사이버 안보와 다층적 당사자주의
: 사이버 영역에서의 처벌을 위한 대안적 접근법

고려대학교 석사과정 강준모

초록

언택트 사회가 도래하며 사이버 위협은 점차 증대하고 있지만, 그 대응 방안에 대한 논의는 여전히 미흡하다. 사이버 위협은 사이버 영역이 가진 불확실성에 기인한 특수성으로 인해 전통적 군사안보위협과 다르다. 이 특수성으로 인해 방어 위주 전략은 공격 우위의 상황을 본질적으로 바꿀 수 없을 뿐 아니라 비효율적이다. 따라서 본 연구는 방어가 아닌 감시와 처벌에 의한 공격 억지가 사이버 안보의 문제의 해결책임을 제시한다. 먼저, 사이버 위협에 대한 단일국가의 대응으로는 감시와 처벌이 불가능하며, 따라서 국가 중심적인 다자주의 접근으로는 위협 대응에 한계가 있음을 보이고자 한다. 이어 국가 뿐 아니라 비국가 행위자를 포함한 '다층적 당사자주의' 접근의 효과성에 대해 고찰한다. 비국가적 행위자의 역할을 강조한 유럽의 사이버 범죄 방지 협약 사례를 통해, 다층적 당사자주의가 효과적으로 작동하기 위한 조건을 제시하고자 한다. 이를 바탕으로 기존의 다자주의 접근에서 벗어나, 국가 행위자들이 비국가 행위자들을 포섭하기 위해 취해야 할 태도와 적실성있는 안보망 구축을 위해 행위자들이 가져야 할 자세에 대해 제언하고자 한다.

키워드 : 사이버 안보, 비국가 행위자, 처벌을 통한 공격 억지, 다층적 당사자주의, 민관협력(PPPs)

Ⅰ. 서론

COVID-19(이하 코로나)는 전 지구적인 WHO가 선언한 범유행전염병(Pandemic)으로(WHO, 2020), 전 지구적으로 유래가 없을 만큼 거대한 규모의 영향을 미치고 있다. 인간에 의해 직접 전파되는 코로나 바이러스는 인류가 서로에게 거리를 두게끔 하는 행동양식을 강요하였다. '되도록 다른 사람과의 접촉을 피한다.'는 단순한 행동양식은 다양한 산업 분야에서 변화를 초래하였다. '언택트' 생활은 곧 사이버영역의 역할과 중요성이 확대됨을 의미한다. 하지만 사이버 영역의 역할과 중요성이 커질수록 사이버 위협 역시 증가한다. 국가와 기업 조직들은 국민, 고객에 대한 서비스를 계속 유지하기 위해 활동의 대부분을 사이버 영역으로 이관했고 이로 인해 사이버 공격의 위험성을 높였다. 민관의 핵심 기능들이 중단 없이 운영되도록 하면서 새로운 원격 작업의 관행을 확보하여야 한다. 또한 사이버 영역은 군사 영역과도 연결되어 실질적인 공격력으로 사용되기도 한다. 러시아와 그루지아의 사이버전의 사례에서 볼 수 있듯 사이버 영역은 전쟁이 벌어질 수 있는 제5의 영역이 되었다. 따라서 상황의 불확실성을 이용하는 불특정, 불확실한 공격자로부터 조직을 보호하는 방법이 강구될 필요가 있다(KPMG, 2020)

하지만 사이버 공격의 문제로 인해 심화될 수 있는 안보 위기에 대한 논의는 여전히 미흡하다. 사이버 영역 그 자체가 가지는 특성과 사이버 공격의 특성은 기존의 '물리적 공간'의 특성과 전통 안보에서의 위협과는 상당히 이질적이다. 본 연구에서는 이 이질성을 다양한 차원의 '불확실성'으로 규정하고, 전통 안보에서의 위협, 공격 개념들과의 차이를 조망하고자 한다. 사이버 안보에 있어서 불확실성은 공격 식별을 어렵게 하여 공격에 대한 직접적 처벌의 가능성을 낮춘다. 이 때문에 기존 연구는 사이버 공격 억지를 위해 처벌보다 방어 역량 강화를 강조했다. 하지만 본 연구는 방어 역량 강화가 사이버 공격의 불확실한 특징과 공격 우위 상황을 바꿀 수 없다는 점에서 비효율적이라는 점을 지적한다. 근본적인 공격 억지를 하기 위해선 방어가 아닌 처벌에 기반한 사이버 안보 전략이 필요하다. 하지만 단일 국가는 사이버 공격의 불확실한 특징으로 인해 식별과 처벌을 하기 어렵다는 한계를 가진다.

따라서 본 연구는 이 한계를 극복하기 위한 방안으로 '다층적 당사자주의'를 제시하고자 한다. 먼저 사이버 안보 측면에서 단일 국가 차원의 대응에 비해 다자주의 접근이 보다 유리함을 보인다. 다자 협력을 통해 사이버 공격의 불확실성을 줄이고 처벌에 대한 합의를 만들 수 있다. 다음으로, 다자주의적 접근 논의가 전통 안보 영역과 같이 국가 중심으로 진행될 때 발생할 수 있는 한계를 언급한다. 이어 이를 극복하기 위해 비국가 행위자 포섭이 보다 수평적으로 이뤄져야 함을 강조한다. 특히 유럽의 사이버범죄방지협약을 예시로, 보다 수평적인 다자주의 접근법의 장점을 살펴보고자 한다. 이후 사이버범죄방지협약의 한계를 밝히고, 이를 보완하는 '다층적 당사자주의' 접근법을 제시하고자 한다. 마지막으로 현재 상황에서 비추어 한국의 사이버 안보 국가 전략에 대해 제언하고자 한다.

Ⅱ. 사이버 안보 및 다자주의 접근에 대한 기존 연구 분석

1. 사이버 안보의 성격 및 방어적 접근법

사이버 공격이란 해킹, 컴퓨터 바이러스, 서비스거부, 전자기파 등 전자적 수단에 의하여 정보통신기기, 정보통신망 또는 이와 관련된 정보시스템을 침입·교란·마비·파괴하거나 정보를 위조·변조·훼손·절취하는 행위 및 그와 관련된 위협을 말한다(국가정보원, 2020). 사이버 공격에서 국가를 안정적으로 지키기 위한 선행 연구들이 진행되었으며(김길동, 2017; 김상배, 2015; 김상배, 2018; 김상배 등, 2019; 김종호, 2016; 라광현, 윤혜성, 2019; 민병원, 2017; 오명호 등, 2016) 이를 통해 핵 억지와 비견되는 사이버 억지라는 주장도 나왔다(백상미, 2018; 이대성, 주성빈, 2016; 장노순, 한인택, 2013). 하지만 사이버 안보는 영역적 특성과 행위·행위자의 불확실성에 대해서 전통 안보와 구분되는 특징을 가진다. 이는 다음과 같다.

첫째, 사이버 안보는 물리적이지 않고 인공적으로 만들어진 가상의 영역에서 이뤄진다. 사이버 영역은 인터넷, 통신 네트워크 등 정보·기술 기반으로 한 정보환경의 영역이다.(오명호 등, 2016) 사이버 영역은 물리적 영역과 다르게 가상의 영역이기 때문에 지정학적 제약을 적고 국경이 명확하지 않다. 사이버 영역은 아무리 멀리 있는 존재라 하더라도 네트워크로 연결될 수 있으며, 연결되어 있다면 언제든지 피해를 입힐 수 있다. 이러한 요소에 대해서 김상배(2015)는 사이버 안보의 비지정학적 요소라 하며 전통 안보와 구분됨을 강조했다. 또한 사이버 영역에는 뚜렷한 국경이 없기 때문에 국가 주권이 어디까지 영향을 끼칠 수 있고 책임을 져야 하는지 불확실하다. 한편 사이버 영역은 물리적 영역에서의 다양한 활동들과 높은 연결성을 가진다. 따라서 사이버 영역에서의 피해는 단순 사이버 영역에 머무르지 않고 다른 영역에도 치명적인 피해를 입힐 수 있다. 2007년 에스토니아는 디도스(DDos)공격으로 인해서 금융, 행정이 마비가 되는 치명적인 피해를 입었다. 이에 오명호 등(2016)은 사이버 영역을 육해공, 우주에 이어 제5의 전장으로 제시했다. 사이버 영역은 사회 전반에 있어서 높은 연결성을 띠고 있기 때문에 가상의 공간이라 해도 높은 중요성을 가지며, 비지정학적 특징으로 인해 전통 안보와는 다른 접근을 필요로 한다.

둘째, 사이버 안보는 행위자에 있어서 국가뿐만 아니라 비국가 행위자를 고려해야 하는 특징을 가진다. 국가 대 국가 행위자를 다루는 전통 안보와 달리 사이버 안보는 공격자와 피해자가 비국가 행위자일 수 있다. 사이버 영역에서의 공격은 대표적인 비대칭전력으로, 적은 비용을 가지고 공격을 시행할 수 있다는 특징을 가진다.(Arquilla, Ronfeldt, 1996; 2001; Libicki, 2009; 김상배, 2015에서 재인용) 따라서 국가가 아닌 개인이 공격력을 가질 수 있다는 점에서 전통 안보와 다르다. 사이버 안보를 위협하는 행위자는 개인, 조직, 국가로 나눌 수 있다. 공격자는 단순히 경제적 이익을 위해서 사이버 공격을 가할 수 있으나 2000년대 들어 정치 사회적 목적을 위해 공격을 감행하는 '어나니머스(Anonymous)'와 같은 핵티비즘[1] 집단 움직임이 나타나고 있다. 따라서 사이버 안보는 행위자의 범위가 불확실하기 때문에(Rattray, Healey, 2011) 보다 광범위한 고려를 요구한다. 또한, 사이버 영역의 공격자는 사이버영역의 비지정학적 요인과 네트워크의 복잡성을 이용해 가상의 공간에 숨어 공격을 수행할 수 있다(Matusitz, 2006). 국경을 넘어 일어난 공격에 대해 해당 국가의 협력이

1) 해커와 액티비즘(정치행동주의)의 합성어로, 정치적 목적을 위해 사이버 공격을 감행하는 운동을 뜻하는 표현이다.

없다면 처벌이 불가능할 뿐만 아니라 식별도 불가능할 수 있다. 사이버 공격의 비대칭성, 사이버 영역의 비지정학적 특징, 복잡성으로 인해서 행위자를 특정하기 어렵다.

셋째, 사이버 영역에서의 공격 행위 여부는 불확실, 즉 식별이 어렵다. 전통 안보의 영역에서 물리적 공격은 유형(有形)의 수단으로 식별 가능한 피해를 입힌다. 하지만 사이버 영역에서의 공격은 무형의 존재로 식별 자체가 어렵다. 구체적으로 사이버 공격에서는 정보와 기술이 직접적인 전략 자원으로 사용된다. 공격 대상의 사이버 공간에 존재하는 결함인 착취혈을 파악하고 착취혈을 통해 시스템을 무너뜨리는 방식으로 사이버 공격은 이뤄진다(김상배, 2018). 이때 방어자는 사이버 공격을 당했다 하더라도 자신이 공격을 당한 것인지, 시스템 설계 상에 문제가 있는 것인지 바로 알지 못한다. 미국이 이란을 상대로 펼친 올림픽 대회 작전(Operation Olympic Games)에서 이란은 미국의 사이버 공격에 의해 나탄즈 원자력 발전소가 타격을 입었지만 그 원인이 사이버 공격 때문이라고 바로 인식하지 못했다(김길동, 2017). 따라서 사이버 공격은 전통 안보와 달리 공격 행위 자체가 불확실하여 식별에 어려움이 있다.

즉, 사이버 공격의 불확실성은 공격자에 대한 처벌을 어렵게 하고 예측을 불가능하게 한다는 특징을 가진다. 방어자들은 복잡한 사이버 공간에 숨은 공격자에 대해 제대로 식별하기 어렵고, 설령 공격자를 특정할 수 있다고 하더라도 비지정학적 사이버 영역에서 벌어진 일에 대해 누가 처벌해야하는가에 대한 문제가 추가로 발생할 수 있다. 나이(Nye 2017)는 불확실성으로 인해서 사이버 안보 영역은 기존의 핵 억지와는 다른 방식의 억지 전략이 필요하다고 주장한다. 억지(Deterence)는 상대방으로 하여금 행위로 인한 이득보다 손실이 크다고 믿도록 설득하여 자신이 원치 않는 행위를 상대방이 못하도록 막는 것이다(Schelling, 1970). 예를 들어, 전통 안보의 영역인 핵 억지는 국가 행위자만이 공격자가 될 수 있기 때문에 감시할 명확한 대상이 있다. 또한 적대국이 핵 공격을 감행할 경우 적대국에 대해 직접 보복을 하거나 외교적인 방법의 제재를 가할 수 있기 때문에, 공격에 대한 처벌도 비교적 명백하게 작동한다. 하지만 김상배(2018)에 의하면 사이버 안보 영역에서는 불확실성으로 인해 공격주체와 처벌 대상을 명확히 판별하기 어렵다. 따라서 불확실성이 처벌의 가능성을 극도로 줄이기 때문에 처벌에 기반한 억지 정책은 효과적이지 않음을 주장하는 새로운 접근법이 요구되었다.

나이는(Nye 2017)는 방어와 회복탄력성을 통해 사이버 공격 억지가 가능함을 주장했다. 나이(Nye 2017)에 따르면 사이버 안보는 영역의 복잡성과 행위자의 불확실성으로 인해서 처벌에 의한 억지가 이뤄지기 어렵다. 따라서 처벌에 의한 공포의 균형으로 억지가 이뤄지던 핵무기와 달리 사이버 안보의 영역은 방어를 통해 억지를 실현한다. 그는 이에 대해 거부에 의한 억지(Deterrence by denial)라는 개념을 제시했다. 방어자가 공격을 당하더라도 빠르게 회복할 수 있는 역량을 가지고 있다면 피해를 최소화 할 수 있을 것이다. 회복탄력성(resilience)에 의해 공격자는 공격으로 얻는 이익이 줄어들고 시간과 비용이 제한되어있기 때문에 공격을 포기하게 된다. 즉, 나이(Nye 2017)는 방어와 회복탄력성을 통해 사이버 영역의 공격이 억지될 수 있음을 제시했다. 하지만 본 연구에서는 먼저 나이(Nye, 2017)와 같은 방어적 접근법이 가지는 한계에 대해 지적하고자 한다.

2. 방어 역량 강화의 한계

먼저, 사이버 영역은 공격이 방어보다 우위를 점할 수밖에 없는 특징을 가지기 때문에 방어를 통한 억지는 공격을 원초적으로 봉쇄하지 못하는 한계를 가진다. 이는 공수이론(Offense-Defense

Theory of War)을 통해 판단할 수 있다. 저비스(Jervis 1978)은 안보딜레마에 영향을 미치는 요인으로 공수균형과 변별을 제시한다. 그에 따르면 공수 균형, 즉 공격의 용이성은 기술과 지리에 의해 결정된다. 기술 발전을 통한 기동력의 증가와 이동을 촉진하는 지리적 요소는 공격의 우위를, 반대로 기술 발전을 통한 화력의 증강과 이동을 저해하는 지리적 요소는 방어의 우위로 나타난다. 하지만 그의 이론은 공격이 실제로 용이한 경우는 매우 드물고, 공수 균형을 결정하는 요인이 기술과 지리 외에도 다양하다는 한계를 가지고 있다. 하지만 물리적 영역과 비교했을 때, 사이버 영역은 저비스(Jervis 1978)가 제시한 공격이 유리한 요소들을 모두 충족하고 있다. 유효한 타격을 위해 인원과 장비, 물자의 이동 혹은 첨단 설비가 필요한 물리적 공격 수단과 다르게 사이버 공격은 인터넷과 서버를 통해 이뤄지는 만큼 기동성이 굉장히 빠르고, 방어자가 인지하기 전에 이미 공격이 시작될 수 있다. 물리적 공간에서 행해지는 것이 아닌 만큼 방어에 유리한 지리적 이점은 존재하기 어렵다. 또한 사이버 공격수단은 공격이 실제로 행해지기 전까지는 공격수단의 존재를 인지하기조차 어렵다.

반 에베라(Van Evera 1999)는 이를 바탕으로 공수이론(Offense-Defense Theory of War)를 주장하였다. 반 에베라(Van Evera 1999)는 공격이 용이할 때 전쟁 위험성이 더 크다는 것을 주장하고, 행위자들이 공격에 나서게 되는 상황들에 대해 소개한다. 그 중 사이버 영역에서도 적용되는 행위 동기와 상황으로는 기회주의적 팽창이 있다. 기회주의적 팽창은 공격 시 승산이 높고 비용이 낮을 때 공격 유인이 높게 결정됨을 의미한다. 사이버 영역은 현실의 물리적 공간과 다르게 주권이 미치는 범위가 확실하게 정해지거나 고정되어있지 않다. 따라서 행위자들은 사이버 영역 내에서 자신의 영역 - 자신이 통제력을 발휘할 수 있는 공간을 최대한 확충하고자 할 것이다. 또한, 사이버 영역에서의 공격 비용은 물리적 공간과 비교했을 때 굉장히 저렴하다. 승산 역시 상술한 사례에서 볼 수 있듯, 굉장히 높다. 사이버 영역에서의 영향력이 정보의 확보와 통제 등 점차 강조되는 전략자원인 만큼, 사이버 공간에서의 팽창은 실제 공격에 나서는 동기를 부여할 수 있다.

뿐만 아니라, 사이버 공격의 부담이 전통 안보에서보다 훨씬 적다는 사실 역시 사이버 공간의 공격 우위 논리를 강화한다. 먼저 비용에 측면에서, 사이버 공격은 물리적 공격에 비해 보다 저렴하다. 전통 안보에서 공격은 물리적인 전투를 포함한다. 이는 인력과 물자, 자본을 급격히 소모시켜 경제에 악영향을 줄 수 있다. 반면 사이버 공격은 이와 같은 자원의 소모량이 상대적으로 저렴하다. 투입되는 인력의 사망률이 극도로 적으며, 이는 공격부담을 감소시킬 수 있다. 한편, 사이버 공격은 물리적 공격에 비해 사후 책임 부담으로부터 상대적으로 자유로울 수 있다. 전통 안보의 물리적 공격은 확실하게 공격자와 그 행위를 식별할 수 있다. 국가 행위자의 경우, 국제 사회의 규범으로 민주주의가 자리 잡은 시점에서 '전쟁광'과 같은 이미지는 결코 가볍지 않다. 물리적 공격을 시행한 비국가 행위자에 대해서도 이를 합당한 방식으로 사후적인 책임을 물을 수 있다. 하지만 사이버 공격은 상술하였듯 행위자와 행위 여부가 모두 불확실하다. 공격자의 식별이 어렵다는 것은 곧 책임 소재를 묻기 어렵다는 것이다. 덧붙여, 공격자가 방어자에 대해 정보의 우위를 가지고 있기 때문에 이 같은 책임 소재를 회피하기 더욱 수월할 수 있다.

즉, 사이버 영역에서는 (1) 물리적 공간에 비해 공격력 확보가 용이하고 (2) 공격 수단 및 공격 준비 과정에 대해 물리적 영역보다 더 불확실하며 (3) 공격 부담이 물리적 영역보다 적어 공격을 선택하기 더욱 쉽다는 특징이 있다. 따라서 방어자가 방어 능력을 높인다고 하더라도 공격우위의 현상이 본질적으로 바뀌는 것은 아니기 때문에 공격을 억지하지 못한다. 이는 곧 방어력 향상을 통한

억지 정책의 비효율성으로 나타나게 된다.

상술한 특징 때문에, 사이버 공격에 대한 방어를 통한 억지는 효율적이지 못하다. 특히 투입된 비용 및 자원에 비교했을 때 그에 상응하는 이익 – 안보 효능감 –을 가져다주지 못한다는 점에서 비효율적이다. 그 논리는 다음과 같다. 먼저, 공격 유인이 높다는 것을 인지한 행위자들은 보다 의도의 불확실함을 더 걱정하게 된다. 그 결과 방어 역량 확보에 더욱 매진하게 된다. 물론 '적정한 방어 수준' 은 물리적 공간에서도 정확히 알 수 없고, 안보딜레마를 야기한다. 하지만, 사이버 영역에서 이 방어 수준은 물리적 공간보다 더 불확실하다. 공격행위의 주체가 국가, 혹은 국내의 반국가 무장세력 뿐으로 한정되는 전통 안보와 다르게 사이버 안보의 공격 행위는 상술한 집단과 개인, 심지어 비인간행위자까지 확대되기 때문이다. 전통 안보는 인접국의 군사력과 지리적 요소를 종합적으로 고려한 지정학적 판단을 기반으로 방어 전력을 전략적으로 배치할 수 있다. 하지만 사이버 공격은 가능한 잠정적 행위자가 너무 많고 그 존재의 확인이 공격전까지는 불가능하다. 따라서 특정 부분에 방어 역량을 집중할 수 없고 따라서 전방위적인 방어가 요구된다. 사이버 공격의 대상이 국가기관 뿐 아니라 민관 기관, 심지어 개인이 될 수 있다는 점에서 방어 범위는 더욱 넓어진다.

뿐만 아니라, 올림픽 대회 작전 사례에서 볼 수 있듯 해당 행위가 발생하였는지 확인이 되기 전까지는 공격을 식별할 수 없다. 이는 곧 존재, 공격자, 공격 대상 모두 불확실함을 의미하고, 따라서 방어에 대한 투자가 과도해짐을 의미한다. 사이버 공격은 개인 메일, 클라우드, 오픈소스, 인공지능, POS 기기와 원격 제어 프로그램 등 다양한 경로로 발전해오고 있고, 방어자가 해당 경로에 대한 방어 역량을 확충한다면 새로운 경로를 이용하거나 기존 방식을 비트는 방식으로 발전하고 있다(금융보안원, 2020). 이에 국가들은 사이버 안보 예산을 점차 늘리고 있지만, 그럼에도 국가기관에 대한 전면적인 위협이나 개별 기업과 개인에 대한 국지적인 공격은 줄어들지 않았다.

따라서 사이버 안보에 있어서 방어에만 의존한 방식은 공격을 억지하는데 한계가 있다. 따라서 기존의 국가 행위자들은 방어 역량을 강화함과 동시에 처벌 및 감시와 같은 적극적인 공격 억지를 시도하고 있지만, 이는 나이(Nye)의 주장대로 실질적으로 그 효과를 발휘하지 못한다. 본 연구는 처벌이 실질적으로 이루어지지 못하는 이유가 사이버 영역의 불확실성에 기인한 공격 행위·행위자 식별의 어려움으로 판단하였다. 불확실성은 행위 식별을 어렵게 할 뿐만 아니라, 비국가 행위자의 처벌 주체를 확정하기 어려워 자칫 국가 간 분쟁으로 이어질 수 있기 때문이다. 이에 본 연구는 먼저 중국, 러시아 등 기존의 단일 국가 행위자들 중심으로 진행되고 있는 단일국가 차원의 처벌의 적실성과 가능성에 대해 분석한 후, 그 한계와 대안을 제시하고자 한다.

3. 단일 국가 대응의 한계 : 처벌 불가능

단일국가 대응 방식의 가장 큰 문제점은 실질적인 처벌로 이어지기 어렵다는 것이다. 공격자와 처벌자의 관계는 다음과 같이 분류할 수 있다. 우선, 확실하게 규명이 가능한 국내 행위자가 공격을 실행한 경우, 이는 국내법에 의거해 국가 내의 처벌이 가능하다. 개인정보를 이용한 소규모 해킹이 이에 해당된다. 다음으로 특정 국가가 공격을 실행한 경우, 공격을 당한 국가는 국제사회에서 이를 비난(blaming)해서 공격자에 대한 실질적인 제재를 가하거나, 양자 관계에서 무역 등의 이슈를 연계함으로 보복이 가능하다. 하지만 이 경우들을 제외한 불확실성이 지배하는 경우는 실질적인 처벌이 매우 어렵다. 실질적인 처벌이 어려운 이유는 다음과 같다.

첫째, 사이버 영역에서는 불확실성에 의해 전통 안보 영역에 비해 공격 행위자의 범위가 증가하여 공격 식별에 대한 국가의 부담이 증가한다. 사이버 영역에서는 비지정학적 요인으로 인해 물리적으로 인접한 행위자가 아니더라도 공격을 감행할 수 있다. 또한 대부분의 공격이 국가 행위자에 의해 진행되는 전통 안보에 비해 사이버 영역에서는 비국가 행위자의 공격에 대한 식별도 필요하다. 이렇듯 공격의 범위가 넓어지며 이에 대한 처벌은 더욱 어려워진다. 처벌의 전제는 처벌 대상의 특정이기 때문이다. 처벌 대상을 특정할 수 없다면, 처벌은 불가능하다. 한편, 처벌 대상이 '어나니머스(Anonymous)'와 같은 실체를 확인할 수 없는 집단인 경우 역시 마찬가지다. 만약 특정할 수 있는 대상이 인터넷 상에서 만난 다국적 개인들의 집합인 경우, 누가, 어떤 근거로 이들을 처벌할 수 있을 것인가. 만약 이들의 실체가 밝혀진다고 한다면, 현행 국제법 상 이들에게 피해를 입은 국가와 기업 등이 이들의 기소를 요청할 수 있다. 하지만 이는 개별 행위자의 출신 국가가 판결하거나 국제사법위원회 등 국제 사법 기관의 권고로 마무리된다. 즉, 국가가 유일한 처벌 능력을 가지고 있지만, 단일 국가의 능력만으로는 사이버 안보 위협과 공격을 억지하는 것이 사실상 불가능함을 보여준다.

둘째, 행위자의 특정에 성공하더라도, 사이버 영역의 비지정학적 특징에 기대어 공격을 했을 경우, 누가 처벌을 할 것인가의 문제가 생긴다. 국내 행위자가 타 국가 혹은 타 국가의 국내 행위자를 공격한 경우가 있다. 이 경우는 각 국가가 어떤 법원칙을 가지고 있느냐에 따라 문제가 복잡해진다. 형법원칙 중 속인주의와 속지주의의 구분 때문이다. 이들 사이에서 발생하는 문제는 국제법 상에서 범죄인 인도 조약에 의해 해결된다. 문제는 범죄인 인도 조약이 쌍방 가벌성(Dual Criminality)의 원칙을 따른다는 것이다. (범죄인 인도법 제 6조)[2] 이는 범죄인 인도 청구시 그 범죄는 청구국과 피청구국 쌍방에서 일정한 기준 이상의 중대한 범죄(한국의 경우 사형, 무기징역, 무기금고, 1년이상의 징역에 해당되는 경우)에 국한됨을 의미한다. 따라서 사이버 공격과 안보가 타국의 비국가 행위자에 의해 자행된 경우, 이에 대한 처벌은 국가들이 해당 공격을 어떻게 처벌하고 있는지, 그리고 그 국가들 사이에 범죄 인도 조약이 체결되었는지에 의해 좌우된다. 2002년 한국에서 발생한 미군 여중생 압사사건을 누가 재판할 것인가에 대한 논쟁은 이와 같은 경우가 자칫 외교적 문제까지 발전할 수 있음을 보여준다. 처벌을 할 수 있는 행위자가 국가라는 점에서, 속인주의와 속지주의, 국내법의 규정 차이, 조약에 의존하는 국제법의 특성은 결국 타국에 대한 비국가 행위자의 사이버 위협의 처벌을 어렵게 만든다.

정리하자면, 사이버 영역의 비지정학적 특징과 행위자의 불확실성으로 인해 단일국가 차원에서는 사이버 공격의 식별과 처벌이 불가능하다. 사이버 영역에서 방대한 범위와 차원의 행위자의 공격 행위를 식별하는 것은 단일국가에게 막대한 부담이다. 또한 사이버 공격을 식별한다 하더라도, 사이버 영역이라는 특수한 영역에서 일어난 공격에 대해 처벌을 누가 할 것인지에 대해 국가 간 분쟁이 생길 수 있다. 따라서 처벌을 통한 적극적 공격 억지는 단일국가만의 대응으로는 불가능하다. 단일 국가 차원의 접근법에 대한 대안으로는 다자주의 접근법이 제시될 수 있다.

4. 국가 중심적 다자주의 접근법과 사이버 영역에서의 한계

양자주의에 비해 다자주의가 유리한 이유는 사이버 영역에 특수성에 기인한다. 위협에 대한 다자주의적 접근방식은 전통 안보 이론에서의 집단안보 개념과 유사하다. 집단안보론은 행위당사자, 즉

2) 대한민국 범죄인인도법 제2장 제1절 제6조

국가들이 분쟁을 평화적으로 다루는데 동의함을 전제로, 국가의 협소한 이익보다 국제 공동체의 이익을 고려해야 함을 주장한다. 집단안보론은 국제정치학에서 현실주의자들의 주장에 반박하는 자유주의자들의 이론 중 하나로, 그 실효성에 대해서는 학설 대립이 첨예하게 일어나고 있다. 집단안보론이 무의미하다는 주장의 근거 중에는 동맹국 사이의 책임 전가(Buck-passing) 문제와 대응성의 문제가 있다. 하지만 물리적 공간이 아닌 사이버 공간의 특수성을 고려한다면, 이 같은 집단안보론의 흠결이 상당수 극복될 수 있다. 앞서 본 연구는 사이버 공간에는 지정학적 제약이 없고, 정보와 기술이 직접적인 전략 자원이 될 수 있음을 언급하였다. 이러한 특수성은 책임 전가의 문제와 대응성의 문제를 동시에 해결한다. 전통 안보 영역의 경우, 공격이 발생했을 때 이에 대한 방어 및 복구 등에 드는 비용이 인적, 물적 등으로 발생하며, 이러한 자원이 소모적이라는 것에서 행위자들에게 부담으로 다가올 수 있다. 하지만 사이버 안보 영역에서 물리적 영역에 비해 소모적이라고 할 수 없기 때문에 연루에 대한 부담이 적다. 오히려 방어 시스템과 역량에 대한 확인 및 점검 등 행위자에게 이득이 될 수 있다. 한편 즉각 대응의 문제는 지정학적 제약에서 벗어나며 해결된다. 사이버 영역에서는 동맹에 대한 공격 발생을 인지하는 순간부터 방어 지원까지 걸리는 시간은 지정학적 요소로 인해 결정되는 전통 안보에 비해 매우 짧기 때문이다. 뿐만 아니라 집단안보가 제대로 작동한다는 것은 공격 행위자에 대한 처벌이 가능함을 의미한다. 물리적 영역에 비해, 상기한 이유로 집단안보가 작동하기 쉬운 사이버 영역의 특수성을 고려한다면 이는 곧 공격자에 대한 처벌의 가능성을 높일 수 있다.

다자주의적 접근은 집단안보 뿐 아니라 다른 방식으로도 공격 억지에도 훨씬 탁월함을 보인다. 코헤인(Keohane 1984)에 따르면, 다자 간 협의를 통해 형성된 국제 제도는 규칙과 기구를 통해 거래 비용을 줄이고 국제 협력을 이끌어낸다. 그 근거는 다음과 같다: (1) 국제 제도는 정보의 제공과 교환을 촉진한다. 이를 통해 공통 이익을 파악할 수 있고, 비대칭 문제를 일부 해결할 수 있다. (2) 국제 제도는 합의 내용에 대한 상이한 견해를 조정할 수 있으며, 법적 구속력을 갖는 판결을 내리기도 한다. (3) 협의된 내용을 이행하는지 감시할 수 있다. (4) 국가 간 거래에 반복성을 부여해, 속임수에 대한 처벌과 이행에 대한 보상을 제공한다. (5) 제도가 충분한 효력을 가진 경우, 제재 등의 방안을 통해 직접적으로 합의 위반을 방지할 수 있다.

이 근거들은 사이버 영역의 특수성을 고려했을 때 보다 효율적으로 발현될 수 있다. 이 논리에서 사용하고자 하는 특수성은 사이버 안보에서 사용되는 주 전략 자원이 정보와 기술이라는 것이다. 먼저, 국제 제도로 인해 정보의 제공과 교환이 촉진된다는 것은 곧 '서로 양보할 수 있는 범위 내'에서 사이버 영역에서의 전략자원 교환이 빈번해질 수 있음을 의미한다. 또한 이를 통해 '사이버 위협에 대한 억지와 처벌, 위협으로부터의 안보 효능감 확보'라는 공통 이익을 파악할 수 있다. 또한, 다자주의적 접근을 통해 제도와 기구가 형성된다면, 이 국제기구는 보다 '효율적'으로 사이버 영역에 대한 감시가 가능하다. 뿐만 아니라, 해당 사항에 대한 '합의'가 선행된다면 책임 소재를 묻기 어려운 위협이 발생했을 때 이에 대한 법적 구속력을 확보할 수 있다.

하지만, 국가 중심적인 다자주의가 사이버 영역에서의 공격을 억지하지 못하는 데에는 먼저 '불확실성에 기인한' 다음과 같은 이유가 있다. (1) 사이버 공격에 대한 식별이 어려워, 규범이 확립되어도 처벌의 실행으로 나아가지 못한다. (2) 행위 자체가 불확실하여 공격 여부를 즉각적으로 식별하기 힘들다. (3) 공격이라 판단하더라도 행위자의 불확실성으로 인해 처벌 대상을 확실히 판단할 수 없다. 즉, 처벌을 할 규칙은 있지만, 공격자를 식별하지 못해 처벌로 나아가지 못한다. 따라서 사이

버 공격에 대해 처벌을 실행하기 위해선 사이버 안보의 불확실성을 해소해야한다.

한편, 사이버 공격에 대한 감시와 처벌을 수행하기 위해서는 각 국가가 가지고 있는 역량과 자원의 확인 및 어느 정도의 공유가 필요하다. 문제는 사이버 영역에서 전략 자원이 되는 '정보'가 오남용되기 굉장히 쉽다는 것이다. 물리적인 영역에서의 군사력의 공유와 사이버 영역에서의 정보와 보안체계를 공유하는 것은 큰 차이가 있다. 물리적인 자원의 공유는 그 공유 내용과 정도에 있어 통제가 가능하다. 하지만 정보와 보안체계의 공유는 자칫 타 국가에게 엄청난 상대적 이익을 제공할 수 있다. 완전한 협력이 보장된다고 하더라도 문제는 가라앉지 않는다. 협력을 약속한 국가 외의 행위자가 공격에 성공한다면, 이들의 집단 안보 체계는 도미노처럼 순차적으로 붕괴하게 된다. 이들이 공유하는 정보를 통해 공격자는 2차, 3차 공격 비용을 줄일 수 있기 때문이다. 즉, 국가들 사이의 신뢰성 문제를 해결하고 협력을 더욱 견고하게 해줄 방안이 없다면 국가 중심의 다자주의 협력은 제대로 작동하기 어렵고 처벌의 기능을 완전히 수행할 수 없다.

Ⅲ. 다층적 당사자주의 접근을 통한 억지와 처벌의 실현

1. 탈(脫) 다자주의 접근법의 필요조건

물리적 공격의 역사는 국제 정치의 역사와 궤를 같이한 만큼, 이에 대해 책임 및 처벌 규정이나 방지하기 위한 국제법과 조약들이 갖춰져 있다. 반면 사이버 공격은 현재까지 이러한 국제법적 제약으로부터 비교적 자유롭다. 탈린 매뉴얼의 경우 사이버 공격 행위에 대한 문제의식을 공유했으나, 구속력 있는 매뉴얼이 아니며 국가 간 의견 차이를 반영하지 못했다(이민효, 2017). 따라서 처벌을 통한 사이버 공격 억지로 나아가기 위해선 다양한 행위자가 규범을 만들고 논의하며 합의를 도출해야한다. 이에 본 연구는 국가 중심적인 표현인 다자주의 개념에서 벗어나, 비국가 행위자를 포함하는 새로운 형태의 당사자주의 접근법인 '다층적 당사자주의' 접근법을 제시한다. 다양한 수준의 행위자의 공격을 식별하기 위해선 국가 행위자뿐만 아니라 비국가 행위자가 포함된 당사자주의, 특히 보다 넓은 층위를 포괄할 필요가 있다. 뿐만 아니라, 비국가 행위자는 국가들 간의 협력에서 발생할 수 있는 잠재적인 문제 해결에 기여할 수 있다. 즉 비국가 행위자가 협의체 내에 적극적으로 참여하는 당사자주의를 통해 사이버 공격에 대한 보다 효율적인 식별이 가능해지고, 처벌을 통한 사이버 공격 억지의 가능성이 높아진다.

비록 아무리 국가들이 사이버 안보에 대한 예산을 늘리고 보다 많은 신경을 기울인다고 하더라도, 실질적인 행정 기관이 가지고 있는 한계는 그 실효성을 극대화하는데 한계가 있다. 먼저 대부분의 국가 행정 기관은 관료제 모델을 차용하고 있다. 이는 평시에는 효율적이지만, 돌발 상황이나 이슈에 있어서는 다소 경직된 모습을 보인다. 또한, 국가 행위자와 산하 행정 기관이 아무리 사이버 안보에 역량을 기울인다고 하더라도, 이들은 그 역량을 오롯이 사이버 안보 이슈에 투자하기 어렵다. 국가에 귀속되어 있기 때문에 국가 간의 상대적 이익에 대한 문제를 해결할 수 없다는 문제 역시 존재한다. 따라서 이를 극복하기 위해 비국가 행위자를 국가 행위자와 동등하게 다자주의의 틀 안에 포섭할 필요가 있다. 이들은 행정기관과 다르게 그 역량을 완전히 사이버 안보에 투자할 수 있는 전문가 집단을 포함하고, 행정기관처럼 국가에 종속되어 있지 않기 때문에 다자주의 제도 내의 행위자들에 대한 상호 감시가 보다 용이하다. 이를 통해 국가들로만 이루어졌을 때 발생하는 효율

성의 한계를 극복할 수 있다.

더 나아가, 비국가 행위자들이 당사자주의에 포섭되어 사이버 안보라는 공통의 이익을 위해 활약한다면, 이들은 국가 간 협상에서 이슈 연계를 최대한 활용하게끔 하거나 보다 긴밀한 형태의 상호의존을 촉진할 수 있다. 사이버 안보에 대한 협력체가 보다 견고해지면 국가들은 타국의 비국가 행위자, 초국가 행위자들과의 대화 채널을 확보할 수 있고, 이들이 속한 국가들과 다른 이슈에서도 보다 긴밀한 협력이 가능해진다. 이는 곧 보다 많은 정보의 교환을 촉진하게 되고, 결과적으로 사이버 안보를 위한 협력체에게 긍정적인 상승작용을 만들 수 있다. 결국 다양한 행위자로 이루어진 협의체가 실효성을 확립하기 위해서는 비국가 행위자의 포섭이 필요하다.

실제로 국가행위자들은 사이버 안보 측면에서 다양한 비국가 행위자와 협업하고 있다. 인터넷 서비스 제공자(ISP: Internet Services Providers)와 구글(Google), 페이스북(Facebook)등의 다국적 정보기업들, 민간 사이버 보안 업체 등은 국가 행위자의 범위 바깥에서 사이버 안보 확립에 도움을 주고 있다(Carr, 2016). 비국가 행위자가 사이버 영역에서 차지하는 역량을 고려한다면, 이들에 대한 포섭 없이 국가 간 다자주의적 협력을 한다고 하더라도 이를 바탕으로 한 감시망, 억지 역량와 처벌은 실효성을 발휘하기 어렵다.

기존의 국제 협력 모델이 비국가 행위자에 대해 고려하지 않은 것은 아니다. 김상배 외(2019)에 의하면 정보 사회 세계 정상회의(WSIS:World Summit on the International Society), 세계사이버스페이스총회(GCCS: Global Conference on Cyberspace)와 같은 글로벌 거버넌스는 다중이해당사자주의를 지지하는 모델이었다. 다중이해당사자주의란, 해당 영역에 이해관계를 가진 모든 당사자들이 평등한 위치에서 참여하여 논의함을 의미한다(DeNardis, 2014; Kurbalija, 2014; Mueller, 2010 - 김상배 외, 2019에서 재인용). 사이버 안보는 국가 행위자 뿐만 아니라 비국가 행위자도 역량을 가지고 참여할 수 있는 영역이다. 따라서 국가행위자뿐만 아니라 비국가 행위자를 포함한 광범위한 글로벌 거버넌스의 필요성을 나타낸다. 김상배 외(2019)에 의하면 WSIS는 2014년 결과 문서(Outcome Document)를 통해 사이버 안보 영역에서 정부, 민간 영역, 시민사회, 기술자 공동체, 학계에 걸친 노력의 중요성을 강조해 다중이해당사자주의를 확인했다. GCCS는 개최국의 정부 주도로 이루어지는 회의이긴 하지만 2015년 헤이그 회의에서 '다중이해당사자접근'이라는 주제가 포함되고 '시민사회사전회의'조직을 만들어 다양한 행위자의 참여를 이끌어내려는 노력을 보였다(김상배 외, 2019). 다양한 글로벌 거버넌스에서 비국가 행위자의 역할이 강조되는 것을 통해 국제적으로 사이버 안보에서 비국가 행위자의 역량이 인정받고, 그 역량을 사이버 안보에 있어서 활용해야한다는 합의된 시각이 있음을 알 수 있다.

하지만 민병원(2017)은 사이버 영역에서의 다중이해당사자주의 원칙을 '신화'에 비유하며 해당 개념이 제대로 작동하지 않고 있음을 비판했다. 민병원은 미국이 지향하는 다중이해당사자주의를 시장자본주의에 비유하며 포괄적인 참여가 이뤄지는 것이 아니라 인터넷 공동체를 구축하고 참여해온 소수의 구성원들에게만 배타적으로 작동하는 원칙이라고 비판했다. 이 때문에 상향식, 민주주의와 같은 다중이해당사자주의가 아닌 자유 시장에서의 독과점 상태와 같은 글로벌 거버넌스가 생기고 이는 다시 촘촘한 망이 아닌, 어딘가 구멍이 뚫릴 수밖에 없는 망을 만들도록 한다. 이는 안보가 다면적 이슈이기 때문에 다양한 행위자에 의해 다양한 방면에서 고려되어야 한다는 점을 보완하지 못한다.

이런 측면에서, 기존의 다중이해당사자주의 모델이 효과적으로 작동하지 못한 것은 모델 내의 행위자들이 대등한 관계를 형성하지 못했기 때문이라고 해석할 수 있다. 거버넌스를 형성한 소수의 행위자들에 의해 주도되는 하향식 의사결정 모델은 결국 목적으로 하는 이슈가 발생했을 때 소수 행위자들의 이해관계를 반영할 수 있다. 하향식 모델의 국제 거버넌스에 비 국가 행위자가 포함되며, 이 문제는 더욱 심각해진다. 국제사회에서 국가가 주요 행위자라는 공유된 인식 하에, 비국가 행위자, 특히 국내 행위자는 국가에 종속되었다는 인식이 팽배하였다. 국내 행위자들이 협의 내에서 공유된 이해관계에 투자하기 보다는 소재 국가의 이익을 반영하게 되기 때문이다. 따라서, 다중이해당사주의의 한계를 극복하고 뚫리지 않는 촘촘한 사이버 안보의 망을 형성하기 위해선 민주적 상향식 의사결정 절차가 반영된 보다 수평적인 글로벌 거버넌스가 필요하다. 누구나 평등한 위치에서 문제를 바라보고 지적할 수 있어야 사이버 안보의 다면적인 문제를 인식하고 효과적인 해결로 나아갈 수 있기 때문이다. 이에 본 연구는 다중이해당사자주의의 한계를 극복하기 위해, 국가와 비국가 행위자를 동등한 위치로 놓고 서로 연계된 협력체계를 형성하는 '다층적' 당사자주의를 제시하고자 한다.

2. 다층적 당사자주의

본 연구에서 제안하는 대안적 모델인 '다층적 당사자주의'는 거버넌스 모델 내의 행위자들의 동등함을 전제로 한다. 웨튼홀(Wettenhall 2003)에 따르면, 국가 행위자가 비국가 행위자를 포섭하여 의사를 결정하는 데에는 두 가지 방식이 있다. 첫 번째는 수직적 관계가 아닌 수평적 관계로, 동의에 기반한 의사결정 과정을 강조하는 방식이다. 두 번째는 한 행위자가 전체 과정을 이끌어가는 수직적 관계에 기반한 방식이다. 기존의 다중이해당사자주의 모델은 비국가 행위자를 포섭 하는데 성공하였다. 하지만 대부분이 거버넌스 형성을 주도한 소수의 국가 주도로 진행되는 두 번째 모델이었고, 자연스럽게 국가 중심으로 논의가 진행되었다. 따라서 국가 행위자와 비국가 행위자는 기능으로 구별되기 보다는 종속관계로 귀결되었다. 즉, 이는 소수의 국가 주도로 진행되는 하향식 모델이었고, 자연스럽게 국가 중심으로 논의가 진행되었다. 따라서 국가 행위자와 비국가 행위자는 기능으로 구별되기 보다는 종속관계로 귀결되었다. 반면 '다층적 당사자주의 모델'은 사이버 안보의 당사자들과 행위자들이 대등함을 고려한다. 이 때의 대등함은 국가 - 비국가 행위자의 수직적 위계가 없이, 국가 행위자와 비국가 행위자는 사이버 안보를 위해 서로 비교 우위가 있는 기능을 특화시키는 방식으로 분화됨을 의미한다. 이 차이를 강조하는 이유는 다음과 같다.

첫째, 기존의 사이버 안보가 비효율적인 이유 중 하나는 개별 행위자가 사이버 위협에 대한 모든 요소를 고려해야했기 때문이다. 즉 위협에 대한 감시, 공격에 대한 방어, 사후 처벌 등 모든 요소를 모든 행위자가 고려하며 이는 비효율성으로 나타나게 된다. 하지만 분명 국가 행위자와 비국가 행위자는 이 안보 요소들에 있어 각자 비교우위가 있는 부분이 존재한다. 물론 국가 행위자가 모든 부분에서 우월할 수도 있고, 반대로 특정 비국가 행위자가 모든 요소에서 절대 우위를 가질 수 있다. 하지만 행위자들 간 서로 다른 특성을 고려한다면 보다 효율적인 방식으로 사이버 안보를 갖출 수 있다.

둘째, 비국가 행위자가 국가에 종속되는 경우, 비국가 행위자들은 국가 중심적으로 진행된 논의를 실천하는 수동적 행위자가 된다. 이런 경우 국가 간 사이버 안보에 대한 인식은 충분히 공유될 수 있고, 이 논의 과정이 실현될 수 있다. 하지만 비국가 행위자의 사이버 안보 고려 사항은 적실하게

반영되지 않을 수 있다. 국가에 대한 공격 뿐 아니라, 비국가 행위자에 대한 공격도 국가 내 모든 행위자들에게 위협이 될 수 있다는 점에서, 이들이 동등하게 논의에 포함될 필요가 있다.

이렇게 비국가 행위자가 대등하게 접근하는 다층적 당사자주의 접근법이 가지는 가장 큰 장점은 사이버 공격에 대한 식별은 전문가 집단을 포함한 비국가 행위자들의 연계가 발생했을 때 가장 효율적으로 이뤄질 수 있다는 것이다. 국가와 비국가 행위자의 구분 없이, 대부분의 행위자들은 자체적으로 사이버 안보 역량을 확충하기 어렵고, 안보 방식이나 프로그램의 구성에 있어서 전문가의 도움을 받는다. *Crowdstrike, Fireeye, NortonLifeLock* 등 민간 보안업체 등 예방 시스템을 구축할 수 있는 전문가 집단이 감시를 전담하는 경우, 나머지 행위자들은 다른 요소에 역량을 조금 더 투자할 수 있다. 즉 방어나 예방 시스템을 구축할 수 있는 전문가 집단이 감시를 전담하는 경우, 나머지 행위자들은 다른 요소에 역량을 조금 더 투자할 수 있다.

비국가 행위자를 포함한 당사자주의는 기존 다자주의의 규범이 미처 고려하지 못한 부분에 대해 보완할 수 있다. 앞서 본 연구는 피해자, 혹은 피해 국가가 가해자를 처벌하기 어려울 수 있음을 지적하였다. 각자에게 미치는 주권의 범위와 법적 효력이 다를 수 있기 때문이다. 사이버 영역의 경우 국가와 이해당사자간의 합의된 법규범이 필요하다. 실질적인 처벌권을 가진 국가들과 비국가 행위자들이 법규범에 대한 합의를 이뤄내야 한다. 다양한 국가에 걸친 다국적 기업과 같은 비국가 행위자를 고려한 보완된 규범을 만들 수 있다. 이를 바탕으로 법 규범을 확립할 수 있다면 비국가 행위자에 대한 '애매한 경우'의 처벌이 가능해진다.

비국가 행위자를 포함한 다층적 당사자주의 사이버 안보의 가능성을 보여준 예시로는 유럽의 사이버범죄방지협약을 들 수 있다. 유럽은 사이버 안보의 비지정학적 특수성을 이해하고 다자주의적 협력의 필요성을 인식해 다자 협력을 규정하는 협약을 체결하였다. 본 협약은 앞서 언급한 당사자주의가 실효성을 발휘하기 위한 조건을 일부 만족했다. 사이버범죄방지협약은 사이버 범죄에 대해 세세한 규정을 세우고 사회 안전을 도모했을 뿐만 아니라, 국가 간, 기업 간 상호 협력을 명시했다(김상배 외, 2019). 사이버범죄방지협약은 사이버 범죄의 수사와 기소 및 관할권에 관한 절차법을 만들어 다자주의 협력의 걸림돌이던 처벌에 대한 문제를 해결하고자 했다. 사이버 범죄에 대해 형사사법공조의 권리와 의무 및 절차를 명시하고, 범죄자 인도에 관련된 규칙을 만들어 사이버 범죄 처벌 능력을 가지게 되었다. (김상배 외, 2019) 이를 통해 사이버범죄에 대한 효율적 대응, 국가 간 정책 재조정을 통한 양보 범위 확보, 그리고 처벌을 위한 법적 구속력 확보를 위한 합의를 해냈다.

총 67개국이 가입한 사이버범죄방지협약은 다양한 정보 공유와 처벌 가능성을 도입해 가입 국가의 사이버안보를 강화했다. 사이버범죄방지협약은 가입국가 간 정책적 협력 및 조정 개선과 민관 측면의 협력을 강조했다(Christou, 2018). 라광현, 윤해성(2019)은 사이버범죄방지협약이 사이버범죄에 대응하기 위한 국제적인 협력이라는 상징성뿐만 아니라 국가 간 형사사법공조 및 민간과의 협력을 활용하여 활발하게 활용되고 있다고 평가했다. 해당 협약은 사이버 범죄의 수사와 기소 및 관할권에 대한 절차법을 규정하여 효과적인 처벌을 가능하게 하였고, 국제 공조를 바탕으로 이를 용이하게 하고 있다(COE 2015, 김상배 외, 2019에서 재인용).

이런 방식으로 유럽의 사이버 안보 체제가 억지와 처벌이 가능했던 이유는 다음과 같다. 먼저 유럽의 경우 국가 간 협력의 수준이 매우 높다. 앞서 상술하였듯 사이버 위협 및 관련 이슈가 발생하

였을 때, 부다페스트 협정 국가들 사이의 긴밀한 공조를 통해 추적을 성공할 수 있었고, 실효적인 처벌이 이뤄질 수 있었다. 다음으로, 국가 간 합의가 민간 기업, 이익집단, 시민사회로 확대되며 이와 같은 안보 전략의 실효성이 증가할 수 있었다. 부다페스트 협정의 효력은 높은 수준의 PPPs(Public-Private Partnerships, 이하 민관협력)을 바탕으로 하고 있다. 독일의 KRITIS-UP가 IT 위기의 조기 탐지 및 완화에 기여하듯(ENISA, 2017), 높은 수준의 민관협력는 사이버 안보 역량 확충에 있어 효율성을 제고하고 그 범위와 역량을 더욱 크게 할 수 있다. 민간 기업, 이익집단과 시민사회는 국가 간 협정에 대해 감시하고, 이들 간의 이익 관계를 결정하는 중요한 행위자로 역할을 할 수 있었다. 또한 국가 간 상호의존을 국내 영역까지 확장하며 더욱 복잡하게 만들었고, 이는 다양한 이슈로 연계되며 사이버 안보 영역에서의 이해관계에 대한 '공유된 인식'을 공고히 하였다.

더 나아가 본 연구는 유럽의 국가 - 비국가 행위자 간의 긴밀한 협력을 가능케 한 원인을 유럽 내 행위자들의 복합 상호 의존에서 찾고 있다. 부다페스트 협정 체결 당시 당사국들은 대부분 유럽 소속이었으며, 이들은 기존부터 유럽연합(EU: European Union)를 형성해 높은 수준의 경제적 상호의존을 유지, 발전하고 있었다. 국가 차원에서 하나의 경제 블록으로 발전한 EU는 세금 감면 등 역내 비국가 행위자들이 활동하기 유리한 조건을 제시하였다. 따라서 EU 소속 국가, 비국가 행위자들은 이를 바탕으로 다양한 이슈를 연계하고 상호 의존을 높이고 있다. 앞서 설명한 효율성의 조건 중 비국가 행위자를 포함한 이슈연계가 용이한 것이다. 높은 수준의 통합은 역내 모든 행위자들 간의 다양한 협상이 가능하게 하였다. 이는 사이버 안보 이슈에 대해서도 모든 행위자들 사이의 공유된 이해관계를 형성할 수 있었다. 이를 바탕으로 당사자들은 개별적, 국가 중심적 접근보다 훨씬 효율적인 집단적, 다층위적 사이버 안보 시스템을 구성할 수 있었다.

하지만 유럽의 사이버 범죄 방지 협약이 완전히 성공적으로 정착했다고 평가하기는 어렵다. 일부 성과가 있었지만 실제로 사이버 위협, 범죄의 수를 유의미하게 줄이지 못했기 때문이다. 이들이 확실하고 안정된 성과를 내지 못한 이유는 다음과 같다. 사이버공격이 복합적인 특징을 가지고 있음에도 불구하고, 사이버 범죄 방지 협약의 조인국과 그 행위자가 한정되어 있었다는 것이다. 당사자들 사이에서는 사이버 영역에 대해 정보가 공유되며, 공유된 반경 내의 행위에 대해서는 민감하게 반응할 수 있다. 하지만 그 영역 밖의 행위에 대해서는 상대적으로 반응성이 떨어질 수밖에 없다. 사이버 영역이 비지정학적이라고 하더라도, 감시망으로부터 상대적으로 먼 행위에 대한 인식은 늦을 수 있고, 영역 외 행위자에 대한 처벌이 어렵기 때문이다. 따라서 협정 외부의 행위자들로부터의 공격에는 다소 취약할 수 있다.

이에 본 연구는 다층적 당사자주의가 제대로 작동하기 위해선 포괄적인 차원(level)의 행위자뿐만 아니라 포괄적인 범위의 행위자에 대한 포섭이 필요함을 주장한다. 유럽의 사이버범죄방지협약은 부분적 협력이 사이버 공격에 대해 가지는 한계를 보여줬다. 따라서 협상 외부에서 자행되는 공격에 대응하기 위해서는 더욱 많은 국가와 비국가 행위자가 포함된 당사자주의가 필요하다. 외부의 영역을 줄이고 사이버 공격에 대한 처벌 가능성을 늘리기 위해서 다층적 당사자주의가 요구된다.

3. 다층적 당사자주의의 실현 조건

다층적 당사자주의는 실증적인 거버넌스 모델보다는, 모든 행위자들의 행태 변화를 촉구하는 당위적인 사고 모델에 가깝다. 따라서, 다층적 당사자주의의 실현을 위해서는 행위자들의 인식의 전환

및 사고방식의 변화가 필요하다. 따라서 본 연구에서는 경험적 근거에 기반한 실현 근거를 제시하기 보다는, 다층적 당사자주의의 실현을 위해 행위자들이 견지해야야 할 태도를 제시하고자 한다. 먼저, 협력체 내의 모든 행위자들은 사이버 안보의 이익이 제로 섬(Zero-sum)이 아닌, 협력을 통해 절대적 이익을 늘릴 수 있다는 점을 인식하여야 한다. 협력체 내의 실효성 있는 논의를 위해, 그리고 협력체 외부의 행위자들을 포섭하기 위해 행위자들은 협력을 통해 사이버 공격에 대한 안보 효능감이라는 공통의 절대적인 이익을 인지해야 한다. 특히 협력체 외부의 국가를 포섭하기 위해서 협력체 내의 국가들은 협의를 위해 '서로 양보할 수 있는 범위'를 확대하여야 한다. 협력체 외부의 국가들이 내부로 포섭된다면 협력체는 보다 강력한 감시망을 확충하고 처벌 가능성을 높힐 수 있을 뿐 아니라, 잠재적인 공격 행위자를 줄일 수 있기 때문이다. 협력체 외부의 행위자를 포섭하기 위해 국가들은 사이버 영역의 모든 행위자와, 정보 및 기술이라는 전략자원을 군사력, 경제력 등의 핵심 전략 자원들과 대등하게 볼 필요가 있다. 그리고 이들을 연계함으로 협의 가능성을 높이고 협의 내용의 범위를 넓힐 수 있을 만큼의 윈셋(Win-set)을 확보할 수 있다. 국가들 간의 협의에서는, 정보와 기술의 공유를 하나의 협상 품목으로 삼아 타 이슈와의 연계를 통해 협의 가능성을 높일 수 있다.

한편, 관념적으로 국가 행위자들은 국가 중심주의적인 접근법을 포기할 필요가 있다. 국가 행위자들은 비국가 행위자 포섭의 필요성을 인식하여야 한다. 물론 국가 중심의 논의가 국가 행위자 각각에게 이득이 될 수 있다. 하지만 공유된 인식을 바탕으로 공공선을 지향할 수 있는 거버넌스가 형성된 이후에는, 국가들 사이에는 상대적 이득에 대한 우려 혹은 속임수에 대한 우려가 상당수 절감된다. 적실하고 효율적으로 작동하는 체제에서 벗어나는 것이 단기적인 이익을 부여할 수는 있지만, 사이버 영역의 중요성과 기술이 발전하며 장기적으로는 집단 안보 체제에서 벗어나는 것이 손해가 될 수 있기 때문이다. 특히 국가와 비국가 행위자들 사이의 협의에서는, 비국가 행위자에게 국가가 세금 감면 등의 혜택을 부여해 보다 적극적으로 포섭할 수 있다. 국내의 비국가 행위자를 행정 기관처럼 국가에 종속된 것으로 보는 것이 아니라, 국가 간 협의에서처럼 대등한 관계로 고려하며 협상을 진행할 필요가 있다.

특히 정보라는 전략자원에 집중해, 국가와 비국가 행위자 사이에는 '시놉티콘Synopticon' 형태의 상호감시체계가 형성될 필요가 있다. 벤담의 파놉티콘Panopticon이 일방적인 감시를 가능케 하는 시선의 비대칭성을 활용했다면(Bentham, 1843), 정보 기술의 발전은 이를 초월하는 시놉티콘의 형태를 가능하게 했다. 매티슨(Mathiesen, 1997)은 정보통신 기술의 발전으로, 다수의 일반 대중이 소수의 권력자를 감시할 수 있게 되었으며, 권력자와 대중이 동시에 서로를 보는 매커니즘이 가능함을 주장했다. 물론 전통 안보 및 사회 구성에서 국가와 비국가 행위자 사이에는 파놉티콘 형태의 감시망이 형성되는 것이 타당할 수 있다. 홉스의 사회계약과 마찬가지로, 사회 질서 유지를 위해 개인들이 가진 주권의 일부를 국가에 양도하고, 이를 통해 국가가 범죄 등의 행위를 통제하기 위해 정보를 감시하는 것이 정당화되듯 말이다. 이는 피감시자의 자발적인 협조에 의해 이루어진다는 특징을 가지는 '수퍼파놉티콘Superpanopticon'의 전자감시 체제(Poster, 1996)와도 의미가 상통한다. 하지만, 국제적인 차원에서, 다시 말해 주권의 양도가 불가능한 행위자들이 모인 상황에서 파놉티콘 형태의 감시망은 '비교적 대등한 행위자로 고려되는' 국가들에 의한 감시일 뿐이며, 이는 상술하였듯 국가중심주의의 부작용을 가져올 수 있다. 따라서 사이버 영역에서, 국가와 비국가 사이에는 서로가 서로를 충분히 감시하고, 통제할 수 있는 대등한 위치의 시놉티콘 형태의 감시망이 형성될 필요가 있다. 이를 위해서는 국가 행위자의 인식 변화 뿐 아니라, 국제 기구의 능력을 더 책임있는

것으로 만들고, 시민단체, 노조, 환경운동 및 여성운동 집단을 포함한 시민 사회 전체가 국가 및 국제기구의 의사결정을 지속적으로 감시해야 한다(홍성욱, 2001).

이를 위해 국가 행위자들은 물질적 개념에서 비국가 행위자에게 당사자주의에 들어올 수 있을 만큼의 이득을 줄 수 있어야 한다. 비국가 행위자 역시 사이버 영역에서의 정보와 기술이 중요한 전략 자원이자 거래 수단임을 인식하고 있다. 이를 개별 행위자의 이익을 위해서가 아니라 국제 공동체 전반의 이익을 위해 사용하기 위해서는 당위를 포함한 설득도 필요하다. 뿐만 아니라 이들에게 정보와 기술의 독점권 등을 일부 양보할 수 있을 만큼의 유인을 부여할 필요가 있다. 국제 사회 내의 수많은 비국가 행위자들에게 국제 사회 차원에서의 시장 확보, 세금 혜택 등을 통해서 보다 많은 비국가 행위자들이 공공의 이익을 고려할 수 있게끔 해야 한다.

비국가 행위자들의 경우는 크게 이익집단과 시민사회로 나누어 생각할 수 있다. 민간 기업 등의 이익집단은 이익 극대화를 목적으로 한다. 현실적으로 이들은 다른 행위자의 제안에서 이득이 생긴다고 판단할 때 이를 수용할 것이다. 하지만, 이익집단 역시 제안에 참여했을 때의 이득 뿐 아니라 참여하지 않았을 때의 손해를 고려할 필요가 있다. 전통 안보 네트워크는 국가가 제공하는 공공재의 성격을 가진다. 하지만 사이버 안보 네트워크는 전통 안보에 비해 국가가 제공할 수 있는 수준이 부족할 수 있고, 개별 이익집단들이 고유의 안보 시스템을 구성할 수 있다. 그럼에도 불구하고, 개별 기업이 오롯이 해당 기업의 사이버 안보를 확립하는 것은 높은 비용을 요구한다. 따라서 기업들은 다자주의 안보망에 포함될 때와 그렇지 않을 때의 기회비용을 계산할 필요가 있다.

시민사회와 NGO는 국가 행위자와 비국가 이익집단 행위자들을 연결해주는 교량의 역할을 수행할 수 있다. 이들이 '공공선'과 공익을 추구하며, 포괄적 다자주의 내의 상충하는 이해관계를 조정할 수 있고, 이들 사이의 균형을 확립할 수 있기 때문이다. 더 나아가, 사이버 안보 확립이라는 목적을 가진 시민 사회의 기구와 NGO는 국가와 이익집단들과 다르게 해당 목적 달성에 매진할 수 있고, 이는 곧 감시망 형성에 있어 큰 역할을 할 수 있다. 따라서 시민사회는 목적 달성을 위한 책임성을 가져야 한다.

Ⅳ. 결론

본 글에서는 지금까지 처벌을 통한 억지 가능성 제고와 이를 위한 포괄적 다자주의 접근법의 필요성을 주장하였다. 지금까지의 논리를 요약하면 다음과 같다. 사이버 영역이 점점 더 중요해지며 사이버 위협과 안보에 대한 논의가 필요하다. 하지만 사이버 영역과 사이버 공격이 가지는 특수성 때문에, 사이버 안보는 기존의 전통 안보와는 다른 방식의 접근법이 요구된다. 불확실성과 공격 우위 때문에 방어 역량의 강화만으로는 안보 확립에 한계가 있는 것이다. 따라서 방어 역량 강화 뿐 아니라 다른 방법으로도 억지력을 확보해야 하는데, 본 연구는 감시와 처벌을 통해 억지력을 가질 수 있음을 주장한다. 하지만 단일 국가는 감시와 처벌의 주체로 부적절하며, 그 대안으로 다자주의 접근법이 보다 적실하다. 이 때, 국가 중심의 다자주의 접근법은 사이버 안보 역량 확립을 위해 비효율적이며, 국가 중심으로 확립된 안보망에는 결함이 생길 수 있다. 이 결함을 막기 위해서는 비국가 행위자를 당사자주의의 틀 안으로 포섭해야 한다.

비국가 행위자를 포섭하는 방식에는 국가 행위자와 비국가 행위자 간의 관계를 수직적으로 보는 방법과 수평적으로 보는 방법이 있다. 대부분의 다자주의 국제 레짐이 비국가 행위자를 국가의 하위 요소로 보는 수직적 접근법을 채용하는 반면, 사이버 안보 영역에서는 높은 수준의 민관협력(PPPs)를 비롯한 수평적 접근이 필요하다. 실제로 수평적 접근 방식을 채택한 유럽 사이버 범죄 방지 협약의 사례를 분석하며, 사이버 안보 역량 강화를 위한 적극적 민관협력의 양태와 이를 통한 감시와 처벌의 가능성을 살펴보았다. 사이버 범죄 방지 협약의 일정 성과를 인정함과 동시에, 보다 효율적이고 적실한 거버넌스 형성을 위해서는 협약 '외부자'를 줄이고 더 많은 행위자를 내부에 포섭할 수 있는 '포괄적 다자주의'가 필요하다. 이를 위해서는 국가 행위자들은 전통 안보에서 발생하는 상대적 이익의 문제가 사이버 안보에서는 다른 방식으로 나타난다는 사실을 인지하고, 보다 높은 수준의 상호 연계를 통한 공공선을 지향할 필요가 있다. 이를 위해 비국가 행위자를 국가의 하위 행위자로 인지하기 보다는 국가와 대등한 공격 및 억지 능력을 가진 수평적인 행위자로 인지할 필요가 있다. 이익 극대화를 고려하는 기업 등의 행위자는 정보와 기술이라는 전략 자원에 대해 배타적인 견해를 고수하기 보다는, 건전하고 실효성있는 거버넌스가 갖춰졌을 때를 고려하며 협상에 적극적으로 임하는 것이 요구된다. 마찬가지로 이는 국가 행위자가 이들의 목적과 고려대상을 충분히 감안하고, 적실한 협상안을 제시하는 것을 전제로 한다. 그리고 시민 사회와 초국가적 NGO들은 이들 사이에서 교량의 역할을 함과 동시에 안보망의 구성과 작동을 감시하고 확인하는 역할에 대한 책임감을 가질 필요가 있다.

한국은 사이버 기술이 발달해 사이버 영역과 물리적 영역 간에 연결이 긴밀하기 때문에 사이버 영역의 피해가 국가적 피해로 이어질 수 있다. 북한에 의한 사이버 위협에 노출되어 있고 물리적 공격과 함께 사이버 공격이 함께 이뤄질 경우 심각한 피해를 입을 수 있다. 사이버 영역이 취약하고 국가적 위기로 이어질 수 있지만 사이버 안보 전략에 대한 논의는 단일 국가적 차원에 머물러 있다. 정부가 발표한 2019년 국가사이버안보전략은 민관군의 협력을 통해 사이버 위협에 효율적으로 대응할 것을 추구한다(청와대 국가안보실, 2019). 단일국가 차원에서 다양한 행위자를 고려한 사이버 안보 전략은 국가 단일 대응 체계에 비해 발전되었지만, 이 역시 방어와 회복에 초점을 맞췄기 때문에 실질적인 공격 억지로 나아가지 못하고 비효율적이다. 따라서 한국이 불확실한 사이버 공격을 억지하고 사이버 영역을 안전하게 운용하기 위해서 포괄적 다자주의에 기반한 다양한 국가, 비국가 행위자와의 협력이 필요하다. 사이버 공격이라는 버추얼 창을 막기 위해서 포괄적인 행위자들이 포함된 망을 이용한 감시와 처벌을 통한 적극적인 공격 억지가 필요하다.

참고문헌

Arquilla, John and David Ronfeldt. 1996. The Advent of Netwar. Santa Monica, CA: RAND Corporation.

Arquilla, John and David Ronfeldt. 2001. “The Advent of Netwar (Revisited).” In John Arquilla and David Ronfeldt (eds). 2001. Networks and Netwars: The Future of Terror, Crime and the Militancy. Santa Monica, CA: RAND Corporation.

Bentham, J. 1843. The Works of Jeremy Bentham (Vol. 7). W. Tait.

Carr, Madeline. 2016. "Public-private partnerships in national cyber-security strategies." *International Affairs* 92.1, 43-62.

Christou, George. 2018. “The challenges of cybercrime governance in the European Union”, *European Politics and Society* 19:3, 355-375

Jervis, Robert. 1978. “Cooperation under the Security Dilemma”. *World Politics*, 30(2), 167-214.

Keohane, Robert. 1984. *After Hegemony: Cooperation and Discord in the World Political Economy.* Princeton; New Jersey: Princeton University Press.

Libicki, Martin C. 2009. *Cyber Deterrence and Cyber War*. Santa Monica, CA:RAND Corporation

Mathiesen, T. 1997. The viewer society: Michel Foucault'sPanopticon'revisited. Theoretical criminology, 1(2), 215-234.

Matusitz, Jonathan A. 2006. *Cyberterrorism: A Postmodern View of Networks of Terror and How Computer Security Experts and Law Enforcement Officials Fight Them*. Ph.D. Dissertation, University of Oklahoma.

Nye Jr, Joseph S. 2017. “Deterrence and Dissuasion in Cyberspace.”. *International Security Volume 41. Issue 3.* 44-71

Poster, M. 1996. Databases as Discourse; or, Electronic Interpellations Mark Poster. Computers, surveillance, and privacy, 175.

Rattray, Gregory J. and Jason Healey. 2011. “Non-State Actors and Cyber Conflict.” In Kristin M. Lord and Travis Sharp (eds). America’s Cyber Future: Security and

Prosperity in the Information Age. Vol. 2. Washington, DC: Center for A New American Security

Schelling, T. C. 1970. “The diplomacy of violence”. *In Theories of Peace and Security* . Palgrave Macmillan, London. 64 - 84

Van Evera, Stephen. 1999. *Causes of War: Power and the Roots of Conflict*. Ithaca; London: Cornell University Press.

Wettenhall, Roger. 2003, “The Rhetoric and Reality of Public-Private Partnerships.”, *Public Organization Review* 3, 77-107

김상배, 2015, "사이버 안보의 복합지정학 : 비대칭 저쟁의 국가전략과 과잉 안보담론의 경계" 『국제지역연구』 Vol.24 No.3. 1-40

김상배, 2018, 『버추얼 창과 그물망 방패 : 사이버 안보의 세계정치와 한국』. 한울아카데미

김상배, 김소정, 김규동, 정태진, 유인태, 차정미, 이승주, 윤민우, 양정윤, 유지연. 2019. 『사이버 안보의 국가전략 2.0. : 국제규범의 형성과 국제관계의 동학』. 사회평론아카데미.

김종호. 2016. 사이버 공간에서의 안보의 현황과 전쟁억지력. 법학연구, 16(2), 121-158.

라광현, 윤해성, 2019, "유럽평의회 사이버범죄방지협약 성과에 대한 실증적 검토." 『범죄수사학연구』 5.1 : 49-73.

민병원. 2017. "인터넷 거버넌스와 다중이해당사자주의의 신화." 『국제지역연구』 26.4 , 153-183.

백상미. 2018. 사이버공격 억지를 위한 적극적 방어개념의 국제법적 적법성. 국제법학회논총, 63(2), 81-110.

오명호 ,유진철 ,한창희 ,신규용 ,강정호 ,이종덕 ,이인수 ,전병진 ,박기택 ,유대훈 ,엄영문 ,박명환 ,김재철 ,김송현 ,황재룡 ,남호림 ,신상복 ,한덕수 ,김호길 ,육군사관학교 ,해군사관학교 ,공군사관학교 컴퓨터과학 ,육군3사관학교, 2016, 『사이버전 개론 : 사이버전 전문가를 위한 필독서 = Introduction to Cyber warfare』, 서울 : 민음사

이대성, 주성빈. 2016. 사이버 테러리즘에 대한 억지력 모색. Crisisonomy, 12(9), 129-142.

이민효. 2017. "사이버전에 적용될 국제법에 관한 Tallinn Manual 고찰." 『人道法論叢』 37. 9-42.

장노순, 한인택. 2013. 사이버안보의 쟁점과 연구 경향. 국제정치논총, 53(3), 579-618.

홍성욱. 2001. 벤담의 파놉티콘 (Panopticon) 에서 전자 시놉티콘 (Synopticon) 까지: 감시와 역감시, 그 열림과 닫힘의 변증법. 한국과학사학회지, 23(1), 69-96.

ENSIA, “Public Private Partnerships(PPP) - Cooperative models”, https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models (검색일 : 2020. 06. 19)

KPMG, 2020, “The cyber security implications of COVID-19” https://home.kpmg/xx/en/home/insights/2020/04/the-cyber-security-implications-of-covid-19.html (검색일 :2020. 06. 08)

WHO, 2020, “WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020”, https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020 (검색일 : 2020. 06. 08)

국가정보원, 2020, 사이버안보 업무규정, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%82%AC%EC%9D%B4%EB%B2%84%EC%95%88%EB%B3%B4%EC%97%85%EB%AC%B4%EA%B7%9C%EC%A0%95/(31356,20201231) (검색일 : 2021. 1. 21)

금융보안원, 2019, “2020년 사이버보안 이슈 전망”. http://www.fsec.or.kr/user/bbs/fsec/42/312/bbsDataView/1363.do?page=1&column=&search=&searchSDate=&searchEDate=&bbsDataCategory= (검색일 : 2020. 06. 14)

김길동, 2017, “사이버 ‘전쟁’? 새로운 조약이 필요한 이유”, http://www.asaninst.org/contents/%EC%82%AC%EC%9D%B4%EB%B2%84-%EC%A0%84%EC%9F%81-%EC%83%88%EB%A1%9C%EC%9A%B4-%EC%A1%B0%EC%95%BD%EC%9D%B4-%ED%95%84%EC%9A%94%ED%95%9C-%EC%9D%B4%EC%9C%A0/ (검색일 : 2020. 06. 14)

청와대 국가안보실, 2019, “국가사이버안보전략”, http://www1.president.go.kr/articlesqi/5893 (검색일 : 2020. 06. 24)