 사건에 직면하게 되고, 이 사건을 계기로 주요기반시설 보호의 중요성이 더욱 부상한다. 부시 행정부는 재임기간 동안 행정명령 발효

3) 본 고에서의 복원력(Resilience)은 민·관 협력, 사이버위협 정보공유 등 사이버위협의 대응력을 의미

4) 1980년부터 1990년대에 제정된 미국의 사이버안보 관련 법안은 아래와 같다. 「위장접근수단·컴퓨터사기 및 컴퓨터남용법」(Counterfeit Access Device and Computer Fraud and Abuse Act)(1984), 「전자통신 사생활보호법」(Electronic Communications Privacy Act)(1986), 「컴퓨터 보안법」(Computer Security Act)(1987), 「문서감축법」(Paperwork Reduction Act)(1995), 「정보기술관리 개혁법」(Information Technology Management Reform Act 또는 Clinger-Cohen Act)(1996) KISA, 주요정보통신기반보호 강화 방안 마련, 2013. 12

5) 김은혜·이재일, 미 오바마 정부의 사이버보안 주요 정책 및 법안, 인터넷 & 시큐리티 이슈, 2011. 8

와 법안 제정을 통해 주요 기반시설에 대한 중앙정부의 보안 정책을 추진하였고, 2002년 11월 제정한 「국토안보법」(Homeland Security Act)를 근거로 국토안전 및 사이버보안 주무부처인 국토안보부(Department of Homeland Security)를 신설하였다. 국토안보부는 9.11 테러의 충격으로 미국 내 분립되어 있던 안전 정보 관련 정보기관들을 통합해 당시 17~18만 명의 직원을 거느리는 거대 부처[6]로 출범하였고, 오바마 대통령이 취임했던 2009년까지 미국의 사이버보안과 국토 안보를 주도하였다.

2009년에 오바마 행정부가 수립된 이후에도 사이버보안은 핵심적인 국정 과제로 주목받게 되었으며, 이에 따라 2009년 5월에는 ▶백악관, 연방정부 등 최상위 리더십에 따른 정책 추진(Leading from the top), ▶보안교육, 전문 인력 양성 등 디지털 국가 구축을 위한 역량 제고(Building Capacity for a Digital Nation), ▶민·관 협력을 위한 파트너십 구축 등 공동 책임(Sharing Responsibility for Cybersecurity), ▶효율적인 정보 공유 및 사고 대응 능력제고(Creating Effective Information Sharing and Incident Response), ▶혁신 촉진(Encouraging Innovation) 등의 내용[7]을 담은 '사이버공간 정책 리뷰(Cyberspace Policy Review)'를 발표하였다. 본 전략에는 주요 목표들의 달성을 위한 단기(Near-term) 액션플랜 10개 그리고 중기(Mid-term) 액션플랜 14개도 포함되어 있다. 사이버공간 정책 리뷰의 발표는 기존 국토안보부에서 주도했던 국가 사이버보안 업무가 대통령을 중심으로 백악관에서 정책을 추진하는 체계로 재편된 것을 의미한다. 또한, 국가 기관의 사이버위협 대응 능력제고 뿐만 아니라 보안 교육과 인력 양성, 혁신 또한 중요시하기 시작했으며 여러 분야에서 민간 부문의 책임과 의무를 강조했다는데 의의가 있다고 볼 수 있다.

이러한 정책 추진에도 불구하고 주요 기반시설과 언론사들이 사이버공격에 지속적

6) 국토안보부(DHS)는 대통령 경호를 담당하는 재무부 산하의 비밀검찰부를 비롯해 해안경비대, 국경수비대, 이민귀화국(INS), 세관, 연방비상관리국(FEMA), 교통안전국(TSA) 등 22개 연방 기관이 합쳐져 탄생 http://www.dhs.gov/history

7) http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

으로 노출[8]되는 사고를 겪자 오바마는 2013년 2월 주요 기반시설의 사이버보안 강화를 위한 행정명령(Executive Order 13636)과 정책지침(PDD 21)을 발표한다. 행정명령 13636호는 주요 기반시설의 보호체계 구축을 위한 사이버보안 프레임워크의 개발과 보급을 핵심 목적으로 하며, 정책지침 21호는 주요 기반시설 보호에 관련되는 중앙 부처들의 역할과 의무를 적확하게 규정하는 것을 주요 목적으로 한다. 2009년에 발표했던 사이버공간 정책 리뷰 혹은 타국가의 사이버보안 전략과 달리 주요 기반시설의 보안 강화에 초점을 맞춘 정책이라는 점이 특징적이다. 행정명령에 따라 '국가기반보호계획 2013' ('14. 1), '사이버보안 프레임워크' ('14. 2) 등이 수립되는 등 민·관을 포괄하는 사이버보안 강화정책이 진행되고 있다.

2. EU

EU의 사이버보안 논의는 디지털 아젠다 논의에서 시작한다. EU는 2010년 디지털 기술 활용을 통한 지속 가능한 성장을 이룰 수 있도록 하는 디지털 아젠다(Digital Agenda for Europe) 7개가 발표하였고 사이버보안도 그 중 하나로 선정되었다. 7개의 아젠다는 ▶브로드밴드 신규 규제 환경 조성, ▶유럽의 시설 자금 연계를 통한 공공 디지털 서비스 기반 신규 조성, ▶디지털 기술습득과 채용 관련 대연합 착수, ▶EU 사이버보안 전략 및 지침(Directive) 제안, ▶EU저작권 프레임워크 개정, ▶공공분야 시장을 통한 클라우드 컴퓨팅 활성화, ▶신규 전자산업 전략 추진 등으로 구성되었다. 아젠다들은 새로운 디지털 시대를 맞아 신규 시장 발굴 및 활성화를 중요시 하고 있다. 미국이 주요 기반시설의 보안 강화를 중시하고 있다면 EU는 디지털에서 새로운 성장 동력을 찾으려는 노력에서 사이버보안에 대한 관심이 시작된 것이다.

이 중 4번째 항목인 'EU 사이버보안 전략 및 지침 제안'에 따라 EU의 사이버보안 전략(Cybersecurity Strategy of the European Union)이 2013년 수립된다. 사이버보

8) 2013년 1월 국토안보부 산하 ICS-CERT의 악성코드 감염 사고와 뉴욕타임즈 및 월스트리트 저널의 해킹 사고가 발생

안 전략은 궁극적으로 EU의 안전한 온라인 이용 환경 구축 및 시민들의 권리 증진을 목적으로 하며 이를 위한 EU의 구성, 시민의 권리 보호와 관련해 필요한 활동을 제시하고 있다. 본 전략에서는 사이버보안 정책 수립 시 기초가 되어야 할 5가지 원칙을 제시하고 이에 기초한 사이버보안 전략에 대해 명시하는 내용으로 구성된다. 본 전략은 사이버 복원력을 강화하고 사이버 범죄를 줄이는 등의 전략 목표 달성을 위해서는 EU 차원에서 중앙 집중감독이 아닌 각국 정부 스스로가 사이버위협 예방 및 대응 수단, 정책·법적 수단 마련을 통한 민간과의 협력 체계 확립이 중요함을 서술하고 있다.

〈표 1〉 EU 사이버보안 전략 세부 실행과제

구 분	설 명
사이버보안 정책수립 원칙	– 오프라인 세계에서의 핵심가치를 온라인에서 동일하게 적용 – 기본권, 표현의 자유, 개인정보 및 프라이버시 가치 중시 – 인터넷 접근성 향상을 위한 인터넷의 무결성, 보안성 확보 – 다수 이해관계자(Multi-stakeholder) 거버넌스 접근법 지지 – 사이버 위협 해결을 위한 민간·공공 등 관련 부문 간 효율적 대응
사이버보안 전략	– 사이버 복원력(resilience) 강화 – 사이버 범죄의 획기적인 감소 – 사이버보안력 제고를 위한 산업 및 기술 자원 개발 – 공통 보안 및 방어 정책과 관련된 사이버 방어 정책 및 역량 개발 – EU의 통일된 사이버공간 정책수립 및 EU의 핵심가치 실현

출처: EU 사이버보안 전략(Cybersecurity Strategy of the European Union), 2013. 2.

이와 같이 각 회원국들의 사이버보안 체계 마련을 지원하기 위해, 보안 조치를 의무화하고 기준을 제시하는 '네트워크 및 정보보호 지침(Directive on Network and Information Security)'이 전략의 후속조치로 2013년 12월 수립된다. 네트워크 및 정보보호 지침은 국가 네트워크 정보보안 체계, 관할기관 간 협력, 공공행정 및 기업의 정보보안 등의 내용으로 구성되어 있으며 국가·국가 간·민간 기업 등의 의무를 모두 규정하고 있다는 특징이 있다. 지침에서는 EU 회원국 내 컴퓨터긴급대응팀(CERT) 설치, 회원국 간 보안 정보 공유 체계 구축, 주요 사업자들에게 보안 요건 준수 의무

부과 등을 명시하며 실질적인 보안 강화 요건을 제시하고 있다. 최근 유럽의회(EP)에서 2014년 3월 13일에 본 지침 초안을 채택하였으며, 향후 유럽이사회(Council of the European Union)와 함께 네트워크 및 정보보호 지침의 최종 합의를 위한 협상이 예정되어 있다.

3. 영국

영국은 사이버 공간에서 증대되는 공격으로부터 모든 시민들 안전하게 보호하기 위해 2009년 6월 최초로 사이버보안 전략을 수립하였다. 사이버보안 전략 수립 전에는 정보보호법(Data Protection Act 1998)을 근거로 정보보호 관련 사항을 규제했던 영국은 본 전략의 발표를 통해 사이버범죄의 인식 제고와 민간 대응능력 강화 등을 목표로 설정하였다. 그럼에도 불구하고 국가기반시설을 위협하는 사이버공격의 위험에 노출되면서 사이버보안 전략의 목표에 따른 계획 및 진행현황에 관한 보고서를 매년 발표하게 된다.

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, ▶사이버 공격에 대한 복원력 강화와 사이버상의 권익 보호, ▶열린, 역동적, 안정적인 사이버 공간 구현, ▶사이버보안 지식·기술·능력 구축 등의 네 가지 목표 하에 세부 실행과제 57개를 제시하였다. 또한, 4년 동안 6억 5천만 파운드(약 1조 1천억 원)의 국가사이버보안프로그램(National Cyber Security Programme)을 통해 사이버보안 정책 운영에 요구되는 예산을 마련하는 등 전략 추진을 위해 체계적으로 정책을 추구하는 모습을 보여주었다.

사이버보안 핵심 전략을 근거로 보면 영국은 국가 기관 전반의 사이버보안 대응력 및 복원력 강화 외에도 민간 사이버범죄 소탕, 민간기업의 사이버보안 관리 강화 및 필수적 정보공유, 사이버공격의 효과적 대처를 위한 국제협력 강화 등 공공·민간·국가 간 협력을 통해 안전한 사이버 공간 구현을 주요 정책 목표로 삼고 있다. 또한, 사

이버보안 위협이 사이버범죄를 유발하고, 국가 안보에 악영향을 미칠 수 있는 것으로 판단하여, 법 집행기관·수사기관·민간·개인 등 여러 주체간의 협력 및 각각의 능력 제고를 위해 노력해야 한다는 것을 제안하고 있다.

사이버보안 전략 세부 과제의 지속적인 평가 및 관리를 위해 매년 전략 추진과정 검토 작업을 수행하고 있으며 목표별 진행현황도 발표하고 있다. 또한 영국은 사이버보안 전략 추진과정 검토 보고서를 2013년 12월에 발표하였고, 전략 추진 방향을 제시하는 '국가 사이버 보안 전략 계획(The National Cyber Security Our Forward Plans)'을 발표하며, 영국 사이버보안 전략의 4가지 기본 목표를 비롯하여 사이버 공격의 국가적 대응 능력제고, 주요기반 시설·네트워크의 복원력 강화, 사이버보안 인식 확산 및 위험관리 능력 향상, 전문 인력 양성, 국제협력 등에 관한 계획을 추진하고 있다.

〈표 2〉 국가 사이버보안 전략 계획 추진 내용

① 고도화된 사이버 위협에 대비한 대응 능력제고
② 인터넷 비즈니스 안정성 강화 및 사이버범죄 감소를 위한 법 집행기관 역할 강화
③ 영국 주요 시스템 및 네트워크 복원력 강화
④ 영국 산업 내 사이버 리스크 관리능력 향상
⑤ 제품, 서비스에 대한 높은 수준의 사이버 보안 수준 요구
⑥ 사이버 보안 관련 연구 및 교육을 통한 전문 인력 양성
⑦ 원활한 사이버 범죄 해결을 위한 국제 협력 지원

출처: 국가 사이버 보안 전략 계획(The National Cyber Security Our Forward Plans), 2013. 12

Ⅲ. 주요국 사이버보안 전략 비교·분석

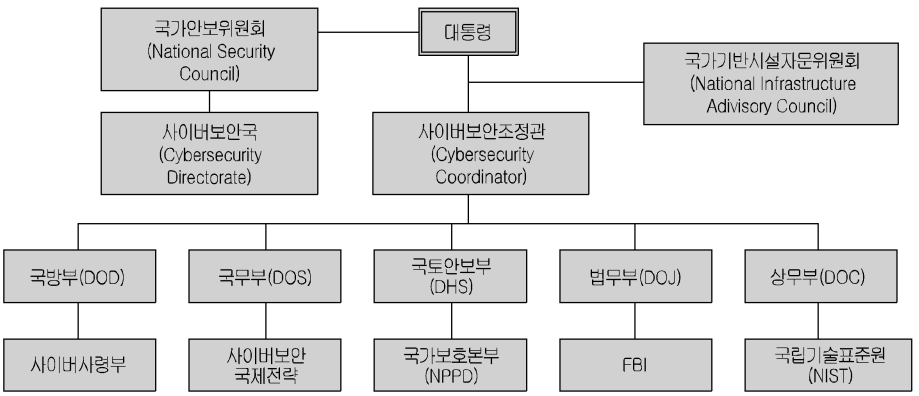
1. 사이버보안 전략 추진체계

(1) 미국

미국은 오바마 대통령 취임 직후 정부의 핵심과제로 사이버보안을 채택하여 2009년 2월 사이버보안 정책과 체계에 대한 종합적 검토를 지시하였으며, 같은 해 5월 사이버공간 정책 리뷰를 발표하였다.

사이버공간 정책 리뷰 발표 이후 기존 국토안보부 장관이 총괄하던 사이버보안 컨트롤 타워의 역할을 백악관 내 사이버보안조정관 직위를 신설하여 국가 사이버보안 총괄 조정과 리더십 기능을 담당하도록 역할과 기능을 이전하였다. 국가안보위원회(National Security Council)내 사이버보안조정관[9]을 총책임자로 하는 사이버 보안국

〔그림 1〕 미국 사이버보안 추진 체계



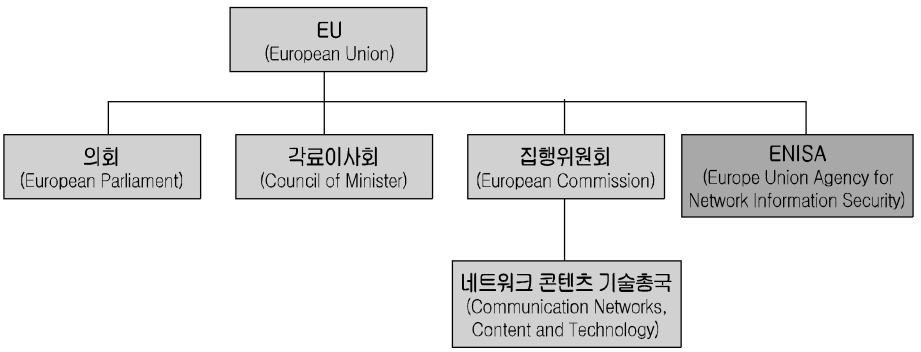
9) 사이버보안조정관은 다음과 같은 역할을 담당한다. ① 사이버보안 조정관은 대통령에게 직접 사이버보안 정책을 직접 보고, ② 주, 지방정부 및 민간부문을 포함하는 미국의 모든 사이버보안 담당자들과의 긴밀한 협력이 가능하도록 규정, ③ 국방부, 국가안보국, 국토안보부 등과 협력하여, 대규모 침해사고 발생시 총지휘관 역할을 담당, ④ 국가안전보장회의에 상주하며 대통령과 안전보장회의에 사이버보안 관련 정책을 정기적으로 보고, ⑤ 미군과 민간기관의 연방정부 사이버안보정책 마련을 위한 자문관 역할 수행

(Cybersecurity Directorate)을 설치하여, 사이버스페이스 정책 리뷰에 나와 있는 정책 방안을 더 자세히 설명하고 발전시킬 임무를 부여하였다. 이외에도 주요기반시설에 대한 사이버보안을 담당하고 있는 국토안보부와 사이버전에 대비를 위한 활동을 하고 있는 국무부·상무부 등 관련 정부부처 내 담당 부서와 산하 기관을 통해 미국의 사이버보안 전략을 추진하는데 있어 필요한 업무를 지원받고 있다. 여러 부처에 걸쳐 있는 사이버보안 업무가 사이버보안조정관을 통해 대통령에게 리더십을 부여하고 있다는 것이 특징적이다.

(2) EU

EU는 단일국가가 아닌 연합체이기 때문에 사이버보안 추진 체계도 다소 상이한 구조이다. 사이버보안은 집행위원회(European Commission) 산하 네트워크콘텐츠기술총국(Communication Networks, Content and Technology)[10]에서 총괄하고 있으며, 산하기관인 유럽네트워크정보보호기구(ENISA)에서 지원을 받고 있다. 유럽네트워크정보보호기구는 EU회원국 네트워크 및 정보보안을 지원하며, 국가 간 정보교류 증대와 네트워크 보안 기능 조정 등의 역할을 수행하는 기관으로 EU규정에 의거하여

〔그림 2〕 EU 사이버보안 추진 체계



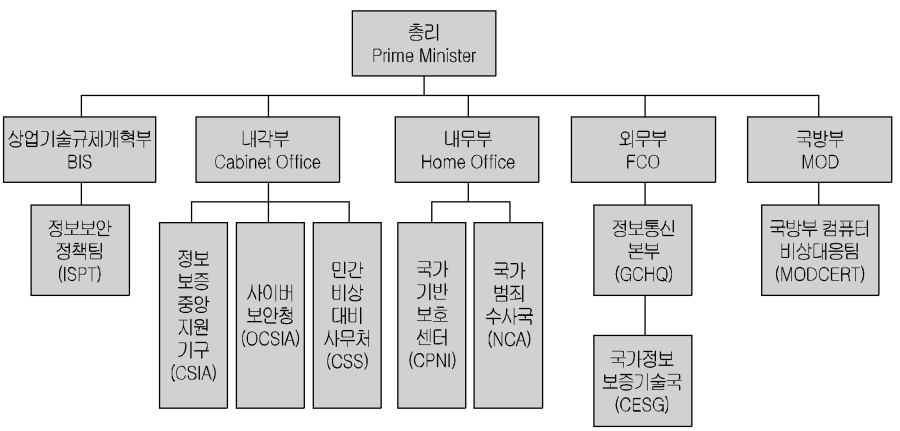
10) 네트워크·콘텐츠·기술총국(Communications Networks, Content and Technology): 지식정보사회 구현을 목표로 유럽의 정보사회 정책연구, 디지털 콘텐츠 및 인터넷 등 디지털 아젠다 총괄

2004년에 설립되었다. 특히, 집행위원회, 회원국, 회원국의 기업체 등의 사이버보안 업무 지원 및 자문·연구를 통해 사이버보안 위협 대응능력을 개선하는데 노력하고 있으며, 매년 사이버위협평가보고서를 발간하고 있다.

⑶ 영국

영국의 사이버보안 추진 체계는 내각부(Cabinet Office)를 중심으로 한다. 정보보호 정책을 총괄하고 있는 내각부는 정부기관 정보보호 정책을 조율하고 있으며, 산하기관으로 정보보증중앙기구(CSIA), 사이버보안청(OCSIA), 민간비상대비사무처(CSS) 등이 있다. 또한 주요기반 시설 보안은 내무부(Home Office), 산업 활성화를 위한 정보보호 관련 정책은 기업혁신기술부(Department for Business Innovation and Skills), 외무부(Foreign&Commonwealth Office)는 통신정보 수집·제공을 담당하고 있다. 그 외에도 상업기술규제개혁부(Department for Business Innovation and Skills)와 국방부(Ministry of Defence)도 사이버보안 업무를 수행하고 있어 여러 부서의 정보공유 및 일관된 정책추진이 요구되는 구조이다.

〔그림 3〕 영국 사이버보안 추진 체계



2. 복원력 강화

(1) 사이버위협 정보공유

1) 미국

오바마 대통령은 미국 상원에서 사이버 정보공유 및 보호법(안)(Cyber Intelligence Sharing and Protection Act)과 사이버보호법(안)(Cyber-security Act of 2012)이 연이어 부결됨에 따라 주요 기반시설 보호 강화를 위해 2013년 2월 대통령 행정명령(Executive Order 13636)을 공표하였다. 공표된 대통령 행정명령을 살펴보면, 주요 기반시설 사이버위협 정보공유체계 강화를 위해 사이버공격 징후 포착 시 신속한 공격징후보고서 작성과 대상기관에 전파하기 위한 체계 마련과 함께 국토안보부가 사이버 위협정보를 민간사업자에게 제공하는 것이 주요 내용이다. 사이버 침해위험을 감소시키는 서비스인 사이버보안 정보공유서비스(Ehanced Cybersecurity Services) 대상을 일부 상용서비스제공업체에서 주요 기반시설로 확대하겠다는 내용을 담고 있는 등 민·관 협력에 기반 한 사이버위협 정보 공유체계 구축에 노력을 기울이고 있는 상황이다.

2) EU

EU는 사이버보안 전략을 통해 국가별 네트워크 및 정보보호(Network and Information Security) 권한 기관 간, 유럽경찰기구(Europol), 유럽방위청(European Defense Agency) 등 민·관·군의 위협 정보 공유의 중요성을 밝혔다. 이에, 유럽경찰기구는 유럽검찰기구와 함께 사이버범죄 대응 관련 정보공유에 노력하고 있으며, 더불어 유럽경찰기구 내 유럽 전역의 인터넷 범죄자들의 신원, 범죄 행태 등에 대한 정보를 공유하고 있다. EU는 효과적인 사이버범죄 위협에 공동 대응하고자 유럽사이버 범죄센터(European Cybercrime Centre)를 2013년 1월에 설립하는 등 효과적인 사이버위협 정보 공유를 위한 노력을 기울이고 있다.

3) 영국

영국은 2013년 3월 안전한 사이버 공간 구현을 위해 민간과 공공의 사이버위협 정보를 실시간으로 교류할 수 있는 플랫폼인 사이버보안정보공유협력체(CISP)를 발족

하였으며, 주요기반시설 사업자들과의 사이버위협 정보를 공유하는 협력 체계를 마련하였다.[11] 또한, 국가범죄수사국(NCA) 역시 사이버범죄 단체에 대한 정보를 민간부문과 공유하여, 효과적인 사이버범죄 퇴치를 위해 노력을 기울이고 있는 중이다.

⑵ 민·관 협력

1) 미국

미국은 효과적인 사이버위협 대응을 위해 사이버사고 예방·탐지·대응을 위한 민·관 협력 프로세스를 개발하였으며 주요기반시설의 보호체계 구축을 위해 사이버보안 시스템 구축을 위한 기술표준·방법론·구축 단계 및 절차 등의 내용을 담고 있는 사이버보안 프레임워크를 개발하는 등 민·관 협력에 기반한 복원력 강화를 꾀하고 있다.[12] 또한, 향후 예상치 못한 사이버위협에 대한 효과적 대응을 위해 민·관 관련 종사자들이 참여하는 국가단위의 사이버 훈련을 수행하는 등 민·관 부문의 사이버보안 준비성 검토 및 강화에도 주의를 기울이고 있다.

2) EU

EU는 사이버보안 및 개인정보 침해 사고 발생에 따른 관련 규정 법제에 기반한 보고 체계를 마련하는 등 공공과 민간부문의 사이버 대응 능력 개발 및 협력 지원하고 있다.[13] 특히, 네트워크 및 정보보호와 관련한 최소한의 공통요건 규정을 통한 네트워크 및 정보보호 전담 국가 지정 및 컴퓨터긴급대응팀 설치, 국가 네트워크 및 정보보호 전략 및 협력 계획 채택 장려하는 등의 내용을 담고 있는 네트워크 및 정보보호 지침을 마련하는 등 EU 전반에 걸쳐, 국경을 넘어서는 사고 발생 시 국가 간 조율,

11) 사이버보안정보공유협력체는 민·관 네트워크 보안 전문가들로 구성되어 있으며, 2013년 약 250여개의 가입조직을 2014년 말까지 500여개로 확대시킬 계획을 가지고 있음.

12) 최근 미국은 2014년 5월 미국내 주요기반시설에 대한 보안 위협과 취약점 등을 조사한 분석 보고서 '섹터 리스크 스냅샷(Sector Risk Snapshot)'을 발간하는 등 주요 기반시설별 잠재적 피해를 줄일 수 있는 대비책 강구를 촉구하고 있음.

13) EU는 Framework Directive for electronic communications 및 EU data protection legislation을 통해 전자통신서비스제공사업자 및 데이터 관리자들에게 보호 조치 및 침해사고 발생 시 보고 조치 등을 하도록 명시하고 있음.

민간의 참여 대비 측면에서의 법률을 마련하는 노력을 기울이고 있다. 또한, 민·관 협력을 통해 유럽 내 사이버위기 대응을 위한 기존의 표준절차와 협력 메커니즘을 점검하기 위해 격년으로 범유럽 차원의 사이버사고 대응 훈련을 지원하고 있다.[14] 이외에도 유럽집행위원회 차원에서 주요기반시설 운영자들과 함께 네트워크 및 정보보호 취약점 파악과 복구 시스템 개발 노력을 기울이고 있는 중이다.

3) 영국

영국 역시 정부 네트워크 및 민간 주요 기반시설 사업자들과의 협력을 통해 사이버 위협 대응 능력을 강화하고 있다. 모든 정부부처 이사회, 정부기관 이사회는 자체 위험 관리 제도를 통해 사이버위험 관리를 지원하는 등 매년 사이버위협 대응 준비상태가 감사의 일환으로 면밀히 검토되고 있다. 또한, 국가기반시설보호센터(CPNI)와 정보통신본부(GCHQ)간 협력을 통해 주요기반시설 사업자들에게 잠재적 취약점 및 피해 완화 관련 조언, 지침을 제공하고 있으며, 금융 부문 사이버 방어 및 사고 대응 실태 점검을 위한 사이버 훈련 프로그램을 수행하고 있다.

(3) 사이버보안 R&D

1) 미국

미국은 사이버 문제를 근본적으로 해결할 수 있는 새로운 기술 개발과 함께 연구 성과의 극대화와 실용화를 통한 사이버보안 혁신을 촉진하고 있는 국가다.[15] 사이버보안 R&D와 관련한 대표적인 예로 2011년 12월 사이버공간 정책 리뷰 내 사이버보안 연구개발 추진을 위해 연방 사이버보안 R&D 전략 계획(Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity R&D Program)을 예로 들 수 있다.[16] 동 전략계획은 ① 연구는 사이버보안 문제의 근본적인 원인을 이해하는데 주력, ② 사이버보안은 다면적인 문제로 전략은 폭넓은 분야에 걸쳐 다양한 전문지식과 역

14) 2014년 4월 EU는 EU 차원의 사이버위협 대응 효율성 제고를 위한 사이버유럽 2014(Cyber Europe 2014) 훈련을 실시

15) 민경식·지순정, “미국의 사이버보안 정책과 R&D 전략에 관한 분석”, 2013. 1.

16) 백악관 과학기술국(OSTP) 산하 국가과학기술회의(NSTC)에서 발표

량을 투입하는 것이 필요, ③ 기술과 위협의 변화에 관계없이 안전한 환경을 유지하기 위해 사이버보안의 원칙을 유지 등 3가지 기본 원칙에 기반하며, ① 현재의 사이버시스템에 대한 공격을 무력화 시키는 game-changing적 기술개발,[17] ② 미래 사이버시스템의 보안과제에 대응하는 과학적 접근기반 구축 등 2가지를 추진 목적으로 하고 있다. 연방 사이버보안 R&D 전략 계획의 주요 내용은 〈표 3〉과 같이 4개의 내용으로 구성되어 있다.

〈표 3〉 사이버보안 R&D 전략 주요내용

구성	내용
(1) 변화의 유발 (Inducing Change)	전략의 중심이 되는 4개 연구테마를 의미하는 것으로 game-changing적인 기술을 상정한 이들 연구테마는, 모두 위협의 근본적인 원인을 이해하고 지금까지와는 다른 접근방식으로 사회의 중요한 사이버 시스템, 인프라의 보안을 향상시키는 것을 목적으로 함
(2) 과학적인 기반의 확립 (Developing Scientific Foundations)	구체적인 실현방법으로 이질적 분야의 지식을 체계화(Organizes disparate areas of knowledge), 보편적 법칙의 발견(Enables discovery of universal laws), 과학적 수법에 대한 엄밀성 적용(Applies the rigor of the scientific method) 등 3개의 방향성을 제시
(3) 연구효과 극대화 (Maximizing Research Impact)	전략에 근거하여 실시되고 있는 연구효과의 극대화를 위해, 타 분야 연구의 연계 혹은 민관협력의 커뮤니티 활동을 추진
(4) 실용적 이행 가속 (Accelerating Transition to Practice)	연구개발에서 얻어진 성과를 사이버공간의 신뢰성 향상에 활용하기 위해 각종 실용화 프로그램을 추진

자료: 민경식·지순정, "미국의 사이버보안 정책과 R&D 전략에 관한 분석", 2013. 1.

2) EU

EU는 ICT 보안 관련 기술 연구개발에 대한 투자 확대를 통한 해외 기술에 대한 의존성을 축소하려는 노력을 기울이고 있다. 유럽의 국제 경쟁력 강화를 목표로 한

17) game-changing이란 종래의 연구개발의 과제·문제(Hard Problem)와 다른 새로운 정보보호 대책이나 비즈니스에 대한 보다 근본적 변화를 요구하는 생각을 의미

호라이즌 2020(Horizon 2020) 연구혁신 프레임워크 프로그램(Framework Programme for Research and Innovation)을 적극 활용하여, 사이버위협 대응 도구 및 수단 개발을 지원하고 있으며, 회원국간 사이버보안 연구 의제 조율 장치 마련 및 연구 활동 촉진을 위한 유인책을 마련 중에 있다. 또한, 유럽집행위원회는 유럽경찰기구와 유럽네트워크정보보호기구에 대해 회원국들이 최신 사이버범죄 수사 및 대응을 위해 부족한 부분을 식별하고 역량을 강화할 수 있도록 적절한 디지털 과학수사 도구와 기술을 개발할 것을 요구하고 있다.

3) 영국

영국은 산·학·연과의 협력을 통한 사이버보안 연구개발을 추진하고 있다. 영국 내 대학교 3곳(버밍업, 캠브리지, 뉴캐슬)에 '사이버보안 연구 학술 센터(Academic Centres of Excellence in Cyber Security Research)를 설립하는 등 영국 내 사이버 연구 역량 강화 및 사이버 산업 성장 촉진을 위한 자금을 지원하고 있으며, 국가기반시설보호센터(CPNI), 공학 및 자연과학 연구협회(EPSRC)와 함께 산업기술 보호 역량 구축을 위해 연구소를 설립하는 등 사이버보안 연구 공동체 확대를 위해 노력을 기울이고 있다.

3. 산업 육성

(1) 미국

미국은 국가차원에서 사이버보안이 충족된 제품과 서비스의 보급을 지원하기 위해 연방조달청(GSA)의 사이버보안 관련 조달·계약 업무를 강화하며 산업 육성을 꾀하고 있다. 앞서 전략에서 살펴본 것처럼 미국은 주요 기반시설의 보안 강화를 중요시하고 있어, 보안 산업 육성과 더불어 사이버보안을 강화하는 정책을 시행하고 있다. 오바마 정부 2기 때 발표된 행정명령에 의해 사이버보안 프레임워크가 완성되었고 그에 따라 프레임워크를 자발적으로 도입하고 기준을 갖춘 기업에게 주어지는 인센티브 방안도 수립되었다. 프레임워크 도입과 사이버보안 강화를 위해 주어지는 인센티브는 보조금, 세금혜택, 우선적 기술지원, 규제완화, 보험요건 책임경감 등으로 다양하다. 또한, 상무부는 국방부·조달청·무역대표부 등과 협력해 정부구매도 인센티브 방안으

로 활용될 수 있는지 검토하는 등 보안 기준을 적용하는 기업의 진흥에 상당한 의지를 보이고 있다.

(2) EU

EU는 EU 외 다른 국가에서 개발된 보안 솔루션에 과도하게 의존될 위험에 대비하기 위해 사이버보안 제품 단일 시장을 구축하려는 계획을 가지고 있다. 이를 위해 사이버보안 분야의 가치사슬을 구성하는 모든 이해당사자들(예: 장비 제조업체, 소프트웨어 개발자, 정보 사회 서비스 제공업체)이 보안을 우선순위로 인식할 때 비로소 수준 높은 보안 체계를 구축할 수 있다고 판단, 사이버보안 수행을 표시하기 위한 라벨을 제정하고 사이버보안 성과와 기록이 우수한 회사에 라벨을 부여하여 이것을 홍보 및 경쟁 우위 수단으로 활용하게 하는 등 유럽에서 사용되는 ICT 제품과 관련된 가치사슬 전반에 걸쳐 사이버보안 강화를 장려하고 있다. 또한, 사이버보안 우수 사례를 식별하고 ICT 솔루션 개발과 채택을 위해 유럽의 관련 공공·민간 이해당사자들이 한 자리에 모여 가치 사슬을 논의할 수 있는 장을 마련하여 우호적인 시장 환경 조성에 박차를 가하고 있다.

(3) 영국

영국은 사이버보안 산업의 내수시장을 확대하고 수출을 촉진하기 위해 정부와 산업계간 협력체인 '사이버 성장 파트너십(Cyber Growth Partnership)'을 설립하였다. 또한, 민간의 사이버보안 역량 강화를 위해 사이버 보안 전문가의 자격 공시, 사이버 보안 제품 및 서비스의 산업규격합격품표시(kite marking)의 확대 등의 계획을 밝히고 있다.

4. 인력 양성

(1) 미국

미국은 2010년 4월 국가 사이버보안 교육 이니셔티브(The National Initiative for Cybersecurity Education)를 발표하며, 국가차원의 체계적인 사이버보안 인력 양성을 도모하고 있다. 국립표준기술연구소(NIST)가 국가 사이버보안 교육 이니셔티브의 전

반적인 정책 관리 역할을 수행하고 있으며 국가 사이버보안 인식 제고를 포함해 교육기관의 사이버보안 교육 도입, 연방 사이버보안 인력 구조 구축, 사이버보안 인력 훈련 및 전문화 등 4가지의 정책방향을 담고 있다. 이중 연방 사이버보안 인력구조 구축의 경우, 2011년 국립표준기술연구소가 발표한 사이버보안 인력 프레임워크(Cybersecurity Workforce Framework)[18]로 더욱 체계화 시켰으며, 이를 통해 보안 역량에만 초점을 맞추기보다 시스템 관리, 운영, 데이터 분석 등 사이버 영역 전반을 포괄하는 범위에서 적재적소에 필요한 인재를 체계적으로 양성하고 있다. 사이버보안 인력 프레임워크는 〈표 4〉와 같이 실제 시스템의 구축과 운영, 관리 및 유지보수 차원에서 사이버보안 업무를 7가지로 분류하고 업무별 하위 직종에 따른 요구사항을 명시하고 있다.

〈표 4〉 사이버보안 인력 프레임워크 7가지 주요 내용

분류	설 명
안전한 기술 보급 (Securely Provision)	• 시스템 개발 영역 • 안전한 IT 시스템의 기획, 디자인, 실질적인 구축 업무 • 정보 신뢰성 보장, SW 엔지니어링, 기업 아키텍처, 기술 시연, 시스템 요구사항 계획, 테스트 및 평가, 시스템 개발 등
운영 및 관리 (Operate and Maintain)	• 시스템 운영 영역 • 시스템 운영과 행정, 관리, 유지보수 업무 • 데이터 행정, IT 시스템 보안 관리, 정보 관리, 고객 서비스, 네트워크 서비스, 시스템 행정, 시스템 보안 분석 등
보호 및 방어 (Protect and Defend)	• 보안 강화 영역 • 시스템 안정성 강화, 위협요인 최소화, 외부 공격 대응 업무 • 컴퓨터 네트워크 보안, 사고 대응, 컴퓨터 보안 인프라 지원, 보안 프로그램 관리, 취약성 조사 및 관리 등
조사 (Investigate)	• 사후 대응 영역 • 사고 및 외부 공격 원인 분석, 증거 확보 업무 • 디지털 포렌식, 사고 조사 등

18) 사이버보안 인력 프레임워크는 2013년 7월 최종 버전이 공개된 이후 점진적인 보급 및 업데이트가 이뤄지고 있는 것으로 파악

분류	설 명
운영 및 수집 (Operate and Collect)	• 정보 수집 영역 • 사이버보안 강화를 위한 정보수집 업무 • 정보 수집 운영, 사이버 운영 계획 및 수행 등
분석 (Analyze)	• 정보 분석 영역 • 통계 분석, 사이버보안 계획 수립 지원 업무 • 사이버 위협 분석, 전방위 정보활동, 취약성 분석, 타깃 분석 등
지원 (Support)	• 외부 지원 영역 • 법률 자문, 교육, 정책 연구 등

자료: 한국인터넷진흥원(2014), “주요국 사이버보안 인력양성 정책 분석”.

사이버보안 인력 프레임워크는 각 업무 분류별 세부 직종마다 주요 업무 내용과 필요한 지식 등을 구체적으로 정리해 두고 있어 기업 및 단체의 경우, 현재 필요한 인재를 파악해 추가 인력을 확보하고 사이버보안 교육 프로그램 계획을 마련하는 등 다양한 용도로 폭넓게 활용이 가능 할 것으로 보인다. 또한, 기술 훈련이 필요한 개인 역시 프레임워크를 통해 시장에서 수요가 있는 기술이 무엇인지, 해당 직종에서 구체적으로 어떠한 업무를 수행하는지 이해할 수 있어 커리어 구축에 도움이 된다.

(2) EU

EU는 회원국들에게 네트워크 및 정보보호 교육과 훈련을 위한 국가적 차원의 노력 강화의 필요성을 계속해서 제기하고 있는 상황이다. EU 사이버보안 전략 내 회원국들에게 2014년까지 학교 교과 과정에 네트워크 및 정보보호 교육을 포함시키고 컴퓨터 과학 전공 학생들을 대상으로 네트워크 및 정보보호 및 안전한 소프트웨어 개발과 개인정보 보호에 관한 교육을 실시하고, 공공 기관에 근무하는 인력들을 위해 기본적인 네트워크 및 정보보호 교육을 실시해 줄 것을 밝히고 있다. 또한, 유럽네트워크정보보호기구에 IT 전문가들(예: 웹사이트 관리자)의 기술과 역량 강화를 위한 자발적 인증프로그램인 네트워크 및 정보보호 운용자격증(Network and Information Security driving licence) 로드맵을 제안했다. 이외에도 유럽경찰대학(CEPOL)과 유럽경찰기구 등 사법 기관에 대해 사이버범죄에 효과적으로 대응하기 위해 필요한 지식과 전문

기술을 강화할 수 있도록 교육 과정의 설계와 계획을 조율해 줄 것을 언급 한바 있다.

⑶ 영국

영국은 학계와 산업 부문의 협력기관을 통해 사이버보안 인재 풀을 넓히고 수급을 강화하는 노력을 기울이고 있다. 특히 IT분야 인력 교육기관인 e-skill[19]과의 공동연구를 통해 다른 직종에서 사이버분야 경력으로의 이직을 희망하는 사람들이 참고할 만한 사이버보안 경력을 위한 직업경로를 개발하는 등 단순 인력양성을 넘어 사이버

〈표 5〉 영국 사이버보안 전문가 인증 제도의 7가지 전문가 직종

전문가 직종	역할	주요기술역량
선임자(Accreditor)	IT 시스템이 산업 기준에 부합하는지 여부를 판단하는 결정권자	리스크 평가 및 관리, 법제도 지식 등
정보보증 감사 (IA Auditor)	보안 시스템의 기준 부합 여부를 평가하는 감시자	규제환경 이해, 조사 및 평가 능력 등
정보보증 아키텍트 (IA Architect)	보안 시스템의 기획, 구축을 담당하고 리스크를 최소화하는 현장 실무자	보안 아키텍처, 개발 능력 등
정보보안 리스크 자문 (Security and Information Risk Advisor)	보안 리스크를 식별하고 해결방안을 제시하는 조언자	리스크 평가 및 관리, 사후 대청 능력 등
IT 보안 총괄 (IT Security Officer Family)	사이버보안 관련 각종 업무를 총괄하는 책임자	의사결정, 규제환경 이해, 시스템 운영·관리 능력 등
통신 보안 직업군 (Communications Security Family)	특히 통신 네트워크 분야의 전문 영역인 암호화 관련 보안 업무 책임자	의사결정, 규제환경 이해, 시스템 운영·관리 능력 등
도입 테스터 (Penetration Tester)	실제 시스템 도입 전 적합성 여부를 판단하는 테스터	테스팅 및 취약성 평가, 실무 연구 능력 등

자료: 한국인터넷진흥원(2014), “주요국 사이버보안 인력양성 정책 분석”.

19) e-skills UK(The National Skills Academy IT): 경쟁력있는 IT분야 인력 육성을 위해 IT교육 전략 및 프로그램 수립, 기업체의 문제해결 지원 등을 수행하는 교육기관

보안 경력의 체계적 관리도 지원하고 있다. 또한, 사이버보안 전략의 일환으로 정보통신본부(CGHQ)산하 국가정보보증기술국(CESG)에서 사이버보안 전문가 인증제도(Certified Professional)를 시행해, 사이버보안 및 정보보호와 관련된 직업들을 상세하게 분류하고, 각 직군별 기술 수준을 데이터화[20]함으로써 정보보안 관련 여러 직종별 역할 및 역량을 정립하였다.

5. 인식제고

(1) 미국

미국은 사이버보안 인식을 위해서도 적극적인 활동을 벌이고 있다. 범국가차원의 홍보와 캠페인을 실시하는데 대표적인 캠페인으로 'STOP, THINK, CONNECT'과 '국가 사이버보안의 인식 제고의 달' 운영을 들 수 있다. 'STOP, THINK, CONNECT' 캠페인은 '사이버공간 정책 리뷰('09)'를 기초로 고안되었으며 국토안보부에서 사이버보안 인식 제고를 위해 보안 준수사항을 알리는 캠페인이다. 또한, 매해 10월로 지정된 '사이버보안 인식 제고의 달'은 올해로 11번째를 맞았으며 'STOP, THINK, CONNECT' 캠페인과 연계되어 범국민 사이버보안 교육도 함께 운영되고 있다.

(2) EU

유럽도 마찬가지로 사이버보안의 중요성을 강조하기 위해 유럽네트워크정보보호기구를 비롯한 유럽 경찰기구, 유럽 검찰기구, 각 국 데이터보호기관 등은 인식제고 노력에 힘쓰고 있다. 유럽의 '사이버보안의 달'이 2012년 10월 시험적으로 실시되었고 매해 10월이 사이버보안의 달로 지정되어 각종 세미나와 교육 프로그램 등이 운영된다. 또한, 대학생들 간에 경합을 벌이는 사이버보안 선수권 대회도 추진하면서 민·관·학 협력을 강조하고 있다.

20) 각 직업별 인증 기준을 통과하기 위한 기술 역량을 크게 9가지 카테고리로 구분하고, 각 역량들을 카테고리별로 A부터 F까지의 코드로 분류해 점수를 부여할 수 있게 하였음.

(3) 영국

영국은 다양한 주체별 대상의 맞춤형 사이버보안 인식제고 방안을 마련하고 추진중에 있다. 사이버보안의 학위를 신설해서 학생들의 관심을 모으고 있으며 보안 박람회 등을 개최해 중소기업의 인식제고에도 앞장서고 있다. 올해 8월, 영국은 새로운 인식제고 프로그램인 '사이버 상식(Cyber Streetwise) 캠페인'과 '사이버 센츄리온(Cyber Centurion)'의 추진을 발표했다. 사이버 상식 캠페인은 범죄수사국을 주체로 해서 영국 시민들이 안전한 사이버 생활을 영위하는데 필요한 보안 관련 정보와 상식을 알려주는 행사이며, 사이버 센츄리온은 12~18세 청소년들이 참여하는 대회로 청소년들이 사이버보안 진로에 관심을 갖도록 독려하기 위한 목적으로 시행되는 행사이다.

6. 국제협력

(1) 미국

미국은 사이버보안 및 범죄에 효과적으로 대응하기 위해 EU·영국·인도 등 주요국 및 글로벌 기업들과 협력 관계를 강화하는 움직임을 보이고 있다. 미국과 EU는 사이버보안 및 사이버범죄 워킹그룹이 출범하였고, 미국과 인도는 사이버테러 정보 공유 등 사이버보안 협력을 위한 양해각서를 체결하기도 했다.

(2) EU

EU는 인터넷 개방성과 자유 증진, 디지털 양극화 해소, 사이버보안 역량 강화 등의 핵심가치를 옹호함과 동시에 사이버 기술이 평화적이고 개방적으로 이용되도록 세계 차원으로 노력하고 있다. EU 집행위원회, 고위대표부, 유럽평의회, 경제협력개발기구(OECD), 유럽안보협력기구(OSCE), 북대서양조약기구(NATO), 국제연합(UN) 등과 같은 국제기구들과의 정책 대화 및 협력을 통해 사이버 방위 능력을 강화하고 있다.

(3) 영국

영국도 EU와 마찬가지로 자유롭고 개방적인 인터넷의 미래 가치를 보호하기 위한 여러 가지 국외 활동들을 보여주고 있다. EU, 북대서양조약기구 등과의 공동 작업을

통해 국제 협력을 강화하는 것을 비롯해 다른 국가, 조직과의 공동 작업을 통한 사이버공간의 행동 규범 조성을 위해 국제협력 및 글로벌 사이버 역량강화, 인식제고 등의 활동을 계획 중에 있다.

Ⅳ. 결론 및 시사점

이상 본고에서는 추진체계·복원력 강화·산업 육성·인력 양성·인식제고·국제협력 등 6개 부문으로 나누어 미국·EU·영국의 사이버보안 전략을 비교해서 살펴보았다. 그리고 이를 통해 다음과 같은 분석결과를 도출해 낼 수 있다.

- **추진체계**: 미국·EU·영국은 사이버보안 전략을 추진, 실행할 총괄·전담 부처를 지정하여, 세부 추진사항에 대해서는 전략 실행 시 업무 특성에 따라 해당 관계부처와의 협력을 통해 추진하고 있다. 이러한 부분은 국가 차원의 사이버위협이 발생할 경우, 대응력에 대한 즉응성(卽應性) 강화와 함께 전략 추진 시 필요한 전문성을 십분 활용하는데 큰 기여를 할 수 있을 것으로 생각한다. 특히 미국의 경우, 백악관을 사이버보안 컨트롤타워로 하고 사이버보안조정관 직위를 신설하여, 국가 최상위 수준에서 사이버보안 전략을 총괄 담당하고 있는 것을 살펴볼 수 있었다. 이는 사이버보안 전략 추진 시 책임의 명확화와 함께 부처 내 사이버보안 전략 추진 시 부처 간 역할 조정, 국가 차원의 사이버보안 전략 추진에 있어 대통령의 지시사항을 명확하게 반영할 수 있는 효과가 있을 것으로 판단된다.
- **복원력 강화**: 주요국들은 효과적인 사이버위협 대응을 위해 민·관 협력을 추진함과 동시에 국가 또는 국가 간 사이버훈련을 수행함으로써 사이버위협 대응의 절차와 부족한 부분을 점검·검토 할 수 있는 노력을 하고 있다. 영국은 사이버위협 정보를 실시간으로 교류할 수 있는 플랫폼인 사이버보안정보공유협력체(CISP)를 발족하여 주요기반 시설사업자들과의 효과적인 사이버위협 정보 공유의 장을 마련했으며, 미국은 주요기반 시설별 보호체계 구축을 위한 사이버보안 프레임워크

를 개발해 사업자별, 담당자별 자체적인 복원력 강화 노력에 기울일 수 있는 수단을 마련하였다.

- **산업육성**: 세 국가 모두 자국 내 사이버보안 제품과 서비스의 확산을 통해 보안 솔루션에 대한 제3국의 의존도를 낮추는 것과 동시에 내수시장 확대는 물론 해외 수출을 통한 경제성장의 새로운 동력으로 활용하고 있는 것을 살펴볼 수 있다. EU는 사이버보안 전략 내에서 제3국의 보안 솔루션에 과도하게 의존하게 될 것을 우려해 민간부문의 사업자 등 관련 이해관계자들의 사이버보안 수행 요건에 필요한 유인책 마련 필요성을 밝히고 있는 등 보안 솔루션 자주권 확보를 위한 구상을 하고 있는 것으로 판단된다.
- **인력양성**: 세 국가들은 국가차원의 사이버보안 인력 양성 계획 수립과 함께 사이버보안 직업 경로 개발을 통해 사후관리에도 관심을 기울이고 있는 것으로 나타났으며, 학교 교과과정과의 연계를 통한 전 국민의 사이버보안 기본 역량까지 고려하고 있다. 특히 미국과 EU의 경우, 사이버보안 인력 프레임워크와 사이버보안 전문가 인증제도를 마련해 업무별 직종 간 구체적인 전문기술의 내용과 요구사항을 제시하며, 공공과 민간 분야에서 사이버보안 인력의 역량을 직관적으로 판단할 수 있는 근거를 마련해 주었다.
- **인식제고**: 미국·EU·영국은 범국가 차원의 국민 대상 사이버보안 인식 프로그램과 각종 캠페인 등을 마련·실시하고 있으며, 민간과의 협력을 통해 효과적인 인식제고를 위해 노력 중에 있다. 이는 사이버보안의 중요성과 심각성에 대해 각인시켜주는 것과 동시에 국민 스스로가 사이버보안을 선제적으로 예방할 수 있게 하는 근원적 동인을 이끌어내는 조치라고 생각된다.
- **국제협력**: 분석한 국가들은 국가 간에 국경이 없는 사이버위협의 특성상 하나의 국가 단위에서의 사이버보안 대응이 어렵다는 것을 인식함에 따라 이를 위해 국가·국제기구 등과 함께 다양한 협력을 추진 및 체결하고 있다. 또한, 자국 내 사이버 상의 가치를 전 세계로 전파하기 위해 다양한 국제기구활동에 적극적으로 참여하고, 국가를 넘어 글로벌 사이버 역량 강화를 위한 노력을 기울이고 있다.

이상 주요국의 사이버보안 전략 비교·분석을 토대로 국내 사이버보안 전략 추진에 관한 제언을 하면 다음과 같다.

첫째, 주요국의 사이버보안 전략의 핵심이라고 할 수 있는 사이버위협 정보공유와 민·관 협력의 강화이다. 사이버위협에 효과적으로 대응하기 위해서는 민간과 공공의 정보가 원활하게 공유되어야 하고 이를 통한 협업이 필수적이다. 미국의 정보공유서비스(ECS), EU의 협력 메커니즘 운영, 영국의 사이버보안정보공유협력체(CISP) 등이 소속을 초월한 협업 프로세스를 만들기 위한 노력을 보여준다고 할 수 있다. 국내도 이러한 정책들을 참고해 사이버위협 정보를 공유하고 협력을 강화하는 협력체 설립 혹은 프로세스 확립 등을 검토해 볼 수 있을 것이다.

둘째, 효과적인 사이버위협 대응을 위한 체계적인 사이버침해 정보 공유 절차 마련 등 민·관 사이버보안 협력 프로세스 마련과 함께 이를 점검할 사이버보안 훈련을 분야별(금융, 의료, 제조 등)로 수행하는 것도 생각해볼 수 있다. 이를 위해 국내 유관기관(산·학·연·관) 담당자로 구성된 침해정보 공유 협의체를 구성하여 효과적인 사이버위협 정보(대응 우수사례 포함) 공유 방안과 절차를 마련하고, 산업 분야별로 이를 점검하는 대응 훈련을 시행해야 할 것이다.

셋째, 국내 사이버보안 제품 확산 지원 및 해외 사이버보안 제품 수출 판로 개척을 지원할 필요가 있다. 사이버 공간을 통해 국가와 기업 내 기밀 유출사고 등 사이버 피해가 계속해서 증가함에 따라 이에 대응할 보안 솔루션, 컨설팅 서비스 등의 수요가 계속해서 증가할 것으로 생각된다. 이에 국가 차원의 사이버보안 제품 R&D 지원과 함께 해외 시장 진출에 필요한 기본적 제반 사항을 지원해 국내 사이버보안 제품의 글로벌 경쟁력을 강화시켜야 할 것이다.

넷째, 일관성·연속성 있는 사이버보안 전문 인력 양성 계획 수립과 함께 사이버보안 전문 인력 커리어를 관리할 수 있는 로드맵을 마련할 필요가 있다. 사이버보안 전문 인력에 대한 국가 차원의 명확한 정의와 함께 민간과 공공부문에 분산되어 있는 사이버보안 교육을 통합 관리해야하기 때문이다. 또한, 단순 전문 인력 양성에 치우친 것이 아닌 급변하는 보안 트렌드에 맞는 전문성을 갖춘 인재를 양성할 수 있도록 사

후 관리에도 관심을 가져야 할 것이다.

마지막으로 국제연합·북대서양조약기구 등 국제기구 및 국가 간 사이버보안 협력을 강화해야 한다. 우리나라가 사이버보안 역량에 대한 비교우위가 있는 것을 활용하여 협력을 추진해야 할 것이며, 더불어 국제기구가 주관하는 여러 사이버보안 관련 논의 회의에 적극 참석한다면 사이버보안 가치와 함께 글로벌 사이버보안 패러다임을 생성하고 이끌어갈 수 있을 것이다.

참고문헌

국토안보부 홈페이지(www.dhs.gov).

김은혜·이재일, "미 오바마 정부의 사이버보안 주요 정책 및 법안", 2011. 8.

민경식·지순정, "미국의 사이버보안 정책과 R&D 전략에 관한 분석", 2013. 1.

백악관 홈페이지(www.whitehouse.gov).

한국인터넷진흥원 (2014), "주요국 사이버보안 인력양성 정책 분석".

Cabinet Office, "Progress against the Objectives of the National Cyber Security Strategy", 2013. 12. 12.

_____, "The National Cyber Security Strategy: Our Forward Plans", 2013. 12. 12.

DHS, "Executive Order 13636: Improving Critical Infrastructure Cybersecurity –Incentives Study Analytic Report", 2013. 6. 12.

____, "Sector Risk Snapshots", 2014. 5.

European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", 2013. 2. 7.

NIST, "Framework for Improving Critical Infrastructure Cybersecurity", 2014. 2. 12.

The White House, "Cyberspace Policy Review", 2009. 5.

_____, "Executive Order – Improving Critical Infrastructure Cybersecurity",

2013. 2. 12.

The White House, “Presidential Policy Directive – Critical Infrastructure Security and Resilience”, 2013. 2. 12.