INSS 연구보고서 2021-18

2021 INSS Research Report

사이버안보의 국제정치적 추세와 한국의 전략구상

채재병

INSS INSTITUTE FOR NATIONAL SECURITY STRATEGY 국가안보전략연구원
06295 서울시 강남구 언주로120 인스토피아 빌딩
Tel. 02-6191-1000 Fax.02-6191-1111 www.inss.re.kr

비매품/무료
94080
9 791189 781705
ISBN 979-11-89781-70-5
ISBN 979-11-89781-52-1(세트)

INSS 연구보고서 2021-18
사이버안보의 국제정치적 추세와 한국의 전략구상 | 채재병
INSS 국가안보전략연구원

2021 INSS Research Report

INSS 연구보고서 2021-18

사이버안보의 국제정치적 추세와 한국의 전략구상

채재병 chaejb@inss.re.kr

INSS INSTITUTE FOR NATIONAL SECURITY STRATEGY 국가안보전략연구원

2021 INSS Research Report

INSS 연구보고서 2021-18

사이버안보의 국제정치적 추세와 한국의 전략구상

채재병

INSS INSTITUTE FOR NATIONAL SECURITY STRATEGY 국가안보전략연구원

INSS 연구보고서 2021-18

사이버안보의 국제정치적 추세와 한국의 전략구상

채재병

채재병 (蔡載秉)

| 국가안보전략연구원 수석연구위원

성균관대학교에서 정치학 박사학위를 받았으며, 주요 관심분야는 (사이버)안보, 한반도 통일, 동북아 질서 등이다. 주요 저서 및 논문으로 『국제사회의 해킹 변화 추세 및 대응방안』, 『국제 사이버공격 전개 양상 및 주요국 대응전략』, 『주변국의 사이버 환경과 한반도 평화체제 구축』(공저), 『한반도 평화의 국제정치학』(공저), "안보환경의 변화와 사이버안보", "동북아 지역질서 변화와 한국의 전략"(공저), "동아시아의 주권인식과 지역협력" 등이 있다.

목차

국문초록 6

I. 서론 8

1. 문제제기 및 연구목적 9
2. 선행연구 검토 12

II. 사이버안보의 국제정치 14

1. 사이버공간에 대한 국제정치적 인식 15
2. 사이버주권과 사이버안보 20
3. 사이버안보 국제규범 28

III. 사이버안보의 국제정치적 추세 38

1. 미중경쟁 속 사이버안보 39
2. 코로나19 팬데믹에 따른 사이버공격 양상 45
3. 포스트코로나 시대의 사이버안보 54

IV. 결론: 한국의 전략구상 62

Abstract 68

참고문헌 72

국문초록

본 연구의 목적은 국제사회에서 나타나고 있는 사이버안보의 국제정치적 추세를 분석하고, 동시에 코로나19 팬데믹의 영향으로 인한 사이버안보의 변화, 그리고 포스트코로나 시대에서의 사이버안보를 전망해 봄으로써 이와 같은 사이버안보의 변화에 대한 우리의 대응전략을 구상하여 제시하는 것이다.

최근 국제사회는 코로나19 팬데믹으로 인해 뉴 노멀 시대를 맞이하고 있고, 미중 간 패권경쟁이 더욱 격화되고 있는 상황이다. 사이버안보도 이와 같은 상황의 영향으로 크게 변화하고 있다. 따라서 이러한 변화에 대한 검토가 요구되고 있고, 특히 포스트코로나 시대가 도래할 경우 나타날 사이버안보 변화와 이에 대한 대비를 위한 검토도 요구되고 있다.

이를 위해 우선 논의의 토대로서 사이버안보의 국제정치적 의미를 살펴보기 위해 사이버공간에 대한 국제정치적 인식, 사이버주권의 안보적 함의와 사이버안보와의 관계, 사이버안보 관련 국제규범 형성 상황을 분석한다. 다음으로 사이버안보의 국제정치적 추세를 분석하기 위해 미중경쟁 속 사이버안보 전개 양상, 코로나19 팬데믹에 따른 사이버공격 변화 양상, 포스트코로나 시대의 사이버안보 변화 전망을 살펴본다. 마지막으로 이와 같은 분석을 기반으로 한국의 향후 사이버안보 관련 전략구상을 도출하여 제시한다.

제시된 전략방안들을 통해 네트워크와 클라우드를 포함한 사이버공격 범위 전체에 대한 감시, 탐지, 차단, 보호를 제공할 필요가 있다. 그리고 코로나19의 영향으로 확대된 공격 범위를 포괄할 수 있도록 기존의 사이버공격 대응체계를 개선하고, 새로운 취약점들을 보호할 수 있는 사이버안보 플랫폼을 구축함으로써 포스트코로나 시대의 사이버위협에 대응해야 할 것이다.

핵심어

사이버안보, 사이버공간, 사이버주권,
코로나19 팬데믹, 포스트코로나 시대

I

서론

1. 문제제기 및 연구목적
2. 선행연구 검토

1. 문제제기 및 연구목적

정보통신기술(ICT)의 발달에 따라 국제사회에는 사이버공간에서의 사이버테러나 사이버범죄 등 여러 가지 사이버 안보위협이 크게 증가하면서 국제사회 안보구조의 기반을 흔들어 놓고 있다. 2019년 10월 서울에서 개최된 “바르샤바 프로세스 사이버안보 워킹그룹 회의”에서 볼 수 있듯이 이제 국제사회는 바르샤바 프로세스와 같은 국제적, 지역적 평화를 위한 토의과정에서 사이버안보와 관련된 이슈들을 매우 중요하게 다루고 있다. 그러나 이와 같이 국가차원의 사이버위협이 국제사회의 안보를 심각하게 훼손하고 있는 상황임에도 불구하고 국제사회는 각국의 상이한 이해관계와 입장차이로 인해 사이버위협에 대응하는 국제적 조약이나 규범을 도출해내지 못하고 있다. 이러한 이유로 국제사회에 대한 사이버위협은 지속적으로 확대되어왔고, 이로써 사이버안보는 국제정치의 핵심 이슈로 대두되었다.

사이버위협은 초국가적인 형태로 진행되기 때문에 일국차원에서 대응한다는 것은 한계가 있고, 특히 사이버공간이 갖는 익명성이라든지 공격수월성과 같은 특수한 성격은 사이버안보가 국제정치 차원에서 연구되어질 필요가 있다는 것을 보여준다. 더욱이 국가차원의 사이버공격과 사이버 인프라를 활용한 활동들이 다른 국가의 안보에 커다란 위협이 되고 있는 상황에서 국제안보 차원에서 사이버안보를 연구할 필요성도 함께 제기되고 있다. 지금까지 이루어진 사이버안보 관련 연구는 주로 스팸, 개인정보보호, 사이버범죄 등 사이버위협의 세부적인 영역에 한정되었고 기술적인 측면에 치중하여 연구를 진행해왔기 때문에 사이버안보 이슈를 국제정치 차원에서 포괄적으로 다루지 못하는 한계를 보이고 있다.

사이버안보 분야에서 국제질서가 정립되기까지는 많은 시간이 필요할 것으로 보인다. 국제사회는 아직까지 사이버안보와 관련하여 어떠한 실질적인 협의체 구성이나 국제레짐의 창설 등을 이루어내지 못하고 있다. 즉 국제사회의 사이버안보에 대한 국제질서는 비록 많은 국가들이 그 필요성에는 동의하고 있음에도 불구하고, 세계 각국 간의 이견으로 인해 이에 대한 합의 도출이 가까운 시일 내에 이루어지기는 쉽지 않은 상황이다. 수많은 이유가 있지만 사이버 국제질서에 대한 합의가 이루어지기 힘든 가장 큰 이유는 미국을 비롯한 서방국가들과 이들처럼 정보통신 강국이면서도 입장이 다른 중국과 러시아 같은 국가들 간의 첨예한 이해관계의 충돌 때문이었다. 그리고 정보통신 분야에서 앞서 가는 국가들과 그렇지 못한 국가들 간에 사이버 국제질서에 대한 상당한 의견 차이가 존재하고 있다. 만약 미국 및 서방국가들과 중국 및 러시아 간에, 그리고 정보통신 선진국과 후진국 간에 이해조정과 의견조율을 통해 협력이 이루어졌다면 아마 사이버 국제질서는 벌써 수립되었을 것이다. 현재 사이버안보의 국제정치는 미중 간에 벌어지고 있는 영향력 확대 경쟁과 상호 간 견제, 국제전기통신연합(ITU), 국제인터넷주소관리기구(ICANN) 등 국제기구 간에 벌어지고 있는 사이버 패권경쟁 등으로 나타나고 있다.

이처럼 사이버공간에서 국제사회는 현실공간에서와 유사하게 미중 간 경쟁을 중심으로 하고 있다. 즉 미국을 중심으로 한 소위 서방진영은 자유로운 정보의 유통과 기존 국제법을 사이버공간에 그대로 적용하자는 주장이고, 중국과 러시아를 포함하는 소위 비서방진영은 각국의 국가주권에 기초하여 사이버공간을 통제하고 관리하자는 주장이다. 이와 같이 양분된 상황에서 비서방진영의 중국과 러시아는 사이버공간, 즉 인터넷 거버넌스에서의 국가주권을 강화하려는 입장이고, 서방진영의 미국은

중국과 러시아가 주장하는 사이버공간에서의 국가주권과 불간섭 원칙을 인정할 수 없다는 입장이다. 이 같은 입장에 따라 과거 미국은 사이버공간에 관한 국제규범을 만드는데 있어 매우 소극적인 입장이었다. 그러다가 최근 입장을 선회하여 국제사회의 사이버 국제규범 설립과정에 적극적으로 개입하면서 관련 논의들을 주도하고 있다. 이는 미국이 사이버공간에서도 미국의 원칙과 가치를 관철시킬 수 있는 사이버 국제규범을 확립하려는 목적으로 보인다. 그러나 미중 간 입장 차이는 물론이고 서방진영과 비서방진영의 입장 차이가 큰 현 상황에서 양측 모두를 만족시키는 사이버 국제규범을 도출하기는 사실상 거의 불가능하다고 할 수 있다.

한편 최근 국제사회는 코로나19 팬데믹으로 인해 뉴 노멀 시대를 맞이하고 있고, 미중 간 패권경쟁이 더욱 격화되고 있는 상황이다. 사이버안보도 이와 같은 상황의 영향으로 크게 변화하고 있다. 따라서 이러한 변화에 대한 검토가 요구되고 있고, 특히 포스트코로나 시대가 도래할 경우 나타날 사이버안보 변화와 이에 대한 대비를 위한 검토도 요구되고 있다.

따라서 본 연구의 목적은 국제사회에서 나타나고 있는 사이버안보의 국제정치적 추세를 분석하고, 동시에 코로나19 팬데믹의 영향으로 인한 사이버안보의 변화, 그리고 포스트코로나 시대에서의 사이버안보를 전망해 봄으로써 이와 같은 사이버안보의 변화에 대한 우리의 대응전략을 구상하여 제시하는 것이다. 이를 위해 우선 논의의 토대로서 사이버안보의 국제정치적 의미를 살펴보기 위해 사이버공간에 대한 국제정치적 인식, 사이버주권의 안보적 함의와 사이버안보와의 관계, 사이버안보 관련 국제규범 형성 상황을 분석한다. 다음으로 사이버안보의 국제정치적 추

세를 분석하기 위해 미중경쟁 속 사이버안보 전개 양상, 코로나19 팬데믹에 따른 사이버공격 변화 양상, 포스트코로나 시대의 사이버안보 변화 전망을 살펴본다. 마지막으로 이와 같은 분석을 기반으로 한국의 향후 사이버안보 관련 전략구상을 도출하여 제시한다.

2. 선행연구 검토

기존에 사이버안보에 관한 연구들은 대부분의 경우 사이버 안보능력을 제고하기 위한 전략연구에 치중되어 있다. 그리고 이를 뒷받침하는 법제와 정책 개선을 위한 사이버안보 법제 또는 사이버안보 정책 연구가 상당수이다. 그 외에 사이버공간의 생소함으로 인한 이론화 작업으로서 사이버안보 담론 등의 이론연구가 있고, 사이버안보에 대한 국제사회의 관심이 높아짐에 따라 사이버안보 국제규범 등 국제협력 혹은 갈등을 다루는 연구들로 구성되어 있다. (박노형·정명현. “국제사이버법의 발전: 제5차 UNGGE 활동을 중심으로,” 2018; 함승현·박대우. “국가 사이버안보를 위한 정책 연구,” 2017; 장노순. “사이버안보와 국제규범의 발전: 정부전문가그룹(GGE)의 활동을 중심으로,” 2016; 배영자. “사이버안보 국제규범에 관한 연구,” 2017)

그리고 사이버안보를 국가안보 차원에서 국제정치적으로 접근하고 있는 연구들은 급속한 과학기술의 발전과 정보화혁명에 따라 국제안보환경이 변화하고 있다는 점에 주목하여 국가안보 차원 중심의 연구 성과를 도출하고 있다. (김상배 외. 『사이버 안보의 국가전략: 국제정치학의 시각』, 2017; 박종재·이상호. “사이버 공격에 대한 한국의 안보전략적 대응체계와 과제,” 2017; 민병원. “사이버공격과 사이버억지: 국제정치적 의미와 대안적 패러다임 모색,” 2015; 장노순. “사이버안보와 선도국 우위의 전략적 선택,” 2017)

이와 같은 연구들은 사이버안보와 관련하여 분야별로 구체적인 연구 성과를 도출하였고, 국가안보 차원에서도 상당한 연구 성과를 도출함으로써 향후 사이버안보 연구에 기여함은 물론 지속적으로 발전적인 연구 성과를 기대하게 한다. 그러나 국제정치적으로 접근하는 연구들은 사이버안보가 이미 국제정치의 주요 이슈로 부상한 현재 포괄적인 국제정치적 시각에서의 접근이 충분히 이루어지지 않고 있다. 특히 아직까지 코로나19 팬데믹 상황을 구체적으로 반영하지 못하고 있고, 사이버안보의 국제정치적 추세와 관련한 포스트코로나 시대의 사이버안보 변화를 전망하기에는 미흡한 실정이다. 이제 사이버공간은 국제정치의 주요한 전략영역의 하나이다. 따라서 사이버위협에 대한 시의적절한 전략대응이 필요한 바, 국제정치적 추세를 반영하는 동시에 코로나19 팬데믹이라는 새로운 국제환경 변화를 적시에 반영하는 사이버안보 전략연구가 요구되는 상황이다.

II

사이버안보의 국제정치

1. 사이버공간에 대한 국제정치적 인식
2. 사이버주권과 사이버안보
3. 사이버안보 국제규범

1. 사이버공간에 대한 국제정치적 인식

일반적으로 사이버공간을 어떻게 인식해야 하는지에 대한 논의는 여전히 진행 중이라고 할 수 있다. 사이버공간은 수많은 형태와 개념으로 이해되고 있으나 대체로 다음과 같이 이해되고 있다. 우선 사이버공간은 물질적인 동시에 비물질적이라는 것이다. 우리가 사이버공간에 물질적으로 접촉하고 접촉한 이후에 나타나는 대부분의 현상은 비물질적이라는 것이다. 따라서 사이버공간은 하나의 공간만을 형성하고 있지 않고 현실세계와 연결되고 상호 영향을 미친다. 사이버공간에서는 현실세계에서처럼 개인이나 집단, 국가 등이 행위자로서 활동하고 현실사회와 유사한 질서도 갖고 있지만 물리적인 실체를 갖고 있지는 않다. 그리고 사이버공간은 과거에 없었던 새로운 것이며 따라서 그것이 어디로 발전해 나갈지 알기 어렵다는 것이다. 따라서 사이버공간을 이해하기 위해서는 기술에 대한 이해뿐만 아니라 현실세계의 정치, 경제, 사회, 문화적인 이해도 동시에 요구된다. 사이버공간은 현실세계와 동일하게 인간의 삶에 영향을 미치는 하나의 권력공간인 것이다.[1]

사이버공간에 대한 국제사회의 다양한 인식에 관해 살펴보면, 주요 국가 및 국제기구들은 사이버공간에 대한 정의들을 나름대로 규정해왔다. 미국은 2011년 발표한 사이버공간정책검토에서 사이버공간을 "상호의존적인 정보기술기반시설 네트워크"라고 규정했다.[2] 여기에는 인터넷, 컴퓨터 등 전기통신 시스템과 주요 산업에서 사용되는 프로세서와 제어

1 채재병, 『국제사회의 해킹 변화 추세 및 대응방안』, INSS 연구보고서 2020-17, 2020. p. 17.

2 White House, *Cyberspace Policy Review* (2011), p. 1.

기 등이 포함된다. 북대서양조약기구(NATO)는 탈린매뉴얼에서 "물리적, 비물리적 요소로 구성된 컴퓨터 네트워크를 통하여 컴퓨터와 전자기적 스펙트럼을 이용한 정보의 변경·저장·교류로 특징지어지는 환경"이라고 사이버공간을 규정했다.[3] 국제전기통신연합(ITU)은 "컴퓨터·전기통신·인터넷 네트워크에 직간접적으로 연결된 시스템 및 서비스"라고 사이버공간을 규정했다.[4] 이를 종합하면 사이버공간이 인터넷을 중심으로 컴퓨터 및 전기통신 네트워크를 기반으로 하는 가상의 정보 처리 공간이라는데 주요 국가 및 국제기구들이 대체로 동의하고 있다는 것을 알 수 있다. 다만 사이버공간의 물질적 기반인 단말기와 정보통신 시설 등을 사이버공간에 포함시킬지는 각 국가 및 국제기구들 간에 약간의 견해 차이를 보이고 있다. 미국의 경우에는 단말기 등 하드웨어를 명시적으로 사이버공간의 일부로 포함시키고 있고, 유럽연합(EU)의 경우에도 네트워크와 정보시스템을 규정하면서 하드웨어를 사이버공간에 포함시키고 있다. 반면에 캐나다, 일본 등과 북대서양조약기구, 국제전기통신연합 등은 명시적으로 사이버공간을 가상공간 또는 전자적 세계 등으로 표현함으로써 정보통신기술을 기반으로 한 변경·저장·교류 등의 정보 처리 영역으로 한정시키고 있다.[5]

3 Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Defence Centre of Excellence* (Cambridge University Press, 2013), p. 258.

4 ITU, *National Cybersecurity Strategy Guide* (2011), p. 5.

5 NATO, *NATO 2020: Assured Security; Dynamic Engagement: analysis and recommendations of the group of experts on a new strategic concept for nato* (NATO Public Policy Division, 2010. 5. 17), pp. 5-6.

이와 같이 사이버공간을 규정하는데 있어 아직 국제적으로 명확한 합의에는 도달하지 못하고 있다. 그런데 사이버위협이 행해지는 사이버공간의 의미와 범위를 명확히 규정하는 것은 사이버안보 개념 논의 및 정립을 위한 전제가 된다. 그리고 사이버위협에 대한 대응이 효과적으로 이루어지기 위해서는 사이버안보 개념을 가능한 명확히 정립하여 사이버공격·사이버테러·사이버범죄 등 관련 개념들을 규정하고 그런 규정을 통하여 국내·외의 사이버안보 관련 규범의 적용대상을 구분해내야 한다. 따라서 사이버안보 개념을 정립하기 위해서는 사이버공간에 대한 규정이 우선되어야 하며 결국 사이버공간의 의미와 그 범위를 명확히 파악하는 것이 매우 중요하게 된다.[6] 사이버공간은 현실세계에서의 안보 공간이 영토, 영공, 영해, 우주로 확장되었던 것과 마찬가지로 또 하나의 확장되는 새로운 안보 공간으로 등장했다. 그러나 사이버공간이 갖는 추상적 성격으로 인해 새로운 안보 공간으로서 명확한 개념을 갖지 못하고 있다. 그나마 사이버공간이 네트워크상에 구축된 가상공간으로서 현실세계 전반에 걸친 정보 인프라와 그 안에서 실제로 사용되고 있는 모든 정보를 의미한다고 볼 수 있을 것이다.

사이버공간은 현실세계와 모호하게 연결되어 있기 때문에 가상공간에 국한시킬지 아니면 물질적인 부분 즉 현실공간도 포함시킬지가 문제가 된다. 이는 사이버안보의 대상을 결정짓는 중요한 사안으로 사이버공간을 가상공간에 국한시킨다면 물질적인 피해는 사이버안보의 대상에서 벗어나고 네트워크와 시스템에 대한 전자적 피해만이 대상이 될 것이다. 반면에 물질적인 부분을 사이버공간에 포함시킬 경우에는 정보통신

6 채재병. "안보환경의 변화와 사이버안보."『정치·정보연구』제16권 2호. 2013, pp. 181-182.

기반시설을 포함한 물리적 피해와 정보를 통해 형성된 사회 전반에 걸친 피해가 모두 사이버안보의 대상이 될 것이다. 실제로 사이버공간을 가상공간에 국한시키고 있는 국가들조차도 정보통신기반시설에 대한 피해를 사이버안보 대상으로 간주하고 있다는 점에서 사이버공간은 가상공간과 현실공간의 통합이라고 할 수 있다.

단말기 등을 비롯해 물질적인 시설을 통해서 연결되는 사이버공간을 현실공간과 별개로 보기는 어렵다. 실제 사이버공간은 주로 인터넷으로 연결되고 그 출발은 컴퓨터라고 할 수 있다. 사이버공간이 가상의 정보처리 공간이라고 해도 결국 컴퓨터와 정보통신망을 통한 모든 네트워크와 시스템이다. 사이버공간은 현실공간과 분리시킬 수도 없고 오히려 현실공간과 더 밀접해지고 있는 현실세계와의 유기체적 결합체라고 할 수 있다.[7]

대개 사이버공간에서 발생하는 해킹 등에 의한 피해는 직접적 피해와 간접적 피해로 구분되는데 해킹처럼 전자적 수단에 의한 피해뿐만 아니라 여타 물리적인 수단에 의한 피해도 포함된다. 직접적 피해는 주로 해킹에 의해 이루어지며 물리적으로 정보통신 설비에 대해 가해지는 피해도 포함된다. 간접적 피해는 사이버공간을 원활하게 작동시키고 있는 여러 기반시설에 대한 피해를 말하는데 여기에는 주요 정보통신기반시설과 이와 관련된 일반적인 사회기반시설에 가해지는 피해도 포함된다. 케이블이나 라우터 같은 전산시설은 주요 정보통신기반시설에 당연히 포함되지만 이들을 작동시키는 전력을 공급하는 전력시설 등은 포함여부가 불확실하다. 왜냐하면 이러한 전력시설이 사이버공간을 직접 구성하

7 채재병,『국제사회의 해킹 변화 추세 및 대응방안』, pp. 18-19.

고 있지는 않기 때문이다. 하지만 이러한 전력시설 등이 피해를 입게 되면 사실상 사이버공간이 작동되지 않는 커다란 문제가 발생하게 된다. 따라서 비록 이러한 전력시설 등이 사이버공간의 구성요소는 아니지만 주요 정보통신기반시설에 포함되어야만 사이버공간에 대한 안전을 확보할 수 있게 된다.

이처럼 사이버공간을 어떻게 인식하느냐 하는 문제는 여전히 논쟁거리로 남아 있으며 국제적인 합의도 도출되지 못하고 있는 상황이다. 그러나 사이버공간이라는 가상세계와 현실세계 간의 경계는 허물어지고 있다는 것은 분명하고 양 세계 간의 연결과 서로에 대한 상호의존성도 크게 높아지고 있는 것이 사실이다. 사이버공간에서의 위험이 가상세계뿐만 아니라 현실세계에도 커다란 영향을 미치고 있고 국제사회에 대한 사이버위협은 간과할 수 없게 되었고 이에 대한 대응인 사이버안보 또한 매우 중요해졌다. 국제사회에서 벌어지고 있는 영역 갈등이나 전쟁 그리고 평화와 같은 주요 이슈들이 이제는 가상의 사이버공간에도 나타나고 있는 것이다. 국제사회의 갈등이 사이버 상의 갈등으로 나타나고 이에 대한 사이버공간에서의 제도화 노력도 진행되고 있다. 그리고 이미 4세대 전쟁 시기에 접어들면서 국제사회에서는 육상, 해상, 공중, 우주라는 영역 이외에도 사이버영역에서의 안보체제 구축을 서두르고 있다. 일본의 육·해·공·우주 그리고 사이버 영역에서의 방어체제 구축, 중국의 육·해·공·천·전 5개 영역에서의 방어체제 구축 등이 이러한 맥락에서 추진되고 있는 것이다.[8]

8 Ibid. pp. 19-20.

2. 사이버주권과 사이버안보

전통적인 주권 개념으로 볼 때 주권은 규범적, 실천적 요인을 함께 가지고 있는 역사적인 산물로,[9] 권력, 권위, 합법성, 질서 등과 같은 정치적인 개념들로 구성되어 있다. 주권은 정치적 결사체인 국가의 등장과 동시에 발전하였으며,[10] 국제사회를 구성하는 자격의 부여로 이해될 수 있다. 이에 따라 주권개념이 국가들에게 내재화되고 현실적으로 체험되는 과정은 곧 국가가 국제사회로 편입되는 과정과 그 역사라고 할 수 있다. 대표적으로 주권에 대한 웨스트팔리아적 전통인 대내적 대중성과 대외적 합법성은 시공간적 흐름 속에서 여러 역사적 사건들을 경험하면서 주권의 개념을 발전시켜왔다.[11] 현재 국제사회에서 나타나고 있는 세계화 현상들은 주권의 개념변화를 이끌어오고 있으며 이 과정에서 역사적인 변화과정을 겪고 있는 주권개념과 이에 대한 동양과 서양의 인식 및 적용에서 나타나는 차이점들, 그리고 국제사회에 투영되는 주권의 유형별 특징들은 매우 중요한 의미를 갖는다. 궁극적으로 국제사회의 안정을 위한 제도화가 진행되고 국가들 간에 나타나는 다양한 쟁점들을 해결하기 위한 논의의 장으로서 초국가적인 제도의 등장으로 귀결되었다.[12]

국가들 간 관계의 국제법적 질서를 제공해 준 웨스트팔리아조약(Treaties of Westphalia) 이후 웨스트팔리아적 주권은 영토, 인구, 권위, 인정으로 구성되며, 대외적 배타성, 대내적 권위의 인정, 사법적 독립권, 상호의존적 규제 등을 근거로 주권을 실현시켰다.[13] 웨스트팔리아적 주권은 국민을 전제로 일정한 정치체 내에서 효율적으로 통제할 수 있는 공적 권위체로서의 능력을 가지며 국내의 공식적인 정치적 권위조직이며 국제관계에서 대외적 배타성의 원리가 상호 인정된다는 점에서 중요한 의미를 갖는다. 따라서 웨스트팔리아적 주권 개념은 절대적 주권에 대한 상호 보장을 의미하며 세계화적 국제질서의 관점에서 보면 이러한 주권 개념은 소위 웨스트팔리아적 족쇄라고 할 수 있다. 왜냐하면 국제자본주의의 안정성 확보, 국제 금융의 관리, 유럽에서의 주권통합을 위한 실험, 생태적 환경 보존의 문제 등으로 나타나는 현 국제사회의 주요 현안들은 서구 근대국제체제의 역사적 정체성을 확립해 주었던 웨스트팔리아 주권 개념의 변화이기 때문이다.[14]

안보는 위협의 부재라고 할 수 있는데,[15] 이러한 위협의 부재는 근대국제체제 이후 냉전적 국제질서에서 웨스트팔리아적 주권 개념을 기반으로 하였다. 전쟁과 관련한 대내적 합의는 전통적인 주권 개념이 무너지면서 그 정당성을 획득하였고, 개별 국가의 주권에 대한 대외적 독립성과 대내적 질서를 인정함으로써 국제사회에 반영되었다. 국제사회는 안보 확보를 위해 주권에 대한 존중을 합의한 것이다. 그러나 탈냉전적 안보는 이러한 국제사회의 합의를 근본적으로 변화시켰다. 다시 말해 안보 차원에서 주권이 구체화되는 실천양식이 변하고 전쟁 요인과 전쟁 수행

9 Joseph A. Camilleri, & Jim Falk, *The End of Sovereignty?* (Aldershot: Edward Elgar, 1992).

10 Jorge A. Bartelson, *Genealogy of Sovereignty* (Cambridge: Cambridge University Press, 1995).

11 Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (Princeton: Princeton University Press, 1999).

12 채재병 외, 『주변국의 사이버 환경과 한반도 평화체제 구축』, KINU 연구총서 19-29, 2019. pp. 36-37.

13 Stephen D. Krasner, Sovereignty: Organized Hypocrisy.

14 채재병 외, 『주변국의 사이버 환경과 한반도 평화체제 구축』, pp. 40-41.

15 Barry Buzan, *People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era* (Colorado: Lynne Rienner Publisher, 1991) p. 363.

의 정당성 근거도 변한다는 점은 웨스트팔리아적 주권 개념에 근본적인 변화가 일어나고 있다는 것이다. 인종, 종교, 권위의 부재, 빈곤 등 다양한 차원에서 안보를 위협하고 있는 안보부재는 국제질서의 세계화적 변화의 원인인 동시에 결과라고 할 수 있다. 탈냉전적 국제사회에서 발생하는 전쟁의 원인들은 웨스트팔리아적 관점에서 주권의 대외적 독립성에 대한 부정이며, 웨스트팔리아적 주권 개념은 안보에 대한 합의의 주요한 토대가 되었다. 주권 개념의 발달을 통해 국가들 간의 서로 다른 이해관계를 조정하고 안정적인 국제관계를 유지할 수 있다. 유럽연합의 등장은 주권 개념의 확장과 국내외적 문제들에 대한 탈주권적 해석이 이루어짐으로써 가능했다. 탈냉전적 국제상황은 국가들로 하여금 주권의 개념적 구성을 고민하게 했으며 국제관계의 다양한 변화요인들로 인해 국가들 간의 안정적인 국제질서를 모색할 시기이다.

이와 같은 전통적인 주권 개념이 과연 사이버공간에서도 통용될 수 있는지 그리고 사이버공간에서의 주권 개념이 현실공간의 안보차원에서의 주권 개념과 어떠한 차이점 또는 공통점이 있는지 살펴볼 필요가 있다. 이를 위해 우선 안보개념의 확장이라는 측면에서 사이버안보를 살펴본다. 일반적으로 사이버안보란 사이버공간을 해킹을 비롯한 다양한 형태의 공격으로부터 보호하는 것이라고 할 수 있다. 따라서 사이버공간에 대한 공격으로부터 국가와 국민을 보호하기 위한 모든 수단들의 집합이라고 할 수 있다. 그런데 사이버라는 용어가 추상적인 개념이라 현실에 적용하기 쉽지 않기 때문에 실제 사이버안보 개념을 논의하는 것은 어렵다. 사이버라는 용어는 컴퓨터와 인터넷 등을 기반으로 하는 정보통신망과 이를 통해 실현되는 가상공간 등 정보통신기술과 관련된 거의 모든 것을 의미한다. 이러한 사이버라는 용어의 추상적인 성격은 현실세계

와 가상세계의 경계를 모호하게 만들었고 사이버공간에 대한 규정도 어렵게 하고 있다. 현재 사이버공간이 무엇인지에 대한 명확한 정의도 존재하지 않는 상황에서 이와 관련된 사이버안보 개념을 논의한다는 것은 매우 어려운 일이다. 실제로 사이버안보를 규정하는 국제적 합의는 아직 도출되지 않고 있으며, 다수의 국가들과 국제기구들이 사이버안보에 관한 다양한 개념들을 언급하고 있다. 또한 대부분의 국가들은 안보전략상의 이유로 사이버안보 및 관련 개념들에 대해 규정하지 않고 있기도 하다.[16] 다만 각국에서 발표한 사이버안보 전략의 범위와 내용들을 살펴보면, 사이버공간의 개념을 보다 광범위하게 받아들여 기존의 정보통신망, 정보, 정보통신기술 보호 등 특정 영역에 대한 보호에서 벗어나 사이버안보의 개념을 확장하고 있다는 것을 알 수 있다. 즉 과거에는 사이버공간의 안전을 정보통신망. 정보, 정보시스템 보호로 인식하고 있었던데 반해 국가 차원에서 사이버안보 개념을 인식하여 국가 사이버공간에 대한 다양한 위협으로부터 안전을 확보하는 조치로 보고 있는 것이다.

포괄사이버안보 개념은 사이버안보를 정보보호 등보다 좀 더 폭넓은 범위로 발전시키고 있다. 사이버공간의 안전을 위해서는 정보보호가 필수적이지만 좀 더 포괄적으로 정보뿐만 아니라 정보통신망 등의 안전도 사이버안보의 핵심요소가 되었다. 따라서 포괄사이버안보 개념은 보호대상에 있어서 기존과 같이 정보의 안전성 보장에 중점을 두기 보다는 현실세계에서와 마찬가지로 전반적인 사이버공간에서 안전을 보장하는데 중점을 두었다. 사이버공간을 독립된 영역으로 보지 않고 현실공간

16 ENISA, *National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace* (2012. 5), p. 5.

과 연결되어 있는 유기적 공간으로 보고 있기 때문에 사이버공간에서의 안보는 기존의 보호개념보다는 더 확장될 수밖에 없는 것이다. 여기에는 기존의 정보보호에 더하여 정보통신망에 대한 보호도 필요하며 결국 사이버안보의 보호대상은 사이버공간에서 저장되고 이용되고 전송되는 정보만이 아니라 사이버공간 그 자체에 대한 안전도 중요한 것이다.

안보차원에서 주권은 당연히 웨스트팔리아적 주권 개념에서 비롯된다. 그런데 안보가 단순히 국가관리 차원을 넘어 주권을 더 확장하기 위해 포괄적인 전략을 구사한다는 점, 다시 말해 육상, 해상, 공중, 우주를 포함하는 전 영역에서의 안전보장과 지역안보 및 전 세계적 차원의 안보를 추구하고 정치, 경제, 사회, 문화 등 전 분야에서의 안보를 추구한다는 점에서 안보는 포괄안보 차원에서 추진되고 있는 것이다. 이는 안보차원에서의 주권 개념이 웨스트팔리아적 주권 개념의 변화를 통해 안보개념의 확장으로 나아가고 있음을 보여준다.[17]

안보차원에서의 주권 개념이 사이버공간의 특수성으로 인해 현실공간과 마찬가지로 사이버공간에 그대로 적용될 수는 없을 것이다. 그렇지만 안보가 주권과 주권의 충돌이라는 점에서 이를 논리적으로 확장해보면 사이버공간에서도 주권이 충돌하는 지점이 존재하므로 사이버공간에서의 주권개념도 안보차원에서의 주권개념과 연결될 수 있다고 볼 수 있다. 특히 사이버안보가 포괄적인 차원에서 안보와 마찬가지로 전개되고 있다는 점에서 더욱 그러하다. 그리고 사이버공간에서의 주권개념과 안보차원에서의 주권개념은 주권의 정체성이라는 측면에서 볼 때 사실상 별다른 차이가 없다. 물론 사이버공간에서의 주권개념을 현실공간의 안

17 채재병 외, 『주변국의 사이버 환경과 한반도 평화체제 구축』, pp. 44-45.

보차원에서의 주권개념과 동일시할 수 없는 부분도 있다. 이는 사이버공간의 특수성 때문이며 우선 사이버국가의 존재가 가능하느냐의 문제이다. 사이버공간에서 이러한 물리적 구분은 상당히 어려운 일이며 우선 사이버공간에서 나타나는 현상들은 가시적이지 않다는 점이다. 그렇다고 눈에 보이지 않으므로 발생하지 않는 것은 아니며 더욱이 발생하는 현상들이 감지되지 않는 것도 아니다. 사이버공간에서의 현상들은 대개의 경우 현실세계로 이어지며 사이버공간에서의 분쟁이 보이지는 않지만 주권과 주권의 충돌이 일어났으며 실제로 존재하는 것이다. 이런 이유로 주권의 정체성이라는 측면에서 볼 때 사이버공간의 주권개념과 안보차원에서의 주권개념은 사실상 동일하다고 할 수도 있을 것이다.

사이버안보와 관련된 논의는 사이버공간이라는 새로운 안보영역이 현실공간에서의 국가와 밀접하게 연결되어 있으며 안보와 상관성을 갖고 있다는 것을 보여준다. 국가라는 현실공간은 현실보다도 더 현실과 밀접한 가상현실의 공간과 결합되어 있고 새로운 공간 네트워크를 만들어 내고 있다. 이와 같은 불가분의 관계에 있는 현실공간과 가상공간은 서로 확장된 공간만큼이나 다양한 위협들에 노출되어 있다. 이와 같은 안보개념의 확장은 안보개념 변화 과정을 통해서도 이해될 수 있다. 안보개념 변화는 냉전이 종식된 이후 안보에 대한 인식이 변화되면서 시작되었다. 안보인식의 변화는 우선 안보의 대상 즉 위협하는 주체가 무엇인지에 대한 인식의 변화이다. 그리고 안보의 내용 즉 무엇을 어디까지 보호해야 하느냐에 대한 인식의 변화이다. 마지막으로 안보의 추구방법, 즉 위협 방지를 위한 수단이 무엇이냐에 대한 인식의 변화이다. 구체적으로 안보의 대상은 적국으로부터 주권, 영토, 국민의 생명과 재산 등에 대한 보호라는 국가 중심적 시각에서 테러, 기근, 질병, 환경오염 등 초국가적

위협으로부터의 보호로 변화했다. 안보의 내용은 이러한 초국가적 위협으로 인해 군사적 안보 이외에도 경제안보, 환경안보, 사회안보, 인간안보 등을 포함하는 포괄안보로 변화했다. 안보의 추구방법은 위협에 대처하기 위해 동맹체제를 통한 힘에 의존한 안보에서 초국가적 위협에 대응하는 관계국들 간 협력안보로 변화했다. 국가 중심적이고 군사력에 의존하는 전통안보로부터 초국가적, 비군사적인 비전통안보로 변화했다. 이는 냉전 이후 종교, 인종, 문화, 자원 등을 둘러싼 분쟁이 분출되면서 테러, 국제범죄, 난민, 환경문제 등과 같은 초국가적 위협들이 크게 나타났기 때문이다. 그리고 새로운 사회 문제들이 안보를 위협하는 국제안보환경의 변화 상황에서 포괄안보개념이 크게 부상하였다.[18] 따라서 냉전 이후 국제사회에는 군사문제 외에 테러, 국제범죄, 환경, 자원 등을 대상으로 하는 포괄안보가 핵심 안보개념으로 확립되었다.[19] 즉 냉전기의 안보개념이 군사적인 차원에서의 외부 위협에 대한 대응이었다면 탈냉전기에는 환경, 자원, 경제, 사회 문제 등 비군사적인 요소들을 포함하는 개념으로 변화한 것이다.[20] 포괄안보 개념은 군사안보와 비군사안보 요소를 포괄하여 안보정책을 추진한다는 점에서 비전통안보 개념으로 볼 수 있다. 포괄안보는 군사안보와 비군사안보 간의 조화에 의해 안보정책목표를 달성하고자 한다. 포괄안보 개념을 통해 안보의 범위가 크게 확대되었고 이제 안보는 정치와 군사뿐만 아니라 환경, 경제, 사회 등 각 분야를 포괄하지 않고서는 이해할 수 없는 개념이 되었다.[21] 반면 이와 같은 안보개념의 변화는 위협의 주체가 다양해지고 위협요인이 다양해짐에 따라 어떤 대상에 대해 어떻게 대응해야 할지 훨씬 더 복잡해졌고 안보의 개념과 목표를 불투명하게 만드는 결과를 초래하기도 했다.

이러한 안보 개념의 변화에 토대를 두고 있는 안보 개념의 확장과 동일한 범주에서 사이버안보도 출발하고 있다. 사이버위협은 냉전 종식 이후 비약적인 정보통신기술의 발전에 기인하여 안보개념의 변화 속에서 나타난 새로운 안보위협이라고 할 수 있다. 실제로 사이버안보에 대한 논의는 지금까지 앞에서 언급한 안보개념 논의 과정에 따라 안보와 유사한 경로를 통해 전개되어왔다. 안보의 대상, 내용, 추구방법의 변화는 사이버안보의 변화양상과 거의 일치하고 있다. 또한 해킹 등의 사이버위협은 테러와 거의 동일한 속성을 갖고 있는데 테러와 마찬가지로 사이버위협은 공격과 방어를 하는데 있어 비대칭성을 갖고 있다는 점에서 특히 그러하다. 이와 같은 이유로 해킹 등의 사이버위협이 현실화되었을 때 이것이 사이버테러라는 이름으로 이슈화되었고 현재도 테러의 영역에서 다루어지고 있는 것이다. 또한 해킹의 주체가 개인이나 집단, 그리고 국가차원에서도 이루어지고 있다는 점이 테러와 유사하며 그 피해에 있어서도 막대하다는 것이 유사하다. 이러한 유사성 때문에 해킹 등의 사이버위협이 사이버테러라는 이름으로 아직까지도 테러리즘의 영역에서 논의되고 있지만 향후에는 새로운 방향에서 사이버안보에 관한 논의로 전개될 것이다. 왜냐하면 사이버안보는 사이버공간이라는 가상공간 영역

18 Richard N. Haas, "Paradigm Lost," *Foreign Affairs*, Vol. 74, No. 1 (Jan./Feb. 1995), pp. 43-58.

19 Carolyn M. Stephenson, "New Approaches to International Peacemaking in the Post-Cold War World," in Michael T. Klare (eds.), *Peace & World Security Studies: A Curriculum Guide* (Boulder: Lynne Rienner Publisher, 6th ed, 1994), p. 18.

20 Kanti Bajpai, "The Idea of Human Security", *International Studies*, Vol. 40(3), p. 223.

21 Barry Buzan, *People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era* , p. 363.

을 갖고 있어서 기존에 논의되는 안보영역과는 별개의 완전히 새로운 영역이기 때문이다. 또한 사이버안보는 현실 안보 차원에서 다루어져야 하고, 군사적, 비군사적 수단이 함께 사용되어야 하는 대처방법이나 수단을 효과적으로 구사하기 위해서는 반드시 국제협력이 필요하다는 점에서 안보개념의 확장이라는 측면에서 접근해야 한다.[22] 이러한 사이버안보의 특성은 안보 개념의 확장과 연결되고 현실공간과 가상공간을 연계해주는 동시에 사이버공간에서 안보 개념을 정립할 수 있는 근거를 제공해준다. 사이버공간에서의 안보 개념의 적용이 동일할 수는 없겠지만 안보개념의 재정립이라는 관점에서 사이버공간과 안보의 상관성을 찾을 수도 있을 것이다.

3. 사이버안보 국제규범

사이버안보와 관련된 국제규범에 대한 논의는 국제법 및 국제기구와 연관된 탈린매뉴얼(Tallinn Manuel), 유엔 정부전문가그룹(GGE) 활동, 정부 간 협의체로서 사이버공간총회(Conference on Cyberspace), 유럽사이버범죄협약(COC), 그리고 글로벌 거버넌스로서의 상하이협력기구(SCO), 국제인터넷주소관리기구(ICANN), 국제전기통신연합(ITU) 등을 통해 전개되었다.

기존 국제사회의 국제법을 사이버공간에 적용하여 사이버공간에서 발생하는 사이버공격에 대응하려고 시도한 것이 바로 탈린매뉴얼

22 Joseph S. Nye Jr., "Power and National Security in Cyberspace," in Kristin M. Lord and Travis Sharp (eds.), *America's Cyber Future: Security and Prosperity in the Information Age*, Vol. II (Center for a New American Security, June 2011), p. 9.

(Tallinn Manuel)이다. 탈린매뉴얼 1.0은 나토 합동사이버방어센터(Cooperative Cyber Defence Centre of Excellence, CCDCOE)가 주도하여 국제법 전문가들의 공동연구를 통해 2013년 3월에 발표한 사이버안보 관련 매뉴얼이다. 탈린매뉴얼 1.0은 주로 사이버전과 관련해 연구한 결과이기 때문에 기존의 국제법 중에서 전쟁법이 사이버공간에서도 적용할 수 있는지 검토했다. 여기서 사이버전이란 국가들을 주체로 사이버공간에서 사이버공격을 하는 행위로 상대국에 인명피해나 시설손상 등의 물리적 피해를 가하는 것을 뜻한다. 탈린매뉴얼 1.0은 기존 국제법을 적용하여 사이버공간에서의 무력행위를 정의하였기 때문에 새로운 국제법을 만들지는 않았다. 따라서 기존 국제법이 사이버공간에 그대로 적용될 수 있는지는 논란의 여지가 있지만 새로운 법을 둘러싼 논란은 애초에 배제시키고 있다.[23]

탈린매뉴얼 1.0이 주장하는 주요 핵심 사항은 사이버공간에서도 기존의 교전수칙이 적용될 수 있고, 사이버공격으로 인해 인명 피해가 발생하면 공격국가에 대해 군사적으로 보복할 수 도 있다는 것이다. 또한 비국가 행위자들에 대해서도 마찬가지라는 것이다. 나아가 사이버공격을 위한 편의를 제공한 국가 등에 대해서도 기존의 국제법을 적용하여 처벌할 수 있다는 것이다.[24] 탈린매뉴얼 1.0이 발표되자 사이버공간에서의 무력행위를 어떤 기준으로 규정할 수 있는지, 그리고 사이버공격의 주체를 확인한다고 해도 과연 그 소재지나 경유지가 책임이 있는지, 또 어떤

23 Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Defence Centre of Excellence*.

24 Ibid.

책임의 수준과 처벌의 수준을 정할 기준은 무엇인지 등의 많은 문제점이 제기되었다.[25] 사실 탈린매뉴얼 1.0은 구속력도 없으면서 그나마 사이버전에서의 국제법적인 교전수칙을 마련하려는 의도였지만 그마저도 어려운 상황이 되었다. 실제 2007년 에스토니아 사태가 계기였으며 참여한 인원도 주로 북대서양조약기구 회원국의 전문가들이었기 때문에 중국과 러시아 등 비서방진영을 배제하고 서방진영의 입장에 충실했다는 비판으로부터도 자유로울 수 없다.[26]

2017년 2월 발표된 탈린매뉴얼 2.0은 사이버 작전에 적용 가능한 국제법을 검토한 것이다. 여기서 사이버전(cyber warfare)이란 국가 간 사이버전쟁을 뜻하고 사이버 작전(cyber operation)이란 초국경적 사이버범죄에 대한 대응을 뜻한다. 사실 탈린매뉴얼 1.0이 다룬 사이버전은 전쟁법을 통해 다룬 사이버공격 사태가 없다는 점에서 알 수 있듯이 아직 발생한 적도 없고 또 앞으로 발생할 가능성도 그리 많지 않다. 그렇지만 지금도 그렇고 앞으로도 수많은 사이버공격이 행해지고 많은 피해가 발생할 것이다. 그렇다면 이와 같은 사이버공격에 대해서는 어떻게 해야 할 것인지 검토해야 하는데 바로 탈린매뉴얼 2.0이 이와 같은 수준의 사이버공격에 대해 어떻게 국제법을 적용해야 하는지에 대해서 검토한 것이다.[27]

25 김상배 외.『사이버 안보의 국가전략: 국제정치학의 시각』. 서울: 사회평론, 2017. p. 33.

26 김상배 외.『사이버 안보의 국가전략 2.0』. 서울: 사회평론, 2019. p. 31.

27 Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, MA: Cambridge University Press.. 2017)

2004년부터 시작된 유엔 정부전문가그룹(Group of Governmental Experts, GGE)은 국제연합(UN) 차원에서 사이버안보 문제를 논의하고 있는데 제1차와 제2차의 경우 당시만 해도 국가가 인터넷을 통제하는 입장의 중국, 러시아 등 비서방진영과 반대 입장의 미국을 비롯한 서방진영이 첨예하게 대립하고 있었다. 그런데 2013년 6월 제3차 유엔 정부전문가그룹에서 합의한 보고서에서는 참여국들이 사이버공간에서도 기존 국제법이 적용될 수 있다는 점에 합의하고, 이러한 규범을 어떻게 적용할지는 계속 연구한다는데 합의했다. 이는 상당히 주목할 만 한 점으로 사실 이런 내용은 처음에 러시아가 먼저 제안했었는데 당시 미국은 이러한 사이버안보 관련 국제협력에 대해 상당히 소극적으로 대응했었다. 그런데 입장에 변화를 보이면서 제3차 유엔 정부전문가그룹에서는 합의에 도달한 것이다.[28]

사실 중국과 러시아도 처음에는 기존 국제법이 사이버공간에 적용될 수 없다는 입장이었고 따라서 새로운 규범이 만들어지지 않으면 사이버공간에서의 규범은 없다는 주장이었다. 그런데 제3차 유엔 정부전문가그룹에서는 러시아와 중국이 입장 변화를 보여 기존 국제법을 사이버공간에 적용할 수 있다고 합의한 것이다. 동시에 미국과 유럽 국가들도 사이버공간에서 국가주권과 불간섭원칙을 인정하지는 않았지만 제3차 유엔 정부전문가그룹을 계기로 사이버공간에서의 국가책임성을 부정하지는 않는 입장 선회를 보였다. 결국 기존 국제법이 사이버공간에 적용될 수 있는지에 대한 서방진영과 비서방진영 간의 논란이 양측의 입장 변화

28 장노순. "사이버안보와 국제규범의 발전: 정부전문가그룹(GGE)의 활동을 중심으로."『정치·정보연구』제19권 1호. 2016. pp.10-17

를 통해 합의점을 찾는 양상이 되었다. 기존 국제법이 사이버공간에도 적용된다고 보고서에도 명시됨으로써 앞으로 큰 논란은 없을 것으로 보인다.[29]

제3차 유엔 정부전문가그룹 보고서를 계승한 2015년 6월 제4차 유엔 정부전문가그룹에서는 더 나아가 보고서에 사이버공간의 국제규범에 관한 논의를 국제법과 규범 부문으로 분리했으며 유엔헌장 등 국제법의 기본원칙인 주권평등, 국제관계에서 무력사용의 자제, 국제분쟁의 평화적 해결, 인권과 기본적 자유의 존중, 국내문제 불간섭 등이 사이버공간에서도 동일하게 적용된다는 것을 적시했다. 그리고 국제법 원칙, 자위권, 관할권, 국제인도법, 대리자 및 국가책임에 관한 6가지 항목도 제시했다. 그러나 이러한 국제법 원칙들이 어떻게 적용되는지에 대해서는 서방진영 국가들과 비서방진영 국가들의 입장 차이가 커서 이를 구체적으로 논의하지는 못했다.[30]

2016년 제5차 유엔 정부전문가그룹은 제4차 보고서에서 합의한 내용을 유지하면서 구체화시켰지만 서방진영과 비서방진영 국가들 간에 자위권, 국제인도법, 대응조치의 허용, 사이버테러·범죄와 인터넷 거버넌스 등을 의제에 포함시킬지의 여부 등에 대해 합의점을 찾지는 못했다. 제5차 유엔 정부전문가그룹에서는 서방진영의 국가들 간에도 입장이 일치하지 않는 내용들이 다수 제기되었는데, 소위 적절한 성의의 성격을 규정하는 문제를 비롯해 데이터 관할권 문제, 사이버기술 수출통제 규범 제정 문제, 비정부 행위자에 대한 사이버 공격무기 사용금지에 관한 규범 제정 문제 등이었다. 결국 2017년 6월 서방과 비서방 진영 간의 의견이 지속적으로 대립하여 보고서 채택에는 실패하였다. 최종회의에서 합의 도출에 실패한 핵심 의제는 국제법 적용 및 향후 계획이었는데, 미국은 이미 제4차 보고서를 근거로 미국에 유리하게 국제법 해석을 할 수 있는 상황이었기 때문에 굳이 중국과 러시아 등이 주장하는 개방형 워킹그룹 창설 및 유엔의 역할 확대를 수용할 필요가 없었다. 반면 중국과 러시아도 상세하게 제시된 국제법적 요소를 수용할 필요가 없었다.[31]

사이버안보와 관련된 직접적인 이해당사국들이 모여 사이버공간이라는 포괄적 의제를 명시적으로 논의한 최초의 회의인 사이버공간총회(Conference on Cyberspace)가 2011년 출범했다. 유엔 정부전문가그룹 활동이 국가 간 안보문제를 주로 논의했던 반면 사이버공간총회는 각국 정부가 주도하지만 다양한 민간 행위자들이 참여하여 안보 이외의 다양한 의제들을 포괄적으로 논의하였다. 따라서 사이버공간총회는 정치적, 외교적 합의를 도출하는 것 이외에도 사이버공간에서 나타나는 인권문제나 경제적, 사회적 이익 등 다양한 의제를 함께 논의할 수 있었다. 회의가 지속적으로 개최되면서 회의에 참여하는 주체들도 증가하고 관련 논의도 매우 활발하게 진행되었지만 회의 성격 자체가 공식적인 국제기구가 아니라는 점과 그때그때 바뀌는 주최국과 참여국의 구성에 따라 회의가 진행되는 포럼 형식이라는 점에서 회의의 위상이 다소 모호하게 되고 있는 것은 문제점으로 지적되었다.[32]

29 김상배 외. 『사이버 안보의 국가전략 2.0』. p. 33.

30 Ibid. p. 34.

31 Ibid. p. 35.

32 배영자. "사이버안보 국제규범에 관한 연구." 『21세기정치학회보』 제27집 1호. 2017. pp.105-106.

각국 정부들이 사이버범죄에 대응해 서로의 법제도를 조율하는 정부 간 네트워크로는 2001년 미국과 유럽평의회(Council of Europe)가 주도해서 합의한 유럽사이버범죄협약(European Convention on Cybercrime, COC), 일명 부다페스트 협약을 들 수 있다. 인터넷을 이용한 모든 범죄들에 대해 규정하고 그에 따른 처벌을 명시적으로 제시한 국제협약은 부다페스트 협약이 최초라고 할 수 있다. 2004년 공식 발효된 부다페스트 협약은 초국경적인 사이버범죄를 수사하기 위한 국제공조를 목표로 한 것으로 당시 세계 각국은 이러한 사이버범죄에 대응하는데 어려움을 겪고 있었다. 초국경적 사이버범죄는 사이버공간에서 행해지는 디도스, 해킹, 피싱, 스미싱 등의 각종 사이버공격들이 하나의 국가 내에서가 아니라 해외에 근거지를 두거나 해외로 우회하여 공격이 이루어지는 사례들을 말한다. 이러한 사이버범죄는 국가 간 형사사법공조를 통해 수사할 수는 있으나 많은 시간을 소비하는 경우가 대부분이다. 왜냐하면 이러한 사이버범죄는 신속한 수사가 생명인데 이를 위한 신속한 정보교환이 사실상 매우 어렵다. 따라서 부다페스트 협약에 가입한 국가들은 서로간에 신속한 정보공유가 가능하기 때문에 사이버범죄를 추적할 수 있는 각종 전자정보를 공유하여 이러한 사이버범죄에 공동으로 대응할 수 있다. 현재까지 부다페스트 협약에는 미국·영국·독일·프랑스·일본 등 세계 71개국이 가입한 상태이지만 한국은 아직 가입하지 않고 있다.[33]

33 채재병, "'바르샤바 프로세스'와 사이버안보협력: 전망과 시사점," 『이슈브리프』 통권 154호 국가안보전략연구원 (2019. 10. 30.).

2001년 7월에 설립된 지역협력기구인 상하이협력기구(Shanghai Cooperation Organization, SCO)는 중국, 러시아, 카자흐스탄, 우즈베키스탄, 키르기스스탄, 타지키스탄 6개국으로 구성되었다. 상하이협력기구는 미국이나 유럽 국가들의 입장과는 다른 중국과 러시아 등의 입장을 잘 보여주고 있기 때문에 사이버안보의 국제규범 형성과정에서 상당한 주목을 받고 있다. 2000년대 중반부터 지속적으로 사이버안보를 위한 지역협력을 강조해오고 있는 상하이협력기구는 2009년 6월 러시아 예카테린부르크에서 열린 상하이협력기구 정상회담에서 국제정보보안강화협력에 대한 협정, 일명 예카테린부르크협정을 체결했다. 이 협정은 사이버공간의 주요 위협에 대한 정의, 국가이익과 관련된 정보통신기술의 사용 등 사이버안보에 관한 포괄적인 지역협정 구상을 제시하고 있다.[34]

초기부터 인터넷을 관리해온 국제인터넷주소관리기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 미국 소재 비영리 민간기관으로 미국을 중심으로 시작된 인터넷 분야의 제도 형성 과정에서 등장했다. 인터넷 초창기에는 자율적 거버넌스를 주장하는 비국가 행위자들이 인터넷 관리에서 중요한 역할을 담당했는데 바로 국제인터넷주소관리기구가 그 대표적 사례이다. 따라서 국제인터넷주소관리기구는 도메인이름체계(DNS), 최상위도메인 생성 및 관리기관 위임, DNS루트서버 관리, 도메인 및 IP주소 관련 정책개발 등을 주요 업무로 하고 있다. 1998년 미국 상무성이 비영리 민간법인으로 설립했던 국제인터넷주소관리기구는 2009년에 인터넷주소관리체계를 자율적으

34 김상배 외. 『사이버 안보의 국가전략 2.0』. p. 40.

로 운용하는 의무협약을 상무성과 체결하여 명실공히 개인, 전문가집단, 기업, 시민사회 등 다수의 이해관계자가 참여하는 글로벌 거버넌스로 전환하였다.[35]

국제인터넷주소관리기구는 설립 초기부터 미국에 편향되어 있다는 비난을 받았다. 미국 주도로 인터넷 자체가 추진된 상황에서 피할 수 없는 일이라고 볼 수도 있다. 이로 인해 국제인터넷주소관리기구를 개혁해야 한다는 요구가 국제사회에서 꾸준히 제기되어왔다. 이런 상황 속에서 2013년 에드워드 스노든의 폭로 사건은 미국에 큰 부담으로 작용했고 마침내 미국은 국제인터넷주소관리기구에 대한 개혁을 받아들일 수밖에 없게 되었다. 미국은 국제인터넷주소관리기구에 대한 감독 권한을 각국 정부와는 무관한 이해당사자들로 구성된 감시기구에 넘기기로 했다. 이 경우 가장 큰 문제는 인터넷할당번호관리기관(Internet Assigned Numbers Authority, IANA)의 관리권한을 넘기는 문제였다. 인터넷할당번호관리기관의 관리권한이란 IP주소, 도메인이름 등에 대한 관리기능이 주를 이루는데 IP주소의 경우 기술적이고 비정치적인 분야이기 때문에 권한을 이전하는데 별다른 문제가 없다고 할 수 있다. 그러나 도메인이름의 경우 일반 이용자가 인터넷에 접속하는 수단인데다가 상표권이나 표현의 자유 등 법률적인 문제가 있고 국가적인 이해관계도 상이하므로 각국 정부는 예민하게 반응할 수밖에 없다. 마침내 미국은 2016년에 인터넷할당번호관리기관의 관리권한을 46년 만에 민간에 이양했다.[36]

35 Ibid. pp. 44-45.

36 배영자. "사이버안보 국제규범에 관한 연구." pp.126-127.

인터넷 거버넌스 분야의 개혁을 위해 국제인터넷주소관리기구의 대안을 찾는 상황에서 기존의 관련 국제기구들이 가세하였다. 특히 오랜 기간 전기통신 분야에서 중심 역할을 해오던 유엔 산하의 국제전기통신연합(International Telecommunication Union, ITU)의 움직임이 주목할 만하다. 1932년 유선통신에 대한 국제협력을 도모하기 위해 설립된 국제전기통신연합은 기술발달로 인해 활동영역이 유무선 통신뿐만 아니라 전파, 위성 분야 전반으로 널리 확대되어왔다. 국제전기통신연합은 2003년 제네바, 2005년 튀니스에서 개최된 정보사회세계정상회의(World Summit on Information Society, WSIS)를 계기로 인터넷 거버넌스 분야에 적극적으로 개입하기 시작했다. 정보사회세계정상회의에서 제기된 다양한 이슈들 중에서도 인터넷에 대한 관리 문제와 국제인터넷주소관리기구의 개혁 문제가 가장 큰 쟁점으로 부각되었다. 그러나 회의에서는 네트워크 보안의 신뢰성 강화, 범죄와 테러 목적의 사용 예방, 프라이버시 및 고객보호, 스팸 대응 등 인터넷 관리 문제가 주로 논의되었다. 국제인터넷주소관리기구의 개혁 문제에 대해서는 별다른 진전을 보지 못한 대신 인터넷거버넌스포럼(Internet Governance Forum, IGF)을 제안하여 지속적으로 인터넷 관련 정책을 논의할 수 있게 하였다.[37]

37 김상배 외. 『사이버 안보의 국가전략 2.0』. p. 47.

III

사이버안보의 국제정치적 추세

1. 미중경쟁 속 사이버안보
2. 코로나19 팬데믹에 따른 사이버공격 양상
3. 포스트코로나 시대의 사이버안보

1. 미중경쟁 속 사이버안보

국제사회에서 사이버안보를 둘러싼 국가 간 경쟁은 세계 패권을 두고 다투는 미중관계의 주요 이슈로 대두되었다. 현실공간에서의 강대국의 지위를 사이버공간에서도 확보하기 위해 미국과 중국은 선도적인 사이버전력을 추구하고 있다. 동시에 서로 간의 우위를 점하기 위한 치열한 경쟁과 공방을 지속하고 있다. 현실공간에서 국제정치의 핵심이 미중관계 즉 미중 간 패권경쟁이듯이 사이버공간에서의 사이버안보의 국제정치 또한 미중관계가 그 핵심이다. 따라서 사이버안보의 국제정치적 추세를 이해하기 위해서는 현실 국제정치에서의 미중관계가 반영된 미중 사이버안보 관계를 살펴볼 필요가 있는 것이다.[38]

미중 간 사이버갈등이 본격적으로 시작된 것은 2000년대 중반 이후로 미국은 중국 해커 위협론을, 중국은 미국 기술패권 경계론을 주장하고 나섰다. 중국 해커 위협론이란 중국 정부와 군의 지원을 받고 있는 중국의 해커들이 해킹을 통해 미국의 정부 및 공공기관, 인프라, 기업정보 등을 탈취하고 있다는 것이다. 2009년 발생한 오로라 공격(Aurora attack)이라는 해킹 사건은 중국 해커들이 구글과 같은 미국의 주요 기업을 해킹한 기술정보 탈취사건이라는 것이다.[39] 2010년 초에 구글이 중국에서 철수한 사건도 중국 해커들의 개입으로 보고 있다.[40] 반면 미국 기술패권 경계론이란 정보통신기술 분야에서 미국의 기술패권에 대

38 고경민·정영애. "미·중 사이버안보와 프레임워크 형성의 역사적 다이내믹스," JOURNAL OF PLATFORM TECHNOLOGY, 5(4), 2017. p. 82.

39 김상배. "사이버 안보의 미중관계." 『한국정치학회보』, 49(1), 2015. p. 78.

40 조현석, "미중 사이버 안보 협약 연구," 『21세기정치학회보』, 27(2), 2017. p. 217.

한 중국의 우려에서 출발한다. 중국은 인터넷 보안기술을 미국의 정보통신기업들에 지나치게 의존하고 있는 상황에서 미국 기업의 컴퓨터와 네트워크 장비의 보안문제를 우려하고 있다. 특히 시스코, 퀄컴, 마이크로소프트, 구글, 페이스북 등 미국의 정보통신기업들이 사이버공간으로 통하는 중요한 기술들을 거의 독점하다시피 하고 있는 상황에서 이들 기업들은 미중 간 사이버갈등이 격화되는 상황에서는 중국에 등을 돌릴 것이 분명하기 때문이다.[41]

이와 같이 상반된 입장의 미중 간 사이버갈등을 살펴보면, 미국은 2010년대에 들어와 중국의 해킹 공격에 대해 더욱 거칠게 비난하면서 마침내 2011년 5월 사이버공간 국제전략(International Strategy for Cyberspace)을 발표하였다. 특히 7월에 발표된 미 국방부의 사이버 국방전략에서는 사이버공간을 제5의 전쟁 영역으로 제시하기에 이르렀다.[42] 이처럼 미중 간 사이버갈등이 심화되는 상황에서 지난 2010년 발생했던 이란에 대한 스턱스넷 공격이 미국과 이스라엘의 합작 공격이라는 사실이 드러났다.[43] 미국의 사이버공격 능력에 대한 중국의 우려는 더욱 커졌으며,[44] 사이버공간을 군사적 공간으로 인식한 미국의 사이버 국방전략에 대한 중국의 비난도 더욱 거세졌다.[45] 반면 미국도 2013년 2

41 김상배. "사이버 안보의 미중관계." p. 80.

42 Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: Public Affairs. 2016). pp. 91-92.

43 David Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran." *New York Times* (June 1. 2012) http://www.nytimes.com/2012/06/01/world/middleeast/obama-orderedwave-of-cyberattacks-against-iran.html (accessed: April 30, 2021).

44 조현석, "미중 사이버 안보 협약 연구." p. 217.

45 Scott W. Harold, Martin C. Libicki, and Astrid S. Cevallos. *Getting to Yes with China in Cyberspace*. (Rand Corporation: Santa Monica, GA. 2016).

월 컴퓨터 보안회사인 맨디언트(Mandiant)의 보고서를 통해 중국군의 사이버테러와 사이버공격 실태를 종합적으로 분석하면서,[46] 중국군의 61398부대가 2006년 이후 미국의 정보통신·항공우주·위성·과학연구·행정·컨설팅 분야에서 기술정보를 탈취하기 위해 100여 차례 이상 사이버공격을 시도했다고 주장했다.[47]

그간 미중 간 사이버공방이 주로 중국의 해킹을 미국이 비난하는 것이 주였는데 중요한 변곡점이 발생했다. 바로 2013년 6월 미 중앙정보국(CIA) 직원이던 에드워드 스노든(Edward Snowden)이 중국을 대상으로 한 미국의 비밀작전을 폭로한 사건이다. 스노든에 따르면 미국의 국가보안전자감시 체계인 프리즘(PRISM)을 통해 오랜 기간 개인 이메일 등 각종 정보들을 감청해왔다는 것이다. 특히 미국이 2009년부터 중국의 정보기관과 기업들에 대해 사이버감시와 해킹을 했다는 사실도 밝혀졌는데 스노든의 폭로 사건으로 인해 중국은 미국에 대해 반격할 수 있는 기회를 얻게 되었다.[48] 스노든의 폭로 사건이 미중 간 사이버안보 관계에서 미국을 곤란하게 만들었지만 미국은 곧바로 반전의 기회를 잡게 되었다. 2014년 5월 미 법무부가 펜실베니아 주연방지방법원에 중국군 소속 장교 5명을 산업스파이 등의 혐의로 기소한 것이다. 미 법무부는 이들 5명이 웨스팅하우스 등 기업과 미 철강노조의 컴퓨터를 해킹해서 제품이나 재무구조에 대한 정보를 빼냈으며, 이로 인해 경쟁관계였

46 김상배. "사이버 안보의 미중관계." p. 78.

47 "2013. APT1: Exposing One of China's Cyber Espionage Units." Mandiant. www.mandiant.com (accessed: April 30, 2021).

48 고경민·정영애. "미·중 사이버안보와 프레임워크 형성의 역사적 다이내믹스." p. 85.

던 중국기업들이 큰 이익을 봤다는 것이다.[49] 이들 중국 해커들은 중국군 61398부대 소속으로 이 부대는 미국의 통신기업들을 해킹하는 또 다른 부대인 61486부대와 함께 엘리트 해킹 그룹의 일부인 것으로 드러났다. 이 사건 이후 미국은 스노든 사건으로 소극적이었던 태도에서 벗어나 중국을 사이버공격 주체로 직접 지목하는 등 적극적인 태도로 전환했다.[50]

그렇지만 이 사건은 오히려 미국의 기술패권에 대한 중국의 우려를 더욱 심화시키면서 중국의 반발을 강하게 불러왔다. 중국은 미국에 대한 보복조치로 미국 기업들의 정보통신제품에 대해 인터넷 안전검사를 의무화하는 조치를 시행하면서 그 대상으로 마이크로소프트와 IBM, 시스코, 애플 등을 지목했다. 실제 중국은 보안강화를 이유로 기관용 PC에 마이크로소프트의 윈도 운영체계 사용을 금지시켰는데 이는 .미국산 운영체계를 사용할 경우 발생할 수 있는 보안문제에 대한 우려 때문이라기보다는 미국이 중국군 현역 장교 5명을 사이버간첩 혐의로 기소한 것에 대한 보복 성격이 강했다.[51] 이어서 2014년 7월에 미국 인사관리청의 서버가 해킹당해 수만 명의 공무원의 개인정보가 노출되는 사건이 발생했다. 그 피해정도는 매우 심각해서 약 2,200만개의 기록이 훼손되었는데 거기에는 정보인력과 군 인력의 배경기록과 약 560만 명의 지문기록이 포함되어 있었다. 또한 금융문제, 약물사용, 알코올 남용 등에 관한 사적인 내용도 포함되어 있었다. 중국 해커들의 사이버 해킹이 매우 광범위하게 벌어지면서 미국에서는 해킹 당하지 않은 기관을 찾기가 어려운 지

49 김상배. "사이버 안보의 미중관계." p. 79.

50 Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, p. 114. pp. 131-132.

51 김상배. "사이버 안보의 미중관계." p. 80.

경이 되었다.[52]

미중 간 사이버공방은 스노든 폭로 사건과 미국의 중국군 장교 기소 사건 이후 더욱 가열된 측면이 있다. 이러한 여파로 중국의 해외 특히 미국 기업에 대한 견제는 더욱 강화되고 있다. 2014년 8월 중국은 해킹과 사이버범죄를 둘러싼 미중 간 긴장이 고조되는 가운데 정부 조달 목록에서 애플의 아이패드, 맥북 프로, 맥북 에어 등 총 10개 모델을 제외했다. 중국은 최근 백신 소프트웨어 업체인 시만텍 제품의 구매도 중단했고, 마이크로소프트 제품도 에너지 효율성이 있는 컴퓨터 제품군 목록에서 제외시켰다. 또한 중국은 중국내 은행의 IBM서버를 중국산 서버로 대체하기로 했다. 이러한 중국의 조치는 IBM이외의 미국 기업들에게도 영향을 미쳐 기업의 비밀 유출을 방지하기 위한 거래 중단 명령이 내려지기도 했다. 미국과의 사이버갈등이 거세지면서 중국은 정부기관 서버의 IBM 의존도를 낮추기 위해 자국 브랜드 서버로 교체해서 사용하도록 지시하기도 했다.[53]

이와 같은 정보통신 장비와 관련된 미중 간 견제에서 주요 쟁점은 중국 내에서 약 70%의 점유율을 차지하고 있는 미국의 통신장비업체 시스코(Cisco)라고 할 수 있다. 시스코는 금융업계에서는 약 70% 이상의 점유율을 차지하고 있고, 해관, 공안, 무장경찰 등 정부기관들에서는 약 50%의 점유율을 넘어서고, 철도시스템에서는 약 60%의 점유율을 보이고 있다. 민간항공, 공중 관제 백본 네트워크에서는 모두 시스코의 장비

52 Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, pp. 114-116.

53 김상배. "사이버 안보의 미중관계." pp. 80-81.

를 사용하고 있고, 항공, 공항, 부두에서도 약 60% 이상, 석유, 제조, 경공업, 담배 등 업계에서도 60% 이상의 점유율을 차지하고 있다. 심지어 인터넷 업계에서도 시스코가 차지하는 비율이 약 60%에 달하고, 대중매체 업계에서는 약 80% 이상이다. 시스코도 스노든 사건 이후 중국의 견제를 더욱 많이 받게 되었는데, 미국이 중국에서·감청 프로그램을 운용할 때 시스코의 장비를 활용했다는 사실이 폭로되었기 때문이었다. 중국 내 유관기관의 검증결과에 따르면 시스코의 라우터 제품에 히든백도어를 삽입한 것이 밝혀졌고, 결국 상하이유니콤, 광둥모바일, 차이나텔레콤 등이 잇달아 시스코의 장비를 다른 제품으로 교체하기 시작했다.[54]

이에 대응해 미국도 자국의 주요 기술이 유출될 수 있다는 우려 때문에 IBM의 x86서버 사업이 중국 기업인 레노버로 인수되는 것을 지연시켰다. IBM서버 사업부가 레노버로 인수될 경우 중국의 해킹 공격으로부터 미 국방부 등이 취약해질 수 있다는 이유였다. 미국은 과거에도 IBM-레노버 간 인수거래에 대해 우려를 표명해왔는데, 2005년 IBM이 자사 PC 사업부를 레노버에 매각했을 때도 공군에 공급된 레노버 제품이 중국의 해킹 공격에 노출돼 있다는 의혹을 제기했으며, 결국 해당 제품들은 반품되고 미국 제품으로 교체되었다.[55]

최근의 화웨이 사태도 마찬가지로 이와 같은 해킹 위험에 미중 간 5G 패권경쟁이 더해진 결과이다. 중국 화웨이가 주도하고 있는 5G 기술은 미래 생활을 변화시킬 원천기술로 경제적, 군사적 측면에서 매우 중요하다. 약 12조 달러로 추정되는 5G 시장은 미중 간 기술 패권경쟁의 핵심

54 Ibid. p. 81.

55 Ibid.

인 것이다. 미국은 5G를 비롯한 4차 산업혁명 관련 기술에 대한 주도권 상실을 우려하여 2018년 화웨이 제품이 보안상 위험하다며 국방수권법을 통해 미국 행정기관의 화웨이 통신장비 조달을 금지시켰다. 2019년에는 당시 트럼프 대통령이 '정보통신기술 및 서비스 공급망 확보' 행정명령을 통해 화웨이 등 외국정보통신 업체의 기술을 미국 기업들이 사용하지 못하게 하였다.[56]

이와 같은 미국과 중국의 상대 기업에 대한 견제는 미중 간 사이버갈등과 밀접히 연관되어 있다. 현실공간에서나 사이버공간에서나 최강국의 지위를 갖고 있는 미국과 중국은 국가안보 차원에서 사이버안보를 확대, 강화하기 위해 서로간의 사이버공방을 계속할 것으로 전망된다.[57]

2. 코로나19 팬데믹에 따른 사이버공격 양상

코로나19 팬데믹으로 인해 국제사회의 사이버안보 상황은 새로운 국면을 맞이하고 있다. 특히 감염병 시대의 변화된 상황으로 인해 사이버공격의 양상이 크게 변화하였다. 이와 같이 변화된 사이버공격 양상은 사이버안보와 관련된 지금까지의 인식과 대응을 새로이 생각하게 하는 계기가 될 것으로 보인다. 우선 코로나19 팬데믹 상황을 악용한 피싱과 랜섬웨어 등 사람들의 취약점을 공략하는 사회공학적 공격이 급증했다. 과거에도 메르스와 에볼라 바이러스 발생 시 바이러스 관련 내용이 포함된 문자메시지나 이메일 등을 통해 악성코드 유포가 증가했었다. 또한

56 오일석, "코로나19 확산과 5G 기술 패권경쟁," 『이슈브리프』 통권 182호 국가안보전략연구원 (2020. 4. 7.).

57 고경민·정영애. "미·중 사이버안보와 프레임워크 형성의 역사적 다이내믹스," p. 85.

이러한 감염병 관련 정보제공 사이트로 위장한 사이버공격도 증가했었다. 현재 코로나19 팬데믹 상황을 활용하여 전 세계적으로 다양한 사이버공격이 시도되고 있는데, 의료, 통신, 기술, 금융, 교육 분야에서 코로나19 관련 내용을 미끼로 한 랜섬웨어 공격이 크게 증가했다.[58]

다음으로 코로나19 팬데믹은 새로운 취약점을 공략하는 사이버공격의 급증을 초래했는데, 우선 코로나19 팬데믹으로 인해 감염병 예방을 위한 사회적 거리두기를 실천하고 있기 때문에 온라인을 통한 활동이 대폭 확대되면서 단기간에 성장한 비대면 서비스를 대상으로 한 원격접속에 대한 사이버공격이 급증했다. 코로나19와 그에 따른 재택 원격근무로의 전환이 사이버공격 양상을 크게 변화시킨 것이다. 원격근무자의 수가 크게 증가했기 때문에 기관과 기업들은 데이터 침해에 매우 취약해졌고, 사이버공격이 급증하고, 직원들의 업무 방식이 전례 없이 달라지면서 새로운 사이버안보 리스크가 대두되었다.[59]

코로나19 팬데믹으로 재택 원격근무가 뉴노멀이 된 운영모델이 적용되면서 전 세계는 새로운 도전에 직면했다. 대부분의 국가들은 디지털 전환을 가속화하고 있고, 사이버안보에 크게 주목하고 있다. 각국의 기관과 기업들은 코로나19 팬데믹에 대응하여 직원들이 재택근무를 하도록 장려하고 있다. 결과적으로 사이버 관련 기술은 일과 개인 생활 모두에서 훨씬 더 중요해졌다. 그러나 이러한 기술발전 요구의 증가에도 불구하고 많은 기관과 기업들이 여전히 사이버안전 원격근무 환경을 제공

58 채재병, 『국제사회의 해킹 변화 추세 및 대응방안』, p. 10.

59 채재병·김일기, 『코로나19 팬데믹에 따른 사이버공격 변화 양상과 대응방안』, INSS 전략보고 No. 128, August 2021. p. 3.

해주지 못하고 있는 것이 문제이다. 전통적으로 회의가 직접 열리던 곳에서는 대부분 가상으로 회의가 진행되고 있는데 집에서 일하는 개인이 근무환경에 있어서 사무실과 동일한 수준의 인터넷 보안의 고유한 보호조치를 누리지 못하고 있다.

정보기술(IT) 기업 VM Ware는 '2021 글로벌 보안 인사이트 보고서'에서 코로나19 팬데믹으로 글로벌 기업 76%에 대한 사이버공격이 급증했고, 원격근무로 인한 사이버위협도 크게 증가했다고 분석했다.[60] 글로벌 보안기업 체크포인트도 2021년 4-5월 동안 아태 지역에서 사이버공격 건수가 53% 증가했고, 특히 원격근무 환경이 해커들이 악용할 수 있는 보안상의 허점을 크게 하고 있다고 분석했다.[61]

이외에도 관리 감독 및 기술 통제력이 떨어지는 집에서 근무하는 악의적인 직원이 스캠(scam) 또는 기타 범죄 행위를 수행하려고 할 수 있다. 이러한 사이버위협의 대부분은 코로나19 팬데믹 중에 발생한 다양한 기회 때문에 더욱 위험해졌다. 사이버공격이 급증한 이유 중 하나는 일부 기관과 기업들이 'BYOD(Bring Your Own Device)' 액세스 방식을 취하기 때문이며, 이는 직원들이 전화, 태블릿 또는 랩톱 등의 개인기기를 사용하여 조직 정보에 액세스할 수 있다는 것을 의미한다. 집에서 일하는 것이 사무실 환경과 같은 수준의 사이버 보안을 보장하지는 않기 때문에 개인 컴퓨터 또는 랩톱을 사용하여 회사 파일 및 데이터에 액세스할 때 사용자는 사이버공격에 훨씬 쉽게 노출된다. 예를 들어 직원은 바

60 정태일, "글로벌 기업 76% '팬데믹에 사이버공격 급증, 원격업무로 위협↑'," 2021. 6. 9. http://news.heraldcorp.com/view.php?ud=20210609000994 (검색일: 2021. 6. 22).

61 김윤희, "아태 지역 사이버공격 53%↑…원격근무가 보안 허점 확대," 2021. 6. 14 https://zdnet.co.kr/view/?no=20210614170657 (검색일: 2021. 6. 22).

이러스 백신 또는 악성 프로그램 방지 검사를 정기적으로 실행하지 않을 수 있고, 집에서의 작업 환경은 정교한 기관이나 기업의 예방 및 탐지 조치를 갖고 있지 않다. 더욱이 가정용 와이파이 네트워크는 사이버공격에 훨씬 취약하다.[62]

가. 사회공학적 공격의 증가

2020년에는 랜섬웨어(ransomware) 공격 3건 중 1건이 서비스형 랜섬웨어(RaaS)인 소디노키비(Sodinokibi)를 포함했다. 소디노키비의 경우 이중 갈취(double extortion) 전술로 피해자의 약 67%가 대가를 지불한 것으로 추산된다.[63] 그들은 손상된 데이터를 공개 또는 다크 웹(dark web)에 노출시킨 다음 대가를 요구하며 위협한다. 기관이나 기업이 지불을 거부하면 그들은 피해자의 서비스를 이용할 수 없게 만드는 디도스 공격을 감행한다. 또한 서비스형 랜섬웨어 모델은 랜섬웨어 개발자들이 해커들과 협력하여 수익을 얻게 만든다. 예를 들어 소디노키비는 39개 이상의 파트너들과 계약을 맺었다.[64] 이외에도 BazarLoader, Conti, Egregor, Phobos/EKING, Ragnar, Ryuk, Thanos, WastedLocker 등의 랜섬웨어가 활동했으며 이들은 의료, 전

62 Cedric Nabe, “Impact of COVID-19 on Cybersecurity,” https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html (accessed: June 15, 2021).

63 원병철, “코로나19 관련 산업과 유럽 노린 사이버공격 늘었다,” 2021. 2. 25. https://blog.naver.com/widgetnuri4/222256085790 (검색일: 2021. 6. 22).

64 Yulia De Bari, “2021 Cybersecurity Trends Report,” https://www.infosys.com/iki/insights/2021-cybersecurity-trends-report.html (accessed: June 15, 2021).

문 서비스 및 소비자 서비스 기업, 금융 서비스 기업 및 공공 조직 등 다양한 분야를 공격 대상으로 삼았다.[65] 이러한 랜섬웨어가 앞으로 기관과 기업들에는 가장 큰 위협이 될 것으로 보인다.

해커들은 병원, 의료 센터 및 공공기관을 주요 랜섬웨어 공격 대상으로 삼고 있다. 왜냐하면 건강 위기로 인해 시스템을 멈출 수 없으므로 해커들은 이들 기관이 대가를 지불할 가능성이 높다고 믿고 있기 때문이다. 실제로 코로나19는 랜섬웨어의 공격시간을 크게 단축시켰는데 이는 피해자가 피해를 최소화하기 위해 대가를 신속히 지불했기 때문이다. 랜섬웨어는 감염된 링크나 첨부 파일이 포함된 이메일, 손상된 직원 자격증명 또는 시스템의 취약성을 이용하여 시스템에 진입한다.[66] 많은 해커들이 기관이나 기업들이 원격근무로 전환하는 것을 활용하기 위해 그들의 시스템을 공격하고 침투하기 위한 새로운 악성 프로그램을 개발했다. 팬데믹 이전에 사이버공격의 약 20%는 이전에 보이지 않았던 악성 프로그램이나 방법을 사용했는데, 팬데믹 시기 그 비율은 35%까지 증가했다.[67] 해커들은 악성 프로그램, 스파이웨어 및 트로이 목마를 대화형 코로나 바이러스 지도 및 웹 사이트에 포함시키고, 사용자가 컴퓨터나 모바일 장치에 악성 프로그램을 다운로드하는 링크를 클릭하도록 속이고 있다.

한편 인터넷에는 ‘corona-virus’, ‘covid-19’ 등의 용어를 포함하는

65 조경화, “포티넷, 사이버공격 확장으로 전례없는 사이버 위협 환경 직면,” 2021. 3. 11. http://www.efnews.co.kr/news/articleView.html?idxno=89125 (검색일: 2021. 6. 22).

66 “COVID-19 cyberthreats,” INTERPOL, https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats (accessed: June 15, 2021).

67 Cedric Nabe, “Impact of COVID-19 on Cybersecurity.”

등록된 도메인들이 상당히 많이 있다. 일부는 합법적인 웹 사이트이지만 해커들은 스팸 캠페인(spam campaign), 피싱(phishing) 또는 악성 프로그램 확산을 위해 매일 수천 개의 새로운 사이트를 만들고 있다.[68] 전 세계 사이버 공격의 90%는 여전히 피싱 메일을 통해 이루어지며, 피싱 메일은 인터넷 사용자들로부터 개인정보를 탈취하는 가장 오래된 방법 중 하나이다. 최근에는 인터넷 사용자들의 호기심과 불안감을 이용하는 사회공학적 공격 등 다양한 방법을 활용하고 있다.[69] 해커들이 개인이나 기업, 기관의 특성을 사전에 파악하여 관심을 끌만한 주제로 이메일 등을 발송하는 스피어 피싱(spear phishing) 공격도 자주 활용되고 있다.[70]

코로나19 백신 접종이 계속 발표되면서 사람들은 백신이 어디서 제공되고 있는지, 누가 백신을 받을 수 있는지와 같은 백신 정보를 점점 더 많이 찾고 있다. 불행히도 이것은 코로나19 백신과 관련된 상당한 수준의 피싱 공격을 초래했다. 예방접종 약속 이메일을 가장한 이메일 피싱 공격과 함께 제약회사와 백신 유통업체에 대한 사이버공격이 급증하고 있다.[71]

또한 스캠(scam)도 코로나19 팬데믹 상황에서 더욱 자주 발생하고 있다. 2020년 4월 FBI는 코로나19를 이용한 스캠을 포함하여 자금 이체

68 "COVID-19 cyberthreats."

69 "포스트 팬데믹 시대 속 주목받는 '사이버 보안'," 안랩(AhnLab), 2020. 5. 11. https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=29230 (검색일: 2021. 6. 22).

70 금융위원회, "코로나19 관련 상황을 틈탄 사이버공격에 대응하여 금융회사 등의 보안조치를 강화하고, 해킹 등 피해 예방수칙을 마련하였습니다," 보도자료, (2020. 3. 9).

71 "11 Emerging Cybersecurity Trends in 2021," panda, https://www.pandasecurity.com/en/mediacenter/tips/cybersecurity-trends/ (accessed: June 15, 2021).

를 수행하는 기업을 대상으로 하는 비즈니스 이메일 타협(BEC) 스캠이 증가하고 있다고 경고했다. 미국 연방수사국(FBI)은 코로나19와의 싸움에서 필요한 개인 보호 장비나 기타 물자를 구입하는 자치 단체를 대상으로 한 비즈니스 이메일 타협 스캠의 증가에 크게 주목했다.[72] 앞으로도 코로나19가 기업과 사회에 미치는 영향을 고려하면 이러한 공격은 해가 거듭될수록 커질 것으로 보인다. 기관이나 기업들이 새로운 현실에 계속 적응함에 따라 해커들은 이러한 취약한 시기를 이용하여 사이버공격을 확대할 것이다. 2020년에 해커들이 어떻게 코로나19를 둘러싼 공포와 불확실성을 이용하고 테마 피싱 캠페인(theme phishing campaign), 위반 시스템 및 악성 프로그램을 전달했는지 잘 알려져 있다. 코로나19가 뉴스의 헤드라인을 계속 차지함에 따라 해커는 이 주제를 피싱 캠페인에 사용할 것이고. 국가나 국가와 연계된 악의적인 해커들은 이 상황을 이용할 기회를 계속 모색할 것이다.

나. 원격근무의 영향

기술 지형이 끊임없이 변화하고 있다는 사실은 새로운 현상은 아니지만 확실히 2020년에는 새로운 단계로 진입했다. 팬데믹 기간 동안 디지털화 및 클라우드(cloud)로의 마이그레이션(migration)과 같은 많은 추세가 가속화되었다. 대부분의 경우 새로운 원격 환경을 수용할 수 있도록 계획되지 않은 클라우드 마이그레이션과 정보기술 제품 및 서비스의

72 Eric Richardson and Jake Mahle–Vorys, "Cyberattacks on the rise during the Covid-19 pandemic," Jun 1, 2020, https://www.bizjournals.com/cincinnati/news/2020/06/01/cyberattacks-on-the-rise-during-covid-19.html (accessed: June 15, 2021).

신속한 공급이 이루어졌다. 많은 기관과 기업들이 일반적인 보안 조치에 그치면서 클라우드, 홈 네트워크 등 모든 영역에 걸쳐 새로운 수준의 취약성과 위험이 초래되었다.

우선 코로나19 이후 원격근무가 빠르고 광범위하게 도입됨에 따라 클라우드 기반 서비스와 인프라에 대한 필요성이 급격히 증가했다. 원격근무는 직원이 어디에서나 효율적으로 업무를 수행할 수 있도록 지원하는 클라우드 컴퓨팅 애플리케이션을 사용한다. 클라우드를 통해 기관과 기업은 필요에 따라 워크로드를 조정할 수 있으며 분석 및 인공지능과 같은 새로운 기능을 보다 쉽게 추가할 수 있어 이러한 기능이 결합되어 조직의 탄력성이 향상되었다. 클라우드에서 작업을 수행하면 보안 패치가 즉시 설치되는데 이는 기존 시스템에서 흔히 발생하는 문제이다. 클라우드 서비스를 사용하는 조직의 위험은 일반적으로 잘못 구성된 스토리지, 잘못된 아이디(ID) 및 액세스 관리 제어, 안전하지 않은 애플리케이션 프로그래밍 인터페이스(API), 데이터 손실, 침해 및 누출과 관련된다. 이러한 위험은 점점 더 많은 기관과 기업들이 클라우드 호스팅 프로세스를 채택하고 있기 때문에 앞으로도 지속될 것이다. 클라우드 서비스는 확장성, 효율성 및 비용 절감과 같은 다양한 이점을 제공하지만 여전히 사이버공격에 매우 취약한 상태로 남아있게 되었다.[73]

다음으로 재택 원격근무의 증가로 기관이나 기업의 네트워크가 집에까지 확대됨에 따라 새로운 공격 기회가 제공되면서 사이버공격 범위가 확장되고 있다. 더 많은 엔드 포인트(end point)가 확산됨에 따라 위협 면이 증가했다. 해킹 방지 기업인 파이어아이(FireEye)에 대한 최근

73 “11 Emerging Cybersecurity Trends in 2021.”

의 해킹은 기관이나 기업이 최고의 도구를 가지고 있더라도 동기부여가 된 해커가 외부 또는 내부 벡터를 통해 네트워크로의 길을 찾을 수 있다는 것을 보여주었다. 코로나19로 인한 재택근무의 일상화는 이러한 사이버공격을 더욱 증가시킬 것이다. 향후 5G는 더 빠른 속도와 용량을 제공하고 짧은 대기 시간을 제공하여 더 나은 연결을 제공할 것이다. 이는 개인과 기업의 연결성이 높아짐에 따라 엔드 포인트의 확산으로 이어진다. 2025년까지 27억 대의 기기가 5G에 연결되어 해커가 점점 더 많은 엔드 포인트와 연결 취약점을 공격하게 될 것이다. 앞으로 더 많은 사물인터넷(IoT) 기기들이 와이파이 라우터보다는 5G 네트워크에 직접 연결될 것이다. 이러한 패턴으로 인해 사물인터넷 장치는 직접 공격에 대해 점점 더 무방비 상태가 될 것이다. 가정용 클라이언트의 경우 중앙 라우터에서 모든 사물인터넷 기기가 벗어나기 때문에 더욱 취약해질 것이다. 특히 대량의 데이터를 효과적으로 클라우드 기반 스토리지에 백업하거나 전송할 수 있게 되면 해커가 공격할 수 있는 새로운 대상도 더 많이 확보될 수 있다.[74]

한편 2021년에는 내부자 데이터 위반이 전체 사이버 보안 사고의 3분의 1에 달할 것으로 예측되고 있다. 직원들이 원격근무로 전환함에 따라 미처 많은 기관과 기업들은 무단 원격 액세스를 모니터링하고 취약한 암호를 처리할 준비가 되어 있지 않다. 코로나19는 직원들이 업무에 개인용 기기를 사용할 수 있도록 허용할 것을 조직에 강요했다. ‘BYOD(Bring Your Own Device)’ 개념은 유연성을 통해 비용을 최소화하고 생산성을 높이는 방법이나 앞으로 원격 직원 및 해당 기기가 기

74 Yulia De Bari, “2021 Cybersecurity Trends Report.”

관이나 기업의 정보 보안에 위협이 될 수도 있다. 홈 라우터는 보안 제어 기능이 충분하지 않은 경우가 많아 해커들은 보안 수준이 낮은 홈 네트워크를 통해 기관이나 기업의 시스템에 진입하기 위해 네트워크 취약점을 공격할 것이다. 또한 기관이나 기업들은 홈 모델에서 작업을 채택하고 있으며, 이로 인해 협업 보안에 대한 우려도 커지고 있다. 생산성을 높이기 위해 원격 직원들은 슬랙(slack), 마이크로소프트 팀(microsoft teams) 및 줌(zoom)과 같은 더 많은 협업 도구를 사용하고 있다. 이러한 애플리케이션은 더 큰 데이터 보안 및 규정 준수 문제를 야기하고 내부자 위협의 위험을 높일 것이다.[75]

3. 포스트코로나 시대의 사이버안보

코로나19 팬데믹 상황은 전 세계적으로 우리의 일상 생활환경을 변화시켰다. 디지털 전환과 각 분야의 전통산업과 정보통신기술 간 융·복합이 가속화되었고, 교육과 근무 등 다양한 일상 활동을 비대면 중심으로 변화시켰다. 일상생황에서의 비대면 활동의 확대는 사이버영역을 확장시키는 결과를 가져왔고, 이로 인해서 사이버공격 범위가 크게 확대되면서 네트워크 등 사이버영역 전반에 대한 사이버공격을 급증시켰다. 특히 교육, 근무, 상업의 온라인화 등 비대면 서비스의 증가는 이와 같은 전방위적인 사이버공격의 급증을 가져오는 주요 요인으로 작용했다. 이에 작년 코로나19 팬데믹에 이어 금년에는 코로나19 바이러스처럼 사이버공격이 전 세계적으로 유행한다는 뜻을 가진 사이버 팬데믹이 올 것이라는 전망도 나오고 있는 가운데 포스트코로나 시대의 사이버안보는 다음과 같은 특징들로 나타날 것으로 보인다.[76]

최근 나타나는 새로운 공격들 중 일부는 머신러닝(ML)의 형태를 사용하고 있다. 인공지능(AI)과 머신러닝(ML) 활용으로 인해 자동화된 피싱 공격이 점점 더 정교해지고 있으며 문자나 음성 메시지와 같은 다양한 채널들을 사용하고 있다. 게다가 백신 개발에 관한 뉴스도 피싱 캠페인에 사용되고 있다. 이외에도 공급망에 대한 공격이 증가하고 있고, 지정학적 긴장 상태에 따른 사이버공격 양상의 변화도 목격되고 있다. 요컨대 코로나19 팬데믹으로 사이버공격의 범위와 대상이 일상 활동 전반으로 확대되었고, 사이버공격의 방법도 크게 고도화된 것이다.

가. 초자동화(hyperautomation)

인공지능(AI)과 머신러닝(ML) 활용이 사이버안보 환경에서 주목받고 있다. 혁신적인 기술은 사이버위협을 최소화하고 중요한 인프라를 보호하며 원치 않는 침입을 막는 데 도움이 되는 여러 가지 이점을 제공한다. 인공지능은 다양한 소스에서 대량의 위험 데이터를 분석하여 중요한 위협 정보를 제공할 수 있다. 위협 식별 시스템은 완전히 새로운 위험을 식별함으로써 사이버 보안 팀이 탐지, 대응 및 문제 해결에 소비하는 시간을 줄일 수 있다. 앞으로는 인공지능과 머신러닝 기술이 더욱 성숙해지고 보다 높은 효과를 제공할 것이다. 기관과 기업들은 또한 사이버 보안

75 Eric Richardson and Jake Mahle-Vorys, “Cyberattacks on the rise during the Covid-19 pandemic.”

76 이유지 “원격근무 확산·복합공격 급증, ‘사이버팬데믹’ 보안대책 필요,” 2021. 4. 13. https://byline.network/2021/04/13-116/ (검색일: 2021. 6. 22).

위험 관리 시스템을 개선하기 위해 이러한 솔루션을 채택하고 구현할 것이다. 그런데 인공지능이 기관이나 기업 간 위협 탐지를 강화할 수 있는 중요한 기회도 제공하지만 이 기술의 진화와 활용 증가는 실제 양방향으로 진행된다. 즉 범죄 네트워크는 인공지능을 이용해 공격을 자동화하고 있다. 인공지능은 해커들이 공격을 개선하는 데 사용할 수 있기 때문에 해커들에게도 매우 유익하다. 따라서 해커들은 비용이 적게 들고 더 자동화되며 규모 면에서 더 쉽게 사이버공격을 실행할 수 있게 된다. 해커들은 인공지능과 머신러닝을 사용하여 오래된 악성 프로그램의 새로운 변형을 만들고, 취약성을 찾고, 암호를 추측하고, 음성을 복제한다. 인공지능이 제어하는 자동화 시스템은 시스템과 네트워크를 테스트하여 악용될 수 있는 새로운 취약점을 검색할 수도 있다. 이 기술은 또한 사회공학적 공격의 성공률을 크게 높일 수 있다. 향후에는 해커가 인공지능을 조작해 새로운 스마트 악성 혁신을 설계할 것으로도 예상된다.[77]

한편 데이터 가용성, 자동화 및 높은 가치의 사용자에 대한 타겟팅 증가로 인해 자동화된 피싱 공격을 탐지하기는 매우 어렵다. 오늘날 해커는 보다 고급 방법을 사용하여 제대로 실행되는 이메일 손상 공격을 만든다. 피싱 위협은 고도로 지역화되고 개인화되고 지역적으로 대상이 지정된다. 이메일이 여전히 공격 벡터 1위로 남아 있는 한 해커들은 피해자들에게 개인 정보나 로그인 자격 증명을 포기하게 하거나 심지어 돈을 보내도록 속이기 위해 다양한 방법들을 사용하고 있다. 점점 더 많은 피싱이 모바일 장치에 대한 문자 메시지 공격 또는 소셜 미디어 및 게임 플랫폼에서의 메시지 사용을 포함하고 있다. 향후 자동화된 윈도우 피싱

77 Yulia De Bari, “2021 Cybersecurity Trends Report.”

공격이 감염병, 정치, 경제를 둘러싼 공포를 넘어설 것으로 예상된다. 역사적으로 악성 행위자들은 악성 첨부파일이나 하이퍼링크로 윈도우 피싱 이메일을 만드는 데 많은 시간을 보냈다. 그러나 해커들이 수작업 과정을 자동화하기 위해 인공지능과 머신러닝을 사용함에 따라 이러한 경향은 변화할 것으로 보인다. 예를 들어, 고급 피싱 도구 키트를 사용하는 국가 지원 해커는 소셜 미디어 네트워크 및 조직 웹 사이트를 검색하여 엄청난 양의 데이터를 얻을 수 있다. 이 데이터를 사용하면 각 피해자에게 맞춤화된 신뢰할 수 있는 콘텐츠를 사용하여 대량의 윈도우 피싱 공격을 시작할 수 있다. 이 자동화된 프로세스는 해커가 한 번에 보낼 수 있는 윈도우 피싱 이메일의 수를 증가시켜 성공 가능성도 높일 것이다.[78]

나. 공급망 보안

공급망은 모든 기관과 기업들의 글로벌 운영에 있어서 매우 중요한 요소이다. 사이버공격 10건 중 4건은 조직이 아니라 공급망 링크 중 하나에서 발생한다. 그러므로 공급망 보안의 성패는 그것의 가장 약한 고리에 달려 있다. 타 기관이나 기업의 공급업체가 조직의 데이터를 손상시킬 수 있도록 허용하면 많은 조직들이 공급업체 시스템을 통해 위반을 경험하게 된다. 기관이나 기업은 중요한 정보를 공급업체와 지속적으로 공유해야 하는데 일단 정보가 공유되면 조직은 그것에 대한 직접적인 통제력을 잃게 된다. 이로 인해 정보의 기밀성, 가용성 및 무결성이 위협받게 된다. 이와 같은 공급망에 대한 공격은 상당 기간 동안 계속되어져 왔

78 Ibid.

다. 특히 2020년 12월 대규모 글로벌 공급망 공격을 유발했던 미국의 소프트웨어 개발업체인 솔라윈즈(SolarWinds)에 대한 해킹은 공급망 보안의 중요성을 한 단계 높인 사례로 당시 피해 조직들은 상당한 양의 정보를 노출시켰다. 이와 함께 공급망 공격의 상호 연결된 범위를 보여주고, 공급망 위험 관리의 중요성도 보여주는 여러 최신 사례들도 확인되었다.[79] 코로나19로 인한 신속한 디지털화는 기관과 기업들이 더 많은 제3자 관계를 갖게 했고 그러한 제3자가 더 많은 디지털 연결을 가질 것이기 때문에 더 많은 취약성을 야기한다. 공급망이 점점 더 연결되고 복잡해짐에 따라 향후에는 타 기관이나 기업의 리스크 관리가 최우선 순위가 될 수도 있을 것이다.

다. 지정학적 긴장

지정학은 공격적인 사이버 활동의 중요한 원동력이다. 앞으로 이러한 긴장감이 높아지면서 사물인터넷(IoT) 기기 및 산업제어시스템(ICS)에 대한 파괴적인 사이버공격이 나타날 수 있다. 의료, 에너지, 석유, 가스, 제조업이 그러한 공격의 최우선의 목표가 될 것이다. 그리고 다크 웹에서는 산업제어시스템 인프라를 공격하기 위해 특수하게 조작된 파괴적인 악성 프로그램의 판매가 급증할 것이다. 해커는 공격 수명 주기에 잘못된 플래그를 배치하여 공격 뒤의 자신의 흔적과 이유를 감추기도 한다. 예를 들어, 북한의 라자루스(Lazarus) 그룹이 러시아어를 사용하는 것과 특이한 도구 세트를 사용하는 것은 분석가의 초점을 다른 조직으로 돌리게 할 수 있다. 보안 전문가는 조사 중에 증거를 매핑하는 데 있어 문제에 직면할 수 있으며 이것은 잘못된 판단과 거짓 주장으로 이어질 수도 있다.[80]

미국의 경우 바이든 대통령은 러시아가 미국에 가장 큰 안보 위협이 되는 국가이자 적국이라고 규정했다. 또한 중국을 미국 경제와 안보에 대한 위협으로 인식하고 있다. 향후 미국과 러시아 및 중국 간에 주요 인프라를 겨냥한 사이버공격이 더욱 증가할 것으로 예상할 수 있다. 러시아도 2020년에는 팬시 베어(Fancy Bear)로도 알려진 러시아 사이버 스파이 단체 스트론티움(Strontium)이 미국의 정당과 캠페인, 옹호 단체, 미국 공화당과 민주당에 봉사하는 컨설턴트 등 200여 개 단체를 사이버 공격 대상으로 삼기도 했다. 또 러시아 해외정보국의 APT29는 미국의 최고 사이버 보안업체와 재무부, 상무부, 에너지부, 국가원자력안전국 등 정부 기관들을 공격했다. 앞으로도 러시아 해커들이 정치인과 정책입안자들의 계획과 동기를 파악하기 위해 정부 기관을 대상으로 계속 공격할 것으로 전망된다. 중국의 경우, 2020년 중국이 새로운 코로나 바이러스를 무기로 만든다고 비난한 국가들을 대상으로 하는 중국 국가 해킹 그룹의 공격이 있었다. 앞으로는 중국이 지원하는 해커들이 모바일 네트워크를 공격해 미국 국민을 상대로 대대적인 감시·스파이 캠페인을 벌일 것으로 예상할 수도 있다.[81]

포스트코로나 시대의 사이버안보는 이상의 특징들을 중심으로 나타나는 사이버공격들로 인해 국제사회에서의 인식과 대응에 있어 다양한 변

79 조경화, "포티넷, 사이버공격 확장으로 전례없는 사이버 위협 환경 직면."

80 Yulia De Bari, "2021 Cybersecurity Trends Report."

81 Ibid.

화를 겪을 것으로 전망된다. 기본적으로 코로나19 팬데믹으로 사이버공간의 활용도가 대폭 증가된 상황에서 기술적인 발달과 공급망에 대한 위협 증가, 지정학적 긴장으로 인한 사이버위협 등이 지속적으로 사이버공간에 대한 위기 상황을 증폭시킬 것이다. 따라서 세계 각국은 이와 같은 포스트코로나 시대의 새로운 사이버안보 상황에 맞추어 사이버안보 대응전략을 구상할 것으로 예상된다.

IV

결론: 한국의 전략구상

코로나19 팬데믹 상황에서 세계 각국은 기관과 기업들을 중심으로 안전한 비대면 사회 정착을 추구하고 있다. 미국은 연방기관의 원격근무 시 발생하는 사이버안보 이슈와 가이드라인을 발표했고, 유럽연합도 코로나19 팬데믹으로 인한 근무 형태의 디지털화와 디지털 인프라에 대한 의존 확대로 사이버안보전략을 개정했다. 중국이나 러시아도 코로나19 팬데믹으로 인한 정보환경의 변화에 대응하고 있다. 한국도 국가적 대응 차원에서 비대면 시대의 위험에 대한 국가정보보안 기본지침 관련 내용을 개정하고, 원격업무 통합매뉴얼을 발표하는 등 일반화되는 재택근무와 원격서비스 확산에 대비하고 있다.[82]

코로나19 팬데믹으로 확산된 원격근무는 전 세계 기관과 기업들에게 많은 과제를 안겨주었다. 그들은 정교한 사이버공격의 급증에 대한 충분한 준비가 되어 있지 않았으며, 사이버 보안 인식을 높이기 위해 앞으로 많은 노력이 필요하다. 코로나19가 유행하기 전에 일부 기관과 기업들은 원격근무, 특히 기밀 데이터에 대한 액세스에 대해 반대했다. 단기간에 그들은 원격근무를 위한 용량과 기능을 늘려야 했지만 불행히도 원격근무 기능의 신속한 배치에서 사이버 보안이 항상 중요한 우선순위는 아니었다. 예를 들어 일부 기관과 기업은 직원이 회사 데이터에 액세스하기 전에 개인 기기가 표준 보안 보호 기능을 갖추고 있는지 확인하지 않았으며, 기본적으로 설계되지 않은 작업을 '가상 사설망(Virtual Private Network, VPN)' 기술에 의존했다.[83] 많은 정보기술 부서와 기관이나 기

82 정순채, "코로나19와 포스트 코로나 시대의 정보보호," 2021. 6. 21. https://www.asiatime.co.kr/article/20210621500119 (검색일: 2021. 6. 22).

83 Cedric Nabe, "Impact of COVID-19 on Cybersecurity."

업이 가상 사설망에 의존하여 조직 네트워크에 쉽게 액세스할 수 있지만 가상 사설망은 불완전하다. 랜섬웨어의 가장 일반적인 입력 벡터는 피싱이며 기관과 기업은 이러한 공격에 대응해야 한다. '제로 트러스트 네트워크 액세스(Zero-Trust Network Access, ZTNA)'는 중요한 데이터에 대한 원격 액세스를 제어하고 공격 가능성을 줄이기 위한 보다 안전한 방안이다. 2023년까지 60%의 기관과 기업이 가상 사설망을 단계적으로 폐지하고 제로 트러스트 네트워크 액세스로 전환할 계획으로 제로 트러스트 네트워크 액세스로 전환하여 조직의 원격 액세스 네트워크를 강화하여 공격 위험을 줄이겠다는 것이다.[84] 이는 포스트코로나 시대 사이버안보의 토대전략을 구성할 것으로 전망된다.

구체적인 전략방안을 살펴보면, 첫째, 점점 더 많은 기관과 기업들이 클라우드로 마이그레이션함에 따라 안전하게 정보를 보호하는 것이 매우 중요하다. 클라우드에서 발생하는 대부분의 사고는 기관이나 기업의 강력한 사이버 보안 전략이 부족하기 때문에 발생한다. 기관과 기업들은 클라우드 설계를 보호하고, 효과적인 리스크 관리를 허용하며, 클라우드 거버넌스를 안전하게 보호할 수 있는 보안 위협의 문제 해결을 위한 영구적인 모델을 구축하는 것이 중요하다. 기관과 기업에서는 클라우드와 함께 발생하는 보안상의 영향을 파악하고 현재 인프라에 존재하는 취약성을 파악해야 한다.

둘째, 홈 네트워크는 기관이나 기업 네트워크보다 최소 하나의 악성 프로그램 제품군을 가질 가능성이 3배, 5개 이상의 고유한 유형의 악성 프로그램을 가질 가능성이 7배 더 높다. 홈 오피스를 확보하기 위해 기

84 "11 Emerging Cybersecurity Trends in 2021."

관이나 기업은 범용 멀티 팩터 인증을 요구할 필요가 있다. 기관이나 기업은 바이러스 백신 업데이트 및 보안 패치를 통해 시스템을 업데이트해야 한다. 데이터 유출을 방지하기 위해 기관이나 기업은 보안되지 않은 장치와 프로토콜을 비활성화하고 엔드 포인트 제어를 시행하며 업무 및 개인 사용 장치를 분리해야 한다. BYOD(Bring Your Own Device)와 모바일 기기의 보안을 유지하려면 직원들이 암호나 개인식별번호(PIN)를 보호하고, 정기적으로 새 업데이트를 설치하고, 신뢰할 수 있는 개발자의 애플리케이션만 설치하고, 개인 정보는 문자 메시지에 노출되지 않도록 하는 등 위험한 온라인 행동에 대해 교육하는 것이 중요하다.[85]

셋째, 원격 인력을 계속 탐색함에 따라 내부자 위협은 더욱 우려되는 영역이 되고 있다. 모든 사이버 보안 위협이 외부 영향력에 의해 발생한다고 쉽게 믿지만, 기관이나 기업은 자신의 조직 내에서 증가하는 위협 행위자의 현실과 정교함을 무시해서는 안 된다. 특히 전 세계에 흩어져 있고, 가상으로 만난 뒤 채용했을 가능성이 있는 원격 전담 직원을 기관이나 기업이 계속 채용하고 있기 때문에 더욱 그렇다. 보안 침해 사고의 15%-25%가 신뢰할 수 있는 비즈니스 파트너에 의해 발생한다는 사실에서 기관이나 기업은 내부자 위협과 데이터 도난 가능성에 더 주의해야 한다. 내부 위협은 보안 리더에 의해 심각하게 받아들여지고 실제 위험으로 간주되어야 하며, 조직이 보안 위협을 발견하고 차단할 수 있는 적절한 도구를 갖추고 있어야 한다.[86]

넷째, 사회공학적 피싱 공격은 원격근무자가 널리 분포하는 상황에서

85 Yulia De Bari, "2021 Cybersecurity Trends Report."

86 "11 Emerging Cybersecurity Trends in 2021."

더욱 큰 문제이며 이를 해결하기 위해 조직은 신원 관리 및 보안 전략을 고려하고, 적시에 필요한 리소스에 적합한 인력만 적절한 수준으로 액세스할 수 있도록 해야 한다.

다섯째, 해커들이 공격 전략을 개선하기 위해 인공지능을 사용한다는 점에서 기관이나 기업이 혁신적인 기술 솔루션을 채택하는 것이 중요하다. 인공지능과 머신러닝이 탑재된 플랫폼을 활용해 행동 기반 분석을 대규모로 수행할 수 있으며, 이러한 액세스 방식은 프로세스 초기에 지능적인 사이버 위협을 탐지 및 해결하기 위해 사용될 수 있다. 매일 증가하는 데이터의 양으로 인해 기관이나 기업이 가능한 한 많은 정보기술 프로세스를 자동화하는 프로세스인 초자동화(hyperautomation)가 그 어느 때보다 절실하다. 자동화된 보안 시스템을 구현하면 데이터 도난 및 위반을 완화하는 기관이나 기업의 능력이 강화될 뿐만 아니라 운영 효율성과 사이버 보안 위협에 대한 전반적인 복원력도 향상된다.

여섯째, 기관이나 기업은 전체 공급망에서 가시성을 제공하고, 위협과 약점을 식별하며, 새롭게 부상하는 위험을 모니터링하는 강력한 리스크 관리 프로그램이 필요하다. 타사 리스크를 효과적으로 관리하려면 조직은 책임, 소유권 및 통합 워크플로우를 명확히 구분하는 통합 거버넌스 및 에스컬레이션 프레임워크를 생성해야 한다. 취약성을 해결하려면 '제로 트러스트(Zero-Trust)' 원칙을 사용하여 보안 제어를 만들고 파트너 액세스를 평가해야 한다. 조직은 적절한 시스템 액세스 인증을 위해 위험 기반 파트너 세분화를 구현해야 하고, 공급업체 보안 상태와 파트너 리스크를 평가해야 한다.

일곱째, 지정학적 동기와 국가가 지원하는 사이버 활동 사이의 명확한 연관성에서 보듯이 기관이나 기업은 지정학적 영향을 충분히 이해해야 한다. 이는 심각한 사이버위협이 발생하기 전에 이를 예측하고 대비할 수 있기 때문이다. 기관이나 기업들이 목표 대상이 되는 방법, 시기, 장소를 결정하려면 지정학적 정보와 기존의 위협 정보 수집 기술을 결합해야 한다.

여덟째, 잘 훈련된 사이버 보안 전문가를 찾는 것은 항상 모든 기관과 기업에서 어려운 과제였지만 기관과 기업들은 조직 네트워크의 보안을 강화하기 위해 잘 훈련된 전문가를 구해야 한다. 사이버 보안 인력 부족은 오늘날 기관과 기업들이 직면한 보안 위험을 계속 커지게 하고 있으며, 기관과 기업들은 빠르게 확장되고 있는 디지털 세계를 보호하기 위해 사이버 보안 인력을 늘리고 이에 대한 기술 교육에 우선순위를 두어야 한다.[87]

이와 같은 전략방안들을 통해 네트워크와 클라우드를 포함한 사이버 공격 범위 전체에 대한 감시, 탐지, 차단, 보호를 제공해야 한다. 그리고 코로나19의 영향으로 확대된 공격 범위를 포괄할 수 있도록 기존의 사이버공격 대응체계를 개선하고, 새로운 취약점들을 보호할 수 있는 사이버안보 플랫폼을 구축함으로써 포스트코로나 시대의 사이버위협에 대응해야 할 것이다.

87 Ibid.

Abstract

International Political Trends in Cybersecurity and Korea's Strategic Plan

Chae, Jae-Byung

(Institute for National Security Strategy)

The purpose of this study is to devise and present our response strategies to such changes in cybersecurity by analyzing the international political trend of cybersecurity in the international community, and at the same time to predict changes in cybersecurity due to the impact of the COVID-19 pandemic and cybersecurity in the post-corona era.

Recently, the international community is entering a new normal era due to the COVID-19 pandemic, and the competition for hegemony between the U.S. and China is intensifying. Cybersecurity is also changing significantly under the influence of this situation. Therefore, a review of these changes is required, and in particular, cybersecurity changes that will occur when the post-corona era arrives and a review for preparation for these changes is also required.

To this end, first, to examine the international political meaning of cybersecurity as a basis for discussion, the international political perception of cyberspace, the security implications of cyber sovereignty and the relationship between cybersecurity, and the formation of international norms related to cybersecurity are analyzed. Next, in order to analyze the international political trend of cybersecurity, the development of cybersecurity amid the U.S.-China competition, changes in cyberattacks due to the COVID-19 pandemic, and prospects of changes in cybersecurity in the post-corona era are examined. Finally, based on this analysis, Korea's future cybersecurity-related strategic plans are derived and presented.

It is necessary to provide monitoring, detection, blocking, and protection for the entire scope of cyberattacks, including networks and clouds, through the proposed strategies. In addition, it is necessary to respond

Abstract

to cyber threats in the post-corona era by improving the existing cyber attack response system to cover the expanded attack range due to the impact of COVID-19, and building a cyber security platform that can protect new vulnerabilities.

Keywords

cybersecurity, cyberspace, cyber sovereignty, COVID-19 pandemic, post-corona era

참고문헌

고경민·정영애, “미·중 사이버안보와 프레임워크 형성의 역사적 다이내믹스,” JOURNAL OF PLATFORM TECHNOLOGY, 5(4), 2017.

금융위원회, “코로나19 관련 상황을 틈탄 사이버공격에 대응하여 금융회사 등의 보안조치를 강화하고, 해킹 등 피해 예방수칙을 마련하였습니다,” 보도자료, (2020. 3. 9).

김상배 외, 『사이버 안보의 국가전략 2.0』. 서울: 사회평론, 2019.

김상배 외, 『사이버 안보의 국가전략: 국제정치학의 시각』. 서울: 사회평론, 2017.

김상배, “사이버 안보의 미중관계.” 『한국정치학회보』, 49(1), 2015.

김윤희, “아태 지역 사이버공격 53%↑…원격근무가 보안 허점 확대,” 2021. 6. 14. https://zdnet.co.kr/view/?no=20210614170657 (검색일: 2021. 6. 22).

배영자, “사이버안보 국제규범에 관한 연구.” 『21세기정치학회보』 제27집 1호. 2017.

안랩(AhnLab), “포스트 팬데믹 시대 속 주목받는 ‘사이버 보안’,” 2020. 5. 11. https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=29230 (검색일: 2021. 6. 22).

오일석, “코로나19 확산과 5G 기술 패권경쟁,” 『이슈브리프』 통권 182호 국가안보전략연구원 (2020. 4. 7.).

원병철, “코로나19 관련 산업과 유럽 노린 사이버공격 늘었다,” 2021. 2. 25. https://blog.naver.com/widgetnuri4/222256085790 (검색일: 2021. 6. 22).

이유지, “원격근무 확산·복합공격 급증, ‘사이버팬데믹’ 보안대책 필요” 2021. 4. 13. https://byline.network/2021/04/13-116/ (검색일: 2021. 6. 22).

장노순, “사이버안보와 국제규범의 발전: 정부전문가그룹(GGE)의 활동을 중심으로.” 『정치·정보연구』 제19권 1호. 2016.

정순채, “코로나19와 포스트 코로나 시대의 정보보호,” 2021. 6. 21. https://www.asiatime.co.kr/article/20210621500119 (검색일: 2021. 6. 22).

정태일, “글로벌 기업 76% ‘팬데믹에 사이버공격 급증, 원격업무로 위협↑’,” 2021. 6. 9. http://news.heraldcorp.com/view.php?ud=20210609000994 (검색일: 2021. 6. 22).

조경화, “포티넷, ‘사이버공격 확장으로 전례없는 사이버 위협 환경 직면’,” 2021. 3. 11. http://www.efnews.co.kr/news/articleView.html?idxno=89125 (검색일: 2021. 6. 22).

조현석, “미중 사이버 안보 협약 연구,” 『21세기정치학회보』, 27(2), 2017.

채재병·김일기, 『코로나19 팬데믹에 따른 사이버공격 변화 양상과 대응방안』, INSS 전략보고 No. 128, August 2021.

채재병, 『국제사회의 해킹 변화 추세 및 대응방안』, INSS 연구보고서 2020-17, 2020.

채재병 외, 『주변국의 사이버 환경과 한반도 평화체제 구축』, KINU 연구총서 19-29, 2019.

채재병, “‘바르샤바 프로세스’와 사이버안보협력: 전망과 시사점,” 『이슈브리프』 통권 154호 국가안보전략연구원 (2019. 10. 30).

채재병, “안보환경의 변화와 사이버안보.” 『정치·정보연구』 제16권 2호. 2013.

Bajpai, Kanti, “The Idea of Human Security”, *International Studies*, Vol. 40(3), 2003.

Bartelson, Jorge, A. *Genealogy of Sovereignty* (Cambridge: Cambridge University Press, 1995).

Buzan, Barry, *People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era* (Colorado: Lynne Rienner Publisher, 1991).

Camilleri, Joseph A. & Jim Falk, *The End of Sovereignty?* (Aldershot: Edward Elgar, 1992).

De Bari, Yulia, "2021 Cybersecurity Trends Report," https://www.infosys.com/iki/insights/2021-cybersecurity-trends-report.html (accessed: June 15, 2021).

ENISA, *National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace* (2012. 5).

Haas, Richard N. "Paradigm Lost," *Foreign Affairs*, Vol. 74, No. 1 (Jan./Feb. 1995).

Harold, Scott W., Martin C. Libicki, and Astrid S. Cevallos. *Getting to Yes with China in Cyberspace* (Rand Corporation: Santa Monica, GA. 2016).

INTERPOL, "COVID-19 cyberthreats," https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats (accessed: June 15, 2021).

ITU, *National Cybersecurity Strategy Guide* (2011).

Krasner, Stephen D, *Sovereignty: Organized Hypocrisy* (Princeton: Princeton University Press, 1999).

Mandiant. "2013. APT1: Exposing One of China's Cyber Espionage Units." www.mandiant.com (accessed: April 30, 2021).

Nabe, Cedric, "Impact of COVID-19 on Cybersecurity," https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html (accessed: June 15, 2021).

NATO, *NATO 2020: Assured Security; Dynamic Engagement: analysis and recommendations of the group of experts on a new strategic concept for nato* (NATO Public Policy Division, 2010. 5. 17).

Nye Jr. Joseph S. "Power and National Security in Cyberspace," in Kristin M. Lord and Travis Sharp (eds.), *America's Cyber Future: Security and Prosperity in the Information Age*, Vol. II (Center for a New American Security, June 2011).

panda, "11 Emerging Cybersecurity Trends in 2021," https://www.pandasecurity.com/en/mediacenter/tips/cybersecurity-trends/ (accessed: June 15, 2021).

Richardson, Eric and Jake Mahle–Vorys, "Cyberattacks on the rise during the Covid-19 pandemic," Jun 1, 2020, https://www.bizjournals.com/cincinnati/news/2020/06/01/cyberattacks-on-the-rise-during-covid-19.html (accessed: June 15, 2021).

Sanger, David. "Obama Order Sped Up Wave of Cyberattacks Against Iran." *New York Times* (June 1. 2012) http://www.nytimes.com/2012/06/01/world/middleeast/obama-orderedwave-of-cyberattacks-against-iran.html (accessed: April 30, 2021).

Schmitt, Michael N. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, MA: Cambridge University Press, 2017).

Schmitt, Michael N. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Defence Centre of Excellence* (Cambridge University Press, 2013).

Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: Public Affairs. 2016).

Stephenson, Carolyn M. "New Approaches to International Peacemaking in the Post-Cold War World," in Michael T. Klare (eds.), *Peace & World Security Studies: A Curriculum Guide* (Boulder: Lynne Rienner Publisher, 6th ed, 1994).

White House, *Cyberspace Policy Review* (2011).

INSS 연구보고서 2021-18

사이버안보의 국제정치적 추세와 한국의 전략구상

발행처 사단법인 국가안보전략연구원
발행인 김기정
주소 06295 서울시 강남구 언주로 120 인스토피아 빌딩
전화 02-6191-1000 (Fax. 02-6191-1111)
홈페이지 http://www.inss.re.kr
인쇄일 2021년 12월
발행일 2021년 12월
편집 굿플러스커뮤니케이션즈(주)
ISBN 979-11-89781-70-5
979-11-89781-52-1(세트)
가격 비매품

※ 본지에 실린 내용은 집필자 개인의 견해이며, 본 연구원의 공식입장이 아닙니다.