JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 20, No. 9, pp. 1809-1815, Sep. 2019

적대적인 사이버활동에 대한 판단기준 발전방안

김 광 제[1] · 최 영 동[2] · 한 경 석[3]
[1,2]숭실대학교 일반대학원 IT정책경영학과
[3]숭실대학교 일반대학원 경영학부 교수

Evolution of judging criteria for hostile cyber activities

Kwangje Kim[1] · Youngdong Choi[2] · Kyeong Seok Han[3]
[1,2]Department of IT Policy Management, Soongsil University, Seoul 06978, Korea
[3]Department of Business Administration, Soongsil University, Seoul 06978, Korea

[요 약]

2010년 11월 미얀마에서 DoS공격 발생, 2014년 12월 소니픽처스에 대한 사이버공격이 발생하였으며, 2017년 5월 12일 유럽과 아시아를 비롯한 약 100개국에서는 사상 최대의 사이버 공격이 발생해 일부 정부 기관과 병원, 기업의 업무가 마비되거나 차질을 빚는 등 전 세계가 혼란에 빠졌다. 이와 같이 사이버공간은 판도라의 상자처럼 열려졌고, 이 공간의 악용을 막는 것이 모든 국가의 당면한 과제가 되었으며, 그 방법과 절차에 대해 국제적 논의가 진행되고 있다. 이에 따라 사이버공간에 대한 특징과 규범 정립을 위한 국제적인 노력에 대해 고찰해 보았다. 또한, 사이버공간에서의 적대적인 사이버활동에 대한 판단을 위한 탈린매뉴얼과, 효과기반 스펙트럼 등의 적용방법에 대해 분석하였다. 이를 바탕으로 증가되는 사이버위협에 대응하기 위해 적대적인 사이버 활동에 대한 판단기준과 대응시스템을 어떻게 구축할 것인가에 대한 발전방안을 제시하였다.

[Abstract]

In November 2010, there was a DoS attack in Myanmar, in December 2014 there was cyber attack on Sony Pictures. On May 12th, 2017, the biggest cyber attack occurred in 100 countries including Europe and Asia, And the work of hospitals and corporations became paralyzed or disrupted and the whole world was in chaos. In this way, cyber space has been opened like a box of Pandora, and the prevention of exploitation of this space has become an urgent task for all nations, and international discussions on the method and procedure are under way. As a result, I have examined the international efforts to establish the characteristics and norms of cyber space. In addition, Tallinn manual for judging hostile cyber activities.

색인어 : 사이버공간, 적대의도, 탈린매뉴얼, 사이버규범, 사이버공격

Key word : Cyberspace, Hostile intent, Tallinn manual, Cyber norm, Cyber attack

http://dx.doi.org/10.9728/dcs.2019.20.9.1809

Received 20 August 2019; **Revised** 16 September 2019
Accepted 20 September 2019

***Corresponding Author;** Kyeong Seok Han

Tel: +82-2-820-0585
E-mail: kshan@ssu.ac.kr

Ⅰ. 서 론

인류가 탄생한 이후 인간이 활동할 수 있는 영역은 땅과 바다뿐이었지만, 정보통신 기술발달에 따라 사이버공간이라는 영역이 추가되었다. 우리는 이제 금융, 산업, 방송, 교육, 국방 등의 모든 서비스와 업무를 사이버공간을 통해 수행하고 있다. 주요 사이버공격 사례로 국외는 1991년 미국의 걸프전, 2007년 에스토니아에 대한 러시아의 공범위한 사이버공격, 2008년 그루지아전쟁, 2010년 이란 핵시설에 대한 스턱스넷 공격[1] 등이 있고, 국내는 2003년 인터넷 마비사태, 2009년과 2011년 DDoS 공격, 2013년 320, 625사이버테러, 2016년 8월 초유의 군 인터넷망, 국방망 해킹 등의 사례가 있었다. 사이버공간에서 자행되는 해킹을 비롯한 불법적인 행위가 원자력발전소, 국가전력공급체계, 통신체계와 군 방어시스템 등 국가안보에 심각한 영향을 끼칠 수 있는 국가주요기반시설을 공격한다면 그 피해는 상상하기 어려울 것이다. 이과 같이 점증하는 국내외 사이버공격에 대해 사이버공간상에서 어떻게 규율할 수 있는가와 관련한 논의가 국제적으로 계속 진행되고 있지만, 아직 국제적인 규범으로 정의된 것이 없다. 따라서, 지금까지 연구된 사이버공간상의 활동에 대해 어떻게 판단기준을 설정하고 대응을 하는지 분석해 보고, 발전방안을 제시하는 것이 필요하다.

Ⅱ. 기존연구 분석

2-1 사이버공간의 특징과 규범정립 노력

사이버공간은 공간과 시간개념이 없는 상태에서 자신의 신분을 감추거나 드러내지 않는 익명성과 실시간 정보유통이 가능한 쌍방향성, 지역의 한계를 벗어나 동시에 넓고 신속하게 모두와 소통할 수 있는 시공간적 무제한성과 동시성, 그리고 정보유통의 다양성 등의 특징이 있다[2]. 다른 측면으로는 사이버공간은 인간과 조직이 필요한 기술을 이용해서 활동하고 효과를 내는 공간이고, 이를 활용하기 위해서는 전자기적 기술을 사용하는 것이며, 이 수단을 통해 정보를 생성하고, 저장하고, 수정하고, 교환하고, 이용하는 것이다. 또한, 상호의존적인 네트워크로 연결되어 있기 때문에 그 중요성과 영향력이 큰 것이다[3].

사이버공격에 대한 정의로 미국정부 보안전문가인 R. Clarke는 “사이버전쟁이란 다른 국가에게 피해를 주거나 혼란을 야기할 목적으로 그 국가의 컴퓨터 또는 네트워크에 침투하는 국가의 행동”이라 했으며 사이버공격 행위는 해킹, 파괴, 침투, 감염 등의 수단으로 이루어지며, 그러한 행위가 사이버공격이 되기 위해서는 컴퓨터 네트워크의 기능을 저하시키거나 교란하려는 의도를 가지고 있어야 한다[4].

사이버공간에서의 공격행동을 보면 사이버범죄, 사이버테러, 사이버전으로 크게 구분할 수 있다. 사이버범죄는 개인 혹은 조직화된 단체가 사이버공간에서 시간과 장소에 관계없이 개인과 단체들에 대하여 정치적 특성을 내포하지 않고 경제적 이익과 관련된 행위 또는 반사회 문화적 행위를 범하는 경우라고 하고, 사이버테러는 특수한 목적을 가진 개인, 테러집단이 컴퓨터 시스템 운영방해, 침해행위 또는 전자적 침해행위를 통해서 사회혼란을 야기하거나 국가안보를 침해, 위협하는 행위라 정의한다. 사이버전은 특정국가가 다른국가의 컴퓨터나 네트워크를 공격하여 피해를 입히거나 파괴할 목적으로 취하는 행동으로 정의 한다[2].

우리는 북한으로부터 계속적인 사이버공격을 받고 있다. 북한의 공격에 대응하기 위해서는 남북한 사이버환경과 수행능력에 대한 정확한 평가를 하여야 하는데, 호주전략정책연구원(ASPI : Australian Strategic Policy Institute)이 발표한 보고서에 따르면 남북한 사이버성숙도 지표는 남한이 75.5, 북한이 20.7로 나타난다[5]. 우리의 입장에서 보면 이러한 사이버환경의 차이가 사이버공간에서의 취약점을 증가시키고 있으며, 대응하기 위해서는 많은 노력이 필요하다.

2-2 규범정립을 위한 국제적 노력

사이버공간에서의 공격이 단순범죄를 넘어 국가안보에 직접적인 영향을 미치고 있는 상황에서 국제적 규범 마련을 위해 다양하게 논의가 되고 있다. 첫째는 UN를 중심으로 한 UN정부전문가그룹(Group of Government Experts : 이하 UNGGE)과 비서구국가들을 중심으로 한 상하이협력기구(Shanghai Cooperation Organization : 이하 SCO)와 같은 순수 정부 간 논의로 안보문제에 있어 국가들은 자국의 이익을 극대화 할 수 있는 방향으로 규범형성을 유도하며 경쟁하고 있다. 둘째는 사이버스페이스총회 등과 같은 다중 이해당사자가 참여한 논의로 사이버공간에 대한 논의를 전통적인 행위자인 국가에게만 맡겨두는 것이 아니라, 비정부기구, 전문가와 기술자 등 다양한 행위자들과의 논의를 통해 규범을 형성하고자 하는 시도이다. 셋째는 탈린매뉴얼과 같은 국제법학계의 논의가 있다. 사이버공간에 대한 국제적 핵심 논란은 인터넷 자유와 사이버안보의 적절한 균형을 어떻게 설정할 것인지에 집중되고 있다[6].

사이버안보의 국제규범과 관련한 논란은 크게 2가지이다. 첫째, “정보통신기술 발전이 국가안보와 국가에 어떤 영향을 미치는가?, 특히 국가들이 정보통신기술을 군사 및 국가안보에 적용하는 것을 어느 수준까지 용인 또는 규제해야 하는가?”이고, 둘째, “정보컨텐츠와 정보인프라가 국경을 넘나드는데 이러한 정보컨텐츠가 국가안보의 문제로서 규제되어야 하는가?”이다. 이에 대해 서방국가는 현존 국제법을 중심으로 규범이 형성되어야 하고, 새로운 규제와 개입이 불필요하다는 입장이며, 중국과 러시아를 중심으로 한 비서구 국가들은 국가중심의 규제 및 개입이 필요하다는 주장을 하고 있다.

2-3 적대적인 의도에 대한 판단 접근방식

유엔헌장 2조 4항에 "모든 회원국은 자신들의 국제관계에서 유엔의 목적과 부합하지 않는 방법으로 다른 국가의 영토보전이나 정치적 독립에 대한 위협 또는 무력의 사용을 삼가야 한다."고 명시되어 있다. 사이버공간에서는 물리적인 힘이 아닌 데이터 표시의 추상적인 영역에서 발생하기 때문에, 사이버공간에서의 적대행위를 다룰 때는 어려움이 있다. 하지만, 사이버공간에서의 행위가 반드시 금지된 무력의 사용이 아니다. [그림 1]은 Level of Conflict와 Level of Combat의 관계를 보여주는 분쟁 스펙트럼이다.

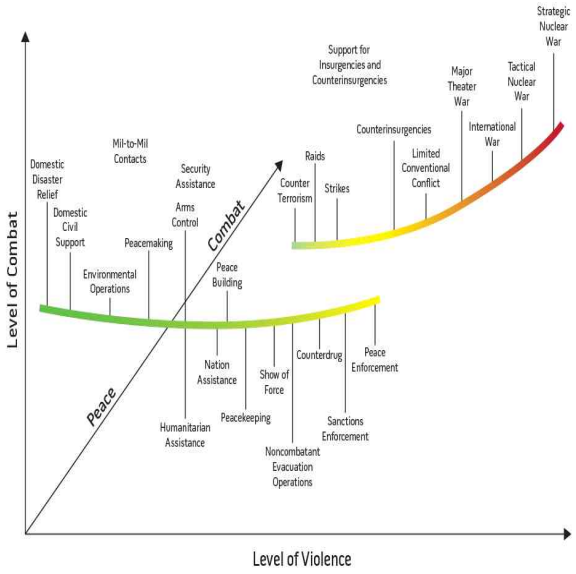

그림 1. 분쟁 스펙트럼
Fig. 1. Spectrum of Conflict

사이버공간에서 국제법상의 무력에 대한 관점이 다양하게 있다. 첫째, 효과기반의 접근방식으로 일정강도 이상의 피해를 발생시키는 사이버작전이 있을 때 이것이 사이버공간에서의 무력이라는 관점이고, 둘째, 물리적 동등성으로 사이버공간 내 행위가 물리적 공격으로 동일하게 달성 될 수 있는 경우 이를 무력사용이라 정의하는 것이며, 셋째, 표적기반의 틀로 국가 중요시설에 대한 사이버공격이 무력이라는 관점이다. 그러나, 이러한 기준도 국가별 전략적 이해에 따라 해석이 달라질 수 있다는 문제가 있다.

2-4 적대의도 판단을 위한 주요 요소

탈린매뉴얼 2.0에서 "(규칙 32) 국가에 의한 평시의 사이버 첩보활동은 그 자체로 국제법을 위반하지 않으나, 그것이 수행되는 방법은 그러할 수 있다."고 했다. 하지만, 사이버공간에서의 첩보활동과 공격적 사이버작전은 구분이 어려운 것이 특징이다. 이는 노출된 시스템을 통한 접속으로 첩보활동을 하다가도, 시스템의 기능저하, 방해, 파괴 등의 추가적인 공격이 가능하기 때문이다. "(규칙 69) 사이버활동을 통해 그 규모와 효과가 무력사용의 수준에 이르는 비사이버작업에 상응할 때 무력사용을 구성한다."고 한 것처럼, 사이버활동이 무력사용 가능성이 있는가를 판단하는 것이 중요하다.

탈린매뉴얼에서는 무력사용 여부를 판단하기 위해 8개의 구성요소를 제시하였다. ① 가혹성 : 최소허용규칙을 조건으로 물리적 위해를 수반하는 결과로 피해의 범위, 지속시간, 강도가 중요한 요소이다. ② 즉시성 : 무장공격에 의한 피해는 즉시 발생하는 반면 다른 형태의 강압은 더 천천히 진행되며, 결과가 빨리 발현될수록 해로운 결과를 방지할 기회가 적다. ③ 직접성 : 사이버공격이 결과와 더 직접적으로 연결 될수록 무력사용으로 간주될 가능성이 높다. ④ 침략성 : 사이버작전이 국가 영토보전이나 주권을 더 많이 침해할수록 무력사용으로 간주될 가능성이 높다. ⑤ 효과의 측정가능성 : 무력공격의 결과처럼 결과가 쉽게 식별되고 객관적으로 정량화 될수록 사이버작전이 무력으로 간주될 가능성이 높다. ⑥ 군사적 성격 : 행위자와 표적이 군과 관련이 깊을수록 무력으로 간주된다. ⑦ 국가관여도 : 국가와 사이버활동 간의 연계성이 크면 무력으로 간주된다. ⑧ 합법성 추정 : 자기방어의 범위를 벗어나는 부적절한 대응을 하였을 때 무력으로 판단될 수 있다.

이는 Schmitt가 기존에 제시한 7개의 구성요소에 군사적 성격이 추가되는 형태로 탈린매뉴얼 2.0에 반영되어 있다[7]. 적대의도 분석은 탈린매뉴얼 2.0에 제시된 구성요소 8개를 이용하여 분석할 수 있다. 먼저, 사이버공간에서 발생되는 일반적이고 광범위한 다수의 행위에 대해 목록을 작성하고, 각 목록에 대한 정성적 분석을 통해 무력사용효과와 흡사한지에 대해 요소별로 평가가 가능하다.

[표 1]은 Schmitt가 제시한 요소별로 무력사용에 근접하였는지를 분석한 예이다. 표에서 숫자 1은 물리적 효과가 떨어지고, 10은 물리적 효과와 동일함을 의미한다. 이렇게 집계된 정보로 어떠한 행위가 더 적대의도를 가지고 있는지 합리적으로 판단할 수 있다.

표 1. Schmitt의 분석 예시[8]
Table 1. Example of Completed Schmitt Analysis[8]

Cyber action	Severity	Immediacy	Directness	Invasiveness	Measurability	Presumptive Legitimacy	Responsibility
Ping map	1	1	5	7	7	1	3
Probe	2	1	5	7	7	2	3
Implant malware	3	4	5	7	7	3	3
Erase logs	5	5	5	8	7	6	4
Email fishing	4	4	5	5	5	5	5
Access networks	4	5	6	8	5	6	5
Access email	4	5	6	8	5	6	5
Steal data	6	6	6	9	8	6	6
Change or delete data	7	6	6	9	8	8	6
Distributed denial-of-service attack (DDoS)	7	7	7	9	8	8	7
Email bomb	7	5	6	7	7	6	5
Influence operations in social media	6	7	6	6	7	5	7
Disable critical infrastructure	9	8	8	9	8	8	8
Damage critical infrastructure	9	9	8	9	8	8	8
Attack financial industry	8	9	8	9	8	8	8
Military command and control attack	9	9	9	9	9	9	9

2-5 사이버공간에서의 효과기반 스펙트럼

Gary Brown과 Owen Tullos는 사이버공간상에 행위를 효과기반으로 사이버 활동에 대한 스펙트럼을 제시하였다. 그들은 사이버 행동을 3가지 기본 범주로 나누었다. 스펙트럼의 맨 왼쪽은 단순한 첩보행위로, 이러한 사이버첩보행위의 특징은, 첫째는 사이버공간상의 정보를 대상으로 하고, 둘째는 비인가적 접근을 통해서 이루어지며, 셋째는 단순한 경제적 이득을 넘어선 동기에 의해 수행이 된다.

스펙트럼 중간은 사이버방해로 물리적 손상이나 부상은 일으키지 않으나, 정보흐름이나 정보시스템의 기능을 물리적 손상이나 상해 없이 중단시키는 행위까지를 포함하고 있다. 이러한 사이버방해 효과가 크면 녹색에서 빨간색으로 스펙트럼을 따라서 이동하게 되는 것이다. 탈린매뉴얼 2.0의 규칙66에서는 국가에 의한 간섭을 "국가는 타국의 대내적 또는 대외적 문제에, 사이버 수단에 의한 것을 비롯해 간섭할 수 없다."라고 명시하였다. 따라서, 우리가 불간섭의 원칙을 위반하여 적대적인 의도를 가지고 있는지 판단할 수 있는 고려요소로 "첫째는 사이버활동이 정부의 웹사이트나 컴퓨터 시스템에 직접적으로 영향을 주었는가?, 둘째는 국가나 상당수의 국민들이 심각성을 알 수 있도록 활동하였는가?, 셋째는 정부가 영향을 받은 집단에 대해 공개적으로 지지를 표명하고, 해당 국가가 악영향을 받았는가? 넷째는 측정 가능한 방식으로 국가안보에 악영향을 미칠 가능성이 있는가?"로 불간섭 원칙의 위반을 판단하고 적대적 의도를 파악할 수 있다.

스펙트럼의 맨 오른쪽 끝은 사이버공격으로, 여기서 재산상의 손상과 파괴, 사망과 상해 등의 상황이 발생한다. 사이버공격에 공격의도를 추론하기 해서는 주체를 개인과 국가로 구분하여 주체가 개인이라면 개인이 가지고 있는 신념과 욕구에 영향을 주려 할 것이며, 공격주체가 국가라면 국가안보차원에서 정치, 경제, 군사적인 요소에 영향을 줄 것이다.

사이버공격을 의도에 따라 공격주체를 추론하면 공격에 대응하기 위한 전략수립도 효과적이다. 공격의 다양한 의도를 비교하기 위해서는 목적에 도달하기 위해 가장 합리적인 방법을 선택한다는 가설을 선정하고 영향력 비교를 통해 최선의 선택을 하면 된다[9].

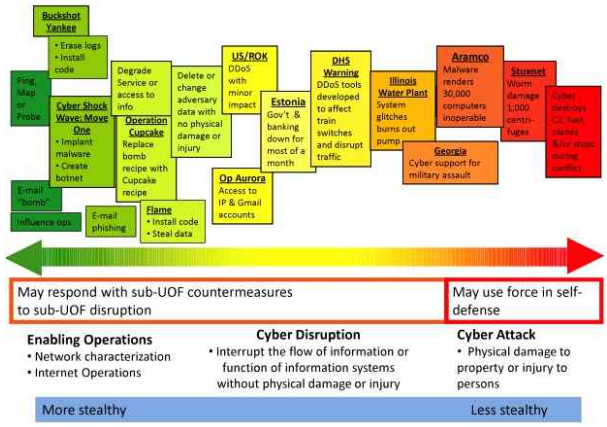

그림 2. 사이버작전의 스펙트럼[10]
Fig. 2. On the Spectrum of Cyberspace Operations[10]

Ⅲ. 제안방안

위에서 살펴본 탈린매뉴얼 2.0의 구성요소에 의한 분석의 틀과 Gary Brown과 Owen Tullos의 사이버 공간상에 행위를 효과기반의 틀로 분석하는 것이 다양한 사이버 행위에 대한 적절한 대응범위를 결정하는 것을 돕는 유연한 도구가 될 수 있다. 탈린매뉴얼은 전략적 차원에서 판단에 유용하고, 효과기반 스펙트럼은 전술적 수준에서의 판단에 유용할 것이다. 하지만, 위의 2가지 틀로만 사이버공간에서의 적대의도를 판단하고 대응하기에는 한계가 있다.

따라서, 사이버공간에서의 적대의도를 판단하고 대응하기 위해서는 적대적 사이버활동에 대해 물리적 피해와 인명 피해의 규모와 효과에 대한 분석과, 무력공격에 준하는 행위로 임박한 것인지 또는 우리가 방어할 시간과 능력이 있는지를 판단하며, 개인·조직·국가 피해대상별 분석을 통해 대응방법을 결정하여야 한다. 자위권 차원의 무력사용을 할 것인지, 비무력적인 방법으로 적극적 대응을 할 것인지, 방어체계를 보완하고 피해복구 노력을 할 것인지에 대한 판단을 위한 사이버활동이 식별되었을 때의 대응 알고리즘을 [그림 3]과 같이 제안한다.

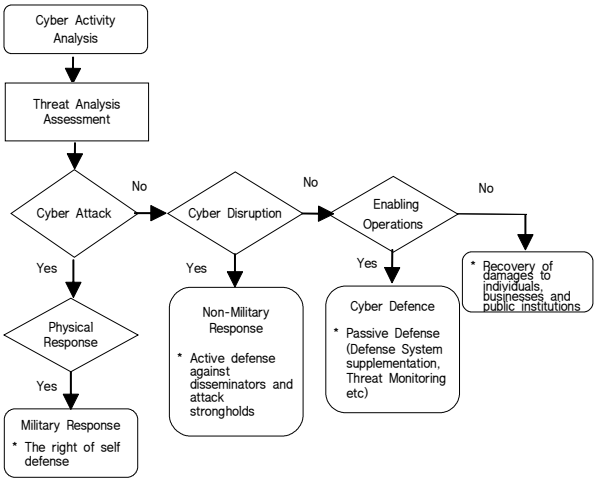

그림 3. 적대적 사이버활동 대응 알고리즘
Fig. 3. Hostile Cyber Activity Response Algorithm

여기서 사이버 교란(Cyber Disruption) 상황에서 적극적 방어의 개념은 원래 적의 위협이 아군 지역에 도달하기 전에 이를 제거하여 부대의 전투력을 보존하는 전략을 뜻하는 군사용어로 적의 미사일 발사 징후 포착 시 위협의 근원지를 선제 타격하는 활동을 포함한다. 사이버 공간에서의 적극적 방어는 외부 네트워크에서 악의적 트래픽이 탐지된 단계에서도 추적을 통해 봇넷에 침투하여 조치를 취하거나 봇넷 조사를 통해 C&C서버에 침투하여 역해킹을 시도하는 등의 조치를 취하는 것을 말한다.

대응 알고리즘에서 사이버활동에 대한 위협수준 평가를 위한 위협 분석 평가(Threat Analysis Assessment)가 중요한데 Schmmit 분석을 참고하여 [표 2]와 같이 항목별 위협수준을 제시하였다.

평가항목을 제시함에 있어서 퍼지추론의 방식을 이용하였다. 퍼지 추론이란 몇 개의 모호함이 포함된 언어적 명제로부터 하나의 다른 근사적 명제를 도출하는 추론 방식이다[11]. 세로축의 공격대상(Target)은 국가기반시설, 공공·기업, 개인으로 구분하였고, 즉시성(Immediateness)은 피해효과가 언제 나타나는가에 따라 시간적으로 긴급대응이 필요한 것은 H(High), 일반적 대응은 N(Normal), 낮을 시는 L(Low)로 구분하였다.

피해(Damage)는 피해강도를 말하여 강도가 높을 시 H(High), 일반적은 N(Normal), 낮을 시는 L(Low)로 구분한다. 국가지원 해커는 S(State Sponsored), 범죄그룹은 C(Crime Group), 비악의적 행위자는 K(Script Kids)로 표현하였다. 위협수준을 나타내는 언어적 변수는 매우 심각(A)은 0.9, 심각(B)은 0.7, 보통(C)은 0.5, 낮음(D)은 0.3, 매우 낮음(E)은 0.1로 정의할 수 있다. 예를 들어 범죄집단(C)이 피싱 이메일과 같은 방법으로 개인에 대한 랜섬웨어를 유포 시 피해규모가 크지 않고, 즉시대응이 필요성이 낮다면 언어적으로는 D로 정량적 수치는 0.3으로 표현할 수 있으며 이에 대한 대응은 알고리즘에 따라 피해복구 등의 활동을 하면 될 것이다.

표 2. 위협수준에 대한 정량적 평가
Table 2. Quantitative Assessment of Threat Levels

Agent / Damage / Immediateness / Target		S (State Sponsored)			C (Crime Group)			K (Script Kids)		
		H	N	L	H	N	L	H	N	L
National Infra-structure	H	A	A	B	A	A	C	B	B	C
	N	A	A	B	B	B	C	C	C	D
	L	B	B	B	C	C	C	D	D	D
Public Institution · Private enterprise	H	A	B	B	B	B	D	D	D	E
	N	A	B	B	B	D	D	E	E	E
	L	B	B	C	D	D	D	E	E	E
Individual	H	B	B	C	C	C	D	D	D	E
	N	C	C	C	C	D	D	E	E	E
	L	C	C	C	D	D	D	E	E	E

Ⅳ. 결 론

사이버공간에서의 적대의도 판단은 실시간으로 발생하는 위협 또는 공격에 대한 대응이 목표이다. 이는 적극적 방어의 개념으로 위협 또는 공격 탐지 시 이를 저지하기 위한 합당한 강도로 공격거점을 대상으로 조치를 취하는 것이다. 그것은 지난 역사에서 전쟁을 통해 얻은 교훈이다

본 연구를 통해 적대적 사이버 활동에 대한 대응 알고리즘과 위협에 대한 정량적 평가 방안을 제시하였다. 이는 상황발생시 대응을 위한 의사결정을 더욱 신속하게 할 것이며, 공통된 위협인식과, 대응수준과 규모에 대한 모호성을 배제시켜 대응을 위한 명확한 기준을 제공하게 될 것이다. 특히, 사이버전과 물리전 연계를 위해 정성적, 정량적 분석기술은 공세적이며 입체적인 대응체계를 구축하는 기반이 될 것이다.

참고문헌

[1]Hayeon Jeong, Cyber Coercion in International Relations : A Study of Cyber Attacks an d Conflicts among States, *The Graduate School Ewha Womans University* (2018), pp.1-2

[2]Dongman Shin, A Study on the North Korea's cyber threat and its i mpact on National Security, *The Graduate School Chosun University* (2016), pp.8-9.

[3]HyunJung Kim, A Study of the International Cooperative Model for Cyber Terrorism. *THE JOURNAL OF INTERNATIONAL RELATIONS* (2016), 19(2), pp.249-282.

[4]Richard Clarke & Robert Knabe, Cyber War : The NextThreat to National Security and What to Do About It, 6(2010). O. Hathaway et al., supra note 16, p.823.

[5] http://www.asaninst.org/contents/, Apr 16 (2015)

[6]Tae-Kyung Ryu, Regulating Cyber Espionage and International Law : The Role of Epistemic Communities and

the Tallinn Manual, *Ewha Womans University*. 2018, pp. 17-20

[7]Foltz, Andrew C. Stuxnet, Schmitt Analysis, and the Cyber Use-of-Force Debate. *NATIONAL DEFENSE UNIV FORT MCNAIR DC,* 2012.

[8]Ramberto A. Torruella, Determining Hostile Intent in Cyberspace, *Joint Force Quarterly* 75, Oct. (2014)

[9]Sang-min Park, Jong-in Lim, Study On Identifying Cyber Attack Classification Through The Analysis of Cyber Attack Intention, *Journal of The Korea Institute of Information Security & Cryptology*(2017), Vol.27, NO.1, p.111

[10]Brown, Gary D., and Owen W. Tullos. "On the Spectrum of Cyberspace Operations." *Journal Article,* Dec 4, (2012).

[11]Do Yongtae, *Artificial intelligence : concept and application*. SciTech Media, 2009.

김광제 (Kwang-Je KIM)

2003년 : 세명대학교 대학원(경영학석사)
2019년 : 숭실대학교 IT정책경영학과(박사과정 수료)

1987～2017 : 공군장교
2017～현재 : 공군사관학교 교수
※관심분야 : 정보보호, 사이버전, 가상현실(VR), 사이버국제법

최영동 (Young-Dong Choi)

2003년 : 공군사관학교(이학사)
2011년 : 美 공군대학원(공학석사)
2019년 : 숭실대학교 IT정책경영학과(박사과정 수료)

2011년～2013년 : 공군 작전정보통신단
2013년～2015년 : 공군 연구분석평가단
2017년～현 재 : 합동참모본부
※관심분야 : 인공지능(AI), 빅데이터(Big Data) 등

한경석 (Kyeong-Seok Han)

1979년 : 서울대학교 문학사
1983년 : 서울대학교 경영학과(경영학 석사)
1989년 : 미국 퍼듀대학교 대학원
(경영정보시스템전공 박사)

1989년～1990년 : 미국 휴스턴대학교 조교수
1993년～현 재 : 숭실대학교 경영학부 경영정보시스템 교수
※관심분야 : ※관심분야 : 경영정보시스템,Digital Economy, Agent-Based Simulation, Web Programming,ERP, C++,회계정보시스템, e-Business, 전자상거래, 중소기업 정보화, 기업자금지원. 정책 연구, ERP 등