JEJU PEACE INSTITUTE
제주평화연구원

JPI 정책포럼

발행인 | 문태영 · 주소 | 제주특별자치도 서귀포시 중문관광로 227-24 (697-858) · Tel: 064)735-6500 · Fax: 064)738-6552 · www.jpi.or.kr

No. 2015-19

사이버공격과 사이버억지:
국제정치적 의미와 대안적 패러다임의 모색

민병원 (이화여자대학교 정치외교학과 교수)

사이버공간의 지속적인 발전은 국가 간 교류를 활성화시키는 역할을 수행하는 동시에 복잡한 갈등의 원천으로 자리 잡고 있다. 사이버공간에서는 사이버침해, 사이버공격, 첩보 등 다양한 형태의 공격이 매우 빈번하게 일어나고 있으며, 이를 방어 또는 억지하기 위한 노력도 지속적으로 강화되고 있다. 사이버공격은 지난 10여 년에 걸쳐 간헐적으로 이루어져 왔지만, '올림픽게임' 작전과 같이 물리적 피해를 야기하는 수준에 이르렀다. 특히 지능형 지속위협(APT)으로 알려진 사이버공격은 구체적인 목표를 달성하기 위한 체계적인 노력으로서 오늘날 사이버공간에서 군사적 목표뿐 아니라 일상생활에서도 위협의 중요한 원천이 되고 있다. 이처럼 사이버공간에서 벌어지는 새로운 유형의 갈등은 '사이버안보' 문제가 국제정치와 안보 연구에서 더 이상 등한시할 수 없는 핵심적인 과제라는 점을 잘 말해주고 있다. 하지만 기존의 방대한 담론과 달리 실제 사이버안보의 구체적인 현안들은 매우 불명확할 뿐더러 앞으로 지속적인 논의가 필요한 상황이다. 사이버공격 및 억지와 관련하여 '전쟁의 정당성에 관한 법'과 '전쟁 중 무력 행위에 관한 법'으로 구분되는 국제규범이 중요한데, 사이버공격이 이러한 기준에 얼마나 부합하는가는 여전히 불명확하다. 또한 사이버공격을 사전에 방지하기 위한 사이버억지의 개념도 사이버공간의 특성상 냉전기의 핵억지 논리를 그대로 수용하기 어렵다는 의견이 많다. 이러한 한계를 극복하기 위해 누적적 억지, 맞춤형 억지, 자기 억지, 보증전략, 우호적 점령, 신(新)일상성과 같은 대안적 패러다임들에 관한 논의에 주목할 필요가 있다.

* JPI정책포럼 세미나(2015.07.17) 발표자료

목 차

1. 들어가는 말

○ 사이버안보의 문제와 국제정치

– 2015년 미국은 소니사 해킹사건과 관련하여 북한에 대한 보복 조치를 단행한 것으로 추정되고 있는데, 군사적 수단을 통해 대응하기 어려운 상황에서 정보기술을 이용한 보복 및 대응 조치를 취하는 추세는 점차 강화되고 있음. 북한과 같은 불량국가(rogue states)를 다루기가 쉽지 않은 상황에서 폐쇄된 사회에 외부의 분위기와 정보가 유입되도록 함으로써 내부 개혁을 이끌어내는 데 도움이 될 수 있다는 생각이 점차 커지고 있음. 그럼에도 불구하고 사이버공간에서 벌어지는 다양한 안보 문제들은 기존의 안보 문제와 달리 상대적으로 복잡하고 대응이 쉽지 않은 상황임

○ 사이버안보의 새로운 담론과 접근법

– 21세기에 들어와 다양한 방식의 사이버침해와 위협이 발생하였고, 이로 인하여 각 국가들은 사이버안보 태세를 확립하고 사이버사령부를 설립하는 등 새로운 종류의 위협에 대응하기 위한 담론을 양산해 왔음. 기술사회의 발전으로 말미암은 이러한 새로운 유형의 공격이 21세기의 상호의존적 네트워크 사회와 국가시스템에 심각한 위해를 가할 수 있다는 우려가 점차 커지고 있음

2. 사이버공간의 안보와 사이버공격

가. 사이버시대의 안보

○ 사이버전쟁의 개념과 특징

– 사이버안보 문제를 촉발시킨 결정적 계기로서 2007년의 에스토니아 사례, 2008년의 조지아 사태, 2009년 미국과 한국의 사이버침해, 2010년 이란의 핵시설에 대한 악성코드 공격 등은 사이버공간의 안보 문제가 담론화되는 데 큰 기여를 함. 사이버공간에서 정보통신기술과 네트워크를 통해 이루어지는 사이버공격과 위협은 오늘날 전통적인 형태의 공격이나 위협과 더불어 정보화시대의 국가 역량에 결정적인 변수로 작동하고 있음. 일각에서는 이러한 현상을 부각시키면서 '사이버전쟁(cyber war)'의 화두를 강조하고 있음

– 새롭게 부각되고 있는 '사이버전쟁' 개념은 동역학적 공격에 치중하는 기존 물리적 차원의 전쟁과 달리, 커뮤니케이션 시스템, 전력망, 석유화학공장, 핵발전소, 상하수도 시스템 등 주요 기간망에 대한 공격을

위주로 하는 '보이지 않는 침해'가 주종을 이루고 있음. 이러한 특성을 고려할 때 사이버전쟁은 '한 나라가 의도적으로 다른 나라의 컴퓨터 시스템 또는 디지털 기간시설에 대하여 사이버공격을 가함으로써 정치적 이득을 얻거나 보복을 가하는 행위'로 정의할 수 있음. 이처럼 사이버전쟁은 새로운 유형의 위협을 통해 사회 각계각층의 네트워크에 공격을 가해 정치적인 의도를 부각시키고 양보를 이끌어내려는 목표를 지니고 있음

○ 사이버전쟁 개념의 한계

- 사이버전쟁의 새로운 개념이 21세기의 분쟁 양상을 규정하는 데 도움이 되기는 하지만, 지금까지의 논의는 대부분 전통적인 '전쟁'의 개념을 그대로 사이버공간에 적용하고 있다는 한계를 넘어서지 못하고 있음. 한편, 1) 사이버공격과 위협의 원천을 파악하기 어렵다는 점에서 '책임 소재'를 따지기가 매우 어려움. 일반적으로 인터넷을 포함한 네트워크의 위치 설정 및 확인은 인터넷주소(IP) 프로토콜을 따르지만, 이 주소가 특정한 컴퓨터나 개인을 1:1로 매칭하는 것이 아니며 다양한 우회적 지정 방법이 존재하기 때문에 정확한 사이버공격의 주체를 확인하기가 사실상 불가능함. 2) 국가 이외에 기업이나 조직, 비공식 단체, 개인 등도 사이버공격에 가담하는 경우가 잦은데, 이는 진입비용이 상대적으로 낮기 때문임. 나아가 국가 차원에서 이러한 해킹이나 은밀한 공격 행위를 부추기는 경우도 많으나 증거를 확보하기가 매우 어려우며 예방이나 사전 방어가 어렵다는 난점이 있음. 3) 기존의 전쟁이 명확한 적의 존재를 규정하는 반면, 사이버공격은 은밀한 형태로 이루어지는 경우가 많기 때문에 일반적인 전쟁 규범으로 다스리기가 어려움
- 최근에 빈번하게 발생한 사이버공격의 추세를 살펴보면, 사이버공간에서의 행위만으로 의도했던 목표를 달성한 경우는 드물었음. 오히려 사이버공격은 일반적인 물리력과 함께 사용되는 경우가 많았음. 따라서 새롭게 제기되고 있는 '사이버전쟁'이라는 개념이 전통적인 전쟁양식을 대체하는 새로운 유형의 분쟁이라고 보기에는 한계가 존재함. 사이버공간의 역사가 일천한 상황에서 이러한 사이버전쟁이 새로운 패러다임으로 간주될 만한 수준에 도달한 것인가에 대해서는 학자들 사이에 논란이 지속되고 있음

사이버공격은 은밀한 형태로 이루어지는 경우가 많기 때문에 일반적 전쟁규범으로 다스리기 어려움. 한편, 사이버전쟁 개념을 전통적인 전쟁양식을 대체하는 새로운 유형의 분쟁으로 보기에는 한계가 존재함

○ 사이버공간의 분쟁: 국제정치적 문제와 국제규범의 적용

- 정보통신기술의 발전으로 인해 만들어진 사이버공간은 복잡한 네트워크로 이루어진 비현실적 '가상(virtual)' 공간이지만, 그로부터 야기되는 다양한 부작용과 피해가 우리의 현실에 미치는 영향은 무시할 수 없는 수준임. 특히 한 나라의 의도적인 사이버공격이 상대 국가에 치명적인

효과를 야기할 수 있기 때문에 이를 국제법과 규범을 통해 규제해야 한다는 요구가 높아지고 있음. 무엇보다도 이러한 침해 행위 및 위협이 미치는 공격적 속성을 감안할 때 전통적인 국제법에 의한 적대 행위의 규제, 즉 '무력분쟁법(Law of Armed Conflict)'을 적용할 수 있는지, 그렇지 않을 경우 대안의 규제 프레임이 가능한지에 대한 논의가 필요함. 나아가 법적 장치를 추구하는 데 필요한 국가들 사이의 협상과 제약을 고려할 때 이러한 문제는 단순한 '법적 문제'의 차원을 넘어 '정치적 문제'로 간주되고 있음

사이버공간에서는 사이버침해, 사이버공격, 그리고 첩보를 포함하는 여러 가지 유형의 공격 행위가 이루어지고 있음

- 과거 핵무기를 둘러싼 대결이 주종을 이루던 냉전기에는 상호 견제를 하는 국가들이 소수라는 점에서 핵무기를 이용한 보복의 균형이 상대적으로 손쉬웠음. 이러한 합리적 견제의 균형을 가리켜 '상호확증파괴(Mutually Assured Destruction)' 원칙이라고 부르는데, 이는 핵억지라는 냉전기의 대표적인 전략으로 자리 잡았고, 새로운 핵보유 국가가 등장하지 못하도록 기존 보유국들 사이에 기득권 유지를 위한 NPT 협조체제가 순조롭게 작동하는 계기를 만들어 줌. 그런데 이와 같은 규제와 협력의 프레임워크가 사이버공간에서도 그대로 적용될 수 있는가에 대해서는 확신하기 어려움. 그 이유는 사이버공간에서 이루어지는 행위들의 경우, 확산이 용이하며 책임 소재를 추적하기 어렵고, 나아가 기술적 진입장벽이 낮은데 비해 이를 규제하기는 어렵다는 난점이 존재하는 등 여러 장애요인들 때문임

○ 대안의 개념: 사이버공격과 사이버안보

- 오늘날 사이버공간에서는 사이버침해(cyber exploitation), 사이버공격(cyber attack), 그리고 첩보(espionage)를 포함하는 여러 가지 유형의 공격 행위가 이루어지고 있음. 사이버침해는 상대방의 정보를 몰래 취득하려는 일반적인 범죄 행위인 반면, 사이버공격은 의도적으로 적대국의 컴퓨터 시스템이나 네트워크를 파괴하려는 행위를 가리킴. 사이버첩보의 경우 정보 절취 행위라고 할 수 있는데, 정보기술의 발전과 더불어 이러한 행위가 더욱 활발하게 일어나고 있다는 점에서 국제적인 문제로 비화되고 있음
- 사이버안보 문제는 냉전 시기의 전통 안보나 핵무기 경쟁, 특히 핵억지 논리와 매우 다른 양상을 보임. 사이버공격 행위는 전통적인 공격이나 핵공격과 마찬가지로 특정한 목표물을 대상으로 삼기는 하지만, 그러한 공격 행위로 인하여 글로벌 네트워크에 공존하는 우방국, 민간, 심지어 자국의 시스템에도 의도하지 않았던 피해를 줄 수 있다는 점에서 차이를 보임. 상호 연결된 네트워크상에서 이루어지는 사이버공격은 그만큼 복잡하고 불확실하기 때문에 재래식 무기나 핵무기에 비해 훨씬 더 불안정한 상태를 야기할 수 있음. 이에 비하여 인명이나 물리적

시설에 대한 사이버공격의 파괴력은 상대적으로 덜 치명적이기 때문에 오히려 공격 행위에 대한 자제력이나 억지력이 상대적으로 약화되거나 공격적 성향이 강화될 소지가 큼

- 한편 정보기술이 발달하고 네트워크화가 고도로 진행된 국가일수록 사이버공격에 오히려 취약하다는 '비대칭성 역설(Cyberwar Asymmetric Paradox)'이 주목을 받고 있는데, 공격능력과는 별도로 정보사회가 외부로부터의 공격에 취약해질 수밖에 없는 상황을 가리킴. 대표적으로 미국과 같은 최상위의 정보기술을 갖춘 나라들일수록 사이버위협에 대한 우려가 크다는 점은 아이러니라고 할 수 있음. 이와 같은 기술적 비대칭성으로 인해 적대세력이 사회 기간망 등 주요 시설에 공격을 가할 가능성이 크며, 이럴 경우 공격을 받는 국가의 피해 규모는 상대적으로 커질 수밖에 없음. 따라서 재래식 전력과 핵전력에서 미국이 세계 최고의 수준을 지니고 있다는 점에서 미국에 적대적인 세력들의 공격 목표가 사이버공간 및 네트워크에 집중될 가능성이 매우 크다고 할 수 있음

나. 사이버공격의 개념과 기본 속성

○ 사이버공격의 개념화와 유형

- 2011년 미국 합참은 사이버공격을 '컴퓨터 관련 네트워크나 시스템을 이용하여 적국의 주요 사이버 시스템, 자산, 또는 기능을 무력화하거나 파괴할 목적으로 이루어지는 적대 행위'로 규정함. 한편 중앙아시아 안보협력체인 상하이협력기구(SCO: Shanghai Cooperation Organization)에 따르면, 사이버공격이란 포괄적 맥락에서 사이버 '수단'에 의한 위협으로 정의됨. 기존의 이러한 접근을 감안할 때 '사이버공격'은 '정치 또는 안보의 목적을 위해 컴퓨터 네트워크의 기능을 저해하기 위해 취하는 행동'으로 볼 수 있음
- 세부적인 내용에 있어서 사이버공격은 분산형 서비스거부(DDoS) 공격, 정보 교란, 그리고 네트워크 침해가 주종을 이루고 있음. 분산형 서비스거부 공격은 악성코드를 통해 수많은 '좀비 컴퓨터'들을 양산하여 공격 목표가 되는 네트워크와 사이트에 과도한 접속을 통해 마비현상이 일어나도록 하는 행위임. 2007년의 에스토니아 및 2008년의 조지아 공격, 2009년의 한국 정부 및 민간 기업에 대한 공격도 분산형 서비스거부 방식의 공격이 이루어진 대표적인 사례임. 네트워크 침해는 2010년에 일어난 이란의 핵시설을 대상으로 한 스턱스넷(Stuxnet) 사건과 같이 상대국의 컴퓨터 시스템을 대상으로 고의적인 오작동이나 파괴를 도모함. 이러한 침해 행위는 주요 기간시설이나 핵시설과 같이 외부로부터 고립된 네트워크를 주요 대상으로 함

네트워크화가 고도로 진행된 국가일수록 사이버공격에 오히려 취약하다는 '비대칭성 역설'이 주목을 받고 있는데, 공격능력과는 별도로 정보사회가 외부로부터의 공격에 취약해질 수밖에 없는 상황을 가리킴

○ 사이버공격과 지능형 지속위협

– 사이버공간의 공격 행위들이 점차 분명한 목표와 대상을 설정하고, 이를 위한 체계적인 공격패턴을 보이게 되면서 '지능형 지속위협(APT: Advanced Persistent Threat)'이라는 군사적 개념화가 이루어져 왔음. 이것은 2006년 미 국방부와 정보 당국 등 관련 기관 사이의 커뮤니케이션을 위해 개발된 개념으로, 사이버위협을 야기하는 체계적인 '지능형' 공격 행위를 의미함. 이와 같은 APT는 시스템에서 기존에 알려지지 않았던 취약성을 찾아내고 이를 집중 공격함으로써 적절한 대응책이 만들어지기 전에 시스템에 침해를 가하려는 목적을 지님. 이와 같은 '제로데이(zero-day) 공격'은 주어진 목표를 달성하기 위해 사전에 설정된 임무를 완수하는 데 주력하며, 주어진 목표를 달성하기 위해 체계적인 조직과 이에 대한 적절한 지원을 특징으로 함

첨단 사이버공격은 목표물에 직접적인 물리적 공격을 가하지 않고도 치명적인 효과를 야기할 수 있기 때문에 국제사회에서 이를 규제하기 위해 노력하고 있음

– APT 공격의 사례로서 가장 대표적인 것이 이란의 핵시설을 겨냥한 미국과 이스라엘의 '올림픽게임(Olympic Games) 작전'임. 2006년 부시 행정부에 의해 추진된 이 작전은, 오바마 행정부에서도 계속되어 나탄즈(Natanz)의 핵시설을 공격하는데 치중함. 우라늄 농축에 이용되는 원심분리기를 관리하는 산업통제시스템(ICS: Industrial Control System)이 주된 목표가 되었음. 이때 사용된 악성코드인 스틱스넷은 외부와 연결이 차단된 이란의 ICS에 침입하여 원심분리기의 작동에 영향을 미친 바 있음. 이러한 사이버공격은 역사상 처음으로 이루어진 본격적이고 체계적인 사이버공간의 APT로서 의미를 지님

– APT의 주요 수단인 악성코드는 인터넷에 연결된 네트워크뿐 아니라 외부로부터 차단된 독립적인 네트워크를 공격함. 스틱스넷과 유사한 방식으로 작동하는 두쿠(Duqu)는 미래의 공격을 위해 특정한 컴퓨터 시스템에 침입하여 정보를 수집하는 기능을 수행함. 또한 악성코드 플레임(Flame) 역시 윈도우 컴퓨터 시스템을 대상으로 하며, 중동 여러 나라에 확산되어 사이버첩보에 이용되고 있음. 이 코드는 악성코드 중에서도 가장 정교한 형태로서 USB 드라이브와 LAN을 통해 컴퓨터 시스템에도 침투하며, 음성, 화면, 키보드 움직임, 네트워크 트래픽 등에 관한 정보를 기록했다가 외부로 전송하는 것으로 알려짐

○ 사이버공격의 딜레마와 정치적 범죄

– 오늘날의 첨단 사이버공격은 목표물에 직접적인 물리적 공격을 가하지 않고도 치명적인 효과를 야기할 수 있기 때문에 국제사회에서 이를 규제하기 위한 노력을 기울이고 있음. 특히 미국과 같이 첨단기술을 통해 복잡하게 네트워크화된 사회가 사이버공격에 더욱 취약하게 노출되어 있다는 점으로 인해, 이를 국제규범으로 규제하려는 시도들이 서서히 등장하고 있음. 이에 비해 그동안 사이버공격의 위협을 받는

국가들이 이란이나 북한처럼 상대적으로 정보화가 미미한 국가였다는 점을 고려할 때, 과연 사이버공격이 충분한 성과를 거두고 있는가에 대한 비판도 제기되고 있음

- 이러한 비판과 관련하여, 사이버공격을 국가 간 공식적인 전쟁보다는 정치적 범죄의 새로운 유형으로 다룰 필요가 있다는 주장에 설득력이 있음. 정보기술이 발전함에 따라 정치적인 의지를 내세우고 이에 대한 공감대를 형성하는 일이 용이해지면서 사이버공격의 빈도 및 강도는 더욱 심각해지고 있음. 사이버공격은 사보타지(sabotage), 첩보(espionage), 전복(subversion)과 같은 행위를 통해 정치적 목표를 추구하는데, 사보타지의 경우 경제 또는 군사시스템을 무력화하거나 파괴하기 위한 시도임. 첩보는 특정 목표물에 침입하여 민감한 정보나 금지된 내용을 절취하는 행위이며, 전복 행위는 고의적으로 특정 조직이나 정부를 무력화함으로써 사회적 유대감과 신뢰를 약화시키려는 시도를 뜻함

3. 사이버공격의 정당성과 법적 규제

○ 사이버공격의 규제: 국제법 규범

- 오늘날 사이버공격 행위가 기존의 전쟁법 및 규범의 적용을 어느 정도 받는가의 여부가 중요한 국제적 현안으로 떠오르고 있음. 부분적으로 사이버공격이 물리적 공격에 버금가는 피해를 야기할 수 있기는 하지만, 근원적으로는 성격이 다르다는 점에서 이는 쉽게 판단할 수 없는 문제임. 사이버공격을 규제하는 국제법 규범을 크게 '전쟁의 정당성에 관한 법(jus ad bellum)'과 '전쟁 중 무력 행위에 관한 법(jus in bello)'으로 구분해 볼 필요가 있는데, 다음과 같은 현안들이 제기되고 있음

○ 전쟁의 정당성에 관한 법: 사이버공격과 무력 사용의 조건

- '전쟁의 정당성에 관한 법'으로서 국제연합헌장 제2조 4항은 '자위(self-defense)'의 목적을 위한 최소한의 합법적인 무력 사용 조건을 규정하고 있는데, 모든 국가는 회원국의 영토적 통합(territorial integrity)이나 정치적 독립성(political independence)을 해칠 수 있는 '위협(threat)' 또는 '무력 사용(use of force)'을 중지해야 함. 그렇지만 여기에서 무엇이 '무력'의 범주에 해당하는지에 대해 보다 구체적으로 밝히지 않고 있기 때문에 개념의 해석을 둘러싸고 의견이 분분한 상황임
- 사이버공격이 '물리적 폭력'을 동반하지 않을 경우 무력으로 보기 어렵지만, 공격으로 인한 파괴 범위를 고려할 경우 이 역시 무력 공격으로 보아야 한다는 주장도 타당한 면이 있음. 서로 호환되지 않는 이와 같은 해석의 논거를 고려할 경우, 2010년 미국과 이스라엘의 '올림픽게임'

사이버공격이 '물리적 폭력'을 동반하지 않을 경우 무력으로 보기 어렵지만, 공격으로 인한 파괴 범위를 고려할 경우 이 역시 무력 공격으로 보아야 한다는 주장도 타당

작전이 국제연합헌장의 '무력 사용' 금지 의무를 위반한 것인가에 대해 확실한 결론을 내리기는 어려운 상황임. 2014년 미국 소니사에 대한 해킹 공격의 경우에도 북한의 행위로 의심할 만한 여러 정황이 있었지만 확실하게 이를 입증하기는 불가능했음. 공격의 주체인 해커들을 추적하기 위한 단서는 인터넷 프로토콜 주소인데, 인터넷상의 데이터 전송이 복잡한 라우팅 과정을 거치기 때문에 공격의 주체와 그 위치를 정확하게 짚어내기는 어려움

사이버공격은 공격의 도구, 목표, 효과 중 어디에 초점을 맞추는가에 따라 각각의 입장이 구분됨. '도구 기반' 시각에서는 사이버공격이 물리적 특성상 그 자체로서 무력으로 분류될 수 없으며, 오로지 군사적 목적으로 활용되는 경우에만 무력으로 봄

○ 사이버공격과 집단안보 및 자위권

– 국제연합헌장 제39조는 안전보장이사회가 필요하다고 판단할 경우 국제평화와 안보를 위해 필요한 조치를 취할 수 있다고 규정함으로써 '집단안보(collective security)'를 통한 합법적인 무력 사용의 조건을 명시하고 있음. 또한 헌장 제51조는 개별 회원국 또는 집단이 무력 공격을 받을 경우 '자위(self-defense)'를 위한 본연의 권리를 지닌다고 규정함. 이 조항에 따르면, 국제연합 회원국에 대한 무력 공격이 이루어질 경우, 안전보장이사회가 국제평화와 안전을 위한 별도의 조치를 취하지 않는 이상 국제연합헌장의 어떤 조항도 개별 또는 집단자위를 위한 본연의 권리를 침해할 수 없음. 따라서 사이버안보와 전쟁법의 연관성을 논의하는 데 있어 중요한 이슈는 사이버공격 또는 사이버침해 행위가 국제연합헌장에서 금지하는 '무장 공격(armed attack)'에 해당하는가를 판단하는 기준임. 헌장 제2조 4항이 무력 사용의 조건을 규정하고 있는 반면, 헌장 제51조는 무력 사용에 합법적으로 대응할 수 있는 조건을 규정하고 있는데, 이 역시 사이버공격에 적용하기에는 여전히 모호한 규정임

– 사이버공격은 공격의 도구, 목표, 그리고 효과 중 어디에 초점을 맞추는가에 따라 각각의 입장이 구분됨. 우선 '도구 기반(instrument-based)' 시각에서는 사이버공격이 물리적 특성상 그 자체로서 무력으로 분류될 수 없으며, 오로지 군사적 목적으로 활용되는 경우에만 무력 사용으로 해석될 수 있다고 봄. '목표 기반(target-based)' 시각은 주요한 컴퓨터 시스템을 대상으로 한 공격이 이루어지는 경우 이를 무력 공격으로 간주함. '효과 기반(effects-based)' 시각은 사이버공격이 야기하는 효과의 정도에 따라 무력 공격 여부가 달라진다고 봄. 이 시각이 오늘날 가장 보편적인 것으로 통용되고 있기는 하나, 공격의 효과가 발생한 이후에만 무력 행사 여부를 판단할 수 있다는 문제가 있음

– 한편 국제연합헌장이나 국제관습법에 따라 합법적인 무력 사용이 이루어질 경우 사이버공격이 가능하다는 견해도 있음. 즉 단독으로 이루어지는 사이버공격이든, 물리적 공격과 병행하여 이루어지는 사이버공격이든, 일정한 법적 기준이 충족되는 자위권 행사의 경우 사이버공격이 허용

된다는 것임. 이 경우 자위권을 바탕으로 한 '선제적(anticipatory) 조치'가 반드시 '예방적 자위(preventive self-defense)'를 의미하는 것은 아님. 따라서 미국과 이스라엘의 '올림픽게임' 작전이 국제법적으로 합법적인지의 여부는 여전히 불확실하다고 할 수 있음. 이란의 핵시설이 야기할 위협과 그에 대한 자위권 발동의 요건에 대한 해석이 다분히 주관적이기 때문임

- 사실 단독으로 이루어지는 사이버공격의 경우 몇 가지 문제를 안고 있는데, 우선 사이버공격으로 인한 피해가 국제법에서 규정하는 '자위권'을 행사할 정도로 치명적이지 않다는 점을 꼽을 수 있음. 또한 그러한 피해가 광범위하게 발생했다 하더라도, 누가 그에 대한 책임을 질 것인가를 밝혀내는 일이 결코 쉽지 않음. 이처럼 사이버공격이 추가적인 물리적 공격 없이 단독으로 일어날 경우, 정보의 부족과 법적 근거의 미흡함으로 말미암아 적당한 대응 조치를 취하기가 어려움. 소니사에 대한 해킹 공격에 대하여 미국이 북한을 책임 국가로 지목하고 그에 대한 보복으로서 사이버공격을 감행하기로 결정했지만, 어느 정도의 공격이 국제법상 허용될 수 있는가에 대한 아무런 기준이 없는 실정임. 또한 보복 대상을 구체적으로 설정한 공격 행위로 말미암아 상호간에 위기가 증폭될 가능성도 상존하며, 나아가 비대칭적인 사이버능력을 갖춘 미국과 같은 나라들이 오히려 보복 공격에 더 취약해지는 상황도 얼마든지 야기될 수 있음

○ 사이버공격과 전쟁 중 무력 행위에 관한 법

- 사이버공격이 전개되는 과정에서도 국제규범이 중요한 제약이 될 수 있는데, 이러한 '전쟁 중 무력 행위에 관한 법'은 관습법으로 존재하며 정당한 무력행사에 요구되는 조건으로서 '필요성(necessity)의 원칙'과 '비례성(proportionality)의 원칙'을 강조해옴. 여기에서 필요성의 원칙은 최후의 수단으로써 무력 행위가 선택되어야 한다는 것이며, 비례성의 원칙은 무력 사용의 범위와 강도가 실질적이고 긴급한 위험 수준을 초과해서는 안 된다는 점을 강조함. 이와 더불어 '구분(distinction)의 원칙'과 '차별적 공격(discriminatory attack)의 원칙'은 적에 대한 공격이 군사 목표에 국한되어야 하며 민간을 대상으로 한 공격은 허용되지 않는다는 점을 강조함. 그렇지만 사이버공격의 와중에 이러한 '부수적 피해(collateral damage)'를 모두 예방하는 일은 거의 불가능에 가깝다고 할 수 있음. 네트워크의 속성상 민간과 군사 부문을 명확하게 분리하는 것이 사실상 어렵기 때문임
- 국제 분쟁과 관련하여 '전쟁 중 무력 행위에 관한 법'은 민간 목표물에 대한 공격을 제한하며, 공격의 결과가 '의미 있는 군사적 우위(meaningful military advantage)'를 달성하려는 취지에서만 정당성을 부여함. 사이버

사이버공격의 와중에 '부수적 피해'를 모두 예방하는 일은 거의 불가능. 네트워크의 속성상 민간과 군사 부문을 명확하게 분리하는 것이 사실상 어렵기 때문

공격의 경우 그 속성상 민간 목표물에 대한 '부수적 피해'가 양산될 수밖에 없는 까닭에 '전쟁 중 무력 행위에 관한 법'을 어떻게 실효성 있게 부과할 것인가는 국제사회의 중요한 과제가 됨. 따라서 최근 가속화되고 있는 '탈린 매뉴얼(Tallinn Manual)' 작업은 '사이버전쟁에 적용 가능한 국제법'을 구축하기 위한 다국적 차원의 진지한 노력임. 이 매뉴얼은 북대서양조약기구 산하 사이버방위 협력센터(Cooperative Cyber Defense Centre of Excellence)의 주도하에 사이버공격과 사이버전쟁의 상황에서 국제법을 어떻게 해석할 것인가를 집중 논의함. 아직까지 구속력을 갖추고 있지는 않으나, 사이버안보에 관한 국제조약이 강력하게 요구되는 상황에서 의미 있는 출발점이라 할 수 있음

20세기에 들어와 첨단기술이 활용되기 시작하면서 기존의 국제법 규범을 통해 이를 규제하려는 시도가 점차 난관에 봉착하게 됨

- 20세기에 들어와 첨단기술이 활용되기 시작하면서 기존의 국제법 규범을 통해 이를 규제하려는 시도가 점차 난관에 봉착하게 됨. 특히 사이버공격의 빈도와 강도가 심각해지는 상황에서 이를 전통적인 전쟁법으로 관리 및 규제하기는 사실상 어려움. 한 가지 바람직한 현상은 분쟁에 관한 국제규범이 여전히 사이버공격에 대하여 어느 정도의 법적 통제장치로 작동해 왔다는 점임. 기술적 통제가 불가능함에도 불구하고 기존의 핵무기 통제 레짐이 국가 간의 협력을 통해 핵확산을 막는 데 어느 정도 기여해 왔음을 고려할 때, 사이버안보 분야에서도 이러한 추세가 가능할 것으로 전망됨

4. 사이버억지와 새로운 패러다임

가. 사이버억지의 개념과 한계

○ 억지와 강요: 사이버억지의 개념

- 억지전략은 상대방의 행동에 영향력을 가하기 위한 행위로서, 강요(compellence)와 더불어 위협외교(coercive diplomacy)의 주된 수단이었음. 냉전기의 억지전략은 총력전과 민족주의 감정, 파괴적 무기로 인한 치명적인 피해를 막기 위해 고안된 일종의 '저렴한 승리 전략(cheap-victory strategy)'이었음. 특히 핵무기는 이러한 목적을 수행하는 데 있어 재래식 무기에 비해 훨씬 더 효율적인 도구였음. 한편, 핵무기를 이용한 공격과 보복을 전제로 수립된 핵억지의 논리가 사이버공격과 억지의 경우에도 적용될 수 있는가에 대해 최근 많은 관심이 생겨나고 있음. '사이버억지'는 1990년대 초 데어 데리안(James Der Derian)이 고안한 말로서, 상호의존적 네트워크화의 추세 속에서 상대방을 통제하기 위한 새로운 전략적 패러다임이 필요하다는 인식을 바탕으로 한 표현임. 핵무기 시대의 억지전략과 마찬가지로 가급적 전쟁을 하지 않으면서

상대방을 굴복시키거나, 또는 전쟁을 하더라도 신속하고 결정적인 승리를 거둘 수 있는 대안의 전략이 절실한 상황에서 사이버억지의 개념은 이후 안보연구 및 국제정치학의 중요한 화두로 떠오름

○ 보복을 통한 억지와 거부를 통한 억지

- 억지전략은 '보복(punishment)을 통한 억지'와 '거부(denial)를 통한 억지'라는 두 가지의 방식으로 실행됨. 우선 '보복을 통한 억지'는 적의 공격적 행위가 예상될 경우 상대방에게 그러한 공격의 이익보다 비용이 더 클 것이라는 부담을 줌으로써 사전에 차단하는 것을 목표로 함. 적대국가가 핵공격을 시도할 경우 그에 상응하는 핵무기로 무차별 보복하겠다는 메시지를 전달함으로써 적국의 공격이 이루어지지 않도록 견제할 수 있다는 메시지가 바탕에 깔려 있음. 이를 위해서는 선제적인 핵공격을 당하더라도 반드시 '보복'을 할 수 있는 '2차 핵공격 능력'이 필수적임. 한편 '거부를 통한 억지'는 예상되는 상대방의 공격에 대한 '방어'를 강화함으로써 그것이 성공하지 못할 것이라는 확신을 주는 전략임. 이를 위해서는 상대방의 공격을 무력화하는 '방어 시스템'의 구축이 중요한데, 1980년대 레이건 행정부의 '전략방위구상(SDI)'이나 2000년대 부시 행정부의 '미사일방어계획(MD)'은 이와 같은 거부를 통한 억지 개념을 구현한 경우였음
- 보복을 통한 억지전략이 성공하기 위해서는 억지능력의 확보, 억지위협의 신뢰성, 그리고 억지위협의 전달이 제대로 구현되어야 함. 그러나 사이버위협이나 사이버공격의 경우 과거와 같은 냉전식 논리를 그대로 적용하여 억지효과를 기대하기가 난망해짐. 사이버공격의 경우 핵공격에 비해 진입비용이 낮기 때문에 상대적으로 열세인 국가 또는 비국가 행위자들의 참여가 손쉬우며, 따라서 사이버공격을 사전에 탐지하기도 곤란함. 나아가 보복을 가한다고 하더라도, 사이버수단을 이용한 보복의 가능성이나 효과도 크지 않은 편임. 만약 방어하는 쪽의 취약성이 클 경우 억지나 보복 행위로 인한 사태 악화(deescalation)의 가능성 때문에 보복 의지를 강하게 전달하기 어려운 점도 고려할 필요가 있음

보복을 통한 억지전략이 성공하기 위해서는 억지능력의 확보, 억지위협의 신뢰성, 그리고 억지위협의 전달이 제대로 구현되어야…

○ 사이버억지와 상호확증파괴

- '거부'를 통한 사이버억지 전략은 사전에 적의 사이버공격을 방어할 수 있는 시스템을 체계적으로 구축함으로써 상대방의 공격 의지를 무산시키는 것을 주된 목표로 함. 여기에는 네트워크 보안(invulnerability), 다중화(redundancy) 및 재건(reconstitution)을 통한 시스템의 탄력성(resilience) 제고, 시스템 보호, 상대국과의 시스템 상호의존성 증가 등 여러 방법이 동원됨. 한편, 공격이 방어보다 유리하다는 사이버공간의 특징으로 인해 '사이버억지'의 개념이 '공포의 균형'이라는 극단적인

모습으로 바뀌기도 함. 또한 방어가 기술적으로 쉽지 않은 상황에서 완벽한 사이버방어 시스템을 구축하겠다는 계획은 합리적이지도, 바람직하지도 않음. 역설적으로, 사이버공격의 가능성에 대비하는 최선의 방법은 공격 가능성에 대한 '공포'가 공유되는 '상호 억지' 시스템을 지속시키는 것임. 한 국가가 사이버공간을 압도적으로 지배하기보다 상호 억지가 이루어질 수 있는 시스템이 더 안정적인 균형을 유지할 수 있다는 견해에 무게가 실리고 있음. 이와 같이 사이버공간에서 이루어지는 공포의 균형을 '사이버 상호확증파괴(Mutually Assured Debilitation)'라고 일컫는데, 공포의 균형 속에서 국가들이 공개적으로 사이버공격 능력을 유지하면서 공격에 대한 자신들의 취약성을 유지함으로써 상호 안정을 도모하고자 함

공포의 균형 속에서 국가들은 공개적으로 사이버공격 능력을 유지하면서 공격에 대한 취약성을 유지함으로써 상호 안정을 도모

○ 사이버억지의 한계

- 이상과 같이 냉전기의 제한적 억지전략이 21세기의 사이버공간에서 그대로 작동할 것으로 예상하기는 쉽지 않음. 과거 냉전기에는 서로 비슷한 수준의 핵무기와 파괴력을 지닌 초강대국 사이에 양극화 구도가 상대적으로 안정적으로 유지될 수 있었는데, 이는 핵전쟁에 대한 공포가 서로에게 공유되고 있었기 때문임. 그러나 정보기술을 기반으로 하는 사이버공간에서 이런 상황이 동일하게 재연 또는 반복될 것으로 전망하기는 어려움. 적은 수의 강대국들만이 참여하던 냉전기의 상호 억지 관계와 달리, 사이버공간에서는 수많은 비국가 행위자들이 동시에 공존하기에 시스템 예측성과 안정성이 크게 줄어들기 때문임. 이와 더불어 냉전기에는 초강대국들이 유사한 수준의 물리적 파괴력을 보유함으로써 메시지의 교환과 기대의 수렴을 통해 억지전략을 손쉽게 실행할 수 있었지만, 오늘날 사이버공간에서는 기술의 비대칭성으로 말미암아 단순한 형태의 억지효과를 기대하기 어려움
- 무엇보다도 사이버공간의 억지전략을 구현하는 데 있어 공격자의 출처와 신원을 파악하는 '책임 소재'의 문제가 장애요인이 됨. 공격 행위에 대하여 적절한 보복을 가하기 위해서는 누가 공격에 책임이 있는지를 파악해야 하는데, 사이버공간의 특성상 이를 명확하게 가려내기란 결코 쉽지 않음. 또한 이를 밝혀낸다 하더라도 실제 보복 공격을 수행하는 데 있어 여러 애로사항이 존재하는데, 사이버공격의 주체가 비국가 행위자일 경우 그에 대한 보복 행위는 불가피하게 행위자가 속한 국가의 주권을 침해하는 결과를 초래할 수 있음
- 정책결정자들은 사이버공격의 효과를 제대로 인식하지 못하는 것으로 알려져 있는데, 이는 핵무기를 이용한 억지전략과 달리 사이버공격은 인명을 직접 겨냥하지 않는다는 선입견 때문임. 또한 그동안 사이버공격의 효과와 위협이 지나치게 과장되었기 때문에 억지전략이 실제로

작동하지 않을 것이라는 비판도 존재함. 사이버공격은 물리적 공격과 달리 독자적이고 효과적인 타격을 가하기 어렵기 때문에 전통적인 분쟁의 보조적인 기능을 수행하는 것에 그친다는 것임. 이러한 관점에서는 사이버공격에 의해 '하늘이 무너질까' 우려할 이유가 없다고 보며, 따라서 사이버안보를 '전략적' 차원으로 격상시키는 것은 그 효과를 지나치게 과대평가한 결과로 간주함

- 사이버공간의 위협이나 위험이 사회적으로 확대 포장되는 이유는 이것이 군사적인 프레임의 형태를 띠기 때문임. 사이버공간의 위협을 전략적, 군사적 차원으로 격상시킴으로써 제로섬 게임과 같이 '승리 아니면 패배'라는 이분법적 사고방식 속에서 다루려 하는 성향이 지배적이었으며, 따라서 다른 위협과 달리 적이 분명하지 않은 상황에서 승패를 어떻게 결정할 수 있는지는 여전히 해소되지 않는 문제로 남아있는 상황임. 이러한 비판을 염두에 둔다면 사이버공간의 위협을 한 단계 낮은 수준에서 '사이버범죄'나 '사이버첩보(cyber espionage)'로 간주해야 한다는 주장은 설득력이 있음. 모든 사이버위협에 대하여 군사적인 대응 조치를 취하겠다는 발상은 정보의 속성상 가능하지도 않을뿐더러 사이버안보의 중요한 측면을 간과하기 때문임. 따라서 대부분의 사이버위협은 고도로 안보화(securitized) 또는 정치화된(politicized) 이슈라는 비판이 가능한데, 이는 정책 또는 정치 차원에서 이루어지는 왜곡된 인식의 결과임

사이버공간의 위협을 전략적, 군사적 차원으로 격상시킴으로써 제로섬 게임과 같이 '승리 아니면 패배'라는 이분법적 사고방식 속에서 다루려 하는 성향이 지배적

나. 사이버억지의 새로운 패러다임

○ 사이버억지의 가능성

- 이상에서 논의한 바와 같이 사이버억지가 상대적으로 실행이 어렵다는 주장에도 불구하고, 현실에서 일어나고 있는 사이버공격의 여러 면모를 고려할 때 이것이 불가능한 것은 아님. 예를 들어 사이버공간에서 책임 소재를 가리는 일이 기술적으로 어려운 문제이기는 하지만 아주 불가능한 일도 아니며, 미국과 같은 나라의 기술력은 이러한 문제를 극복하는 데 매우 빠른 성장세를 보이고 있음. 따라서 사이버억지의 어려움이 이론적 차원에서 지나치게 과장되어 왔으며, 실제 현장에서는 이보다 억지전략이 훨씬 더 수월하게 이루어진다는 반론이 제기되기도 함. 특히 사이버공격 패턴은 정보기술의 우위가 여전히 강대국의 전유물이라는 점을 잘 보여주고 있는데, 스턱스넷 공격은 그 효과나 충격 면에서 새로운 문제로 인식되기에 충분한 것이었음

○ 사이버억지의 새로운 패러다임: 누적적 억지

- 억지전략을 실행하는 경우, 분쟁이 일어나지 않으면 그것이 성공했다고

간주되는 반면, 분쟁이 일어날 경우에는 실패했다고 평가됨. 이러한 이분법적 사고방식은 냉전기의 오랜 산물로, 오늘날 사이버공간의 복잡성은 그보다 더 진화된 형태의 대응전략을 요구하고 있음. 과거 분쟁과 억지 사이에 하나의 선택만이 가능하다고 보았지만, 오늘날에는 이 두 가지 현상이 복합적으로 존재하는 경우가 빈번하게 나타나고 있음. 그러므로 억지의 결과가 성공 또는 실패 중의 하나라고 명확하게 규정하기도 불가능하고 또 그럴 필요도 없음. 상황에 따라 억지전략을 구사하거나 분쟁에 직접 개입하는 복합적인 해결책을 얼마든지 구현할 수 있다는 것이 이러한 시각의 골자임. 이스라엘은 분쟁이 발생할 경우 무력 사용의 위협과 실제 무력 사용을 동시에 운용하면서 주변국가들의 도전을 억지하는 복합 전략을 효과적으로 구사해 옴. 이러한 전략을 '누적적 억지(cumulative deterrence)'라고 부르며, 이 전략은 장기간에 걸쳐 이스라엘의 전략적 입지 강화로 이어짐. 사이버공간에서도 이와 같은 복합 전략의 채택이 요구되고 있음

상대방의 공격 가능성과 선호를 고려한 여러 대응 조치를 추구하는 이와 같은 전략을 가리켜 '맞춤형 사이버억지'라고 일컬음

○ 사이버억지의 새로운 패러다임: 맞춤형 억지와 비대칭적 자기 억지

- 사이버억지 전략을 구현하는 과정에서 냉전기와 마찬가지로 '보복 위협을 통한 억지'와 '거부를 통한 억지'의 두 가지 방법이 모두 활용될 수 있는데, 공격의 책임 소재를 가리는 일이 쉽지 않지만 대규모의 사이버공격은 예방이 가능하며 대부분의 경우 구체적으로 진원지를 추적할 수 있음. 보복 위협이나 방어 이외에도 궁극적으로 적의 '자제(restraint)'를 유도함으로써 효과적인 억지가 이루어지도록 할 수 있기 때문임. 예를 들어 경쟁 관계에 놓여 있는 적국이 노골적인 공격 행위를 취하는 대신 스스로 자제한다면 상대방에게 훨씬 더 매력적인 결과가 보장될 것이라는 확신을 줄 수 있음. 이를 위해서는 상대방의 이해관계와 선호도를 파악해야 하며, 어느 정도 수준의 제안과 설득이 이러한 자제를 가능하게 할 것인지에 대한 고려가 전제되어야 함. 상대방의 공격 가능성과 선호를 고려한 여러 대응 조치를 추구하는 이와 같은 전략을 가리켜 '맞춤형(tailored) 사이버억지'라고 일컬음
- 강대국의 경우 사이버공간의 특성상 이와 같은 맞춤형 사이버억지 전략을 효과적으로 운용할 수 있는데, 이는 과거 핵억지의 경험을 기반으로 하고 있음. 핵보유국과 비보유국 사이의 비대칭적인 관계에서 핵무기를 이용한 억지전략은 의외로 신뢰성 있는 메시지를 전달하기 어려웠음. 그 이유는 핵무기는 '사용할 수 없는 무기'라는 '금기(taboo)'의 관행이 작동하므로 핵무기를 보유하고 있다는 사실 자체가 스스로의 선택을 제한하는 '억지효과'를 유발하기 때문임. 이와 같이 상대방을 억지해야 하는 핵무기가 자신의 발목을 잡는 '자기 억지' 상황이야말로 강대국들이 적절한 방식으로 '자제'를 실천함으로써 맞춤형 억지를

도모하도록 만드는 배경이 됨. 따라서 사이버공격 능력이 비대칭적으로 분포된 상황에서도 이와 같은 자기 억지의 가능성이 존재하며 억지 전략의 맞춤형 실행이 기대된다고 할 수 있음

○ 사이버억지의 새로운 패러다임: 재보장전략

- 한편 사이버억지의 관념이 '갈등'의 상황만을 전제로 하고 있다는 점을 고려할 때, 그 한계를 극복하기 위한 포괄적 대안으로서 '재보장(reassurance)' 전략으로 전환해야 한다는 주장에 관심이 쏠리고 있음. 원래 억지전략은 '받아들이기 어려운(unacceptable) 피해'를 입을 수 있다는 위협을 상대방에게 전달함으로써 목표를 달성하려는 것이었음. 이러한 관계의 이면에 존재하는 위협의 상호의존성을 서로 간에 인식한다면, 위협과 억지의 실패로 인한 분쟁 가능성 대신 협력을 통한 상호 이익의 가능성을 부각시키는 것이 훨씬 효과적인 전략이라고 할 수 있음. 이처럼 갈등 관계 속에서 상대방에 대한 '동기(incentives)' 부여를 통해 자발적인 억지를 유도하는 전략을 '재보장전략'이라고 함. 재보장전략은 상대방의 선호도와 취약성을 간파하여 선의의 이해관계 증진을 목표로 하며, 이러한 점에서 '자기 억지'를 유도하는 전략이자 협력의 규범을 지향하는 혼합 전략이라고 할 수 있음

갈등 관계 속에서 상대방에 대한 '동기' 부여를 통해 자발적인 억지를 유도하는 전략을 '재보장전략'이라고 함. 재보장전략은 상대방의 선호도와 취약성을 간파하여 선의의 이해관계 증진을 목표로 하며, 이러한 점에서 '자기 억지'를 유도하는 전략이자 협력의 규범을 지향하는 혼합 전략이라고 할 수 있음

- 재보장전략이나 자기 억지의 개념은 다양한 정치적 행위자들 사이에 복잡한 상호의존 관계가 존재하는 경우 특히 유용함. 이는 사이버공간이 네트워크의 연결과 교류를 통한 상호의존성의 기반 위에서 우호적 관계와 적대적 관계를 동시에 포함하기 때문임. 처음부터 적대적인 관계가 존재하는 경우란 거의 없으며, 협력적 관계와 적대적 관계를 동시에 유지하는 경우가 다반사임. 이러한 관계는 시간과 장소, 상황에 따라 수시로 변화하는데, 네트워크상에서 이루어지는 적대적 관계의 이면에 존재하는 '우호적 점령(friendly conquest)' 현상에 주목할 필요가 있음. 이것은 사이버공간에서 행위자들 사이에 자발적인 교류를 통해 발생하는 상호의존 상태를 유지하면서 한 나라가 다른 나라에 영향력을 행사하는 상태임. 점령의 우위를 지닌 국가는 상대국에 대하여 지속적인 접촉 요구를 창출함으로써 선호와 가치체계를 통제할 수 있게 됨
- 적대적 관계가 상당한 정도로 우호적인 교류 관계를 동시에 유지하고 있다는 점을 고려할 때, '우호적 점령'은 '적대적 점령'이 일어나기 전부터 상대방의 시스템에 침투하고 상호의존적인 관계를 강화함으로써 이탈 비용을 증가시키고 억지효과를 부과하는 데 효율적인 전략임. 미국은 인터넷의 기술적 하부구조를 통제함으로써 동맹국뿐 아니라 적대국가도 우호적으로 점령할 수 있는 기반을 구축해 왔음. 그리하여 인터넷 시스템에 자발적으로 참여하는 모든 나라에 대하여 '우호적 점령'을 지속하고 있으며, 동시에 일부 국가에 대해서는 '적대적 점령' 관계로

전환하기도 함. 이와 같은 이중적 속성은 특히 사이버공간에서 집중적으로 관찰되고 있는데, 네트워크를 통해 복잡하게 연결된 오늘날의 국가 간 관계를 이해하는 데 중요한 단서를 제공하고 있음

'신(新)일상성'은 사이버안보가 하나의 위기라는 시각 대신에 다른 종류의 범죄 현상과 마찬가지로 어느 사회에서나 일어나는 현상이라고 보는 것을 의미

○ 사이버억지의 새로운 패러다임: 신(新)일상성

- 이상과 같이 확대된 억지전략의 시각과 별도로, 사이버공간에서 제기되는 위협을 '비정상적인 위기'로 간주하기보다 항상 발생하는 정상적 상태, 즉 '신(新)일상성(new normalcy)'으로 보아야 한다는 주장도 제기되고 있음. 이는 사이버안보가 하나의 위기라는 시각 대신에 다른 종류의 범죄 현상과 마찬가지로 어느 사회에서나 일어나는 현상이라고 보는 것을 의미함. 따라서 위기 담론이나 안보 담론의 지나친 확장 대신 한정된 자원으로 외부의 위협에 적절하게 대처해야 한다는 우려가 이런 주장의 바탕에 깔려 있음. 그동안 테러와 사이버공격에 투입된 노력과 자원에 비례하여 그 성과가 눈에 띄게 나타났다고 보기는 어려움. 이런 점에서 자원과 위협의 인식 사이에 적절한 균형, 즉 '신균형(new balance)'의 인식이 필요하다는 것이며, 특히 일상생활에 상존하면서 지속적으로 진화를 거듭하는 사이버위협을 보편적인 사회적 범죄 현상으로 간주하자는 것임. 이러한 일상화 전략은 전염병을 완벽하게 퇴치하는 대신 적절한 수준에서 통제하려는 보건전략과 마찬가지로, 사이버공격과 위협을 어느 정도 받아들이면서 자원과 노력의 적절한 배분을 도모해야 한다는 현실적 한계에 대한 인식을 제고하자는 것을 바탕으로 함

5. 맺는 말

- 21세기 사이버공간의 발전은 세계를 하나로 묶는 통합의 역할을 수행하면서 동시에 더욱 복잡한 갈등의 원천이 되고 있음. 특히 사이버침해, 사이버공격, 첩보 등 다양한 형태의 공격이 네트워크상에서 일상화되면서 이를 방어 또는 억지하기 위한 군사전략적 대응태세도 점차 강화되고 있는 추세임. 사이버공격은 지난 10여 년에 걸쳐 간헐적으로 이루어져왔지만, '올림픽게임' 작전과 같이 심각한 물리적 피해를 야기하는 경우도 발생하고 있음. 이와 같이 지능형 지속위협(APT)으로 알려진 사이버공격은 전략적으로 구체적인 목표를 달성하기 위한 체계적이고 총체적인 노력으로, 사이버공간에서 국가안보를 위협하는 중요한 원인으로서 오늘날 안보담론과 국제정치의 중요한 화두가 되고 있음
- 사이버공간의 갈등과 억지행태는 기존의 재래식 무기 및 핵무기를 둘러싼 논의와 달리 구체적인 현안의 내용과 성격을 규정하기가 어려움.

특히 사이버공격 행위가 국제규범에서 금지하거나 제한적으로 허용하고 있는 무력 행사에 해당되는가의 여부가 관심을 끌고 있지만, '전쟁의 정당성에 관한 법'과 '전쟁 중 무력 행위에 관한 법'에 관한 논의에서 드러났듯이 지금까지의 국제규범과는 크게 다른 양상을 보이고 있음. 또한 사이버억지의 개념이 과거의 핵억지전략에서 통용되던 논리를 그대로 답습한 것이라고 보기에는 여러 가지 차이점들이 존재함. 이와 같이 사이버공간의 안보 문제 및 억지전략에서 나타나는 기존 패러다임의 한계를 극복하기 위해 누적적 억지, 맞춤형 억지, 자기 억지, 보증 전략, 우호적 점령, 신(新)일상성과 같은 대안적 시각에 대한 논의가 지속될 필요가 있음

사이버억지의 개념이 과거의 핵억지전략에서 통용되던 논리를 그대로 답습한 것이라고 보기에는 여러 가지 차이점들이 존재

참고문헌

Almog, Doron. 2004. "Cumulative Deterrence and the War on Terrorism." *Parameters* 34(4), 4-19.

Ambinder, Marc and D. B. Grady. 2013. *Deep State: Inside the Government Secrecy Industry*. Hoboken, NJ: Wiley.

Arquilla, John and David Ronfeldt. 1997[1993]. "Cyber War Is Coming!" In John Arquilla and David Ronfeldt, eds. *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND), 23-60.

Auerswald, David P. 2006. "Deterring Nonstate WMD Attacks." *Political Science Quarterly* 121(4), 543-568.

Bejtlich, Richard. 2010. "What APT Is (and What It Isn't)." *Information Security* (July/August), 20-24.

Bencsáth, Boldizsár et al. 2011. *Duqu: A Stuxnet-like Malware Found in the Wild*. Technical Report by the Laboratory of Cryptography and System Security. Budapest: Budapest University of Technology and Economics.

Boyer, Dave. 2015. "Obama Says Internet More Powerful Than Military, Sanctions Against North Korea." *Washington Times* (January 22).

Brecher, Aaron P. 2012. "Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations." *Michigan Law Review* 111, 423-452.

Bumiller, Elisabeth and Thom Shanker. 2012. "Panetta Warns of Dire Threat of Cyberattack on U. S." *The New York Times* (October 11).

Cimbala, Stephen J. 2011. "Nuclear Crisis Management and 'Cyberwar': Phising for Trouble?" *Strategic Studies Quarterly* 5(1), 117-131.

Clarke, Richard A. and Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do about It*. New York: ECCO.

Coll, Steve. 2012. "The Rewards (and Risks) of Cyber War." *New Yorker* (June 6).

Crosston, Matthew D. 2011. "World Gone Cyber MAD: How 'Mutually Assured Debilitation' Is the Best Hopw for Cyber Deterrence." *Strategic Studies Quarterly* 5(1), 100-116.

Danilenko, Gennady M. 1991. "International Jus Cogens: Issues of Law-Making." *European Journal of International Law* 2, 42-65.

Debus, Keith. 2012. "What Is Cyber War?" *Hacking* (April), 8-11.

Dunn Cavelty, Myriam. 2012. "The Militarization of Cyberspace: Why Less May Be Better." *Proceedings of the 4th International Conference on Cyber Conflict*, 141-153.

Farrell, Henry. 2013. "Cyber-Pearl Harbor Is a Myth." *The Washington Post* (November 11).

Farwell, James P. and Rafal Rohozinski. 2011. "Stuxnet and the Future of Cyber War." *Survival* 53(1), 23-40.

Farwell, James P. and Rafal Rohozinski. 2012. "The New Reality of Cyber War." *Survival* 54(4), 107-120.

Gardam, Judith. 2004. *Necessity, Proportionality and the Use of Force by States*. Cambridge: Cambridge University Press.

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38(2), 41-73.

Gates, Robert M. 2009. "A Balanced Strategy: Reprogramming the Pentagon for a New Age." *Foreign Affairs* 88, 28-40.

Geers, Kenneth. 2011. *Strategic Cyber Security*. Tallinn, Estonia: NATO CCDCOE.

Gill, Terry D. and Paul A. L. Ducheine. 2013. "Anticipatory Self-Defense in the Cyber Context." *International Law Studies* 89, 438-471.

Goldsmith, Jack. 2010. "Can We Stop the Global Cyber Arms Race?" *Washington Post* (February 1).

Goodman, Will. 2010. "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* 4(3), 102-135.

Gray, Colin S. 2013. *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling*. Carlisle Barracks, PA: US Army War College Press.

Harknett, Richard J. 1996. "Information Warfare and Deterrence." *Parameters* (Autumn), 93-107.

Hathaway, Oona A, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan,

William Perdue and Julia Spiegel. 2012. "The Law of Cyber-Attack." *California Law Review* 100, 817-885.

Huntington, Samuel P. 1983. "Conventional Deterrence and Conventional Retaliation in Europe." *International Security* 8(3), 32-56.

Inkster, Nigel. 2015. "Cyber Attacks in La-La Land." *Survival* 57(1), 105-116.

Jensen, Eric Talbot. 2012. "Cyber Deterrence." *Emory International Law Review* 26, 773-824.

Korns, Stephen W. 2009. "Cyber Operations: The New Balance." *Joint Force Quarterly* 54(3), 97-102.

Kugler, Richard L. 2009. "Deterrence of Cyber Attacks." In Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security* (Washington, D. C.: National Defense University Press), 309-340.

Levy, Jack S. 1988. "When Do Deterrent Threats Work?" *British Journal of Political Science* 18(4), 485-512.

Libicki, Martin C. 2007. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge: Cambridge University Press.

Liff, Adam P. 2012. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35(3), 401-428.

Lindsay, Jon R. 2013. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22, 365-404.

Lupovici, Amir. 2011. "Cyber Warfare and Deterrence: Trends and Challenges in Research." *Military and Strategic Affairs* 3(3), 49-62.

Lynn III, William J. 2010. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89(5), 97-108.

McGraw, Gary. 2013. "Cyber War Is Inevitable (Unless We Build Security In)." *Journal of Strategic Studies* 36(1), 109-119.

Montgomery, Evan Braden. 2006. "Breaking Out of the Security Dilemma: Realism, Reassurance, and the Problem of Uncertainty." *International Security* 31(2), 151-185.

Morgan, Patrick M. 2003. *Deterrence Now*. Cambridge: Cambridge University Press.

Paul, T. V. 2009. "Complex Deterrence: An Introduction." In T. V. Paul, Patrick Morgan and James Wirtz, eds. *Complex Deterrence: Strategy in the Global Age* (Chicago: The University of Chicago Press), 1-27.

Rathbun, Brian C. 2007. "Uncertain about Uncertainty: Understanding the Multiple Meanings of a Crucual Concept in International Relations Theory." *International Studies Quarterly* 51, 533-557.

Rid, Thomas. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35(1), 5-32.

Sanger, David E. 2012. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Crown.

Schmitt, Michael N. ed. 2014. *Tallinn Manual*. 한국전자통신연구원 부설연구소 옮김.『탈린 매뉴』. 서울: 글과 생각.

Sterner, Eric. 2011. "Retaliatory Deterrence in Cyberspace." *Strategic Studies Quarterly* 5(1), 62-80.

Stone, John. 2013. "Cyber War Will Take Place!" *Journal of Strategic Studies* 36(1), 101-108.

Symantec. 2011. "W32.Duqu: The Precursor to the Next Stuxnet." *Security Response*, Version 1.4(November 23).

Wazman, Matthew C. 2011. "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)." *Yale Journal of International Law* 36, 421-459.

Wehberg, Hans. "Pacta Sunt Servanda." *American Journal of International Law* 53, 775-786.

Yannakogeorgos, Panayotis A. 2012. "Internet Governance and National Security." *Strategic Studies Quarterly* 6(3), 102-125.

❖ 저자 약력

▌민병원

現 이화여자대학교 정치외교학과 교수. 서울대학교 외교학과 및 동 대학원 졸업. 미국 오하이오주립대학교 정치학 박사. 주요 연구 분야로는 국제정치이론, IT정치학, 안보, 동아시아 국제관계 등임. 주요 저술로는『동아시아의 보편성과 특수성』(공편),『집단지성의 정치경제』(공저),『복잡계로 풀어내는 국제정치』 등이 있으며, 주요 학술지에 국제정치이론과 안보, 복잡계이론, 문화와 국제정치 등에 관한 다수의 논문을 출간한 바 있음.

기획 및 감수: 이성우 (제주평화연구원 분쟁해결연구부장)
편집: 강현희 (제주평화연구원 연구원)
강윤미 (제주평화연구원 연구보조원)

제주특별자치도 서귀포시 중문관광로 227-24 (697-858)
전화: 064) 735-6500 팩스: 064) 738-6552
E-mail: policyforum@jpi.or.kr http://www.jpi.or.kr

ISSN: 2005-9760