국외 장기훈련 결과보고서

국방 사이버 분야 국제협력 방안 연구

2022. 12.

국 방 부
김 성 규

< 목 차 >

Ⅰ. 서론

제1절 연구배경 및 목적

정보통신기술의 발전으로 국제사회는 초연결성·초지능성 사회로 진출하면서 국민들의 삶이 더욱 윤택해지고 편리해지는 등 우리 인류는 사회와 문화, 경제적으로 수많은 혜택을 경험하고 있다. 그러나 아이러니하게도 사이버 공간에서 사이버범죄나 사이버 공격도 고도화되면서 각종 위협이 증가하였고, 국가 공공기관과 기업 그리고 국민의 삶에 큰 불편과 함께 국제사회의 안보구조는 커다란 도전에 직면해 있다. 사이버위협은 해킹, 디도스(DDoS), 기밀정보 절취, 정보시스템 무력화 등 여러 형태로 발생하고 있으며, 군사기밀은 물론 첨단무기 및 적대세력에 관한 기밀자료, 금융기관의 시스템 정보, 국가 공공기관의 중요 정보시스템 등 국가의 안보에 큰 영향을 미치는 요소들은 사이버 공격의 위협에 항상 노출되어 있다. 정보통신기술의 급격한 발전에 따라 국제사회의 안보환경이 새롭게 급변하고 있는 것이다.

인터넷이 급속도로 확산됨에 따라 어느 누구든지 익명으로 공격 대상을 설정하여 위협을 가할 수 있게 됐다. 특히 해커에 의한 사이버 공격은 개인 또는 작은 단체의 수준임에도 불구하고 국가의 안전을 위협할 수 있는 일종의 테러 행위만큼 위협적이다. 사이버테러는 '인터넷을 통해 특정 사이트를 공격하여 정치·이념·경제·종교 그리고 군사적 목적을 달성하기 위한 행위'라고 규정할 수 있다. 지금 현재 이러한 사이버 공격은 전 세계에서 지속적으로 발생하고 있는 것이다.

Joe Biden 美 대통령이 취임한 이후 처음으로 개최된 美·러 양국 간의 정상회담에서 사이버 공격 금지시설에 대한 합의를 정하기로 하면서 사이버 무기에 대한 의제를 다루었다. New York Times의 David Sanger 기자는 "강대국 간의 정상회담은 과거에는 핵무기에 관한 것이었으나 지금은 사이버 무기에 관한 것이다"라고까지 표현했다. 핵무기

와 관련된 사안은 여전히 강대국 간의 주요한 회담 의제지만 이제는 사이버위협이 강대국 정상 간의 회담 시 최우선으로 다루어지는 의제가 될 정도로 중요해졌다.

사이버 전쟁은 정보기술을 이용하여 사이버 공간에서 벌어지는 작전으로 전쟁이 시작되자마자 단숨에 승부를 결정지을 수 있는 전쟁이다. 아이러니하게도 정보기술이 발달된 나라일수록 불리할 수 있다는 것이 사이버 전쟁의 특성이다. 다시 말하며, 인터넷이 발달된 나라일수록 사이버 공격에 취약할 수밖에 없다는 뜻이다. 인터넷과 같은 네트워크를 이용하는 사이버 공격은 저비용 고효율의 공격방식이다. 시공간 제약 없이 공격할 수 있고, 빠르게 확산되며 피해 규모도 엄청나다. 금융, 전력, 통신망 등 국가 정보인프라 시스템을 포함해 우리 군의 무기와 지휘통제체계 등에 대한 사이버 공격은 재래식 무기를 통한 군사적 위협과 함께 국가안보를 위협하는 요인이다.

정보통신 기술과 인프라의 발전에 따라 군 업무와 군사작전 수행도 사이버 공간에서 이루어지는 비율이 증가하고 있으며, 이미 우리나라의 전장 환경은 컴퓨터와 온라인 네트워크에 크게 의존하고 있다. 지휘통제체계와 감시·타격을 위한 첨단 무기체계가 네트워크로 연동되어 작전을 수행하고 있으며, 대부분의 국방자원이 초연결 네트워크로 연결되고 있는 현실을 볼 때 사이버안보는 곧 국가방위의 안보와 직결된다고 할 수 있다. 이렇게 첨단과학기술이 활용되는 군의 작전환경은 사이버 전장의 보이지 않는 적에게 대응할 수 있는 능력을 요구한다. 최근 러시아의 우크라이나 침공을 보면 이제는 국가가 사이버 공격 전면에 나서는 양상을 보이고 있다. 우리도 지속적으로 발생하고 있는 북한의 사이버 공격이 전쟁 발발시 핵과 미사일 공격 이전에 우선적으로 자행될 수 있음을 최근 우크라이나 전쟁을 통해 경험하였다. 세계 각국은 이미 사이버 공격을 국가적 안보위협으로 인지하고, 사이버 안보태세를 강화함과 동시에 사이버 전장에서 우위를 차지하기 위한 전략을 구체화하고 있다.

사이버위협은 초국가적 형태로 진행되므로 하나의 국가 차원의 대응으로는 한계가 있는 것은 분명하다. 그것은 사이버 공간이 갖는 익명성과 공격 수월성으로 인해 사이버위협 문제는 국가 간 협력을 통해서만 해결할 수 있는 글로벌 문제 중 하나이다. 특히, 최근 단순 호기심 목적의 해킹 차원이 아닌 국가안보 차원의 사이버 공격으로 확대되고 공격 양상이 하나의 국가에만 국한되지 않고 여러 국가를 동시에 대상으로 하는 형태를 띄고 있어 사이버안보에 대한 국제협력이 절대적으로 필요하다. 그러나, 국제사회는 UN 등 국제기구나 지역 차원의 협력기구를 통한 초국적 협력 대응을 하고 있으나 국경을 봉쇄하고 스스로 고립하는 등의 자국 최우선주의 정책도 확산되고 있어 이러한 상황은 다양한 안보위협에 대한 국제사회의 결속과 다자안보협력을 약화시키는 요인이 되고 있다.

최근 국제사회는 코로나19 팬데믹으로 인해 뉴노멀 시대를 맞이하고 있고, 미중 간 패권경쟁이 더욱 격화되고 있는 상황이다. 사이버안보도 이와 같은 상황의 영향으로 크게 변화하고 있다. 현재 사이버안보의 국제정치는 미중 간에 벌어지고 있는 영향력 확대 경쟁과 상호간 견제, 국제기구 간에 벌어지고 있는 사이버 패권경쟁 등으로 나타나고 있다. 사이버안보 분야에서의 국제협력은 각국이 참여하는 실질적 협의체 구성이나 국제규범 등의 필요성에도 불구하고 미국과 중국 진영 간의 이견으로 사이버 공간에 대한 국제적 합의 도출이 쉽지 않은 상황이다. 이러한 합의가 이루어질 수 없었던 근본적인 원인은 미국 등 서방 진영 국가와 러시아·중국 등 정보통신 강국 간의 이해관계가 충돌하기 때문이다. 즉, 자유로운 정보의 유통을 보장하되 사이버 위협행위에 대해서만 기존 국제법을 적용해 통제하자는 미국을 포함한 서방 진영과 각국의 국가 주권에 기초하여 국제법과 다른 별도의 사이버 관련 법을 제정하여 사이버 공간을 통제하고 관리하자는 중국과 러시아를 포함한 비서방진영이 대립되고 있는 양상이다. 만약 미국 및 서방 진영 국가들과 러시아·중국 등 정보통신 강국 간에 그리고 정보통신 선진국과 후진국 간에 이해조정과 의견조율을 통해 협력이 이루어졌다면 아마 사이버 국제질서는 벌써 수립되었을 것이다.

사이버 공격의 형태가 다양화되고 북한 해커에 의한 피해 규모가 커지면서 사이버위협에 대한 우려와 걱정은 날로 심화되고 있다. 또한, 사이버 전쟁이 현실화되고 그에 따른 사이버 무기 경쟁도 치열해질 수밖에 없다. 따라서, 심각해지는 사이버위협을 제거하여 사이버 전쟁이 발생되지 않도록 미연에 방지하고 사이버 평화안보체제를 구축할 수 있는 국방 차원의 사이버 국제협력의 노력이 매우 필요한 시점이다.

이에 본고에서는 최근 발생하고 있는 사이버위협 사례와 우리나라를 포함한 사이버 주요국가들의 사이버 동향 분석과 더불어 사이버 공격에 대한 대응전략과 체계를 살펴보고 국방 사이버를 포괄하는 사이버안보 분야에서의 국제협력 사례를 통한 시사점을 도출하여 우리가 추진해야 하는 국방 차원의 실질적인 사이버 국제협력 발전방안을 제언하고자 한다.

제2절 연구내용 및 방법

1. 연구목표

사이버안보 평화체제 구축을 위한 국방 분야에 있어서 사이버안보 국제협력 발전방안을 모색한다.

2. 연구내용

최근 사이버위협 동향 분석과 국제 및 지역 다자안보협력기구 현황과 활동 등을 조사하고, 사이버위협에 대한 국가별 국제협력을 포함한 대응전략과 추진체계를 분석하여 우리 군의 군사적 사이버 신뢰 구축과 사이버역량 강화를 위한 구체적인 국방 분야의 국제협력 발전방안을 고찰하고자 한다.

가. 주요 사이버위협 사례 조사

우리나라뿐만 아니라 해외 주요국들에게 발생한 과거 주요 사이버위협 사례를 조사하고 사이버위협이 어떠한 형태로 발생하고 변화하고 영향을 주고 있는지 사이버위협 사례를 통해 알아본다.

나. 국제 사이버 협력 기구 조사

점증하는 사이버위협에 대응하기 위한 국제사회의 사이버 관련 협의기구들의 역할과 특성, 최근 활동 사례들을 조사하고, 국제기구 차원의 협력 외에도 각 지역별 지역 기구와 양자 차원의 사이버 신뢰 구축을 위한 사례를 조사한다.

다. 주요국들의 사이버안보 동향 분석과 대응체계 분석

지속적으로 증가하는 사이버 공격에 대비하기 위한 세계의 주요국가들의 다양하고 독창적인 사이버안보 대응전략과 이행을 위한 사이버안보 관련 조직별 임무와 기능, 그리고 국제협력 활동 사례를 조사한다.

라. 우리나라의 국제협력 현황 및 국방 분야 국제협력 발전방안 모색

북한 이외에도 우리의 사이버 공간을 공격하는 주요 근원지인 중국·러시아로부터의 사이버위협이 지속되고 있는 상황에서 우리나라가 추진하고 있는 국가 차원의 대응전략과 미국을 비롯한 동맹국과의 양자·다자간의 사이버 국제협력 사례를 조사한다. 또한, 국방부 차원의 동맹국 및 우방국들과 양자 및 다자적 사이버 국제협력 관계를 조사하고, 타국가와 군사적인 유대를 강화하며 교류 협력 확대 및 사이버역량을 강화하기 위한 국방 사이버 분야의 국제협력 발전방안을 모색한다.

3. 연구 수행 방법

본 연구는 사이버 국제협력 방안에 대한 연구이니만큼 국내·외 문헌을 인터넷과 도서관 기록물을 활용하여 조사하였고, 관련 기관 웹사이트 방문 및 언론기사 등을 조회하여 관련 자료를 추가로 확보하였다. 국가 차원의 사이버 국제협력과 관련되어서는 여러 논문과 동향보

고서 형태로 많이 기술되고 있으나 국방·군 차원의 사이버 관련 협력 활동 사례를 조사하는 데는 어려움이 있었다. 캐나다 방문 연구소(Centre of Asia-Pacific Institute, CAPI) 연구기록물과 대학 도서관 자료, 외국 국방·군 관련 웹사이트를 통해 국방 분야의 사이버 관련 자료를 조사하였고, 인근 대학의 사이버 관련 교수와 방문 연구소(CAPI) 연구진들과의 인터뷰를 통해 국방 차원의 사이버 협력방안에 대한 아이디어를 얻고자 하였다.

가. 문헌 연구

최근 국제사회의 사이버안보 환경과 이슈, 주요 국가별 사이버 대응 체계 및 전략, 국제협력 활동 사례, 국제기구 및 다자안보협의기구의 역할과 성격, 성과 등을 각종 국내·외 논문 및 동향보고서, 관련 기관 웹사이트, 언론기사, 세미나 자료, 그리고 방문 연구소(CAPI) 및 대학 도서관 기록물 등을 통해 자료를 수집하여 분석하였으며, 국제·다자안보 기구 및 양자 차원의 다양한 협력 활동과 각국의 사이버위협 대응 전략 차원의 협력 사례를 참고하여 우리가 적용 가능하고 더욱 확대해야 할 국방 차원의 국제협력 발전방안에 대한 아이디어를 도출하고자 하였다.

나. 방문 조사 및 토의

동맹국과의 사이버 전쟁 역량을 강화하고 비우호국과의 사이버 갈등을 최소화할 수 있는 국방 분야 사이버 신뢰 구축을 위한 국제협력 방안에 대한 아이디어를 도출하기 위해 인근 대학의 사이버 관련 교수 및 방문 연구소(CAPI) 연구진들과 토의를 실시했다.

Ⅱ. 과거 주요 사이버위협 사례 및 최근 동향

제1절 해외 사이버위협 사례

2007년 러시아 해커집단의 사이버 공격으로 에스토니아 국가기능이 마비되었다는 사실은 전 세계에 엄청난 충격을 주었는데 사이버 전쟁이 곧 현실화될 수 있다는 우려를 낳기도 했다. 에스토니아는 그 당시 세계에서 가장 먼저 인터넷으로 전자투표를 실시하여 'e-스토니아'라는 별명을 가질 정도로 인터넷 활용이 활성화되었고 발트해의 인터넷 강국(强國)으로 불리는 나라였다. 그러던 중 에스토니아 수도 탈린에 있던 소련군의 동상 이전 문제로 러시아와 갈등이 발생하였다. 1000여 명의 러시아계 시민들의 동상 이전 반대 시위로 유혈사태가 발생했고 이를 계기로 러시아와 에스토니아 간의 갈등이 빚어졌다. 당시 대통령궁을 포함한 총리실, 의회를 비롯한 대부분의 정부 중앙부처, 신문사 은행 등 홈페이지와 전산망에 디도스(DDoS) 공격이 발생하였다. 공격은 3주 동안 지속되었고 국가 기간망이 1주일 이상 마비되고 금융거래와 행정업무가 불통 상태가 되었으며 수천만 달러의 피해를 입혔다. 에스토니아 정부는 북대서양조약기구(NATO) 국방장관 회의에서 사이버 공격의 배후로 그 당시 외교적 갈등을 빚던 러시아의 소행이라며 문제제기를 했다. 이전 소규모 사이버 공격과 달리 국가 전체에 큰 피해를 미침으로써 사이버 공격이 국가안보를 위협하는 심각한 요인이 된다는 점을 국제사회에 인식시켜 준 사건이었다. 이후 에스토니아·독일·스페인·이탈리아·슬로바키아·라트비아·리투아니아 등 북대서양조약기구(NATO) 소속 7개 국가가 에스토니아 수도 탈린에 '사이버테러 방어센터'를 설립하였다.

2008년에는 조지아에서 분리 독립하려는 남오세티야 자치공화국과의 전쟁 과정에서 남오세티아에 이미 주둔해 있던 러시아군 몇 명이 사망했다는 것을 명분으로 러시아가 조지아를 공격했다. 이 전쟁 과정에서 러시아는 조지아의 정부와 금융기관은 물론 軍 정보시스템을 해킹하여

오작동을 유도하였다. 군대에 의한 물리적 공격과 동시에 사이버 공격이 이루어진 첫 번째 전쟁으로 전쟁 시작 5일 만에 조지아는 결국 손을 들었다. 이 사건은 총성 없는 사이버 전력의 강력한 위력을 전쟁터에서 여실히 보여준 사례로 사이버 공격은 상대국의 국가시설을 마비시키고 군사작전을 무력화하여 상대국을 파괴하는 미래전의 양상이 될 수 있음을 국제사회에 각인시켜 주었다.

2010년에는 나탄즈라는 이름의 이란 핵시설에 위치한 원심분리기가 파손된 사건이 발생하였는데 이란의 핵무기 프로그램을 방해할 목적으로 이스라엘과 미국이 감행한 사이버 공격이었다. 이때 악성코드 '스턱스넷(Stuxnet)[1]'이 사용되었는데 이전까지 등장한 악성코드가 자기 과시를 하거나 금전적인 이익을 목적으로 한 것과 달리 집중 타켓으로 설정한 시설의 파괴만을 목표로 하고 있다는 점이다. 이 공격으로 원심분리기 가운데 20%의 가동을 중단시켰고 이란의 핵무기 개발 일정이 지연되었다. 이 사건은 악성코드가 사이버 무기로 사용된 첫 번째 사례로 이란의 원전이 외부와 차단된 폐쇄망 형태의 네크워크로 운영되었음에도 피해를 입었다는 점에서 국제사회에 큰 경각심을 일깨워 주었다.

소니픽처스에서 북한 김정은이 암살되는 내용의 영화를 제작하여 북한과 갈등이 발생하였으며 북한은 미국과 해당 영화를 개봉한 국가에게 무자비한 보복을 가할 것이라 엄포와 함께 2014년 11월 평화의 수호자(Guardians of Peace)라는 해커집단이 소니픽처스의 기밀정보를 유출하고 내부 시스템을 파괴하였으며, 2014년 12월 해커는 소니픽처스 직원명단과 미개봉 영화, 기밀문서 등을 인터넷에 공개하였다. 이에 미국은 소니픽처스 해킹이 북한 소행으로 규정하고, 정찰총국을 대상으로 하는 고강도 대북 제재를 담은 행정명령을 발동하기도 했다. 미국이 특정 국가를 해킹의 배후로 지목하고 공식적인 보복에 나선 최초의 사건이었다.

2015년 러시아 해커들이 백악관 전산망을 침입하여 버락 오바마 미

1) 스턱스넷(Stuxnet)은 웜 바이러스의 일종으로 MS Window를 통해 감염되어 산업시설을 감시하고 파괴하는 악성 소프트웨어임

국 대통령의 일정과 관련된 비공개 정보에 접근한 사건이 발생하였다. CNN에 따르면 美 국무부 시스템의 허점을 이용한 백악관의 컴퓨터 시스템 해킹 사건으로 美 연방수사국(FBI), 비밀경호국(SS), 정보국 등이 참여한 조사결과 해킹에 사용된 코드 등에서 이들이 러시아 정부를 위해 일한다는 흔적이 발견되었다고 한다. 하지만 백악관, 국무부 등 美 정부는 구체적으로 해킹이 누구에 의해 일어났는지 언제 어떻게 일어났는지에 대한 공식적인 입장을 밝히지 않았다. 이 사건을 계기로 미국은 러시아를 중국·북한·이란과 함께 사이버 분야의 잠재 적대세력으로 꼽았다.

2017년 5월 발생한 워너크라이 랜섬웨어(Ransomware) 사이버 공격으로 전 세계 150개국 30만대 이상의 컴퓨터가 피해를 입었다. 워너크라이 랜섬웨어라는 악성코드는 PC, 시스템 등을 마비시킨 후 복구하려면 가상자산을 지불하라는 단순한 방식을 취했다. 워너크라이 사이버 공격의 피해는 미국을 비롯하여 러시아, 유럽, 인도, 대만 등에 특히 집중되었고 가장 큰 피해를 입은 국가는 러시아로 내무부와 은행, 통신사 그리고 철도업체 등이 감염돼 시스템이 폐쇄되었다. 한국, 일본, 중국 등에서도 사례가 여럿 발견되었다. 페덱스(FeDex), 도이체반, 닛산(Nissan) 등 대기업이 피해를 보았고, 수십만 대의 컴퓨터가 이 워너크라이 사이버 공격으로 피해를 입었다. 몇몇 사이버 전문가들은 워너크라이의 배후가 북한일 것으로 추정하고 있다. 이 사건은 사이버 공격이 경제적 목적을 위한 수단으로 활용될 수 있음을 보여준 사례이다.

2020년 12월 전 세계를 들썩이게 한 러시아발 공급망 해킹 공격 사건이 발생하였다. 사이버 글로벌보안 기업인 'FireEye(파이어아이)'를 시작으로 국방부, 국토안보부 등 정부 기관들이 잇달아 러시아 정부 산하에 있는 첩보조직과 관련된 해커집단의 소행으로 추정되는 해킹 공격에 뚫렸다. 국가안보국(NSA)과 국방부 등 미국 정보기관 모두 공격이 몇 달 전부터 진행 중이었지만 이를 감지하지 못했다. 솔라윈즈 공격은 중대한 물리적 결과를 초래할 수 있는 전례가 없는 사건으로 미국 역사상 최악의 사이버 공격이자 미국 사이버보안 자체의 문제를 드러낸 사례로 평가받고 있다.

2022년 2월 15일 러시아의 우크라이나 침공 가능성으로 긴장이 고조되고 있는 가운데 우크라이나에서 軍과 국방부, 은행 등이 사이버 공격을 받았다. 우크라이나 국방부, 외무부 등 정부 기관 사이트들과 대형 은행 등 적어도 10개 주요 사이트가 사이버 공격을 받아 접속에 장애가 발생하였다. 러시아가 자국 해커들을 동원해 우크라이나 내 주요 시설 및 기관에 대해 여러 차례 사이버 공격을 자행했는데 마이크로소프트(MS)社는 해커들이 우크라이나 침공 이후 지속적으로 파괴적인 맬웨어인 '와이퍼[2]'를 이용하여 사이버 공격을 감행했다고 했다. 또한, 영국 언론사인 The Times는 중국이 러시아의 우크라이나 침공 직전 우크라이나의 군사 및 핵시설에 대해 대규모 사이버 공격을 시도한 사실도 드러났다고 보도하기도 했다. 이 사건은 사이버 무기를 활용한 공격이 새로운 형태의 강력한 전쟁 도구가 되고 있음을 여실히 보여준 사례이다.

제2절 우리나라 사이버위협 사례

국제사회에서 발생한 사이버 공격 사례와 같이 우리나라도 정보기술의 발전으로 지속적으로 사이버 공간상의 취약점이 발견되고 피해사례 및 규모가 폭증하고 있다. 사이버 공격으로 인한 경제적 손실, 개인정보 유출, 군사 분야의 정보 유출도 기하급수적으로 발생하고 있다. 최근 들어서는 해킹·컴퓨터바이러스 유포 등의 기술을 이용한 산업 기밀 절취, 정보시스템 마비 등 새로운 유형의 위협이 등장하고 있는데 이제 우리나라의 사이버 공격 피해 가능성은 미국 등 정보통신 강대국 수준에 도달한 것으로 판단된다. 우리나라도 국경없는 사이버위협에서 자유롭지 못하다는데 전문가들의 공통된 주장이다.

우리나라에서 발생한 주요 사이버 피해사례들을 살펴보면, 2003년 1월 25일 우리 인터넷망이 서비스 거부 공격으로 마비된 사건이 일어났

2) 와이퍼는 일단 감염되면 Computer의 Hardware를 완전히 삭제해 버리는 프로그램임

다(1.25 인터넷 대란). 이는 미국, 호주 등으로부터 유입된 SQL 슬래머 웜(Slammer Worm)[3]이 PC를 감염하여 대량의 데이터를 생성해 네트워크를 공격함으로써 KT 혜화전화국이 운영하는 시스템 서버에 트래픽 급증과 인터넷 접속 장애를 일으켜 중단된 사고이다. 미국의 인터넷 측정 및 연구를 위한 세계 최고의 조직으로 인정받고 있는 산·학·연·관 협력 협회인 CAIDA(The Cooperative Association for Internet Data Analysis)의 발표에 따르면, 전 세계 감염시스템의 11.8%가 우리나라에서 감염되어 일본이나 중국에 비해 크게 7배에 달하는 것으로 보고되었다. 우리나라의 피해가 다른 국가에 비해 규모가 가장 컸던 것은 정보통신 관련자들의 사이버보안에 대한 안일한 인식이 대규모 사태를 키웠다고 보고 있다. 1.25 대란 이후 유사한 상황이 재발되지 않도록 다양한 대책이 마련되었는데 그 중 인터넷 상태를 항상 감시하고 대응할 수 있는 '인터넷침해대응센터(KISC)'가 설립되었고 정보통신망법 등 관련 법체계도 정비되었다.

2009년 7월 7일 북한의 110호 연구소의 소행으로 보이는 인터넷 대란이 발생하였는데 청와대 및 백악관, 주요 언론사와 주요 정당 그리고 금융기관 등을 대상으로 3차에 걸친 사이버 공격이었다. 이 공격의 특징은 국가 차원에서 치밀하게 계획하에 실행된 것으로 보인다는 것이다. 당시 사이버 공격으로 감염된 컴퓨터는 2만 대 이상이며, 최대 74개국에서 대략 17만대에 이르는 감염된 컴퓨터가 공격에 활용되었다. 이 사건은 최초로 북한 소행의 사이버 공격이었다는 점에서 우리나라의 사이버안보에 있어서 큰 전환점이 되었다. 북한발 사이버 공격으로부터 대응역량을 강화할 필요성과 사이버 공격에 대비한 사이버 관련부처 간 긴밀한 공조체계의 중요성 등을 인식하고 국정원 주관하에 '국가 사이버 위기 종합대책' 수립·시행되었고, 국방부는 '사이버사령부'를 신설하는 등 범정부 차원의 대책 마련을 위해 노력하게 되었다.

2011년 3월 3일을 기점으로 포털 사이트 및 공공기관의 웹사이트를 대상으로 한 공격징후가 나타났고, 다음 날 청와대·국방부 등 정부기

3) 슬래머 웜(Slammer Worm)은 여러 인터넷 호스트에 DDos로 공격하는 웜으로, 네트워크에 매우 위협적임

관 및 다음, 네이버 등 이용자들이 많은 40여 개의 인터넷 사이트가 분산 서비스 거부 공격(DDoS)에 의해 일시적으로 두 차례 장애가 발생하였다. 이것은 2009년에 발생한 7.7 대란보다 진화된 형태였지만, 다행히 국내 피해 규모는 그리 크지 않았다. 7.7 대란 이후 국가 사이버 안전대책이 마련·시행되면서 한국인터넷진흥원(KISA)를 중심으로 국가정보원, 국방부 등 정부 기관과 민간 백신 개발 사업자들 간의 실시간 정보공유시스템이 만들어진 덕분이었다는 평가를 받았다.

2011년 4월 12일에 발생한 농협 전산망 마비 사건은 우리나라 금융업무 사상 초유의 사태였다. 농협 전산센터 엔지니어에 악성코드가 주입되어 농협 전산망에 있는 자료가 손상되고 그로 인해 총 587대의 서버 중 273대가 파괴되면서 현금인출기 사용은 물론 인터넷뱅킹까지 차단되었다. 이 사건을 계기로 금융기관들이 사이버 관련 전문인력들을 추가로 확보하였고, 특히 국방부는 사이버사령부 역할 확대를 위한 개편 논의도 이루어졌다. 또한, 국가정보원 주관으로 범정부 차원의 일원화된 대응체계를 구축하고 사이버 전문조직 구성과 인력 확보를 위한 사이버안보 마스터플랜을 마련하기로 하였다. 또한, 국가정보원 주도의 국가 사이버 안전 총괄체계를 강화할 필요가 있다는 지적과 함께 국가 사이버보안 수준을 높이기 위한 관련 법체계 정비 및 사이버 기술개발 등을 관장할 수 있는 컨트롤타워 필요성이 제기되었다.

2013년 3월 20일에 안랩 서버 및 다수의 컴퓨터가 악성코드에 감염되어 막대한 피해를 입힌 대형 사이버테러 사건인 3.20 사이버테러가 발생하였다. KBS 및 YTN 등 주요 방송국과 농협·신한은행 등 주요 금융기관의 전산망이 장애를 일으켰고 이로 인해 인터넷뱅킹 거래와 현금인출기 사용 등이 중단되는 사고였다. 특히, 3.20 사이버테러를 일으킨 조직은 북한 정찰총국 소행으로 밝혀졌으며, 2007년부터 우리나라의 군사 관련 기밀정보 탈취를 시도해온 조직으로, 국가안보에 관련된 기밀문서를 탈취해 왔던 것으로 드러났다. 3.20 사이버테러가 발생한 지 얼마 지나지 않아 해커에 의한 사이버테러가 6월 25일에 발생했다. 청와대·통일부, 스포츠 서울 등 언론사 홈페이지를 포함한 여러 기관

의 홈페이지 접속 장애를 일으킨 정보보안 사고로 웹사이트 변조 및 디도스(DDoS), 정당·군과 주한미군 병력의 개인정보 유출 등의 공격이 감행되었다. 6.25 사이버테러는 과거 북한의 사이버 공격 수법과 유사한 것으로 확인되어 정부는 북한의 소행이라고 발표했다. 3.20과 6.25 사이버테러가 있던 2013년부터 사이버위협이 점점 더 지능화되고 다양해지며 고도화되는 등 많은 변화가 있었다.

2014년에 발생한 한국수력원자력 해킹 사건은 한수원 내 악성코드가 퇴직자 명의의 이메일을 통해 전파되었으며, 악성코드를 통해 원자력 발전소 기밀정보 탈취 및 PC 파괴 명령이 실행되었고 한수원 임직원 10,799명의 개인정보(이름, 이메일 주소, 휴대폰 번호 등 총 8가지 항목)가 외부로 유출된 것에서 시작되었다. 유출된 정보가 개인정보뿐만 아니라 설계도 등 중요 파일이 다수 유출된 것으로 드러났다. 수사결과 공격에 사용된 악성코드는 북한 해커조직이 사용하는 악성코드와 동일하다는 결론을 내렸다. 이 한수원 해킹 사건은 국민의 안전과 관련된 국가 인프라시설을 이용하여 국민들의 불안 심리를 자극하고 사회 혼란을 야기한 전형적인 사이버테러의 성격을 가졌다고 볼 수 있다.

국방부 직할부대인 국방통합데이터센터(DIDC: Defense Integrated Data Center)의 계룡대 데이터 서버가 북한으로 추정되는 해킹 세력에게 사이버 공격을 당했다. 2016년 8월 우리 국방망이 해킹을 당해 한·미연합 전면전 작전계획인 작계(作計) 5015와 미군 병력 증원, 일부 전시계획이 담긴 군사기밀 자료 등이 탈취당한 것이다. 북한 추정 해커들이 이 서버를 통로로 삼아 기밀자료를 빼낼 수 있는 악성코드를 군 내부 전용망에 유포한 것이었다. 해킹에 사용된 악성코드도 북한이 그동안 해킹에 사용했던 것과 비슷하고, 침투 경로를 파악할 수 있는 인터넷 주소(IP)도 북한이 주로 이용하는 중국 선양 지역이었다. 이 사건으로 인해 보안이 무엇보다 중요한 軍 내부망이 뚫렸다는 점에서 軍의 안이한 보안의식에 대한 비판이 제기되기도 하였다.

중국의 고고도미사일방어체계(THAAD)가 한반도 내에 전격 배치를

결정한 것에 대한 보복의 일환으로 중국의 해킹 공격이 발생하였다. 2017년 3월 중국 정부는 주한미군의 한반도 사드 배치가 그들의 안보에 악영향을 끼칠 것을 우려하여 사드 배치를 철회해 줄 것을 우리에게 요청했으나 받아들여지지 않자 디도스(DDoS) 공격으로 우리 주요 정부기관과 주요 웹사이트, 민간기업들의 시스템에 침투하여 기능을 마비시켰다. 사드 보복의 일환으로 중국 당국과 관련된 해커조직이 우리 정부를 상대로 사이버 공격을 감행한 것이었다.

2021년 5월과 6월에 국가기관을 대상으로 한 대형 해킹사고가 연속적으로 발생하였다. 원전과 핵연료 원천 기술을 보유한 한국원자력연구원(KAERI)의 경우 약 12일간 해킹에 노출되어 한국원자력연구원 소속 이메일, 휴대폰, 아이디·비밀번호가 포함된 개인정보가 북한 해커에 의해 유출된 것으로 확인되었다. 이러한 최상위 국가보안시설인 한국원자력연구원(KAERI)이 북한 정찰총국 산하 해커 조직인 "킴수키(kimsuky)"로 추정되는 IP를 통해 원자력 기술 일부가 해킹당한 것이다. 이 사건을 계기로 북한은 물론 중국·러시아 등의 사이버 공격에 효과적으로 대응하기 위해 미국과 호주, 일본과 인도가 참여하는 4자 안보협의체 쿼드(Quad)[4]의 사이버 담당 협의체와 쿼드(Quad) 확장을 위한 '쿼드 플러스(Quad Plus)'에 우리나라의 참여 필요성이 제기되기도 하였다. 한국항공우주산업(KAI)의 경우 우리 군 최초 전투기인 KF-21 설계도면 등 다수의 기술 정보들이 해킹되었다. 이뿐만 아니라 한국항공우주산업(KAI)에서 추진 중인 전력사업 관련 대량 정보들이 탈취된 것으로 전해졌다. 과기정통부, 국가정보원에서 조사를 진행하였으며 특정 업체의 VPN(Virtual Private Network)[5] 취약점을 이용한 해킹 시도로 확인되었고 국가정보원은 한국항공우주산업(KAI)의 해킹 주체가 북한 연계조직으로 추정된다고 밝혔다.

4) 4자 안보협의체인 쿼드는 미국과 핵심동맹국인 일본, 인도, 호주를 합한 4개국이 국제 안보 관련 정상 회담
5) VPN(Virtual Private Network)는 암호화된 인터넷 연결로 내부망처럼 이용할 수 있는 가상 사설망

제3절 사이버위협 동향

기술의 발전에 따라 사이버위협도 진화를 거듭하고 있다. 기술의 발달이 공격을 더욱 정교화하게 만들기 때문이다. 최근 사이버 공격 양상이 다양해지고 고도화되면서 사이버 공격에 의한 피해 규모와 파급효과는 더욱 크고 심각해지고 있으며, 사이버 공격의 주체가 국가행위자뿐만 아니라 민간으로 확대되면서 사이버 공격의 횟수와 규모도 증가하고 있다. 사이버위협 유형은 의도가 악의적이고 지능화되고 있다. 단순 호기심으로 시작된 개인 해커에 의한 사이버 공격이 조직화되면서 국가기능 자체의 혼란을 목적으로 하는 악의적이고 고도화된 해킹이 이루어지고 있는 것이다.

사이버 공격은 시간이 흐르면 변화하는 특성이 있기 때문에 정치, 경제, 사회, 국방 등 전 분야로 공격 목표 대상이 확대되고 있는 양상이다. 정치적 갈등 관계에 있는 국가를 대상으로 하는 사이버 불법 해킹, 불법 자금 조달 목적의 가상자산을 활용한 지능범죄, 군사기밀 및 방위산업 등의 국방 관련 기밀정보 탈취, 그리고 금융기관 해킹을 통한 불법 인출 등 전 방위적 사이버 공격으로 인한 피해가 다양하고 심각한 정도에 이르렀다. 이처럼 사이버위협의 수준은 점점 진화되고 정교해지고 있으며 공격의 범위는 확장되어 가고 있으며 이는 국가기능을 마비시키거나 혼란을 일으키고 국가안보를 위협하는 대상으로 발전하고 있다.

최근 글로벌 사이버위협은 크게 증가했고, 특히 그러한 경향은 코로나19 팬데믹이 발생된 이후 더욱 증가되었다. 사이버위협 조사기관인 체크포인트리서치(Check Point Research)에 의하면 2021년은 작년과 비교 시 전 세계의 다양한 기관을 대상으로 한 사이버 공격은 40%가 증가했고, 2020년에서 2021년 사이 사이버 공격 대상으로서 가장 큰 폭으로 증가한 지역은 유럽과 북미였다. 전 세계적으로 일어나고 있는 사이버 공격의 주요 진원지는 러시아와 중국, 북한 그리고 이란으로 미국 등 서방 국가와 외교적 갈등 관계에 있는 국가이다. 특히 북한발

사이버범죄가 크게 증가했는데 이는 국제연합(UN)의 대북제재와 함께 코로나19 팬데믹 기간 동안 더욱 악화된 경제 상황을 북한이 암호화폐 혹은 블록체인 신생 기업을 가장한 사이버 절도를 통해 외화벌이 활동하려는 공격적인 시도를 보였기 때문이다.[6] 2022년 이후에도 사이버 공간에서의 위협은 지속될 것이고 인공지능(AI) 기술 및 빅데이터 기반의 사이버 공격이 적용되면서 공격의 방식이 한층 복잡해지고 파괴력도 상당해 질 것으로 예상해 볼 수 있다.

군사적 측면에서 보면, 이러한 고도로 전개되고 있는 사이버 공격은 물리적 전쟁과 병행한 사이버 전쟁 등과 같이 전장 환경의 변화에 맞는 새로운 형태의 사이버위협 양상으로 발전하고 있다. 군사 전문가나 전문기관은 사이버위협과 이에 대한 대응이 국가 안보와 전쟁의 승패에 직결되는 중대한 사안이라는 것에 인식을 같이하고 있다고 볼 수 있다.

[표 1] 사이버전 관련 주요 기관 및 인사의 예상

구 분	발언내용
UN	제3차 세계대전이 일어난다면 그것은 사이버전이 될 것이다.
영국 국제전략문제연구소	사이버전은 핵전쟁과 비슷할 것이다.
버락 오바마 (前) 미국 대통령	사이버안보 확립 없이는 미국의 21세기 미래를 장담할 수 없다. 국익과 연관이 있는 영역에 대한 사이버 공격은 영토 침공과 같이 대응할 것이다.
리언 파네타 (前) 美 국방부장관	다음 진주만 공격은 사이버 공격이 될 것이다.
포스 라스무센 (前) NATO 사무총장	회원국들은 사이버 공격에 더 적극적 자세를 취해야 한다.
닉 하비 (前) 英 국방부차관	사이버 전력은 미래 전쟁의 결정적 요소로 영국군은 사이버 공간에서의 적대행위에 대비한 공격력을 갖출 것이다.

현대전의 전장은 지상, 해상, 공중 차원뿐만 아니라 우주 및 사이버

6) 외교부, 「2022 국제정세전망」,

공간까지 확장되었다. 현재 주요국들은 신형 첨단 무기체계와 사이버 무기의 결합을 통한 새로운 방식의 안보위협이 점점 다가오고 있다고 인식하고 있으며, 특히 사이버전 무기를 군사적 옵션으로 활용하고자 하는 군사적 측면에서 중요한 위협으로 부상하고 있다. 사이버 무기는 공격 발원지 확인이 거의 확인이 불가하다는 점에서 핵이나 대량살상 무기 등과 마찬가지로 비대칭 전력 수단으로 볼 수 있어 높은 수준의 사이버 공격 능력은 국가안보를 크게 위협하고 있다. 최근 발발된 러시아-우크라이나전쟁은 현대 전면전(a full-fledged war)에서 사이버전이 실제로 어떻게 전개되고 어느 정도의 비중을 차지하는지 예상해 볼 수 있다. 이번 전쟁에서 러시아가 보여준 공격의 특징 중 하나는 군사작전과 사이버전이 결합된 '하이브리드(hybrid)[7]' 작전을 펼쳤다는 것이다. 러시아는 우크라이나를 침공하기 2개월 전부터 우크라이나에 대한 다양한 유형의 대규모 사이버 공격을 감행했다. 러시아의 이번 공격형태는 군사공격과 사이버 공격이 협동하는 형태로 반복적으로 이루어졌으며, 이제 사이버전이 전통적인 군사수단과 완전히 결합되어 조직적으로 움직이는 전쟁의 새로운 수단으로 자리매김한 것으로 보인다.

국제사회는 이러한 사이버위협에 대한 인식이 고조되면서 국제협력을 통한 다양한 활동을 전개해 가고는 있으나, 사이버안보에 대한 개념조차도 각국이나 국제기구 간의 견해 차이로 인해 아직까지 국제적으로 합의된 정의가 정립되지 못하고 있다. 또한, 사이버 행위에 따른 불필요한 오해로 인한 갈등과 분쟁을 방지하고 사이버전 확전 가능성을 최소화할 수 있도록 하는 군사적 신뢰 구축을 통한 평화 체계구축에 관한 합의가 제대로 도출이 되지 않은 실정이다. 이처럼 국제사회가 사이버안보에 관한 국제규범이나 군사적 신뢰 구축에 대한 합의가 제대로 이루어지지 못하면서 고도화되고 국경을 초월하는 형태를 지니는 사이버 공격에 효과적으로 대응하기 위한 국제협력은 매우 어려운 상황에 직면해 있다고 볼 수 있다.

7) 하이브리드 전쟁(hybrid warfare)은 기존의 정규전과 비정규전 같은 재래식 전쟁을 테러 행위, 가짜 뉴스, 외국 정치 개입 그리고 사이버 공격까지 포함하는 다양한 형태의 작전들과 혼합된 군사전략

Ⅲ. 국제사회의 사이버 협력 관련 기구

사이버 공간은 한 나라에 의해서 규칙이 만들어지고 질서가 유지될 수 있는 공간이 아니다. 앞에서 살펴보았듯이, 현재 사이버 공간에서는 국가 간 사이버테러, 개별 해커집단에 의한 사이버 공격 그리고 국가 차원의 사이버 공격이 빈발하고 있다. 국제사회는 이러한 직면한 문제들을 국가 개별차원에서 대응이 불가함을 인지하고 공동의 노력을 통해 해결하기 위하여 사이버범죄 및 테러의 예방과 대응, 국가 간 사이버안보 문제해결을 위한 상호 신뢰성 제고, 사이버안보 국제규범의 확립 등과 같은 이슈에 대한 협력체계를 구축하고 있다.

국제사회는 증가하는 사이버위협에 대응하기 위해 최근 20여 년간 국제연합(UN)을 중심으로 하는 국제기구와 지역 차원의 다자기구에서 국제규범 마련 및 대응전략을 제시하고 있다. 국제사회는 국제연합(UN), 북대서양조약기구(NATO), 유럽안보협력기구(OSCE), 아세안지역안보포럼(ARF), 동아시아정상회의(EAS), 아시아유럽정상회의(ASEM), 아시아태평양경제협력체(APEC), G20 정상회의 등 국제기구와 지역 차원의 안보기구 및 협의체에서 사이버안보를 위한 다양한 논의를 추진하고 있다. 그럼에도 불구하고 이러한 국제기구 및 다자안보 협의기구 간에 뚜렷한 입장 차이가 존재하고 있으며 이것이 사이버 국제협력의 가장 큰 장애 요소가 되고 있다.

사이버 공간상의 위협은 하나의 국가 차원의 대응으로는 한계가 있다. 다중이해관계자(Multi-stake holder)가 참여하는 개방적이고 포괄적인 국제협력을 바탕으로 한 거버넌스[8]을 구축하고 국제·지역적 차원에서 국제규범 논의가 이루어지고 있는데 아직까지는 가시적인 성과가 나타나지 않고 있다고 볼 수 있다. 이는 사이버 분야가 가지는 익명성·개방성·자율성, 행위자의 의도, 대응조치 등 여러 가지 요소가 복잡

8) 정책 결정에 있어 정부 주도의 통제와 관리에서 벗어나 다양한 이해당사자가 주체적인 행위자로 협의와 합의 과정을 통하여 정책을 결정하고 집행해 나가는 사회적 통치 시스템(Jon Pierre, B.Guy Peters)

한 관계로 얽혀 있고 국가 간의 입장이 지속적으로 대립되고 있는 상황 때문이다.

제1절 국제기구를 통한 사이버 협력

사이버안보와 연관된 국제사회의 노력은 정보통신기술(ICT) 발전에 따른 사이버위협이 다양화되기 시작한 2000년대 이후부터 본격적으로 이루어져 왔다. 국제사회 내 사이버안보 협력은 국제연합(Untied Nations, UN) 중심으로 진행되고 있는데 국제연합(UN)은 사이버 공간상의 이슈들이 다양하게 나타나면서 UN 총회뿐만 아니라 여러 산하 조직에서 의제 논의를 추진하고 있으며 또한 새로운 조직을 신설하여 논의를 계속 진전시키고 있다. 국제연합(UN)이 사이버 공간에 나타난 이슈에 대한 논의가 중요한 이유는 국제연합(UN)이 평화와 인권, 안전과 환경 등의 국제규범 등을 가장 우선으로 협의를 추진하며, 논의된 결과는 회원국뿐만 아니라 전 세계적으로 국가정책에 반영되어 실효성을 가진다는 점에서 국제연합(UN)에서 추진되는 사이버안보에 대한 논의는 국제규범으로써의 의미를 가진다고 할 수 있다.

러시아가 1998년 처음으로 국제연합(UN) 총회에 의정서를 제출하면서 UN 내 사이버안보 논의는 급물살을 타기 시작하였고 사이버안보 노력이 UN을 중심으로 다양하게 실행되고 있다. 특히 UN 차원뿐만 아니라 산하 기구 중 국제전기통신연합(ITU)과 국제사이버안보다자간협력기구(IMPACT) 등에서 사이버안보 분야에 대한 대응과 협력, 사이버보안 관련 기술연구와 정책 자문 등의 역할을 수행하고 있다. 하지만, 국제연합(UN) 차원에서 사이버안보 의제를 정기적으로 설정하였음에도 불구하고 사이버안보에 대한 선진국들의 적극적이지 못한 태도와 개도국들의 무관심이 국제규범을 마련하는 데 있어서 심도 있는 논의가 이루어지지 못하고 있는 실정이다.(유준구, 2018) 다시 말하면, UN에 가입된 국가 간의 명확한 입장의 차이로 인해 국제규범 결의가 쉽지는 않은 상황이다.

미국·EU를 포함한 서방 국가들은 UN에서의 논의보다는 서방 국가 위주의 논의를 선호하였고, 사이버 공간의 개방성과 자율성 보장을 통한 사이버 경제의 지속적인 성장을 추구하며 현재의 사이버 국제협약인 사이버범죄협약(Convention on Cybercrime)[9] 이행 강화와 다양한 이해관계자(Multi-stake holder)가 참여하는 사이버 거버넌스 구축을 주장하고 있는 반면에, BRICS·제3세계 국가 등 비서방국 및 개발도상국들은 사이버 공간에 대한 국가 중심의 규제 필요성과 국제연합(UN) 차원의 논의를 통해 우위 확보를 추구하고 새로운 국제협약을 수립하자고 주장하고 있다.

[표 2] 사이버 관련 이슈에 대한 각국의 입장차

구 분	서방국가(미국, 영국 등)	비서방국가(중국, 러시아 등)
사이버 공간에 대한 입장	중립적인 공간	국가주권이 미치는 공간
규제(개입)	민간 중심 (국가 규제 및 개입 불필요)	국가 중심 (국가 규제 및 개입 필요)
국제규범	ICT 활용과 개발을 저해할 수 있어 국제규범은 불필요 (기존 규범 적용 가능)	ICT 발전에 따라 새로운 국제규범 마련 필요

1. UN GGE(정부 전문가 그룹) / OWEG(개방형 실무 그룹)

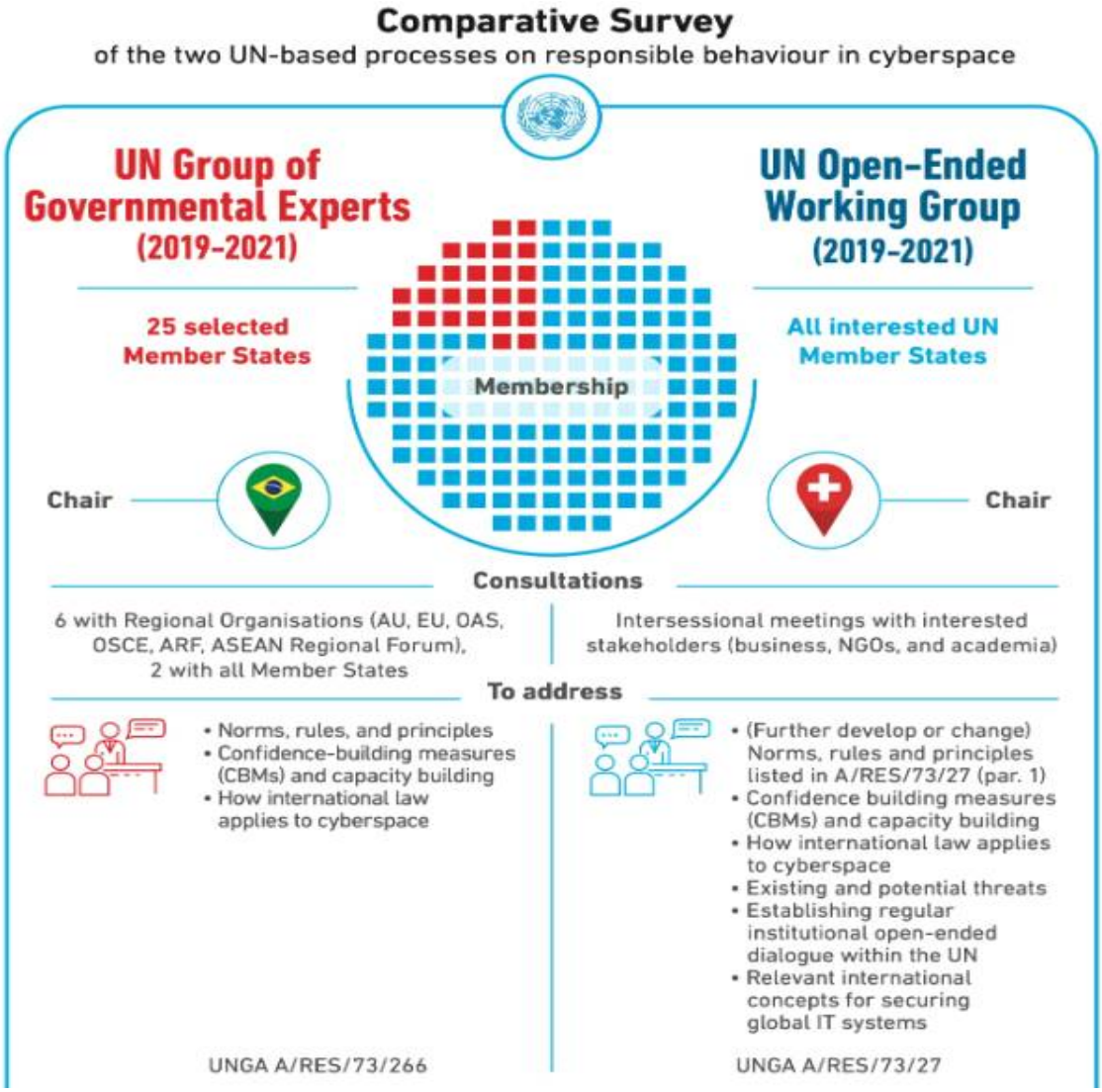
UN은 사이버안보 관련 국가 간의 사이버위협, 국제규범, 그리고 사이버 공간의 신뢰 구축 조치 마련 및 이행, 역량 강화 활동 등을 논의하기 위해 공평한 지리적 배분을 특별히 고려하여 UN의 제한된 국가들만이 참여하는 UN 차원의 실질적인 사이버안보 협의체인 UN GGE(Group of Governmental Experts, 정부전문가그룹)[10]을 설립하여 논의를 진행해 오고 있다. GEE는 미국을 포함한 UN 회원국 중 25개

9) 사이버범죄협약(일명 부다페스트 조약)은 인터넷을 활용하는 범죄행위 규정하고 처벌토록 하는 최초의 국제조약으로 51개국이 동의하였으며, 수사절차 및 공조체제도 규정함

10) 2004년부터 국제안보의 맥락에서 정보 및 통신 분야의 발전에 관한 GGE를 구성·운영. UN총회 승인을 위해 GGE 권장 사항을 사무총장에게 합의 보고서를 제공

국으로 구성되어 있으며, '04년 UN 제1위원회 산하 GGE가 출범된 이후 2022년 현재까지 총 6차례 회의가 구성되었다. 이를 통해 사이버 공간에서의 주권 규범성, 사이버 공격에 대한 물리적 공격에 버금가는 자위권 차원의 무력 사용(use of force)의 기준 설정, 국가가 아닌 개인 행위자의 행위에 대한 관할 국가의 책임 등에 대한 국제규범을 마련하고 있다. GGE 구도는 기본적으로 미·서방과 중·러 진영의 대립 기조를 반영하고 있으며, 일부 국가들이 특정 문제에 대해서 중도적인 입장을 보이고 있다. 특히 개발도상국들은 미국 등 서구 국가들이 비대칭적 사이버 도전에 맞서 무제한적인 자위권을 주장함으로써 군사적 패권을 유지하려 한다는 두려움에 점점 목소리를 높이고 있는 상황이다.

UN OEWG(Open-Ended Working Group, 개방형실무그룹)는 사이버 위협 및 국제규범에 있어서 두 진영 간 첨예한 대립이 지속되고, GGE가 2017년 최종 회의에서 보고서 채택의 실패함에 따라 GGE 실효성에 대한 의구심이 제기되었다. 이에 새로운 협의체 창설 필요성이 UN 내에서 논의되면서 2018년 미국과 러시아 주도로 채택된 UN총회 결의안을 통해 OEWG가 신설되었다. OEWG에서는 제한된 국가로 구성된 GEE와는 달리 UN 회원국뿐만 아니라 민간기업, 비정부기구(NGO), 학계 등 모든 이해관계자의 참여를 도모하여 개방성, 투명성, 포용성을 제고하고자 하였다. 향후 OEWG의 위상과 역할에 따라 UN 내 사이버 안보 논의가 OEWG 단일 트랙으로 진행될지 혹은 현재와 같은 두 개의 트랙(GGE/OEWG)으로 논의될지 결정될 것으로 보인다.(유준구, 2021)



<그림 1> UN GEE와 OEWG 조직 구성 및 중점분야

2021년 10월 미국 중심의 GGE와 러시아 중심의 OEWG가 제출한 보고서 제안이 모두 포함된 '공동 사이버안보 이니셔티브(Joint Cybersecurity Initiative)'가 UN에 제출되었다 것은 매우 큰 의미를 가진다. 이는 GCE와 OEWG 협의체가 경쟁적인 관계이지만 사이버 공간에서의 제반 문제를 해결하기 위한 공동선언문이 두 협의체의 제안을 모두 담은 것 자체에서 향후 국제사회의 사이버위협과 관련된 국제규범 형성 논의가 긍정적인 여건 속에서 진행될 가능성이 클 것으로 전망할 수 있다. 앞으로도 사이버안보의 국제규범은 강대국 간의 전략적

이익 편차가 줄어드는 방향으로 합의가 이루어질 것이며, 강대국 간의 상대적 이익이 균형점을 찾을 때까지 더 많은 논의와 타협이 요구될 것으로 보인다.

2. 국제전기통신연합(ITU)

국제전기통신연합(International Telecommunication Union, ITU)은 국제주파수, 위성 궤도, 기술표준 등 전기통신과 관련한 기술 개발과 합리적 이용을 위한 국제협력의 증진, 회원국 간 기술 보급 및 확대 등 전기통신 사용 보장을 위해 창설된 국제연합(UN)의 산하의 정보통신 부문 전문기구이다. 1865년 설립된 국제전신연맹(International Telegraph Union)을 전신으로 148년 역사의 가진 세계에서 가장 오래된 국제기구 중 하나이다. ITU 본부는 는 스위스 제네바에 있으며, 회원국은 193개국, 750여 개의 산업·연구·학계 민간회원이 가입하고 있다.

<그림 2> 국제전기통신연합(ITU) 조직

국제전기통신연합(ITU)은 정보사회정상회의(World Summit on the Information Society, WSIS)[11]와 전권회의(ITU Plenipotentiary Conference, IPC)[12]를 통해 사이버안보 이슈들을 논의하고 있다. 2003년 제네바에서 정보사회세계정상회의(WSIS)를 처음으로 개최된 이후 사이버안보와 관련된 활동을 추진하기 시작했으며, 현재까지 활동 범위를 사이버 공간으로 확대하고 있다. 특히, 정보사회세계정상회의(WSIS)에서 정보기술 발전과 사용자들 간의 신뢰 구축을 위해서는 신뢰할 수 있는 정보보안 프레임워크(Framework)[13] 강화가 기본적인 요건이라고 지적하며, 모든 이해 당사자가 협력하는 글로벌 사이버안보 문화의 필요성을 강조하며 국제협력을 촉구하고 있다.

3. 국제사이버안보다자간협력기구(IMPACT)

국제연합(UN)은 '08년 사이버안보 국제협력 강화를 위한 추진기구인 국제사이버안보다자간협력기구(International Multilateral Partnership Against Cyber Threats, IMPACT)을 설립하고, 사이버보안 관련 기술 연구와 정책 자문 등의 역할을 수행하고 있다. 국제사이버안보다자간협력기구(IMPACT)는 국가 및 공공·민간 협력까지 범위를 확대해 포괄적이고 개방적인 사이버위협에 대한 대응방안 모색을 추진하고 있으며, 국제연합 가맹국 대다수가 국제사이버안보다자간협력기구(IMPACT)와 사이버 협력 관계를 맺고 있는데 이중 많은 국가가 사이버보안 지원 서비스를 제공받는 등 국제사회에서 상당한 영향력을 발휘하고 있다.

국제사이버안보다자간협력기구(IMPACT)는 말레이시아 사이버자야(Cyberjaya)에 본사를 두고 4개의 주무부처를 설치하여 운영하고 있다.

11) 정보사회세계정상회의(WSIS)는 UN 회원국들이 정보통신에 관련된 것들을 의논하는 회의
12) ITU 전권회의는 4년마다 개최되는 ITU 최고 의사결정회의로 협약, 규칙, 결의 및 권고 등의 제·개정 임무 수행
13) 정보보안 프레임워크는 허가되지 않은 자로부터 정보를 보호하는 기술적이고 관리적인 행위

<표 3> 국제사이버안보다자간협력기구 주무부처별 역할

주무부처	역할
글로벌 대응 센터 (Global Response Centre)	전세계 다양한 사이버위협 관련 데이터를 수집 및 분석하는 역할 수행
보안 보장 및 연구 센터 (Centre for Security Assurance & Research)	각국 정부의 안보 역량 개선을 촉구하는 효과를 도모
정책 및 국제협력센터 (Centre for Policy & International Cooperation)	각국 정부가 효과적으로 사이버위협에 대응할 수 있도록 정책적 방향성을 제시
훈련 및 기술개발센터 (Centre for Training & Skills Development)	사이버안보 인력 양성과 관련 기술 연구 수행

특히 국제사이버안보다자간협력기구(IMPACT)는 국제전기통신연합(ITU)과 '11년부터 긴밀한 협력 관계를 맺고 전 세계의 사이버안보 능력 확대를 위한 공동대응 시스템을 구축하고 있다. 양 기관의 협력은 '08년 국제전기통신연합(ITU)이 글로벌 사이버안보 의제를 수립할 무렵에 본부를 국제사이버안보다자간협력기구(IMPACT) 산하에 두면서부터 시작하였고 이후 '11년에 양 기관 간 양해각서(MOU) 체결이 이뤄지면서 협조체계를 갖추고는 있으나, 미국·러시아 등의 중요한 국가들이 참여하지 않아 사이버안보를 위한 국제협력 기구로서의 역할은 크지 않다.

4. 세계사이버스페이스총회(GCGS)

세계사이버스페이스총회(Global Conference on Cyberspace, GCGS)는 경제·사회적 혜택, 국제안보, 사이버보안 및 범죄 등 사이버 관련 이슈 등을 포괄적으로 논의하기 위한 각국 정부 및 지역·국제기구 고위 인사, 민간대표가 참석하는 고위급 국제포럼으로 2011년 런던에서 1차 회의를 개최하였다. 이후 2012년 헝가리 부다페스트, 2013년 서울, 2015년 네덜란드, 2017년 인도에서 5차 회의가 개최된 바 있다. 세계사이버스페이스총회(GCCS)는 러시아와 중국을 중심으로 하는 '정보보안을 위한 행동 규약(Code of Conduct for Information Society)을 UN

총회에 제출하려는 움직임을 견제하기 위한 미국·영국 등 서방 국가들의 대응적인 성격의 국제 회의체이다. GCGS는 인터넷 사용에 대한 각 국가의 주권을 보장하고 정보기술의 군사적 이용을 금지하는 새로운 국제규범보다는 기존 군사적 충돌에 대한 국제규범을 사이버 공간에 적용하고 국가 중심적인 인터넷 정책이 아닌 기업과 시민사회 등 다양한 이해관계자 참여에 기반한 인터넷 정책 형성을 지지하고 있다.

세계사이버스페이스총회(GCGS)는 사이버 국제규범을 마련하는 회의체는 아니나, UN GEE에서 주요규범으로 논의되는 정보공유와 국제공조 등에 대해서는 다양한 이해관계자들이 참여하여 의견을 교환하는 장이 되었다. 2013년 3차 세계사이버스페이스총회(GCCS)를 서울에서 개최하여 기존에 논의된 사이버테러와 범죄에 국제사회가 공동으로 대처하기 위한 국제규범(서울원칙)을 채택하여 문서화하였고, 2015년 헤이그 4차 회의와 2017년 뉴델리 5차 회의는 정부 외에 기업과 시민사회, 학계 등 다양한 이해관계자가 참여하여 의견을 교환하는 회의체가 되었다. 하지만, 국제연합(UN) 차원의 논의가 효율성이 떨어진다는 취지에서 그 대안의 성격으로 출발한 사이버스페이스총회(GCGS)는 현재 차기 총회 개최를 희망하는 국가가 나오지 않는 등 사이버스페이스총회(GCGS)의 모멘텀(momentum) 상실이 우려되고 있는 상황이다.

제2절 지역 차원의 사이버 협력

국제기구 차원의 협력 외에도 각 지역별 기구들을 통해 사이버안보를 위한 국제협력 역시 이루어지고 있다. 유럽연합(European Union, EU)과 동남아국가연합(Association of Southeast Asian Nations, ASEAN) 등 지역의 평화와 안정을 추구하는 지역 연합기구와 북대서양 지역 안보를 위한 북미와 유럽 등 서방 국가들의 군사동맹체인 북대서양조약기구(North Atlantic Treaty Organization, NATO), 유럽과 중앙아시아, 북아메리카 등 57개 국가가 가입되어 있는 유럽안보협력기구(Organization for Security and Cooperation in Europe, OSCE),

중국·러시아 등 9개국이 모여 군사·안보·정치 등 다방면에서 협력하는 집단안보 기구인 상하이협력기구(SCO), 인도네시아·태국·말레이시아·필리핀 등 동남아시아 지역 중심의 지역 협력기구인 아세안지역안보포럼(ASEAN Regional Forum, ARF) 등을 중심으로 지역 차원의 사이버 협력이 활발하게 이루어지고 있다.

1. 북대서양조약기구(NATO)

유럽지역의 북대서양조약기구(NATO)의 사이버는 주로 사이버 공격에 대한 방어에 중점을 두는 범국가적 방어시스템 구축에 집중하고 있으며, 동맹국 및 파트너국가의 정보공유, 기술개발, 사이버훈련 등을 적극적으로 추진하고 있다. 사이버 방어 교육 및 훈련뿐만 아니라 북대서양조약기구 회원국들의 사이버안보 의식을 고취시키고, '사이버 연합훈련(Cyber Coalition Exercise)'과 같은 합동훈련을 연례 정기적으로 수행하면서 회원국 간 공동대응 시스템 강화를 도모하고 있다.

북대서양조약기구(NATO) 사이버 방어 정책이 2008년에 최초로 수립되었으며, 이후 지속적으로 정책 및 실행계획 수정·보완하고 연합군 방위계획과의 연계 등을 거치며 점점 실효성을 갖추게 되었다. 사이버 방어 정책의 가장 중요한 목표는 NATO가 운영 중인 정보시스템을 보호하는 것이나, 이와 동시에 회원국 각국의 정보시스템 보호도 NATO의 중요한 역할에 해당하는 만큼 회원국 방어시스템 구축을 지원하는 것도 NATO의 핵심임무로 볼 수 있다. 또한, 국제연합(UN) 및 유럽연합(EU)과도 사이버 방어 공동대응을 위한 긴밀한 협력 관계를 추진 중이며, NATO와 산업계가 사이버 영역에서 공동의 위험에 직면함을 인식하에 산업 사이버 파트너십(NATO Industry Cyber Partnership)을 통해 사이버위협 및 정보보안 모범 사례뿐만 아니라 사이버위협 지표 및 완화 조치에 대한 정보를 공유하는 등 민간 부문의 사이버 동향도 계속 파악하고 있다.

NATO는 회원국 간 정보교류 활성화와 사이버위협 대응역량 강화를

목표로 사이버방위협력센터(Cooperative Cyber Defence, Centre of Excellence, CCDCOE)를 중심으로 사이버안보 관련 논의가 진행되고 있다. 2007년 에스토니아 대상으로 한 러시아의 사이버 공격이 발생한 이후 NATO는 사이버 대응의 필요성을 인식하고, 2008년 에스토니아의 수도인 탈린에 사이버방위협력센터(CCDCOE)를 설립했다. 사이버방위협력센터(CCDCOE)는 NATO의 사이버안보 관련 정책 개발 및 기술 연구를 수행하고 있으며 컨설팅 및 교육·훈련 등의 역할을 담당하고 있다. 2013년에는 사이버 전쟁에서 적용되는 국제법을 담은 '탈린매뉴얼'을 발표한 바 있는데 이는 사이버 공간에서의 국제법 적용 방안을 모색함으로써 각국의 사이버안보 정책과 전략 수립의 기초가 될 수 있다는 점에서 많은 시사점을 제공했다(김규동, 2018). 또한, 사이버보안 전문가가 실시간 공격에서 국가 IT 시스템과 중요 인프라를 방어하는 기술을 향상시키기 위해 매년 '락트쉴즈(Locked Shields)' 훈련을 실시하고 있다.

2019.12월 NATO 29개 회원국 정상이 모여 커지는 중국의 도전에 대응할 필요성을 인식하고 공동방위 원칙을 재확인하는 공동선언문을 채택했다. 여기서 5세대 이동통신(5G)을 비롯한 사이버보안 보장 필요성에 대해서도 언급하였는데 이는 NATO와 서방 국가에서 차세대 이동통신 네트워크 구축에 있어 중국 통신장비 업체인 화웨이의 역할에 대한 우려를 공유하고 NATO 회원국 간의 결속과 안보 원칙을 명시한 '워싱턴 조약(NATO 조약)'에 대한 약속("어느 체결국이든 공격을 받을 경우 그것을 전체 체결국에 대한 공격으로 간주한다")을 지속할 것을 촉구한 바 있다[14]. 우리나라는 CCDCOE의 사이버 공격과 방어 기술, 사이버안보 전략 및 정책 등을 공유하기 위해 국정원 주도하에 2022년 5월 非NATO 국가로는 유일하게 정회원국이 되었으며[15], CCDCOE 회원국들과 사이버 공격 및 방어훈련, 전략 및 정책연구 등 글로벌 사이버위협에 공동대응하고 있다.

14) 연합뉴스, 'NATO 공동선언 중국의 도전 명시...균열 속 집단방위 재확인', 2019.12.5.
15) 연합뉴스, '국정원, 한국 NATO 사이버방위센터 정회원 가입식 개최', 2022.5.9.

2. 유럽안보협력기구(OSCE)

유럽안보협력기구(Organization for Security and Co-operation in Europe, OSCE)는 회원국 간의 지역 안보협력을 위해 유럽과 북아메리카, 중앙아시아 등 57개 국가가 가입되어 있는 세계에서 가장 규모가 큰 정부 간 협력기구이다. 1975년 8월 헬싱키 정상회의 협정에 의해 유럽안보협력회의가 창설되었으며, 1995년 1월에 지금과 같은 이름으로 변경되었다. OSCE의 최고 의사결정 기관은 회원국 정상회담으로 중요한 사안에 대한 의사결정을 위해 필요시 개최되며 상시적인 의사결정은 매년 말 연례적으로 개최되는 장관급 회담에서 이루어진다.

OSCE는 회원국 간 사이버위협 요소 제거 및 안정적인 신뢰 관계를 증진하기 위한 사이버안보 분야에서의 신뢰 구축 조치(CBMs : Confidence Building Measures)[16]에 중점을 두고 있으며 CBMs 확보를 위한 작업반을 구축하여 구체적인 방안을 도출하기 위해 적극적으로 노력하고 있다. 논의되고 있는 사이버 CBMs 내용을 간략히 보면, △사이버안보 대응 관련 정보 공개와 인사교류를 통한 상호이해를 제고하고 △사이버위협에 공동대처하기 위한 연락창구 설치 및 공동 사이버 연습 등을 토해 사이버안보 역량을 강화하며 △국가 간 상호합의를 통해 민간 핵심기반시설 사이버 공격 금지 등 사이버 공간을 불안정하게 만드는 활동을 제한하는 조치들을 포괄하고 있다.(이상현, 2022)

우리나라는 1994년부터 OSCE의 협력동반자국으로 참여하여, OSCE-한국회의, OSCE-아시아협력동반자국 회의 등을 통해 유럽의 안보협력 경험을 공유하고 사이버안보 정책에 대한 OSCE 회원국의 이해를 제고하는 등의 OECE와의 협력관계를 유지하고 있다.

3. 상하이협력기구(SCO)

16) 사이버 공간에 적용 가능한 군사적 신뢰 구축 조치(CBMs)는 군사적으로 깊은 신뢰 관계가 형성되지 않은 국가들 간에 사이버 공간에서의 오판과 오해로 인한 위험 발생 가능성을 최소화할 수 있도록 국가 간 무력분쟁을 예방하는 도구

2001년 7월에 설립된 지역협력기구인 상하이협력기구(Shanghai Cooperation Organization, SCO)는 중국, 러시아 등 5개국의 지역 안보 협력을 위해 창설된 국제기구로서 2022년 현재 9개 회원국(옵저버 포함 총 21개 회원국)[17]으로 성장했다. 당시 설립 목적은 접경 국가 간의 국경선 획정 등 역내 안정과 군비 축소를 위함이었으나, 정상회담이 거듭되면서 군사·안보·정치 등 여러 방면에서 지역협력을 확대하는 기구로 변화되었다. 2000년대 중반부터 지속적으로 사이버안보를 위한 지역협력을 강조해오고 있는 SCO는 집단 안보협력 기구 성격으로 회원국 간의 정치, 경제 및 신규 안보(사이버안보 포함) 등 다양한 이슈에 대한 협력에 중점을 두고 있다. 특히 사이버 협력은 2006년부터 정상회담 및 전문가그룹(국제정보보안 전문가그룹, 지역 대테러조직 산하 전문가그룹)을 통해 SCO 정상회담 합의문과 사이버 관련 협정서에 명시한 사이버 공간 이용에 관한 규범제정을 추진하고 있으며, 회원국 간의 비정기적인 사이버 공동훈련, 대터러 및 범죄 대응훈련도 시행하고 있다. 실제로 SCO는 미국의 주도로 창설된 NATO에 대응하기 위한 안보협의체 성격의 군사협력체로 볼 수 있다.

SCO는 사이버 공간이 국가가 관할해야 할 대상이며, 기존의 국가주권 및 타국의 내정불가침 원칙을 존중하면서 정보통신 기술의 오용을 방지하고 정보통신 기술을 이용한 테러리즘, 분리주의 및 폭력적 극단주의 전파·확산 방지를 위한 국제협력을 강조하고 있다. SCO는 미국이나 유럽국가들의 입장과는 달리 개별 국가들이 자국 내 네트워크를 감시하거나 통제할 수 있다는 국가주권 원칙을 강조하는 중국과 러시아 등의 입장을 잘 보여주고 있기 때문에 사이버안보의 국제규범 형성과정에서 상당한 주목을 받고 있다. 2021년 11월 SCO 회의에서 회원국 간의 정책조율과 안보협력, 방해받지 않는 무역, 금융통합과 인적교류 강화를 통해 안전하고 깨끗한 세계를 만들기 위해 노력할 것임을 시사하면서 향후 국제 사이버안보 관계에서 SCO가 서방진영과의

17) 상하이협력기구 회원국 및 초청국가(기구)
(정회원 9개국) 중국, 러시아, 카자흐스탄, 우즈베키스탄, 키르기스스탄, 타지키스탄, 인도, 파키스탄. 이란
(옵서버 3개국) 아프가니스탄과 몽골, 벨라루스
(대화 동반자 9개국) 스리랑카, 터키, 아르메니아, 캄보디아, 네팔, 이집트, 카다르, 사우디아라비아, 아제르바이잔
(초청국가 및 기구) 투르크메니스탄, 독립 국가 연합과 동남아시아 국가 연합, UN

힘의 균형에서 우위를 선점하기 위해 어떤 새로운 형태의 국제관계를 구축할지 지켜볼 필요가 있다.

4. 동남아국가연합(ASEAN)

동남아국가연합(ASEAN)은 1960년대 중반 국제전으로 확산하는 베트남전과 인도차이나 공산주의 확산에 대한 공동대응을 위해 인도네시아·태국·말레이시아·필리핀·싱가포르 등 5개국이 창설한 지역 협력기구이다. 2022년 기준 회원국(대화 상대국 포함)은 25개국으로 증가했으며, 싱가포르와 인도네시아는 미국과 긴밀한 협력 관계를 유지하고 있는 반면에, 캄보디아와 라오스는 전통적으로 중국에 우호적인 국가로 볼 수 있으며 베트남은 1990년대 미국과 수교하고 러시아와도 협력하는 미국과 비서구 국가 간의 균형된 협력 관계를 유지하고 있다. 이같이 복잡한 ASEAN 국가들의 대외관계는 사이버 공간에도 유사하게 나타난다.

사이버안보는 코로나19 팬데믹 대유행으로 인한 혼란 이후 ASEAN 지역 지도자들의 우선순위 중 하나가 되었는데 ASEAN은 회원국 간 협력의 장으로서 사이버안보를 실현하는 데 중요한 역할을 하고 있다. ASEAN 회원국은 사이버 공간의 안보를 유지하고 개인정보를 보호하는 동시에 혁신과 경제를 향상시키는 인터넷 플랫폼의 개방성을 보장하기 위한 사이버안보 정책 및 법률을 구현하는 등 사이버안보 개선을 위한 구체적인 전략을 추진 중이다.[18] ASEAN의 사이버 협력은 △ASEAN 자체의 협력(정상회담, 정보통신 장관회의, 아세안지역안보포럼), △ASEAN-싱가포르 사이버 협력, △ASEAN-일본·중국·EU와의 협력으로 구분할 수 있다.

첫째, ASEAN 정상회담은 사이버 공간을 위협이자 경제성장의 기회로 인식하면서 회원국들의 사이버안보 정책과 역량 개발, 국제협력체계 구성 등이 포함된 사이버안보 협력 선언문을 채택한 바 있으며,

18) Khotimah Estiyovionita, 「ASEANs role in cybersecurity maintenance and security strategy through an international security approach」, 2022

ASEAM 정보통신장관회의에서는 CERT 설치 및 운영, 위협정보교류 합의, 사이버안보 협력 전략 및 추진 방향 등이 논의되었다. ASEAN의 정치, 안보 문제에 대한 협의와 아시아 태평양지역의 신뢰 구축을 목적으로 둔 회의체인 아세안지역안보포럼(ARF)이 있는데 1994년 5월 창설된 후 현재 아세안 회원국 10개국과 한국, 미국, 일본 등 대화 상대국 16개국과 국제기구(유럽연합) 등 총 27개국으로 구성되어 있다. 아세안지역안보포럼(ARF)은 사이버안보 이슈를 포괄적으로 다루는 대표적인 지역 다자안보 협의체로 사이버안보를 중점협력 분야 중 하나로 논의하고 있다. 아세안지역안보포럼(ARF)은 사이버 공격 및 테러리즘에 대한 대응, 사이버 공간 신뢰 구축조치(CBMs) 등과 관련한 세미나·워크숍을 통해 사이버안보 논의를 적극적으로 진행하고 있으나, 대체로 원론적인 입장 표명에 그치고 있으며 사이버공간에 적용되는 국제법 등 규범과 사이버 공간 신뢰 구축조치(CBMs)에 대해서는 회원국 간의 이견 차이로 미국 등 서방국과 중국·러시아 간에 발생하고 있는 대립양상이 재현되는 문제점을 안고 있다. ARF에서 논의되고 있는 CBMs의 내용을 보면, △국가 정책·전략·규정에 관한 정보공유 △핵심 기반시설 역량 강화를 위한 협력 프레임워크 실시 △사이버침해사고에 대한 인식제고 및 정보공유 △국가 사이버안보 전략 및 사이버범죄 대응을 위한 워크샵 실시 등의 이행 방안을 마련하고 있다.

둘째, 2018년 설립된 ASEAN-싱가포르 사이버안보 전문센터는 ASEAN의 사이버역량 프로그램을 통해 사이버안보 국제규범과 국내법규 및 정책을 수립하고 사이버 방어 대응 및 관련 훈련을 통해 대응 경험을 공유한다.

셋째, ASEAN은 회원국 간의 협력뿐만 아니라 비회원국가와 국제기구와도 긴밀하게 협력 관계를 유지하면서 미국, 러시아, 유럽연합(EU), 일본 그리고 중국과 사이버역량 및 협력 채널 구축을 강화하고 있다. 미국과는 사이버안보 및 사이버범죄 대응에 관해 긴밀한 협력을 추진하고 있으며, 일본과는 ASEAN-일본 사이버안보 역량강화센터를 설립하였고 중국과는 사이버 공간 포럼 개최 및 정보공유를 실시하고 있다.

국방 분야에서는 2006년 ASEAN 10개국으로 아세안국방장관회의(ASEAN Defence Ministers' Meeting)가 출범하였고, 2010년 8개국[19]이 추가 참여하는 아세안확대국방장관회의(ADMM-Plus)가 개최되었다. 우리 국방부는 아세안확대국방장관회의(ADMM-Plus)에 참석하여 각국 장관들과 공동의 안보위협을 극복하기 위한 협력의 필요성을 공유하고 역내 평화와 안정을 위해 노력해 나가기로 약속한 바 있다. 특히 2017년부터 사이버분과회의를 시작하여 2022년 7월 8차 회의까지 진행되었는데 이 회의를 통해 사이버 전략 및 정책 공유, 국제법적 이슈 논의, 최신 사이버위협 공동대응 절차 마련, 사이버훈련 실시 등 회원국 간의 사이버안보 강화와 신뢰 구축 증진을 위한 구체적인 협력방안을 논의하고 있다.

제3절 양자 차원 및 기타 사이버 협력

국제기구, 지역 차원의 다자안보 노력 외에도 개별 국가 간 양자 차원의 사이버 협력, 민간 차원의 사이버 협력 역시 이루어지고 있다. 또한, 국제회의 및 콘퍼런스 등을 통해 정책 및 전략, 기술 등 사이버안보 전 분야에 대한 다양한 논의도 이루어지고 있다. 개별 국가 간 양자 차원의 노력은 사이버안보 국제협력에 있어 가장 기본적인 요소로서 각 국가 간 신뢰를 구축함과 동시 긴밀한 협력체계를 마련한다는 점에서 중요한 의미를 갖는다. 양자 간 협력은 주로 안보 전반에 관련된 이슈들을 논의하는 가운데 사이버안보를 공동 의제로 올리면서 이루어지는 경향이다. 우리나라 역시 미국·영국을 비롯한 우방국들과의 양자·삼자 간 협력을 통해 국제 사이버안보 역량을 강화해왔으며 최근 중국과도 고위급 소통 채널을 통해 한반도 및 지역·국제 외교·안보 문제를 논의하는 과정에서 사이버안보 양자 협력 역시 추진되고 있다

먼저 미국 사례를 살펴보면, 미국은 현재 우리나라를 비롯하여 일본, 중국, 프랑스, 독일, 우크라이나, 에스토니아, 아르헨티나, 케냐 등 아시

19) 뉴질랜드·미국·러시아·인도·일본·중국·한국·호주 등 8개국

아·유럽, 남미·아프리카 11개국과 양자 사이버 협의를 실시하고 유럽연합(EU)과 동남아국가연합(ASEAN) 등 지역 안보기구와의 협력대화 추진과 더불어 북대서양조약기구(NATO), 유럽안보협력기구(OSCE), 아세안지역협력포럼(ARF) 등 지역 안보기구와 안보협의체와도 협력을 통한 긴밀한 신뢰 구축을 추진하고 있다.[20] 중국과는 2009년 이후 미·중 사이버보안 실무그룹 협의나 고위급 공동대화를 진행해 왔으나 중국의 미국에 대한 해킹 사례로 미·중 간의 사이버 갈등은 여전히 진행 중이다.

일본은 현재 가장 큰 동맹국인 미국을 비롯하여 영국, 프랑스, 독일, 러시아, 에스토니아, 우크라이나, 이스라엘, 호주, 인도, 한국 등 유럽·아시아 11개 국가와 양자 사이버 대화를 실시하고, 유럽연합(EU), 동남아시아국가연합(ASEAN) 등 지역 안보기구와도 사이버협의를 실시하고 있다. 특히 미국과의 이해관계가 부합된 아시아 재균형 정책에 따라 양국 간의 협력이 그 어느 때보다 강화되고 있는데 '핵우산'과 같은 개념의 '사이버안보 우산'을 제공하기로 합의하고 인터넷 경제정책협력대화, 사이버 대화, 사이버방어정책 워킹그룹 등을 지속 추진중에 있다.

영국은 미국과 함께 사이버 공간에서 개개인의 프라이버시권과 표현의 자유, 사생활 보호 및 자유로운 정보의 유통이라는 공통의 가치에 합의하고 기반시설 보호(위협정보 공유, 네트워크 방호 훈련)와 사이버 방어 협력(CERT 간 정보공유, 유관기관 간 Cyber Cell 설립 통합 협력), 사이버보안 연구 협력(MIT-케임브리지대학 사이버보안 경진대회 개최) 등 세부적인 사이버 협력을 구체화하고 있다.

중국과 러시아는 사이버 공간을 이용한 특정 이념과 사상 전파로 인한 국가 체제 위협행위를 차단해야 한다는 데 인식을 같이하면서 사이버 협력 강화를 위해 2015년 5월 중·러 사이버안보 협약을 체결하였다. 이는 중국과 러시아가 사이버 공간에서 상호 간의 감시를 지양하고 양국의 관련 기관을 통해 기술을 전수하고 정보를 공유하겠다는 약

20) U.S. Department of State, "Office of the Coordinator for Cyber Issues," <https://www.state.gov/bureaus-offices/bureaus-and-offices-reporting-directly-to-the-secretary/office-of-the-coordinator-for-cyber-issues/> (accessed september 20, 2019).

속 이행을 담고 있다.

앞에서 살펴본 국가 차원의 협력 이외에도 민간 부문 차원의 양자 협력 역시 국제협력을 위한 중요한 역할을 수행하기도 한다. 미국과 러시아의 경우 미동서연구소(East West Institute)와 러시아의 모스크바 대학정보보안연구소의 각 분야 민간전문가들이 정보공유와 협력을 통해 의미 있는 성과를 도출하고 있다. 국제정보안보에 관한 국제학술회의 등 국제 정보보호 콘퍼런스 역시 사이버안보에 대한 입장 확인과 최신 사이버 기술 및 전략·정책 동향을 파악하고 국제안보 이슈 및 주요 기반시설의 보호 등 중요현안을 논의할 수 있는 주요 협력체계라고 볼 수 있다.

Ⅳ. 주요국 사이버 국제협력을 포함한 대응전략

세계 각국은 다양한 사이버위협에 대응하기 위해 사이버 방어 기술 역량을 강화하는 것과 더불어 사이버안보 국가전략을 마련하고 국제협력을 강화하는 등의 자구책 마련에 총력을 기울이고 있다. 세계의 주요국가들은 다양화되고 고도화되는 사이버 공격에 대비하기 위해 사이버위협 유형에 맞게 효과적으로 대응하고 종합적인 국가위기관리전략과도 일관성을 가질 수 있도록 국정과제로 사이버안보를 지정하는 동시에 기존 사이버위협 대응시스템을 현재 안보환경에 맞게 최적화하기 위해 획기적이고 다양한 사이버안보 전략들을 수립하고 있다.

제1절 서방 주요국 대응전략

1. 미국

미국은 자국의 정보시스템 파괴 및 지적재산 절도로부터 보호하기 위해서 일찍부터 사이버 공간을 보호하며 사이버안보 문제를 국가전략의 일부로 보는 공세적인 전략을 추진해 왔다. 이러한 과정에서 중국, 러시아, 이란, 북한 등 4개국으로부터 해킹 등 사이버 공격의 양적 증가가 미국의 사이버 전략 수립에 큰 영향을 미쳤다. 이러한 맥락에서 2017년 사이버사령부(Cyber Command)를 전략사령부 휘하 조직에서 독자적인 지휘체계를 갖춘 10번째 통합 전투사령부로 지위를 격상시키는 조치를 단행하는 등 선제적으로 사이버안보 대응 개념을 도입하기도 했다. 또한, 2013년부터 4년 동안 사이버 작전에 사용되는 무기[21] 개발을 위한 대규모 프로젝트인 '플랜X'를 추진하는 등 군 차원에서도 사이버위협에 발 빠르게 대응해 왔다.

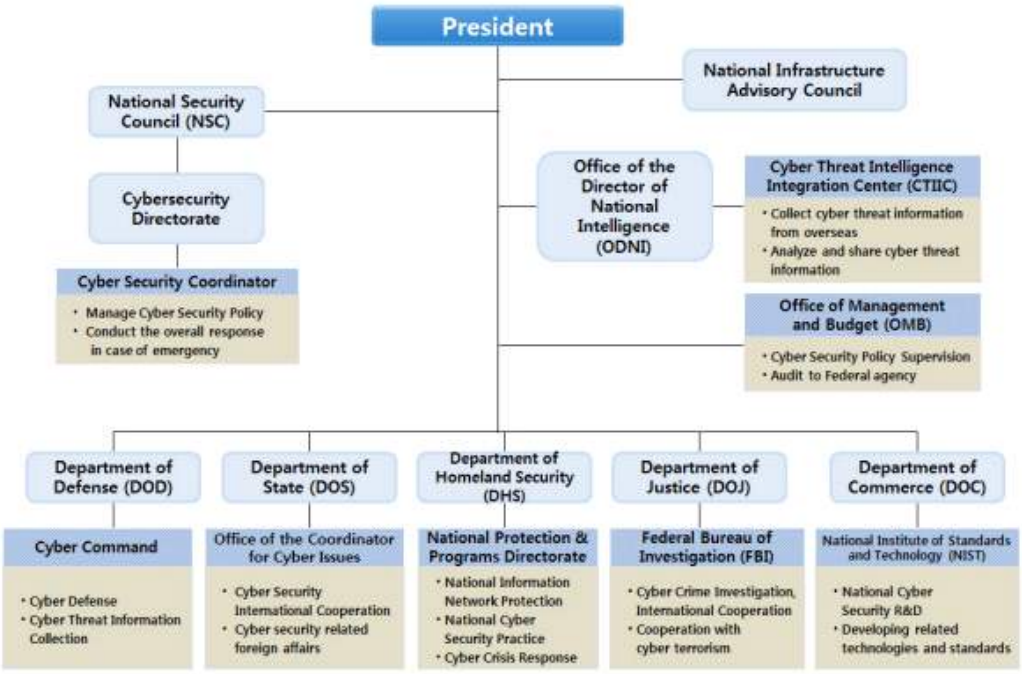
미국은 자유롭고 개방된 규칙에 기반한 국제질서(rule-based international order) 등 기본원칙에 기반한 국제규범과 거버넌스 구축을 추구하고

21) 미래형 사이버 무기 : 플레임(스파이 바이러스), 스턱스넷(Stuxnet), EMP(전자기펄스)탄, 디지털 게놈 등

있으며 우방국들과의 연대를 강화하여 중국·러시아에 대항함으로써 사이버안보에서 전략적 우위를 장악하고자 하고 있다. 지역 및 양자 차원의 사이버 협력 강화를 통해 아시아-태평양지역과 유럽지역에서 미국이 주도하는 사이버안보 전략을 구축하고, 초국가적 이해당사자들이 참여하는 글로벌 거버넌스(Grobal Governance) 매커니즘을 적극 활용하고 있다.

가. 사이버안보 추진 체계

미국에서 사이버안보를 담당하는 기관으로 국방부의 사이버사령부 및 국가안보국(National Security Agency, NSA), 국토안보부(United States Department of Homeland Security, DHS), 연방수사국(Federal Bureau of Investigation, FBI) 등이 있다. 미국 연방정부 사이버안보 추진체계는 아래 그림과 같다.



<그림 3> 미국 연방정부 사이버안보 관련 추진체계

美국방부는 2010년 사이버사령부(United States Cyber Command, USCYBERCOM)[22]를 창설하여 사이버 공간에 대한 작전 능력을 강화

22) 미 사이버사령부는 전략사령부(U.S. Strategic Command, USSTRACOM)에 속하여 육군 사이버사령부(Army Cyber Command, ARCYBER), 제24공군(24th USAF), 함대 사이버사령부(Fleet Cyber Command, FLTCYBERCOM), 해병 사이버사령부(Marine Forces Cyber Command, MARFORCYBER)로 구성

하기 시작했고 2017년 8월에는 사이버사령부를 독자적인 지휘체계를 갖춘 10번째 통합 전투사령부로 격상하였다. 사이버사령부는 육·해·공·해병대에 개별 조직으로 운영된 사이버 관련 업무를 통합하였고 미군의 사이버안보 체계구축뿐만 아니라 다양한 분야의 정부 부처와 연계하여 사이버 공격 대응체계를 구축하였다. 사이버사령부는 사이버상의 군사활동을 포함해 국방부 및 주요 군 시설의 네트워크 시스템 방어 및 민간 영역의 주요 기반시설 방어 등의 업무를 담당하고 있다. 임무별로 보면 세계 전역에 파견되어 있는 미군의 사이버 군사 임무를 지원하는 임무를 담당하는 사이버 전투파견부대(Cyber Combat Mission Force), 국방부 네트워크 시스템 보호를 담당하는 사이버 보호부대(Cyber Protection Force), 사이버사령부 명령에 따라 본토 내의 주요 민간시설 및 해외 주요 거점에 대한 방어를 담당하는 사이버 국가파견부대(Cyber National Mission Force) 등으로 구성되며, 육군, 해군, 공군 등 각 군마다 존재하는 사이버 방어 전담부대를 통해 임무를 수행하고 있다. 군사조직 외에도 국토안보부(DHS), 국가안보국(NSA), 연방수사국(FBI) 등 민간 분야에 중점을 두고 임무를 수행하는 정부 기관과도 긴밀하게 업무협조체계를 구축하고 있으며, 군사적 역량 강화뿐만 아니라 민간 차원의 사이버 대응능력을 지원받고 있다. 이외에도 전쟁 시 부대 배치를 받고 활동을 수행하지만 평시 훈련의 의무는 없는 방호인력인 사이버예비군을 조직하고 운영하고 있는데 사이버 공격에 대한 즉각적인 대응이 가능하도록 법률로 권한을 부여받고 있다.

국가안보국(NSA)은 美국방부 소속의 정보수집 기관으로 통신정보, 감청, 전자정보 등의 수단을 사용하여 암호 작성·해독, 관리를 주요 임무로 하는 기관이다. 국가안보국(NSA)은 국방부 산하 조직이지만 사이버사령부보다 더 광범위하고 활동하는데 군 외 정부 기관과 산업기관을 비롯하여 민간과 더욱 긴밀하게 활동하고 있다. 특히 국가안보국(NSA)은 유럽, 일본 그리고 한국 등 안보 동맹국 및 우호국들에 대한 사이버위협에 대한 방어와 억지 역량 구축에 대한 지원도 수행하고 있다.

국토안보부(DHS)도 사이버안보를 담당하는 주요 기관으로 9·11테러를 기반으로 설립된 국토안보부의 역할은 매우 광범위한데 그 중 핵심

임무가 '사이버 공간의 보호 및 안전 확보'이다. 국토안보부에서 사이버안보는 산하에 미국 사이버안보 및 통신통합센터(National Cybersecurity and Communications Integration Center, NCCIS)가 담당하고 있고 그 임무는 사이버침해 사고에 대한 대응 능력 및 협력을 강화하고 이를 위해 미국의 사이버위협 정보수집과 위기시 대응체계를 마련한다. 또한, 사이버 공격과 관련 수집된 정보를 각 연방정부 기관에 전파하고, 주요 기관들의 시스템 감시를 위해 상시 모니터링을 실시하고 있다. 특히 바이든 정부 출범하여 국토안보부(DHS) 내 사이버·인프라안보국(Cybersecurity and Infrastructure Security Agency, CISA)을 통해 연방정부 주요 기관 간의 사이버안보를 조정하는 역할을 하고 있는데 이것은 국가 최고 수준에서 사이버안보 의제를 다루고 있다고 볼 수 있다.

연방수사국(FBI)은 법무부 소속으로 법 집행기관이면서도 범죄 수사와 정보를 수집하는 업무를 담당하고 있다. 연방수사국(FBI)의 사이버안보는 사이버범죄수사대(Cyber Crime)가 담당하며 사이버테러 등 범죄 활동 측면에서 활동하고 있는데 사이버 범죄행위에 대한 사법기관들의 조사 및 수사를 주도하고, 사이버테러조직 및 테러리스트를 예방하고 검거하는 역할은 물론 정부 기관, 민간기업 및 비영리기관과 활발하게 정보를 공유하는 등의 업무를 수행하고 있다.

나. 사이버안보 대응 전략

미국은 9·11 테러 사건을 계기로 사이버안보를 보편적인 보안 영역이 아닌 국가안보 차원의 위중한 문제로 접근하기 시작했다. 2008년 1월, '국가 사이버안보 종합 기획(Comprehensive National Cybersecurity Initiative, CNCI)을 발표했는데 이는 사이버안보 문제에 대한 국가안보 차원의 포괄적 대응책을 마련한 최초의 작업으로 평가받았다. 2009년 5월에 발표된 '사이버 공간 정책 검토(Cyberspace Policy Review)를 기점으로 지금까지 수많은 보고서를 통해 미국의 사이버안보에 대한 논의가 체계화되고 사이버전에 적극 대응하고 있다.

오바마 행정부가 출범하면서 사이버위협을 미국에서 가장 심각하고 국가안보의 중요한 위험요소 중 하나로 간주하였으며 소극적 대응에서 벗어나 적극적 대응으로 방식이 변화하기 시작했다. 국가 주요기반시설에 대한 해킹을 국가안보에 대한 위협으로 간주하고 미사일 발사를 통해 적극적으로 대응하겠다는 의지를 보이며 사이버안보를 국가안보의 중요한 고려요소로 인식하였다. 2012년 이후 사이버위협을 억제하기 위해서 자위권 차원에서 공격 진원지를 선제 타격하겠다는 완강한 입장이 등장하였다. 美국방부는 2012년 5월 국방부 주관으로 Plan-X 프로젝트에 착수하였는데 이 프로젝트는 美국방부의 사이버 전력을 증강시키는 목적으로 사이버 무기 개발을 본격화하고, 전 세계 수백억 개의 컴퓨터 도메인과 서버, 그리고 그것들의 연결 관계 분석을 통해 적의 공격 루트를 찾고 적의 공격징후를 포착하여 선제공격한다는 사이버 전장지도를 개발하는 계획을 담고 있었다. 2016년 「사이버보안 관련 국가 행동계획(Cybersecurity National Action Plan, CNAP)」을 발표하였는데, 사이버 공격에 대해 정부가 조직적으로 대처하고 고도화하는 사이버 공격에 대응하기 위해 민간기관과 군, 정보기관이 상호 협력할 수 있는 연방 기구를 설립하여 범정부부처 간 공동대처 능력을 강화하는데 노력하였다. 사이버안보에 대한 총괄 책임을 국토안보부(DHS)에서 백악관으로 옮기며 사이버안보 확보를 위한 연방정부의 역할 강화와 민간 부문과의 협력을 제도화해 나가는 사이버안보 거버넌스 대응체계를 구축하고자 하였다.

2017년 트럼프 행정부 출범 이후 사이버 공격 횟수가 오바마 행정부에 비해 월등히 증가하였고 그 수법도 고도로 지능화, 다양화되어 갔다. 이에 트럼프 행정부는 힘에 의한 미국을 중심으로 하는 국제질서를 바탕으로 '미국 우선주의'를 앞세우면서 오바마 행정부에 비해 보다 공세적인 사이버안보 정책을 견지하였다. 트럼프 행정부의 사이버 대응은 자국을 대상으로 하는 해킹공격에 대해서는 맞공격도 마다하지 하겠다는 단호한 입장과 함께 국가수권법을 근거로 사이버 공간에서의 군사적 방위 활동을 승인하였다. 또한, 트럼프 정부에서는 사이버 공격을 국가안보와 경제, 사회에 심각한 교란을 초래하는 위험요인으로 간

주하고 연방정부 차원의 대책 마련에 주력하였다. 2017년 사이버사령부를 중심으로 사이버 방어 및 공격 능력 개발하고 국토안보부(US Department of Homeland Security)를 중심으로 사이버안보 역량 강화를 추진하도록 하는 행정명령을 발령하였다. 이후 2018년 9월에는 국토안보부(DHS)를 중심으로 하는 '국가 사이버안보 전략'을 공개하였는데 글로벌 차원에서 사이버안보 관련 국제협력을 이끌어 내기 위한 사이버위협 평가 및 합동군사훈련 등과 같은 정부 간 활동과 동반자 국가들의 사이버 위협대응을 위한 역량 구축 지원 등 국무부의 외교적 노력 강화와 범정부 차원의 다층적이고 통합적인 대응시스템 구축을 담고 있다. 트럼프 행정부는 사이버안보 전략 기조가 '미국 우선주의'를 사이버 공간에도 우선적으로 반영하여 사이버 공격에 대한 대응방식 및 안보관에 있어서 오바마 행정부와 확연히 다른 차별성을 두었다. 특히 백악관이 아닌 국토안보부(DHS)에게 사이버안보 대응에 주도적인 역할을 부여하고 권한을 강화하여 복잡해지는 사이버안보 환경을 효율적으로 관리하도록 하는 한편, 민간기업들과의 적극적인 파트너십을 구축함과 동시에 국가가 필요시 민간 영역에 개입할 필요성이 있도록 하는 방향으로 정책이 전환되었다.(김근혜, 2019)

바이든 행정부 출범 전후 미국은 러시아에 의한 솔라윈즈 사태, 중국의 마이크로소프트 이메일 해킹, 북한의 코로나19 백신 기술 탈취를 위한 사이버 공격 등 악성 사이버 활동에 직면하는 사례가 늘어났다. 바이든 행정부는 2021년 미국 국방수권법을 근거로 백악관에 사이버국장실(cyber director office)을 신설하고 사이버안보를 국가안보의 주요한 핵심과제로 간주하기 시작했다. 또한, 2021년 3월 미국의 세계적 관여에 관한 새로운 비젼을 담은 잠정국가안보전략지침(Interim National Strategic Guidance)을 발표하고 미국인의 안전과 경제적 번영, 민주적 가치 실현을 국가안보의 우선순위로 부여하면서 사이버 공간에서의 대응역량과 회복력(resilience)을 강화할 것을 천명하였다. 민간과 정부의 협력을 통해 사이버 위험을 관리하고 사이버안보 인력 양성에 집중하며 사이버 공격에 대응하기 위해 사이버 수단뿐만 아니라 비사이버적 수단으로 대응할 것임을 밝혔다. 바이든 행정부는 "미국의

귀환(America is Back)을 기치로 미국 우선주의 하에 트럼프 행정부의 국가 안보전략을 상당 부분 계승하면서 국제사회에서의 미국의 역할을 강조하였으며, 동맹국들과의 협력을 통해 중국·러시아를 견제하고 사이버 공간에 관한 새로운 국제규범 창설을 역설하였다.

미국 행정부별 사이버안보 외교전략을 보면, 오바마 행정부는 사이버위협을 국가안보의 중요한 축으로 간주하였지만, 이를 중국·러시아 등을 압박하는 도구로 활용하지는 않았다. 그 대신 사이버안보 국제규범 마련과 거버넌스 구축의 주도권을 확보하고자 다자안보 협력기구 논의에 적극적으로 참여하였다. 반면에 트럼프 행정부는 잠재적 패권 도전국인 중국을 봉쇄하기 위한 전략의 일환으로 파이브 아이즈(Five Eyes)[23], 쿼드(Quad)[24] 등 소규모의 다자 동맹과 안보협력을 사이버안보 분야에서의 중국을 압박하는 용도로 이용하는 외교 행보를 보였다. 그리고 현재 바이든 행정부는 사이버안보 분야를 첨단기술 경쟁과 21세기 강대국 간의 경쟁 핵심무대로 여김에 따라 사이버안보 전략에 기술동맹을 추진하는 외교전략으로 발전하는 한편 기존의 다자 동맹과 안보협력을 연계하여 중국을 더욱 견제하고 있다.(오일석, 2022)

<표 4> 미국 행정부별 사이버안보 전략의 특징

시 기	사이버안보 특징
오바마 행정부 1, 2기 (2009.2~2017.1)	· 사이버 공간을 전쟁영역으로 간주 · 사이버 공격자들에 대한 비용 부담과 회복력 강조 · 중국이나 러시아 등의 도전에 대한 미온적인 태도
트럼프 행정부 (2017.2~2021.1)	· 힘을 통한 사이버 공간의 안전성 확보 · 사이버 군사력을 포함한 모든 수단 사용하여 선제적 방어 · 사이버 억지와 책임 귀속 강화 등 공세적 사이버안보 정책
바이든 행정부 (2021.2~현재)	· 트럼프 정부 정책 계승 및 강화 · 동맹국 및 파트너 국가들과의 연대 강화 · 국제적 연대와 규범 정립 강조

23) 파이브 아이즈(Five Eyes)는 미국, 영국, 캐나다, 호주, 뉴질랜드가 상호 첩보 동맹을 맺고 있는 기밀정보 공유협의체

24) 쿼드(Quadrilateral Security Dialogue, QSD)는 미국, 일본, 인도, 호주로 이루어진 4자 정상회담 간의 전략적 안보 대화체

미국은 사이버 공간에서의 표현의 자유와 지적 재산권의 보호, 프라이버시의 보호, 사이버 범죄행위 색출 강화, 사이버 공격에 대한 예방적 자위권 행사 등을 위해서는 국제협력 강화가 필요하다고 인식하고 지역 다자기구 및 양자 협력 차원에서 사이버 공간에도 기존의 동맹관계를 활용하는 전략을 추구하고 있다. 미국은 가짜뉴스(fake news), 온라인 허위정보(disinformation) 등 민주주의 가치를 위협하고 사회혼란 및 분열을 가져오는 중국·러시아 등 권위주의 국가에 의한 사이버 공격에 적극적으로 대응하기 위해 파이브 아이즈(Five eyes) 등 정보동맹 국가와 인도·태평양 지역의 쿼드(Quad) 협력체 국가들과 협력하고 있다. 특히 유럽지역에서는 NATO나 EU, 특히 영국과의 사이버 협력을 강화했고 아태지역에서도 한국, 일본, 호주 등과 사이버안보 협력을 확대하고 있다. 반면에, 미국은 G7·NATO·EU 등과 함께 중국을 '구조적 도전(Systemic Challenge)'으로 규정하고 중국 견제체제를 구축하고 있다.

미국은 과거 사이버 공간에 관한 국제규범을 만드는데 소극적이었으나 최근 입장을 선회하여 사이버 이슈에 관한 기존 동맹국과 함께 사이버 공간에 관한 기존 국제규범을 검토하고 국제사회의 사이버 국제규범 설립에 적극적으로 개입하면서 관련 논의들을 주도하고 있다. 이러한 과정에서 UN GGE나 국제전기통신연합(ITU) 등과 같은 기존의 국제기구의 틀을 활용하기보다는 유럽안보협력기구(OSCE), NATO, 아세안안보지역포럼(ARF) 등 지역 차원에서 존재하는 지역 안보기구를 통한 협력체계 구축과 정부·학계·NGO 등 민간 이해당사자들이 모여 대화하는 글로벌 거버넌스의 논의에 주력하고 있다.

2. 영국

영국은 사이버 관련한 기술과 고급 인력을 보유한 사이버안보 선진국가에 속한다. 영국은 2009년 6월 최초로 사이버안보 전략을 발표한 후 2010년 'A Strong Britain in an Age of Uncertainty: The National Security Strategy' 보고서에서 사이버위협을 테러 행위와 함께 국가 안

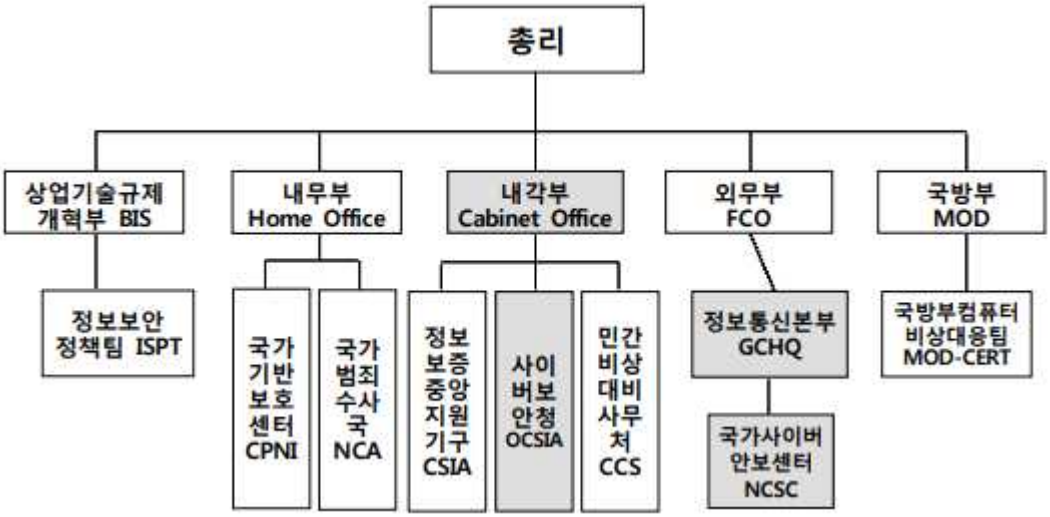
보를 위한 가장 큰 우선순위로 꼽은 바 있으며 유럽국가 중에서 가장 활발하고 적극적으로 대응하고 있다. 2021년 12월 「국가사이버전략 2022」을 발표하였는데 이전과 달리 사이버 전략을 단순한 사이버 공격·방어 차원이 아닌 국가의 운명을 결정지을 수 있는 중요한 국가전략으로 인식하였다. 영국의 사이버안보 전략은 국익의 보호와 체제 수호를 위한 핵심 기반시설의 안전을 확보하고 국내 사이버위협에 대응하는 역량을 강화하는 동시에 사이버안보 공간의 안보 증진을 위한 서방 국가와의 국제연대의 필요성을 강조하고 있다. 영국은 자유롭고 개방된 사이버 공간을 지지하고 발전시키고자 노력하면서 영국의 이익을 확보하기 위한 새롭고 유연한 동맹 구축을 모색하고 있다.

미국의 쇠퇴와 함께 미·영 주도의 세계질서가 도전을 받는 가운데 브렉시트(Brexit) 이후 영국은 제2의 대영제국을 꿈꾸며 유럽연합(EU)과 일정한 거리를 두고 '글로벌 브리튼(Global Britain)'이라는 새로운 국가전략을 기치 아래 아시아·태평양 지역과의 협력 강화에 비중을 두고 있다. 새로운 사이버 환경에서 주도적으로 자국의 이익과 가치를 증진하고 동시에 국가안보를 위협하는 행위를 능동적으로 제거하면서 미국과 함께 새로운 질서를 수립하고 주도권을 확보하는 시도를 보였다. 특히 악의적이고 범죄적인 사이버 공격에 대해서는 자기방어적 차원의 군사적 보복공격과 더불어 비용 및 책임부담, 경제제재 등 모든 수단을 동원한 대가를 치르게 될 것이라는 강력한 의지와 강경한 태도를 보이고 있다.

사이버 공간 내에서도 미·중 기술 패권경쟁과 갈등이 지속되고 있는 상황에서 영국은 사이버 공간에서 미국이 주도하는 국제질서에 적극 동참하고 자신들의 위상을 제고하고자 노력하며, 러시아·중국으로부터 지속적으로 발생하는 공동의 위협을 탐지하고 저지하기 위해 동맹국들과 계속 협력하며 집단안보를 강화하고 있다. 우방 국가들과의 양자협력과 UN, EU, NATO 등을 통한 다자 파트너십의 구축을 확대하고 있다.

가. 사이버안보 추진 체계

영국은 내각부(Cabinet Office)가 주도하여 사이버안보 전략을 수립하고 시행해 오고 있다. 모든 사이버안보 정책을 총괄하고 정보보호 활동 및 업무 조정을 하는 내각부 산하에 정보보증중앙기구(CSIA), 사이버안보청(OCSIA), 민간비상대비사무처(CSS) 등이 소속되어 있다. 이외에도 영국 주요기반시설 보호와 테러 대응 등을 담당하고 있는 내무부(Home Office)와 통신정보 수집 및 제공을 담당하고 있는 외무부(Foreign & Commonwealth Office), 국가 산업 발전을 위해 정보보호 정책을 담당하고 있는 상업기술규제개혁부(Department for Business Innovations and Skills), 사이버 관련 군사정보 수집과 방첩 활동을 하는 국방부(Ministry of Defense) 등이 영국의 사이버안보 관련 정부 부처이다.



<그림 4> 영국의 사이버안보 관련 추진체계

내각부 산하의 정보보증중앙기구(CSIA)는 영국 정부의 정보보증 개선이 주업무로 ICT를 활용한 정부의 공공서비스 지원 및 훼손될 위험이 있는 정보 및 시스템을 보호하는 업무를 수행하고 있다. 사이버안보청(OCSIA)는 사이버안보의 전략적 방향을 제공하고 범정부적 국가사이버보안 프로그램(NCSP) 관장하며 민간기업과의 정보교환 및 국제협력 등의 업무를 수행하고 있다. 민간비상대비사무처(CSS)는 내각부 내의 비상사태에 대응하는 업무를 맡고 있다.

내무부 산하 국가범죄수사국(NCA)은 미국의 연방수사국(FBI)와 유사한 국가 사이버 범죄 대응기구로서 업무를 담당하고 있고, 국가기반보호센터(CPNI)는 주요 기반시설을 보호하는 업무를 수행하고 있다. 외무부 정보통신본부(Government Communications Headquarters, GCHQ)는 통신정보(Signals Intelligence) 관련 업무는 물론 사이버 범죄를 포함한 사이버위협의 탐지 및 분석, 해외 동맹 기관과의 협력 등을 수행하고 있다. 외무부 GCHQ 산하의 국가사이버안보센터(NCSC)는 국가 사이버 기반시설이 공격을 받는 경우 군의 사이버안보작전센터와 협력하여 적극적으로 대응하고 사이버 위협정보에 관해서 정부 행정부처와 민간기업체 등과 공유하고 있다.

국방부 산하에 군사와 관련된 모든 정보를 전담하는 영국 국방정보국(DI)이 있으며, 영국 정보청 보안부인 군사정보총국 제5과(MI5), 대외정보기관인 비밀정보국(SIS 또는 MI6)을 통해 군사정보 수집과 방첩활동을 수행하고, 국방 등 영국의 중대한 이익과 관련된 해외 비밀정보를 수집하고 있다. 또한, 사이버 공격 발생 시 영국군을 지원하고 사이버 방어를 담당하는 군사조직인 '사이버예비군'을 국방부 산하의 합동사령부 내에 창설하여 사이버 공간에서의 네트워크 시스템 보호 및 적국에 대한 사이버 공격을 담당하고 있다. 미국과 달리, 사이버예비군은 전역한 군인과 민간인 중 컴퓨팅 기술이 탁월한 인력을 중심으로 군사조직 내에 편성되어 있는데, 군대에 종속되어 있지 않고 필요시 소집되어 임무를 수행하고 있다. 영국은 사이버 인재들의 역량을 민간영역에서 효율적으로 활용함으로써 군사력 강화 측면과 더불어 사이버 인력들의 역량 강화로 사이버 관련 산업 육성에도 도움이 되고 있다.

나. 사이버안보 대응 전략

2011년 내각부(Cabinet Office)가 정부뿐만 아니라 민간기관, 국제기구와의 협력을 통한 사이버 공간의 안전한 사용을 강조하였다. 2013년에는 정부와 민간기업 간의 원활한 정보공유를 위한 Cyber Security Information Sharing Partnership(CISP)와 네트워크의 복원력을 강조한 The National Cyber Security Our Forward Plans를 발표했다. 2016년

에는 내각부 외 재무부가 동참하여 National cyber Security Strategy 2016-2021이라는 새로운 사이버안보 전략서를 발표하였다. 이 전략서에는 사이버위협으로부터 공격을 받는 경우에 신속하게 회복하여 경제적 번영을 추구할 수 있는 비전하에 방어(Defend), 억지(Deter), 개발(Develop)이라는 3가지 목표를 설정하고 추진되었다. 이를 달성하기 위해 다양한 실행과제들이 제시되었는데, 고도화되는 사이버위협으로부터 스스로 방어할 수 있는 능력을 갖도록 하고 적대적 행위에 대해서는 범법자를 추적하여 기소하며 기술개발 능력을 향상하여 혁신적인 사이버안보 산업을 발전시키고자 하였다.

2021년에 영국은 2030년까지 책임감 있고 민주적인 사이버 영향력의 선도국으로서 사이버 공간에서의 영국의 이익을 보호하고 증진할 것임을 비전으로 제시하고 목표를 달성하기 위한 5대 실행계획을 골자로 한 '국가 사이버 전략 2022'를 발표하였다. 이 전략은 National cyber Security Strategy 2016-2021과 안보·국방·외교 정책을 근간으로 작성되었다. 그간 영국은 고도화되고 다양한 사이버위협으로부터 자국의 보호하기 위하여 사이버 전문인력 육성과 미래 기술개발, 사이버 범죄예방과 탐지, 국가 사이버군(National Cyber Force, NCF) 운영 등 대응전략을 착실히 실행해 나갔다. 또한, 사이버위협에 대응하는 역량과 회복력을 강화하고 사이버위협에 대한 국민의 인식을 제고시켰으며, 글로벌 중추 국가 차원에서 국제협력을 선도하고자 하고 있다. 또한, 영국 정부가 사이버 공간을 국가이익 실현을 위한 주요 핵심 공간으로 인식하고 사이버 공간에서 국제규범 강화 및 자발적 합의에 의한 규범 마련을 강조하며 국가 간의 신뢰 구축을 실천하고자 하는 외교의 방향을 추구하고 있다.

자유롭고 안전한 사이버 공간에 대한 국제적인 합의를 이끌어 내기 위해 UN, G20, NATO, OSCE 등 국제기구와 다자 안보협력기구를 활용한 국제공조에도 적극 참여하고 있다. 특히 미국과는 사이버안보 역량 강화를 위해 사이버 해킹에 대한 광범위한 대응을 위한 훈련인 사이버 워게임을 추진하고 있다.

3. 독일

독일은 사이버 공격으로 인한 재산적 피해가 지속적으로 증가하고 있는데 연방헌법수호청(Bundesamt für Verfassungsschutz: BfV)[25]에 따르면, 러시아·중국·이란 등의 국가들이 독일에서 가장 빈번한 사이버 첩보 활동을 펼치고 있으며 사이버 공격은 정치, 경제, 학계, 군 영역까지 다양한 대상을 향해 이루어지고 있다고 하였다.

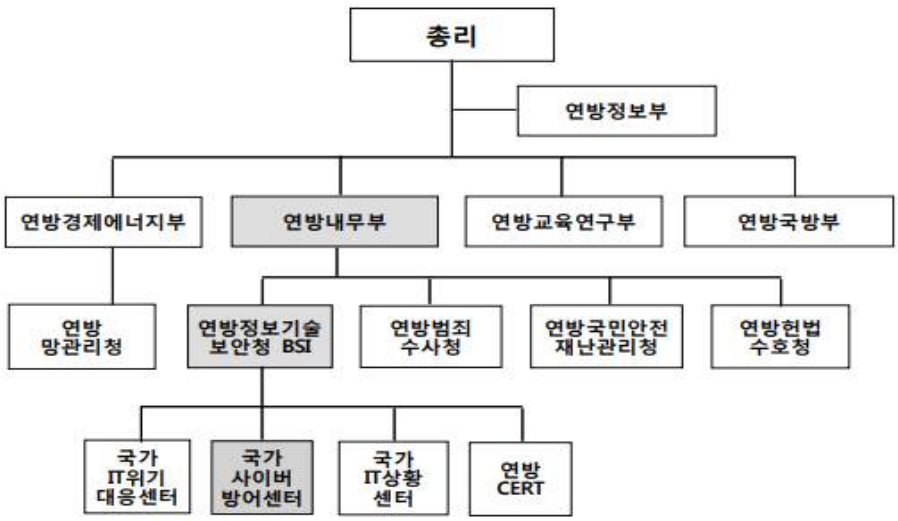
2011년에 독일 연방정부는 최초의 국가 사이버안보 전략(NCSS)을 채택(Bundesministerium des Innern 2011)했는데 NCSS는 사이버안보 정책이 명백히 민간에 초점을 맞춰져 있으며 사이버안보 능력 보호 조치로 독일 연방군(Bundeswehr)의 지원을 받을 수 있도록 하였다. 독일 연방군 운영은 독일 헌법에 의해 제한되어 있고 연방의회의 명시적인 승인을 받아야 하나 연방의회가 승인한 독일 연방군의 해외 임무의 틀 내에서 사이버 작전을 수행하는 것은 문제가 되지 않는다는 입장이다. 2015년에 국방부는 자체 사이버 전략을 개발하기 시작했는데 사이버 및 정보 공간 사령부(Kommando Cyber- und Informationsraum, CIR) 설립, 부처 개편 및 독일군 대학에 사이버안보 연구 자원 설립과 같은 기타 지원 조치로 군은 사이버안보 정책에 크게 기여를 하고 있다[26]. 2016년에 발표한 사이버안보 전략은 2011년 사이버안보 전략을 기초로 작성되었는데 그 기조가 IT산업이나 개인의 프라이버시 보호보다는 국가 주요 기반시설에 대한 사이버 방어 강화를 강조하면서 독일 연방군의 적극적인 참여와 제도적 변화를 모색했다.

유럽 차원에서의 사이버안보 국제협력을 위해서 외교·안보 관계뿐만 아니라 유럽의 사이버범죄협약에 따라 범죄예방과 단속 등의 업무를 주체적으로 수행하고 있다. 독일의 사이버역량 강화를 위해 주변국들과 우호적인 관계를 형성하고 양자 및 지역협력을 추진하고 있다. 독일은 미국·영국과는 달리 민간 이해당사자들이 주도하는 글로벌 거버넌스 구축에 기여하기 보다는 정부가 주도적인 역할을 수행하는 전통적인 다자안보 협력기구의 틀을 활용한 지역협력에 중점을 두고 있다.

25) 독일 연방내무부 소속으로 정보 수집, 분석 및 반연방 활동의 감시하는 정보기관임
26) Martin Schallbruch,「Cybersecurity in Germany」, 2018.

가. 사이버안보 추진 체계

연방제 국가인 독일은 연방내무부(BMI) 산하에 연방정보기술보안청(BSI)을 설치하여 사이버안보 관련 업무를 총괄하고 있으며, 연방 경제에너지부, 교육연구부, 국방부 등에서 사이버안보를 분담하여 업무를 수행하고 있다. 연방내무부와 산하 연방정보기술보안청(Federal Office for Information Security, BSI)은 기술 업무 외 사법적 임무 수행 지원, 테러 관련 정보획득 및 분석, 정보보호 자문 지원 등 포괄적인 사이버안보 업무를 총괄하고 있다. 연방정보기술보안청(BSI) 산하 국가사이버방어센터(National Cyber Defense Center)는 국가 차원의 컨트롤타워 기능을 수행하며 연방정부 내 여러 국가기관에서 동시에 사이버 공격이 발생할 경우 위기관리를 대응하고 총괄하는 역할을 담당한다. 이외에도 연방내무부 산하의 연방범죄수사청(Federal Criminal Police Office)은 사이버범죄를 수사하며 특별 수사기관(Quick Reaction Force, QFR)을 설립하고, 연방헌법수호청(Federal Office for the Protection of the Constitution, BfV)은 연방정부 차원에서 외국 정보기관 및 극단주의자와 테러리스트들의 활동에 대한 수사를 관장하고 있다.(김상배, 2017)



<그림 5> 독일의 사이버안보 관련 추진체계

독일은 북대서양조약기구(NATO) 회원국 중에서 사이버 부대를 가장 처음으로 운영한 나라로, 국방 차원에서 사이버 공격으로부터 국가 주요 기반시설을 방어하기 위한 임무를 수행하기 위해 2009년 76명의 군

인으로 구성된 사이버 해킹 부대를 창설하였다. 이 부대를 모체로 2011년에는 사이버국방센터가 신설되었고, 2017년에는 독일 연방군이 사이버 공격을 당했을 경우 맞대응할 수 있는 사단급 이상의 사이버 정보사령부((Organisationsbereich Cyber-und Informationsraum, CIR)를 창설했다. 병력 1만 4000명 규모의 군인과 민간인으로 구성된 사이버 대응군 사령부로 출범하면서 연방군 네트워크가 공격받으면 자위 차원에서 대등할 수 있는 부대를 창설한 것이었다.[27] CIR 사령부의 개념은 하나의 군사조직 영역에서 사이버 공간의 정찰, 작전 및 관리에 필요한 모든 병력을 결합하는 것으로 연방군 정보통신시스템의 보호하고 운영하며, 사이버 공간에서의 정찰 역량을 강화하며 지속적으로 발전시키는 임무를 수행하고 있다.

나. 사이버안보 대응 전략

2011년 처음으로 독립적인 국가사이버안보 전략을 수립할 때까지 독일의 사이버안보 전략은 敵이 자국의 네트워크에 침투하지 못하도록 견고하게 방어하고 빠르게 복구할 수 있는 역량을 강화하는 방어적 접근에 중점을 두었다. 이후 사이버 공격에 대한 위협이 고조되며 독일은 새롭게 사이버안보 전략을 고민해야 했다.

2016년 발표된 새로운 사이버안보 전략은 구체적인 실행전략을 구체화하며 사이버안보를 全 국가적인 과제로 강조했다. 2016년 사이버안보 전략은 4대 활동영역으로 구성되었는데, 국민들의 사이버역량 강화를 위해 디지털 기술을 안전하고 독립적으로 행동할 수 있도록 지원하고, 경제 전반에 사이버보안을 강화하여 공공시설에 대한 안전을 확보하고자 하였다. 특히, EU와 NATO의 동맹국과의 국제협력 및 신뢰 구축 및 분쟁 해결 메커니즘과 같은 외교적 조치를 강화하였는데 유럽 및 국제 사이버안보 정책에서의 독일의 적극적인 참여 등을 강조하면서 높은 수준의 사이버안보를 보장하기 위한 국제 파트너와의 협력체계 구축을 추진하고자 하였다. 아울러, 두 번째 국방 전략인 "독일 안보 정책과 연방군(국군)의 미래에 관한 백서"(Federal Government

27) 한국경제, 「독일, 사이버 공격 맞대응하는 군 부대 창설」, 2017.4.6

2016)를 통과시켰는데 이 백서는 처음으로 사이버안보의 전략적 군사적 측면을 담고 있다. 이를 통해 사이버를 제5전장으로 인정하고 연방군의 적극적인 역할을 모색하였는데 사이버 정보사령부(CIR 사령부) 정보군 부대를 창설하는 등 사이버 공간에서의 군의 역할을 확대하였다.

2021년 9월 독일 연방정부는 2016년에 수립한 국가사이버안보 전략 추진에도 독일 내 사이버 공격 발생 건수가 늘어나고 코로나19 팬데믹에 따른 디지털화 진행으로 위험도가 증가하고 있어 정부·기업·시민사회·학계의 공동과제로 정립한 "독일을 위한 사이버 안보전략 2021"을 의결하고 향후 5년간 독일의 사이버안보 정책 기본방향을 설정하였다. 이전 사이버안보 전략과 비교해 볼 때 디지털 소비자 보호 및 사이버 공격 예방을 위한 연방정부의 능력 향상뿐만 아니라, 정부·기업·국민 간의 협력 강화와 연방정부기술안정청(BSI)의 역할을 확대하고 사이버 공간에 대한 규범 강화 및 책임 있는 국가 행동을 위해 노력할 것을 강조하였다. 또한, 국제법 집행을 강화하고 국제 사이버 범죄 퇴치를 위해 EU에서 협력할 것을 강조하였다.

국제협력 측면에서는 2011년부터 사이버 공간을 보호하기 위해서는 국제사회의 협력과 역량 제고를 강조하였다. UN, EU, NATO, G8 등 국제기구 및 다자안보협력기구와의 협력을 강조하고 효과적인 유럽 사이버안보 정책 형성과 NATO 사이버 방어 정책을 더욱 발전시키며, 책임 있는 국가 행동에 대한 규범과 UN 또는 OSCE의 신뢰 구축조치를 포함하여 사이버안보를 국제적으로 형성하는 데 적극적으로 참여해 왔다. EU보다는 NATO 활동을 통해 사이버전에 대응하는 방위력을 증강시키고 있으며 유럽의 타 국가와 동일하게 사이버 공간에서 러시아와 대립하고 있다.

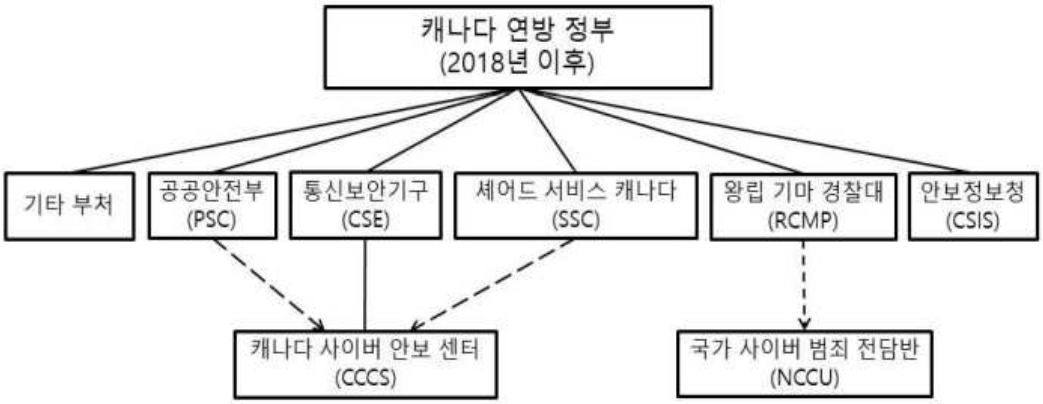
4. 캐나다

캐나다는 2004년 최초의 국가 안보 정책을 제시하였고, 2010년 사이버안보 전략(Canada's Cyber Security Strategy)이 처음 발표하였다. 캐

나다의 사이버안보는 사이버위협을 예방하고 탐지하며 제거함으로써 캐나다의 이익에 도움이 되도록 사이버 공간을 활용해야 함을 강조했다. 이 문서가 발행된 것은 미국, 영국, 그리고 호주와 같은 가까운 동맹국들이 차례차례 사이버안보 전략을 확립해 나가던 추세와 무관하지 않았다. 캐나다가 사이버안보에 대해 정부의 책임의식을 인식한 시점은 2000년 후반부터 시작했던 미국 및 서방 선진국들과 유사하다. 사이버 공격이 국가 안보위협 사안이며 개방적이고 자유로운 정보 흐름을 강조하고 다양한 이해당사자들의 참여해야 한다는 인식은 동맹국과 유사한 특징이다. 하지만, 다른 나라들에 비해 국제 전략적 관점이 부족하고, 사이버안보의 군사적 측면이 덜 강조되는 모습을 보였다. 2018년에 캐나다 정부는 진화하는 사이버범죄에 대처하고 민간 및 공공부문 조직에 대한 사이버범죄의 위협을 줄이기 위해 새로운 사이버안보 전략을 발표하였다.

가. 사이버안보 추진 체계

캐나다에서는 공공안전부(Public Safety Canada, PSG)가 사이버안보 전략의 시행을 조정하는 역할을 맡고 있는데, 캐나다인의 보호 및 공공안전유지 정책에 관한 행정, 규제 등의 업무를 담당하고 있다. 이는 美 국토안보부의 역할과 비슷하다고 볼 수 있다. 2018년 이전에는 공공안전부(PSC) 내의 정부작전센터(Government Operations Centre, GOC)가 국가 긴급 위기 대응시스템의 허브 역할을 담당하며, 그 안에 설치된 캐나다 사이버사고대응센터(Canadian Cyber Incident Response Center, CCIRC)가 사이버위협의 감시·자문·대응을 담당해 오다가 2018년에 캐나다 사이버안보센터(Canadian Cyber Security Center, CCSC)가 설립되면서 사이버안보 관련 사안들을 총괄하여 처리하는 구심점 역할을 수행하고 있다.



<그림 6> 캐나다의 사이버안보 관련 추진체계

캐나다의 국가보안법이라 불리는 C-59 Bill이 입법되면서 캐나다 첩보기관인 통신보안기구(Communications Security Establishment, CSE)가 사이버위협의 첩보 외에 새로운 권한을 부여받았고, 그 권한은 단순한 정보수집을 넘어 연방정부 내에서 그리고 파이브 아이즈(Five Eyes)와 같은 동맹국들과 위협정보를 공유할 수 있게 되었다. 이처럼 통신보안기구(CSE)가 美국가안보국(National Security Agency, NSA)과 같은 역할을 수행하고 있다. 왕립기마경찰대(Royal Canadian Mounted Police, RCMP)는 우리나라로 보면 경찰청이라 불리는 이 기관은 범죄 수사를 담당하며, 비인가된 컴퓨터 사용이나 데이터 관련 피해 범죄 사건들을 다룬다. 안보정보청(CSIS)과 연계하여 국내 사이버 범죄 수사에 집중하는 기관이다. 안보정보청(Canadian Security Intelligence Service, CSIS)은 캐나다 네트워크와 주요 정보시스템에 대한 사이버 범죄를 수사한다. 안보정보청(CSIS)은 캐나다 보안정보법(Canadian Security Intelligence Service Act)에 따라 국가안보 관련 사건을 조사하고 안보 위협에 대한 보고를 담당하는 부서로서 사이버위협과 행위자들의 의도와 수준을 분석한다. 안보정보청(CSIS)에 의해 캐나다 정부가 사이버위협 상황 인식, 사이버 취약점 파악, 사이버위협의 예방과 공공 인프라의 보호를 위한 조치를 취할 수 있다.

국방부((Department of National Defence, DND)와 캐나다군(the Canadian Armed Forces, CAF)은 네트워크를 수호하는 역량 강화에

집중한다. 그리고 사이버안보와 관련된 정부 부서들과 함께 공동으로 위협에 대한 대응업무를 수행하며 NATO를 포함한 동맹국 군조직과 함께 정보를 공유할 뿐만 아니라, 군사적 관점에서의 정책 및 규범을 개발한다. 또한, 국방부(DND)는 동맹국으로부터의 사이버안보 정보나 위협을 감시하여 보고함으로써 정부의 상황 인식에 도움을 주며 군사적 대응 옵션들을 제공한다. 2017년 3월 캐나다군(the Canadian Armed Forces)에 Cyber Operator occupation이 창설되었는데 Cyber Operator는 사이버 공격·방어 작전을 수행하며, 국내의 사이버 관련 기관들과 캐나다 동맹국과 협동하여 임무를 수행하고 있다. "사이버 공간은 군사작전의 필수 요소가 되었다"라고 국방부의 사이버 공간 사무총장인 프랜시스 앨런 준장의 말처럼 사이버위협은 국방부와 캐나다 군대의 최우선 과제로 인식하고 있으며, 캐나다군 사이버 부대는 군사 시스템을 방어하고 미래 사이버 부대를 구축하며 사이버 작전을 광범위한 군사작전에 통합하는 능력을 강화하고 있다.[28]

나. 사이버안보 대응 전략

캐나다의 사이버안보 전략은 2010년 CCSS(Canada's Cyber Security Strategy)에서 시작하여 2018년 NCSS(National Cyber Security Strategy)에 이르는 과정에서 독자적인 안보전략의 형태를 갖추어 갔다. 캐나다의 사이버안보 추진체계와 마찬가지로 대응전략 또한 미국과 여러 부분 유사하게 발전했다. 구체적인 실행계획에 있어서는 규범을 따르고 프라이버시 등 캐나다의 자국민을 보호하고, 사이버위협에 대응하기 위한 지속적인 개선 노력을 추구하며, 사이버 공격 발생 시 범정부 차원에서 총력 대응을 하고, 연방정부 및 주정부는 상호 협력을 강화하며, 동맹국들과의 긴밀한 협력관계 구축을 강조했다.

2010년 전략 발표 후 시행된 정책과정에서 얻어진 경험과 반성, 기술적 변화 그리고 국제정세의 변화를 반영하여 새로운 사이버안보 전략을 2018년에 발표하였다. 주목할 부분은 기존의 행위자들에 전문가, 학계, 그리고 활동 중인 시민들이 추가되었고 사이버 공간에서 증진해

28) https://defence.frontline.online/article/2017/3/7065-Cyber-Aptitude--in-the-Military(2022.11.17 검색)

야 하는 가치에 권리(rights)와 자유(freedoms)가 명시되었으며 디지털 시대에 안정적인 경제 행위를 위한 환경 조성을 위해 사이버안보가 매우 중요한 요소로 인식되었다. 또한, 사이버안보에서의 연방정부의 리더십이 재차 강조되고 구체화 되었는데 정부의 지속적인 조언과 지침 제공, 정부의 기대와 요구사항을 명확히 하기 위한 사이버안보 기준과 법제 제정, 사이버범죄 대책 마련 등을 포함하였다(유인태, 2019). 경제·사회·정치 분야에 광범위하게 구축되어 있는 핵심 정보 인프라에 대해서 가해지는 다양하고 고도화된 사이버 공격이 우려의 대상이었는데, 최근에는 온라인상의 지적재산에 대한 중국 해커들의 공격이 주요 관심사로 부상하였다. 캐나다는 미국의 전통적 군사 동맹국이며 양국은 공통적으로 중국을 최상위 사이버위협 국가로 인식하고 있다. 그럼에도 캐나다의 사이버안보 전략은 전통적인 군사안보의 차원보다는 주요 인프라가 미국과 연결되어 있다는 관점에서 볼 때 정보보호 차원에서 전략을 수립하고 있다.

캐나다는 미국·영국과 같이 사이버 공간에서의 접근성·개방성·신뢰성 등을 강조하고, 사이버 공간을 인권과 정보의 자유로운 흐름을 보장하는 방식으로 사용되어야 한다고 주장한다. 또한, UN GGE, 유럽안보협력기구(OSCE), 아세안지역안보포럼(ASEAN Regional Forum)과 같은 다자간 안보협력기구에서 형성되는 규범들을 지지하고 있다. 국제협력 차원에서는 미국, 영국, 호주 등 이른바 파이브 아이즈(Five Eyes)[29] 국가들과의 정보공유와 공조를 통해서 진행되고 있으며, UN, NATO, G8 등과 같은 서방 진영과의 다자외교의 장에서도 활발한 활동을 펼치고 있다. 캐나다는 유럽의 사이버범죄협약(Convention on Cybercrime)에 속해 있으며, 글로벌 사이버 거버넌스에도 참여하고 저개발국에 대한 사이버안보 역량 강화를 위해 계속 지원을 하고 있다. 양자 차원에서 지리적 근접성으로 미국과 협력하고 있는데 캐나다 공공안전부(PSG)가 미국 국토안보부(DHS)와 사이버안보 실천 계획(Cybersecurity Action Plan)을 수립하였다. 또한, EU와 일본과도 양자

29) 파이브 아이즈(Five Eyes)는 미국, 영국, 캐나다, 호주, 뉴질랜드로 이루어진 5개국 간의 군사 동맹 및 정보 네트워크이다. 이는 미국의 최우방국이자 가장 핵심적인 가치를 공유하는 영미권 정보기관들이 군사정보의 수집, 공유 및 활용에 관한 협력을 목표로 UKUSA 안보 협정을 맺음으로써 창설되었다.
* 5개국의 정보기관: 미국의 NSA, 영국의 GCHQ, 캐나다의 CSE, 호주의 ASD, 뉴질랜드의 GCSB

협력을 추진하고 있으며 일본과는 군사안보 차원의 협력이 아닌 기술자들 간의 정보공유 차원에서 협력이 이루어지고 있다.

5. 이스라엘

이스라엘은 오랫동안 지속되어 온 아랍권 국가들과의 군사충돌로 국가안보에 많은 인적 자원과 최첨단 장비를 투입하고 있다. 이스라엘은 사이버 공격이 단순한 분쟁 수준이 아닌 국가 존립을 위협하고 이스라엘인의 생존에 심각한 영향을 미치는 현안으로 인식하고 접근하고 있다. 이스라엘은 2000년 초반부터 정보통신기술(ICT) 영역의 사이버위협을 인지하고 세계 최초로 사이버안보 정책을 수립하였다. 특히 2010년 스턱스넷 사건 이후 이란과 시리아 등 반이스라엘 국가들이 사이버역량을 강화하고 있는 상황이 이스라엘에게는 더욱 큰 위협으로 작용하면서 사이버 국방 역량 개발의 동인으로 작용하였다.

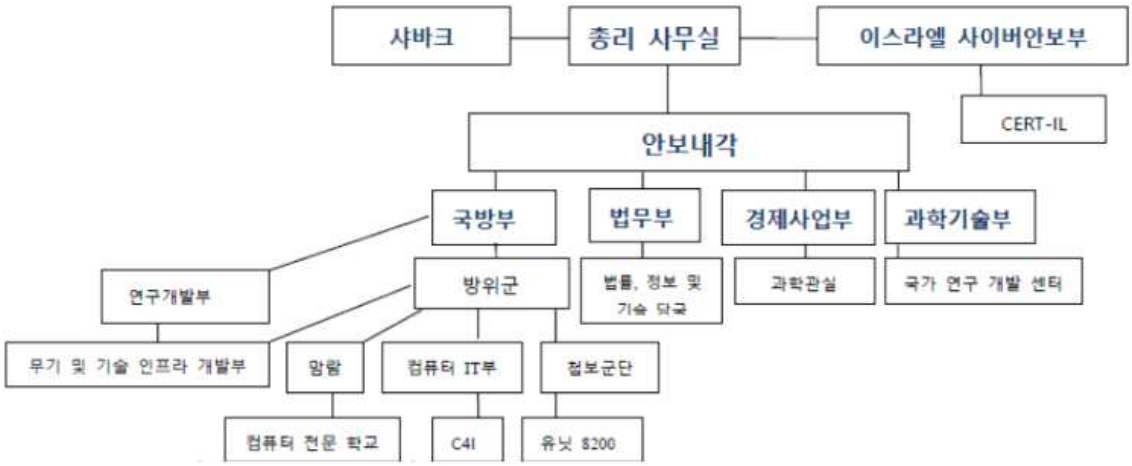
이스라엘은 사이버 국방 역량 개발뿐만 아니라 경제적 이익을 추구하는 방향으로 사이버안보를 접근함으로써 정부와 민간기업과의 연계를 통한 국가안보 확립과 경제적 번영을 동시에 얻고자 했다. 그 결과 이스라엘은 미국과 함께 세계 사이버보안 시장을 선도하는 국가로 도약하였다. 이스라엘에서는 非안보 부처일지라도 국가안보 능력 강화와 밀접하게 관련이 되어 있는데 가령 경제산업부의 사이버보안 산업 육성이나 교육부와 국방부에서의 우수한 인재 양성의 궁극적인 목적은 핵심 기술과 인적 자원을 확보함으로써 국가안보를 강화하는 데로 귀결된다.

이스라엘은 국가 존립을 인정하지 않는 아랍국가들로 인해 국제적으로 지지를 받지 못함에 따라 사이버 분야의 국제규범 논의보다는 자국의 사이버역량 강화에만 집중하는데 중점을 두고 있다. 또한, 사이버안보 분야에서 이스라엘이 취하는 국제협력 전략의 방향은 주로 미국과 친미 성향 국가와의 사이버안보 협력 및 공조하고 있으며 특히 일본·인도·싱가포르·태국 등 아시아 국가와 사이버안보 파트너로 협력하고

확대해가고 있다.

가. 사이버안보 추진 체계

사이버안보 정부 기관으로는 첩보활동을 하는 샤바크(Israel Security Agency, ISA)가 있고, 총리실 산하 사이버안보부(Israel National Cyber Directorate)가 경제산업부, 국방부 등 타 부처를 컨트롤타워하는 역할을 수행하고 있으며 사이버 공격에 대한 대응역량 강화, 사이버 기술 연구개발, 국제협력 및 대응 공조 등 사이버안보 관련 업무를 총괄하고 있다.



<그림 7> 이스라엘의 사이버안보 관련 추진체계

경제사업부(Ministry of Economy & Industry)는 사이버보안을 포함한 산업 분야 전반의 연구개발을 담당하고 있으며, 과학기술부 산하에 국가연구개발센터(National Research and Development Center)에서 이스라엘의 사이버안보 전략을 결정하는 핵심적인 역할을 수행하고 있다. 국방부 산하의 이스라엘 방위군은 군인, 일반인, 사이버 인재 등 국가 인력 양성에 직접적으로 개입하고 있어 국방부가 국정 운영에 큰 영향력을 행사하고 있다. 특히 유닉 8200은 방위군 첩보군단(Military Intelligence Corps) 예하부대로 정보 수집과 암호 해석을 담당하며 방위군 컴퓨터IT국(Computer IT Directorate) 산하의 C4I국은 네트워크 전쟁을 관할하고 있다. 맘람은 이스라엘 방위군의 정보통신기술 네트워크 전반을 담당하고 있는데 사이버 분야에 관심 있는 군 인력을 대

상으로 하는 교육하는 컴퓨터전문학교(School of Computer Professionals)를 운영하고 있다. 국방부 산하 연구개발부(MoD Directorate for Research and Development)는 사이버 무기를 포함한 국방 관련 기술을 선정하고 새로운 무기체계를 군에 제공하는 임무를 수행하고 있다.

나. 사이버안보 대응 전략

이스라엘은 2000년대 이전부터 공군과 정보기관의 정보수집 활동의 목적으로 사이버 공간을 활용하기 시작하였다. 이후 국가 주요 인프라 시설과 민간이 사이버위협에 노출되면서 본격적으로 사이버안보 전략의 필요성이 강조되었다. 2002년 이스라엘 최초의 사이버안보 전략인 특별 결의 B/84(Special Resolution B/24)가 채택되었고 반이스라엘 국가에 의한 인프라 테러 위험이 커짐에 따라 샤바크(Israel Security Agency)를 사이버 영역에서의 안보를 전담하게 하였다.

이후 2010년 스턱스넷 사건으로 인해 이란·시리아 등 중동국가가 사이버 전력과 공격적 역량을 강화하는 등 군사 경쟁이 벌어지면서 결국 이스라엘도 군사적 차원에서 사이버안보 역량 강화에 투자하기 시작했다. 2010년의 국가 사이버 이니셔티브(정부 결의 3611호)를 발표하고 사이버 영역에서의 군사 역량 강화와 5년 내 사이버 강국 반열에 오르는 것을 정책 목표로 제시하였다. 이를 위해 군사 기술 영역에서 사이버안보 담당 기관 설립 필요성이 인정되면서 국가사이버국(Israel National Cyber Bureau, NCB)이 설립되고, 민간 분야의 사이버안보를 담당하는 국가사이버안보국(National Cyber Security Authority, NCSA)이 신설되었다. 이후 사이버안보 추진체계 일원화를 위해 2017년 국가사이버국과 국가사이버안보국이 통합되어 군사와 민간 영역을 아우르는 사이버안보 담당 기관인 이스라엘 국가사이버안보부(Israel National Cyber Directorate)가 창설되고 운영되고 있다.

국방전략 차원에서 보면, 주요국가 인프라 전반에 사이버 공간이 차지하는 비중이 커지고 의존하게 되면서 이스라엘에게는 물리적 공격 없이 사이버 공간을 통해 적국의 인프라를 파괴할 수 있다는 인식이

확산되었고 이스라엘 군사 내에서 사이버 영역의 중요성은 꾸준히 증가하였다. 이라스엘은 사이버를 제5세대의 전쟁영역뿐만 아니라 미래전에 있어 사이버전이 군사적 우위를 가져올 수 있는 핵심요소로 인식하였고 사이버군의 존재와 사이버역량 개발은 군사력 강화에 있어서 필수적인 기능으로 여겨지게 되었다.

이러한 결과로 이스라엘은 미국에 버금가는 사이버안보 강대국으로 발전했으며 이러한 사이버역량을 바탕으로 국가 간의 양자 협력이 활발히 진행되고 있다. 특히 미국과는 2018년 사이버 공격이 발생하였을 때 국가 주요 인프라를 보호하고 공격행위자를 추적하며 사이버 공격 공동 대응팀을 설립하고 보안 솔류션도 공유하는 등 사이버 영역에서의 협력을 강화해 가고 있다. 미국과의 협력 이후에 이스라엘이 다른 친미 성향의 국가와도 사이버안보 협조체계를 구축해 가고 있는데 특히 일본과는 사이버보안 연구와 정보공유를 위한 양해각서를 체결하기도 하였다. 또한, 인도, 싱가포르, 태국 등 아시아 국가와 사이버보안 솔류션(solutions) 등 사이버 관련 수출을 통한 사이버안보 파트너로 협력하고 확대해가고 있다.

제3절 한반도 주변국 대응 전략

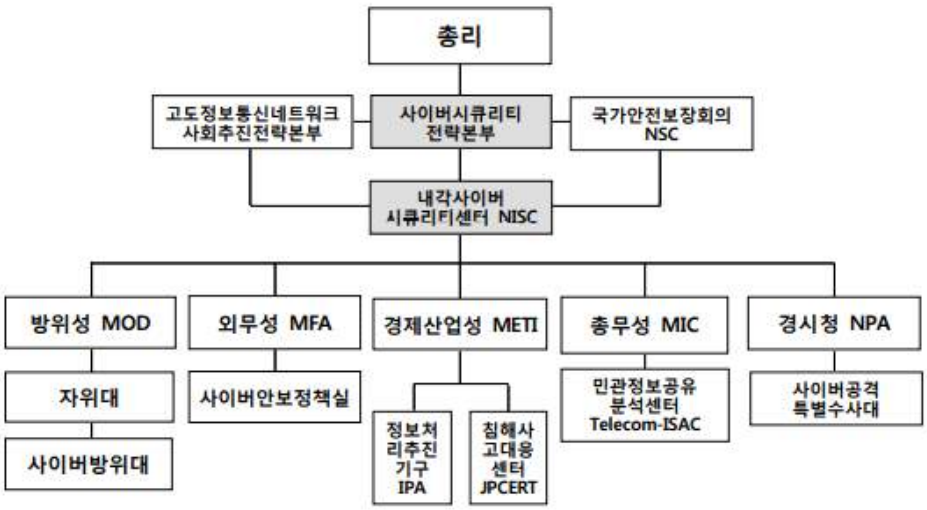
1. 일본

2010년대 들어서면서 일본의 사이버안보 전략은 점증하고 있는 사이버위협을 중대한 국가안보 위협으로 인식하고 국가안보의 차원에서 적극적으로 대응하는 선제적이고 주도적인 정책으로 전환하고 있다. 2013년 6월「사이버시큐리티전략」발표 이후 기존의 정보보호 전략에서 사이버안보 전략으로 설정하고 변화를 강조하고 있다. 사이버 국방전략의 차원에서도 사이버안보가 동북아 지역 안보의 핵심 사안으로 부상했음을 인지하고 일본 방위성과 자위대는 사이버 공격에 대응하는 군사적 역량 강화를 추진하고 있으며, 자위대 산하에 사이버 방어를 감독하는 사령부를 창설하여 사이버 방위 부대(CDU)를 지휘하고 사이

버 방위 인력도 천명 수준까지 증원하고 있다. 또한, 자국의 정책만으로는 감당하기 벅찬 위협에 대응하기 위해 타정부와의 협력을 통한 공조체계 구축, 국제법에 근거한 대응체계 마련에 노력하면서 특히 우방인 미국과의 국제협력을 강화하고 양자 협력이나 다자외교를 추진하고 있으며 아세안 지역 국가들과의 협력에도 주력하고 있다.

가. 사이버안보 추진 체계

내각사이버시큐리티센터(NISC)는 사이버안보 전략 초안을 작성하고 정부 사이버 정책에 대한 제안을 하며 내각관방에 보고서를 제출하는 등 정부 차원의 사이버안보 정책에 대한 조정과 통제하는 컨트롤타워의 역할뿐만 아니라 정부 정보시스템을 모니터하여 사이버위협을 감시·분석·대응하는 역할을 담당하고 있으며 국제협력 업무도 수행하고 있다.



<그림 8> 일본의 사이버안보 관련 추진체계

개별 정부부처 차원의 업무를 보면, 방위성과 자위대는 군사 관련 사이버 정책, 외무성은 사이버 국제협력, 경제산업성은 정보통신기술 관련 산업정책, 총무성은 통신 네트워크 정책, 경시청은 사이버 범죄 정책 등의 분야를 담당하고 있다. 특히 경제산업성 산하에 설치된 정보처리 추진기구(IPA)는 사이버보안 강화, 정보시스템의 신뢰도 제고, 전문인력 육성 등 사이버역량 강화에 초점을 두고 업무를 수행하고 있

다. 일본 방위성과 자위대는 사이버 공격에 효과적으로 대응하는 군사적 역량 강화를 위해 육상, 해상, 항공자위대 소속 사이버 전문인력과 사이버안보 컨트롤타워의 역할을 담당하는 내각사이버시큐리티센터(NISC)의 전문인력이 파견된 사이버방위대를 창설하고 운용하고 있다. 사이버방위대는 육·해·공 자위대별로 별도 운영하고 있던 사이버 방어부대를 통합하여 방위성 예하 자위대 지휘통신시스템대대 예속 부대로 편성·운영되고 있으며 방위성과 자위대의 네트워크 시스템을 항시 감시하고 사이버 공격 발생시 신속한 대응과 위협정보를 수집하고 조사하는 등 사이버 관련 정보활동을 총괄하고 있다.

나. 사이버안보 대응 전략

일본의 사이버안보 전략은 2014년 사이버안보기본법의 제정을 통해 사이버안보 정책의 기본방향이 제시되었다. 이후 2015년 9월 사이버시큐리티 전략이 내각에서 처음 채택되었는데, 경제·사회적 활력 제고, 국민들의 안전한 삶을 위한 사회 건설, 국제사회의 평화와 안정 및 국가안보 확보 등 세 가지 정책 목표로 설정되었다. 이는 사이버 공간의 문제를 경제적 손실뿐만 아니라 국가안보 측면에서 군사안보 문제로 인식하고 대응하겠다는 의미를 내포하고 있다. 다시 말하면, 사이버위협을 단순히 사이버 공간만의 문제가 아닌 국가안보 전체의 위협으로 인식하고 사이버안보에 대한 대응을 집단적 자위권의 수단으로 활용하겠다는 의도이다.

일본 정부는 중국·북한·러시아의 사이버 활동이 매우 심각한 국가안보 리스크가 될 것을 강조하고 있다. 2021년 9월, 일본 정부가 사이버안보 전략을 확정했는데 주목할 점은 국가 차원에서 사이버 공격을 가해올 주체로 북한과 중국, 러시아를 처음 적시한 것이다. 이 전략은 최근 사이버 공간에서 발생하고 있는 정세와 관련해서 국가 차원의 개입이 확실히 의심되는 사이버 활동 주체로 중국, 러시아, 북한을 차례로 거론한 것이다. 또한, 모든 가능한 외교적 수단과 능력을 활용하여 단호하게 대응한다는 입장을 강조하고 사이버 분야에서 자유롭고 개방적인 인도·태평양을 실현하기 위해 중국 견제 동맹체인 '쿼드(Quad) 구성

국가와 동남아시아국가연합(ASEAN)과의 협력을 적극적으로 추진한다고 발표했다.[30]

일본의 사이버안보 협력 국제전략은 국제협력을 위한 기본 정책과 우선순위 영역을 기술하고 있는데 미국·EU 및 다자간 프레임워크와의 협력, ASEAN과의 지역협력에 초점을 맞추고 있다. 미국은 일본을 포함한 동맹국들과 집단적 사이버 대응구축 능력을 확보하기 위해 노력해 왔고 이러한 측면에서 일본은 미국과 사이버안보 협력을 다양한 수준에서 진행하고 있다. 미·일 사이버 대화, 미·일 인터넷 경제에 대한 정책협력대화, 미·일 사이버 방위 정책 워킹그룹 등을 통해 사이버 정책 및 정보공유, 사이버 사고 대응 및 인적개발 협력, 자위대와 미군의 협력 강화를 모색하고 있다. 또한, 일본은 ASEAN 국가들과 지역 전략적 파트너를 형성하고자 노력하고 있는데 일·ASEAN 정보보안정책회의, 일·ASEAN 정보보안 훈련, 일·ASEAN 사이버범죄 대화 등을 통해 중국에 대한 공동대응 체제를 구축하고 사이버 공격에 대비한 공동훈련을 실시하여 사이버 방어 능력을 제고하고 있다. 호주와는 미국과의 삼각 안보 사이버 협력을 통해 중국의 사이버위협에 대응하고 아태지역 국가들의 사이버역량 강화를 지원하고 있다. 사이버안보 위협이 초국가적으로 발생하는 만큼 다자 차원의 사이버안보 협력도 이루어지고 있는데 UN, OECD, APEC 등 국제기구와 다자 안보협력 기구 등 국제적 논의에 적극 참여함으로써 국제적 규범 형성에 주도적인 역할을 하려는 의도를 보여주고 있다.

2. 중국

중국은 미국과 국제질서의 수립과 운영에 있어 주도권을 경쟁하는 강대국이다. 그러나 중국은 아직까지 군사력 전반에 있어서 미국에 열세이기 때문에 이것을 극복하기 위한 수단으로 사이버 정보망에 일찍부터 투자를 해왔다. 중국은 사이버전에 매우 적극적인 모습을 보이고 있는데, 美국방부가 연례적으로 발표하는 '중국 군사력 보고서'에 따르

30) 연합뉴스, 「일본, 사이버 공격 주체로 북중러 첫 명기 보안전략 마련」, 2021.

면 중국은 2007년 이후 사이버 네트워크 공격 및 방어를 위한 대책 수립에 많은 노력을 기울이면서 투자를 아끼지 않는다고 한다.(임종인, 2013)

중국의 사이버안보 전략 및 정책은 1990년 후반부터 시작된 금순공정(Golden project)부터 시작되었으며 정보 검열 및 감시 체계 구축을 위한 통제에 집중되어 있다. 중국의 사이버안보 전략은 국내 핵심 인프라에 대한 사이버위협뿐만 아니라 집단지도체제의 안정과 미국의 기술패권에 대응하기 위한 방어적 성격을 띠고 있다. 그러나 시진핑 체제가 들어서면서 사이버 공격에 대한 보복공격이 포함된 적극적 사이버 방어 전략으로 바뀌고 있으며, 이는 사이버 공격을 군사작전 수단으로 활용하고 해커부대·전자전부대·사이버사령부(인터넷기초총부) 등 사이버전을 담당하는 사이버 부대 창설을 통해 가시화되었다. 중국은 「사이버 안전법」 제1조에 사이버 공간 주권 수호를 목적으로 한다고 명시하고 있듯이 사이버 주권의 중요성을 강조하면서 사이버안보 정책을 추진해 나가고 있는데 사이버 공간에서 국가이익과 주권을 수호하며 사이버 공간의 발전과 안전을 추구해 나갈 것임을 밝혔다.[31]

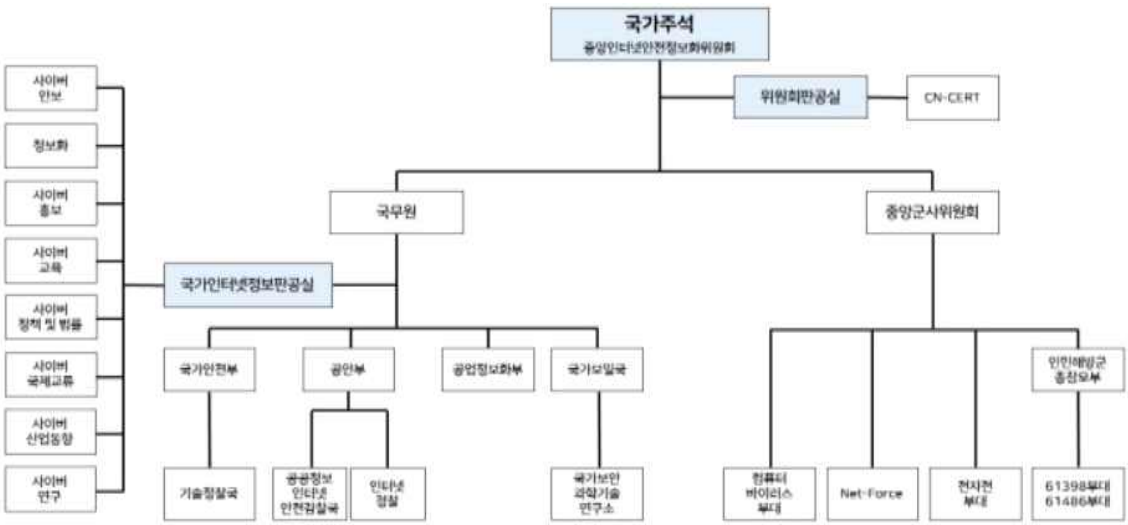
중국이 추진하는 국제협력 전략의 기조는 미국이 주도하는 글로벌 거버넌스의 질서 구축에 견제하는 중국 주도의 사이버 진영을 새롭게 구축하는 것을 목표로 국제협력을 모색하고 있다. 또한, 중국의 입장에 동조하는 국가들과 상하이협력기구(SCO)나 세계인터넷대회(WIC) 등 지역협력과 UN 등 국제기구 활동에도 적극적으로 나서고 있다.

가. 사이버안보 추진 체계

중국의 사이버안보 추진체계의 가장 큰 특징은 국가 주권 및 체제 수호를 목적으로 중앙으로 권한이 집중된다는 것이다. 국가주석이 총괄하는 중앙인터넷안전정보화위원회가 중앙 컨트롤타워로 사이버안보와 인터넷 단속을 총괄하고 있으며, 국무원 산하에 국가인터넷정보판공실이 인터넷 정보 관리 강화를 위해 사이버와 관련 있는 정부 부처

31) 체제병 외, 「주요국 사이버안보 전략과 한국에의 시사점」, INSS전략보고, 2020.

들을 지도·감독하고, 인터넷 뉴스 검열 관련 제품 또는 서비스에 대한 허가 및 감독권을 갖고 있다. 국가안전부는 정보 및 보안 기관으로 국내적 차원의 사이버안보 업무를 총괄하고 산하의 기술정찰국에서 사이버안보 정책을 수립하고 있다. 또한, 공안부는 범죄 활동을 예방하고 단속하는 업무를 수행하고 있으며 산하에 인터넷 경찰이 사이버 범죄를 전담하고 인터넷 반체제 활동에 대한 감시활동을 하고 있다. 공업정보화부는 국가 정보화 시스템 구축을 총괄하며 산하의 침해사고대응센터가 민간 분야에 발생하는 사이버 침해사고를 조사하고 대응한다. 국가보밀국은 정부 내부 문서 및 자료, 컴퓨터 등의 보안을 책임지는 정부 기구로 보안정책 수립 및 감사, 지도 감독 등 보안 업무 전반을 관장하고 있다.



<그림 9> 중국의 사이버안보 관련 추진체계

중국은 사이버안보의 강화 필요성 인식하에 2010년 이전까지 분산적으로 운영하던 사이버 부대를 사령부급에 해당하는 인터넷기초총부로 통합하였다. 이 부대는 미국의 사이버사령부(USCYBERCOM)에 해당하는데 인민해방군 산하 총참모부의 제3부 소속으로 육·해·공군의 사이버사령부를 총괄한다. 또한, 2016년에는 군구조 개혁을 통해 사이버군이 포함된 전략지원부를 창설하여 정보수집, 사이버 공격 및 방어, 심리전 등을 수행하는 등 사이버안보에서 軍의 역할이 격상되었음을 알 수 있다.

미국 정보 당국에 따르면, 중국의 인민해방군 사이버 부대는 18만 명 이상 규모로 추산하지만, 민간 및 학계 등 비공식적인 인원까지 고려한다면 40만 명 이상으로 추정된다. 또한, 사이버예비군으로 활동 중인 '중국홍객연맹(HUC)'이라는 막강한 민간 해커를 보유하고 있는데 조직원의 수는 14만 명으로 추산되고 있다. 이 조직은 해커집단이면서 친정부 노선을 타고 있어 중국 정보 당국의 묵인 아래 모든 국가를 대상으로 무차별적인 사이버 공격을 감행하고 있다. 특히 2001년 4월에 발생한 미·중 사이버 전쟁을 통해 전 세계에 존재를 과시한 이후 한국, 일본, 대만, 미국 등을 대상으로 마구잡이로 해킹을 감행하는 사이버 극우 조직으로 알려졌다.[32] 또한, 이러한 해커집단과 달리 최대 800만 명으로 추산되는 이른바 '사이버 의용군(Cyber Militias)'이 있는데 이들의 주요 임무는 국가 긴급훈련의 일부로서 군사훈련에 참가하고 인민해방군의 사이버전에 관련된 인력이나 연구를 위한 훈련 임무를 수행하고 있다.

나. 사이버안보 대응 전략

미·중간의 패권경쟁은 대내·외적으로 사이버위협을 증가시켰고, 사이버안보 전략 수립의 필요성을 증대시켰다. 2015년 전국인민대표회의에서 새로운 국가안전법이 통과되면서 사이버 공간에서의 국가안보 강조와 주권 수호 활동의 명분을 마련하는 등 사이버 공간에 대한 감독 강화를 명문화하였다. 2016년에는 '인터넷안전법' 제정을 통해 중국 정부의 인터넷 검열 및 정부 당국 개입을 명문화함과 동시에 제품과 서비스에 대한 규제를 공식화하고 사이버 공격을 군사작전으로 다루는 군사전략을 통해 정보 검열 및 감시 중심의 소극적 방어에서 사이버 공격에 대한 보복공격까지 포함하는 적극적 방어 수준으로 사이버안보 개념이 확대되었다(김진형, 2022). 2016년 12월 중국의 사이버안보 정책을 전면에 내세운 최초의 전략서인 「국가사이버공간안보전략」을 발표하였는데 이 전략서는 사이버 공간에서의 국가 주권의 중요성을 강조하면서 국가안보 수호, 핵심 정보인프라 보호, 건전한 사이버 문화 조성, 사이버테러 및 범죄 단속, 사이버 관리체계 구축, 사이버보안 강화,

32) 보안뉴스, 「사이버 전쟁을 주도하는 국가정보기관 : 중국」, 2020.

사이버 방어능력 향상, 그리고 사이버 국제협력 강화 등 사이버안보 이념과 정책을 명시하고 있다.

중국이 추진하는 사이버안보 분야 국제협력 전략의 기조는 사이버 주권 수호와 내정불간섭의 원칙을 기반으로 미국이 주도하는 글로벌 거버넌스의 질서 구축에 대항하는 우호적 국가들과 지역협력 및 국제연합 전선을 구축하고 자체 기준을 국제 표준으로 삼고자 하는 것이다. 사이버 안전 전략과 사이버 안전법에는 사이버 공간의 국제협력을 전략 임무 중 하나로 제시하고 있으며, 2014년 최초로 중국 우전에서 세계인터넷대회(World Internet Conference)[33]를 개최하고 각국의 사이버 주권을 강조하며 안전한 사이버 공간의 활용을 위한 국제협력을 강화했다. 2017년 3월 시진핑 주석은 사이버 공간에 대한 최초의 대외 전략인 '사이버 공간 국제협력 전략'을 발표하였는데 사이버 공간의 주권을 강조하고, 사이버 기술의 표준화를 통해 사이버 거버넌스를 주도하겠다는 구상을 밝힌 바 있다. 중국은 상하이협력기구(Shanghai Cooperation Organisation, SCO), 아세안지역안보포럼(ASEAN Regional Forum, ARF) 등 지역 내 협력기구에서의 적극적 논의를 통해 영향력을 확대했을 뿐만 아니라 국제연합 GGE나 국제전기통신연합(ITU) 등과 같은 국제기구에서 진행되는 국제규범 수립과정에도 적극적으로 참여하고 있다. 앞으로도 상하이협력기구(SCO)나 국제전기통신연합(ITU)에서의 국제적 소통을 증가시켜 미국의 영향력이 강한 글로벌 사이버 안보 거버넌스를 견제하는 지역적 네트워크를 구축할 것으로 보인다.

3. 러시아

러시아 사이버안보 전략의 기본방향은 정보의 자유롭고 개방적인 공간보다는 러시아의 국가 주권을 확보하는데 집중되어 있다. 러시아는 2010년 미국과 이스라엘이 스턱스넷으로 이란의 핵 시설을 공격한 이후부터 본격적으로 사이버안보에 관심을 가지기 시작했다. 2010년대

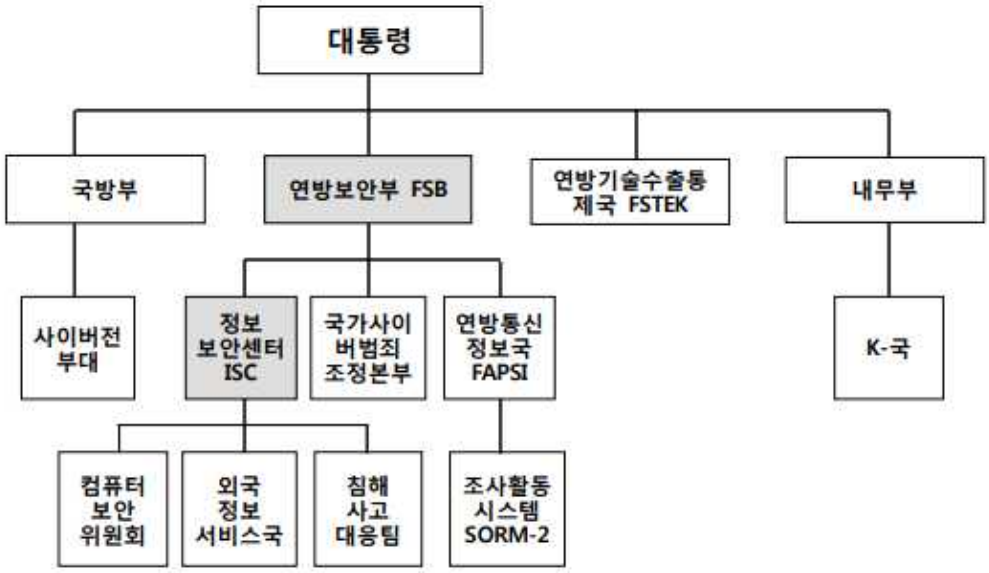
33) 세계인터넷대회(WIC: World Internet Conference)'는 중국이 인터넷 강국의 위상을 높이기 위해 유치한 국제회의로 중국 국가 인터넷정보판공실 주최함. 2014년 11월에 처음 개최되었으며 인터넷 거버넌스, 모바일 인터넷, 전자상거래, 보안 등 다양한 분야에 걸쳐 토론이 진행됨

들어서면서 사이버 환경의 변화에 따라 국방전략과 관련된 사이버안보 대책들을 강조하는 방향을 변화하고 있다. 특히 다른 국가에 비해 사이버 부대의 운영이나 사이버사령부의 창설 논의 등이 일찍부터 시작되었고 보다 적극적이고 공세적인 대책들을 마련하고 있다.(신범식, 2020)

러시아의 사이버안보에 대한 전략과 정책들은 미국 등 서방국의 사이버안보와 뚜렷이 구분되며 독자적이다. 러시아는 미국 등 서방국들의 사이버안보와 관련된 인식과 접근방식에 동의하지 않으며 사이버 공간에서도 국가 주권이 존중되어야 한다는 입장이다. 러시아의 이러한 독자적인 태도는 미국의 사이버 패권에 대한 강한 거부와 저항에서 시작되었는데 사이버 공간에서 자유롭고 개방적인 정보의 흐름을 보장하려는 미국의 인터넷 확장 정책은 러시아의 정치사회체계를 위협하는 행위로 받아들여진다. 국제협력 차원에서 보면 러시아는 UN GGE와 같은 기존의 국제기구 활동이나 우호세력 확보를 위해 지역 협력체를 활용하여 사이버안보 국제질서를 주도하고자 노력하고 있다.

가. 사이버안보 추진 체계

러시아의 연방보안부(FSB)가 사이버안보 관련 기관을 총괄하면서 국가 비밀을 포함한 주요 정보 통제와 범죄예방 조치뿐만 아니라 관련 기관에게 기술 및 암호 서비스를 제공한다. 연방보안부(FSB) 산하 정보보안센터(Information Security Center, ISC)는 정보통신 보안 및 정보보호 업무를 총괄·조정하고 침해사고대응팀(ISC)를 운영하며 비밀리에 공격기술 개발 및 각급 정보수집 업무도 담당하고 있다. 또한, 연방보안부(FSB) 산하에 국가사이버범죄조정본부는 러시아 연방기관들의 인터넷 홈페이지 보안을 담당하고 있는 것으로 알려져 있다. 연방통신정보국(Federal Agency of Goverment Communications and Information, FAPSI)에서는 러시아 내의 인터넷 서비스망을 통해 광범위한 정보를 수집하고 있고, 연방기술수출통제국(Fenderal Service for Technical and Export Control, FSTEK)에서는 국가정책의 시행과 부처 간 정책조정 및 협조, 정보보호 문제 등에 대한 통제 기능을 수행하고 있다.



<그림 10> 러시아의 사이버안보 관련 추진체계

러시아는 2002년 세계에서 처음으로 해커부대를 창설하였고, 2022년 4월 이미 3,000여 명 이상의 사단급 병력 편제를 갖고 있다고 전해지고 있다. 또한, 정확한 규모는 알려지지 않고 있지만, 러시아 군사작전 내 사이버전을 전담할 수 있는 인력은 정규 조직을 비롯해 민간 해커 그룹까지 포함하면 최대 5만 명 규모가 될 것으로 알려져 있는데 그동안 사이버 전문인력의 양성과 기술개발을 적극 추진하면서 물리적 전쟁을 위한 지원역량으로 그들을 활용해 오고 있다.

나. 사이버안보 대응 전략

러시아의 사이버안보 전략의 기본방향은 정부의 통제하에 핵심 정보기반시설 보호와 함께 네트워크를 통한 정보를 보호하는데 목표를 두고 있다. 사이버 공간에서 자유로운 정보의 흐름을 강조하는 서방국가와 달리 무분별한 정보의 유입을 방지하고 러시아에서 발생한 정보가 해외로 나갈 때 정부 검열을 거치도록 하고 있다. 이러한 러시아의 정책이 서방국가들과 대립하는 핵심적인 요소이며 사이버 국제규범의 확립과 사이버 공간의 질서 구축을 두고 국제사회 내 심각한 갈등의 원인이 되고 있다.

러시아는 또한 2004년 UN 내에서 사이버안보 분야의 정부간 협의체인 정부 전문가그룹(Group of Government Experts, GGE)을 구성하여 사이버 공간에서 국제 평화와 안보 문제를 다루기 위한 논의를 시작하였고, 2018년에는 UN 내에 개방적 워킹그룹(Open-Eneded Working Group, OEWG) 구성을 제안하여 사이버 공간에서의 국제규범 형성, 신뢰 구축, 역량 강화 활동 등에 관한 논의를 UN 全 회원국으로 확대시켰다.

국제협력에 있어서는 국제연합(UN) 등 기존의 국제기구나 집단안보조약기구(CSTO)[34], 상하이협력기구(SCO), 독립국가연합(CIS)[35] 등과 같은 지역 협력체의 틀을 활용하여 주권 국가들이 협의하는 사이버안보 질서 구축을 모색하고 있다. 이외에도 미국이라는 위협에 맞서기 위해 러시아는 브릭스(BRICS) 국가들과도 사이버안보 협력 강화와 사이버 범죄 대응을 위한 네트워크 정보보안 행동 준칙 마련 등 사이버 협의를 진행해 왔으며, 유럽안보협력기구(OSCE)나 아세안지역안보포럼(ARF)의 사이버안보 협의에도 적극 참여하고 있다. 중국과는 2015년 사이버안보 협약을 체결하는 등 협력을 지속적으로 추진하고 있다.

제4절 주요국들의 사이버 대응 전략이 주는 시사점

최근 사이버 공격이 국가안보의 문제로 인식되면서 이에 대응하는 사이버안보 전략이 군사, 외교, 정치, 사회 등을 아우르는 총체적인 국가전략으로 이해되고 있다. 또한, 지속적으로 발전하는 복잡한 사이버 공간에서의 각종 위협은 과거와 같은 획일적인 수준을 넘어서는 새로운 개념의 안보 거버넌스를 요구하고 있다.

앞에서 살펴본 국가들의 사이버 안보전략을 살펴보면 몇 가지 공통

34) 집단안보조약기구(Collective Security Treaty Organization (CSTO)는 2002년 10월 7일에 창설된 옛 소련의 공화국 6개국(러시아, 아르메니아, 카자흐스탄, 우즈베키스탄, 타지키스탄, 키르기스스탄)의 집단안전보장 조직

35) 독립국가연합(獨立國家聯合, Commonwealth of Independent States)은 소련 해체로 인해 독립국가가 된 구 소련 공화국들의 연합체로서 결성된 국제기구

점을 발견할 수 있다. 첫째, 전 세계 국가들이 진화하는 사이버위협의 이슈를 국가안보의 관점에서 바라보고 이에 대한 대비책을 새로운 대응전략을 통해 더욱 강화하고 있다는 것이다. 사이버안보 문제를 단순한 안보 차원이 아니라 군사화하는 경향이 있는데 군 차원의 사이버역량 강화, 사이버사령부와 같은 사이버 작전 수행 부대의 창설과 사이버 자위권 차원의 대응, 사이버위협에 대한 사후적 반응이 아닌 선제적이고 공격적인 대응전략 수립 등에서 확인될 수 있다.

전 세계 국가들의 사이버안보 전략 측면에서는 차이가 있는데 개인, 학계 전문가, 민간기업, 시민사회 등 민간 주도로 기술·경제적 논리를 바탕으로 지적재산 및 사회적 권리 보호를 위한 글로벌 매커니즘을 지향하는 이른바 '글로벌 사이버 거버넌스 프레임'의 국가들이 있는가 하면 국가 주권의 논리를 앞세워 국내체제의 안전을 고수하려는 '국가주권 프레임'을 강조하는 국가들이 있다. 다시 말하면 미국과 영국으로 대변되는 서방 진영의 프레임과 중국과 러시아로 대변되는 비서방 진영의 프레임의 대립 구도를 나타내고 있다. 사이버안보 국제협력과 외교전략의 추진이라는 관점에서 주변 국가들과의 공조체제를 어떻게 구축하고 있으며, 지역 차원의 국제협력에는 어떻게 참여하고, 더 나아가 글로벌 차원의 국제규범 형성과정에 대해 어떠한 입장을 취하느냐의 문제도 사이버안보 전략에 차이가 나타난다. 미국이 주도하는 사이버안보 동맹전략이나 유럽연합 차원의 국제협력, 중국과 러시아가 주도하는 지역협력으로 구분되어질 수 있다.

앞에서 살펴본 국가별 사이버안보 전략이 우리에게도 일종의 모델로서의 의미가 있을 수 있으나 그 어느 나라도 우리가 그대로 모방할 수 있는 벤치마킹의 사례로 볼 수는 없다. 각국의 정치, 사회, 문화와 직면해있는 사이버위협의 유형과 국제안보 상황이 서로 다르기 때문이다. 우리의 사이버안보의 현실은 인터넷 강국이긴 하나 북한발 사이버 공격과 중국·러시아의 사이버 공격마다 계속 증가하고 있으며 사이버 위협도는 세계적으로 유례가 없을 정도로 높아가고 있다. 또한, 글로벌 차원에서도 미·중 사이버 갈등에 따른 서방 진영과 비서방 진영의 사

이에서 국제적 쟁점에 대한 중견국 위치에서의 우리나라의 안정과 이익을 위한 외교적 주장이 쉽지 않다. 사이버안보 위협의 심각성, 국제사회의 사이버안보 노력 등 현대 사회의 안보환경 변화를 직시하고 이와 관련된 사이버 국제협력 방안이 마련되어야 할 것이다.

각국은 사이버 공격에 대한 대응을 단순한 방어 차원이 아닌 적극적 공세로 바뀌고 있으며 사이버 공격 발생시 군사적 보복공격도 포함된 강경한 태도와 의지를 보이고 있으므로 국가안보 차원에서 사이버 공격 대응체계 구축을 위한 국방부 차원의 역할이 매우 중요해 지고 있다고 볼 수 있다. 각국은 국가안보를 위협하는 사이버 공격에 효과적으로 대응하고 사이버전 수행능력을 확보하는 등 군사적 차원에서의 사이버 전문인력의 역량 강화에 집중하고 있으며 군사안보 차원에서 우방국들과의 정보공유와 기술 연구개발을 통한 국제공조 활동을 적극적으로 진행하면서 사이버 억지력을 확보해 나가고 있어 우리가 적용할 사이버 군사적 협력 모델로써 이를 추진할 필요가 있다. 또한, 사이버 공간상의 범죄 및 테러는 하나의 국가 차원의 대응으로는 한계가 있기 때문에 국가별로 양자·다자간의 협의체를 적극 추진하고 있는데 우리나라도 사이버안보를 논의할 수 있는 다자협의체를 주도적으로 마련하여 국제사회의 일원으로서 역할을 수행하고 구축된 글로벌 사이버 거버넌스에도 적극적으로 참여할 필요가 있겠다.

Ⅴ. 우리나라의 사이버안보 대응전략 및 국제협력 현황

제1절 사이버안보 대응전략

우리나라는 정보화를 통해 국가 인프라를 구축하고 경제·사회시스템을 비약적으로 발전시켰으며 행정기관을 중심으로 전자정부의 행정 효율성과 국민의 편의성을 크게 확장하는 등 사이버 내에서 삶의 지평을 확장하고 있다. 특히, 2020년에는 OECD 디지털정부 평가 1위를 달성한 바 있으며.[36] 가장 최근 발표된 국제정보화 지수별 한국 순위를 보면 ICT발전지수 2위, 전자정부발전지수 2위, 온라인 참여지수 1위, 네트워크준비지수 14위를 달성하였다.[37] 2022년 9월 말 기준 국내 이동전화 가입 회선이 약 7,632만 개, 스마트폰 회선은 약 5,564만 개이며[38], 보급률은 95% 수준에 달하는 등 정보통신 인프라는 세계 최고 수준이다. 이러한 탄탄한 인터넷 인프라를 기반으로 현재 산업·행정·국방 등 국가·사회 전반으로 정보화가 확산되고, 정부와 기업, 개인 등 모든 경제활동 주체의 기반이 사이버 공간으로 확대되었다.

그러나 한국 사회가 사이버 공간에 대한 의존도가 높아지면서 해킹과 악성코드를 활용한 사이버 공격 등 사이버위협은 지속적으로 증가하고 개인뿐만 아니라 기업과 공공·국가기관까지 확대되고 있으며 그 피해 규모가 대형화되고 파급효과는 장기화되고 있다. 또한, 사이버위협의 주체가 개인이나 해커집단에서 테러 단체나 국가 차원으로 확대되고 있다. 특히 북한은 비대칭 전력 확보를 위해 사이버 부대를 증강하고 사이버 공격기술을 연마하고 있는데 사이버 공간을 활용한 공격에는 시·공간의 제약이 없어서 책임 추궁이 어렵다는 한계가 있어 북한은 이를 적극적으로 활용하고 있다. 김정은 집권 이후 사이버 능력은 핵·미사일과 함께 인민군의 3대 수단 중 하나로 간주되고 있으며 현재 북한의 사이버 공격 역량은 미국과 중국, 러시아에 이어 거의 세

36) 한국정보화진흥원, 「2020 국가정보화백서」, 2020
37) 국가정보원 등, 「2021 국가정보보호백서」, 2021.
38) 과학기술정보통신부, 「무선통신서비스 통계 현황(2022.9월말 기준)」, 2022.

계 최고 수준인 것으로 평가받고 있다. 김정은 또한 사이버전을 “핵·미사일과 함께 우리 인민군대의 무자비한 타격 능력을 담보하는 만능의 보검”으로 부를 정도로 군사작전의 중요한 영역으로 간주되고 있다. 최근까지도 북한은 금융정보 탈취나 국가기밀 유출을 위해 세계 각국의 정부, 금융권, 군사시설 및 방위산업업체 등을 대상으로 사이버 공격을 광범위하게 시도하고 있다.(김보미, 2021)

국방부가 발간한 ‘2020 국방백서’에 따르면 현재 북한은 약 6,800명 수준의 사이버 전사를 운용중인 것으로 추산된다. 북한은 국가 차원에서 체계적으로 사이버 전사를 대량으로 양성하고 사이버 부대를 운영한다. 북한이 사이버 부대(전자전부대)를 창설하기 시작한 것은 1986년부터이다. 김정일 국방위원장의 지시로 군 지휘자동화대학(2000년 김일군사대학으로 명칭 변경)이라는 사이버 인력 양성 기관이 신설하면서 사이버 전사 100여 명을 배출한 것이 시초이다. 1991년 걸프전에서 전자전의 중요성을 인식하고 북한군 총참모부 직속으로 지휘자동화국과 각 군단에 전자전연구소를 창설했다. 1995년에는 100여 명 수준의 중앙당 35호실 기초자료조사실을 만들어 해외 국가기관, 단체, 개인에 대한 기밀자료를 인터넷을 통해 해킹했으며, 1998년 사이버전 부대인 사이버전지도국(121국)을 창설해 남한에 대한 사이버테러와 공격, 인터넷 대란 작전을 총괄하게 하고, 1999년 200여 명 수준의 적공국(204소)를 설립해 국군과 남한의 청소년, 일반인을 대상으로 사이버심리전을 펼치기 시작했다. 2004년 중반부터는 중국 단둥에 비밀 거점을 두고 사이버 부대 공작원들을 운영하였으며 2010년 정찰총국[39]을 창설하고 사이버 부대(121국) 병력을 500명에서 3000명으로 증강시켰다. 2012년에는 전략사이버사령부를 창설해 병력을 이전 2배 수준인 6,000명으로 확대하였다.

39) 정찰총국은 2009년 노동당 작전부와 35호실, 인민무력성 정찰국을 통합하여 설립되었으며 현재 육·해상 정찰국(1국), 정찰국(2국), 기술정찰국(3국(기술국)), 해외정찰국(5국(구 35호실)) 등 총 6개국으로 구성. 이중에서 기술정찰국이 사이버지도국, 121국 등으로 통칭되고 있음

<그림 11> 북한의 사이버 관련 추진체계

북한과 연계된 것으로 의심되는 대부분의 사이버 정보작전은 정찰총국의 6개국 가운데 하나인 일명 '121국'('사이버전지도국')에서 관할하는 것으로 추정한다. 북한의 사이버 공격 유형을 분석해 보면, 북한 최고 존엄 수호, 사이버전을 대비한 군사적 목적, 은행 및 금융권 대상 외화벌이 목적, 댓글선동 등을 통한 대남공작 목적, 최신 국방 및 자연과학기술 탈취 목적 등에 의해 감행된다.(김진광, 2020)

북한 해킹조직은 크게 라자루스(Lazarus), APT38과 블루노로프(BlueNorOff), APT37과 김수키, 안디리엘(Andarial) 등으로 구분할 수 있다.[40] 라자루스(Lazarus)는 2007년에 창설된 북한 정찰총국 소속의 해킹 단체로 바이러스와 랜섬웨어를 통해 주로 정부, 금융, 방송 분야를 공격해 왔는데 우리 정부와 軍의 컴퓨터를 감염시킨 후 군사기밀을 빼내 간 해킹 사건의 주범이다. APT38은 라자루스 해킹그룹의 산하조직으로 북한 내 다른 해킹조직과 정보공유를 통해 북한 정권을 위한 자금 마련 임무를 수행하고 있으며 전 세계 은행을 대상으로 해킹을 시도하고 있다. 김수키는 2012년 한국·미국 등에 대한 사이버 공격을 목적으로 만들어 졌으며 라자루스와 함께 북한 해킹조직 가운데 가장 활발하게 활동하는 조직이다. 주로 한국·일본·미국을 대상으로 국내 외

40) 'APT'는 지능형지속위협을 뜻하는 약어로 글로벌 보안업체 파이어아이가 명명하는 방식. 보안업체에 따라 블루노로프를 라자루스로 통합해 부르기도 함.

교 및 국가안보 기밀 등에 대해 지속적인 공격을 시도하고 있는데 2014년 한국수력원자력 해킹 사건의 주범으로 확인된 바 있다. 안다리엘은 라자루스의 하위 조직으로 국내 언론·금융·방산·네트워크 업체 등을 대상으로 데이터 탈취 및 삭제 등의 공격을 자행하며 2021년 초부터 공격 시도 정황이 활발하게 탐지되고 있다. 주로 한국 국방·우주 관련 업체에 대한 사이버 공격이 안다리엘에 의해 이뤄지고 있고 있다. 이러한 북한의 해커들은 대부분 중국, 인도, 러시아, 벨라루스, 말레이시아 등 해외에서 활동하고 있다.[41]

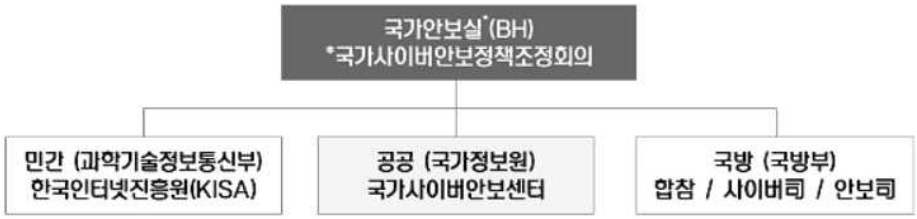
<표 5> 북한 해킹조직별 개요

해킹조직	공격대상	목 적
라자루스(Lazarus)	정부, 금융, 방송	사회적 혼란, 정보 탈취, 금전 이득 등
APT38	전 세계 금융 산업, 암호화폐거래소, 스위프트(SWIFT)	
스카크러프트(APT37) &김수키	탈북자, 정치인, 통일 관련 연구원 및 정부기관, 금융사 특정업무 담당자	
안다리엘(Andarial)	국내 금융, 방산, 민간 기업, 보안솔루션 업체, 정부기관	

북한 이외에도 우리의 사이버 공간은 사이버 공격의 주요 근원으로 식별되고 있는 세계 최대의 해커조직을 보유한 중국발 사이버 공격에 노출되어 있는 상황이며, 국제적인 민간 헤커집단 등 국제 사이버테러 조직의 공격을 받을 가능성도 크게 증가하고 있다. 이렇듯 사이버 공격의 증가에도 불구하고 공격 시도에 대한 징후를 미리 예측하기 어려우며 민·관·군을 총망라한 모든 정보인프라를 공격대상으로 삼기 때문에 모든 사이버 공격에 대한 방어가 어렵고 정보통신기술의 급속한 발달로 사이버 공격에 쉽게 취약할 수 밖에 없는 우리의 사이버 공간은 우리가 지켜야 할 새로운 안보영역이 되고 있다.

41) U.S. Army Headquarters, “North Korean Tactics,” July 2020, p.E-2, https://irp.fas.org/doddir/army/atp7-100-2.pdf

우리나라는 2005년부터 국가안보 차원에서 사이버위협에 대한 대응을 본격화하기 시작하였는데 청와대 국가안보실이 컨트롤타워가 되고 공공부분은 국가정보원, 민간부문은 과학기술정보통신부, 국방부문은 국방부가 각각 분담하는 종합 대응체계로 구축되어 있다.



■ 민 · 관 · 군 주관기관은 관계법령에 따라 분야별 사이버보안 업무 총괄

부처	법령	내용
과기정통부	정보통신망법, 기반보호법, 정보보호산업법	민간사업자 및 민간기반시설 사이버보안, 정보보호 산업육성
국정원	국정원법, 기반보호법	공공기관 및 공공기반시설 사이버보안
국방부	국방정보화법	국방분야 사이버보안

※ (기타) △(검 · 경찰) 수사 관련 협조 △(외교부) 국제협력 등 협조 · 지원

<그림 12> 우리나라의 사이버안보 관련 조직

먼저, 국가안보실은 사이버안보 컨트롤타워의 기능을 가지고 체계적인 사이버안보 수행체계 정립 및 능력 확보, 사이버 공간의 안전한 보호 등 실질적인 사이버안보 대응역량 강화를 추진하고 있다. 또한 「국가사이버안보전략」을 수립·시행하고 있으며 민·관·군 사이버안보 협력체계 확립을 위한 법제도 개선, 사이버위협 예방 및 대응역량 강화, 국제협력 내실화 등을 추진하고 있다.

2021년 12월 청와대가 과학기술정보통신부 등 연관 부처 간 협력 활성화를 통해 안보 관련 부처와 민간부문의 협력을 발전시키는 목적으로 국가안보실 1차장 산하 안보전략비서관이 담당해 왔던 핵심기술 관련 업무에 사이버정보비서관의 사이버안보 업무를 통합하여 '신기술·사이버안보비서관'을 신설하였다. 이를 통해 한·미간 협력을 강화하며 과학기술 역량이 우수한 국가들과 공동연구를 추진하는 등 신흥·핵심기술 연구개발 및 보호와 관련된 국제업무를 확대하는 등의 역할을 수행하면서 사이버안보 부문 정부 컨트롤타워 역할도 겸하도록 했다. 또한,

신기술·사이버안보비서관의 주요업무 중 하나는 한미정상회담 후속 조치인 한미사이버워킹그룹 운영을 비롯한 국제협력이다. 우리나라는 2022년 한미정상회담을 계기로 인공지능, 양자, 우주, 5G·6G 등 한·미 간 협력이 강화되었는데 미국 외 우수한 과학기술 역량을 보유한 국가와도 공동연구, 인적교류 확대, 정보공유 등 다방면에 걸친 국제협력이 이뤄질 것으로 예상된다.

국가정보원은 국가안보 차원에서 국가정보원 산하에 '국가사이버안전센터(National Cyber Security Center, NCSC)를 두고 국가 全 영역을 포괄하는 사이버안보 관련 정보를 수집·작성·배포하고 국가·공공기관 등 공공부문의 사이버 공격 및 위협에 대한 예방·대응업무를 수행하고 있다. 또한, 사이버안보와 관련된 정책 및 관리 업무를 총괄·조정하는 한편, 직무 수행과 관련하여 필요한 경우 국가기관이나 그 밖의 관계 기관 또는 단체에 대하여 사실의 조회·확인, 자료의 제출 등 필요한 협조 또는 지원을 요청할 수 있다.

국방부는 국방 사이버안보 정책 수립 및 수행체계를 마련하고 군 내 사이버 전문인력의 육성과 교육 훈련, 군 사이버체계의 획득과 운영, 국방정보시스템의 보호와 침해대응 및 위기관리 업무를 수행하고 있다. 또한, 사이버 공간에서 사이버 작전을 수행하기 위해 사이버작전사령부를 편성·운영하고 있는데, 사이버작전사령부는 2010년 1월 '사이버사령부'로 신설되었으며 창설 당시에 국방정보본부 예하 조직으로 두었다가 「국방개혁 307개혁」에 따라 2011년 국방부 직할부대로 개편되었다. 사이버작전사령부는 사이버전을 시행하는 최일선 부대로 국방부문의 사이버안보를 담당하고 있으며 사이버 공간에서의 사이버 작전의 계획 및 시행, 사이버 작전과 관련된 사이버보안 활동, 사이버 작전에 필요한 체계 개발 및 구축, 사이버 작전에 필요한 전문인력의 육성 및 교육 훈련, 사이버 작전 유관기관 간의 정보공유 및 협조체계 구축, 사이버 작전과 관련된 위협정보의 수집·분석 및 활용하는 등 사이버 작전과 관련된 사항 등의 임무를 수행하고 있다.[42]

42) 사이버작전사령부령(대통령령 제29561호, 1019.2.26.)

과학기술정보통신부는 민간부문 침해사고 예방·대응체계의 구축과 운영, 민간부문 주요 정보통신기반시설의 지정 권고 및 사이버위협에 대한 취약점을 종합적으로 분석·평가하며, 정보보호 관련 주요 정책 수립 및 추진 등 민간부문 정보보호에 관한 업무를 수행하고 있다. 또한, 국내 인터넷 이상 징후 모니터링과 홈페이지 악성코드 감염 등 인터넷 침해사고 동향을 파악하는 업무를 수행하고 있다. 이외에도 국가기관으로 행정안전부, 방송통신위원회, 금융위원회, 개인정보보호위원회가 있으며, 전문기관으로 한국인터넷진흥원, 한국전자통신연구원, 국가보안기술연구소, 금융보안원, 한국지역정보개발원 등이 사이버 관련 기관으로 있다.

그간의 우리나라의 사이버안보 전략은 그동안 사이버 공격이 발생할 때마다 임시 처방식 대책 마련 차원에서 이루어져 왔다. 2005년 「국가사이버안전관리규정」을 제정한 이후, 2009년 대규모 디도스(DDoS) 공격을 받고 「국가사이버 위기 종합대책」을 마련하였고, 2011년 NH농협 전산망 마비 사태로 「국가사이버안보 마스터플랜」을 발표하였으며, 2013년 3.20 사이버테러와 6.25 사이버 공격 이후에 「국가사이버안보 종합대책」과 2015년 한국수력원자력 해킹 사건을 계기로 만든 「국가사이버 안보태세 강화 종합대책」 등을 거쳐 2019년 4월 사이버 공격을 예방하고 위협을 신속히 탐지·차단하여 국가 주요기능이 안정적으로 운영될 수 있도록 국가안보실 주축으로 「국가사이버안보 전략」을 마련하였다.

「국가사이버안보전략」 수립 이전의 사이버안보 전략들이 과제 중심의 action plan 성격을 가졌다고 한다면, 「국가사이버안보전략」은 포괄적·종합적인 국가대응 체계 기반을 마련했다고 평가할 수 있다(체재병, 2019). 「국가사이버안보전략」이 수립됨으로써 대내적으로 국민들에게 안전한 사이버 공간을 제공하는 것이 가능해지고 대외적으로는 다양한 사이버위협으로부터 핵심 정보인프라를 적극적으로 예방하고 방어할 수 있는 계기를 마련했다고 볼 수 있다. 「국가사이버안보전략」 비전은 “자유롭고 안전한 사이버 공간을 구현하여 국가안보와 경제 발전을 뒷

받침하고 국제 평화에 기여"하는 것이며 전략과제로 △국가 핵심 인프라 안전성 제고, △사이버 공격 대응역량 고도화, △신뢰와 협력 기반 거버넌스 정립, △사이버보안 산업 성장기반 구축, △사이버보안 문화 정착, △사이버안보 국제협력 선도 등 6개 과제를 제시하고 있다.[43]

우리 정부는 2019년 9월 「국가사이버안보전략」을 수행하기 위한 후속조치로 범부처 차원에서 이행할 구체적인 실행계획을 수립하여 발표하였고, 각 부처별로 「국가 사이버안보 시행계획」을 수립하여 국가사이버안보에 대한 중장기 로드맵을 구축하였다. 「국가 사이버안보 기본계획」의 중점·세부과제는 아래와 같다.

[표 6] 우리나라의 「사이버안보 전략별 기본계획」의 주요내용

전략과제	주요내용	세부 과제 수
국가 핵심 인프라 안전성 제고	· 국가 핵심 인프라의 생존성과 복원력을 강화하여 어떠한 사이버 공격에도 국민생활의 기반이 되는 서비스는 중단 없이 제공 * 국가정보통신망 및 주요 기반시설 보안 강화, 차세대 보안인프라 개발	24
사이버공격 대응역량 고도화	· 사이버공격을 사전에 억지하고 상고 발생 시 신속하고 능동적으로 대응할 수 있도록 선제적이고 포괄적인 역량 확충 * 사이버공격 억지력 확보 및 대비태세 강화, 포괄적·능동적 수단 강구	28
신뢰와 협력 기반 거버넌스 정립	· 개인, 기업, 정부 간의 상호 신뢰와 협력을 바탕으로 민·관·군 영역을 포괄하는 미래지향적 사이버안보 수행체계 확립 * 국가안보실이 사이버안보 컨트롤타워 역할, 범국가 정보공유체계 구축	16
사이버보안 산업 성장기반 구축	· 사이버안보의 기반 역량이 되는 기술·인력·산업의 경쟁력 확보를 위해 보안산업 혁신생태계 조성 * 사이버보안 투자 확대, 전문인력 집중 육성, 공정경쟁 원칙 확립	14
사이버보안 문화 정착	· 국민은 사이버보안의 중요성을 인식·실천하고, 정부는 정책 수행 과정에서 기본권을 존중하고 국민 참여를 활성화 * 사이버보안 기본수칙 개발·보급, 사이버안보 관련 정보의 적극적 공개	9
사이버안보 국제협력 선도	· 국제적인 파트너십을 강화하고 국제규범 형성을 주도하는 등 사이버안보 선도국가로서의 리더십을 확보 * 국방·정보·수사 등 분야별 협력, 국제규범 정립 과정에 참여 확대	9

43) 국가안보실, 「국가사이버안보전략」, 2019.

국방부는 2019년 사이버사령부의 부대 명칭을 사이버사령부에서 '사이버작전사령부'로 변경하고 합참의장이 지휘하는 합동부대로 지정하여 작전사령부로서의 역할과 위상을 정립하였다. 동시에 사이버심리전 기능을 완전 폐지하고, 부대원의 정치개입 금지를 명문화하는 등 불법적 정치 관여를 근원적으로 차단하여 사이버작전사령부가 합동부대로서 사이버 작전에만 전념할 수 있도록 조직을 개편하였다. 또한, 합참 중심의 사이버위협 대응체계를 구축하고 효과적으로 수행될 수 있도록 합참과 사이버작전사령부, 그리고 각 군 간의 유기적인 사이버 작전 통제 및 보고체계를 새롭게 정립하였다. 아울러 국방 사이버 공간에 대한 실시간 상황인식 및 관리 강화를 위해 작전센터를 신설하고 사이버 작전 수행을 위한 정보수집과 상황판단, 결심, 대응 등 단계별 작전 수행체계를 구축하여 지휘관의 신속한 의사결정과 지휘 통제가 가능하도록 하였다. 끝으로 악성코드를 비롯한 네트워크상의 이상 행위를 식별하기 위한 탐지·분석체계를 지속적으로 고도화하고 있다.

제2절 사이버 국제협력 현황

사이버 관련 대응은 한 국가 차원의 대응만으로는 역부족임은 주지하는 사실이다. 따라서 포괄적인 사이버안보 국제협력의 필요성에 대한 인식이 확대되고 이를 위한 국제적인 움직임이 활기를 띠고 있으며, 우리나라도 이 같은 상황 인식에서 사이버 관련 이슈에 대한 국제적인 공조에 동참하고 있다.

우리나라의 사이버안보 국제협력은 국제사회의 사이버안보 논의와 유사하게 국제연합 참여, 양자·삼자 협력, 아세안 지역 국가와의 협력, 세계 사이버스페이스총회 등을 중심으로 추진하고 있다. 우리나라는 UN 차원에서 사이버안보 국제규범을 논의하는 UN GGE에 적극적으로 참여해 오고 있다. 2004년 UN GGE가 구성된 이래 현재까지 총 6차례 회의가 개최되었는데 우리나라는 제1차, 2차, 4차, 5차 회의를 포함하여 총 4차례 참여한 바 있다. 아울러, 우리나라는 2019~2021년간

개최된 UN OEWG에도 적극적으로 참여하여 2021년 3월 全 UN 회원국의 합의를 통한 결과보고서가 채택되는데 기여하기도 하였다.

우리나라는 또한 양자·삼자 협력을 통한 사이버안보 국제협력에도 추진하고 있는데 특히 한미동맹의 최우선 아젠다로 부상한 사이버안보를 협력하기 위해 미국과 비전을 공유하고 협조 채널 구축을 추진하고 있다. 한미 간 사이버안보 논의는 정상회담과 사이버정책협의회를 통해 이루어지고 있으며, 2022년 5월 한미정상회담에서 대북안보, 경제협력, 글로벌 동맹 등 크게 3가지 주제로 토의가 진행되었고 3가지 주제 모두가 사이버안보 협력방안이 다뤄졌다. 그만큼 포괄적 동맹 관계 구축에 있어서 사이버안보가 매우 중요하며 사이버위협에 대응하기 위한 국제협력이 필수적이라는 인식에 공감대가 이루어졌음을 알 수 있다. 2021년 7월에는 우리 정부는 미국과 함께 글로벌 사이버위협에 공동대처하고 관계 부처가 참여하는 '한미 사이버 워킹그룹'을 출범시켜 한미 간 협력체계를 강화해 나가기로 했다. 정부가 사이버위협 대응을 위해 한미 간 사이버 워킹그룹을 출범토록 한 것은 2021년 5월 양국 정상회담에서 사이버안보 협력을 강화하기로 합의한 것을 이행하기 위한 조치로 이루어졌다.

또한, 미국뿐만 아니라 태국(2022.3월), 호주(2021.12월), 네덜란드(21.12월), 영국(2020.1월), 러시아(2019.1월), EU(2020.11월), 체코(2019.6월) 독일(2016.6월), 폴란드(2019.6월), NATO(2017.2월) 등과도 양자 사이버정책협의회를 개최하고 있으며, 일본 및 중국과는 삼자 사이버정책협의회(2020.12월)를 그리고 미국과 일본과는 삼자 사이버 대화를 진행하고 있다.[44] 또한, 아세안지역안보포럼(ASEAN Regional Forum, ARF)을 통해 아세안 지역 국가와도 사이버안보 협력을 추진하고 있다. 아세안지역안보포럼(ARF)은 2015년 8월 아세안지역안보포럼(ARF) 외교장관회담에서 사이버안보 작업계획을 채택하고 회원국 간에 사이버안보 분야 신뢰 구축과 분쟁 방지, 상호이해를 증진하기 위해 사이버안보 회기간회의(ISM, Inter-Sessional Meeting)[45]를 통해 3대 중점협력 분

44) 외교부, 「글로벌 안보협력 개요」, (2022.10.26 인터넷 검색)
45) ARF 사이버안보 회기간회의(ISM, Inter-Sessional Meeting on Security of and in the Use of ICTs) : 2017년 ARF 외교장관회의 계기 사이버안보 신뢰구축 방안 논의를 위해 설립

야 중 하나로 사이버안보 이슈를 논의하고 있다. 2018년에는 본격적으로 아세안지역안보포럼(ARF) 내 사이버 분야 신뢰 구축조치 논의를 위한 연구그룹이 시작되었고, 2022년 5월 우리나라는 아세안과 미국, EU, 일본, 중국, 러시아가 참여하는 아세안지역안보포럼(ARF) 사이버안보 회기간회의(ISM)의 금년도 주재국이자 공동 의장국으로 회의를 개최하면서 아세안지역안보포럼(ARF) 내 사이버안보 신뢰 구축조치와 협력 증진방안을 모색한 바 있다.

이외에도 우리나라는 2017년부터 격년으로 아시아·유럽지역 정부·국제기구 관계자와 학계·업계 인사들이 참석하는 유럽안보협력기구(OSCE)와 공동으로 사이버안보, 테러, 신기술안보 등 국경을 초월하는 안보위협에 적극적으로 대응하기 위해 한·OSCE 콘퍼런스를 개최하고 있으며, 아시아와 유럽지역의 사이버안보에 대한 다양한 경험을 상호 공유하고 각 지역 간 협력방안을 논의하는 등 아시아·유럽지역 간 협력의 가교역할을 수행해 오고 있다. 또한, EU와는 안전하고 안전하며 지속 가능한 디지털을 가능하게 하는 인터넷과 사이버 공간에 대한 규범에 대한 공통의 글로벌 비전을 통해 디지털 문제와 위협이 해결될 수 있도록 국제협력의 필요성을 인식하고 2020년 10월 사이버 분쟁 확대 방지를 위한 신뢰 구축, 사이버 범죄 퇴치 등을 논의하기 위해 양자 사이버 협의를 실시하였다.

국방부 차원에서는 국방부가 주도하는 최고위급 연례 다자안보대화체인 서울안보대화(Seoul Defense Dialogue, SDD)가 개최되고 있다. 2012년 11월에 '안보와 평화를 위한 협력(Cooperation for Security & Peace)'을 슬로건으로 국제사회의 이해와 협력을 통해 한반도의 평화와 안정을 도모하고 한반도를 포함한 아시아·태평양지역의 우호적인 안보환경 조성 및 다자간 군사적 신뢰 구축을 위해 처음 개최되었다. 서울안보대화(SDD)를 통해 세계 각국의 국방 분야의 고위 관료들과 민간 안보전문가들이 한자리에 모여 긴밀한 소통을 하며 국제 안보협력방안을 논의해 왔으며 국방 분야를 대표하는 다자간 안보협의체로 자리를 잡아가고 있다. 점차 아시아·태평양 지역을 넘어 유럽지역과 국제기구

주요 인사들의 참여도가 높아지고 있어 다양한 글로벌 현안이 논의되고 있다.

마지막으로 우리나라는 2011년 런던, 2012년 부다페스트에 이어 사이버테러, 사이버 범죄, 국제안보 등을 비롯한 포괄적으로 사이버안보 이슈를 중심으로 다루는 고위급 국제포럼인 세계사이버스페이스총회를 서울에서 2013년 10월 개최한 바 있다. 우리나라는 의장국으로서 개도국들의 역량 강화를 논의하는 의제를 제안하여 개도국의 관심과 지지를 확보하고, 중견국으로서 역할을 강조했다. 이후 2015년 네덜란드 헤이그 총회에서 우리나라는 전임 의장국으로서 사이버 공간을 규율할 국제규범 부재한 상황에서 국가 간 신뢰 구축 노력의 필요성, 사이버 공격에 대응할 수 있는 견고하고 효과적인 파트너십의 필요성, 그리고 개도국들의 사이버역량 강화를 위한 국제협력의 필요성을 강조한 바 있다. 우리나라는 2017년 인도 뉴델리 총회에서 초국경적 사이버위협이 단순한 기술적 차원의 문제를 넘어 외교적 문제임을 강조하고, 국제사회 협력과 견고한 파트너십, 신뢰 구축조치, 개도국 역량 강화, 국제규범 정립 등 국제협력 중점분야를 국제사회에 제시하였다.[46]

46) 외교부 보도자료(2017.11.22.)

Ⅵ. 국방 분야 사이버 국제협력 발전방안 고찰

제1절 국방 사이버 국제협력 현황

국방부는 미국 등 동맹국 및 우방국들과 양자 및 다자적 사이버 국제협력 관계를 맺어왔다. 국방부가 추진 중인 회의체는 아래 표와 같다. (조성림, 2019)

<표 7> 국방 사이버 국제협력 현황

구 분	회의명		기간	주기
한·미	한·미 국방사이버 정책실무협의회		'14~	연2회
	한·미 사이버 실무협의체		'16~	월2회
	한·미 정보보증 /컴퓨터 네트워크 방어정보교환		'15~	월1회
양자	한·UAE	국방사이버안보협력회의	'15~	연1회
		국방협력운영위원회	'16~	연1회
		공동고위급군사위원회	'11~	연1회
	한·이스라엘 사이버협력 실무회의		'14~'15	
	한·호주 ICT포럼		'14~	연1회
	한·사우디/한·체코/한·프랑스 정책협의			
다자	서울안보대화		'12~	연1회

우선 한미 간 국방 사이버 협력사례를 보면 사이버위협에 대비한 한미 간의 대응능력을 향상시키기 위해 사이버 정책·전략·교리 관련 정보공유와 사이버 공조체계 관련 협력 강화를 목표로 2014년부터 한미 국방사이버정책실무협의회를 만들어 추진중에 있으며, 합참과 주한미군사가 공동 주관으로 연합 사이버 작전소요 및 연합 사이버조직 구성을 검토하는 비상설 협의체인 한미 사이버 실무협의체를 운영하고 있다. 또한, 한·미 당국은 사이버전(戰)에 대비한 양국 간 상호협력 필요성에 따라 '한.미 정보보증 및 컴퓨터네트워크 방어 협력에 관한 양해각서(MOU)'를 체결하고 양국군 간 정보 및 정보체계의 상호운용성을

향상시키고 사이버공격의 예측 탐지 및 대응능력 강화를 위한 협력을 추진하였다. 아울러, 한·미간 효과적이고 적시적인 사이버위협 정보를 교환하기 위하여 운영예규를 체결하는 등 사이버 공격 시 한미 공동대응절차를 토의하는 실질적인 협력방안을 논의한 바 있다. 2022년 8월 한미 사이버사령부는 양해각서(MOU)를 체결하고 사이버 작전 분야 협력과 발전을 위한 사이버위협 정보공유 및 연습·훈련 기회를 확대하는 등의 사이버 공조 협력을 강화하고 상호 사이버 작전 역량을 강화하여 공동의 적으로부터 위협을 완화할 수 있는 중요한 계기를 마련하였다.

미국을 제외한 양자 차원에서의 사이버안보 협의체로는 우선 UAE와 추진중인 국방 사이버안보 협력 협의체가 있으며 국방협력운영위원회 제7차 운영위에서 사이버분과를 신설하여 운영중에 있다. 최근 양국은 방위산업 협력을 계기로 정보·사이버 분야에서 협력을 확대 강화하고 있다. 2022년에 한측 국방부장관과 UAE측 국방특임장관과 양자회담을 갖고 인적 자원 교류 및 상대방 사이버 교육 훈련 참관 등 실질적인 교류 협력을 활성화하고, 사이버위협에 공동대응하기 위한 사이버안보 협력을 강화하기로 했다. 또한, 이스라엘과는 사이버위협 양상을 평가하고 사이버 방어 전략 및 조직개편 현황 등을 공유하며 상호 교육과정을 소개하는 등 한·이스라엘 사이버 협력 실무회의를 추진하고 있다. 호주와는 양국 정상 간에 합의된 사이버 분야 협력 강화 후속 조치로 국방 사이버 협력, 사이버범죄 공동 대응을 추진하고 있으며 양국 국방부 차원의 정보화 분야 교류 및 협력 활성화를 위해 한·호주 ICT(Information and Communication Technologies) 포럼 약정서를 체결하고 사이버워킹그룹을 운영하고 있다. 또한, 2022년 수교 60주년을 맞아 외교·국방(2+2) 장관회의를 통해 상호관계를 포괄적·전략적 파트너십 관계로 격상하고 급변하는 안보환경에 효과적으로 대응하기 위해 양자 간 합동·연합훈련을 늘리는 한편 사이버를 포함한 국방 분야의 교류 협력을 확대하기로 했다.

다자간 협력 차원에서는 국방부가 주도하는 서울안보대화(Seoul Defense Dialogue, SDD)를 계기로 사이버안보에 특화된 전문가 대화

체인 사이버워킹그룹(CyberWG)이 개최되고 있다. 사이버워킹그룹(CyberWG)은 초국경적 사이버위협 속에서 국방 차원의 사이버 도전과제를 논의하며 신뢰를 구축하는 다자 대화의 장이다. 이를 통해 사이버안보 분야에 있어서 국제사회의 대응역량을 증진시킬 수 있는 새로운 국방 사이버 전략을 공유하며 사이버 관련 국제법적 이슈를 검토하고 사이버 인력 양성 정책 등을 논의해 오고 있다.

세계 각국은 사이버 공간에 대해 다양한 입장을 견지하고 있으며 사안에 따라 국가 간 다양한 협력과 갈등이 공존하고 있다. 거듭해서 언급하지만, 사이버 공간의 광역성, 개방성, 자율성, 익명성이라는 특성으로 인해 진화하는 사이버위협에 하나의 국가 차원에서 문제를 해결하는 것은 불가능하다. 우리나라의 경우 우방국과의 관계나 지원에 크게 의존할 수밖에 없는데 국방 사이버 분야의 국제협력 발전을 위해서는 타국과의 군사적인 유대를 강화하고 교류 협력을 확대함과 동시에 군사적 역량을 증진시키며 외국의 군사적 지원을 획득할 수 있는 방안 등을 모색하여야 한다.

제2절 국방 분야 국제협력 발전에 대한 정책적 제언

국방 분야 사이버 국제협력의 목적은 다른 국가들과의 협력을 통해 핵·미사일과 함께 현대 3대 전쟁수단 중 하나인 사이버전을 최대한 억제하고, 사이버 무기의 발전으로 사이버전의 위협이 점점 증가하는 가운데 자국과 우방국들의 사이버 전력 강화를 통해 사이버전에서 국가와 국민의 안위를 보장하며, 사이버 행위에 따른 불필요한 오해로 인한 갈등과 분쟁을 방지하고 확전 가능성을 최소화할 수 있도록 군사적 신뢰와 평화체계를 구축하기 위한 글로벌 차원의 논의를 주도하기 위한 것이다.

특히 우리의 국방 사이버 국제협력의 목표는 한반도에서의 사이버전을 억제하고 사이버전 발생 시 사이버 전력을 최대한 활용하여 반드시

승리하며 우방국들과의 실질적인 사이버 협력과 비우호적인 국가들과의 사이버 신뢰 구축 활동을 통해 아시아·태평양지역은 물론 세계의 평화와 안전을 보장하는 것이라고 볼 수 있다.

이러한 우리의 국방 사이버 국제협력의 목표를 달성하기 위해서는 우리나라의 사이버 전력을 강화하고 사이버 억지력을 확보하기 위해 미국 등 우방국들의 사이버 전력을 활용하는 사이버 군사협력 활동과 비우호적인 국가들과의 갈등을 최소화하고 확전을 예방하기 위한 장치로서의 군사적 사이버 신뢰 구축 활동을 병행해야 한다고 볼 수 있다.

사이버 전쟁은 공격의 진원지는 물론 배후세력도 눈에 보이지 않고 선전포고도 없이 은밀하고 조용히 이루어지는 '사일런스 전쟁'이다. 특히 사이버 영역에서의 위협이 익명성이라는 사이버 공간의 특성으로 인해 사이버 공격 행위자와 동기(목적), 대상, 수단·방법, 효과(피해) 등을 식별하기 어렵기 때문에 갈등과 확전 가능성을 최소화하고 평화를 유지하기 위한 기본적인 장치로서의 군사적 사이버 신뢰 구축 활동이 매우 중요하다고 할 수 있다. 이제 보다 구체적으로 국방 분야의 사이버 국제협력 발전방안을 제시해 본다면, 3가지 측면에서 제안하고자 한다.

① 국가 간 상호이해 및 신뢰 제고를 위한 인적교류 확대를 활성화하여야 한다.

인적교류는 양국 협력의 기본적이고 중요한 요소이다. 상호 사이버 부대를 방문하거나 사이버 교육·훈련을 경험하는 것만으로도 상대국과의 사이버안보 협력을 강화할 수 있는 계기가 될 수 있다. 현재 국방부 차원의 양자 실무협의체를 통해 UAE·이스라엘·호주 등과 인적교류 등의 협력방안이 마련되고 시행이 되고 있으나, 다양한 국가로 확대할 필요가 있다. 미국을 포함한 우방국과 사이버안보 분야의 공조 협력의 일환으로 인적교류를 위한 양해각서(MOU)를 체결하여 상대방 국가의 사이버 부대를 상호 정기적으로 방문하고, 사이버 정책과 최신 기술을 경험할 수 있는 기회를 가질 수 있도록 국방부가 여건을 마련해야 한

다. 미국 등 사이버 선진국들은 사이버위협에 체계적으로 대응하기 위한 사이버 작전 수행 전문인력 획득과 양성에 많은 노력을 경주하고 있다. 특히 사이버 전문인력을 획득하고 양성하기 위한 기준을 수립하고 이를 기반으로 다양한 정책 및 프로그램 등을 운영하여 사이버 전문인력을 체계적으로 획득 중이다. 또한, 사이버전 수행을 위해 필요한 군사 지식, 사이버 환경에 대한 기반 지식, 사이버 공격 및 방어기술 등을 구축하고 최신 사이버 전사 훈련 프로그램도 운영하고 있다. 국가 간의 국방 사이버 전문인력들이 상호 간에 경험을 교류하고 사이버전 관련 군사 지식을 공유함으로써 사이버 작전 역량을 강화함과 동시에 국방 분야에서의 사이버안보 공동의 문제에 대한 해결방안을 함께 모색해 나갈 수 있을 것이다.

특히, 국가 軍 당국 간의 이해증진과 군사외교 강화를 위한 국방부 고위급 인사의 역할이 매우 중요하다. 2022년 9월 국방부 차관이 미국 사이버사령부를 방문하여 미 사이버사의 주요 능력과 작전수행체계 등을 소개받고, 한미 연합 사이버 작전 역량 강화를 위한 다양한 협력방안을 논의한 바와 같이 군 고위급 인사가 정기적으로 상대방 국가의 사이버 부대를 방문하여 협의하는 것만으로 국가 상호 간의 사이버 협력관계가 더욱 진전될 수 있으며 미래지향적인 협력관계가 지속 발전될 수 있는 계기가 될 수 있다.

사이버 현안을 논의할 수 있는 국제 학술 행사에도 관심을 가져야 한다. 우리 군은 美국방부 NII(Network and Information Integration) 차관보실 주관으로 개최되는 국제 사이버 방어 워크샵에 2004년부터 참가하여 전 세계 사이버 방어 요원들과의 교류를 활성화하고 국제 사이버전 동향파악을 통해 우리 군의 사이버전 가상훈련을 위한 체계구축 발전에 활용하고 있다. NATO의 사이버방위센터(CCDCOE)에서 연례 개최하는 'Cy Con(사이버 충돌에 관한 국제 콘퍼런스)'뿐만 아니라 美 사이버사령부가 주관하는 다국적군 연합 사이버 방어훈련인 사이버 플래그(Cyber Flag) 훈련이 전술적 수준의 사이버 방어훈련 외에도 협력 발전방안을 논의하는 심포지엄 형태의 세미나도 함께 진행이 되어

학술적 토론이 이루어지고 있어 사이버 준비태세 점검뿐만 아니라 사이버전 동향을 파악할 수 있는 좋은 기회가 될 것이다. 또한, 랜섬웨어 해킹 공격에 대한 국제적 협력을 강화하기 위한 '랜섬웨어 대응 이니셔티브 정상회의(International Counter Ransomware Summit)'나 'APEC 사이버 보안·테러 대비 민·관 세미나', 국제 사이버보안 콘퍼런스(International Cybersecurity Conference) 등 민간 영역에서의 국제협력을 위한 국제회의와 콘퍼런스 역시 진행되고 있어 이를 적극적으로 참가하여 활용할 필요가 있다. 이러한 국제 학술행사 역시 국가 간의 중요한 사이버 현안을 논의할 수 있는 주요 협력체계라고 볼 수 있다.

② 국가 간 공동의 안보목표를 달성하기 위해 정보공유 및 공조체계 구축을 강화해야 한다.

외교부는 미국을 포함하여 영국·EU·일본·중국 등과 양자·삼자 사이버정책협의회를 정례적으로 추진중에 있으며 이를 통해 사이버위협에 대응하기 위한 최근 사이버안보 환경, 사이버안보 정책과 전략, 사이버위협 동향 및 대응, 양국 간 협력 강화 방안 모색, 사이버 공간상 국제규범 및 신뢰 구축 등 주요 이슈들에 대해 논의하고 있다. 이렇듯 사이버 정책협의회는 양국 간의 사이버안보 분야의 정책과 전략 등을 정기적으로 공유하고 발전시키며 상호 간의 정보교환 및 협력을 증진하는 중요한 역할을 하고 있다. 국방 분야도 상대국과의 사이버안보 정책협의체 구성을 정례화하여 전략 및 정책을 공유하고 사이버위협에 공동 대응하기 위한 실질적인 협력을 확대·강화해 나가야 한다. 우선 안보 동맹국과 정보공유 협력체계를 긴밀히 하고 사이버 공격 발생 시에 즉각적으로 대응할 수 있는 역량 구축에 힘써야 한다. 국방부는 미국과 2014년부터 사이버 정책협의회를 구성하여 운영하고 있으나 다른 국가와는 실질적인 정책협의가 미흡한 실정이라고 볼 수 있다. 전통적인 우방국과는 물론 일본·중국·러시아와도 정책협의 확대를 통해 사이버안보 전략·정책을 공유하고 협력방안을 발전시켜 나가야 한다. 사이버 공간에서 이루어지는 군사 활동에 대한 국가 간 이해관계와 진영 간 갈등이 심각한 상황이므로 중국·러시아 등 비서방국과의 정책협의

가 현실적으로 어려움이 있을 것이다. 그러나, 사이버위협을 포함한 사이버 공간의 현실태를 평가하고 협력이 가능한 분야부터 논의를 시작할 필요가 있다.

국방 사이버 정보공유체계 구축 확대도 요구된다. 정보공유는 점점 더 경로가 다양화되고 수준이 지능화·고도화되어 가고 있는 사이버 공격을 선제적으로 대응하고 사이버 방어 수준을 강화할 수 있는 가장 현실적인 수단으로, 주변국들과 사이버 공격 관련 위협정보를 공유하고 더 나아가 글로벌 및 지역 차원에서 협력하기 위한 체제도 가동되어야 한다. 현재 군 차원에서는 사이버 선진국이자 우방국인 미국과 사이버 정보공유가 활성화되어 있는데 2009년 사이버 공격의 예측 탐지 및 대응능력 강화를 위한 한미 정보보증 및 컴퓨터 네트워크 방어 협력을 체결하고, 2021년 정보통신기술 협력위원회를 통해 '파잇 투나잇(Fight Tonight) 준비태세가 가능하도록 다양한 지휘 통제 및 정보공유체계 구축에 협력을 강화하고 있다. 이를 확대하기 위해서는 우선 APEC 국가와의 국방 사이버 정보공유체계 구축을 고려해 볼 수 있다. 이는 우리 정부가 APEC(아시아태평양경제협력체) 사이버안보 세미나를 개최하는 등 APEC 차원의 사이버 협력을 주도하고 있으며, 사이버 위협 대응 노력에 선도적인 역할을 수행할 필요가 있기 때문이다. 최근 코로나19 팬데믹으로 인해 급격하게 비대면 사회로 전환되면서 전 세계를 강타한 랜섬웨어 등 해외에서 유입되는 사이버 공격을 예방하고 대응하기 위해서는 국가 간 정보공유가 더욱 필수가 되었으며, 정책협의회 구성과 별개로 각국 국방부와의 정보공유체계 구축 확대를 통해 잠재적인 사이버위협을 최소화하고 국방 사이버 환경을 강화해 나가야 한다.

사이버 핫라인 설치도 고려해 볼 필요가 있다. 2012년 미국과 러시아는 국가 간 사이버 공격 양상이 심화하고 있다는 판단하에 러시아측의 요청으로 핵전쟁을 막기 위해 설치한 안전통신채널(핫라인)에 사이버 핫라인 설치를 포함한 사이버안보 협상을 한 바 있으며, 2015년 미국과 중국은 사이버범죄에 대한 정보교환과 공동대응을 위한 장관급

회담을 개최하고 상대방 요청에 즉각적이고 효과적으로 대응하기 위해 사이버 핫라인 설치를 합의한 바 있다. 이처럼 사이버 핫라인을 설치하고자 하는 이유는 사이버 공간에서의 의사소통을 높여 의도를 바로 확인할 수 있어 오해로 인한 갈등을 방지하고 불필요한 긴장과 분쟁을 해소함으로써 양국 간의 관계 회복에 긍정적인 기능을 줄 수 있기 때문이다. 우리나라는 국방 당국 간의 사이버 핫라인을 설치한 사례는 없다. 하지만, 역내에서 긴급사태가 발생할 경우 각국 국방 당국 간에 직접 연락을 주고 받는 시스템인 국방 핫라인을 국제사회의 주요 이슈가 되고 있는 사이버안보를 포함하여 확대할 필요가 있다. 국방 핫라인은 무력충돌의 우려가 있거나 군사적으로 협력할 필요성이 클 때 개설되는 것으로 양국 관계 긴장을 해소하고 지역 평화와 안정을 위한 중요한 도구로서 역할을 하고 있다.[47] 2021년 6월 상원 군사위원회 청문회에서 로이드 오스틴 美국방부 장관은 동맹국뿐만 아니라 중국과 같은 적국들과의 '핫라인 구축' 또한 매우 중요한 일이라고 강조한 바 있다. 국경 없는 사이버 공간에서는 국가 또는 개인에 의한 사이버 공격이 한 국가에 집중되기보다는 다양한 국가에 동시 다발적으로 발생하기 때문에 군사시설 무력화를 위한 사이버 공격 발생 시에 신속한 대응을 통한 군사적 피해를 최소화하고 사이버 공격 억지력을 확보하기 위해서 다양한 국가와의 사이버 핫라인 설치는 필요할 것으로 보인다. 단기적으로 우리나라는 전통적인 주변 4강(强)인 미국을 포함한 일본, 중국, 러시아와 사이버 핫라인을 개설하고 장기적으로 유럽안보협력기구나 동남아국가연합 국가들과도 사이버 핫라인을 개설하여 北 사이버 공격에 대한 긴밀한 공조체계를 유지하는 것이 바람직하다.

방산기술 보호를 위한 국가 간 사이버 협력을 고려해 볼 수 있다. 최근 국제사회에서는 기술 우위 선점을 위한 경쟁국 간 기술패권 확보 노력이 치열하게 전개되고 있다. 이에 따라 정보기술의 발전에 따른 기술 정보 침해 위험이 커지고 있어 기술 보호를 위한 강력한 대응이 요구되고 있다. 일반기업은 물론 정부 기관도 산업기술 탈취나 해킹 등의 목표 대상이 되고 있다. 특히, 방산기술의 탈취는 국내·외적으로

47) 한국은 군사동맹 국가인 미국(1994년), 일본(1999년), 중국(2015년)과 국방 핫라인을 개설한 바 있음

영향이 크기 때문에 그 어떤 기술보다도 중요하게 인식되고 있다. 특히, 방산기술의 경우 외부로 유출되면 일반 산업기술과 달리 경제적 손실 및 기술개발 위축뿐만 아니라 국가안보를 위협하게 되고 나아가 국제안보와 평화를 침해하는 매우 심각한 문제에 직면하게 된다. 이러한 방산기술을 보호하기 위해 특정 국가의 노력만으로는 한계가 있으며, 국제사회에서의 상호 신뢰와 공조체계가 반드시 필요하다. 다행히 방위사업청 주관 방산기술 보호 국제 콘퍼런스가 매년 정기적으로 개최하여 국제사회의 방산기술 보호 정책 공조를 강화하고 신뢰를 구축하는 계기를 마련하고는 있다. 그러나, 방위산업기술이 국방과학기술 중 국가안보 및 국제사회의 안정을 위하여 보호되어야 하는 기술로서 국방부 차원에서도 관심을 갖고 방산기술 보호를 위한 국제공조 활동을 추진할 필요가 있다.

③ 국가 간 군사적 사이버 신뢰 구축조치를 위한 다양한 안보협력이 추진되어야 한다.

국방 차원에서의 연습 및 훈련 분야 국제협력은 아직 적극적인 참여가 미흡한 상태라 할 수 있다. 우리 군은 사이버전 수행역량을 강화하고 사이버안보 분야에서 국제협력을 확대할 수 있도록 각 나라에서 실시하는 사이버 분야 국제훈련에도 적극적으로 참여하거나 주관하여 시행할 필요가 있다. 2022년 6월 워싱턴의 한 민간연구단체인 헤리티지 재단(The Heritage Foundation)[48]이 공개한 '미한 사이버 협력 기회' 보고서에서 다수의 동맹국과 협력을 통한 사이버훈련은 상호 운용성과 의사소통을 강화하고 교리를 시험하기에 최적의 훌륭한 도구라면서 이 같은 사이버 연합훈련이 복원력과 예비력을 강화하고 북한과 중국 등의 사이버위협에 효과적으로 대응하기 위해 미국과 한국이 전략적 협력을 강화해야 한다는 제언하기도 했다.

일본은 2015년 4월 미국과 양자 동맹을 맺고 사이버 공간과 우주까지 확대하는 방위협력지침 개정안을 발표하면서 사이버 합동훈련 실

48) 헤리티지 재단은 1973년에 설립된 미국의 보수적 성향의 싱크탱크로 미국 정치, 경제, 외교, 국방 등에 관한 정책개발을 주로 하고 있으며, 미국 공화당의 브레인 역할을 수행(브레이킹연구소는 미국 민주당의 싱크탱크)

시, 사이버훈련 기술협력과 인적교류 등에 이르기까지 다양한 협력과 공조가 진행 중이다. 일본은 기밀정보 공유협의체인 '파이브 아이즈(Five Eyes)'와의 관계를 강화하고 있는데 안보협력 강화의 노력으로 미국 우주사령부가 주관하는 우주·사이버 분야 연합 및 합동훈련인 '슈리버워게임(Schriever Wargame)[49] 훈련에 일본 방위성·외무성이 2018년부터 참가하고 있다. 그러나 우리 군은 2021년부터 슈리버워게임 훈련에 참관은 하고 있으나 아직은 일본과 같이 참가하는 수준으로 발전시키지는 못했다. 2021년 11월 미국 국방부가 사상 최대 규모의 다국적 사이버 연합훈련인 '사이버 플래그(Cyber Flag)을 실시하였는데 미국 버지나아주 통합기지에서 23개국 200여명의 작전 요원들이 참석한 대규모 사이버훈련이었다. 매년 두 차례 실시되는 '사이버 플래그' 훈련은 사이버전 방어 능력을 키우기 위한 종합훈련으로 미국의 전통 우방국인 영국, 캐나다. 프랑스, 독일 등이 참석하였고 특히 덴마크, 에스토니아, 리투아니아, 폴란드 등 다양한 유럽국가들이 참석하였지만 안타깝게도 동맹국인 우리나라는 포함되지 않았다. 한미안보협의회(SCM)를 통해 사이버 능력을 활용해 억제태세를 강화하기로 합의한 바 있었지만, 그동안 우리 군은 미국이 주관하여 실시해 온 사이버 연합훈련에 한 차례도 참석한 적이 없었다는 것은 사이버위협에 대한 통합적 대응이 어려울 수 있다는 우려도 제기되었다.

그러나, 다행히도 최근 군 차원에서 미국과 NATO를 중심으로 합동군사훈련을 확대하는 실질적인 사이버 안보협력이 빠르게 진전되고 있다. 2022년 5월 한·미 정상회담에서 우리나라와 미국은 사이버 관련 기술협력을 위해 한·미 사이버 정책협의회와 사이버워킹그룹의 논의를 가동할 것과 디지털 권위주의에 의한 위협 증가에 대처하고 자유로운 정보의 흐름을 보장하는 개방적이고 안전한 인터넷 공간을 만들기 위해 공조할 것을 합의하면서 우리 군은 2022년 10월에 실시하는 사이버 플래그(Cyber Flag) 훈련에 처음으로 참가하였다. 또한, 우리나라가 아시아 최초로 NATO사이버방위센터 (Cooperative Cyber Defence

49) 슈리버워게임(Schriever Wargame) 훈련은 가상 적국의 GPS(인공위성위치정보)와 위성통신 전파 교란, 위성 관제시설에 대한 사이버 공격 등을 가정해 공조 대응을 연습하는 훈련으로 미국 육·해·공군과 국방부, 상무부, 교통부, NASA(항공우주국)를 비롯해 영국과 캐나다, 호주, 뉴질랜드, 프랑스, 일본 등 7개국이 참가

Centre of Excellence, CCDCOE) 회원국으로서 가입을 계기로 2017년부터 참관만 해오고 있던 세계 최대 규모의 사이버 연례 연합 군사훈련인 '사이버 코얼리션(Cyber Coalition)'[50]에 2023년부터 참가할 예정이다. 2022년 7월 윤석열 대통령의 NATO 정상회의 참석을 계기로 NATO와의 안보협력 강화 차원에서의 사이버훈련이 앞으로 발전적으로 확대될 것으로 기대가 되고 있다. 아울러 최근 국방부는 2022년 11월 동남아시아국가연합(ASEAN · 아세안)과 한미일 등 ADMM-Plus 참가국들의 사이버안보 역량 강화를 목적으로 사이버 국제훈련을 주관할 것을 밝히기도 하였다. 앞으로 미국·NATO뿐만 아니라 사이버 우방국에서 연례적으로 실시하는 다양한 다국적 사이버훈련에도 적극적으로 참가하고 주기적으로 국제 사이버훈련을 주관하여 시행함으로써 동맹·우방국과의 연합 사이버 준비태세 및 파트너십을 강화하고 사이버 전략 및 전술, 관련 정보를 공유하면서 사이버 위기대응 협력체계를 더욱 견고하게 다져야 할 것이다.

국방 사이버 전문인력 양성과 사이버 공격 대응역량 강화를 위해 국방 분야의 사이버훈련에만 한정하지 말고 민간에서 실시하는 훈련에도 적극 참여할 필요가 있다. NATO에서 주관하는 훈련에도 민간전문가가 참여하듯이 사이버안보는 민과 군이 분리되기 어려운 측면이 있기 때문이다. 우리 군은 2021년부터 북대서양조약기구(NATO) 사이버방위협력센터가 주관하는 세계 최대 규모의 민·관·군이 참여하는 사이버 공격·방어훈련인 '락트쉴즈(Locked Shieds)'[51]에 참가해 오고 있으나, 민·관·군이 참여하는 사이버테러 대응훈련인 미국 국토안보부가 시행하는 사이버스톰(Cyber Storm)[52]과 한국인터넷진흥원(KISA)이 참여하는 아태지역 침해사고대응팀협의회(APCERT: Asia Pacific Computer Emergency Response Team)[53]가 주관하는 국제공동모의훈련에도 국방

50) 사이버 코얼리션(Cyber Coalition) 훈련은 NATO 합동방위센터가 주관하는 연례 집단 사이버방어 훈련으로 전략·전술 및 기술, 정보공유 및 소통을 목적의 세계 최대 규모의 사이버 연합훈련임. 2008년부터 미국, 일본 등 NATO 회원국과 파트너 국가 30개국이 참가

51) 락트실즈(Locked Shied) 훈련은 NATO 회원국과 파트너국 간 사이버 위기 대응 협력체계 강화를 목적으로 매년 개최하는 다국적 사이버훈련.

52) 사이버스톰(Cyber Storm) 훈련은 미국 국토안보부 주도로 2006년부터 격년제로 실시하고 있는 민·관·군이 참여하는 국가 차원의 사이버테러 대응훈련, 사이버 공격에 맞서 정보기술, 통신, 에너지, 교통부문 시스템을 보호하는 훈련임

53) 아태지역 침해사고대응팀협의회(APCERT)는 2003년 출범한 아태 지역내 침해사고 대응 협력 강화를 목적으로 각 국가의 대표 침해사고대응팀(CERT) 협의체로 2004년부터 매년 공동모의훈련을 실시

사이버 인력이 참여하여 사이버 공격에 대한 글로벌 공조체계 및 사이버위협 대응태세를 점검하면서 사이버역량 구축을 위한 경험과 기술을 축적하는데 도움이 될 것이다.

사이버 군사지원도 생각해 볼 수 있다. 2022년 우크라이나에 대한 사이버공격이 연일 발생하였고 우크라이나 사이버보안센터는 그 배후로 러시아를 지목하면서 사태 해결을 위한 서방 국가들의 기술지원 확대 등 국제사회의 지원을 요청하였다. 러시아의 우크라이나 침공으로 그간에 염려해 왔던 사이버 전쟁이 현실화된 것이다. NATO의 전문가인 비타우타스 부트리마스는 "미래의 전쟁은 사이버 요소가 반드시 포함될 것이며 이는 사이버 전쟁이 아니라 그냥 전쟁일 뿐"이라고 말했다. NATO 회원국 국방부 장관들은 사이버 공간을 전쟁의 한 영역으로 인정하면서 사이버 공격을 동맹국과의 협력을 통해 공동 대응할 것임을 밝히기도 했다. 이에 북대서양조약기구(NATO)는 우크라이나와 사이버 협력 강화 방안에 합의하였고, 캐나다와 호주는 우크라이나에 대한 군사적 지원과 아울러 사이버안보를 지원하는 방안을 제의하였다. 우리나라도 우크라이나의 사이버안보 능력 강화를 위한 협조를 요청받기도 하였다. 이렇듯 현대전은 침공 이전에 전산망 해킹 등 사이버 공격을 통해 혼란을 조성하고 심리전 등 모든 형태의 공격을 병행하며 침공하는 양상으로 변모하고 있다. 약소국이 국가 존립의 위협에 직면한 순간에 국가생존이라는 목표를 달성하기 위해서는 동맹국의 사이버 군사지원은 필수적이다. 21세기 변화하는 안보 환경과 사이버전이 포함된 현대전에 능동적으로 대응해 나가기 위해서는 단순한 군사동맹을 넘어 사이버 군사지원을 통한 상호 신뢰에 기반한 동맹 관계로 발전해야 할 것으로 보인다.

또한, 세계 사이버안보 전문가들이 한자리에 모여 다양한 안보위협에 대한 대응전략을 논할 수 있는 협의체를 확대하여 개최할 필요가 있다. 학자들은 과거 유럽에서 군사적 신뢰를 구축하고 성공할 수 있었던 주요한 요인으로 안보 대화를 상설화하고 제도화 한데서 찾는다. 사이버안보 문제를 해결하기 위해서는 이해관계가 있는 국가가 참가하는 안

보 대화 채널의 구축이 무엇보다 중요하다. 우리가 당면하고 있는 위협은 북한의 사이버위협이겠지만 더불어 중국·러시아 등 다양한 국가 행위자들로부터의 위협도 염두에 둘 필요가 있다. 현재 국방부가 주관하는 서울안보대화(SDD: Seoul Defense Dialogue)는 국방 차원의 사이버안보 협력을 논의하고 발전시켜 나가기 위해 우리나라가 주도해 사이버안보에 특화된 전문가 대화체인 「사이버워킹그룹」을 발족하였고 사이버 현안에 대한 의견과 경험을 공유하며 신뢰를 구축하는 다자안보 대화의 장으로 자리매김하고 있다. 서울안보대화(SDD)에서 추진하는 사이버워킹그룹 구성은 상설 사이버안보협의기구 설치에 좋은 본보기가 될 수 있다. 국방 사이버 분야의 협의체를 통한 교류와 협력은 국방외교의 유용한 도구가 될 수 있으므로 앞으로 국방부가 주도하는 다자간 협의체 구성을 점차 확대하여 국제 사이버안보 이슈를 실천적이고 선도적으로 논의하고 발전시켜 나가야 한다.

마지막으로, 국방 분야의 국제협력 활동을 위한 「국방 사이버협력단」(가칭) 창설을 건의한다. 사이버 분야에 대한 국제협력 활동은 매우 전문적이어야 한다. 우선 국방 사이버협력단 인력의 자격요건으로 사이버 공간에 대한 이해를 바탕으로 발전하는 사이버 기술에 대한 전문지식을 갖추어야 한다. 또한, 국방 사이버 분야의 각종 법령과 정책 수립절차, 작전 수행체계 등에 대한 포괄적이고 종합적인 이해도 충분히 갖추어야 한다. 이러한 인력으로 구성된 「국방 사이버협력단」 조직을 신설하여 국방 분야의 통합적이고 국제적인 대응능력을 확보해야 할 것이며 전략적으로 우리 국방의 사이버 이익을 지키는데 매우 큰 역할을 수행할 것으로 기대된다. 사이버 분야의 국제협력 활동을 원활하고 추진력 있게 수행하기 위해서는 국방부 내 사이버 정책부서에서 기존 인력으로 추진하기에는 다소 무리가 있으며, 국방 사이버 공간에서의 사이버 작전 시행 및 그 지원에 관한 업무를 관장하는 국방부장관 직할부대인 사이버작전사령부 예하에 조직을 두고 국방부 사이버 정책부서의 통제를 받으면서 통합적이고 전문적으로 임무를 수행하는 것이 바람직할 것으로 판단된다.

Ⅶ. 결 론

정보통신기술의 발전과 함께 급격히 증가하는 사이버위협이 국가안보를 위협하고 있어 국제사회는 이전과 다른 차원의 안보위기 상황을 맞이하고 있다. 2022년 러시아의 우크라이나 침공에서 보듯 전장 환경도 육상, 해상 및 공중으로 대변되는 전통적 개념의 군사작전과 병행한 사이버전이 가미된 새로운 형태로 변화하고 있다. 이제 국방생태계는 막대한 전력 자산의 투입이 없어도 악성코드를 이용한 사이버 무기 하나만으로 적을 제압할 수 있는 사이버 공간이 매우 중요해 졌다.

세계 각국은 사이버 공간이 상호연결되어 있어 개별 국가의 노력으로는 한계가 있음을 인식하고 사이버 위협대응 역량을 강화하는 것과 더불어 사이버안보 국가전략을 마련하고 국제협력 등 사이버 동맹정책을 강화하는 등의 자구책 마련에 총력을 기울이고 있다. 이제 각국은 사이버 공격에 대한 대응을 사후약방문 형태의 소극적이고 방어 중심에서 벗어나 군사적 보복공격도 포함된 적극적 공세로 사이버안보 전략을 수정하고 있으며 군사안보 차원에서 국제공조 활동을 진행하고 있다. 우리나라도 사이버안보 신뢰 구축과 협력 증진을 위한 국제연대 필요성을 인식하고 국제기구 및 다자안보 협력기구를 활용하여 다양한 경험을 공유하며 각 지역 간 협력방안을 논의하고 있다.

이렇듯 사이버 환경의 급격한 변화로 인해 국가안보 차원의 사이버안보와 관련한 국제협력 논의가 진전되고 있어 미래 사이버전을 대비하는 국방부 주도의 사이버안보 대응체계 구축도 매우 중요하다고 볼 수 있다. 특히, 국방 분야에서는 서울안보대화(SDD)의 사이버워킹그룹(CyberWG)을 중심으로 국방 사이버 전략을 공유하고 사이버 관련 국제적 이슈를 검토하며 실무적으로는 양자 간 정책실무협의회 운영을 통해 사이버 대응역량을 강화해 오고 있으나 사이버전 수행능력 확보와 군사적 사이버 신뢰 구축 활동 등 실전적 수준의 국제협력은 미흡하다고 볼 수 있다.

본고에서는 현존하는 사이버위협을 평가하고 국제 사이버안보 환경과 동향(주요국 정책/전략)을 검토하여 국방 차원의 사이버 국제협력에 대한 정책적 발전방안을 제언하고자 하였다. 사이버 대응능력을 강화하고 사이버 억지력을 확보하기 위해 미국 등 우방국들의 사이버 전력을 활용하는 사이버 군사협력 활동과 비우호적인 국가들과의 갈등을 최소화하고 확전을 예방하기 위한 장치로서의 군사적 사이버 신뢰 구축 활동을 병행해야 한다고 볼 수 있다. 이런 점에서 사이버 분야에서 군사적인 유대를 강화하고 교류 협력을 확대함과 동시에 군사적 역량을 강화하고 외국의 군사적 지원을 확보할 수 있는 방안을 세 가지 측면에서 제언해 보았다.

국방 차원의 다양한 협력사례를 조사하고 전문가 자문 및 실무 토의를 통해 추진방안에 대한 아이디어를 도출하였으나 이를 실무적으로 추진하는 과정에서는 여러 현실적인 어려움이 있을 수 있다. 따라서, 제시된 여러 방안을 국방 여건을 고려하여 즉시 추진 또는 장기과제로 구분하여 충분한 검토와 준비를 거쳐 단계적으로 추진할 필요가 있다. 국제기구 또는 지역 안보협의체를 통해 사이버안보 이슈에 대한 논의와 협력은 앞으로 더욱 활발하게 이루어질 것이며 차후 연구들이 국방 차원에서 추진해야 할 사이버 국제협력의 실천방안을 조금씩 구체화할 수 있었으면 한다.

참고 문헌

정태일, ‘글로벌 기업 76% 팬데믹에 사이버 공격 급증, 원격 업무로 위협’, 2021.6.9일자

연합뉴스, ‘NATO 공동선언 중국의 도전 명시..균열 속 집단방위 재확인’, 2019.12.5일자

연합뉴스, ‘국정원, 한국 NATO 사이버방위센터 정회원 가입식 개최’, 2022.5.9일자

연합뉴스, ‘외교부, 유럽안보협력기구와 사이버안보 협력방안 논의’, 2021.6.30.일자

한국경제, ‘독일, 사이버 공격 맞대응하는 군부대 창설’, 2017.4.6일자

연합뉴스, ‘일본, 사이버 공격 주체로 북중러 첫 명기 보안전략 마련’, 2021.9.27일자

보안뉴스, ‘사이버 전쟁을 주도하는 국가정보기관 : 중국’, 2020.3.20일자

과학기술정보통신부, ‘무선통신서비스 통계 현황(2022.5월말 기준)’, 2022.

관계부처 합동, ‘국가사이버안보 강화를 위한 이행방안 확정-「국가사이버전략」 후속으로 기본계획 마련·시행’, 보도자료, 2019.9.3.일자

체재병, ‘사이버안보의 국제정치적 추세와 한국의 전략 구상’, 국가안보전략연구원, 2021.

유준구, ‘UN 정보안보 개방형작업반(OEWG) 최종보고서 채택의 의의와 시사점’, 외교안보연구소, 2021.

김규동, ‘국제 사이버법에 관한 경쟁과 탈린매뉴얼’, 국제문제연구소, 2018.

이상현, ‘사이버외교의 국제비교: OSCE와 ARF의 사이버 신뢰구축조치 비교분석, 한국세계지역학회, 2022

국립외교원 외교안보연구소, ‘2022 국제정세전망’, 2021.

체재병 외, ‘주변국의 사이버 환경과 한반도 평화체제 구축’, 통일연구원, 2019.

홍건식, ‘미국의 사이버안보 거버넌스 구축과 워너크라이 대응’, 중앙대학교 국익연구소, 2021.

오일석, ‘미국 사이버전략의 평가와 전망’, 국가안보전략연구소, 2022.

김근혜, ‘트럼프 행정부의 주요기반시설 사이버보안 정책분석에 관한 연구’, 고려대학교, 2019.
김상배, ‘세계 주요국의 사이버안보 전략’, 서울대학교 국제·지역연구 26권 3호, 2017.
유인태, ‘캐나다 사이버안보와 중견국 외교: 화웨이 사례에서 나타난 안보와 경제 · 통상의 딜레마 속에서’, 한양대학교 평화연구소, 2019.
체제병 외, ‘주요국 사이버안보 전략과 한국에의 시사점’, INSS전략보고, 2020.
김진형, ‘중국 사이버안보의 전략과 체계’, CSF 중국전문가포럼, 2022.
신범식, ‘러시아의 사이버안보 전략 실현의 제도와 정책’, 2020.
한국정보화진흥원, ‘2020 국가정보화백서’, 2020.
국가정보원 등, ‘2021 국가정보보호백서’, 2021.
김보미 외, ‘김정은 시대 북한의 사이버위협과 주요국 대응’, INSS전략보고, 2021.
김진광, ‘북한의 사이버조직 관련 정보 연구’, 합동군사대학교, 2020.
채재병, ‘주변국의 사이버 환경과 한반도 평화체제 구축’, 통일연구원, 2019.
국가안보실, 「국가사이버안보전략」, 2019.
조성림, ‘NATO 사이버 연습, 우리도 참여할 수 있어’, KIDA 국방논단, 2019.
유준구, 「최근 사이버안보 거버넌스 논의 동향과 우리의 대응」, 외교안보연구소, 2018.
UK National Cyber Security Strategy, 2022.
U.S. Army Headquarters, ‘North Korean Tactics’, 2020.
U.S Department of Defense, ‘Cyber Strategy 2018’, 2018.
Tobias Liebetrau, ‘Organizing cyber capability across military and intelligence entities: collaboration, separation, or centralization’, Policy Design and Practice, 2022.

Duncan B. H ollis & Matthew C. Waxman, ‘Promoting International Cooperation: lessons from the proliferation security initiative’, 2018.

Anna Felkner, Cybersecurity Research Analysis Report for Europe and Japan, 2021.

Martin Schallbruch, ‘Cybersecurity in Germany’, 2018.

Khotimah Estiyovionita, 「ASEANs role in cybersecurity maintenance and security strategy through an international security approach」, 2022.

Yoo, In Tae, ‘Cybersecurity Crisscrossing International Development Cooperation: Unraveling the Cyber Capacity Building of East Asian Middle Powers Amid Rising Great Power Conflicts’, Korea Observer; Seoul Vol. 53, 2022.

Sokolova, Elizaveta S, ‘Cybersecurity Cooperation between Russia and China: Prospects and Problems’, Contemporary Chinese Political Economy and Strategic Relations; Kaohsiung Vol. 7, Iss. 3, 2021.

Thomas Christiansen, ‘The European Union’s Security Relations with Asian Partners’, the European Union in International Affairs, 2021.

Mikael Weissmann, ‘Hybrid Warfare: Security and Asymmetric Conflict in International Relations’, 2021.

George Christou and Ji Soo Lee, ‘EU-Korea Security Relations’, EU-ROK cooperation on cyber-security and data protection(p.55 ~ 77), 2021.

Lester and S. Moore, ‘Responding to the Cyber Threat: A UK Military Perspective’, The Quarterly Journal, 2020.

Colonel Jaak Tarien, ‘National Cyber Defence Policies and the Role of International Cooperation’, The Quarterly Journal, 2020.

Theresa Hitchens, ‘Building confidence in the cybersphere: a path to multilateral progress’, Journal of Cyber Policy VOL. 4, 2019.