Crisisonomy Vol.12 No.9, 129-142
ISSN 2466-1198 (Print) ISSN 2466-1201 (Online) http://dx.doi.org/10.14251/crisisonomy.2016.12.9.129


Crisisonomy

# In Search of Deterrence Strategy against Cyber Terrorism to Strengthen the National Security

**Dae Sung Lee[1#], Seong Bhin Joo[2+]**

[1] Department of Police Administration, Dong Eui University, 176 Eomgwang-ro, Busanjin-gu, Busan, Korea
[2] Department of Fire Service Administration, Dong Eui University, 176 Eomgwang-ro, Busanjin-gu, Busan, Korea

## Abstract

Recently, a growing number of researchers have expanded the discussion of deterrence strategy to address a host of new cyber threats. South Korea's allies and neighboring countries have begun to address terrorism beyond its conventional approach to cyber defense, from reactive to proactive, which may include international deterrence. South Korea should join this trend from passive to active approach to cyber terrorism, such as deterrence by denial and deterrence by punishment. Deterrence by denial is a strategy in which an adversary is physically prevented from acquiring a threatening technology, while deterrence by punishment is a strategy of last resort. Since it appears that deterrence by denial was not possible or has failed, the South Korean government should go beyond its passive attitude and develop timely and appropriate policies.

**Key words:** cyber attack, 4th Wave of Deterrence, active defense, deterrence by denial, deterrence by punishment

## Ⅰ. 서 론

최근 미국 국토안보부(United States Department of Homeland Security: DHS) 관계자는 이슬람국가(Islamic State: IS)가 사이버 공격을 개시할 가능성에 대하여 언급하면서, 에너지(전기・가스 등)와 발전소 등의 전력망에 대한 사이버 보안 수위를 높여야 한다는 주장하였다(Yonhap news, 2015년 11월 27일). 또한 현(現) 고노 타로(河野太郎) 일본 국가공안위원장은 IS(Islamic State)가 홍보와 모집을 위해 사용해온 인터넷을 중요 사회기반시설에 대한 사이버 공격에 이용할 가능성에 대하여 우려를 표명하였다(Newsis, 2015년 12월 2일). 이러한 일관된 주장은 IS(Islamic State)의 사이버전(戰) 역량이 매우 높은 것으로 밝혀지면서 신빙성이 더해지고 있고, 한국도 IS(Islamic State)가 테러리즘 대상국으로 지목한 만큼 그 위협의 예외가 될 수 없다는 사실을 인지하여야 한다.

사이버 테러리즘은 전통적 범죄 및 다른 특수범죄와 비교해보더라도 그 개념과 범위가 명확히 규정되어 있지 않고, 범죄의 특성상 공식적으로 이를 통한 직접적인 사망자가 나타나는 등 물리적・가시적 피해 사례도 제시하기 어렵기 때문에 실질적인 대응방안을 마련하

# The 1st author: Dae Sung Lee, Tel. +82-51-890-2195, e-mail. dorian3145@deu.ac.kr
+ Corresponding author: Seong Bhin Joo, Tel. +82-51-890-4292, e-mail. tjdqlswn@deu.ac.kr

기에는 한계가 있다. 그러나 2007년 에스토니아, 2008년 그루지야 등에서 발생한 사이버 테러리즘의 유형과 특성이 알려지게 되면서, 이에 대한 개념과 분류기준을 재정립하는 과정이 필수적임을 인식하게 되었다.[1] 최근에는 사이버 공간에서 지능형 지속 위협(Advanced Persistent Threat: APT)이라는 정보 절취 방법이 이용되는 등 공격되었는지조차 모르는 양상의 사이버 공격이 이루어지고 있어, 그 피해의 정도를 가늠하기가 쉽지 않은 실정이다. 특히, 세계 유일의 분단국가라는 우리의 현실과 북한의 사이버 공격 능력이 상당 수준에 도달했음을 감안해볼 때 사이버 테러리즘을 효과적으로 대응할 수 있는 방안을 고민하는 것은 무엇보다 선제적 과제로 인식되어야 한다.[2]

우리나라는 대(對) 테러리즘 전략을 수립하기 위해 지속적으로 노력해왔다. 하지만, 대(對) 테러리즘 전략에 있어 실질적인 기준이 될 「테러방지법」(안) 및 「사이버 테러방지법」(안)은 그 필요성에 대한 공감대가 형성되어 있음에도 불구하고, 특정 조직에 대한 권한의 남용과 통제의 부재라는 운영상의 문제점만 부각한 채, 본연의 실익은 가려져 있는 실정이다. 물론, 2001년 첫 발의된 「테러방지법」(안)이 2016년에 「국민보호와 공공안전을 위한 테러방지법」으로 제정・시행되는 결과로 이어졌지만, 관련 법률인 「국가 대테러활동과 피해보전 등에 관한 기본법」, 「테러예방 및 대응에 관한 법률」 등의 법안과 「국가 사이버테러 방지에 관한 법률」, 「사이버 테러리즘 방지 및 대응에 관한 법률」 등 사이버테러 방지 법안의 제정과 관련된 논의는 지지부진한 실정이다.

2016년 현재, 우리나라와 동맹관계를 유지하고 있거나 지리적 접근성을 보이는 국가들이 사이버 테러리즘을 바라보는 시각은 과거와 같이 테러집단에 의한 테러리즘 발생 가능성과 주도권을 사전에 인정하고, 이를 대응하기 위한 사전적 방안으로 예비・음모 처벌 논의, 범죄 발생 전 증거수집과 관련된 쟁점사항들을 논의하는 것에 그치는 것이 아니라, 적극적 억지전략(deterrence strategy) 방안을 구체화시키고 있다. 억지전략은 테러리즘 용의자와 테러리즘 계획에 관한 정보를 확보하여 테러리즘 공격이 구체화되기 이전에 무력화[3]시키는 것이 핵심내용이다. 테러리즘 공격의 결과는 물적 피해뿐만 아니라 시민의 심리적 불안감을 고려한다면, 테러리즘 발생 이후의 처벌보다는 사전 예방이 반드시 이루어져야 한다. 이런 정보의 억지전략은 광범위한 정보수집과 분석 그리고 정보기관들의 원활한 정보공유에 의하여 성패가 결정된다. 물론, 억지이론이 대(對) 테러리즘 정책을 수립함에 있어 유효성을 가지는가에 대한 많은 논란이 있는 것도 사실이다.

오늘날 사이버 공간에 대한 접근과 효과적인 활용은 각국의 안보와 사회・경제적인 발전에 필수적이다. 동시에 사이버 공간은 국가의 배타적 관할권 밖에 있기 때문에 글로벌 공공재(global commons)로서의 성격을 가지고 있다.[4] 따라서 사이버 공간에서 국가들 및 민간

1) 테러범죄의 유형을 정치・민족・이념의 목적의 달성을 위한 수단으로 테러리즘(terrorism), 준테러리즘(quasi-terrorism), 게릴라전(guerrilla-warfare)으로 분류하고(Lee, 2008: 270-271) 사이버 공격은 사이버범죄(Cyber Crime), 사이버테러(cyber terrorism'), 사이버전쟁(cyber war) 또는 사이버전(cyber warfare)으로 분류할 수 있다. 이러한 분류에 따라 어떤 기관이 어떤 형태로 개입할 것인가가 결정되고, 그것에 적용되는 규범이 달라진다. 따라서 이러한 분류는 상당한 의미를 갖는다고 할 수 있다.

2) 현재 북한은 6,000여명 정규 사이버 전문 인력을 보유한 것으로 알려졌다. 북한 해킹 수준은 2009년 세계 6위 수준이었지만 지금은 조직과 규모에서 미국, 중국에 버금가는 수준으로 평가되고 있고, 북한의 최고 영재를 차출해 지속적으로 사이버 전문가로 성장시키고 있다(Kim & KMARMA, 2015: 137-142; Hankookilbo, 2014년 12월 23일).

3) 억지이론(deterrence strategy)을 적용하기 위해서는 2가지 기본조건이 충족되어야 하는데, 첫째는 기습공격을 받은 뒤 보복할 수 있는 능력을 잠재적인 공격자가 인식하고 믿을 수 있어야 하며, 둘째로는 실제로 보복하겠다는 의지가 확실할 필요는 없지만, 그럴 가능성이 있다는 것을 잠재적인 공격자가 인식해야 한다(Min, 2015: 11-12).

4) 글로벌 공공재(global commons)는 인류공동자산이라는 의미로 이러한 공공 영역은 오늘날 주요국을 중심으로 하는 다양한 주체의 권력과 이익이 공존하는 새로운 국제 안보 무대로 볼 수 있다. 공공재(commons)는 원래 소유자를 특정 할 수 없이 그것이 때문에 불특정 여러 주체의 자유로운 접근이 가능한 공유지를 의미한다. 미국의 생태학자 Garrett Hardin의 유명한 논문인 '공유지의 비극(The tragedy of the commons)'에서 개인주의적 사리사욕은 결국 공동체 전체를 파국으로 몰고 간다는 것을 목초지의 이야기를 통해서 설명하고 있다. 자신의 이득을 극대화하려는 합리적인 선택의 결과 전체적으로 가공의 황폐 비극이 생긴다는 역설을 논하고 있다(The White House, 2010: 49-50).

기관에 의한 자율적인 질서가 요구되고 있다. 그러나 기존의 국제적 질서를 유지함에 중요한 역할을 담당했던 억지 메커니즘[5]은 육상, 해상, 공중, 우주에 이은 제5의 영역인 사이버 공간에서 많은 논란에 직면하고 있다. 최근까지 이러한 메커니즘은 미국의 국방・안보 공동체를 중심으로 몇 가지 요소로 인하여 사이버 공간에서의 처벌적 억지력 구축은 어렵다고 생각되어 왔다.

그러나 최근에는 국제적으로 사이버 공격의 출처를 확인하고 공격에 대응하기 위한 억지력을 마련하기 위한 노력을 하는 등 인식의 변화가 이루어지고 있다. 이러한 사이버 공간의 국방・안보 정책의 변화, 즉 처벌적 억지력의 추구를 한국의 현실에 접목시키는 법적・제도적으로 미비한 부분이 많이 있다. 이들의 개선을 바탕으로 물리적 공간에서의 증거를 바탕으로 한 억지전략뿐만 아니라 사이버 공간에서 활용 가능한 영역들을 범죄를 예방하고 진압하는 업무에 접목 가능하도록 미리 준비해야 한다. 특히 범죄가 발생하면 어떠한 범죄유형보다 물질적・정신적 피해가 극심하고 피해의 원상복구가 어려운 테러리즘 등 안보범죄에 대한 사이버 상 증거능력을 포괄적으로 인정하여 이들 범죄가 발생하기 전에 사전 감시가 가능한 증거로 인정될 수 있는 방안을 마련해야 한다. 또한 사이버 테러리즘은 한 국가의 시스템 구축으로만 해결될 수 없는 초국가적 범죄유형으로 국가간 테러리즘 범죄자들에게 강력한 대응이 이루질 수 있도록 공조체계 구축이 동시에 이루어져야 한다.

## II. 이론적 검토

### 1. 사이버 테러리즘의 의의

사이버 테러리즘의 개념을 검토하기 위하여 한국의 국가정보원과 미국의 국제관계 전략연구소(The Center for Strategic and International Studies: CSIS), 캐나다 안보정보청(Canadian Security Intelligence Service: CSIS), 주법 제정을 위한 국가연구회의(The National Conference of State Legislatures: NCSL)에서 제시하고 있는 내용을 살펴보면 다음과 같다.

먼저, 「국가사이버안전관리규정」은 사이버공격을 해킹・컴퓨터바이러스・논리폭탄・메일폭탄・서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입・교란・마비・파괴하거나 정보를 절취・훼손하는 일체의 공격행위라 규정하고 있다. 그리고 '사이버위기'란 사이버공격으로 정보통신망을 통해 유통・저장되는 정보를 유출・변경・파괴함으로써 국가안보에 영향을 미치거나 사회・경제적 혼란을 발생시키거나 국가 정보통신시스템의 핵심기능이 훼손・정지되는 등 무력화되는 상황(동 규정 제2조)으로 명시하고 있다(http://www.lawnb.com/, 2016년 8월 25일 검색). 미국의 국제전략연구소(Center for Strategic and International Studies: CSIS)는 에너지, 교통, 정부기관 등 주요 국가기반시설을 중단시키거나 정부 또는 시민들을 강제 또는 협박하기 위하여 컴퓨터 네트워크 도구를 이용하는 것이라 정의하였고(https://www.csis.org, 2016년 8월 25일 검색), 캐나다 안보정보청(Canadian Security Intelligence Service, CSIS)은 에너지, 교통, 정부기관 등 주요 국가기반시설을 중단시키거나 정부 또는 시민들을 강제 또는 협박하기 위하여 컴퓨터 네트워크 도구를 이용하는 것으로(https://www.csis.gc.ca/, 2016년 8월 26일 검색), 주법 제정을 위한 국가연구회의(National Conference of State Legislatures: NCSL)는 자신(들)의 의도를 성공시키기 위해 테러리스트 집단 또는 개인에 의한 정보기술의 이용. 이는 네트워크, 컴퓨터 시스템, 텔레커뮤니케이션 기반시설을 대상으로 공격을 조직・실행하거나 전자적으로 정보를 교환하거나 위협하기 위한 정보기술의 이용을 포함하는 활동으로

5) 억지력(deterrence)은 자율적인 질서 형성・유지에 공헌한다. 억지는 상대에 네거티브 메시지를 보내는 것으로 '상대방이 하고자 하는 행위를 단념시킬 것'을 의미하는 것으로 범죄를 예방하고 진압하는 형사사법체계의 관점에서 살펴본 억지의 일반적인 모델은 무력에 의한 보복을 시사하면서 상대방 행위를 단념시키는 처벌적 억지 또는 징벌적 억지(punitive deterrent)이다. 이는 과거 냉전기에 핵 및 재래식 전력에 의해 구성된 억지 메커니즘의 형태로 미・소(美・蘇) 대립 구조에 일정한 안정성을 주는 '평화적' 역할도 담당하였다.

정의하고 있다(www.ncsl.org, 2016년 8월 26일 검색).

## 2. 사이버 공간의 억지론(deterrence)

### 1) 억지(deterrence)의 의의

억지의 개념은 제2차 세계 대전 이전에도 존재했지만 그 정교한 이론화 과정은 핵 전략의 발전과 밀접하게 관련되어 있다.[6] 왜냐하면 이란의 사례에서 볼 수 있듯이 핵무기의 보유하여 국방・안보 정책의 목적(또는 군조직의 역할)을 전쟁에 승리하기 위한 것에서 전쟁을 일으키지 않는 형태로 억지의 메커니즘을 변화시켰기 때문이다. 이러한 역할도 억지의 개념으로 본다면, 냉전시대로 상징되는 억지형태인 보복을 시사하면서 상대방 행위를 단념시키는 처벌적 억지로 과거의 단순한 보복(retaliation)을 의미하는 개념보다 오늘날 안보정책에서 표현되는 억지는 더 넓은 개념으로 볼 수 있다(Lee, 2013: 4-6; Lee, 2011: 16-18; Nye, 2011: 33).

억지의 개념을 상대에게 부정적인 메시지를 보내기 위한 "상대가 하려고 하는 행위를 단념시키는 것이다"라고 정의한다면, 그 형태는 다양하다. 예를 들어 누구를 억지하느냐에 따라 자국 억지(central deterrence)와 동맹국을 포함한 확장 억지(extended deterrence)로, 언제 억지하느냐에 따라 유사 억지(immediate deterrence)와 평시 억지(general deterrence) 등으로 구분할 수 있다(Jun, 2010: 1-6; Freedman, 2004: 124-125; Morgan, 1983, 2003: 9-10).

특히 주의해야 할 것은 억지 메커니즘이다. 이 메커니즘에서 억지가 성립하는 경우는 공격 실패 비용의 기대 값이 공격 성공 이익의 기대치를 상회하는 것이다. 억지 메커니즘을 성립시키기 위한 방법은 크게 두 가지로 구분될 수 있다. 하나는 상대의 이익을 부인하는 거부적 억지(deterrence by denial)이며, 다른 하나는 상대에게 비용을 부과하는 처벌적 억지(deterrence by punishment)이다(Nevill & Hawkins, 2016: 6-8; Van Der Putten, *et. al.*, 2015: 35-36; Iasiello, 2014: 55-60; Ko, 2014: 218-222; Wenger & Wilner, 2012: 21-30; Knopf, 2010: 10-12; Dunn, 2008; Quinlan, 2004: 11-17).[7]

### 2) 사이버 공간에서의 억지(deterrence) 메커니즘의 변화

과거에는 사이버 공간에서는 종래적인 억지 메커니즘이 ① 사이버 공격의 출처를 확인하기 어렵이라는 점(귀속 문제, attribution problem), ② 인터넷 공간에서는 방어보다 공격이 유리한 점(공격 우위, superiority of attack)을 근거로 작동하지 않는다고 생각되어 왔다. 즉, 사이버 공간의 현상은 방어에 대한 공격이 우세하고, 그 공격의 출처를 특정 짓기 어려우므로 이러한 상황에서 처벌에 의한 억지 메커니즘은 작동되기 어렵다는 접근 방법이 지배적이었다. 또한 부시(George W. Bush), 오바마(Barack Obama)의 두 정권에서 사이버 보안 정책에 참여한 클라크(Richard A. Clarke) 역시

6) "Deterrence"는 우리나라 표현으로 억지(抑止) 혹은 억제(抑制) 등으로 번역되고 있다. 국립국어원은 억제를 "감정이나 욕망, 충동적 행동 따위를 내리눌러서 그치게 함" 또는 "정도나 한도를 넘어서 나아가려는 것을 억눌러 그치게 함"으로 정의하고 있다. 하지만 이러한 정의는 개인적・미시적인 개념으로 국가안보 등의 분야에서 사용될 용어로는 지엽적인 경향이 있다. 따라서 통상 국제안보와 군사전략 분야에서는 "deterrence"를 억지로 번역하고 있다(국립국어원, 2016년 8월 19일 검색; Jun, 2012: 13).

7) 억지이론은 그 이론적 견고함과 현실적인 적용 가능성에 대해 많은 논의가 진행되었다. 특히, 핵무기가 개발된 이후, 핵에 기반한 억지이론이 주류를 이루면서 핵 억지에 대한 부분에서 특히 많은 논의들이 이루어졌다. 최근에는 4세대 억지이론(4th Wave of Deterrence)에 대한 논의가 대(對) 테러리즘 정책 부문에서도 활발하게 진행되고 있다. 첫째, 간접적 억지(indirect deterrence)이다. 이는 테러리즘을 지원하는 국가 및 개인에 대한 재정적 제재조치나 투옥 등을 포함한 위협을 제3자적 행위자에게 강요함으로써 테러리즘 행위를 근절하고자 하는 억지정책이다. 둘째, 처벌적 억지(deterrence by punishment)이다. 테러단체에 대한 직접적인 처벌적 억지의 적용은 억지의 실현가능성이 매우 낮다는 것은 이미 많은 연구들을 통해 주장되고 있다. 그러나 테러단체의 수장 등에 대한 공격이 전체적인 테러리즘 활동량을 감소시키지는 못하였다고 하더라도, 테러의 대상이 되는 목표물의 중요성, 테러의 강도, 효과 등에 대해서는 약화시켰다는 직접적인 연구결과도 있다. 셋째, 거부적 억지(deterrence by denial)이다. 즉, 테러리스트들이 선호하는 전략적/전술적 이점들을 제거함으로써, 그들이 원하지 않는 행동 및 결과가 나타나게 할 수 있다는 것이다. 이를 다시 해석하면, 테러리즘 행위자들에게 그들이 계획한 테러리즘 행위가 충분한 효과를 거두지 못할 것이라는 것을 인지시킴으로써 테러리즘 행위의 발생을 억지할 수 있다는 것이다(Ko, 2014: 219-222; Wilner, 2010; Alexander, 2003: 465).

'전략적 핵 전쟁 방지의 중요한 개념이자 이론인 억지이론은 현 단계에서 사이버 테러리즘을 저지하는 데 아무런 중요 역할을 수행하지 않는다'고 언급하였다. 억지 연구의 전문가인 모건(Patrick M. Morgan)도 현재 사이버 공격의 문제는 규모와 특징면에서 냉전시대와 매우 다름을 인정하고, 냉전시대의 억지적 방법과는 다른 방식으로의 접근방법이 효과적인 대응방안이 될 수 있음을 언급하였다(Bendiek & Metzger, 2015: 560; Lupovici, 2011: 54-57).

그러나 이러한 견해는 변화하고 있다. 최근 미국의 안보 정책은 사이버 공간에서 공격원을 특정하고 보복이나 처벌하기 위한 억지 메커니즘(처벌적 억지력)을 모색하고 있다. 이러한 변화는 2011년 11월 의회에 제출된 '미국 국방부 사이버 정책 보고서(Department of Defense Cyberspace Policy Report)'에 반영되어 있다(Min, 2015: 13-16; Department of Defense, 2011: 1-2).[8)]

## Ⅲ. 사이버 공간에서 억지력 모색의 새로운 국면

사이버 공간은 공격자 우위이며, 공격원을 특정하기 어렵다. 그러므로 미국 국방·안보 공동체는 냉전시대와 같은 처벌적 억지력이 작동하지 않을 것으로 판단하여 왔다. 그러나 현재는 사이버 공간에서 처벌적 억지력을 추구하려는 정책을 모색하고 있다.

### 1. 린(Lynn)의 억지론과 적극적 방어(Active Defense)

#### 1) 린(William J. Lynn, Ⅲ)의 억지론

린(William J. Lynn, Ⅲ)은 미국 국방부 등의 사이버 보안 대책의 주요 인사이며, 오바마(Barack Obama) 행정부에서 국방부 장관을 역임한 사이버 테러리즘 전문가이다. 앞에서 살펴본 바와 같이, 사이버 공간의 특수성과 시대적 상황의 변천으로 인하여 냉전 시대에 확립된 처벌적 억지 정책은 사이버 공간에 적용할 수 없다. 이것이 최근까지 사이버 공간에서 발생하는 범죄를 대응하기 위한 다양한 방법론 중 억지 정책에 대한 미국 국방부의 공식적인 입장이었다. 사이버사령부(United States Cyber Command: CYBERCOM) 사령관 알렉산더 장군(Keith B. Alexander)은 2010년 9월 상원위원회 청문회에서 사이버 상에서 발생하는 각종 사안들을 억지시키기 위한 프레임 구축에 어려움을 토로하였다. 그는 사이버 분야의 억지는 다른 분야와는 사이하고 냉전시대와 같은 기능은 적절하지 않고, 다양한 관점에서 억지를 쇄신하는 연구를 하여야 함을 강조하였다(http://abcnews.go.com, 2016년 9월 2일 검색; http://archive.defense.gov, 2016년 9월 2일 검색).

#### 2) 적극적 방어

냉전시대의 처벌적 억지를 대신하여 강조한 것이 거부적 억지력(deterrence by denial)이다. 즉, 사이버 공간에서는 보복에 의해 사이버 공격자에 비용을 부과하는 처벌적 억지(deterrence by punishment)는 어렵지만, 사이버 공격자의 이익을 부정하는 거부적 억지력의 실현은 가능하다. 사이버 공간의 거부적 억지력을 국가정책과 연결시켜 보면 '적극적 방어(active defense)'라고 표현되고 있는 사이버사령부(CYBERCOM)의 중점방향과 유사하다고 볼 수 있다. 즉, '공격 및 위협에 대응하기 위한 사이버 공간에서의 운영 전략(Department of Defense Strategy for Operating in Cyberspace)'에 따르면 국방부는 '네트워크와 시스템에 대한 침입을 예

8) 미국 국방부는 국가 안보를 영위하기 위한 공간으로 사이버의 중요성을 인식하였다. 따라서 군사·정보·비즈니스 작전을 수행할 때 사이버공간이 지닌 잠재력을 조직화·훈련·장비하기 등의 작전 영역으로 활용하고, 적극적인 사이버 방위의 필요성 인식, 동맹국 및 국제 파트너 국가들과 공고한 관계를 구축하여 정보를 공유하고 집단 사이버보안 강화 등의 방법으로 안보영역의 현실적 노력에 초점을 맞추고 있다. 특히, 미 국방부는 사이버 공간의 복잡한 도전과제와 기회를 통합적인 방식으로 다루고 있고, 거부적 억지(deterrence by denial)와 처벌적 억지(deterrence by punishment)의 두 가지 주요 메커니즘을 따르고 있다(Lee, 2015: 128-129; Jun, 2012: 16-17; Department of Defense, 2011: 2).

방하고 침입한 적의 행위를 진압하는 적극적인 사이버 방어(active cyber defense)를 전개하겠다고 언급하였고 적극적인 사이버 방어는 위협과 취약점을 발견하고 분석함으로써 피해를 줄이기 위한 실시간으로 노력해야 한다고 하였다. 즉, 적극적인 방어는 사이버 공격을 사전에 탐지하고 실시간으로 분석・감지하여 네트워크를 방어하는 것과 이러한 일련의 투자 및 업데이트를 일컫는다(川口 貴久, 2014: 18). 그러나 원래 거부적 억지력(deterrence by denial)의 메커니즘은 '제약(restriction)'이 핵심 키워드이다. 따라서 사이버 공격의 이익과 성공 확률을 최소화시키도록 해야 한다. 사이버 공격으로 인한 비용이 0에 가까우면, 공격의 인센티브가 항상 존재한다. 따라서 사이버 억지 정책을 펼침에 있어 거부적 억지력뿐만 아니라, 처벌적 억지력(deterrence by punishment)을 추구하게 된다.

## 2. 패네타(Panetta) 연설과 처벌적 억지력(Deterrence by Punishment)

### 1) 개요

공격 소스를 특정하여 사이버 테러리즘에 대응하는 방법이 처벌적 억지력(deterrence by punishment)을 모색하는 방편 중에 하나이다. 전(前) 미국 합동참모본부(Joint Chiefs of Staff: JCS) 부의장인 카트라이트(James E. Cartwright)가 해병대 대장직을 수행할 때 미국은 처벌적 억지와 공격 옵션의 필요성을 언급해왔다. 그에 따르면 21세기의 억지는 그것이 핵무기든 생물무기든 사이버 공격이든 넓은 의미에서 익명성(anonymity)와 귀속(attribution)에 관한 것으로 보고 효과적인 억지력의 형태로 방어적인 옵션만으로는 불충분하며 공격적인 옵션이 필요하다고 하였다. 이처럼 최근에는 공격적 옵션이 필요하다는 견해가 주 의견으로 형성되어 가고 있다. 미 국방부가 의회에 제출한 '공격 및 위협에 대응하기 위한 사이버 공간에서의 운영 전략(Department of Defense Strategy for Operating in Cyberspace)'에서는 사이버 공간에서의 억지는 2가지 기본 메커니즘에 입각한다고 하였다. 즉, 적의 목적을 부정하는 것이며, 필요하다면 침공하는 적에게 비용을 부과한다는 것이다. 2012년 10월의 패네타(Leon E. Panetta) 국방 장관의 연설은 사이버 억지를 생각하는 데 있어서 큰 전환점이 되었다(http://www.cfr.org/, 2016년 9월 1일 검색; "Secretary of Defense Leon Panetta discusses the global threat of cybersecurity attacks at the Business Executives for National Security in New York City, October 11, 2012"; Panetta, 2012: 4).

> 국방부의 네트워크를 방어하기 위해, 우리는 공격자에 대한 억지 방안을 강구하고 지원한다. 우리가 사이버 공격자를 추적할 수 있는, 혹은 사이버 공격이 강력한 방어 능력으로 인해 실패할 수 있음을 공격자가 인식하고 있으면 그들이 우리를 공격할 가능성은 낮아진다. 국방부는 사이버 공격의 억지를 복잡하게 하는 문제, 즉 공격원을 특정하는 문제들을 해결한다는 점에서 지속적인 진전을 이루고 있다. 국방부는 특정 문제를 해결하기 위하여 "Forensics" 분야에 많은 투자를 해왔고 투자에 알맞은 성과를 보이고 있다.

### 2) 처벌적 억지력

패네타(Leon E. Panetta)가 말하는 '진전'의 구체적 내용은 불명하지만, 국방부 '공격 및 위협에 대응하기 위한 사이버 공간에서의 운영 전략(Department of Defense Strategy for Operating in Cyberspace)'에서 제시한 대응방향과 유사한 맥락으로 보인다. 구체적으로는 공격의 물리적 발신 근원을 추적하는 방법 및 행동을 기반으로 하는 알고리즘(behavior-based algorithms)에 따라 공격자들을 평가하고 자료를 구축하기 위한 사이버 포렌식(cyber forensics, 사이버 공격이 이루어진 경우 컴퓨터 및 네트워크 등의 로그를 통한 증거보전과 공격 전 조사), 지능형 커뮤니티와 CYBERCOM을 중심으로 하는 전문가를 육성하고, 국토안보부(Department of Homeland Security)와의 연계 등의 대응방안이다. 또한 부처 간이나 국가간에 새로운 악성 코드 표시기를

교환하고 교류하는 것도 효과적인 대응방법이 될 것이다(http://www.jag.navy.mil, 2016년 9월 3일 검색; 川口 貴久, 2014: 19-20).

사이버 공간에서 공격원을 특정하기 어렵다. 그러나 이러한 문제를 넘어 처벌적 억지력(deterrence by punishment)이 형성되고 있다. 중요한 점은 적극적인 방어(거부적 억지력)과 처벌적 억지력은 상당 부분 중복되는 경향이 있다는 것이다. 냉전시대는 공격용과 방어용 핵무기・미사일을 구별할 수 있었다. 하지만 사이버 공간에서는 거부 억지력・처벌적 억지력, 공격・방어를 명확하게 구분할 수 없다. 사이버 무기는 하나의 시스템에서 여러 가지 요소를 겸비한 것이다. 따라서 이들에 대응하기 위해서는 사이버 공간에서의 억지 공격이며, 방어적이고 지능적인 운영 및 대응이 필요하며, 이들을 융합시킨 것이 요구된다.

### 3. 광범위한 억지 및 단계별 통제

사이버 공간의 억지력은 사이버 공간에만 한정되지 않고 공격에 대한 보복이나 처벌행위는 광범위하게 나타난다. 실제로 미국은 사이버 공격에 육・해・공・우주에서 역학적(kinetic) 방법에 의한 보복을 시사하고 있다. '사이버 공간에서의 정책 보고서(Department of Defense Cyberspace Policy Report, A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934)에서는 다음과 같은 내용이 있다(Department of Defense Cyberspace Policy Report, 2011: 2-5).

> 사이버 공간의 악의적인 행위로부터 미국 동맹국, 파트너, 국익을 보호하기 위해 미합중국 대통령은 필요한 수단(all necessary means)을 사용하여 해당 권한을 가진 … (중략) … 대통령의 지시에 따라 국방부에서 제공하는 사이버 능력 및 물리적 능력(kinetic capabilities) 중 하나 또는 모두를 포함한다.

이러한 물리적 능력은 핵 전력을 포함하는 견해도 있다. 국방부의 자문 기관인 국방 과학위원회(Defense Science Board: DSB)는 최근 보고서에서 효과적인 국방부 사이버 전략에 억지 요소가 필수적이라고 언급한 내용에서 사이버 공격에 대한 억지력으로 핵 전력을 유지할 것을 권고하고 있다. 그것은 핵무기 시스템이 가장 사이버 공격에 강하고, 효과성이 높은(resilient)는 대응이라 판단했기 때문이라 여겨진다. 그러나 실제 군사 행동을 시사하는 것으로, 위기가 점점 더 커지고 있는 위험상황이 항상 존재하고 현실적으로 핵 전력을 유지하기는 쉽지 않은 국제정세 속에서 사이버 테러리즘을 방지하기 위하여 대상과 수단을 고려한 강력한 단계별 통제전략이 요구된다는 의미로 재해석할 수 있다(川口 貴久, 2014: 20; Defense Science Board, 2013: 40-43).

## Ⅳ. 한국적 상황에서 사이버 공간에서의 억지력 모색

### 1. 국내외 억지력 모색

#### 1) 거부적 억지력(deterrence by denial) 접근

거부적 억지력(deterrence by denial)의 접근방법은 적극적인 사이버 방어방법으로 테러리스트 등의 안보위협 요인과 취약점을 발견하고 분석함으로써 피해를 감소시키기 위한 노력을 실시간으로 노력해야 한다고 보는 관점이다. 즉, 이러한 적극적인 방어는 사이버 공격을 사전에 탐지하고 실시간으로 분석・감지하여 네트워크를 방어하는 것과 이러한 일련의 투자 및 업데이트를 일컫는다.

첫째, 「사이버 테러리즘 기본법」 제정이 필요하다. 산재해 있는 사이버 테러리즘 대응 및 위기관리 관련 법제를 정비하여 국가차원의 사이버 위기를 예방하고, 위기 발생 시 일원화된 종합적인 사이버 테러리즘 대응 및 위기관리 체계를 구축하기 위해서 관련법을 제정할 필요가 있다. 즉, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「정보통신기반 보호법」, 「국가사이버안전관리규정」을 통합한 사이버 테러리즘 기본법 제정이

필요하다. 기본법에 국가차원의 대응체계, 부처 간 역할과 책임을 명확히 규정하여 불필요한 갈등을 없애야 할 필요가 있다. 가령, 예방・대응 조직과 수사기관, 수사기관과 군, 군과 예방・대응조직 간의 역할을 규정하고, 사이버 테러리즘에 대한 명확한 개념정의에 대하여도 고려해야 한다. 왜냐하면 추상적이고 모호하게 설정할 경우 국가안보라는 이유로 국민의 프라이버시를 과도하게 침해할 수 있고, 범죄수사의 개념으로 축소하여 설정할 경우 사이버 테러리즘 위협에 선제적으로 대응하지 못한다는 비난을 받을 수 있기 때문이다. 따라서 사이버 테러리즘에 대한 종합적이고 체계적인 사이버 위기관리가 이루어질 수 있는 내용을 골자로 각계의 의견을 수렴 후, 발생 가능한 운영상의 부작용을 최소화할 방안을 강구해야 한다.

둘째, 「통신비밀보호법」의 개정이 필요하다. 테러범죄자들은 주로 국제적인 조직망을 두고 테러범죄를 준비, 실행하기 때문에 범죄정보를 수집하고 테러혐의자를 추적하기 위해서는 유・무선 통신에 대한 통신제한조치가 필요하다. 따라서 간첩・테러리즘・산업스파이・국제범죄 조직 등과 관련된 외국인에 대한 휴대전화 및 SNS 감청을 허용하는 것은 필요하다. 또한, IS(Islamic State) 등 국제 테러단체들과 내국인 간 연계에 의한 테러리즘 발생가능성도 간과해서는 안 되므로 「통신비밀보호법」 개정 논의시 내・외국인이라는 대상 한계를 구분 짓지 아니한 상황에서 세밀한 검토가 이루어져야 할 것으로 보인다. 물론, 감청 대상자에 대한 엄격한 기준을 정립하여 개인의 사생활 침해 및 민간인 사찰이 이루어질 수 있다는 여지를 사전에 차단하는 입법적 조치가 선행되어야 함은 당연하다.

2) 제도적 접근

테러리스트 등에 의한 안보위협 요인과 취약점을 발견하고 분석하기 위해 테러리즘 발생상황에 대한 충분한 위험 범위를 설정하고 이에 적절한 제도적 접근이 이루어져야 한다.

〈Table 1〉은 테러리즘이라는 불확실하지만 높은 위험성을 가진 범죄행위에 관한 인지 모델(simple cognitive model)과 같은 제도적 접근방법을 고민해봄으로써, 사전 예방 및 사후 최소한의 피해 및 복구가 가능하도록 도구적 프레임을 제시할 수 있다.

## 2. 국제적 억지력 모색

1) 처벌적 억지력(deterrence by punishment) 접근

처벌적 억지력(deterrence by punishment)의 접근방법은 공격의 물리적 발신 근원을 추적하는 방법 및 행동을 기반으로 하는 알고리즘(behavior-based algorithms)에 따라 공격자들을 평가하고 자료를 구축하기 위한 사이버 포렌식(cyber forensics, 사이버 공격이 이루어진 경우 컴퓨터 및 네트워크 등의 로그를 통한 증거보전과 공격 전 조사), 지능형 커뮤니티와 CYBERCOM을 중심으로 하는 전문가 육성 등으로 구체화할 수 있을 것이다.

첫째, 디지털 포렌식(Digital Forensic)을 통한 전문영역의 확장이다. 디지털 포렌식(Digital Forensic)은 디지털 증거를 수집하여 분석하는 기술을 말하며 디지털 정보의 상태와 그것들로부터 알 수 있는 정보 및 현 상태에 이르게 한 일련의 사건들을 설명하는 것을 주목적으로 하고 있다. 디지털 증거 수집 및 분석 과정은

Table 1. A simple cognitive model

| Subjectively estimated with deep uncertainty; qualitative | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Option | Worst-case outcome | | Expected outcome | | Best-case outcome | | Net Assessment* | |
| Model | ModelA | ModelB | ModelA | ModelB | ModelA | ModelB | ModelA | ModelB |
| Do nothing different | | | | | | | | |
| Conduct Attack X | | | | | | | | |
| Do something else | | | | | | | | |

※ Source: Paul K. Davis, 2014: 18.

*: Net Assessment is a function of the preceding columns and the decision maker (e.g., Model A or B)—e.g., on the decision maker's risk-taking propensity or passion for the possibility of a best-case outcome.
Cell values might be subjective assessments of outcome on a scale of, e.g., -10 to 10.

기술적으로 복잡하고 난해하여 분석가의 전문성에 의해 증거의 무결성과 신뢰성이 결정된다. 요즘에는 과거에 비해 사이버 범죄가 보다 빈번해지고 인권에 대한 의식 수준이 많이 향상된 것을 볼 수 있다. 이런 상황 속에서 IT 관련 기관과 기업, 검찰과 경찰을 중심으로 하여 디지털 포렌식에 관심이 집중되고 있다. 더욱이 미국에서는 전자증거개시(E-Discovery)라는 분야에서 디지털 포렌식에 대한 관심이 개인의 민사소송과 기업의 보안 차원까지 이르고 있으며, 우리나라에서는 아직 전자증거개시에 대한 법률적 도입이 미비하나 논의가 이루어지기 시작한 단계이므로 안보사범의 수사에 있어서도 활발히 활용될 것으로 보인다(Yun & Joo, 2014: 168-169).

둘째, 사이버 테러리즘 대응 전문가 양성이다. 테러조직은 인터넷을 통해 잠재적 테러리스트를 확보하는 사례[9]가 확인되는 등 테러리스트들의 활동을 감시하는 도구로 활용되었던 인터넷 등의 소셜 네트워크가 테러리스트들을 모집하는 수단이 될 수 있다는 점을 감안한 대응방안이 마련되어야 할 것이다. 따라서 대(對)테러리즘 활동을 함에 있어서 테러조직의 활동의 체계적으로 분석하고 예측할 수 있는 전문적 자질을 갖춘 인적자원이 필요하다. 특히, 오늘날 테러리즘 발생 현황을 살펴보면, 중동에서 발생 또는 중동의 역사적 배경을 공유하는 이들에 의해 발생하고 있다. 따라서 테러리즘 및 사이버 테러리즘에 효과적으로 대응하기 위해서는 관련 업무에 대한 선행지식은 기본적으로 함양하고, 그와 더불어 테러리즘 빈발지역 및 대상자들에 대한 역사적 배경을 바탕으로 현 실태를 정확히 진단할 수 있는 전문적인 지식을 가진 인적자원이 확보되어야 한다.

2) 제도적 접근

사이버 공간에서 발생하는 사이버 테러리즘은 단순히 국내의 법제도 개선만으로는 근본적인 대응방안을 모색함에 있어 어려움이 많다. 따라서 그에 대한 효과적인 대응을 위해서는 국제적 정서의 정확한 진단과 국제법에 의한 절차에 대한 이해가 선행되어야 한다. 특히, 물리적 공간에서 발생한 국지전(戰) 형태가 아닌 사이버 상에서 이루어진 공격행위를 무력 또는 물리력 행사에 준하는 행위를 사용하여 대응할 수 있는지에 대한 문제에 대해서는 UN헌장에서 다루어지고 있다(Lee & Lee, 2015: 322).

3) 국제적 합의 도출

최근, 북한에 의해 행하여진 사이버공격을 '탈린 매뉴얼(The Tallinn Manual on the International Law Applicable to Cyber Warfare: TM)'[10] 기준에 의해 살펴보면, 무력사용의 수준에 높지 않아, 우리의 대응은 매우 제한적이다. 하지만 수년 간 지속된 사이버 공격의 수행주체가 북한으로 고정되어 있다는 점에 주목한다면 그 평가가 달라질 수 있다.

지난 몇 년간 발생한 사이버위기 상황에서 각 사건을 개별적으로 살펴보면, 각각의 사건은 앞서 검토한대로 무력사용의 수준에 이르지 못하지만, 연속적인 선상에서 보면 북한은 우리의 정보통신기반 시설에서부터 국

9) 알-카에다에 자발적으로 동참하기 위해 파키스탄에 갔다가 최근 체포된 미국 국적의 무슬림 청년 5명이 테러리즘 관련조직과의 첫 접촉을 인터넷을 통한 것으로 밝혀졌는데, 북버지니아에 거주하는 18-24세 사이의 이들 미국인 5명 가운데 한 명이 미군에 대한 공격 장면을 보여주는 동영상을 반복적으로 유튜브에 올렸고, 파키스탄에 있던 테러리스트 모집책이 이를 본 뒤 이 청년과 첫 접촉을 시작했다는 것이다(Hankookilbo, 2016년 8월 15일 검색).

10) 탈린 매뉴얼(Tallin Manual)은 기존의 육상, 해상, 공중에 대한 무력분쟁의 논의들인 '제네바 협약과 각 부속서, 해양에서의 무력충돌에 적용되는 국제법에 관한 산레모 매뉴얼(San Remo Manual on International Law Applicable to Armed Conflict at Sea: San Remo Manual)', '공중전에 적용되는 국제법에 관한 매뉴얼(Manual on International Law Applicable to Air and Missile Warfare: Harvard Manual or AMW Manual)과 마찬가지로 기존 규범들을 사이버전에 적용할 수 있음에 대한 다양한 문제들에 대하여 논의점을 제공하고 있다는 공통점을 가지고 있지만, 현재까지 국제사회에서 어떠한 구속력도 없는 "가이드라인"으로만 제시되고 있다는 한계가 있다. 그러나 현재까지 이루어져 온 국제법 체계의 합의 동향을 고려한다면 향후 사이버전 분야의 국제법적인 기준은 탈린 매뉴얼이 근간을 이루게 될 것임은 쉽게 판단이 가능하다(Choi, 2014: 391; Michael N. Schmitt, 2013; Harvard University Program on Humanitarian Policy and Conflict Research, 2009; Louise Doswald Beck, 2005).

Table 2. Evaluation of the North Korea cyber terrorism by tallinn manual

| | 7.7 DDoS (2009) | 3. 4 DDoS (2011) | NH (2011) | 3.20 CT (2013) | KHNP CT (2014) |
|---|---|---|---|---|---|
| Seriousness | △ | △ | ○ | ○ | × |
| Extemporaneity | ○ | ○ | ○ | ○ | × |
| Immediacy | △ | ○ | ○ | ○ | △ |
| Invasiveness | △ | △ | ○ | △ | × |
| Feasibility of Measurement | △ | △ | ○ | △ | ○ |
| Military Purpose | △ | △ | △ | △ | △ |
| Responsibility | ○ | ○ | ○ | ○ | ○ |
| Justification | △ | △ | ○ | ○ | △ |
| sign of attack | × | × | × | × | × |
| Record | × | △ | △ | △ | △ |
| Target of Attack | △ | △ | ○ | ○ | ○ |
| Evaluation | △ | △ | ○ | △ | × |

※Source : Lee & Lee, 2015: 326-327.

가기반시설에 이르기까지 그 목표를 바꿔가며 지속적으로 사이버공격을 감행하였다. 이것을 '사건의 누적' 이론[11]에 대입시켜보면 충분히 무력사용의 수준에 이름을 알 수 있다.

이처럼 특정국가 또는 특정단체에 의한 지속적・누적형 사이버 테러리즘에 대하여 국제 합의 기준을 마련하여 강력한 정치・경제・군사적 제재가 이루어진다면, 처벌적 억지 관점(deterrence by punishment)에서 예방적 대응이 이루어질 수 있다고 여겨진다. 또한, 북한과 같이 국가와 국가간 사이버 분쟁뿐만 아니라 IS(Islamic State)에 의해 이루어지는 비국가행위자에 의한 사이버 위협과 사이버 무력분쟁과 관련한 무력대응에 대한 관련 사항들에 대한 국제적 합의 도출과 의견교환이 필요하다. 사이버 공격, 사이버 위협, 사이버 무력분쟁은 기본적으로 국가를 표방하지 않고 있고, 상황에 의해 또는 증적에 의해 국가에 의한 행위라는 것을 인식하는 경우에도, 실질적으로 대응하는 데에는 여러 문제가 있기 때문이다.

## References


Alex, S. Wilner. 2010. Targeted Killing in Afghanistan: Measuring Corecion and Deterrence in Counterterrorism and Counterinsurgency. *Studies in Conflict and Terrorism.* 33(4): 307-329.

Alexander, L. George, 2003. The Need for Influence Theory and Actor-Specific Behavioral Models of Adversaries. *Comparative Strategy.* 22(5): 465-477.

Amir, Lupovici. 2010. The Emerging Fourth Wave of Deterrence Theory: Toward a New Research Agenda. *International Studies Quarterly.* 54(1): 705-732.

Beeker, Kevin R., Rober F. Mills, Michae R. Grimaila, and Michael W. Haas. 2013. Operationally Responsive Cyberspace: a Critical Piece in the Strategic Deterrence Equation. In Adam Lowther, (ed.). *Thinking about Deterrence Enduring Questions in a Time of Rising Powers.* Rogue Regimes, and Terrorism, Maxwell AFB, Ala.: Air University Press.

Bendiek, Annegret and Metzger Tobias. 2015. Deterrence Theory in the Cyber-century: Lessons from a Sate-of-the-art Literature Review. Lecture Notes in Informatics (LNI).


11) 사건이나 효과가 누적될 수 있다는 '사건의 누적'(accumulation of events) 또는 'Nadelstichtaktik'이론은 사이버 조작이 동일한 공격자 또는 제휴하여 행동하는 공격자들에 의하여 수행되고, 목적에 관련성이 있고, 규모와 효과의 기준을 충족하는 경우에 무력공격의 기준을 충족하기 위하여 동사이버 조작의 효과가 결합될 수 있다는 것이다. 이 이론은 미국과 이스라엘 등이' 치고 빠지는'(hit and run)방식의 테러범에 대하여 행사하는 압박적 조치를 정당화한다.이 이론이 사이버 테러리즘에 적용되어야 할 필요성은 악의적인 데이터 흐름(data-streams)이 의도적으로 매우 천천히 또한 작게 분산되어 보내지면, 목표 컴퓨터 시스템의 안전센서가 이를 배경 잡음(background noise)으로 인식하여 위험하지 않다고 분류하기 때문이다. 예컨대, 핵심기반시설의 기능불량은 사소한 침해(nuisance)라고 간주되지만, 다른 핵심기반시설들의 기능불량이 누적되면 무력사용에 해당한다고 평가할 수 있어야 한다는 것이다(Lee & Lee, 2015: 328; Park & Jung, 2014: 85-86; Feder, 1987: 415).

*Gesellschaft für Informatik*. 553-570.

Bracken, Paul. 2012. *The Second Nuclear Age: Strategy, Danger, and the New Power Politics*. New York: Times Books.

Bruce, Jentleson and Christopher Whytock. 2015. Who "Won" Lybia? The Force Diplomacy Debate and Its Implications for Theory and Politics. *International Security*. 30(3): 51-75.

Buzan, Barry. 1991. *People, States & Fear: An Agenda for International Security Studies in the Post-Cold War Era*. London: Harvester Wheatsheaf.

Choi, June Sung, Kwang Ho Kook, Moon Jeong Choi, and Young Sub Yang. 2014. Limitation of Armed Response to Cyber Armed Conflict. *Journal of Security Engineering*. 11(5): 387-398.

Defense Science Board. 2013. *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

Department of Defense. 2011. *Department of Defense Cyberspace Policy Report*. A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011. Section 934.

Department of Defense. 2013. *Air-Sea Battle: Service Collaboration to Address Anti-Access and Area Denial*. Washington, D.C.: Department of Defense.

Freedman, Lawrence. 2004. *Deterrence*. London; Polity.

Gompert, David C. 2013. *Sea Power and American Interests in the Western Pacific*. Santa Monica, Calif.: RAND Corporation.

Goodman, Will. 2010. Cyber Deterrence: Tougher in Theory Than in Practice, *Strategic Studies Quarterly*. Fall: 102-134.

Harvard University Program on Humanitarian Policy and Conflict Research. 2009. *Manual on International Law Applicable to Air and Missile Warfare*. Harvard University Press.

Iasiello Emilio. 2014. Is Cyber Deterrence an Illusory Course of Action?. *Journal of Strategic Security*. 7(1): 54-67.

Joo, Seong Bhin. 2012. A Study on Cyber Security System in South Korea. *Korean Journal of Criminal Justice*. 2(1): 137-174.

Joo, Seong Bhin. 2015. A Study on Procedure of Criminal Cases Related to the Security. *Korean Security Science Review*. 43: 231-257.

Jun, Sung Hun. 2012. Review of United States Nuclear Umbrella Policy Toward North Korea. Korea Institute for National Unification. *KINU Series 12-01*.

Khalilzad, Zalmay. 1999. Defense in a Wired World: Protection, Deterrence, and Prevention. In Zalmay Khalilzad and John P. White(eds.). *Strategic Appraisal: the Changing Role of Information in Warfare*. Santa Monica CA: RAND.

Kim, In Soo and KMARMA. 2015. North Korea's Cyber Warfare Capabilities: Assessment and Prospects. *Korea Institute for National Unification*. 24(1): 117-148.

Knopf, Jeffrey W. 2010. The Fourth Wave in Deterrence Research. *Contemporary Security Policy*. 31(1): 1–33.

Ko, Kyung Yun. 2014. The 4th Wave of Deterrence Theory And Counterterrorism Policy: Focus on the China`s Counterterrorism Policy. *Journal of Korea Air Force Academy*. 65: 209-239.

Lebow, Richard Ned and Stein, Janice Gross. 1994. *We All Lost the Cold War*. Princeton, NJ: Princeton University Press.

Lee, Dae Sung. 2005. A Study on the Necessity for the Anti-Terrorism Act. *The Korean Association of Police Science Review*. 9: 105-134.

Lee, Dae Sung. 2008. A Constitutional Study on Trends Analysis and its Response of International Terrorism Occurred in South Korea. *World Constitutional Law Review*. 14(3): 263-288.

Lee, Jeong Seo and Soo Jin Lee. 2015. Defense Cyber Warfare Development Direction Based on the International Legal Review of the NK's Cyber Attacks. *Journal of Security Engineering*. 12(4): 319-336.

Lee, Sang Ho. 2015. Reinforcement of the Future Cyberwar Potential of the Korean Military: A Focus on Navy's Cyber Warfare Capability Building. *National Intelligence Review*. 7(2): 117-151.

Lee, Sang Hyun. 2013. Planning Papers: U・S・Extended Deterrence Policy in the Asia-Pacific and Its Implications for South Korea`s Security. *Journal of National Defense Studies*. 56(2): 1-22.

Lee, Sung Hun. 2015. Enhancing Effectiveness of Deterrence Strategies against North Korea Provocation. *National Strategy*. 21(3): 125-160.

Lee, Won Woo. 2012 The Subdivision and Application of Security Cooperation Concepts: Implications for Security Studies and

Policy. *Korean Journal of International Relations*. 51(1): 33-62.

Louise, Doswald Beck. 2005. *International Institute of Humanitarian Law, San Remo Manual on International Law Applicable to Armed Conflict at Sea*. Cambridge University Press.

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

Michael, N. Schmitt. 2013. *The Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press.

Min, Byoung Won. 2015. Cyberattacks and Cyberdeterrence: Focused on Means of the International Politics and New Paradigms. *Jeju Forum for Peace & Prosperity*. 172: 1-20.

Morgan, Patrick M. 1983. *Deterrence: A Conceptual Analysis*. Beverly Hills, CA: Sage Publications.

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

Nevill, Liam and Hawkins Zoe. 2016. Deterrence in Cyberspace: Different Domain, Different Rules. *SPECIAL REPORT(ISSN 2200-6648)*. Australian Strategic Policy Institute. 1-28.

Nye, Joseph S. 2011. Nuclear Lessons for Cyber Security?. *Strategic Studies Quarterly*. 5(4): 18-38.

Park, No Hyoung and Myung Hyun Chung. 2014. Basic Concepts of Cyber Warfare in International Law: Focusing on the Tallinn Manual. *The Korean Journal International Law*. 59(2): 65-93.

Paul, K. Davis. 2014. Deterrence, Influence, Cyber Attack, and Cyberwar. *RAND National Security Research Division*. 1-26.

The White House. 2010. *National Security Strategy of the United States*. Washington D.C.: White House.

Ullman, Richard H. 1983. Redefining Security. *International Security*. 8(1): 129-153.

Van der Putten, Frans-Paul, Meijnders Minke, and Rood Jan. 2015. *Deterrence as a Security Concept against Non-traditional Threats*. Netherlands Institute of International Relations Clingendael.

Walt, Stephen M. 1991. The Renaissance of Security Studies. *International Studies Quarterly*. 35(2): 211-239.

Wenger, Andreas and Alex Wilner. 2012. *Deterring Terrorism: Theory and Practice*. Stanford Security Studies.

William, J. Lynn, III. 2010. *Deputy Secretary of Defense, Remarks at STRATCOM Cyber Symposium*. Omaha, Nebraska.

Wyn, Q. Bowen. 2004. Deterrence and Asymmetry: Non-State Actors and Mass Casualty Terrorism. *Contemporary Security Policy*. 25(1): 58-67.

川口 貴久. 2014. グローバル・コモンズ（サイバー空間、宇宙、北極海）における日米同盟の新しい課題. The Japan Institute of International Affairs. 平成25年度外務省外交・安全保障調査研究事業（調査研究事業). 1-98.

## *Korean References Translated from the English*

고경윤. 2014. 제4세대 억지이론과 대테러정책: 중국의 대테러 정책을 중심으로. 공사논문집. 65: 209-239.

김인수, KMARMA. 2015. 북한 사이버전 수행능력의 평가와 전망. 통일정책연구. 24(1): 117-148.

민병원. 2015. 사이버공격과 사이버억지: 국제정치적 의미와 대안적 패러다임의 모색. Jpi정책포럼. 172: 1-20.

박노형, 정명현. 2014. 사이버전의 국제법적 분석을 위한 기본 개념의 연구. 국제법학회논집. 59(2): 65-93.

윤해성, 주성빈 외. 2014. 해외 안보형사특례 법제도 분석을 통한 국내 법제 개선방안에 관한 연구. 한국형사정책연구원.

이대성. 2008. 테러범죄의 동향분석과 대응방안에 관한 헌법적 연구. 세계헌법연구. 14(3): 263-288.

이대성. 2005. 테러방지법의 필요성에 관한 연구. 한국경찰학회보. 9: 105-134.

이상현. 2013. 미국의 아태 확장억지 정책과 한국 안보. 국방연구. 56(2): 1-22.

이상호. 2015. 한국군 미래 사이버전 능력 강화 방안 연구: 해군 사이버전력 건설을 중심으로. 국가정보연구. 7(2): 117-151.

이성훈. 2015. 대북 억제전략의 효과성 제고 방안에 관한 연구: 新억제전략의 3요소를 중심으로. 국가전략. 21(3): 125-160.

이원우. 2011. 안보협력 개념들의 의미 분화와 적용: 안보연구와 정책에 주는 함의. 국제정치논총. 51(1): 33-62.

이정석, 이수진. 2015. 북한 사이버공격에 대한 국제법적 검토

를 바탕으로 한 국방 사이버전 수행 발전방향. 보안공학연구논문지. 12(4): 319-336.

전성훈. 2012. 미국의 對韓 핵우산정책에 관한 연구. 통일연구원. KINU 연구총서 12-01.

주성빈. 2012. 우리나라 사이버안보 대응전략의 문제점 및 발전방안. 형사사법연구. 2(1): 137-174.

최준성, 국광호, 최문정, 양영섭. 2014. 사이버 무력분쟁에서 무력대응의 한계. 보안공학연구논문지. 11(5): 387-398.

Received: Sep. 7, 2016 / Revised: Sep. 13, 2016 / Accepted: Sep. 19, 2016

# 사이버 테러리즘에 대한 억지력 모색

국문초록 최근에 많은 연구자들은 새로운 사이버 위협들로부터 억지 전략을 강구하고 있다. 우리나라와 동맹관계를 유지하고 있거나 지리적 접근성을 보이는 국가들이 사이버 테러리즘을 바라보는 시각은 과거와 같이 테러집단에 의한 테러리즘 발생 가능성과 주도권을 사전에 인정하고, 이에 대응하기 위한 방안으로 예비·음모 처벌 논의, 범죄 발생 전(前) 증거수집과 관련된 쟁점사항들을 논의하는 것에 그치는 것이 아니라 사이버 공간에서 공격원을 특정하여 보복이나 처벌을 위한 억지 메커니즘(처벌적 억지력)을 모색하고 있다. 우리나라도 사이버 테러리즘에 대한 수동적인 대응방법에서 벗어나 국제 정세를 고려한 적극적 억제 전략을 모색해야 한다. 사이버 테러리즘에 대응하기 위한 적극적인 접근방법에는 크게 두 가지로 구분될 수 있다. 하나는 상대의 이익을 부인하는 거부적 억지이고, 다른 하나는 상대에게 비용을 부과하는 처벌적 억지이다. 따라서 우리는 사이버 테러리즘을 대응함에 있어 소극적 태도에서 벗어나 현실적으로나 시기적으로 적절하고 효과적인 정책을 마련해야 한다.

주제어 : 사이버 공격, 4세대 억지이론, 적극적 방어, 거부적 억지력, 처벌적 억지력

Profiles **Dae Sung Lee** : He received his Ph.D. from Dongguk University. He is a associate professor of the Department of Police Administration at Dong Eui University, in which he has taught since 2009. His research interests include terrorism, security, north-south relations and international situation. He has published 63 articles in journals since 2015(dorian3145@deu.ac.kr).
**Seong Bhin Joo** : He received his Ph.D. from Dongguk University. He is a assistant professor of the Department of Fire Service Administration at Dong Eui University, in which he has taught since 2015. His research interests include security, safety and social policy. He has published 19 articles in journals since 2015(tjdqlswn@deu.ac.kr).