Jeju Peace Institute 제주평화연구원

JPI PeaceNet

신흥안보 시대의 사이버 평화

윤 정 현
국가안보전략연구원

[기획자 註] 정보통신기술의 발달은 사이버 공간이라는 새로운 온라인 영토를 인류에게 제공하고 있다. 하지만 이 온라인 공간에서도 인간의 폭력성은 여과 없이 드러나고 있으며 사이버 공간에서 평화를 어떻게 이룰 것인지에 대한 논의가 필요하게 되었다. 사이버 공간은 인류가 물리적으로 존재하고 있는 오프라인 공간과는 질적으로 다른바, 이 새로운 공간에서 인류가 어떻게 폭력을 줄이고 평화를 구축해나갈 수 있을지에 대한 논의는 오프라인 공간의 평화 논의와는 별도로 진행될 필요가 있다. 이에, 국가안보전략연구원의 윤정현 박사의 글을 통해 사이버 공간에 대한 평화논의와 신흥 사이버 평화론에 대해 듣고자 한다. (기획: 임해용 연구실장 (haeyonglim@jpi.or.kr)

머리말

기술의 발전은 새로운 공간의 출현을 낳고, 새로운 공간의 출현은 그에 따른 국제질서와 안보적 파급력을 낳는다. 새로운 공간의 출현은 곧바로 그 공간을 누가 지배하고, 어떻게 이용하느냐에 대한 전략적 고민을 안겨주기도 한다. 육지, 해양, 우주 등 인간의 의지나 행동과는 무관하게 존재하는 자연적 공간과 달리 사이버 공간은 탄생이나 존재, 확대에 있어서 전적으로 인간의 의지와 노력이 낳은 산물이다. 사이버 공간은 행위자들에 의해 매일매일 '구성되는' 공간이기도 하며, 사이버 공간에 대해 행위자가 갖는 관념과 선택은 사이버 공간의 성격을 결정하는 중요한 변수로 작용한다. 사이버 공간을 얼마나 잠재적으로 위험한 공간으로 보느냐에 따라 행위자들의 사이버 공간에 대한 전략과 행동은 달라질 수밖에 없으며, 사이버 공간의 안전을 확보하고자 하는 궁극적인 목표의 지향이 어디냐에 따라 사이버 평화의 개념과 거버넌스의 형태, 노력의 수준은 큰 차이를 낳을 수밖에 없다.

현재 사이버 공간에서는 소극적 의미에서부터 적극적이고 포괄적인 의미에 이르기까지 사이버 평화 개념을 둘러싼 다양한 해석이 존재하고 있다. 중요한 점은, 사이버 공간이 창출된 이후로 인류가 영위하는 온라인 활동 범위가 비약적으로 확장되었으며, 이에따라 '안전하고 평화적인 사이버 공간'이 갖는 포괄적 의미 역시 한정하기 어려워지고 있다는 점이다. 특히, 증대되고 있는 '신흥안보(emerging security)' 이슈의 부상은 사이버 공간의 평화 개념을 어디까지 확장할 것인가에 중요한 영향을 미치는 주요 변수로 자리잡고 있다. 다시 말해, 사이버 평화에 대한 논의의 시작은 기존의 물리적 세계를 기준으로 국가중심적 시각에서 통용되던 전통적 평화론을 넘어 사이버 공간의 양적·질적 진화를 고려하여 살펴볼 필

요가 있는 것이다.

신흥안보 시대의 사이버 공간이 갖는 위험의 불확실성

사이버 공간은 자연 창발로 형성된 세계가 아니며, 정보통신 기술과 네트워크를 통하여 구축되는 완전한 인공적인 영역이라 볼 수 있다. 거리나 시간의 의미가 물리적 세계에서와는 다르며, 현실세계에서는 중요한 국경이나 국적 등이 사이버 공간 속에서는 의미가 없거나 중요성이 크지 않다. 그렇다고 해서 사이버 공간이 현실세계와 완전히 별개로 존재하는 것도 아니다. 현실세계와 사이버 공간은 서로 밀접하게 결합되어 있어서, 사이버 공간과 현실세계가 존재하고 기능하기 위해서는 상호의 존재와 기능이 필수적이다.[1)]

문제는 평화와 안보에 대한 기존 관념과 전략이 신흥안보 시대의 사이버 공간이 보여주고 있는 양적·질적 변화와 역동성을 충분히 반영하지 못하고 있다는 것이다. '신흥안보(emerging security)' 개념은 시스템 내 미시적 위험 요소가 상호작용을 통해 변화의 임계점을 넘을 때, 다양한 경로를 통해 초국가적 차원의 안보 문제로 확장될 수 있다고 보는 대안적 접근이다.[2)] 특히, 제한적인 하나의 위험 요소가 해당 부문을 넘어 거시적이고 복합적인 안보문제로 증폭되는 동태적 변화에 주목하며, 이 과정에서 발견되는 '양질전화-이슈연계-지정학적 피드백'의 특성을 강조한다.[3)] 최근의 사이버 공간에서는 이 같은 신흥안보적 파급력의 특성이 나타나고 있다. '양질전화(良質轉化)'의 경우, 긴밀히 연결된 디지털 네트워크를 통해 악성코드를 마치 전염병처럼 동시다발적으로 감염시켜 국가안보의 임계점을 넘는 피해를 유발하는 현상이 관찰된다. 지식·정보, 가상자산 탈취, 페이크 뉴스 살포로 인한 사회적 혼란 등은 어느 한 개인이나 집단에 머물지 않기 때문이다. '이슈연계' 측면에서 볼 때, ICT공급망 셧다운, 백신연구기관의 해킹, 전력 제어시스템의 오작동 유발과 같은 공격은 단순한 디지털 공간의 사고에 그치지 않는 경제·보건·에너지·환경 등 물리적 안보 이슈와 결합된다. 마지막으로 이처럼 진화된 사이버 공격은 '사이버 동맹', '디지털 진영화'와 같은 민감한 군사안보적 대응의 결과를 초래한다. 이른바 '지정학적 피드백'으로의 귀결인 것이다. Bloom and Savage 등은 오늘날 사이버 안보 이슈를 유발하는 구조적인 문제와 이에 대한 기술적·제도적 관리의 어려움을 언급하면서, 사이버 안보 환경은 필연적으로 불확실하며, 완벽한 안보는 달성 불가능하다고 주장한 바 있다.[4)] 이 같은 사이버 공간의 속성 하에서 평화를 어떻게 정의하고, 어떤 수준의 사이버평화를 추구하느냐는 실천적 차원에서 중요한 문제가 될 수밖에 없다.

---

1) 한인택, "사이버 공간의 평화적 이용을 위한 이론과 전략의 탐색", (2014), p. 2.
2) 김상배, "신흥안보와 메타거버넌스: 새로운 안보패러다임의 이론적 이해." 『한국정치학회보』, 50권 1호, (2016), pp. 75-104; 윤정현, "신흥안보 거버넌스: 이론적 고찰과 대안적 분석틀의 모색." 『국가안보와 전략』, 제19권 3호, pp. 1-46.
3) 김상배, "신흥안보의 미래전략 2.0: 새로운 연구와 지평의 모색", (신흥안보 라운드테이블, 2022.9.7.)
4) Les Bloom and John E. Savage, "On Cyber Peace", Atlantic Council, (AUGUST 2011) https://www.atlanticcouncil.org/wp-content/uploads/2011/08/080811_ACUS_OnCyberPeace (검색일: 2022.10.31.)

사이버 공간 내 소극적·적극적 평화론 적용의 쟁점

사전적으로 '평화'는 평온하고 화목한 상태로서 전쟁이나 분쟁 등이 존재하지 않는 상황으로 정의된다. 그러나 이 같은 전통적 의미의 평화 개념으로는 복잡성과 다양한 이해관계자가 난립하는 현실에서 평화의 난제를 이해하기 어려워졌다. 즉, 전쟁에까지는 치닫지 않더라도 삶에 지대한 영향을 미치는 변수들을 포착하기 어려워졌기 때문이다.[5] 현실 세계에서의 평화의 개념이 다양하게 존재하는 것처럼 사이버 공간에서의 평화에 대해서도 다양한 시각이 존재할 수 있다. 사이버안보의 목표는 무엇인가? 안보를 통해 달성하고자 하는 목표가 평화라는 데 이의를 제기하기는 어려울 것이다.

평화는 자유와 평등 못지않게 인간이 추구하는 보편적 이상이라고 할 수 있다. 기존의 사이버 평화에 대한 논의는 상당부분 안보화 담론에 기반하여 전개된 측면이 있었다. 특히, 미중 간의 사이버안보 이슈를 다루는 연구들은 양자의 관계를 '사이버 안보화'의 시각으로 조명하는 공통점이 있었다. 그러나 이 같은 관점에 내재된 문제는 아직 존재하지 않는 잠재적 위협을 실체화하거나 파괴력을 과장하기 쉬운 한계를 내재하고 있었다. 또한, 이 과정에서 전문지식이 높은 기술 전문가들이 안보담론을 독점하게끔 허용하는 문제를 낳기도 하였다.[6] 무엇보다도 사이버 위협을 국가안보의 차원에서 접근하는 것은 개인과 사회적 차원에서 직면하게 되는 사이버 위협을 과소평가거나 그러한 위협들까지 국가안보의 시각으로 흡수하는 우를 범할 수 있다. 즉, 사이버 안보는 사이버 평화 논의의 핵심적인 초점이 되어야 하지만, 안보에만 경도된 접근은 국가에 비해 개인과 사회를 부차적인 관심 대상으로 치부할 수 있다는 점을 유의해야 하는 것이다.

사이버안보를 통해 도달하고자 하는 최종 상태를 사이버 공간의 평화라 가정할 경우, 사이버평화에 관한 논의의 시작은 갈퉁(Johan Galtung)의 평화론에서 출발하는 것이 유용할 것이다. 갈퉁은 평화가 폭력이라는 개념과 함께 설명된다고 보았다. 폭력은 '직접적(물리적) 폭력', 구조적 폭력, 그리고 이를 뒷받침하는 '문화적 폭력' 등이 있는데, 단순히 직접적 폭력이 없는 상태를 평화라 보는 시각은 '소극적 평화(negative peace)'에서 벗어나지 못한 것이다.[7] 그는 눈에 보이지 않는 다른 나머지 폭력들 또한 모두 제거한 상태만이 '적극적 평화'를 의미한다고 보았다.[8] 따라서, 전쟁의 부재와 같은 소극적 평화 영역은 불안정한 기반에서만 유지되거나 위협, 폭력적인 능력 부족과 같은 소극적인 수단에 의해서만 유지되는 영역이다. 반면, 안정된 평화의 영역은 상호적이고 합의된 기반 위에서 평화가 유지되는 영역으로 폭력 발생에 대한 기대가 없는 환경을 의미한다.[9]

---

5) 김상배, "신흥안보의 미래전략 2.0", 『신흥안보 이슈리포트 세미나(미발간 자료)』, (2022), p. 1.
6) 정영애(2017), p. 109.
7) Johan Galtung, "Violence, Peace, and Peace Research," *Journal of Peace Research,* Vol. 6, No. 3 (1969), pp. 167-191.
8) 홍용표, "북한의 평화개념과 평화 만들기,", 『JPI PeaceNet』, 제2호, (2021).
9) Inversini(2020), p. 265.

갈퉁의 논의를 사이버 공간에 적용한다면, 소극적 사이버평화는 '사이버전쟁', '사이버테러', '사이버범죄' 등이 부재한 상태라 할 수 있을 것이다. 그런데 사이버평화를 소극적 평화론의 시각에서 보는 것은 진정한 사이버 안보의식을 확립하는데 필요한 규범과 정책을 설명하기에는 충분하지 않다.[10] 가장 큰 문제는 공식적인 '전쟁의 부재'가 왜곡하는 불안정한 현실이라 할 수 있을 것이다. 물리적 환경에서와 같이 '전쟁권(Jus ad Bellum)'의 원칙은 사이버 공간에 그대로 적용되기 어려운데, 전쟁을 선포하려면 적을 규정하고 책임을 귀속시킬 수 있어야하기 때문이다.[11] 물리적 영역과 달리 사이버 공간을 공격자를 식별하는데 더 많은 어려움이 따른다. 대부분의 국가들은 사이버 공간에서 전쟁 행위로 간주될 수 있는 직접적 행동을 조심하지만, 특정 집단을 앞세우고 배후에서 지원할 수 있으며, 실제로 그러한 빈도 역시 증가하고 있다. 따라서, 공식적인 전쟁 선포 없이도 사이버 공간에서는 전쟁과 같은 폭력적 상황에 놓일 수 있는 위험을 안고 있는 것이다.

두 번째 문제는 '직접적 폭력의 부재' 이상의 적극적 평화를 사이버 공간에 적용할 수 있는가에 대한 문제이다. 갈퉁 조차도 모두가 납득할 수 있는 평화와 폭력에 대한 보편적인 정의를 수립하는 것은 비현실적이라 보았다. 사회와 기술이 변화함에 따라 평화와 폭력에 대한 범위와 사회적 이해 또한 변화할 수밖에 없기 때문이다. 이는 특히 가치 판단의 주체를 누구로 설정할 것인가의 문제로 귀결된다. 로프(Heather M. Roff)는 탈냉전과 함께 마주한 사이버 공간의 질서를 인간안보와 적극적 평화의 관점에서 접근할 필요성을 제기하였다.[12] ITU 역시 이같은 맥락에서 사이버 평화를 "건강한 평온함과 무질서, 혼란, 폭력의 부재(wholesome state of tranquility, the absence of disorder or disturbance and violence)"에 바탕한 "사이버 공간의 보편적 질서(universal order of cyberspace)"로 정의한 바 있다. 그럼에도 불구하고 적극적 평화 역시 앞서 언급한 사이버 공간의 속성에서 '무결한 환경'의 달성을 목표로 하는 것은 매우 어려운 문제이다. 매 순간 우리는 인지하지 못하는 가운데도 사이버 공격과 방어의 메커니즘에 끊임없이 마주하고 있다. 또한, 상술한 정의에서 볼 수 있듯이 사이버 평화는 인권, 경제, 안보, 국제협력 등의 여러 측면을 지닌 복합적 현상을 띠게 되며, 이는 일국 차원의 노력만으로 달성할 수 없는 도전이기도 하다. 동시에 개인정보보호 이슈 등 개인 단위에서도 일상에서 마주하는 미시적인 문제들은 끊임없이 제기되는 사안으로서, 이 모든 것들을 포함할 경우, 과잉안보화의 위험성을 피하기 어렵다. 결국, 사이버 평화에 대한 논의는 사이버 공간의 실질적 안전 확보나 이를 위한 실천방안에서 보더라도 단순히 적극적 개념이나 소극적 개념의 구분을 넘어야할 필요성을 제기한다.

가상공존의 초월적 공간이자 과정으로서 사이버 공간의 진화

신흥안보 시대의 사이버 평화 논의를 위한 첫 번째는 사이버 공간의 확장이 갖는 가상·물리

10) Heather M. Roff, "Cyber Peace: Cybersecurity Through the Lens of Positive Peace", (2016), p. 3.
11) Inversini(2020), p. 261.
12) Heather M. Roff, Cyber Peace: Cybersecurity Through the Lens of Positive Peace, (New America org, 2016).

적 구분의 초월성이 낳는 함의점을 포착하는 것이다. 사이버 공간의 확장은 사이버 위협의 양적, 질적 변화를 야기시키고 있다. 이는 사이버 평화의 포괄 범위 역시 이에 부합하여 확장되어야 함을 의미한다고 볼 수 있다. 실제로 최근의 사이버보안 문제는 악성코드 또한 전염병 바이러스처럼 빠르게 복제되는 과정에서 변종이 나타나는 특징을 보이며 이른바 '사이버 팬데믹'의 현실화 위협(랜섬웨어에 의한 동시다발적 국가기반시설 위협, 'Log4j'의 치명적인 보안 취약점 발견 등)을 낳은 바 있으며, 나아가 메타버스 패러다임의 확산으로 가상과 현실의 경계를 초월한 가상융합공존 세계까지 논의되고 있는 상황이다. 나아가 최근의 사이버전 양상은 사이버 전장과 물리적 전장이 상호 긴밀히 연결되고 있으며 무력 공격에 앞선 전초작전으로서의 기능까지 수행하고 있다. 인프라, 금융, 미디어, 정부기관 등에 대한 사이버 공격을 감행, 사회적 혼란을 유발하고 정보·심리전을 통해 적국의 항전 의지를 약화시키는 등 '하이브리드전'의 핵심으로 기능하고 있는 점이 이를 설명해준다.[13)]

사이버 평화론의 발전을 위해 두 번째로 주목할 점은 사이버 활동이 갖는 이슈연계 측면의 파급력이다. 사이버물리시스템의 원격·제어를 통해 감행되는 사이버 공격의 피해는 물리적 공간인 물적·인적 피해로 이어질 수 있다. 지금까지 별개의 영역으로 간주하였던 사이버 공간에서 기원한 위험이 현실세계의 연계·비연계 영역으로까지 전이되는 현상들이 빈번하게 목도되고 있다. 일례로 코로나19 국면 이후, 소프트웨어 해킹을 통한 주요 정보 유출, 백신 연구기관을 대상으로 백신개발 정보를 탈취하려는 사이버 첩보활동이 본격화되었으며, 이는 사이버 안보이슈를 넘어 감염병 통제와 관련된 보건 안보를 위협하는 양상으로 나타났다. 실제로 당시 중국의 배후로 의심받고 있는 해커 집단의 미국 내 사이버공격은 주로 백신 등 핵심 기술과 지식재산권, 정보 탈취 목적을 위한 소행으로 분석되었다. 뿐만 아니라 2020년 12월 백신과 치료제 연구개발 중인 '존슨앤존슨', '노바백스' 등 6개 제약사가, 2021년 2월에는 화이자가 북한으로 의심되는 사이버공격을 받기도 하였다. 에너지 안보 측면에서는 러시아 배후로 추정되는 콜로니얼 파이프라인(Colonial Pipeline) 공격이 감행되자, 미국 동부 지역 전체가 랜섬웨어 공격 때문에 연료를 공급받지 못하게 되는 초유의 사태 발생하였으며, 전력 및 제조 부문 기업의 산업 제어시스템이 치명적 피해를 입기도 하였다. 이 같은 변화들은 연계 신흥안보 위협의 연계 지점으로서 사이버 공간의 복합화를 낳고 있다.

세 번째 검토해야할 부분은 '과정'으로서의 사이버 평화를 지향해야 한다는 점이다. 가변성과 불확실성을 상정하는 신흥안보적 패러다임에서는 주요 위험이슈들이 직간접적 연계를 통해 거시적 안보문제로 증폭되는 동태적 양상에 주목한다. 또한, 최근 나타나고 있는 안전한 사이버 공간 구현을 위한 기술·제도적 보완 역시 이 같은 흐름과 궤를 같이 하고 있다. 다양한 참여자들이 끊임없이 정보를 공유함으로써 불신을 해소하고, 안정화된 시스템으로 개선해나갈 수 있도록 지속가능한 유인을 제공하는데 초점을 두고 있는 것이다. 이는 사

13) Microsoft, "Special Report: Ukraine: An overview of Russian's cyber attack activity in Ukraine", (April 27, 2022), p. 7.

이버 공간에서의 평화 또한 궁극적으로 달성해야하는 어느 한 지점으로 보기보다는, 역동적인 변화에 발맞춰 진화해가는 동태적 과정으로 볼 수 있음을 시사한다. 유사한 맥락에서 최근 사이버 범죄를 예방하기 위한 국제 규범들은 개인정보보호 뿐만 아니라 이해당사자들의 올바른 활용 가이드라인을 구체화함으로써, 규제와 진흥을 균형적으로 추진할 수 있도록 하고 있다.[14] 즉, 보다 안전하고 지속가능한 사이버 생태계의 건강성 유지에 방점을 둔 것이다. 이를 위해, 정부와 민간 사이의 원활히 작동하는 다중심적(polycentric) 파트너십의 형성 또한 사이버 평화를 유지해가는 주요한 기제라 볼 수 있다.

결론: 사이버 공간의 진화를 반영한 '신흥 사이버 평화론'의 필요성

팬데믹과 4차 산업혁명이 촉발한 디지털 전환의 심화는 일상과 분리될 수 없는 새로운 활동 영역으로서 사이버 공간의 중요성을 부상시켰다. 특히, 가상과 현실이 융합하고 이슈간 경계를 허물고 있는 사이버 공간의 진화는 사이버 안보 뿐만 아니라 사이버 평화의 개념에 대해서도 새롭게 접근해야할 필요성을 제기한다. 이를 위해 우리는 신흥안보적 관점에서 기존의 물리적 세계에서 통용되던 적극적 차원, 소극적 차원의 평화 논의를 넘어설 필요가 있다. 사이버 활동 범위의 확장과 새로운 가치의 구현, 사이버 공간과 물리적 공간의 경계 소멸, 동태적 과정으로서의 사이버 평화를 바라보는 시도는 그 첫 번째 실천이 될 것이다.

이 같은 맥락에서 사이버 안보의 대척점으로 사이버 평화를 바라보는 시각은 분명 한계를 갖지만, 이들을 완전히 분리해 접근하는 태도 역시 바람직하지 못하다. 사이버 공간의 진화는 양자가 서로 다른 세계가 아닌 하나의 '연속체(a continuum)'일 수 있으며, 이 연속체의 안에서 다양한 형태의 폭력과 갈등이 내재되는 동시에, 반대의 측면에서는 다양한 행위주체 간 합의와 신뢰구축, 규범화의 노력 또한 이루어질 수 있음을 시사하기 때문이다. 중요한 점은, 복잡화되고 진화해가는 사이버 공간을 안전하게 구현할 수 있도록 어떠한 실천적 노력을 기울일 것인가이다. 美백악관 국가사이버국장 Chris Inglis의 언급처럼 "21세기의 인류는 사이버를 위해 존재하는 것이 아니라 사이버 때문에 존재"하기 때문이다. 사이버 공간은 개인, 기관, 기업, 사회, 국가 등 사이버에 의존하는 모든 이들이 영위하는 활동들을 뒷받침하기 위해서이다.[15] 신흥 사이버 평화의 논의는 이 같은 당위적 명제에서 출발해야 할 것이다.

14) Shackelford(2013), https://ndias.nd.edu/news-publications/ndias-quarterly/the-meaning-of- cyber-peace/ (검색일: 2022. 11. 20.)

15) Chris Inglis, "Cyberspace Democratic Values, and National Efforts", *International Conference on GCPR 2022,* (2022. 9. 15.), https://www.youtube.com/watch?v=YBJZ0glZo50 (검색일: 2022.11.3.)

저자소개

윤정현 박사는 현재 국가안보전략연구원의 부연구위원으로 과학기술정책연구원 선임연구원 및 대통령직속 국가과학기술자문회의의 전문위원을 지냈다. 서울대학교 대학원에서 외교학 석사, 박사 학위를 받았다. 과학기술과 국제정치를 아우르는 학제간 융합 연구에 많은 관심을 갖고 있으며, 주요 논문으로는 "메타버스 공간에서의 남북 교류 가능성에 대한 고찰" (세계지역연구논총, 2022), "Governance on COVID-19 as Emerging Security Challenges" (Korean Political Science Review, 2022), "Issues and Prospects of Artificial Intelligence Utilization in the Defense Field" (Korean Journal of Defense Analysis, 2021), "신흥안보 위험과 네트워크 거버넌스" (한국정치학회보, 2020), "인공지능과 블록체인의 도입이 사이버 안보의 공수 비대칭 구도에 갖는 의미" (국제정치논총, 2019) 등이 있다.

2022년 12월