creative commons

COMMONS DEED

저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

법학석사 학위논문

사이버 공간에서 상당주의 의무 (due diligence)의 적용 가능성

2023 년 8 월

서울대학교 대학원

법학과 국제법전공

김소희

사이버 공간에서 상당주의 의무 (due diligence)의 적용 가능성

지도 교수 이 재 민

이 논문을 법학석사 학위논문으로 제출함

2023 년 5 월

서울대학교 대학원

법학석사

김소희

김소희의 법학석사 학위논문을 인준함

2023 년 7 월

위 원 장 _____ (인)

부위원장 _____ (인)

위 원 _____ (인)

국문초록

본 연구는 국제법상 '상당주의 의무'(due diligence)의 사이버 공간에서의 적용 가능성과 적용 상의 법적 쟁점을 검토함으로써 사이버 공간에서 동 의무가 보다 효율적으로 기능하기 위한 방안을 모색하는 것을 일차적 목적으로 한다.

오늘날 사이버 공간을 매개로 발생하는 사이버 공격은 고도의 '익명성'(anonymity)과 '비대칭성'(asymmetry)을 그 특징으로 하며, 공격 수행 과정에서 '비국가행위자'(Non-state actor)와 '국가'(State)가 다양한 방식으로 연계된다. 사이버 공격의 이러한 특성이 국제사회에 야기하는 문제점은 다음의 두가지로 요약된다. 첫째, 사이버 공격의 기술적 특성으로 인해 공격의 직접적인 배후국에 대한 책임 귀속(attribution)이 어려우며, 그 결과, 국가책임법의 적용이 용이하지 않다. 둘째, 복잡다단한 방식으로 이루어지는 사이버 공격의 특성 상 공격과 연관된 제3국인 '경유국'(transit state)의 역할이 점차적으로 확대되고 있으나, 경유국의 행위를 규율하기 위한 국제법적 규범은 미비하다. 본 연구는 사이버 공격으로부터 파생되는 이러한 문제점에 대한 대안으로 국제법상의 상당주의 의무를 사이버 공간에도 적용할 것을 제안한다. 상당주의 의무는 자국의 관할권 내에서 초국경적 피해를 예방할 것을 요구하는 규범인 바, 사이버 공격으로 인해 발생하는 문제 해결의 실마리가 될 수 있을 것이다.

본 연구는 다양한 국제법의 영역에서 원용되는 규범인 상당주의 의무를 전반적으로 개관한 뒤, 동 의무의 사이버 공간에서의 적용 가능성과 적용상의 법적 쟁점, 한계 및 함의에 대하여 검토한다. 사이버 공간에 상당주의 의무를 적용하는 것에 대한 국제사회의 긍정적 인식과는 별개로, 동 의무가 사이버 공간에 적용되어 효율적으로 기능하기 위해서는 추가적인 논의를 필요로 하는 법적 쟁점이 여전히 존재한다. 상당주의 의무의 규범적 가치 확보에

관한 논의, 상당주의 의무의 구체적 적용 기준에 대한 합의, 그리고 상당주의 의무의 집행력 확보 수단에 관한 논의를 통해 동 의무가 사이버 공간에서 보다 효율적으로 기능할 수 있을 것으로 판단된다. 본 연구는 상당주의 의무가 갖는 본질적인 딜레마와 기술적 난점 등 일부 한계를 갖는다. 그러나, 사이버 공간에서 상당주의 의무의 역할에 대해 검토한 본 연구는 사이버 공격을 활용한 위협이 증대되는 상황에서 분단국인 우리나라의 사이버 안보의 측면에 큰 함의를 갖는다. 또한 본 연구는 새롭게 대두되는 영역인 사이버 공간을 적절하게 규율하고, 또한 사이버 공격에 효율적으로 대처하기 위하여 노력하는 국제사회의 전반적인 논의의 흐름과 맞닿아 있으므로 논의의 실익이 있다.

주요어 : 사이버 공격, 사이버 안보, 상당주의 의무, 비대칭성, 익명성, 경유국, 관할권, 비국가행위자

학번 : 2021-25948

목 차

제 1 장 서 론 **1**

제 1 절 연구의 필요성 1

제 2 절 연구의 목적과 범위 6

제 2 장 사이버 공간과 국제법 **10**

제 1 절 사이버 공간에 관한 이론적 논의 10

I. 용어의 정리 10

1. 사이버 공간 10

2. 사이버 조작 11

3. 사이버 공격 12

II. 사이버 공간 및 사이버 공격의 특수성 14

1. 이중적 특성 14

2. 공격양태로 인한 귀속의 어려움 15

3. 비국가행위자의 영향력 증대 16

4. 소결 18

제 2 절 사이버 공간에서의 국제법 적용과 관련된 논의 19

I. 사이버 공간의 '행위규율'에 관한 논의의 쟁점 19

1. 사이버 안보에 대한 관점: 서방진영 21

2. 사이버 안보에 대한 관점: 비서방진영 23

3. 제3차 UNGGE의 논의 25

II. 사이버 공간에 적용될 국제법의 논의 과정 26

1. 탈린매뉴얼 27

2. UN정부전문가그룹 29

III. 소결 34

제 3 절 사이버 공간과 국가책임법 적용의 한계 35

I. 국가책임법 36

1. 정의 및 의의 36

2. 국가책임법 성립요건 37

3. 비국가행위자의 행위 39

II. 사이버 공간에서 국가책임법 적용과 그 한계 41

1. 사이버 공격의 특성 41

2. 귀속의 어려움 43

3. 소결 45

제 3 장 일반 국제법과 상당주의 의무 47

제 1 절 주권(sovereignty)과 상당주의 의무 47

제 2 절 상당주의 의무의 개념 및 발전 과정 48

I. 상당주의 의무의 개념 48

1. Corfu Channel Case 49

2. Island of Palmas case 50

II. 상당주의 의무의 발전 과정 51

1. Alabama Arbitration case 51

2. ILC 국가책임법 초안 편찬과 상당주의 의무 52

III. 국제환경법 영역에서의 상당주의 의무 54

1. Trail smelter case 58

2. Pulp Mills case 58

IV. 소결 60

제 3 절 상당주의 의무의 주요 내용 및 적용상의 쟁점 60

I. 타국의 권리에 반하는 행위 62
II. 장소적 범위 63
III. 인식의 여부 64

제 4 장 사이버 공간에서의 상당주의 의무 66

제 1 절 사이버 공간에서의 상당주의 의무 적용 필요성.....66
I. 사이버 공간에서 상당주의 의무에 대한 국제사회의 관심.....66
II. 사이버 공간에서 상당주의 의무의 도입 필요성 69
1. 국가책임법 적용의 한계에 대한 대안.....70
2. 사이버 공간의 평화적 활용을 도모하기 위한 수단.....71

제 2 절 사이버 공간과 상당주의 의무의 적용 가능성 73
I. 국제법협회 (ILA) 보고서.....73
II. TM 그룹 (탈린매뉴얼).....75
III. UN 정부전문가그룹.....77
IV. 소결.....78

제 3 절 사이버 공간에서의 상당주의 의무 적용상의 쟁점.....80
I. 영토의 범위 81
II. 타국의 권리에 반하는 행위 및 심각한 부정적인 결과를 초래하는 행위 85
III. 인식의 기준 87

제 4 절 사이버 공간에서 상당주의 의무의 규범적 지위 89
I. UN 정부전문가그룹에서의 논의.....91
II. 사이버 공간의 특수성과 상당주의 의무의 신축성 94

제 5 장 사이버 공간에서 상당주의 의무의 활성화를 위한 국제법적 쟁점과 한계 97

제 1 절 상당주의 의무의 활성화를 위한 법적 쟁점 검토..... 97

I. 국제법적 구속력 부재에 따른 규범적 가치 확보.....98

1. 국제법적 구속력 부재에 따른 한계와 규범적 가치 탐구 필요성 98

2. 상당주의 의무의 규범적 가치 검토 – 비구속적 규범.....99

1) 연성법의 가치 및 역할 검토 100

2) 상당주의 의무의 연성법으로서의 역할 검토.....102

3. 상당주의 의무의 규범적 가치 검토 – 국제관습법 105

1) 논의의 필요성 105

2) 상당주의 의무의 지위 변화 가능성 검토.....105

II. 구체적 적용 기준 설정의 필요성.....110

1. 상당주의 의무의 신축적 특성과 한계.....110

2. 상당주의 의무의 '구체적 적용 기준' 설정의 필요성.....112

3. 상당주의 의무의 '구체적 적용 기준' 검토를 위한 과제 114

III. 상당주의 의무의 집행력 확보 – 이행확보수단 구축 117

1. 다자간환경협정에서 비준수절차의 의의.....118

2. 비준수절차를 통한 사이버 공간에서의 상당주의 의무의 집행력 제고 120

제 2 절 연구의 한계와 함의 123

I. 본 연구의 한계.....123

1. 상당주의 의무의 본질적인 딜레마 123

2. 기술적 한계 126

II. 본 연구의 함의.....129

1. 우리나라의 사이버 안보에 갖는 함의.....129

2. 국제사회의 안보 전반에 갖는 함의.....132

제 6 장 결 론 134

참고문헌 139

제 1 장. 서론

제 1 절. 연구의 필요성

'사이버 공간'(cyber space)은 인류에게 다양한 도전의 기회를 제공하였으며 인류가 누릴 수 있는 혜택의 범위 역시 급격하게 확장하였다. 그러나 사이버 공간은 이러한 이점과 함께 다양한 형태의 '사이버 위협'(cyber threat)을 통해 인류의 삶에 부정적인 영향을 미치기도 한다. 사이버 공간을 매개로 발생하는 불법적인 '사이버 조작'(cyber operation) 혹은 '사이버 공격'(cyber-attack)은 사이버 공간이 인류의 삶을 위협하는 방식으로 활용될 수 있음을 보여주는 대표적인 사례이다. 재래식 공격에 필적할 만큼은 아니지만 사이버 기반시설을 활용한 불법적인 사이버 조작의 빈도는 급격하게 증가하고 있으며 피해의 종류와 규모 역시 점차 다양화 되는 추세이다. 재래식 공격과 대비되는 사이버 공격의 가장 큰 특성은 '익명성'(anonymity)과 '비대칭성'(asymmetry)이며 이러한 공격의 특성으로부터 오늘날 국제사회에 야기되는 문제점은 크게 두가지로 요약된다. 첫째, 사이버 공격은 그 특성상 공격에 대한 책임 귀속(attribution)이 매우 어려운 바, 피해국이 공격에 직접적인 책임이 있는 국가를 상대로 국제법상의 국가책임을 추궁하는 것에는 상당한 현실적·기술적 어려움이 따른다. 둘째, 일련의 공격 과정이 비교적 가시적이고 직선적인 재래식 공격과는 달리, 사이버 공격은 제3국에 위치한 공격 거점을 경유하는 복잡한 방식으로 시행되는 경우가 대다수이다. 그 결과, 사이버 공격의 수행 과정에서 제3국의 역할이 점차적으로 확대되고 있지만 이들의 행위를 규율할 수 있는 별도의 국제법 규범은 미비하다. 본 연구는 익명성과 비대칭성에 기반한 사이버 공격이 국제사회의 안보에 미치는 부정적 영향력에 대한 대안으로 전통적인 국제법 영역에서 활용되어 온 규범인 '상당주의 의무'(due diligence)를 사이버 공간에도 적용할 것을 제안하고자 한다. 국제법상 '상당주의 의무'는 자국의 관할권 내에서 초국경적 피해를 예방

하고 방지할 것을 요구하는 국제법상 규범으로, 공격과 관련한 제3국의 역할이 증대되는 사이버 공간에서 피해국의 유효한 권리 구제와 사이버 공간의 평화적 활용을 위한 효과적인 역할을 수행할 수 있을 것으로 기대된다.

2007년 에스토니아의 국가 전산 시스템 전반을 마비시켰던 대규모의 '분산서비스 공격'(Distributed Denial of Service: DDoS, 이하 DDoS 공격)을 통해 사이버 공격이 가지는 특성과 함께 사이버 공격의 대응 방안으로 국제법상 상당주의 의무를 도입하여야 할 필요성을 확인할 수 있다. 당해 공격의 결과 에스토니아의 정부와 의회를 비롯한 각 부처의 웹사이트, 주요 은행 그리고 핵심 언론사 등 국가의 전반적인 전산 시스템이 약 3주 가량 마비되었으며 에스토니아는 극심한 사회적 혼란과 경제적 손실 등을 부담하였다.[1] 2007년 에스토니아를 상대로 이루어진 전방위적인 DDoS 공격은 사이버 공격으로는 전례 없는 피해의 규모와 기간의 측면 만큼이나, 공격의 가장 확실한 배후국으로 지목되는 러시아 정부가 사태의 대한 어떠한 책임도 부담하지 않았다는 측면에서 국제사회의 이목을 끌었다. 당해 공격의 배후에 러시아 정부가 있었다는 증거로는, 공격에 동원된 100만 대의 PC 중 상당 수의 PC가 러시아의 관할권 내에 소재하였다는 점과 함께 공격에 사용된 대표적인 PC의 IP주소 일부가 러시아 정부 기관의 IP주소와 동일하다는 사실 등이 지목되었다.[2] 더불어 에스토니아의 전산망에 가해진 사이버 공격의 정교함과 광범위한 규모 역시 러시아의 개입을 의심케 하는 요소였다.[3] 그러나 러시아는 위 사태에 대한 자국 정부의 관련성을 강력하게 부인하였으며 이는 단순히 애국 해커 집단의 독단적인 행동에 따른 결과라는 점을 강조하였다.[4] 당해 공

---

[1] James Pamment et al., "Hybrid Threats: 2007 cyber-attacks on Estonia", NATO Strategic Communications Centre of Excellence (2019), p.52.

[2] Ibid; Macro Roscini, Cyber Operation and the Use of Force in International Law, (UK: Oxford University Press, 2014), p.5.

[3] Jeffrey T. G. Kelsey, "Hacking into International Humanitarian Law: The Principle of Distinction and Neutrality in the Age of Cyber Warfare", The Michigan Law Review, Vol. 106, No. 7 (2008), p.1429.

[4] James Pamment et al., supra note 1, p.52; Gadi Evron, "Battling Botnets and Online Mobs – Estonia's Defense Efforts during the Internet War", Georgetown Journal of International Affairs (2018), p.124; Stephen Herzog, "Revisiting the

격의 배후에 러시아 정부가 있었다는 정황 증거가 존재하였음에도 불구하고 에스토니아는 러시아 정부가 공격에 대해 구체적인 지시 및 통제를 하였는지에 대한 충분한 수준의 입증을 하지 못하였으며, 결과적으로 러시아 정부에 대한 별도의 국가책임을 역시 추궁할 수 없었다. 즉, 사이버 공격으로 인해 국가 기반 시설의 전반이 3주 가량 마비되는 막대한 피해를 입었음에도 불구하고 에스토니아는 자국이 입은 피해를 전혀 구제받지 못하였고, 유책국에 대한 어떠한 책임도 추궁할 수 없었던 것이다. 본 사태 이후 피해국인 에스토니아는 사이버 공간에서 '상당주의 의무'가 적용되어야 할 필요성에 대해 강력하게 주장한 바 있다.[5] '상당한 주의'(due diligence)는 자국의 영토가 타국의 권리에 악영향을 미치는 방법으로 사용되지 않도록 노력하여야 할 의무를 의미하는 것으로, 에스토니아는 특히나 동 의무가 국가책임법이 유의미한 역할을 할 수 없는 상황에서 피해국이 기댈 수 있는 유일한 구제 수단이 될 수 있다는 점을 피력하였다.[6]

사이버 공격에 대한 책임을 특정 '국가'에 귀속시키기 위해서는 일차적으로 공격을 자행한 사인 혹은 단체를 특정한 뒤, 어떠한 배후국이 당해 공격을 지시, 지휘 혹은 직접적으로 통제하였는지에 대하여 추가적으로 입증할 것이 요구된다.[7] 이때 입증의 정도는 '명확하고 설득력 있는 수준'(clear and convincing evidence)의 증거 기준을 충족해야 한다.[8] 그러나 2007년 에스토니아 사태에서도 확인할 수 있는 것처럼 사이버 공격은 비대칭성과 익명성

Estonian Cyber Attack: Digital Threats and Multinational Responses", Journal of Strategic Security, Vol 4, No. 2 (2011), p.53.

[5] UNGA, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, UN Doc. A/76/136 (2021), p.26/142. (이하 UNGA 컨펜디엄)

[6] UNGA 컨펜디엄 UNGA, p.26/142.

[7] 박노형·김효권, "국제사이버법상 상당한 주의 의무에 관한 국가실행", 『국제법학회논총』, 제66권 제4호 (2021), pp.74-75.

[8] Macro Roscini, supra note 2, pp.101-102.

을 가장 큰 특징으로 하는 바, 책임의 귀속(attribution)과 국가책임의 추궁 과정에 상당한 기술적·현실적 어려움이 뒤따른다.[9] 사이버 공격 결과에 대한 국가책임 추궁을 위한 일련의 입증 과정이 상당히 복잡한 것과는 달리, 상당주의 의무의 위반에 대한 증명은 피해국의 입증 부담을 한층 완화시켜 준다. 앞선 에스토니아 사태에 상당주의 의무를 적용한다면, 우선 에스토니아는 일정한 수준의 DDoS 공격이 러시아 영토로부터 개시되었다는 점을 '기술적'으로 입증할 수 있으며, 나아가 이러한 기술적 입증을 근거로 러시아가 '자국의 관할 내에 존재하는 서버가 타국에 위해를 가하는 방식으로 사용되는 것을 허용하지 않도록 가능한 모든 조치를 다하여야 할 의무'인 '상당한 주의'를 다하지 못하였다는 사실을 보다 수월하게 주장할 수 있다.[10] 그리고 바로 이 지점에서, 본 연구에서 다루고자 하는 사이버 공간에서 상당주의 의무가 적용되어야 할 일차적 필요성을 찾을 수 있을 것으로 판단된다.

다른 한편, 사이버 공간에서의 상당주의 의무에 관한 논의의 또 다른 필요성은 오늘날 사이버 공격 과정에서 제3국의 역할이 점차적으로 확대되는 현실로부터 찾을 수 있다. 사이버 공간을 매개로 발생하는 사이버 공격은 공격의 익명성과 비대칭성을 매우 주요한 특성으로 삼는 바,[11] 상당수의 사이버 공격은 공격자의 컴퓨터에서 공격 목표 지점으로 직접적이고 단순한 방법으로 시행되는 것이 아닌 제3의 '공격 거점'을 별도로 둔다.[12] 이처럼 공격자가 제3국의 공격 거점을 경유하는 방법으로 사이버 공격을 행하는 이유는 공격이 포착되더라도 역추적을 방지하거나 혹은 교란하기 위함이다. 이들은 제3

---

[9] Russell Buchan & Nicholas Tsagourias, "Special Issue: Non-State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence", Journal of Conflict & Security Law, Vol. 21, No. 3 (2016), p.378.

[10] James Pamment et al., supra note 1, p.57.

[11] 박기갑, "사이버 전쟁 내지 사이버 공격과 국제법" 『국제법평론』, 통권 제32호 (2010), p.70; 박노형, "사이버안전 관련 국제규범의 정립을 위한 연구", 『안암법학』, 제37호 (2012), p.799.

[12] Russell Buchan, Macro Roscini & Nicholas Tsagourias, "State Responsibility for Cyber Operations: International Law Issue", British Institute of International and Comparative Law (2014), p.2.

국에 위치한 서버를 우회하거나 봇넷(Botnet)과 C&C서버를 활용함으로써 사이버 공격의 진원지 파악을 더욱 어렵게 만든다.[13] 결국, 공격을 당하였다는 사실을 인식한 피해국이 공격의 진원지를 찾기 위하여 역추적을 실시하더라도 이는 결과적으로 제3국에 존재하는 공격의 거점을 찾아내는 것일 뿐, 실질적인 공격의 진원지 혹은 배후국 등을 찾게 될 가능성은 매우 희박하다. 이처럼 사이버 공격 과정에서 제3의 공격거점을 경유함으로써 얻을 수 있는 이점은 명백하다고 할 수 있으며, 그 결과 오늘날 사이버 공간에서 공격의 '경유국'이 차지하는 역할이 점차적으로 확대되는 추세이다. 불법적인 사이버 조작과 관련하여 제3국의 역할이 점차적으로 확대되는 현실을 고려하였을 때, 이들 제3국으로 하여금 사이버 공격으로 인한 초국경적 피해를 방지하거나 혹은 최소화 하도록 유도하는 일련의 의무를 부과할 수 있다면, 이는 사이버 안보를 강화하고 사이버 공간의 평화적 활용을 도모함에 있어서 매우 유의미한 방안이 될 것으로 사료된다. 그리고 바로 이 지점에서 상당주의 의무가 사이버 공간에 적용되어야 할 또 다른 필요성을 찾을 수 있는 것이다.

정보통신기술의 발달이 정보통신기술(ICTs)의 발전이 가속화 되고 그로부터 누릴 수 있는 인류의 혜택이 확대됨에 따라 사이버 공간을 악용하고자 하는 사례가 급증하고 있다. 특히, 국가를 상대로 한 강도 높은 사이버 공격이 만연한 오늘날, 이러한 불법적 사이버 조작에 대응해 국가는 국제법상 어떠한 권리를 행사할 수 있으며 또한 어떠한 국가에게 사이버 공격을 예방하고 방지할 의무를 부과할 수 있는지에 관한 논의는 필연적으로 이루어져야 한다. 사이버 공격의 과정에서 제3국의 역할이 점차적으로 확대되고 있으며 더불어 공격의 결과에 대한 국가책임법의 적용이 어렵다는 점을 종합적으로 고려한다면 공격과 관련한 제3국이 부담하는 '상당주의 의무'에 주목할 필요가 있다. 즉, 사이버 공간에서의 상당주의 의무는 공격 피해국의 권리를 구제하고, 더 나아가 사이버 공간의 평화로운 활용을 도모하기 위한 현실적 방안이 될 수 있으므로 그 논의의 실익이 크다고 할 것이다.

---

[13] 박노형·김효권, supra note 7, p.74; 백상미, "사이버공격 억지를 위한 적극적 방어개념의 국제법적 적법성", 『국제법학회논총』 제63권 제2호 (2017), p.84.

제 2 절. 연구의 목적과 범위

본 연구는 전통적인 국제법상 상당주의 의무의 사이버 공간에서의 적용 가능성과 동 의무 적용 상의 국제법적 쟁점에 대하여 검토하는 것을 일차적인 목적으로 한다. 국제법상 상당주의 의무는 다수의 국제재판소 판례를 통해 발전되어 왔다. 그 중 ICJ의 Corfu Channel 사건에 명시된 '모든 국가는 자국의 영토가 타국의 권리에 반하는 행위에 사용된다는 것을 인식하고도, 이를 허용해서는 안된다'라는 판시 내용은 상당주의 의무에 관한 '당대의 정의'(contemporary definition)로 인정받고 있다.[14] 이후 상당주의 의무는 초국경적 환경피해를 규율하는 국제환경법의 영역에서 가장 깊이 있게 다루어졌으나, 오늘날 동 의무는 사이버 공간을 규율하는 규범으로서 새롭게 주목받고 있다. 사이버 공간에서 상당주의 의무는 일반적으로 '정보통신기술(ICTs)을 활용한 사이버 위법행위에 자국의 영토가 활용된 것을 알게 된 이상 이를 허용하지 말아야 할 영토국의 의무'를 의미한다.[15] 본 연구는 상당주의 의무의 사이버 맥락에서의 적용 가능성과, 실질적 적용 과정에서 추가적인 논의를 필요로 하는 구체적 법적 쟁점을 검토하는 것에서 더 나아가, 동 의무의 한계와 본 연구의 함의에 대해서도 분석하고자 한다. 이러한 논의를 통해 본 연구는 사이버 공간에서 상당주의 의무가 국가의 행위를 규율하고 사이버 공간의 평화적 활용을 도모하기 위한 수단으로서 보다 효율적으로 기능하기 위한 방안을 모색하는 것을 궁극적인 목적으로 한다.

한편, 국제법상 '상당주의 의무'는 국가를 상대로 자행되는 사이버 공격이 만연한 사이버 공간에서 공격의 배후국이 아니더라도 공격과 일정한 관련성이 있는 '제3국의 의무'를 도출하고자 하는 개념이다. 따라서 본 연구에서 언급되는 불법적인 '사이버 조작'(cyber operation) 혹은 불법적인 사이버 공

---

[14] Corfu Channel case, Judgment of April 9th, 1949, I.C.J. Reports 1949, p.4, p. 22. 판례의 원문은 다음과 같다. (… every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.)

[15] 탈린매뉴얼 2.0, Rule 6.

격(cyber-attack)의 범위는 '국가'(State)를 상대로 자행되는 '초국경적인 사이버 공격'로 한정하고자 한다.

보다 구체적인 논의의 순서는 다음과 같다. 우선 제2장에서는 사이버 공간과 관련한 이론적 논의를 검토하였고 관련 용어의 정의에 대한 검토에 더불어 사이버 공간과 사이버 공격이 갖는 특수성에 대하여 살펴보았다. 또한 전통적인 국제법을 사이버 공간에 적용함에 있어 제기되는 쟁점에 대하여 다루었으며, 이는 UN 제1위원회 산하의 정부전문가그룹(GGE)과 NATO 산하의 TM 국제전문가그룹에서 이루어지는 논의를 기반으로 하였다. 나아가 전통적인 국제법 법리 중에서 특히 '국가책임법'이 사이버 공간에서 갖는 한계에 대하여 분석하였다. 사이버 공간에서 국가책임법 적용의 한계는 고도의 익명성과 비대칭성이라는 사이버 공격의 특수성으로부터 기인하며 본 연구는 이러한 한계를 극복하기 위한 방안으로 현행 국제법상의 규범인 '상당주의 의무'를 사이버 공간에도 적용할 것을 제안하였다.

상당주의 의무를 사이버 공간에 적용하기에 앞서, 제3장에서는 전통적인 국제법 영역에서 상당주의 의무가 정의되어 온 방식, 상당주의 의무의 국제법 체계 내에서의 발전 과정, 그리고 동 의무를 특정한 국제법 분야에 적용하였을 시 발생하는 적용상의 쟁점 등에 대하여 검토하였다. 우선, 상당주의 의무의 정의에 대해 확인하기 위하여 주권 국가의 본원적 권리인 '주권(sovereignty)'과 이러한 '주권 상호존중의 의무'로부터 국제법상의 상당주의 의무가 파생된다는 점에 대해 살펴보았다. 나아가, 국제재판소의 판례에 나타난 판시 내용 등을 검토함으로 전통적인 국제법 영역에서 상당주의 의무가 어떻게 정의되고 또한 발전되어 왔는지에 대하여 검토하였다. 한편, 상당주의 의무는 국제환경법의 영역에서 보다 깊이 있게 발전해온 바, 제3절에서는 국제환경법상 상당주의 의무의 발전 과정 및 의의에 대해 보다 상세히 다루었다. 국제환경법 영역에서 상당주의 의무의 구체적인 내용은 대표적인 국제재판소 판례를 바탕으로 검토하였다. 이러한 내용에 기반하여 제3장에서는 상당주의 의무가 실질적으로 적용되는 상황에서 논의되는 주요 쟁점에 대하여 검토하였다. 상당주의 의무의 주요 내용 및 구체적 행위 기준을 검토함에 있어서는 ICJ의 Corfu Channel case의 재판부가 판시한 내용에 기초하였다.

제3장에서의 논의를 바탕으로 제4장에서는 전통적인 국제법 상의 규범인 상당주의 의무를 사이버 공간에 본격적으로 적용하고 검토하였다. 우선, 사이버 공간에서 상당주의 의무가 적용되어야 할 필요성에 대하여 검토한 뒤 동 의무의 구체적인 적용 가능성에 대해 살펴보았다. 이를 위해서 Corfu Channel 사건을 기반으로 상당주의 의무의 의미와 역할에 대해 분석한 국제법위원회의 보고서, 탈린매뉴얼, 그리고 UN 정부전문가그룹의 최종 보고서를 종합적으로 검토하였다. 이러한 논의에서 더 나아가 제4장에서는 상당주의 의무를 사이버 공간에 적용하였을 때 쟁점이 되는 사안들에 대하여 다루었다. 가령, 사이버 공간에서의 '영토(territory)'범위, 상당주의 의무를 발동하기 위한 피해의 '심각성(serious)' 정도, 영토국의 '인식(knowledge)'의 기준 등이 문제되었으며, 이에 대한 합의가 요구된다. 끝으로 제4장에서는 사이버 공간에서 상당주의 의무의 국제법적 지위에 대하여 검토하였다.

앞선 장에서의 논의를 바탕으로 하여 제5장에서는 상당주의 의무를 사이버 공간에 적용함에 있어서 추가적인 논의를 요하는 국제법적 쟁점에 대하여 검토하고, 나아가 본 연구의 한계 및 함의에 대하여 살펴보았다. 사이버 맥락에 상당주의 의무가 적용되어야 할 필요성에 관한 긍정적인 인식과는 별개로 동 의무가 사이버 공간에서 효율적으로 기능하기 위해서는 추가적인 논의를 필요로 하는 국제법적 쟁점이 존재한다. 보다 구체적으로 제5장에서는 상당주의 의무의 국제법적 구속력 부재에 따른 규범적 가치 확보의 필요성, 구체적인 적용 기준 대한 합의, 그리고 상당주의 의무의 집행력 확보 수단에 대한 논의가 이루어져야 함을 명시하였다. 끝으로 제5장에서는 상당주의 의무가 가지는 한계로 본질적 한계 및 기술적 난점에 대해 검토하였으며, 본 연구가 갖는 함의에 대해서도 살펴보았다. 이때의 함의는 본 연구가 분단국인 우리나라의 안보에 갖는 함의와, 오늘날 국제사회의 안보 전반에 갖는 함의로 나누어서 검토하였다.

끝으로 제6장에서는 앞서 검토하였던 기존 국제법이 사이버 공간에 적용되었을 때의 핵심적 논의와 그 한계 (제2장), 현행 국제법 체제 하에서의 상당주의 의무의 역사와 적용상 쟁점 (제3장), 상당주의 의무의 사이버 공간에서의 적용 가능성과 구체적 쟁점 (제4장), 그리고 상당주의 의무의 효율적 역

할 수행을 위한 법적 쟁점 및 한계와 함의 검토 (제5장) 등의 전반적인 내용을 종합하고 요약하였다. 나아가, 사이버 공간에서 상당주의 의무가 갖는 중요성과 동 의무를 사이버 공간에 적용하여야 할 필요성에 대해 상기하였으며, 상당주의 의무가 사이버 공간에서 적극적으로 활용되기 위하여 국제사회가 기울여야 하는 노력에 대해 제시하였다.

제 2 장. 사이버 공간과 국제법

-국가책임법 적용을 중심으로-

제 1 절. 사이버 공간에 관한 이론적 논의

I. 용어의 정리

1. 사이버 공간 (cyber-Space)

'사이버 공간'(Cyber-Space)은 기존의 육지, 바다, 상공 및 우주에 더한 새롭고 인위적인 공역으로 인식되어 왔다.[16] 그러나 다른 한편, 사이버 공간은 기존의 국제 공역과는 달리 사용자의 자유로운 접근을 허용하는 국제사회의 유연한 규범이 일부 요구되는 공간임과 동시에, 사이버 행위나 인프라 기술에 대한 국가 주권의 배타적인 관할권이 미치는 '이중적 특성'을 가지는 특수한 영역으로 간주되기도 한다.[17] 한때 사이버 공간을 물질적 실체 및 현실과 동떨어진 오직 '가상의 공간'이라고 간주하는 시각도 존재하였으나,[18] 오늘날 우리 삶에서 인터넷에서 차지하는 비중이 현저하게 커짐에 따라 사이버 공간은 단순한 가상의 공간이 아닌 인류의 삶과 현실에서 실질적인 영향력을 갖는 공간으로 인식되고 있다.[19] 사이버 공간을 바라보는 이러한 시각은 탈린 매뉴얼을 집필한 Michael N. Schmitt의 견해로부터 보다 명확하게 확인된다. 그는 2013년에 발표한 자신의 저서를 통해 사이버 공간에 대하여 '컴퓨터

---

[16] 박노형·정명현, "사이버전의 국제법적 분석을 위한 기본개념의 연구 – Tallinn Manual의 논의를 중심으로 –", 『국제법학회논총』, 제59권 제2호 (2014), p.67.

[17] Yaroslav Radziwill, Cyber-Attacks and the Exploitable Imperfections of International Law, (The Netherland Brill, 2015), pp.93-94; Julie J.C.H, Daniel J. Ryan & Eneken Tikk, "Cybersecurity regulation: Using analogies to develop frameworks for regulation", International Cyber Security: Legal & Policy Proceedings (2011), pp.90-91.

[18] 서동주, "한국정치학에서 '사이버 공간 · 안보 연구동향과 정책적 함의", 『국가전략』, 제14권 제2호 (2008), pp.5-6.

[19] 박노형·정명현, supra note 16, p.67.

네트워크를 사용해 데이터를 저장, 수정, 교환하는 것을 목적으로 컴퓨터와 전자기 스펙트럼의 사용을 특징으로 하는 물리적 및 비물리적인 구성요소에 의해 함께 형성되는 환경'이라고 정의한 바 있다.[20] 한편, 오늘날 사이버 공간은 현대전의 새로운 영역으로 포섭하여 정의되기도 한다. 가령 미 국방부(Department of Defense: DoD)의 사이버공간 운영에 대한 국방 전략에 의하면 사이버 공간은 현실에서 상당한 영향력을 가지며, 그 결과 미군은 사이버 공간을 지상, 해양, 우주에 이어 국방부의 전략적 활동에 직접적인 영향력을 가지는 영역으로 간주하는 태도를 보인다.[21] 한국군 합동 사이버작전 강화방안에 관한 보고서에서 사이버 공간을 정의하는 방식 역시 미 국방부의 관점과 유사하다. 동 문서는 새로운 전장 영역을 이해하는 연장 선상에서 사이버 공간을 정의하고 있으며, 이에 따르면 사이버 공간이란 다수의 물적 정보체계, 물리적 기반구조, 소프트웨어 및 정보와 함께 그것을 사용하는 인간에 의해 종합적으로 형성된 네트워크를 의미한다.[22] 이처럼 사이버 공간을 정의하는 방식은 매우 다양하다고 할 것이나, 사이버 공간을 규정함에 있어서 공통적으로 확인되는 바는, 오늘날 인류는 사이버 공간을 더 이상 물리적 공간과 동떨어진 가상의 공간으로 간주하지 않는다는 사실이다.

2. 사이버 조작 (cyber-operation)

'사이버 조작'(cyber operation)은 이를 정의하는 주체와 맥락에 따라 조금씩 다르게 정의된다. 다만 탈린매뉴얼은 사이버 조작을 '사이버공간에서 또

---

[20] Michael N. Schmitt, The Tallinn Manual on the International Law applicable to Cyber Warfare, NATO Cooperative Cyber Defence Centre of Excellence, (Cambridge University Press, 2013), p.258. 원문은 다음과 같다. ("the environment formed by physical and non-physical components, characterized by the use of computers and the electromagnetic spectrum, to store, modify, and exchange data using computer networks.")

[21] Department of Defense, "Department of Defense Strategy for Operating in Cyberspace", Washington D.C, DoD (2011), p.5.

[22] 송재익, "한국군 합동 사이버작전 강화방안 연구 – 합동작전과 연계를 중심으로 – "", 『한국군사』, 제2호 (2017), p.151.

는 이를 통하여 목표를 달성하기 위해 사이버 역량(cyber capacity)을 활용하는 것'이라고 정의하고 있다.[23] 한편 사이버 조작은 유사한 개념인 사이버 활동(cyber activity)과 연계하여 설명될 수 있다. 사이버 조작과 사이버 활동은 유사하지만 분명한 차이점을 갖는다. 탈린매뉴얼은 사이버 활동을 '사이버 기초설비의 이용 또는 그러한 기초설비의 작동에 영향을 주기 위하여 사이버 수단을 사용하는 모든 활동'이라고 정의하고 있으며, 그러한 '활동'에는 '사이버 작전을 포함하나 다만 이에 한정되지 않는다'라고 정의하고 있다.[24] 즉, 사이버 활동은 사이버 조작에 비하여 보다 넓은 개념으로 간주된다.

3. 사이버 공격(cyber-attack)

오늘날 사이버 공격(cyber-attack)을 정의하는 구속력 있는 국제법 조약 혹은 통일된 정의는 부재하다.[25] 국제사회에서 통용되는 사이버 공격에 대한 정의는 매우 다양하며 사이버 공격은 종종 '사이버 전쟁'(cyber war) 등의 용어와 혼용되기도 한다.[26] 미 정부의 보안 전문가인 Richard A. Clarke는 '사이버 전쟁'(cyber war)을 '피해 혹은 혼란을 야기할 목적으로 타국의 컴퓨터 네트워크에 침투하는 국가의 행위'로 정의하였으며 이는 오늘날 사이버 공격과 관련하여 가장 널리 인용되는 정의 중 하나로 여겨진다.[27] 사이버 공격에 대해 최초로 군사적인 정의를 내린 것은 2011년 미국 사이버 사령부(United States Cyber Command)의 초대 합참의장인 것으로 전해진다.[28] 미

---

[23] NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd Edition (Cambridge University Press, 2017), p.568.

[24] Ibid.

[25] 백상미, supra note 13, p.83.

[26] Oona A. Hathaway & Crootof Rebecca, "The Law of Cyber-attack", California Law Review, Vol. 100 (2012), p.823.

[27] Richard A. Clarke & Robert K. Knake, "Cyber War – The next threat to National Security and what to do about it", (HarperCollins Publishers, 2010), p.11.

[28] 장신, "사이버 공격과 Jus in bello", 『국제법학회논총』, 제60권 제4호 (2015), pp.205-206.

사이버 사령부 합참의장의 정의에 따르면 사이버 공격은 '컴퓨터와 관련 네트워크를 활용하여 상대국의 사이버 시스템을 파괴하거나 교란하고자 하는 적대 행위'를 의미한다. 나아가 그는 사이버 수단을 활용하여 상대국의 컴퓨터 시스템과 데이터에 대한 공격 수행 뿐만 아니라 목표국의 사이버 기반시설 전반을 파괴하거나 성능을 저하시키는 일체의 행위 역시 사이버 공격의 범위에 포함된다는 견해를 표명하였다.[29]

한편 탈린매뉴얼을 집필한 국제전문가그룹이 '효과기반 접근법'(effect-based approach)에 기초하여 사이버 공격을 정의한 것은 주목할 만 하다.[30] 탈린매뉴얼은 사이버 공격에 대하여 '공세적(공격적)이든 혹은 방어적이든, 사람에게 상해 또는 사망을 야기하거나 물건의 손해 또는 파괴를 야기할 것이 합리적으로 예상되는 사이버 작업 혹은 사이버 조작(cyber operation)'을 의미하는 것으로 규정하고 있다.[31] 즉, 사이버 공격의 정의에 대한 이견이 존재함에도 불구하고 국제전문가그룹은 모든 불법적 사이버 조작을 곧바로 사이버 공격으로 간주하지는 않는다. 이들은 사람의 상해, 사망, 재물에 대한 심각한 손괴 등 일정한 기준점(threshold) 이상의 피해를 유발하는 사이버 조작을 사이버 공격으로 포함한다. 이를 통해 국제전문가그룹이 단순한 수준의 사이버 조작이 무력 행위(armed force)가 되기 위해서는 해당 사이버 조작이 특정한 수준 이상의 '파괴적 효과'(destructive effect)를 유발해야 한다는 견해를 제시하고 있음이 확인된다.[32] 가령, 사람들로 하여금 단순히 '불편함'을 유발하는 사이버 조작은 그것이 미치는 효과를 고려하였을 때 사이버

---

[29] James E. Cartwright General, Memorandum for Chiefs of the Military Services Commanders of the Combatant commands Directors of the Joint Staff Directorates, Joint Terminology for Cyberspace Operations, Washington, D.C. 201318-9999, p.5.

[30] 백상미, supra note 13, p.83.

[31] 탈린매뉴얼 2.0, Rule 92; NATO Cooperative Cyber Defence Centre of Excellence, supra note 23, p.415.

[32] Johann-Christoph Woltag, "Cyber Warfare", Max Plank Encyclopedia of public International Law, (Oxford Public International Law, 2015), para. 8.

공격에 포함되지 않는 것으로 보아야 한다.[33]

II. 사이버 공간 및 사이버 공격의 특수성

본 연구는 사이버 공간에서 상당주의 의무가 적용되어야 할 필요성과 동 의무의 적용 가능성에 대하여 검토하는 것을 일차적인 목적으로 한다. 초국경적 환경피해를 방지하기 위하여 국제환경법 영역에서 가장 활발하게 원용되어 온 상당주의 의무가 최근 사이버 공간을 규율하는 규범으로서 새롭게 대두된 까닭은, 물리적인 공간과는 달리 사이버 공간만이 갖는 특수성, 혹은 사이버 공간을 매개로 이루어지는 사이버 공격의 특성과 밀접한 관련이 있다. 사이버 공간에서 상당주의 의무의 적용 가능성과 동 의무의 역할에 대하여 논의하기에 앞서, 사이버 공간과 사이버 공격의 특수성에 대한 검토가 선결적으로 이루어질 필요가 있다고 판단하는 바, 아래에서는 관련 내용에 대해 살펴보기로 한다. 사이버 공간과 사이버 공격이 갖는 여러가지의 특수성 중에서 본 연구는 1. 사이버 공간의 이중적 특성, 2. 공격의 복잡한 공격 양태로 인한 귀속의 어려움, 3. 사이버 공격 과정에서 비국가행위자의 영향력 확대에 주목하였다.

1. 사이버 공간의 이중성

사이버 공간은 영토 및 국경의 개념이 명확하게 확립된 물리적 공간과는 달리 기본적으로 '초국경적'(transboundary) 특성을 갖는다. 전 세계로 연결된 네트워크를 통해 행위자는 손쉽게 타국의 네트워크로 접근할 수 있으며 그 결과, 사이버 공간을 매개로 발생하는 사이버 공격을 비롯한 각종 사이버 범죄의 결과물 역시 초국경적이며 세계적이다.[34] 이러한 측면을 고려할 때 사

---

[33] 탈린매뉴얼 2.0, Rule 92(14). 이때 '불편'이라는 용어의 범위는 확정되지 않았다. 다만 국제전문가그룹은 공격이 상해와 사망을 포섭하는 것이기는 하나, 인도주의적 목적에 비추어 보았을 때 상해에 준하는 심각한 질병 및 극심한 정신적 고통도 공격의 범위에 포함된다는 것에는 동의한 바 있다. 탈린매뉴얼 Rule 92(8) 참조.

[34] 박노형, supra note 11, p.796.

이버 공간은 물리적이고 가시적인 국경의 영향에서 비교적 자유로운 공간이라는 것을 확인할 수 있다.[35] 그러나 사이버 공간의 이러한 초국경적 특성은 절대적이지 않다. 사이버 공간은 연결된 네트워크를 통해 정보에 대한 사용자의 보다 자유로운 접근을 허용한다는 측면에서 부분적으로 초국경적이라고 할 수 있으나 다른 한편 사이버 행위, 물리적 기반시설, 인프라, 사이버 기술의 등의 측면에 있어서는 주권 국가의 적극적인 통제가 미치기도 한다.[36]

이처럼 네트워크에 대한 자유로운 접근이 가능한 '초국경성'과 국가 주권의 배타적 관할권이 미치는 '영토성'이 혼재하는 사이버 공간의 이중적 특성은 기존의 국제법을 사이버 공간에 적용함에 있어서 각종 어려움을 유발하게 된다. 가령 사이버 공간의 이중성은 이를 규율하는 방식의 기본적인 관점에 대한 국가 간, 진영 간 견해 대립을 초래함으로써 사이버 공간을 규율하는 규범에 관한 전지구적 차원의 합의를 저해하였다.[37] 이러한 입장은 크게 동 영역을 기존의 국제법 체제 내에 포섭하고자 하는 입장과, 사이버 공간의 특수성을 반영한 독자적 규범을 창설하고자 하는 입장으로 나뉘며, 이는 사이버 공간을 규율하는 규범 형성 과정에서 매우 큰 비중을 차지하고 있다. 관련된 국제사회의 논의와 그 의의는 제2절에서 보다 상세하게 다루기로 한다.

2. 복잡한 공격 양태로 인한 귀속의 어려움

공격 근원지와 공격자에 대한 비교적 명확한 식별이 가능한 재래식 공격과는 달리 사이버 공간을 매개로 이루어지는 사이버 공격은 공격 행위자의 신원을 파악하기 어렵다는 점에서 고도의 '익명성'(anonymity)을 갖는다.[38] 또한 오늘날 발생하는 대다수의 사이버 공격은 제3의 지역 및 국가에 공격 거점을 두고 이루어지는 등의 양상을 보인다. 즉, 사이버 공격은 다수의 수행

---

[35] Nicolò Bussolati, "The rise of Non-State Actors in Cyberwarfare", Cyber War: Law and Ethics for Virtual Conflicts Oxford University Press (2015), p.103.

[36] Yaroslav Radziwill, supra note 17, pp.93-94.

[37] Rahul Prakash & Darshana M. Baruah, "The UN and Cyberspace Governance", ORF Issue Brief. No. 68 (2014), p.2.

[38] Russell Buchan, Macro Roscini & Nicholas Tsagourias, supra note 12, p.2.

자에 의해 운용될 수 있으며 각기 다른 관할권에 놓인 PC가 공격 거점으로 활용되기도 한다.[39] 이때 공격 거점은 공격자의 물리적 위치를 반영하지 않는 것이 일반적이다.[40] 가령, DDoS 공격에 활용되는 좀비 컴퓨터와 서버는 공격의 직접적인 배후국 혹은 행위자와 무관한 제3의 여러 국가의 사이버 기반시설에 소재할 수 있다. 또한 공격자와 전혀 상관이 없는 제3국의 개인 네트워크에 악성코드가 감염되도록 하는 경우도 빈번하다. 상당수의 악성코드는 사용자들이 자주 방문하는 웹페이지에 설치되며, 이는 프로그램에 내장된 안티바이러스 탐지기를 통해서도 쉽게 탐지되지 않으므로 더욱 쉽게 전파되고 악용된다.[41] 이처럼 사이버 공격의 은밀하고 복잡한 공격 양태는 공격자의 위치를 드러내지 않는 것을 기본 원칙으로 하며, 설령 피해국에 의해 공격 행위가 포착되더라도 추적을 교란함에 있어서 매우 유리하다.[42] 고도화 된 탄도미사일의 경우에도 인공위성 등을 통해 공격의 양태를 파악할 수 있으나, 복잡한 공격 양태를 활용하는 사이버 공격은 공격의 양상 파악과 근원지 추적에 큰 어려움이 따른다.[43]

3. 비국가행위자의 영향력 증대

서유럽에서 근대 국제법이 태동한 이래로 약 3세기 동안 국제법의 주체는 국가(State)로 간주되어 왔다.[44] 국가 주권의 절대성은 오늘날에도 여전히 국제 질서의 근간을 이루고 있으나 과학 기술의 비약적으로 발전한 결과, 국제법의 정립과 운영 과정에서 전통적인 국가와는 맥을 달리 하는 다양한 행위 주체들이 새롭게 등장하고 있다.[45] NGO, 다국적기업, 사인, 국제테러조직

---

[39] Ibid.

[40] 백상미, supra note 13, p.85.

[41] Christian Czosseck, Gabriel Klein & Felix Leder, "On the Arms Race Around Botnets-Setting Up and Taking Down Botnets", International Conference on Cyber Conflict (2011), p.108

[42] Russell Buchan, Macro Roscini & Nicholas Tsagourias, supra note 12, p.2.

[43] 박노형, supra note 11, p.799.

[44] 정인섭, 『신국제법강의』 제12판. 서울, 박영사, 2021. pp.174-175.

[45] Ibid., p.174.

등의 새로운 행위 주체는 국제사회에서 '비국가행위자'(non-State actors)로 명명된다. 이들은 국제 관계에서 크고 작은 영향력을 행사하고 있으며, 외교, 경제, 군사 및 안보적 측면에서 비국가행위자의 영향력은 국가(State)의 그것에 견줄 만한 것으로 여겨진다.[46] 그러나 무엇보다도 비국가행위자의 영향력은 사이버 공간에서 더욱 두드러지는 모습을 보인다.[47] 사이버 공간의 활용이 증대됨에 따라 비국가행위자의 활동 반경과 정보에 대한 접근성이 지속적으로 확장되어 왔으며 결과적으로 이들의 국제적 지위와 사이버 공간에서의 영향력 역시 비약적으로 확대되고 있다.[48] 특히 비국가행위자가 오늘날 국제사회에서 발생하는 사이버 공격에 관여하는 비중이 매우 높다는 사실은 상당히 주목할 만한 지점이다.[49] 비국가행위자는 사이버 공간의 접근성과 사이버 수단의 경제성 등 각종 이점을 바탕으로 사이버 공간을 불법적 활동의 주 무대로 적극 활용해 왔으며, 오랜 기간에 걸쳐 상당한 수준의 사이버 공격 및 방어 기술을 축적해 왔다.[50]

그러나 사이버 공간에서 비국가행위자가 주목 받는 보다 결정적인 원인은 이들이 감행하는 사이버 공격 과정에 국가가 다양한 방식으로 연루되어 있기 때문이다.[51] 오늘날 발생하는 상당수의 사이버 공격은 표면적으로 비국가행위자의 자발적 의지에 기반하여 자행되는 것처럼 보이지만, 당해 공격의 배후에 국가의 직접적인 개입과 통제가 존재하는 사실은 공공연한 사실이

---

[46] 정인섭, "왜 비국가 행위자를 말하는가?", 『서울국제법연구』, 제17권 제2호 (2010), p.2.

[47] Yaroslav Radziwill, supra note 17, p.27; Pierluigi Paganini, "Non-State Actors in cyberspace: an attempt to a taxonomic classification, role, impact and relations with a sate's socio-economic structures", Universita Degli Studi Firenze (2022), p.5.

[48] Russell Buchan & Nicholas Tsagourias, supra note 9, p.377; Nicolò Bussolati, supra note 35, p.103.

[49] Sico van der Meer, "How states could respond to non-State Cyber-attackers", Policy Brief, Clingendael Netherlands Institute of International Relations (2020), p. 1; Yaroslav Radziwill, supra note 17, p.27.

[50] Yaroslav Radziwill, ibid.

[51] 김효권, "국가가 연루된 비국가행위자의 사이버공격에 대한 국가책임 귀속성", 『저스티스』, 통권 제193호 (2022), p.294.

다.[52] 대표적인 사례로 2007년 에스토니아의 국가 전산망 전반을 마비시킨 DDoS 공격과, 2008년 이란의 나탄즈 핵 발전소에 가해진 스턱스넷(Stuxnet) 공격을 떠올려 볼 수 있다. 물론 두 사건 모두 공격의 배후국을 공식적인 차원에서 특정하지는 못하였다. 그러나 배후국으로 추정되는 국가와 피해국 간의 정치적 갈등이 명백한 상황에서, 사이버 수단을 통해 타국의 핵심 기반시설을 타격한 행위를 단순히 해커 조직의 소행으로 치부하는 것이 과연 타당한 것인지에 대해서는 여전한 의문이 남는다.[53] 이처럼 사이버 공격을 수행한 비국가행위자의 배후에 피해국과 정치적으로 적대 관계에 있는 국가가 여하한 방식을 통해 영향력을 행사하였을 것으로 의심되는 사례는 적지 않게 발견된다.[54]

사이버 공격 과정에서 비국가행위자의 영향력이 증대되고, 이들이 국가와 다양한 방식으로 연계되는 현상은 공격에 대한 책임 귀속(attribution)과 국가책임법 적용이 어렵다는 또 다른 문제점과도 직결된다.[55] 물론 비국가행위자의 출현으로 인한 주체 식별의 어려움은 재래식 전투 상황에서도 존재하였으나 사이버 공격의 비대칭적 특성으로 인해 그 어려움이 한층 더 심화된 것은 명백한 사실이다.[56] 비국가행위자가 사이버 공격 주체로 대두하고 이들의 영향력이 증가함에 따른 국제법상 국가책임법 적용의 어려움은 본 장의 제4절에서 보다 상세하게 다루기로 한다.

4. 소결

앞선 논의를 종합하면 우선 사이버 공간은 '초국경적 특성'과 '영토적 특성'이 혼재하는 이중적 특성을 가지며, 이러한 특성은 기존의 국제법을 사이

---

[52] Yaroslav Radziwill, supra note 17, pp.27-28; 송태은, "최근 사이버 위협의 추세와 향후 전망 및 국제사회의 대응", 외교안보연구소 주요국제문제분석 (2023), p.1.

[53] 김효권, supra note 51, p.294.

[54] Joyce Hakmeh & Kerstin Vignard, “ICTs, International Security, and Cybercrime: Understanding their Intersections for Better Policymaking”, UNIDIR (2021), p.7.

[55] Joyce Hakmeh & Kerstin Vignard, p.7.

[56] 송태은, "최근 사이버 위협의 추세와 향후 전망 및 국제사회의 대응", p.9.

버 공간에 적용하는 논의에 있어서 어려움을 유발하는 기제가 되었다. 한편 사이버 공격은 복잡한 공격 양태를 통해 공격의 주체를 은닉하거나 추적을 어렵게 한다는 점에서 상당한 수준의 익명성을 가지고 있기도 하다. 더불어, 공격 과정에서 비국가행위자의 영향력이 점차적으로 확대되고 있다는 점 역시 사이버 공격의 주요한 특성으로 간주된다. 특히 비국가행위자가 국가와 다양한 방식으로 연계된다는 점은 앞서 언급된 공격의 비대칭성과 더불어 오늘날 사이버 공격의 주체 식별과 책임 귀속의 어려움을 야기한다. 앞서 살펴본 이러한 사이버 공간 및 사이버 공격의 특성은 물리적 관할권에 기반한 국가 주권의 개념을 퇴색시킬 우려가 있으며, 이러한 주권 개념 하에 성립된 기존의 국제사회의 질서를 위협함으로써 심각한 안보위기 상황을 초래할 수 있다.[57]

제 2 절. 사이버 공간에서 국제법 적용과 관련된 논의

I. 사이버 공간의 '행위 규율'에 관한 논의의 쟁점

제1절에서 확인한 바와 같이 사이버 공간과 이를 매개로 발생하는 사이버 공격의 특성은 크게 '초국경성과 영토성이 혼재하는 이중성', '복잡한 공격 양태에 기한 고도의 익명성', 그리고 '국가와 비국가행위자의 다양한 연계성'으로 요약될 수 있다. 이러한 사이버 공간의 특수성은 전통적인 베스트팔렌 체제 하에서 성공적으로 규율 되어온 기존의 국제 질서에 큰 균열을 가져왔다.[58] 국가 주권(sovereignty)과 물리적 관할권에 기초한 베스트팔렌 체제와는 달리, 오늘날 사이버 공간에 새롭게 대두함에 따라 지리학적 장벽의 중요

[57] 신경수·신진, "국제사회와 사이버 공간의 안보문제", 『국제지역연구』, 제27권 제3호 (2018), p.28.

[58] David Betz & Tim Stevens, Cyberspace and the State: Toward a strategy for Cyber-power, (London: Routledge, 2011), pp.54-74.

성과 주권이 갖는 절대성이 급격하게 쇠퇴하였으며,[59] 이러한 국제 질서의 근본적인 변화는 사이버 공간에서의 행위 규율에 관한 국제사회의 담론을 야기하기에 이르렀다. 특히 물리적 관할에 기초한 전통적인 국제사회의 법질서가 사이버 공간에서도 그대로 적용될 수 있는지에 관한 의문이 지속적으로 제기되었고, 그 결과 사이버 공간에서의 국가 행위를 규율하는 방안에 대한 논의가 국제사회 전체의 차원에서 대두하였다.

사이버 공간에서 불법 행위의 주체는 크게 '국가'와 '개인'의 차원으로 나뉘며 기본적으로 양자는 각각 국제법과 국내법의 영역에서 분리되어 논의된다.[60] 이때 개인의 차원에서 자행되는 사이버 범죄(cyber-crimes)는 2001년 Council of Europe(이하 유럽평의회)에 의해 부다페스트에서 채택된 'Convention on Cyber Crime'(이하 사이버범죄 협약) 하에서 규율 된다.[61] 유럽평의회에서 2001년에 채택되고 2004년 발효한 사이버범죄 협약은 사이버범죄 처벌 대상과 협약 가입국 간의 국제협력 절차 수립 등을 규정하고 있다.[62] 사이버범죄 협약은 사이버 범죄 처벌 대상자에 대한 효율적인 수사를 도모하기 위한 조항을 다수 포함시킨 제2의정서의 채택을 위한 최종 결의를 앞두고 있다.[63] 우리나라 역시 2022년 10월 유럽 평의회에 사이버범죄 협약의 가입의향서를 기탁한 바 있다.[64]

그렇다면 사이버 공간에서 개인에 의해 자행되는 사이버 범죄와는 별도로 일국이 타국을 공격하는 행위인 이른바 사이버 공격(cyber-attack) 혹은 불

---

[59] Nicolò Bussolati, supra note 35, p.103.

[60] 사이버 공간에서 국가와 개인이 자행하는 범죄는 국제법과 국내법의 영역에서 각각 논의되는 것이 일반적이다. 그러나 예외적으로 비국가행위자의 행위가 국가의 행위로 귀속된다고 판단할 수 있는 경우 국가에 대한 국제법적 책임을 추궁할 수 있다.

[61] 'Convention on Cyber Crime'(이하 부다페스트 협약)은 2001년 11월 23일 채택되었고 2004년 7월 1일 발효하였다. 우리나라는 현재 부다페스트협약의 가입의향서를 기탁하고 가입을 추진 중에 있다.

[62] Council of Europe, Convention on Cybercrime, European Treaty Series No. 185, 2001.

[63] 박재성, "사이버범죄 국제조약의 동향 – 부다페스트 협약 제2추가의정서 및 유엔 사이버범죄 조약을 중심으로 –", 『저스티스』, 통권 제185호 (2021), p.249.

[64] 대한민국 외교부 국제기구국, "사이버범죄협약 (부다페스트협약) 가입의향서 제출", (2022. 10. 11), (마지막 접속: 2023.7.27)

법적인 사이버 조작(cyber operation)과 관련하여 국제사회는 어떠한 논의를 진행중인가? 오늘날 국제사회는 초국가적 맥락에서 발생하는 사이버 공격을 '사이버 안보'(cyber-security)의 관점에서 다루고 있다.[65] 이때 사이버 안보에 관한 담론은 크게 미국을 비롯한 서방 세력의 관점과 러시아 및 중국으로 대표되는 비서방 세력의 관점으로 나누어서 살펴볼 수 있다.[66] 보다 구체적으로 이러한 관점은 사이버 공간에 기존의 국제법 체계와 질서를 적용하고자 하는 미국 중심의 서방 세력의 관점과, 이를 개별 국가의 주권 하에서 통제 가능한 공간으로 간주하고자 하는 비서방 세력의 시각으로 구분된다.[67] 사실상 진영 간의 이러한 입장 차이는 이질적인 문화와 정치적, 경제적 배경, 이데올로기 등 복잡하고도 오래된 역사적 경험에 근거한다.[68] 즉, 양 진영이 지금껏 보여준 사이버 안보에 관한 의견 차이는 종래의 유엔 안보리에서 표출되었던 전통적인 안보대립과 유사하다고 볼 수 있을 것이다.[69] 물론 2013년 제3차 UN 정부전문가그룹 회의를 기점으로 사이버 안보에 관한 이들의 입장은 어느 정도의 타협점을 찾은 것으로 보이나 여전히 구체적인 수준에 있어서는 차이를 보인다. 아래에서는 사이버 안보에 관한 서방과 비서방진영의 기본적인 관점을 각각 살펴보고, 다음으로는 제3차 UN 정부전문가그룹의 회의 내용에 대해서 다루기로 한다.

1. 사이버 안보에 대한 관점 : 서방진영

미국 중심의 서방 진영은 원칙적으로 사이버 공간을 통제할 수 있는 새로운 질서 체계가 불필요하며, 기존의 국제법 체제를 사이버 공간에 그대로 적용할 수 있다는 입장을 취한다.[70] 이러한 미국의 입장은 2011년 백악관에서 발표한 'International Strategy for Cyberspace'를 통해 확인할 수 있다.

---

[65] 김효권, supra note 51, p.289.
[66] Rahul Prakash & Darshana M. Baruah, supra note 37, p.2.
[67] Ibid.
[68] 신경수·신진, supra note 57, p.29.
[69] Ibid., p.36.
[70] 박노형·정명현, supra note 16, p.69.

해당 문서에서 미국은 사이버 공간에서의 국가 행위를 규율함에 있어서 국제 관습법의 개혁이 필수적인 것이 아니며, 기존의 국제법 역시 진부한 것이 아니라고 언급한 바 있다. 다만 백악관은 사이버 공간에 기존의 국제법을 적용하는 것과 더불어, 정보통신기술(ICTs)의 독특한 속성에 기하여 기존의 국제법이 적용되는 구체적인 방안에 대해서는 추가적인 논의가 필요하다는 견해를 덧붙이기도 하였다.[71]

한편, 탈린매뉴얼은 사이버 공간에 대한 미국과 서방 진영의 입장을 잘 담고 있는 문서이다.[72] 탈린매뉴얼은 현존하는 국제법이 사이버 공간에 적용된다는 점을 명확히 하였다.[73] 즉, 탈린매뉴얼을 집필한 TM 전문가그룹은 사이버 공간을 별도의 법체계가 적용되어야 하는 별개의 영역으로 간주하지 않았다.[74] 기본적으로 이들은 기존의 국제법이 인터넷 및 사이버 공간을 규율하는 국제규범의 모태가 되어야 한다는 시각을 가지고 있었기 때문이다. 따라서 탈린매뉴얼 집필진은 사이버 공간의 특수성에도 불구하고 전통 국제법 체제 내의 'Jus ad bellum (개전법규)' 및 'Jus ad bello (전쟁법)' 개념을 모두 사이버 공간에 그대로 적용할 수 있다는 점을 전제로 논의를 진행하였다.[75] 그 결과 탈린매뉴얼에서는 별도의 법체계의 마련 없이 주권, 자위권, 무력의 사용, 무력사용에 대한 대응조치 등의 개념이 사이버 공간에서도 적용될 수 있다는 점이 확인된다. 그리고 이러한 논의의 이면에는 중국과 러시아 등이 언론의 자유, 탄압, 통제 등에 인터넷을 이용하는 등 국내 정치의 안전성 확

---

[71] White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, (2011), pp.9-10.

[72] 진영 간의 대립으로 인해 사이버 공간에 대한 국제법의 구체적 적용에 대한 합의가 어려운 상황에서 미국 등의 일부 서방국가들은 NATO를 중심으로 동 이슈를 논하였으며, 이는 탈린매뉴얼의 발간으로 이어졌다. 다만 2013년 발간된 탈린매뉴얼은 평시 규범 중심의 구체적 적용방안을 담고 있지는 않다. 실제로 다수의 사이버 공격은 무력공격의 수준에 이르지 않는 경우가 많아 평시 규범 중심의 구체적 적용방안의 가이드라인 제시가 필요한 바, 이후 기존의 탈린매뉴얼을 개정한 탈린매뉴얼 2.0이 발간되었다. 유준구, "사이버안보 문제와 국제법의 적용", 『국제법학회논총』, 제60권 제3호 (2015), p.153 참조.

[73] 박노형·정명현, supra note 16,p.68.

[74] Ibid., p.69.

[75] 장신, supra note 28, pp.202-203.

보 방안으로써 사이버 공간을 악용하는 것을 방지하고자 하는 숨겨진 의도가 있는 것으로 여겨진다.[76]

2. 사이버 안보에 대한 관점 : 비서방진영

비서방진영의 대표적인 안보협력체제는 2001년 출범한 '상하이협력기구'(Shanghai Cooperation Organization, 이하 SCO)이다. SCO는 정보통신 기술의 발달에 따른 정보 위협에 이어 '사이버 안보'(cyber security)를 상당히 비중 있는 안보 현안으로 다루고 있다.[77] 비서방 국가가 SCO를 통해 수립하고자 하는 사이버 안보 규범의 특징은 사이버 공간에서의 '국가 주권 강화', '국가의 정보통제권 인정', 그리고 '국제 인터넷 거버넌스 체제 변경'으로 요약된다.[78] 이러한 논의 중 비서방진영의 가장 핵심적 논지는 사이버 공간을 본질적으로 국가 주권이 미치는 통제 가능한 공간으로 인식하여야 한다는 점이다.[79] 이를 위해 비서방진영은 궁극적으로 사이버 공간의 특이성을 반영한 새로운 형태의 국제규범을 창설할 것을 주장하며 전통적인 국제규범으로는 사이버 공간을 적절히 규율할 수 없다는 점을 강조한다.

사이버 공간에서 국가의 주권을 더욱 강화하고자 하는 비서방진영의 태도는 인터넷이 국내 정치 체제의 전복 수단으로 사용될 것에 대한 우려에서 비롯한다.[80] 이러한 우려를 불식시키고 국내 정치 체제를 공고히 하기 위한 방안으로서 비서방진영은 사이버 공간에서의 국가 주권과 정보 통제력 강화를

---

[76] 김소정·박상돈, "국제협력을 통한 사이버안보 강화방안 연구", 『융합보안논문지』, 제13권 제6호 (2013), p.53.

[77] 장노순, "사이버안보와 국제규범의 발전: 정부전문가그룹(GGE)의 활동을 중심으로", 『정치정보연구』, 제19권 제1호 (2016), pp.8-9.

[78] 양정윤, "상하이협력기구의 사이버 안보 논의: 러시아와 중국의 역할", 국제문제연구소 워킹 페이퍼, No. 103 (2019), p.1.

[79] 유준구, supra note 72, p.153.

[80] 양정윤, supra note 78, p.10; Jon Lindsay, "China and Cybersecurity: Political, Economic and Strategic Dimensions", Report from workshops held at the University of California, San Diego (2012), p.8, pp.30-31. (본 연구에서는 중국 정부를 상대로 한 '정치적'인 목적을 지닌 사이버 공격에 대하여 우려를 표명하고 있다.)

주장하는 것이다.[81] 사이버 안보에 관한 비서방진영의 이러한 태도는 SCO가 '정치적 안정성을 저해하는 사이버 기술'(cyber technology to undermine political stability) 역시 사이버 공격(cyber-attack)의 정의에 포함하였다는 사실로부터 재확인된다.[82] 더불어 이들은 사이버 공간을 규율하는 별도의 국제 규범이 부재한 현 상황에서 사이버 공격 수단을 개발하기 위한 군비가 경쟁적으로 확대되고 사이버 수단이 국가의 안보를 위협하는 방식으로 남용될 수 있다는 점에 대한 우려를 표명하였다.[83] 그리고 이를 해결하기 위해서는 역시 전통적인 국제법의 확장 적용이 아닌, 사이버 공간의 특수성을 반영한 별도의 국제법 형성이 필요하다는 입장을 취한다.[84] 같은 맥락에서 이들은 사이버 공간에 적용되는 전쟁 법규 역시 전통적인 국제법의 'Jus ad bellum' 및 'Jus ad bello'를 대신하는 새로운 군축 조약 등 새로운 국제규범이 창설되어야 한다는 견해를 피력하였다. 러시아와 중국 등 비서방진영의 이러한 주장에는 기존의 인터넷 체계를 구성하고 주도해 온 서방 진영의 의도대로 인터넷과 사이버 공간을 규율하는 체제를 수용할 수는 없다는 의도가 담겨있으며, 궁극적으로는 미국 등의 서방 중심의 국제 인터넷 거버넌스 체제의 근본적인 변화를 꾀하고자 하는 의도가 내재된 것으로 볼 수 있다.[85] 사실상 인터넷은 태동단계에서부터 실질적으로 미국 중심의 거버넌스 구조에 기반하여 발전해 왔으며 이러한 미국 패권체제가 인터넷 공간에서 확산 및 유지되는 것을 방지하고자 하는 기조는 중국과 러시아의 국가 정책에서도 잘 드러난다.[86] 보다 구체적으로 이들은 UN 등 정부간 기구에 의한 사이버 공간의 철저한 관리감독을 주장함으로써 미국 중심의 패권 체제를 약화하고, 정부 중심의 의사결정체계를 사이버 공간에 반영하기 위한 적극적인 노력을 기울이고 있다.[87]

---

[81] 양정윤, supra note 78, p.10

[82] Oona A. Hathaway & Crootof Rebecca, supra note 26, p.825.

[83] 유준구, supra note 72, p.152.

[84] Ibid.

[85] 김소정·박상돈, supra note 76, p.54.

[86] 양정윤, supra note 78, pp.13-15.

[87] Ibid., pp.13-4

3. 제3차 UNGGE의 논의 (2012년-2013년)

앞서 확인한 바와 같이 사이버 공간을 규율하기 위한 방안에 대하여 국제사회는 큰 이견을 보여왔다. 즉, 사이버 공간에 기존 국제법을 그대로 적용할 수 있는지, 혹은 사이버 공간의 특이성을 반영한 새로운 국제 규범이 창설되어야 할 것인지에 대한 서방과 비서방의 지난한 논의가 이어져 온 것이다. 이러한 관점의 대립은 2012년에 개최된 제3차 UN정부전문가그룹 회의를 계기로 전환점을 맞게 된다. 제3차 UN정부전문가그룹 회의에서는 유엔헌장을 비롯한 기존의 국제법의 사이버 공간에서의 적용 가능성에 대한 일정 부분의 합의를 이루었다는 점에서 매우 큰 의의와 함께 사이버 규범에 관한 논의의 측면에서 큰 진전을 이루었다고 할 수 있다.[88]

2012년에 개최된 제3차 UN 정부전문가그룹 회의에서는 사이버 보안과 관련하여 실존하는 위협, 정보통신기술환경을 보호하기 위한 방안, 국가책임 행위에 대한 국제규범, 정보 교류와 신뢰구축 조치 등을 포함한 사이버 안보의 전반적인 분야에 대한 폭넓은 논의가 이루어졌다.[89] 제3차 GGE의 논의 과정에서 가장 의미 있는 것은 UN 헌장을 비롯한 국제법의 기본원칙 등이 사이버 공간에 적용될 수 있다는 것에 대하여 합의를 이룩하였다는 점이다.[90] 다시 말해, 이러한 합의는 국내문제불간섭의 문제, 불법적인 무력행사 금지원칙, 자위권 등의 주권과 주권으로부터 파생된 국제법의 원칙들이 사이버 공간에서도 적용될 수 있음을 의미하는 것이다.[91] 제3차 정부전문가그룹의 합의는 비서방 진영인 러시아를 포함한 GGE 참여국 모두가 동의한 것이라는 점에서 보다 큰 의미를 갖는다. 다만,

---

[88] 박노형·정명현, supra note 16, pp.70-71.

[89] 제3차 UN정부전문가그룹 회의는 2012년 개최되었으며 2013년 6월 최종 보고서 채택에 합의하였다. UNGA, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98/AR (2013) (이하 UNGA 제3차 보고서)

[90] UNGA 제3차 보고서, p.2.

[91] 장규현·임종현, "국제 사이버보안 협력 현황과 함의: 국제안보와 UN GGE 권고안을 중심으로.", 『정보통신정책연구』, 제26권 제5호 (2014), p.40.

II. 사이버 공간에 적용되는 국제법의 논의 과정 – UN GGE와 탈린매뉴얼

앞서 확인한 바와 같이 사이버 공간에 적용되는 국제법에 관한 논의 과정에서, 서방과 비서방 진영의 부분적 견해 차이가 존재함에도 불구하고 기존의 국제법이 사이버 공간에도 적용될 수 있다는 전반적인 시각에 대해서는 제3차 UN 정부전문가그룹의 회의를 기점으로 하여 합의에 이르렀다고 판단된다. 상술한 바와 같이 제3차 UN 정부전문가그룹의 회의에서는 국제법, 특히, UN 헌장과 그로부터 파생되는 국제법의 일반 원칙들이 사이버 공간에도 적용될 수 있음이 명시되어 있다.[92] 즉, 국제법의 구체적인 적용 원칙과 발동요건 등의 세부적인 측면에 있어서는 여전히 국제사회의 추가적인 논의를 필요로 하지만, 사이버 공간에서도 기존의 유엔헌장을 비롯한 기본적인 국제법 체계가 적용된다는 사실 자체에 대해서 만큼은 양 진영 간 합의에 도달한 것으로 볼 수 있다.[93]

한편, 오늘날 사이버 공간에서의 국제법 적용에 대한 논의는 국제기구 및 다자지역기구 등 여러 층위에서 이루어지고 있다. 가령, 국제기구의 차원에서는 UN에서의 논의가 대표적이며, 다자지역기구의 차원에는 유럽연합(이하 EU), 북대서양조약기구(이하 NATO), SCO 등에서의 논의가 활발하게 이루어지고 있다. 그 중에서도 NATO 산하의 탈린매뉴얼 국제전문가그룹과 UN 제1위원회 산하의 정부전문가그룹(GGE)에서 사이버 공간에 적용되는 국제법 및 사이버 안보에 관한 가장 활발한 논의가 이루어지고 있다. 탈린매뉴얼을 집필한 국제전문가그룹과 UN 정부전문가그룹은 사이버 공간에 전통적인 국제법이 적용된다는 전제에 기반하여 논의를 진행한다는 측면에서 유사하나, 구체적 쟁점에 따라 적용상 견해의 차이 역시 적지 않게 존재한다. 탈린매뉴얼과 UN 정부전문가그룹의 회의보고서는 오늘날 사이버 공간에 적용될 국제법에 대해 논함에 있어서 가장 핵심적인 지침서로 여겨진다. 아래에서는 양 그룹에서 이루어지는 논의를 바탕으로 사이버 공간에 적용되는 국제법에 대하여 검토하고자 한다.

---

[92] UNGA 제3차 보고서, p.2.

[93] 유준구, supra note 72, p.151.

1. 탈린매뉴얼(Tallinn Manual)

1) 논의의 배경

지속적으로 발생하는 사이버 공격에 대응하여 국제사회는 이러한 불법적인 사이버 조작 등을 규율하는 법적 기초를 마련하기 위한 노력을 기울여 왔다. 이러한 논의는 2007년 에스토니아에 대하여 행해진 광범위한 DDoS 공격을 계기로 더욱 가속화 되었다. NATO는 에스토니아에 대한 사이버 공격을 계기로 NATO 사이버방위센터(NATO CCD COE: Cooperative Cyber Defence Centre of Excellence)를 설립하고 사이버 규범을 수립하기 위한 전문가그룹을 구성함으로써 사이버전에 대한 법적 규제와 규범의 마련에 상당한 노력을 기울였다.[94] 그 결과 2013년 최초의 '탈린매뉴얼'(Tallinn Manual)이 채택되었으며, 2017년에는 사이버 작전 상황에 적용되는 국제법에 관한 '탈린매뉴얼 2.0'이 발표되었다.[95] 2013년에 발간된 '탈린매뉴얼 1.0'이 사이버 전쟁(cyber warfare)에 적용 가능한 국제법 규범을 위주로 서술되었다면, 2017년에 발표된 탈린매뉴얼 2.0은 평시의 사이버 활동에도 적용되는 국제법에 관해 다룸으로써 탈린매뉴얼 1.0에 비하여 적용 범주가 더욱 확대된 것으로 볼 수 있다.[96]

2) 국제법의 적용에 대한 시각

탈린매뉴얼의 집필에 참여한 국제전문가그룹은 일차적으로 현존하는 국제규범이 사이버 공간에 어떠한 방식으로 적용되는지에 대하여 결정하고, 그로

---

[94] 이민효, "사이버전에 적용될 국제법에 관한 Tallinn Manual 고찰", 『인도법논총』, 제37호 (2017), pp.13-15.

[95] 탈린매뉴얼 2.0은 19명의 국제법 전문가가 작성한 문서로 2013년 Tallinn Manual의 채택을 이끌었던 Michael Schmitt가 책임을 맡았다. 탈린매뉴얼 2.0은 국가가 일상적으로 직면하는 보다 일반적인 사이버 사고에 관한 법적인 분석을 포함한다.

[96] 신경수·신진, supra note 57, pp.38-39.

인한 사이버 영역 특유의 법적 측면을 규명하고자 노력하였다.[97] 그리고 이러한 고민의 결과물인 탈린매뉴얼은 '존재하는 법'(lex lata), 즉 '현존하는 국제법'이 사이버 공간에서 펼쳐지는 새로운 형태의 전투에 적용되는 방법에 대한 논의를 담고 있다.[98] 기존의 국제법이 사이버 공간에서도 적용된다는 국제전문가그룹의 기본적인 시각은 탈린매뉴얼의 구체적인 조항을 통해 보다 구체화된다. 가령, 탈린매뉴얼의 Rule 1에서는 '국가 주권'의 원칙이 사이버공간에서도 적용된다는 점이 명시되어 있다.[99] 탈린매뉴얼에서는 동 조항의 주석을 통해 주권이 국제법의 근본 원칙이며, 사이버 공간의 물리적, 논리적 및 사회적 차원 모두가 당해 원칙으로 포섭된다는 점을 확인하였다.[100] 실제로 다수의 국제법 조약, 국제관습법 그리고 국제법의 일반원칙이 국제법상 주권의 원칙으로부터 유래한다는 사실을 고려할 때 오늘날 국제사회의 근간이 되는 주권의 원칙이 사이버 공간에서도 적용된다는 점을 확인한 것은 사이버 공간에서의 국제법 적용가능성의 측면에서 상당한 의의를 갖는다.

탈린매뉴얼은 본 연구의 핵심적 논의 대상인 '상당주의 의무'의 정의를 ICJ의 Corfu Channel 사건의 판결로부터 차용하고 있으며 상당주의 의무 역시 국제법상 주권 개념으로부터 파생되는 원칙으로서, 국가에게 "[자국의] 영토 내에서 다른 국가의 권리를 보호할 것"을 요구한다는 점을 확인하고 있다.[101] 이외에도 탈린매뉴얼은 사이버 작전과 관련한 규정에 대하여 논하는 과정에서 대부분의 기존 국제법을 수용하는 모습을 보이고 있다. 탈린매뉴얼에는 국가책임법 (제4장), 국제인권법 (6장), 외교 및 영사관계법 (7장), 해양법 (8장), 우주법 (10장), 국제전기통신법 (제11장) 등이 "개별 국제법 체계와 사이버 공간 (제2부)" 아래에서 논의되고 있다. 또한 "국제평화 및 안전과 사이버 활동" (제3부)에서는 분쟁의 평화적 해결, 간섭의 금지, 무력사용의 금지, 자위권, 집단 안보 등에 대하여 본격적으로 논의함으로써 유엔 헌장에서 규

---

[97] 이민효, supra note 94, p.26.

[98] Ibid; Michael N. Schmitt, 탈린매뉴얼 2.0: 사이버 작업에 적용되는 국제법, 국가보안기술연구소 편역, 박영사, 2018, p.1.

[99] 탈린매뉴얼 2.0, Rule 1.

[100] 탈린매뉴얼 2.0, Rule 1(1),(3),(4) 각각 참조.

[101] 탈린매뉴얼 2.0, Rule 6(2).

정한 내용을 대부분 수용하고 있다.[102] 또한 전투수단과 방법을 규율하는 제4장에서는 전반적으로 헤이그 법의 계열을 수렴한 것으로 볼 수 있으며, 일정한 사람, 물건, 활동의 보호에 관한 제5장의 경우 제네바 법 계열을 수용한 것으로 볼 수 있다.[103]

2. 정부전문가그룹 (Group of Governmental Experts: GGE)

1) GGE 설립의 배경

1998년 러시아는 유엔 총회(UN General Assembly)의 제1위원회에 정보안보 사안에 관한 결의안의 초안(draft resolution)을 제출하였다. 제1위원회는 국제 안보와 관련한 의제를 다루는데, 구체적으로 핵무기 감축, 핵확산 금지, 군비 경쟁, 불법 무기 거래 등에 대한 국가들의 행위를 논의한다.[104] 러시아가 제출한 결의안 초안은 별도의 표결 없이 유엔 총회에서 받아들여졌으며,[105] 2004년에 사이버 안보와 관련한 정부전문가그룹(Group of Governmental Experts, GGE)이 설치되었다. 정부전문가그룹은 UN에서 사이버 안보 논의가 총회의 고정적 의제로 채택되었음에도 불구하고 실질적인 논의에는 별다른 진척이 없다는 문제의식에 기반하여 고안되었다.[106] 초창기의 UN 정부전문가그룹은 러시아가 주도하였는데, 러시아는 UN 정부전문가그룹에서의 논의를 통해 사이버 공간을 규율하는 국제 담론이 한층 심화된 수준에서 이루어질 수 있을 것으로 기대하였다.[107]

---

[102] 신경수·신진, supra note 57, p.39.

[103] 이민효, supra note 94, p.27.

[104] Resolution on "Developments in the Field of Information and Telecommunications in the Context of International Security", UN Doc. A/RES/53/70, (1999).

[105] Francois Delerus, Cyber Operations and International Law, (Cambridge University Press, 2020), p.14

[106] 김소정 · 김규동, "UN 사이버안보 정부전문가그룹 논의의 국가안보 정책상 함의", 『정치정보연구』, 제20권 제2호 (2017), p.94.

[107] Rahul Prakash & Darshana M. Baruah, supra note 37, p.2.

2) UN 정부전문가그룹(GGE) 보고서 및 국제법 적용 가능성

탈린매뉴얼과 차별화되는 유엔정부전문가그룹의 가장 큰 의의는 글로벌 다자주의의 대표적인 기구인 UN 산하에서 주권 국가를 주도로 사이버 안보와 국제법의 적용 가능성에 관한 논의가 이루어진다는 점이다. 국제법의 주체는 원칙적으로 주권 국가라는 점을 고려할 때 사이버 공간을 규율하는 규범에 대한 각국의 의견을 표명하고 이를 국제사회 전반의 맥락에서 종합하는 것은 그 자체로 상당한 의미를 가진다.[108] 이러한 논의 과정은 향후 국제 사이버 법리의 형성에 큰 영향을 미칠 것으로 기대된다.[109] 다만 전술한 바와 같이 사이버 공간을 규율하는 방안을 논의하는 과정에서 진영 간 대립 국가 간 의견의 차이 및 충돌은 꾸준히 존재해 왔다. 특히 주요 강대국은 물리적 공간에서의 패권 관계를 사이버 공간에서 연장하거나 혹은 이를 저지할 것인지를 국가의 사활적 이익으로 여기는 경향이 있었다.[110] 이와 같은 대립에 기한 어려움은 총 6차례 이루어진 GGE 회의와 그 결과물에도 드러난다. GGE는 총 6차례의 논의를 진행하였고, 2차, 3차, 4차 그리고 6차 그룹에서 합의 보고서를 도출하였다.[111] 제1차와 제2차 GGE에서는 주요 이해당사국 간 입장 차이를 확인하였으며 유의미한 결과를 도출하지 못하였다.[112] 특히 제2차 GGE에서는 미국과 EU 등의 서방 진영과 러시아와 중국 등의 비서방 진영의 입장차이를 확인하였으며, 무엇보다도 사이버 공간을 바라보는 양 진영의 시

---

[108] 김소정 · 김규동, supra note 106, pp.92-93.

[109] GGE 회의에 참여하는 회원국은 외교적으로 매우 민감하고 국가 안보와 관련한 논의를 진행하므로 더욱 폐쇄적이다. 자연스럽게 GGE는 정치적 색채를 강하게 띠며 종종 글로벌 강대국의 정치를 대변하는 경향이 있다는 견해도 존재한다. 유인태, "경쟁적 사이버 안보 다자주의의 출현", 『국제정치논총』 제62집 제1호 (2022), pp.165-166 참조.

[110] 김소정 · 김규동, supra note 106, p.95.

[111] UN 정부전문가그룹 회의는 총 6차례 개최되었다. 회의가 이루어진 시기는 다음과 같다. 제1차(2004-2005), 제2차(2009-2010), 제3차(2012-2013), 제4차(2014-2015), 제5차(2016-2017), 제6차(2019-2021).

[112] Eneken Tikk-Ring, "Developments in the field of information and telecommunication in the context of international security: work of the un first committee 1998-2012", ICT peace Foundation (2012), pp.9-10.

각 자체에서 근본적인 차이가 있다는 점을 재확인 하였다.[113] 다만 제2차 GGE에서는 향후의 회의에서 다루어야 할 의제의 범위를 설정함으로써 이후의 GGE 활동을 위한 근간을 마련하였다는 데에서 부분적인 의의를 찾을 수 있을 것이다.

국제법의 적용과 관련하여 주목할 만한 성과가 있었던 것은 제3차 GGE의 합의 내용이다. 2012년 개최되어 2013년 6월에 마무리 된 제3차 GGE에서는 사이버 공간에서의 국가행위에 대하여 기존의 국제법과 국가 주권의 원칙이 적용된다는 점을 처음 확인함으로써 국제사회에 큰 반향을 일으켰다.[114] 기존 국제법의 사이버 영역에서의 적용 가능성 여부는 서방과 비서방진영이 가장 첨예하게 대립하는 지점이었기 때문이다.[115] 이에, 제3차 GGE에서는 기존 국제법의 사이버공간에 대한 적용 가능성을 전반적으로 긍정하되, 사이버 공간의 특성을 고려할 때 새로운 규범이 필요로 하는 사각지대가 존재할 가능성을 인정하였다.[116] 즉, 제3차 GGE는 기존의 규범이 사이버 공간에서 적절하게 활용되기 위한 국제사회의 추가적 연구와 합의를 요구하는 수준에서 타협이 이루어진 것으로 볼 수 있다.[117] 제4차 GGE에서는 제3차 GGE에서의 합의를 바탕으로 보다 구체적인 적용 방안을 도출하기 위해 노력하였다. 제4차 보고서에서는 제3차 보고서에서 사이버 공간에 국제법이 적용된다는 점을 언급한 내용과 함께 국제법이 ICT의 활용되는 방안에 대해서도 보다 상세히 논함으로써 제3차 GGE 보고서에 비하여 진전된 내용을 담은 보고서가 제

---

[113] 김소정 · 김규동, supra note 106, p.96.

[114] Ibid., p.97.

[115] Ibid.

[116] UNGA 제3차 보고서, p.2. 원문은 다음과 같다. (… Given the unique attributes of ICTs, the report notes that additional norms could be developed over time. The report reflects the Group's conclusion that international law and in particular the United Nations Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.)

[117] UNGA 제3차 보고서, p.2.; 김소정 · 김규동, supra note 106, p.96.

70회 UN 총회의 본회의에서 채택되었다.[118] 제4차 GGE의 가장 두드러진 특징 중 하나는 국제사회에 대해 구속력을 갖는 '국제법'의 영역과 국가의 자발적인 참여를 요하는 '비구속적이고 자발적 규범'의 분야를 구분하여 논의하였다는 점이다.[119]

이후 2016년부터 2017년 까지 이루어진 제5차 GGE에서 당사국은 최종 보고서 채택에 실패하였다. 5차 GGE에서 가장 큰 이슈가 된 의제는 국제 안보의 차원에서 국가의 사이버 행위를 국제법에 적용하는 방안과 관련한 것이었다.[120] 양 진영은 국제인도법의 원칙의 사이버 공간 적용 가능성, 사이버 범죄 및 테러에 대응하기 위한 별도의 국내법 제정의 필요성, 그리고 사이버 안보를 국제적 거버넌스의 일부로 규정할 필요성의 측면에서 대립하였다. 이들은 결과적으로 입장의 차이를 극복하지 못하고 최종 보고서 채택에 실패하였다.[121] 유엔 헌장의 내용을 사이버 공간에 적용됨을 선언하는 제3차 GGE 보고서가 채택됨으로써 서방과 비서방 세력 간의 의견 대립이 좁혀지는 듯하였으나, 여전히 글로벌 사이버 안보 규범의 수립에 자국의 이익을 반영하고자 하는 기본적인 태도가 견지되고 있음을 확인할 수 있는 대목이다. 가장 최근의 제6차 GGE 회의는 2021년 5월 28일 총의(consensus)로 최종보고서를 채택하였다.[122] 이는 제5차 GGE 보고서의 최종 채택이 불발 된 이후 채택된 보고서라는 점, 그리고 사이버 공간에 적용되는 국제법에 관한 합의

---

[118] UNGA, Resolution on “Developments in the field of information and telecommunications in the context of international security”, UN Doc. A/RES/70/237 (2015); 박노형 · 정명현, “제4차 정보 안보에 관한 유엔정부전문가그룹 논의 분석과 국제 사이버법의 발전 전망”, 『국가전략』, 제22권 제3호 (2016), p.178.

[119] 김소정 · 김규동 supra note 106, p.100.

[120] 유인태, "경쟁적 사이버안보 다자주의의 출현", p.170.

[121] Ibid., pp.162-163; Michael Schmitt & Liis Vihl, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms", Just Security (30 June 2017), (2023.7.27 최종방문)

[122] UNGA, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/76/135 (2021), (이하 UNGA 제6차 보고서); 박노형 · 박주희, "제6차 UNGGE 보고서 채택과 국제사이버법의 발전", 『국제법학회논총』, 제66권 제3호 (2021), p.174.

에서 상당한 진전을 이루었다는 점에서 큰 의미가 있다. 제6차 GGE 최종보고서의 가장 큰 특성은 참가국으로 하여금 사이버 공간에 적용되는 국제법에 관한 자국의 국가실행을 제출할 것을 요구하였다는 점이다.[123] 제출된 국가실행에서 다수의 국가들이 본 연구에서 다루어지는 상당한 주의의무에 대한 많은 관심을 보였다. 이 부분의 상세한 내용에 대해서는 후술하기로 한다.

UN 총회는 2021년 7월 13일까지 제출된 국가실행을 통합한 문서인 '자발적 국가 기여의 공식 컨펜디엄 (Official compendium of voluntary national contributions, 이하 컨펜디엄)'을 회람하였다.[124] 자발적 국가 기여를 통해 국가의 실행에 대한 제출을 요구하는 것은 제5차 GGE의 최종보고서 채택이 불발된 것에서 기인한다. 2017년 제5차 GGE는 어떠한 국제법이 사이버 공간에 적용될 수 있는지에 관한 진영 간 대립으로 인하여 논의가 계속적인 답보 상태에 머물렀으며 그 결과, 최종 보고서 채택 역시 무산되었다.[125] 최종 보고서 채택의 불발은 사이버 공간을 바라보는 국가 간 인식 차이를 쉽게 좁히기 어렵다는 것을 의미한다. 제6차 GGE 보고서에 포함되는 국가들의 '자발적 국가 기여'는 사이버 공간에 적용되는 각국의 실행을 자발적으로 공개하고 이러한 실행을 다른 국가가 열람할 수 있도록 유도한다. 이를 통해 사이버 공간을 바라보는 시각과, 사이버 공간에 적용되는 규범에 관한 국가 간 입장 차이를 조율할 수 있을 것으로 기대된다. 또한 정부전문가 그룹에서 자발적 기여의 형식을 채택한 것은 기존의 국제법이 사이버 공간에 적용될 수 있다는 대전제 하에 사이버 공간을 규율하는 규범에 관한 논의를 이어가고자 하는 국제사회의 의지를 보여주는 대목이기도 하다.

---

[123] 박노형 · 김효권, supra note 7, p.62.

[124] 컨펜디엄 문서의 공식 명칭은 다음과 같다. Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, UN Doc. A/76/136 (2021).

[125] Michael Schmitt & Liis Vihl, supra note 121.

III. 소결

이상의 논의를 종합하면, 사이버 공간의 행위 규율에 관한 가장 핵심적인 논의가 이루어지는 국제전문가그룹과 UN의 정부전문가그룹에서는 사이버 공간에 대하여 기존의 국제법을 적용하는데 전반적으로 긍정적인 입장을 취하고 있음을 확인할 수 있다. 물론 정부전문가그룹의 내에서 서방과 비서방 진영 간의 꾸준한 의견 대립이 존재해 왔으나, 사이버 공간에 현존하는 국제법이 적용된다는 기본적인 골격에 대해서는 합의에 이른 것으로 볼 수 있다. 탈린매뉴얼 역시 기본적으로 국제법의 사이버 공간의 적용가능성에 자체에 대해서는 긍정하는 입장이다. 물론 탈린매뉴얼은 NATO 회원국의 입장을 대변하거나 국제사회의 공식적인 문서로 인정받지 못한다는 점에서 한계가 있다. 그러나 사이버 안보와 관련한 논의에 있어 국제사회에서 탈린매뉴얼이 갖는 권위를 고려할 때, 탈린매뉴얼이 취하는 입장은 사이버 공간에서의 국제법을 논함에 있어 유의미한 지침서가 될 수 있을 것이다.

사이버 공간은 전통적인 국제법이 적용되어 온 물리적 공간과는 여러가지의 측면에서 상이하다. 그러나 이러한 기본적인 차이에도 불구하고 더이상 사이버 공간은 물리적 공간과 완전히 분리되는 '가상의 영역'으로 분류되지 않는다. 국제법의 근간이 되는 국가 주권과 그로부터 파생되는 국제법의 원칙을 사이버 공간에 적용하고자 하는 시도는 사이버 공간을 바라보는 인식이 변화하였음을 보여주는 대표적인 결과물이라고 할 수 있다. 물론 사이버 공간의 특이성을 고려할 때 기존의 국제법이 적용되는 구체적인 방식과 범위에 있어서는 국제사회의 지속적인 논의가 필요하다고 할 것이다. 그럼에도 불구하고 기존의 국제법을 사이버 공간에 적용하고자 하는 큰 틀에서의 합의는 사이버 공간을 바라보는 국제전문가그룹과 UN 정부전문가그룹의 기본적인 입장이며, 이러한 시류는 앞으로의 국제사이버 법리의 발전 방향에도 큰 영향을 미칠 것으로 생각된다.

제 3 장. 사이버 공간과 국가책임법의 한계

사이버 공간과 국제법에 대한 국제사회의 논의는 전통적인 국제법을 새롭게 대두한 영역인 사이버 공간에도 적용하는 것으로 수렴하고 있다. 특히, UN 정부전문가그룹의 제3차 회의에서는 '국제법 및 특히 UN헌장'(International law, and in particular the Charter of the United Nations)이 사이버 공간에도 적용됨을 총의로 합의하였다. 이와 같은 사이버 공간에서의 국제법의 적용 가능성은 NATO와 G20 등에서도 지속적으로 확인되고 있다.[126] 그러나 사이버 공간에는 물리적 공간을 전제한 그간의 논의 영역과는 명백하게 차별화되는 특성이 존재한다. 따라서 기존의 국제법을 사이버 공간에 적용하고자 하는 국제사회의 합의에도 불구하고 여전히 크고 작은 적용상의 어려움이 존재한다. 가령, 사이버 공간에 국가의 '주권' 개념이 적용된다는 점에 대해서 합의하였으나, 여전히 국가 간 견해 차이로 인해 국제사회에서는 '주권 침해의 임계점' 혹은 '사이버 공간에서의 주권의 지위' 등에 대한 명백한 합의를 이루지 못하고 있다. 실제로 제6차 GGE 보고서는 국가의 주권 존중에 대해서는 다수 언급하지만, 정작 사이버 공간에서 주권의 국제법상 지위에 대해서는 언급하지 않는다.[127] 또한, 국제위법행위에 대한 '집단적 대응조치'(collective countermeasures)가 사이버 공간에서 허용되는지 여부에 대한 국가 간 이견이 존재함에 따라 사이버 공격 결과에 대한 대응조치와 관련한 국제사회의 논의 역시 순조롭지 못한 상황이다.[128] 이처럼 기존의 국제법을 사이버 공간에 적용하는 과정에서 구체적인 쟁점에 대하여 여전히 국제사회의 공통된 이해가 마련되지 못하고 있는 실정인 것이다.

기존 국제법을 사이버 공간에 적용함에 있어서 발생하는 여러가지의 어려

---

[126] 박주희, "UNGGE의 자발적 규범과 국내 사이버안보법제", 한국법제연구원, Vol. 1 (2022), p.2.

[127] 박노형 · 박주희, supra note 121, pp.186-187.

[128] 가령, 에스토니아는 사이버 공격에 대한 집단적 대응조치를 긍정한다. 그러나 가장 대표적으로 프랑스의 경우 국제법적 대응조치는 '스스로의 역량'에 의해 이루어져야 한다는 점에서 사이버 공간에서의 집단적 대응조치에 대하여 부정적인 견해를 취한다. 박노형 · 박주희, supra note 121, p.191 참조.

움 가운데, 아래에서는 특히 '국가책임법'을 사이버 공간에 적용하였을 때 발생하는 한계에 대하여 상세하게 다루고자 한다. 사이버 공격의 특수성은 유책국에 대한 국가책임을 추궁함에 있어서 상당한 현실적, 기술적 어려움을 유발한다는 것은 앞서 확인한 바와 같다. 본 연구에서 주목하고자 하는 사이버 공간에서의 '상당주의 의무'의 중요성 역시 사이버 공간에서는 국가책임법의 적용이 용이하지 않다는 점에 기인하는 것이라고 할 수 있다. 따라서, 이하에서는 기존 국제법의 여러가지 영역 가운데 '국가책임법'을 사이버 공간에 적용하였을 때 발생하는 적용상의 한계에 대해 중점적으로 살펴보기로 한다. 보다 구체적으로, 전통적인 국가책임법의 정의 및 성립 요건과 함께 국가책임법을 사이버 공간에 적용함에 있어서 어떠한 현실적 어려움이 발생하는지에 대하여 다룬다.

I. 국가책임법

1. 정의 및 의의

국제법상 '국가책임'(State responsibility)은 국가의 '국제위법행위'(internationally wrongful act)에 대한 책임을 다루는 내용으로, 국제법 질서의 중심을 이루는 논의이다.[129] 오늘날 국가책임에 관한 논의는 UN 국제법위원회(UN International Law Commission, 이하 'ILC')가 2001년에 성안한 '국제위법행위에 대한 국가책임 초안'(2001 ILC's Draft Articles on Responsibility of States for Internationally Wrongful Act, 이하 ILC 국가책임 초안)을 중심으로 이루어진다.[130] ILC 국가책임 초안은 구속력 있는 조약의 형태가 아닌 '가이드라인(지침)'에 불과하다는 한계가 있으나 동시에 복잡하고 대립적인 국가책임에 대한 원칙을 종합적으로 정리함으로써 국제법의 성문화

[129] James Crawford & Simon Olleson, The Nature and Forms of International Responsibility, in Malcolm D. Evans(ed), International Law (Oxford University Press, 2003), p.449.

[130] 정인섭, supra note 44, p.408.

에 기여하고 있다는 평가를 받기도 한다.[131] 또한 ILC 국가책임 초안의 조항은 다수의 국제재판소의 판례에서 직간접적으로 인용되고 있으며 국가의 실질적인 관행에도 큰 영향을 미치고 있다. 즉, 오늘날 ILC 국가책임 초안은 국가의 행위를 규율하고 지도하는 지침으로서의 권위를 확보하였다고 볼 수 있다.[132]

2. 국가책임 성립 요건

ILC 국가책임 초안은 국제법상 국가책임이 성립하기 위한 요건으로 두가지를 제시하였다. ILC 국가책임 초안 제2조의 원문은 다음과 같다.

> Article 2: Element of an internationally wrongful act of a State.
> There is an internationally wrongful act of a State when conduct consisting of an action or omission:
> (a) is attributable to the State under international law; and
> (b) constitute a breach of an international obligation of the State.

ILC 국가책임 초안 제2조로부터 확인할 수 있는 것처럼 국제법상 국가책임이 성립하기 위해서는 우선 문제된 행위의 국가로의 귀속(attributable to the State)이 인정되어야 하며, 당해 행위가 '국제 의무'(international obligation)를 위반할 것이 요구된다. 한편 고의 및 과실의 여부가 국가책임 성립의 요건이 되는지에 대해서는 의견 대립이 있었으나, ILC 국가책임 초안의 주석서에서는 고의 및 과실의 여부를 국가책임의 독자적인 성립 요소로

---

[131] 오병선, "국가책임의 본질과 성립요건에 대한 비판적 고찰", 『국제법학회논총』, 제52권 제2호 (2007), p.210.

[132] 정인섭, supra note 44, p.408; David D. Caron, “The ILC Articles on State Responsibility: The Paradoxical Relationship Between Form and Authority”, American Journal of International Law, Vol. 96, No. 4 (2002), p.858.

보지 않았으며, 다만 피해 배상 시 이에 대하여 검토할 수 있음을 명시하고 있다.[133]

1) 국가의 행위

국가는 법적으로 추상적인 개념이므로 그 자체로 특정한 행위를 할 수 없다.[134] 즉, 국가 스스로 위법행위를 할 수 없기 때문에 국가의 책임 문제는 결국 국가의 기능을 직접적으로 수행하는 사인 혹은 단체의 작위 및 부작위로 인하여 발생하게 된다.[135] 따라서 사인 및 단체의 특정한 행위가 국가의 행위로 귀속되는지 판단하는 것은 국가책임을 추궁하기 위해 해결되어야 할 선결적인 과제라고 할 수 있다. ILC 국가책임 초안의 제2장 제4조부터 제11조까지는 특정한 행위가 국가로 귀속되기 위한 기준에 대하여 규정되어 있다. 구체적으로는 국가 기관(state organ)의 행위(제4조), 정부권한을 행사하도록 권한을 위임 받은 자의 행위(제5조), 권한 초과 혹은 지시위반 행위(제7조), 국가에 의하여 감독되거나 통제된 행위(제8조), 공적기관의 부재 또는 직무수행이 불가능한 상태에서 수행된 행위(제9조), 반란단체 또는 다른 단체의 행위(제10조), 국가에 의하여 자국의 행위로 추인 된 행위(제11조)는 ILC 국가책임법 초안의 제2장에 명시된 바에 의하여 국가의 행위로 귀속된다.

2) 국제의무의 위반 (breach of an international obligation)

국가책임이 발생하기 위해서는 우선 '국가의 국제의무 위반'(breach of an international obligation)이 존재하여야 한다. ILC 국가책임 초안의 제3장의 제12조에서 제15조까지는 국제의무의 위반에 대하여 다루고 있다. 이

---

[133] Report of the International Law Commission on the work of its fifty-third session, 23 April - 1 June and 2 July - 10 August 2001, Official Records of the General Assembly, Fifty-sixth session, Supplement No.10,A/56/10 (2001), p.108. (이하 'ILC 국가책임초안')

[134] James Crawford & Simon Olleson, supra note 129, p.454.

[135] ILC 국가책임초안 제2조, cmt. 5, p.35; ibid., pp.453-454 참조.

때 국제의무는 국제법의 연원인 조약이나 관습은 물론 그 밖의 연원으로부터 발생할 수 있으며, 국가의 행위가 국제의무에 의해 당해 국가에게 요구되는 바와 합치하지 않을 때 국가의 국제의무 위반이 발생하게 된다.[136] 국제의무의 위반은 국가의 작위 또는 부작위를 통해 발생할 수 있으며 양자가 결합되어 발생할 수도 있다.[137]

3. 비국가행위자 (Non-State actor) – 국가의 행위로 귀속 (제8조)

국가책임이 성립하기 위해서 문제되는 행위가 '국가'로 귀속되어야 함은 앞서 확인한 바와 같다. 원칙적으로 사인이나 민간단체의 행위는 국제법상 국가의 행위로 귀속되지 않는다. 그러나 ILC 국가책임 초안에서는 공식적으로 특정 국가기관의 지위를 갖지 않은 자들의 행위임에도 불구하고 당해 행위를 국가의 행위로 귀속할 수 있는 특수한 상황들에 대해서 열거하고 있다.[138] 그 중에서도 ILC 국가책임 초안 제8조에 명시된 '국가에 의하여 감독되거나 통제되는 행위'를 국가의 행위로 귀속시키는 데 있어서는 보다 복잡한 판단이 요구된다.[139] 즉, 국제의무에 대한 위반행위가 의심의 여지없이 명백하게 '국가'의 행위로 귀속되는 경우에는 전혀 문제될 것이 없으나, 사인과 국가가 특수한 관계에 있기 때문에 당해 행위가 국가에 귀속되는 경우는 보다 어려운 판단을 요하는 것이다. 가령, 국가기관이 자국의 목적을 달성하기 위하여 민간인을 경찰이나 군대의 보조원(auxiliary)으로 활용하거나, 개인이 특수한 임무의 수행을 위하여 외국에 보조원(volunteer)의 신분으로 파견되는 경우가 이에 해당할 것이다.[140] 이처럼 행위의 귀속성에 있어 국가의 감독

---

[136] 오병선, supra note 131, p.215.

[137] 정인섭, supra note 44, p.423.

[138] ILC 국가책임초안 제8조, 제9조, 제10조, 제11조.

[139] ILC 국가책임초안 제8조 원문은 다음과 같다. "Conduct directed or controlled by a State: The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."

[140] ILC 국가책임초안, p.47. 정인섭, supra note 44, p.415.

과 통제를 고려하는 것은 곧 국가와 사인 간의 현실적 연관성(real link) 혹은 구체적 사실 관계(specific factual relationship)를 고려하는 것으로 볼 수 있다.[141]

이때 주의해야 할 것은 사인 및 민간단체의 등 비국가행위자의 행위를 국가의 행위로 귀속함에 있어서는 이들이 국가의 "지시"(instruction)에 의하거나 혹은 "감독 또는 통제"(direction or control)에 따라 행동하였을 것이 전제되어야 한다는 사실이다.[142] 그렇다면 해당 행위를 국가의 행위로 귀속하기 위한 통제의 임계점은 어느 정도인가? 다시 말해, 국가가 어느 정도의 통제권을 행사한 경우까지 비국가행위자의 행위를 국가에 귀속시킬 수 있는가에 대한 의문이 제기되는 것이다. 아직까지 통제의 기준과 관련하여 확립된 관습국제법은 존재하지 않는다. 다만, 책임의 귀속을 논의함에 있어 국제법상 요구되는 통제의 정도에 대하여 다수의 판례와 학설이 존재하는 바, 이는 크게 '실효적 통제'(effective control)의 기준과 '전반적 통제'(overall control)의 기준으로 나뉜다.[143] ICJ는 Nicaragua 사건[144]에서 Contra 반군의 행위를 미국으로 귀속할 수 있을지에 대한 여부를 판단함에 있어서 실효적 통제의 기준을 활용하였다. 이후 ICTY는 Tadic 사건[145]에서 행위기준으로 전반적 통제의 기준을 제시한 바 있으나, 그 이후 Bosnian Genocide 사건[146]에서 ICJ는 전반적 통제가 아닌 실효적 통제의 기준을 다시금 적용하였다. 책임귀속에 필요한 통제의 정도로서 '실효적 통제'는 '전반적 통제'에 비하여 비교

---

[141] ILC 국가책임초안 제8조, cmt 1, p.47.

[142] ILC 국가책임초안 제8조, cmt 3, p.47.

[143] 정인섭, supra note 44, pp. 415-418; 김보연, "인공지능의 국제법상 책임추궁에 관한 소고", 『경희법학』, 제57권 제4호 (2022), pp. 189-191.

[144] Military and Paramilitary Activities in und against Nicaragua (Nicaragua v. United State of America), Merits, Judgment. I.C.J. Reports 1986, pp.62-65, paras. 109-115.

[145] Prosecutor v. Dusko Tadić (IT-94-1), ICTY, Appeals Chamber, Judgement of 15 July 1999, para.131.

[146] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p.43, para. 39.

적 더 엄격한 기준을 채택하고 있다. 오늘날 다양한 비국가행위자 등장을 비롯한 국제사회의 변화를 고려하여 보았을 때 '전반적인 통제'의 기준을 채택하는 것이 더 타당하다는 의견이 지속적으로 제기되었으나 국가의 자율성에 기한 책임주의를 채택하는 ICJ는 국가책임법상의 '실효적 통제'의 법리를 고수하고 있는 것으로 보인다.[147]

III. 사이버 공간에서 국가책임법 적용과 그 한계

1. 사이버 공격의 특성 - 비국가행위자의 대두 및 공격의 익명성

국가책임법을 사이버 공간에서 적용하는 것의 어려움은 "사이버 공격의 특수성"에 따른 귀속(attribution)의 어려움에 기인한다. 사이버 공격의 대표적인 특성은 1) 직접적인 사이버 공격 수행자의 상당수가 '비국가행위자'이며 이러한 비국가행위자의 공격 행위에 국가가 다양한 방식으로 '연루'된다는 점, 2) 재래식 공격과는 다르게 사이버 공격은 매우 복잡한 양태를 띄고 있다는 점으로 요약할 수 있을 것이다. 국가책임법상 귀속의 문제는 기본적으로 그 증명이 상당히 어려운 것이 사실이지만, 이러한 어려움은 사이버 공간의 특성으로 인해 더욱 심화된다.[148]

오늘날 사이버 공간에서의 국가책임에 대한 상당수의 논의는 '비국가행위자(non-state actor)가 행한 사이버 공격을 특정 국가로 귀속할 수 있는가'로 귀결된다. 최근의 이러한 논의 추세는 국가가 자행하는 사이버 공격과 개인이 저지른 사이버범죄 간 경계가 모호하고, 또한 비국가행위자가 행하는 사이버 공격의 배후에 여하한 방식으로 국가가 개입되거나 연루되었다고 추정되는 경우가 상당수 존재하기 때문이다.[149] 실제로 최근 급증하고 있는 사이버 위협의 추세 중 하나는 국가가 배후에 있는 사이버 공격 현상의 증대이

---

[147] Antonio Cassese, International Law. (New York: Oxford University Press, 2011), pp. 650-668. 오시진, "국제테러와 국가책임법", 『강원법학』, 제37권 (2012), p.217, p.239 각각 참조.

[148] Russell Buchan, Macro Roscini & Nicholas Tsagourias, supra note 12, p.2.

[149] Sico van der Meer, supra note 49, p.1; 김효권, supra note 51, p. 295.

며, 비국가행위자의 행위에 국가가 연루되는 방식은 실로 다양하고 복잡하다.[150] 오늘날 비국가행위자를 조종하여 국가가 배후에서 공격에 관여하였거나 혹은 정황상 국가의 개입이 의심되는 사이버 공격의 구체적인 사례는 적지 않게 발견된다.[151] 에스토니아에 대한 DDoS 공격은 가장 대표적인 사례이다. 2007년 에스토니아를 상대로 행해진 대규모의 DDoS 공격은 러시아 애국주의 해커 단체에 의해 자행된 것으로 밝혀졌으나, 국제사회는 당해 공격의 배후에 러시아 정부가 있다는 점에 대해 지속적으로 의심하였다.[152] 실제로 공격에 동원된 PC의 상당수가 러시아에 위치하였으며 공격에 활용된 대표적인 PC의 IP주소 일부가 러시아 정부 기관의 것이라는 조사 결과가 발표된 바 있다. 이러한 조사 결과와 더불어 당시 양국이 극심한 정치적 갈등을 겪고 있었다는 사실을 종합적으로 고려하였을 때, 당해 공격을 단순히 애국 단체인 비국가행위자의 단독 범죄로 치부할 수 있는가에 대한 판단은 더욱 어려워진다.[153]

한편, 전술한 바와 같이 국가가 '연루된' 것으로 사이버 공격은 당해 공격의 정확한 귀속(attribution)을 위하여 피해국으로 하여금 추가적인 판단을 내릴 것을 요한다. 즉, 피해국은 비국가행위자의 공격 행위가 1) 단순한 개인 혹은 민간단체의 자발적인 동기 하에 수행된 것인지, 혹은 2) 국가의 직접적인 "지시"(instruction)에 의하거나 혹은 "감독 또는 통제"(direction or control) 하에 이루어진 행위인지에 대해 판단해야 하는 것이다.[154] 그러나 비국가행위자의 공격에 국가가 연루되는 방식의 다양성에 더불어, 사이버 공격의 또 다른 특성인 비대칭성과 '익명성 등의 복잡한 공격 양태는 양자 간의 구분을 더욱 어렵게 만든다. 오늘날 대부분의 사이버 공격은 공격자의 컴퓨터에서 목표 시스템으로 직접적으로 실행되는 형태가 아닌, 제3의 공격 거점을

---

[150] 김효권, ibid; Andraz Kastelic, "Due Diligence in the cyber space", United Nations Institute for Disarmament Research (2021), p.7.

[151] Sico van der Meer, supra note 49, p.1.

[152] Gadi Evron, supra note 4, p.124; Stephen Herzog, supra note 4, p.53; James Pamment et al., supra note 1, p.52.

[153] James Pamment et al.,ibid.

[154] 김효권, supra note 51, p.305.

두고 이루어진다.[155] 이때 제3에 설정되는 공격 거점은 공격자의 지정학적 위치를 반영하지 않는 것이 대부분인데, 이는 공격자 본인의 신분을 은닉하거나 위장하고, 공격이 포착되더라도 역추적을 어렵게 하기 위함이다.[156] 제3의 공격거점의 대표적인 형태로는 봇넷(botnet)과 C&C 서버를 들 수 있다.[157] 가령, 앞서 언급된 2007년 에스토니아에 대한 DDoS 공격 역시 IP 주소가 여러 국가 및 지역에 분포하고 있는 까닭에 공격의 근원을 찾기가 더욱 어려웠다는 평가가 존재한다.[158]

2. 귀속(attribution)의 어려움

앞서 확인한 바와 같이, 특정 행위에 대한 국가책임이 성립하기 위해서는 문제되는 행위가 국제의무에 위반되어야 함과 동시에, 해당 행위가 특정 국가의 행위로 귀속되어야 한다. 이때 사이버 공격에 대한 책임을 특정 국가에 귀속(attribute)시키기 위해서는 1) 기술의 귀속(technical attribution)에 대한 입증과 더불어 2) 인적 귀속(human attribution)이 이루어져야 하는데, 이때 인적 귀속은 다시 공격을 자행한 자에 대한 식별(행위자의 소속 국가 또는 도시)과 함께, 어떠한 배후국이 그러한 공격을 지시, 지휘 및 통제하였는가에 대한 추가적인 입증으로 나뉘게 된다.[159] 이때, ILC 국가책임초안 제8조과 ICJ Nicaragua 판결에서의 기준으로 제시되었던 실효적 통제 기준을 적용하여 귀속성을 판단한다.[160] 실효적 통제에 대한 국제사회의 통일된 정의는 없으나, Nicaragua 사건의 판시 내용에 따르면 국가가 비국가행위자의 행위를 단순히 지원 및 계획하거나 일반적으로 통제(general control)하였다

---

[155] Russell Buchan, Macro Roscini & Nicholas Tsagourias, supra note 12, p.2.

[156] 백상미, supra note 13, p.84.

[157] Ibid.

[158] Gadi Evron, supra note 4, p.123.

[159] 박노형 · 김효권, supra note 7, pp.74-75; Jawwad A. Shamsi et al., "Attribution in cyberspace: techniques and legal implications", Security and communication networks (2016), p.2889.

[160] ILC 국가책임초안 제8조, cmt. 4, p.47 참조.

는 사실만으로는 당해 행위를 국가로 귀속할 수 없다고 하였다.[161] 즉, 구체적 작업의 계획과 실행 과정을 결정하는 것이 국가이고, 비국가행위자가 행하는 것은 그러한 작업의 불가결한 부분일 때 당해 국가의 사이버 공격에 대한 '실효적 통제'가 충족된다.[162] 이를 사이버 공격의 맥락에 적용한다면 사이버 공격을 일반적으로 지지하거나 장려하는 것만으로는 실효적 통제가 성립하지 않는다.[163] 가령, 국가가 비국가행위자에게 공격을 위한 멀웨어를 제공하는데 그친다면, 비국가행위자가 해당 멀웨어를 활용하여 사이버 공격을 감행하더라도 이는 국가의 실효적 통제에 이르지 않는다.[164] 그러나, 국가가 비국가행위자에게 악성소프트웨어를 제공함에 더불어 이를 타국에 심는 작업을 계획하고 감독한다면 이러한 일련의 행위에 대해서는 국가의 '실효적 통제'가 충족된다고 볼 수 있으며, 당해 공격 행위는 국가에 귀속될 수 있다.[165]

그러나 국가가 연루된 비국가행위자의 사이버 공격 증대와 국가-비국가행위자 간의 연계 방식의 다양성, 그리고 사이버 공격의 복잡한 양태를 종합적으로 고려할 때 국가가 비국가행위자의 공격 행위를 실효적으로 통제하였음을 입증하는 것에는 상당한 현실적, 기술적 어려움이 따른다. 즉, 이를 입증하기 위해서는 사이버 공격이 국가의 주도 하에 전반적으로 계획되고 진행되었으며 그 과정에서 국가 주도의 적극적인 개입이 이루어졌음을 밝혀내야 한다. 앞서 언급되었던 2007년 에스토니아 사태에는 국가의 "실효적 통제"를 입증하여 국가책임법을 적용하는 작업의 어려움이 매우 잘 드러난다. 본 사건에 대해 러시아는 에스토니아를 상대로 감행된 DDoS 공격은 온전히 러시아의 애국주의 단체의 자의에 의해 행해진 것이며, 자국 정부의 어떠한 개입도 없었음을 강력하게 주장하였다. 이후 러시아계 에스토니아 학생이 정당의 웹사이트에 대한 공격을 감행한 사유로 기소되어 유죄 판결을 받은 바 있으나, 에스토니아 전반에 행해진 공격의 규모, 수준, 자금 지원 등의 측면을 종

---

[161] Military and Paramilitary Activities in und against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, paras.105-115.

[162] ILC 국가책임초안 제8조, cmt. 3, p.47.

[163] 탈린매뉴얼 2.0, Rule 16(8).

[164] 탈린매뉴얼 2.0, Rule 16(8).

[165] 탈린매뉴얼 2.0, Rule 16(7).

합적으로 고려할 때 단순한 단체의 소행이 아닌 국가적 차원의 배후가 존재할 가능성이 지속적으로 제기되었다.[166] 그럼에도 불구하고 에스토니아는 공격 행위에 대한 러시아 정부의 실효적 통제를 명확하고 설득력 있는 수준으로 입증하지 못하였으므로 러시아에 대한 국가책임을 추궁할 수 없었다.[167] 에스토니아에 대한 DDoS 공격 이후 국제사회는 비국가행위자의 사이버 공격에 국가가 다양한 방식으로 연루될 수 있으며, 사이버 공격의 특성 상 국가가 자국의 개입에 대하여 쉽게 부인할 수 있다는 사실에 대해서도 인식하게 되었다.[168] 실제로 국가가 연루된 것으로 의심되는 다수의 사이버 공격이 2007년 에스토니아 사태 이후에도 지속적으로 발생하였다. 따라서, 상당수의 사이버 공격이 비국가행위자에 의해 발생한다는 점과 함께 사이버 공격은 비대칭성과 익명성 등을 가장 큰 특징으로 갖는다는 점, 그리고 비국가행위자에 의하여 발생한 사이버 공격을 특정 국가로 귀속시키기 위해서는 공격에 대한 당해 국가의 실효적 통제 여부를 입증하여야 한다는 점을 종합적으로 고려할 때, 사이버 공격을 특정 국가로 귀속함에 있어서는 상당한 어려움이 따른다는 것을 확인할 수 있다.

3. 소결

오늘날 상당수의 사이버 공격은 '비국가행위자'에 의해 자행되며, 이들에 의해 행해지는 사이버 공격은 재래식 공격과는 달리 익명성, 비대칭성, 신속성 등 매우 복잡한 공격의 양태를 가진다.[169] 그리고 이러한 사이버 공격의 특성은 공격자 특정에 상당한 어려움을 야기하며 더 나아가 공격을 특정 국가로 귀속함에 있어서도 큰 어려움을 야기한다. 즉, '국가책임법'은 그간 국제사회에서 발생하는 크고 작은 갈등을 평화롭게 해결하는 가이드라인으로서

---

[166] James Pamment et al., supra note 1, p.61.

[167] Macro Roscini, supra note 2, pp.101-102.

[168] Scott J. Shackelford, "State responsibility for cyber-attacks: Competing standards for a growing problem", CCECOE Publications (2010), p.198.

[169] Russell Buchan, Macro Roscini & Nicholas Tsagourias, supra note 12, p.2.

역할을 성공적으로 수행해 왔음에도 불구하고, 사이버 공격에 대하여 국가책임법을 적용하는 것은 결코 용이하지 않다. 그러나, 국제법 상 명백히 위법한 행위에 대하여 적절한 책임을 추궁할 수 없다는 것은 그 자체로 국제법질서의 존립을 위협하게 된다.[170] 더불어, 국가책임법을 적절히 원용할 수 없다는 것은 자국을 상대로 발생하는 불법적인 사이버 공격 행위를 적절하게 대응할 수단의 부재를 의미하게 된다. 오늘날 국가는 자국의 안보를 위협하는 '사이버 공격'에 합법적으로 대응할 수 있는 실효적인 규범의 필요성에 대하여 인식하게 되었고 그 결과 오늘날 다수의 국가 및 학계는 그 대안으로 사이버 공간에서의 상당주의 의무에 주목하고 있다. 사이버 공간에서 상당주의 의무가 적용되어야 할 보다 구체적인 사유와 함께 적용상의 쟁점에 대해서는 후술하기로 한다.

[170] Russell Buchan & Nicholas Tsagourias, supra note 9, p.378.

제 3 장. 일반국제법상 상당주의 의무

제 1 절. '주권'(sovereignty)과 상당주의 의무

국제법상 상당주의 의무의 정의와 동 의무의 국제법적 지위를 논의하기에 앞서, 상당주의 의무와 불가분의 관계에 있는 '주권'(sovereignty)의 개념과 속성에 대하여 간략하게 살펴보고자 한다. 국제법상 주권의 개념은 교황의 권위에 대응하여 군주가 자국 내에서는 최고의 권위를 가진다는 대내적인 지배 질서 강화의 목적에서 재발견되었다.[171] 이후 주권 개념은 역사와 흐름과 사회적 환경의 변천 속에서 여러가지의 의미를 거치며 발전해 왔다.[172] 특히 오늘날 특수한 근대적 상황 속에서 발전한 주권은 '대외적 독립성', '대내적 최고성', 그리고 '영토성'이라는 세 가지의 특성을 갖는 것으로 이해되고 있다.[173] 즉, 주권의 이러한 특성은 '특정한 공동체 내의 최고 권위'(supremely authoritative within a territory)를 의미하게 된다.[174]

한편 베스트팔렌체제와 함께 등장한 주권 평등의 원칙은 본질적으로 '타국을 배제할 권리'(jus excludendi alios)를 내포하는데,[175] 이러한 주권의 특성은 Island of Palmas 사건의 판시 내용을 통해 보다 명확히 확인된다.[176] 필리핀 남부 해역에 위치한 Palmas 섬의 영유권이 문제가 되었던 본 사안에

---

[171] 소병천, "국제법상 주권담론에 대한 소고", 『국제법학회논총』, 제58권 제4호 (2013), p.153. 재인용.

[172] 정인섭, supra note 44, p.168.

[173] Nico Schrijver, "The changing nature of State Sovereignty", British Yearbooks of International Law, Vol. 70, Issue 1 (1999), pp.70-71; 김성주, "주권 개념의 역사적 변천과 국제사회로의 투영", 『정치외교사논총』, 제27권 제2호 (2006), p.3; 소병천, supra note 171, p.153.

[174] Daniel Philpott, "Westphalia, Authority and International Society", Political Studies (1999), p.580.

[175] Antonio Cassese, supra note 147, pp.50-51.

[176] Island of Palmas case (the Netherlands, USA), 4 April 1928, R.I.A.A. vol. II, pp. 829-871. (이하 Island of Palmas case)

서 Max Huber 중재재판관은 주권은 곧 국가 간의 관계에서 '독립'(independence)을 의미하는 것이고, 이때의 독립은 타국을 배제하고 자국의 국가 기능을 행사하기 위한 권리라는 점에 대하여 명시한 바 있다.[177] 나아가 Max Huber 중재재판관은 주권의 개념이 타국을 배제할 권리를 내포함과 동시에, 이러한 권리로부터 도출되는 필연적인 결과로서 국가로 하여금 '타국에 대한 의무' 역시 부과한다고 보았다.[178] 즉, 국가 주권의 속성인 '타국을 배제할 권리'는 모든 국가가 동일하게 보유하고 있으므로 결과적으로 국가는 자국의 주권을 향유할 권리를 갖게 됨과 동시에 타국의 주권을 존중할 의무 역시 갖게 되는 것이다.[179] 결과적으로 이는 오늘날 국제사회에서 '주권 상호 존중의 의무'의 형태로 드러난다. 주권 상호 존중의 의무는 자국의 영토 주권으로부터 파생되는 국가의 의무로서, 보다 구체적으로는 '타국의 권리를 자국의 영토 내에서 보호해야 할 국가의 의무'를 의미한다.[180] 본 연구에서 중점적으로 다루고자 하는 국제법상 '상당주의 의무'는 국가가 지니는 이와 같은 '영토 주권의 배타성' 및 '주권 상호 존중'의 의무로부터 도출되는 개념으로 이해할 수 있을 것이다.[181]

제 2 절. 상당주의 의무의 개념 및 발전 과정

I. 상당주의 의무의 개념

'상당주의 의무'(due diligence)는 우리말로 '상당주의' 또는 '상당한 주

---

[177] Island of Palmas case, p.838.

[178] Island of Palmas case, p.839.

[179] Michael N. Schmitt, "In Defense of Due Diligence in cyberspace", 125 The Yale Law Journal Forum, Vol. 68 (2015), pp.71-72.

[180] Island of Palmas case, p.839.

[181] Michael N. Schmitt, supra note 179, p.71; International Law Association, "ILA Study Group on Due Diligence in International Law", First Report (2014), pp.2-4 (이하 ILA 2014 Report).

의의무'로 번역된다. 상당주의 의무는 오늘날 국제환경법을 비롯한 국제인권법, 국제경제법 등 다양한 국제법 분야에서 원용되어 국가의 행위에 일정한 제한을 가하거나 혹은 특정한 의무를 부과하는 개념으로서 활용되고 있다.[182] 이처럼 상당주의 의무는 국제법의 다양한 분야에서 원용되어 왔으나 동 의무에 관한 범세계적인 정의는 확립되지 않았다.[183] 오늘날 상당주의 의무의 개념과 구체적인 내용은 국제재판소의 판시 내용을 통해 발전되어 온 것으로 여겨진다. 아래에서는 상당주의 의무와 관련하여 대표적으로 원용되는 판례의 내용 및 해당 판례의 판시내용으로부터 도출되는 상당주의 의무의 의미에 대하여 살펴보기로 한다.

1. Corfu Channel Case

상당주의 의무를 논의함에 있어서 가장 대표적으로 원용되는 국제법 판례는 영국과 알바니아 사이에서 1947년에 발생하였던 분쟁인 Corfu Channel 사건이다. 본 사건은 ICJ에서 상당주의 의무의 기준에 대하여 언급하였던 최초의 사례이기도 하다.[184] 본 사안에서 영국은 Corfu Channel을 통항하던 자국의 군함 2척이 해당 해협에 매설된 기뢰에 의해 폭파되자 연안국인 알바니아의 국가책임을 추궁하고자 하였다. 영국의 청구에 대하여 ICJ는 알바니아 정부가 자국의 영해에 기뢰가 매설되었다는 사실을 인식하고 있었음에도 불구하고 영해를 통과하는 영국의 선박에 이러한 사실을 경고하거나 혹은 적절히 통지하지 않았다는 사실에 주목하였다.[185] 그 결과, ICJ는 '모든 국가는

---

[182] Joanna Kulesza, Due Diligence in International Law, (Boston: Brill, 2016), p.262.

[183] Ian Brownlie, Principle of Public international law, (New York: Oxford University press, 2008), p.440.

[184] Scott J. Shackelford, Scott Russell & Andreas Kuchen, "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors", Chicago Journal of International Law, (2016), p.8.

[185] 재판부는 알바니아 정부가 기뢰 매설 사실에 대하여 인식하고 있었음을 판단하는 과정에서 다음의 사실 관계에 주목하였다. 우선 재판부는 문제된 기뢰 폭발 사건 전후 알바니아 정부의 활동과 태도를 관찰하였다. 알바니아 정부는 1946년 5월 이후 North Corfu Channel을 지속적이고 면밀하게 감시하였다. 가령, 알바니아는 동 해협

타국의 권리에 반하는 행위를 위해 자국의 영토가 사용되는 것을 알고도 (knowingly) 이를 허용해서는 안되는 의무를 갖는다'라고 판시하였으며,[186] 나아가 알바니아에게 부작위(omission)로 인한 국가책임이 성립한다고 판단하였다.[187] 즉, 본 사안에서 알바니아는 자국의 영해가 미국의 선박에 위해가 되는 행위를 위해 사용되고 있다는 것을 충분히 인식하고 있었으며, 이러한 위법 행위를 방지할 능력을 보유하고 있음에도 불구하고, 이를 방지하기 위한 합리적인 조치를 취하지 않았으므로 국제법상 '상당한 주의'를 다하지 못한 것으로 간주된다.

2. Island of Palmas case

한편, 국제법상 상당주의 의무의 정의는 Island of Palmas 사건에서 Max Huber 중재재판관의 판시 내용을 통해서도 유추할 수 있다. 필리핀 남부 해역에 위치한 Palmas섬의 영유권이 문제가 되었던 본 사안에서 Max Huber 중재재판관은, '영토주권에서 파생된 의무로서, 전시 및 평시에 영토 보전과 불가침성에 관한 타국의 권리를 자국의 영토 내에서 보호해야 할 영

을 통과하는 외국 선박에 대해 외교 공한을 발송하는 등의 적극적인 감시 및 통제를 하고 있었으며, 해당 사건이 발생하기 전 동일한 수역에서 다른 폭발사건이 발생함에 따라 해당 수역에 기뢰가 존재한다는 점에 대하여 명백하게 인지하고 있었다. 재판부는 이러한 점으로 미루어 볼 때 영해에 기뢰가 매설되었음을 인지하지 못하였다는 알바니아의 주장에는 신빙성이 없다고 판단하였다. 두번째로 재판부는 지뢰가 매설된 해역에 대한 알바니아의 '관찰 가능성'(possibility of observing)을 검토하였다. Corfu 해협에 기뢰가 매설되는 데 대략적으로 2시간 가량의 시간이 소요된다는 점, 기뢰 매설 지역에서 알바니아 해안경비대 초소까지의 거리가 약 500m에 불과하다는 점 등을 종합적으로 고려하였을 때, 알바니아 정부의 인식 없이 해당 지뢰가 Corfu Channel에 매설될 수 없다고 판단하였다. Corfu Channel case, pp.18-22 참조.

[186] Corfu Channel case, p.22. 원문은 다음과 같이 명시하고 있다. “(…) every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.”

[187] Corfu Channel case, p.23. 원문은 다음과 같이 명시하고 있다. "(…) These grave omissions involve the international responsibility of Albania."

토국의 의무'에 대하여 명시한 바 있다.[188] Max Huber 중재재판관은 이러한 영토국의 의무가 곧 '상당주의 의무'라는 점에 대하여 직접적이고 명시적인 정의를 내리고 있는 것은 아니다. 그러나 Max Huber 중재재판관의 이와 같은 판시 내용은 일반적으로 상당주의 의무에 관한 논의를 담고 있다고 여겨지며, 오늘날 상당주의 의무에 대해 논하는 대다수의 문서에서 이상의 판시 내용이 원용된다는 점에서 그 의의를 찾을 수 있을 것이다.[189]

II. 상당주의 의무의 발전 과정

1. Alabama Arbitration case

상당주의 의무는 1872년 영국과 미국 간에 발생하였던 Alabama Arbitration 사건을 계기로 국제법의 영역에 본격적으로 등장하였다.[190] 본 사건에서는 미국의 남북전쟁 중 미국과 영국 간 체결되었던 '워싱턴 협약'(the Treaty of Washington)의 이행 여부, 보다 구체적으로는 중립국(a neutral Government)으로서의 의무를 명시한 동 협약 제6조에 대한 위반이 문제되었다. Alabama Arbitration 사건의 중재재판부는 영국이 자국의 민간 조선소에 건조 중이던 Alabama호를 비롯한 총 5척의 선박을 미국의 남군이 사용할 수 있도록 진수함으로써, 워싱턴 협약 제6조 등에 명시된 '중립국의 의무'를 위반하였다고 판단한 바 있다.[191]

---

[188] Island of Palmas case, p.839. 원문은 다음과 같다. "Territorial sovereignty, as has already been said, involves the exclusive right to display the activities of a State. This right has as corollary a duty: the obligation to protect within the territory the rights of other States, in particular their right to integrity and inviolability in peace and in war, together with the rights which each State may claim for its nationals in foreign territory."

[189] 이종현, "제3국이 연관된 사이버 조작에 관한 국제법적 검토", 고려대학교 박사학위논문 (2017), p.45.

[190] Alabama Claims (US v. Great Britain), Reports International Arbitral Award 1871.(이하 Alabama Claims)

[191] Alabama Claims, p.131.

그렇다면 본 사건은 국제법상 상당주의 의무와 관련하여 어떠한 시사점을 갖는가? 국제법상 상당주의 의무와 관련하여 본 판결이 시사하는 바는, 제3자, 가령 개인의 국제위법행위에 대하여 국가는 원칙적으로는 책임을 지지 않으나 본 사안에서의 영국에게는 '부작위'(omission)에 의한 국가책임이 성립하며 이를 판단하는 기준으로 재판부는 영국이 '상당주의 의무'를 다하였는지 여부를 고려하였다는 점이다.[192] 즉, 본 사건의 중재재판부는 영국의 민간조선소에서 건조되고 있던 Alabama호를 비롯한 총 5척의 전함이 남부 연맹에 매각되는 일련의 과정에서 이를 방지하기 위한 '상당주의 의무'를 다하지 못하였던 영국 정부의 부작위에 주목한 것으로 볼 수 있다.[193]

2. ILC 국가책임법 초안 편찬과 상당주의 의무

상당주의 의무는 국제사회가 직면한 중대한 변화의 시기에 국가 간 발생하는 갈등을 중재하기 위하여 대두된 개념으로도 여겨진다.[194] 19세기와 20세기 동안 국경을 넘나드는 이동이 증가함에 따라 국가는 자국의 영토 내에서 외국인을 보호하기 위하여 합당한 조치를 취할 필요성에 대해 인식하게 되었으며,[195] 그 결과, 외국인 보호와 관련한 상당주의 의무의 개념이 발전하게 된 것이다. 이러한 기조는 UN 국제법위원회의 국가책임법 편찬 작업 과정에서 상당주의 의무가 중요한 요소로 고려되었다는 사실과도 연관된다.[196] 국제법의 발전과 성문화의 목적 하에 UN 국제법위원회가 출범한 이후, '국가책임'(State Responsibility)은 가장 먼저 법전화 되어야 할 항목으로 지정되었으며, 국제법위원회는 1955년부터 국가책임법 영역의 법전화를 위한 본격적인 작업에 착수하였다.[197] 국제법위원회는 국가책임에 관한 주제를 작업하

---

[192] Alabama Claims, p.131.

[193] Alabama Claims, pp.125-131.

[194] ILA 2014 Report, p.2.

[195] ILA 2014 Report, p.2.

[196] Joanna Kulesza, "Due Diligence in international law", Journal of Internet Law (2014), p.27.

[197] 정인섭, supra note 44, p.408.

기로 결정한 이래, Garcia-Amador을 비롯한 총 5인의 특별보고관이 제출한 33개에 달하는 보고서를 중심으로 국가책임 초안을 위한 논의를 진행해 왔다.[198]

국가책임 편찬 작업의 첫번째 특별보고관(Special Rapporteur)이었던 Garcia-Amador은 1957년 '외국인 신체 및 재산상 손해에 대한 국가책임'(international responsibility of the State for injuries caused in its territory to the person or property of aliens)을 중심으로 국가책임 초안을 작성하였다.[199] 동 초안의 제10조에서는 '개인의 행위'(acts of ordinary private individuals), 제11조에서는 '국내적 혼란 상황'(internal disturbances in general)에서의 행위, 제12조에서는 '당국의 행위 및 성공적인 저항단체의 행위'(acts of constituted authority and of successful insurgents)에서 비롯한 국가책임에 관한 내용을 규정하고 있다.[200] 상술한 제10조~제12조의 규정들은 전통적인 국가의 지위에서 행한 결과에 대하여 국가책임을 부담하는 것이 아니라, 개인 혹은 반란단체가 행한 국제위법행위를 방지하고 처벌해야 하는 국가의 구체적 작위의무를 다하지 않음에서 비롯하는 책임을 국가가 부담하여야 함을 의미하는 것이다.[201] 이때, '상당주의 의무'는 이와 같은 국가의 구체적 작위 의무 위반 여부 및 그러한 위반으로 인한 국가책임의 성립 가능성을 판단하는 하나의 '기준'(standard)으로 활용되었다.[202]

그러나 1960년 이후 Robert Ago가 특별보고관으로 새롭게 선임되었고, Robert Ago의 주도 하에 작성된 1963년 ILC 국가책임법 초안은 '외국인 신체 및 재산상 손해에 대한 국가책임'이 아닌, '국제관계에서 국가의 국제위법행위에 대한 위반 책임'을 전반적으로 다루는 것을 초안 작성의 목표로 삼았

---

198 임예준, "국가책임조항의 규범적 지위에 관한 소고(小考)", 『국제법학회논총』, 제65권 제3호 (2020), p.179.

199 ILC, "State Responsibility – Second report by F. V. Garcia Amador, Special Rapporteur", UN Doc. A/CN.4/106 (1957), p.104. (이하 ILC, UN Doc. A/CN.4/106)

200 ILC, UN Doc. A/CN.4/106, p.121.

201 김보연, "국제투자협정상 완전한 보호와 안전 의무의 해석기준 – 상당한 주의 기준의 비판적 고찰 –", 『국제거래법학회』, 제31권 제1호 (2022), p.114.

202 ILC, UN Doc. A/CN.4/106, pp.121-122.

다.[203] 초안 작성 방향이 선회 된 것의 배경에는 외국인의 신체 및 그들의 재산권 보호에 관한 국가의 의무 내용에 대하여 국제사회에서 합의를 도출하기 어려웠다는 점이 자리한다.[204] 외국인의 손해에 대한 국가책임만을 중점적으로 다룬 국제법위원회에 대한 비판과 함께, 국제관계 전 분야의 의무 위반에 공통적으로 적용될 수 있는 일반적인 책임 규범이 편찬되어야 할 필요성이 제기되었던 것이다.[205] 결과적으로 2001년 국제법위원회가 최종적으로 채택한 '국제위법행위로 인한 국가책임 초안'(Draft Articles on Responsibility of States for Internationally Wrongful Act, 이하 '국가책임 초안')에서는 상당주의 의무의 명시적인 정의는 배제되었으며, 동 의무는 간접적으로만 검토되었다. 국가책임 초안 제2조의 (3)에서는 국가가 상당주의 의무를 준수하였는지에 관한 문제는 관련된 '1차 의무'(primary obligation)를 발생시키는 구체적 조항 및 '조약의 대상과 목적'(object and purpose of the treaty provision) 등을 비롯한 전반적인 맥락과 함께 검토되어야 한다고 보았다.[206] 나아가, 국가책임 초안에서는 동 초안이 상당주의 의무에 관한 '일반적인 규정'(general rule)을 정립하고 있지 않다는 점에 대하여 명시함으로써 결과적으로 초안에서 상당주의 의무가 가지는 중요성이 비교적 감소한 것으로 볼 수 있다.[207]

III. 국제환경법 영역에서의 상당주의 의무

상당주의 의무는 국제법상 국가책임의 개념과 결부되어 외국인에 대한 보호, 전쟁법과 관련한 중립의무, 국제투자법, 국제환경법 등의 다양한 국제법 분야에서 국제법상 일정한 의무 이행에 요구되는 개념으로 활용되어 왔

---

[203] 정인섭, supra note 44, p.406.

[204] Ibid.

[205] 이종현, supra note 189, p.51.

[206] ILC 국가책임초안, p.34.

[207] ILC 국가책임초안, p.34. 원문은 다음과 같다. "The articles lay down no general rule in that regard."

다.[208] 또한 상당주의 의무는 ICJ, ITLOS, 중재재판 등 다수의 국제법원의 판시 내용을 통해서도 구체화되어 왔다. 앞서 확인한 바와 같이 상당주의 의무는 UN 국제법위원회에서 진행한 초창기 국가책임 분야의 법전화 과정에서 중요한 요소로 여겨져 왔으나, 2001년에 최종적으로 채택된 국가책임초안에서는 비교적 그 중요성이 감소한 것으로 보인다. 그럼에도 불구하고 상당주의 의무는 오늘날 국제환경법이라는 비교적 특화된 영역에서 그 중요성을 인정받고 있으며, 해당 영역에서의 국제법적 지위 역시 여타의 국제법 분야에서의 지위에 비해 비교적 명확하다.[209] 상당주의 의무의 구체적인 내용과 의의 역시 국제환경협약과 대표적인 국제환경법 판례 등을 통해 명확히 파악할 수 있을 것이라고 판단되는 바, 아래에서는 관련된 내용을 상세히 살펴보기로 한다.

상당주의 의무는 20세기 후반 이래로 국제환경법 분야에서 보다 깊이 있게 발전해 왔으며, 다수의 국제환경협약 역시 국제법상 상당주의 의무의 개념을 직간접적으로 수용하고 있다.[210] 국제환경법 영역의 발전의 바탕이 되는 원칙이자, 가장 기본적인 원칙으로서 지위를 갖는 1972년의 '유엔 인간 환경 선언' (Declaration of the United Nations Conference on the Human Environment, 이하 스톡홀름 선언)과 1992년의 '환경과 개발에 관한 리우 선언' (Rio Declaration on Environment and Development, 이하 리우 선언)은 공통적으로 초국경환경피해를 방지하기 위한 영토국의 의무를 구체적인 원칙으로 포함하고 있다.[211] 스톡홀름 선언은 제21원칙을 통해 '자국 내에서

---

[208] International Law Association, “ILA Study Group on Due Diligence in International Law”, Second Report (2016), p.1. (이하 ILA 2016 Report)

[209] Timo Koivurova, "Due Diligence", Max Plank Encyclopedia of Public International Law [MPEPIL] (2013), para.9.

[210] ILA 2014 Report, p.5; Medes Malaihollo, "Due Diligence in International Environmental Law and International Human Rights Law: A Comparative Legal Study of the Nationally Determined Contributions under the Paris Agreement and Positive Obligations under the European Convention on Human Rights", Netherlands International Law Review, Vol. 68 (2021), p.124.

[211] 한삼인·강홍균, "초국경 환경피해와 국가책임", 『환경법연구』, 제31권 제2호 (2009), pp.361-362.

의 활동이 타국 또는 국가 관할권의 범위를 벗어난 지역에 환경피해를 주지 않도록 할 책임'이 있음을 명시하고 있다.[212] 리우 선언 제2원칙은 스톡홀름 제21원칙과 마찬가지로 국가의 자원 개발 권리를 인정함과 동시에, '영토국은 그러한 자원 개발 활동이 초국경적 피해를 야기하지 않도록 할 책임을 져야 한다'는 점에 대해 명시하였다.[213] 스톡홀름 선언과 리우 선언은 초국경적 환경피해를 예방하기 위해 필요한 모든 적절한 조치를 취하여야 할 영토국의 의무를 언급함에 있어서 '상당주의 의무'라는 명시적인 용어를 사용하지는 않았다. 그러나, 국제환경법 영역에서의 상당주의 의무가 '초국경적 환경피해를 방지하기 위한 영토국의 의무'라는 맥락에서 발전해왔다는 점을 고려할 때, 각 선언의 제21원칙 및 제2원칙은 영토국으로 하여금 환경보호와 관련한 상당주의 의무를 부과하고 있는 것으로 해석될 수 있다고 판단된다.[214]

한편, 2001년 국제법위원회가 제출한 '위험한 행위로 인한 초국경적 손해의 방지에 관한 규정 초안'(Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, 이하 초국경적 손해 방지 초안)에서는 초국경적 환경오염을 예방하여야 할 국가의 의무를 보다 명확하게 확인할 수 있다. 동 초안 제3조는, 오염발생국은 심각한 초국경 피해(significant transboundary harm)를 예방(prevent)하고 그 위험을 최소화하기 위하여 모든

---

[212] Declaration of the United Nations Conference on the Human Environment, Principle 21: "States have, in accordance with the Charter of the United Nations and the principles of international law, the sovereign right to exploit their own resources pursuant to their own environmental policies, and the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction."

[213] Rio Declaration on Environment and Development, Principle 2: "States have, in accordance with the Charter of the United Nations and the principles of international law, the sovereign right to exploit their own resources pursuant to their own environmental and developmental policies, and the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction."

[214] 한삼인·강홍균, supra note 211, pp.361-362.

적절한 조치를 취해야 한다고 규정하였다.[215] 이때, 초안 제3조에 명시된 '예방'(prevention)이란, 중대한 위해나 손해가 발생하기 이전 단계에서 오염발생의 기원국이 심각한 초국경적 피해를 방지하거나, 혹은 위험을 최소화하기 위하여 '모든 적절한 조치'를 취할 것을 의미한다.[216] 더불어, 동 초안 제3조의 (7)에서는 제3조에 명시된 초국경적 환경피해를 방지하기 위한 모든 적절한 조치를 취해야 할 오염발생 기원국의 의무가 곧 '상당주의 의무'의 하나라는 점에 대해 명시하고 있다.[217] 즉, 심각한 초국경적 환경피해를 예방하거나 혹은 그 위험을 최소화하기 위하여 '모든 적절한 조치를 취할 의무'(shall take appropriate measures)는 '상당주의 의무'(due diligence)의 하나로서, '모든 적절한 조치를 취할 의무'는 추상적인 '상당주의 의무'를 이행하기 위한 보다 구체적인 절차적 규칙으로 제시된 것으로 볼 수 있다.[218]

앞선 논의를 통해 상당주의 의무는 국제환경법 분야에서 보다 다양하고 깊이 있는 논의를 거듭해 왔다는 점을 확인할 수 있다. 우선, 상당주의 의무는 국제환경법의 핵심적인 원칙을 담고 있는 문서인 스톡홀름 선언과 리우 선언을 비롯한 다양한 국제환경협약에 직간접적으로 수용되었으며, '초국경적 환경피해를 예방하거나 그 위험을 최소화 하기 위한 모든 적절한 조치를 취하여야 할 영토국의 의무'라는 맥락에서 발전해 왔다. 더 나아가, 국제환경법 분야에서 상당주의 의무는 2001년 UN 국제법위원회에 제출된 '초국경적 손해방지 초안'의 규정 및 주해를 통하여 보다 구체화 되었다. 아래에서는 상당주의 의무와 관련한 국제환경법 영역에서의 핵심적인 판례를 검토함으로써 상당주의 의무의 적용례와 그 의의를 찾고자 한다.

---

[215] ILC 국가책임초안 제3조의 원문은 다음과 같다. "The State of origin shall take all appropriate measures to prevent significant transboundary harm or at any event to minimize the risk thereof."

[216] ILC 국가책임초안, p.153.

[217] Ibid., p.154.

[218] 소병천, "국제환경법의 예방원칙과 상당한 주의 – 초국경 환경영향평가를 중심으로 –", 『국제법학회논총』, 제66권 제4호 (2021), p.108. ("적절한 조치를 취하는 것은 지극히 추상적인 상당한 주의를 담보하기 위해 절차적 규칙으로 제시된 것이며, 해당 절차들이 상당한 주의를 통해 이루어져야만 예방원칙의 소기의 목적이 달성될 수 있다.")

1. Trail Smelter Case

Trail Smelter 사건은 미국과 캐나다 간에 발생한 초국경환경피해에 관한 분쟁으로 초국경적 환경오염에 대한 국제책임과 관련한 최초의 판례이다. 캐나다 브리티시 콜럼비아 주의 강변에 위치한 트레일 제련소에서는 납과 아연을 생산하였는데, 해당 제련소로부터 배출되는 아산화유황(SO2)이 캐나다의 국경과 인접한 미국의 워싱턴 지역에 심각한 환경 피해를 야기한 것이 문제가 되었다. 이후 양국은 1928년 '국제공동위원회'(International Joint Commission)에 분쟁 상황을 회부하였으며, 캐나다가 미국에 보상금을 지불함으로써 분쟁이 일단락 되는듯 하였다. 그러나 트레일 제련소는 이후에도 지속적으로 대기 중에 유해물질을 배출함으로써 미국에 피해를 야기하였으며, 그 결과, 1935년 본 사안은 중재재판에 회부되었다.[219]

Trail Smelter 사건에서는 국가가 '자국 영토 내에서 발생한 행위로 인하여 타국에 피해가 발생하지 않도록 할 의무를 부담하는지 여부'가 쟁점이 되었다. 이러한 쟁점에 대하여 본 사건의 중재재판부는 '국제법과 미국 국내법에 따라 어떤 국가도 자국 영토의 사용을 통해 타국 혹은 타국 내의 재산이나 개인에게 피해를 초래할 수 없다'고 판시하였다.[220] 본 사안은 타국에 대해 초국경적 환경오염(transboundary pollution)을 직간접적으로 야기한 국가는 이러한 자국의 위법 행위에 대하여 국제법적 책임을 진다는 국제환경법상의 기본 원칙을 형성하였다는 점에서 매우 중요한 의의를 가진다.[221]

2. Pulp Mills Case

Pulp Mills 사건에서는 아르헨티나와 우루과이가 1975년에 체결한 '우루과이강 조약 (이하 1975년 조약)'의 적용 및 해석이 문제가 되었다. 양국 간 1975년 조약의 체결 이후 우루과이가 해당 강변에 제지 공장을 건설하자,

---

[219] 김석현, "트레일 제련소 사건 연구", 『법학논총』, 제22권 (1996), pp.217-218.

[220] Trail Smelter Arbitration. USA & Canada, 3 RIAA 1905(1941), p.1965.

[221] 정인섭·이재민·정서용, 신국제법판례 120선, 박영사, 2020, p.441.

아르헨티나는 수질 오염을 이유로 이에 반대하였다. 이후 아르헨티나는 우루과이의 제지 공장의 건설이 1975년 조약에 위배된다고 주장하며 본 사건을 ICJ에 제소하였다.[222] 보다 구체적으로, 본 사안에서는 우루과이가 제지 공장을 건설하는 일련의 과정 및 절차와 관련하여 '우루과이강 행정위원회'(Administrative Commission of the River Uruguay, CARU)와 조약의 타방 당사국인 아르헨티나에게 적절히 통보하지 아니한 행위가 1975년 조약의 제7조를 위반한 것인지가 문제되었다.[223] ICJ는 이러한 쟁점에 대하여 우루과이가 조약 준수의 실체적 의무와는 별개로 절차적 의무를 준수하지 못하였다고 판단하였다.[224]

한편, 본 사안에서 ICJ는 국제환경법상의 '예방의무'(obligation of prevention)의 개념과 내용에 대해 자세히 확인하고 있다. 재판부는 예방의무에 대해 설명하면서, '모든 국가는 타국의 권리에 반하는 행위를 위해 자국의 영토가 사용되는 것을 알고도 이를 허용해서는 아니되는 의무를 갖는다'는 Corfu Channel 사건의 판시 내용을 원용하였다. 즉, 재판부는 '예방의무'가 자국의 영토 내에서 초국경적 환경피해를 예방하고 방지할 것을 요구하는 의무인 '상당주의 의무'에 기원을 두고 있다고 간주하는 것이다. 더불어 본 사건의 재판부는 이러한 예방의무가 오늘날 환경과 관련한 국제관습법의 지위를 갖는다고도 판시한 바 있다.[225] 이와 같은 재판부의 판시 내용으로부터 국제환경법 영역에서의 상당주의 의무와 예방의무 간의 관계성을 짐작해볼 수 있다. 즉, 국가는 예방의무를 행함에 있어서 상당한 주의를 다해야 하므로, 상당주의 의무의 준수는 예방의무를 제대로 이행하였는지를 판단함에 있어서의 기준이 되는 것이다.[226] 더불어, 예방의무가 상당주의 의무를 이행하기 위한 실체적 의무로 기능한다는 점 또한 유추할 수 있다.[227]

---

[222] 정인섭, supra note 44, pp.439-440.

[223] Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, I.C.J. Reports 2010, p.14, p.44, para.94. (이하 Pulp Mills on the River Uruguay)

[224] Ibid., p.48, para.111, p.50, para.122 각각 참조.

[225] Ibid., p.45, para.101.

[226] 소병천, supra note 218, p.112.

[227] 박노형·김효권, supra note 7, p.69.

IV. 소결

이상의 논의를 요약하면, 상당주의 의무는 미국 남북전쟁의 종전 이후 미국과 영국 간에 발생한 분쟁인 Alabama Arbitration 사건을 계기로 국제법의 영역에 본격적으로 등장하게 된 개념으로 보여진다. 이후, 19세기를 기점으로 국경을 넘나드는 이동이 증가함에 따라, 외국인의 신체 및 재산에 대한 보호의 측면에서 상당주의 의무의 중요성이 대두하게 되었다. 이러한 맥락에서 국제법상 상당주의 의무는 UN 국제법위원회의 초창기 국가책임 편찬 작업에서 매우 중요한 역할을 하게 되나, 2001년 최종 국가책임 초안의 채택 과정에서 동 의무의 중요성은 비교적 상실된 것으로 보인다. 국가책임법의 영역에서 그 중요성을 제대로 인정받지 못하던 상당주의 의무는 이후 국제환경법의 영역에서 비교적 깊이 있게 발전하였으며, 의무의 구체적인 내용에 관해서도 지난한 논의의 과정을 거쳐왔다. 특히 상당주의 의무는 '초국경피해를 예방하고 이로 인한 피해를 최소화하기 위한 영토국의 의무'의 맥락에서 발전해 왔다. 이를 바탕으로 상당주의 의무는 국제환경법의 기본적인 원칙을 담고 있는 문서인 스톡홀름 선언과 리오 선언을 비롯한 다수의 국제환경협약에 직간접적으로 수용됨으로써 국제환경법에서의 중요성을 인정받고 있다. 국제환경법 분야에서 상당주의 의무의 성격 및 구체적인 내용은 2001년 제출된 국제법위원회의 초국경적 손해방지 초안의 조항과 주해를 통해 보다 명확하게 확인된다.

제 3 절. 상당주의 의무의 내용 및 적용상 쟁점

상당주의 의무는 구체적인 상황과 무관하게 자체적 개념이 완비된 개념이 아닌, 관련된 문제 영역과 국제법의 세부 분야에 따라 조금씩 다른 방식으로 적용되어 온 개념으로서 본원적으로 신축적이고 유연한 특성을 갖는다.[228] 즉

[228] Colin Patrick, "Debugging the Tallinn Manual 20.'s Application of the Due diligence principle to cyber operation", p.583. ("Due diligence, while eminently

오늘날 상당주의 의무를 규율하는 범세계적인 국제법 기준은 존재하지 않으며, 오히려 상당주의 의무는 '기존의 국제법'(pre-existing rule of international law)을 이행하기 위한 하나의 '행위 기준'(standard of conduct)의 역할을 수행해 온 것으로 이해하는 것이 타당하다.[229] 그러므로 특정한 1차 법률을 이행함에 있어 '상당주의 의무'를 제대로 준수하였는지 여부는 국제법의 특정 영역의 구체적인 내용 및 1차 법률이 요구하는 바에 따라(case-by case basis) 조금씩 다르게 해석되어 왔다.[230] 그렇다면 상당주의 의무의 내용 및 쟁점은 구체적인 적용 영역에 따라서 다르게 해석될 여지가 있는 바, 아래에서는 상당주의 의무의 내용과 동 의무가 구체적인 영역에 적용되었을 때 부각되는 쟁점에 대하여 다루기로 한다. 한편, 오늘날 상당주의 의무에 대한 명시적이고 범세계적인 정의는 부재한 상태이다. 다만, 국제법의 각 분야에서 상당주의 의무를 논의할 때, ICJ의 Corfu Channel 사건 결정문에서 언급된 내용이 가장 빈번하게 활용되고 있으며, 이는 소위 상당주의 의무에 관한 '당대의 정의로 인정받고 있다. ICJ의 Corfu Channel 사건의 관련 판시 내용은 다음과 같다.

> "Every state [has the] obligation not to allow (1) knowingly its (2) territory to be used for (3) acts contrary to the rights of other States."[231]

특정 국가가 상당주의 의무를 위반하였는지에 대하여 판단하기 위해서는 1차 법률이 명시하고 있는 내용에 대한 이해와 함께, 상당주의 의무가 담고 있는 내용을 구체적이고 명확하게 파악할 필요가 있다. 아래에서는 Corfu

---

flexible in application, still contains two essential elements."); Neil McDonald, "The role of Due Diligence in International Law", International & Comparative Law Quarterly, Vol. 68, No. 4 (2019), p.1044.

229 Neil McDonald, ibid.

230 Ibid.

231 Corfu Channel case, p.22.

Channel 사건의 재판부가 판시한 내용에 기초하여 상당주의 의무의 주요 내용 및 적용 상의 쟁점에 대해 살펴보고자 한다.

1. 타국의 권리에 반하는 행위

국가는 '타국의 권리에 반하는 행위'(acts contrary to the rights of other States)에 자국의 영토가 사용되지 않도록 허용하지 말아야 할 상당주의 의무를 부담한다. 즉, 국가는 자국의 관할권 내에 있는 영역이 '타국의 권리에 반하는 행위'에 사용되지 않도록 일정한 행위를 허용하지 않아야 할 것이 요구된다. 이때, 타국의 권리에 반하는 행위는 '국제법상 위법행위'로서, 타국에 피해를 끼치는 행위를 의미한다. 한편 상당주의 의무의 적용의 대상이 되는 행위는 타국의 주권에 의해 보호되는 사람 또는 사물에게 '심각한 피해'(serious injury)[232]를 야기하거나 또는 그러한 피해를 야기할 '가능성'이 있는 행위까지 포괄하는 것으로 해석하는 것이 적절하다. 상당주의 의무가 발생하기 위한 요건은 심각한 피해를 야기하는 '수준'의 행위인 것이지, 실제로 그 결과가 '발생'해야 함을 의미하지는 않기 때문이다.

상당주의 의무에 대하여 담고 있는 '초국경적 손해방지 초안'에서는 상당주의 의무로 하여금 영토국이 심각한 피해를 '완전히 방지할 것'을 보장하는 의무는 아니라고 명시하였다.[233] 다시 말해, 피해국의 입장에서 영토국에게 상당주의 의무를 다하지 못하였음을 주장하기 위해서는 자국에게 심각한 피해가 발생하였다는 점이 전제되어야 함은 확실하지만, 이러한 피해가 발생하였다는 이유만으로 영토국에게 피해 발생을 근거로 한 위반을 주장하기에는 불충분하다는 것이다. 이는 '결과의무'가 아닌 '행위의무'라는 상당주의 의무의 특성에서 기인한다.[234] 즉, 영토국에게는 타국에 대하여 발생할 수 있는

[232] 다만 이때의 '심각성'의 정도에 대해서 객관적으로 명시된 바는 없다. 상황 및 사안에 따라 상당주의 의무의 요건이 될 수 있는 심각성의 정도는 달리 해석함이 타당하다.

[233] ILC 국가책임법 초안, p.153.

[234] United Nations, Report of the International Law Commission on the work of its forty-sixth session, 2 May-22 July 1994, UN Doc. A/49/10, p.103. ("It is an obligation of conduct, not an obligation of result"); UNIBO, "International law and

심각한 피해를 완전하게 방지할 것이 요구되는 것이 아니라, 해당 피해를 방지하거나 혹은 그 위험을 최소화하기 위하여 가능한 최선의 노력(its best possible efforts)을 다할 것이 요구되는 것이다.[235]

2. 장소적 범위 (territory)

상당주의 의무를 구체화함에 있어서 장소적 범위가 논의되어야 할 필요가 있다. Corfu Channel 사건의 판시 내용에 따르면 국가는 자국의 영토가 타국의 권리에 반하는 행위에 사용되는 것을 허용해서는 아니될 의무를 갖는다.[236] 이때의 타국의 권리에 반하는 행위로 사용되어서는 안되는 '영토'(territory)의 범위는 국가의 관할권 개념에 기반하여 해석되어야 한다. 그러므로, 단순히 자국의 영토, 영해, 영공 뿐만이 아니라 영토의 바깥에 위치함에도 불구하고 당사국의 배타적 통제 및 관할이 미치는 장소라면, 해당 장소는 타국의 권리에 반하는 행위로 사용되지 않도록 당해 국가가 '상당한 주의'를 다하여야 하는 영토의 범위에 포함된다고 해석하는 것이 타당하다. 이처럼 상당주의 의무는 국가에 의해 통제되는 배타적 관할권을 가진 공간 체계를 기반으로 하는 개념이다. 그렇다면, 물리적 관할권과는 다른 특성을 갖는 가상의 공간인 사이버 영역에 대해서는 영토의 개념이 어떻게 적용되고 해석되어야 하는지에 대한 의문이 생긴다.[237] 이러한 의문에 기반한 사이버 공간에서 상당주의 의무의 쟁점은 제4장에서 보다 상세하게 다루기로 한다.

Cyberspace", Ministry of Foreign Affairs and International Cooperation (2021), p.27.

[235] ILC 국가책임법 초안, p.154.

[236] Corfu Channel case, p.22.

[237] 이종현, "사이버 영역에서의 국제법상 상당주의 원칙의 적용에 관한 고찰", 『국제법평론』, 통권 제49호 (2018), p.154.

3. 인식의 여부 (knowledge)

국가는 상당주의 원칙에 따라 타국의 권리에 반하는 행위에 자국의 영토가 사용된다는 것을 '알고도 (knowingly)' 허용해서는 아니되는 의무를 부담한다.[238] 이는 국가에게 상당주의 의무를 부과하기 위한 요건인 '인식'의 수준을 의미하는데, 상당주의 의무를 해석함에 있어서 인식의 해석 범위는 매우 중요한 것으로 여겨진다. 이때 국가의 인식 수준은 크게 '실제적 인식'(actual knowledge)와 '추정적 인식'(presumptive knowledge)으로 나눌 수 있다.[239] 국가가 자국의 영토가 타국의 권리에 반하는 목적으로 사용될 수 있다는 사실을 실제적으로 인식하였음에도 불구하고 이를 방지하거나 혹은 그로부터 발생하는 피해를 최소화하기 위하여 적절한 모든 조치를 취하지 않았다면, 당해 국가의 부작위(omission)로 인하여 상당주의 의무의 위반을 구성하다는 점은 확실하다. 이는 ICJ의 Hostage case 판시를 통해서도 드러난다. ICJ는 본 사건에서 이란의 국가책임을 인정함에 있어서, 이란 당국의 인식 여부에 대하여 '완전히 알고 있었음'(were fully aware of)이라고 명시한 바 있다.[240]

인식과 관련하여 오늘날 국제사회에서 보다 쟁점이 되는 것은 국가의 '추정적 인식'(presumptive knowledge)에 관한 내용이다. 특정 국가가 문제가 되는 사안에 대한 실제적 인식에 도달하지 못하였지만, 당해 국가의 전반적인 역량을 고려하였을 때 '해당 위험을 알아차릴 수 있었다고 판단되는 경우'에는 추정적으로 인식하였을 경우에도 상당주의 의무가 적용될 수 있다고 보는 것이 일반적이다.[241] 이는 Corfu Channel 사건의 판시에서도 확인되고 있다.[242] Corfu Channel 사건의 재판부는 설령 알바니아가 Corfu 해협의 기뢰 매설 여부에 대하여 실제적으로 인식하지 못하였다 하더라도, 사실관계를

---

[238] 탈린매뉴얼 2.0, Rule 6; Francois Delerus, supra note 69, p.366.

[239] Corfu Channel case, p.22.

[240] United States Diplomatic and Consular Staff in Tehran, Judgement, I.C.J. Reports 1980, p.3, para. 68.

[241] 이종현, supra note 189, p.61.

[242] Corfu Channel case, pp. 18-20; Colin Patrick, supra note 228, pp. 589-590.

종합적으로 고려하였을 때 지뢰 매설을 인식할 수 있었을 것이라고 판시한 바 있다. 다만 '추정적 인식'에 대해 판단하는 경우, 국가의 기술력을 포함한 여타의 역량이 매우 중요한 요소가 된다. 국가의 역량에 따라 자국의 배타적 관할이 미치는 범위 내에서 벌어지는 '위협'에 대한 추정적 인식 여부가 달라질 수 있기 때문이다.

제 4 장. 사이버 공간과 상당주의 의무

제 1 절. 사이버 공간에서 상당주의 의무의 적용 필요성

I. 사이버 공간에서 '상당주의 의무'에 대한 국제사회의 관심

제3장에서 논의한 바와 같이 국제법상 상당주의 의무는 초국경적 환경피해를 규율하는 국제환경법의 영역에서 보다 깊이 있게 논의되고 발전되어 왔다. 그러나 상당주의 의무는 물리적인 공간을 전제하는 국제환경법 분야에서의 논의와는 또 다른 맥락에서 오늘날 새롭게 대두되는 영역인 '사이버 공간'의 주요 화두로 주목받고 있다. 사이버 공간에서의 상당주의 의무에 대한 국제사회의 관심은 국가 및 국제기구의 성명, 국제 회의의 결과 보고서, 학계의 연구보고서 등 다수의 국제 문서를 통해 확인된다.

우선, COVID-19와 관련한 EU 이사회의 성명을 통해 EU 회원국의 사이버 공간에서의 상당주의 의무 적용에 대한 관심을 엿볼 수 있다. EU 이사회는 COVID-19 상황이 장기화됨에 따라 사이버 공간의 활용이 급격하게 증대되고, 그 결과로 EU 국가를 상대로 한 사이버 공간에서의 '악의적인 사이버 조작'(malicious cyber activities) 역시 급증하고 있다는 점에 대한 우려를 표명한 바 있다. COVID-19 팬데믹 기간 동안 독일, 프랑스, 오스트리아, 벨기에 등 상당수 EU 국가의 주요 국가기관, 병원, 산업체 등을 표적으로 삼은 악의적인 사이버 조작이 급증하였다. 이러한 사이버 공격의 결과, 정부 전산망과 주요 웹사이트를 비롯한 주요 전산시스템이 마비되거나 병원의 전산망이 마비되어 의료진 및 환자들이 불편을 겪는 사건 등이 빈번하게 발생하였다.[243] 이후, EU 이사회는 이러한 불법적이고 악의적인 사이버 조작을 방지하고 그 피해를 최소화하기 위하여 EU 회원국으로 하여금 UN 정부전문

[243] Cyber security in Estonia 2023, Republic of Estonia Information System Authority, pp.29-30.

가그룹 합의 보고서에 명시된 '상당주의 의무'에 따라 영토국 내에서 적절한 조치를 취할 것을 촉구하였다.[244]

한편, 2007년 발생하였던 대규모 DDoS 공격의 피해국인 에스토니아는 물리적 공간뿐만이 아니라 사이버 공간에서도 상당주의 의무가 적용되어야 한다는 주장을 매우 강력하게 표명하였다. 특히 에스토니아는 국가책임법이 본연의 역할을 다하지 못하는 사이버 공간에서 상당주의 의무는 피해국이 기댈 수 있는 유일한 해결책이 된다는 점을 강조하였다. 더불어 에스토니아는 각 국의 기술적, 정치적 역량 등을 종합적으로 고려하여 상당주의 의무를 부담해야 한다는 입장을 전개한 바 있다. 더불어 진행 중인 불법적인 사이버 활동을 '중단'(halt)하기 위한 모든 합법적이고 실현가능한 조치를 취하고, 나아가 불법적 사이버 공격을 식별하기 위한 수단을 '개발'(develop)해야 함을 주장하기도 하였다.[245] 이러한 견해를 종합적으로 고려할 때, 에스토니아는 상당주의 의무의 준수 범위를 비교적 넓게 설정함으로써 사이버 공격을 예방하거나 혹은 중단하기 위한 수단으로서 상당주의 의무의 보다 적극적인 역할을 기대하는 것으로 보여진다.[246]

탈린매뉴얼의 대표 집필자인 M. Schmitt 역시 자신의 저서를 통하여 주권의 원칙으로부터 파생된 상당주의 의무가 사이버 공간에 적용되어야 함을 주장하였다.[247] 그는 국가들이 상당주의 의무의 적용을 꺼려하는 이유가 동 의무의 상호적인 성격으로부터 비롯한다는 것을 인식함에도 불구하고 사이버 공간의 평화로운 활용을 위해 상당주의 의무가 긍정적인 역할을 할 수 있을 것이라는 입장을 개진하였다.[248]

---

[244] European Council, "Declaration by the High Representative Josep Borrell, on Behalf of the European Union, On Malicious Cyber Activities Exploiting the Coronavirus Pandemic", EU Press Release (May 1, 2020) (마지막 방문: 2023.7.27)

[245] UNGA 컨펜디엄, p.26/142; International cyber law: interactive toolkit, "National position of Estonia", DDEDOE (2021) (마지막 방문: 2023.7.27)

[246] International cyber law: interactive toolkit, ibid.

[247] Michael N. Schmitt, supra note 179, pp.70-71.

[248] Ibid., p.69.

사이버 맥락에서 상당주의 의무에 대한 국제사회의 관심은 무엇보다도 UN 정부전문가그룹의 논의 과정에서 가장 명확히 드러난다. UN 정부전문가그룹 제6차 회의의 최종보고서에 포함된 부속서에는 사이버 공간에 적용되는 국제법에 관한 자국의 국가실행인 '자발적 국가 기여'(voluntary national contribution)가 포함되어 있다. 제6차 회의의 참여국은 자발적 국가 기여를 통해 어떠한 국제법이 사이버 공간에 적용되는지에 관한 자국의 견해와 실행을 제출할 것이 요구된다.[249] 해당 문서에 반영된 사이버 공간에서 '상당주의 의무'에 관한 참여국의 지대한 관심은 주목할 만 하다. 회의의 참여국이 제출한 국가실행을 통합한 컨펜디엄은 총 15개 참여국의 국가 실행을 포함하고 있다. 그리고 자국의 국가실행을 제출한 15개 국가 가운데 무려 11개국이 상당주의 의무에 관한 자국의 실행 및 견해를 밝히고 있다.[250] 다만, 사이버 안보에 관한 담론에서 주요한 위치를 차지하는 중국은 자발적 국가 기여를 제출하지 않았고, 러시아는 자발적 국가 기여를 제출하였으나 상당주의 의무에 관한 내용을 포함하지 않았다. 사이버 공간에서의 법리를 형성함에 있어서 비서방 지역의 중요한 의견을 담당하고 있는 러시아와 중국이 상당주의 의무에 대한 자국의 견해를 제출하지 않았다는 점은 아쉬움이 남는 부분이다. 그러나 15개 국가의 자발적 국가 기여를 통합한 컨펜디엄은 사이버 공간에 적용되는 국제법에 관한 국가의 실행을 확인하는 가장 명확한 기준이 될 것으로 기대된다. 또한 컨펜디엄의 회람을 통해 사이버 공간에서의 각국의 실행을 자발적으로 공개하고 이를 타국이 열람할 수 있도록 함으로써 사이버 공간에 적용되는 법리에 관한 국가 간, 진영 간 입장 차이를 조율할 수 있을 것이다. 무엇보다, 대다수의 참여국이 사이버 공간에서의 상당주의 의무에 관

---

[249] 제6차 GGE를 개최하면서 UN총회는 참여국에게 사이버 공간에 적용되는 국제법에 관한 자국의 국가실행을 제출할 것을 요구하였다. UNGA, Advancing responsible State behavior in cyberspace in the context of international security, UN Doc. A/RES/73/266 (2019), para.3.

[250] '자발적 국가 기여(voluntary national contribution)' 문서에 상당한 주의의무와 관련한 자국의 실행 및 견해를 포함한 국가는 미국, 영국, 독일, 네덜란드, 일본, 노르웨이, 호주, 루마니아, 에스토니아, 스위스, 싱가포르의 총 11개 국가이다. 중국은 자발적 국가 기여를 제출하지 않았고, 러시아는 자발적 국가 기여를 제출하였으나 상당한 주의의무에 관한 자국의 견해를 담지는 않았다. UNGA 컨펜디엄 참조.

한 자국의 견해 및 실행을 제출하였다는 점은 사이버 공간에서의 상당주의 의무에 대한 국가들의 지대한 관심을 잘 보여주는 대목이다. 이로부터 앞으로 사이버 공간에서의 상당주의 의무에 관한 논의가 더욱 활발해질 것을 기대해볼 수 있다.

II. 사이버 공간에서 '상당주의 의무'의 도입 필요성

앞서 살펴본 바와 같이 EU 이사회와 UN 정부전문가그룹을 비롯한 다양한 국제기구, 국가, 그리고 학계에서는 상당주의 의무를 사이버 공간에 적용하는 것에 대하여 지대한 관심을 보이고 있다. 그렇다면, 사이버 공간에 적용되는 국제법을 논의하는 과정에서 이들이 상당주의 의무에 이토록 주목하는 까닭은 무엇인가? 그 이유는 다름 아닌, 상당주의 의무를 부담하는 주체가 사이버 공격과 연관된 '제3국'이라는 점에 기인한다. 주권 상호 존중의 개념으로부터 비롯한 일반국제법상의 상당주의 의무를 정의하는 범세계적인 규정은 부재하나 일반적으로 동 의무는 '타국에 위해를 가할 수 있는 초국경적 피해를 예방 혹은 방지하기 위하여 자국 관할권 내에서 모든 합리적인 수준의 조치'를 취해야 하는 영토국의 의무를 의미하는 것으로 여겨진다. 이러한 상당주의 의무의 개념은 오늘날 사이버 공간에서 '정보통신기술을 활용한 국제위법행위에 자국의 영토가 활용되는 것을 알면서도 이를 허용해서는 아니 되는 국가의 의무'를 의미하는 것이 된다.[251] 즉, 사이버 공간에서 상당주의 의무는 공격의 직접적인 배후국이 아니더라도, 타국에 위법한 영향을 줄 수 있는 사이버 공격에 자국의 영토가 활용된다는 것을 인지한 국가, 가령, 사이버 공격과 관련한 제3국인 '경유국'(transit state)에 대해서도 부과될 수 있는 의무인 것이다.[252]

이처럼 공격과 관련한 경유국에 부과될 수 있는 사이버 상의 상당주의 의무는 두가지 측면에서 적용의 필요성이 대두된다. 첫째, 사이버 상 국가책임법 적용의 한계의 대안으로 상당주의 의무는 피해국이 원용할 수 있는 유

[251] 탈린매뉴얼 2.0, Rule 6; UNGA 제4차 보고서, p.8; UNGA 제6차 보고서, p.10.
[252] 탈린매뉴얼 2.0, Rule 6.

효한 권리 구제 수단이 될 수 있다. 두번째로는, 오늘날 발생하는 대다수의 사이버 공격이 제3국을 경유하거나 제3의 공격 거점을 기반으로 발생한다는 사실을 고려할 때, 상당주의 의무는 사이버 공간에서의 역할이 점차적으로 확대되는 제3국에게 부과되는 의무라는 점에서 그 적용상의 이점을 찾을 수 있다. 이러한 논의를 바탕으로 아래에서는 사이버 공간에 상당주의 의무가 도입되어야 할 필요성에 대해 보다 상세하게 검토하기로 한다.

1. 국가책임법 적용의 한계에 대한 대안 – "피해국의 권리구제 수단"

국가는 오늘날 자국의 안보를 실질적으로 위협해 온 크고 작은 사이버 공격에 대한 경각심과 더불어 자국을 상대로 행해진 사이버 공격에 합법적으로 대응할 수 있는 실효적인 규범이 정립되어야 할 필요성에 대해 절감하고 있다.[253] 앞선 제2장에서 검토한 바와 같이 사이버 공격은 매우 복잡한 공격 양태와 높은 익명성을 특징으로 하여 수행된다. 또한 국가가 비국가행위자의 배후가 되어 자행되는 악의적인 사이버 공격 역시 일상적으로 발생한다.[254] 사이버 공격의 이러한 특성은 공격 주체의 식별과 귀속의 어려움을 야기하며, 궁극적으로는 전통적인 국가책임법을 사이버 공격 상황에 적용하는 데 상당한 어려움을 유발하게 된다.

ILC 국가책임초안은 국가의 국제위법행위에 대한 책임을 추궁하고 국제사회의 갈등을 평화롭게 해결하는 가이드라인의 역할을 성공적으로 수행해 온 것으로 평가된다. 그러나 이러한 국가책임법이 사이버 공간을 규율하는 방안으로도 과연 적절한 것인지에 대해서는 근본적인 의문을 제기하지 않을 수 없다. 국제위법행위에 대한 국가책임을 추궁함에 있어서 가장 전통적이고 실효적인 방법으로 간주되었던 국가책임법이 사이버 공간을 규율하는 방안으로는 더이상 효과적이지 못하다는 국제사회의 공통된 이해 하에, '상당주의 의무'는 피해국이 유효하게 기댈 수 있는 권리 구제 수단의 측면에서 그 필

---

[253] 박노형·김효권, supra note 7, p.74.

[254] 김소정, "미국의 사이버공격 대응정책과 한국에의 시사점: 솔라윈즈 해킹 대응사례를 중심으로", 국가안보전략연구원 연구보고서 (2022), p.71.

요성이 점차적으로 대두되고 있다. 상당주의 의무의 적용에 긍정하는 다수의 국가 가운데 특히 에스토니아는 사이버 공간에서의 상당주의 의무가 피해국의 권리를 구제하는 효과적인 수단이 될 수 있다고 주장하였다.[255] 더욱이, 에스토니아는 상당주의 의무가 국가책임법이 실제적인 역할을 할 수 없는 상황에서 더욱 실효적인 역할을 수행할 수 있다는 입장을 개진한 바 있다. 즉, 사이버 공격의 결과에 대하여 국가책임법이 본연의 역할을 다하지 못하는 상황에서 상당주의 의무마저 원용할 수 없게 된다면 공격의 피해국과 국제법은 무방비 상태(defenseless)에 놓이게 된다고 본 것이다.[256] 이처럼, 상당주의 의무는 국가책임법을 통한 권리구제가 용이하지 않은 사이버 공간에서 피해국이 기댈 수 있는 실효적인 권리구제 수단이 될 수 있으며, 바로 이러한 측면에서 사이버 공간에서 상당주의 의무가 적용되어야 할 첫번째 필요성을 찾을 수 있다.[257]

2. 사이버 공간의 평화적 활용을 도모하기 위한 수단

오늘날 발생하는 상당수의 사이버 공격이 제3국을 경유하여 이루어지고 있으며, 그 결과, 사이버 공격과 연관된 '제3국의 역할'이 점차 확대되고 있는 추세이다. 이처럼 직접적인 공격 개시국과 공격 피해국이 아닌 공격과 연관된 제3국의 역할이 점차 중요해지는 사이버 공간에서, 제3국에게 부여되는 상당주의 의무는 사이버 공간의 평화적 활용을 도모하기 위하여 일정한 역할을 수행할 수 있으므로 논의의 실익이 뚜렷하다고 할 것이다. 사이버 공격은 공격의 '익명성'과 '비대칭성'을 매우 중요한 특성으로 삼고 있으며, 이러한 공격은 공격자의 IP 주소를 은닉한 채 공격을 실시하는 '스푸핑'(Spoofing) 기법이나, 제3의 공격 거점을 경유하여 공격 루트를 설계하는 방식 등을 통해 구체화 된다.[258] 공격 수행 과정이 비교적 가시적인 재래식 공격과는 달리

---

[255] UNGA 컨펜디엄, p.26/142.

[256] UNGA 컨펜디엄, p.26/142.

[257] Michael N. Schmitt, supra note 179, pp.79-80.

[258] 백상미, supra note 13, p.84; 황지환, "북한의 사이버 안보 전략과 한반도 : 비대칭적, 비전통적 갈등의 확산", 『동서연구』, 제29권 제1호 (2017), p.140.

오늘날 발생하는 대다수의 사이버 공격은 이처럼 복잡다단한 방식을 통해 시행된다. 가령, 2009년 7월 우리나라의 주요 언론사와 메인 포털 홈페이지 등을 상대로 감행되었던 디도스 공격이 발생한 이후 국가정보원은 당해 공격의 배후가 북한과 관련된 세력으로 추정된다고 발표하였다. 그러나 해당 공격의 경우, 여러 국가의 IP 주소를 활용하여 공격의 루트를 우회하는 기법을 사용하였기 때문에 배후국을 북한으로 특정하는 과정이 매우 복잡하고 어려웠다.[259]

이처럼, 사이버 공격의 과정에서 공격의 진원지 혹은 공격 배후국과는 직접적 관련성이 낮지만, 결과적으로 공격 과정에 연루되는 '제3국'이 존재한다는 사실은 사이버 안보의 측면에서 상당히 주목할 만한 현상이다. 가령, 앞서 확인한 2007년 북한에 의해 감행된 것으로 추정되는 사이버 공격의 경우 중국 선양과 베트남에 위치한 거점을 우회하였으며, 같은 해에 에스토니아를 상대로 발생하였던 러시아 발 대규모의 디도스 공격 역시 조지아를 비롯한 다수의 제3국 거점을 경유한 것으로 밝혀졌다.[260] 북한과 러시아 발 사이버 공격 이외에도, 오늘날 발생하는 대다수의 사이버 공격에서는 공격과 관련된 '제3국'의 존재를 쉽게 확인할 수 있다. 그렇다면 이처럼 복잡다단한 사이버 공격의 과정에 빈번하게 연루되는 '제3국', 가령 공격의 '경유국'에게 초국경적 사이버 공격을 예방하고 방지할 책임과 의무를 부과할 수 있다면, 이는 사이버 안보의 전반적인 증진 차원에서 매우 유의미할 것이라고 판단된다. 즉, 해당 논리를 앞선 사례에 적용하자면, 북한의 공격 서버가 경유하는 '중국'과 러시아 발 사이버 공격 서버가 경유하는 '조지아'는 공격과 관련한 제3국으로서, 자국의 관할 시설이 타국에 위해를 가하는 방법으로 사용되지 않도록 주의를 다하여야 하는 '상당주의 의무'를 부담하게 되는 것이다. 그리고 바로 이 지점에서, 상당주의 의무를 사이버 공간에 적용하여야 할 두번째 필요성을 확인할 수 있다. 사이버 공격의 과정에서 경유국이 차지하는 영향력이 점차적으로 확대되는 오늘날, 상당주의 의무를 통해 이들의 행위를 규율하고 공격의 피해를 방지하기 위하여 일정한 의무를 부과할 수 있다면 이는

---

[259] 황지환, ibid., pp.140-141.

[260] James Pamment et al., supra note 1, p.52.

궁극적으로 사이버 공간의 평화적 활용과 질서 유지에 큰 기여를 할 수 있을 것으로 판단된다.

제 2 절. 사이버 공간과 상당주의 의무의 적용 가능성

상당주의 의무는 국제환경법, 국제투자법, 국제인권법 등을 비롯한 다양한 국제법 분야에서 논의되고 발전되어 왔으며,[261] 오늘날 다수의 국가, 학계, 국제기구는 사이버 공간을 규율하는 규범으로서의 상당주의 의무의 역할에 주목하고 있다. 그렇다면, 이처럼 다양한 국제법 분야에서 원용되어 왔으며, 또한 학계 및 국가로부터 지대한 관심을 받고 있는 국제법상 상당주의 의무는 오늘날 새롭게 대두된 영역인 '사이버 공간'에서도 적용 가능한가? 아래에서는 이와 관련한 국제사회의 논의를 검토함으로써, 상당주의 의무를 사이버 공간에 적용할 수 있을지에 대해 살펴보고자 한다. 보다 구체적인 논의를 위하여, 국제법과 상당주의 의무에 관한 심도 깊은 논의가 담겨 있는 국제법협회(International Law Association, ILA)에서 발간된 보고서를 비롯하여, 사이버 안보에 관한 가장 핵심적인 문서로 여겨지는 TM 그룹의 탈린매뉴얼과 UN 정부전문가그룹이 발간한 보고서를 전반적으로 살펴보고자 한다. 나아가, 상당주의 의무와 사이버 공간에 대해 각 문서들이 담고 있는 내용을 종합적으로 살펴보는 과정을 통하여 상당주의 의무의 사이버 맥락에서의 적용 가능성을 모색하고자 한다.

I. 국제법협회(ILA) 보고서

사이버 공간에서 상당주의 의무를 적용할 수 있는지에 관한 논의를 진행함에 있어서, 상당주의 의무에 관하여 국제법협회가 발간한 보고서는 유의미한 참고 자료가 된다. 상당주의 의무에 관한 국제법협회의 연구그룹은 '상당

[261] ILA 2016 Report, p.1.

주의 의무가 적용되고 있는 국제법 고유의 영역 간의 공통된 이해 '(commonality of understanding between distinctive areas of international law)에 대해서 검토하는 것을 목적으로 지난 2012년에 설립되었으며,[262] 2014년과 2016년 두 차례에 걸쳐 상당주의 의무에 관한 심층적인 보고서를 발간하였다.[263]

2016년에 발간된 국제법협회의 두번째 보고서에서는 상당주의 의무가 '더욱 폭넓은 국제법의 원칙들을 포함할 수 있는가'(whether due diligence embraces/constitute a broader principles of international law)에 관한 주제가 상세하게 검토되었다.[264] 국제법협회는 해당 주제를 검토하는 과정에서 ICJ의 Corfu Channel 사건 판시 내용을 적극적으로 활용하였다. 국제법협회 보고서는 Corfu Channel 사건의 판결문에 언급된 '타국의 권리에 반하는 행위를 위해 자국의 영토가 사용되는 것을 알고도 이를 허용해서는 아니되는 국가의 의무'가 곧 국제법상 '상당주의 의무의 핵심적인 내용'(the core content of the due diligence)이라고 보았다. 더불어, 국제법협회 보고서는 이러한 원칙(principle)이 매우 오랜 기간에 걸쳐 발전해 왔고, 해당 원칙이 오늘날 명백하게 관습국제법의 일부(now clearly a part of customary international law)가 되었다고 보았다. 또한 국제법협회는 관습국제법의 일부가 된 상당주의 의무가 국제법의 근본적인(cornerstone) 개념인 '주권', '영토보전', '국내문제 불간섭' 등의 원칙을 반영하고 있다는 입장을 개진하였다.[265]

이러한 국제법협회의 견해로부터 상당주의 의무가 비단 국제환경법 영역에만 적용되는 것이 아닌, 국제투자법, 국제인권법, 국제인도법과 같은 광범위한 국제법 분야에도 적용된다는 것을 확인할 수 있으며, 더 나아가 사이버

---

[262] Ibid.

[263] 2014년에 발간된 국제법협회(ILA)의 보고서는 상당주의 의무의 역사, 국제법 영역에서의 상당주의 의무의 발전 과정 및 그 역할에 대하여 담고 있다. 이후 발간된 2016년 국제법협회 보고서는 보다 분석적인 접근법을 취함으로써, 상당주의 의무가 어떠한 기능을 하는지에 대하여 검토하고, 더 나아가 국제법의 다양한 분야에서 상당주의 의무가 행위의 표준으로 사용되는 이유에 대해서도 검토하는 것을 목적으로 하고 있다. ILA 2016 Report, p.1 참조.

[264] ILA 2016 Report, p.5.

[265] Ibid.

영역에서의 적용 가능성 역시 긍정적으로 검토해볼 수 있을 것이다.[266] 더불어, 국제법협회 보고서는 국제법의 다양한 분야에 적용되는 상당주의 의무가 국제법의 특정한 분야에 적용될 수 있는 보다 '구체적인 규칙'(specific rules)을 기저에 두고 있는 개념이라는 것에 대해 언급한 바 있다.[267] 이러한 국제법협회 보고서의 입장을 종합하면, 상당주의 의무는 오늘날 새롭게 주목받고 있는 영역인 사이버 공간에 적용됨에 있어서 추가적인 논의가 필요한 적용상의 쟁점이 존재할 여지는 있으나, 여전히 상당주의 의무의 사이버 공간에서의 적용 가능성 자체는 긍정적이라고 판단할 수 있을 것이다.

II. TM 그룹 (탈린매뉴얼)

국제전문가그룹은 국가의 주권과 그로부터 파생되는 국제법의 기본원칙들이 사이버 공간에도 적용될 수 있다는 대전제 하에 전반적인 논의를 전개하였으며, 탈린매뉴얼 역시 이러한 시각을 바탕으로 작성되었다.[268] 같은 맥락에서, 주권의 원칙으로부터 파생된 국제법의 기본원칙 중 하나인 상당주의 의무 역시 사이버 공간에서의 적용이 가능하다고 볼 수 있을 것이다. 탈린매뉴얼 2.0은 구체적 조항을 통해 사이버 맥락에서의 상당주의 의무를 설명하고 있다. 매뉴얼 Rule 6에서는 상당주의 의무의 일반적인 내용을 개관하였으며, Rule 7은 사이버 공간에서 상당주의 의무의 준수와 관련한 구체적인 내용 및 요건에 대하여 다루었다. 탈린매뉴얼에서 구체적인 조항 및 주해를 통해 상당주의 의무를 직접적으로 명시하고 있다는 점으로부터, TM 그룹이 상당주의 의무의 사이버 공간에서의 적용 가능성을 긍정하고 있음을 보다 명확히 확인할 수 있다.

TM 그룹은 국제법상 상당주의 의무를 정의함에 있어서 국제재판소의 판시 내용을 적극 활용하였다. 우선, ICJ의 Corfu Channel 사건에 명시된 격

---

[266] Ibid., p.1. 상당주의 의무가 국제환경법에 전속된 법리가 아닌, 국제인권법, 국제인도법, 국제투자법 등 다양한 국제법 분야에 적용될 수 있다는 내용은 2014년에 제출된 국제법협회 보고서의 전반적인 내용을 통해서도 확인할 수 있다.

[267] Ibid., p.6.

[268] 탈린매뉴얼 2.0, Rule 1, Rule 6 (2).

언을 활용함으로써, 해당 내용이 상당주의 의무에 관하여 일반적으로 수락된 '동시대적인 정의'라는 점에 대해 언급하였다.[269] 또한, Island of Palmas 중재재판의 판시 내용을 원용하여 국제법상 상당주의 의무에 대해 설명하였다. 동 사건 판시 내용에 따르면 상당주의 의무는 국제법상 '주권'의 원칙으로부터 유래한 개념으로서, 영토국으로 하여금 '자국의 영토 내에서 타국의 권리를 보호할 것을 요구'하는 것이다.[270] 전통국제법의 영역에서 받아들여지는 이와 같은 상당주의 의무의 정의는 사이버 공간에서도 적용 가능하다고 할 것인데, TM 그룹은 국제법상 '주권'의 원칙이 사이버 공간에서도 적용된다는 사실에는 논란의 여지가 없으며, 따라서 주권으로부터 파생된 원칙인 상당주의 의무 역시 사이버 공간에 적용된다고 보는 것이 자연스러운 귀결이라는 입장을 개진하였다.[271] 즉, TM 그룹은 새롭게 대두되는 영역인 사이버 공간에서도 국가는 여전히 '자국의 영토로부터 발생되는 사이버 활동'(cyber activities emanating from, their territory)으로 인하여 타국에 피해를 가하지 않도록 하기 위하여 '상당한 주의'(due diligence)를 다해야 한다는 입장을 취하고 있다.[272]

한편, TM 그룹은 상당주의 의무가 국제법의 개별적인 영역의 특성에 따라서 구체화 과정을 거쳐 온 '일반원칙'이라는 점에 주목하였다.[273] 상당주의 의무의 이러한 발전 과정을 고려할 때, TM 그룹은 동 의무를 사이버 공간에 적용함에 있어서의 명확한 적용 범위나 구체적인 발동 요건 등에 대해서는 여전히 이견이 존재할 수 있음을 인정하였다.[274] 그럼에도 불구하고 국제전문가그룹은 사이버 법리 상 '상당주의 의무'라는 개념이 명백히 존재하고, 또한 사이버 공간에서 상당주의 의무가 적용될 수 있다는 점 자체는 논박의 여지가 없는 주지의 사실이라는 입장을 견지한다. 또한, 이들은 새로운 기술은 기존 국제법에 의한 명시적 배제가 존재하지 않는 한 금지되지 않는다는 ICJ

---

[269] 탈린매뉴얼 2.0, Rule 6 (2).

[270] 탈린매뉴얼 2.0, Rule 6 (2).

[271] Michael N. Schmitt, supra note 179, p.72.

[272] Ibid., p.70.

[273] 탈린매뉴얼 2.0, Rule 6 (4).

[274] Michael N. Schmitt, supra note 179, p.70.

Nuclear Weapons의 권고적 의견을 원용하며,[275] 기존 국제법으로부터의 명시적인 배제가 존재하지 않는 한, 상당주의 의무 역시 사이버 공간에 적용될 수 있다는 견해를 표명하였다.[276] 이러한 논리를 통해 TM 그룹은 상당주의 의무가 여전히 사이버 공간에서 '실재하는 법'(lex lata)의 지위를 갖추지 못하였다는 일각의 견해를 강력하게 반박하며,[277] 기존의 다양한 국제법 분야에서 원용되어 온 상당주의 의무가 사이버 공간에서도 무리 없이 적용될 수 있음을 주장한다. 그리고 이러한 국제전문가그룹의 견해는 탈린매뉴얼의 구체적인 조항 및 주해를 통해 보다 명확하게 확인된다.

III. UN 정부전문가그룹

제2장에서 확인한 바와 같이, 2013년 6월에 마무리 된 제3차 GGE 회의에서 UN 정부전문가그룹은 기존의 국제법과 특히 UN 헌장이 사이버 공간에 적용되며, 국가 주권의 개념과 주권으로부터 파생되는 국제법의 원칙들 역시 사이버 공간에서의 국가 행위에도 적용된다는 것에 대해 합의를 이루었다.[278] 물론, 제3차 UNGGE 회의에서 이루어진 본 합의는 사이버 공간의 특수성을 감안하였을 때, 기존의 국제법 규범이 사이버 공간에 적용되기 위해서는 여전히 추가적인 논의가 필요하다는 것을 전제하는 수준에서 이루어진 것이었다.[279] 이러한 부분적인 한계에도 불구하고, 국제법상 상당주의 의무가 국가의 '주권' 개념에서 유래한다는 사실과 국가 주권에서 파생된 일반 원칙들이 사이버 공간에도 적용된다는 정부전문가그룹의 합의를 종합적으로 고려하였을 때 상당주의 의무의 사이버 공간에서의 적용 가능성을 긍정적으로 검토해볼 수 있으므로, 제3차 UNGGE 회의의 합의는 본 연구에 있어서도 상당히 큰 의미를 갖는다.

---

[275] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p.226, p.224, para.39.

[276] 탈린매뉴얼 2.0, Rule 6 (4).

[277] 탈린매뉴얼 2.0, Rule 6 (3).

[278] UNGA 제3차 보고서, p.2.

[279] UNGA 제3차 보고서, p.2; UNGA 제4차 보고서 p.8.

제3차 UNGGE 회의의 합의 내용에 기초하여 국가 주권으로부터 파생된 원칙인 상당주의 의무 역시 사이버 공간에 적용될 수 있다는 점을 추론할 수 있었다면, 제4차 UNGGE 보고서는 사이버 공간에서의 상당주의 의무에 대하여 보다 명시적으로 규정하였다. 제4차 UNGGE 보고서는 '국가의 책임 있는 행동에 대한 규범, 규칙 및 원칙 (Norms, rules and principles for the responsible behaviour of States)'의 하위 항목에서 '국가는 정보통신기술(ICTs)을 이용한 국제위법행위에 자국의 영토가 사용되는 것을 알면서도(knowingly), 이를 허용해서는 안된다'라고 명시하였다.[280] 이는 1949년 ICJ의 Corfu Channel 사건에서 언급된 '자신의 영토가 다른 국가의 권리에 반하는 행위로 사용되는 것을 알면서도 허용하지 않을 국가의 의무'라는 고전적인 판시 내용을 환기하는 문구로, 정부전문가그룹은 이를 통해 사이버 공간에서 상당주의 의무를 다하여야 하는 국가의 의무를 의도하였다고 볼 수 있다.[281]

가장 최근 발행된 제6차 UNGGE 보고서에는 제4차 보고서와 동일한 문장을 사용하여 국가는 정보통신기술을 이용한 국제위법행위에 자국 영토가 사용되는 것을 알면서도 이를 허용하여서는 안된다는 내용을 명시하였다.[282] 다만, 제6차 UNGGE 보고서는 상당주의 의무에 관한 보다 실체적인 내용을 동 보고서 본문의 주해에 포함하였으며, 나아가 상당주의 의무를 이행함에 있어서의 일종의 가이드라인을 제시하고 있다.[283] 이러한 측면에서, 제6차 UNGGE 보고서는 제4차 보고서와 비교하였을 때 상당주의 의무에 대해 보다 심화된 국가들의 합의 내용을 담고 있다고 보여진다.[284]

---

[280] UNGA 제4차 보고서, 제13(c), p.8/17. ("States should not knowingly allow their territory to be used for internationally wrongful acts using ICTS.")

[281] Jan Martin Lemnitzer, "Back to the roots: The Laws of Neutrality and the future of Due Diligence", The European Journal of International Law, Vol. 33, No. 3 (2022), p.792.

[282] UNGA 제6차 보고서, 제13(c), p.10/26. ("States should not knowingly allow their territory to be used for internationally wrongful acts using ICTS.")

[283] UNGA 제6차 보고서, 제13(c), pp.10-11/27.

[284] 박노형·김효권, supra note 7, p.72.

다만, UN 정부전문가그룹의 보고서는 상당주의 의무를 구속력이 있는 국제법(international law)의 영역이 아닌, 비구속적이고 자발적인 국제규범(norms, rules and principles for the responsible behaviour of States)의 영역에 포함하였다. 즉, 탈린매뉴얼과 달리 UN 정부전문가그룹의 논의 과정에서는 상당주의 의무의 국제법적 지위를 합의함에 있어 어려움을 겪고 있는 것이다. 따라서 상당주의 의무의 국제법적 구속력에 대해서는 여전히 추가적인 논의가 이루어져야 할 것으로 보인다. 이러한 한계에도 불구하고, 제3차, 제4차 그리고 제6차 UN 정부전문가그룹의 보고서에 담긴 상당주의 의무에 관한 내용을 종합적으로 고려한다면, 상당주의 의무의 사이버 공간에서의 적용 가능성 측면에서는 합의가 이루어진 것으로 볼 수 있다.

IV. 소결

제2장에서 확인한 바와 같이 국제사회는 전통적인 국제법이 새로이 대두된 영역인 사이버 공간에도 적용된다는 것에 대하여 전반적인 합의를 이룬 것으로 판단된다. 본 절에서 검토한 국제법협회(ILA)의 상당주의 의무에 관한 두 차례의 보고서, TM그룹이 발간한 탈린매뉴얼, 그리고 UN 정부전문가그룹에서 채택한 최종보고서 역시 현존하는 국제법의 사이버 공간에서의 적용 가능성에 대하여 긍정하는 태도를 보인다. 이들은 공통적으로, 사이버 공간에 UN헌장을 비롯한 국제법과 국제법으로부터 파생되는 일반원칙이 적용된다면, 결과적으로 '상당주의 의무' 역시 사이버 공간에 적용된다고 간주하는 것이 타당하다는 논리를 전개한다. 즉, 이들은 국제법상 '주권' 개념으로부터 파생되는 원칙인 '상당주의 의무' 역시 사이버 공간에서 국가의 행위를 제한하고 의무를 부과하는 규범으로서 일정한 역할을 수행할 수 있다고 간주하는 것이다. 또한 이들 보고서는 공통적으로 Corfu Channel 사건에서 상당주의 의무를 환기하는 판시 내용을 원용함으로써, 사이버 공간에서의 상당주의 의무의 적용 가능성에 대하여 긍정적인 입장을 보이고 있다. 다만, 비대칭성, 익명성, 가상성 등 사이버 공간이 갖는 특수성을 감안한다면, 상당주의 의무의 적용 범위, 발동 요건, 국제법적 지위 등에 대해서는 추가적인 논의가 필요할 것이

다. 사이버 맥락에서 상당주의 의무와 관련하여 발전적인 논의가 이루어져야 한다는 학계 및 국가의 견해는 탈린매뉴얼과 UN 정부전문가그룹의 보고서를 통해서도 확인할 수 있으며, 앞으로의 국제사회의 논의 역시 이러한 부분에 기반하여 진행되는 것이 바람직하다고 판단된다.

제 3 절. 사이버 공간에서 상당주의 의무의 적용상의 쟁점

확인한 바와 같이 국제법의 다양한 분야에서 원용되던 상당주의 의무가 새롭게 대두된 분야인 사이버 공간에도 적용될 수 있다는 점에 대해서 국제사회는 전반적인 합의를 이룬 것으로 보인다. 탈린매뉴얼에서는 사이버 공간에서의 상당주의 의 무의 역할을 매뉴얼의 조문을 통해 직접적으로 명시하고 있으며 UN 정부전문가그룹 역시 최종 보고서를 통해 상당주의 의무가 사이버 공간에 적용됨에 대하여 전반적으로 긍정하는 입장을 취한다.[285] 다만, 전술한 바와 같이 상당주의 의무는 구체적인 상황과 무관하게 그 자체로 객관적인 요건을 완비한 규범은 아닌 것으로 여겨진다.[286] 실제로 그간 상당주의 의무의 적용 범위와 발동 요건은 국제법의 영역, 혹은 구체적인 규범에 따라 조금씩 달리 적용되어 왔다.[287] 이는 다름 아닌 상당주의 의무가 갖는 신축적이고 유연한 특성에 기인한다.[288] 상당주의 의무의 이러한 특성은 동 의무가 사이버 공간에 적용되는 상황에서도 여러가지 적용상의 쟁점을 야기할 가능성이 있다. 가령, '물리적인 영토 관할권에 기반하였던 '영토'의 개념은 사이버 공간에서는 어떻게 해석되어야 하는가', '사이버 조작의 결과로서 발생하

---

[285] 탈린매뉴얼 2.0 Rule 6; UNGA 제4차 보고서, p.8; UNGA 제6차 보고서, p.10.

[286] Colin Patrick, supra note 228, p.583. ("Due diligence, while eminently flexible in application, still contains two essential elements.")

[287] 상당주의 의무는 국제인권법, 국제해양법, 국제투자법, 국제환경법 등 다양한 국제법 분야에 원용되어 왔으나 구체적인 적용 방식과 발동 요건은 구체적 맥락에 따른 차이를 보였다. 관련 내용은 International Law Association가 2014에 발간한 보고서 참고.

[288] ILA 2014 Report, p.2.

는 '타국의 권리에 반하는 행위'는 구체적으로 무엇을 의미하는 것인가', 또한, '상당주의 의무가 발동되기 위해서는 사이버 조작이 타국에 심각한 피해를 야기할 것이 요구된다면, 심각성의 요건을 충족하기 위해서는 어떠한 요건이 구비되어야 하는가' 와 같은 적용상 쟁점에 관한 의문이 끊임없이 제기되는 것이다.

지금까지 국제사회는 사이버 공간에서 상당주의 의무의 구체적인 적용 범위나 요건에 대한 초국가적 합의를 이루지 못하였다. UN 정부전문가그룹 역시 제3차 정부전문가 회의를 기점으로 국제법이 사이버 영역에 적용되어야 한다는 점에는 합의를 하였으나, 여전히 상당주의 의무의 법적 지위 및 구체적 적용 범위에 대한 진전된 논의에는 이르지 못하였다.[289] 상당주의 의무를 사이버 공간에 적용함에 있어서 앞선 질문들에 대한 국제사회의 공통된 기준을 도출하지 못한다면 상당주의 의무는 실질적 적용이 어려운 모호한 개념으로 남게 된다. 아래에서는 상당주의 의무가 사이버 공간에 적용되었을 시, 동 의무가 실질적으로 이행되기 위하여 검토를 필요로 하는 사안에 대하여 다루고자 한다.

I. 영토의 범위 (territory)

사이버 공간에서의 상당주의 의무를 논함에 있어서 '영토(territory)'의 범위가 문제될 수 있다. 전통적인 국제법은 국가의 관할권에 의해 통제되는 물리적 공간 체계를 기반으로 논의되기 때문에 상당주의 의무를 적용함에 있어서 '영토'가 갖는 의미가 비교적 명확하였다. 예컨대, 초국경적 환경피해를 예방하기 위한 국가의 상당주의 의무 역시 물리적인 영토, 영해, 영공의 체계에 기반하여 논의되었다.[290] 그렇다면 물리적인 영토 및 국경 등에 기초한 상

[289] Tomohiro Mikanagi, "Application of the Due Diligence Principle to Cyber Operations", International Law Studies, Vol. 97 (2021), p.1031.

[290] Robert Kolb, "Reflection on due diligence duties and cyberspace", German Yearbook of International Law, Vol. 58 (2015), p.120.

당주의 원칙을 이러한 개념이 비교적 불분명한 사이버 공간에서도 그대로 적용할 수 있는지에 대한 의문이 생긴다.

제2장에서 논의한 바와 같이, 사이버 공간은 그 자체로는 가상의 영역이지만, 동시에, 컴퓨터, 라우터, 서버 등의 물리적인 단계를 토대로 구성되는 이중적인 특성을 가지는 특수한 영역이다.[291] 즉, 컴퓨터, 라우터, 서버 등은 사이버 공간을 구성하는 '물리적 요건'으로 간주되는 것이다.[292] 실제로 '영토'의 개념을 사이버 영역에 적용함에 있어서, 국제전문가그룹 역시 사이버 공간의 이러한 이중적인 특성에 집중한 바 있다. 즉, 국가는 사이버 공간 자체에 대한 주권을 주장할 수는 없지만, 해당 국가의 관할권 내에 위치한 사이버 기반 시설(cyber infrastructure)과 해당 사이버 기반 시설과 관련된 활동에 대해서는 주권을 행사할 수 있다고 간주된다.[293] 이때 국가가 상당주의 의무를 다하여야 하는 사이버 기반 시설은 두가지로 나눌 수 있다. 첫째는 국가는 자국의 영토 내에(State's own territory) 있는 사이버 기반시설이며, 둘째는 국가의 영토가 아닌 다른 곳에 존재하지만 당해 국가의 법률상(de jure) 혹은 사실상(de facto)의 배타적 통제권을 미치는 기반시설이다.[294] 즉, 사이버 공간이 가지는 이중성에 기해 오늘날 국제사회는 사이버 공간에도 '영토'의 개념을 적용할 수 있을 것으로 사료된다.[295] 결과적으로 국가는 자국의 물리적 관할권 하에 있는 사이버 기반시설이 타국에 악영향을 미치는 방법으로 활용되는 것을 허용하지 않을 상당주의 의무를 부담하게 되는 것이다.

II. 타국의 권리에 반하는 행위 및 심각한 부정적인 결과를 초래하는 행위

영토국은 사이버 공간에서 '피해국의 권리에 반하는 (affects the rights of)', 그리고 '피해국에게 심각하게 부정적인 결과를 가져오는 (produce

---

[291] Yaroslav Radziwill, supra note 17, pp.93-94.

[292] 유준구, supra note 72, p. 157.

[293] 탈린매뉴얼 2.0, Rule 1(7).

[294] Eric Talbot Jensen, "State Obligations in Cyber Operations", Baltic Yearbook of International Law of International Law, Vol. 71 (2015), p.8.

[295] Yaroslav Radziwill, supra note 17, pp.93-94.

serious adverse consequences for other States)' 모든 사이버 조작을 위하여 자국의 영토가 사용되는 것을 허용하지 않을 의무를 부담한다.[296] 즉, 탈린매뉴얼에 의하면 특정한 사이버 조작에 대하여 국가가 상당주의 의무를 부담하기 위해서는, 당해 사이버 조작이 피해국의 '권리'에 반하는 조작임과 동시에 피해국에 '심각하게' 부정적인 결과를 가져오는 행위일 것이 동시에 요구되는 것이다.[297] 아래에서는 각각의 요건에 대하여 보다 상세하게 다루기로 한다.

1. 피해국의 권리에 반하는 사이버 조작

탈린매뉴얼 2.0의 Rule 6은 영토국으로 하여금 '타국의 권리에 반하는 사이버 조작'(cyber operations that affect the rights of other States)을 위하여 자국의 관할권 하에 있는 영토 및 사이버 기반시설 등이 사용되지 않도록 상당한 주의 를 다하여야 할 의무가 있음을 명시하였다. 즉, 특정한 사이버 조작이 국제법을 위반한다면, 이는 '타국의 권리에 반하는' 사이버 조작이 된다.[298] 이때, 상당주의 원칙은 초국경적 피해를 방지할 국가의 의무이므로, 문제가 되는 사이버 조작은 오직 국제법상의 '국제위법행위'(internationally wrongful act)에 해당되어야 한다.[299] 따라서 해당 사이버 조작의 결과로서 피해가 발생하였음에도 불구하고 그 행위가 국내법만을 위반한다면 상당주의 의무의 적용 대상이라고 보기 어렵다.[300] 그렇다면 구체적으로 어떠한 사이버 조작이 피해국의 권리에 반하는 '국제위법행위'에 해당하는가? 아래에서는 이에 대하여 살펴보고자 한다.

---

[296] 탈린매뉴얼 2.0, Rule 6.

[297] 탈린매뉴얼 2.0, Rule 6(15); Francois Delerus, supra note 69, pp.363-364.

[298] 탈린매뉴얼 2.0, Rule 6(15)

[299] Andraz Kastelic, supra note 150, p.14; Robert Kolb, supra note 290, p.121. ("This unlawfulness has to be reckoned mainly under international law.")

[300] Andraz Kastelic, ibid., p.2.

1) 타국의 주권을 침해하는 행위

국가는 국제법상 '영토주권'(territorial sovereignty)을 향유한다. 그리고 이러한 영토주권은 국내 문제에 대하여 타국의 개입을 받지 않고 자유롭게 결정할 수 있는 국가 권력의 독립과도 밀접하게 관련된다.[301] 탈린매뉴얼 2.0에서는 특정 사이버 조작이 타국 정부의 고유한 기능의 수행에 간섭하거나, 이를 침탈하는 경우 주권 침해가 발생할 수 있음을 규정하고 있다.[302] 다만, 구체적으로 무엇이 타국의 영토보전에 대한 침해인지, 혹은 정부의 고유한 기능에 대한 간섭인지에 대하여 확정적인 정의를 내리는 것은 어렵다. 가령, 사회 서비스의 제공, 선거의 실시, 세금 징수, 외교 및 국방 기능 등 오로지 '정부'만이 할 수 있는 기능은 정부의 본질적 기능으로 간주될 수 있을 것이다.[303]

2) 무력사용 행위

특정한 사이버 조작이 '규모와 효과'(scale and effect)의 측면에서 결과적으로 '무력 사용'(use of force)의 수준에 이른다면, 이는 피해국의 권리에 반하는 사이버 조작이라고 간주되어야 한다. 그리고 국가는 자국의 영토 및 영토 내에서의 사이버 관할시설이 이러한 '무력 사용'을 목적으로 활용되지 않도록 상당한 주의를 다해야 할 의무를 부담한다. UN 헌장에서는 국제사회에서 무력의 위협이나 사용(the threat or use of force)을 일반적으로 금지하고 있다.[304] UN이 창설된 이래 헌장 제2조 제4항의 내용은 무수한 국제문서와 국제재판을 통해 지지되었으며, 타국에 대한 무력사용금지원칙은 오늘날 조약상의 의무를 넘어 관습국제법으로 확립되었다.[305] 그리고 이러한 무력사용금지원칙은 일반 국제법 영역을 넘어서 사이버 공간에서도 적용된다고 보

---

[301] Nico Schrijver, supra note 173, pp.70-71, 86-87 각각 참조.

[302] 탈린매뉴얼 2.0, Rule 4(15).

[303] 탈린매뉴얼 2.0, Rule 4(16).

[304] UN 헌장 제2조 제4항.

[305] 정인섭, supra note 44, p.1143.

는 것이 타당하다. 이는 ICJ의 Legality of the Threat or Use of Nuclear Weapons 권고적 의견으로부터 추론이 가능한데, 본 권고적 의견에서는 헌장 제2조 제4항 및 자위권에 대하여 규정한 제51조가 '이용되는 무기와 관계없이 어떠한 무력 사용에도 적용된다'고 명시한 바 있다.[306] 이러한 권고적 의견의 내용을 고려할 때, 재래식 무기체계가 아닌 사이버 수단에 의한 행위 역시 헌장에서 규정하는 '무력사용'으로 간주될 수 있을 것이다.

다만, 특정 사이버 조작이 단순히 타국에 피해를 야기하는 수준을 넘어서서 무력사용에 해당하는지를 판단함에 있어서는 '규모와 효과'(scale and effect)가 고려되어야 한다. 이를 판단하는 권위있는 정의나 기준은 부재하다.[307] 그러나 일반적으로 사이버 조작이 그 규모와 효과의 면에서 재래식 무기의 무력 사용의 수준과 유사한 피해가 야기하였다면, 이를 무력사용으로 판단하는 것이 합당할 것이다.[308] 가령, 단순히 악성프로그램을 유포하는 것은 무력사용에 이르지 못하나, 악성프로그램이 유포된 결과, 인명이 살상되거나 혹은 심각한 물리적 피해를 발생시키는 행위는 '규모와 효과'의 면에서 무력사용에 해당된다고 볼 수 있다.

2. 피해국에게 심각하게 부정적인 결과를 가져오는 사이버 조작(produce serious adverse consequences)

영토국에게는 '타국에게 심각하게 부정적인 결과를 가져오는 사이버 조작'이 자국의 관할권 내에서 이루어지지 않도록 상당한 주의를 다하여야 할 의무가 존재한다. 이러한 기준은 영토국이 모든 초국경적 피해를 방지하고 예방할 의무가 있는 것이 아니라, '심각한 결과를 초래하는 피해'라는 임계점(threshold)을 설정함으로써, 상당주의 의무를 다하여야 할 영토국의 의무의

---

[306] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J.

[307] 탈린매뉴얼 2.0, Rule 69(2).

[308] 탈린매뉴얼 2.0, Rule 69.

범위에 대한 한계를 설정하고 있는 것이기도 하다.[309] 다만 국제전문가그룹은 무엇이 심각한 부정적인 결과를 초래하는 사이버 조작인지에 대하여 명확하게 서술하지는 않았으며 국제사회 역시 이 부분에 대하여 일관된 합의를 이루지 못하였다. 그러나 상당주의 의무의 실질적인 적용을 위해서는 '심각성'에 대한 기준 정립이 필수적이므로, 아래에서는 우선 현재 논의되고 있는 내용에 대하여 다루고자 한다. 우선 피해의 '심각성'(seriousness)은 문제되는 사이버 조작의 구체적인 상황에 따라 각기 다르게 판단되어야 한다. 이는 전술한 바와 같이 상당주의 원칙의 신축적인 특성 때문이다.[310] 동시에 이러한 심각성의 판단은 피해의 규모와 성격, 그리고 이것이 피해국에 미치는 구체적인 영향과 같은 객관적인 사실에도 근거하여 평가되어야 한다.[311]

심각성의 기준과 관련하여, 해당 사이버 조작이 반드시 물리적 피해(physical damage)를 수반해야 하는가 역시 논의되어야 할 부분이다. 이에 관하여 탈린매뉴얼에서는 문제가 되는 사이버 조작이 무조건적으로 물리적 피해를 수반하여야 할 필요는 없는 것으로 보고 있다.[312] 즉 해당 사이버 조작이 보호받는 물체 혹은 인간의 신체에 직접적인 상해를 초래하는 결과가 상당주의 원칙의 필수적인 발동 요건은 아니게 되는 것이다. 실제로 사이버 공간에서 발생하는 상당수의 해로운 사이버 조작은 인명피해를 위시한 물리적 피해를 입히지 않고도 국가의 정보전산망 마비, 은행 시스템 마비, 전력 시스템 마비 등을 통하여 국가의 필수적인 시스템에 심각하게 부정적인 영향을 초래하는 경우가 많다. 이러한 사이버 조작의 특성과 피해의 유형을 고려

---

[309] Collin Patrick, "Debugging the Tallinn Manual 2.0's Application of the Due diligence principle to cyber operation", Washington International Law Journal, Vol. 28, No. 2 (2019), p.593.

[310] Antonio Coco & Talita Dias, "Cyber Due diligence in international law", European Journal of International Law, Vol. 32, Issue 3 (2021), p.146. ("The determination of what amounts to significant harm involves a somewhat subjective or value-based assessment that varies depending on the circumstances prevailing at the time, in particular, existing scientific knowledge and the economic value of the activity or good in question.")

[311] Ibid.

[312] Robert Kolb, supra note 290, p.121.

할 때 물리적 피해를 수반할 것을 필수적인 요건으로 채택하지 않는 것이 타당해 보인다.

III. 인식(knowledge)의 기준

영토국이 초국경적 피해를 방지하고 그로부터 발생하는 피해를 최소화하기 위한 상당주의 의무를 이행하기 위해서는 우선적으로 당해 위험을 인식하고 있을 것이 요구된다.[313] 이때 '인식(knowledge)'의 기준은 상당주의 의무의 적용에 있어 합의가 필요한 또 하나의 쟁점이다. 즉, 국가가 '인식'을 하였다는 것이 무엇을 의미하는지, 또한 구체적으로 어떠한 경우 '인식'을 한 것으로 보아야 하는지가 중요한 문제가 된다. 한편, 인식의 여부는 '실제적 인식'(actual knowledge)과 '추정적 인식'(constructive knowledge)으로 나누어져서 논의되고 있다.

1. 실제적 인식 (actual knowledge)

타국에 대한 적대적인 사이버 조작을 위하여 자국의 관할권 내에 위치한 서버 및 기타의 사이버 기반시설이 활용되었음을 영토국이 '실제적'으로 인식한 경우에 상당주의 원칙이 적용된다는 점은 당연하다.[314] 이때의 '실제적 인식'이란, 자국의 서버 혹은 사이버 기반시설 등이 타국에 대한 국제위법행위를 목적으로 사용되었다는 사실에 대해 영토국이 명확하게 인지하였음을 의미한다. 오늘날 특정 국가들은 사이버 공간에서의 상당주의 원칙 적용요건으로 국가의 '실제적 인식' 수준을 들고 있다.[315] 영토국의 실제적 인식에 대한 구체적인 예는 다음과 같다. 가령, 자국의 관할권 내에서 타국에 유해한 영향

---

[313] Colin Patrick, supra note 228, p.599; Eric Talbot Jensen, "The Tallin Manual 2.0: Highlights and Insights", Georgetown Journal of International Law, Vol. 48 (2017), p.744. ("For a state to be responsible for applying due diligence to prevent transboundary harm, the state must have knowledge of the harm.")

[314] 탈린매뉴얼 2.0, Rule 6(37).

[315] Andraz Kastelic, supra note 150, p.13.

을 미칠 수 있는 사이버 조작이 진행 중이라는 사실에 관하여 신뢰할 수 있는 정보를 획득한 상황은 '실제적 인식'에 이르렀다고 볼 수 있을 것이다.[316] 또한, 정보기관 혹은 국가기관이 운영하는 사이버 전담 팀, 사이버 경찰 등이 이러한 위험을 직접적으로 감지하고 이러한 사안에 대해 보고 받은 경우 역시 국가가 '실제적 인식'에 도달한 것으로 볼 수 있을 것이다.[317]

2. 추정적 인식 (constructive knowledge)

상당주의 의무의 발동 요건인 인식의 기준과 관련하여 보다 복잡한 판단을 요하는 영역은 '추정적 인식'(constructive knowledge)이다.[318] 즉, 영토국이 자국의 영토가 타국에 피해를 입히는 사이버 조작을 위하여 사용이 되고 있었다는 것을 '알았어야' (should have known) 하는 경우, 이를 방지하거나 예방하기 위한 적절한 조치를 취하지 않았다면 상당주의 원칙을 위반한 것으로 간주해야 하는가? 이때의 '알았어야' (should have known) 한다는 것의 의미는, 결과적으로 실제적인 인식에 도달하지는 못하였지만, 제반 사실을 종합적으로 판단하였을 때 객관적으로 해당 사실을 '알았어야 한다는 것'을 의미한다.[319] 상당주의 원칙의 적용 요건으로 '추정적 인식'의 기준을 적용한다면, 이는 앞서 언급한 '실제적 인식'보다 영토국의 의무의 범위를 넓히는 결과를 가져온다.[320] 탈린매뉴얼의 국제전문가그룹은 인식의 기준에 '추정적 인식'을 포함하여야 한다고 주장하며 그 근거로서 ICJ의 Corfu Channel 판결과 Genocide 을 들고 있다. 즉, 국가는 실제로 위법한 사이버 행위를 인식하지 못하였다고 하더라도, 자국의 영역이 그 작업에 이용되는 것을 객관

---

316 Robert Kolb, supra note 290, p.124.

317 Ibid., pp. 123-124; 이종현, supra note 189, p.84; 탈린매뉴얼 2.0, Rule 6(37).

318 Robert Kolb, supra note 290, p.124.

319 Andraz Kastelic, supra note 150, p.14.

320 Ibid., p.13. ("The norm could also be subject to a wider interpretation. Accordingly, it could be argued that a State fails to meet the normative expectation when it does not employ its best efforts to prevent a cyber operation about which it should know.")

적으로 알았어야 했다면 상당주의 의무를 위반한 것이라고 간주된다.[321] 한편, 네덜란드, 스위스, 루마니아 등은 상당주의 의무의 발동 요건인 인식의 기준으로, 실제적 인식과 추정적 인식을 모두를 포함한다는 자국의 견해를 자발적 국가 기여를 통하여 제출하였다.[322]

여전히 문제가 되는 것은 '알았어야' (should have known) 하는 상황이 구체적으로 무엇인지에 대한 구체적인 기준이 부재하다는 것이다. 전통적인 국제법 영역에서도 상당주의 원칙을 적용함에 있어서 추정적 인식의 구체적 범위가 문제되었던 바 있다. 사이버 공간의 특성상 이러한 적용상 기준의 모호함이 더욱 심화된다.[323] 그러나 인식의 기준으로 '추정적인 인식'을 채택한다는 사실이 영토국으로 하여금 타국에 부정적인 영향을 미치는 사이버 공격에 대하여 예방적 조치를 취하거나, 당해 영토국이 감시의 의무를 부과하는 것을 의미하지는 않는다.[324] 즉, 영토국은 자국의 관할 내의 사이버 기반시설이 타국에 위해가 되는 사이버 조작을 위한 용도로 사용되지 않도록 지속적인 감시를 해야 하는 등의 '적극적인 작위 의무'를 부담하지는 않는다. 이는 추정적 인식의 범위를 과도하게 확장하여 영토국의 부담을 가중시키는 결과를 낳게 됨으로써 합리적인 기준이라고 보기 어려울 것이기 때문이다.

제 4 절. 사이버 공간에서 상당주의 의무의 규범적 지위

지금까지 사이버 공간에서 상당주의 의무가 적용되어야 할 필요성과 적용 가능성을 검토하였으며, 이러한 검토 사안을 바탕으로 상당주의 의무가 사이버 공간에 적용됨에 있어서 합의되어야 할 세부적 쟁점을 간략하게 살펴보았다. 아래에서는 이러한 상당주의 의무가 사이버 공간에서 어떠한 규범적

---

[321] 탈린매뉴얼 2.0, Rule 6(39).

[322] UNGA 컨펜디엄, p.59/142, p.76/142, p.91/142.

[323] Collin Patrick, supra note 257, p.593. ("The Manual does, however, recognize that advances in malware and other cyber capabilities may render proving constructive knowledge extremely difficult.")

[324] Ibid., p.593; 탈린매뉴얼 2.0, Rule 6 (41),(42).

지위를 갖는지에 대해서 본격적으로 논의하고자 한다. 오늘날 '국제법의 법원'(source of law)을 설명함에 있어서 출발점이 되는 국제사법재판소(ICJ) 규정 제38조 제1항은 '국제 협약'과 '국제 관습'을 가장 중요한 재판의 준칙으로 삼고 있다.[325] 국제협약은 체약국에 대하여 구속력을 가지는 반면, 국제관습은 국가들의 일반관행을 기반으로 하여 명시적으로 동의를 표하지 않은 모든 국가를 구속할 수 있는 유일한 국제법 유형이다.[326] 현재 사이버 법리의 영역에서 상당주의 의무의 국제법적 지위나 동 의무의 구속력 여부를 명확하게 적시한 국제협약은 존재하지 않는다. 따라서, 사이버 공간에서 상당주의 의무의 국제법적 지위를 논의하기 위해서는 결국 상당주의 의무가 '국제관습법'의 지위를 갖는지 여부가 검토되어야 한다.

상당주의 의무에 관한 각종 국가의 실행, 학계 및 국제기구에서의 논의를 종합하였을 때, 사이버 공간에서 상당주의 의무가 국제관습법적 지위를 획득하였다고 간주하는 것은 시기상조라고 판단된다. 상당주의 의무는 피해국의 권리를 실효적으로 구제하고 사이버 공간의 평화를 달성하기 위한 규범으로 주목받고 있지만, 여전히 국제사회는 사이버 공간 상 상당주의 의무의 국제법적 지위에 대해서 원만한 합의에 도달하지 못하였기 때문이다. UN 정부전문가그룹에서는 상당주의 의무를 구속력 있는 '국제법'이 아닌, '비구속적, 자발적 규범'의 영역에서 검토하고 있으며, 나아가 자발적 국가기여를 제출한 일부 국가 역시 동 의무의 국제관습법 지위 획득에 부정적인 견해를 취하고 있다. 한편, 국제환경법 영역에서 상당주의 의무의 규범적 지위를 확장하여, 사이버 공간에서도 동 의무가 '국제관습법'으로서의 지위를 확립하였다는 일각의 주장 역시 충분한 근거가 뒷받침되지 못한 것으로 판단된다. 본 연구에서는 이러한 내용을 바탕으로 상당주의 의무가 사이버 공간에서의 국제법적 구속력이 부재하다고 판단하는 바, 아래에서는 관련된 내용에 대해 상세하게 검토하고자 한다.

---

[325] 정인섭, supra note 44, p.43-45.

[326] 김상걸, "입법적 국제관습법과 법적확신 개념의 재구성", 『국제법학회논총』, 제65권 제1호 (2020), p.9.

I. UN 정부전문가그룹에서의 논의

1. 사이버 안보 담론에 대한 UN 정부전문가그룹 논의의 '대표성'

사이버 공간에서의 상당주의 의무가 국제관습법적 지위를 획득하였는지 검토하기 위하여 우선 UN 정부전문가그룹에서의 논의 내용을 살펴보고자 한다. 상당주의 의무의 국제법적 지위에 관련하여 UN 정부전문가그룹에서 이루어지는 논의가 보다 중요한 이유는, 국제법을 창설하는 종국적인 주체가 다름 아닌 '국가'라는 점에 있다. UN 정부전문가그룹의 회의는 UN 산하의 국제회의이며 회의를 통해 도출되는 합의는 곧 사이버 공간에 대한 주권 국가 사이의 합의를 의미한다.[327] 따라서 UN 정부전문가그룹의 상당주의 의무에 관한 견해는 동 의무의 '국제법적 지위 형성' 과정에 있어서도 충분한 영향력을 행사할 수 있을 것이라고 판단된다. 물론 정부전문가그룹의 논의 과정에는 UN 회원국 중 일부 국가만이 참여한다는 사실 때문에 구성이 제한적이라는 비판도 존재한다. 그러나, 본 논의에 참여하고 있는 국가는 '형평한 지리적 배분'(equitable geographical distribution)에 기반하여 분배되었으며, 미국, 중국, 러시아, 프랑스, 영국 및 독일과 같은 주요 사이버 역량 국가들이 논의 과정에 포함되었다는 점에서 사이버 안보에 관한 동 그룹의 최종보고서가 국제사회에서의 대표성을 가질 수 있을 것이라고 판단된다.[328] 더불어, EU 등의 국제기구를 비롯한 다수의 국가가 UN 정부전문가그룹의 논의에 관한 자국의 견해를 개별적으로 제출하였으며 국가의 공식 연설에 GGE 최종보고서의 내용을 원용한 바 있고, 더 나아가 정부전문가그룹 논의를 기반으로 자국의 사이버 안보 법제를 점검한다는 사실을 종합적으로 고려하였을 때 동 그룹에서 이루어지는 논의가 사이버 안보 측면에서 갖는 권위를 확인할 수 있다.[329]

---

[327] 박노형·김효권, supra note 7, p.62.

[328] 박노형·정명현, supra note 77, p.174; 박주희, supra note 126, p.2.

[329] 박주희, ibid., p.2; UNGGE의 자발적 국가기여 문서 제출과는 별개로 상당수의 국가가 'UN 총의 결의'(A/RES/73/27)에 따라 사이버 공간에 적용되는 국제법에 관한 자

2. '비구속적·자발적 규범' 의제

UN 정부전문가그룹은 제4차 GGE 회의를 기점으로 사이버 공간에 적용되는 규범을 '국제법(international law)' 의제와 '비구속적·자발적 규범(norms, rules and principles for the responsible behaviour of States)' 의제로 구분하여 논의해 왔다.[330] 이때, 상당주의 의무는 국제법이 아닌 '비구속적·자발적 규범'으로 분류되었는데,[331] 이는 사이버 공간에서 상당주의 의무의 규범적 지위와 관련해서 상당한 시사점을 갖는다고 볼 수 있다. UN 정부전문가그룹 보고서 내의 '국제법'은 조약 등이 부재한 경우에도 국가들이 준수해야 할 국제관습법을 가리킨다. 그러나, 국제법과 달리 상당주의 의무가 포함된 '규범'의 경우에는 국제공동체의 기대를 반영하고 책임 있는 국가 행동의 기준을 설정하지만, 국제법상 구속력이 없으므로 국가의 행위를 제한하거나 금지할 수 없다는 명백한 한계를 가진다.[332] 즉, 국가들은 강제력이 있는 '국제법' 의제로 다루기 부담스러운 사항들을 '자발적 규범'의 차원에서 논의함으로써 보다 유연한 이해를 모색하고자 하였다고 볼 수 있다.[333] 이러한 맥락에서 상당주의 의무가 국가의 행위에 대하여 구속력을 갖는 '국제법' 의제가 아닌 '자발적, 비구속적 규범'에 포함되었다는 사실은 상당주의 의무가 국제관습법이 되기 위한 국제사회의 충분한 법적 확신과 일반적 관행이 축적되지 못하였음을 방증하는 대목이라고 할 수 있다.

국의 견해와 평가를 제출하였다. 우리나라 역시 사이버 공간에 적용되는 국제법에 관한 견해와 평가를 두차례 제출한 바 있다.

[330] UNGA 제4차 보고서.

[331] UNGA 제4차 보고서, p.8/17.

[332] UNGA 제4차 보고서, p.7/17. 원문은 다음과 같다. "… Accordingly, norms do not seek to limit or prohibit actions that is otherwise consistent with international law. Norms reflect the expectations of the international community, set standards for responsible States behaviour and allow the international community to assess the activities and intentions of States."

[333] 박주희, supra note 126, p.2.

3. '자발적 국가 기여'를 통해 드러난 한계

한편, UN 정부전문가그룹 제6차 회의 부속서의 '자발적 국가기여'를 통해 제출된 국가의 견해는 사이버 공간에서의 상당주의 의무가 국제관습법적 지위를 확립하지 못하였음을 보여주는 또 다른 근거가 된다. 회의의 참여국 가운데 총 15개국이 자발적 국가기여를 제출하였으며, 그 중 상당수의 국가가 사이버 공간에 적용되는 '상당주의 의무'에 관한 자국의 견해를 자발적 국가기여에 포함하였다. 사이버 공간에서 적용되는 규범인 상당주의 의무에 많은 국가가 관심을 표하였다는 점은 향후 상당주의 의무에 대한 활발한 논의로 이어질 수 있다는 점에서 매우 고무적이다. 그러나 동시에 자발적 국가기여는 상당주의 의무의 규범적 강제력의 측면에서는 한계점을 보였다는 지적도 가능하다. 이는 다름 아닌 상당주의 의무의 국제관습법적 지위를 명백히 부정하거나 혹은 동 의무에 대해 언급하지 않은 국가의 대다수가 당해 논의의 주축을 이루는 사이버 핵심 역량 국가이기 때문이다.

가령, 사이버 공간에 관한 논의에 있어 서방 국가의 의견을 대표하는 미국과 영국은 상당주의 의무의 필요성을 인정하는 것과는 별개로, 동 의무가 국제관습법의 지위를 획득하였다고 판단하는 것은 시기상조라는 입장을 밝힌 바 있다.[334] 영국은 제6차 보고서의 Norm 13(c)에 명시된 상당주의 의무의 필요성과 유용성을 인정하지만, 동 의무가 국제관습법적 지위를 갖기에는 충분한 국가관행이 뒷받침되지 못하고 있다고 주장한다. 그리고 그 근거로, 상당주의 의무가 '비구속적 규범'(non-binding norm)으로 분류되었다는 점에 주목한다.[335] 미국 역시 다수의 국가가 상당주의 의무에 대한 관심을 가지고 있다는 것을 인지하고 있으나, 여전히 동 의무가 '국제법 영역에서의 일반적 의무'(general obligation under international law)가 되기에는 충분한 국가

---

[334] 박노형·김효권, supra note 7, p.186; 상당주의 의무에 관한 영국과 미국의 견해는 UNGA 컨펜디엄, pp.106-135/142, pp.136-142/142 각각 참조.

[335] UNGA 컨펜디엄, p.117/143. ("But the fact that States have referred to this as a non-binding norm indicates that there is not yet State practice sufficient to establish a specific customary international law rule of 'due diligence' applicable to activities in cyberspace.")

실행과 법적의무가 뒷받침 되지 못하고 있음을 지적하였다.[336] 한편, 비서방 진영의 대표적 국가인 러시아와 중국의 경우, 자발적 국가 기여를 통해 상당주의 의무에 대한 자국의 견해를 언급하고 있지 않다는 사실 역시 주목할 만하다. 중국은 '자발적 국가 기여' 자체를 제출하지 않았으며, 러시아는 이를 제출하였으나, 상당주의 의무에 관한 내용을 포함하지 않았다.[337] 물론 상당수의 국가가 자발적 국가기여 및 여타의 국가 문서를 통해 사이버 공간에서의 상당주의 의무가 국제관습법적 지위를 가진다는 견해를 표명한 바 있다. 그러나 이러한 사실을 감안하더라도 사이버 안보 담론에서 미국, 영국, 중국, 러시아의 영향력과 파급력, 그리고 이들의 사이버 역량을 종합적으로 고려하였을 때, 상당주의 의무에 관한 이들 국가의 견해는 결코 무시할 수 없는 것이 된다.[338] 따라서, 사이버 담론에 관한 각 진영 대표 국가이자 사이버 핵심 역량 국가인 이들의 견해를 종합적으로 고려할 때, 사이버 공간에서의 상당주의 의무에 대한 국제사회의 일반적 관행(general practice)이 충족되지 않았으며 나아가 국제관습법적 지위 역시 아직은 획득하지 못하였다고 판단할 수 있을 것이다.

II. 사이버 공간의 특수성과 상당주의 의무의 신축성

일각에서는 상당주의 의무가 사이버 공간에서 이미 국제관습법의 지위를 획득하였다고 주장한다. 이들의 주장은 상당주의 의무가 국제환경법 영역에서 국제관습법적 지위를 획득하였음을 고려할 때, 동 의무가 새로운 국제법 영역인 사이버 공간에 적용되는 과정에서 '규범적 지위' 역시 동일하게 적용

---

[336] UNGA 컨펜디엄, p.141/142.

[337] 사이버 안보에 관한 러시아의 견해는 다음을 참조. UNGA 컨펜디엄, pp.79-81/142.

[338] 사이버 공간에서 상당주의 의무에 관해 논의함에 있어서 러시아와 중국이 갖는 견해가 적극적으로 고려되어야 한다. 이들은 상당한 사이버 역량을 갖추고 있을 뿐더러, 오늘날 발생하는 상당수의 사이버 공격과 직간접적인 연관성을 가진다. 가령, 러시아 정부가 배후에 있을 것이라고 추정되는 상당한 규모의 사이버 공격이 빈번하게 발생하고 있으며, 중국의 경우 북한을 비롯한 여타 국가의 사이버 공격 과정에서 제3국 경유지로 자주 활용된다.

되는 것이 타당하다는 점에 근거한다. 즉, 국제사회는 현존하는 국제법이 사이버 공간에도 적용된다는 점에 대하여 합의를 하였고 그렇다면 국제환경법에서 관습법의 지위를 갖는 상당주의 의무가 사이버 공간에서도 동일한 법적 지위를 가지는 것이 타당하다는 것이 바로 이들의 논리인 것이다. 이들의 주장처럼 국제환경법 영역에서 국제관습법의 지위를 갖는 상당주의 의무가 곧바로 사이버 공간에서도 동일한 법적 지위를 갖는다고 간주하는 것은 과연 타당한가? 이러한 논리는 사이버 공간의 특수성과 상당주의 의무의 신축적이고 유연한 특성 모두를 간과한 것으로, 사이버 공간에서 상당주의 의무가 국제관습의 지위를 획득하였다고 간주하는 것은 시기상조라고 판단된다.

2011년 미국 백악관은 '사이버 공간에서의 국제 전략(International Strategy for Cyberspace)'을 발표한 바 있다. 백악관은 해당 성명을 통해 사이버 공간을 규율하기 위한 새로운 국제관습법에 대한 논의가 요구되지 않으며 전통적인 국제법이 사이버 공간에 적용되는 것 역시 진부하지 않다는 견해를 표명하였다.[339] 다만, 백악관은 사이버 공간의 '독특한 특성'으로 인해 기존의 국제규범이 적용되는 구체적인 방식과 이러한 규범을 적용함에 있어 어떠한 추가적인 이해가 필요한지에 대해서는 별도의 작업과 논의가 필요하다는 점을 강조하였다.[340] 이러한 시각은 2012년 당시 미국 국무부 법률자문을 역임하였던 Harold Koh 교수의 견해를 통해서도 확인할 수 있다. Koh 교수는 기존의 국제법이 사이버 공간에 적용된다는 점에 대하여 일부 긍정하면서도 사이버 공간이 갖는 특수한 성질을 고려할 때, 기존 규범을 사이버 공간에 적용하는 과정에서 추가적인 논의와 함께 기존 규범에 대한 재평가가 요구된다는 견해를 표명한 바 있다.[341] 현행 국제법을 사이버 공간에 적용함에 있어서의 백악관과 Koh 교수의 견해는 사이버 공간에서의 상당주의 의무의 법적 지위를 논하는 과정에서도 유의미하게 활용될 수 있다.

---

[339] White House, supra note 71, p.9.

[340] Ibid., pp.9-10.

[341] Harold Hongju Koh, "International Law in Cyberspace", Harvard International Law Journal, Vol. 54 (2012), p.3.

다시 말해, 국제환경법 및 여타의 국제법 분야에서 활용되던 상당주의 의무가 사이버 공간에 적용될 때 사이버 공간의 독특한 속성을 고려하여 추가적인 이해 내지는 별도의 논의 과정이 요구될 수 있다는 판단이 가능하다. 실제로 상당주의 의무는 국제환경법을 비롯하여 다양한 국제법 영역에서 원용되어 왔으나 각 영역에 적용됨에 있어 핵심적인 근원은 같지만 세부적인 측면에서는 동일하지 않은 모습을 보여왔다. 다시 말해, 상당주의 의무는 적용되는 분야의 특성과 구체적인 맥락 혹은 상황에 맞게 신축적(flexible)인 내용과 범위를 가지고 그 역할을 해오고 있으며, 상당주의 의무가 다른 국제법의 영역에 '그대로' 적용되는 것을 의미하지 않는다는 것이다.[342] 따라서, 상당주의 의무는 각 국제법 영역에 적용됨에 있어 동일한 기준을 근거로 취급되고 적용되는 것이 아니라, 오히려 상황에 따라 구체적인 내용과 범위가 적절히 변형되어 적용된다고 보는 것이 타당하다. 그렇다면, 사이버 공간이 갖는 특수성을 감안할 때, 상당주의 의무가 국제환경법에서 갖는 구체적 기준 내지는 범위 등을 사이버 공간에서 그대로 적용하는 것은 바람직하지 못하다. 같은 맥락에서, 상당주의 의무가 국제환경법 영역에서 국제관습법의 지위를 갖는 것을 근거로 이를 '그대로' 적용하여 상당주의 원칙이 사이버 영역에서도 국제관습의 지위를 갖는다고 판단하는 것 역시 '상당주의 의무'의 신축적 특성과 사이버 공간의 특수성을 제대로 파악하지 못한 것으로 볼 수 있다.

[342] 이종현, supra note 189, p.191; Abhijeet Shrivastava & Rudraksh Lakra, "Revisiting due diligence in cyberspace: crafting international law's arsenal against transboundary Botnets", International Journal of Law and Information Technology, Vol. 30, Issue 3 (2022), p.371.

제 5 장. 사이버 공간에서 상당주의 의무의 활성화를 위한 법적 쟁점과 한계

제 1 절. 상당주의 의무의 활성화를 위한 법적쟁점 검토

오늘날 국제사회는 사이버 공간에 상당주의 의무가 적용되어야 할 필요성에 대해 절감하고 있다. 또한 상당수의 국가와 국제기구 역시 사이버 공간에서 상당주의 의무의 적용 가능성에 대해서도 긍정적인 입장을 취하고 있는 것으로 보인다. 상당주의 의무가 사이버 공간에 적용되는 규범으로 보다 큰 주목을 받게 된 이유는 동 의무가 불법적인 사이버 조작과 관련한 '제3국'에 부여되는 의무라는 점에 기인한다. 즉, 사이버 공격의 특성상 공격의 귀속과 국가책임법의 적용이 용이하지 않고, 더불어 오늘날 발생하는 사이버 공격 과정에서 제3국의 역할이 점차적으로 확대됨에 따라 공격과 관련한 제3국, 가령, 경유국에게 상당주의 의무가 부여되어야 할 필요성과 그 유용성이 더욱 증대되고 있는 실정이다. 이처럼 상당주의 의무는 사이버 공간에 적용됨으로써 피해국의 권리를 구제하고 사이버 공간의 평화적 활용을 도모하기 위한 수단으로서 효과적인 역할을 수행할 것으로 기대된다.

그러나 이와 같은 상당주의 의무의 적용상의 이점과는 별개로, 사이버 공간에 상당주의 의무를 실질적으로 적용함에 있어서는 여전히 추가적인 검토와 논의를 필요로 하는 법적 쟁점이 존재한다. 상당주의 의무가 사이버 공간에 적용되어서 본연의 역할을 다하기 위해서는 추가적인 법적 쟁점에 대한 충분한 논의가 필요하다. 이러한 논의의 필요성에 따라서 제5장에서는 우선 상당주의 의무를 사이버 공간에 적용함에 있어서 제기되는 대표적인 법적 쟁점에 대하여 검토하기로 한다. 보다 구체적인 논의는 1) 상당주의 의무의 국제법적 구속력 부재에 따른 규범적 가치 확보의 필요성, 2) 상당주의 의무의 구체적 적용 기준 설정의 필요성, 3) 상당주의 의무의 집행력 확보 수단 확립의 필요성의 순서로 진행하고자 한다.

I. 국제법적 구속력 부재에 따른 규범적 가치 확보

1. 구속력 부재에 따른 한계와 논의의 필요성

국제사회는 사이버 공간에서 상당주의 의무의 역할에 대해 높은 관심을 표하고 있으며 '자발적 국가기여'를 제출한 15개 국가 중 상당수의 국가는 동 의무를 국제관습법으로 인식하고 있다. 그러나 여전히 UN 정부전문가그룹의 논의 과정에서 상당주의 의무는 '국제법'(international law)이 아닌 '비구속적이고 자발적인 규범(norm)'으로 분류된다. 더불어, 상당주의 의무는 국가들의 실행(practice)을 통해 검토되고 있기도 하다. 이러한 사실은 곧 사이버 공간에서 상당주의 의무에 대한 지대한 관심에도 불구하고 국제사회가 사이버 공간에서 동 의무의 국제법적 지위에 대해서는 원활한 합의에 도달하지 못하였음을 의미한다. 즉, 사이버 공간에서 상당주의 의무는 일부 국가와 국제기구의 시각에 따라서 국제관습법의 지위를 획득한 것으로 여겨지기도 하나, 또 다른 측면에서는 여전히 비구속적이고 자발적인 참여를 요하는 규범으로 간주되기도 하는 것이다.

규범적 지위가 확립되지 않음에 따라 발생하는 이러한 혼란은 기존의 규범이 새로이 대두되는 영역에 적용될 때 드물지 않게 발견되는 현상이다. 그러나 상당주의 의무의 도입 목적과 동 의무의 사이버 공간에서의 역할을 고려한다면 사이버 맥락에서 상당주의 의무가 갖는 규범적 가치는 필수적으로 검토되어야 한다. 즉, 공격 결과에 대한 국가책임법의 적용이 용이하지 않고 공격의 직접적인 배후국과 피해국 이외의 '제3국'이 공격 과정에 관여하는 상황이 점차적으로 확대되는 사이버 공격의 특성을 고려할 때, 피해국의 권리를 효율적으로 구제하고 사이버 공간의 평화로운 활용을 도모하기 위한 수단으로서 상당주의 의무는 그 도입이 절실히 요구된다. 그렇다면 사이버 공간에서 상당주의 의무가 국제법적 구속력을 갖지 못하는 현 시점에서 동 의무의 규범적 가치와 역할에 대해 논하는 것은 향후 상당주의 의무가 사이버 공간에서 실효적인 역할을 수행하기 위해 필연적으로 논의되어야 할 법적 쟁점임이 분명하다. 이러한 논의의 실익에 기하여 아래에서는 우선 상당주의

의무가 국제법적 구속력을 획득하지 못한 현 상황에서 어떠한 규범적 가치를 지닐 수 있으며 또한 어떠한 역할을 수행할 수 있는지에 대해서 검토하고자 한다. 나아가, 장기적인 관점에서 상당주의 의무가 사이버 공간에서 국제관습법의 지위를 획득할 가능성에 대하여 추가적으로 검토하고자 한다.

2. 상당주의 의무의 규범적 가치 검토 – "비구속적 규범"

사이버 공간에서 상당주의 의무가 실효성을 획득하기 위한 가장 확실한 방법은 동 의무가 모든 주권 국가를 구속할 수 있는 국제관습의 지위를 획득하는 것이다. 그러나 UN 정부전문가그룹 내부에서 조차 상당주의 의무의 규범적 지위에 관한 합의를 이루지 못한 현 시점에서 동 의무의 국제관습법적 지위 획득을 기대하는 것은 다소 이른 감이 있다. 또한 동 의무가 범세계적 구속력을 갖추는 구체적인 시기를 예측하는 것 역시 매우 어려운 일이다.[343] 그렇다면 상당주의 의무가 국제관습법 지위의 획득에 난항을 겪거나 혹은 명백하게 국제법적 강제력을 가지지 못하는 현재의 상황이 지속될 때 사이버 공간에서 상당주의 의무가 어떠한 규범적 가치를 지닐 수 있으며, 또한 구체적으로 어떠한 역할을 수행할 수 있는지에 관한 논의는 보다 현실적인 필요성을 갖는다고 할 것이다. 이러한 논의의 필요성에 따라 아래에서는 사이버 공간에서 비구속적 규범의 지위를 갖는 상당주의 의무의 규범적 가치와 역할에 대해서 검토하고자 한다. 본 연구는 사이버 공간에서 비구속적 규범의 지위를 갖는 상당주의 의무가 '연성법'(soft law)으로서 일정한 역할을 수행할 수 있을 것으로 판단하였다. 아래에서는 우선 연성법의 가치 및 역할에 대하여 검토한 뒤, 상당주의 의무의 연성법으로서의 역할에 대해서 상세하게 다루기로 한다.

[343] Jan Martin Lemnitzer, supra note 281, pp. 795-796.

1) 연성법의 가치 및 역할 검토

신흥 기술이 빠르게 발전함에 따라 오늘날 국제법의 전통적인 법리가 한계를 드러내고 그 자리를 비정형적이고 끊임없이 진화하는 '연성법'이 대체하는 현상을 쉽게 목격할 수 있다.[344] 빠르게 발전하는 과학 기술은 국가의 안보와 국가 간 이익 관계에 크나큰 영향을 미치지만 이러한 변화에 대응하여 기존의 국제조약을 개정하거나 후속 협상을 개시하는 것은 결코 쉽지 않다.[345] 전통적인 국제 규범을 새롭게 대두되는 영역인 사이버 공간에 적용함에 있어서도 새로운 기술과 기존 법리 간의 괴리는 쉽게 확인될 수 있다. 특히 사이버 공간에서 상당주의 의무의 규범적 지위에 관한 논의에 있어 그 갈등이 더욱 첨예하다. 확인된 바와 같이, 상당주의 의무는 사이버 공간에서 국제관습의 지위를 명백하게 획득하지 못한 것으로 보인다. 그러나 상당주의 의무가 비록 구속력을 갖는 국제관습의 지위를 획득하지는 못하였으나 여전히 사이버 공간에서의 동 의무가 '연성법'으로서 일정한 역할을 할 수 있을 것으로 판단된다.

오늘날 국제법에서 연성법을 일컫는 독립된 정의는 부재하며 연성법은 학자에 따라 다양하게 정의된다. 우선, '연성법'(soft law)을 수범자에 대하여 직접적인 법적 구속력을 갖지는 않으나, 사회구성원의 행위에 실질적인 영향력을 미치기 위하여 만들어진 행위규범(rule of conduct)의 일종으로 정의하는 견해가 존재한다.[346] 또한 연성법은 공공기관 혹은 사적 기관이 설정한 기준, 원칙 등의 총체로서 그 준수에 대한 강제력이 부재한 규범을 일컫기도 한다.[347] 국제법학계의 이론 파편화를 고려할 때 연성법을 국제법상 단일한

---

[344] Ryan Hagemann, Jennifer Huddleston Skees & Adam Thierer, "Soft Law for Har Problems: The governance of emerging technologies in an uncertain future", Colorado Technology Law Journal, Vol 17, No. 1 (2018), p.38.

[345] Ibid., p.40.

[346] Francis Snyder, "Soft Law and Institutional Practice in the European Community", The Construction of Europe (1994), p.197.

[347] Melvin Aron Eisenberg, " The Architecture of American Corporate Law: Facilitation and Regulation", Berkeley Business Law Journal, Vol. 2 (2005), p.182.

개념으로 다루는 것은 위험한 시도가 될 수 있음을 지적하며, 경성법 혹은 국제사법재판소 규정 제38조에 규정된 내용에 대한 잔여 범주로 연성법을 정의하고자 하는 의견 역시 주목할 만 하다.[348] 한편, 법학자들마다 '연성법 문서'를 분류하는 기준이나 범주에도 상당한 차이가 있다. 일반적으로 UN협정이나 선언, 또는 국제단체에서 배포한 가이드라인은 연성규범의 범주에 속한다고 볼 수 있다.[349] 연성법 문서를 매우 좁게 규정하는 경우, 오직 연성적인 내용으로 된 조약과 법규범창설이 의도된 결의만이 연성법 문서의 범주에 포함되기도 한다.[350] 이보다 넓게 연성법을 규정하는 경우에는 국제기구의 결의, 행동계획, 아직 발효되지 않은 조약의 조문, 국제협약에 대한 해석선언, 비구속적 합의, 국제기관이 채택하거나 국제회의에서 채택된 권고 및 보고서가 포함된다고 보는 견해가 있다.[351]

그렇다면 주권 국가에 대하여 직접적인 구속력을 가지지 않는 연성법은 국제사회에서 어떠한 역할을 수행해 왔으며 또한 어떠한 규범적 가치를 지니는가? 조약체결과정의 일부로서 연성법의 규범적 지위와 역할을 살펴보면 구속력이 없는 연성법 문서가 종종 다자조약 체결을 선도하는 과정의 첫 단계가 되는 경우가 많다. 가령, 다수의 인권 분야의 조약은 유엔 총회의 결의를 출발점으로 삼아서 결과적으로는 동일 주제 하에서 동일한, 또는 유사한 내용의 조약이 채택되는 과정을 거쳐왔다.[352] 한편, 연성법은 종종 국제관습법의 형성과 변경에 대해서도 영향을 미친다는 견해가 존재한다.[353] 조약이나 관습국제법은 성립에 상당한 시일이 걸리고 국제사회 변화에 즉각적인 대응을 하지 못하기 때문에 일종의 잠정 대응방안으로 연성법이 나타난다는 것이다. 연성법은 새로운 관습국제법의 형성에 자극을 주기도 하며 그 형성과정

---

348 정경수, "국제법상 연성법의 재인식", 『안암법학』, 제34호 (2011), pp. 942-943.

349 연성법의 상대적인 개념인 '경성법'(hard law)이란, 일반적으로 국가에 의해 입법권한이 위임된 기관에 의해 정식으로 제정 및 공포 절차를 밟은 법률이나 법규명령 등 기타 규범을 의미한다.

350 김석현, "국제법에 있어서 Soft Law", 『국제법평론』, 통권 제8호 (1997), pp.25-26.

351 Daniel Thürer, "Soft Law", Max Plank Encyclopedias of International Law [MPIL], (2009), paras. 10-16.

352 정경수, supra note 348, p.950.

353 Ibid., pp.951-952.

에서 국가관행이나 법적 확신의 증거가 될 수 있다.[354] 이러한 측면에서 본다면 연성법은 법적 구속력을 도출하는 합의 또는 경성규범으로 나아가기 위한 첫걸음으로 여겨지며, 장기적으로 사회문화규범과 관습을 형성하는데 일조한다.[355] 한편, 연성법은 '법률을 선도하는(para-law)' 기능을 가진다고 보는 견해도 존재한다. 이러한 견해에 따르면 연성규범은 사회구성원의 행위에 대하여 안내 또는 조정하는 기능을 담당하며 이를 통해 국가 정책목적이나 방향이 더욱 효율적일 수 있도록 조력한다. 이는 권고(recommendation)나[356] 결의안(resolution) 또는 윤리강령(codes of conduct)의 형식으로 나타난다.[357]

2) 상당주의 의무의 연성법으로서 역할 검토

국가간 이익의 다양성, 사적행위자의 출현, 신흥 기술의 발전 등으로 인해 다양한 국제법의 영역에서 새로운 조약 혹은 보충의정서의 체결이 어려워지는 상황이 빈번하게 발생하고, 이러한 상황을 해결하기 위해서 국제사회에서는 '연성법'을 채택하는 방식이 점차 증가하고 있다는 점은 앞서 확인한 바와 같다. 즉, 연성법은 새로이 대두되는 국제법 분야에서 자주 발견되고, 국가 간 이해 관계의 상충으로 인해 구속력 있는 합의 도출이 어려울 경우에 그 대안으로 자주 활용된다고 볼 수 있다.[358] 오늘날 다수의 국제법 영역에서 연성법이 활용되는 이러한 경향은 국가 및 진영 간의 이익 충돌이 극심하고, 비국가행위자의 대두 등으로 인해 단기적이고 범세계적인 합의 도출을 기대하기 어려운 사이버 공간에서의 규범 형성 과정에서도 시사하는 바가 있다. 특히 연성법은 사이버 공간에서 '상당주의 의무'의 규범적 지위 및 역할과 관련하여 논의의 실익이 있을 것으로 판단된다. 상당주의 의무는 공격과 관련된 제3국에 부여되는 의무라는 점에서 사이버 안보의 측면에서 명백한 적용

---

354 정인섭, supra note 44, p.81.

355 최난설헌, "연성규범의 기능과 법적효력 -EU경쟁법상 논의를 중심으로-", 『법학연구』, 제16집 제2호 (2013), p.97; Daniel Thürer, supra note 351, para. 32, 34.

356 Daniel Thürer, supra note 351, para. 35.

357 최난설헌, supra note 355, p.98.

358 정인섭, supra note 44, p.81.

상 이점이 있지만, 동시에 이러한 상당주의 의무의 특성은 사이버 공간이 고도로 연결된 공간이라는 점을 고려할 때 국가로 하여금 동 의무에 대한 강제력 부여를 기피하게 만드는 기제로 작용하기도 한다. 이처럼 국가적, 정치적 이해 관계의 충돌에 기해 상당주의 의무의 법적 지위에 관한 합의가 어려운 현재의 시점에서 '연성법'의 지위를 가지는 상당주의 의무가 사이버 공간 내에서 어떠한 역할을 수행할 수 있는지에 대해 검토할 필요가 있다.

상당주의 의무가 연성법으로서 사이버 공간에서 어떠한 역할을 할 수 있는지에 관해 논하기에 앞서, 사이버 공간에서의 상당주의 의무가 '연성법'으로 분류될 수 있는지에 대하여 간략하게 살펴보고자 한다. 이를 검토하기 위하여 UN 정부전문가그룹 차원에서 상당주의 의무가 논의되는 과정과 방식, 그리고 논의의 내용에 주목하고자 한다. 현재 국제사회에서 연성법을 정의하는 확립된 규정은 부재하다. 그러나 그 가운데 연성법을 넓게 보는 정의에 따르면, 연성법 문서는 '오직 연성적 의무만을 포함하는 조약'(treaties but which include only soft obligations)부터 '국제기구 및 지역기구가 성안하거나 수락한 비구속적 또는 자발적인 결의 및 행동규준'(non-binding or voluntary resolutions and codes of conduct formulated and accepted by international and regional organizations)까지 그 범위가 매우 넓은 것으로 판단된다.[359] 즉, 광의의 연성법과 연성법 문서에는 국제기구 혹은 지역기구 내에서 채택된 '보고서' 혹은 '자발적인 결의' 등이 포함된다고 볼 수 있는 것이다. 그렇다면, UN 총회의 결의로 설립된 UN 정부전문가그룹에서 주기적인 회의의 결과로서 채택되는 '최종보고서'와 동 문서의 규범 영역에 포함된 '상당주의 의무'(due diligence)는 각각 '연성법 문서'와 '연성 규범'으로서의 지위를 갖는다고 볼 여지가 있다.

그렇다면, 연성법의 지위를 갖는 상당주의 의무는 과연 사이버 공간에서 어떠한 역할을 수행할 수 있는가? 연성법은 새로운 관습국제법의 형성에 영향을 미치고, 이러한 의무의 준수에 관한 국제사회 전반의 기대를 창설한다.

---

[359] C. M. Chinkin, "The challenge of soft law: Development and Change in International Law", The international and comparative law, Vol. 38, No. 4 (1989), p.851.

또한 각국의 정책결정자들은 연성법을 가볍게 무시하고 이탈하는 행동을 취하기 어려우므로, 연성법은 단순한 '도덕'이나 '국제 예양'과는 구별되는 개념으로 볼 수 있다. 특히 UN 정부전문가그룹의 최종보고서 및 자발적 국가기여와 같은 연성 규범의 지위를 갖는 문서는 비록 주권 국가에 대하여 직접적인 구속력을 갖지는 못하나, 사이버 영역과 같이 일관된 국가 관행이 충분하지 못한 분야에서 국가들의 실행을 확인하고 공유할 수 있다는 점에서 의미가 있다. 특히 상당주의 의무는 구체적인 적용상의 쟁점이나 국제법적 지위 등에 있어서 국가 간 입장 차이를 좁혀야 한다는 현실적인 어려움이 존재한다. 때문에, 이러한 현실적 어려움을 극복하기 위해서는 '자발적 국가기여'를 통해 사이버 공간에 상당주의 원칙이 어떠한 방식으로 적용되어야 하는지에 대해 국가들의 지속적인 의견 교환 및 토의 과정을 거치는 것이 매우 중요하다.[360]

다른 한편, 연성법 문서는 국제관습법을 명료, 특정, 체계화하는데 기여를 하기도 하고 다자조약 체결의 첫걸음으로서 역할을 하기도 한다.[361] 또한 합의가 용이하지 않은 분야에 대한 연성법 문서의 채택은 국가들의 참여를 보다 활발하게 이끌 수 있는 방안이 되기도 한다. 상당주의 의무는 현재로서는 구속력을 갖지 않으나, 지금처럼 UN 정부전문가그룹에서의 지속적인 논의를 통해 권고안과 보고서를 발행하는 등의 논의가 활발하게 이루어진다면 궁극적으로 사이버 공간에 적용되는 국제법에 관한 법적 확신이 축적되고 또한 국가실행 역시 확립될 수 있을 것으로 판단된다. 즉, UN 정부전문가그룹에서 발행하는 보고서 및 자발적 국가 기여의 연성법 문서로서의 지위와, 정부전문가그룹 내에서 상당주의 의무가 논의되고 있는 과정 및 방식을 종합적으로 고려한다면 이러한 논의의 과정은 결국 동 원칙을 규율하는 조약 체결 내지 국제관습법의 형성의 첫걸음이 될 것으로 기대된다.

---

[360] 제6차 UNGGE에서도 현행국제법과 미래 국제법의 추가적 발전에 저촉하지 않고 사이버 공간에서 발생하는 국가 행위에 대하여 어떠한 국제법 규칙과 원칙이 적용되는지에 대한 국가 간 지속적 토의와 의견 교환이 사이버 공간에 대한 공통의 이해를 심화하고 오해를 방지하며 예측 가능성과 안정성을 증대하는데 필수적이라는 사실을 강조하고 있다. UNGA 컨펜디엄, Art.72(1) 참조; 박노형·김효권, supra note 7, p.65.

[361] 정경수, supra note 348, p.944.

3. 상당주의 의무의 규범적 가치 검토 - 국제관습법

1) 논의의 필요성

앞서 비구속적 규범의 지위를 갖는 상당주의 의무가 사이버 공간에서 연성법으로서 역할을 수행할 수 있음을 확인하였다. 그러나 상당주의 의무가 사이버 상에서의 역할을 효과적으로 수행함으로써 사이버 공간에 도입된 본연의 목적을 다하기 위해서는 궁극적으로 동 의무가 구속력 있는 규범의 지위를 획득할 필요가 있다고 판단된다. 상당주의 의무가 사이버 공간에 적용되어야 한다는 점에 대해 다수의 국가가 이해하고 동의하지만 여전히 동 의무가 국제법적 구속력을 창설하지 못하고 국가의 자발적인 참여를 독려할 수 밖에 없는 '지도 원칙'(guiding principle)의 수준에 머무른다면, 문제되는 상황에서 상당한 주의를 다하여야 하는 관련 국가의 실질적인 의무 이행을 담보할 수 없기 때문이다.[362] 또한, 상당주의 의무의 국제법적 강제력이 부재한 상황에서는 공격과 관련한 제3국의 책임을 추궁할 때 피해국이 상당주의 의무의 위반을 원용하기 어렵다는 점 역시 문제로 제기된다.[363] 이와 같은 상황이 지속된다면 결국 상당주의 의무 사이버 공간에서 실효적인 역할을 수행하지 못한 채, 오직 논의의 과정만이 존재하는 공허한 규범으로 전락하게 될 우려가 있다. 이처럼 상당주의 의무는 궁극적으로 국제법적 지위 변화의 필요성이 요구되는 바, 아래에서는 현재 비구속적 규범의 지위를 갖는 상당주의 의무가 향후 구속적 지위를 획득할 가능성에 대하여 검토하고자 한다.

2) 상당주의 의무의 지위 변화 가능성 검토

상당주의 의무의 규범적 지위 변화 가능성을 모색하기에 앞서, 현재 상당주의 의무의 국제관습법적 지위에 대해 명시적으로 반대하거나 혹은 관련 논의에 침묵으로 일관하는 상당수의 국가가 '사이버 핵심 역량 국가'로 분류된

---

[362] 이종현, supra note 237, p.116.

[363] Michael N. Schmitt, supra note 179, p.79.

다는 점에 주목할 필요가 있다. 이러한 현상은 제6차 UN 정부전문가그룹의 부속서인 '자발적 국가기여'에 제출된 국가의 견해를 통해 보다 명확하게 확인된다. 가령, 영국과 미국은 자발적 국가기여를 통해 상당주의 의무가 사이버 공간에서 관습국제법의 지위를 획득하지 못하였다는 자국의 주장을 제출한 바 있다.[364] 이들은 공통적으로 사이버 공간에 상당주의 의무가 적용되어야 할 필요성에 대해서는 공감하지만 동 의무가 구속력을 갖는 규범이 되기 위해 갖추어야 할 충분히 일관된 국가실행 및 법적 확신을 확인하지 못하였다는 점을 그 근거로 들었다. 비서방 지역의 사이버 핵심 전략 국가로 간주되는 중국과 러시아의 경우에는 자발적 국가기여 문서에서 사이버 공간에서의 상당주의 의무의 규범적 지위 및 역할 등에 대한 직접적인 견해를 표출하지 않고 있다.[365]

상당주의 의무의 규범적 지위에 관한 논의에서 이러한 사이버 핵심 역량 국가의 견해는 보다 큰 중요성을 갖는데, 그 이유는 다름 아닌 이들이 사이버 규범과 관련한 국제사회의 담론을 주도하고 있을 뿐만 아니라 사이버 공간을 규율하는 논의와 관련하여 '특별히 영향을 받는 국가들'(specially affected states)로 간주될 수 있기 때문이다.[366] 상당수의 사이버 핵심 역량 국가는 고도로 발전된 사이버 기반 시설을 갖추고 있으며, 이러한 사이버 기반 시설은 종종 타국을 목표로 하는 사이버 공격의 '경유국' 내지는 '공격의 거점'으로 악용되는 경우가 빈번하다. 가령, 오늘날 발생하는 북한 발 사이버 공격의 상당수는 중국을 경유한다는 사실이 확인된 바 있으며 사이버 공간에서 상당주의 의무의 규범적 강제성을 인정함에 있어서 사이버 핵심 역량 국

---

[364] 상당주의 의무에 관한 미국과 영국의 견해는 UNGA 컨펜디엄, pp.106-135/142, pp.136-142/142 각각 참조.

[365] 중국은 자발적 국가기여를 제출하지 않았고, 러시아는 자발적 국가기여를 제출하였으나, 상당주의 의무에 관한 내용을 포함하지는 않았다.

[366] 관습국제법의 성립 요건 중 하나인 '국가 관행'(state practice)의 형성에 있어서 그러한 관행이 형성됨에 따라 '특별히 영향 받는 국가들'(specially affected states)의 참여는 매우 중요한 요소이다. ICJ는 북해 대륙붕 사건의 판례를 통하여 짧은 기간 내의 관습 형성에 있어 '특별히 영향 받는 국가들'의 지위를 강조한 바 있다. 관련 내용은 North Sea Continental Shelf, Judgement, I.C.J. Reports 1969, p.3, para. 73 참조.

가가 회의적인 태도를 보이는 큰 원인이 바로 여기에 있다고 할 것이다. 실제로 탈린매뉴얼의 대표 집필자인 Michael N. Schmitt은 사이버 강대국이 상당주의 원칙에 대한 구속력을 부여하는 것을 주저하는 이유는, 자국 역시 그 위반에 대한 책임을 부담할 가능성이 크다는 우려에 근거한다는 입장을 제시한 바 있다.[367] 사이버 공격을 직접적으로 지시한 주체가 아니더라도 사이버 기반시설 소재국의 의무를 규정하는 상당주의 의무의 특성 상, 다수의 사이버 기반시설을 보유한 사이버 강대국의 입장에서는 상당주의 의무의 위반에 대한 우려 역시 커지기 때문이다. 그러나 오늘날 발생하는 상당수의 사이버 공격은 이들 국가를 단순한 경유국 혹은 공격의 거점으로 삼는 것에서 더 나아가 사이버 핵심 역량 국가를 직접적인 공격의 표적으로 삼고 있기도 하다. 즉, 최근 사이버 강대국을 상대로 발생한 수많은 사이버 공격과 이에 대한 국가들의 반응을 통해 상당주의 의무의 국제법적 지위에 관한 이들의 입장 수정 가능성을 기대해 볼 수 있을 것이라고 판단된다. 사이버 공간을 규율하는 과정에서 사이버 핵심 역량 국가가 갖는 지위와 중요성을 고려하여, 아래에서는 상당주의 의무에 관한 이들 국가의 견해를 재검토하기로 한다.

영국 '정보통신본부'(SCHQ) 산하의 국가사이버안보센터는 2022년 하반기의 연례보고서를 통해 악의적 의도를 가진 일부 국가 행위자로부터 영국의 사이버 안보가 크게 위협받고 있음을 언급하였다. 국가사이버안보센터는 이란, 중국, 러시아와 북한 등을 자국에 대한 사이버 공격의 주요 배후국으로 지목하고 있으며 영국의 공공기관, 의료, 교육기관, 민간기업을 포함한 수백 곳의 기관이 사이버 공격의 피해를 입었다고 주장하였다. 또한, 영국은 사이버 보안에 위협을 가할 역량을 가진 국가 주도 행위자들이 앞으로 더욱 늘어날 것을 우려하기도 하며, 국가사이버안보센터 차원의 대응을 확대해 나가겠다고 밝힌 바 있다.[368]

---

[367] Michael N. Schmitt, supra note 179, p.69.

[368] National Cyber Security Centre (NCSC), "Annual Review 2022 - NCSC View: future threat challenge", (2022), available at https://www.ncsc.gov.uk/collection/annual-review-2022/threats-risks-and-vulnerabilities/ncsc-view-future-threat-challenges (마지막 방문: 2023.7.27)

2021년 미국의 최대 송유관 관리업체인 콜로니얼 파이프라인을 대상으로 자행된 랜섬웨어 공격과 당해 공격과 관련한 바이든 대통령의 발언 역시 주목할 만하다. 콜로니얼 파이프라인은 2021년 5월 랜섬웨어 공격을 받아 가동이 중단되었으며, 회사 측은 재가동을 위해 당시 약 500만 달러에 달하는 비트코인을 몸값으로 지불하였다고 밝힌 바 있다.[369] 이 사건의 배후에 러시아 정부가 있다는 확실하고 설득력 있는 수준의 증거를 확보하지 못한 미국은 본 사안에 대해 러시아 정부에 대한 국가책임을 물을 수 없었다. 그러나 바이든 대통령은 당해 공격에 러시아 정부가 직접적으로 개입하였다는 증거를 확보하지는 못하였지만, 해당 공격이 러시아로부터 '개시'되었다는 점을 입증할 수 있는 충분한 근거를 확보하였으므로 러시아 정부는 이에 대한 일정한 책임을 부담해야 된다고 언급하였다.[370] 물론 바이든 대통령은 백악관 공식 성명에서 러시아 정부가 일정한 책임을 부담하여야 함을 언급하면서 '상당주의 의무(due diligence)'라는 직접적인 용어를 사용하지는 않았다. 그러나 해당 공격이 명시적으로 러시아 정부의 직접적인 지시 내지 명령 하에 개시되었음을 증명하기에 앞서, 당해 공격의 개시국이 러시아라는 점으로부터 러시아 정부가 '일정한 책임'을 부담하여야 한다는 바이든 대통령의 발언은 곧 사이버 공간에서의 상당주의 의무를 인정하는 것으로 해석될 여지가 크다.

---

[369] Sarah Morrison, "How a major oil pipeline got held for ransom", Vox, (Jun 8, 2021), available at https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices. (마지막 방문: 2023.7.27)

[370] Josh Wingrove & Jennifer Epstein, "Biden says Russia has "Some Responsibility" in Colonial Attack", Bloomberg, (May 11, 2021), available at https://www.bloomberg.com/news/articles/2021-05-10/colonial-pipeline-is-undamaged-white-house-official-says?leadSource=uverify%20wall (마지막 방문: 2023.7.27) ; White House Government, "Remarks by President Biden on the Colonial Pipeline Incident", (May 13, 2021), available at https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/. (마지막 방문: 2023.7.27)

이처럼 자국을 상대로 감행되는 적대적 사이버 공격이 증가하고 있다는 사실은 사이버 강대국으로 하여금 상당주의 의무에 대한 자국의 입장이 수정될 수 있다는 가능성을 제공한다. 즉, 이들 사이버 강대국은 사이버 공간에서의 상당한 주의를 다하여야 함에 대한 부담과 함께, 자국을 향한 무수한 사이버 공격에 효과적으로 대응하기 위한 수단으로서 상당주의 의무의 필요성에 대해서도 더불어 인지하게 되는 것이다. 사이버 공간에 적용되는 국제법을 논하는 과정에서 이들 사이버 강대국이 갖는 영향력을 고려해볼 때, 이들의 입장 선회는 상당주의 의무의 국제법적 지위 변화에 긍정적인 영향을 미칠 것이라고 예상된다.

한편, 상당주의 원칙에 대하여 UN 정부전문가그룹의 차원에서 진행되고 있는 논의는 UN GGE 회의의 각 회차 최종보고서 및 제6차 GGE 이후 제출된 '자발적 국가 기여' 문서를 통해 보다 구체화된다. 이러한 문서는 연성법 문서로서의 지위를 갖는다고 볼 수 있으며, 참여국을 포함한 UN 회원국에 대하여 구속력을 갖는 것이 아닌 권고 정도의 효력을 갖게 된다. 그럼에도 불구하고 회원국은 국내외 사이버 관련 정책을 수립하거나 사이버 관련 법률을 제정함에 있어 UN 정부전문가그룹의 틀 내에서 논의된 상당주의 의무에 관한 내용을 가볍게 무시할 수는 없으며, 관련 논의 내용을 국내 정책 및 법률 제정 과정에 반영할 가능성 역시 존재한다.[371] 제한적이기는 하나 UN 정부전문가그룹의 몇몇 참여국들은 상당주의 의무가 국제법적 구속력을 갖는다는 자국의 견해를 제출하였는데, 이는 동 원칙에 대한 참여국의 '법적확신(opinio juries)'으로 이해할 수 있다. 더욱이, '자발적 국가 기여'를 통해 상당주의 의무에 대한 국가들의 실행을 확인할 수 있으며, 상당주의 의무에 대한 보다 활발한 의견의 교환이 가능할 뿐 아니라, 타국의 의견에 대해서도 열람할 수 있다. 물론, 현 시점으로서는 상당주의 의무가 국제관습법적 지위를 획득한다는 예측이 다소 추상적일 수 있다. 그럼에도 불구하고 동 의무에 대한 국가 실행의 꾸준하게 확인되고 더 많은 국가들이 이러한 국가 실행에 동의하며, 더 나아가 이러한 관행이 보다 구체적인 법적 확신으로 나타난다

[371] 이종현, supra note 237, p.206.

면 상당주의 의무가 국제관습법적 지위를 획득할 가능성 역시 기대해볼 수 있을 것이다.

II. 구체적 적용 기준 설정의 필요성

1. 상당주의 의무의 신축적 특성과 한계

앞선 제4장에서 짧게 언급한 바와 같이 '적용상의 구체적인 기준'을 설정하는 것은 상당주의 의무를 사이버 공간에 적용함에 있어서 검토하여야 할 또 다른 법적 쟁점에 해당한다. 앞서 확인한 바와 같이 상당주의 의무는 국가의 국제의무 이행에 있어서 상당한 자율성과 유연성(autonomy and flexibility)을 갖는다.[372] 즉, 상당주의 의무는 일부 공통적 요소를 가짐에도 불구하고 상황 및 맥락에 무관하게 존재하는 객관적인 적용 기준을 갖는 개념은 아닌 것으로 이해되어왔다.[373] 이처럼 개방적 기준 또는 규범의 특성을 갖는(open-ended standard of principle) 상당주의 의무는 특정 의무의 구체적인 준수 범위와 명백한 요건을 사전에 명백하게 설정함으로써 발생하는 각종 갈등 상황을 방지하고, 타국에 미칠 수 있는 피해를 최소화화기 위한 방안으로 '합리성과 적절성'(reasonable and appropriate)이라는 보다 유연한 판단 기준을 제공하는 역할을 수행해 온 것으로 평가된다.[374] 상당주의 의무가 갖는 이러한 '유연성'(malleability)으로 인해 동 의무는 국제법의 보다 다양한 상황과 넓은 맥락 하에서 활용될 수 있었다. 실제로 ICJ를 비롯한 여러 국제재판소에서 원용하였던 상당주의 의무의 기준은 관련된 문제 영역과 국제법

---

[372] ILA 2016 Report, p.4. 원문은 다음과 같다. ("Due Diligence standards preserve for States a significant measure of autonomy and flexibility in discharging their international obligation")

[373] Colin Patrick, supra note 228, p.583. ("Due diligence, while eminently flexible in application, still contains two essential elements."); ILA 보고서는 Corfu Channel 사건을 통해 상당주의 의무의 핵심 내용이 구체화된 것으로 보고 있다. ILA 2016 Report, p.5 참고.

[374] ILA 2016 Report, p.3.

의 세부 분야에 따라 상이한 방식으로 적용되어 왔는데, 이 역시 상당주의 의무의 신축적 특성으로 말미암은 결과라고 할 것이다.[375] 또한 상당주의 의무는 이행에 대한 국가들의 보다 '유연한 접근'(flexible approach) 방식을 보장하고 의무의 완벽한 동등성(perfect parity of obligations)을 회피함으로써 조약과 관습적인 체제에 국가의 광범위한 참여를 보장하기 위한 방안으로 적극 활용되기도 하였다.[376]

이처럼 상당주의 의무는 신축적이고 유연한 특성으로 말미암아 동 의무가 적용되는 구체적인 상황에 따라 달리 해석되고 적용 될 여지를 제공함으로써 보다 다양한 분야에 원용되어 왔다. 그러나 다른 한편 상당주의 의무의 이러한 신축적이고 유연한 특성은 적용상의 불확실함을 유발하는 기제가 되기도 하였다.[377] 즉, 상당주의 의무의 이점으로 여겨져 온 자율성과 유연성이 또 다른 측면에서는 적용상의 모호함과 불확실성을 야기한 것이다. 상당주의 의무의 이러한 모호함과 불확실성은 국제법의 특정 분야에 상당주의 의무가 원용되어 온 방식을 통해 확인할 수 있다. 가령, UN 해양법협약 제56조 제2항에는 배타적 경제수역(Exclusive Economic Zone: EEZ) 내에서 연안국의 권리를 행사할 때 타국의 권리 의무를 '적절히 고려'(due regard)하여야 함을 적시하고 있으며,[378] 동 협약 제87조 제2항 역시 공해의 자유를 행사함에 있어서 타국의 이익과 권리를 '적절히 고려'(due regard)해야 함을 명시한 바 있다.[379] 그러나 이때 조약 상 명시된 '적절히 고려하여야 함'의 기준과 범위

---

375 Colin Patrick, supra note 228, p.584.

376 ILA 2016 Report, pp.2-3.

377 ILA 2016 Report, p.3.

378 유엔해양법협약 제56조 제2항. 원문은 다음과 같다. "In exercising its rights and performing its duties under this Convention in the exclusive economic zone, the coastal States shall have due regard to the rights and duties of the other States and shall act in a manner compatible with the provisions of this Convention."

379 유엔해양법협약 제87조 제2항. 원문은 다음과 같다. "These freedoms shall be exercised all States with due regard for the interests of other States in their exercise of the freedom of the high seas, and also with due regard for the rights under this Convention with respect to activities in the Area."

는 문언만으로는 확정이 어려우며 문언의 실질적인 적용을 위해서는 당사국의 추가적 합의와 국제재판소의 해석을 필요로 한다. 다른 한편, 상당주의 의무의 가변성과 그에 따른 적용상의 모호함은 국제해양법재판소의 Seabed Mining 사건의 권고적 의견을 통해서도 확인된 바 있다.[380] 동 사건의 권고적 의견에 따르면 상당주의 의무는 정확한 용어로 정의하기 어려운데, 이는 상당주의 의무의 기준이 과학 및 기술의 발전에 따라 변화할 수 있는 '가변적인 개념'(variable concept)이라는 점에 기인한다.[381] 이처럼 상당주의 의무는 적용상의 구체적 요건과 범위가 명확히 확립되지 않은 바,[382] 이는 유연함과 동시에 불명확하고 추상적인 상당주의 의무의 본질적 한계로부터 비롯하는 것으로 볼 수 있다. 무엇보다도 앞서 확인된 한계는 상당주의 의무에 대한 국가의 통일적 이해를 저해하고 동 의무의 실제적 적용 과정에서 국가 실행의 혼란을 초래할 우려가 있다. 무엇보다도 이러한 적용상의 혼란은 새롭게 대두되는 영역인 사이버 공간에서 보다 심화된 형태로 나타날 가능성이 매우 크다. 이러한 논의의 필요성에 기반하여, 아래에서는 관련된 문제점과 그에 따른 상당주의 의무의 구체적 적용 기준이 마련되어야 할 필요성에 대하여 보다 상세하게 살펴보기로 한다.

2. 상당주의 의무의 '구체적 적용 기준' 설정 필요성

사이버 공간에 상당주의 의무를 적용함에 있어서 구체적인 적용 기준을 확립하여야 한다는 주장은 우선 UN 정부전문가그룹의 논의 과정에서 참여국이 제출한 의견서를 통해 확인할 수 있다. 가령, 싱가포르의 경우 제6차 GGE 보고서의 부속서인 '자발적 국가 기여'를 통해 상당주의 의무의 적용 범위와 실제적 적용 사안에 관하여 추가적으로 검토되어야 할 내용에 대해

---

[380] Responsibilities and obligations of States with respect to activities in the Area, Advisory Opinion, 1 February 2011, ITLOS Reports 2011, p.10.

[381] Ibid., para.117.

[382] ILA 2016 Report, p.3.

언급했다.[383] 싱가포르는 상당주의 의무를 사이버 공간에 적용함에 있어서 보다 '명확한 범위'(more clarity on the scope and practical applications)의 설정이 요구된다는 점을 강조하였다. 특히, 국가가 상당한 주의를 발동하여야 할 '임계점'(threshold)과 국가에게 요구되는 '인식의 정도'(degree of knowledge required of States), 그리고 악의적인 사이버 활동이 발생한 국가에 대하여 취해져야 하는 조치 등에 대하여 국제사회 차원의 폭넓은 논의가 이루어져야 한다는 입장을 개진하였다. 한편, 일본의 경우 자발적 국가 기여를 통해 사이버 공간에서의 상당주의 의무가 갖는 유용성에 대해 언급함과 동시에, 동 의무를 실질적으로 사이버 공간에 적용할 때의 범위와 요건이 명확하지 않다는 점을 지적하였다. 즉, 영토국이 상당주의 의무를 이행하는 범위를 결정함에 있어서는 사이버 작전의 심각성과 함께 영토국의 전반적인 능력이 함께 고려되어야 하며, 이러한 논의를 기반으로 하여 상당주의 의무의 요건이 구체화되어야 한다는 주장을 개진한 것이다.[384] 이외에도 다수의 국가들은 사이버 공간에 상당주의 의무가 적용될 때 '구체적인 적용 기준'이 결여된 현 상황에 대하여 우려를 표하고, 국제사회에서 이러한 논의가 조속히 진행되어야 할 필요성에 대해 지적한 바 있다.

국내법 체계와는 다르게 초국가적 입법기관이 부재한 국제사회와 국제법의 특성을 고려할 때, 특정한 국제 규범을 구체적인 상황에 적용하는 과정에서 크고 작은 해석상의 어려움이 존재해 왔던 것은 주지의 사실이다. 더욱이, 국제법상 상당주의 의무는 본원적인 신축적 특성으로 인해 해석상의 유연함과 함께 다소간의 적용상 모호함이 병존하는 규범인 것으로 간주되어 왔다. 그렇다면, 기존의 물리적 영역과는 달리 사이버 공간에 상당주의 의무를 적

---

[383] UNGA 컨펜디엄, p.84/142. '상당한 주의 (due diligence)'에 대하여 싱가포르가 제출한 자국의 의견은 다음과 같다. ("There is a need for more clarity on the scope and practical applications, if any, of due diligence in cyberspace. Issues such as the threshold required to trigger an obligation on States to act or respond, the degree of knowledge required of States, and the measures expected of a State from which the malicious cyber activity originates, are some examples of the questions that need to be further discussed and addressed among States.")

[384] UNGA 컨펜디엄, p.48/142. ("The outer limit of the due diligence obligation of territorial States with respect to cyber operations is not necessarily clear.")

용함에 있어서 유난히 구체적인 적용 기준 설정이 법적 쟁점으로서 제기되고, 또한 해당 논의의 필요성이 새롭게 부각되는 까닭은 무엇인가? 이는 상당주의 의무의 본원적인 특성인 '유연함'과 '신축성'에 사이버 공간이라는 새로운 영역이 갖는 '특수성'이 더해짐에 따라 동 의무를 사이버 공간에 적용함에 있어서 더욱 극심한 해석상 혼란과 적용상의 모호함이 야기되기 때문인 것으로 판단된다. 물론, 전통적인 국제법 영역에서도 상당주의 의무는 그 구성 요건 자체가 명시적이고 객관적이었던 것은 아니지만 시간이 지남에 따라 적용상의 요건과 범위가 점진적으로 구체화 되어 온 경향이 있다.[385] 그러나 사이버 공간은 물리적인 관할권을 기반으로 하는 전통적인 국제법 영역과는 공통적인 요소가 희박하거나와, 그 자체로도 매우 특수한 성질을 가지므로 사이버 영역에 상당주의 의무를 적용함에 있어서는 보다 확실한 기준이 마련되어야 할 필요성이 지속적으로 제기되는 것이다.

3. 상당주의 의무의 '구체적 적용 기준' 검토를 위한 과제

상당주의 의무를 사이버 공간에 적용하여 공격과 관련한 제3국의 행위를 보다 효율적으로 규율하기 위해서는 동 의무의 구체적인 적용 기준 및 요건과 관련하여 국제사회가 추가적으로 합의하여야 할 사안들이 다수 존재한다. 아래에서는 보다 구체적으로 어떠한 쟁점들에 대한 합의가 필요한 지에 대하여 검토하고자 한다. 우선, '심각성'의 기준에 대한 합의가 부재하다. 탈린매뉴얼에서는 특정 사이버 조작이 상당주의 의무의 적용 대상이 되기 위해서는 '심각한(serious)' 피해를 야기할 것이 요구됨을 명시하고 있다.[386] 그러나 이때의 '심각성'이 어떠한 수준의 피해를 의미하는 것인지에 대한 국제법상 명확한 기준은 확립되어 있지 않은 상태이다. 재래식 무기를 활용한 공격의 결과가 '심각성'에 이르는 정도에 대해서는 다각도의 논의와 연구가 이루어져 왔으며 국제재판소의 판례 역시 축적된 상태이다. 그러나 사이버 수단을 활

---

[385] ILA 2016 Report, p.3. ("The content of due diligence duties themselves are not fixed. They can and do evolve over time.")

[386] 탈린매뉴얼 2.0, Rule 6.

용한 불법적인 사이버 공격은 재래식 공격과는 명백한 차이점이 존재하는 바, '심각성'에 이르는 사이버 공격의 범위와 정도에 대해서는 추가적인 연구와 국제사회의 논의를 통해 통일된 이해를 형성해 나갈 필요가 있다.

다른 한편, 공격에 대한 경유국 '인식'(knowledge)에 관한 부분도 논란이 되는 지점이다. 영토국은 자국의 영토 및 사이버 관할시설이 타국에 위해를 가하는 방식으로 활용된다는 사실을 '인식(knowledge)'하는 경우 상당주의 의무를 다하여야 한다.[387] '인식'의 요건은 영토국이 불법적인 사이버 조작과 관련하여 얼마나 많은 정보와 당해 정보에 대한 확실성을 구비하였는가에 관한 논의로, 상당주의 의무의 발동을 위한 결정적인 요인 중 하나이다.[388] 그러나 여전히 국제사회는 상당주의 의무를 발동하기 위한 인식의 '정도'(degree)에 대해서는 여전히 합의를 이루지 못하였다. 공격과 관련된 제3국이 불법적 사이버 조작이 발생하였음을 '실제적으로 인식'(actual knowledge)하였다면 당해 국가가 상당한 주의를 다하여야 함은 명백하다.[389] 그러나, 이때 관련된 국가가 불법 사이버 조작의 발생 사실에 대하여 '추정적으로 인식'(constructive knowledge)한 경우에도 상당한 주의를 다하여야 하는지에 대해서는 의견의 대립이 존재한다.[390] 상당주의 의무의 발동 요건인 '인식'의 범위에 대해서는 탈린매뉴얼을 집필한 국제전문가그룹 내부에서도 합의를 이루지 못한 바, 이는 국제사회의 통일된 이해를 필요로 함에도 불구하고 첨예한 대립이 예상되는 지점이다.

더불어, 사이버 공간에서 상당주의 의무를 이행함에 있어서 사이버 작전을 감시하고 위험한 사이버 조작을 방지하기 위한 영토국의 '역량(capabilities)'이 고려되어야 한다.[391] 가령, 사이버 핵심 역량국과 비교적 그 역량이 부족한 국가 사이에는 자국의 영토에서 불법적인 사이버 조작이 발생하는 상

---

[387] 탈린매뉴얼 2.0, Rule 6 (37).

[388] Antonio Coco, "'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law", The European Journal of International Law, Vol. 33, No. 3 (2021), p.789.

[389] Antonio Coco, ibid., p.789; Robert Kolb, supra note 290, pp.123-124.

[390] 박노형·김효권, supra note 7, p.81; Michael N. Schmitt, supra note 179, p.71.

[391] Eric Talbot Jensen, supra note 294, p.14.

황을 '감시하고 예방'(monitor and prevent cyber activities)하는 의무를 차등적으로 부과하여야 할 필요성이 제기되는 것이다.[392] 그러나, 영토국마다 상이한 사이버 기술 역량(technological capabilities)을 보유하고 있다는 점을 감안할 때, 사이버 역량을 평가하는 명확한 기준을 수립하는 것에는 상당한 어려움이 따른다.[393] 이외에도 국제사회는 상당주의 의무의 적용상 기준과 관련하여 사이버 공격에 따른 위험의 종류(types of harm), 위험의 임계점(threshold of harm) 등에 대한 구체적인 기준을 제시하여야 할 필요가 있다.[394]

이처럼 상당주의 의무는 사이버 공간에 적용됨에 있어 적용상의 구체적 기준과 요건을 상당 부분 결여하고 있다. 적용상의 구체적인 기준의 부재는 상당주의 의무를 적용하는 상황에서 국가들의 자의적 해석을 야기할 뿐만 아니라, 상당주의 의무를 준수하는 국가들의 실행에도 혼선을 초래한다. 상당주의 의무가 사이버 공간에 적용되어 본연의 역할을 다하기 위해서는 추상적이고 불분명한 영역에 대하여 명확한 합의를 도출함으로써 동 의무에 관한 국제사회에서의 통일적 이해를 형성할 필요가 있다. 이를 위해서 가장 우선시되어야 할 작업은 '상당주의 의무'의 정의에 관한 초국가적인 합의를 이룩하는 것이다. 현재 사이버 공간에서의 상당주의 의무는 탈린매뉴얼, UN 정부전문가그룹, 각종 국제기구 및 학자 개인의 차원에서 파편화 되어 정의되고 있다. 물론 이러한 상당주의 의무의 정의는 ICJ의 Corfu Channel 사건에 명시된 정의를 일정 부분 차용하였다는 점에서는 부분적으로 유사한 측면을 지니지만 그럼에도 불구하고 상당주의 의무를 설명하는 구체적인 용어와 범위 등에 있어서는 통일성이 결여된 모습을 보인다.[395] 이렇듯, 파편적이고 독립적

---

[392] Ibid.

[393] Ibid., pp.13-14; Antonio Coco, supra note 336, p.792.

[394] Antonio Coco, ibid., pp.790-792.

[395] 가령, 탈린매뉴얼은 상당주의 의무의 정의에 대해서 '타국의 권리에 반하는 사이버조작을 위하여 자국의 관할권 하에 있는 영토 및 사이버 기반시설 등이 사용되지 않도록 상당한 주의를 다하여야 할 의무가 있다'고 명시한다. (탈린매뉴얼 Rule 6 참조) 한편 UN 정부전문가그룹에서는 사이버 공간 상 상당주의 의무에 대하여 '국가는 ICTs를 이용한 국제적인 불법행위에 자국 영토가 활용되는 것을 알고도 이를 허용해서는 안된다'라고 명시하고 있다.(UN GGE 제6차 보고서, p.10/26) 양자는 동일한 상당주

으로 형성되어 있는 상당주의 의무에 관한 각종 국제기구 및 국가의 견해를 하나의 통일된 정의로 형성하는 작업은 사이버 공간에서 상당주의 의무의 구체적 적용 기준을 설정함에 있어서 유의미한 첫걸음이 될 것이다. 사이버 공간에서 상당주의 의무의 초국가적인 정의가 형성된 이후에 통일된 정의에 내포된 '용어'(가령, '인식'과 '심각성' 등)를 면밀히 검토함으로써 상당주의 의무의 구체적인 기준과 범위를 설정하는 작업이 순차적으로 이루어질 수 있을 것이다. 이러한 후속 작업에 있어서는 UN 개방형작업반 혹은 UN 정부전문가회의에서의 보다 적극적인 논의를 기대해볼 수 있다.

III. 상당주의 의무의 집행력 확보 – '이행 확보 수단 구축'

사이버 공간에서 상당주의 의무가 본연의 역할을 다하기 위하여 추가적으로 검토되어야 할 법적 쟁점은 상당주의 의무의 '집행력 확보'이다. 상당주의 의무는 사이버 공간의 평화적 활용을 도모하고 피해국의 권리를 구제하기 위한 방안으로서 그 도입이 요구되는 바, 이러한 상당주의 의무의 효과적인 역할 수행을 위해서는 우선 동 의무를 성실하게 준수하고자 하는 국가들의 이행 의지가 선행되어야 함은 물론이다. 그러나 사실상 국가들의 순수한 이행 의지만으로는 사이버 공간에서 상당주의 의무의 효과적 준수를 담보하기 어려우며, 따라서 국가로 하여금 상당주의 의무를 보다 확실하게 준수할 수 있도록 유도하는 별도의 기제를 도입할 필요성이 제기된다고 할 것이다. 그러나 지금까지는 상당주의 의무의 '이행 확보 수단'을 확립하기 위한 국제사회의 논의가 충분히 이루어지지 않은 것으로 보인다. 따라서 아래에서는 상당주의 의무의 이행 확보 수단을 구축함으로써 사이버 공간에서 동 의무의 집행력을 확보하는 방안에 대하여 검토하고자 한다. 보다 구체적으로, 본 연구에서는 사이버 공간에서 상당주의 의무의 집행력을 확보하기 위한 방안으로 '다자간환경협정'(Multilateral Environmental Agreements: MEAs)에서 적극적으로 활용되고 있는 '비준수절차'(Non-Compliance Procedures: NCPs)의

의 의무에 대해 명시하고 있음에도, 이를 설명하는 용어에 있어서는 명백한 차이를 보인다.

역할에 주목하고자 한다. 다자간환경협정에서 원용되는 '비준수'(Non-Compliance)란, 환경협약에서 규정한 구체적인 의무를 준수하지 않았음을 의미하며, '비준수절차'는 이러한 의무 위반에 대하여 국제법적 제재보다는 '재정 및 기술적 지원'을 행함으로써 의무위반 상태를 '비강제적'으로 해소하도록 유도하는 제도이다.[396] 비준수절차는 몬트리올 의정서에 처음으로 도입되어 성공적인 역할을 수행하였다고 평가된 이후에 다수의 다자간환경협정에 지속적으로 포함되어왔으며 각 환경 협정의 구체적인 성격에 따라 조금씩 다른 내용을 담고 있다.[397]

다만 여기서 유의할 점은 다자간환경협정의 비준수절차는 국제법상 구속력이 있는 국가간 합의, 가령, '국제협약' 등을 전제로 한다는 것이다. 그러나 전술한 바와 같이 사이버 공간에서 상당주의 의무의 경우 아직 구속력 있는 국제법 규범의 지위를 획득하였다고 판단하기는 어렵다. 따라서 본 연구에서 제안하고자 하는 상당주의 의무의 집행력 확보 방안으로서의 '비준수절차'는 상당주의 의무가 사이버 공간에서 구속력 있는 규범적 지위를 획득한 이후의 상황을 전제로 하며 이하에서의 논의 역시 이러한 맥락 하에서 이루어진다는 점을 명시하고자 한다. 아래에서는 우선 다자간환경협약에서 채택되고 발전해 온 비준수절차의 특성과 의의에 대해서 살펴본 뒤 이러한 비준수절차가 사이버 공간에서 상당주의 의무의 실질적인 집행력 확보에 있어서 어떠한 역할을 수행할 수 있는지에 대해서 검토하고자 한다.

1. 다자간환경협정에서 '비준수절차'의 의의

상당수의 다자간환경협정은 국가의 협정 비준수를 방지하고 이행을 촉진하며, 협정의 원활한 집행을 보장하기 위한 방안으로 '비준수절차'를 활용해

---

[396] 이일호, "국제환경법 이행체제의 개선방안에 관한 제안 – 기후체제에서의 이행문제와 그 대안을 중심으로 –", 『국제법평론』, 통권 제47호 (2017), 146면.

[397] Antonio Cardesa-Salzmann, "Constitutionalizing Secondary Rules in Global Environmental Regimes: Non-Compliance Procedures and the Enforcement of Multilateral Environmental Agreements", Journal of Environmental Law, Vol. 24, No. 1 (2011), p.103.

왔다.[398] 다자간환경협정 내 비준수절차는 오존층 보호를 위한 몬트리올 의정서의 제8조의 수권조항(enabling clause)을 통해 최초로 그 도입을 예정하였으며, 1992년 개최된 코펜하겐 당사국 회의에서 정식으로 도입이 확정되었다.[399] 몬트리올 의정서에서 비준수절차 매커니즘이 최초로 도입된 이후, 유사한 형태의 비준수절차가 '1997년 교토의정서'(Kyoto Protocol) 제18조, '바이오 안전성 의정서'(Biosafety Protocol) 제34조, '오르후스 협약'(Aarhus Convention) 제15조 등을 비롯한 다수의 다자간환경협정의 조항에 포함되어 왔다.[400]

비준수절차 내에서 협약 당사국의 의무 준수를 촉진하는 과정은 총 4가지의 단계로 구분된다.[401] 첫번째 단계는 의무의 비준수가 주장되기 이전의 단계로, 협약의 당사국은 '보고서'(report) 혹은 '통보'(communication) 등을 통해 의무와 관련한 자국의 견해를 표출한다. 두번째 단계는 비준수 절차의 핵심적인 절차로서, 본 단계에서는 각종 원조(assistance)를 통해 비준수 당사국의 의무 준수를 촉구(facilitate)하게 된다. 이때의 원조는 당사국이 의무를 이행하는 데 도움이 될 수 있는 금전적, 기술적 지원(financial and technical assistance)을 모두 포괄하는 것으로 볼 수 있다.[402] 세번째 단계는 비준수 행위를 '관리'(management)하는 단계이다.[403] 끝으로 네번째 단계에서는 비준수 상황의 해결을 위하여 중재재판 혹은 국제사법재판 등을 통해 의무 위반을 결정하고 이에 대한 제재를 가하게 된다. 보통 '비준수절차'라고 함은 제3자가 개입된 네번째 단계에 이르기 전에 당사국의 의무 이행을 촉진

---

398 박병도, "신기후체제의 국제법적 쟁점", 『국제법학회논총』, 제62권 제1호 (2017), 40면; MA Fitzmaurice & C Redgwell, "Environmental Non-Compliance Procedures and International Law", Netherlands Yearbooks of International Law, Vol. 31 (2009), p.36.

399 MA Fitzmaurice & C Redgwell, ibid.

400 MA Fitzmaurice & C Redgwell, ibid., pp.36-37; Pierre-Marie Depuy & Viñuales Jorge E, International Environmental Law, (Cambridge University Press, 2018), p.345.

401 Pierre-Marie Depuy & Viñuales Jorge E, ibid., pp.328-329.

402 Ibid.

403 Ibid., p.329.

하는 제도를 의미한다.[404] 즉, 다자간환경협정에 이와 같은 비준수절차를 도입한 일차적 목적은 국가로 하여금 조약상 의무를 준수하도록 장려하고 (encouragements to states to comply with their treaty obligation), 당해 의무를 준수하지 않았을 때 이를 국제법상의 전통적인 분쟁해결절차에 맡기기 보다는, 비준수를 다루는 보다 '유연한 체제'(a softer system)를 제공하는 것에 있음을 확인할 수 있다.[405] 전통적인 분쟁해결절차와 비교하였을 때 비교적 덜 경직적인 특성을 띄는 비준수절차는 협약 이행을 위한 강제적 시행(enforcement)을 통해 주권이 제약 받는 것을 최소화 하고자 하는 국가의 의견이 반영된 결과물이기도 하다.[406] 또한 전통적인 분쟁해결절차를 비롯한 책임 추궁 수단이 전지구적인 환경문제를 해결함에 있어서 더 이상은 실효적이지 않다는 국제사회의 반성 하에, 비준수절차는 '지속적인 감시'(continuous oversight), '공식적인 권고'(official prodding), 그리고 '제도적 지원'(institutional assistance) 등을 통해 당사국의 궁극적인 '의무 이행'을 목표로 삼고 있다.[407]

2. 비준수절차를 통한 사이버 공간에서의 상당주의 의무의 집행력 제고

상당수의 다자간환경협정에서 널리 도입되어 온 비준수절차의 특성을 고려하였을 때 비준수절차는 사이버 공간에서 상당주의 의무의 집행력 제고를 위한 '이행 확보 수단'으로서 의미 있는 역할을 수행할 수 있을 것으로 판단된다. 비준수절차는 사이버 공간에 상당주의 의무를 도입하고자 하는 국제사회의 목적 달성에 도움이 될 수 있으며, 상당주의 의무의 도입과 관련하여

---

[404] 박병도, supra note 346, p.41.

[405] MA Fitzmaurice & C Redgwell, supra note 346, p.39.

[406] 박병도, "국제환경협약의 이행 및 준수 메커니즘 – 비준수 절차를 중심으로 -", 『환경법연구』, 제36권 제3호 (2014), 70면.

[407] Tseming Yang, "International Treaty Enforcement as a Public Good: Institutional Deterrent Sanctions in International Environmental Agreements", Michigan Journal of International Law, Vol.27 (2006), p.1141; MA Fitzmaurice & C Redgwell, supra note 346, pp.36-37.

주권 국가가 가지는 우려를 해소할 수 있는 적합한 방안이 될 수 있을 것으로 보인다. 관련된 내용을 아래에서 보다 상세하게 검토하기로 한다.

확인한 바와 같이 사이버 공간에서 상당주의 의무는 현재 국제법상 구속적 지위를 획득하지 못하였다. 국가들이 상당주의 의무의 규범적 강제력을 인정하는 것을 주저하는 가장 큰 사유는 사이버 공간과 사이버 공격의 높은 '상호의존성'과 '상호연계성' 때문이라고 할 수 있다.[408] 즉, 상당주의 의무는 사이버 공격의 개시국 뿐만이 아닌 '경유국'에게도 부과된다고 보는 것이 일반적이므로, 동 의무에 규범적 강제력을 부여하게 된다면 고도로 연결된 사이버 공간의 특성 상 주권국가로서 상당주의 의무의 준수에 관한 부담과 함께 동 의무를 위반하였을 시 자국에 부과되는 제재에 대한 우려가 지속적으로 제기되는 것이다.[409] 이때, 다수의 다자간환경협정에서 활용되어 온 비준수절차는 상당주의 의무의 이행을 확보하는 수단으로서 상당히 적절한 방안이라고 할 수 있을 것인데, 이는 다름 아닌 비준수절차가 제재보다는 의무의 '궁극적 준수'를 장려함으로써 국가 주권의 제약을 최소화하고자 하는 절차이기 때문이다.[410] 즉, 비준수절차의 일차적 목적은 위반에 대한 처벌이나 제재보다는 비준수의 원인을 밝히고 해당 국가가 그 원인을 시정하고 의무를 이행하도록 하는데 있다.[411] 물론 협약상의 의무를 성실히 이행하지 않은 국가에게 제재가 부과될 수는 있으나, 그럼에도 불구하고 비준수절차는 기본적으로 대립적이고 징벌적인 분쟁해결절차를 회피하고자 하는 특성을 가진다.[412] 즉, 주권의 제약을 최소화하고 제재보다는 준수를 장려하는 방식을 채택한다는 점에서 비준수절차는 사이버 공간에서의 상당주의 의무의 불이행에 따른 공식적 제재 및 불이익에 대한 국가의 불안감과 부담감을 완화함으로써 사이버 공간에서 상당주의 의무의 집행력을 확보하기 위한 적절한 수단이 될 수 있을 것이다.

---

408 Michael N. Schmitt, supra note 179, p.69.

409 박노형·김효권, supra note 7, p.87.

410 박병도, supra note 354, p.70.

411 Ibid., p.71.

412 Tseming Yang, supra note 355, p.1148; Pierre-Marie Depuy & Viñuales Jorge E, p.344.

다른 한편, 비준수절차는 상당주의 의무를 이행하기 위한 사이버 역량이 부족한 국가들에 대한 지원 가능성을 확대함으로써 궁극적으로 사이버 공간의 평화적 활용에 기여할 수 있을 것으로 보여진다. 상당주의 의무는 영토국으로 하여금 타국에게 위해를 가하는 목적에서 수행된 사이버 공격이 자국 내에서 개시되거나 혹은 자국을 경유하지 않도록 상당한 주의를 다 할 것을 요구한다.[413] 사이버 공간에서 상당주의 의무의 일환으로, 영토국은 가시적으로 드러나지 않는 사이버 공격을 측정하고 탐지하며 더 나아가 이를 종료할 의무를 부담하게 된다.[414] 그러나 공격을 탐지하고 측정하는 역량은 국가의 사이버 안보 기술의 발전 속도에 따라 큰 차이를 보인다. 물론 상당주의 의무의 불이행 여부를 결정함에 있어서 국가의 개별적 사이버 역량이 고려 대상이 되기는 하나, 여전히 그 기준이 불명확할 뿐만 아니라 무엇보다도 사이버 역량이 부족한 국가는 상당주의 의무 불이행에 노출될 가능성이 확대되는 것이 현실이다. 이러한 어려움 속에서 비준수절차가 협약의무를 준수할 역량이 부족한 국가에 대해서는 제재에 앞서 제도적인 원조와 인센티브를 제공한다는 것은 상당히 주목할 만 한 측면이다.[415] 즉, 비준수절차의 이러한 측면은 조약상 의무에 대한 비준수의 원인이 이행 제도 자체의 결여나 재원 또는 기술적 자원의 부족에 있다면, 제재보다는 동 의무를 준수할 수 있도록 적절한 지원을 제공하여 당사국을 '의무의 준수 상태'로 복귀할 수 있도록 하는 것이 보다 실효적이라는 판단에 기반한 것으로 볼 수 있다.[416] 이러한 특성을 가지고 있는 비준수절차를 상당주의 의무의 집행력 확보 수단으로 활용한다면, 사이버 역량이 부족한 국가에 대한 기술과 시스템의 발전을 위한 적극적인 지원을 제공함으로써 이들 국가의 사이버 역량을 증진하고 결과적으로는 상당주의 의무를 보다 원활하게 준수하는 기반을 만드는 데 기여할 수 있을 것이다. 나아가 사이버 공간의 평화적 활용을 도모하고자 하는 상당주의 의무의 도입 목적 역시 달성할 수 있을 것으로 판단된다.

---

[413] 탈린매뉴얼 2.0, Rule 6.

[414] 탈린매뉴얼 2.0, Rule 7.

[415] Tseming Yang, supra note 355, pp.1141-1142.

[416] 박병도, supra note 354, p.71; Pierre-Marie Depuy & Viñuales Jorge E, supra note 360, p.344.

끝으로, 상당주의 의무의 집행력 확보 방안으로 제시된 비준수절차의 실질적 운영을 제고하기 위한 제도적 장치 역시 검토되어야 한다. 다자간환경협정에 포함된 비준수절차의 구체적인 내용은 협정의 성격에 따라 다소간의 차이를 보이지만 그럼에도 불구하고 대다수의 협정은 공통적으로 '당사국 총회'(Conference of the Parties to the Convention: COP)와 '준수위원회'(Compliance Committee) 등 비준수절차의 이행을 위한 제도적 장치를 포함하고 있다.[417] 이러한 제도적 장치는 개별 당사국의 의무 준수 상황을 확인하고 심사하는 것을 주요 기능으로 삼고 있다.[418] 따라서 사이버 공간에서도 상당주의 의무에 대한 비준수 절차의 효과를 극대화하기 위해서는 마찬가지로 준수위원회 등의 제도적 장치를 필요로 할 것이다. 비준수절차를 위한 준수위원회는 회원국의 대표나 여타의 전문가들로 구성될 수 있으며 이들을 선발함에 있어 당사국총회가 일정한 기능을 수행할 수 있을 것으로 판단된다.[419] 또한, 설립된 준수위원회는 개별 당사국의 사이버 공간에서의 상당주의 의무의 준수 상황을 심사하고 당사국이 제출한 보고서 등을 평가함으로써 상당주의 의무의 궁극적 '준수'를 위한 실질적 기여를 할 수 있을 것으로 보인다.

제 2 절. 연구의 한계와 함의

I. 본 연구의 한계

1. 상당주의 의무의 본질적인 딜레마

[417] 박병도, ibid., 75-76면; Francesca Romanin Jacur et al., "Triggering Non-Compliance Procedure", pp.380-383; Nils Goeteyn & Frank Maes, "Compliance Mechanisms in Multilateral Environmental Agreements: An Environmental Agreements: An Effective Way to Improve Compliance?", Chinese Journal of International Law, Vol. 10, No. 4 (2023), p.793.

[418] Nils Goeteyn & Frank Maes, ibid., pp.693-794; 박병도, supra note 354, p.79.

[419] 박병도, ibid.

상당주의 의무는 사이버 공격의 개시국 뿐만이 아닌, 자국의 관할권 내에서 발생하는 초국경적 피해에 적절히 대응하지 못한 공격의 경유국(transit state)에게도 부과되는 의무라는 측면에서 적용상의 명확한 실익이 있다. 그리고 이러한 적용상의 이점으로 인하여 상당주의 의무에 대한 국제사회 및 학문적 차원에서의 관심이 더욱 증가하고 있는 것으로 보인다.[420] 그러나 동시에 상당주의 의무의 특성은 단순히 공격과 관련이 있는 경유국 등이 부담하여야 할 의무와 책임의 범위를 과도하게 확장할 수 있다는 우려로 이어지기도 한다.[421] 이러한 우려는 결과적으로 사이버 핵심 역량 국가들이 상당주의 의무에 관습국제법의 지위를 부여하는 것을 주저하게 만드는 사유가 되었으며, 또한 사이버 역량이 부족한 일부 국가로 하여금 상당주의 의무의 적용에 대한 회의적인 태도를 견지하는 결과를 유발하기도 하였다. 다시 말해, 상당주의 의무는 경유국으로 하여금 자국의 영토 내에서 사이버 공격의 피해를 방지하고 최소화 할 의무를 부과한다는 점에서 사이버 공격의 귀속(attribution)에 대한 어려움 등을 해결하기 위한 획기적인 규범으로 주목받고 있으나, 동시에 상당주의 의무의 이러한 측면은 동 의무의 법적 지위와 구체적인 발동 요건 등에 대한 국제사회의 합의를 저해하는 원인이 되기도 하였다. 즉, 사이버 공격과 관련한 경유국에 대하여 일정한 의무를 부담하도록 하는 것이 상당주의 의무의 핵심이자 본질적 요소이지만, 동시에 상당주의 의무는 오늘날 국제사회로 하여금 동 의무의 준수가 관련국에 대한 불합리한 수준의 부담으로 이어지지 않도록 하기 위한 적정 기준에 대해 고민할 필요성을 제기하기도 한다. 그리고 이러한 지점이 바로 상당주의 의무가 갖는 적용상의 본질적인 딜레마라고 볼 수 있을 것이다.

이러한 맥락에서 국제사회는 상당주의 의무를 사이버 공간에 적용하는 과정에서 경유국이 동 의무를 준수하기 위한 적절한 수준의 '기준'과 '한계'

---

[420] Abhijeet Shrivastava & Rudraksh Lakra, "Unpacking Cyber Due Diligence Practice: Detection, Mitigation, and Prevention", Opinio Juries (2020), available at https://opiniojuris.org/2023/03/20/unpacking-cyber-due-diligence-in-practice-detection-mitigation-and-prevention/ (마지막 접속일: 2023. 07. 13)

[421] Ibid.

를 명확하게 설정하는 작업을 우선적으로 실시할 필요가 있다. 다시 말해, 이는 경유국이 상당주의 의무를 다하기 위한 구체적 요건은 무엇이며, 또한 이러한 요건이 경유국으로 하여금 과도한 부담으로 이어지지 않도록 하기 위하여 국제사회는 어떠한 제반 사실과 맥락을 고려하여야 하는가에 관한 문제인 것이다. 이와 관련하여 탈린매뉴얼을 집필한 국제전문가그룹이 상당주의 의무를 준수해야 하는 경유국의 범위를 보다 세밀하게 분류하였다는 사실은 주목할 만 하다.[422] 탈린매뉴얼은 불법적인 데이터가 영토국의 사이버 기반시설인 광섬유 케이블을 단순히 '통과'하는 경우와, 악의적인 목적을 가지는 봇넷 등의 사이버 기초설비가 한 국가의 사이버 기반시설에 완전히 '구축'되는 경우를 구분하였다.[423] 양자는 자국의 의도와 직접적인 관련이 없는 집단 혹은 타국에 의하여 발생한 사이버 공격이 자국의 관할권 하에 있는 사이버 기반시설을 경유하였다는 점에서 유사하지만, 기반시설이 사이버 공격 과정에 연루된 '정도'의 측면에서는 다소간의 차이를 보인다. 이러한 차이에 대하여 탈린매뉴얼은 불법적인 데이터가 단순히 사이버 기반시설을 통과하는 전자의 상황에 대해서는, 봇넷 등이 완전히 구축된 후자의 경우에 비하여 상당주의 의무의 발동 요건을 비교적 엄격하게 설정할 필요가 있다는 견해를 제시하였다.[424] 즉, 전자의 경우 악성 데이터가 자국의 사이버 관할시설을 경유하고 있다는 사실을 당국이 인식하고 있으며, 동시에 이를 종료 시키기 위해 실행 가능한 조치를 취할 수 있는 사이버 역량을 보유한 경우에 한정하여 당해 국가에 상당주의 의무를 부담하도록 해야 한다는 것이다.[425] 탈린매뉴얼의 이러한 논의로부터 주목해야 할 점은 사이버 공간에서 상당주의 의무가 발동되는 요건을 세분화함으로써 경유국의 과도한 부담을 지양하고 합리적인 기준을 제시하고자 하였다는 사실이다. 국제전문가그룹은 악성 데이터가 단시간 동안에 사이버 기반시설을 단순히 '통과'하는 것을 영토국이 식별함에 있어서는 상당한 기술적인 어려움이 따른다는 사실을 충분히 고려한 것으로 보인다.[426]

---

[422] 탈린매뉴얼 2.0, Rule 6 (13).

[423] 탈린매뉴얼 2.0, Rule 6 (13).

[424] 탈린매뉴얼 2.0, Rule 6 (13); Michael N. Schmitt, supra note 179, pp.72-73.

[425] 탈린매뉴얼 2.0, Rule 6 (13); Michael N. Schmitt, ibid., p.72.

[426] 탈린매뉴얼 2.0, Rule 6 (14); Michael N. Schmitt, ibid.

결국 상당주의 의무의 적절한 발동 요건과 한계를 설정함에 있어서는 앞서 언급하였던 영토국의 인식(knowledge) 여부에 대한 검토가 이루어져야 한다.[427] 다른 한편, 영토국의 전반적인 사이버 역량 역시 고려되어야 함은 물론이다.[428]

고도로 연결된 사이버 공간에서 국가는 무엇보다도 자국이 상당주의 의무를 부담하여야 하는 상황에 광범위하게 노출되는 것을 가장 우려하고 있으며, 이는 곧 상당주의 의무의 적용 및 준수에 대한 국가의 소극적이고 부정적인 태도로 이어진다.[429] 국가가 가지는 이러한 우려를 불식시키기 위해서는 앞선 검토와 같이 국제사회의 논의를 통해 상당주의 의무의 발동 요건을 보다 치밀하게 설정할 필요가 있으며, 이때 '상당주의 의무의 도입 목적'과 '적절한 부담의 수준' 양자가 모두 적절히 고려되어야 한다. 이러한 논의는 관련 국가가 가지는 상당주의 의무에 대한 막연한 부담감의 해소에 기여할 수 있을 것이고, 나아가 상당주의 의무의 규범적 지위에 대한 국제사회의 원활한 합의를 이끌어 내는데 긍정적인 역할을 할 수 있을 것으로 기대된다. 사이버 공간에서 상당주의 의무를 준수하는 주체와 범위를 확장하는 것은 사이버 공간의 평화적 활용을 위하여 물론 중요하다. 그러나 현 시점에서는 상당주의 의무의 준수에 대한 국제사회 전반의 우호적인 분위기를 형성하고, 또한 동 의무의 준수를 위한 적합하고 합리적인 기준을 설정하는 작업이 우선되어야 할 것이다.

2. 기술적 한계

다른 한편, 오늘날 국가의 사이버 방어 역량과 사이버 공간 및 공격의 특이성(peculiarity)을 고려할 때, 사이버 공격의 경유국이 상당주의 의무를 부담하는 것에는 명백한 기술적 한계가 존재한다는 주장이 지속적으로 제기되고 있다. 이들의 주장은 크게 사이버 공격을 '인식'할 수 있는 경유국의 기술

---

427 Maja Bergwik, "Due Diligence in Cyberspace", p.48.

428 Ibid.

429 Michael N. Schmitt, supra note 179, pp.71-72.

적 능력에 대한 한계와 인식된 사이버 공격을 적절히 '방어'할 수 있는 기술적 한계로 나뉜다. '인식'의 어려움을 문제 삼는 견해의 경우, 경유국이 자국의 관할을 통과하는 사이버 공격을 인식하고 식별하는 작업 자체가 기술적으로 상당히 어렵다는 점을 지적하고 있다.[430] 가령, 단시간 내에 사이버 기반시설을 통과하는 악성소프트웨어의 '표지'(signature)를 인식하는 것은 그 자체로 용이하지 않으며, 표지가 인식되지 않았다면 안티바이러스 소프트웨어에서 이러한 멀웨어(Malware)가 탐지되지 않거나 혹은 이미 암호화 되었을 가능성이 크기 때문에[431] 결과적으로 경유국이 상당한 주의의 일환으로 특정한 조치를 취하는 것에는 기술적, 현실적 어려움이 뒤따른다는 것이다.

그렇다면 사이버 역량이 향상됨에 따라 경유국이 악성 소프트웨어의 경유 사실을 보다 쉽게 인식하게 된다면, 사이버 공간에서 상당주의 의무를 적용하는 것의 기술적인 문제는 해결되는 것으로 볼 수 있는가? 공격의 인식 요건에 대한 고민이 해결되더라도 악성 소프트웨어를 방어할 수 있는 기술에 대한 문제는 추가적 논의를 요하는 하는 별개의 영역이다. 즉, 사이버 공격을 위한 악성소프트웨어가 자국의 기반시설을 경유할 것을 경유국이 사전에 명백히 인식하였음에도 불구하고, 구체적인 공격의 일자, 범위, 루트 등을 파악할 수 없음에서 기인하는 방어의 어려움 역시 상당주의 의무 적용 상의 기술적 한계로 지적된다.[432] 가령, 사이버 공격이 자국의 관할을 경유할 것이라는 정보를 입수 및 인식하였을 때, 이를 방어하기 위해 관할권 하의 모든 사이버 기반시설을 차단(block)하는 조치에 대해 검토해볼 수도 있을 것이나, 이는 국제법상 비례성(proportionality) 및 합리성(reasonableness)의 원칙에 비추어 볼 때 결코 타당하지 않다.[433] 무엇보다도 사이버 공격의 특성상 하나의 경로가 차단되면 자동적으로 새로운 경로가 재지정(rerouted along a different transmission path)된다는 점을 고려한다면[434] 악성소프트웨어의 경로

---

[430] Ibid., pp.72-73.

[431] 탈린매뉴얼 2.0, Rule 6(14).

[432] Robert Kolb, supra note 290, p.126.

[433] Ibid.

[434] Ibid.

를 파악하고 이를 사전에 방어하기 위해서는 상당한 수준의 방어 기술을 갖추어야 할 것으로 판단된다.

지금까지의 내용을 요약하자면 사이버 공격의 경유국이 상당주의 의무를 부담함에 있어서 현재로써 명백한 기술상의 한계가 존재하며, 이러한 기술적 한계를 근거로 경유국의 상당주의 의무 부담에 대한 우려의 시선이 존재하는 것으로 정리할 수 있다. 사이버 공간에서 경유국이 상당주의 의무를 부담하는 것에 대해 우려하는 국가가 다수 존재하며, 또한 실질적인 기술적 어려움 역시 적지 않게 확인되는 것이 사실이다. 더욱이, 악성 소프트웨어가 단시간에 걸쳐 기반시설을 경유하는 상황에서 이러한 기술적 한계가 쉽게 확인될 것이라는 점은 자명하다. 그럼에도 불구하고 사이버 공간에서 공격의 경유국이 상당주의 의무를 부담하여야 한다는 기본적인 원칙은 견지되어야 한다. 상당주의 의무는 사이버 공격의 특성 상 공격의 배후국 혹은 관련 비국가행위자를 특정하는 것이 기술적으로 매우 어렵고, 그 결과로 국가책임법의 적용이 용이하지 않다는 국제사회의 인식 하에 도입의 필요성이 제기된 것이다. 즉, 상당주의 의무의 핵심적 가치이자 동 의무의 핵심적인 도입 목적은 사이버 공격의 경유국에 대해서도 공격으로 인한 초국경적 피해 방지와 사이버 평화의 유지를 위한 일련의 책임을 부담하도록 하는 것에 있다. 따라서 현재 제기되는 기술적 한계는 사이버 역량의 향상을 통해 극복되어야 할 필요가 있다. 탈린매뉴얼의 대표 집필자인 Michael N. Schmitt는 기술의 끊임없는 발전을 통해 이러한 기술적 한계가 충분히 극복될 수 있으며, 이미 상당 부분은 극복되었다는 의견을 제시한 바 있다.[435] 오늘날 다양한 방식을 통해 이루어지는 사이버 공격은 국가 안보에 대한 실질적인 위협으로 작용하고 있으며 상당주의 의무는 이러한 위험에 효율적으로 대응하기 위한 수단이 될 수 있다. 때문에 국가의 사이버 역량 향상을 통해 기술적 한계를 극복할 필요가 있으며, 더불어 이러한 과정에서 사이버 핵심 역량 국가의 기타 국가에 대한 기술적 원조 역시 긍정적으로 검토되어야 한다.

[435] Michael N. Schmitt, supra note 179, p.72.

II. 본 연구의 함의

상당주의 의무는 사이버 공간과 관련한 국제사회 담론의 가장 핵심적 논제라고 해도 과언이 아니다. 본 연구는 전통적인 국제법의 영역에서 널리 원용되어 온 상당주의 의무의 사이버 공간에서의 적용 가능성, 적용상 법적 쟁점, 그리고 적용상 한계에 대해 검토하는 것을 주 목적으로 한다. 앞선 논의를 바탕으로 하여 아래에서는 본 연구가 가지는 함의에 대해 살펴보고자 한다. 본 연구가 분단국인 우리나라의 사이버 안보에 갖는 함의에 대하여 우선 살펴본 뒤, 다음으로 국제사회의 안보 전반에 갖는 함의에 대하여 검토하고자 한다.

1. 우리나라의 사이버 안보에 갖는 함의

사이버 공간에서 상당주의 의무의 적용가능성과 역할에 대하여 다룬 본 연구는 분단국인 우리나라의 사이버 안보의 측면에서 중요한 함의를 갖는다. 오늘날 사이버 공격은 재래식 공격에 버금갈 정도로 매우 빈번하게 발생하고 있으며 피해의 규모와 형태 역시 예측 불가한 수준에 이르렀다. 북한은 이러한 사이버 수단을 국가 안보의 핵심 전략으로 사용하고 있으며 나날이 발전하는 북한의 사이버 공격 역량은 한국을 비롯한 국제사회의 안보에 상당한 위협 요인으로 작용한다.[436] 북한은 2004년에 우리나라와 미국을 정찰하기 위한 목적으로 사이버 수단을 처음 활용한 바 있다. 이들의 사이버 공격은 2009년 DDoS 공격을 기점으로 보다 정교해 졌으며, 공격의 영향력 역시 점차적으로 확대되고 있다.[437] 2021년을 기준으로 북한은 2004년에 비해 약 300배 더 많은 사이버 공격을 감행한 것으로 추정되며, 이러한 추세는

[436] Tae Eun Song, "DPRK's Illicit Cyber Activities: Latest Development and ROK's Responses", IFANS FOCUS, 2022-28E (2022), p.1.

[437] Hyeong-wook Boo, "An assessment of North Korean Cyber Threats", The Journal of East Asian Affairs, Vol. 31, No. 1 (2017), p.100.

COVID-19에 따른 북한의 국경 폐쇄와 함께 더욱 심화되고 있는 것으로 보인다.[438]

북한의 사이버 공격과 관련하여 '상당주의 의무'에 대한 논의가 우리나라의 사이버 안보에 보다 큰 함의를 갖는 이유는, 오늘날 발생하는 상당수의 북한 발 사이버 공격이 중국과 동남아를 비롯한 세계 각국에 공격의 진원지를 두거나 혹은 해당 제3국의 기반시설을 경유하는 방식을 통해 이루어지고 있기 때문이다. 가령, 북한 당국이 배후에 있을 것으로 추정되는 2014년 '소니 픽처스(Sony Pictures Entertainment) 해킹사건'의 경우 당해 공격이 볼리비아, 키프로스, 이탈리아, 태국, 폴란드 등 세계 각지의 인터넷 프로토콜 주소를 통해 라우팅 되었다는 사실이 확인된 바 있다.[439] 이외에도 북한은 불법 게임 사이트 개발과 운영을 위한 악성코드를 태국과 캄보디아에 심음으로써 이들 국가를 사이버 공격의 진원지로 사용하고 있다.[440] 또한 북한은 인프라의 발달과 안보의 측면에서 사이버 공격에 보다 유리하다는 판단 하에 중국의 베이징, 선양, 다롄 등 제3국의 지역을 사이버 해킹의 거점으로 적극 활용하고 있기도 하다.[441] 그러나 보다 심각한 문제는 자국 관할의 사이버 기반시설이 북한의 사이버 공격을 위해 사용되고 있다는 것을 명백히 인지하고 있음에도 불구하고 이들 국가가 이러한 행위를 저지하기 위한 특별한 제재를 부과하지 않음에 있다. 즉, 제3국을 경유하는 북한의 사이버 공격은 이들 제3국의 명백한 '묵인'(tacit consent) 하에 이루어지고 있는 것으로 볼 수 있는 것이다.[442]

---

438 Tae Eun Song, supra note 436, p.1.

439 Brooks Barnes & Nicole Perlroth, "Sony Pictures and F.B.I Widen Hack Inquiry", The New York Times, (Dec. 3, 2014), available at https://www.nytimes.com/2014/12/04/business/sony-pictures-and-fbi-investigating-attack-by-hackers.html (마지막 접속: 2023.7.27)

440 윤태영·우정민, "북한의 대남 사이버공격 양상과 행태: 사이버파워와 강압이론을 통한 분석", 『융합안보논문지』, 제18권 제1호 (2018), p.128.

441 Daniel Schearf, "North Korea's 'World Class' Cyber Attacks coming from China", VOA, (Nov. 21, 2013) (마지막 접속: 2023.7.27)

442 Ibid.

오늘날 사이버 공격은 '비대칭적 위협'(asymmetric threat)의 대명사가 되었다. 즉, 사이버 공격은 저비용으로 강대국의 정보통신기술의 핵심 자산에 치명적인 타격을 입힐 수 있기 때문에 핵, 미사일과 더불어 오늘날 북한 정권에 보다 필수적인 공격 수단으로 자리매김하게 된 것이다.[443] 무엇보다도 우리나라는 정보통신기술이 고도로 발달하였고 네트워크 간의 의존도가 매우 높으므로 북한의 사이버 공격에 대한 취약성이 배가 된다.[444] 사이버 공격이 갖는 이러한 비대칭적 위협의 특성과 파급력을 감안할 때 북한의 사이버 공격 방식은 시간이 지남에 따라 더욱 정교해질 것이고, 우리나라의 피해 역시 그 규모와 수준의 측면에서 점차적으로 확대 및 심화 될 가능성이 농후하다. 북한의 전방위적인 사이버 공격에 대처하기 위한 보다 본질적이고 거시적인 차원의 대응 방안이 절실한 시점인 것이다. 국정원은 북한의 사이버 위협에 대응하기 위하여 2022년에 '국가사이버안보협력센터'를 개소한 사실이 있다.[445] 그러나 앞서 확인한 바와 같이 북한의 사이버 공격은 공공과 민간을 가리지 않을 뿐만 아니라 공격의 방식 역시 결코 재래식 공격처럼 단순하고 직관적이지 않다. 북한의 사이버 공격 과정에서 가장 대표적으로 확인되는 특성은 다양한 제3국 거점을 경유하여 공격자의 신분 노출을 최소화하는 전략을 활용함으로써 정권에 대한 국제적 제재와 책임을 회피하고자 한다는 점이다.[446] 우리나라를 향한 사이버 공격 과정에 내재된 북한의 이러한 전략적 계산과 사이버 공격이 갖는 특성을 종합적으로 고려한다면 북한의 사이버 공격에 대한 방어와 무력화 과정에서 제3의 '경유국'이 보다 중요한 역할을 할 수 있다고 판단된다. 따라서 사이버 공간에서 상당주의 의무의 적용 가능성과 구체적인 적용 방안에 대한 본 연구는 제3국을 경유하는 방식으로 이루어지는 북한의 지속적인 사이버 공격에 효율적으로 대처하고, 분단국인 한국의 사이버 안보 역량 증진에 있어서 보다 큰 함의를 가진다고 할 것이다.

---

[443] Hyeong-wook Boo, supra note 437, p.104.

[444] Ibid., p.110.

[445] 이승열, "북한 사이버 공격의 현황과 쟁점", 국회입법조사처, 제2034호 (2022), p.4.

[446] Brooks Barnes & Nicole Perlroth, supra note 439.

2. 국제사회의 안보 전반에 갖는 함의

사이버 공간에서 상당주의 의무의 적용 가능성을 모색하고 동 의무의 적용상 쟁점에 대하여 검토한 본 연구는, 사이버 공간을 적절히 규율하고 사이버 공격에 효율적으로 대처하기 위하여 노력하는 국제사회의 전반적인 논의의 흐름과 맞닿아 있다. 최근 국제사회는 가속화 된 기술의 발전과 COVID-19 팬데믹 등으로 인하여 이른바 '뉴 노멀(New Normal)' 시대를 맞이하게 되었다.[447] 뉴 노멀 시대의 화두는 다름 아닌 물리적인 영역과는 차별화되는 사이버 영역과 그로부터 파생되는 각종 쟁점 사안이라고 할 수 있다. 앞서 확인한 바와 같이 오늘날 국제사회는 사이버 공간에 적용되는 국제 규범을 논의함에 있어서의 여러가지 쟁점 중 특히 '상당주의 의무'의 역할에 지대한 관심을 표해 왔다. 사이버 공간에서 상당주의 의무의 구체적 적용 방안과 적용상 법적 쟁점에 대하여 논의하는 것은, 변모된 '안보 개념' 하에서 국제사회 전반의 안보를 증진하기 위한 방안으로서 매우 중요한 함의를 갖는다.

그간 국제사회는 지정학적 요인 혹은 패권에 기초한 이익 관계 등을 종합적으로 고려함으로써 재래식 전쟁에 보다 효율적으로 대처하기 위한 '군사 동맹'을 형성해 왔다. 군사 동맹은 재래식 전투에 대처하고 국가 안보를 증진하기 위한 측면에서 오늘날에도 여전히 유효하다고 할 것이다. 다만 재래식 전투와는 차별화 된 특성을 지니는 사이버 공격에 효과적으로 대처하기 위해 국제사회는 이전과는 차별화 된 방안을 모색할 필요가 있다. 사이버 공간은 초국경성과 높은 익명성을 본원적인 특성으로 가지는 바, 특정 지역 혹은 패권 관계 등에 기반하여 형성된 군사 동맹이 사이버 공격을 방지하기 위한 적절한 역할을 수행하지 못할 우려가 있기 때문이다. 사이버 공격의 수행자는 특정 국가와의 직접적 연관성을 장담하기 어려운 비국가행위자인 경우가 상당수이며, 이들의 공격 근거지 역시 특정 영역 혹은 명백한 하나의 국가로 단정짓는 작업 역시 용이하지 않다.[448] 결과적으로 오늘날 일상화 된 사이버

---

[447] 채재병, "사이버 안보의 국제정치적 추세와 한국의 전략구상", 국가안보전략연구원, 연구보고서 2021-18, (2021), p.6.

[448] Antonio Coco & Talita Dias, supra note 310, p.7.

공격은 국제사회의 '안보 개념'을 크게 변화시켰으며, 안보 개념의 변화는 위협 주체의 다양성, 대응 방안의 불투명성 등을 야기하였다고 볼 수 있다.[449]

이처럼 위협의 형태가 변화한 상황을 고려할 때 국가의 안보를 추구하는 방법 역시 변모할 필요가 있다.[450] 즉, 초국경적인 차원에서 발생하는 사이버 위협을 방지하기 위한 방안은 한정된 국가 간에 형성된 물리력에 의존한 동맹 체제보다는, 절대 다수의 주권 국가가 참여하는 초국가적 협력의 맥락에서 이루어지는 것이 보다 효율적일 것으로 판단된다.[451] 그리고 바로 이 지점에서, 국제사회 전반의 안보를 증진시키기 위한 방안으로서 '상당주의 의무'는 보다 큰 의의를 가진다고 할 것이다. 상당주의 의무는 초국경적 피해를 유발할 가능성이 있는 악성 소프트웨어가 자국 관할의 사이버 기반시설을 경유하거나 혹은 자국 관할 내에서 개시되는 것을 인지한 경우, 당해 국가에 부과되는 규범이다. 즉, 사이버 공격을 방지하기 위한 의무가 '공격의 명백한 배후국', 혹은 공격에 가담한 '비국가행위자의 국적국'에 대하여 제한적으로 부담되는 경우와 비교한다면 상당주의 의무는 의무 부담의 주체를 확장함으로써 초국가적인 협력을 달성하고 사이버 안보를 보다 굳건히 하는 데 기여할 수 있을 것이다.

---

[449] 채재병, supra note 447, p.27.

[450] Ibid., p.25.

[451] Ibid.

제 6 장. 결론

본 연구는 사이버 공간을 매개로 발생하는 사이버 공격의 특성상 공격의 결과를 특정 국가로 귀속하여 직접적인 유책국에 대한 국가책임을 추궁하기 어렵고, 공격 과정에서 제3국이 차지하는 비중이 점진적으로 확대되는 현상에 주목하였다. 그리고 이러한 현실 속에서 피해국의 권리를 실효적으로 구제하고 사이버 공간의 평화적인 활용을 도모하기 위한 방안으로 전통적인 국제법 영역에서 널리 활용되어 온 '상당주의 의무'(due diligence)를 사이버 공간에도 적용할 것을 제안하였다.

상당주의 의무는 국가의 '주권(sovereignty)'과 '주권의 상호 존중'으로부터 비롯한 개념이다. 전통적인 국제법 영역에서 상당주의 의무는 국제환경법을 비롯한 국제인권법, 국제투자법, 국제환경법 등의 다양한 분야에서 국가의 행위에 일정한 제한을 가하거나 의무를 부과하는 개념으로 활용되어 왔다. 이처럼 전통적인 국제법의 영역에서 활발하게 원용되어 온 상당주의 의무가 오늘날 새롭게 부상하는 영역인 사이버 공간에서 국제사회의 큰 주목을 받는 이유는, 다름 아닌 동 의무의 준수 주체가 공격과 관련된 '제3국', 가령 공격의 '경유국'이라는 사실에 있다. 제2장에서 검토된 바와 같이 사이버 공간에서 수행되는 사이버 공격은 공격 결과에 대한 책임 귀속이 매우 어려우며, 결과적으로 국제법상 국가책임법을 적용하는 것 역시 용이하지 않다. 사이버 공격의 결과를 특정 국가로 귀속하기 어려운 이유는 '국가와 비국가행위자 간의 다양한 연계 방식', '비대칭적이고 복잡한 공격의 양태', 그리고 '공격의 익명성' 등 매우 종합적이고 다양한 원인으로부터 기인한다. 더불어, 상당수의 사이버 공격이 제3국을 경유하여 발생하는 현실을 고려할 때, 사이버 맥락에서 공격의 직접적 배후국과 피해국 이외의 '제3국'이 차지하는 역할과 중요성은 점진적으로 확대된다고 할 것이다. 오늘날 다수의 국가와 국제기구, 그리고 국제법 학자들이 사이버 공간에서 상당주의 의무의 적용 가능성에 지대한 관심을 표하는 이유를 바로 여기서 찾을 수 있다. 즉, 상당주의 의무는 사이버 공격의 피해국이 기댈 수 있는 실효적인 권리 구제 수단이라는 점에

서도, 또한 제3국의 역할이 점차적으로 증대되는 사이버 맥락에서 공격과 관련된 경유국에게 자국의 관할 내에서 초국경적 피해를 방지하기 위한 일정한 의무를 부과할 수 있다는 점에서도 매우 유용한 수단이 될 수 있는 것이다.

다만, 본 연구를 통해서 살펴본 바에 의하면 상당주의 의무의 명백한 적용상 이점에도 불구하고 실질적으로 동 의무를 사이버 맥락에서 활용함에 있어서는 추가적인 논의를 필요로 하는 법적 쟁점이 존재한다. 첫번째로, 사이버 공간에서 상당주의 의무의 국제법적 구속력이 부재하므로 동 의무의 규범적 가치 확보에 관한 논의가 이루어질 필요가 있다. 현재 사이버 맥락에서 상당주의 의무는 국가들의 자발적 참여를 요하는 '비구속적 자발적 규범'의 영역으로 분류된다. 본 연구는 사이버 맥락에서 상당주의 의무의 규범적 지위에 대한 단기적이고 범세계적인 합의를 도출하지 못하는 현 상황에서, 상당주의 의무가 연성법으로서 일정한 역할을 수행할 수 있을 것으로 보았다. 다만 상당주의 의무가 국가의 실질적인 의무 이행을 담보하고 사이버 상에 도입된 본연의 역할을 다하기 위해서는 궁극적으로 규범적 강제력을 획득할 필요가 있다고 판단되는 바, 상당주의 의무의 국제관습법으로의 지위 변화 가능성 역시 검토하였다. 현재 상당주의 의무가 규범적 강제력을 갖는 것에 부정적인 견해를 취하는 대표적인 국가는 사이버 핵심 역량 국가들이지만, 오늘날 이들을 상대로 감행되는 적대적 사이버 조작이 급격하게 증가하고 있는 현실을 고려할 때 동 의무의 국제법적 지위에 관한 논의 과정에서 향후 사이버 강대국의 입장 선회를 기대해볼 수 있을 것으로 사료된다.

두번째 법적 쟁점은 사이버 공간에 상당주의 의무를 적용함에 있어서의 구체적 적용 기준 마련의 필요성과 관련된다. 상당주의 의무는 본연적으로 상당한 유연성과 자율성을 가지는 규범으로, 이러한 특성으로 말미암아 동 의무는 보다 다양한 국제법 분야와 넓은 맥락 하에서 원용될 수 있었다. 그러나 동시에 상당주의 의무의 이러한 특성은 동 의무가 구체적인 상황에 적용되었을 때 적용상의 모호함을 유발하는 기제가 되기도 하였다. 특히나 상당주의 의무가 사이버 맥락에 적용됨에 있어서는 동 의무의 본원적 특성인 유연함과 신축성에, 사이버 공간이 가지는 특수성이 더해짐에 따라 극심한 해석상의 혼란과 적용상의 모호함이 야기될 우려가 있다. 이러한 문제의 인

식 하에, 본 연구에서는 상당주의 의무를 사이버 공간에 실질적으로 적용함에 있어서의 구체적 기준과 발동 요건에 대한 합의를 도출할 필요가 있다고 판단하였다. 이를 통해 상당주의 의무의 이행에 대한 국가의 자의적 해석을 방지하고 동 의무를 준수하는 국가의 실행에서도 일관성을 확보할 수 있을 것이다. 끝으로, 사이버 공간에서 상당주의 의무의 집행력을 확보하기 위한 논의가 이루어져야 한다. 사이버 맥락에서 상당주의 의무의 집행력 확보 수단 구축에 관한 논의는, 동 의무를 이행하고자 하는 국가의 순수한 의지만으로는 확실한 의무의 준수를 담보하는 데 한계가 있다는 현실 인식에 기초한다. 이에, 본 연구는 국제환경법의 다자간환경협정에서 적극적으로 활용되는 '비준수절차'의 역할에 주목하였으며 비준수절차를 상당주의 의무의 집행력을 제고하기 위한 방안으로 적극 활용할 것을 제안하였다. 다만, 다자간환경협정상 비준수절차는 구속력이 있는 국가간 합의에 기반하여 논의돼왔다. 따라서 상당주의 의무의 집행력 확보 방안으로서의 비준수절차에 관한 논의 역시 동 의무가 사이버 공간에서 구속력 있는 규범적 지위를 획득한 이후의 상황을 전제로 한다.

한편, 사이버 공간에서 상당주의 의무의 적용 가능성과 구체적 방안에 관해 검토한 본 연구에는 일정 부분의 한계가 존재하는데, 이는 크게 상당주의 의무가 갖는 본질적 한계와 의무 준수 과정에서 나타나는 기술적 한계로 요약된다. 가령 공격과 관련한 경유국에게 일정한 의무를 부담하도록 하는 것이 상당주의 의무의 핵심이자 본질이지만 동시에 상당주의 의무의 이러한 특성은 동 의무의 준수가 관련국에 대한 불합리한 수준의 부담으로 이어지지 않도록 할 적정 기준에 대하여 고민할 필요성을 제기하기도 한다. 이는 상당주의 의무가 사이버 공간에 적용됨에 있어서의 본원적 딜레마라고 할 수 있으며, 국제사회는 상당주의 도입 목적과 적절한 부담 수준 양자를 모두 적절히 고려할 필요가 있다. 다른 한편으로 국가의 사이버 역량과 사이버 공격이 갖는 특이성을 고려할 때, 공격의 경유국이 상당주의 의무를 부담하는 것에는 명백한 기술적 측면의 한계가 존재한다는 지적이 제기된다. 이러한 한계는 각각 사이버 공격의 인식 기술과 인식된 공격을 적절히 방어할 기술 측면의 한계로 분류할 수 있다. 이처럼 사이버 맥락에 상당주의 의무를 적용함에

있어서는 앞서 언급한 일부 한계가 존재하지만 상당주의 의무의 적용 가능성과 역할에 관해 논의한 본 연구는 우선 오늘날 분단국인 우리나라의 사이버 안보의 측면에서 큰 함의를 갖는다. 비대칭적 위협의 전형인 사이버 공격은 핵, 미사일과 함께 오늘날 북한의 핵심적인 국방 전략으로 자리매김하였다. 북한의 사이버 공격에서 대표적으로 확인되는 특성은 대다수의 공격 과정에서 중국과 동남아시아 등 제3의 공격 거점을 매우 빈번하게 경유한다는 점이다. 이러한 측면에서, 사이버 공격의 경유국에 일정한 의무를 부여하는 규범인 상당주의 의무에 관한 논의는 북한의 사이버 공격에 대처하고 우리나라의 사이버 안보를 증진함에 있어서 유의미한 방안이 될 것으로 판단된다. 끝으로 본 연구는, 새롭게 대두한 영역인 사이버 공간을 적절하게 규율하기 위한 국제 규범을 모색하고, 특히 급격하게 증가하는 사이버 공격에 효율적으로 대처하기 위한 방안에 대해 고민하는 국제사회의 전반적인 논의의 흐름과 맥을 함께 한다. 국제사회의 안보 개념에 근본적인 변화를 가져온 사이버 공격에 효율적으로 대처하기 위해서는 이에 대처하는 방안 역시 변화할 필요가 있다. 이에, 상당주의 의무는 단순한 공격 배후국과 피해국을 넘어서 공격과 관련한 경유국에게 일정한 의무를 부과하는 규범인 바, 사이버 맥락에서의 의무 부담의 주체를 확장함으로써 사이버 공격으로부터 발생하는 국제사회의 안보 공백을 최소화 하는데 기여할 수 있을 것으로 판단된다.

과학 기술이 고도로 발달하고 그에 따른 새로운 국제적 이슈가 대두함에 따라 국제사회는 크고 작은 변화를 겪어왔다. 이처럼 과학과 기술 발전에 따른 사회상의 변화는 국가의 권리와 의무의 원천이 되는 국제법에도 상당한 영향력을 행사하였다. 가령, 비인도적인 방식으로 활용됨으로써 인류를 위협할 수 있는 신무기의 등장은 동 무기의 사용을 제한하거나 혹은 전면적으로 금지하는 국제협약의 탄생으로 이어졌다. 다른 한편, 환경 오염 내지 기후변화 문제를 극복하기 위한 방안으로 국제사회는 다수의 환경 관련 국제 선언과 협약을 채택함으로써 인류가 직면한 환경 위기를 극복하기 위한 토대를 마련하기도 하였다. 이처럼 국제법은 국가와 인류가 직면한 난제를 해결하고 궁극적으로는 국제사회의 평화와 상생 그리고 안전을 추구하기 위하여 국제사회의 요구에 따라 끊임없이 변화하고 발전해 왔다. 그렇다면 새로운 이해

를 필요로 하는 사이버 공간을 적절히 규율하고, 사이버 공간을 매개로 발생하는 사이버 공격에 효율적으로 대처하기 위한 방안을 모색함으로써 국제사회의 궁극적 평화와 상생을 도모하는 것은 오늘날의 국제법이 직면한 또 하나의 새로운 과제라고 할 수 있다. 이때, 국제법상 '상당주의 의무'는 사이버 공간이 대두하고 사이버 공격이 일상화 됨에 따라 발생하게 되는 문제에 대한 유효한 대안이 될 것으로 판단된다. 물론 상당주의 의무가 사이버 공간에서 본연의 역할을 다하기 위해서는 여전히 추가적인 논의를 요하는 법적 쟁점이 존재하는 것이 사실이다. 그럼에도 불구하고, 초국경적이고 비대칭적인 방식으로 이루어지는 사이버 공격을 보다 효율적으로 규율함으로써 사이버 공간의 평화적 활용을 도모하고, 나아가 국가책임법리의 원용이 어려운 현 시점에서 피해국이 유효하게 기댈 수 있는 수단으로서 상당주의 의무는 적용상의 실익이 명백하다. 상당주의 의무의 규범적 지위에 관한 궁극적 합의와 구체적인 적용상 기준을 마련하기 위한 국제사회의 논의가 지속적으로 이루어져야 하며, 이를 통해 사이버 공간의 평화로운 활용을 기대할 수 있을 것이다.

참고문헌

■ 단행본

[국문]

김대순, 『국제법론』 제21판. 서울, 삼영사, 2021.

정인섭, 『신국제법강의』 제12판. 서울, 박영사, 2021.

정인섭, 이재민, 정서용, 『신국제법판례 120선』, 서울, 박영사, 2020.

Michael N. Schmitt et al., 『탈린매뉴얼 2.0: 사이버 작업에 적용되는 국제법』, 국가보안기술연구소 편역, 박영사, 2018.

[영문]

Antonio Cassese, International Law, (New York: Oxford University Press, 2011).

David Betz and Tim Stevens, Cyberspace and the State: Toward a Strategy for Cyber-power (London: Routledge, 2011).

Francois Delerus, Cyber Operations and International Law, (Cambridge University Press, 2020).

Ian Brownlie, Principle of Public international law, (New York: Oxford University press, 2008).

James Crawford & Simon Olleson, The Nature and Forms of International Responsibility, in Malcolm D. Evans(ed). (Oxford University Press, 2003).

Joanna Kulesza, Due Diligence in International Law, (Boston: Brill, 2016).

Lan Brownlie, Principle of Public international law, (New York: Oxford University press, 2008).

Macro Roscini, Cyber Operation and the Use of Force in International Law, (UK: Oxford University Press, 2014).

Michael N. Schmitt, The Tallinn Manual on the International Law applicable to Cyber Warfare, NATO Cooperative Cyber Defence Centre of Excellence, (Cambridge University Press, 2013).

NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd Edition (Cambridge University Press, 2017).

Pierre-Marie Depuy & Viñuales Jorge E, International Environmental Law, (Cambridge University Press, 2018).

Richard A. Clarke & Robert K. Knake, Cyber War – The next threat to National Security and what to do about it, (HarperCollins Publishers, 2010).

Yariskav Radziwill, Cyber-Attacks and the Exploitable Imperfections of International Law, (The Netherlands Brill Nijhoff, 2015).

■ 학술논문

[국문]

김보연, "국제투자협정상 완전한 보호와 안전 의무의 해석기준 – 상당한 주의 기준의 비판적 고찰 –", 『국제거래법학회』, 제31권 제1호 (2022).

김보연, "인공지능의 국제법상 책임추궁에 관한 소고", 『경희법학』, 제57권 제4호 (2022).

김상걸, "입법적 국제관습법과 법적확신 개념의 재구성", 『국제법학회논총』, 제65권 제1호 (2020).

김석현, "트레일 제련소 사건 연구", 『법학논총』, 제22권 (1996).

김성원, "국제법상 사이버 간첩활동에 관한 일고찰", 『법학논총』, 제33권 제3호 (2021).

김성주, "주권 개념의 역사적 변천과 국제사회로의 투영", 『정치외교사논총』, 제27권 제2호 (2006).

김소정·박상돈, "국제협력을 통한 사이버안보 강화방안 연구", 『융합보안논문지』, 제13권 제6호 (2013).

김소정·김규동, "UN 사이버안보 정부전문가그룹 논의의 국가안보 정책상 함의", 『정치정보연구』, 제20권 제2호 (2017).

김한택, "국제법상 우주폐기물감축 연성법의 역할에 관한 연구", 『한국항공우주정책법학회지』, 제30권 제2호 (2015)

김효권, "국가가 연루된 비국가행위자의 사이버 공격에 대한 국가책임 귀속성", 『저스티스』, 통권 제193호 (2022).

박기갑, "사이버 전쟁 내지 사이버 공격과 국제법", 『국제법평론』, 통권 제32호 (2010).

박노형, "사이버안전 관련 국제규범의 정립을 위한 연구", 『안암법학』, 제37호 (2012)

박노형·김효권, "국제사이버법상 상당한 주의 의무에 관한 국가실행", 『국제법학회논총』, 제 66권 제4호 (2021).

박노형·박주희, "제6차 UNGGE 보고서 채택과 국제사이버법의 발전", 『국제법학회논총』, 제66권 제3호 (2021).

박노형·정명현, “사이버전의 국제법적 분석을 위한 기본개념의 연구 - Tallin Manual의 논의를 중심으로 -,” 『국제법학회논총』, 제59권 제2호 (2014).

박노형·정명현, "제4차 정보안보에 관한 유엔정부전문가그룹 논의 분석과 국제사이버법의 발전 전망", 『국가전략』, 제22권 제3호 (2016).

박병도, "국제환경협약의 이행 및 준수 메커니즘 – 비준수 절차를 중심으로 –", 『환경법연구』, 제36권 제3호 (2014).

박병도, "신기후체제의 국제법적 쟁점", 『국제법학회논총』, 제62권 제1호 (2017).

박재성, "사이버범죄 국제조약의 동향 – 부다페스트 협약 제2추가의정서 및 유엔 사이버범죄 조약을 중심으로 – ", 『저스티스』, 통권 제185호 (2021).

박휘락, “사이버 공간 작전의 등장과 한국의 과제”, 『신아세아』, 제18권 제4호 (2011).

배덕현, "사이버공간의 정의와 특징", 『문화역사지리』, 제27권 (2015).

백상미, "사이버공격 억지를 위한 적극적 방어개념의 국제법적 적법성", 『국제법학회논총』, 제63권 제2호 (2017).

서동주, "한국정치학에서 '사이버 공간·안보 연구동향과 정책적 함의", 『국가전략』, 제14권 제2호 (2008).

소병천, "국제법상 주권담론에 대한 소고", 『국제법학회논총』, 제58권 제4호 (2013).

소병천, "국제환경법의 예방원칙과 상당한 주의 - 초국경 환경영향평가를 중심으로 -", 『국제법학회논총』, 제66권 제4호 (2021).

송재익, "한국군 합동 사이버작전 강화방안 연구 - 합동작전과 연계를 중심으로 - "", 『한국군사』, 제2호 (2017).

신경수, 신진, "국제사회와 사이버 공간의 안보문제", 『국제지역연구』, 제27권 제3호 (2018).

신소현, "국제인도법상 무력충돌의 분류를 위한 사이버 공격의 귀속 연구", 『법학논총』, 제37권 제2호 (2020).

이기범, "국제법상 초국경적 환경영향평가에 관한 소고", 『국제법학회논총』, 제64권 제1호 (2019), p. 183.

이민효, "사이버전에 적용될 국제법에 관한 Tallinn Manual 고찰", 『인도법논총』, 제37호 (2017).

이일호, "국제환경법 이행체제의 개선방안에 관한 제안 - 기후체제에서의 이행문제와 그 대안을 중심으로 - ", 『국제법평론』, 통권 제47호 (2017).

이종현, "사이버 영역에서의 국제법상 상당주의 원칙의 적용에 관한 고찰", 『국제법평론』, 통권 제49호 (2018).

이종현, "제3국이 연관된 사이버 조작에 관한 국제법적 검토", 고려대학교 박사학위논문 (2017.06).

임예준, "국가책임조항의 규범적 지위에 관한 소고(小考)", 『국제법학회논총』, 제65권 제3호 (2020).

오병선, "국가책임의 본질과 성립요건에 대한 비판적 고찰", 『국제법학회논총』, 제52권 제2호 (2007).

오시진, "국제테러와 국가책임법", 『강원법학』, 제37권 (2012).

유인태, "경쟁적 사이버 안보 다자주의의 출현: 2004년 유엔 정부전문가 그룹부터 2021년 개방적 작업반까지의 분석", 『국제정치논총』, 제62집 제1호 (2022).

유준구, "사이버안보 문제와 국제법의 적용", 『국제법학회논총』, 제60권 제3호 (2015).

윤태영·우정민, "북한의 대남 사이버공격 양상과 행태: 사이버파워와 강압이론을 통한 분석", 『융합안보논문지』, 제18권 제1호 (2018).

장노순, "사이버안보와 국제규범의 발전: 정부전문가그룹(GGE)의 활동을 중심으로", 『정치정보연구』, 제19권 제1호 (2016)

장신, "사이버 공격과 Jus in bello", 『국제법학회논총』, 제60권 제4호 (2015).

장규현·임종현, "국제 사이버보안 협력 현황과 함의: 국제안보와 UN GGE 권고안을 중심으로.", 『정보통신정책연구』, 제26권 제5호 (2014).

정경수, "국제법상 연성법의 재인식", 『안암법학』, 제34호 (2011).

정인섭, "왜 비국가 행위자를 말하는가?", 『서울국제법연구』, 제17권 제2호 (2010).

최난설헌, "연성규범의 기능과 법적효력 -EU경쟁법상 논의를 중심으로-", 『법학연구』, 제16집 제2호 (2013).

최영진, "국제환경법상 사전주의원칙의 법적 지위에 관한 연구", 『경희법학』, 제51권 제1호, p. 161.

하대청, “사전 주의의 원칙은 비과학적인가?: 위험 분석과의 논쟁을 통해 본 사전주의 원칙의 ‘합리성’”, 『과학기술연구』, 제10권 제1호 (2010).

한삼인·강홍균, "초국경 환경피해와 국가책임", 『환경법연구』, 제31권 제2호 (2009).

황지환, "북한의 사이버 안보 전략과 한반도 : 비대칭적, 비전통적 갈등의 확산", 『동서연구』, 제29권 제1호 (2017).

[영문]

Abhijeet Shrivastava & Rudraksh Lakra, "Revisiting due diligence in cyberspace: crafting international law's arsenal against transboundary Botnets", International Journal of Law and Information Technology, Vol. 30, Issue 3 (2022).

Antonio Cardesa-Salzmann, "Constitutionalizing Secondary Rules in Global Environmental Regimes: Non-Compliance Procedures and the Enforcement of Multilateral Environmental Agreements", Journal of Environmental Law, Vol. 24, No. 1 (2011).

Antonio Coco, "'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law", The European Journal of International Law, Vol. 33, No. 3 (2021).

Antonio Coco & Talita Dias, "Cyber Due diligence in international law", European Journal of International Law, Vol. 32, Issue 3 (2021).

Antonio Coco & Talita Dias & Tsvetelina van Benthem, "Illegal: The Solarwinds Hack under International Law", The European Journal of International Law, Vol. 33, No. 4 (2022)

Catherine Lotrionte, "Reconsidering the consequences for state-sponsored hostile Cyber Operation under International Law", The Cyber Defense Review, Vol. 3, No. 2 (2018).

Christian Czosseck, Gabriel Klein & Felix Leder, "On the Arms Race Around Botnets-Setting Up and Taking Down Botnets", International Conference on Cyber Conflict (2011).

C. M. Chinkin, "The challenge of soft law: Development and Chang e in International Law", The international and comparative law, Vol. 38, No. 4 (1989).

Colin Patrick, "Debugging the Tallinn Manual 2.0's Application of t he Due diligence principle to cyber operation", Washington International Law Journal, Vol. 28, No. 2 (2019).

Daniel Philpott, "Westphalia, Authority and International Society", P olitical Studies (1999).

David D. Caron, “The ILC Articles on State Responsibility: The Par adoxical Relationship Between Form and Authority”, Ameri can Journal of International Law, Vol. 96, No. 4 (2002).

Dennis Broeders et al., "Revisiting past cyber operations in light of new cyber norms and interpretations of international law: i nching towards lines in the sand", Journal of Cyber Policy, Vol. 7, No. 1 (2022).

Eric Talbot Jensen, "Computer Attacks on Critical National Infrastru cture: A Use of Force Invoking the Right of Self-Defence", Stanford Journal of International Law, 38:207 (2002).

Eric Talbot Jensen, "The Tallin Manual 2.0: Highlights and Insights", Georgetown Journal of International Law 735, Vol. 48 (201 7).

Eric Talbot Jensen, "State Obligations in Cyber Operations", Baltic Yearbook of International Law of International Law, Vol. 7 1 (2015).

Francesca Romanin Jacur et al., "Triggering Non-Compliance Proce dure"

Francis Snyder, "Soft Law and Institutional Practice in the Europea n Community", The Construction of Europe (1994).

Gadi Evron, "Battling Botnets and Online Mobs – Estonia's Defense Efforts during the Internet War", Georgetown Journal of International Affairs (2018).

Harold Hongju Koh, "International Law in Cyberspace", Harvard International Law Journal, Vol. 54 (2012).

Hyeong-wook Boo, "An assessment of North Korean Cyber Threats", The Journal of East Asian Affairs, Vol. 31, No. 1 (2017).

Ian Yuying Liu, "The due diligence doctrine under Tallinn Manual 2.0", The International Journal of Technology Law and Practice (2017).

Jan Martin Lemnitzer, "Back to the Roots: The Laws of Neutrality and the Future of Due Diligence in Cyberspace", The European Journal of International Law, Vol. 33, No.3 (2022).

Jawwad A. Shamsi et al., "Attribution in cyberspace: techniques and legal implications", Security and communication networks (2016).

Jeffrey T. G. Kelsey, "Hacking into International Humanitarian Law: The Principle of Distinction and Neutrality in the Age of Cyber Warfare", The Michigan Law Review, Vol. 106, No. 7 (2008).

Joanna Kulesza, "Due Diligence in international law", Journal of Internet Law (2014).

Johann-Christoph Woltag, "Cyber Warfare", Max Plank Encyclopedia of public International Law, (Oxford Public International Law, 2015).

Jon Lindsay, "China and Cybersecurity: Political, Economic and Strategic Dimensions", Report from workshops held at the University of California, San Diego (2012).

Julie J.C.H, Daniel J. Ryan & Eneken Tikk, "Cybersecurity regulation: Using analogies to develop frameworks for regulation", International Cyber Security: Legal & Policy Proceedings (2011).

MA Fitzmaurice & C Redgwell, "Environmental Non-Compliance Procedures and International Law", Netherlands Yearbooks of International Law, Vol. 31 (2009).

Melvin Aron Eisenberg, " The Architecture of American Corporate Law: Facilitation and Regulation", Berkeley Business Law Journal, Vol. 2 (2005).

Medes Malaihollo, "Due Diligence in International Environmental Law and International Human Rights Law: A Comparative Legal Study of the Nationally Determined Contributions under the Paris Agreement and Positive Obligations under the European Convention on Human Rights", Netherlands International Law Review, Vol. 68 (2021).

Melvin A. Eisenberg, “The Architecture of American Corporate Law: Facilitation and Regulation”, Berkeley Business Law Journal, Vol. 2 (2005).

Michael N. Schmitt, "In Defense of Due Diligence in cyberspace", 125 The Yale Law Journal Forum, Vol. 68 (2015).

Neil McDonald, "The role of Due Diligence in International Law", International & Comparative Law Quarterly, Vol. 68, No. 4 (2019).

Nico Schrijver, The changing nature of State Sovereignty, British Yearbooks of International Law, Vol. 70, Issue 1 (1999).

Nicolò Bussolati, "The rise of Non-State Actors in Cyberwarfare", Cyber War: Law and Ethics for Virtual Conflicts, Oxford University Press (2015).

Nils Goeteyn & Frank Maes, "Compliance Mechanisms in Multilateral Environmental Agreements: An Environmental Agreements: An Effective Way to Improve Compliance?", Chinese Journal of International Law, Vol. 10, No. 4 (2023).

Oona A. Hathaway & Crootof Rebecca, "The Law of Cyber-attack", California Law Review, Vol. 100 (2012).

Rahul Prakash & Darshana M. Baruah, "The UN and Cyberspace Governance", ORF Issue Brief. No. 68 (2014).

Robert Kolb, "Reflection on due diligence duties and cyberspace", German Yearbook of International Law, Vol. 58 (2015).

Roy Schöndorf, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations", Stockton Center for International Law Studies, Vol. 97 (2021).

Russell Buchan, Macro Roscini & Nicholas Tsagourias, "State Responsibility for Cyber Operations: International Law Issue", British Institute of International and Comparative Law (2014).

Russell Buchan & Nicholas Tsagourias, " Special Issue: Non-State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence", Journal of Conflict & Security Law, Vol. 21, No. 3 (2016).

Ryan Hagemann, Jennifer Huddleston Skees & Adam Thierer, "Soft Law for Har Problems: The governance of emerging technologies in an uncertain future", Colorado Technology Law Journal, Vol 17, No. 1 (2018).

Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," Berkeley Journal of International Law, Vol. 27, No. 1 (2009).

Scott J. Shackelford, "State responsibility for cyber attacks: Competing standards for a growing problem", CCECOE Publications (2010).

Scott J. Shackelford, Scott Russell & Andreas Kuchen, "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors", Chicago Journal of International Law, (2016).

Stephen Herzog, "Revisiting the Estonian Cyber Attack: Digital Threats and Multinational Responses", Journal of Strategic Security, Vol 4, No. 2 (2011).

Timo Koivurova, "Due Diligence", Max Plank Encyclopedia of Public International Law [MPEPIL] (2013).

Tom Bingham, "The Alabama Claims Arbitration", Cambridge University Press, Vol. 54, No. 1 (2005).

Tomohiro Mikanagi, "Application of the Due Diligence Principle to Cyber Operations", 97 International Law Studies, Vol. 97 (2021).

Tseming Yang, "International Treaty Enforcement as a Public Good: Institutional Deterrent Sanctions in International Environmental Agreements", Michigan Journal of International Law, Vol.27 (2006).

Yochong Li & Qinghui Liu, "A Comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments", Energy Report, Vol. 7 (2021)

■ 판례

Alabama Claims (US v. Great Britain), Reports International Arbitral Award 1871.

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p. 43.

Corfu Channel case, Judgment of April 9th, 1949, I.C.J. Reports 1949, p.4.

Fisheries case, Judgement of December 18th, I.C.J. Reports 1951, p. 116.

Island of Palmas case (the Netherlands, USA), 4 April 1928, R.I.A.A. vol. II. pp. 829- 871.

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p.226.

Military and Paramilitary Activities in und against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986.

Prosecutor v. Dusko Tadić (IT-94-1), ICTY, Appeals Chamber, Judgement of 15 July, 1999.

Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, I.C.J. Reports 2010, p. 14.

Responsibilities and obligations of States with respect to activities in the Area, Advisory Opinion, 1 February 2011, ITLOS Reports 2011, p.10.

Trail Smelter Arbitration. USA & Canada, 3 RIAA 1905(1941).

United States Diplomatic and Consular Staff in Tehran, Judgement, I.C.J. Reports 1980, p.3.

■ 국제문서

Council of Europe (COE), Convention on Cybercrime, European Treaty Series, No. 185, 2001.

International Law Association, “ILA Study Group on Due Diligence in International Law”, Second Report (2016).

ILC, "State Responsibility – Second report by F. V. Garcia Amador, Special Rapporteur", UN Doc. A/CN.4/106 (1957)

ILC, Report of the International Law Commission on the work of its fifty-third session, 23 April - 1 June and 2 July - 10 August 2001, Official Records of the General Assembly, Fifty-sixth session, Supplement No.10, A/56/10 (2001).

James E. Cartwright General, Memorandum for Chiefs of the Military Services Commanders of the Combatant commands Directors of the Joint Staff Directorates, Joint Terminology for Cyberspace Operations, Washington, D.C. 201318-9999.

UN, Report of the International Law Commission on the work of its forty-sixth session, 2 May-22 July 1994, UN Doc. A/49/10.

UNGA, Advancing responsible State behaviour in cyberspace in the context of international security, UN Doc. A/RES/73/266 (2019).

UNGA, Resolution on "Developments in the Field of Information and Telecommunications in the Context of International Security", UN Doc. A/RES/53/70 (1999).

UNGA, Advancing responsible State behavior in cyberspace in the context of international security, UN Doc. A/RES/73/266 (2019).

UNGA, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98/AR (2013).

UNGA, Group of Governmental Experts on Development in the Field of Information and Telecommunication in the context of International Security, UN Doc. A/70/174, (2015).

UNGA, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/76/135 (2021).

UNGA, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, UN Doc. A/76/136 (2021).

UNGA, Resolution on “Developments in the field of information and telecommunications in the context of international security”, UN Doc. A/RES/70/237 (2015).

White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, (2011).

■ 기타 자료

[국문]

김소정, "미국의 사이버공격 대응정책과 한국에의 시사점 : 솔라윈즈 해킹 대응사례를 중심으로 ", 국가안보전략연구원 연구보고서 (2022).

박주희, "UNGGE의 자발적 규범과 국내 사이버안보 법제", 한국법제연구원 Global Legal Brief, Vol. 1 (2022).

송태은, "최근 사이버 위협의 추세와 향후 전망 및 국제사회의 대응", 외교안보연구소 주요국제문제분석 (2023).

양정윤, "상하이협력기구의 사이버 안보 논의: 러시아와 중국의 역할", 국제문제연구소 워킹페이퍼, No. 103 (2019).

이승열, "북한 사이버 공격의 현황과 쟁점", 국회입법조사처, 제2034호 (2022).

채재병, "사이버 안보의 국제정치적 추세와 한국의 전략구상", 국가안보전략연구원, 연구보고서 2021-18, (2021).

[영문]

Abhijeet Shrivastava & Rudraksh Lakra, "Unpacking Cyber Due Diligence Practice: Detection, Mitigation, and Prevention", Opinio Juries (2020) (마지막 방문: 2023.7.27)

Andraz Kastelic, "Due Diligence in the cyber space", United Nations Institute for Disarmament Research (2021). (마지막 방문: 2023.7.27)

Brooks Barnes & Nicole Perlroth, "Sony Pictures and F.B.I Widen Hack Inquiry", The New York Times, (Dec. 3, 2014), available at https://www.nytimes.com/2014/12/04/business/sony-pictures-and-fbi-investigating-attack-by-hackers.html (마지막 방문: 2023.7.27)

Daniel Schearf, "North Korea's 'World Class' Cyber Attacks coming from China", VOA, (Nov. 21, 2013), available at https://www.voanews.com/a/north-koreas-world-class-cyber-attacks-coming-from-china/1795349.html. (마지막 방문: 2023.7.27)

Department of Defense, "Department of Defense Strategy for Operating in Cyberspace", Washington D.C, DoD (2011), available at https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (마지막 방문: 2023.7.27)

Eneken Tikk-Ring, "Developments in the field of information and telecommunication in the context of international security: work of the un first committee 1998-2012", ICT peace Foundation (2012).

European Council, "Declaration by the High Representative Josep Borrell, on Behalf of the European Union, On Malicious Cyber Activities Exploiting the Coronavirus Pandemic", EU Press Release (May 1, 2020). (마지막 방문: 2023.7.27)

International Law Association (ILA), "ILA Study Group on Due Diligence in International Law", First Report (2014).

James Pamment et al., "Hybrid Threats: 2007 cyber-attacks on Estonia", NATO Strategic Communications Centre of Excellence (2019). (마지막 방문: 2023.7.27)

Josh Wingrove & Jennifer Epstein, "Biden says Russia has "Some Responsibility" in Colonial Attack", Bloomberg, (May 11, 2021), available at https://www.bloomberg.com/news/articles/2021-05-10/colonial-pipeline-is-undamaged-white-house-official-says?leadSource=uverify%20wall. (마지막 방문: 2023.7.27)

Joyce Hakmeh & Kerstin Vignard, "ICTs, International Security, and Cybercrime: Understanding their Intersections for Better Policy-making", UNIDIR (2021),

Michael Schmitt & Liis Vihl, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms", Just Security (30 June 2017).

Pierluigi Paganini, "Non-State Actors in cyberspace: an attempt to a taxonomic classification, role, impact and relations with a sate's socio-economic structures", 2022 Commentary, Universita Degli Studi Firenze (2022). (마지막 방문: 2023.7.27)

Sarah Morrison, "How a major oil pipeline got held for ransom", Vox, (Jun 8, 2021), available at https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices. (마지막 방문: 2023.7.27)

Sico van der Meer, "How States could respond to non-state cyber-attackers", Policy Brief, Netherlands Institute of International Relations (2020). (마지막 방문: 2023.7.27)

Tae Eun Song, "DPRK's Illicit Cyber Activities: Latest Development and ROK's Responses", IFANS FOCUS, 2022-28E (2022). (마지막 방문: 2023.7.27)

Una Aleksandra at el., "Hybrid Threats: A Strategic Communications Perspective", NATO Strategic Communications Centre of Excellence, (2019). (마지막 방문: 2023.7.27)

UNIBO, International law and Cyberspace, Ministry of Foreign Affairs and International Cooperation (2021). (마지막 방문: 2023.7.27)

White House Government, "Remarks by President Biden on the Colonial Pipeline Incident", (May 13,2021), available at https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/ (마지막 방문: 2023.7.27)

Abstract

Applicability of 'Due Diligence' in Cyberspace

Kim, Sohee
International Law
School of Law
Seoul National University

The purpose of this study is to find ways to function more efficiently in cyberspace by examining the applicability of due diligence under international law in cyberspace and legal issues in application.

Cyber-attacks that occur through cyberspace today are characterized by a high degree of anonymity and asymmetry. In addition, non-state actors and states are linked in various ways in the process of conducting attacks. The problems caused by this nature of cyber-attacks to the international community are summarized in the following two ways. First, due to the technical nature of cyber-attacks, it is difficult to attribute responsibility to the malicious cyber actors and as a result, it is not easy to apply the National Liability Act. Second, due to the complex nature of cyber-attacks, the role of transit states related to attacks is gradually expanding, but international legal norms to regulate the actions of transit countries are insufficient. This study proposes the application of due diligence under international law to cyberspace as an alternative to these problems derived from cyber-attacks. Due

diligence is a norm that requires the prevention of transboundary damage within its jurisdiction, which could provide a possible direction for solving problems caused by cyber-attacks.

This study reviews the applicability of due diligence in cyberspace and its legal issues, limitations, and implications after an overall overview of obligation, which is a norm used in various areas of international law. Apart from the international community's positive perception of applying due diligence to cyberspace, there are still legal issues that require further discussion in order for obligation to be applied to cyberspace and function efficiently. It is believed that obligation can function more efficiently in cyberspace through discussions on securing the normative value, agreement on specific application standards of due diligence, and ways to secure the execution power of due diligence. This study has some limitations, including the essential dilemmas and technical difficulties of due diligence. However, this study, which reviews the role of due diligence in cyberspace, has notable implications for cybersecurity in South Korea, a divided country, in the face of increasing threats using cyber-attacks. In addition, this study is beneficial because it is aligned with the overall flow of discussions in the international community that properly regulates cyberspace, a newly emerging area, and also is striving to efficiently cope with cyber-attacks.

Keyword: Cyber-attack, Cybersecurity, Due diligence, Asymmetry Anonymity, Transit state, Jurisdiction, Non-State actor

Student Number: 2021-25948