아 산 정 책 연 구 원

이슈브리프

No. 2025-29

사이버 공간에서의 국제법 적용에 관한 한국 정부 입장의 현재와 미래

신소현

연구위원

2025-09-12

한국 정부는 2025년 7월 미국 뉴욕에서 열린 유엔 개방형 실무그룹(Open-Ended Working Group, OEWG)의 마지막 회의에서 '사이버 공간에서의 국제법 적용에 관한 우리 정부의 입장'을 최초로 공식 발표했다. 이로써 2025년 7월 기준, 33개 국가와 2개의 지역기구(유럽연합 및 아프리카연합)가 사이버 공간에서의 국제법 적용에 관한 공식적인 국가 입장을 발표했다. 국가입장문의 공표는 조약과 관습법으로 대별되는 국제법의 형성 및 발전 과정에서 국가 실행(state practice)에 해당하면서 동시에 국가 전략의 성격도 띤다. 즉, 사이버 공간에서 발생하는 각종 행위에 대해 해당 국가가 이를 어떻게 해석하고 대응해 나갈지에 대한 의지의 표현으로 해석될 수 있다. 최초의 입장문에서 우리 정부는 원칙적으로 기존 국제법은 사이버 공간에서도 존중되고, 주권 및 불간섭의 원칙이 사이버 공간에서도 적용된다고 했다. 무력사용금지와 자위권, 국가책임, 그리고 국제인권법과 국제인도법의 사이버 공간에서의 적용에 대해서도 입장을 밝혔다.

이번에 발표한 국가입장문은 한국 정부가 해석하는 사이버 공간에서 적용 가능한 국제법에 관한 현재의 입장과 방향성을 공표한 것이지 최종적이고 불변하는 것은 아니다. 개인과 집단, 기업과 공공 기관 및 정부에 이르기까지 모든 주체들은 사이버 공간에서 활동하며 서로 연결되어 있으므로 사이버 공간에서 적용되는 국제 규범의 발전은 우리 모두에게

영향을 준다. 이번에 공표된 주요 국제법 분야의 내용을 간단히 소개하고 구체적으로 어떤 사안에서 적용되는 것인지 분석한다. 그리고 다른 유사입장국들의 입장 및 국제적 동향을 고려하여 아쉬운 부분이나 앞으로 더 발전시켜 정리해야 할 국제법적 논점에 대하여 고찰한다.

사이버 공간에서의 국제법 적용에 관한 국가입장문의 함의

1. 논의의 경과

1990년대 중반 이후부터 미국을 중심으로 국가들은 사이버 공간을 규제 대상으로 인식하기 시작했고, 국경을 초월하여 연결된 사이버 공간에서 국가들 간에 공격과 충돌이 벌어지는 상황에 대한 우려가 생겨났다. 이에 사이버 공간에서 책임 있는 국가 행위를 유도하기 위해 사이버 공간에서 지켜야 할 국제 규범을 모색하려는 움직임이 일어났다. 사이버 공간에서 적용 가능한 국제법에 관한 본격적인 논의는 2004년 유엔 정부간 전문가 그룹(Group of Governmental Experts, GGE)부터 시작되었고, 2021년까지 총 6차례의 회기를 가졌다. 이후 더 많은 국가들과 다양한 (비국가)이해관계자들이 참여하도록 한 유엔 개방형 실무그룹에서 논의가 이어졌다. 2021년부터 5년간 이어진 OEWG를 마무리하면서 기존 및 잠재적인 위협, 책임 있는 국가 행위를 위한 규칙, 규범 및 원칙, 국제법, 신뢰 구축 조치, 그리고 어려운 지정학적 환경에서의 역량 강화 등에 대해 합의한 최종보고서를 채택했다.[1] 이후의 논의는 '국제 안보 및 ICT 사용에 있어 책임 있는 국가 행동 증진이라는 맥락에서 ICT 분야 발전에 관한 글로벌 메커니즘(Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible State behaviour in the use of ICTs)'이라는 새로운 단일 트랙의 상설(permanent) 메커니즘을 통해 계속될 예정이다. 이 메커니즘은 정보통신기술(ICT)의 사용에 관련된 크게 5가지 영역(기존 및 잠재적 위협, 책임 있는 국가 행동에 관한 규범, 국제법의 적용, 신뢰구축조치 및 역량 강화)에서 책임 있는 국가 행동 프레임워크에 대한 논의를 이어 간다. 글로벌 메커니즘은 2026년 3월부터 활동하며 유엔 총회 산하 기관으로서 제1위원회에 보고하도록 되어 있다.

2. 국가입장문의 국제법적 의의

국가들의 관행이 축적되어 법적 확신(*opinio juris*)을 획득하면 국제관습법이 성립한 것으로 평가되는데, 이는 때로는 국제재판소 판결을 통해, 때로는 관습법의 내용을 확인하는 국제조약의 체결을 통해, 때로는 유엔 총회의 결의나 선언 등을 통해 확인된다. 다양한 경로로 확인되는 국제관습법의 존재는 보통 그 성립을 위해 상당한 시간이 필요하지만, 개별 주권국가가 관련 국제법 주제나 사안에 대하여 자신의 해석과 판단을 공표하는 것은 국가 실행을 스스로 확인해주는 행위로서 그 국제법 형성 과정에 걸리는 시간을 단축시키는 효과가 있다. 특히, 사이버 공간과 같이, 법적 규율이 첨단 기술의 발전 속도를 따라가지 못하는 경우에는 국가들이 보다 적극적으로 나서서 자신의 의지를 표명함으로써 그 간극을 줄이려고 하기도 한다.

3. 국가입장문의 전략적 가치

국가 입장의 발표는 국제 사회에서 국가 간 관련 사안에 대하여 어느 정도 서로 이해하고 반응을 가늠할 수 있는 정보를 미리 제공할 수 있다. 정리된 입장문은 사이버 공간에서 벌어지는 혹은 벌어질 수 있는 국가 간 갈등 상황에 대하여 국가들은 미리 전략적으로 자신의 임계치(red line)나 예상하는 대응의 수위나 종류 등에 대하여 사전 정보를 제공하는 역할을 한다. 구체화된 국가 입장일수록 현실에서 더 유용한 사전 정보 제공이 될 것이다. 그러나 또한 의도적으로 모호한 입장을 내거나 입장 표명 자체를 꺼리는 경우도 있는데, 이 역시도 전략적 고려가 담긴 경우가 많다. 한국을 포함해 2025년 7월까지 발표된 33개국의 국가입장문은 정도 차이는 있지만, 아주 상세한 버전이라고 볼 수는 없다. 대체적으로 국가들이 입장을 내는 주권, 무력사용, 국가책임 등과 같은 주요 국제법 분야가 특정되고 있어 큰 맥락은 파악이 가능하지만, 그래도 많은 여백이 남아 있다.

4. 국가입장문의 한계

국가입장문의 발표는 현재도 발전중인 관습 국제법 형성 과정이므로 일회적으로 결정된 것이 아니라 일련의 변화에 따라 함께 진화할 수 있다. 국제 정세에 맞춰 국가 및 국제기구가 의사를 변경하거나 새로운 첨단기술이 국가가 취할 수 있는 수단과 방법에 혁신을 가져올 때 등이 그 예이다. 인류가 발명한 사이버 공간에 적용되는 국제 규범에 관한 포괄적인 국가

간 합의는 아직 이루어진 적이 없다. 40개국의 비준을 통한 조약 발효까지는 상당한 시간이 소요되겠지만, 2024년 12월 24일 유엔 총회에서 통과된 '사이버 범죄에 관한 UN 협약'은 그래도 상당한 진전이다.[2] 디지털 민주주의 진영 국가 그룹과 디지털 권위주의 진영 국가 그룹 간에 실질적인 사이버 범죄 대응을 위한 국제 협력이 가능할지에 대해서는 좀 더 국가 실행의 경과를 봐야 한다. 역사적으로 국제법이 변화·발전해 온 지난한 과정에 비해, 국가들이 입장문 등을 공표하는 방식으로 적극적으로 국가 실행을 형성하고 있기 때문에 사이버 공간에서 적용 가능한 국제 규범의 발전 과정은 상대적으로 그 속도가 빠를 수 있다.

그러나 여전히 한계도 존재한다. 첫째, 국가입장문은 발표한 해당 국가가 국제법의 해석을 이렇게 하고 있으며 관련 사안이 발생하면 발표한 것처럼 국제법 적용을 하겠다는 선언적 의미가 있을 뿐, 그 확정적 실행을 반드시 담보하는 것은 아니다. 둘째, 총 193 유엔 회원국 중 절반에도 못 미치는 대략 40개국 정도의 입장 발표로 국제 규범 형성이 가능한가 하는 반박이 제시될 수 있다. 이에 나토 사이버방어협력센터(NATO Cooperative Cyber Defence Centre of Excellence, NATO CCDCOE)와 유엔 군축연구소(UN Institute of Disarmament Research, UNDIR)를 비롯하여 지역 국제기구들(아세안, 유럽안보협력기구, 미주기구 등)이 가이드라인을 제시하거나 실무자 대상 교육 프로그램을 운영하는 등 국가들의 입장 개발 및 발표를 독려하고 있다. 셋째, 2025년 7월 현재까지 발표된 국가입장문의 내용은 대부분의 국가들이 국제법의 가장 큰 범주에 해당하는 주제들에 대한 대략적인 적용 가능성에 대한 입장을 표명한 것으로 실제 사이버 공간에서 벌어지는 혹은 벌어지게 될지도 모르는 사안에 대한 구체적인 국제법 적용에 대해서는 여전히 해석이 유보된 채 남아 있다.

한국 정부의 입장에[3] 대한 비판적 분석과 적용

우리 정부는 유엔 헌장을 비롯하여 국제 사회에서 일반적으로 인정되는 국제 규범과 국제관습법이 사이버 공간에도 동일하게 적용되는 것이 바람직하다는 기본적인 입장이다. 입장을 공개한 거의 모든 국가들은 사이버 공간이 무법(lawless) 지대가 아니고 기본적인 국제법 질서가 존중되는 공간이라는 점에 동의한다.

1. 국가 주권과 불간섭의 원칙

(1) 정부 입장

주권평등 원칙 및 이에서 도출되는 원칙, 즉 분쟁의 평화적 해결, 무력위협 및 사용의 금지, 국내문제 불간섭 원칙들이 사이버 공간에서 국가의 활동에 대하여도 적용된다고 본다. 주권의 영토적 관할권에 기초하여, 국가는 자국의 영토에 위치한 사이버 기반 시설, 자국의 영토 내에서 사이버 활동을 하는 자 및 그 사이버 활동에 대하여 관할권을 향유한다.

(2) 분석 및 적용

사이버 공간에서는 불법 행위의 법적, 기술적 귀속(attribution)이 어려운데 반해, 전 세계가 초국경적으로 초연결되어 실시간으로 정보를 주고 받는다. 따라서 대부분의 사이버 침해 행위는 국제법상 위법성이 명백하지 않은 경우라도 주권 침해적 요소를 갖게 되므로 사이버 공간에서 주권 침해의 법적 성격과 효과에 대한 입장을 표명한 국가들도 있다. 예를 들어, 최근 문제되고 있는 온라인 정보 조작 등을 이용하여 타국의 선거에 개입하려는 행위는 강압(coercion)을 동반하지 않는 한, 국제법상 불간섭의 원칙 위반은 아니다. 그러나 여전히 상대국의 주권 침해는 될 수 있다. 영국 정부는 일반적인 주권 원칙은 인정하지만, 사이버 활동을 이용한 간섭 금지의 규범을 넘어선 정도로 주권 침해에 대한 특별히 부가적인 금지나 특별한 규칙을 설정하지 말아야 한다는 입장이다. 그렇게 할 경우 주권 원칙이 오히려 사이버 공간에서 기본적 인권이나 자유를 해치고 지나친 규제를 하게 될 가능성이 있기 때문이라고 한다.[4] 즉, 강압을 동반한 국제법상 간섭의 수준에 못 미치는 정보수집 등 타국의 네트워크에 들어가는 것(exploitation)만으로는 불법이 되지 않는다는 입장이다. 그러나 프랑스, 독일, 네덜란드 등 다수의 국가들은 특별히 주권 침해의 효과를 원칙 위반 정도로 제한하지 않고 규범성을 인정한다.[5] 즉, 타국의 사이버 인프라에 개입하면 주권 침해에 해당하고 그 중대성 정도에 따라 국제법상 가능한 대응조치나 국가책임을 물을 수 있다. 우리 정부는 다른 국가가 우리의 사이버 공간이나 인프라에 권한없이 접근하거나 침입한 경우 주권 침해가 발생한다고 보지만, 그 침해가 대응조치를 취하거나 국가책임을 물을 수 있을 정도의 불법인지 아니면 단순히 주권 원칙을 위반한 것일 뿐인지에 대한 확실한 입장을 정리하고 있지 않다.

2. 무력사용금지의 원칙과 자위권

(1) 정부 입장

무력사용 및 위협 금지의 원칙은 사이버 공간에서의 활동에도 그대로 적용된다고 본다. 사이버 활동이 무력사용(use of force)에 해당하는지에 대해서는 행위의 결과, 성격, 주체 및 대상 등을 종합해서 결정해야 하고, 특정한 사이버 활동으로 인해 전통적인 국제법적 의미의 무력사용에 상응하는 물리적인 결과가 발생하면 일견, 무력사용에 해당한다고 본다. 또한 무력사용을 무력공격(armed attack)을 포괄하는 더 넓은 개념으로 보며, 국제사법재판소(ICJ) 판결을[6] 비롯한 다수의 국제 재판 및 저명한 학설, 여러 국가의 국가관행에 의해서도 뒷받침된다고 했다. 사이버 공간에서도 분쟁의 평화적 해결을 위해 노력해야 한다. 우리 정부는 특정 사이버 활동의 결과가 그 규모와 효과에 비추어 무력공격에 해당하면, 피해국이 자위권을 행사할 수 있다고 본다. 이때 자위권 행사에는 비례성과 필요성 등 관련 요건이 준수되어야 한다. 사이버 활동이 무력공격에 이르지 않은 무력사용에 해당하는 경우에는 무력행사에 이르지 않은 대응조치(countermeasure)를 취할 수 있다.

(2) 분석 및 적용

우리 정부는 다른 유사입장국가들과 비교할 때, 무력사용금지의 원칙과 자위권에 관한 최소한의 무난한 내용만을 제시하고 있다. 특히, 자위권의 행사를 위해서는 사이버 활동이 무력사용이나 무력공격이 되는지 여부와 함께 행위의 귀속이 결정적인데, 우리 정부는 귀속에 대한 일반적인 국제법 내용을 따른다. 귀속 판단을 정확하고 신속하게 하기 위해서는 국가 간 정보 공유를 비롯한 긴밀한 협력이 요구된다. 특히, 우리 정부는 악의적인 사이버 활동을 특정 국가에 귀속시키는 결정을 내릴 때 근거로 삼았던 정보를 공개할 국제법상 의무는 없고, 공개 여부는 스스로 결정할 수 있다고 했다. 한 국가가 다른 국가로부터 사이버 공격을 받은 사실을 공개하면서 외교적 비난을 하거나 일정한 조치를 취하려 할 때, 기술적·법적 귀속을 주장해도 공격자로 지목된 국가는 보통 발뺌하며 어떠한 책임과 비난도 받지 않으려 한다. 이럴 때 유사입장국가들끼리 정보 공유 및 공동 조사 등을 통해 공적·정치적 귀속을 하게 되는데, 이 경우 모든 상세한 근거 정보를 공개할 의무가 없으며 공개 여부도 자유로이 결정할 수 있음을 미리 밝힌 것이다. 실제 한국은 미국, 영국, 일본,

독일, 호주 등 여러 국가들과 수차례 공동으로 사이버 공격의 배후국을 지목하였다. 이 경우 모든 기술적 정보 등을 공개하지는 않겠다는 의미이다.

대다수의 국가는 물리적인 무력사용 또는 무력공격에 상응하는 규모와 효과를 일으키는 사이버 활동이 있어야 사이버 무력사용이나 사이버 무력공격이 발생한 것으로 보지만, 프랑스는 앞으로 꼭 물리적·파괴적인 효과가 발생하지 않더라도 그에 준하는 본래 기능의 상실이 있으면 사이버 무력사용이 될 수도 있다는 입장이다.[7] 미국 군과 국방부는 무력사용과 무력공격의 층위를 따로 구분하지 않고 무력사용이 있으면 무력공격으로 보아 자위권을 행사할 수 있다고 본다. 반면, 우리 정부는 무력공격이 무력사용보다 심각하고 중대하다고 보는 통설적인 입장을 취하고 있어 미국과 다르다. 한미 군사동맹을 고려할 때, 실전 상황에서 무력사용에 해당하는 사이버 공격이 발생한 경우, 한국 정부의 입장에선 자위권 발동 요건이 충족되지 않지만, 미국 측 입장에서는 자위권 행사도 가능하다. 이 부분의 해석 차이가 실제 사이버 공간에서 무력사용이 촉발된 경우 어떻게 조율될 것인지에 대한 관련 부처들의 입장 정리가 필요하다.

현재는 필요성과 비례성의 원칙을 반영한 자위권을 행사할 수 있다는 입장만 밝히고 있으나, 다음 입장 표명에서는 사이버 공격에 대응한 자위권 행사가 반드시 동일한 사이버 수단일 필요가 없고 물리적 반격을 할 수도 있다는 점을 명시적으로 밝히는 것이 좋다. 예를 들어, 사이버 무력공격의 거점에 대한 폭격이나 드론 암살 등을 의미한다. 이는 사이버 무력공격에 반격하기 위해 우리가 취할 수 있는 수단의 범위를 미리 넓게 밝혀 놓는 것이므로 잠재적 사이버 공격자들에 대한 억지 효과를 좀 더 높일 수 있다. 이밖에 국가가 아닌 테러 집단과 같은 비국가행위자로부터 사이버 무력공격을 받은 경우에도 자위권 행사를 할 수 있는지에 대해서도 입장을 밝힐 때를 대비하여 추가 검토가 필요하다.

3. 국가책임

(1) 정부 입장

우리 정부는 국제법상 위법행위에 상당하는 사이버 활동이 발생한 경우, 확보된 증거를 기반으로, 해당 활동과 관련된 기술적, 법적 분석, 의도 등을 종합한 분석을 통해 귀속성을 판단한다. 귀속과 관련된 국가책임법의 내용은 사이버 활동에도 적용된다고 본다. 국제법상

적법한 대응조치는 사이버 공간에서도 허용되며, 피해국의 대응조치는 유책국의 국제법 위반행위와 동일한 성격을 가질 필요는 없다. 따라서 국제법을 위반하는 사이버 활동의 경우 유책국에 대해서 피해국은 사이버 공간을 활용한 대응조치 혹은 사이버 공간과 상관없는 대응조치 어느 쪽이라도 취할 수 있다.

상당주의 원칙(due diligence)을 사이버 맥락에 적용해보면, 온라인상에서 국가는 자신의 관할권 내에서의 활동들로 인해 타국에 피해를 입히지 않도록 상당한 주의를 기울일 필요가 있다. 사이버 공간의 특성상 시·공간의 물리적 한계를 뛰어넘어 사이버 활동이 이루어지기 때문에, 피해국이 악의적인 사이버 활동을 하는 행위자를 신속히 파악하기는 매우 어렵다. 피해국이 악의적인 사이버 행위가 발생하거나 경유하는 타국에 이를 공식적으로 통지할 경우, 통지를 받은 국가는 동 행위에 대해 인지한 것으로 간주되어야 하며, 지체 없이 협조하고 국내·국제법에 따라 악의적인 행위를 중단시킬 필요가 있다.

(2) 분석 및 적용

상당주의에 대한 이러한 입장은 법리적으로 타당하다. 사이버 현실에 비추어 각국의 실제 사이버 역량에 따라 지게 되는 상당주의 의무의 내용 편차가 클 수 있음도 정책적으로 고려해야 한다. 예를 들어, 자국내 네트워크나 사이버 인프라가 제3국에 대한 사이버 공격(침해)의 경유지로 활용된 경우, 피해국이 이를 지체없이 중단시켜 달라고 요청하면 이를 중단시키기 위한 조치를 취해야 한다는 말인데, 구체적인 사이버 역량이 부족한 경유국은 그렇게 하지 못할 수도 있다. 그러면, 우리나라처럼 사이버 인프라가 잘 되어 있고 사이버 역량이 높은 국가일수록 더 많은 상당주의 의무를 지게 되는 결과가 된다. 특히 좋은 인프라와 높은 인터넷 속도 덕분에 한국은 경유지로 많이 이용된다. 상대적으로 역량이 부족한 국가는 자신을 향한 공격에 대한 중단 요청만 주로 하거나, 자국내에서 일어난 악의적 사이버 행위를 중단시켜 달라는 요청에 부응할 수 없는 다소 불공정한 상황이 발생하게 된다. 이러한 상당주의에 기한 중단 의무를 담당하는 부처에 과중한 부담이 될 수도 있으므로 우리나라의 실정을 반영한 부처간 정책 조율을 통해 어떤 식으로 피해국의 요청을 들어줄지에 대한 입장을 차기에 발표할 수 있다.

4. 국제인권법

(1) 정부 입장

인권 존중은 국제인권법상 확립된 의무로서 사이버 공간에서도 마찬가지이다. 우리 정부는 국제인권법이 오프라인에서와 마찬가지로 온라인상에서도 동일하게 적용된다고 본다. 사이버 공간에서도 프라이버시권, 표현의 자유와 정보접근권, 차별금지 및 혐오표현 방지 등을 포함한 기본적 인권이 여성과 사회적 약자를 포함한 모든 사람에게 보장되어야 한다.

(2) 분석 및 적용

국제인권법이 오프라인과 마찬가지로 사이버 공간에서도 적용된다는 것은 대다수의 국가가 동의하는 바이다. 하지만, 프랑스, 독일은 이에 대해 입장을 따로 밝히지 않았다. 프라이버시권, 표현의 자유와 정보접근권, 차별금지 및 혐오표현 방지 등의 기본적 인권이 보편적으로 보장되도록 하여야 한다는 것도 많은 국가들의 입장에서 공통적으로 도출되는 사항이다. 그러나 장래에는 선언적 수준을 넘어서 국가들이 사이버 공간을 규율하는 입법이나 정책을 추구할 때, 기본권 제한 여부 등 국제인권법 준수를 위한 검토를 해야 한다는 정도로 더 나아간 입장을 표명해도 된다. 그러나 인권 침해 피해자(내·외국인)를 위한 구제책을 마련해야 하는 의무를 부과하는 방식으로 더 강화된 국제인권법의 적용은 신중해야 한다. 이런 사항들은 국가의 의무를 확대하는 방향이라 특별한 결단이 필요하다. 아울러 인공지능을 비롯한 디지털 신기술의 발달로 인해 사이버 공간에서 발생할 인권 침해의 가능성을 인지하고 글로벌 플랫폼 사업자를 국가들이 적절히 규제하여 개인의 인권을 보호하는 등의 국가 간 모범 사례(best practice)에 관한 공유 체계를 제안할 수 있다.

5. 국제인도법

(1) 정부 입장

우리 정부는 사이버 활동으로 인하여 무력충돌이 발생하면, 국제인도법이 적용된다고 본다. 전시에 전투원들이 전투 수단 및 방법을 선택할 권리는 무제한적인 것이 아니며, 특정

무기가 무기체계의 적법성 검토에 부합한다고 하더라도, 실제 운용에서 구별의 원칙, 비례의 원칙 및 예방주의 등 국제인도법을 준수해야 한다고 했다.

(2) 분석 및 적용

국제인도법 분야에서 우리 정부는 순수하게 사이버 수단만을 이용한 국제적 혹은 비국제적 무력충돌이 발생할 수 있는지에 대해서는 언급하지 않는다. 일본은 이러한 'stand-alone cyber armed conflict'의 발생도 가능하다고 본 반면,[8] 독일은 국제적 무력충돌(국가 간 사이버 전쟁)은 몰라도 비국제적 사이버 무력충돌(사이버 내전)은 거의 발생할 가능성이 없다고 봤다.[9] 왜냐하면 독일 정부는 국가와 비국가단체 사이의 사이버 공격의 강도가 내전에 이를 정도가 될 가능성이 희박하다고 봤기 때문이다. 현재까지 물리적 무력충돌을 동반하지 않은 채 순전히 사이버 공간에서만 무력충돌이 발생한 적은 없기 때문에 의견이 나뉘지만, 기술이 고도로 발전된 미래의 전장은 누구도 장담할 수 없으므로 이 문제도 향후 검토해 볼 만하다.

사이버 공격은 은밀하게 기습적으로 수행해야 전략적 목표를 달성할 수 있는 특성이 있는데, 민간인 보호 등을 위해 사전에 '예방주의 원칙'(precaution)을 실천할 수 있는지에 대해서는 다소 의문이다. 즉, 군사 시설에 대한 사이버 공격을 하기 전에 주변에 민간 시설이나 민간인에게 미리 고지를 하게 되면 원래 의도한 군사적 사이버 공격은 수포로 돌아갈 가능성이 크다. 따라서 이 예방주의 부분에 대해서는 차기를 대비해 재검토할 필요가 있다. 지금은 국제인도법의 기본 원칙을 준수하겠다는 국가 의지의 표명 정도로 읽힐 수 있지만, 향후 국가들의 실행 양상에 따라 자기 발목을 잡을 수도 있기 때문이다.

결론: 우리 정부 입장의 현재와 미래

이번에 발표한 국가입장문은 현재 한국 정부가 해석하는 사이버 공간에서 적용 가능한 국제법에 관한 입장과 방향성을 공표한 것일 뿐, 최종적이고 불변하는 것은 아니다. 우리의 입장은 먼저 입장을 표명한 국가들과 비교할 때 전반적으로 무난하고, 딱 필요한 정도까지만 입장을 밝혔다. 프랑스 같은 국가들은 국제법 해석에 대한 나름의 자신감을 보이면서 분야에 따라 조금 더 나간 특징적인 논리를 펴기도 했다. 실제 국가들은 여러 차례에 걸쳐 자신의

입장을 조금씩 변경하거나 확장하는 등 국가 입장을 표명하는 중이다. 조약의 형태로 포괄적인 사이버 관련 국제법 체제가 한순간에 국제적 합의를 통해 도출될 가능성이 거의 없기 때문에 이러한 국가들의 입장 표명 과정 자체가 갖는 의미가 크다. 우리나라는 상시적으로 북한의 사이버 공격이나 사이버 범죄에 노출되어 있으므로 사이버 무력사용 및 무력공격과 그로 인한 자위권 행사 분야에 대해 좀 더 발전된 입장을 밝히고, 그에 미치지는 못하지만 사이버 주권 침해를 당한 경우에는 대응조치를 취하거나 국가책임을 물을 수 있다고 입장을 명확히 하면 좋겠다. 그리고 국제인권법을 비롯한 다른 분야에 대한 입장은 현재 입장을 유지하고 새로운 국가 관행이나 국제 규범이 나타날 때 다시 표명해도 될 것이다.

한국 정부의 첫 공식 입장 발표는 다소 늦은 감이 있지만, 그동안 관련 국제 기구의 논의나 국제 사회에서 사이버 관련 사안들에 대하여 적극적으로 참여하고 교류해 왔다. 신중했던 첫 국가입장문 발표 이후에는 더 적극적인 의견 표명과 참여를 지속하여야 할 것이다. 발표의 형식도 반드시 종합적으로 갱신된 국가입장문의 형식일 필요는 없다고 본다. 분야별로 필요하다고 판단할 때는 외교부 장관의 성명이나 앞으로 출범할 상설 '글로벌 메커니즘'에서의 논의에서 입장 발표 등 다양한 방식으로 국가 입장을 발전시킬 수 있다. 앞서 살펴본 국제법 주요 분야에 대한 입장을 변경하거나 더 발전된 해석을 밝힐 수 있다. 또한 국제형사법이나 외교·영사 관계 등 다른 국제법 분야로 확장하여 입장을 밝혀도 된다. 사이버 공간에서 계속 진행되는 국제적 사안들에 대한 국제법적 고려는 다른 국제 정치, 경제적 정세 및 전략적 고려 등과 함께 복합적으로 맞물려 돌아가는 것이므로 포괄적이고 전략적인 입장 검토가 요구된다. 그리고 그러한 국가 입장의 표명은 한국 정부의 구체적인 실행에 반영되어야 한다. 그렇게 함으로써 한국 정부의 공식 발표는 국제 사회의 신뢰를 얻을 수 있다.

[표 1] 한국의 국가입장문과 유사입장국과의 비교

	한국	미국	영국	프랑스	독일	일본
사이버 공간에서 국제법 적용	적용	적용	적용	적용	적용	적용
주권 불간섭 원칙	사이버 공간에서도 존중	사이버 공간에서도 존중	기본적 존중, 주권 효력 제한	사이버 공격은 주권 침해	사이버 공간에서도 존중 (기능손상포함)	사이버 공간에서도 존중
무력사용금지 자위권	적용	적용, 비국가행위자 대상 자위권 행사 가능	적용	적용 (물리적 결과 없는 기능손상 포함 가능성)	적용, 비국가행위자 대상 자위권 행사 가능	적용
국가책임 상당주의	적용, 경유국의 상당주의 의무	적용, 합리적 조치 취할 의무	적용, 합리적 조치 취할 의무	적용, 상당주의 의무	적용, 상당주의 의무	적용, 상당주의 의무
국제인권법	적용	표현의 자유 강조	오프라인과 동일한 보호	-	-	적용
국제인도법	적용, 구별, 비례성, 예방주의	적용, 필요성, 비례성	적용, 구별, 비례성, 필요성	적용, 구별, 비례성, 예방주의	적용 구별, 비례성, 예방주의	적용

저자

신소현 박사는 아산정책연구원의 외교안보센터의 연구위원이다. 주요 연구 분야는 정보보호 기술을 비롯한 신기술 (인공지능, 우주기술, 양자컴퓨팅 등)의 발전으로 생겨난 새로운 공간인 사이버 공간과 우주 공간과 관련된 각 국제법 분야의 변화와 발전이다. 무력충돌, 군사, 무기, 사이버첩보 등의 전통안보 뿐만 아니라 경제, 재난, 환경 등 새로운 비전통 안보분야들을 국제 및 국가안보의 관점에서 분석하고 관련 국제 및 국내규범의 형성과 변화 및 정책적 이슈들을 융합적으로 연구한다. 세종연구소 사이버안보센터 창립 멤버였으며 사이버안보포럼을 조직한 바 있고, 고려대학교 정보보호연구원 연구위원을 역임하였다. 최신 저작으로는 "사이버공간에서 국가의 적대적 허위조작정보 작전에 대한 규율", "우주안보와 국제법", "사이버 억지와 미국의 선제적 방어전략의 국제법적 검토" 등이 있다.

---

[1] UNGA, *Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025 Draft Final Report* (A/AC.292/2025/CRP.1 11 July 2025)

[2] United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (adopted 24 December 2024 open for signature 25-26 October 2025) <https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=_en> accessed 25 June 2025.

[3] 외교부, [사이버안보] 사이버 공간에서의 국제법 적용에 관한 우리 정부의 입장 (2025.07.07) <https://overseas.mofa.go.kr/www/brd/m_3993/view.do?seq=366224&page=1> accessed 10 July 2025.

[4] Jeremy Wright MP, *Cyber and International Law in the 21st Century* (23 May 2018)

[5] Ministère des Armées, *Droit International Appliqué aux Opérations dan le Cyberspace* (9 September 2019)

[6] *Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America)* (Merits) [1986] ICJ Rep 14.

[7] *Supra* note 4.

[8] Ministry of Foreign Affairs of Japan, *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations* (28 May 2021)

[9] Federal Government of Germany, *On the Application of International Law in Cyberspace (Position Paper)* (March 2021)