Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.1, Feb. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.1.237

사이버공격시 게임이론을 활용한 집단지성간 전략결정 모델 연구 - 한수원 해킹사건을 중심으로 -

박 상 민,† 이 경 호,‡ 임 종 인
고려대학교 정보보호대학원

Strategic Decision Making Model Among Collective Intelligences Using The Game Theory in Cyber Attacks - Case study of KHNP Hacking -

Sang-min Park,† Kyung-ho Lee,‡ Jong-in Lim
Center for Information Security Technologies, Korea University

요 약

최근 다양한 유형의 사이버공격이 발생하였고 공격의 전략적 목적 및 전술적 수단도 진화하고 있다. 특히 한수원 사이버공격은 해킹과 심리전을 결합시킨 핵티비즘형으로 공격자는 국민을 사이버전에 참여시키려 하였고 기밀정보 공개 및 원전중단 협박으로 정부의 의사결정을 지속적으로 강요하였다. 따라서 본 논문에서는 사이버공격시 효과적 전략결정을 도출하기 위하여 개방형 정책결정모델에 공격지성을 포함시키고 게임이론을 활용하여 연구한다.

ABSTRACT

Recently various types of cyber attacks have occurred. The strategic goals & tactical means of these have evolved. Especially KHNP cyber attack was the type of hacktivism combined hack and psychological warfare. The cyber attackers have forecd the nation to participate in the cyber warfare and the government to make strategic decisions to the releases of confidential information and the threats of stopping KHNP. In this paper, we would like to study the effective strategic decision-making model utilizing the game theory and including an attack intelligence on open policy Decision framework.

Keywords: Game Theory, Collective Intelligence, Cyber Attack, Strategic Decision, KHNP

I. 서 론

최근 다양한 유형의 사이버 공격이 발생하고 있고 공격의 목적과 전술도 진화하고 있다. 사이버 공격 목적은 자기과시형에서 금품갈취, 사회혼란, 사이버 테러 등으로 진화하였으며, 사이버 전술도 수동방식에서 은닉, 지능화, 조직화 등 진화하고 있다[28]. 이러한 사이버 공격은 목적에 따라 시스템 장악, 기반시설 마비, 핵티비즘 등 3단계로 분류할 수 있다.

1단계(~'08) 사이버 공격은 개인의 이익과 과시를 추구하는 것이 목적이다. '03년에 발생한 대규모 사이버 공격인 '1.25 인터넷 대란'은 MS사의 윈도우즈 프로그램의 취약점을 활용한 자기과시형 공격이었으며[1], '08년에 발생한 '옥션 해킹사고'는 시스템의 취약한 보안설정으로 1,860만 명의 회원 개인정보가 유출되었다[2].

Received(10. 06. 2015), Modified(11. 24. 2015), Accepted(12. 02. 2015)
† 주저자, 2011572306@korea.ac.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

2단계(~'11) 사이버 공격은 주요 시설을 공격하여 인터넷 기반시설에 대한 불신감을 조성하는 것이 목적이다. '09년에 발생한 '7.7 DDoS 대란' 및 '11년에 발생한 '3.4 DDoS 대란'는 국내·외 주요 공공기관을 대상으로 분산 서비스 거부 공격이 수행되었다[3,4].

3단계(~'15) 사이버 공격은 해킹과 심리전을 결합한 핵티비즘형으로 사회 전반에 불안감을 조성하는 것이 목적이다. '13년 발생한 '320 사이버공격' 및 '625 사이버공격'는 어나니머스를 활용하였으며[5], '14년 '국방과학연구소 군사자료 유출 사건'은 국회의원 및 기자를 활용하였다[6]. 그리고 '14년 '한국수력원자력 정보유출사고'는 블로그와 트위터 등 소셜네트워크를 활용하였다[7].

이처럼 사이버 공격은 개인적인 목적에서 사회 불안감 조성 등의 전략적 수단으로 발전하는 것을 확인할 수 있다[8]. 그리고 사례를 통하여 전략적 효과를 극대화하기 위해 정보 외에 국민을 사이버전에 참여시키려는 다양한 전술을 사용하는 것을 알 수 있다[9].

이에 정부는 컨트롤타워인 국가안보실을 신설[10]하는 등 법령, 제도, 기술, 훈련 등 체계적으로 대비하며 실시간 발생하는 사이버 위협에는 국가사이버안전센타를 통한 사이버위기경보발령, 유관기관을 통한 언론보도 등 사이버 분야의 피해를 예방하고 차단하는데 주력하고 있다.

실제 '한국수력원자력 정보유출사고'는 해킹 후 상황을 1차 기밀문서 유출('14년 12월), 2차 원전중단 협박('14년 12월), 3차 금전요구('15년 3월), 4차 불안감 조성('15년 7월)으로 나눠볼 수 있다[14]. 그리고 정부는 대응과정에서 총 12건의 보도/설명/해설자료를 발표하였으며[12], 공격자는 총 79회의 트윗을 사용하였다[11]. 1차/2차 상황에서 정부에 대한 국민의 신뢰는 급격히 하락하였으나[13] 3차 상황에서는 공격이 발생하지 않아 공격자에 대한 신뢰도가 추락하였으며, 4차 공격에서는 공격집단에 대한 불신을 확인할 수 있다.

즉, 정부는 국민을 대상으로 불안감을 낮추기 위해 언론보도를 사용하였으며 공격자는 불안감을 높이기 위해 소셜네트워크를 사용하였다. 그리고 국민은 정부의 언론보도와 공격자의 소셜네트워크의 정보의 영향을 받아 소셜네트워크 내에서 지속적으로 정보를 수집하며 집단지성을 형성하게 된다. 그리고 형성된 집단지성의 긍정적인 표현과 부정적인 표현을 통해 대상의 신뢰도가 변화한다는 것을 알게 되었다[27].

기존 정책적 의사결정을 위한 모델은 과거의 폐쇄적 중앙지성에서 개방적 집단지성을 고려한 정책방안까지 발전하였으나, 집단지성에 영향을 주는 제3자의 존재에 대한 부분은 배제되었다. 또한 정부도 사이버 공격이 발생하면 사건을 확인하고 대응하며 그 결과를 보고하거나, 공격자의 거짓을 확인하고 보도하는 등 단편적인 대응만을 하였다.

이에 본 논문에서는 정부의 입장에서 효과적인 대응전략 및 정책을 수립하기 위해 3개의 서로 다른 집단이 참여하여 정보를 공개하며 사이버전을 전개하는 과정에 게임이론을 적용하고자 한다.

II. 관련연구

2.1 집단지성(Collective Intelligence)

집단지성은 다수의 지적개체들이 서로 협력하거나 경쟁을 통해 얻게 된 집단의 지적 능력으로 과거 폐쇄적인 환경의 중앙 집권적인 피라미드형 지성에서 현재는 정보화시대의 도래로 개방적인 환경의 분산형 집단지성으로 발전하였다[17].

집단지성이 형성되기 위해서는 사이버공간에서 지식의 분점, 지속적인 가치부여, 실시간 조정, 지성의 인정이라는 4가지가 핵심요소를 반영하여야 하며 집단지성을 극대화하기 위해서는 다양성을 전제로 자유로운 참여를 보장할 수 있는 환경이 조성 되어야 한다[18].

위키피디아[19]에서 한미FTA 촛불집회 사례를 통한 집단지성의 생성과정을 살펴보면 다음과 같다. 최초 촛불집회 관련문서가 생성된 시점은 '08년 5월 3일 생성되었으며, 한 달 사이에 500회 이상 변경되며 그 후 감소세를 보였다. 이는 6월 10일을 정점으로 7월부터 약화되는 모습과 유사하며[20], 이를 통하여 일정 기간이 지나면 집단지성이 안정화 단계에 진입한다는 것을 알 수 있다. 또한 집단지성이 형성되어 가능 과정에서 초기에는 새로운 정보가 지속적으로 등록되는 반면, 후기에는 단순 문구수정으로 변화하는 것을 알 수 있다.

이와같이 정부는 정책결정과정에서 집단지성의 중요성을 인지하고 이를 활용하기 위해 웹2.0, 정부3.0 등 의사결정과정에서 국민과 소통하는 절차를 수립하였다[20]. 하지만 중앙지성 및 집단지성에 부정적인 영향을 미치기 위한 조직적인 공격지성 또한 확인할 수 있다. 하지만 중앙지성 및 집단지성에 부

정적인 영향을 미치기 위한 조직적인 공격지성 또한 확인할 수 있다. 이러한 현상은 Fig. 1.과 같이 정부의 중앙지성이 집단지성으로부터 영향을 받으며, 집단지성은 기타 공격지성과 같은 기타 이해집단으로부터 영향을 받게 됨을 알 수 있다.

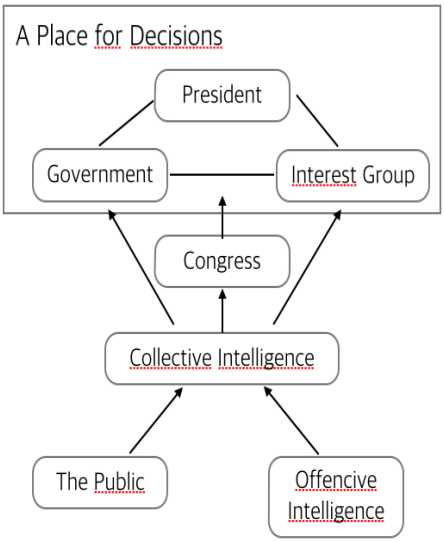


Fig. 1. Complicated Decision Object

2.2 정책(전략)결정 모델

정책결정 모델은 정보화 사회 진입을 기준으로 전통적인 정책결정 모델과 개방형 의사결정 모델로 구분할 수 있다[16].

전통적인 정책결정 모델은 합리주의, 만족, 점증, 혼합주사, 최적, 쓰레기통, 엘리슨 모형 등으로 최고결정자 및 조직 차원의 정책결정을 위한 방법이다. 기존의 모형은 엘리트이론으로 과거 관료주의사회의 정책결정에는 적합하나, 현 사회의 복잡해진 이해관계를 표현하지 못하는 단점이 있다[15].

이에 정책결정시 복잡해진 이해관계를 수렴하기 위해 Fig. 2.와 같은 집단지성형 정책결정 모델이 등장하였다[16]. 집단지성형 정책결정 모델은 다수의 창조적 참여자를 전제로 집단지성이 형성된 경우 활용되며 중앙지성의 문제해결방안에 대하여 집단지성과 상호 대립함으로써 개선된 해결방안을 얻을 수 있게 된다. 지성간의 검증과정을 통하여 식별된 문제점은 폐지/수렴/보완 하는 과정을 거치며 개선점을 확인할 수 있다.

정부의 정책결정에 집단지성모델이 활용된 대표적 사례는 한미FTA와 관련하여 쇠고기 분야이다[16]. 미국산 쇠고기 문제는 '07년 노무현 정부에서 제한적 허용이라는 부분이 '08년 이명박 정부에서 전면허용으로 변경되면서 발생된 상황으로 다양한 포털 사이트를 통하여 집단지성이 형성되었으며 집단지성과 중앙지성간 충돌 후 조정과정을 거쳐 정부의 정책이 변경되었다.

군사전략 분야에서는 전략결정 관련 정보전에서 전략적 우위에 설 수 있는 전략결정모델이 등장하였다. OODA 루프 전략결정 모델[25]은 관찰, 방위확인, 결정, 행동의 첫 글자를 따서 만든 용어로 전략적인 결정을 할 때 사용하는 프레임워크다[23].

Fig. 3.의 OODA 루프 모델은 현 상황을 관찰(Observe) 후 전략적 방향(Orient)을 설정하고 필요한 분야에 대하여 전략 결정(Decide) 후 전략을 행동(Act)하는 4가지 과정으로 구성되어 있다. 그리고 선택한 전략을 행동한 후에는 다시 그 결과를 관찰하며 지속적인 전략적 행동을 반복하게 된다.

이처럼 정책결정모델은 집단지성과 같이 다양한 주체로부터 정보를 수집하고 상황판단을 통해 정책의 방향을 결정 및 추진하며 결과를 다시 관찰하여 기존의 정책 및 전략을 수정하는 과정을 순환한다.

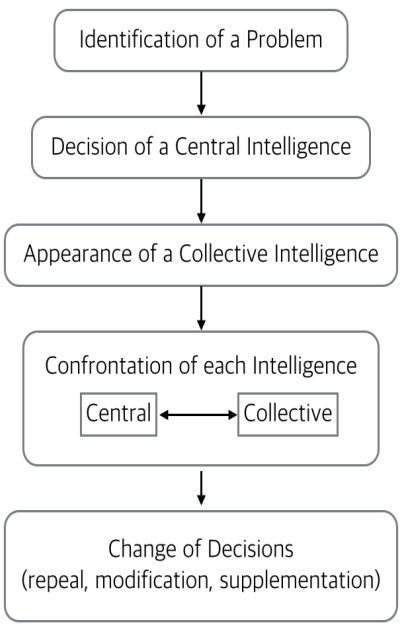


Fig. 2. Collective Intelligence Type Strategic Decision Model

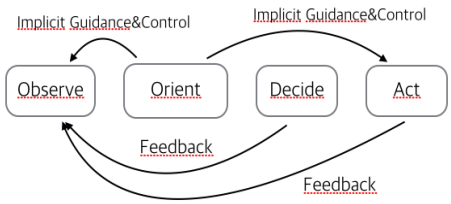


Fig. 3. OODA Loop Model

2.3 게임이론

게임이론은 두 명 이상의 사람들이 상호 연관 관계를 통해 자신의 이익을 추구하고 있으나 그 결과를 어느 누구도 마음대로 결정할 수 없는 경쟁적인 상황에서 합리적인 선택을 할 수 있도록 지원하는 의사결정방법중 하나이다[26].

게임이론의 기본적인 구성요소는 게임을 하는 사람인 경쟁자, 각각의 경쟁자가 결정할 수 있는 전략, 각각의 전략을 선택하였을 경우 받을 수 있는 보수로 구분된다.

또한 전략 선택 시 게임에 참여하는 경쟁자간 약속이 구속력이 있는지 없는지에 따라 협조게임과 비협조게임으로 분리할 수 있으며 각각의 게임방식에 따라 표현방식은 특성 함수형이나 전개형, 일반형으로 구분할 수 있다. 또한 경쟁자들이 동시에 진행되는지 차례대로 진행되는지에 따라 동시게임과 순차게임으로 구분하는 등 다양한 게임이론 모델이 지금도 연구 및 발전되고 있다.

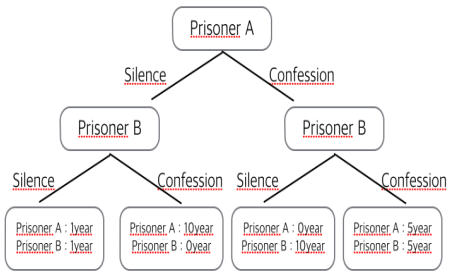
Fig. 4.는 게임이론에서 사용하는 대표적 딜레마인 죄수의 딜레마를 게임이론적 해석관점으로 정리하였다. 두 명의 죄수를 서로 다른 장소에 분리시킨 후 둘 중 먼저 죄를 진술하는 사람에게 낮은 처분을 내린다고 한다면 죄수는 어떠한 선택하는 것이 올바른 선택인지 결정하는 것이다.

게임이론은 정부정책 및 군사전략 분야에서 의사결정방법으로 사용되었다. 정부정책의 예로는 한미FTA 쇠고기 협상시 정부와 국민간의 분쟁을 게임이론 전략으로 해석하였다[22]. 정부의 한미FTA전략은 Fig. 5.와 같이 정부와 미국간의 외교적인 문제만이 아닌 정부와 국민간의 신뢰문제도 전략적으로 해결할 필요성이 있었다.

군사전략 분야에서는 정보전의 정보전략 중 하나인 OODA 루프 모델에서도 게임이론을 접목하여 사용하였다. OODA 루프 모델에 게임이론을 활용한

Category	Prisoner B Silence	Prisoner B Confession
Prisoner A Silence	1Year,1Year	10Year,0Year
Prisoner A Confession	0Year,10Year	5Year,5Year

a)Prisoner's dilemma : The Payoff Matric



b)Prisoner's dilemma : The Game Tree

Fig. 4. Case of Game Theory

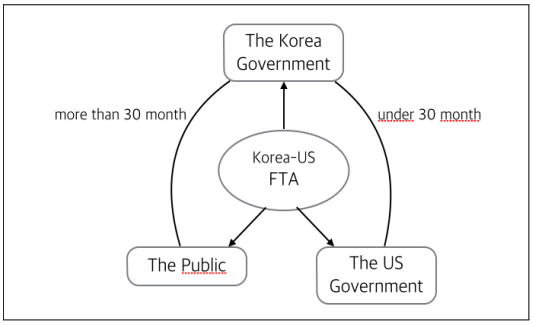


Fig. 5. Game Model in Korea-US FTA

사이버 정보전 시나리오로는 테러리스트와의 대립 게임, 악의적인 해커와의 대립 게임, 서비스 파괴자와 대립 게임, 사회적반항자와의 대립 게임 등 다양한 형태의 게임에 대하여 연구되고 있다[24].

III. 사이버공간에서 집단지성을 활용한 정책결정모델

3.1 기존 모델의 한계 및 개선된 모델 제안

'08년 한미FTA로 인한 촛불집회 이후 정책결정 모델은 집단지성의 다양성을 신뢰한 정책결정모델로 발전하고 있다. 하지만 집단지성을 구성하는 정보는 유통과정에서 잘못된 정보, 부족한 정보, 의도적으로 조작된 정보, 소수의 의견 등이 혼재되어 유통되기

때문에 집단지성을 무조건 신뢰할 수 없다[21]. 또한 '14년 한국수력원자력 문서유출 사건을 보면 악의적인 목적을 가진 제3의 요소가 집단지성에 영향을 주기 위해 조작된 허위정보를 유포하는 것을 알 수 있다.

이에 따라 중앙지성과 집단지성의 대립을 기반으로 한 집단지성형 정책결정모델을 개선하여 모델 내 중앙지성과 집단지성 外 공격지성을 추가하고 게임이론을 적용하여 3가지 지성의 전략을 비교하는 개선된 집단지성형 정책결정모델을 제안한다.

Fig. 6.과 같이 문제점이 식별되면 우선 중앙지성에서 해결안을 모색한다. 그 후 집단지성이 형성되고 이해관계에 따라 공격지성이 형성되게 된다. 그 후 3개의 지성이 대립하며 문제를 검증하게 되고 그 결과에 의해 중앙지성의 해결안이 수정 및 개선되고 다시 수정된 해결안을 두고 집단지성과 공격지성이 재형성된 후 각각 대립하며 다시 해결안이 개선되게 된다.

개선모델의 기본 구성은 기존의 집단지성형 정책결정모델과 유사하지만 핵심인 관계분석을 기존모델은 중앙지성과 집단지성간의 사실관계에 근거한 대립으로 설명하였다면 개선된 모델은 중앙지성에 대립하여 집단지성에게 영향을 줄 수 있는 제3의 공격지성을 추가하고 3자간에 게임이론을 적용하여 전략적 의사결정이 가능하도록 고려하였다.

이때 각 지성의 분류는 정보를 공개하는 과정에서 식별할 수 있는 외부적인 요소를 기반으로 분류하였으며 정부의 언론보도, 위기경보발령 등의 정보를 사용하는 기관을 중앙지성으로, 공격집단으로 언론제보, SNS를 통하여 전략 및 정보를 공개하는 집단을 공격지성으로, 마지막으로 위키피디아, 게시판 등 사이버 공간을 통하여 의견이 취합되는 지성을 집단지성으로 하였다.

이는 각각의 지성이 정보를 얼마나 보유하고 있는가를 기준으로 영향력을 식별하고 전략을 확인하기 위한 것으로 제한하였으며, 개선된 정책결정 모델은 이 3가지 지성을 게임이론적 관점에서 최적의 결과를 도출한 후 중앙지성의 정책을 폐지, 수정, 보완하게 된다.

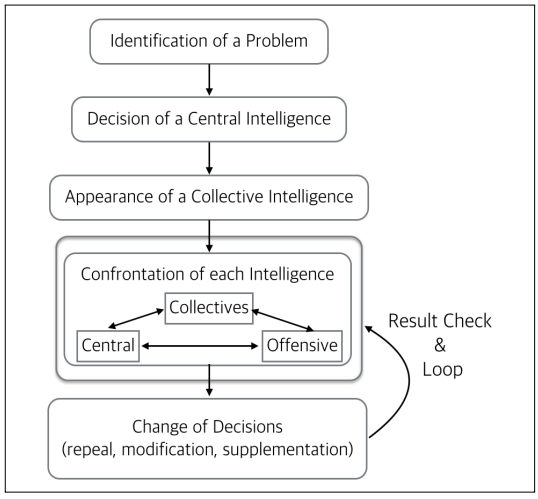


Fig. 6. Improved Collective intelligence type strategic Decision Model

3.2 정보기반의 게임이론적 집단지성간 관계분석

3.2.1 대립관계의 게임이론적 배경

사이버공간에서 공격과 같은 하나의 이벤트가 발생하면 중앙지성, 집단지성, 공격지성이 생성된다. 그러면 Fig. 7.과 같이 3가지 지성이 서로 대립하게 되는 모습을 확인할 수 있다.

최초 공격이 발생하면 Table 1.과 같이 공격지성은 공격을 직접 수행하여 100%이라는 정보를 가지고 있다면, 중앙지성은 식별한 공격을 검증하는 과정을 거쳐 전체에 50%이라는 정보를 가지게 된다. 그리고 집단지성은 양쪽이 공개한 정보가 없는 상황으로 0%의 정보를 가지고 있다.

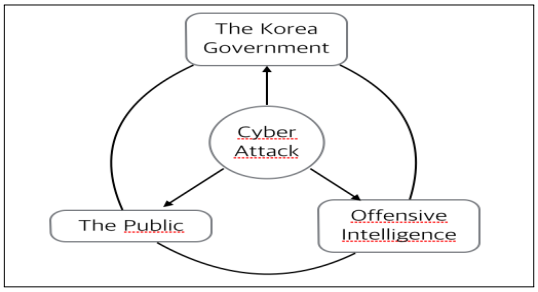


Fig. 7. Korea's Game Model in Cyber Attack

Table 1. The first amount of information by object incase of cyber attack

Category	Central intelligence	Offensive intelligence	Collective intelligence
The first amount of information	50%	100%	0%

이때 중앙지성과 공격지성은 전략적 선택을 할 수 있으며, 가지고 있는 정보에 대하여 공개/일부공개/거짓/비공개 등 4가지 전략적 요소를 선택하게 된다. 그리고 집단지성은 공개된 정보를 수용하는 과정에서 '수용/무시' 두 가지 선택이 가능하다.

전략의 결과인 보수는 '신뢰/일부신뢰/불신/없음'로 게임을 단순화 하였으며, 집단지성의 보수는 '중앙지성 신뢰/공격지성 신뢰'로 단순화하여 분석하였다.

그리고 개선된 정책결정 모델에서는 이 3가지 지성을 게임이론적 관점에서 대립시킨다.

3.2.2 집단지성 대립관계의 보수행렬

보수행렬은 게임이론에 구성요소인 경쟁자, 전략, 보수를 표현하는 방법 중 하나로 사전에 정의한 대립과정을 보수행렬을 통하여 해결할 수 있다.

최초 사이버공격이 발생한 상황에서 집단지성은 인지한 정보가 없기 때문에 정보를 비공개하지 않는 이상 공개한 쪽을 수용하며 100% 신뢰한다. 그러나 50% 지성이 형성되어 정보의 진위를 가려 수용한다면 신뢰여부도 50%정도로 판단할 수 있다. 그리고 모든 정보를 알고 있는 경우 100% 진위여부를 판단할 수 있게 된다.

보수행렬표는 총 3가지로 집단지성이 정보를 판단하여 거짓을 식별하거나 수용할 정보를 판단할 확률에 따라 구분하였다. 이때 보수로 신뢰한다는 1, 신뢰하지 않으면 0, 불신할 경우 -1이라 가정하였다.

Table 3.은 집단지성이 최초 거짓을 식별할 수 없는 상황에 따른 보수행렬표로 거짓 전략을 선택하더라도 집단지성에 신뢰를 얻을 수 있다.

Table 2. Game Theoretical background in cyber attack

competition	strategy	payoff	
		Collective intelligence accept	Collective intelligence ignore
Central intelligence (CI)	Open	CI Trust	
	Part	CI Some Trust	
	Fake	CI Trust. OI Distrust	CI Distrust OI Trust
	Close	None	
Offensive intelligence (OI)	Open	OI Trust	
	Park	OI Some Trust	
	Fake	OI Trust CI Distrust	OI Distrust CI Trust
	Close	None	

Table 3. A payoff matrix in the first cyber attacks

CI \ OI	Open	Part	Fake	Close
Open	1,1	1,0.5	1,1	1,0
Part	0.5,1	0.5,0.5	0.5,1	0.5,0
Fake	1,1	1,0.5	1,1	1,0
Close	0,1	0,0.5	0,1	0,0

Table 4. After completion collective intelligence

CI \ OI	Open	Part	Fake	Close
Open	1,1	1,0.5	1,-1	1,0
Part	0.5,1	0.5,0.5	0.5,-1	0.5,0
Fake	-1,1	-1,0.5	-1,-1	-1,0
Close	0,1	0,0.5	0,-1	0,0

집단지성이 완벽하게 형성되어 거짓을 100% 판단하면 Table 4.와 같이 변경된다.

집단지성이 어느 정도 형성되어 50% 확률로 거짓을 판단할 수 있게 된다면, 만약 공격지성이 거짓 전략을 선택하고 집단지성이 거짓을 확인한다면 보수는 Table 5.와 같이 수정되며 집단지성의 완성상태와 동일함을 알 수 있다.

그러나 집단지성이 50%의 확률로 거짓을 판단할 수 없다면 Table 6.와 같이 수정되며, 최초 상황과 동일함을 알 수 있다.

3.2.3 집단지성 형성 후 합리적인 대응전략

게임이론을 기반으로 한 다양한 전략 가운데 지배전략은 상대가 어떠한 전략을 선택하더라도 자신에게 항상 좋은 결과를 가져오는 절대 우위 전략이다.

Table 5.와 같이 거짓을 판단할 수 있는 집단지성 형성되었다면 중앙지성은 공격지성이 어떠한 전략을 선택 하더라도 집단지성의 신뢰를 얻을 수 있는 절대 우위전략인 공개 또는 일부공개 전략을 선택하는 것이 합리적이다. 하지만 거짓을 판단할 수 없는 집단지성인 Table 6.의 경우 집단지성의 신뢰를 가장 크게 얻을 수 있는 공개 또는 거짓 전략을 선택하는 것이 합리적이다.

게임이론의 다른 전략인 최소극대화전략은 상대가 가장 불리한 전략을 사용하여 최대한의 피해를 발생시키는 것이 목적이다. Table 6.와 같이 거짓을 판단

Table 5. In Case of false judgments of collective intelligence

CI \ OI	Open	Part	Fake	Close
Open	1,1	1,0.5	1,-1	1,0
Part	0.5,1	0.5,0.5	0.5,-1	0.5,0
Fake	-1,1	-1,0.5	-1,-1	-1,0
Close	0,1	0,0.5	0,-1	0,0

Table 6. In Case of false misjudgments of collective intelligence

CI \ OI	Open	Part	Fake	Close
Open	1,1	1,0.5	1,1	1,0
Part	0.5,1	0.5,0.5	0.5,1	0.5,0
Fake	1,1	1,0.5	1,1	1,0
Close	0,1	0,0.5	0,1	0,0

할 수 없는 상황이라면 중앙지성의 피해를 최대한으로 발생시키기 위해 공격지성은 거짓을 선택하는 것이 합리적인 선택이다.

또한 내시 균형 전략은 경쟁자가 선택하는 전략이 최선인 동시에 전략적 최선의 선택인 게임으로, 표에서는 양쪽이 정보를 모두 일부 정보만을 공개하는 것이 합리적인 선택이다.

하지만 거짓과 일부의 정보를 가지고 있는 경우 등 복잡한 경우에 대해서는 보수행렬표로 정리하기에는 제한점이 있어 본 논문에서는 고려하지 않았다.

3.2.4 사례연구

한수원 개인정부 유출사고의 경우 공격지성인 원전반대그룹, 중앙지성에 한수원, 집단지성에 국민으로 판단할 수 있다. 각각의 상태변화를 확인하기 위해서 공격지성은 공격에 사용된 트위터를 분석하였으며, 중앙지성은 보도자료를 기반으로 분석하였다. 또한 집단지성의 경우 트위터, 블로그, 뉴스를 수집하고 반응을 분석하는 미디어분석서비스를 활용하여 변화를 확인하였다[27].

한수원 개인정보 유출사고는 4단계의 국면으로 정리할 수 있다. 1단계 기밀문서 유출('14.12.19 이전), 2단계 원전중단 협박('14.12.23), 3단계 금전요구(15.3.12), 4단계 불안감 조성 및 금전요구('15.7.8)로 분류하며 분석 기간은 '14.12.1 에서 '15.8.31 까지 9개월 간 분석하였다.

9개월 간 중앙지성과 공격지성은 단계별로 Table 7.과 같이 진행되었다. 그 결과 공격지성은 1단계에서 4차례 진행하며 신뢰를 확보하였으며, 중앙지성은 0건 대응하였다. 2단계에서는 공격지성은 2차례 활동한 것에 비해 중앙지성은 11건 대응활동을 보이면서 적극적으로 활동하는 것을 알 수 있다. 하지만 마지막 4단계 에서는 공격지성이 3차례 활동한것에 비해 중앙지성은 1차례 활동함으로 그 대응을 마무리한다.

이와 관련하여 집단지성의 변화는 공격지성과 중앙지성을 각각 분리하여 확인하였다. 집단지성 관점에서 중앙지성은 총 4차례 관심이 증가하는 것을 확인할 수 있다. 그중 1단계, 2단계는 부정적인 인식이 굉장히 높은 것을 알 수 있다. 하지만 3단계, 4단계에서는 중앙지성은 평상시를 유지하고 오히려 공격지성에 대한 부정적인 인식이 굉장히 높아지는 것을 알 수 있다.

1단계에서 공격지성인 원전반대그룹은 해킹사실을 알리기 위해 유출된 문서정보를 공개한다. 이때 중앙지성은 아직 인지하지 못하여 즉시 대응하지 못하며 집단지성은 공격지성의 정보를 신뢰하며 중앙지성에 부정적인 인식을 가지기 시작한다.

2단계에서 공격지성인 원전반대그룹은 원전을 마비시킬수 있다는 거짓과 자료를 유출하였다는 사실을 혼합하여 집단지성에게 정보를 공개하였다. 그와는 반대로 중앙지성은 공격지성의 정보 중 확인된 사항이 미흡하여 일부 대응하나 불신을 제거할 수준으로 대응하지 못하였다. 따라서 집단지성의 반응은 중앙

Table 7. Central and Offensive's Timeline

Stage	Date	Offensive	Central
1 stage	'14.12.15	forecast	
	'14.12.17	1th	
	'14.12.18	2th	
	'14.12.19	3th	
2 stage	'14.12.20		1case
	'14.12.21	4th(threat)	1case
	'14.12.22		1case
	'14.12.23	5th	1case
	'14.12.25		4case
	'14.12.28		1case
	'14.12.30		2case
3 stage	'15.3.12	6th(demand)	1case
	'15.3.17		1case
4 stage	'15.7.8	7th(demand	1case
	'15.7.13	8th	
	'15.8.4	9th	

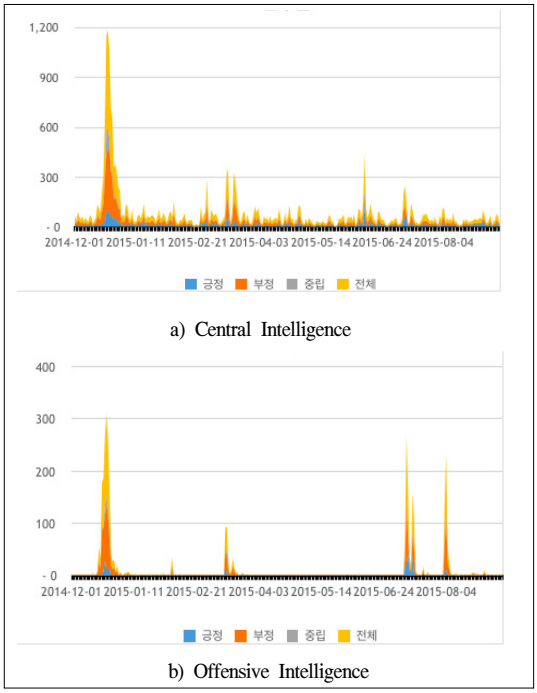


Fig. 8. Corrective Intelligence's Awareness

지성에 더욱 더 부정적인 반응을 보이게 된다. 하지만 예정일에 공격지성의 공격이 실행되지 못하며 거짓임을 확인하게 된다.

3단계에서 공격지성은 다시 작전을 수립하기 위해 1단계와 동일하게 일부 정보를 공개하며 금전을 요구한다. 하지만 중앙지성은 해당 사실에 대한 신뢰성만 확인하고 추가 대응하지 않으며 집단지성은 공격지성의 거짓을 인지한 후 추가 정보에도 소극적으로 반응한다.

4단계에서 공격지성은 다시 한 번 공격을 수행하려 하지만 오히려 집단지성의 부정적인 인식만을 높이가 작전을 마무리하게 된다.

즉, 원전반대그룹의 전략적 변화를 정리하면 최초 사이버공격을 통해 확보한 정보의 일부를 공개하며 절대우위전략 또는 내시균형 전략을 선택하였다. 그리고 2차 공격 시 집단지성이 거짓을 판단할 수 없어 최소극대화전략을 사용하여 사회적 불안감을 극대화 하였다. 하지만 3차, 4차 공격 시 집단지성이 거짓을 판단하여 공격집단이 최소극대화전략을 선택하였으나, 효과를 보지 못한 것을 알 수 있다.

IV. 결 론

한수원 사태를 계기로 사이버전이 해킹과 심리전이 결합된 양상으로 발전하고 있다. 이에 효과적 대응을 위한 중앙 컨트롤타워의 전략적 의사결정은 나날이 그 중요성이 대두되고 있다.

본 연구는 사이버전이 심리적 양상으로 변화함에 따라 지금까지 전략적 대상으로 고려되지 않은 집단지성을 전략의 대상으로 포함시키고자 하였다. 또한 사이버전을 게임이론적 관점으로 해석하여 중앙지성, 집단지성, 공격지성을 대립시킨 후 효과적인 전략적 선택 방안에 대하여 연구하였다.

하지만 전략의 다양성 및 거짓에 대한 현실성, 영향력 등은 전략적 의사결정을 위해 해결하여야 할 과제로 남아 있다.

이에 향후 연구방향으로 한수원 사태를 예로 전략의 다양성과 공개된 정보에 거짓이 포함된 경우를 고려하고, 지성 간 보수의 문제를 합리적인 방안을 통하여 해결하고자 한다.

References

[1] Kim Eun young, Park Jung gil, 1.25 Internet Crisis Diagnosis, Korean Institute of Information Scientists and Engineers, 2003

[2] Kim Kyung hwan, The 10 Class Action Related Personal Information, Security News, 2013.8.8

[3] Oh Byeong min, 7.7 DDoS Attacks, "What was the Events?, Security News, 2010.7.7

[4] AnnLab, 3.4 DDoS Analysis Reports, AnnLab, 2011.3

[5] Red Alert, 3.20 Cyber-Terror Incident Analysis Reports, Red Alert, 2014

[6] Kim Gyeong ae, ADD, 'Domino' of Leaked Military Secrets, Security News, 2014.4.8

[7] Kwon Jun, KHNP Hacking Terror! Since The First Reports, The 15 Days' Records, Security News, 2014

[8] Sin Jong hwan, The Invasion Incident Status Thorough Domestic Internet Events Experience, KISA, 2013.9

〔9〕 KISA, National Information Security White Paper, KISA, 2015
〔10〕 Choe Byong taek, The Seeking of Cyer Response Capabilities Strengthening In Civil Areas, MSIP, 2015
〔11〕 @john_kdfifj1029, https://twitter.com/john_kdfifj1029
〔12〕 KHNP, KHNP Press Release, https://cms.khnp.co.kr/news/
〔13〕 Kim Seung ju, To Prevent The Second KHNP Crisis, Korea University, 2015
〔14〕 Choe Yun su, 〔Press Release〕 Intermediate Investigation Results of KHNP Cyber-Terror, The Government Joint Investigation Units about Personal Information Criminals, 2015.3
〔15〕 Yun Sang oh, "E-government Promotion Policy Evaluation of The Participating Governments" Korea Public Administration Gazette 22.2 (2008): 89-123.
〔16〕 Yun Sang oh, "The Informationization Effect on The Government Decision-Making: On US Beef Imports Decision-Making", Journal of Korea Information Region No. 13.3.
〔17〕 Park Jae cheon, Sin Ji ung, "The Study of Collective Intelligence Utilization in Web 2.0 Platform", Korea Society for Internet Information Vol.8 No.2, 2007.6
〔18〕 Gruber, Thomas. "Ontology of folksonomy: A mash-up of apples and oranges." International Journal on Semantic Web and Information Systems (IJSWIS) 3.1 (2007): 1-11.
〔19〕 Wikipedia, Wikipedia:Introduce, https://ko.wikipedia.org/wiki/Wikipedia:Introduce
〔20〕 Jo Hwa sun, Choe Jae dong, The Politics of Collective Intelligence, Information Policy 2010,
〔21〕 Kim Hong yeol, 'Collective Intelligence' is Right Absolutely?, Ohmynews, 2014
〔22〕 Hwang Kwangseon, Social Implications from the Analysis on the Government Negotiation by Using Game Model, Korea Journal of Social Issues Vol.21, 2011
〔23〕 Boyd, John R. Destruction and Creation. U.S. Army Command and General Staff College, 1976
〔24〕 Jormakka, Jorma, and Jarmo VE Mölsä. "Modelling information warfare as a game." Journal of information warfare 4.2 (2005): 12-25.
〔25〕 Brehmer, Berndt. "The dynamic OODA loop: Amalgamating Boyd's OODA loop and the cybernetic approach to command and control." Proceedings of the 10th international command and control research technology symposium. 2005.
〔26〕 Myerson, Roger B. Game theory. Harvard university press, 2013.
〔27〕 pulsek, http://www.pulsek.com/pulsek/,
〔28〕 Sangwon Seo , Woojin Oh , Hogil Kim, "Research on cyber warfare manpower training strategy for securing Defense Information System using AHP analysis", Journal of Security Engineering, 12.2, 2015

〈저자소개〉

박 상 민 (Sang-Min Park) 종신회원
1994년 2월: 울산대학교 법학과 졸업
2012년 2월: 고려대학교 정보보호대학원 석사
2014년~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 사이버전, 사이버 정보, 사이버 심리, 사이버 공격, 전략결정

이 경 호 (Kyung-Ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사
2009년 8월: 고려대학교 정보보호대학원 박사
1994년 2월~현재: 삼성그룹, NHN, 시큐베이스 등 근무
2011년 9월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 위험관리, 정보보호컨설팅, 정보보호 및 개인정보보호정책

임 종 인 (Jong-In Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
청와대 안보특별보좌관, 고려대학교 정보보호대학원 교수, 개인정보보호위원회 위원, 한국인터넷진흥원 비상임이사, 방송통신위원회 기술자문위원, 대검찰청 디지털수사자문위원장, 경찰청 사이버테러대응센터 자문위원, 국가정보원 국가보안협의회 위원
〈관심분야〉 사이버 국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안