사이버 안보와 규범

2023

한국사이버안보학회
KACS

한국사이버안보학회 워킹페이퍼 12호
발간일: 2023년 12월 29일

김소정 (국가안보전략연구원)

〈요 약〉

지난 20여년간 사이버공간을 규율할 수 있는 규범 정립에 대한 논의가 지속되어 왔음에도 불구하고, 사이버공간을 악용한 공격은 지속되고 있으며 이에 대한 책임부과는 전무하다. 2022년 발발한 러시아의 우크라이나에 대한 사이버공격은 피해국인 우크라이나에 심각한 피해를 야기했음에도 불구하고, 국제사회가 이에 대해 책임을 부과할 수 있는 규범은 아직 정립되지 않았다.

국제사회는 NATO의 CCDCOE를 중심으로 강제성을 띄는 국제법 제정을 위한 노력을 진행했고, 동시에 비구속적 · 자발적 규범 정립을 위한 논의를 다자적 국제기구차원과 지역기구 차원에서 진행했다. 또한 자발적 규범 정립 노력은 다양한 형태의 소다자회의체와 양자협력시 다루어지기도 했다. 규범 형성을 위한 노력의 주체적 측면에서 보면, 상기 플랫폼에서 국가 중심의 규범 형성 논의들과병행해 민간기업 및 시민사회 등의 주도의 이니셔티브들도 별개로 진행되었다. 이 속에서 국제사회는 국가가 주도한 사이버 공격 행위를 어떻게 규제 및 저지할 것인지에 대한 국제적 규범을 자국에 유리한 방향으로 정립하고자 치열히 경쟁해 왔으며, 그간 미국과 영국으로 대표되는 서방측과 중국과 러시아로 대표되는 非서방측은 인터넷 공간을 규율하는 규범 및 원칙 설립에 큰 이견을 보여 왔다.

상기의 규범 형성 논의들은 주로 국제법 및 주권 개념의 적용가능성, 비구속적 규범 제안 및 이행 등에 대해 논의해 왔다. 특이한 사항은 해당 주제들이 논의되는 플랫폼과 관계없이 진영간 의견이 명확히 갈리고 있어, 합의점을 얻기 어려운 상황이라는 점이다. 이에, 규범의 개념과 정의에 대해 간략히 살펴보고, 사이버 공간에 적용가능한 규범 정립 노력을 강제성의 측면, 규범 형성 주체의 측면에서 살펴본다. 그리고 이들 논의가 주목하는 대주제별 진영간 입장과 논리를 살펴본다. 앞으로 전개될 사이버 안보 규범 형성 논의의 방향을 전망함으로써, 해당 논의에서의 우리나라의 역할과 시사점을 찾는데 활용하고자 한다.

I. 서론

지난 20여년간 사이버공간을 규율할 수 있는 규범 정립에 대한 논의가 지속되어 왔음에도 불구하고, 사이버공간을 악용한 공격은 지속되고 있으며 이에 대한 책임부과는 전무한 실정이다. 2022년 발발한 러시아의 우크라이나에 대한 사이버공격은 피해국인 우크라이나에 심각한 피해를 야기했음에도 불구하고, 국제사회가 이에 대해 책임을 부과할 수 있는 규범은 아직 정립되지 않았다.[1] 사이버공간에서 발생한 무력공격 수준의 심각한 공격에 대해서도 그 귀속을 명확히 하고 책임을 부여한 사례가 없다.

물론 국제사회가 무법지대로 사이버 공간을 두고 있었던 것만은 아니다. 국제사회는 NATO의 CCDCOE를 중심으로 강제성을 띄는 국제법 제정을 위한 노력을 진행했고, 동시에 비구속적 · 자발적 규범 정립을 위한 논의를 다자적 국제기구차원과 지역기구 차원에서 진행했다. 또한 자발적 규범 정립 노력은 다양한 형태의 소다자회의체와 양자협력시 다루어지기도 했다. 규범 형성을 위한 노력의 주체적 측면에서 보면, 상기 플랫폼에서 국가 중심의 규범 형성 논의들과병행해 민간기업 및 시민사회 등의 주도의 이니셔티브들도 별개로 진행되었다. 이 속에서 국제사회는 국가가 주도한 사이버 공격 행위를 어떻게 규제 및 저지할 것인지에 대한 국제적 규범을 자국에 유리한 방향으로 정립하고자 치열히 경쟁해 왔으며, 그간 미국과 영국으로 대표되는 서방측과 중국과 러시아로 대표되는 非서방측은 인터넷 공간을 규율하는 규범 및 원칙 설립에 큰 이견을 보여 왔다.

상기의 규범 형성 논의들은 주로 국제법 및 주권 개념의 적용가능성, 비구속적 규범 제안 및 이행 등에 대해 논의해 왔다. 특이한 사항은 해당 주제들이 논의되는 플랫폼과 관계없이 진영간 의견이 명확히 갈리고 있어, 합의점을 얻기 어려운 상황이라는 점이다.

본 장에서는 규범의 개념과 정의에 대해 살펴보고, 사이버 공간에 적용가능한 규범 정립 노력을 강제성의 측면, 규범 형성 주체의 측면에서 살펴본다. 그리고 이들 논의가 주목하는 대주제별 진영간 입장과 논리를 살펴본다. 특히 2024-2025 기간동안 한국은 유엔 안보리 비상임이사국에 진출하여, 안보리 내에서 평화유지와 평화구축, 여성·평화·안보 등 뿐만 아니라 사이버안보, 기후와 안보 등 신흥안보 논의를 주도해 나갈 계획이라고 밝힌 시점에서[2], 앞으로 전개될 사이버 안보 규범 형성 논의의 방향을 전망함으로써, 해당 논의에서의 우리나라의 역할과 시사점을 찾는데 활용하고자 한다.

II. 규범의 개념 및 이론적 배경

국제규범은 국제사회에서 통용되는 권리와 의무로 규정된 행동 기준으로 국가 행위에 영향을 미치며, 국가이익을 재구성한다. 특히, 냉전 종식 후 국제사회에서 전쟁과 같은 고강도 분쟁이 점차 사라지면서, 국제규범의 영향력이 상대적으로 증가하고 있다. 성공한 국제규범은 출현, 확산, 그리고 내재화로 구성되는 생애주기를 가진다(조동준, 2019).

규범이란 “특정한 정체성을 지닌 행위자들을 위한 적절한 행위의 기준”이며 (Finnemore and

1) 김소정, “러시아-우크라이나 전쟁과 사이버안보 전략구상의 함의”, 국가안보전략연구원 이슈브리프 제358호
2) 외교부 보도자료, “2024-25년 임기 유엔 안보리 비상임이사국 진출”, 2023년 6월 7일, https://www.mofa.go.kr/www/brd/m_4076/view.do?seq=370029&page=1

Sikkink 1998, 891), 주어진 정체성을 가진 행위자들의 적절한 행동에 대한 집단적 기대로 정의할 수 있다(Katzenstein 1996, 5). 규범은 습관(habit)에서 기인하거나 혹은 인센티브 제공, 설득, 사회화 등의 과정을 통해 적극적으로 구축 할 수 있다(Finnemore, 2017). 따라서 규범은 국가의 행동을 제약함에 따라 갈등의 범위를 제한하고, 국가 간 안보, 무역, 정치적 이슈의 상호연계에 대한 예측과 기대를 가능하게 한다. 국제안보규범은 국제안보질서의 안정성과 평화를 위협하거나 유해한 결과를 초래하는 행위를 통제하려는 기준이며 국제안보질서의 안정성을 유지하기 위해 주요 행위자에게 요구되는 행위를 규정한다.

안보 협력을 통한 이해득실에 따라 규범의 시발점, 형태, 주요 초점에 관한 이슈를 해결함으로써 국제규범은 정립될 수 있으나, 사이버분야는 규제 성격의 규범이 형성되는 규범 등장의 단계로 볼 수 있다(김소정 2018). 이는 규범형성을 위한 규제 대상 및 범위 논의에 있어 미 · 러 · 중 등 강대국의 입장차가 커 단시간 내 국제적 규범 형성을 어려울 것으로 보이기 때문이다. 세력우위에 있는 국가가 자국의 전력을 통제하는 규범을 수용하여 안보전략의 효과를 제한시키는 양보를 하지 않을 것이기 때문에 단기간에 규범이 만들어 질 것으로 기대하기는 어렵다(장노순 2016).

국가안보 측면에서 국제규범은 안보위협 행위나 행위자에 대한 대응요건과 수단에 대한 가이드라인의 역할을 한다. 예방과 대응, 복구활동 전반에 걸쳐 허용되는 조치의 기준과 활용할 수 있는 규범적 해결책을 제시한다. 국가는 이러한 제약 하에 자신에 게 주어진 재량 하에 적절한 수단과 수준을 선택한다. 어떤 수단을 언제 발동할 것인지는 정책적 결심의 문제이다(김소정 · 김규동, 2017).

사이버공간에 대한 규범은 결국 각국이 기존 국제법과 주권 등의 개념을 온라인에 어떻게 적용할 것인가를 구체화한 내용이 큰 틀에서 합의되어 만들어지는 과정으로 볼 수 있는데, 이에 대해서는 세계 각국의 환경과 기술수준의 편차가 커 쉽게 형성될 수는 없을 것이다. 기존 국가안보의 일부 요소로써 사이버를 인식하는 시각과 IT기술을 활용한 사이버에 기반한 국가안보의 다양한 확장성을 고려한 인식은 국가안보가 사이버를 해석하는 맥락을 다르게 규정하고, 이는 국제사회에서 자국의 전략적 이익 달성을 위한 목표지향을 다르게 설정하고 있다(김소정 · 김규동, 2018).

III. 사이버안보 규범 논의 현황

사이버공간에서의 국가 행위에 대한 규범 논의는 크게 순수 정부간 논의와 다중이해당사자 참여 논의, 학계에서의 논의로 구분될 수 있다. 정부간 기구 논의의 대표적인 예로 UN GGE와 OEWG가 있다. 이는 ICT 기술 발전이 국제안보에 미치는 영향을 위해 해결되어야 할 문제로 국제법과 규범, 신뢰구축조치, 글로벌 역량강화 등을 선정하여, 이에 대한 각 국의 입장을 반영한 보고서를 도출함을 목적으로 한다.

안보문제의 특성상 지역 또는 우방국 간의 소다자적 차원에서 보다 구체적 논의가 진행되기도 한다. 그 중 유럽안보협력기구(OSCE: Organization for Security and Co-operation in Europe)의 신뢰구축조치 프로세스와 상하이협력기구(SCO)의 국제정보안보행동수칙이 대표적이다. OSCE는 사이버공간에서의 국가간 긴장 방지를 위하여 투명성-협력-안정화 단계의 신뢰구축조치를 구체적으로 발전시켰으며[3] 아시아 지역에서는 아직 구체성은 부족하나 아세안지역안보포

럼(ASEAN Regional Forum: 이하 ARF)을 중심으로 지역 사이버 신뢰구축조치 발전을 위한 작업반이 설립되는 등 논의가 진행중이다. 본 장에서는 UN을 중심으로한 GGE, OEWG 및 SCO 국가들이 제안한 Code of Conduct, 민간 중심의 활동을 구체적으로 살펴본다.

1. UN 중심의 진영간 경쟁

1.1 정부전문가그룹(GGE)과 개방형 워킹그룹(OEWG)

1) 경과

UN 총회에서 다루는 의제에 관한 실체적 이슈를 검토하기 위해, 총회는 군축·국제안보위원회(제1위원회), 경제·금융위원회(제2위원회), 사회· 인도주의·문화위원회(제3위원회), 정치 및 탈식민지 특별위원회(제4위원회), 행정·예산위원회(제5위원회), 법률위원회(제6위원회)의 6개 주요 위원회를 두고 있다. UN 총회의 사이버 관련 논의는 제1위원회의 정보안보 논의, 제2위원회의 개발을 위한 정보통신 기술문제, 제3위원회의 디지털 인권문제로 구분되고, 각각 총회 결의를 채택하고 있다. 그 중 사이버공간의 안보적 측면과 규범적 차원의 논의는 제1위원회에서 진행되고 있다.

사이버안보 또는 디지털안보는 그 영역이 점차 더욱 확대되고 있다. 이들은 사이버첩보, 검열, 프라이버시 침해, 디도스 공격, 랜섬웨어, 멀웨어 오퍼레이션 등이 포함된다. 이들은 국가들과 개인에게 다양하게 영향을 미치며, ICT를 표적으로 하거나 활용하여 이루어진다. 국가들의 이러한 활동은 필수적인 물리적 기반시설 또는 국가안보 및 시민의 인권을 저해하거나 무력화시키고, 파괴하기도 한다.

국제사회는 국가가 주도한 사이버 공격 행위를 어떻게 규제 및 저지할 것인지에 대한 국제적 규범을 자국에 유리한 방향으로 정립하고자 치열히 경쟁해 왔다. 미국과 영국으로 대표되는 서방측과 중국과 러시아로 대표되는 비서방측은 인터넷 공간을 규율하는 규범 및 원칙 설립에 큰 이견을 보여 왔다. 특히 미국, EU 등 서방 국가는, UN에서의 논의에 비협조적이었으며, 서방국가 위주의 논의를 선호하는 경향이 있었다. 이들은 기업 등 민간을 논의에 포함시키는 다중이해당사자주의를 표방하여, 국가 중심적 규제와 규범체계를 추구하는 러시아, 중국 등의 국가들과 대립적인 양상을 보였다. 이 국가들은 정부간 국제기구인 UN 및 ITU에서의 논의를 통해 국제적으로 우위를 확보하고자 노력하는 한편, SCO 등 지역협력을 통한 주도권 경쟁을 지속하고 있었다(김소정, 2013).

1998년 이래 국제사회에서 사이버공간에 보편적으로 적용가능한 국제규범의 필요성을 논의해 왔으나, 규범 창출 과정에서 진영 간 대립과 이해관계 득실에 따른 입장 차이가 지속되었다. 제1위원회에서 ICT 어젠다를 다루기 시작한 것은, 1998년 러시아가 정보안보에 관한 결의안을 제출하면서 시작되었다. 러시아는, 정보통신기술의 발전에 따른 국제안보적 위협을 UN 총회 제1위원회(군축)의 의제로 다룰 것을 제안하였다. 이 결의안은 UN총회에서 투표없이 채택되었고

3) OSCE Decision No. 1039, "Development of Confidence-Building Measures to reduce the risks f conflict stemming from the use of information and communication technologies", PC.DEC/2039, 2012. 4. 26; Decision No. 1201, "OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communications Technologies", PC.DEC/1202, 2016. 3. 10. 참조.

(A/RES/53/70), 그 이후 국제안보 차원에서 ICT의 이용을 다루는 여러 정부간 절차가 진행되었다.

2003년 러시아가 제1위원회를 통해 제출한 결의안(UN Doc. A/58/457)을 채택하여, 사무총장에게 자문을 제공하는 역할로서 정부전문가그룹 설립을 권고하였고, 2004년 제1차 UN 정보안보 정부전문가그룹(Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security, 이하 'GGE')이 설립되면서부터 국제안보 차원에서 ICT의 이용에 의한 위협을 어떻게 다룰 것인지에 대한 논의가 본격화되었다. GGE 최종보고서가 UN 총회에서 4차례 채택되었는데, 특히 2015년에 채택된 최종보고서를 포함하는 UN 결의(A/RES/70/237)에서는 국가들이 자국의 ICT 이용에 대해 2015 GGE 보고서에 따르도록 촉구하였다.

6차에 걸친 GGE 논의 중, 특히 제3차, 제4차 회의에서 괄목할 만한 성과를 거두었다. 2013년 제3차 GGE에서 참가국들은 기존의 국제법과 주권이 온라인에도 적용된다는 점에 합의함으로써, 사이버공간 국제규범 형성을 위한 기초를 다졌다(김소정 외, 2017). 2015년 종료된 제4차 GGE는 주요기반시설에 대한 공격 금지 등 11개 규범에 합의함으로써 최소한의 규범 형성을 위한 기본이 되고 있다.

2015년 "국제안보에서 정보통신 분야의 발전에 관한 정부전문가그룹 보고서"는 미국과 러시아의 입장이 기본 골격으로 반영되어 있고, 우리나라가 제출한 보고서의 일부 내용도 신뢰구축방안에 담겨있다. 특히 2022년 발발한 러시아의 우크라이나 침공은 주요기반시설에 대한 공격을 지양하고자 합의한 GGE 결의의 위반이라는 점에서 국제사회의 비난을 받을 수 있는 근거가 되었다(김소정, 2022e).

2019년부터 러시아가 제안한 개방형 워킹그룹(OEWG : Open-ended Working Group)과 미국이 제안한 제6차 UNGGE가 동시에 진행되었다. 제6차 GGE는 뚜렷한 성과없이 종료되었음에 반해 OEWG는 제2차 회기(2021-2025)가 진행중이다. 2021년에 종료된 제6차 GGE는 최종보고서를 제출(GA Resolution 73/266)하고, 국가간 이견이 존재하고 있는 국가의 책임있는 행동에 관한 규범, 규칙 및 원칙, 신뢰구축조치(CBMs :Confidence-Building Measures) 및 역량강화(Capacity Building), 국가의 ICT 사용에 있어 국제법 적용 문제 등에 관해 지속적으로 연구할 필요성을 제기하였다.

두 개의 유사한 포럼 창설은, 미국과 러시아 사이의 마찰의 결과로 나타난 것으로서, 대부분의 UN 회원국들은 우려를 갖고 있었다. 제1차 OEWG는 2021년 3월 마지막 세션에서 보고서를 채택하였고(A/75/816), 2020년 UN총회 제1위원회에서는 러시아가 2021-2025년 제2차 OEWG 설립 결의안을 상정하면서 마찰이 재발했다. 다수의 회원국들은 제1차 OEWG가 작업을 완료하기 전에 제2차 OEWG의 설립에 동의하는 것은 시기상조라는 이유로 반대했지만, 결국 이 결의안은 투표로 채택되었고, 2025년까지 제2차 OEWG가 진행 중이다.

OEWG의 논의는 현존 및 잠재적 위협, 국제법, 규범, 정기적 대화체 설립, 신뢰구축조치, 역량강화의 여섯 가지 의제로 나누어 진행되고 있으며, 국가들은 의제별 회의를 통하여 자국의 의견을 교환하였다. 2022년 7월 제2차 OEWG의 제3차 실무회의는 연례보고서(annual report) 의장 초안을 검토하고 채택하는 과정으로 진행되었다. 채택된 연례보고서는 기존 GGE 및 OEWG 보고서 등에서 합의되었던 사항들에 대한 재확인이 주를 이루었으며, 신규 어젠다 추가는 제한적이었다(김소정, 2022e).

[2022년 OEWG 연례보고서 의장 초안 주요 내용]

서론에서 국가 및 비국가행위자의 주요정보통신기반시설 및 핵심시설 대상 악의적 정보통신기술 사용 증대에 따른 위험성을 제기하고, 지역 및 소지역 기구들의 활동 및 정보공유 활성화, 여성 참여자 증대 및 논의 활성화를 긍정적으로 평가했다. 기존 및 신규 위협으로 군사적 목적의 정보통신기술 사용 증대, 국가 · 비국가행위자 · 테러리스트 · 범죄조직의 악의적 정보통신기술 사용 증대, 국가간 분쟁시 정보통신기술 활용 증대 등을 지속적인 위협으로 재확인하였다. 주요기반시설 정보통신기술에 대한 위해행위, 신규 및 신흥 기술 발달에 따른 신규 취약점을 악용한 악의적 활동, 특히 인터넷 및 의료분야 서비스 가용성 및 무결성에 필수적인 주요정보통신기반시설을 대상으로 한 악의적인 정보통신기술 사용에 대한 위험성을 재인식하였다.

책임있는 국가 행위에 관한 규칙, 규범 및 원칙 분야에서는 규범 이행 현황 및 결론과 제안의견 추가, 기술용어 정의에 관한 국가입장 공유, 추가 규범 개발 및 제안, 공급망 무결성 강화 활동 지원 및 협력 강화 등이 추가 활동 분야로 식별되었다. 국제법 적용에 있어서도 기존 논의와 유사했으며, 추가적으로 유엔 헌장의 적용에 관한 각국 입장 파악 등이 식별되었다. 기타 신뢰구축을 위한 지역기구들의 활동의 중요성을 인정하면서, UN 차원에서 외교 및 기술 담당 컨택포인트 디렉토리 개발, 정보공유 등의 투명성 조치 시행, 비국가행위자 및 관련 다중이해관계자와의 적극적 교류를 지원할 필요성을 인식하였다. 또한 디지털 격차 극복 방안 개발, 2030 지속가능 개발 과제(Sustainable Development Agenda)과의 연계성, 관련 예산 지원 증액, 디지털 분야 성격차 해소, 다중이해관계자와의 협력 강화 등을 고려하면서 액션 프로그램(PoA: Programme of Action) 정교화 등 정례적 교류 및 역량 지원을 위한 플랫폼 개발 논의를 지속할 필요성을 강조하였다.

UN 제1위원회의 사이버안보 관련 규범 논의와 사이버안보 정책 발전을 위한 회원국들의 노력은, 앞으로도 다양한 플랫폼을 통해 추진될 것으로 예상된다. UNIDIR는 사이버안정성 작업과 컨퍼런스, 그리고 사이버정책포털 등을 통하여, 국가들의 보다 심화된 논의와 정보공유를 지원하는 역할을 하고 있다. 또한 UN GGE와 OEWG 프로세스에서는 사이버안보 관련 규범과 국제법 분야를 포함한 어젠다를 논의하여, 회원국간 보다 진전된 컨센서스를 도출하기 위해 노력하고 있다.

2) 쟁점

이러한 UN 차원에서의 논의를 추구하면서도, 국제사회는 국가가 주도한 사이버 공격 행위를 어떻게 규제 및 저지할 것인지에 대한 국제적 규범을 자국에 유리한 방향으로 정립하고자 치열히 경쟁해 왔다. 미국과 영국으로 대표되는 서방측과 중국과 러시아로 대표되는 서방측은 非인터넷 공간을 규율하는 규범 및 원칙 설립에 큰 이견을 보여 왔었다. 우선 서방측의 주장을 살펴보면 다음과 같다. 첫째 사이버공간과 인터넷 표현의 자유 · 개방 · 신뢰 등 기본 원칙 존중, 둘째 ·

개인 · 산업계 · 시민사회 · 정부기관 등 다양한 구성원들의 의견이 수렴된 국제적 규범 제정, 셋째 유엔헌장 등 기존 국제법이 사이버공간을 규율하는 국제규범의 모태가 되어야 한다, 넷째 사이버공간에 적용 가능한 신뢰구축조치(CBMs)의 이행이 필요하다. 이에 대립하는 중국 및 러시아 등의 주장은 첫째 사이버공간에서도 국가주권은 인정되며 필요시 정보통제가 가능한 공간임, 둘째 서방측의 의도대로 인터넷과 사이버공간을 규율하는 체제를 수용 불가, 셋째 국가의 인터넷 통제 강화 등을 내용으로 한 국제정보보안 행동수칙(Code of Conduct)에 대한 합의의 필요성 강조 등이다(김소정 2013).

2015년 보고서에서는 사이버공격이 무력공격으로 인정되는 요건을 제시하였고, 자위권의 정당성이 명시되었다. 하지만 자위권 행사를 위해서 국제법과 유엔헌장이 규정하고 있는 무력사용 억제와 자위권 행사의 정당성을 둘러싸고 강대국들 사이에 힘의 균형이나 안보 취약점을 극복하려는 전략적인 고려가 첨예하게 대립하고 있음을 보여주었다. 그러나, 사이버공간에서 비국가 행위자 혹은 대리행위자(proxies)의 유해한 행위를 규제할 필요성을 인정하고 있고, 국가의 의무를 포괄적으로 제시하고 있다.

미국은 정보통신기술의 우위를 바탕으로 사이버공격에 대해 안보전략의 효과를 확보하려는 방안으로 자위권과 사이버 혹은 물리적 공격의 정당성을 강조하고 있다. 반면에 러시아와 중국은 미국의 공세적인 사이버 안보전략을 제어하기 위해 노력하고 있다. 사이버공간이 군사화하거나 무력충돌의 분쟁으로 확대되는 환경을 방지하려는 의도가 있다. 이런 점에서 러시아는 유엔안보리 혹은 유엔헌장 등을 적극 활용하고자 하고, 미국은 인권법 혹은 새로운 국제 레짐(international regime) 구축에 비중을 두고 있다. 그럼에도 불구하고, 이들 강대국은 사이버 정보활동(cyber espionage)에 대해 구체적으로 논의하지 않음으로써 사이버공간에서 정보수집의 필요성을 인정하고 있는 것으로 보인다(김소정, 2022a).

3) 역량강화 필요성 인정

GGE와 OEWG 모두 개발도상국과 저개발국의 사이버안보 수준 향상이 보편적 사이버안보 수준 향상에 기여할 것이라는 점에는 합의하고 있다. 이는 보안의 속성상 가장 취약한 고리가 전체 보안의 수준을 결정한다는 점을 인식한 때문이다. 이에 진영에 관계없이 모든 국가들은 역량강화의 필요성에 대해 공감하고 이를 강화하는데 적극적으로 노력할 것을 요구하고 있다. 물론, 일부 국가들은 역량강화 활동이 자국 기업의 시장진출 기회를 확보하는 행위라고 보는 시각도 있으나, 그럼에도 불구하고 대다수 저개발국 및 개발도상국들은 자국의 역량강화 기회를 절실히 원하고 있기에, 별다른 힘이 실린 주장이 되지는 않고 있다.

특히, 국제법 등 경성규범의 합의도출은 단기간 성공할 가능성이 희박하지만, 역량강화는 대다수 참가국들이 동의하는 가치이므로, 이에 대해서는 우리나라도 쉽게 지지의사를 표명하고 있으며, 실질적으로도 많은 역량강화 활동을 시행하고 있다. 하지만 우리는 이를 개발협력이나 ODA 등과 체계적으로 매핑시키지 못하고 있어, 이 부분은 앞으로 제도적 개선이 필요한 부분으로 식별된다.

사이버안보를 위한 국제법 및 규범 형성은 더디게 진행되고 있다. 특히 국제연합을 모태로 하는 플랫폼에서는 국가간 이해관계가 첨예하게 대립하며, 저개발국 및 개발도상국의 표심이 규범 결정에 큰 기여를 하고 있다. 이들 저개발국 및 개발도상국들과 IT 선진국간 기술격차는 심각한 수준이나, 보안의 속성상 이들의 보안수준이 전세계 전체의 보안 수준을 결정하는 수준이다. 이

에, 요원한 규범마련을 통한 사이버공간 악의적 행위자 대응 외, 이들 저개발국 및 개발도상국의 사이버보안 역량 강화를 지원함으로써 전세계 보안수준 향상에 기여하고, 이를 통한 사이버안보 규범 형성시 우리 입장을 옹호할 수 있는 우호세력을 확보할 필요가 있다. 또한 대통령이 발표한 디지털 권리장전의 주요 원칙을 확산시키는데 긍정적으로 활용할 수 있는 어젠다가 될 수 있다. 대상국가의 법 · 제도 · 인력양성 · 교육훈련 등 제반 역량강화에 기여함으로써 궁극적으로 우리 보안산업의 해외진출을 위한 기반 마련하는 간접 효과도 기대 가능한 분야이다.

그러나 한국은 개발협력에 대해 KOICA 재원을 활용한 일부 사업을 추진하고 있으나, 사이버 역량 강화가 별도 ODA 재원 항목으로 구분 설정되지 않은 실정이다. 기존 ODA 사업은 IT 설비 및 시설 확충, 사이버안보센터 구축 사업, 관련 인력 교육훈련이 파편적으로 운영되어, 국가 차원의 종합적인 사이버 역량 강화 사업을 추진하지는 못하고 있다(김소정 외 2022). 2023년 외교부 과학기술자문회의에서 발간한 정책권고안에도 ODA 체계를 개선하여 사이버분야 ODA를 활성화함으로써 인류보편적 IT접근권 보장 및 사이버보안 수준 향상에 기여할 것을 피력했고, 2022년 발표한 우리나라의 인태전략에도 사이버 역량강화를 인태전략의 주요 축으로 다루고 있어, 국내 관심은 제고되기 시작한 상황이라고 볼 수 있다.

이에, ODA 사업 추진을 위한 사업 구분 기준에 사이버 역량 강화를 추가 및 구분해서 식별하고, 이에 대한 성과평가 방안을 추가함으로써 각급기관의 ODA 사업에 사이버 역량강화가 자연스럽게 포함되어 시행될 수 있도록 제도를 개선할 필요가 있다. 또한 사이버분야 역량강화를 위한 ODA 사업 수행 대상 선정국을 식별할 수 있는 기준을 마련하고, 수여국의 사이버분야 정책 우선순위를 설정할 수 있는 기준과 방법론이 개발되어야 한다. 해당 기준 및 평가방법론에 따른 수여국의 사이버안보수준 향상을 위한 정책 우선순위 식별을 지원하고 사업 시행 체계를 구축하여 우리나라가 추진하고자 하는 관련 사업을 체계화 시킬 수 있을 것이다. 마지막으로, 기 구축된 국제협력 플랫폼 및 양자 · 소다자 협력 체계를 통해 사이버 역량 강화 지원 사업 가시화시키고, 협력 활동 전개를 지원해야 한다. 여기에는 특히, 기관 단위 외 전문가 단위의 지원이 가능하도록 유관인력의 출장 및 사업시행 지원 예산 확보가 필수적일 것이다.

1.2 Code of Conduct

UN 차원의 사이버안보 규범 논의는 GGE와 OEWG를 중심으로 진행되고 있으나, 중국 · 러시아를 중심으로 비서방진영 국가들은 사이버공간의 책임있는 국가행위를 규율하기 위한 가이드라인으로 Code of Conduct를 제시했다.

2011년 UN 총회 제66차 회기에서 중국, 러시아, 타지키스탄, 우즈베키스탄 4개국은 미국, 유럽 주도의 서방 중심적 사이버공간 국제규범 수립에 대응하여 사이버공간 국가주권, 인터넷 거버넌스 체계 개선, 국가의 정보통제권 인정 등을 주요 내용으로 하는 국제정보보안행동수칙(International Code of Conduct for Information Security)을 제안하였으며, 카자흐스탄, 키르기스탄이 추가로 가입하였다. 6개 당사국은 2015년 UN 사무총장에 정보보안국제행동수칙 개정을 통보하였다.[4)]

개정안은 제3차 UN GGE 보고서 권고내용 및 UN 인권위원회의 인터넷 인권 결의를 반영하여 개정되었으며, 신뢰구축조치 등 현안이 추가되었다. 정보안보 영역에서의 기존 및 잠재적 위

4) United Nations, A/69/723, “Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General“, Jan. 9, 2015.

협과 국가행위에 관한 규범, 규칙, 원칙, 정보공간에서의 신뢰구축조치 등 위협 대응을 위한 협력조치, 관련 국제적 개념에 관한 연구에 대한 제3차 UN GGE의 평가 및 권고사항 고려를 선언했다. 국가에 의한 ICT 이용에 관한 기존 국제법 규범의 적용 방법에 대한 보편적 이해 도출 필요성을 강하고, 향후 ICT 고유의 특성에 따른 추가적 규범 발전 가능성을 인식했다.

그리고 정보무기 또는 관련 기술 확산 금지에 관한 명시적 규정 삭제, 국내문제 불간섭 원칙 강화, 민족적, 인종적, 종교적 증오를 부추기는 정보 유통 억제, 자국 정보공간 및 주요정보통신기반시설 보호 권리/의무 강조, 인터넷거버넌스, 국가 정보안전에 관한 국가중심적 기술 완화 등이 주요 내용이다. 개정안은 사이버 국제규범 관련, 기존 입장에서 크게 벗어나지 않았다. 인권존중 선언에도 불구, 국가의 정보통제 및 정보통신기술 독립성, 정보공간 주권 등 통제가능성을 열어두고 있다.

2. 소다자 협의 활성화

UN 차원의 사이버안보 규범 논의는 현재 지지부진한 실정이다. 국제사회는 UN 외 OSCE, ARF 등의 지역기구를 통한 사이버안보 규범 논의도 활성화했고, 특히 OSCE의 경우 신뢰구축조치(CBMs : Confidence Building Measures)의 개발에 합의, 이를 시행한 바가 있었다. 한국과도 격년으로 사이버안보 컨퍼런스를 진행해오는등 역량 강화를 위한 활동을 지속하고 있다. ARF에서도 OSCE의 CBMs을 적용할 수 있는 노력을 지속해오고 있다.

2011년 런던에서 시작된 런던프로세스의 일환으로 세계사이버스페이스 총회를 5회 개최했으며, 서방진영 중심의 사이버안보 규범 논의를 주도하고자 노력했다. 우리나라도 2013년 서울에서 제3회 세계사이버스페이스 총회를 개최한 바 있다. 2015년 네델란드, 2017년 인도 이후 개최가 중단되었다. 2014년 중국도 우젠회의를 개최하면서, 중러 주도의 사이버안보 규범 논의를 별도로 발족시키면서, UN 차원이 아닌, 그러나 중국이 주도하는 사이버안보 규범 논의도 별도로 진행되었다. 현재는 진행되지 않고 있다.

이에 2021년을 전후로 새로운 소다자차원의 협력을 추진해오고 있으며, 특히 QUAD와 AUKUS 등 미국 동맹국과 우방국 중심의 활동이 활발히 진행되고 있다. 이하에서는 이들의 노력에 대해 살펴보고자 한다.

2.1 쿼드(Quad)

QUAD (Quadrilateral Security Dialogue)은 인도, 호주, 일본 및 미국 간의 안보 및 국방 협력을 강화하기 위한 포럼으로 주로 안보, 국방, 지역 안정성 및 자유와 개방을 강조하는 원칙에 초점을 맞추고 있다. 2004년 재난대응을 위한 협력체로 출범했으나 각국의 정치 상황과 중국의 반발 등으로 중단되었다. 이후 2017년 쿼드 재결성 이후, 자유롭고 개방적이며 포괄적인 인도·태평양에 대한 비전을 공유하고 역내 안보와 발전을 위한 협력을 추구했다.[5)]

바이든 행정부는 인태전략에 중요한 쿼드를 정상급 협의체로 격상해 쿼드 국가와의 상호 전략적 이해 증진과 연대를 강화하고 있으며,[6)] 미·중 간 사이버 안보를 둘러싼 경합이 첨단기술 경

5) https://www.voakorea.com/a/world_behind-news_quad-china/6058122.html
6) 바이든 행정부는 2022년 2월 새로운 『인도-태평양 전략서』를 통해 "자유롭고, 개방적이며, 번영하고, 안전하며, 탄

합으로 확전되면서 협력 사안들이 확대되면서 안보적 함의가 강한 협력이 점차 증가하는 추세이다. 사이버 안보 이슈는 이러한 안보 협력의 중요한 측면 중 하나로 간주된다. 사이버 공격의 증가와 사이버 범죄의 위협에 직면하면서, 회원국들은 정보 공유, 사이버 위협 정보 교환, 사이버 보안 정책 조율 등을 통해 사이버 공간에서의 협력을 강화하고자 한다.

2021년 9월 쿼드 정상회담에서 사이버 안보에 대한 논의가 더욱 확장되었다.[7] 이전의 쿼드 정상회담 공동성명과는 다르게 사이버 안보 관련 내용을 별도로 구성하여 쿼드 차원의 대응 방안을 보다 구체적으로 제시했으며, 중점 협력 분야를 기반시설, 사이버 안보, 우주로 확대하고 각 분야별 전문가 워킹그룹을 구성하기로 결정했다. △ 공유된 사이버 표준의(cyber standards)의 채택과 이행, 보안이 안전한 소프트웨어(secure software) 개발을 위한 민관 협력, 인적 자원(workforce) 확대, 확장성(scalability) 증진과 보안이 안전하고 신뢰할만한 디지털 인프라의 사이버안보 증진, △ 차세대 과학자 및 기술자 간의 유대 관계 구축을 위한 Quad Fellowship 공식 출범시켰다.

2022년 5월 도쿄 정상회의에서는 '쿼드 사이버 안보 파트너십(QCP, Quad Cybersecurity Partnership)' 체계 강화와 쿼드 각 국가가 주도하고 있는 분야를 구체적으로 명시하였다.[8] 이를 위해, 첫째, 사이버 취약점과 위협에 대응하는 '새로운 공동 사이버 원칙' (new joint cyber principles)을 마련하고, 사이버 보안 취약점(vulnerabilities)과 사이버 위협에 대응해여 회복력 구축을 위해 개별국의 주도 분야 설정했다. 둘째, 국가 주요기반시설 보호 강화를 위해 △ 디지털 공급망 위험 요인 식별 및 평가, △ 정부 조달 소프트웨어 보안 표준 기준선 조정, △ 집합적인 구매력을 활용해 광범위한 소프트웨어 개발 생태계 개선△ 5G 및 기술 공급망에 대한 파트너십, 기술 표준 설정, △ Quad Fellowship 프로그램 등을 시작했다. 셋째, 잠재적인 사이버 사고 예방·대비와 신속 대응을 위한 역량 구축 사업 조율, 국가 CERT(Computer Emergency Response Teams) 간의 교훈과 모범 사례 교환 등 정보 공유 강화를 추진하고자 한다. 넷째, 사이버 안보에 대한 인식과 행동 강화 : 민관 협력으로 '사이버 안보의 날 캠페인' 추진 등이다.

2023년 1월 말 쿼드(Quadrilateral Security Dialogue)는 북한과 중국의 사이버 위협에 대한 대응 방안을 논의하고 "책임있는 사이버 습관 증진을 위한 협력을 위한 쿼드 공동성명(Quad Joint Statement on Cooperation to Promote Responsible Cyber Habits)"을 발표[9]했다.

2023년 5월 히로시마 정상회의에서는 사이버 안보, 첨단기술뿐만 아니라 인프라 투자, 해양 안보, 공급망 다각화를 위한 공공-민간 파트너십, 기후, 건강, 우주에 대한 주요 이니셔티브 강화를 강조하면서, 올해 처음으로 쿼드 사이버 챌린지가 개최[10]되어 사이버 인식을 제고하였으며, 중요 인프라, 소프트웨어에 이르기까지 사이버 보안을 위한 공동 원칙을 개발하고자 한다.

2.2 오커스(AUKUS

력적인 인도-태평양 지역을 위한 포괄적인 비전"을 발표

7) The White House, "Fact Sheet: Quad Leaders' Summit," September 24, 2021.

8) The White House, "Quad Joint Leaders' Statement," May 24, 2022; The White House, "FACT SHEET: Quad Leaders' Tokyo Summit 2022," May 23, 2022.

9) The White House, "Quad Joint Statement on Cooperation to promote Responsible Cyber habits", Feb. 07, 2023
https://www.whitehouse.gov/briefing-room/statements-releases/2023/02/07/quad-joint-statement-on-cooperation-to-promote-responsible-cyber-habits/

10) 인도 태평양 전역에서 약 85,000명이 챌린지에 참여했으며 약 600개의 학교, 대학, 기업 및 비영리 단체가 자신과 지역 사회를 보호하기 위해 조치를 취했다고 언급.The White House, "Quad Leaders' Summit Fact Sheet," May 20, 2023.

AUKUS는 호주, 영국 및 미국 간의 안보 및 군사 협력을 강화하기 위한 구심점이다. AUKUS 출범은 인태 지역에서 일본, 호주, 인도를 거쳐 유럽의 영국까지 연결하는 거대한 해양 안보 전선을 구축한다는 의미로 대중 견제를 위한 미국의 의도가 반영된 것으로, 주로 군사, 정보 교류, 기술 협력 및 안보 문제에 초점을 맞추고 있다. 특히 영국은 오커스는 물론 미국의 정보 동맹인 '파이브 아이즈' 핵심 국가로 러시아, 중국 등의 사이버공격 행위에 대한 공동성명, 사이버 규범 제정 등에서 미국과 긴밀하게 공조하고 있다.

AUKUS의 회원국인 호주, 영국 및 미국은 모두 사이버 공격 및 사이버 범죄에 대한 대응 및 방어를 강화하기 위해 노력하고 있다. 이러한 노력은 국가 간 정보 공유, 기술 협력, 사이버 보안 정책 조율 등 다양한 측면을 포함한다.

특히 인태지역의 중요성이 커짐에 따라, 사이버와 AI를 포함하는 신기술 분야 협력 강화는 3국간 주요 협력 아이템이 되고 있다. 사이버, 인공지능(AI), 양자 컴퓨팅, 핵심 기술 분야에서 협력을 강화함과 동시에 안보 정보 및 기술 공유에 주안점을 두고 있다.[11] 여기에는 전략적 차원의 사이버안보 대응 외, 사이버보안 기술적 측면의 협력 강화, 정보전 및 심리전 대응 공조 강화, AI와 사이버간 융합 현상 대응, 주요기반시설보호, 자율무기체계의 보안, 우주 및 5G 인프라 측면 등 다양한 측면이 고려되어야 한다.[12]

오커스는 자유롭고 개방적이며 평화롭고 안전한 사이버공간을 위한 글로벌 거버넌스 구축을 지향하며, 대서양 지역과 인태 지역을 연계해 사이버안보 진영화를 선도하고자 한다. 인태 지역에서 해저케이블의 안전 확보와 데이터 보호 등 사이버공간의 안전성 확보를 위한 국제 협력 강화로 대중국 견제에 공조하고 있다.

쿼드에 참여하는 호주의 오커스 동참과 미국이 예외적으로 호주에 핵 잠수함에 대한 기술을 제공하기로 한 것은 인태지역에서 중국 견제 전선을 강화하려는 목적으로 볼 수 있다. 2022년 9월 자료에 따르면, 영국과 미국은 양국이 지원하는 호주의 핵 원자력 잠수함 구축 삼자 협정은 사이버 스파이들에게 큰 공격 대상이 될 수 있다는 점을 인식하고, 동 프로그램에서 사이버보안의 중요성이 크다고 언급하고 있다.[13]

2022년 2월 미국의 FBI, CISA, NSA, 호주의 ACSC, 영국의 NCSC 등 사이버안보 당국은 오커스 차원의 랜섬웨어 위협에 관한 공동 안내서를 발표했다.[14] 안내서를 통해 사이버공간을 이용한 중국의 기술 탈취를 차단하고 사이버공격에 대한 책임귀속과 비용 부과를 위한 규범 정립과 재재, 비난 성명 발표, 수출통제, 전진 방어 등 외교적 협력하고자 함을 알 수 있다.

또한 2023년 5월 오커스 정상회의에서는 사이버 역량 강화 및 온라인 아동 보호를 강조했다.[15] 미래 사이버 보안 역량 구축 과정에서 인태 파트너 국가의 우선순위를 반영하고, 온라인

11) The White House, "FACT SHEET: Implementation of the Australia - United Kingdom - United States Partnership (AUKUS)." April 5, 2022.
12) Vijay Varadharajan, "AUKUS-Cyber Security Aspects", https://www.newcastle.edu.au/__data/assets/pdf_file/0008/864323/AUKUSCyberSecurityAspectsAAPowerToday.pdf
13) Stew Magnuson, "JUST IN : AUKUS Agreement Poses Cybersecurity Risk to Allies", 29 Sept. 2022, https://www.nationaldefensemagazine.org/articles/2022/9/29/aukus-agreement-poses-cybersecurity-risk-to-allies
14) https://www.minister.defence.gov.au/media-releases/2022-02-10/australia-us-and-uk-stand-together-confront-global-ransomware-threat
15) The White House, "Australia-United States Joint Leaders' Statement - An Alliance for our Times," May 20, 2023.

아동 성 착취 퇴치를 위한 호주-미국 합동 위원회 설립을 명시했다.

2.3 랜섬웨어 대응 이니셔티브(CRI : Counter Ransomeware Initiative)

미국 바이든 대통령은 전세계적인 랜섬웨어 공격 활성화에 대응하기 위해, 35개국 정상들과 긴급협의 후 랜섬웨어 대응 이니셔티브를 발족시켰다.[16] 이후 CRI는 3개 분과로 나뉘어 교율 및 훈련, 시나리오 개발 등을 진행한 것으로 알려지고 있으나, 세부사항은 비공개로 진행되고 있다.

일부 언론에 공개된 내용에 따르면, △ 국제 랜섬웨어 태스크 포스(InternationalCounter Ransomware Task Force) 구축, △ 지역 사이버방어센터(Regional Cyber Defense Centre) 지역거점 설립, △ 조사관을 위한 툴킷 제공, △ 적극적, 지속적 민간분야 협력 강화, △ 주요 식별된 행위자들의 TTPdp 대한 합동 권고문 발간, △단일 프레임워크로 우선순위가 높은 타겟 식별 및 조율, △역량강화 툴 개발, △랜섬웨어 대응 격년 훈련 실시 등을 논의한 것으로 알려졌다.[17]

3. 민간주도 규범 경쟁

3.1 디지털 제네바 협약

디지털 제네바 협약(Digital Geneva Convention)은 마이크로소프트가 2017년 제안한 국제 사회에서 디지털 영역에서의 국가 행위에 대한 규범을 설정하고 사이버 공격과 사이버 전쟁을 방지하기 위한 노력을 목표로 하는 제안이다. 이 협약은 국가 간의 협력, 사이버 보안, 개인 정보 보호 등 다양한 측면을 다루고 있다.

디지털 제네바 협약은 사이버 공격의 방지와 사이버 전쟁의 규범화에 초점을 맞추고 있다. 이는 국가 간의 사이버 공격을 금지하고, 개인 정보와 사이버 인프라의 보호, 국제 사이버 공간에서의 협력 강화 등을 목표로 한다. 또한, 국가 간의 전쟁 상황에서도 국제 인도적 법률의 적용을 보장하고 사이버 공격으로 인한 인재적 피해를 최소화하는 것을 목표로 한다.

디지털 제네바 협약은 현재까지 국제 사회에서 폭넓은 지지를 받고 있으며, 여러 국가와 국제 기구들이 이를 채택하고자 노력하고 있다. 그러나 아직까지 협약이 완전히 구체화되거나 법적으로 구속력을 갖추지는 않았다. 디지털 제네바 협약은 국제 커뮤니티의 논의와 협력을 통해 계속 발전하고 있으며, 사이버 보안과 사이버 공간에서의 국제 규범을 강화하기 위한 중요한 노력으로 인식되고 있다.

3.2 인터넷 미래 선언

미국은 2022년 4월, 60개 글로벌 파트너 국가와 함께 인터넷의 미래를 위한 선언

16) https://therecord.media/u-s-convenes-30-countries-on-ransomware-threat-without-russia-or-china

17) https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/fact-sheet-the-second-international-counter-ransomware-initiative-summit/

(Declaration for the Future of the Internet)을 발표했다.[18] 동 선언은 미국과 60개의 글로벌 파트너 국가rk 인터넷과 디지털 기술의 비정치적 비전을 제시하고, 세계의 단일 인터넷을 촉진하기 위해 발표했다. 우리나라는 2022년 한미 정상회담에서 이에 동참하는 것을 선언했다.[19]

IV. 사이버안보 규범 논의 – 진영간 입장 중심[20]

1. 국제법 적용

제4차 UN GGE의 가장 두드러진 특징 중 하나는 국제법의 적용방법과 새로운 자발적 규칙의 분야를 구분하여 논의하였다는 점이다. 자발적 규범은 기존 국제법에서 아직 불명한 부분을 추가적으로 규율하기 위한 것으로, 이를 수정하거나 대체하는 것은 아니다(para. 10). 그러나 이 역시 진영 간 시각차가 존재한다. 미국 등 서방은 기존 국제법 적용이 이미 원칙으로 합의된 상황에서 자발적 규범이 새로운 규칙을 정하고자 하는 것이 아니라는 입장을 취한 반면, 비서방국가는 기존 국제법이 모든 행위를 규율하지 못하기 때문에 필요한 새로운 규범이라고 보았다. 단, 서방국가 역시 기존 국제법이 모든 문제를 규율하지는 못할 것이라는 데 원칙적으로 동의하며, 이에 대해서는 새로운 법규칙이 논의되어야 하나, 현행법에 대한 충분한 검토가 완료된 후의 문제로 취급하고 있어 향후 조약 또는 관습법이 형성될 여지는 남아있다.(Koh 2012)

국제법의 적용 방법에 대해서는 상당히 심도 있는 논의가 이루어졌으나, 최종적으로 UN 헌장 등의 국제법상 기본원칙을 재확인하고, 적용방법의 권고는 단지 6개의 예시적 단락을 제시하는 데 그쳤다는 아쉬움을 남겼다. 명시된 기본원칙으로는 주권평등의 원칙, 국제분쟁의 평화적 해결원칙, 무력사용의 위협 또는 행사 금지, 인권과 자유의 존중, 국내문제 불간섭 원칙으로 UN 헌장의 기본원칙과 일치한다. 구체성은 부족하나, 사이버 공격에 대한 자위권 행사의 가능성(para. 28(c)), 무력충돌시 국제인도법상 기본원칙인 비례성과 필요성, 구분의 원칙적용을 명시하였다는 점은(para. 28(d)) 진일보한 것으로 평가할 수 있다. 또한 국제법에 따른 국제위법행위에 대하여 국제적 의무를 준수할 것을 규정하여 국가책임법의 적용을 재확인하였다(para 28(f)). 다만 국제위법행위가 국가의 의무 위반 행위를 전제로 한다는 점에서 개별 행위가 어떠한 규범을 어떻게 위반하는지에 대해서는 즉시 적용하기에 어려움이 있으며, 또한 이에 대한 국가의 대응에 대해 피해국의 입증책임 여부에 대해서는 합의가 이루어지지 않았다.

미국은 제네바협약이 전세계적으로 비준된 몇 안되는 국제조약의 하나라는 점을 강조하고, 제네바협약은 국제인도법의 성문화뿐만 아니라 전쟁 중의 윤리적 행동규범으로서도 기능해 왔다고 하였다. 미국은 민간인과 민간물자에 대한 보호는 무력충돌이 사이버공간에서 수행되는 경우에도 계속 적용되어야 한다는 점을 인식하고 있다. 이에 따르면 사이버공간에서 국제인도법 적용의 재

18) The White House, FACT SHEET: United States and 60 Global Partners Launch Declaration for the Future of the Internet“, 28 April 2022

19) 김소정, “2022 한미정상회담과 사이버안보-억지력 강화를 위한 전략적 과제” 국가안보전략연구원 이슈브리프 361호, 2022

20) 본 장의 내용은 GGE와 OEWG에 제출된 각국 position paper를 참고하여 아래 논문의 주요 내용을 재정리하였다.
김소정 · 김규동, 2017. “UN 사이버안보 정부전문가그룹 논의의 국가안보 정책상 함의”, 『정치 · 정보연구』 제20권 제2호, pp. 87-122

확인은, 장래의 충돌가능성을 증대시키는 것이 아니라, 국가들에게 무력충돌 상황에서 민간인을 존중하고 보호하는 중대한 책임을 상기시키는 것이다. 역량강화에 관한 향후 작업은 귀속의 문제를 다루는 데 도움이 될 것이지만, 법적 관점에서는 국가책임법이 귀속행위에 대한 기준을 규정하고 있으며, 국가책임법에서는 국가들이 프록시를 통하여 국제위법적 사이버행위를 하는 경우에도 그 책임을 면할 수 없다는 점을 명확히 하고 있다고 강조하였다.

중국은 무력충돌법을 적용하는 것은 사이버전쟁의 규칙을 제정하고 사이버전쟁을 허용하는 것과 같은 잘못된 정치적 메시지를 전달할 수 있다고 우려하였다. 이에 따르면 사이버공간에서 jus ad bellum과 jus in bello의 적용은 법적·기술적으로 어려움이 많고, 국가간 사이버 충돌에서는 승자를 가릴 수 없으므로, 전쟁이 발생해서는 안 된다. 대신 UN 헌장의 적용에서 인식해야 하는 핵심 이슈는, 무력사용 또는 무력사용의 위협 금지, 국제분쟁의 평화적 해결, 다른 국가의 국내문제 불간섭이다. 따라서 OEWG의 최종 보고서에는 이러한 내용이 포함되어야 한다고 강조하였다.

러시아는 국제법이 사이버공간에 적용된다고 확정되더라도 이를 적용하는 데는 여전히 문제가 있을 것이라고 지적하고, 사이버공간에 적용되는 협약 초안을 작성할 것을 제안하였다. 이에 따르면, 사이버공간에 국제법을 적용하는 것은 찬성하지만 사이버 세계의 현실에 적절하게 적용되어야 할 것이라는 점을 지적하고 있다. 국제법의 적용을 어렵게 하는 것은, 모든 국가가 사이버 공격을 무력공격으로 인식하지 않는다는 사실이다. 많은 국가들이 '예방적 사이버 타격'(preventive cyber strike) 이론을 갖고 있으며, 먼저 타격할 권리를 주장하는데, 이는 먼저 타격할 절대적인 권리에 대한 경쟁으로 이어질 수 있고, 따라서 사이버전쟁의 발발로 이어지게 될 것이다. 이와 함께 모든 사이버안보 이슈를 함께 다룰 수 있는 상설기관을 창설할 필요가 있다고 하였다.

2. 주권 적용

인터넷 주권은 사이버 주권(cyber sovereignty) 또는 디지털 주권(digital sovereignty) 등과 같은 확대된 개념으로도 사용된다. 이는 각국 정부가 사이버 영역에 존재하는 각종 디지털 자원에 대해 독립적인 통제 권한을 행사하는 것을 의미한다. 예를 들어, 중국은 자신들의 영토 내 인터넷을 통제하고 규제할 권리가 국가에게 있다고 주장하며, 2003년부터 국가 차원에서 인터넷을 검열하는 시스템인 만리 방화벽(Great Firewall)을 구축해 구글(Google)·페이스북(Facebook)·유튜브(YouTube) 등의 일부 해외 서비스와 콘텐츠를 차단하고 있다. 또한 중국과 국경 문제로 갈등 중인 인도는 2020년 틱톡(TikTok)·위챗(WeChat)·웨이보(Sina Weibo) 등의 중국 모바일 앱이 인도의 주권과 안보 및 공공질서를 침해한다며 이들에 대한 접속을 금지했다. 또한 러시아는 2019년 자국의 인터넷망이 글로벌 인터넷과 단절될 경우를 대비한다는 명분으로 러시아 인터넷인 루넷(Runet)을 구축하고 인터넷에 대한 국가 통제를 강화했다.[21]

사이버주권의 개념은 사이버안보 규범 논의에 있어 종종 등장하고 있으나, 현재 명확한 개념 정립이 되어 있지는 않다. 기술의 발전과 전세계적인 디지털 전환의 흐름 속에서 사이버 공간은 국가의 권한과 국가관계에 있어 중요한 질문들을 제기하고 있다. 자국 영토안의 사이버 공간을 통제하고자 하는 국가의 열망은 '사이버 주권 (cyber sovereignty)' 개념의 부상과 이를 행사하기

21) [네이버 지식백과] 인터넷 주권 [Internet Sovereignty] (두산백과 두피디아, 두산백과) https://terms.naver.com/entry.naver?docId=6685412&cid=40942&categoryId=32854

위한 다양한 제도적 조치들이 부상하고 있다.[22] 동시에 미국과 유럽은 중국, 러시아, 북한과 같은 권위주의 정권은 그들의 온라인 검열과 통제를 정당화하기 위해 전통적으로 사이버 주권을 언급해 왔다고 비판한다.[23] 사이버 주권 논쟁은 강대국 경쟁의 부활, 자유주의 국제질서의 쇠락과 권위주의 국가의 부상이라는 국제질서 변화와 밀접히 연계되어 나타나고 있다.

UN GGE 보고서는 6장 국제법 부분에 "국가의 ICT관련 활동에 대한 주권적용과 영토내의 ICT인프라에 대한 관할권에 이르기까지 국가주권과 국제규범과 원칙이 적용된다"고 확인하고 국가가 ICT관련 위협으로부터 자국영토의 ICT인프라를 보호하는 데 필요한 메커니즘을 수립하는 등 관할권을 행사하는 데 국제법에 따른 기존 의무가 국가의 ICT관련 활동에 적용된다고 명시하고 있다.[24]

UN GGE 보고서는 대내적 주권과 대외적 주권의 문제와 연계해서도 다른 국가의 주권을 고려하여 자국의 영토에서 초래되는 악의적인 ICT활동을 완화하는 합당한 요청에 응해야 한다고 강조하고 있다. 이른 국제평화와 안보를 위협할 가능성이 있는 행위를 다룰 때 중요하다고 강조한다.[25]

사이버공간은 기본적으로 국가주권이 인정된다는 전제를 부정하지 않고 있다. 사이버공간에서 유해한 행위는 다른 국가의 주권, 영토 불가침, 정치적 독립을 침해하는 것으로 간주될 수 있음을 유엔 보고서, 미국, 러시아, 중국의 보고서에서 모두 일치하는 내용이다. 사이버공간에 관한 국가의 정책은 개별 국가의 독자성을 인정하고, 자국의 영토상 사법권과 국가 통제는 인정하고 있다. 이는 영토적인 위치, 정보통신기술의 시설 혹은 국가기간시설에 대해 주권적 권한을 확인한 것이다.

미국의 입장은 국가주권의 기본 원칙을 인정하지만, 사이버공간에서 국가의 책임을 강조하고 있다. 미국은 국가주권의 제약 요소가 되는 인권 혹은 인도주의적 국제 규칙이나 협정에 각 국가가 부합하도록 노력해야 한다는 주장을 강조하고 있다. 하지만 중국은 인터넷 활용과 정책에서 주권을 강조하고 외부의 내정 간섭을 차단하려는 의지를 강력하게 보이다. 중국은 사이버 주권이 명백히 존재하며, 중국은 유엔헌장에서 제정한 주권평등 원칙을 인터넷 공간에 적용해야 한다고 주장한다.[26]

3. 비구속적 규범 제안 및 이행

제4차 GGE 보고서에서 자발적 규범은 상대적으로 발전적 내용이 다수 추가되어 일반적 협력의무, 상당주의의무, 기반시설보호, 침해사고 대응시 긴장 고조 방지, 디지털 프라이버시와 인권 증지, 공급망 보안 등의 11개의 규범이 규정되었다(para. 13). 이들 중 일부는 국제법적 지위

22) Madhuvanthi Palaniappan. "Cyber Sovereignty: In Search of Definitions, Exploring Implications," ORF ISSUE BRIEFS AND SPECIAL REPORTS. 2022.12.28. https://www.orfonline.org/research/cyber-sovereignty/ (검색일: 2023/05.21)

23) INDO-PACIFIC DEFENSE FORUM STAFF, "Cyberspace Freedom, Allied and Partner Nations Resist Authoritarian Controls Imposed Under the Guise of Digital Sovereignty," 2023.04.12. https://dialogo-americas.com/articles/cyberspace-freedom-allied-and-partner-nations-resist-authoritarian-controls-imposed-under-the-guise-of-digital-sovereignty/

24) UN General Assembly. "Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security," 2021.7.14. p.17.

25) UN General Assembly. "Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security," 2021.7.14. pp.13-14

26) http://www.scio.gov.cn/zfbps/32832/Document/1732898/1732898.htm

또는 내용의 명확성에 대한 합의가 도출되지 못한 부분을 반영한다.

〈표 1〉 2015 GGE 보고서 자발적 규범 주요 내용

	주요 내용
13. a	국제 정보안보를 위한 조치 개발, 적용을 위해 협력할 것
13. b	CT 침해사고시 관련 정보와 환경에 대한 종합적 고려를 거친 대응 요구
13. c	영토의 국제위법행위 사용 허용 금지
13. d	정보교환, 사법공조 등 협력조치 이행을 위한 방법을 개발할 것
13. e	정보인권 관련 총회 및 인권이사회 결의 준수를 강조
13. f	국제적 의무에 반한 주요기반시설 위해 행위의 수행 또는 지원 금지
13. g	자국 주요정보통신기반시설 보호를 위한 조치를 취할 것
13. h	타국 주요기반시설 침해시 피해국의 공조요청 대응
13. i	CT 제품 공급망 보안과 악성도구, 기능 확산 방지 위한 노력
13. j	기반시설 보안을 위한 ICT 취약성의 보고 및 해결책 국가간 공유
13. k	타국의 CERT 위해 금지 및 CERT를 활용한 위해행위 금지

※ 김소정 · 김규동, 2017. “UN 사이버안보 정부전문가그룹 논의의 국가안보 정책상 함의”, 『정치 · 정보연구』 제20권 제2호, p. 102

미국은 사이버공간에서 국가행동을 규율하고 위협을 다루는 새로운 국제법문서(international legal instrument)는 필요하지 않다고 강조하였다. OEWG가 새로운 법적 구속력 있는 규칙을 발전시키는데 중점을 두는 제안을 하기로 한 부분에 관하여, 미국은 장기적인 시간을 필요로 하는 법적 협상은 악의적 사이버활동에 의해 나타나는 새로운 위협에 대응하기에 올바른 방법이 아니라고 언급하였다. 그보다 비구속적 규범에 대한 기존의 정치적인 약속이 이행되는 것이 바람직하며, OEWG는 모든 회원국들에게 이들 규범에 대해 인식을 제고시켜야 하고, 역량있는 국가들은 이들 규범의 준수와 광범위한 국제 사이버안정 프레임워크를 위해 노력해야 한다고 강조하였다.

EU는 2016년 채택된 EU NIS 지침을 통한 규범과 원칙의 이행 경험을 공유하였다. 이 EU의 사이버안보 입법은 국가 역량과 국가간 협력 증진, EU 전역의 중요 분야에 대한 감독을 증대시킨다. 동 입법은 합의한 규범을 어떻게 이행할 것인지, 그리고 회원국간 신뢰구축을 어떻게 이행할 것인지에 대한 구체적인 사례가 되며, 지역체제 차원에서 악의적 사이버활동 문제를 다루는 시도라고 하였다.

중국은 국가들이 정보통신기술과 ICT 네트워크를 국제평화와 안보 유지에 반하는 활동을 수행할 목적으로 이용하지 않겠다고 선언해야 한다고 하였다. 중국은 모든 국가가 국제 인터넷 자원의 관리와 유통에 동등하게 참여할 권리가 있다고 보며, 핵심 기반시설에 관하여 국가는 다른 국가의 핵심 기반시설을 훼손해서는 안된다고 언급하였다. 중국은 OEWG가 국가의 ICT 기반시설 보호에 대한 권리와 책임을 논의해야 하며, 개인정보 및 국가안보, 공중 및 경제안보에 관한 데이터 안전을 보장하는 권리와 책임을 다루어야 한다고 권고하였다. 사물인터넷, 인공지능, 빅데이터, 클라우드 컴퓨팅, 블록체인에 관하여 아직 발전 중인 규칙, 규범 및 원칙은, 이들 기술의 위험을 최소화하면서도 기술이 경제 발전에 주는 혜택을 얻을 수 있는 방식으로 탐색되어야 한다고 강조하였다.

중국은 또한 5G 이슈에 대해서도 언급하며, 2015년 UNGGE 보고서 9항이 공급망의 안전에 대해 언급한 것을 상기하였다. 특히 5G 공급망 안전에 대한 규범을 지지하는 국가들이 중국 기업을 비윤리적으로 차별하고자 하는 상황에서, 5G 공급망 안전을 별도의 규범으로 다루는 것이 적절한지 의문을 제기하고, 중국은 다음과 같은 규범을 고려해야 한다고 하였다. 첫째, 국가들은 자국의 우월적 지위를 다른 국가의 ICT 상품과 서비스의 공급망 안전을 훼손하는 데 이용해서는 안된다. 둘째, 국가들은 ICT 상품 및 서비스 제공자가, 불법적으로 이용자의 데이터를 획득하고 이용자의 시스템과 장비를 통제 및 조작하기 위해, 상품과 장비에 백도어를 설치하는 것을 금지해야 한다. 셋째, IT 공급자는 자신의 상품에 의존하는 이용자에 대해 우월적 지위를 이용하거나, 이용자가 시스템 또는 장비를 업그레이드하도록 강제함으로써 부당한 이익을 추구하는 것이 금지되어야 한다. 넷째, 공급자들은 자신의 상품에서 심각한 취약점이 탐지된 경우, 자신의 협업 파트너와 이용자들에게 시의적절하게 통지하도록 노력해야 한다. 다섯째, 국가들은 공정하고 비차별적인 시장 환경을 유지하기 위해 노력해야 한다. 여섯째, 국가들은 국가안보를, 정상적인 ICT 발전과 협력을 제한하거나, ICT 상품에 대한 시장접근과 하이테크 상품 수출을 제한하는 구실로 이용해서는 안 된다.

V. 평가 및 전망

국제연합에서의 사이버안보 규범 형성 논의는 약 20여년간 답보상태를 밟고 있으나, 그럼에도 불구하고 해당 플랫폼을 배제한 사이버안보 규범 논의가 이루어지지도 않고 있다. GGE는 사이버공간에 대한 국제법 적용에 관한 합의를 이루고 컨센서스에 의한 보고서를 여러 차례 채택하였다는 점에서 그 자체로 어느정도 성공적이라 평가할 수 있다. 다만 종래부터 논란이 되어왔던 사이버공간에서의 국제위법행위에 대한 대응조치의 적용을 명시적으로 언급하지 못하였고, 주권과 상당주의에 대한 국제법적 지위에 관하여 합의하기 어려웠다는 한계가 있다. 그럼에도 6차 GGE에서는 자발적 규범에 대해 발전적 논의를 하였고, 사이버공간에서 책임있는 국가 행동에 대한 규범들이 향후 국제관습법으로 발전될 수 있는 가능성을 열어놓았다는 점에서 그 의미가 있다.

한편, UN 전 회원국이 참여하는 개방형 워킹그룹(OEWG)에서도 결과보고서(A/AC.290/2021/CRP.2)를 통해, 사이버공간의 위협 인식, 국가행동에 대한 규범, 국제법 적용, 신뢰구축, 역량강화, 정례적·제도적 협의체 등 의제에 대한 유엔 전체 회원국들의 현재 인식을 확인하였다. GGE와 OEWG 모두 추후에도 활동을 지속할 것을 결의하였으나, GGE에서 드러난 바와 같이 진영 간의 근본적 시각차는 여전히 지속되고 있다. 자위권 행상의 수단과 범위, 사이버공간에서 주권의 범위, 민간분야의 정보통신기술 기반시설에 대한 공격 허용 여부, 비국가 행위자 혹은 대리행위자들의 사이버활동에 대해 국가 책임의 범위 등은 향후 지속적인 논의를 통해 구체화 될 필요가 있다.

OEWG는 제한된 회원국만이 참여하는 GGE 논의 구조에 대한 비판적인 관점에서 출범했으나, OEWG가 갖는 구조적인 한계도 인식할 필요가 있다. UN 전 회원국과 비정부기구, 다중 이해관계자에게까지 참여가 확대된 플랫품은, 기존 논의 결과를 단순 취합하는 연례보고서 채택에도 상당한 이견이 제시되어 의견 수렴을 어렵게 하고 있으며, 특히 견해가 첨예하게 대립하는 분야에서는 유의미한 결과를 도출하기 어려울 것으로 예상된다.

다만, 국가들이 다양한 의견을 제시할 수 있고, 국제법의 적용에 관한 국가들의 입장보고서 제출을 독려하는 등, 공개된 포럼이면서도 앞으로 다른 전문 분야별 포럼을 구성하여 진행될 수 있는 가능성이 열려 있다는 점에서, 우리나라의 준비가 필요하다. 특히 구체적인 규범이나 국제법 분야의 논의는, 국가들이 실행을 통하여 자국의 규범을 형성해 나가는 과정에 있으므로, 우리나라도 주요 원칙들에 대해 입장을 정립하고, 향후 규범 형성 논의에 기여할 수 있도록 대비해야 할 것이다.

미중간 경쟁의 심화, 한미일 동맹 강화에 따른 북중러 협력 강화로 진영 구분이 두드러지면서 앞으로의 규범 형성도 쉽게 성과를 낼 수 있을 것으로는 판단되지 않는다. 더욱이 러시아-우크라이나 전쟁에서 사이버 공격을 물리전을 지원하는 보조적 수단으로 활용했고, 이에 대응하기 위해 미국이 전진 방어(Defend Forward) 전략을 시행했다는 점에 있어, 미국의 직접적 개입과 동맹국들의 직간접적 지원이 더욱 증가할 것으로 보여진다. 이는 보편적으로 적용가능한 규범이 아직 형성되지 않은 시점에서, 특정 국가의 행위에 기반한 관습이 규범으로 굳어질 가능성이 높아진 것이다.

2022년 한미정상회의 이후 우리나라는 미국과의 동맹을 강화하면서, 사이버공간에서의 협력도 강화하고 있다. 이는 2023년 한미정상회의시 체결된 “전략적 사이버안보 협력 프레임워크”로 증명되고 있으며, 2023년 8월 개최된 한미일 정상회의를 계기로 일본을 포함한 협력 확대를 천명하고 있다. 이는 미국이 주도하는 가치기반의 동맹간 협력강화를 통해 적대 세력에 대응하고 기술적, 전략적 우위를 지속 과정에 주요 구성원으로 참여함을 의미한다. 이는 랜섬웨어 대응 이니셔티브 등에서와 같이 미국 주도의 소다자 협의에 무게가 실리고 있다는 점에서도 알 수 있다.

우리나라는 아직 사이버안보 규범 경쟁속에서 적극적인 목소리를 내오지는 않았으나, 한미정상회의 이후 미국이 지지하는 “인터넷 미래를 위한 선언”에 동참하기로 하는 등 조금씩 진영을 분명히 해 가고 있다. 이 과정에서 모든 규범 논의 과정에 동일한 지분으로 참여하기 보다는 우리의 국익에 직접적 연관이 있는 대북 대응 등에 집중함으로써 실리와 명분을 같이 찾을 수 있는 길을 모색해야 할 것이다. 또한, 동맹국으로써 향후 요구받을 수 있는 역할과 기대에 대해 충분한 고려가 필요할 것이다.

앞으로 우리나라가 사이버안보 관련 규범 논의, 사이버안보 강화를 위한 정책 및 기술협력시 고려해야 할 사항을 다음과 같이 제안한 바 있다. OEWG의 활성화 및 구체적 협력 아이템 도출에는 구조적인 한계가 존재한다는 점을 인지하고 그에 맞는 대응을 취해야 한다. 둘째, 국제안보 차원의 규범 논의 대응 과정에서 사이버공간과 관련한 다양한 이슈 대응력을 향상시키기 위한 관련부처의 인력지원 및 역량 강화가 절실하다. 셋째, 앞으로 구체적 · 실무적 사이버안보 정책 및 제도개선 논의, 협력 구체화는 양자 및 소다자 회의체를 통해 논의될 가능성이 높을 것으로 예상되므로, 개별부처의 단독 행동보다는 유관부처간 충분한 정보공유와 공통된 상황인식을 바탕으로 올바른 정책 방향을 결정하고 추진이 필요하다(김소정, 2022e).

〈참고문헌〉

국가보안기술연구소 옮김, 사이버 전쟁에 적용 가능한 국제법 : 탈린매뉴얼, 글과 생각, 2014

김소정. 2013. “사이버안보 국제협력과 국가전략”, 제주평화연구원,『JPI PeaceNet』2013-08, 2013. 7.

김소정·박상돈. 2013. “국제협력을 통한 사이버안보 강화방안 연구”,『융합보안논문지』제13권 제6호, 2013. 12.

김소정 · 김규동, 2017. “UN 사이버안보 정부전문가그룹 논의의 국가안보 정책상 함의”,『정치 · 정보연구』제20권 제2호, pp. 87-122.

김소정, 김규동, “사이버공간의 규범 형성을 위한 UN의 노력과 전망”, 서울대 국제문제연구소 워킹페이퍼 No.96, 2018.11.8.

김소정, “2022 한미정상회담과 사이버안보-억지력 강화를 위한 전략적 과제” 국가안보전략연구원 이슈브리프 361호, 2022

김소정 외. (2022). 사이버 안보와 개발협력 연계 전략 : 영국과 한국 사례 비교. 국가안보전략연구원『전략보고』

김소정 (2022a), 사이버공간에서의 정보기관의 역할 확대와 시사점, 서울대 국제문제연구소 이슈브리핑 170

김소정 (2022b), 우크라이나에 대한 러시아의 사이버 공격: 특이성과 함의, 제주평화연구원, JPI-PeaceNet

김소정 (2022c), 러시아-우크라이나 전쟁과 사이버안보 전략구상의 함의, 국가안보전략연구원『INSS 이슈브리프』358호

김소정 (2022d), 한미정상회담과 사이버안보 억지력 강화를 위한 전략적 과제, 국가안보전략연구원『INSS 이슈브리프』361호

김소정 (2022e), 유엔 정보안보개방형워킹그룹(OEWG) 회의결과와 한국에의 시사점, 국가안보전략연구원,『INSS 이슈브리프』(2022.08.)

김소정 (2022f), 북한의 가상자산 탈취 대응을 위한 한 · 미 협력 고려사항, 국가안보전략연구원『INSS 이슈브리프』제395호

김소정 (2022g), 미국의 사이버공격 대응정책과 한국에의 시사점 : 솔라윈즈 해킹 대응사례를 중심으로, 국가안보전략연구원,『INSS 연구보고서』2022-04

박노형. 2012. “사이버안전 관련 국제규범의 정립을 위한 연구”,『안암법학』제37호(2012)

박노형·정명현. 2014. “사이버전의 국제법적 분석을 위한 기본개념의 연구”,『국제법학회논총』제59권 제2호(통권 제133호) pp. 65-93.

장노순. 2016. “사이버안보와 국제규범의 발전: 정부전문가그룹(GGE)의 활동을 중심으로,”『정치· 정보연구』제19권 제1호(2016)

장노순 · 김소정, “미국의 사이버전략 선택과 안보전략적 의미: 방어, 억지, 선제공격전략의 사례 비교 연구,”『정치· 정보연구』제19권 3호, 2016.

조동준, “국제규범을 둘러싼 사회세력 간 경쟁”, 규범의 국제정치, 세계정치 33, 사회평론아카데미, 2019

조지프 나이, 권력의 미래, 세종서적, 2012

한인택. 2013. “사이버 시대의 국가 안보”, 제주평화연구원,『JPI PeaceNet』2013-01, 2013. 1.

Finnemore, Marth, “Theory & Precedents for Cyber Norms,” MIT CCN 5.0, 2017.03.07.
Finnemore, Marth and SIKKINK, Kathryn, 1998, “International Norm Dynamics and Political Change,”『International Organization』Vol. 52, No. 4,
Finnemore, Marth and HOLLIS, Duncon B., “Constructing Norms for Global Cybersecurity”, The American Jounal of International Law, Vo. 110, No. 3, July 2016, pp.425-479
Finnemore, Marth, “Cybersecurity and the concept of norms”, Carnegie Endowment for International Peace, Nov. 30, 2017
MAGNUSON, Stew, “JUST IN : AUKUS Agreement Poses Cybersecurity Risk to Allies”, 29 Sept. 2022,
MARKOFF, Michele. 2015. "Advancing Norms of Responsible State Behavior in Cyberspace", DipNote: U.S. Dept. of State Official blog, 9 July 2015
MAURER, Tim. 2011. "Cyber Norm Emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber Security". Belfer Center for Science and International Affairs
NYE, Joseph. 2011. "Nuclear Lessons for Cyber Security?", Strategic Studies Quarterly 5, No. 4(Winter 2011)
NYE, Joseph. 2014. “International Norms in Cyberspace,” http://therisingnepal.org.np/news/3607
RUHL, Christian, et al., “Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads”, Carnegie Endowment for International Peace, Feb. 2020
국가보안기술연구소 정책연구실,『2014-2015 UN 정보안보 GGE 결과자료집』2015.
The White House, FACT SHEET: United States and 60 Global Partners Launch Declaration for the Future of the Internet“, 28 April 2022
The White House, “Fact Sheet: Quad Leaders’ Summit,” September 24, 2021.
The White House, “Quad Joint Leaders’ Statement,” May 24, 2022; The White House, “FACT SHEET: Quad Leaders’ Tokyo Summit 2022,” May 23, 2022.
UN GA, Draft Resolution, Developments in the field of information and telecommunications in the context of international security, 21 October 2015, UN Doc. A/C.1/70/L.45
UN GA, Draft Resolution, Developments in the field of information and telecommunications in themcontext of international security, 18 October 2013, UN Doc. A/C.1/68/L.37
UN GA, Resolution on "Developments in the Field of Information and Telecommunications in the Context of International Security", UN Doc. A/RES/53/70, 4 January 1999
UN GA, Resolution on "Developments in the Field of Information and Telecommunications in the Context of International Security", UN Doc. A/RES/58/31, 8 December 2003

UN GA, Resolution on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/RES/68/243, 9 January 2014

UN GA, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security(2005 Report), UN Doc. A/60/202, 5 August 2005

UN, Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations: International Code of Conduct for Information Security, UN Doc. A/66/359, 14 September 2011

https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/fact-sheet-the-second-international-counter-ransomware-initiative-summit/

https://therecord.media/u-s-convenes-30-countries-on-ransomware-threat-without-russia-or-china

https://www.minister.defence.gov.au/media-releases/2022-02-10/australia-us-and-uk-stand-together-confront-global-ransomware-threat

https://www.voakorea.com/a/world_behind-news_quad-china/6058122.html

http://www.scio.gov.cn/zfbps/32832/Document/1732898/1732898.htm

이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.