국제·지역연구 27권 3호 2018 가을 pp. 27-55

# 국제사회와 사이버 공간의 안보문제*

신경수** | 경찰대학 치안정책연구소
신　　진 | 충남대학교 정치외교학과

사이버 공간의 등장으로 기술적 번영과 안녕을 추구하던 국제사회는 이제 불가피한 역설에 직면하고 있다. 이른바 초연결성·초지능성 사회로 진입한 국제사회는 이미 악성코드로 무장한 사이버 공격에 직접적으로 노출되어 있으며, 이는 이전에는 경험하지 못한 새로운 형태의 안보문제로부터 국제사회가 위협받고 있다는 것을 의미한다. 그러나 이러한 사이버 공간의 안보문제에 대해 국제사회는 여전히 직접적인 대응방안을 제시하지 못하고 있다. 물론 사이버 세계의 위협행위가 개별국가의 안보를 위협하고 있다는 사실과 이러한 위협이 국제사회의 집단안보의 영역에까지 영향을 미칠 수 있다는 점에서는 인식을 하고 있는 것으로 보이나 아직까지 사이버 안보에 대한 국제규범을 비롯한 전략 및 지침 등에 있어서는 일치된 합의점을 찾지 못하고 있다. 특히 사이버 공간에 적용되는 규범을 구축하고자 하는 미국 중심의 서방진영과 중국·러시아 중심의 진영의 이분법적 사고의 차이로 인해 여전히 정치적 · 외교적으로 공감대를 형성하지는 못하고 있고, 양 진영의 논쟁 공방이 사이버 공간에 대한 안보문제 해결에 있어 기존 국제법 체제의 적용문제와 개별국가의 주권적 개념의 인정에 있는 만큼, 대표주자인 미국과 중국·러시아와의 상호간 연결밀도의 희석이 이루어지지 않고서는 구조적 양분화 과정은 더욱 가열될 것이다. 그리고 이러한 분절성은 점점 더 다층적이고 변화무쌍하게 진화하고 있는 사이버 위협에 직면한 우리의 입장에서도 상당히 불리한 방향으로 작용할 수 있다. 이에 본 연구에서는 사이버 안보에 대한 국제사회의 분절된 시각을 이해하고, 우리에게 필요한 독자적이고 실용적인 대응방안을 모색하고자 사이버 협력체계의 확장, 그리고 적극적 사이버 방어체계의 확립을 제시하고자 한다.

**주제어: 사이버 공간, 사이버 안보, 탈린매뉴얼, 상하이협력기구(SCO)**

* 이 논문은 제1저자의 박사학위 논문인 “북한의 사이버 위협과 대응전략에 관한 연구”의 일부분을 수정, 발전시켜 작성된 연구임을 밝힙니다. 또한, 소중한 논평을 해주신 익명의 심사위원 세 분에게 감사의 인사를 전합니다.

** 제1저자

# I. 서론

사이버 공간의 등장으로 기술적 번영과 안녕을 추구하던 국제사회는 이제 불가피한 역설(逆說)에 직면하고 있다. 이른바 초연결성·초지능성 사회로 진입한 국제사회가 악성코드로 무장한 사이버 공격에 직접적으로 노출되면서, 이전에는 경험하지 못한 새로운 형태의 안보문제가 국제관계의 갈등과 분쟁을 야기하는 위협요인이 되고 있는 것이다.

최근 세계경제포럼(WEF)은 「2018 글로벌 위험 보고서(Global Risks Report 2018)」를 통해 국제사회가 당면하고 있는 주요 위험으로 사이버 공격을 제시하였는데, 이는 특정 국가에 의해 의도된 이른바 '국가지원 해커'를 통한 공격뿐만 아니라, 비(非)국가행위자인 개인 및 소수 집단에 의해서도 사회 전 영역에 심각한 안보위기 상황을 초래할 수 있기 때문이다.

실제로 사이버 위협은 공격의 주체를 감출 수 있는 '익명성'과 함께 시간적·공간적 제약을 초월한 '비동시적 동시성'을 가진 공격을 감행할 수 있는 특징(Garrie et al., 2012)을 가지고 있어, 국가라는 본질적 요소를 바탕으로 설립된 유엔(UN)체제가 추구하는 베스트팔렌식 국제질서 체계를 붕괴시킬 수 있는 비대칭 구조로 새로운 전장(戰場)을 개방(O'Flaherty, 2018)해주는 우회공격 루트로 사용될 수 있다.

그러나 이러한 사이버 공간의 안보문제에 대해 국제사회는 여전히 직접적인 대응방안을 제시하지 못하고 있다. 물론 사이버 세계의 위협행위가 개별국가의 안보를 위협하고 있다는 사실과 이러한 위협이 국제사회의 집단안보의 영역에까지 영향을 미칠 수 있다는 점에서는 공통된 인식을 하고 있는 것으로 보이나, 아직까지 국제사회는 사이버 안보에 대해 일치된 국제규범은 물론 전략 및 지침 등에 있어서도 합의점을 찾지 못하고 있는 실정이다.

이렇게 국제안보를 해석하는 새로운 동적 변수로 작용하고 있는 사이버 공간에서도 국제사회는 여전히 통합된 사고체계를 갖추지 못하고, 각국의 대립적인 목표들을 강조하며 사이버 공간의 역동성을 자국의 체제내로 이끌기

위해 각축을 벌이고 있다. 그 대표적인 양립관계가 바로 사이버 공간을 '공간' 그 자체로의 영역으로 두면서 기존의 국제법 체제를 적용한 방식으로 접근하려는 미국 중심의 서방진영과 이를 더 작은 규모로 분리하여 통제 가능한 방식으로 접근하려는 중국·러시아 중심의 진영의 이질화된 시각으로 볼 수 있다(Roscini, 2014).

우선 미국 중심의 서방진영의 입장은 원칙적으로 사이버 공간에 대한 보편적 권리와 자유를 강조하며 인터넷이라는 가상공간에서 발생하는 정보 데이터의 자유로운 이동을 보장하되 사이버 위협행위에 대해서만 통제를 가함으로서 어느 국가도 사이버 공간을 소유할 수 없는 비(非)국가 영역으로 평가(Kania et al., 2015)하고 있다. 따라서 사이버 공간을 통제할 수 있는 새로운 질서체계는 불필요하며, 기존의 국제법 체제를 그대로 적용해 사이버 공간에서 발생하는 안보문제를 해결하면 된다는 입장이다.

이와 반대로 중국·러시아 중심의 입장은 사이버 공간을 국가가 가지는 영토의 일부로 인식하면서, 사이버 위협에 대한 별도의 질서체계를 구축해 통제권을 행사해야 한다는 입장을 가지고 있다. 이는 기존의 국제질서를 통제하고 있던 국제법과는 다른 별도의 '사이버 국제법'을 제정하거나 자국의 법체계에 따라 사이버 공간을 관리해야 한다고 주장으로 실제로 중국의 영향력이 많이 미치고 있는 상하이협력기구(SCO)는 2009년 회원국 간 정보안보(Information Security)에 대한 협정을 체결하면서, 사이버 공간에 대한 개별국가의 주권(主權)을 명시하였다. 이는 데이터 이동의 자유로운 개방성보다는 국가에 의한 통제된 질서체계를 우선적으로 확보할 것을 공식화한 것으로 볼 수 있다.

이에 본 연구에서는 국제사회가 여전히 정치적·경제적 이익과 사회적 가치 그리고 이질적인 문화를 가진 역사적 경험과 이데올로기(Ideologie) 등 복잡하고도 오랜 가치관의 차이로 인해 분절된 사이버 안보문제의 양 진영의 시각을 이해하고, 이를 바탕으로 사이버 안보에 대해 우리에게 필요한 실용적인 대응방안이 무엇인지 제시하고자 한다.

본 논문은 서론을 포함하여 총 5장으로 구성된다. 우선 II장에서는 사이버 공간이라는 새로운 영역에서 발생하고 있는 국제사회의 안보위협을 검토해

보고, III장에서는 미국 중심의 서방진영과 중국·러시아 중심의 진영으로 대변되는 양 진영 간 사이버 안보논의와 대립관계에 대해 논의해 본다. 이어 IV장에서는 국제사회의 사이버 안보논의에 따른 우리의 대응방안을 모색해 보고, 끝으로 V장에서 분석 내용을 요약하고 본 연구의 함의를 제시하고자 한다.

## II. 사이버 공간의 안보확장성

지난 1999년 신(新)유고연방으로부터 분리·독립을 원하는 알바니아계(Albania) 주민과 이를 반대하는 세르비아계(Serbian) 정부군 사이에서 벌어진 유혈 충돌사태인 일명 '코소보(Kosovo) 사태'를 국제사회에서 발생한 최초의 사이버 공격으로 보는 견해(김인중, 2013)가 있다. 비록 북대서양조약기구(이하, NATO)의 군사령부 홈페이지를 변조하는 정도의 낮은 수준의 기술이었지만, 이전의 군사적 전술에서는 생각하지 못했던 새로운 형태의 네트워크 공격이 발생했다는 점에서 그 의의가 있다. 이후 2005년 중국의 인민해방군(PLA)으로 추정되는 해커집단인 일명 '타이탄 레인(Titan Rain)'이 감행한 사이버 공격에 의해 미(美) 정부기관과 군산 복합체(Military-Industrial Complex)의 네트워크가 마비되는 사례(UPI, 2005/11/25)가 발생하였으며, 2007년에는 사이버 전쟁(Cyber Warfare)이라는 용어의 시초라고 할 수 있는 디도스(DDoS) 유형의 대규모 해킹 공격이 발트 3국 중 하나인 에스토니아(Estonia)에서 발생하였다.

특히, 당시 동(東)유럽 최대 규모의 IT 강국이었던 에스토니아는 수도(首都) 탈린(Tallinn)에 있던 제2차 세계대전 참전기념 구(舊) 소련 군인동상을 외곽으로 이전하는 문제로 러시아와 외교적 마찰을 빚었는데, 이것이 분쟁으로 비화(飛火)되면서 약 3주 이상 대통령궁을 비롯한 의회, 공공 및 금융기관 등 국가 전역의 모든 전산망이 일제히 파괴당하는 사이버 공격을 받았다. 이는 이전까지 발생하였던 소규모 형태의 사이버 공격과 달리 네트워크 시스

템으로 연결된 국가 전체의 영역에 물리적 피해를 가하는 전면전 양상을 띠었다는 점에서 국제사회로부터 군사적 행동(Military Action)으로 간주(Antonenko and Giegerich, 2009)되었고, 이때부터 국제사회는 공식적으로 사이버 공격이 군사 교리(Military Doctrine)의 범주에 포함됨은 물론 국가안보를 침해하는 심각한 위협요인이 된다는 점을 인식(Cardash et al., 2013)하는 계기가 되었다.

이어 2008년 러시아는 분쟁 중이던 조지아(Georgia)를 향해 재래식 공격과 함께 사이버 공격을 동시에 병행하는 해킹 전격전을 감행하였고, 2009년에는 키르기스스탄(Kyrgyzstan) 정부와 그곳에서 주둔하고 있던 미군 기지를 상대로 e-메일 접속 차단 등의 네트워크 차단을 통한 공격을 자행(Clarke and Knake, 2010)하였다. 이러한 러시아의 계속된 사이버 공격의 위험성에 대해 당시 UN 국제전기연합(ITU)의 의장이었던 Hamadoun Toure(2009)는 "만일, 제3차 세계대전이 발생한다면 그것은 사이버戰이 될 것이며, 어떤 국가도 성역으로 남을 수 없을 것이다"라는 성명을 발표[1]하며 국제사회로부터 사이버 공간에서 발생하는 무력 행위에 대한 지정학적 자위권 행사에 대한 명확한 규정의 필요성을 다시금 강조하였으며, 영국의 국제전략연구소(IISS)는 군사균형(Military Balance)지를 통해 미래 "사이버 전쟁은 국가기관 전산망을 마비시키고, 군사정보통신망에 침투하여 군사작전을 혼란케 하여 핵공포와 비슷한 수준의 전쟁양상이 될 것"이라고 기술(임종인, 2014)하였다.

2010년 국제사회는 이란(Iran)의 나탄즈(Natanz) 지역에 있던 우라늄 농축시설의 원심분리기 제어시스템을 파괴한 이른바 스턱스넷(Stuxnet) 공격을 목도하면서 커다란 충격을 받았다. 미국과 이스라엘에 의해 개발된 것으로 추정되는 스턱스넷 공격은 오로지 컴퓨터 네트워크를 파괴하는 것만을 목적으로 제작되었으며, 시스템 사용자의 인지 여부와 관계없이 공격자가 원격으로 악성코드를 실행할 수 있게 설계됨은 물론 특정 프로그램만을 대상으로 정확하게 공격명령을 지정할 수 있다는 기술적 특징을 가지고 있었다. 이는 사실상 악성코드가 사이버 무기화된 첫 번째 사례로, 현존하는 악성코드 가

1. Proceedings of a Workshop on Deterring Cyberattacks, National Academies Press, p. 218.

운데 가장 정교한 것으로도 평가(권진욱·박정화, 2010)받고 있다. 특히, 스턱스넷에 의해 공격당한 이란의 부셰르 원전은 외부와의 네트워크가 철저히 차단된 '폐쇄망' 형태로 운영되었음에도 파괴당했다는 점에서 국제사회에 경각심을 불러일으켰다.

이후에도 2014년 미국의 엔터테인먼트 사업체인 소니 픽처스(Sony Pictures) 해킹사건, 2015년 수니파 극단주의 무장단체인 이슬람국가(ISIL)를 지지하는 테러리스트들이 IS 격퇴를 담당하는 미(美) 중부사령부(CENTCOM)의 소셜미디어(SNS) 계정을 해킹하는 사태가 발생하였고, 2016년에는 북한이 미국 연방준비은행(Federal Reserve Bank)에 보관된 방글라데시 중앙은행 계좌에서 돈을 탈취하고자 스위프트(SWIFT)를 해킹하는 사이버 금융공격까지 발생하였다. 2017년에는 전 세계 150여 국을 대상으로 악성코드를 이용해 수십만 대의 컴퓨터를 감염시켜 PC에 보관된 자료를 임의대로 암호화하고, 이에 대한 시스템 복구를 미끼로 가상화폐까지 요구하는 이른바 워너크라이(WannaCry) 랜섬웨어 공포를 심어주면서 국제사회로부터 가장 큰 논란의 중심이 되었다. 이는 사이버 안보문제가 더 이상 강대국들의 군사 전략으로만 사용되는 것이 아니라 소수의 인원이 자신의 정치적·이념적 그리고 경제적 목적을 위한 수단으로도 이용되고 있다는 것을 말해준다.

이처럼 사이버 공간에서 발전하고 있는 과학기술의 영역은 다층적이고 복합적인 국가안보 위협을 동시에 수반하고 있는 양날의 검(Double Edged Sword)이 될 수 있는 영역이자 한 국가만의 노력으로는 해결할 수 없는 안보문제가 되고 있다. 아울러 악성코드로 무장한 사이버 무기의 남용은 한 국가의 경제를 무너뜨릴 수 있는 절대적 힘(Power)을 가질 수 있고, 나아가 국제사회의 질서체계를 위협할 수 있는 새로운 형태의 강력한 전쟁 도구가 될 수 있다는 안보영역의 확장성을 보여주고 있다.

# III. 국제사회의 사이버 안보논의와 대립성

## 1. 국제사회의 사이버 안보논의: UNGGE 전개과정

1998년 러시아는 정보통신기술(ICT)을 악용한 해킹공격을 예방하고, 사이버 공간이 새로운 전장(戰場)으로 확대되는 것을 방지하자는 내용의 정보안보(Information Security) 문제를 국제사회와 논의하고자 유엔총회(General Assembly) 제1위원회에 결의안(A/RES/53/70, 4 January 1999)[2]을 제출(박노형 · 정명현, 2014)하였다. 이는 네트워크 기술을 이용한 안보위협이 곧 국가안보의 위기로 이어질 수 있다는 인식을 국제사회에 최초로 피력한 사이버 안보논의라고 할 수 있다.

2004년 유엔총회는 사이버 공간에서 발생할 수 있는 잠재적 혹은 현존하는 위협을 보다 체계적으로 연구·분석하기 위해 이른바 'UN 정부 간 전문가그룹(Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 이하 UNGGE)'을 공식적으로 출범시키면서 동시에 러시아를 의장국으로 한 제1차 회의를 2004년부터 2005년까지 진행하였다. 제1차 회의는 러시아의 의견대로 정보통신기술의 발전이 가져온 새로운 사이버 이슈에 대해 국제사회가 공동으로 대응방안을 모색해야 한다는 점과 국제사회의 안보문제를 다루는 기존의 국제법만으로는 사이버 공간에서 발생하고 있는 분쟁을 포괄적으로 적용할 수 없다는 내용을 쟁점으로 하는 초보적 수준의 논의라고 볼 수 있다. 그러나 당시 일부 국가를 제외하고는 아직까지 사이버 위협에 대한 안보체계를 확립해야한다는 필요성에 대한 인식이 상대적으로 미약(Lehto and Neittaanmäki, 2018)했을 뿐만 아니라, 사이버 안보에 대한 참여국들 간의 입장차이가 확연히 들어나면서 결국 일반적인 정보통신기술

2. 결의안 주요내용: 위험한 정보 무기의 사용과 생산, 개발을 방어하기 위한 국제법 차원의 체제를 구성할 것을 요청

의 악용에 대한 공동대응 방안의 필요성만을 강조한 채 마무리되었다.

2009년에 진행된 제2차 회의는 이미 국제사회가 에스토니아(2007)와 조지아(2009)에서 발생한 대규모 사이버 공격의 위력을 체감한 상태에서 진행되었다. 러시아로 추정되는 해커들에 의해 국가네트워크 통제시스템이 철저하게 파괴되는 것을 지켜 본 국제사회의 이러한 사이버 충격은 사이버 공간에서도 군사적 문제를 해결하기 위한 '신뢰구축 조치(Confidence-Building Measures)'의 적용이 필요하다는 인식을 공유하였으며, 사이버 위협이 자국의 안보상황에만 영향을 미치는 것이 아니라 국제평화와 세계 시민사회를 위협할 수 있는 거대한 파괴력을 가졌다는 점에 주목하였다.[3]

하지만 사이버 안보에 대한 상호신뢰구축의 필요성에 대한 의견에는 중론(衆論)을 모았으나, 중국과 러시아가 현실 세계에 존재하는 물리적 공간이라는 제한된 영역만을 염두하고 합의했던 국제법을 무한의 확대가 가능한 영역이자 국경조차 없는 사이버 공간에 적용하기에는 국제적인 기준의 모호성과 타당성의 부족 등 수많은 제약요소가 발생할 수 있음을 주장(Radziwill, 2015)하며 새로운 국제법 신설에 대한 필요성을 제기한데 대해 미국 중심의 서방진영은 사이버 공간의 문제해결은 기존의 유엔 체제에서 작용하고 있던 국제법을 그대로 적용하면 된다는 입장으로 일축함으로서 대립관계를 형성하였다.

2012년부터 2013년까지 진행된 제3차 회의는 사이버 안보에 대한 국제사회의 일치된 합의가 인터넷이라는 개방된 영역에 있어 안전하고 평화로운 접근을 보장할 수 있는 사이버 환경을 만들 수 있다는 점을 주시하여 미국 측과 중국·러시아 측으로 대표되는 양 진영의 대립구도는 어느 정도의 합의를 수용해 이전 회의들과는 다른 수준의 보고서(UN General Assembly resolution 69/243)를 발표할 수 있었다. 특히, 제3차 회의 보고서는 사이버 공간의 활동에 대해 유엔 헌장을 포함한 기존의 국제법에 따라 평화와 안전을 보장받을 수 있도록 하여 돌발적인 사이버 공격으로 인해 발생할 수 있는 막대한 안보위협 행동의 예측 가능성을 높이고자 하였다. 하지만 이와 관련

3. 평화와 번영을 위한 제주포럼 2016, "유엔 정보안보 GGE의 성과와 전망", p. 48.

하여 미국은 무력 충돌법(Law of Armed Conflict)의 개념을 사이버 공격에 포함시켜 국제법적 성격을 지니게 하자고 제시(Radziwill, 2015)하였으나, 중국·러시아 진영이 일축하면서 사이버 안보에 대한 양쪽 진영의 완전한 합의는 성사되지 못했다. 그러나 이러한 국제법의 수용은 엄밀한 의미에서 사이버 공간에 대한 법률적용이라기 보다는 평화안보에 대한 국제법상의 의미와 사상을 받아들이는 데 지나지 않는다는 한계(김소정·김규동, 2017)를 보여주고 있어 근본적인 해결방안에서도 상당한 거리가 있었다.

2014년부터 2015년까지 진행된 제4차 회의는 이전보다 더욱 진정성 높은 내용을 담고자 노력하였으나 실질적으로는 별다른 진전 없이 다음과 같은 포괄적인 부분의 합의점만을 도출[4]하였다. △ 각국은 의도적으로 자신의 영역에서 사용 중인 ICT를 이용하여 국제적으로 부당한 행위에 사용되도록 허용해서는 안 된다는 점, △ 각국은 중요한 인프라를 의도적으로 손상시키는 ICT 활동을 수행하거나 의도적으로 지원해서는 안 된다는 점, △ 각국은 안전한 네트워크망을 확보하기 위한 조치를 취해야하며, 악성 ICT의 확산과 유해한 숨겨진 기능의 사용을 막아야할 의무가 있다는 점, △ 각국은 다른 국가의 비상대응팀(CERT/CSIRTS)의 정보 시스템에 해를 끼치는 활동을 수행하거나 고의로 지원해서는 안 되며, 악의적인 국제 활동을 위해 자체 팀을 사용하면 안 된다는 점, △ 각국은 인터넷상의 인권과 디지털 시대의 사생활과 관련된 유엔 결의안을 존중해야한다는 점이 그것이다. 하지만 제4차 회의는 사이버 안보문제의 해결을 개별 국가의 고유한 자기 방어권 행사에 대해 국제법의 적용 방식에 대한 명확하고 직접적인 진술을 모색하였고, 대책을 포함하여 국가 책임의 범위와 국제법의 기본 틀이 국가에 대한 안정적인 기대치를 창출함으로써 갈등의 위험을 줄이는데 도움이 되는 구속력 있는 행동기준을 국가에 제공한다는 강한 확신에 입각하여 국제 평화와 안보를 위한 진술을 도모했다는 점에서 발전적이라고 볼 수 있다.

2016년부터 2017년까지 진행된 제5차 회의에서는 사이버 분쟁에 대한 국제 인도법(International Humanitarian Law)의 적용 가능성과 관련하여 근

4. NATO Cooperative Cyber Defence Centre of Excellence(CCDCO).

본적인 의견 차이가 계속 되었고, 사이버 공간에 적용되는 규범을 구축하고자 하는 미국 중심의 서방진영과 중국·러시아 중심의 진영의 이분법적 사고의 차이로 인해 여전히 정치적·외교적으로 공감대를 형성하지는 못했다. 의견 불일치의 주요 쟁점인 △ 기존 국제법의 사이버 공간에 대한 적용문제, △ 자국 영토가 사이버 공격에 악용되는 행위, △ 악성코드를 이용한 사이버 공격에 대한 성격 규정 등의 불협화음이 여전히 좁혀지지 않았고, 사실 국제사회에서 인도주의를 표방하는 국제 인도법의 핵심요소는 전쟁을 수행하는 세력에 의해 발생하는 민간인의 부수적 피해(Collateral Damage)를 방지하고 개인의 인권과 기본적 자유의 보장을 목표로 하는데, 사실 사이버 공격에 대해 이러한 구분을 명확히 정의하기란 쉽지 않은 영역임에 틀림없다.

그동안 UNGGE는 사이버 공간에 대한 국제사회의 합의점을 찾기 위해 2004년부터 2017년까지 총 5차례의 논의를 진행하였다. 이 기간 동안 사이버 안보문제에 관한 소기(所期)의 성과는 있었지만, 대부분의 시간은 서로 반복적인 주장과 이에 반대하는 의견의 호소로 마무리되었다. 이는 UNGGE 보고서가 긴 시간의 대화와 협의에도 불구하고, 양 진영의 입장차로 인해 이 문제를 완전히 해결하지 못한다는 비난을 받게 되는 계기(Korzak, 2017)가 되었음은 물론, 미국 중심의 서방진영이 제시한 탈린 매뉴얼(Tallinn Manual)이 사이버 공간에 대한 자기 방어권의 적용이 가능하다는 것을 분명히 보여주는 것과 비교되면서 오히려 UNGGE의 가치가 낮게 평가될 수 있는 단초를 제공하였다.

지금까지 UNGGE가 보여준 사이버 공격에 대한 자위권 발동 여부, 즉 국제법 적용 및 사이버 무력행위에 대한 대응조치 등에 관해 치열하게 대립하는 모습은 종래의 유엔안보리에서 보여준 정치적·군사적인 전통적인 안보대립과 크게 다르지 않다. 물론 UNGGE 보고서는 사이버 공간에서 발생할 수 있는 중요한 이슈에 대해 사이버 분야의 전문가들의 의견을 유엔총회에 제시하는 일종의 권고안에 불과하고, 국제사회를 강제할 수 있는 어떠한 권한과 기능을 가지지 못할 뿐만 아니라, 실제로 사이버 공격이 발생하였을 경우에도 국제사회로부터 강제성을 띤 제재효과가 전혀 동반되지는 않는다. 그러나 UNGGE 보고서가 유엔안보리 이사국을 중심으로 세계 주요 국가들의 사이

버 전문가들의 의견을 담았다는 점에서 그 상징성은 국제정치 분야에 지대한 영향을 미칠 수밖에 없기 때문에 그 중요성을 강조하지 않을 수 없다.

사이버 안보의 진행과정은 비(非)가시적인 형태의 위협으로 사이버 안보 문제에 대해 국제사회가 치열한 '눈치싸움'을 하고 있는 동안 사이버 공간의 군사화를 추구하고 있는 세력들은 무국적 공간이자 치외법권(治外法權) 지역인 사이버 세계를 마음껏 돌아다니며, 자신들의 이익행위를 위해 사이버 공격을 가할 수 있는 위험을 가지고 있다.

## 2. 대응관점의 대립

### 1) 미국 중심의 서방진영: 국제법적 대응과 탈린매뉴얼

미국이 중심이 되어 서방 국가들과 함께 군사동맹을 구성한 북대서양조약기구(NATO)는 집단적 자위권(Collective Self-defence)을 강조하며 강력하고도 공식적인 안보 프레임을 가지고 있다. 그러나 이러한 안보동맹체가 있음에도 불구하고 2007년 당시 회원국인 에스토니아는 대규모 사이버 공격을 받고 있음에도 사이버 공간에서 발생하는 무력행위(Armed Attack)에 대해 어떻게 대응이 가능한지에 대한 명시적인 국제법이 없다는 이유로 NATO 조약 제5조의 원칙[5]을 적용하지 못했다.

이후 NATO는 2008년 사이버 위협에 대한 대응방안을 논의하기 위해 루마니아(Romania)의 수도 부쿠레슈티(Bucharest)에서 회원국 간 정상회담을 개최하였고, 사이버 안보와 관련한 대응조직과 법체계를 갖추고자 국제 군사기구(International Military Organization)의 역할을 수행할 수 있는 조직인 사이버 방어협력센터(Cooperative Cyber Defense Centre of Excellence, 이하, 협력센터)를 설치하였다. 이때부터 협력센터는 유엔헌장 제51조와 제네바·헤이그 협약 등 각종 국제법을 사이버 공간에서 어떻게 적용할 수 있는

5. NATO조약 제5조 원칙은 한 회원국이 공격을 당하면 이것을 모든 회원국에 대한 공격으로 간주하여 '집단적 자위권(Collective Self-Defence)'을 발효할 수 있다는 것을 말한다.

지에 대해 연구하였고, 국제사회가 사이버 안보에 대해 대립하고 있는 사이 적용이 가능한 사이버전 지침서라고 할 수 있는 탈린 매뉴얼(Tallinn Manual 1.0)[6]을 성문법(成文法) 형태로 발간하였다.

이후 사이버戰에 적용이 가능한 국제법을 정리한 이 매뉴얼은 사이버 공간에서 국제법이 어떻게 적용되는지를 자세히 해석할 수 있는 하나의 툴(Tool)로서 작용하며, 현존하는 국제법의 적용범위인 '전쟁 개시결정에 대한 충분조건(Jus ad bellum)'과 '전쟁을 위한 수행 조건(Jus in bello)'에 대해 사이버 공간에도 그대로 적용할 수 있다는 기본원칙(박노형 · 정명현, 2014)을 적시하고 있다. 또한 국제법상 허용되는 무력 사용(Use of Force)의 원칙도 당연히 적용된다고 말하고 있는데, 이러한 무력 사용에 대한 인정 기준으로 명시된 유엔헌장 제7장의 △ UN 안보리의 승인에 따라 국제평화 유지를 목적으로 군사적 강제조치를 취하는 경우(§42), △ '무력 공격'을 당해 자위권 발동이 가능하고, 이를 행사하는 경우(§51)로 한정하는 요건을 대부분 수용하였다.

하지만 여기서 말하는 자위권에 대한 발동요건에 대해 매뉴얼은 사이버 공격으로 인해 '인명 피해'가 발생하거나, 국가 자산이 '치명적이고 파괴적인 물리적 피해가 발생한 경우'라고 제시하고 있어, 이에 대한 명확한 판단기준을 정의하기가 매우 어려울 뿐만 아니라, 회원국을 제외한 타국(他國)에 대해 자의적인 해석으로 자위권을 발동한 역공격을 감행할 수 있다는 우려가 발생한다.

2017년 사이버전 만 아니라 평상시에 활동하고 있는 사이버 범죄에까지 적용범위를 확대한 탈린 매뉴얼 2.0(Tallinn Manual 2.0, 이하, 매뉴얼 2.0)이 공개되었는데, 매뉴얼 1.0이 사이버 전쟁(Cyber Warfare)에 적용 가능한 국제법에 비중을 두었다면, 매뉴얼 2.0은 사이버 작전(Cyber Operation)에 적용할 수 있는 국제법, 즉 국가의 의도와는 별개로 발생하는 비국가, 또는 집단, 개인 등이 행하는 각종 사이버 범죄들을 말한다. 따라서 사이버 전쟁이 국가와 국가 사이에 일어나는 제한적 주체의 전시상태의 충돌을 의미하는 것

6. 2013 Tallinn Manual on the International Law Applicable to Cyber Warfare.

에 비해 범주가 넓어진 것으로 볼 수 있다.

특히, 새 버전(New Version)은 평상시(Peacetime) 사이버 공간에 대한 위험성을 분석한 결과를 많이 반영하였는데, 여기에는 공간(Space), 인권(IHRL), 해상법(IML) 등 사실상 기존의 국제법을 총 망라해 필요한 요소만을 담아 한층 강화된 사이버 법률화를 추구하고 있고, 이를 바탕으로 각 국가가 사이버 공간에 대한 적절한 입장을 결정할 수 있도록 지원하는 역할을 하고 있다.

매뉴얼 2.0은 사이버 위협에 대해 개별 국가들이 스스로를 '방어할 권리'와 '보복 공격을 할 권리', 그리고 '공격 근원지 식별을 할 권리'에 대한 내용을 담고 있는데, 결국 각국이 합리적인 이유가 있다는 전제조건 아래 사이버 공격에 비례해서 대응하는 것이 가능하다고 본다. 이를 위해서는 두 가지 요소가 필요한데, 사이버 공격을 하는 주체가 국가 기관이어야 하고, 반드시 국가의 지시에 의해서 발생되어야 한다는 점이다. 이는 국제법상 위반을 의미하는 것(Aasmann, 2017)으로, 사이버 주권을 침해하는데 대한 국제사회의 제재가 가능한 것으로 해석된다. 이에 따라 매뉴얼 2.0은 사이버 공간에서의 각국의 주권을 인정해야 한다고 해석될 여지가 있다.

이러한 탈린 매뉴얼의 특성을 종합적으로 살펴보면 다음과 같이 정리해볼 수 있다.

첫째, 기존의 국제법은 다른 영역과 마찬가지로 사이버 공간에서도 적용된다. 사이버 공간에서 각 표준이 어떻게 적용되는지는 국가 관행의 문제로 해석된다. 둘째, 평시 사이버 작전에 관한 규정은 국가 책임법, 국제 인권법, 외교 및 영사법, 국제해상법, 항공법, 우주법, 국제전기통신법 등 대부분의 국제법을 모두 수용한다. 셋째, 국제 평화와 안보, 평화 분쟁의 평화적 해결, 유엔 평화 유지, 자기 방어에 대한 유엔 헌장의 성격을 대부분 수용한다.

탈린 매뉴얼은 현존하는 국제법을 거의 대부분 수용하고 있고, 기존의 국제법이 사이버 공격에 대부분 적용된다는 점에서, 사실상 미국 중심의 진영과 입장을 같이 하고 있다. 비록 국제규범은 아니지만 탈린 매뉴얼을 통해 적(敵)의 네트워크 침해에 사이버 역(逆)공격을 할 수 있는 제한적인 근거를 마련하였고, 전통적인 전쟁방식에서 사용되고 있던 각종 교전수칙(交戰守則)

을 사이버 공간에 적용함으로서, 자국민(自國民) 또는 동맹국들 간의 인명 피해가 발생할 경우에 군사적 보복조치를 가능(김상배, 2017)하게 하였다.

이렇게 탈린 매뉴얼은 사이버戰을 둘러싼 국제법상 문제를 유권해석(有權解釋)을 할 수 있는 지침서 역할을 수행하고 있는데, 이는 그동안 국제사회에서 군사적 원칙조차 제대로 정의되어 있지 않던 사이버 전쟁이라는 새로운 영역에 대해 '전쟁이 일어날 수 있는 공간'으로 명명하면서 공식화하는데 의의가 있다. 그리고 이러한 입장의 성명은 사이버 공격에 대한 규제 범위를 확대하여 동맹국들에 대한 사이버 침해에 대해서는 공세적인 전력을 발동해 적극적인 대응을 하겠다는 의도가 담겨져 있고, 사이버 공격을 직접적으로 규제하는 별도의 국제법이 없어도 탈린 매뉴얼을 이용해 통제기능을 수행할 수 있는 전략적 이점을 강화하고자 하는데 있다.

결국 미국 중심의 서방진영은 통상의 개전 법규나 전시 국제법을 사이버 공간에 적용하여 규정을 명확화하고 잠재적인 적(敵)의 행동을 억지하는 한편, 국제법의 제한된 틀에서 벗어나지 않게 군사적 대응을 가능하게 하는 방식을 추구하고 있다.

2) 중국·러시아 중심의 진영: 주권적 대응과 상하이협력기구(SCO)

미국 중심의 서방진영이 탈린매뉴얼을 통해 기존의 국제법을 적용함으로서 사이버 안보문제를 해결하려는 입장을 보이자 중국·러시아 중심의 진영은 불편한 심기를 계속하여 표출(Giles, 2012)하고 있다. 특히, 유엔을 통한 국제사회의 합의된 규범이 아닌 NATO 산하 연구기관에서 작성한 탈린매뉴얼이 사이버戰을 수행하는 기준지침으로 확대될 수 있다는 우려가 높아지면서, 중국·러시아 중심의 진영은 상하이협력기구(SCO)를 기반으로 사이버 안보를 위한 결집을 더욱 강화하고 있다.

당초 상하이협력기구(Shanghai Cooperation Organization, 이하 SCO)는 중국의 제안으로 지난 1996년 러시아, 카자흐스탄, 키르기스스탄, 타지키스탄 등 5개국이 상하이(上海)에서 국경지역의 안정과 신뢰 구축 및 군비축소를 위한 안보 논의[7]를 위한 정상회담에서 출발하였다. 이후 1997년 러시아 모스크바(Moscow)에서 개최한 제1차 회의부터 2000년 타지키스탄 두샨베

(Dushanbe)에서 개최된 제5차 회의까지 SCO는 대부분 지역안보 공동체로서, 군사와 경제영역을 침해할 수 있는 안보문제인 테러리즘, 인종적 분리주의, 종교적 근본주의(과격 극단주의)에 대한 공동 대응방안 모색을 주요 의제로 삼아왔다.

그러다 2009년 러시아의 예카테린부르크(Yekaterinburg)에서 개최한 제14차 회의에서 러시아의 제안으로 사이버 전쟁을 포함하는 모든 분야의 사이버 안보에 대해 회원국 간의 네트워크 시스템을 보호할 것을 의제로 논의하였는데, 여기에서 SCO는 회원국에 대한 사이버 공격에 대해 공격 행위자에 대한 제재를 포함한 공동대응뿐만 아니라 공격에 수반된 기술까지도 무력행위를 해서라도 제재를 가할 수 있도록 광범위하고 강력한 사이버 안보체계를 구축한다는 시각을 선명하게 드러냈다. 이는 사이버 공간을 주권이 적용되는 국토의 일부로 간주하려는 중국과 러시아의 입장이 반영된 결과였다.

2011년 SCO의 중국·러시아·타지키스탄·우즈베키스탄 4개국은 정보안보를 위한 '국제정보안보행동강령 초안(Draft International Code of Conduct for Information Security, 이하 행동강령)'을 유엔총회에 제출하였는데, 이 행동강령에는 사이버 안보가 가져야 하는 핵심 요소에 대해 군사안보 차원의 개념과 동등하게 인식하며, 개별 국가중심의 주권이 부여된 사이버 안보정책이 구현됨은 물론 사이버 위협에 대한 철저한 방위태세를 갖춰야 한다고 규정하고 있다. 이어 2015년에는 중국·러시아·카자흐스탄·타지키스탄·우즈베키스탄 5개국이 2011년에 제출했던 행동 강령 초안에 대해 내용을 수정한 개정안을 보고하였는데, 이 보고서의 핵심 사항은 사이버 공간에 대한 정의를 물리적 개념인 국가의 '주권'과 '영토'의 의미와 동일하다는 원칙을 명확하게 규정한 것에 있다. 이는 사이버 안보가 가지는 함의가 국가안보와 동일시되며, 자국의 정치적·사회적 안정을 위해서는 어떠한 경우에도 지켜야 할 필수불가결한 국가 구성요소(조윤영·정종필, 2016)로서 새로운 사이버 국제법 제정의 필요성을 강조하였다.

중국과 러시아는 오랫동안 미국 등 서방국가들로부터 사이버 공간에 대한

---

7. '국경지역의 군사적 신뢰 강화를 위한 협정(关于在边境地区加强军事领域信任的协定)'.

개방요구를 받음은 물론 국제사회와의 정보공유 등 자국의 영향력을 감소시킬 수 있는 외부적 압박을 상당히 많이 받았다. 이러한 중압감을 해소하기 위해 중국·러시아 중심의 진영은 자국만의 강력한 사이버 통제정책에 대한 대외적 명분을 삼기 위한 방편으로 SCO의 행동강령을 더욱 확장하면서 사이버 안보문제에 있어 국제사회에서의 외교적 우위를 차지하는 방식으로 전략적인 대응방안을 구상하였다.

실제로 중국과 러시아가 주도적으로 이끌어가고 있는 SCO는 미국의 주도로 창설된 NATO에 맞서기 위한 대항적 안보색채가 매우 강한 성격의 군사협력체이며, 국제사회 모두에게 영향을 미칠 수 있도록 사이버 위협에 대한 문제를 국제안보 차원의 영역으로 확대하였다. 이미 사이버 공간에 대한 SCO의 행동 강령은 영토 보전을 확장하기 위한 중국의 전략추진과 동일하게 진행되고 있으며, 개별국가들의 재량에 따라 자국 내에서 사용되는 네트워크 또는 디지털 매체를 순환하거나, 감시, 통제할 수 있다는 사이버 주권의 원칙을 계속 강조하고 있다. 이는 사이버 침해에 대한 강력한 통제만이 안정된 네트워크 사회를 구현할 수 있는 배경이 되면서, 사이버 영역에 대한 미국 중심의 국제사회의 개방 압력을 피해갈 수 있는 구실을 가지고 자국의 체제를 효율적으로 관리할 수 있는 기반을 마련할 수 있기 때문이다.

2017년 인도와 파키스탄이 SCO 회원국으로 가입하면서, 이 기구는 세계 면적의 23%를 차지하고, 전 세계 인구의 45%를 포괄하는 거대 기구로 성장하였다. 특히, IT 강국이라 불리는 인도와의 사이버 안보 협력체계 구축은 미국을 중심으로 한 서방진영과의 국제사회의 사이버 안보정책에서 힘의 균형을 우위로 점할 수 있는 능력을 가질 수 있는 계기를 마련하게 되었다.

# IV. 사이버 안보문제와 우리의 대응

## 1. 전통적 안보체계와의 차별성: 사이버 협력관계의 확장

그동안 국제사회는 각 국가별로 독립적인 정치체계를 갖추어 운영되어 왔으며, 경제·사회·문화 등 각 나라가 추구하는 고유의 가치가 서로 다를 수밖에 없는 특수성을 서로 인정하면서 세계 평화를 제1차적 목표로 하는 국제질서 관계를 유지해 왔다. 이는 어느 한 국가가 다른 국가가 보유한 고유의 가치를 침해하거나 공격하는 경우에는 국제사회가 이를 명백한 침략행위로 규정하여 무력을 동반한 '평화 이행'을 강제할 수 있는 일종의 집단안보체제라고 할 수 있다. 그러나 이러한 국제질서 관계를 유지하는 국제사회의 통제체제는 인터넷이라는 정보의 진화로 인해 탄생한 사이버 공간에서 발생하고 있는 국가 간 또는 개인과 국가 간의 사이버 공격에 대한 명확한 안보체계를 제시하지 못하고 있다. 만약 물리적인 형태의 공격행위 없이 오로지 사이버 공격만을 통해 군사통제 시스템을 전복하고, 국민의 생존을 위협할 수 있는 국가기반시설이 파괴되거나, 국제사회와 연결된 금융·경제체제를 일제히 마비되는 사이버 무력행위가 발생한다면 이를 자국의 힘만으로 대응하는 것은 쉽지 않은 일이다.

통상적으로 국제안보를 위협하는 무력분쟁에 대해 국제사회는 유엔을 통해 다양한 방법과 조치로 그 해결을 모색하여 왔다. 물론 모든 국제문제가 해결되는 것은 아니지만 국제사회는 국제법에 따라 중개와 조정 등의 활동을 권고할 수 있으며, 안전보장이사회의 전속권한에 따라 경제적·외교적·군사적으로 문제해결을 강제할 수 있는 제재조치(Ziring et al., 2005)를 취할 수도 있다. 그러나 비가시적·비영토적 개념을 가지고 있는 사이버 공간은 이렇게 국지적·지역적 개념이 통용되는 현실 공간과 비교해 매우 이질적인 특성을 가지고 있어 동일한 형태의 대응조치를 강구하는 것은 다소 무리가 있다.

특히, 현실 공간에서 산발적으로 발생하고 있는 국제안보 문제를 해결하기 위해 국제사회가 군사적·정치적·경제적으로 연결된 일종의 유기적 망을 통해 국가 간의 평화적 균형 상태를 유지할 수 있도록 질서구조에 많은 영향력을 부여하고 있는데 반해, 사이버 공간에서 보여주는 국제질서 관계는 이러한 지구적 상호연결의 강도에 비해 상대적으로 낮은 단계의 통제력을 가지고 있으며, 국가 간 행동의 다자간 규제조치는 물론 유엔으로 대표되는 집단안보체제의 기능 역시 매우 제한되고 있다. 또한 강대국들의 정치·군사·문화적 기능이 현실 공간에서는 매우 높은 수준으로 유지되면서 국제사회의 중론(衆論)을 이끌어가는 리더십을 발휘하는데 비해 사이버 공간에서는 강대국들의 영향력이 통하는 행동 범위가 제한될 수밖에 없는 새로운 형태의 질서구조가 발생한다.

국제사회는 아직도 사이버 공간에서 발생하는 각종 위협요인에 대해 완전히 통합된 대응방안을 제시하지 못하고 있고, 사이버 공간을 명확히 정의할 수 있는 초월적 권위조차 여전히 부재한 상태이다. 이는 결국 사이버 공격 등 일체의 혼란 상황에 대한 대비책은 각 국가 간의 상이하고 분절된 기준과 준거 방식에 따라 개별적으로 구축해야 한다는 것을 의미한다. 물론 사이버 공간에서도 안보 공동체를 구성하고자 하는 집단체제가 자연스럽게 구성되고 있는데, 주지하다시피 미국 중심의 서방진영과 중국·러시아 중심의 진영으로 대표되는 사이버 공간의 주도권에 대한 세력대립을 들 수 있다.

하지만 두 진영의 논쟁 공방이 사이버 공간에 대한 개별국가의 주권적 개념의 인정과 기존 국제법 체제의 적용문제에 있는 만큼, 대표주자인 미국과 중국의 상호간 연결밀도의 희석이 이루어지지 않고서는 구조적 양분화 과정은 더욱 가열될 것이고, 점점 더 다층적이고 변화무쌍하게 변화하고 있는 사이버 위협에 직면하고 있는 우리의 입장에서도 상당히 불리한 방향으로 작용할 수 있다.

따라서 사이버 안보에 대한 대응전략의 방향의 설정은 사이버 공간이 전통적인 방식의 지정학적 공간과 다르지 않다는 점을 강조하며, 사이버 주권의 개념을 적용해 대응전략에 필요한 기준점을 마련해야 할 것이다. 여기서 말하는 주권의 개념은 국가와 국민에게 위해를 가할 수 있는 일체의 사이버

위협에 대한 방어와 공격을 의미하며, 사이버 공간에서 간섭을 받지 않고 주권을 완전히 행사하는 독립된 권리를 의미한다.

이와 함께 국제사회와의 사이버 공격행위에 대한 대응공조체계가 선행되어야 한다. 이러한 안보 공동체 구축은 상호간의 정치·군사구조의 발전 과정을 말하며, 동맹국 간의 내재해 있는 역동성을 공유하는 것을 말한다. 따라서 우방국인 미국과의 기술과 정보공유 및 협력체계를 구축(김상배 외, 2017)하는 문제를 심도 있게 추진하여야 하고 이행하여야 한다. 이는 사이버 안보체계를 수립하는 데 있어 국제사회가 일류공동체 의식을 바탕으로 시간과 공간을 초월한 일치단결성을 보여주지 않는 한 사이버 공간에 대한 개별 국가들의 목표와 지향점이 서로 상이하다는 점과 함께 공통적 사고에 의해 제한할 수 있는 네트워크 공간의 경계 획정이 사실상 불가능하기 때문이다. 이로 인해 사이버 공간에 의해 발생하는 무력행위는 국제문제로 인식하고, 국민국가의 주권적 시각에서 문제를 해결할 수 있게 된다. 물론 사이버 공간이 가지는 초경계적·초국경적 특성에 의해 경계가 확실한 국가영토와 일치하지 않는다는 점을 들어 침해공간의 경계 획정 문제가 발생할 수 있으나, 국내로 유입되는 트래픽(Traffic)의 경로에 의해 주권침해의 적용을 부여하는 시점과 장소가 명확히 탐지될 수 있으므로 충분히 해결될 수 있는 범위로 보인다.

## 2. 적극적 사이버 방어체계의 확립

사이버 주권의 실현과 이에 따른 능동적 대응을 수행하기 위해서는 이를 뒷받침할 수 있는 대응법규 체계를 반드시 갖추어야 한다. 특히, 비대칭 위협으로 작동하고 있는 사이버 공격에 대한 대응능력을 강화하기 위해서는 최우선적으로 사이버 안보를 확립할 수 있는 방어체계를 확립하여 안보문제를 예방할 필요가 있다.

현재 사이버 안보를 이끌고 있는 법규체계는 대통령 훈령인 「국가사이버안전관리규정(이하, 관리규정)」이다. 하지만 이 규정의 제한범위는 정부기관

을 포함한 공공영역으로 한정되어 민간분야 및 입법·사법기관은 적용범위에서 제외하고 있다. 이는 우리 사회가 사이버 위협에 노출되어 있음에도, 국가적 대응 활동을 위한 근거는 공공과 민간의 영역으로 분리되어 사이버 공격의 위협에 효과적인 대처가 어렵다는 것을 말해준다. 물론 민-관 영역을 모두 포함하는 주요 정보통신기반시설에 대한 보호를 목적으로 제정된 「정보통신기반보호법」이 국가안보 차원의 시각으로 접근하는 중심적인 규정이 될 수 있으나, 이 규정의 목적이 "사이버 테러리즘에 대비한 주요 정보통신기반시설의 보호대책을 수립·시행하여, 동 시설의 안정적 운용을 확보함으로써 국가의 안전과 국민생활의 안정을 보장하려 함이다."라고 명시[8]하고 있어, 핵심기반시설에 대해 방어적 측면으로 해커에 의한 정보시스템으로의 침입을 방지하는데 그 목적이 있다. 결국 사이버 위협행위에 대해 국가안보의 문제로 성격을 부여하기에는 무리가 있는 규정이다.

이처럼 국내에는 아직 사이버 안보에 대한 정부와 민간영역의 명확한 역할과 책임을 규명하고, 공격 주체에 대한 처벌과 대응 등의 안보문제에 대해 구체적으로 어떻게 해결할 것인지에 대한 명문의 규정이 없는 셈이다.

우리 정부는 그동안 2005년 「국가사이버안전관리규정」을 제정한 이후, 법제정 등 별다른 방어체계의 확립 없이 정부의 방침을 담은 대책서 위주의 대응전략을 만들었다. 이러한 기조는 2009년 대규모 디도스(DDoS) 공격을 받은 후, 사이버 안보체계를 강화하기 위해 만든 「국가사이버 위기 종합대책」, 2011년 'NH농협 전산망 마비사태'에 따라 「국가사이버 안보 마스터플랜」 발표, 2013년 '3·20 사이버 테러'와 '6·25 사이버 공격'을 받은 후 발표한 「국가사이버 안보 종합대책」, 그리고 2015년 '한국수력원자력 해킹' 사건의 충격으로 수립한 「국가사이버 안보태세 강화 종합대책」에 이르기까지 계속된 사이버 공격에도 불구하고, 여전히 사이버 안보체계를 강화하기 위한 적극적 방어체계 확보에는 인색함을 보였다. 또한, 공개된 대책방안 보고서가 대부분 사이버 안보에 대한 중요성을 언급하고, 조직의 기능을 강화하는 방향성에 대한 문제만 지적하고 있을 뿐, 새로운 체계로서의 면모를 보여주지

8. 정보통신기반보호법 제1조.

못하였다.

실제로 미국은 지난 2001년 9·11 테러가 발생한 이후, 흩어져 있던 안보 기능을 통합한 「국토안보법」을 제정하면서, 이와 함께 사이버 안보와 관련한 국가 정책을 지속적으로 수립하고, 이를 뒷받침할 수 있는 법규를 체계적으로 정비하고 있고, 일본은 2014년 공식적으로 사이버 안보에 관한 기본법이라고 할 수 있는 「사이버시큐리티기본법(サイバーセキュリティ基本法)」을 제정해 조직법적·작용법적 기본법을 마련하였다. 이는 우리에게 많은 시사점을 주는데, 우리도 사이버 위협에 대해 국가 차원의 종합적인 대응체계를 구축해 정부와 민간이 함께 협력하여 국가 차원에서 체계적이고 일원화된 기준으로 사이버 공격을 예방하고, 국가의 역량을 신속히 결집해 대처할 수 있는 방어체계 구축이 필요하다. 이를 위해 우선적으로 기존 사이버 안보와 관련된 법률에 대한 전체적인 검토가 수반되어야 하고, 새로운 사이버 안보전략에 대한 근본적인 평가가 이루어져야 한다. 그리고 이러한 방어체계 설계는 다음과 같은 조건을 구비해야 한다.

첫째, 사이버 안보체계는 '통합성'을 갖추어야 한다. 현재의 사이버 안보와 관련된 법체계는 분산되어 있어 사이버 문제의 의식을 각 기관별로 필요한 합리성과 전문성의 원리를 강조하는 분산성에 기반을 두고 있는데, 공격의 방식과 피해의 광범위성과 함께 점점 복잡해지는 사이버 위기가 빈발하면서 사이버 대책기관 간 중복 및 혼선, 책임의 분산에 따른 폐해가 나타나기 때문에 이를 통합하는 법체계가 갖추어져야 한다.

둘째, 사이버 안보체계는 '유기성'을 가져야 한다. 현재는 국정원이 「국가사이버안전관리규정」에 의거하여 공공기관을 포함한 민간영역의 안전까지 책임지는 형국으로 민간의 정보네트워크 영역에 국가정보기관이 접근할 수 있는 것에 대한 국민적 반감이 어느 정도 있는 상태에서 유기적인 공조체계의 구축은 사실상 불가능하다. 따라서 법률을 제정하더라도 상명하달식의 기계적이고 경직·폐쇄적인 강제성만을 부여하는 것이 아니라, 사이버 보안기술 산업을 진흥할 수 있고, 사이버 안보체계로 인해 경제적 성장도 동반할 수 있는 유기적 관계를 내재한 법체계를 가져야 한다.

사이버 공간에서 발생하고 있는 수많은 위협 행위들에 대한 일원화된 정

책을 구현할 수 있는 근거가 되는 법체계가 마련되고 있지 않다는 것은 변화되고 있는 사회 전반의 안보에 대한 질서체계를 혼란시킬 수 있는 우려가 있다. 물론 현행 「정보통신기반보호법」과 「국가사이버안전관리규정」을 통해 국가안전보장, 행정, 국방, 치안, 금융, 통신, 운송, 에너지 등의 업무와 관련된 주요 정보통신기반시설에 대하여 국가 위급 상황 시에 정부가 규제하고 명령할 수 있는 권한을 가지고 있기는 하지만, 사이버 공격에 대한 징후를 사전 탐지하여 수집된 정보를 국가가 종합적으로 '분석 및 대응'한다거나 발생한 사이버 공격에 부처별 대응이 아닌 국가종합적인 총력대응을 할 수 있는 근거가 되는 법은 아직 마련되지 않았다.

따라서 우리 사회가 가진 IT 기술 발전의 속도와 제4차 산업혁명시대로의 진입이라는 현실을 감안하였을 때, 이들을 통제하고 제재함과 동시에 국민들의 안보의식을 고양시키고, 불안감을 해소할 수 있는 대응전략을 마련하기 위한 전제로 사이버 안보에 대한 방어체계 기본법이 필수적으로 제정되어야 할 것이다.

## V. 결론

과학기술의 비약적 팽창은 초연결사회와 인공지능(AI) 시대를 열어가며, 인류문명의 또 다른 진화론적 종착역에 다가설 수 있는 기반을 제공하고 있다. 이미 제4차 산업혁명이라 불리는 사물인터넷(IoT), 빅데이터(Big Data) 등의 정보통신기술(ICT)의 혁신적인 발전이 우리 삶의 영역으로 깊숙이 들어왔음은 물론 한반도 국가산업의 발전을 도모하는 핵심전력이 되고 있어 현대 사회에서 사이버 공간이 차지하는 영향력을 분석하는 것은 이제 그 의미가 무색해질 정도로 확장되었다.

하지만 이러한 사이버 공간의 확장성이 오히려 인류의 발전을 위협하는 기술의 역설을 발생하고 있는데, 이는 기술을 오용함으로서 얻을 수 있는 새로운 힘의 불균형을 악용하고자 하는 새로운 안보위해세력의 등장을 용이하

게 하였다. 과거 물리적인 군사적 행동에 의해서만 파괴할 수 있다고 생각되었던 국가중요시설 및 국가기반시설 등의 보호대상이 악성코드를 무기로 하는 사이버 공격만으로도 충분히 붕괴시킬 수 있고, 네트워크 통제권을 해킹해 임의대로 구동할 수 있는 안보 공포감마저 들게 한다.

국제사회는 지금 사이버 공간에 대한 안보문제를 해결하는 대응방식에 대해 현존하는 국제법을 적용해서 사이버 안보문제를 풀어나가야 한다는 미국 중심의 진영과 사이버 주권을 인정하여 개별국가들의 독립된 법체계를 갖추어 해결해야 한다는 중국·러시아 중심의 진영이 팽팽하게 대립하고 있다. 이러한 양 진영 간의 갈등관계로 인해 국제사회는 사이버 위협에 대해 국제안보 공동체로서 대응할 수 있는 구조를 갖추지 못하고, 개별 국가들이 각자 생존과 안전을 지켜야하는 안보 공백 상태를 만들고 있다.

이렇게 국제사회가 전통적인 안보의 대상인 영토·영해·영공의 개념에 대해 특정 국가의 주권이 발휘되는 영역이자 그 국가의 통제를 받는 배타적인 권리를 보장받는다고 인정한 것과 달리, 사이버 공간에 대해서는 배타적 주권에 대해 아직까지 인정된 합의를 갖지 못한 것은 '사이버 공간'을 기존의 전통적인 안보영역과 동일하게 평가하고 유엔이 영향력을 미칠 수 있는 공간으로 제한하여 국제법을 통해 사이버 공간의 위협 문제를 해결하려는 미국의 입장과 유엔체제 하에서 상당한 권한을 가지고 있는 미국의 힘을 약화시키고 자신들이 새로운 영향력을 발휘할 수 있도록 사이버 공간에 대한 별도의 사이버 국제법이 마련되어 적용되어야 한다고 주장하는 중국·러시아의 입장이 다르기 때문이다.

그동안 우리사회는 대규모 디도스(DDoS) 공격과 사이버 금융해킹 등의 각종 위협으로부터 정부기관은 물론 개인에 이르기까지 막대한 피해를 입었음에도 불구하고, 지금까지의 대응형태는 대부분 공세적이고 적극적인 전략을 보여주기보다는 주로 정보보호 시스템을 보완하는 사후약방문(死後藥方文) 형태의 비적극적이고 방어중심적인 대응전략을 보여주었다. 이는 사이버 공포가 주는 파괴력과 비교해 상대적으로 불안정한 대응체계를 보여주고 있는데, 가장 큰 문제는 사이버 위협에 대한 우리의 입장이 명확하지 못하고, 매우 불분명하다는 점에 있다.

사실상 우리 정부의 사이버 안보정책을 추진하는 근거법규인 「국가사이버안전관리규정」에서조차 조직체계 및 운영에 대한 사항만을 규정(배선하 외, 2017)하고 있을 뿐, 사이버 공격에 대해 우리의 주권(Sovereignty)을 침해하는 행위로 인정한다는 명문의 규정을 명시하고 있지 않음은 물론, 이에 대한 자위권(Self-Defence)으로서, 사이버 반격을 가할 수 있다는 근거도 마련되지 못한 상태이다. 이는 외부적 침해에 대해 국가가 가지는 고유권(固有權)이자, 자연법상의 권리(權利)를 방위할 수 있는 우리의 법질서 수호의 원칙을 약화시킬 수 있고, 국제사회에 우리의 입장을 공식적으로 밝히지 않음으로서, 공격에 반격할 수 있는 명분을 미약하게 만들고 있다.

물론 국제정치 논리가 각 집단의 정치적 배경과 목적 그리고 이익에 따라 입장을 달리하는 힘의 균형관계로 이해는 상황에서 이견의 발생은 당연한 귀결로 이어진다. 하지만 문제는 한국 역시 사이버 공간에서 발생하는 공격행위에 대해 아무런 입장을 표명하고 있지 않다는 점인데, 이는 단순하게 표현하자면 사이버 공격에 대해 계속해서 아무런 대응을 할 수 없음을 의미한다고 보인다.

이를 위해 우선적으로 해야 할 전제조건은 사이버 공간을 우리의 주권이 미치는 영역으로 명확하게 규정하여야 한다. 분명 네트워크 공간은 자유를 상징하는 평화적 기반을 가진 구조체이며, 누구든지 접근할 수 있는 평등성을 가진 영역이다. 그러나 이에 대한 침해적 행위가 국가와 국민의 안보를 저해하는 위기상황에 이를 경우에는 자위권을 발동한 대응을 할 필요성이 제기된다. 또한, 언제든 이러한 자위권을 행사할 수 있도록 사이버 무기를 비롯한 IP 차단, 국제공조를 통한 공격 주체의 체포 및 형사 처분까지 감행할 수 있는 능동적 대응을 구사해야 한다. 둘째, 협력적 대응전략을 구사할 수 있도록 대응의 범위를 넓힐 필요가 있다.

이제 사이버 위협을 완화하려는 노력은 통상적인 정책에 의해 해결할 수 있는 수위를 벗어나고 있다. 이는 보다 체계적이고 장기적인 구상에서 접근할 수 있는 방법론이 요구되며, 사이버 공격에 철저하게 방어할 수 있는 시스템 구축도 중요하지만, 무엇보다 이를 시행하는 공격 주체에 대한 원천적인 소멸 또는 파괴를 가할 수 있는 전략적 대응방안을 마련하는 것이 중요하

다는 것을 의미한다.

따라서 우리의 대응방식도 사이버 공간을 침해하는 공격행위에 대해 주권 침해로 간주하고, 이에 대한 자위권으로 역공격을 펼칠 수 있는 능동적 대응 전략을 추진할 필요가 있다. 물론 여기에는 반드시 우리의 힘만으로 사이버 위협에서 완전히 벗어날 수 없기에 국제협력 등 사이버 동맹정책도 수반되어야 할 것이다. 이로서 방어적 우군을 만들고, 공격적 탄력을 부여받을 수 있는 대응전략으로 발돋움할 수 있을 것이라 생각된다.

투고일자: 2018-07-17 심사일자: 2018-09-11 게재확정: 2018-09-13

## 참고문헌

김상배. 2017.「사이버 안보 국제규범의 세계정치: 글로벌 질서변환의 프레임 경쟁」.『국가전략』 제23권 제3호.

김상배 외. 2017.『사이버 안보의 국가전략』. 서울: 사회평론아카데미.

김소정 · 김규동. 2017.「UN 사이버안보 정부전문가그룹 논의의 국가안보 정책상 함의」.『정치 · 정보연구』 제20권 제2호.

김인중. 2013.『사이버 공간과 사이버 안보』. 서울: 글과 생각.

박노형 · 정명현. 2014.「사이버전 국제법적 분석을 위한 기본개념의 연구: Tallinn Manual의 논의를 중심으로」.『국제법학회논총』 제59권 제2호.

배선하 외. 2017.「사이버위협 정보공유 체계 개선방안 연구」.『신안보연구』 제2권 제1호(통권 190호).

신진. 2011.『국제정치와 안보』. 대전: 충남대학교출판문화원.

신진. 2016.「북한의 사이버 공격(Cyber attack)과 국제적 대응」.『통일문제연구』 제28권 제2호.

신경수. 2017.「북한의 사이버 전력과 블록체인 기반 대응체계 연구: 서큘레이팅 모델을 중심으로」.『신안보연구』 제2권 제1호(통권 190호).

임종인. 2014.「사이버 위협 시나리오 개발 및 대응방안 연구」. 합동참모본부 연구용역과제.

권진욱 · 박정화. 2010.「악성코드의 새로운 패러다임, Stuxnet」.『보안이슈』 10월 19일.

조윤영 · 정종필. 2016.「사이버안보(cybersecurity)를 위한 중국의 전략: 국내 정책 변화와 국제사회에서의 경쟁과 협력을 중심으로」.『21세기정치학회보』 제26권 제4호.

Aasmann, Lauri. 2017. “Tallinn Manuel 2.0.” Cyber Conflict Excercise & Contest 2017, Speech.

Antonenko, Oksana and Bastian Giegerich. 2009. “Rebooting NATO-Russia Relations.” Survival Apr-May 2009, Vol. 51 Issue 2.

Bishop, Matt. 2017. *Computer Security: Art and Science*. Boston: Pearson Education, Limited.

Cardash, Sharon L., Frank J. Cilluffo, and Rain Ottis. 2013. *Studies in Conflict & Terrorism*. Sep 2013, Vol. 36 Issue 9, pp. 777-787.

Clarke, Richard A. and Robert Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. EccoPress.

Garrie, Daniel, Michael Gervais, Michael Preciado, Jesse Noa, and Mils Hills. 2012. “The New Frontier of Warfare.” *Journal of Law & Cyber Warfare*, Volume 1, Winter 2012, Issue 1.

Giles, Keir. “Russia’s Public Stance on Cyberspace Issues.” In Czosseck C., Ottis R., Ziolkowski K. (Eds.), *2012 4th International Conference on Cyber Conflict* (NATO CCD COE Publications, 2012), p. 65.

Guerrini, Federico. 2014. “In Search Of A Governance. Who Will Win The Battle For The Internet?” *Forbes*, Oct 24.

Kania, Elsa, Samm Sacks, Paul Triolo, and Graham Webster. 2017. “China’s Strategic Thinking on Building Power in Cyberspace”, CICS.

Korzak, Elaine. 2017. “UN GGE on Cybersecurity: The End of an Era?” *The Diplomat*, July 31. https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

Kott, Alexander, Cliff Wang, and Robert F. Erbacher. 2014. “Cyber Defense and Situational Awareness.” United States Army Research Laboratory.

Lehto, Martti and Pekka Neittaanmäki. 2018. *Cyber Security: Power and Technology*. SpringerVerlag.

Lindsay, Jon R., Tai Ming Cheung, Derek S. Reveron. 2015. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. London: Oxford University Press.

O’Flaherty, Kate. 2018. “Cyber Warfare: The Threat From Nation States”. *Forbes*, 2018/05/03. https://www.forbes.com/sites/kateoflahertyuk/2018/05/03/cyber-warfare-the-threat-from-nation-states/#1e1f3ffc1c78.

Pernik, Piret, Jesse Wojtkowiak, and Alexander Verschoor-Kirss. 2016. “National Cyber Security Organisation: UNITED STATES,” NATO: Tallinn.

Radziwill, Yaroslav. 2015. *Cyber-Attacks and the Exploitable Imperfections of International Law*. BrillAcademicPub.

Roscini, Marco. 2014. *Cyber Operations and the Use of Force in International Law*. UK: Oxford University Press.

United Press International. 2005. “Hacker Attacks in US Linked to Chinese Military: Researchers.” *United Press International*, Nov 24.

WEF, 2018. The Global Risks Report. p.14-15.

Ziring, Lawrence, Robert Edwon Riggs, and Jack C. Plano. 2005. *The United Nations: International Organization and World Politics*. New York: Thomson Wadsworth.

# Security Issues in the International Society and Cyber Space

Kyeongsu Shin
Ph.D., Police Science Institute
Jin Shin
Professor, Chungnam University

The international community, which pursued technological prosperity and well-being with the advent of cyberspace, is now facing inevitable irony. The international community, which has entered the so-called "Superconnectivity· Superintelligence," is directly exposed to cyber attacks armed with malicious code, which poses new threats to the international community.

However, the international community has yet to come up with a direct response to this problem. Of course, are they still aware of the fact that cyber world threat actions are threatening the security of individual countries, and that such threats may not have an impact on the global community's areas of collective security.

In particular, the differences between the two countries' bilateral opinions on the issue of cyber security and those of the U.S. and Russia who want to establish the rules applied to cyberspace have not led to a political and diplomatic consensus. Without dilution of the interconnection density of, the process of structural separation will heat up further. And this fragmentation may pose a significant disadvantage for us in the face of increasingly multilayered and ever-changing cyber threats.

Therefore, In this study, we want to demonstrate the expansion of the cyber cooperation system and the establishment of an active cyber defense system in order to understand the fragmented view of cyber security by the international community and to explore the unique and practical responses we need.

Keywords: Cyberspace, cybersecurity, Tallinn Manual, Shanghai Cooperation Organization(SCO)

신경수. 경찰대학 치안정책연구소 박사
충남 아산시 신창면 황산길 100-50, 경찰대학 치안정책연구소 201호
kurukury81@gmail.com

신진. 충남대학교 정치외교학과 교수
대전광역시 유성구 대학로 99, 충남대학교 사회과학대학 201호
jinshin@cnu.ac.kr