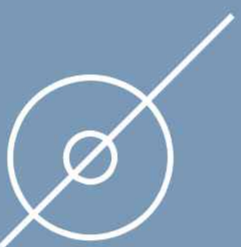
사이버 안보와 평화



2023

한국사이버안보학회
KACS

한국사이버안보학회 KACS

한국사이버안보학회 워킹페이퍼 13호
발간일: 2023년 12월 29일

윤정현 (국가안보전략연구원)

〈요 약〉

최근 급변하는 사이버 공간의 진화는 현실 세계와 마찬가지로 사이버 세계에서도 안정과 평화가 인류의 번영에 필수적임을 시사한다. 실제로 사이버 공간은 지속적으로 확장되고 있으며 기술 및 사회 발전을 주도하는 원동력으로 기능하는 한편, 새로운 불안과 위협요소와도 마주하고 있다. 이 같은 사이버 공간이 양적 팽창 뿐만 아니라 질적 변화 역시 가속화되고 있기 때문이다. 그러나 사이버안보 문제에 대한 관심과 대응 노력에 비해 사이버 공간의 안정과 평화라는 보다 궁극적인 목표에 대한 심도 있는 논의는 좀처럼 다루어지지 않았다. 특히 사이버 공간은 물리적 세계와 구별되는 다이내믹스와 확장, 초월적 특징 등은 이에 대한 신중한 검토를 요구한다. 따라서 본 연구는 사이버 영역의 특성과 작동 메커니즘을 고려한 이론적 분석을 시도하고, 이를 통해 사이버 평화를 위한 대안적 실천 사항들을 살펴보고자 하였다. 여기에는 고려해야할 행위 주체의 다변화, 동태적 시각에서의 사이버 평화 모색, 지속가능성을 고려한 사이버 복원력 등이 포함된다. 사이버 안보 개념이 국제정치학에서 체계적인 연구 대상으로 자리 잡기까지 오랜 시간이 걸렸듯이, 사이버 평화 역시 개념을 정교화하고 의미 있는 논의의 틀을 구축하기 위해서는 더 많은 사례연구와 실천이 필요할 것으로 전망된다.

Ⅰ. 머리말

오늘날 인류의 의존성이 절대적으로 증대하고 있는 사이버 공간은 기술과 사회의 발전을 주도하고 있으며 끊임없이 변화하고 있다. 사용자 간 연결성이 강화되고 있다. 나아가 양적, 질적 확장 또한 가속화되는 중이다. 무엇보다도 디지털 전환의 심화에 따라 상호 영향력이 증대됨으로써 사이버-물리세계 간의 경계가 허물어지는 현상 또한 관찰된다. 그 결과 오늘날 사이버 세계는 기존의 온라인 세계에 대한 의미를 넘어 보다 확장된 공간으로서의 개념적 접근이 필요해지고 있다. 나아가, 이러한 확장에 따라 기존의 온라인 세계에 한정되어 있던 사이버 위협 또한 보다 확장적인 의미를 가지며 진화하고 있다.

즉, 사이버 공간에 대한 복잡성과 위협이 증대되고 비물리적 뿐만 아닌 물리적 공간에까지 영향을 미치게 되면서, 군사안보에 비해 부차적 사안으로 다뤄졌던 사이버 위협 이슈가 이제는 평시와 전시를 가리지 않고 주목받고 있는 것이 현실이다. 하이브리드전 형태의 통합적 작전 뿐만 아니라 EMP 공격과 같은 공격 또한 이제는 살상무기만큼이나 심각한 이슈로 제기되는 중이다. 하지만 이와 같은 사이버 안보 이슈를 향한 관심과 대응 노력에 비해 보다 궁극적 목표라 할 수 있는 사이버 공간의 안정성, 나아가 사이버 평화에 실천적인 논의는 거의 부재한 실정이다. 물론, 물리적 세계의 평화 개념을 사이버 공간에 대입하여 시사점을 짚어본 일부 연구들이 존재하나(Bloom & Savage, 2011; Inversini, 2020), 사이버 공간이 갖는 동태적 확장성과 초월적 특징이라는 물리적 세계와의 차별성을 면밀히 고려하여 검토한 시도들은 찾기 어렵다. 또한, 사이버 공간의 작동 메커니즘을 지정학적 혹은 탈지정학적 시각으로 재해석한 접근이 있으나(Alperovitch 2022; 나용우 2022). 물리적 공간과 본질적으로 구별되는 사이버 공간의 특성과 구성 원리에 초점을 두기 보다는 안보 및 '전장(warfare)'으로서의 유의미성에 보다 집중하는 경향이 있다.

또한, 비물리적 세계의 '사이버'와 물리적 세계의 '평화'라는 다른 영역의 분리된 두 개념을 접합하여 사용하고 있는 경우가 대부분일 뿐, 사이버 평화에 대한 심층적 논의는 충분히 이루어지지 못하였다. 특히, 기존 연구들은 급속한 기술발전에 따라 양적·질적 측면에서 진화하고 있는 사이버 공간의 창발적 현상들과 그 의미를 면밀히 고찰하지 못한 부분이 존재한다. 사이버 공간이 창출된 이후로 인류가 영위하는 활동 범위는 비약적으로 확장되어온 만큼, '안전하고 평화적인 사이버 공간'이 갖는 포괄적 의미는 점차 한정하기 어려워지고 있다. 여기에 양질전화와 이슈연계, 창발적 특징에 기반한 사이버안보의 '신흥안보(emerging security)'적 양상의 흐름은 사이버 공간의 평화 탐색을 위해 일반론으로서의 평화 개념을 접목시키는 시도에 대한 적실성의 문제를 제기하는 중이다. 즉, 사이버 평화에 대한 논의의 시작은 기존의 물리적 세계를 기준으로 국가중심적 시각에서 정태적으로 통용되던 협소한 관점을 넘어, 사이버-물리 공간의 경계 초월과 다양한 주체와 이슈간 연계, 동태적 특징을 반영한 평화 개념의 도입이 필요함을 시사한다.

그렇다면 이 같은 사이버 공간의 진화적 특징을 고려한 사이버 평화 개념은 어떻게 살펴봐야 하는가? 보다 현실적인 대안적 접근방향은 무엇인가? 본 연구는 이에 대한 질문에 대한 답하고자 한다. Ⅱ장에서는 기존 사이버 평화 논의의 쟁점과 한계점을 검토한다. 물리적 세계를 상정한 평화 개념의 접근이 지닌 구조적 문제와 사이버 전쟁의 대척점으로 바라본 협소한 시각들을 비판적으로 고찰하는 한편, 사이버 공간 속 평화의 확장적 특징이 부재함을 짚어볼 것이다. 이를 토대로 Ⅲ장에서는 대안적 '사이버 평화' 개념을 제시하기 위해 국제정치이론의 관점에서 사이버 영역의 특징과 작동 메커니즘을 고찰한다. 주류 이론이라 할 수 있는 지정학 기반의 현실주의적

접근으로 설명할 경우 나타나는 문제점과 대안적 시각으로서 네트워크 이론에 기반한 탈지정학적 접근의 유용성을 검토하고자 한다. 나아가, 사이버 평화 실현을 위한 조건과 주요 가치로서 앞 장의 이론적 검토에 근거하여 사이버 평화를 실현하기 위한 주요 조건들을 제시하고자 한다. 이를 통해 결론에서는 사이버 평화를 실현하기 위한 주요 가치로서 향후에 다뤄야할 사안들을 짚어보기로 한다. 나아가 본 연구가 갖는 의의와 한계 뿐만 아니라 후속 논의에서 검토할 몇 가지 방향들을 제시하며 글을 마무리하고자 한다.

Ⅱ. 선행연구 검토

오늘날 전통적 의미의 평화 개념으로는 더 이상 복잡성과 다양한 이해당사자가 난립하는 현실에서 발생하는 평화의 난제를 이해하기 어려워졌다. 갈퉁(Johan Galtung)에 따르면 소극적 평화는 부정적인 무언가가 없는 상태(without), 적극적 평화는 무언가가 없는 상태를 넘어 기본적으로 긍정적인 무언가가 보장된 상태(with)를 의미한다(Galtung, 1969). 그의 논의를 사이버 공간에 적용한다면, 소극적 사이버 평화는 '사이버 전쟁', '사이버테러', '사이버범죄' 등이 부재한 상태라 볼 수 있다. 그러나 이 같은 물리적 환경에 기반한 개념적 특징들은 사이버 공간에 그대로 적용되기 어렵다. 예를 들어, '전쟁권(Jus ad Bellum)'의 경우, 전쟁의 선포에는 명확히 규정되고, 책임을 귀속시킬 수 있는 '적'이 존재해야 한다(윤정현·이수연, 2023: 5). 그러나 물리적 영역과 달리 사이버 공간은 명시적인 공격자를 식별하는 것이 불가능한 경우가 대부분이다. 공격 대상과 공격의 목표 등을 명확하게 구분할 수 없는 상황에서 물리적 공간에서와 같은 기준으로 전쟁의 시작이 언제인지 파악하는 것은 무의미해진다. 오히려, 공식적인 전쟁 선포 없이도 사이버 공간에서는 전쟁과 같은 폭력적 상황에 놓일 수 있는 위험이 상존하며, 실제로 치열한 사이버전(cyber wafare) 역시 물리적 공격을 함께 수반하는 예외적인 경우를 제외하고는 암묵적으로 벌어진다. 이는 사이버 공간에 소극적 평화 개념을 그대로 원용하는 데에 한계가 있다는 것을 의미한다.

이 뿐만 아니라 '직접적 폭력의 부재' 이상의 적극적 평화를 사이버 공간에 적용할 수 있는가이다. 모두가 받아들일 수 있는 평화와 폭력에 대한 보편적인 정의를 수립하는 것은 갈퉁 역시 비현실적이라 보았다(Galtung, 1969). 사회와 기술이 변화함에 따라 평화와 폭력에 대한 범위와 사회적 이해 또한 변화할 수밖에 없기 때문이다. 또한, 부정적인 상태가 제거되고 기본적으로 보장되는 무언가를 사회적으로 합의하는 데 있어 가치 판단의 개입은 필연적이다. 그러나 여기에는 가치 판단의 주체를 누구로 설정할 것인지의 문제를 수반하게 된다. 결국, 적극적 평화 역시 앞서 언급한 사이버 공간의 속성이 '무결한 환경'의 달성을 목표로 하는 것은 비현실적이며, 달성하기 어려운 문제이다. 특히, 앞서 언급한 것처럼, 디지털 세계에서 우리는 언제나 인지하지 못하는 순간에도 사이버 공격과 방어의 메커니즘에 끊임없이 노출되어 있다. 그것이 체감할 수 있는 임계점에 도달하지 못했을 뿐이다. 이는 적극적 평화의 기본 전제가 되는 부정적 상태를 해소하려는 시도조차도 쉽지 않음을 의미한다.

나아가 사이버 평화는 인권, 경제, 안보, 국제협력 등 초국가적이며 거시적 측면을 지닌 특징뿐만 아니라 개인정보보호 이슈 등 개인 단위에서도 일상에서 마주하는 미시적인 문제들까지도 포괄해야하는 대단히 복합적이고 다차원적인 조건을 만족시켜야 하는 사안일 수도 있다. 그러나 이 모든 것을 포함한다는 것은 달성하기 어려운 문제이자 과잉 안보화로 위험으로 귀결될 위험

성을 내포한다. 또한, 소극적·적극적 평화 개념이 담을 수 없는 사이버 평화의 사각지대 역시 존재할 수 있다. 사이버 평화 논의는 사이버 공간의 실질적 안전 확보나 이를 위한 실천적 측면에서 보더라도 물리적 세계의 적극적·소극적 개념의 구분을 넘어서야 할 필요성을 제기하는 것이다.

둘째, 사이버 공간은 근대적 공간이라기 보다는 탈근대적 속성을 보이는 공간이다. 이를 고려할 때, 우리는 사이버 평화 개념에 대한 본격적인 논의에 앞서 사이버 공간의 특징과 작동 메커니즘에 대해 검토할 필요가 있다. 불충분한 논의 속에서 '사이버 평화'는 어렴풋이 '사이버 전쟁(cyber war)'의 대척점에 있는 개념 정도로 간주되어 왔다(Inversini 2020, 264). 그러나 이 같은 이분법적 구분은 실제 사이버 공간을 둘러싼 작동 메커니즘을 충분히 설명하지 못하며, 논의의 폭을 대폭 한정시킬 수 있다.[1] 심지어 국가 및 국가에 준하는 정치집단, 또는 이들을 지지하는 개인이 정치적 의지를 달성하기 위해 수행하는 다양한 교란, 첩보, 파괴, 선전, 조작 행위 등 '사이버전(cyber warfare)'과 관련된 직간접적 활동(박동휘, 2022: 56) 조차 다루지 못하는 협소한 논의에 머물 수 있다. 실제로 국가 간 폭력적 대립, 갈등 전반을 의미하는 'war'의 하위 개념인 'warfare'는 '화생방전', '전자전'처럼 사이버 전쟁을 수행하는 메커니즘, 방법론 등을 의미하기 때문에(NATO, 2019), 이들은 명시적인 폭력으로 드러나기도 하지만, 정보심리전과 같이 표면적인 평화를 가장한 형태로도 발현된다(RAND 2023).[2] 즉, 긴장과 갈등마저도 인지하지 못하는 고도로 은폐된 상태로도 존재할 수 있는 것이다. 이 같은 가능성은 사이버 평화를 단순히 사이버 전쟁의 대척점으로 바라보는 접근이 내재한 설명력의 한계를 보여준다. 특히, 근대 국제정치에서 안보 개념은 무엇보다도 국가의 생존을 전제로 하고 있는데, 사이버 안보는 국가의 생존에 한정하여 볼 수 있는 문제인지도 의문이다. 그렇다면 사이버 공간에서 국가의 생존도, 인간의 생존도 위협하지 않고 치열하게 벌어진 공격행위가 발생하면 이는 안보가 부재한 상황이라고 볼 수 없는 것인가? 근대적 이분법적 구조에서 생존에 위협을 받지 않았으니 평화 상태에 있는 것인가? 공간의 성격이 바뀌었으니, 근대에 정의된 생존의 문제로만 제한해서 안보의 문제를 바라보는 접근은 적절하지 않은 것이다.

사이버 평화 논의에서 중요한 또하나의 쟁점은 사이버 안보와 평화와의 관계성이다. 평화 상태를 당연한 것으로 영위할 수 있는 상태에서는 평화에 대한 개념적 정립의 필요성을 인식하지 못한다. 평화가 부재한 상황, 즉 안전을 보장해야 하는 필요성이 절실함을 인식하는 순간부터 평화는 인지되기 시작한다. 이러한 이유로 안보와 평화 개념은 상호 분리할 수 없는 관계로 형성되어 왔다. 실제로 안보는 평화를 위한 필요조건으로 간주되며 평화적 상태로 나아가기 위해 우선적으로 달성되어야 하는 단계와 등치되기도 한다. 따라서 평화 논의의 시작에는 평화와 안보의 관계에 대한 검토가 필요하다. 일반적으로 국제정치에서 안보는 생존과 긴밀하게 연결되어 있다. 잘 알려진 대로, 홉스(Thomas Hobbes)는 자연 상태를 "만인의 만인에 대한 투쟁" 상태로 보면서 이것이 바로 안보 부재의 근원이자 죽음에 대한 두려움으로 연결함으로써 안보를 생존의 문제로 만들었다(민병원 2012, 208). 즉, 근대적 개념의 안보는 생존과 연계되어 있는데, 이를 사이버 공간에 그대로 가져갈 경우, 사이버 안보도 생존을 전제로 해야지만 안보화될 수 있느냐의 문제가 발생하게 된다.

전쟁이나 분쟁이 없더라도 인간의 삶을 혹은 세계를 뒤바꿀 만한 변수들은 다양하게 존재하므로, 평화를 좁게 정의할수록 현실의 문제를 해결하는 것은 어려워질 수밖에 없다. 과거 미국은

1) NATO. "Cyberwar: does it exist?" (June 13, 2019); 박동휘, 『사이버전의 모든 것』, (서울: 플래닛 미디어), p. 56.

2) https://www.rand.org/topics/cyber-warfare.html

9.11 테러에 직면했을 당시 '테러와의 전쟁'을 통해 평화를 해치는 폭력 행위에는 그에 상응하는 폭력 행위로 대응하겠다는 의지를 표명한 바 있다. 이와 유사한 맥락에서 지난 20여년 간 발표된 미국의 사이버전략은 단순한 대응에 그치지 않고 잠재적 위협요소에 대한 불안정성을 적극적으로 해소하기 위한 방향으로 발전해왔다. 2003년 부시 행정부는 최초의 국가사이버안보 전략인 '안전한 사이버공간을 위한 국가전략(National Strategy to Secure Cyberspace 2023)'의 경우, 사이버 공격에 대하여 자국 이익에 미치는 해악에 비례하는 무력으로 대응하겠음을 천명한 바 있다(US DHS, 2003). 동 전략은 미국 정부의 최초 사이버안보 전략으로 민관협력 체계 구축과 사이버사고 대응을 위한 연방차원의 대응계획을 수립하는데 기여한 것으로 평가된다(김소정, 2023: 2-3). 2018년에는 2003년 사이버안보 전략을 개정한 '국가사이버전략(National Cyber Strategy)'을 발표했는데, 여기에는 사이버 공격에 대한 '전략적 억지력' 달성을 강조한 점이 특징이다. 가장 최근인 2023년 3월 발표된 국가사이버안보 전략은 보다 광범위해진 사이버안보 확보 영역을 구체적으로 열거했으며(The White House. 2023), 주요 정보통신 기반시설과 공급망 보호, 신기술 발달에 따른 국가안보 강화 방안 및 보안 생태계 구축, 민관협력 강화 등이 명문화되었다(김소정, 2023: 2-3).

세 번째 주목해야할 부분은 기존 사이버 평화 논의가 주로 정태적 평화개념에 기반한다는 점이다. 케네스 볼딩(Kenneth Boulding)은 갈퉁의 평화 개념이 정적인 차원에 지나치게 초점을 맞춤으로써 동적인 진화 과정을 간과한다고 비판한 바 있다(민병원 2023, 10). 이는 갈퉁의 평화 개념이 단선적 확장에만 머물렀기 때문에 제기된 비판이기도 하며, 사이버 공간에 적용해 본다면, 공간이 확장된다고 하여 그 공간에서의 평화 개념이 단순히 외연을 확장하는 데서 그치는 것이 맞을지에 대한 의문으로 연결된다. 공간이 단순히 양적으로만 확장하지 않고 질적으로도 진화한 만큼 그 공간에 대한 평화 개념의 정립을 위해서는 단선적 확장이 아닌 사고의 전환이 필요한 것이다. 볼딩에 따르면, 세계에서 발생하는 동적인 변화들은 무한 생존경쟁이 아니라 오히려 공존하기 위한 상황에서 피할 수 없이 나타날 수밖에 없는 상호 작용으로 이해되어야 한다(민병원 2023, 10). 정적인 상태를 포착하려는 사고에서 동적인 과정을 이해해 보려는 시각으로 보는 각도를 달리 해보는 것이다.

이러한 관점에서 최근 진행되고 있는 평화 개념 연구에서 주목해 볼 만한 개념들이 있다. 먼저, "일상적 평화(everyday peace)"이다. 이는 기존에 구조적이고 거시적 차원에서 평화 논의가 진행됨에 따라 간과되었던 미시적 수준의 개인적이고 평범한 평화까지 아우른다는 점에서 의미가 있다. 미시와 거시를 단순히 이분법적으로 접근하지 않으며 미시와 거시의 관계를 구성하는데 초점을 맞추고 있으며, 이는 '신흥평화'라는 개념을 내세워 새롭게 제기되고 있는 논의에서 말하는 창발(emergence)과도 연결된다(허지영 2022, 180-181; 김상배 2023, 236). 다음은 "양질의 평화(quality peace)" 개념이다. 기존의 주류 국제정치이론에서 국가들은 자력구제(self-help)를 위하여 폭력을 사용할 수밖에 없음을 주장하였기에 여기서 평화는 과도기적으로 존재할 수밖에 없는 개념이었다. 하지만 양질의 평화는 다양한 형태로 존재하는 폭력을 넘어서고 그 상태를 '지속'하는 데에 초점을 맞추고 있다. 이는 신흥안보와 신흥평화 논의에서 복잡계 이론을 원용하여 제시하는 '항상성 유지'와도 맥을 같이 한다(서보혁 2022, 108-109; 김상배 2023, 241).[3] 따라서 우리는 물리적 공간과 대별되는 사이버 공간의 특징을 국제정치이론의 시각에서

3) 김상배는 탈근대 시대의 복합적 안보위협의 창발 속에서도 환원적 제어를 부과하는 상호작용이 발생함으로써 시스템의 안정성을 유지하는 현상이 나타나고 있다고 보았다. 그리고 이를 자기조직화의 메커니즘에서 생성되는 '항상성(恒常性)'의 개념으로 설명한다. 김상배, "신흥평화의 개념적 탐구: '창발(emergence)'의 시각에서 본 평화연구의 새로운 지평", 『한국정치학회보』, 57집 1호 2023 봄, p. 225.

살펴보고 평화 개념의 의미를 폭넓게 고찰할 필요가 있다.

Ⅲ. 사이버 공간의 구성원리에 대한 국제정치적 시각

1. 현실주의적 접근

따라서 우리는 사이버 평화를 정의하기에 앞서 '평화' 개념이 적용되는 사이버 세계의 물리적 공간과의 차별적 특징에 대해 우선적으로 살펴봐야 한다. 현실 세계 혹은 물리적 공간을 암묵적으로 전제해 왔던 평화 논의에 사이버라는 조건 개념을 접목시킬 경우 앞서의 전제들과 구분되는 사이버 공간의 특징을 이해할 필요가 있다. 그렇다면 사이버 공간과 물리적 공간 사이에는 어떠한 차별점이 존재하는가? 사이버 평화의 개념 논의는 이러한 질문에서 출발해야 한다. 국제정치를 설명하는 다양한 패러다임 중, 현실주의 이론은 물리적 공간에 대한 시각을 가장 잘 대변해왔던 접근이었다. 특히, 지정학의 중요성과 국제정치 구조의 메커니즘을 강조해온 현실주의 이론은 물리적 공간의 특성을 이해하는 데 중요한 인식론적 틀을 제공해왔다(Flint 2017, 45).[4] 예를들어, 구조적 현실주의는 주권을 통해 형식적인 평등을 누리고 있는 근대 국가들의 관계를 단위 간 위계가 존재하고 기능이 분화된 국내 정치와 구분하여 무정부 상태에 단위들의 기능이 분화되어 있지 않은 상태로 설명한다(Waltz 1979, 88-97). 또한, 국가들이 불평등한 상태에 있다고 느껴 위계가 존재하는 것이 아닌지에 대한 의문에는 '구조 내 힘의 배분 상태'로 설명을 대신하고 있다(전재성 2014, 8-9). 이처럼 국가 단위로 구성되어 있는 국제체제를 무정부 상태로 규정하고 있지만 진정한 의미에서의 무정부 상태는 사이버 공간의 조직 원리에 해당하는 것일 수도 있다. 국가는 주권을 가진 상위의 '권위체(authority)'라고 볼 수 있는데, 사이버 공간에는 주권의 기본 전제가 되는 물리적 영토부터 존재하지 않으므로 문자 그대로 '무정부' 상태에 있기 때문이다. 물론 근대 주권 국가의 틀 안에서 기술의 발달에 따라 새롭게 창조된 공간이 사이버 공간이다 보니, 기존의 근대적 발상을 뛰어넘지 못하는 한계가 존재할 수밖에 없는 것은 사실이다. 주권을 가진 국가가 사이버 공간에서 영토 개념에 근거한 관할권을 행사하려 하는 것이 대표적이다. 영토의 경계가 명확히 존재한다고 보기 어려운 사이버 공간에서 발생한 문제를 영토 개념을 전제로 한 방법을 통해 접근한다면 모순이 발생할 수밖에 없다.

제국주의 등을 통해 영토를 확장하는 것이 가능하던 시대에서조차도 물리적 공간의 영토는 제한적이었으며, 첨단기술의 발달로 우주, 해저 등 인간이 물리적으로 경험할 수 있는 공간이 확장된다고 하더라도 사이버 공간의 확장성과는 구분된다는 점을 인식할 필요가 있다. 따라서, 물리적 영토가 존재하지 않는다는 이유로 사이버 공간을 완전한 무정부 상태라고 정의하는 것 역시 문제를 내포하고 있다. 무정부성 역시 질서를 구성하는 원리 중 하나의 형태라고 할 수 있기 때문이다. 영토에 근거한 근대적 개념인 무정부성을 적용할 수 없다는 것이 무질서로 연결되지 않는다는 의미이다. 무정부적 상태 개념 역시 근대 국제질서의 발상에서 연원하였으며, 탈근대 패러다임으로 사이버 공간을 이해하는 것은 또다른 차원의 문제이기 때문이다. 물리적 세계와는 다른 또 다른 세계로 지칭하는 점에서 알 수 있듯이, 사이버 세계는 기술 발전에 따라 무한하게

4) 지리학, 특히 정치지리학에 기반하고 있는 지정학(geopolitics)는 '정치적 공간'의 유기체와 그 구조를 탐구하는 관한 학문이라 할 수 있다. 지리적 관점에서 이해된 지역의 본질은 지정학의 틀을 제공하기 때문이다. Colin Flint, *Introduction to Geopolitics,* 한국지정학연구회 역, 『지정학이란 무엇인가』, (서울: 도서출판 길, 2007), p. 45.

확장될 수 있으며, 엄연히 자체의 논리가 적용되는 영역(domain)으로서 존재할 수 있다.

즉, 현실주의는 국제체제 내 실질적인 불평등 관계를 설명하기 위하여 힘의 배분 상태를 제안한다. 그리고 국가 간 힘의 배분 상태는 구조의 안정성을 결정하는 변수가 된다. 근대의 이분법적 사고의 틀 속에서 구조가 불안정하여 갈등이 발생한 상태를 전쟁 상태라고 한다면, 그 반대인 안정된 구조는 평화 상태를 의미한다고 볼 수 있다. 따라서 구조적 현실주의 이론에서는 주로 힘이 배분된 현재의 상태에 주목하며, 어떻게 힘이 배분되어 있을 때 구조가 안정적인가에 관심을 가진다. 즉, 단극, 양극, 다극과 같은 극성(polarity)에 초점을 맞추어 설명하며, 여기서 파생되는 개념 중 대표적인 것이 세력균형이라고 할 수 있다.

현실주의의 논의를 그대로 사이버 공간에 다시한번 적용해보았을 때, 사이버 공간에는 극성이 존재한다고 할 수 있을까? 풀어서 설명하자면, 국가라는 명확한 행위자가 존재하고, 이 국가들의 힘의 배분 상태에 따라 강대국과 약소국이 구분되며, 강대국의 수에 따라 극성이 구분되는, 균형의 여부와 안정성의 여부를 파악할 수 있는 '힘의 배분 상태'라는 것이 사이버 공간상에 존재하는가? 존재한다면 현실 세계와 일치하는가? 만약 힘의 배분 상태 혹은 극성이 존재하지 않는다면, 왜 현실 세계와 차이가 발생하는 것이고, 무엇이 이러한 차이를 유발하는 것인가? 결론부터 말하자면, 사이버 공간에서 힘의 배분 상태는 존재할 수 있으며, 이는 현실 세계와 일치하지 않을 수 있다. 그 이유는 다음에서 찾을 수 있다. 먼저, 힘의 배분 상태에 대한 논의는 공간을 구성하는 행위자를 전제하고 있다. 또한 현실주의의 시각을 그대로 원용하는 경우, 그 행위자는 당연히 국가이다. 하지만 사이버 공간에서의 행위 주체는 국가로 한정되어 있지 않다. 또한 물리적 공간에서 '힘'을 구성하는 요소와 사이버 공간에서 '힘'을 구성하는 요소는 다를 수 있다. 이를 잘 보여주는 것이 '기술 진보의 역설(a paradox of technological advance)'이다. 현실 세계에서 군사력과 경제력이 국가가 가진 힘을 판단하는 척도라면, 오히려 이러한 힘을 가진 국가일수록 사이버 공간이 발달되어 있어 저강도의 사이버 공격에도 대규모 피해를 겪을 수 있기 때문이다(나용우 2022, 2).

2. 네트워크 이론의 대안적 시각

반면, 탈근대 패러다임의 국제정치 이론 중 네트워크 이론은 위계성 여부에 매몰되거나 영토기반 개념에 천착하지 않으면서 사이버 영역의 특징을 잘 설명해 준다. 네트워크는 링크의 맺고 끊기가 유연하므로 끊임없이 형태를 바꿀 수 있으며 영토적 크기나 경계에 구속받지 않는다. 오히려 강한 연결고리를 많이 보유한 노드가 얼마나 중심성을 확보할 수 있는가가 네트워크 세계에서의 위계성을 결정짓는 변수가 되기도 한다(김상배 2008, 53-55). 또한, 네트워크 환경에서 발생하는 이들 분야의 권력은 행위자들이 보유한 자원이나 속성보다는 행위자들이 벌이는 상호작용의 맥락에서 작동한다는 특징을 지닌다. 다시 말해, 단순히 군사력과 경제력과 같은 자원권력에 의지하는 게임이 아니라, 정보·지식·문화·커뮤니케이션 등과 같은 비물질적 자원을 기반으로 작동하는 양상들을 잘 드러내준다(윤정현 2020, 43).

국제정치에서 가장 쉽게 접할 수 있는 현실주의에서 공간의 특성을 설명하기 위해 제시한 개념들을 통해 사이버 공간이 물리적 공간과의 성격이 다른 새로운 공간임을 확인할 수 있었다. 사이버 공간은 그 자체로도 새롭게 창조된 공간이지만 이후에도 계속해서 진화해온 공간이라고 할 수 있다. 공간이 고전 지정학의 전유물이 아닌 탈지정학적 성격을 띨 수 있음을 보인다. 예를 들어, 과거에 거대한 기업들은 대규모 시설과 대규모 인력 등이 필요했지만 현재의 구글이나 메타 등과 같은 거대 기업들은 사이버 공간, 즉 디지털 기반으로 활동하며, 물리적 시설 및 자산은

이전보다 적게 소유하면서 인간에 대한 의존도도 훨씬 낮은 편이며, 지리적 거리의 제약을 받지 않아 확장이 용이하다(Dear 2021, 22). 이러한 특징들은 전형적인 탈지정학적 특징이라고 할 수 있다.

우리가 목도하고 있는 사이버 공간의 또다른 진화 양상은 평화 논의가 사이버 공간에서만 머물러서는 안 된다는 점이다. 사이버 공간에서는 안보가 생존의 문제로 제한되는 것이 적절하지 않을 수 있고, 평화가 물리적 폭력 상태의 부재로는 설명될 수 없는 것이 사실이다. 하지만 물리적 공간과의 연계가 발생하고 이것이 시차 없이 매끄럽게 전환된다면 두 공간의 복합된 형태의 평화 상태를 고민해야 할 필요가 생긴다. 분명 과거에는 사이버 공간에서 행해진 공격으로 사망한 사례가 없다고 주장하는 것이 가능했다. 하지만 이는 점점 수용되기 어려운 주장이 되어가는 중이다. 2017년에 발생하였던 워너크라이 랜섬웨어 공격으로 인하여 영국의 보건 당국이 피해를 겪었고, 환자들의 예약이 대규모로 취소되는 사태가 발생하기도 하였으며, 코로나19 팬데믹 기간에는 병원, 백신을 개발하는 제약 회사, 백신 생산 공장 등이 해커들의 공격 대상이 되기도 하였다(Nye 2022, 34).

동시에 기술의 발전은 사이버 공간을 양적, 질적으로 진화시켰다. 처음 사이버 공간이 등장할 때 비하여 서버가 계속 증축됨에 따라 양적으로 공간이 확장되었다. 또한 통신 기술의 발달로 지연 속도가 빠르게 줄어듦에 따라 물리적 공간과 사이버 공간이 주고받는 영향의 시차가 더욱 좁혀지고, 사물 인터넷도 이러한 초연결성을 더욱 강화함에 따라 물리적 공간과 사이버 공간 간 연계를 통해 사이버 공간의 기능이 질적으로 더욱 확장되는 전환이 일어나기도 하였다. 초기에 사이버 공간은 물리적 공간의 보조적 역할만 수행하는 보완적 성격이 강했다면 이제는 일정 부분에 있어서는 대체될 수도 있을 정도로 질적 성장을 이뤄낸 것이다. 데이터 센터 화재가 사이버 공간에 영향을 미치고, 분산 서비스 거부(DDoS) 공격으로 인한 사이버 공간 마비가 현실 세계에 영향을 주는 사례를 통하여 두 공간이 쌍방향으로 연계된 공간임을 다시 한번 확인할 수 있다(윤정현·이수연 2022, 134-135). 마찬가지로 사이버 공간에서 탈취한 암호화폐를 미사일 개발에 활용하는 북한의 사례 역시 탈지정학적 공간과 지정학적 공간을 넘나드는 안보, 평화 이슈의 대표적 사례라고 할 수 있고, 이를 통해 던질 수 있는 질문이 바로 “사이버 평화는 사이버 공간의 평화만으로 달성할 수 있는 문제인가?”이다. 결국 사이버 공간의 진화 양상에 따라 궁극적으로 사이버 평화는 물리적 공간의 평화와 연계될 수밖에 없는 문제인 것이다. 이러한 이유에서 우리는 동태적인 사이버 공간의 진화적 의미를 포착하는 것이 중요하다.

Ⅳ. 대안적 사이버 평화 개념 논의를 위한 고려사항

1. 주요 이해관계자의 범위 확대

최근 사이버 공간에서 주목받는 행위자는 국가가 아닌 민간 행위자였다. 하지만 최근에는 국가 지원 해커들이 등장하면서 다시 포스트 모더니즘에서 모더니즘으로 역행하는 현상 역시 나타나기도 한다. 실제로 스위스 연방 정보국(FIS) 보고서에 따르면, 최근 외교관이나 정보기관을 통한 첩보 수집 활동이 아닌, 민간인을 활용하는 형태를 보임으로써 행위자의 외연과 권한을 확대하는 양상이 나타나기도 한다(나용우 2022, 2).[5] 그러나 중요한 점은 국가가 전면에 있느냐 배후에 있느냐보다 사이버 공간의 행위자로서 얼마나 다양한 유의미한 주체들을 포함할 수

있느냐이다. 이러한 관점에서 정부와 민간 사이에서 원활히 작동하는 다중 이해당사자 간 파트너십의 형성 또한 사이버 평화를 유지 및 실천해가는 주요한 기제라 볼 수 있다. 즉 다중 이해당사자 간의 협력을 촉진함으로써 거버넌스 메커니즘을 강화할 뿐만 아니라 긍정적인 사이버 평화의 토대를 마련함으로써 사이버 전쟁의 발발을 예방할 수 있다는 시각을 반영하는 것이다.

앞서 설명한 바와 같이 사이버 공간은 역동적이며 시간이 지날수록 네트워크가 기하급수적으로 형성되어 복잡성이 창발한다. 이 같은 사이버 공간의 특성상 평화가 달성되는 특정한 시점이나 고정된 지점이 존재하는 것은 사실상 불가능하다. 그렇다면 끊임없는 평화 추구 과정의 축적을 통해 이상적인 사이버 평화 상태를 달성하고자 지속적인 노력이 필요할 뿐이다. 이처럼 과정으로서의 사이버 평화를 지향하기 위해서는 전방위적인 거버넌스가 필요하다. 국가, 기업, 개인, 포스트 휴먼 등 이해당사자의 다층적인 네트워크 협력이 중요한 것이다. 또한 경계를 초월하는 특성을 기본으로 하는 사이버 공간에 대한 거버넌스를 제대로 구축하기 위해서는 경쟁적, 갈등적 태도보다 협력적 태도가 무엇보다 중요하다.

민간이 주도하였던 규범 형성 노력으로는 디지털 제네바 협약이 있다. 2017년에 마이크로소프트는 국가의 지원을 받는 사이버 공격으로 인해 피해 받는 민간인을 보호하기 위해 디지털 제네바 협약을 제안했고, 구글, 페이스북 등 세계적인 기업들도 이에 동참하였다. 이후 프랑스에서 진행된 회의에서 '파리 콜(Paris Call for Trust and Security in Cyberspace)'이 채택되었고 여기에는 50개 이상의 국가가 참여하였고, 마이크로소프트, 구글, 페이스북 등 기업도 200개 이상 참여하였다. 국가 지원 사이버 공격의 배후로 지목되는 러시아, 중국, 북한 등이 참여하지 않았다는 점에서는 한계가 있긴 하지만 다양한 이해관계를 가진 행위자들이 한자리에 모여 하나의 합의를 이끌어냈다는 데 의의가 있다.

최근 사이버 공간의 공수 비대칭성과 관계정립에 영향을 미치는 기술로서 인공지능과 포스트 휴먼이 회자되고 있다. 포스트 휴먼은 사이버 평화의 대상이 될 수도 있지만 평화에 기여하는 일원이 될 수도 있다. 인공지능은 사이버 공간에서 허위 조작 정보를 생성하여 확산시키는 역할을 함으로써 평화를 위협하기도 하지만, 이러한 위협에 맞서는 인공지능 역시 존재한다. 사실 확인(fact check)을 임무로 수행하는 인공지능이 이에 해당한다고 할 수 있다. 사이버 공간에서 허위 조작 정보로 인한 위협이 점증하고 있고, 권위주의 국가들이 민주주의 국가들을 무너뜨리는 방법으로 전시가 아닌 선거 기간과 같은 평시에도 사이버 공간의 불안정은 지속된다. 인공지능을 통한 확산은 너무 방대하기 때문에 인간이 대응하기 쉽지 않으므로 이를 방어하기 위한 용도의 인공지능을 활용하는 것은 향후 필수적일 것으로 전망된다. 이러한 흐름은 향후 국가, 기업, 시민단체와 같은 행위자 이외에 인공지능과 같은 포스트 휴먼도 다중 이해당사자 중 하나로서 사이버 평화 구축을 위해 기여할 수 있는 영역을 보다 폭넓게 창출시킬 것임을 예상할 수 있다.

2. 동태적 사이버 평화 접근의 필요성

사이버 공간은 양적으로도 변화하고 질적으로도 진화하는 공간이기에 창발적 성격을 지닌다. 특정한 정태적 순간을 포착하여 평화인지 아닌지를 단정할 수 없기 때문에 사이버 공간이 위협받는 메커니즘 전체에 초점을 맞춰서 접근해야 하는 것이다. 즉, 사이버 평화를 고정된 목표가 아닌 '과정'으로 인식할 필요가 있다는 점에 주안점을 둘 필요가 있다. 가변성과 불확실성을 전제로 하는 신흥안보 패러다임은 주요 위험 이슈가 직간접적인 연계를 통해 거시적 안보 이슈로

5) https://m.boannews.com/html/detail.html?idx=119684

증폭되는 역동적인 변화를 강조한다(김상배 2016; 윤정현 2019). 이는 사이버 공간의 위험과 평화를 바라보는 시각에도 많은 시사점을 준다. 사이버 공격행위의 빈도가 증가함에 따라 질적으로 변화하거나 다른 이슈와 연계되어 외연이 확대되는 과정에서 임계점을 넘어서는 지점이 존재하며, 비로소 체감할 수 있는 사이버 보안의 사고로 이어지거나, 심지어 거시적 안보 이슈로 증폭되기도 한다. 다시말해 사이버 평화를 위해서는 완벽한 차단이 아닌, 임계점을 넘지 않도록 관리하는 지속적인 노력이 필요한 것이다.

최근 안전한 사이버 공간 구현을 위한 기술적-제도적 보완책이 마련되고 있는 것도 이러한 흐름과 궤를 같이한다고 볼 수 있다. 다양한 행위자들이 지속적으로 정보를 공유하여 불신을 해소하고 안정적인 시스템으로 발전할 수 있도록 지속 가능한 인센티브를 제공하는 데 집중함으로써 가변성과 불확실성에 기반한 위협이 발생할 가능성을 완화하려는 시도인 것이다. 사이버 공간은 시간이 지남에 따라 기하급수적으로 네트워크가 형성되어 복잡성을 야기하는 역동적인 공간이다. 마찬가지로 이는 사이버 공간에서의 평화가 달성해야 할 하나의 고정된 지점이 아니라 불확실한 변화에 대응하여 진화하는 역동적인 과정으로 보아야 함을 재확인시켜 준다.

실제로 같은 맥락에서 최근 사이버 범죄를 예방하기 위한 국제 규범은 프라이버시 보호뿐만 아니라 이해관계자의 적절한 사용을 위한 가이드라인을 명시함으로써 규제와 촉진의 균형을 추구하고 있다(윤정현·이수연 2023, 19-20). 이는 사이버 공간의 특성상 평화가 달성되는 특정 지점이나 고정된 지점이 존재한다는 것은 사실상 불가능함을 시사한다.

3. 사이버 공간의 지속성을 위한 '복원력' 강화

과정으로서 사이버 평화를 보는 접근은 사이버 공간의 역동성과 불확실성이라는 양면적 속성을 고려하게 만든다. 이는 완전한 사이버 공간의 안전 확보나 갈등의 부재는 불가능할 수 있으며, 따라서 예기치 못한 사이버 위협에 대한 완벽한 예방과 대응 역시 비현실적임을 시사한다. 그렇다면 끊임없이 갈등과 조정이 일어나는 사이버 공간에서 원활한 기능이 유지되고 문제를 개선해 나아가는 역량을 지속적으로 확보할 수 있는가가 관건이 된다. 이는 곧 사이버 공간의 지속가능성을 요구하는 동시에, 급박한 위기상황에도 정상적 단계로 복원할 수 있는 '복원력(resilience)'의 필요성을 암시하는 것이다.

복원력은 '본래의 성질에 가해진 부분적인 손상을 대체하는데 소요되는 복구시간'이라는 공학적 정의와(Walker, B. et al., 2004), '혼란 속에서도 본래의 기능과 구조, 정체성을 유지할 수 있도록 하는 능력'이라는 사회과학적 정의를 내포하고 있는 개념이다(McManus & Polsenberg, 2004). 최근에는 살아있는 시스템이 가진 적응력과 학습능력에 초점을 둔, 사회-생태학적 차원의 복원력을 강조하는 경향이 나타나고 있는데 이러한 관점에서는 복원력을 '혼란에 능동적으로 대처하고 진화하는 시스템의 역동성'으로 설명하고 있다(윤정현, 2013: 12).

사이버 복원력을 유지하거나 강화하기 위해서는 크게 두 가지 방향에서 실천 방안이 논의될 수 있다. 하나는 기술에 의한 회복력 유지·강화이며, 다른 하나는 제도에 의한 회복력 유지·강화이다. 예를들어 집중화된 중앙제어 시스템의 한계를 극복하고 다수의 합의에 의한 무결성을 유지하고자 고안된 블록체인 기술의 경우, 관리자나 제3자가 없는 분산형 네트워크 구조로 이루어져 있기 때문에 사이버 공격의 위협으로부터 중앙의 허브를 공격당하는 치명성에서 안전할 수 있다(윤정현, 2019: 77). 또한, 우크라이나 전쟁에서 보듯이, 러시아는 우크라이나에 침공하기 직전 통신망을 파괴하기 위하여 사이버 공격을 감행, 수도를 포함한 주요 도시에서 통신 장애를 유발하였지만, 사이버 공간의 회복력을 확보하기 위해서 하나의 도메인에만 의존하지 않고 여러 도메

인 간 연계를 통해 우크라이나는 이를 극복하였다. 일론 머스크의 스페이스X사를 통하여 우주를 기반으로 하는 제공하는 통신 서비스를 통해 지상을 기반으로 하는 사이버 공간 인프라가 파괴되었지만, 우주 기반 인프라를 통해 회복한 사례이기도 하였다.

Ⅴ. 결론

결국, 사이버 평화론의 현실적인 첫 출발은 사이버 공간과 일반론적인 평화 개념을 단순 연결하는 기존의 접근에서 벗어나 사이버 공간이 가진 존재론적 차별성과 작동 메커니즘을 이해하는 데서 출발한다. 사이버 공간이 지닌 가변성과 공간의 확장, 질적 변환의 속성들이 단순한 전통적 세계의 평화 개념을 접목시키는 것으로는 이해하기 어려운 양상들을 내재하고 있기 때문이다. 사이버 공간의 진화적 속성에 부합하는 '사이버 평화' 개념을 제시하기 위해 우리는 사이버 공간의 조직 원리와 힘의 배분 상태, 사이버 공간의 동태적 특징에 주목하고 그것이 국제정치적 관점에서 갖는 의미를 재해석할 필요가 있다.

즉, 사이버 평화에 대한 논의는 사이버 공간의 실질적 안전 확보나 이를 위한 실천 방안에서 보더라도 단순히 적극적 개념이나 소극적 개념의 구분을 넘어설 필요성을 제기한다. 특히 안보와 평화의 불가분한 관계를 설명하는 국제정치이론으로 본 사이버 평화 개념은 단순히 무정부 상태의 질서에 해당하는 의미를 넘어 탈근대적, 신흥안보적 속성을 접목시켜 바라보아야 함을 시사하기 때문이다. 본고는 사이버 공간이 가지는 양질전화, 이슈 연계, 새로운 진화체의 창발과 같은 신흥안보의 관점을 활용하여 기존의 소극적·적극적 평화 개념이 담을 수 없는 사이버 평화의 사각지대가 존재할 수 있음을 확인하였다. 나아가 대안적 사이버 평화론의 정립을 위해 이를 단순히 사이버 전쟁의 대척점으로 바라보는 접근의 한계 역시 존재함을 알 수 있다. 안보가 평화를 위한 필요조건으로 간주되며 평화적 상태로 나아가기 위해 우선적으로 달성되어야 하는 단계와 등치되기도 하나, 완전한 갈등의 부재 상태, 혹은 원천적인 사이버 공격에 대한 대비 상태는 불가능하다는 점에서 현실적인 접근을 필요로 한다.

이는 곧 사이버 평화가 안정적인 방향으로 끊임없이 개선되어가는 과도기적 단계로 존재가능함을 시사한다. 즉, 사이버 공간에서의 평화 또한 궁극적으로 달성해야 하는 어느 한 지점으로 보기보다는, 역동적인 변화에 발맞춰 진화해가는 동태적 과정으로 봐야 할 필요가 있음을 보여주기 때문이다. 어떠한 완성된 목표 지점까지의 달성이 아니라 평화를 향한 방향과 발전 경로를 끊임없이 맞추어가는 지속적인 '과정'으로서 사이버 평화개념은 접근할 필요가 있다. 앞서 언급했던 신흥안보 패러다임을 특징짓는 가변성과 불확실성이 높은 환경에서는 주요 위험 이슈들이 직간접적인 연계를 통해 거시적인 초국가 문제로 증폭되는 양상이 목도된다. 이를 관리하기 위해 난제의 속성을 전환시키는 안보화 과정의 동태적 변화에 주목하는 시각도 이와 밀접하다 볼 수 있다. 또한, 사이버 공간에서 발생할 수 있는 위험의 양이 증가함에 따라 질적인 변화를 창출하거나 다른 이슈와 연계되어 외연이 확대되거나 하는 과정에서 임계점을 넘는 지점들이 존재하는데, 사이버 평화를 위해서는 그 지점들을 끊어내려는 노력이 필요하다. 최근 나타나고 있는 안전한 사이버 공간 구현을 위한 기술·제도적 보완은 이 같은 흐름과 궤를 나란히 하고 있음을 알 수 있다.

국가, 기업, 시민단체와 같은 행위자 이외에 인공지능과 같은 포스트 휴먼도 다중 이해당사자

중 하나로서 사이버 평화 구축에 중요한 역할을 할 수 있다. 최근 사이버 공간의 공수 비대칭성과 관계정립에 영향을 미치는 기술로서 각광받고 있는 인공지능과 포스트 휴먼의 존재 역시 갈등 뿐만 아니라 장기적으로는 평화에 기여하는 일원이 될 수 있음을 시사한다. 문제는 이처럼 다양한 행위자들이 참여하는 동태적인 사이버 공간의 질서는 역동성과 불확실성이라는 양면적 속성이 존재한다는 점이다. 이는 완전한 사이버 안보 상태란 비현실적이며 끊임없이 갈등과 조정이 일어나는 사이버 공간에서 원활한 기능이 유지되고 문제를 개선해 나아가는 역량을 지속적으로 확보할 수 있는 항상성과 회복력이 사이버 평화를 담보하는 중요한 실행역량이 될 수 있음을 시사한다. 따라서 우리는 사이버 공간이 가진 경계의 모호함과 역동성과 불확실성이 개념적 정립을 어렵게 하지만, 위에서 열거한 특징들을 기반으로 사이버 평화의 실현 조건을 충족한 실행가치를 탐색하고 실질적 적용사례와 관행 등을 공유하는 것이 중요하다. 사이버 평화론의 정립과 효과적인 실천방안과도 맞닿아 있기 때문이다.

〈참고문헌〉

김상배. 2008. “네트워크 세계정치이론의 모색: 현실주의 국제정치이론의 세 가지 가정을 넘어서.”『국제정치논총』48(4), 35-61.

김상배. 2023. “신흥평화의 개념적 탐구: ‘창발(emergence)’의 시각에서 본 평화연구의 새로운 지평.”『한국정치학회보』57(1), 225-248.

김상배. 2016. “신흥안보와 메타 거버넌스: 새로운 안보 패러다임의 이론적 이해,” 『한국정치학회보』, 50(1), 75-104.

김소정. 2023. “2023 미국 사이버안보 전략의 주요내용과 한국에의 시사점”,『INSS 이슈브리프』 제423호, (2023. 3. 8.), 1-9.

나용우. 2022. “사이버공간의 혼돈 속 한반도 사이버평화를 위한 과제.”『JPI Peace Net』 2022-25, 1-6.

민병원. 2012. “안보담론과 국제정치: 안보개념의 역사적 변화를 중심으로.”『평화연구』가을호, 203-240.

민병원. 2023. “평화의 형이상학과 경합주의적 개념화.”『국제정치논총』63(1), 7-42.

박동휘. 2022.『사이버전의 모든 것』, 서울: 플래닛 미디어.

빌헬름 얀센. 2010.『코젤렉의 개념사 사전 5: 평화』오토 브루너, 베르너 콘체, 라인하르트 코젤렉 편. 한상희 옮김. 서울: 도서출판 푸른역사.

서보혁. 2022. “양질의 평화.” 서보혁, 강혁민 편.『평화개념 연구』서울: 도서출판 모시는사람들: 107-134.

송태은. 2023. “평화.” 김상배, 안태현 편.『디지털 사회의 기본가치』. 서울: 사회평론아카데미, 349-382.

윤정현. 2013. “미래준비역량으로서 사회적 복원력”,『Future Horizon』Spring 2013, Vol. 16, 12-13.

윤정현. 2019. “신흥안보 거버넌스: 이론적 고찰과 대안적 분석틀의 모색”,『국가안보와 전략』 19(3), 1-46.

윤정현. 2019. “인공지능과 블록체인의 도입이 사이버 안보의 공·수 비대칭 구도에 갖는 의미”, 『국제정치논총』59(4), 45-82.

윤정현. 2020. “신흥안보 위험과 네트워크 거버넌스: 불확실성 시대의 초국가적 난제와 대응전략”,『한국정치학회보』54(4), 29-51.

윤정현, 이수연. 2022. “디지털 안전사회의 의미: 안전과 안보의 복합공간으로서 전환적 특징과 시사점.”『정치·정보연구』25(3), 123-150.

윤정현, 이수연. 2023. “사이버 평화론에 대한 소고: 신흥안보 시대의 대안적 접근.” 『정치·정보연구』26(1), 1-28.

임마누엘 칸트. 2018.『영구평화론』박환덕, 박열 옮김. 파주: 범우사.

정영애. 2017. “사이버 위협과 사이버 안보화의 문제, 그리고 적극적 사이버 평화.” 『평화학연구』18(3), 105-125.

전재성. 2014. “국제정치 조직원리 논쟁과 위계론.”『국제정치논총』54(2), 7-45.

조은정, 이성훈, 김성배, 오일석, 윤정현. 2023. “2023년 한미정상회담의 성과와 후속과제: 핵안보, 사이버안보, 기술·경제안보를 중심으로.”『이슈브리프』431, 2023년 4월 28일.

허지영. 2022. “일상적 평화.” 서보혁, 강혁민 편.『평화개념 연구』서울: 도서출판 모시는사람들:

179-204.

Alperovitch, Dmitri. 2022. “The Case for Cyber-Realism: Geopolitical Problems Don’t Have Technical Solutions.” Foreign Affairs, 101(1), 44-51.

Chilton, Jim. “The New Risks ChatGPT Poses to Cybersecurity.” Harvard Business Review, 21 April 2023. https://hbr.org/2023/04/the-new-risks-chatgpt-poses-to-cybersecurity.

Foreign, Commonwealth & Development Office. 2022. “Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion.” Press release, 10 May 2022. https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion.

Galtung, Johan. 1969. “Violence, Peace, and Peace Research.” Journal of Peace Research, 6(3), 167-191.

Inversini, Reto. 2020. “Cyber Peace: And How It Can Be Achieved,” Markus Christen et al. (eds.). The Ethics of Cybersecurity. Springer Open.

ISA. 2022. “The ISA 2022 Country Power Rankings.” 17 October 2022. https://www.isa-world.com/news/?tx_ttnews%5BbackPid%5D=1&tx_ttnews%5Btt_news%5D=595&cHash=d37d2e848d6b79811749a619c74abebc.

McManus, J.W., Polsenberg, J.F. 2004. "Coral-algal shifts on coral reefs: ecological and environmental aspects." Progress in Oceanography 60, 263-279.

NATO. 2019. "Cyberwar: does it exist?" (June 13, 2019)

Nye, Joseph S. 2022. “The End of Cyber-Anarchy?: How to Build a New Digital Order.” Foreign Affairs, 101(1), 32-43.

Flint, Colin. Introduction to Geopolitics, 한국지정학연구회 역, 2007.『지정학이란 무엇인가』, 서울: 도서출판 길.

RAND. 2023. “Cyber Warfare”, https://www.rand.org/topics/cyber-warfare.html

U.S. government via Department of Homeland Security. 2003. “The National Strategy to Secure Cyberspace" (PDF). February 2003. p. 16. Retrieved 2008-05-18.

Voo, Julia, Irfan Hemani and Daniel Cassidy. 2022, “National Cyber Power Index 2022.” Harvard Kennedy School Belfer Center for Science and International Affairs, September 2022.

The White House. 2023. “National Cybersecurity Strategy” (March 1, 2023).

Wakefield, Jane. 2022. “Deepfake presidents used in Russia-Ukraine war.” BBC, 18 March 2022. https://www.bbc.com/news/technology-60780142.

Walker, B. et al. 2004. "Resilience, Adaptability and Transformability in Socio-ecological Systems", Ecology and Society: 9(2).

Waltz, N. Kenneth. 1979. Theory of International Politics, Massachusetts: Addison-Wesley Publishing Company. https://m.boannews.com/html/detail.html?idx=119684

이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.