Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.6, Dec. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.6.1595

사회공학 사이버작전 분석모델 정립연구*

신 규 용,† 김 지 원, 임 현 명, 김 용 주, 유 진 철‡
육군사관학교 사이버전 연구센터

Building an Analysis Model for Social Engineering Based Cyberspace Operations*

Kyuyong Shin,† Jeewon Kim, Hyun-myung Lim, Yongju Kim, Jincheol Yoo‡
Cyber Warfare Research Center at Korea Military Academy

요 약

최근에는 목표시스템을 직접 공격하던 전통적인 기술적 사이버작전보다는 목표시스템을 관리하는 사람이나 조직의 취약점을 우회적으로 공격하는 사회공학 사이버작전이 늘어가고 있는 추세이다. 이에 따라 사회공학 사이버작전 공격기법의 종류나 사회공학 사이버작전 사례분석 연구는 활발히 진행되고 있으나 사회공학 사이버작전을 효과적으로 분석할 수 있는 사회공학 사이버작전 분석모델에 대한 연구는 거의 없다. 따라서 본 논문에서 우리는 사회공학 사이버작전 수행단계와 사회공학 사이버작전의 대상이 되는 인간의 심리기제 등을 종합적으로 분석해 모형화한 사회공학 사이버작전 분석모델을 제안한다. 제안된 사회공학 사이버작전 분석모델은 사회공학 사이버작전 공격시나리오 작성과 사회공학 사이버작전 사례분석을 위한 기준 틀로 활용할 수 있을 것이다.

ABSTRACT

Recently, there has been an increase in the number of social engineering techniques that indirectly attack the target system administrators or organizational weaknesses rather than the traditional technical cyber attacks that directly attacked the target systems. Accordingly, the type analysis and case study of social engineering techniques are being actively conducted. There has been, however, little effort to derive an analysis model that systematically analyzes social engineering based cyberspace operations. Therefore, this paper aims at building a Social Engineering Based Cyberspace Operations Analysis Model, which can be used as a reference framework for a case study or attack scenario generation of social engineering based cyberspace operations.

Keywords: Social Engineering, Cyberspace Operations, Analysis Model

I. 서 론

전통적으로 조직의 정보통신 시스템과 네트워크에 대한 보안 활동은 기술적 보안에 치중되어 왔으며, 인적 보안은 접근 통제와 출입인원의 검문 및 검색, 그리고 보안규정의 준수 등에 한정되어 왔다. 그러나 최근에는 암호 시스템, 침입탐지 및 침입방지 시스템, 보안 프로토콜, 방화벽, 보안 소프트웨어 등 다양한 사이버 방어기술들을 활용해 목표시스템에 대한 보호가 이루어지므로 기술적인 위협행위만으로 공격목적을 달성하기가 어려워졌다. 이러한 상황에서 세계적인 해커인 케빈 미트닉(Kevin Mitnick)에 의해 처음 소개된 사회공학(Social Engineering)적 공격은 목표시스템을 관리하는 인간의 감정이나 인지적 특성과

Received(08. 24. 2018), Modified(10. 29. 2018), Accepted(10. 29. 2018)
* 본 논문은 2017년 제4284부대(2017MCM0017호)와 2018 육사 사이버전 연구센터의 지원을 받아 연구되었음
† 주저자, kyshin@kma.ac.kr
‡ 교신저자, jyoo@kma.ac.kr(Corresponding author)

같은 심리·사회적 특성을 적절히 공격함으로써 공격의 목적을 달성할 수 있기 때문에 전통적인 기술적 공격의 한계를 뛰어 넘을 수 있는 대체수단으로 각광을 받고 있다. 인간 내면의 심리기제(psychological mechanisms)를 이용한 사회공학 공격기법은 기술적인 침투경로의 확보가 어려워질수록 상대적으로 더욱 증가되어갈 것이다. 이러한 의미에서 우리가 아무리 기술적으로 완벽한 보안시스템을 갖추었다 하더라도 보안을 담당하는 인원들의 심리적 행동이 통제되지 않을 경우 사회공학기법을 활용한 사이버작전(이하, 사회공학 사이버작전)의 희생양이 될 가능성이 높다는 것을 시사해준다[1, 2].

최근 들어 2011년에 발생한 국내의 농협 전산망 사건과 같은 사회공학 사이버작전의 빈도가 증가하고 있는 추세이다. 한 연구결과에 따르면 요즘 발생하고 있는 대부분의 사이버 공격은 패치가 되지 않은 소프트웨어를 대상으로 하는 사회공학 사이버작전이며, 특히 사회공학 사이버작전은 2017년 3분에서 4분기 사이에 그 비중이 74%나 증가될 정도로 가파르게 증가되고 있다[3]. 이와 같이 사회공학 사이버작전의 비중과 중요성이 증가하고 있음에도 불구하고 최근 연구들은 사회공학 사이버작전 개념연구[2], 공격기법 연구[4], 사례분석 및 빈도연구[3, 4] 수준에서만 이루어지고 있다. 즉, 사회공학 사이버작전이 수행되는 전체적인 전개 과정에 대한 심도 있는 분석이 이루어지기 보다는 부분적인 측면에서 사례들을 기술하거나 사건보도 식의 소개에 그치고 있는 실정이다. 이러한 측면에서 사회공학 공격기법을 활용한 공격과 방어에 대한 체계적인 분석이나 모델링은 아직까지도 개척상태에 머물고 있다고 보아야 할 것이다.

이에 본 논문에서 우리는 사회공학 사이버작전 수행단계와 사회공학 사이버작전의 대상이 되는 인간의 심리기제 등을 종합적으로 분석해 모형화한 사회공학 사이버작전 분석모델을 제안하고자 한다. 제안하는 사회공학 사이버작전 분석모델은 사회공학 사이버작전의 작용 메커니즘(mechanism)을 쉽게 이해할 수 있도록 안내해 주는 일종의 프레임 역할을 수행하며, 다양한 사례들을 분석하는 준거의 틀로서 활용될 수 있기 때문에 매우 의미가 있다. 또한 경우에 따라서는 사회공학 사이버작전 공격 시나리오를 작성하기 위한 참조모델로 활용될 수도 있을 것이다.

본 논문은 다음과 같이 구성되어 있다. Ⅱ장에서는 사회공학 사이버작전에 대한 개념 및 수행단계에 대해 소개하고, Ⅲ장에서는 사회공학 사이버작전 수행단계에서 인간의 취약점을 공격하기 위해 활용되는 심리기제들에 대해 살펴본다. Ⅳ장에서는 Ⅱ장 및 Ⅲ의 사이버작전 수행단계와 심리기제를 종합적으로 모형화하여 사회공학 사이버작전 분석모델을 정립한 뒤 활용방안을 제시하고, Ⅴ장에서는 사회공학 사이버작전 분석모델을 활용한 사례분석 결과를 제시한다. 마지막으로 Ⅵ장에서는 본 연구에 대한 결론을 맺고, 향후 연구방향에 대해 논의한다.

Ⅱ. 사회공학 사이버작전의 개념

이번 장에서는 먼저 사회공학 기법의 정의 및 종류에 대해 살펴본 뒤 사회공학 사이버작전의 개념 및 수행단계에 대한 기존연구들[1-4]을 통해 개괄적으로 살펴보기로 한다.

2.1 사회공학(social engineering) 기법의 개념

사회공학 기법이란 인간을 속여 공격 행위자가 원하는 목표를 달성하는 심리적 기법을 말한다. 즉, 상대방이 민감한 정보를 누설하게 하거나, 정보의 보안경계(security perimeter)를 효과적으로 우회하기 위한 방법들의 통칭이라 할 수 있다[2]. 이러한 사이버작전에서 사회공학 공격은 주로 공격을 준비하는 단계에서 이루어지며, 목표시스템의 정보를 수집하기 위한 수단으로 활용된다. 따라서 일단 목표시스템 침입에 성공한 뒤에는 전통적인 기술적 사이버작전을 이용해 목표를 달성할 수 있다.

2.2 사회공학 기법의 종류

사회공학 기법은 크게 물리적 방략, 사회적 방략, 기술적 방략, 그리고 혼합 방략으로 구분할 수 있다. 이때 물리적 방략에는 도청(eavesdropping), 어깨너머로 훔쳐보기(shoulder surfing), 쓰레기통 뒤지기(dumpster diving) 등이 있고, 사회적 방략에는 설득(persuasion), 프리텍스팅(pretexting), 보상(quid pro quo), 역사회공학(reverse social engineering) 등이 있으며, 기술적 방략에는 피싱(phishing), 스미싱(smishing), 스피어 피싱(spear phishing), 웨일링(whaling), 파밍(pharming), 베이팅(baiting), 워터링 홀(watering hole) 등이 있다. 마지막으로 혼합 방략에는 테일 게이팅(tailgating)과 비싱(vishing) 등이 있다[1-3].

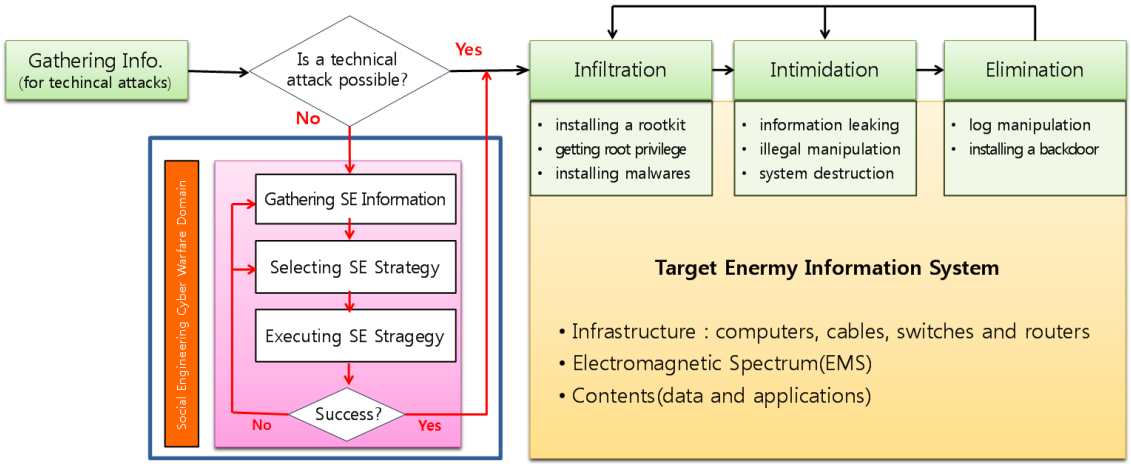

Fig. 1. The Concept and Procedure of Social Engineering based Cyberspace Operations[2, 15].

2.3 사회공학 사이버작전 개념

사회공학 사이버작전은 목표시스템의 직접적인 공격보다는 그것을 관리하는 사람의 취약점을 공격해 우회적으로 목표시스템에 침입하는 공격이라 정의할 수 있다. Fig.1.에서 보듯이 사회공학 사이버작전은 주로 기술적인 사이버작전이 불가능하거나 실패했을 때 활용된다. 최근에는 보안 및 암호기술의 발달로 컴퓨터 시스템과 네트워크에 대해 다중 방어되어 있기 때문에 상대적으로 취약하다고 할 수 있는 시스템 관리자 및 사용자를 공격하는 양상으로 변화하게 되었다[2, 15].

2.4 사회공학 사이버작전의 수행단계

사회공학 사이버작전은 목표시스템을 관리하는 사람 및 조직의 취약점을 이용해 목표시스템에 침입하는 작전이다. 그러므로 목표시스템 접근에 성공하면 그 목표를 달성하게 되는 것이다. 이때 목표시스템에 침입하기 위해서 사회공학 사이버작전은 Fig.1.에서 보는 바와 같이 사회공학 정보수집(Gathering SE Information) 단계, 사회공학 방략선택(Selecting SE Strategy) 단계, 사회공학 방략실행(Executing SE Strategy) 단계 순으로 수행된다. 이때 기존의 연구[14]를 살펴보면 사회공학 사이버작전이 정보수집, 관계형성, 관계이용, 실행 순으로 수행된다고 가정하기도 한다. 하지만 이러한 경우 불특정 다수를 대상으로 하는 피싱 공격과 같이 직·간접적인 관계형성 없이 이루어지는 사회공학 공격에 대한 설명이 어렵다. 따라서 본 논문에서는 사이버전 공격단계를 사회공학 정보수집, 사회공학 방략선택, 그리고 사회공학 방략실행 단계로 구분하고, 각 단계별로 피공격자의 반응과정에서 나타날 수 있는 심리적인 영향요소들을 전반적으로 고려하고자 한다. 즉, 사회공학 사이버작전은 사람을 대상으로 하는 작전이기 때문에 모든 단계에 걸쳐 다양한 심리기제가 활용될 수 있고, 이러한 사회공학 사이버작전 심리기제가 사이버작전의 핵심이라 할 수 있다. 사회공학 사이버작전 심리기제에 대해서는 Ⅲ장에서 자세히 살펴보기로 한다.

2.4.1 사회공학 정보수집(Gathering SE Information)

정보수집 단계는 목표시스템 침입에 필요한 정보를 획득하기 위해 관련자 및 조직에 대한 정보를 수집하는 단계이다. 이때 사회공학 정보는 조직요소(시설, 문화 등), 개인요소(일정, 대인관계, 신상, 업무, 사회현안 등), 접촉요소(개인성격, 동기 그리고 물리적 접촉 여부 등)를 포함한다. 이때 초기 단계에는 공개된 정보를 주로 활용하고, 이후에는 사회공학 방략선택 및 사회공학 방략실행 단계를 통해 획득된 정보들을 포함해 활용한다.

2.4.2 사회공학 방략선택(Selecting SE Strategy)

사회공학 정보수집 단계를 통해 공격하고자 하는 목표시스템 사용자나 관리자의 취약점을 발견되면 그 취약점을 가장 효과적으로 공략할 수 있는 사회공학 공격

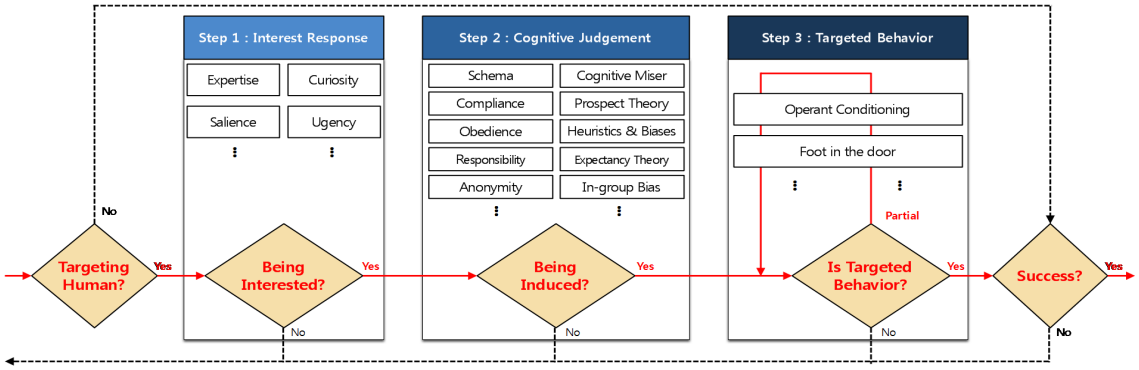

Fig. 2. Psychological Mechanisms for Social Engineering Based Cyberspace Operations

기법(즉, 방략)을 선택하게 되는데 이 단계가 사회공학 방략선택 단계이다. 이때 선택할 수 있는 사회공학 방략에는 앞서 2.2절에서 살펴본 바와 같이 물리적, 사회적, 기술적, 혼합 방략 등 다양하다. 이때 사회공학 방략선택 단계에서는 사회공학 정보수집단계에서 파악된 사용자나 관리자의 취약점을 가장 효과적으로 공략할 수 있는 방략을 선택하여야 한다.

2.4.3 사회공학 방략실행(Executing SE Strategy)

사회공학 방략실행 단계는 사회공학 방략선택에서 선정한 사회공학 공격기법 효과적으로 실행하는 단계이다. 이때 사회공학 방략이 효과적이기 위해서는 공격대상의 사용자나 관리자의 관심을 유도한 후 결심과 행동으로 이행할 수 있도록 심리기제를 적절히 활용해야 한다. 만약 선택된 방략을 실행하여 시스템 침입이 성공하거나 침입에 필요한 충분한 정보(예 관리자 패스워드)를 획득한 경우 성공으로 간주한다. 반대로 방략을 실행하여 필요한 정보를 획득하지 못했을 경우 실패로 간주되어 사회공학 정보수집 혹은 사회공학 방략선택 단계로 되돌아간다.

III. 사회공학 사이버작전 심리기제 분석

앞서 2.2절에서 살펴본 바와 같이 사회공학 방략에는 물리적, 사회적, 기술적, 그리고 혼합 방략 등 다양한 방략들이 존재한다. 이중에서 쓰레기통 뒤지기 등과 같은 일부 물리적 방략의 경우는 직접적으로 사람을 대상으로 하지 않기 때문에 별도의 심리기제가 필요하지 않다. 하지만 대부분의 사회공학 방략들은 사람을 대상으로 하기 때문에 다양한 심리기제를 활용해 대상을 속이거나 설득함으로써 목표시스템에 접근할 수 있는 정보를 유출하게 만들어야 한다. 이때 사람으로 하여금 특정한 행위를 하도록 만들기 위해서는 일반적으로 위 Fig. 2에서 보는 것과 같이 ① 관심반응(Interest Response) 단계, ② 인지적 판단(Cognitive Judgement) 단계, 그리고 ③ 목표행동(Targeted Behavior) 단계를 거치게 되고, 각 단계마다 다양한 심리기제들이 활용될 수 있다. 이때 명심할 것은 본 논문에서 Fig. 2의 각 단계에 제시하고 있는 심리기제들은 가장 효과적일 것으로 예상되는 심리지제들의 예시이므로 경우에 따라 다른 심리기제들이 추가로 활용될 수 있다.

3.1 관심반응 단계 : 관심반응 심리기제

관심반응 단계는 대상이 공격자가 의도적으로 제공한 특정정보에 관심을 갖고 주의를 기울이게 하는 단계이다. 특정정보에 대한 관심은 인지적 판단 과정을 통해 목표행동을 유발하는 출발점이 된다는 면에서 중요하다. 이때 Fig.2.에서 보는 바와 같이 관심반응 단계에서 작용하는 관심영향 심리기제에는 전문성, 현저성, 호기심, 급박성 등이 있다.

첫째, 전문성(expertise)은 제공된 정보가 대상의 전문 분야와 일치하고 양질의 정보로 인식될수록 관심을 기울일 가능성이 높아지는 것을 의미한다. 둘째, 현저성(salience)은 정보의 색, 크기, 선명도, 움직임 등이 현저한 자극일수록 관찰자의 주의를 끄는 힘이 더 강한 것을 뜻한다. 셋째, 호기심(curiosity)은 제공된 정보가 유명인, 금전적 이익, 성(性) 관련 내용과 같이 호기심을 유발하는 내용일수록 관심을 가질 가능성이 높아지는 것을 의미한다. 마지막으로, 급

박성(urgency)은 '긴급'이라는 머리말이 포함되거나, 접근기한 및 처리기한이 한정된 정보와 같이 반응의 급박함을 강조하는 정보에 대해 주의를 기울일 가능성이 더 높아진다는 개념이다.

3.2 인지적 판단 단계 : 인지판단 심리기제

인지적 판단 단계는 관심반응 단계의 과정을 통해 특정 정보에 관심을 갖게 된 대상이 그 정보와 관련된 행동을 취할 것인지를 인지적으로 판단하는 단계이다. 이때 Fig.2.에서 보는 바와 같이 인지적 판단 단계에서 작용하는 인지판단 심리기제에는 도식, 응종, 복종, 책임감, 익명성, 인지절약, 전망이론, 추단과 편향, 전망이론, 내집단편향 등이 있다[1].

먼저, 도식(schema)이란 정보를 체제화하고 해석하는 인지적 개념이나 틀을 의미하는데, 사람은 모든 정보를 자신의 도식으로 판단하는 경향이 있다[5]. 둘째, 응종(compliance)이란 자신이 좋아하지 않는 요청이라도 요구받은 요청과 동일한 행위를 수행하는 것을 말한다. 셋째, 복종(obedience)은 상대방의 권위나 권력 때문에 상대방의 요청에 따르는 것이다. 넷째, 책임감(responsibility)은 책임의 분산 정도에 따라 행위에 대한 적극성이 달라지는 것을 말한다[6]. 다섯째, 익명성(anonymity)은 특정 행위를 한 사람이 누구인지 드러나지 않는 상황에서 일탈행위가 증가하고 사회적 문제가 더욱 빈번히 일어나는 현상을 의미한다[7] 여섯째, 인지절약(cognitive miser)은 사람은 누구나 복잡하고 노력을 요하는 방법보다는 단순하고 노력을 덜 기울이는 방법으로 문제를 해결하려는 경향이 있음을 의미한다[8]. 일곱째, 전망이론(prospect theory)은 사람들은 위험을 수반하는 불확실한 상황에 처하게 되면 합리적인 선택을 하지 못한다는 것을 나타낸다[9]. 여덟째, 추단과 편향(heuristics and biases)은 사람은 인지능력의 한계 내에서 효율적인 빠른 정보처리를 위해 정확성의 일부를 포기하는 경향을 보인다는 의미이다[10]. 아홉째, 전망이론(expectancy theory)은 개인은 결과에 대한 기대의 강도와 결과에 대한 가치 예상에 따라 행동한다는 개념이다[11]. 마지막으로, 내집단 편향(in-group bias)은 동일한 집단에 속한다고 믿는 사람에 대해 보다 긍정적으로 평가하거나 신뢰하는 경향을 의미한다[12].

1) 본 논문의 사회공학 사이버작전 심리기제는 기존의 사이버작전 사례분석을 통해 식별된 인지판단 심리기제들만을 포함하고 있다. 하지만 제도(규제), 규범, 모방 압력과 같은 사회학적 관점에서의 영향요소들도 추가될 수 있을 것이다.

3.3 목표행동 단계 : 행동강화 심리기제

목표행동 단계는 인지판단 단계를 통해 특정 정보와 관련된 행동을 취하기로 결정한 개인이 그것을 실행에 옮기는 단계이다. 이때 피해자가 단번에 공격자가 원하는 행동을 함으로써 공격자가 목표시스템에 접근할 수 있는 정보를 획득한 경우에는 별도의 심리기제가 작동하지 않는다. 하지만 피해자로 하여금 단번에 목표행동을 하도록 하는 것은 현실적으로 매우 어렵다. 이러한 경우 피해자로 하여금 최초의 행동 이후 추가적인 행동들을 하게 함으로써 궁극적으로 목표행동을 이끌어내야 하는데 이때 필요한 것이 행동강화(behavior reinforcement) 심리기제이다. 이때 Fig. 2에서 보는 바와 같이 행동강화 심리기제에는 조작적 조건형성과 문간에 발 들여 놓기 등이 있다.

조작적 조건형성(operant conditioning)은 특정 행동의 확률을 증가시키기 위해 원하는 행동을 할 경우 보상을 주고, 특정 행동의 확률을 감소시키기 위해 원하지 않는 행동을 할 경우 벌을 줌으로써 특정 행동의 확률을 조절하는 것이다[13]. 문간에 발 들여놓기(foot in the door)는 응종의 한 방법으로, 쉬운 부탁 후에 이를 들어줄 경우 점점 더 어려운 부탁을 하여 이를 들어달라고 요구하는 것이다. 설문조사에서 처음에는 간단한 문항으로 시작하여 점점 구체적인 민감한 정보를 요구하는 것이 이에 해당할 수 있다.

IV. 사회공학 사이버작전 분석모델 정립 및 활용

이번 장에서는 사회공학 사이버작전 분석모델을 제안하고, 제안된 모델을 활용해 사회공학 사이버작전 공격을 분석하는 방법론을 제시한다.

4.1 제시하는 사회공학 사이버작전 분석모델

앞서 Ⅱ장 및 Ⅲ장에서 설명한 바와 같이 사회공학 사이버작전은 사회공학 정보수집 단계, 사회공학 방략선택 단계, 사회공학 방략실행 단계를 거쳐 수행되는데, 특히 방략 실행 단계에서 다양한 심리기제들이 활용된다. 이러한 상황에서 사회공학 사이버작전을 효과적으로 분석하기 위해서는 각 단계에서 활용되는 요소, 기법, 기제 등을 포괄할 수 있는 분석모델이 필요하다. 이때 사회공학 사이버작전 분석모델은 사회공학 정보수집 단계에서 정보수집의 대상이 되는

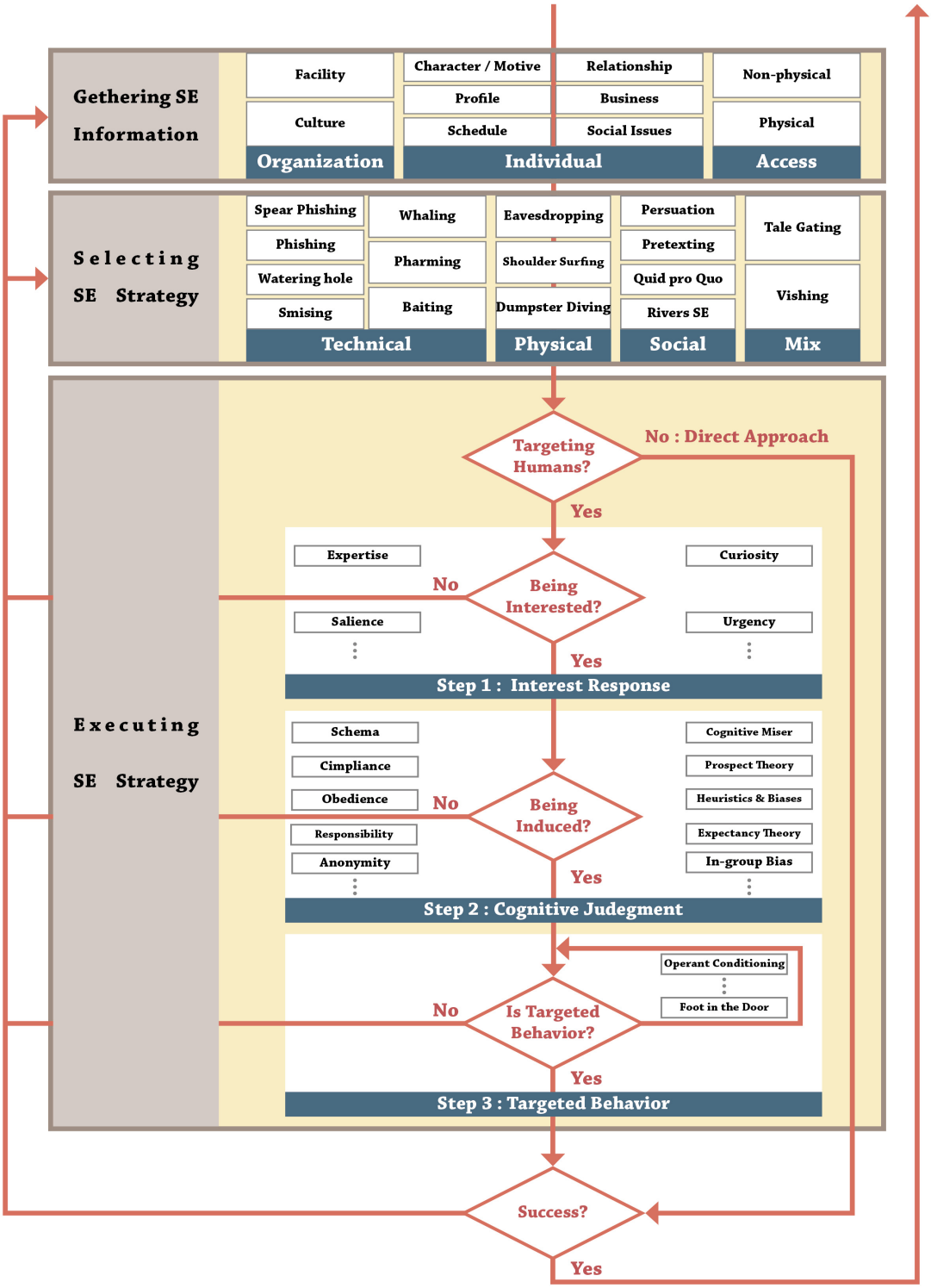

Fig. 3. The Proposed Analysis Model for Social Engineering based Cyberspace Operations

조직 및 개인 요소와 물리적인 접촉 여부를 포함해야하고, 사회공학 방략선택 단계에서는 사회공학 방략으로 활용될 수 있는 물리적 방략, 사회적 방략, 기술적 방략, 혼합 방략을 포두 포함해야 하며, 마지막으로 사회공학 방략실행 단계에서는 관심반응, 인지적 판단, 그리고 목표행동 단계 및 각 단계별로 동작하는 심리기제들을 포괄하여야 한다. 위와 같은 내용들을 포괄해 만들어진 사회공학 사이버작전 분석모델은 Fig.3.에서 보는 바와 같으며, 사회공학 사이버작전 (공격) 각 단계별로 분석해야 하는 내용은 다음과 같다.

4.1.1 사회공학 정보수집(Gathering SE Information)

앞서 2.4.1항에서 설명했듯이 사회공학 정보수집 단계에서의 정보수집은 목표 시스템에 접근하거나 그에 필요한 정보를 획득하기 위하여 조직 및 관련 구성원의 정보를 수집하는 과정을 의미한다. 이때 정보수집을 위해서는 2개의 조직 요소(시설요소, 문화요소), 6개의 개인 요소(개인성격/동기, 개인 신상, 개인 일정, 대인관계, 업무내용, 사회현안), 2개의 접근요소(물리적 접촉, 비(非)물리적 접촉)를 고려하여야 한다. 따라서 사회공학 사이버작전 공격이 발생하였을 경우 정보수집 단계에서는 위 요소들 중 어떤 요소들을 목표로 했는지를 중점적으로 분석해야 한다.

4.1.2 사회공학 방략선택(Selecting SE Strategy)

앞서 2.4.2항에서 설명했듯이 사회공학 방략선택이란 정보 수집 단계에서 얻어진 정보를 바탕으로 취약 대상을 공략하여 목표 시스템에 접근하거나 그에 필요한 정보를 획득할 목적으로 가장 효과적이라고 판단되는 사회공학 방략을 선택하는 것이다. 이때 선택할 수 있는 사회공학 방략에는 2.2절에서 살펴본 바와 같이 물리적, 사회적, 기술적, 그리고 혼합 방략 등 매우 다양한데, 사회공학 사이버작전 공격이 발생하였을 경우 해당 공격이 어떤 방략에 해당하는 지를 분석해야 한다.

4.1.3 사회공학 방략실행(Executing SE Strategy)

앞서 2.4.3항에서 설명했듯이 사회공학 방략실행이란 사회공학 정보수집과 사회공학 방략선택 단계를 거쳐 선정된 사회공학 방략을 실제로 실행해 목표시스템에 접근하거나 그에 필요한 정보를 획득하는 것을 의미한다. 이때 Ⅲ장에서 보는 바와 같이 사회공학 방략실행 단계는 관심반응 단계, 인지적 판단 단계, 그리고 목표행동 단계를 거치게 되고, 각 단계마다 다양한 심리기제들이 활용된다. 따라서 사회공학 사이버작전 공격이 발생하였을 경우 각 단계별로 어떤 심리기제가 활용되었는지 분석하여야 한다.

4.2 사회공학 사이버작전 분석모델 활용

이번 절에서는 Fig.3.의 사회공학 사이버작전 분석모델을 활용해 사회공학 사이버작전 공격을 분석하는 방법을 제안한다. 이때 분석 대상은 2016년에 북한의 4차 핵실험 직후에 발생했던 “국가기관 등 사칭 이메일 발송사건”이다.

4.2.1 사회공학 사이버작전 공격 개요

2016년 1월 13일과 14일, 청와대, 외교부, 통일부를 사칭해 북한 4차 핵실험에 대한 의견을 개진해 달라고 요청하는 이메일이 정부기관과 국책연구기관에 대량으로 발송되었다. 해당 공격은 먼저 피해자에게 악성코드가 첨부되어 있지 않은 일반 이메일을 보내 안심시킨 후 수신자가 해당 메일에 대해 답장을 하는 등 반응을 보이면 악성코드가 첨부되어 있는 메일을 보내 감염을 유도하였다. 이와 관련해 경찰은 압수수색을 통해 확보한 이메일에 첨부된 문서 66개를 ‘한국인터넷진흥원(KISA)’과 공동으로 정밀 분석한 결과, 그중 20개의 파일에서 정보를 유출하는 기능을 가진 악성코드를 발견하였다[2].

4.2.2 사회공학 정보수집 단계 분석

위 공격의 목적은 북한 관련 기관 및 종사자들의 컴퓨터를 해킹해 중요정보를 빼내려는 것으로 추측된다. 이를 위해 공격자들은 사회공학 정보수집 단계에서 청와대, 외교부, 통일부 등 업무 연관성이 높은 국가기관 종사자들 대상으로 그들의 “대인관계”에 대한 정보를 중점적으로 수집하였다. 또한 그들을 공격하기 위해 그들이 관심을 가질 수 있는 “업무내용”(북한)과 적시성 높은 “사회현안”(북한의 4차 핵실험) 등에 대한 정보를 수집하였다. 마지막으로 공격대상에 대한 접촉은 직접적인 접촉보다는 이메일을 활용한 “비물리적인

2) http://goitgo.tistory.com/38

접촉"을 선택해 이메일 정보 확보에 주력하였다.

4.2.3 사회공학 방략선택 단계 분석

위 공격의 경우 사회공학 정보수집 단계에서 획득한 국가기관 종사자들의 이메일 주소를 활용해 "스피어 피싱" 공격을 수행하였다. 이때 단순한 스피어 피싱보다는 최초에는 악성코드가 첨부되어 있지 않은 일반 이메일을 보내 안심시킨 후 수신자가 해당 메일에 대해 답장을 하는 등 반응을 보이면 악성코드가 첨부되어 있는 메일을 보내 감염을 유도하는 "투트랙 스피어 피싱" 방략을 선택하였다.

4.2.4 사회공학 방략실행 단계 분석

관심반응 단계에서 공격자들은 북한 4차 핵실험('16. 1. 6) 직후 "대북정책관련 긴급 설문조사", "청와대 외교안보실입니다.(4차 핵실험 관련)" 등과 같이 "전문성"과 "현저성"이 높은 문구를 선정하여 피해자들의 관심을 유발하였다. 또한 인지적 판단 단계에서는 북한 관련 기관 및 해당 기관 종사자들의 특성을 고려해 권위 있는 국가기관을 사칭함으로써 수신자가 "도식" 및 "복종"의 심리기제를 통해 메일을 열람하도록 유도하였다. 마지막으로 목표행동 단계에서는 피해자로 하여금 한 번에 원하는 행동을 하도록 유도하는 것이 아니라 첫 메일을 통해 상대방에게 안심을 주고 두 번째 메일 및 첨부된 파일을 의심 없이 열어보도록 유도하는 "문간에 발 들여놓기(foot in the door)" 심리기제를 활용하였다.

4.2.5 사회공학 사이버작전 분석결과

위와 같이 사회공학 사이버작전 분석모델(Fig.3)을 활용해 "국가기관 등 사칭 이메일 발송사건"을 분석한 결과는 Fig.4.에서 보는 바와 같다. 결과에서 보듯이 해당 공격은 사회공학 정보수집 단계에서 "대인관계", "업무내용", "사회현안", "비물리적 접촉 방법(즉, 이메일)" 등에 대한 정보를 획득 한 후 사회공학 방략으로 스피어 피싱을 선택하였다. 또한 스피어 피싱에 대한 성공 확률을 높이기 위해 관심반응 단계에서는 "전문성"과 "현저성" 심리기제를 활용하였고, 인지적 판단 단계에서는 "도식"과 "복종" 심리기제를 활용하였으며, 목표행동 단계에서는 "문간에 발 들여놓기" 심리기제를 활용하였음을 확인할 수 있다.

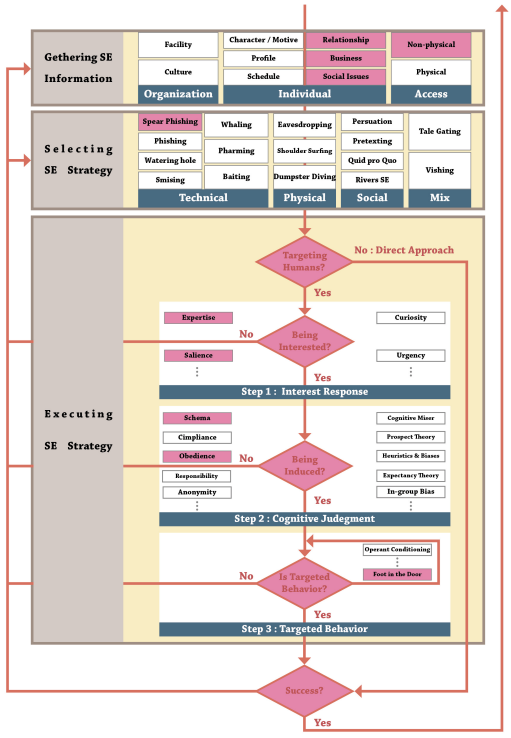

Fig. 4. Analysis Results (Example)

Fig.4에서 보듯이 본 논문에서 제안한 사회공학 사이버작전 분석모델을 활용하면 각 단계별로 사용된 정보획득 요소, 사회공학 방략, 그리고 심리기제들 일목요연하게 식별할 수 있기 때문에 사회공학 사이버작전을 체계적으로 분석할 수 있는 장점이 있다.

V. 제안한 분석모델을 활용한 사례분석 결과

이번 장에서는 앞서 Ⅳ장에서 제안한 사회공학 사이버작전 분석모델을 활용해 최근에 발생한 사이버작전 사례들을 분석한 결과를 제시한다.

5.1 사회공학 사이버작전 공격 분석 대상

본 논문에서 우리는 2007년부터 2017년까지 발생한 북한 관련 사례, 국내 사례, 해외 사례를 포함해 총 40건의 사회공학 사이버작전 공격(해킹)사례들을 분석하였다. 이때 분석대상은 주로 인터넷을 통해 검색하였으며, 가능한 최신 사회공학 사이버작전 사례를 반영하기 위해 대부분 2년 이내의 사회공학 사이버 공격들을 분석 대상으로 한정하였다[2]. 이때 북한

관련 사례는 ADEX 방위산업체 해킹, 청와대 사칭 문자메시지, 인터파크 개인정보 해킹 등과 같이 북한에 의한 공격으로 확인된 또는 추정되는 사례들이고, 국내 사례는 입사지원서 위장 악성코드 공격, 파워 블로거 대상 공격 등과 같이 국내에서 공공기관, 민간기업, 개인 등을 대상으로 발생한 사례들이며, 마지막으로 해외 사례는 달라이라마 컴퓨터 해킹, 왓츠앱 사기 등과 같이 해외에서 공공기관(군 포함), 민간기업, 개인 등을 대상으로 발생한 사례들이다.

5.2 사회공학 사이버작전 공격 분석 결과

이번 장에서는 앞서 5.1장에서 언급한 40개의 사회공학 사이버작전 공격사례들을 다양한 측면에서 분석한 결과를 제시한다.

5.2.1 연도별 사례

먼저 Fig.5.는 2007년도부터 2017년까지 연도별 사회공학 사이버작전 공격의 발생 빈도를 보여준다.

결과에서 보듯이 사회공학 사이버작전은 시간이 지남에 따라 발생빈도가 증가하고 있음을 알 수 있다. 특히 전체 공격 사례 중 반이 넘는 24개의 공격이 2016년과 2017년에 걸쳐 발생했다는 사실에 비추어보면 향후 사회공학 사이버작전 공격은 급격히 증가할 것으로 예상된다.

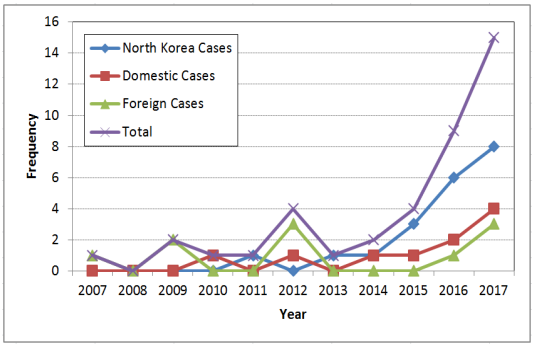

Fig. 5. The frequency per year of the attacks

5.2.2 사회공학 정보수집 분석 결과

다음으로는 Fig.6.은 사회공학 사이버작전 수행을 위해 수집한 정보요소에 대한 분석결과이다.

결과에서 보듯이 조직요소(문화요소와 시설요소)에 대한 정보수집 비중은 상대적으로 높지 않은 반면 개인요소에 대한 정보수집이 높은 편이었다. 특히 개인요소에 대해서는 대인관계(48%), 업무내용(43%), 사회현안(38%) 순으로 정보수집의 비중이 높음을 알 수 있다. 이때 정보수집 대상에 대한 직접적인 접촉은 피한 채 간접적인 방법으로 정보를 수집하였다. 이러한 점에서 사회공학 사이버작전 정보수집은 직접 접촉은 피하면서 공격대상의 인간관계 및 사회적 관계 그리고 사회 현안 등의 관심사를 주요 목표로 정보를 수집하는 것으로 나타났다.

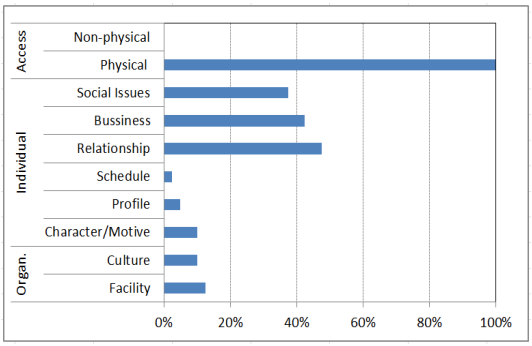

Fig. 6. The information collected by the attacks

5.2.3 사회공학 방략선택 분석 결과

다음으로는 Fig.7.은 사회공학 방략들 중에서 어떤 방략들이 주로 사용되고 있는지에 대한 결과를 보여준다.

결과에서 보듯이 사회공학 사이버작전 수행 시 가장 많이 활용되는 방략은 스피어 피싱(46%), 피싱(22%), 스미싱(12%) 순이었다. 또한 이들은 모두 기술적인 방략으로서 물리적 방략, 사회적 방략, 혹은 혼합방략 등의 사례는 확인되지 않았다.

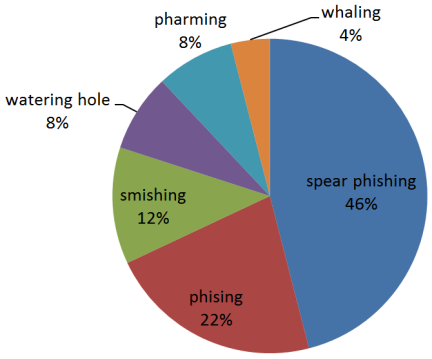

Fig. 7. The ratio of SE strategy

물론 본 논문에서 다루는 사례들은 인터넷 기사를 통해 수집되었기 때문에 다른 종류의 방략들이 사용되고 있지 않다고 결론을 내릴 수는 없지만 기술적인 방략, 그중에서도 스피어 피싱과 피싱이 가장 많이 활용되고 있음을 확인할 수 있다. 이는 Fig.6.에서 언급했듯이 사회공학 사이버작전의 목표가 주로 사람이라는 점과 무관하지 않다. 즉, 사람을 대상으로 하기 때문에 사람에게 더 효과적이라 판단되는 스피어 피싱을 선호했다고 볼 수 있다. 따라서 조직의 관리자들은 조직원들에게 스피어 피싱의 원리를 이해시키고, 그에 대한 대처방법을 주기적으로 교육함으로써 피해를 최소화하려는 노력을 기울일 필요가 있다.

5.2.4 사회공학 방략실행 분석 결과

마지막으로 Fig.8.은 사회공학 사이버작전 수행간 활용된 심리기제의 빈도분석 결과를 보여준다. 결과에서 보듯이 관심반응 단계에서는 전문성(37%), 호기심(28%), 급박성(22%), 현저성(13%)이 대체로 골고루 활용되고 있음을 알 수 있다. 인지판단 단계에서는 주로 도식(38%)과 전망이론(36%)이 활용되었으며, 목표행동 단계에서는 문간에 발 들여놓기(83%)를 통해 피해자가 목표행동을 할 때까지 행동을 강화하는 심리기제로 많이 활용되고 있다는 사실을 알 수 있다. 이와 같은 사회공학 심리기제는 주로 사람의 신뢰를 높이기 위한 방법으로 활용된다고 볼 수 있다.

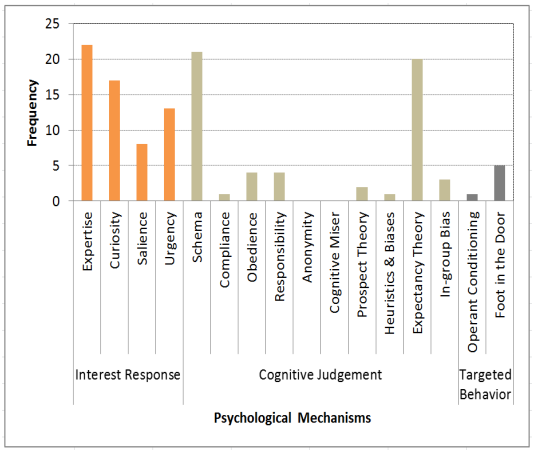

Fig. 8. The frequency of the psychological mechanisms used in the attacks

VI. 결론 및 향후 연구방향

최근 사회공학을 활용한 사이버 공격이 급격히 증가되고 있는 상황에서 사회공학 사이버작전에 대한 체계적인 분석이나 모델링은 반드시 필요하다. 사회공학 사이버작전에 주로 사용되는 사람의 심리적인 특징을 파악하여 분석하고 이를 토대로 모델링이 이루어진다면 사회공학 사이버작전의 수행 메커니즘을 쉽게 이해할 수 있을 뿐만 아니라 사회공학을 활용한 사이버 위협을 예방하는 방법을 찾는데도 도움이 될 수 있다. 이러한 측면에서 우리는 본 논문을 통해 사회공학 사이버작전 분석모델을 제안하였다.

본 논문에서 제안한 사회공학 사이버작전 분석모델은 사이버작전 수행단계 중 공격준비 단계에서 시행되는 사회공학 사이버작전의 수행단계, 활용 가능한 사회공학 방략, 그리고 각 방략의 수행과정에 숨어 있는 사회공학 심리기제들을 총 망라해서 모형화한 것이다. 본 논문에서 제안한 사회공학 사이버작전 분석모델을 활용하면 공격자가 목표나 시스템에 접근하기 위해서 조직이나 관련자의 어떤 정보를 수집했는지, 수집된 정보를 바탕으로 어떻게 취약대상을 공략했는지, 그리고 이때 사용된 사회공학 심리기제들은 어떠한 것들이 있는지를 체계적으로 분석할 수 있기 때문에 향후 사회공학 사이버작전 공격에 대한 대응체계를 만들기 위한 분석적 수단으로 활용될 수 있다. 우리가 아는 범위에서 이와 같이 체계적인 사회공학 사이버작전 분석모델을 제시한 것은 본 논문이 최초이다.

또한 우리는 본 논문에서 제안한 사회공학 사이버작전 분석모델의 효용성을 검증하기 위해 우리는 최근 10년 정도의 사회공학 사이버작전 공격사례들을 분석하였다. 분석결과 사회공학 정보수집 단계에서는 조직적 요소보다는 개인적인 요소에 대한 수집이 주를 이루고 있었으며 특히 개인의 대인관계(48%))와 업무내용(43%)과 연관된 정보수집이 중점적으로 이루어졌음을 알 수 있었다. 사회공학 방략선택 단계에서는 기술적 방략인 스피어 피싱(46%), 피싱(22%), 스미싱(12%)의 활용비중이 매우 높았다. 마지막으로 사회공학 방략실행 단계에서 사용되는 심리기제와 관련해서는 관심반응 단계에서는 전문성(37%), 호기심(28%), 급박성(22%), 현저성(13%)이 대체로 골고루 활용되었고, 인지판단 단계에서는 주로 도식(38%)과 전망이론(36%)이 활용되었으며, 목표행동 단계에서는 문간에 발 들여놓기(83%)가 가장 많이 활용되고 있음을 확인할 수 있었다.

향후에는 우리는 본 논문에서 제안한 사회공학 사이버작전 분석모델을 활용해 보다 많은 사회공학 사이버작전 사례들을 분석해봄으로써 모델을 보완·발전시켜 나갈 것이다. 이를 위해서는 많은 실험자들을 대상으로 다양한 심리 공격을 수행해보고 그에 대한 반응을 관찰함으로써 사회공학 사이버작전에 효과적인 추가 심리기제를 발굴해야 한다. 나아가 그런 사이버작전 심리기제들을 지금의 사회공학 사이버작전 분석모델에 추가해 나감으로써 보다 정확하고 효과적인 모델로 발전시킬 수 있을 것이다.

References

[1] Jungho Kang, Kyuyong Shin, Jincheol Yoo, Jeewon Kim, Sungrok Kang, Hyunmyung Lim, and Yongju Kim, "A Study on the Relationship between Social Engineering and Cyberspace Operations," Ministry of Defense, Dec. 2017.

[2] Kyuyong Shin, Jungho Kang, Jincheol Yoo, Jeewon Kim, Sungrok Kang, Hyunmyung Lim, and Yongju Kim, "A Study on the Concept of Social Engineering based Cyber Operations," Journal of The Korea Institute of Information Security & Cryptology, 28(3), pp. 707-716, June 2018.

[3] Vircom, "18 Cyber Security Trends We Are Watching in 2018," https://www.vircom.com/blog/18-cyber-security-trends-we-are-watching-in-2018/, 12. January, 2018.

[4] Wenjun Fan, Kevin Lwakatare, and Rong Rong, "Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations," Computer Network and Information Security, vol. 9, pp. 1-11, Jan. 2017.

[5] J. Piaget, The Language and Thought of the Child. New York: Harcourt, Brace, 1926.

[6] J.M. Darley and B. Latané, "Bystander Intervention in Emergencies: Diffusion of Responsibility," Journal of Personality and Social Psychology, 8(4), pp. 377, 1986.

[7] P.G. Zimbardo, "The Human Choice: Individuation, Reason, and Order Versus Deindividuation, Impulse, and Chaos," In Nebraska Symposium on Motivation. University of Nebraska press, 1969

[8] S.T. Fiske and S.E. Taylor, Social Cognition. New York: McGraw-Hill, 1991

[9] D. Kahneman and A. Tversky, Prospect Theory. Econometrica vol. 47 pp. 263-291, 1979

[10] D. Kahneman, P. Slovic, and A. Tversky(eds.), Judgment under Uncertainty: Heuristics and Biases. Cambridge University Press, 1982.

[11] V.H. Vroom, Work and Motivation. New York: Wiley, 1964

[12] M. Sherif, O.J. Harvey, B.J. White, W.R. Hood, and C.W. Sherif, Intergroup Conflict and Cooperation: The Robbers Cave Experiment. Norman, OK: University Book Exchange, 1961.

[13] B.F. Skinner, "Superstition' in the Pigeon," Journal of Experimental Psychology, vol. 38, pp. 168-172, 1948.

[14] Jin A Heo, Seong Bhin Joo, Jung Min Lee, and Chan Hyuk Park, "Countermeasures for Industrial Technology Protection in Social Engineering attack", The Journal of Social Science, vol. 23, no. 1, pp. 279-306, March 2016.

[15] Kyuyong Shin, Kyoung Min Kim, and Jongkwan Lee, "A Study on the Concept of Social Engineering Cyber Kill Chain for Social Engineering based Cyber Operations," Journal of The Korea Institute of Information Security & Cryptology, 28(5), Oct. 2018.

〈저자소개〉

신 규 용 (Kyuyong Shin) 종신회원
1996년 03월: 육군사관학교 이학사(전산학)
2000년 02월: 한국과학기술원(KAIST) 공학석사(전산학)
2009년 12월: (미)노스캐롤라이나 주립대(NCSU) 공학박사(전산학)
2010년 02월~현재: 육군사관학교 컴퓨터과학과 교수
2018년 06월~현재: 사이버전 연구센터 사이버전 개념연구실장
〈관심분야〉 분산시스템 보안, 네트워크 보안, 사이버전

김 지 원 (Jeewon Kim) 종신회원
2002년 2월: 동국대학교 졸업(공학사)
2016년 8월: 연세대학교 정보대학원 정보보호 석사
2016년 7월~현재: 육군사관학교 컴퓨터과학과 조교수
2017년 3월~현재: 아주대학교 NCW학과 박사과정
〈관심분야〉 정보보호, 사이버전, IOT 보안

임 현 명 (Hyun-myung Lim) 정회원
2007년 2월: 연세대학교 문학사(영어영문학)
2016년 1월: 국방대학교 국방관리대학원 석사
2016년 1월~현재: 육군사관학교 심리학과 조교수
〈관심분야〉 사회공학, 심리전

김 용 주 (Yongju Kim) 정회원
1985년 3월: 육군사관학교 문학사(독일어)
1992년 2월: 서울대학교 심리학 석사
1997년 9월: (독)기센대학교 심리학 박사
1997년 9월~현재: 육군사관학교 심리학과 교수
〈관심분야〉 사회공학, 심리전

유 진 철 (Jincheol Yoo) 정회원
1989년 3월: 육군사관학교 이학사(전산학)
1993년 8월: (미)아이오와 주립대 석사(통계학)
2003년 5월: (미)펜실베니아 주립대 공학박사(컴퓨터공학)
1994년 3월~현재: 육군사관학교 컴퓨터과학과 교수
〈관심분야〉 컴퓨터시스템, 사이버전, 컴퓨터구조