Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.1, Feb. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.1.103

사이버공격 의도분석을 통한 공격유형 분류에 관한 연구 - 사이버공격의 정치·경제적 피해분석을 중심으로 -

박 상 민,† 임 종 인‡
고려대학교 정보보호대학원

Study On Identifying Cyber Attack Classification Through The Analysis of Cyber Attack Intention

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

요 약

사이버공격은 목적 및 의도에 따라 사이버 전쟁, 테러, 범죄 등의 유형으로 분류할 수 있고 해킹·DDoS·선전 등 다양한 전략과 전술이 동원된다. 사이버공격으로 발생한 피해는 경제·사회·군사 및 물리·정보·인식 등 다양한 범주에서 발생하고 공격주체 식별을 위해 통상 IP·ID·URL 등 사례기반분석이 이용된다. 그러나 최근 사이버공격은 디지털 정보의 조작을 통해 의도와 주체를 은폐하며 클라우드 기반의 사이버환경이 등장함에 따라 공격유형의 분류 및 대응전략 수립이 제한됨에 따라 피해기반분석의 필요성이 대두되고 있다. 이에 본 논문에서는 사이버공격시 발생한 피해를 경제·정치적 관점에서 분석하고 공격의도를 추론함으로써 사이버공격 유형을 분류하고자 한다.

ABSTRACT

Cyber attacks can be classified by type of cyber war, terrorism and crime etc., depending on the purpose and intent. Those are mobilized the various means and tactics which are like hacking, DDoS, propaganda. The damage caused by cyber attacks can be calculated by a variety of categories. We may identify cyber attackers to pursue trace-back based facts including digital forensics etc. However, recent cyber attacks are trying to induce confusion and deception through the manipulation of digital information or even conceal the attack. Therefore, we need to do the harm-based analysis. In this paper, we analyze the damage caused during cyber attacks from economic and political point of view and by inferring the attack intent could classify types of cyber attacks.

Keywords: Cyber Attack, Intent Analysis, Damage Analysis, Cyber Attack Type

I. 서 론

'초연결시대'는 스마트폰 등 모바일 정보통신 기기, 광속의 유·무선 네트워크 및 언제 어디서나 접속할 수 있는 IoT(Internet of Things) 등 ICT 발달의 창조적 산물에 의해 도래하였다. 그리고 트위터, 페이스북 등 소셜미디어의 등장으로 사이버공간은 정보의 저장 공간에서 인간의 생각을 공유하는 의사소통의 공간으로 발전하였다. '12년 미국 대선에서 오바마는 국민과 소통하기 위해 SNS를 활용하였고 우리나라도 '광우병' 등 사회적 이슈 발생시 사이버공간에서 집단지성이 형성되었으며 정책결정시 영향력을 행사하기도 했다. 이러한 사회적 현상을 통해 사이버공간에서 불특정 활동이 개인·집단에 영향을 미친다

Received(10. 10. 2016), Modified(02. 07. 2017), Accepted(02. 14. 2017)
† 주저자, adu_96@naver.com
‡ 교신저자, jilim@korea.ac.kr(Corresponding author)

는 사실을 확인할 수 있었다.

사이버공간은 개인과 집단이 다양한 의도를 가지고 행동하는 가상의 영역이다. 사이버공간에서는 익명성을 이용하여 자신을 가상의 아바타, ID, 닉네임으로 표현한다. 사이버공간에서 가상 주체의 활동은 쇼핑이나 자신의 의견을 게시하는 정상적 행동과 여론호도를 위한 허위사실 유포, 금전갈취를 위한 불법사이트 운영, 국가안보 위해를 위한 교통·통신·금융 등 사회기반시설 해킹 등 악의적 행동도 동시에 존재한다. 그리고 악의적 행동을 위해 가상의 자신은 개인으로 행동하는 경우와 집단으로 행동한 경우 등 다양한 주체로 존재한다.

사이버공격은 사이버공간에서 악의적 의도를 포지하고 행동하는 것을 말한다. 사이버공격이 발생하면 사례기반분석을 통해 공격정보를 식별할 수 있지만 현실공간에서 정확한 공격주체를 찾기에는 제한요소가 많다. 비록 공격주체를 인지해도 공격주체가 개인·집단 중 어느 유형인지 확인하기는 더욱 어렵다. 사이버공격에 효과적으로 대응하기 위해서는 공격주체의 목적을 확인하여야 한다. 그리고 이러한 목적을 우리는 '공격의도'라고 한다. 일반적인 사이버공격은 공격진행 과정에서 예상하지 못한 상황으로 명확한 공격의도에 도달하지 못할 수 있으나, 국가적인 사이버공격에서는 공격의도에 도달하기 위해 행동한다.

기존의 심리학 분야의 '의도적 행동에 대한 상식적 모델'에 의하면 개인의 의도는 욕망, 신념 요소를 통하여 결정되며 집단의 경우 집단의 형태에 따라 정치, 경제 요소를 통하여 개인의 의도가 집단의 의도로 발전된다. 그리고 개인 및 조직의 의도는 장 보드리야르[29]의 소비사회론에 의한 이미지, 게오르그 짐멜[30]의 화폐(자본)로 해석할 수 있다. 따라서 사이버 공격의도를 확인할 수 있다면 공격주체를 식별할 수 있으며 공격주체 및 공격의도를 통해 사이버전쟁, 분쟁, 테러, 범죄를 판별할 수 있으므로 효과적 대응전략도 수립할 수 있다.

이에 본 논문은 공격자가 식별되지 않은 국내의 '14년 DDoS 공격 및 개인정보유출 사건, 북한의 사이버공격으로 확인된 미국 소니픽처스 해킹, 한수원 사이버테러 등 3가지 사례를 정치적 이미지·경제적 자본 피해 관점에서 분석하기 위해 SNS 이미지분석과 주식시장의 변화분석을 통해 공격의도 및 주체를 추론하고 공격유형을 판별하고자 한다.

II. 관련연구

2.1 개인의 행동에 관한 연구

사람이 행동을 선택하는 원인에 대하여 이해하고자 하는 것은 과거부터 중요한 연구과제였다. 그리고 이러한 연구는 '의도 판단'과 '의도적 행동 판단'이라는 연구를 통해 해석되고 있다. Malle와 Knobe[1]은 '의도적 행동에 대한 상식적 모델'을 통해 의도는 욕망, 신념, 자신의 행동에 대하여 인지하는 자각, 행동할 수 있는 기술에 의해 결정됨을 확인하였으며, Knobe[2]은 Wellman[3]의 '마음 이론'을 포함하여 도덕적인 성격이 행동에 영향을 주는 '부수적 의도결정 결과'를 확인하였다. 하지만 '부수적 결과효과'는 이현진[4]이 한국인에게는 효과가 없는 것으로 확인하였으며 박주화[5]를 통해 도덕적 성격이 행동과 의도에 모두 영향을 주는 '보다 강력한 부수적 효과'에 대하여 확인하였다.

소셜미디어의 등장으로 의사소통이 활발해지며 이러한 연구는 사이버공간으로 확대되었다. Suler[6]는 사이버공간에서는 행위자가 긴장이 완화되고 구속감을 훨씬 적게 느끼며, 개방적으로 자신을 표현하는 '탈억제 효과'를 주장하였다. 이는 은폐 및 노출관리가 가능하고 다중 정체성을 가질 수 있는 사이버공간의 대표적인 부정적 특징으로 박주화[5]의 '강력한 부수적 결과효과'는 기술이나 자각은 쉽고 강해진 반면, '탈억제 효과'를 통해 도덕적인 성격은 낮아지게 되어 의도적 행동을 쉽게 수행할 수 있음을 확인하였다. 그리고 이러한 행동에 대하여 김성직[7]은 소셜미디어 커뮤니케이터의 유형분석을 통해 사이버공간에서 행위자는 시청자형, 주인공형, 개인적 참여형, 사회적 참여형으로 구분하였다.

즉, 사이버 공간에서 개인의 행동은 '탈억제효과'에 의해 도덕성의 영향은 낮으나 '의도적 행동에 대한 상식적 모델'에 기반을 두어 행동하며 시청자형, 주인공형, 개인적 참여형, 사회적 참여형 등 4가지 유형으로 표현됨을 알 수 있다.

사이버공간에서 개인을 대상으로 한 대표적인 범죄행위인 해킹의 경우 게임이론을 활용하여 범죄활동을 정의할 수 있다. Becker[8]는 범죄적 행동으로 인한 이득이 범죄활동으로 기대되는 손해보다 클 때 발생한다는 가정아래 범죄자들의 행동을 모형화 하였다[9].

이처럼 악의적 공격자가 개인인 경우 신념과 욕망

을 달성하기 위해서 요구조건을 직·간접 제시하게 된다. '11년도에 발생한 대한민국 정부를 표적으로 사이버공격을 예고한 '어나니머스 사칭사건'의 경우 개인이 정부의 정책을 비난하는 과정에서 어나니머스를 사칭한 것으로 개인의 욕망이 간접 제시된 경우이다. 또한 청탁을 통한 DDoS 공격, 몸캠 협박의 경우도 금전적 이익을 목적으로 하는 개인적 욕망에 표출된 것임을 알 수 있다. Fig.1.는 개인의 행동에 관한 연구를 개념적 모델로 재구성 한 것이다.

2.2 집단(조직)의 행동에 관한 연구

집단 혹은 조직의 행동은 의사결정 과정을 통해서 해석할 수 있다. 의사결정은 최종적 결정에 도달하려는 사고와 행동과정으로서 둘 이상의 문제해결대안들 중에서 의사결정권자가 목적을 달성하는 데 있어 최선의 대안이라고 생각되는 것을 선택하는 행위이다[10]. 사이버공간에서도 네티즌들의 행동은 집단적 사고로 이뤄지며 이는 Lévy[11]의 집단지성을 통해 행위자들의 집단사고를 확인할 수 있다. 과거에는 현안 문제를 해결하기 위한 의사결정은 문제에 대한 해박한 전문가에 의존하여 해결책을 탐색하였다. 하지만 사회의 복잡성 및 불확실성이 증대하면서 소수의 전문가가 모든 상황에 최상의 대안을 제시하는 것이 불가함에 따라 집단사고를 통해 문제를 해결하게 된다[12].

정책분야에서는 다수의 구성원이 효과적으로 정책을 결정하기 위해 합리모형, 만족모형, 점증모형, 혼합탐사모형, 최적모형, 쓰레기통모형, 엘리슨모형으로 의사결정 과정을 해석하며 효과적인 탐구기법으로 브레인스토밍, 마인드맵, 명목집단법, 델파이, 악마의 주창자 등이 있다[13]. 그리고 콜린은 군사전략적 의사결정시 정치, 사회, 경제, 기술, 군사, 지리, 역사 등 8가지 항목을 제시하였다.

하지만 집단적 사고 또는 조직적 사고가 항상 올바른 결과로 귀결되지는 못하였다. Asch[14]는 '동조실험'을 통해 대책이 잘못된 방향이라도 개인은 집단의 의사결정에 따른다는 것을 확인하였으며 밴드왜건효과, 펭귄효과, 스눕효과 등을 통해 집단적 사고의 위험성을 알 수 있다. 또한 대한민국의 한수원 사이버테러 사태를 통해 사이버공간에서 행위자의 행동이 사이버전으로 확대될 수 있다.

박상민[15]은 한수원 사이버테러 사태를 분석하여 공격지성, 중앙지성, 집단지성으로 사이버공간의 집단적인 행위를 구분하고 사이버 공간에서 상호 대립하는 것을 확인하였다. Fig.1.는 집단의 행동에 관한 연구를 개념적 모델로 재구성 한 것이다.

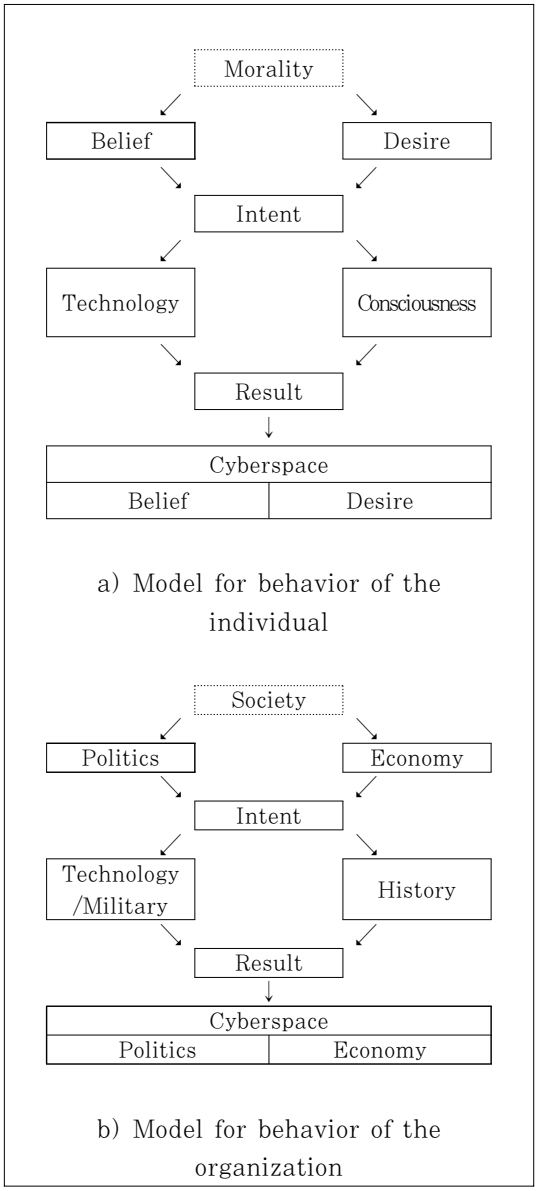

Fig. 1. Conceptual model for behavior of the individuals and organization

2.3 사이버공격에 의한 피해산출에 관한 연구

초기에는 사이버공격에 의해 시스템이 손해를 발생시키는 '제조물책임법'에 의해 피해액을 산출하였

다. 하지만 피해를 보상하는 주체는 제조물의 결함으로 소프트웨어를 개발한 업체에서 피해를 인정하게 되었다. 우리나라도 2003년 1.25 인터넷대란이 발생하고 인터넷가입자, 언론매체, 쇼핑몰 등이 MS, 정통부, 데이콤 등을 대상으로 손해배상책임을 청구하였다[16].

사이버공격의 표적은 사이버공간을 구성하는 유형자산인 네트워크, 서버, PC로 부터 무형자산인 정보 및 신뢰성 등으로 확대되고 있다. 공격대상이 받을 수 있는 피해 유형은 비밀성 상실, 가용성 상실, 무결성 상실로 구분할 수 있다. 1.25 인터넷대란의 경우 네트워크의 가용성이 상실된 예로 볼 수 있다.

가용성에 관하여 피해액을 산정하는 모형은 KISA모형, Gordon모형, Loeb모형 등이 있다. 일반적인 모형의 특징은 피해를 받은 경우 총 피해액은 시스템 또는 네트워크의 가용성 상실로 인한 매출이익의 손실액인 손실이익(LoP)과 시스템 및 네트워크에 의해 수행하던 업무가 불가능해지거나 비효율적인 수단으로 대체되는 과정에서 발생하는 손실액인 업무효율의 저하(LoWE), 사이버공격으로 인해 손상된 시스템을 원상태로 회복시키는데 필요한 비용인 시스템 복구비용(CoSR), 침해사고로 인해 손상된 데이터를 복구하거나, 영구히 파괴되어 복구가 불가능한 데이터를 재생산하는데 필요한 비용인 데이터복구비용(CoDR)을 합산하여 계산한다[17].

비밀성이 상실된 경우로는 개인정보유출사건이 대표적이다. 한창희[18]에 의하면 개인정보유출시 총 피해액은 대응인건비, IR대응비용, 고객감소로 인한 수익 손실, 유출된 정보의 가치, 관련산업 파급효과를 합산한 금액으로 설명한다. 또한 김광용[19], 김민정[20]은 개인정보의 유출이 기업의 주식에 미치는 영향에 대하여도 연구하였다.

무결성이 상실된 경우는 은행전산망 마비사건을 들 수 있다. 3.20 사이버침해사건에 의하면 피해대상중 금융기관의 경우 농협은 26,693대의 PC 및 16,121대의 CD·ATM가 침해당해 490억원, 신한은행은 400만원, 제주은행은 1.8억 등 총 534억원의 피해복구비용이 발생하였다.

경제분야 외 피해를 받을 수 있는 분야는 사회·정치분야가 있다. 미국은 대선에서 소셜미디어를 활용하여 정치적 영향력을 확인하였다. 이처럼 소셜미디어는 사회 및 정치적 이미지에 대한 대표적인 지표로 볼 수 있다. 박상민[15]은 한수원 개인정보유출사건이 발생한 후 대한민국의 소셜미디어를 대상으로 빅데이터 분석을 통해 피해기관 및 정부의 긍정·부정 영향력을 측정하였다.

즉, 기존의 피해산출에 관한 연구는 침해사고가 발생하면 기업의 피해를 설명하는 수준이었고 피해재발 방지를 위한 정보보호 투자를 요구하는 자료였다. 하지만 이러한 단순 피해액 산정에 관한 연구는 공격을 통해 공격자가 얻고자 하는 본질적 이득을 설명하기에는 제한된다.

2.4 사이버 공격주체 식별 및 의도분석에 관한 연구

초기의 공격주체 식별은 백신업체에서 주도하였기 때문에 악성코드를 분류하기 위한 연구가 선행되었다. 일반적인 유사도 산출기법의 절차는 정규화, 비교인자 추출, 비교인자 비교, 분석 순서로 진행된다[21]. 유사한 악성코드를 분류하기 위해 가장 중요한 분야는 비교인자를 선별하는 과정이다. 악성코드 내 비교인자 추출방식은 '동적인 추출방식'과 '정적인 추출방식'으로 구분된다[22]. 동적인 비교인자 추출방식은 악성코드를 에뮬레이터로 동작시켜 나타나는 외형적인 부분(파일, URL 등)을 유사도 산출을 위한 비교인자로 사용하는 방식으로 악성코드의 악성코드 API를 기록하여 비교인자로 사용하였다[23]. 정적인 비교인자 추출방식으로 악성코드의 IAT에 있는 API 목록을 추출하여 비교인자로 사용하거나 악성코드에 있는 문자열을 추출하여 비교인자로 활용하였다[24][25].

그 후 APT공격이 증가하며 악성코드의 유사도 분석기법은 공격주체를 식별하기 위한 분석으로 발전하였다. APT유사도 기반 악성코드 분석기법을 활용한 사례로는 3.4 및 7.7 DDoS가 있다. 경찰청의 3.4 DDoS 보도자료에 따르면 악성코드의 유포방법, 해외 공격근원지, 악성코드 설계방식, 악성코드의 통신방식 등이 일치하기에 3.4 DDoS의 공격범이 7.7 DDoS와 동일범으로 결론지었다[26]. 이는 외부와 통신하는 명령구조, 사용하는 IP·URL 등의 외형적인 요소와 악성코드 기능 및 API, 구조 등 내부적인 요소를 종합적으로 비교하여 식별한 것이다.

APT공격이 나날이 정교해지며 기존 악성코드 내 유사도 비교만으로는 정확한 공격주체를 추론할 수 없게 되었다. 이에 공격주체가 남긴 사이버공간의 흔적을 장기간 사례분석 및 네트워크 분석을 진행하여 공격주체를 추적하는 방식으로 발전하였다[27] 하지만 사이버공격의 피해만을 이용한 공격주체 식별 연

구는 공격의도를 추론하고 전략적으로 대응하는데 제한되었다[15].

초기의 동기분석 및 위협분석은 공격자의 기존위협 데이터베이스에 기반을 두고 시계열 분석과 같은 통계분석을 활용하였다. 또한 DDoS 등의 위협에 대응하기 위해 사전에 임계치를 산정하고 임계치에 근접하였는지를 기반으로 예측을 수행하였다. 하지만 이러한 방식은 단편적인 공격에 대한 위협만을 보여주며 위협의 종류가 변화하면 대응하지 못하는 단점이 있다[28]. FireEye는 국가간 사이버 공격의 동기에 대하여 분석하였으며[32], RiskBasedSecurity는 소니픽처스 해킹과 관련하여 피해기반의 의도분석을 진행하였다[33].

III. 본 론

3.1 사이버 공격의도의 영향 요소

Martin Libicki는 '중요한 사이버공격에는 반드시 동기가 있다'라고 하였다[31]. 사이버공간에서 범죄, 테러, 전쟁과 같은 사이버공격이 발생하면 공격을 수행한 주체가 누구인지 신속하게 확인하여야 하며 주체식별을 통해 공격의도를 파악하여야 한다. 하지만 사이버공격을 ID·IP 정보를 기반으로 공격주체 식별 시 사이버공간 익명성에 의해 정확한 주체의 식별 및 의도분석이 제한된다. 또한 사이버공격에는 다양한 의도와 목적이 복합적으로 결합되어 공격의 피해도 복합적으로 나타남에 따라 어려움이 있다.

국가 관점에서 공격의 유형을 효과적으로 판별하기 위해서는 사이버공격으로 발생한 피해를 분석하여야 한다. 사이버공격으로 인해 발생한 피해는 공격자가 바라는 공격대상에게 가장 큰 영향을 줄 것이다. 개인을 대상으로 공격을 준비하였다면 공격의 대상이 되는 개인의 의사결정에 영향을 주도록 공격을 수행할 것이며, 국가를 대상으로 공격을 준비하였다면 국가의 의사결정에 영향을 주도록 공격을 수행할 것이다.

따라서 사이버공격에 대한 공격의도를 추론하기 위해서는 Fig 2와 같이 공격대상을 개인과 국가로 구분하여 공격대상이 개인이라면 개인의 신념, 욕망에 영향을 주려 할 것이며, 공격주체가 국가라면 국가안보 관점에서 정치적, 경제적, 법률적 요소에 영향을 줄 것이다[35].

이 과정에서 공격주체를 식별하기 위해 피해분석 지표는 다양하게 존재할 수 있으나 본 연구에서는 소

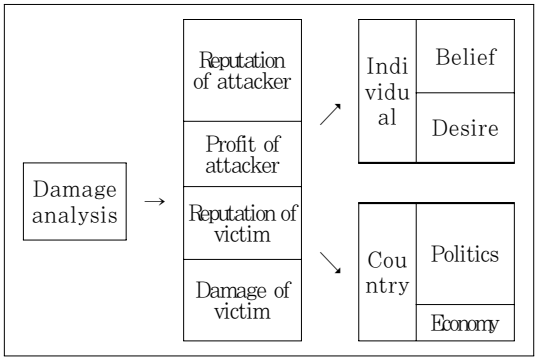

Fig. 2. Elements derived that affect the intention through the analysis of damage

셜미디어 상의 공격자의 명성과 금전적 이익, 피해자의 소셜미디어 상의 명성 및 주식적 손익으로 선정하였다. 공격자가 기술력을 과시하게 위해 디페이스 공격을 수행하면 ①항목인 공격자의 명성에 해당하며, 랜섬웨어로 공격자가 금전적 이익을 원하면 ②항목인 공격자에 이익에 해당한다. 몸캠으로 인한 협박은 ③항목으로 피해자의 명성에 영향을 주기 위함이며, 해킹 후 자료를 삭제하는 것은 ④항목으로 피해자에게 손해를 발생시킨다. ①~④항목을 통해 개인의 신념, 욕망, 정치, 경제에 영향을 분석하여 사이버공격의 대상이 개인인지 국가인지 식별한다.

3.2 사이버 공격유형 분류 모델

사이버공격의 유형은 범죄, 테러, 전쟁으로 분류되며 유형별 대응전략을 수립하여야 한다. Fig 3과 같이 사이버공격이 발생하면 포렌식·역추적을 이용한 기술분석을 통하여 공격주체를 식별한다. 그 후 피해내역 기반의 공격의도를 분석하고 개인 및 국가적 관점에서 공격의도 상호비교를 통해 사이버공격의 유형을 범죄, 테러, 전쟁으로 판별한다.

사이버공격을 의도에 따라 공격주체 및 유형을 추론하면 공격에 대응하기 위한 전략 수립도 효과적이다. 공격의 다양한 의도를 비교하기 위해서는 목적에 도달하기 위해 가장 합리적인 방법을 선택한다는 가설을 선정하고 영향력 비교를 통해 최선의 선택을 유도한다.

예를 들어 한명의 해커가 메일을 활용한 언론사 기자를 대상으로 APT공격을 감행하여 악성코드에 감염시켰다. 만약 개인적 차원에서 언론기자 개인을

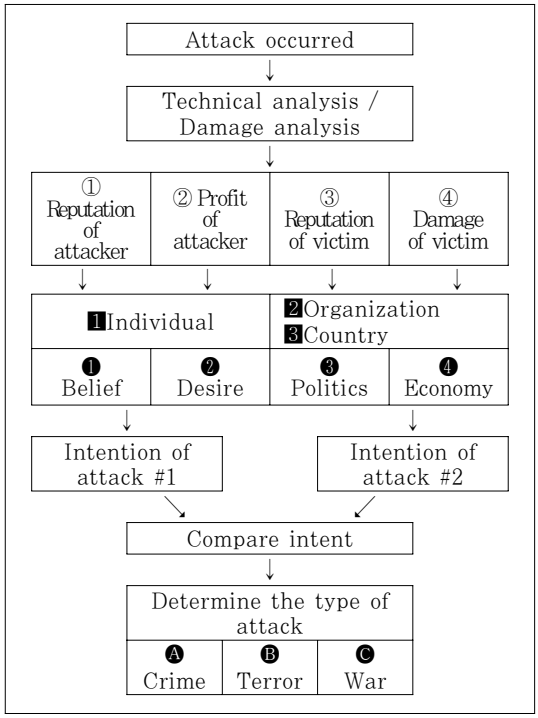

Fig. 3. Model for analysis of the intent of cyber attack

대상으로 공격하였다면 해커는 개인에게 피해를 주기 위해 정보탈위, 자료삭제, 암호화 등의 공격 수행후 금전을 요구할 수 있다. 하지만 국가 및 조직적 차원에서 해킹을 했다면 언론기자의 PC를 허위사실 유포의 매개체로 활용하거나 사칭하여 국가 이미지에 영향을 줄 수 있다. 만약 전자의 상황이라면 범죄로 판단하여 대응하고 후자의 상황이라면 테러 또는 전쟁의 상황으로 대응하여야 한다.

이처럼 악성코드 감염이라는 하나의 시작점이 공격자의 의도에 따라 다양한 방향으로 발전할 수 있으며 시시각각 변화하는 공격의 의도를 확인해야 효율적인 대응전략을 수립할 수 있다.

IV. 제안모델 검증

4.1 의도분석을 위한 실험환경

제안하는 모델에 기반을 둔 사이버공격의 의도 및 동기를 분석하기 위해서는 사회적 지표와 경제적 지표를 산출하여야 한다. 사회적 지표 확인을 위해서는 공개된 소셜네트워크 공간에서 주체에 관련된 자료를 빅데이터 기반으로 수집한 후 수집된 데이터를 대상으로 감성분석을 실시하여 긍정적, 부정적 이미지를 카운트 하였다[15, 34]. 또한 경제적 지표 확인을 위해 기업의 가치를 대표하며 공개된 지표인 주식 정보를 활용하였다[20].

이에 본 논문에서는 객관적인 정보를 얻기 위해 두가지 도구를 이용하였다. 사회적 지표를 얻기 위해 넬리지큐브의 PulseK 서비스를 활용하였으며, 국내외 주식정보를 얻기 위해 Google의 Stock 서비스를 활용하였으며, 두가지 서비스를 활용하여 사이버공격이 발생한 시기의 정보를 조회하였다.

4.2 국내기업 대상 사이버공격

기업을 대상으로 사이버공격이 발생하면 기존의 대응관점은 피해복구에 집중한다. 하지만 사이버공격 피해의 재발을 예방하려면 공격이 발생한 이유 즉 공격의도 확인이 필요하다. 공격자는 피해기관에 개인의 신념·욕망을 표출하거나 정치·경제적 영향의 극대화 방안을 지속적으로 강구할 것이다.

국내에서 발생한 침해사고의 대부분은 피해기관의 자산을 악용하여 사이버공격을 한 경우, 피해기관의 자산이 사이버공격으로 피해 받은 경우, 피해기관의 중요한 자료가 외부로 유출된 경우이다. 그 중 Table 1.과 같이 '14년도에 발생한 4건의 사례를 통해 공격의도를 분석한다.

일반적인 사이버공격의 피해는 ①공격자의 명성 획득 ②개인정보 또는 DDoS 공격으로 공격자의 금전적 이득 획득 ③피해기관의 명성 하락 ④피해기관의 금전적 피해 등으로 나눌 수 있다. 명성은 소셜미디어의 감성분석을 활용하였으며, 대상의 금전적 피

Table 1. Cyber attacks in 2014 (portion)

Date	Damage enterprise	Damage history
'14.11.29	SK Broadband LG U+	DDoS by the device hacking
'14. 7.24	KT	IDC DDoS
'14.10.12	E-MART Inc.	Leakage of personal information - 3,110,000
'14. 7.14	Neungyule Education	Leakage of personal information - 1,040,000

Table 2. Change of stock prices and social media on the occasion of cyber attack

Company	Date	Stock	positiveness	negativeness
SK Telecom	′14.11.26	283,500	56	14
	′14.11.27	280,500	39	11
	′14.11.28	280,500	24	10
	′14.11.29 (Damage)	-	29	232
	′14.11.30	-	11	37
	′14.12.1	285,000	36	21
	′14.12.2	278,000	28	19
	′14.12.3	277,500	24	27
LG U+	′14.11.26	11,300	136	59
	′14.11.27	11,200	123	69
	′14.11.28	10,850	149	37
	′14.11.29 (Damage)	-	83	21
	′14.11.30	-	69	47
	′14.12.1	11,150	133	74
	′14.12.2	10,950	104	57
	′14.12.3	10,950	102	68
KT	′14.7.21	29,750	496	137
	′14.7.22	29,900	463	146
	′14.7.23	29,950	460	125
	′14.7.24 (Damage)	29,800	513	177
	′14.7.25	30,000	690	132
	′14.7.26	-	530	102
	′14.7.27	-	555	76
	′14.7.28	30,750	570	133
E-MART Inc.	′14.10.6	215,000	1,061	184
	′14.10.7	212,500	937	120
	′14.10.8	211,000	877	179
	′14.10.9	-	759	112
	′14.10.10	210,500	941	123
	′14.10.11	-	767	138
	′14.10.12 (Damage)	-	663	135
	′14.10.13	206,500	1,085	173
	′14.10.14	201,000	991	126
	′14.10.15	203,500	1,014	135
Neungyule Education	′14.7.9	3,320	9	0
	′14.7.10	3,365	2	1
	′14.7.11	3,380	6	1
	′14.7.12	-	0	0
	′14.7.13	-	0	1
	′14.7.14 (Damage)	3,375	10	2
	′14.7.15	3,370	9	10
	′14.7.16	3,350	4	4
	′14.7.17	3,350	2	2
	′14.7.18	3,395	3	3

해는 주가정보를 활용하였다.

Table 1.의 사건은 해커가 직접적 등장하지 않았고 신념 및 욕망이 표출되지 않았으므로 ①②의 의도는 없었으며, 소셜미디어 공간에서의 부정적인 영향도 다음날 정상으로 복귀하였으나 ③은 해커의 목적으로 간주할 수 있다. Table 2.는 피해기관의 정보자산이 사이버공격으로 피해 받은 경우로 피해기관의 주식가격은 1~2일 정도 하락하고 영향은 미약하나 ④의 의도로 볼 수 있다. 피해기관의 정보가 외부로 무단 유출된 사건은 피해기관의 주식가격은 5%정도 하락하여 피해가 발생한 경우보다 큰 폭으로 영향을 받으나 동일하게 1~2일 후 정상수준으로 복귀하는 점을 고려할 수 있다.

즉 이러한 유형의 침해사고는 피해기관의 이미지 실추 및 경제적 피해를 발생시키는 것이 목적이 것으로 간주할 수 있다. 同 사이버공격은 개인적 관점에서 신념과 욕망은 없었으나 조직적 관점에서 정치·경제적 손실이 발생했으며 국가적 관점에서 정치·사회적 영향은 미미하였으므로 사이버범죄 유형으로 판별할 수 있다. 이에 해당 국가는 범죄로 진행하였다.

4.3 '14. 소니 픽쳐스 해킹사건

소니 픽쳐스 해킹사건은 GoP(Guardians of Peace)라 지칭하는 해킹그룹에 의해 내부 전산망 마미 및 미개봉 영화 3편이 유출되는 등 최소 2,200억원(NYT)의 피해가 발생한 사건으로 사이버공격이 발생한 상황에서 피해내역은 ①공격자가 명성 ②피해사의 영화 확보 ③피해기관에 명성 하락 ④피해기관의 금전적 피해로 구분할 수 있다.

GoP그룹의 요구사항은 영화 '더 인터뷰'의 상영 금지이며 추가적인 금전을 요구하지는 않은 것으로 보아 ①의 신념적 요소가 있음을 알 수 있다. 또한 영화를 탈취하고 무단으로 제공함으로서 단순히 ②의 목적으로 보기 어렵다. 해킹 후 미국사회 내 소니의 정치적 영향력인 이미지는 해킹으로 인해 변화하지 않아 ③도 목적이 아니다. 하지만 ④의 경제적 지표인 주식가격은 1달 전 28달러에서 19달러로 약 30% 감소하였으며 미상영 영화 다수를 무단으로 공개됨으로써 잠재적 손해가 발생했다.

즉, 공격자 GoP는 ①인 신념을 위해 피해기관의 경제적인 피해를 발생시킨 것인 ④가 GoP의 주요한 목적으로 추론할 수 있다.

동 사이버공격은 개인적 관점에서 신념이 표출되

Table 3. SONY and US stock prices

Monthly (Total)	SNE	DOW	NASDAQ
′14.10.23	28.30	17,646	5,031
′14.11.24 (Damage)	21.63	17,817	4,754
′14.11.25	21.93	17,814	4,758
…			
′14.12.12	20.33	17,280	4,653
′14.12.15	19.72	17,180	4,605
′14.12.16	19.72	17,068	4,547
′14.12.17	20.39	17,356	4,644

었고 조직적 관점에서 경제적 피해가 발생하였으며 국가적 관점에서 정치·사회적 영향 미미하였으므로 사이버범죄로 분류할 수 있다. 참고로 미국은 공격자를 사이버범죄로 국제기관에 고소하였다.

4.4 ’14. 한수원 사이버테러 사고

‘한국수력원자력 사이버테러사고’는 ‘원전반대그룹’이라 자칭하는 해커그룹에 의해 ’14년 12월에서 15년 9월까지 약 10개월간 기밀문서 유출, 원전중단 및 금전을 요구한 사건으로 사이버공격이 발생한 상황의 피해는 ①공격자의 신념인 원전중단 ②공격중단의 금전적 대가 ③피해기관의 명성 하락 ④피해기관의 금전적 손해를 주기 위한 것으로 분류할 수 있다.

공식적인 공격집단인 원전반대그룹의 공격의도는 표면상 원전반대와 내면상 국민분열 유도로 구분할 수 있다. 그리고 핵티비즘적 신념을 목적으로 소셜미디어에서 활동하였다[16].

따라서 ‘원전반대그룹’의 목표가 표면적인 이유라면 SNS에서 활동이 증가할 것이고 활동의 목적은 원전반대그룹을 지지하는 긍정적인 여론을 증가시키는 것이 신념일 것이다. 또한 금전적으로 요구한 원전가동 중지와 100억 달러로 한화 약 10조원에 해당하는 금액은 욕망에 해당된다. 그러나 원전반대그룹의 목표가 내면적인 의도라면 국민이 국가를 불신하도록 소셜미디어에서 활동할 것이며, 국가경제에 위기 및 불안감을 조성해 국가가치를 하락시키려 할 것이다.

공격의도를 확인하기 위해 ①의 신념의 지표로 Table 4.는 ‘원전반대그룹’이 소셜미디어에서 활동한 내용이다. ‘원전반대그룹’은 10개월간 총 1,717건 언급되었으며, 그 중 1,297건은 부정적인 내용임을 알

Table 4. Social media of the opposed group to nuclear power plant

Monthly (Total)	positiveness	negativeness	neutrality	Total
′14.12	85	639	71	795
′15.1	1	32	5	38
′15.2	2	23	1	26
′15.3	28	106	21	155
′15.4	-	1	-	1
′15.5	-	1	-	1
′15.6	-	6	1	7
′15.7	142	271	18	431
′15.8	21	215	24	260
′15.9	-	3	-	3
Total	279	1,297	141	1,717

수 있다. ②의 욕망의 지표로 공격자가 얻을 수 있는 이득은 원전 중단과 100억 달러 이지만 원전이 중단되지 않았고 요구한 금액도 지급하지 않았으므로 해당사항 없다고 볼 수 있다.

공격의 의도가 집단적임을 알기위해 피해자의 소셜미디어의 한수원의 이미지를 확인하면 Table 5. 과 같다. 한수원은 10개월 간 총 12,030건 언급되었으며, 그 중 6,763건은 부정적으로 언급되었다.

경제적으로 미치는 영향력은 대한민국 경제를 대표하는 KOSPI지표로 Table 6. 과 같이 확인할 수 있다. 하지만 ‘원전반대그룹’의 활동은 최초 경제적으로 영향을 주지만 그 후 별다른 영향을 주지는 못한다.

즉 한수원 사이버테러사건에서 ‘원전반대그룹’의 공격의도는 원전중단과 금전요구이지만 원전의 미중단으로 이익은 발생하지 않았으며, 별도로 요구한 100억 달러는 요구만 했을 뿐 실제 획득을 위한 추가 제시가 없었다. 따라서 원전반대그룹은 ③를 목적

Table 5. Social media of Korea Hydro & Nuclear Power Co., Ltd.

Monthly (Total)	positiveness	negativeness	neutrality	Total
′14.12	877	2,869	525	4,271
′15.1	402	552	87	1,041
′15.2	307	450	78	835
′15.3	482	902	113	1,497
′15.4	357	466	72	895
′15.5	225	255	44	524
′15.6	498	480	117	1,095
′15.7	438	429	60	927
′15.8	376	273	88	737
′15.9	102	87	19	208
Total	4,064	6,763	1,203	12,030

Table 6. Domestic stock prices

Monthly (Total)	KOSPI	KOSDAQ
′14.12	1,941	539
′15.1	1,920	577
′15.2	1,961	605
′15.3	2,012	634
′15.4	2,107	685
′15.5	2,114	697
′15.6	2,063	722
′15.7	2,058	753
′15.8	1,952	698
′15.9	1,939	672
Average	2,006.70	658.20

으로 한수원의 국내·외 부정적 이미지를 형성하고 여론분열 조장 및 불안감 조성의 의도를 보인다.

同 사이버공격은 개인적 관점에서 욕망과 신념이 미미하였고 조직·국가적 관점에서 정치·사회적 부정적 영향을 형성되었다. 이에 해당 국가에서는 이를 사이버 테러 또는 전쟁의 영역으로 판별하였다.

V. 결 론

사이버공격이 발생하면 대부분의 해당기관은 피해를 복구하기 위해 노력한다. 하지만 사이버공격의 의도와 유형을 정확히 인식하고 대비하지 않으며 동일한 유형의 피해가 반복적으로 발생할 수 있다.

따라서 사이버공격이 발생하면 기술분석을 통한 주체 식별과 피해분석을 통한 의도분석으로 개인·조직·국가적 관점에서 의도비교를 통해 공격유형을 판별하고자 하였다.

특히 사이버 공격의도를 식별하기 위해 공격자의 명성과 이익 그리고 피해자의 명성과 이익 등 4가지 요소를 소셜미디어상의 이미지와 주식경제 지표상의 손익 등 정치·경제지표를 활용하였고 국내·외 사이버 공격 및 피해사례를 통해 입증하고자 하였다. 소셜미디어와 주식으로 사이버공간의 변화를 모두 해석할 수 없으나 각각 대표적인 지표로 활용됨을 확인하였다.

향후 사이버공간에서 등장하는 다양한 지표에 대하여 연구가 필요하며 해당 지표가 적절한지에 대하여 전문가 델파이 방법 등 다양한 검증이 필요하며, 공격의도 분석의 신뢰도 향상을 위해 정량화 요소를 추가 식별하고, 국가차원에서 공격유형에 따른 효과적 대응전략을 구체화 발전시켜야 한다.

References

[1] Malle, Bertram F., and Joshua Knobe. "Which behaviors do people explain? A basic actor-observer asymmetry." Journal of Personality and Social Psychology 72.2 (1997): 288.

[2] Knobe, Joshua. "Intentional action and side effects in ordinary language." Analysis 63.279 (2003): 190-194.

[3] Wellman, Barry, and Scot Wortley. "Different strokes from different folks: Community ties and social support." American journal of Sociology (1990): 558-588.

[4] Hyeon Jin Lee. "Understanding Desire, Intention, Emotion, and Social Rules in Korean Children." THE KOREAN JOURNAL OF DEVELOPMENTAL PSYCHOLOGY, 22.1 (2009.3): 1-18.

[5] Ju Hwa Park, Kwang Su Cho. "Outcome Determines Intention: Koreans intention and intentionality judgment." THE KOREAN JOURNAL OF COGNITIVE AND BIOLOGICAL PSYCHOLOGY, 26.4 (2014.12): 317-341.

[6] Suler, John R. "Identity management in cyberspace." Journal of Applied Psychoanalytic Studies 4.4 (2002): 455-459.

[7] Kim, Sung-sik, Bae, Jin-ah. "A Study on Classification of SNS Communicators : Focused on the Comparison of Facebook and Twitter." Journal of Cybercommunication Academic Society, 31.4 (2014.12): 97-139.

[8] Gary Stanley Becker and William M. Landes, eds. "Essays in the Economics of Crime and Punishment", National Bureau of Economic Research, 1974

[9] Kshetri, Nir. "The simple economics of cybercrimes." IEEE Security & Privacy 4.1 (2006): 33-39.

[10] Santer, Benjamin D., et al. "A search for

human influences on the thermal structure of the atmosphere." Nature 382.6586 (1996): 39-46.
〔11〕 Lévy, Pierre. Cyberdémocratie. Odile Jacob, 2002.
〔12〕 Yoon Min Jae. "A Study of Political Participation of Netizens: The Case of University Students of Korea." Information Society & Media, .20 (2011.6): 17-48.
〔13〕 Eun Gee Yun. "A Study of the Model of Policy Decision in terms of The Reform's Alternative of National Pension System for the Method of Financial Stability." Korean Public Management Review, 23.1 (2009.3): 231-250.
〔14〕 Ahn Ji-Soo, Lee Won-ji. "Effect of Social Conformity and Individuals' Information Processing Tendencies on Trust in Rumor Messages." Journal of Communication Science, 11.4 (2011.12): 296-320.
〔15〕 Sang-min Park, Kyung-ho Lee, Jong-in Lim. "Strategic Decision Making Model Among Collective Intelligences Using The Game Theory in Cyber Attacks - Case study of KHNP Hacking -." Journal of the Korea Institute of Information Security & Cryptology, 26.1 (2016.2): 237-246.
〔16〕 Choung, Wan. "A Study on Victims and Legal Response against the Internet DDoS Attack" Korean Association of Victimology 18 (2010): 207-228.
〔17〕 Jin Shin. "Economic Analysis on Effects of Cyber Information Security in Korea: Focused on Estimation of National Loss." Journal of the Korea Institute of Information Security & Cryptology, 23.1 (2013.2): 89-96.
〔18〕 Chang Hee Han, Seung Wan Chai, Byung Joon Yoo, Dae Hwan Ahn, Chae Hee Park. "A Quantitative Assessment Model of Private Information Breach." The Jounal of Society for e-Business Studies, 16.4 (2011.11): 17-31.
〔19〕 JeongYeon Kim. "Analyzing Effects on Firms' Market Value of Personal Information Security Breaches." The Jounal of Society for e-Business Studies, 18.1 (2013.2): 1-12.
〔20〕 Min-Jeong Kim, Namgil Heo, Jinho Yoo. "A Study on the Stock Price Fluctuation of Information Security Companies in Personal Information Leakage." Journal of the Korea Institute of Information Security & Cryptology, 26.1 (2016.2): 275-283.
〔21〕 Andrew Walenstein, Arun Lakhotia. "The Software Similarity Problem in Malware Analysis," In Proceedings Dagstuhl Seminar 06301: Duplication, Redundancy, and Similarity in Software, Dagstuhl, Germany, pp. 10 July. 2006.
〔22〕 Kim In kyoung, Im Eul Gyu. "A Study on the Malware Classification using API Call Frequency." Proceedings of Symposium of the Korean Institute of communications and Information Sciences, (2011.2): 943-945.
〔23〕 Q.Miao, Y.Wang, Y.Cao, X.Zhang, Z.Liu, "APICapture - a Tool for Monitoring the Behavior of Malware," Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering, pp. 390-394, August. 2010.
〔24〕 O-chul Kwon, Seong-jae Bae, Jae-ik Cho, Jung-sub Moon. "Malicious Codes Re-grouping Methods using Fuzzy Clustering based on Native API Frequency." Journal of the Korea Institute of Information Security & Cryptology, 18.6A (2008.12): 115-127.
〔25〕 Han, Kyoung-Soo, In-Kyoung Kim, and Eul Gyu Im. "Malware classification methods using API sequence characteristics." Proceedings of the International Conference on IT Convergence and Security 2011. Springer

Netherlands, 2012.
〔26〕 Changwook Park, Hyunji Chung, Kwangseok Seo, Sangjin Lee. "Research on the Classification Model of Similarity Malware using Fuzzy Hash." Journal of the Korea Institute of Information Security & Cryptology, 22.6 (2012.12): 1325-1336.
〔27〕 Wanju Kim, Changwook Park, Soojin Lee, Jaesung Lim. "Methods for Classification and Attack Prediction of Attack Groups based on Framework of Cyber Defense Operations." Journal of KIISE : Computing Practices and Letters, 20.6 (2014.6): 317-328.
〔28〕 Chuvakin, Anton, Kevin Schmidt, and Chris Phillips. Logging and log management: the authoritative guide to understanding the concepts surrounding logging and log management. Newnes, 2012.
〔29〕 Baudrillard, Jean. Société de consommation: Ses mythes, ses structures. Vol. 53. SAGE, 1998.
〔30〕 Simmel, Georg. Philosophie des geldes. BoD - Books on Demand, 2013.
〔31〕 Libicki Martin C, "Conquest in Cyberspace : National Security and Information Warfare." Cambridge University Press, 2007
〔32〕 FireEye, "World War C : understanding nation state motives behind today's advanced cyber attacks", FireEye, 2014
〔33〕 RiskBaseSecurity, "A Breakdown and Analysis of the December, 2014 Sony hack",RiskBaseSecurity, 2015
〔34〕 Min-Jeong Kim, Jinho Yoo,"A Study on the Image and Awareness Change of Corporate and CSR in Personal Information Leakage", 2016 Security Ethics Conference of Korea, Nov.2016
〔35〕 Byoung-Won Min, Cyberattack and Cyber deterrence in International Politics, National strategy, 2015

〈저자소개〉

박 상 민 (Sang-Min Park) 종신회원
1994년 2월: 울산대학교 법학과 졸업
2012년 2월: 고려대학교 정보보호대학원 석사
2016년 8월: 고려대학교 정보보호대학원 박사과정 수료
〈관심분야〉 사이버전, 사이버인식, 사이버정보, 사이버물리, 전략결정 등

임 종 인 (Jong-In Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
현재: 고려대학교 정보보호대학원 및 사이버국방학과 교수, 대검찰청 디지털수사자문위원회 위원장, 국방부 정보화책임관 자문위원, 한국저작권위원회 위원 등
〈관심분야〉 사이버안보, 사이버국방, 정보법학, 디지털포렌식, 개인정보보호 등