https://doi.org/10.33778/kcsa.2019.19.2.021

사이버 공격과 정당방위의 당위성

신 경 수*

요 약

제4차 산업혁명 시대로 불리는 초연결-초지능 사회의 출현은 안보 환경의 새로운 변화를 가져왔다. ICT(정보통신기술) 융·복합 하이테크 기술이 전 방위적으로 도입되면서 현실 공간을 움직였던 사람 중심의 동력은 코드를 중심으로 한 사이버 공간으로 대체되고 있으며, 그 의존도는 계속 높아지고 있다. 하지만 이러한 기술적 변화는 역설적으로 우리 사회를 위협하는 또 다른 안보취약점으로 작용하고 있으며, 과학기술이 가져온 기회와 도전을 동시에 직면하며 사이버 방어체계를 구축해야 하는 당위성을 가져왔다. 이에 본 연구에서는 갈수록 지능화되고 대규모로 진화하고 있는 사이버 공격에 적극적으로 대응할 수 있는 이론적 근거로 정당방위 이론을 제시하였고, 이에 대한 자주적 사이버 안보전략 수립 방향으로 첫째, 사이버 안보법 제정의 필요성 둘째, 미국 등 사이버 강대국들과의 대응공조 체계 마련 셋째, 사이버 인력을 어떻게 양성할 것인가에 대한 방안 마련을 제언하였다.

Cyber Attacks and Appropriateness of Self-Defense

Kyeong-Su Shin*

ABSTRACT

The emergence of a hyper-connected-super-intelligence society, called the era of the Fourth Industrial Revolution, brought about a new change in the security environment. With ICT (Information Communication Technology) convergence and high-tech technologies introduced across the board, the person-centered driving force that moved the real space is replaced by the code-oriented cyberspace, and its dependency is constantly increasing. Paradoxically, however, these technological changes serve as another security vulnerability that threatens our society, and have brought about the justification for building a cyber defense system while simultaneously facing the opportunities and challenges brought by technology. In this study, the theory of self-defense was put forward on the basis of the theoretical basis for actively responding to the increasingly intelligent and mass-evolving cyberattacks, and firstly, the need to enact a cybersecurity law, secondly, and thirdly, the need to develop a response cooperation system with the U.S. and other cyber powers.

Keywords : Cyber Security, Cyber attack, Theory of self-defense, Independent Cyber Security Policy

접수일(2019년 5월 29일), 수정일(1차: 2019년 6월 24일), 게재확정일(2019년 6월 29일)

* 경찰대학 치안정책연구소

1. 서 론

제4차 산업혁명 시대의 출현은 안보 환경의 새로운 변화를 가져왔다. ICT(정보통신기술) 융・복합 하이테크 기술이 전 방위적으로 도입되면서 현실 공간을 움직였던 사람 중심의 동력은 코드를 중심으로 한 사이버 공간으로 대체되고 있으며, 그 의존도는 계속 높아지고 있다.

사이버 공간은 국가와 문화의 경계를 넘어 네트워크가 연결된 모든 도시와 개인 간의 간극을 좁혀가고 있다. 그동안 국가와 영토라는 개념이 제한적이나마 통제될 수 있는 존재였다면, 사이버 공간이라는 비영토적・비제한적 개념은 통제라는 용어가 무의미할 정도로 우리의 의식구조를 재(再)정의하고 있다.

사이버 공간에 대한 평가는 매우 논쟁적이지만 이미 사회 구성원들은 자신의 의지와 상관없이 사이버 세계를 접하고 있으며, 필요 이상의 영향을 받고 있다. 그리고 이러한 기술적 변화는 역설적으로 우리 사회를 위협하는 또 다른 취약점으로 작용하고 있으며, 과학기술이 가져온 성장의 기회와 위협의 도전을 동시에 마주보는 평행선을 달리도록 강요하고 있다.

자신을 철저하게 은닉하면서도 치명적인 위협을 감행할 수 있는 사이버 공격의 특성은 피해를 즉시 인지하는 것조차 쉽지 않을 뿐더러 공격자가 사용한 악성코드(Malicious Code)를 분석・추적하는 일련의 과정도 매우 복잡하다. 이와 같은 장점 때문에 해커들은 우리 사회의 네트워크 방어체계를 무력화시킬 수 있는 사이버 무기를 개발하고 시연하고 있다.

이에 본 연구는 전통적인 방식의 안보개념과는 다른 특성을 가진 새로운 사이버 공격에 적극적으로 대응할 수 있는 이론적 방안을 모색하고, 자주적 사이버 안보전략의 수립 방향을 제시함으로서 안정된 사이버 안보 확립에 기여하고자 함에 그 목적을 두고자 한다.

2. 이론적 배경: 정당방위 이론

2.1 정당방위 이론의 개념

정당방위(Self-Defense)란 인간의 자연적인 자기 보존의 본능으로서, 인류사적으로 모든 시대를 통하여 인정되고 있는 정당화 사유를 말한다.

자기결정 능력을 신뢰하면서 해악에 대한 처벌만을 목적으로 한 응보형주의(應報刑主義)와는 달리 오로지 규범적 사고에서 이루어지는 합법칙적 인과관계에 의해서만 행위책임을 부여하는 상대적인 개념이다. 이 연구에서는 이러한 개념적 정의를 사이버 안보를 위한 대응방안의 핵심 준거로 준용하고자 한다.

정당방위 이론은 사이버 위협에 대한 적극적인 대응방안을 마련하기 위해 즉각적인 역(逆)공격 등 능동적인 대응을 할 수 있는 이론적 뒷받침이 반드시 필요하다는 당위론적 사고에서 출발하였다. 물론 이러한 개념의 기본적인 배경이 반드시 공세적 입장만을 추구하지는 않는다. 이는 오히려 강력한 방어효과를 나타낼 수 있는 안정된 사이버 안보체계를 구축함으로서, 해커들의 공격 의지를 사전에 차단할 수 있는 평화적 해결방안의 일환으로 볼 수 있다.

그동안 발생했던 사이버 공격들의 대부분은, 공격 주체와 침투 방식 등의 개괄적인 내용을 공개하는 것으로 종결되었고, 이들을 처벌하거나 배상을 청구하는 등 해킹 공격에 대한 강도 높은 책임을 부과하지 못하는 모습을 보여 주었다. 뿐만 아니라 공격 행위에 대한 원인과 결과 사이의 연결고리에 중요한 해악성이 있다는 사실을 배제한 채 손실 보상에만 초점을 맞추어 대응함으로서 정부의 대응 프로세스에 대한 신뢰도를 오히려 낮추는 우(憂)를 범하였다.

치밀하게 제작된 악성코드에 의해 발생하는 직접적 또는 부수적 피해에 대해 국가가 공격 주체에게 그 피해에 대한 철저한 책임과 처벌을 부과하지 못하는 모습은 실효적 국가가 가지는 당연한 의무이자 주권국가로서의 안보적 책임에 부합하지 못하는 행동으로 볼 수 있다.

따라서 사이버 침해행위에 대해 강력한 사이버 보호권을 발동할 수 있는 정당방위 이론을 통해 사이버 공격이 탐지됨과 동시에 즉각적인 역공격과 추적 그리고 처벌까지 행할 수 있는 이론적 근거가 마련되어야 한다. 이는 국가가 가진 당연한 자위권의 행사이자 이러한 근거가 뒷받침되어야만 국가안보를 위한 최소한의 방어체계를 구축할 수 있다고 보기 때문이다.

2.2 정당방위 이론의 근거 논의

정당방위 이론을 구성하는 대원칙은 법질서 수호의 원리에서 찾을 수 있는데, 이는 국민 안전과 국가 안보를 위한 기본 원칙으로 작용한다. 물론 우리 형법상의 정당방위의 원칙이 국가적・사회적 법익을 보호하기 위한 개입을 원칙적으로 허용하지 않고 있으나, 이는 어디까지나 현실 공간에서 발생하는 개인적 법익을 위한 법리에 타당한 논리 전개일 뿐, 개인의 보호수준을 넘어선 사이버 공간의 독특한 특성에는 적용될 수 없는 개념이다.

사이버 공간은 그 자체만으로도 매우 광범위하며, 그만큼 공격할 수 있는 취약점도 많은 곳이다. 따라서 국가라는 유기적인 집합체와 연결한 네트워크 공간의 한정적 침해영역을 구분하지 않고서는 사이버 위협에 효율적으로 대응하지 못하는 불안요소로 작용할 수 있다. 이러한 이유로 사이버 안보체계를 안정적으로 구축하기 위해서는 사이버 공격에 대한 자위권 발동으로 한정하지만, 국가의 영역에 포함되는 모든 네트워크를 하나의 방어공간으로 간주해 이에 대한 공격적 침해행위가 발생하였을 경우에는 정당방위 이론을 적용해 동시에 반격을 할 수 있는 개념적 정의를 부여해야 한다.

물론 정보의 자유로운 선택과 접근이 보장된 네트워크 공간에서 사이버 공격에 대한 반격, 응징 등 역공격 행위를 명시하며, 공세적인 대응방안을 천명하는 것은 디지털 공간의 본래의 취지를 왜곡하는 행위로 비난을 받을 수 있으나, 수세적인 입장이 아닌 강력한 대응 공세를 펼칠 수 있는 능동적인 방안을 마련하는 것은 사이버 안보를 확립하기 위해 반드시 필요하다고 본다.

이에 본 연구에서는 이러한 정당방위 이론의 실질적인 근거를 마련해보고자 이론적 유사성을 도출해 보고자 'UN 헌장 제2조 4항, 제52조'와 '탈린매뉴얼'로 한정하여 이론의 근거로 삼을 수 있는지 분석해보았다. 결론부터 말하자면 두 가지 모두 사이버 공간의 침해 행위에 대한 적절한 해답을 갖지 못한 것으로 보인다.

먼저, UN 헌장 제2조 4항에는 "모든 회원국은 그 국제관계에 있어서 다른 국가의 영토 보전이나 정치적 독립에 대하여 또는 국제연합의 목적과 양립하지 아니하는 어떠한 기타 방식으로도 무력의 위협이나 무력행사를 삼간다."라고 규정하고 있고, 제52조에는 "이 헌장의 어떠한 규정도 국제연합회원국에 대하여 무력공격이 발생한 경우, 안전보장이사회가 국제평화와 안전을 유지하기 위하여 필요한 조치를 취할 때까지 개별적 또는 집단적 자위의 고유한 권리를 침해하지 아니 한다…"고 규정하고 있어 무력에 의한 위협을 받았을 경우 개별적 자위권을 발동할 수 있다고 명명하고 있다.

그러나 이러한 조항을 사이버 공간에 적용하기 위해서는 다음과 같은 혼란을 가져 올 수 있다. 우선, 무력의 위협에 대한 범위가 명확하지 않다는 점을 들 수 있다. 일반적으로 무력 분쟁이라 함은 "어느 일방 당사국이 타방당사국을 굴복시켜 그가 바라는 강화조건을 부과하여 본래의 주장을 관철하기 위해 무력을 행사하는 국가 간의 투쟁상태"를 말하는데,[2] 여기서 말하고 있는 무력(Force)의 의미에 사이버 공격을 포함하는지에 대한 국제사회의 합의된 해석은 아직까지 보이지 않는다. 또한, 무력분쟁에 관한 국제법의 논리가 기본적으로 물리적 공간에서 발생하고 있는 적대 세력의 군사적 능력을 무력화화기 위한 수단적 근거로 제시되고 있다는 점에서 사이버 공격에 사용되는 악성코드를 과연 무기(weapon)로 보아야 하는지에 대한 명확한 기준이 마련되지 못하는 문제점이 있다. 만약, 코드를 '악용 하였을 경우에는 무기로 볼 수 있다'라는 가정이 성립하더라도 이를 개인 또는 단체에 자행되는 사이버 공격에 적용할 수 있는지에 대한 해석 역시 모호해진다.

제52조의 규정 또한 해석적 난제에 부딪힌다. 여기서 말하는 개별적 자위권을 행할 수 있는 조건인 “무력 공격이 발생하면(if an armed attack occurs)”이라는 단서조건의 발생 시점과 범위에 대한 모호성이 남아있다.

사이버 공간의 시・공간 개념은 매우 불안전하다. 시간의 왜곡성과 공간의 비(非)분화성은 이것을 조작하는 인위적인 행동에 의해 충분히 변형이 가능하다. 현실 공간에서는 병력과 무기가 실질적으로 이동을 하고 그에 따른 궤적이 실시간으로 파악할 수 있지만, 사이버 공간에서 발생하는 데이터의 이동은 그 궤적을 실시간으로 파악하기가 매우 어려울 뿐만 아니라 설령 파악하더라도 공간에 대한 범위를 측정하는 것이 불가능하다. 따라서 ‘무력 공격이 발생하면’이라는 시간적 제한성을 사이버 공간에서 적용하기란 매우 어려워 보인다.

탈린 매뉴얼은 기본적으로 NATO나 국제사회가 공식적으로 채택한 구속력 있는 법규나 조약이 아니다. 이는 일종의 가이드라인의 성격으로 바라보는 것이 타당한데, 여기에 따르면 사이버 전쟁의 핵심 요소인 사이버 공격은 인명 살상이나 목표물의 손상 등 물리적 타격으로 이어질 수 있는 사이버 환경을 의미한다. 즉 침해를 받은 경우 비례성의 원칙에 따라 대응조치를 취할 수 있는 일종의 자위권을 인정하고 있다. 특히, 무력사용이 가능하다고 기술하고 있으며, 이는 치명적이고 파괴적인 물리적 피해가 있어야 한다는 전제아래 시행될 수 있다.

그러나 탈린매뉴얼은 사이버 공간의 침해행위에 대한 전제를 전쟁을 토대로 작성하였고, 이에 따라 자위권을 행사할 수 있는 근거를 파괴적인 피해가 발생한 시점에서 찾고 있다. 이를 적용하였을 경우, 이미 사이버 공격으로 인해 네트워크가 파괴되고 이 결과가 현실 공간에 치명적인 영향을 미친 후에야 반격이 가능하다는 해석이 나온다. 따라서 UN 헌장 제2조 4항, 제52조와 탈린매뉴얼의 핵심내용은 본 연구에서 제시하는 정당방위 이론과 그 시점에서 상당한 차이를 보이고 있다.

3. 문제점: 사이버 주권의 확립

사이버 안보체계를 확립하기 위해서는 사이버 공간을 위협하거나 침해하는 일련의 공격 행위들에 대해 적극적인 규제와 대응을 할 필요가 있다.

최근 사이버 공격이 주요 국가기간 망에 대한 파괴를 목표로 끊임없이 시도되고 있고, 국가와 민간영역을 구분하지 않고 다양한 형태로 심각한 안보위협을 주고 있는 상황에서 우리 정부는 사이버 공격에 대한 탐지, 차단, 분석 및 대응을 어떻게 해야 하는지에 대해 여전히 체계적이지 못한 모습을 보여주고 있다.

이에 그동안의 대응체계의 문제점을 정리해 본다면 우선, 공격을 감행한 공격 주체에게 상응한 사이버 역공격을 할 수 있는 자위권 발동 요건과 법체계의 부재를 들 수 있다. 공격에 의해 피해를 입은 수많은 사례의 공통점은 모두 이에 대한 책임을 공격 주체에게 묻지 못했다는 점이다. 이는 결정적 증거를 확보하는데 시간이 많이 걸리고 이러한 증거확보를 할 수 있는 체계적인 시스템이 마련되어 있지 못하는 문제점을 가지고 있는 점에도 기인 있지만, 국가의 고유한 영역을 침해받으면서도 이에 대한 단속을 적극적으로 행사하지 않는 수동적 자세 역시 확고한 사이버 안보체계를 마련하는데 문제점으로 발생한다.

아울러 사이버 위협정보에 대한 공유체계가 매우 미흡하다는 점을 들 수 있다. 사이버 공격은 악성코드와 공격방식 등의 정보만으로도 방어의 신속성을 제고할 수 있는 여지가 매우 높은 영역이다. 이는 2차 피해 대상기관에게는 사전방어 효과를 가져 올 수 있고, 이미 피해를 입은 시스템에 대한 추가적인 피해도 막을 수 있다. 물론 공격에 사용된 악성코드가 공개되어 해커들이 C&C 해킹 인프라를 변경하는 등 위험이 따르지만 주체의 식별보다 피해의 확산을 즉각적으로 차단할 수 있다는 측면에서 사이버 위협정보를 공유하는 것이 타당하다.

국제사회는 대부분 군사적・정치적・경제적 연결망을 통해 국가 간의 평화적 균형 상태를 유지

할 수 있도록 질서구조에 많은 영향력을 부여하고 있다. 이에 비해, 사이버 공간에서 보여주는 국제질서 관계는 이러한 지구적 상호연결의 강도에 비해 상대적으로 낮은 단계의 통제력을 가지고 있는데, 이는 국가 간 행동의 다자간 규제조치는 물론 UN으로 대표되는 집단안보체제의 기능 역시 매우 제한된다는 것을 의미한다. 실제로 강대국들의 정치・군사・문화세력이 현실 공간에서는 매우 높은 수준으로 유지되면서 국제사회에 커다란 영향력을 미치고 있으나, 사이버 공간에서는 그 영향력의 범위를 한정할 수 있는 새로운 형태의 흐름이 발생하고 있다는 것을 말해준다.

사이버 공간을 명확히 정의할 수 있는 초월적 권위는 여전히 부재한 상태이며, 개별 국가들의 사이버 공격에 대한 대응체계는 다양한 방식으로 분절되어 나타나고 있다. 결국 사이버 안보는 국제사회가 해결해 줄 수 없는 영역이자 이를 방치할 경우 자칫 안보 공백상태를 가져올 수 있는 위험성을 가지게 되는 요인이 되고 있다.

국가 안보를 바라보는 시각적 정의는 정치 분야에 있어 가장 심오하고 오래된 이슈 중의 하나이며, 이를 정의하는 주체의 준거적 사고에 따라 새롭게 정의되는 가변적 요소가 큰 영역이다. 따라서 사이버 공간에서 주권을 공교히 하는 것은 우리 사회의 안보정체성에 명확한 개념을 부여함으로서 공격자에게 강력한 대응조치를 취한다는 의지를 보여줄 수 있는 효과를 가져 올 수 있다.

결국 체계적이고 강력한 안보전략을 수립하기 위해서는 침해행위에 대한 해석을 어떻게 할 것인지에 대한 명확한 입장을 제시하여야 하는데, 본 연구에서는 사이버 공간을 전통적인 지정학적 원칙과 다르지 않다는 점을 강조하며, 주권국가의 개념을 적용해 정당방위 이론에 필요한 기준점을 제공하고자 한다. 그리고 이러한 주권 개념을 부여하는 이유는 다음과 같이 정리해 볼 수 있다.

첫째, 사이버 공간은 국제사회의 공역으로만 인식해서는 해결할 수 없는 영역으로 반드시 개별 국가의 주권을 인정해 국내법을 적용한 대응방안을 모색해야 한다. 이는 사이버 안보체계를 수립하는 데 있어 국제사회가 일류공동체 의식을 바탕으로 시간과 공간을 초월한 단결성을 보여주지 않는 한 사이버 공간에 대한 개별 국가들의 목표와 지향점이 서로 상이하다는 점과 함께, 공통적 사고에 의해 제한할 수 있는 네트워크 공간의 경계획정이 사실상 불가능하다는 점을 전제로, 사이버 공간에 의해 발생하는 무력행위는 국내문제로 인식하고, 국민국가의 주권적 시각에서 문제를 해결해야하기 때문이다.

물론, 사이버 공간이 가지는 초경계적・초국경적 특성에 의해 경계가 확실한 국가영토와 일치하지 않는다는 점을 들어 침해공간의 경계 획정문제가 발생할 수 있으나, 국내로 유입되는 트래픽(Traffic)의 경로에 의해 국내법 적용을 부여하는 시점과 장소가 명확히 탐지될 수 있으므로 해결될 수 없는 영역으로 보이지는 않는다.

둘째, 사이버 공격행위에 대한 가벌성 책임요소를 부과하기 위한 구조적 배경으로 주권 개념을 부여할 필요가 있다. 이는 정당방위 이론의 근간이 되며 이를 바탕으로 행해지는 적극적인 사이버 안보전략의 기초가 된다. 따라서 여기서 말하는 주권은 국가와 국민에게 위해를 가할 수 있는 일체의 행위에 대한 공격과 방어를 의미하며, 사이버 공간에서 간섭을 받지 않고 주권을 완전히 행사하는 독립된 권리를 의미한다.

셋째, 정당방위 이론에서 말하는 법질서의 불가침성은 사이버 주권이 부여됨으로서 구성될 수 있는 사이버 안보체계의 제1요소로서, 우리 사회에 영향을 미치고 있는 사이버 공간의 질서구조에 대해 혼란을 야기할 수 있는 공격 행위를 국가안보의 심각한 위협 행위로 인식하고, 공공의 안녕을 도모할 수 있도록 주권침해의 개념을 적용해 국가기관이 이를 탐지・식별할 수 있는 기술적 능력을 보유함으로서, 즉시 역(逆)공격을 감행할 수 있는 근거를 마련할 수 있는 기능적 뒷받침을 의미한다.

질서에 대한 관념적 정의는 시대적 특성에 따라 변화하는 유동적이고 상대적인 개념으로 사용자의 시각에 따라 접근방식이 다양하게 변하지만, 사이버 위협이라는 의미는 국가의 보호법익에 대

한 침해 행위뿐만 아니라 침해 가능성까지를 내포하고 있는 보편적 개념으로 사이버 주권의 확립은 네트워크 세계의 평화적 내재화를 위한 최소한의 요건이자 최우선적으로 부여되어야 할 전략적 개념이다.

물론 사이버 영역이 정부뿐만 아니라 민간영역과 매우 밀접하게 연관되어 있고, 이에 대한 침해 행위에 대한 국가의 개입이 자칫 사적자치의 영역을 침해하는 것으로 이해할 수 있으나, 전염병의 확산처럼 개인의 영역에서 발생한 컴퓨터 바이러스를 통해 국가 전체의 네트워크 시스템을 감염시킬 수 있는 여지가 매우 높은 사이버 공격에 있어 국가의 보호활동은 보충적으로 적용해서는 안 된다.

우리사회는 이미 제4차 산업혁명 시대로 접어들었다. 이는 곧 수많은 IT 기술이 정치・경제・문화 등 우리 사회 곳곳에 융합되어 있음을 대변함과 동시에 네트워크 테크놀로지가 현실 공간의 모든 사물과 분리될 수 없음을 의미한다. 하지만 해커들은 이러한 공간융합 시대의 변화의 물결을 오히려 자신들의 정치적・경제적・군사적 수단으로 이용하고 있고, 물리적 공간에선 찾을 수 없었던 새로운 공격 루트인 사이버 공간을 이용해 침투하고자 한다. 따라서 이들의 비인도적 사이버 공격 행위에 대한 확실하고도 강력한 처벌과 대응을 위해서는 반드시 사이버 주권의 개념이 확립되어야 할 것이다.

4. 정당방위 이론을 적용한 자주적 사이버 안보전략 수립 방향

이제 사이버 위협은 광범위하고 다양하게 움직이고 있어 이를 모두 방어한다는 것은 매우 버거운 일이 아닐 수 없다. 이전까지 대응형태가 주로 공격에 따른 피해복구에 집중되어 수습방안을 마련하는 등 수동적 입장의 대응이 주류를 이루어 왔다면, 이제부터는 사이버 안보라는 장기적 목표에 새로운 방향을 설정하여, 다변화되고 있는 사이버 환경에 적합한 실질적인 방어체계의 효과를 기대할 수 있도록 정당방위 이론을 적용한 자주적 사이버 안보전략을 중심으로 패러다임의 전환이 필요하다.

여기서 말하는 자주적 사이버 안보전략이란 사이버 공간에서 치열하게 움직이고 있는 각종 위협에 대해 즉각적인 반격을 포함한 강력한 처벌을 행함으로서, 그동안 침해를 받고도 아무런 제재를 하지 않았던 수세적 입장에서 벗어나 사이버 주권을 통한 힘의 우위를 점하고, 방어와 공격을 동시에 수행할 수 있는 전략형태의 기반을 마련한다는 것을 의미한다.

이를 구체적으로 기술한다면, 기존의 수세적인 사이버 방어체계와 달리 일종의 정치적・군사적 요소가 가미된 공세적인 대응방안으로 적극적인 사이버 역공격을 가할 수 있는 능력을 보여줌으로서, 사이버 영역에 대해 전략적 우위를 차지하고, 더 이상 해커가 도발을 할 수 있는 사기(使氣)를 억지할 수 있는 적극적인 사이버 안보프레임을 의미한다.

그리고 이를 뒷받침하고 있는 정당방위 이론은 적극적인 역공격의 근거를 마련해줌으로서 전략의 완전성을 높여준다. 물론 이 이론이 기존의 안보이론 중의 하나인 선제공격(Preemptive Attack) 및 예방공격(Preventive Attack)과 다소 유사한 형태로 인식될 수 있으나, 선제공격이 가지는 의미가 적(敵)이 공격하려는 의도를 가지고 이미 전쟁 준비가 완료된 상황에서 상실된 주도권을 회복하고자 자신에 대한 자위를 도모하는 차원에서 실시하는 공격을 말하고 있고, 예방공격의 뜻이 아직 임박하지는 않았지만 적의 위협이 확실하게 예견된다는 전제 하에 방어를 목적으로 예방차원에서 미리 공격하여 위협을 제거한다는 것을 의미하는데 비해 접근시점과 방식에 있어 분명한 차이가 발생한다.

이 두 가지 개념을 자주적 안보전략의 근거로 적용하고 싶어도, 물리적인 공간에서 보여주는 외교 중단, 군사력 증강 등 위협 징후에 비해, 사이버 공격은 임박한 위협에 대한 예견이라는 필요조건을 충족할만한 근거를 찾기가 어렵다는 단점이 있다. 이러한 이유로 선제공격과 예방공격을 유사

한 개념으로 해석하는 것은 맞지 않는다고 본다. 하지만 침해에 대한 정당방위를 근거로 한 자주적 사이버 안보전략이라는 개념의 모호성이 분명히 존재한다는 점에 비추어 볼 때, 어느 정도 공세적 안보기조의 이론적 담론이 전이되었다는 점에 대해서는 주지하고자 한다.

사실 사이버 공간에서 발생하는 위협에 대한 즉각적인 탐지와 식별에 대해서는 이를 지극히 단순화한 추정에 의하지 않고서는 쉽게 행할 수 있는 부분이라고 명명하기가 매우 어렵다. 실무적으로 사이버 공격행위를 시행한 공격 주체를 정확히 찾아낸다는 것은 디지털 포렌식 작업을 통해서만 추정할 수 있는데, 만약, 해커들이 세계 각지에 임시 근거지를 두고 차량으로 이동하면서 모바일 네트워크를 이용해 공격행위를 가한다면, 위치측위가 어려워 해당 국가들과의 사이버 공격에 대한 긴밀한 공조체계 없이는 강력한 사이버 안보전략을 구사하기가 매우 어려운 과제임에 틀림없다.[5]

이러한 상황에서 주장하는 자주적 안보전략의 핵심은 현실적으로 모든 사이버 공격을 원천적으로 막아내는 것이 불가능하다는 명제를 거울삼아 침해행위에 대한 명확한 법적 처벌과 국제사회와 공조한 외교압박, 그리고 군사보복을 포함한 역공격행위를 위한 준비태세를 갖추어야 한다는 점에 있다. 이에 대한 세부적인 내용은 다음과 같이 정리해 볼 수 있다.

첫째, 법체계의 정비가 필요하다.[3] 해커들을 상대로 직접적인 법적 처벌을 가할 수 있는 강력한 처벌 법규가 마련되어야 할 것이다. 현재 사이버 안보와 관련 산재된 법률들은 대부분 정보통신 분야에 집중되어 있고, 이는 국가안보차원의 시각으로 바라보는 사이버 문제를 제한하는 오류를 범할 수 있기 때문이다. 특히, 제3국가에서 해킹을 시전한 공격자를 현지에서 체포 인도하여 국내의 법정에 서울 수 있는 관련법을 제정해야 한다.

둘째, 사이버 공격에 대한 미국 등 선진국들과의 대응공조 체계가 마련되어야 한다. 사이버 공격행위를 안보위협 행위로 공식적으로 입장을 내놓고, 이에 대한 공조체제 수립을 위한 방안을 외교적 차원에서 확립해야 할 것이다.[1] 미국은 이미 NATO는 물론 아시아・태평양 지역의 주요 국가들과의 협력을 통해 군사동맹 관계 차원의 사이버 안보 동맹정책을 구현하고 있다.[4] 이러한 사이버 공간에서의 안보 공동체 구축은 상호간의 정치・군사구조의 발전 과정을 말하며, 동맹국 간의 내재해 있는 사이버 역동성을 공유하는 것을 의미한다. 따라서 우방국인 미국과의 기술·정보공유 및 협력체계를 구축하는 문제를 심도 있게 추진하여야하고 이행하여야 한다. 실제로 미국은 수많은 정보기관을 통해 다양하고 복잡한 사이버 정보를 수집·분석하고 있다. 따라서 한·미간 실용적인 정보 공유체계가 구축된다면, 사이버 안보강화에 대단히 유용한 전략적 가치를 가지게 될 수 있다.

셋째, 사이버 인력을 어떻게 양성할 것인가에 대한 구체적인 대책이 반드시 필요하다. 그동안 정부는 민간 기업과 협력하여 사이버 안보환경을 구축하고 사이버 위협에 대처하기 위해 많은 투자를 해온 것이 사실이다. 그러나 자주적 안보전략을 구사하기 위해 가장 필요한 것은 이를 구현할 수 있는 인력과 재능의 양성에 있다. 한국은 아직도 사이버 안보에 대한 인식제고와 교육훈련 프로그램이 매우 미약하다고 할 수 있다. 일부 대학에서 '정보보호학'을 중심으로 사이버 보안기술 분야에 대해 커리큘럼을 만들어 운영하고 있지만, 국가 차원에서 사이버 인력을 구성하는 계획은 아직 마련되지 못했다. 따라서 이에 대한 구체적인 계획 수립이 더욱 강력한 사이버 안보 태세를 갖추기 위한 첫걸음이자 진화하는 사이버 안보에 대한 의식을 확산시키는 방안이라고 생각한다.

그러나 민주주의 체제에서 사이버 공격을 위한 주입식 교육을 기획하는 건 상상하기 어려운 일이다. 이에 민간영역에서 활동하고 있는 해커 전문가들을 국가안보를 위한 공조체제의 영역으로 끌어올 수 있는 동인을 제공해 양성화할 필요가 있다.

민간 사이버 보안전문가들은 그 숫자조차 파악이 어려울 정도로 다양한 분야에서 활동하고 있으며, 이들을 국가적 자산으로 끌어들일 수 있다면

막대한 인력과 자본의 투입 없이도 고급인력의 지식을 활용할 수 있게 된다. 지금까지는「정보통신망법」등에 의하여 민간전문가들이 침해당한 서버 등에 조사를 하지 못하도록 규정하고 있었는데, 이제는 이미 침해당하거나 침해당할 위협에 임박한 경우 이들이 자세한 공격 코드 등을 조사하여 정부에 발 빠르게 신고하여 줌으로서 정부의 대응을 효과적으로 상승할 수 있는 동반효과를 가질 수 있도록 유기적으로 변해야 한다. 결국 이들의 행동이 사이버 안보의 기틀을 마련할 것이다.

이상과 같은 내용은 모두 한국의 효과적인 대응방안을 위해 필요한 제반 조건이며, 사이버 공격에 대한 적극적으로 반응을 보여줌으로서 국가안보를 확립할 수 있는 기반을 마련하는 것이라 할 수 있다.

5. 결 론

사이버 공간에 대한 안보 논의는 끊임없는 논제로 제기되어 왔고, 공격 행위를 포함한 모든 불법행위에 대해 아직까지도 명확한 제재방안을 마련하지 못했음은 물론, 사이버 질서관계를 어떻게 볼 것인가에 대한 기초적인 합의조차 이르지 못하고 있다.

본 연구의 관점이 사이버 관계를 냉엄한 힘의 투쟁 관계로 보는 것은 아니지만 이제 사이버 공격에 대한 균형을 넘어 압도적 우위를 가지는 것이 매우 중요하다고 생각된다. 이를 위해 사이버 안보에 있어 확실한 통제권을 부여할 수 있는 자주적 사이버 안보전략을 수립해야 하고, 그 이론적 근거로 정당방위 이론을 제언하고자 한다.

이는 정당방위 이론을 통해 사이버 공격을 국익에 대한 침해 위협요소로 판단하고 국가의 피해에 대한 보호원칙을 작용해 공격 주체에게 법적 처벌과 응징을 할 수 있는 근거를 마련해 사이버 침해에 대한 강력한 의지를 보여줄 수 있는 역공격 또는 공세적 타격을 할 수 있는 능동전략으로 사고의 전환이 이루어져 한다는 것을 의미한다.

참고문헌

[1] 김동희·박상돈·김소정·윤오준, “사이버 위협정보 공유체계 구축방안에 관한 연구 - 미국 사례를 중심으로”, 융합보안논문지, 제17권제2호, 2017.

[2] 이민효, 『무력분쟁과 국제법』, (서울: 연경문화사, 2008)

[3] 이용석·임종인, “사이버 대응태세 구축을 위한 법·제도적 개선방안 연구”, 융합보안논문지, 제19권제1호, 2019.

[4] 이종진, “미국-일본 사이버 안보 정책과 아시아·태평양 지역 안보동맹”, 한국국제정치학회 60주년 기념 연례학술회의 발표자료, 2016, 3

[5] 황태진·원동호·이영숙, “모바일 포렌식을 이용한 메신저 등거 비교 분석 연구”, 융합보안논문지, 제18권제2호, 2018.

[6] Piret Pernik, Jesse Wojtkowiak, Alexander Verschoor-Kirss, “National Cyber Security Organization: United States, NATO: Tallinn, 2016.

[7] Jenny Jun Scott LaFoy Ethan Sohn, 『North Korea's Cyber Operations: Strategy and Responses』, Rowman & Littlefield, 2016.

[8] Nir Kshetri, “Cyberwarfare in the Korean Peninsula: Asymmetries and Strategic Responses”, East Asia, Volume 31, Issue 3, 2014.

[9] John Robertson, and 5 accompanying persons, 『Darkweb Cyber Threat Intelligence Mining』, UK: Cambridge University Press, 2017.

〔저자소개〕

신 경 수 (Kyeong-Su Shin)
2008년 2월 연세대학교 정치학 석사
2018년 2월 충남대학교 정치학 박사
現. 경찰대학 치안정책연구소
email : kurukury@police.go.kr