

미디어 노출과 사이버범죄 인식 간의 영향 연구

고두희, 원영아
성균관대 신문방송학과

A Study of Effect on Media Exposure and Cybercrime Perception

Du-Hee Ko, Young-A Won

Department of Journalism and Communication, Sungkyunkwan University

요 약 본 연구는 대학생 집단이 미디어를 통해서 획득한 사이버범죄에 대한 위험인식을 확인하는 목적을 갖는다. 이를 위하여 대학생 집단에게 일반적인 위험인식, 과학적 지식, 자발성, 친숙성, 통제성, 제약성, 두려움, 개인적 지식의 8문항으로 사이버범죄에 대한 위험인식을 확인하였다. 연구 결과, 실제로 대학생들이 느끼는 위험인식에서 인터넷 사기가 다른 유형에 비해 가장 낮은 위험인식을 나타냈는데 이는 대학생들이 사이버범죄에 대한 위협 정보를 획득하는 미디어 차이와 노출에서 기인함을 알 수 있었다. 사이버범죄에 대한 정보를 획득하는 미디어 종류에 따라서 대학생의 위험인식도 차이를 보였는데, 오락적 미디어보다는 뉴스 미디어에서 더욱 월등히 나타났다. 이는 우리사회에서 사이버범죄에 대한 정보를 전달하는 창구가 여전히 부족한 것을 알 수 있었다. 또한, 미디어의 이용 환경에 따라 각 개인별로 위험인식의 차이가 있다는 것과 사이버범죄의 영역에서도 미디어 노출에 따라 위험인식이 변화되고 있음을 확인할 수 있었다.

주제어 : 디지털, 사이버범죄, 위험, 심리학적 패러다임, 미디어 노출

Abstract This study focused on university students' risk perception of cybercrime through media exposure. For this purpose, I tried to figure out the results of risk perception on cybercrime with 8 factors. As a result, the lowest type of cybercrime was internet fraud, and it was caused by media type and degree of exposure, where university students get information about cybercrime. There's a difference of students' risk perception by media type, news media was the best. Depending on the media of the environment, even in the area of cyber crime there is a difference of perception of risk for each individual. And it can be confirmed that the risk perception in response to the exposure of the media has changed.

Key Words : Digital, Cybercrime, Risk Perception, Psychometric Paradigm, Media Exposure

1. 서론

정보통신기술의 발전은 인간 생활의 일부를 비롯해

인간 생활 전반에 걸쳐 비약적인 변화를 가져왔다. 인간 문명과 사회는 과학혁명을 통해 더욱 진보된 산업화를 이룩하였으며, 이를 기반으로 합리적인 현재의 사회를

* 본 논문은 2014년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2014S1A3A2044217).

Received 31 March 2016, Revised 29 April 2016

Accepted 20 May 2016, Published 28 May 2016

Corresponding Author: Young-a Won

(Sungkyunkwan University)

Email: youngawon@naver.com

ISSN: 1738-1916

© The Society of Digital Policy & Management. All rights reserved. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0>), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

이룩하게 되었다. 변화된 사회는 이전의 사회보다 훨씬 풍요를 누리게 되었다. 그러나 사회의 변화와 풍요 이면에는 과거사회에는 위협의 요소가 아니었던 새로운 유형의 위협이 발생하게 한 원인이 생기게 되었다. 지속적인 발전은 인간의 삶에 있어서 중요한 영역이라고 말할 수 있으나 그러한 요인과 함께 인간의 삶을 위협하고 더 나아가 인간의 발전 그 자체를 부정하는 요인도 등장할 수 있다는 주장은 다양한 영역에서 영향을 주고 있다. 위험사회는 20세 후반의 사회 즉, 급격한 사회의 변화에 따라 새롭게 등장한 위험 유형이 존재하는 시기에 주목한다. 위험사회에서 주목한 사회의 변화는 시간과 공간, 사회 등 다양한 영역을 모두 내포하고 있다. 현대 사회에서 발생한 위험은 예측과 통제가 불가능하며, 근대로의 발전에 있어서 과학기술의 과도한 사용의 결과로 인간의 삶 그 자체를 위협하고 사회 전역에 만연해있다고 볼 수 있다[1].

정보기술은 개인과 기업에게 새로운 가치를 창출하는 등 긍정적인 면을 가지고 있지만 정보화의 역기능으로 인하여 IT실패를 동시에 겪기도 한다[2]. 정보통신기술의 발전을 통해 등장한 기술 중에서 가장 많은 사람들이 이용하고 있는 것은 사이버공간이라고 할 수 있으며, 현재 사이버공간은 현실의 세계와 동일한 정치, 사회, 문화 등의 양상을 그대로 나타내고 있다. 사이버공간에서는 인간의 일상생활에서 타인과 커뮤니케이션을 하는 것과 유사하게 동시적·비동시적으로 커뮤니케이션을 하고 있다. 이러한 커뮤니케이션을 통해서 긍정적으로 인간관계의 확장을 이어가거나 외부 환경을 인식하는데 도움이 되고 있으나 이면에는 사이버공간이라는 특수한 환경이라는 요인을 기반으로 다양한 범죄, 즉, 사이버범죄에도 이용되고 있다. 사이버범죄는 인터넷을 비롯한 사이버공간과 같은 정보통신망으로 연결된 컴퓨터 시스템이나 이들을 매개로 한 사이버 공간에서 시가과 공간을 초월해 불특정 다수에게 피해를 주는 행위라고도 볼 수 있다[3].

사이버공간에서 자행되고 있는 사이버범죄의 유형은 정의내리기 어려울 정도로 다양한데 이는 사이버공간이라는 환경의 영향으로 범주화하기 어려운 양상을 보이기 때문이다. 예를 들면, 익명의 사용자가 특정 기사에 악성 댓글을 남겨 이를 처벌하고자 한다면, 사이버공간에서의 표현의 자유를 억압하는 이중적인 결과를 가져올 수 있다는 점이다. 또한, 사이버범죄에 이용되는 정보통신기술

은 일반적으로 대중이 알기 어려운 기술을 기반으로 하고 있기에 범죄의 발생 여부나 원인 등을 파악하기 어렵다는 점은 사이버범죄의 유형을 더욱 확대시키고 있으며, 결국, 사이버범죄 유형을 규정하기 어렵게 하며 더 나아가 사이버범죄로 인한 피해를 확대시키는 요인이 되고 있다[4].

이처럼 정보통신기술의 발전에 편승하여 더욱 다각화되고 복잡해지는 사이버범죄를 예방하기 위해서는 일반인의 사이버범죄에 대한 위험인식의 중요성은 더욱 커진다. 위험인식은 특정 행위를 함으로서 발생할 수 있는 잠재적 위험에 대한 주관적 인식이다[5]. 또한, 위험인식은 일반인이 접하는 미디어의 유형에 따라 위험인식에 대한 영향이 다르게 나타난다[6]. 현대 사회는 다양한 미디어를 통해 폭넓은 정보가 공유되는 사회이다.

사이버범죄의 유형과 양상이 확대되는 과정에서 해당 범죄에 대해서 사람들이 어떻게 인식하고 있는지의 확인을 통해서만 올바른 이해에 기초한 위험커뮤니케이션의 제공이 가능해진다. 위험커뮤니케이션은 위험과 관련된 정보를 전달하는 수준이 아니라 이해관계자의 갈등을 최소화하는 것으로 볼 수 있다[7].

정보통신기술의 발달로 확대되고 있는 사이버공간과 이에 접근할 수 있는 다양한 미디어의 등장을 통해서 사람들의 위험인식은 유형에 따라 변화되고 있다. 본 연구는 사이버공간의 접근이 활발하며, 다수의 미디어를 이용하고 있는 것으로 생각되는 대학생들의 사이버범죄에 대한 위험인식을 확인하고자 하였다. 위험인식 연구에서 자주 이용되고 있는 심리측정 접근 방법을 통하여 사이버범죄에 대한 위험인식을 확인하고자 하였으며 또한, 미디어 노출에 따라 사이버범죄에 대한 위험인식의 차이를 보고자 하였다. 이를 통해 사이버범죄에 대한 효율적인 위험커뮤니케이션에 대한 시사점을 제공하고자 한다.

2. 이론적 배경

2.1 사이버범죄의 정의

정보통신기술의 발전으로 인간의 생활 반경이 사이버공간으로 확대되면서 사람들은 과거보다 더욱 편리한 삶을 영위할 수 있게 되었다. 또한, 네트워크 기술이 인간 삶에 깊숙하게 침투하면서 현대 사회에서의 개인적 영역,

사회적 영역, 경제적 영역 등의 다양한 분야에서 이점을 누리게 되었다. 온라인 banking은 재정적인 영역에서 탈소모적이면서 효율적인 방법을 제시하였고 e-커머스는 교환 비용을 크게 줄이면서 상품의 생산성을 향상시키는데 역할을 하였다. 소셜 네트워크 서비스는 인간 관계의 확장에 크게 기여를 하였다. 하지만 이와 같은 편의성의 이면에는 사이버공간만의 특성에 편승하여 사이버범죄라는 새로운 유형의 위협을 양산하게 되었다[8].

사이버범죄는 일상생활에서 자연스럽게 이용되고 있는 단어이지만, 정확한 의미를 정의하는데 있어서는 상당한 어려운 점이 있다. 이는 사이버범죄에 이용되는 소프트웨어(프로그램)와 같은 기술적인 도구를 비롯하여 다양한 영역이 포함되기에 정의내리기 더욱 힘들기 때문이다. 사이버범죄는 일반적인 범죄처럼 다양한 양상을 가지고 있으며, 복잡한 시나리오와 환경을 기반으로 진행된다. 사이버범죄에 대한 현재의 정의는 경험적으로 이루어지고 있는 것으로, 사건의 피해자와 관찰자(혹은 방어자)와의 시각 등을 통해서 정의되는 경향이 크다[8]. 국내에서도 사이버범죄에 대한 정의와 유형을 파악하려는 학술적 시도는 지속적으로 이루어지고 있으며, 사이버범죄에 대한 기존의 법적 범주 등을 정리하여 침해가치기준, 침해성격기준, 침해수단기준 등의 변수를 이용하여 8가지 범주로 정의내린 연구도 있다[3]. 그러나 모든 사이버범죄가 이와 같은 범주에 포함되기는 어려운 특성을 가진다. 이는 사이버범죄는 새롭게 등장한 위협인 동시에 기술적인 위협의 성격이 강하다. 이러한 특성은 전문적인 영역에 속하기 때문에 일반인들이 위협성을 인식하기는 쉬운 일이 아니며, 미디어를 통해서 전달되는 정보를 이해하는 데에도 한계가 따른다[10].

사이버범죄에 대한 명확한 정의가 어려운 부분이 있지만 정부는 사이버범죄에 대한 일반적인 정의를 통하여 해당 범죄를 예방하고 피해를 최소화하고자한다. 이에 ‘경찰청 사이버안전국’과 같은 조직을 통해 사이버범죄의 실제적 유형화의 단계를 진행하고 있으며 사이버범죄의 유형을 정보통신망 침해범죄(해킹, 서비스거부공격, 악성 프로그램), 정보통신망 이용범죄(인터넷 사기, 사이버 금융범죄, 개인위치정보침해, 사이버 저작권 침해), 불법콘텐츠범죄(사이버음란물, 사이버도박, 사이버 명예훼손, 사이버스토킹)의 3가지 유형으로 구분하고 있다. 이와 같은 분류를 통하여 사이버범죄의 유형에 따라 발생한 실제

피해 정도를 확인할 수 있다[11].

경찰청 사이버안전국의 사이버범죄 유형별 분류를 통해 매년 피해빈도를 추산하고 있는데, 우리나라에서 가장 빈번한 사이버범죄는, 2015년 기준 전체 86,658건의 정보통신망 이용범죄 중에서 68,444건이 발생한 ‘인터넷 사기’이다. ‘인터넷 사기’는 정보통신망(컴퓨터 시스템)을 통하여, 이용자들에게 물품이나 용역을 제공할 것처럼 기망하여 피해자로부터 금품을 편취(교부행위)한 경우를 의미하는데, 다른 유형의 사이버범죄에 비해서 일반인이 피해를 인식하기 용이하며 가장 쉽게 피해를 입을 수 있는 범죄라고 할 수 있다. 같은 해 인터넷 사기가 68,444건이 발생한데 비해, 해킹(524건)이나 DDos(19건)는 상대적으로 적게 발생한 것처럼 사이버범죄의 유형에 따라 발생빈도가 서로 다르며 피해 정도도 다른 상황이다[11]. 본 연구는 정부가 규정하고 있는 사이버범죄의 유형에 따라 대학생의 위협인식 정도를 통하여 실제 발생하고 있는 사이버범죄의 객관적인 발생 수치와 연구 대상의 주관적인 인식의 차이를 확인하고자 하였다.

2.2 미디어노출에 따른 위협인식

개인의 위협인식을 결정하는 요인은 다양하게 존재할 수 있는데, 사회문화적 관점에서 위협인식을 형성하는 중요한 요소는 ‘미디어’이다[12]. 정보통신의 발달에 따라 현대사회는 다양한 미디어를 이용할 수 있는 환경이 되었다. 위협과 관련된 정보는 문자, 음성, 동영상 등의 다양한 방법으로 사람들에게 전달되고 있으며 각 개인에게 영향을 미치는 정도는 사회적 맥락이나 메시지의 내용에 따라 메시지의 전달 효과가 다르게 나타난다[12]. 이와 같은 이유로 위협 관련 정보의 전달에 있어서 미디어의 선택이 중요한 의미를 가지게 되는 것이다.

미디어가 개인의 위협판단에 미치는 영향에 대한 이론은 ‘미디어 의존이론’이다[14]. 미디어 의존이론은 사회의 복잡화에 따라 사회 구성원은 매스커뮤니케이션에서 전달되는 정보에 의존하게 되며, 반면 대인적 커뮤니케이션에는 덜 의존한다는 가정에 기인하고 있다. 관련 연구에 따르면, 이용자는 사회 환경의 변화 요인과 정보 획득의 필요성에 의해서도 미디어 의존이 일어날 수 있는 가능성을 보여주었다[15].

한편, 위협인식과 미디어의 영향에 대한 관계는 ‘미디어 효과 이론’과도 관련이 깊다. 일반적으로 모든 개인은

자신의 삶을 통해서 자신만의 지식을 구축하며 특정한 사안이 발생했을 때, 기억 속의 생각이나 개념을 사안에 적용하는 과정을 거친다. 이 과정에서 접근성(accessibility)의 문제가 발생한다. 접근성은 ‘임시 접근성(temporary accessibility)’과 ‘장기 접근성(chronic accessibility)’으로 구분할 수 있는데, 임시 접근성은 자주 활성화됨으로 인하여 높아지는 접근성이며, 장기 접근성은 자주 활성화되는 않았어도 관련 자극물에 노출되었을 때 활성화되는 접근성으로 기억 속에서 보다 깊숙이 저장된 생각이나 개념들을 의미한다. 뉴스미디어를 통해서 해당 위험에 대한 정보가 지속적으로 전달되어 임시적으로 활성화되는 접근성뿐만 아니라 장기적인 기억의 일환으로도 위험에 대한 개인의 인식이 변화될 수 있는 것이다.

위험인식을 형성하는 요인 중에서 중요한 것은 개인의 미디어 노출이라고 볼 수 있다. 미디어의 노출을 통해서 장·단기적인 위험인식이 형성되며 특정 사안이 발생했을 때, 이를 통해 개인의 위험인식이 발현된다. 사이버범죄는 비교적 최근에 발생하고 있는 새로운 형태의 위험유형이라고 할 수 있다. 뿐만 다양한 최근 몇 년에 걸쳐 사회적으로 큰 피해를 주었던 사건(DDos공격, 카드사 해킹 사건 등)들이 연이어 발생하면서 미디어는 이를 지속적으로 전달하고자 하는 움직임을 보이고 있다. 하지만 미디어를 통해 전달되는 정보에 대한 이용자의 위험인식을 확인하고자 하는 연구는 많지 않은 상황이다. 이러한 상황에서 본 연구는 실제 피해유형이 수집되고 있는 사이버범죄의 유형과 미디어 노출이 위험인식에 어떻게 영향을 파악하고자 하였다.

2.3 위험인식과 심리측정접근

실제 발생하는 위험의 객관적인 양적 평가와 개인에 따른 주관적 위험인식은 다양한 요인으로 인해 불일치가 발생할 수 있다[17]. 또한, 전문가들의 위험평가와 일반인들이 느끼는 위험인식의 차이가 나타나는 것은 사람들의 인식이 주관적이며 합리적이지 않다는 것에 기인한다. 위험인식에 대한 연구는 위험에 대한 기본적 관점에 따라 평면적 관점의 기술적 접근, 차원적 관점의 심리측정 접근, 맥락적 관점의 문화·사회학적 접근으로 분류할 수 있으며, 이 중에서 대표적으로 위험인식을 확인하는데 적용되어온 방법은 심리측정접근이라고 할 수 있다[18].

위험이 인식되는 과정은 개인의 주관적이고 가치적인

속성인 위험특성과 관련이 깊다. 위험은 주관적으로 판단하는 경향이 크지만, 위험에 대한 인식은 주관적이고 가치적인 속성에 따라 결정된다[19]. 심리측정접근은 개인의 주관적인 위험인식을 차원적인 관점에서 확인하기 위해서 Slovic의 연구진이 개발한 방법으로 위험인식연구에서 대표적으로 이용되어온 측정방법으로 전통적 기술적 접근 방법의 문제점에 대한 비판으로 발전하였다[20]. 심리측정 접근에서 위험은 사람들의 위험인식에 영향을 미치는 요인들에 의해서 위험이 평가될 수 있으며, 인식된 위험의 예측과 계량화가 가능하다는 점, 동일한 위험이라고 하더라도 각각의 사람들에게는 다른 실체로 인식된다는 점, 위험특성에 의해 다차원적으로 분석될 수 있다는 점의 몇 가지 전체를 가진다[21]. 심리측정 패러다임을 활용한 기존의 연구들에서는 위험지각 요인으로 위해의 통제가능성(Controllable), 두려움(Dread), 파괴성(Global Catastrophic), 결과의 치명성(Consequences Fatal), 정당성(Equitable), 재앙성(Catastrophic), 다음 세대로의 위험 전파(High Risk to Future Generations), 감소가능성(Easily Reduced), 증폭성(Risk Increasing), 자발성(Voluntary), 관찰성(Observable), 개인적 지식(Individual Knowledge), 과학적 지식(Scientific Knowledge), 효과의 즉시성(Effect Immediate), 친숙성(Old Risk) 등이 폭 넓게 사용 되고 있다[16,21,22]. 결국, 심리측정 접근에서의 위험은 사회적·심리적·제도적·문화적 요인 등의 다양하고 광범위한 영역을 통해 개인이 영향을 받아 주관적으로 결정된다고 본다. 주관적인 위험인식의 계량화를 통하여 사회와 개인이 당면하고 있는 위험에 대해 반응하고 있는지를 설명하는데 이용할 수 있다는 것이다[17]. 위험에 대한 일부 연구에 따르면, 과학적 분석에 근거한 통계적 위험 수준과 주관적 이해에 따른 위험 인식 수준의 차이가 존재할 수 있다고 한다. 이는 사회적으로 심각한 문제가 될 수 있다[17].

사이버범죄는 일반적인 자연재해와 달리 새로운 위험의 영역으로 국가와 사회의 근간을 무너뜨릴 수 있는 재앙적 위험성이 높은 범죄이다[11]. 사이버범죄의 유형은 파생적으로 끊임없이 새롭게 등장하고 있으며, 모든 사이버범죄를 정의내리기 어려울 정도로 빠르게 생성되고 피해를 입히는 상황이라고 할 수 있다. 하지만 인간의 삶에 더욱 더 밀접해지고 있는 사이버공간에서 사람들의 물리적, 정신적 피해를 입힐 수 있는 사이버범죄에 대한

사람들의 위협인식에 대한 파악은 효과적인 커뮤니케이션에 이용될 수 있을 것이다.

3. 연구문제와 연구방법

3.1 연구문제

국내에서 발생하는 사이버범죄의 유형의 파악과 이에 대한 대학생들의 위협인식을 확인하고자 하였다. 또한, 해당 위협에 대한 미디어 노출의 정도를 통해 위협인식 간의 차이를 보고자 연구를 설계하였다.

<연구문제1> 사이버범죄의 객관적 사건의 양상과 대학생 집단의 위협 인식의 차이는 어떠한가?

<연구문제2> 심리측정 접근에 따른 사이버 범죄 인식은 어떠한 양상을 보이는가?

<연구문제3> 사이버 범죄와 관련된 미디어 노출은 개인적/사회적 위협 인식에 영향에 어떤 역할을 할 것인가?

이와 같은 내용을 토대로 국내 대학생들의 사이버범죄에 대한 위협을 인식하는 정도를 파악하고자 하였다. 미디어 노출의 정도와 사이버범죄를 인식하는 심리측정 접근을 수치화하여 이를 통하여 국내 미디어 이용자의 사이버 범죄의 위협인식의 탐색적 확인을 하고자 한다. 국가 전반의 위기를 초래할 정도로 강력한 영향력을 지닌 사이버범죄는 다양한 형태로 나타나고 피해를 입힌다. 하지만 사이버범죄는 특정 전문가와 일부 관련자 이외에는 정확한 위협성을 파악하기 어려운 성격을 가지고 있다. 때문에 다수의 이용자는 사이버 범죄의 피해 발생 가능성에도 불구하고 미디어를 이용하고 있다. 이러한 상황에서 현재의 미디어 이용자 중에서 인터넷, 스마트폰 등과 같은 뉴 미디어를 이용하는데 있어서 가장 활발한 연령층인 대학생의 시각으로 위협 인식의 경향을 확인하고자 한다. 이러한 경향성의 확인을 통하여 앞으로의 사이버범죄의 위협 인식의 범위를 확대하고자 한다.

3.2 연구방법

본 연구는 미디어 노출에 따른 국내 대학생 및 대학원

생의 사이버범죄 위협인식을 확인하고자 하였다. 1차 예비조사 후 일부 문항을 수정 및 보완하였으며, 눈덩이 표집법(snowball sampling)을 이용하여 온라인 설문을 진행하였으며, 중도 포기하거나 불성실한 응답으로 판단되는 설문을 제외한 총 203명을 대상으로 분석하였다. 전 대상의 연령은 대학이나 대학원에 재학 중이거나 최근 대학을 졸업한 20대이다. 이 중에서 남성은 98명(48.2%)이었으며, 여성은 105명(51.7%)이었다.

국내에서 발생하는 사이버범죄에 대한 대학생의 위협인식을 미디어 노출의 관점에서 확인하기 위해 일반적인 위협인식의 확인을 위해서 경찰청 사이버안전국에서 제시하고 있는 11개의 범죄를 대상으로 하였다. 또한, 사이버범죄의 객관적인 위험 평가 수치와 대학생들이 개인적으로 느끼는 위협인식의 차이를 확인하기 위해, 국내에서 발생하는 사이버범죄 중에서 가장 큰 빈도를 차지하는 '인터넷 사기'와의 비교를 통하여 대학생의 위협인식 수준을 확인하고자 하였다.

위험특성은 특정 위험대상에 대해서 주관적이고 가치적인 개인의 속성으로 정의할 수 있으며, 본 연구에서는 선행 연구를 바탕으로 문항을 참조하여 구성하였다 [10,18,20]. 일반적인 위협인식, 과학적 지식, 자발성, 친숙성, 통제성, 재양성, 두려움, 개인적 지식의 8문항으로 리커트 5점 척도로 제시하였다.

미디어 노출은 미디어를 통해서 위험과 관련된 정보에 수동적으로 노출되는 것이라고 할 수 있다. 위험 정보를 전달할 수 있는 미디어는 뉴스 콘텐츠를 기반으로 하여 정보를 전달하는 기능을 하는 '뉴스 미디어'와 오락적 콘텐츠를 기반으로 관련 정보를 더욱 실감나게 전달하는 기능을 하는 '오락적 미디어'로 분류할 수 있다. 미디어 노출과 관련된 문항은 기존 연구에서 이용되었던 문항을 연구의 성격에 맞도록 사이버범죄의 11개 유형별로 수정하여 이용하였다[16].

4. 연구 결과

4.1 사이버범죄 위협인식 수준

본 연구는 실제로 발생되고 있는 사이버범죄의 양상과 개인적인 위협인식의 차이를 대학생 집단을 중심으로 확인하고자 하였다. 전술했듯이, 국내에서 가장 많이 발

생되고 있는 사이버범죄는 ‘인터넷 사기’로 나타나고 있다. 응답자의 주관적인 위험인식의 차이를 확인하기 위해서 인터넷 사기와 다른 사이버범죄의 유형 10개를 상호 비교하였으며 결과는 다음과 같다.

<Table 1> Level of Risk Perceptions

Type	M	SD
Telecommunications fraud	4.43	0.751
Hacking	4.36	0.83
Malware	4.28	0.817
DDos	4.1	0.98
Invasion of privacy	4.07	0.983
Cyber Stalking	4.06	1.039
Cyber Copyright Infringement	3.62	1.072
Cyber Gambling	3.4	1.268
Cyber pornography	3.21	1.356
Spam Mail	3.2	1.2
Internet fraud	3	-

앞서 언급한 것처럼 인터넷 사기는 다른 유형에 비해 높은 수준으로 많이 발생하고 있지만, 대학생 집단의 사이버범죄의 위험인식 수준은 가장 낮은 것으로 나타났다. 전체 11개 사이버범죄의 유형 중에서 비교 대상이었던 인터넷사기보다 10개의 사이버범죄 유형에 대한 위험인식이 모두 높게 나타났다. 특히, 피싱·파밍·스미싱 등을 포함하고 있는 전기통신금융사기에 대한 인식이 4.43점으로 가장 높았으며, 해킹 4.36점, 악성코드 4.28점, DDos의 서비스 거부공격이 4.1점, 개인·위치정보 침해가 4.07점, 사이버 명예훼손이 4.06점으로 다소 높게 인식되고 있음을 확인할 수 있었다.

4.2 사이버범죄 심리측정 특성

사이버범죄에 대한 일반적인 위험인식과 위험특성간의 상관관계 분석을 진행하였다. 사이버범죄에 대한 일반적 위험인식은 자발성(Pearson's $r=.166$, $p<.05$)과 두려움(Pearson's $r=.345$, $p<.01$)과 정(+)의 상관관계를 보인다. 한편, 친숙성(Pearson's $r=-.197$, $p<.01$)과 감소가능성(Pearson's $r=-.288$, $p<.01$)은 부(-)의 상관관계를 나타낸다.

<Table 2> Correlations of Risk Characteristics

	Risk Perception	Voluntary	Controllable	Dread	Individual Knowledge	Scientific Knowledge	Old Risk	Easily Reduced
Voluntary	.166*	1						
Controllable	-.109	.053	1					
Dread	.345**	.417**	-.083	1				
Individual Knowledge	.108	.300**	-.141*	.323**	1			
Scientific Knowledge	.043	.254**	-.015	.322**	.625**	1		
Old Risk	-.197**	.154*	.216**	.054	.113	.198**	1	
Easily Reduced	-.288**	-.033	.483**	.088	.151*	.266**	.384**	1

* $p<.05$ ** $p<.01$ *** $p<.001$

각 위험특성 간에 존재하는 상호성과 구조적인 관계를 명확하게 확인하기 위하여 요인분석으로 차원을 축소하였다. 요인 추출법은 주성분 방식으로 고유 값 1을 기준으로 추출하였으며 회전법으로 베리맥스(Varimax)를 사용하였다. 요인분석 결과, 다음과 같이 2개의 요인으로 분류되었다. 대학생이 인식하는 사이버범죄에 대한 위험 특성은 기존의 연구 결과([18,19])와는 다소 다른 결과로 나타났다. 기존의 위험연구에서의 심리측정 위험특성은 ‘위험의 알려지지 않은 정도’의 개인적 지식, 과학적 지식, 친숙성과 ‘위험의 두려운 정도’의 자발성, 두려움, 통제성으로 구분되었으나 사이버범죄와 관련된 본 연구의 요인은 과학적 지식과 개인적 지식, 두려움, 자발성의 1요인과 통제성과 감소가능성, 친숙성의 2요인으로 분류되었다.

<Table 3> Factor Analysis of Risk Characteristics

	Factor 1	Factor 2
Scientific Knowledge	.785	-.120
Individual Knowledge	.743	-.304
Dread	.608	-.327
Voluntary	.571	-.248
Controllable	.140	.782
Easily Reduced	.459	.719
Old Risk	.440	.504

4.3 사이버범죄별 미디어 노출

대학생 집단이 미디어를 통해서 접하게 되는 사이버범죄에 대한 개인적인 노출을 확인하였다. 사이버범죄에

대한 정보를 가장 많이 획득하는 것은 인터넷 뉴스로 나타났다으며, 뒤를 이어 TV뉴스와 신문, 드라마·영화·시트콤이었으며 마지막으로 인포테인먼트 프로그램으로 나타났다. 미디어 노출에 따른 위험인식의 차이를 확인하기 위하여 위계적 회귀분석을 진행하여 다음과 같은 결과를 나타냈다. 위계적 회귀분석은 종속변수에 영향을 미치는 독립변수간의 영향력의 차이를 확인하기 위한 분석방법으로 TV뉴스, 신문, 인터넷뉴스의 뉴스미디어와 드라마 및 영화, 시트콤과 인포테인먼트의 오락적 미디어간의 차이를 확인하기 위해 진행되었다. 인터넷뉴스가 일반적인 위험인식에 가장 큰 영향을 미치는 것으로 나타났다으며 통계적으로 유의미한 결과를 나타냈다. 이외에 TV뉴스, 신문뉴스, 인포테인먼트, 드라마·영화·드라마 등은 통계적으로 유의미한 결과를 나타내지는 못했으나 이 중에서 TV뉴스가 다른 미디어에 비해 근접해있었다. 다시 말하면, 인터넷뉴스를 통해 획득하는 사이버범죄에 대한 정보가 일반적인 위험인식에 가장 큰 영향을 미치고 있었다. 이와 같은 결과가 나타난 것은, 오락적 미디어에서 사이버범죄와 관련된 정보를 시청자들에게 전달하고 있지 않다는 것으로도 볼 수 있다. 사이버범죄의 특성상 일반인들이 이해하기 어려운 부분이 있기에 뉴스미디어에서 이를 간단하게 정리를 해서 보도하는 경향이 큰데, 이와 같은 뉴스미디어 외에도 대학생들 비롯한 일반 시청자들이 쉽게 보고 즐길 수 있는 오락적미디어에서도 사이버범죄에 대한 정보와 위험성 등을 전달해야 할 필요가 있는 것으로 보인다.

<Table 4> Relationship of Risk Perception and Media Exposure

	β	t
(constant)	3.699	13.017 (0.000)
TV News	-0.221	-1.69 (.093)
Newspaper	0.017	0.221 (.825)
Internet News	0.282	2.523 (.012)
Infotainment	-0.008	-0.127 (.899)
Drama, Movie	-0.066	-0.904 (.367)

5. 결론 및 제언

본 연구는 대학생 집단이 미디어를 통해서 획득한 사이버범죄에 대한 위험인식을 확인하기 위해 진행되었다.

일반적으로 발생빈도가 높은 범죄나 사고가 더욱 위험한 것으로 인식하기 쉽다. 하지만 객관화된 통계수치의 범죄에 대한 인식과 일반 개인의 주관적인 위험인식은 서로 차이를 나타내는 경우가 많다[18]. 사이버범죄에 대한 대학생의 위험인식의 경향도 기존의 연구 결과와 유사하게 나타났다. 객관적으로 가장 많은 사건이 발생하는 것은 인터넷 사기로, 인터넷을 통하여 다른 사람과 물건을 거래를 할 때, 물품 및 용역을 제공할 것처럼 거래한 후, 편취하는 행위이다. 다른 사이버범죄에 비해서 기술적인 지식이 요구되지 않기 때문에 가장 쉽게 자행될 수 있다는 이유로 가장 큰 빈도를 보이고 있다. 그러나 실제로 대학생들이 느끼는 위험인식의 양상에서 인터넷 사기는 다른 유형에 비해 가장 낮은 위험인식을 나타냈다. 이는 대학생들이 사이버범죄에 대한 위험 정보를 획득하는 미디어의 차이에서 그 원인을 확인할 수 있다.

사이버범죄에 대한 정보를 획득하는 미디어의 종류에 따라서 대학생의 위험인식의 차이를 보인 것은 기존의 미디어 의존의 연구 결과와 유사하게 나타났다. 다만, 연구대상이 사이버범죄에 대한 정보를 획득하는 경로가 오락적 미디어보다는 뉴스 미디어에서 더욱 월등히 나타났다는 점은 아직까지 한국 사회에서 사이버범죄에 대한 정보를 전달하는 창구가 부족한 것을 알 수 있는 부분이다. 뉴스미디어를 통한 정보 전달 뿐만 아니라 오락적 미디어를 통해서 사이버범죄의 유형과 위험성 등을 전달한다면, 시청자들이 더욱 쉽게 사이버범죄에 대한 인식을 높일 수 있을 것이라고 생각된다.

이밖에도 특정 사이버범죄에 대한 정보가 가장 많이 전달되고 있는 것으로 응답되었는데, 이는 실제로 발생하고 있는 사이버범죄의 유형과는 큰 차이를 나타내고 있음을 확인할 수 있었다. 다시 말하면, 실제 사이버범죄 발생 빈도와 대학생들이 더욱 위험하다고 인식하는 사이버범죄의 위험 유형과는 다소 거리가 있다는 것을 의미한다.

사이버범죄는 스마트폰이나 스마트패드와 같은 새로운 기술을 기반으로 SNS, 소셜 커머스 등의 서비스가 폭발적으로 확대됨에 따라 더욱 기승을 부리고 있는 범죄라 할 수 있다[23]. 기존에 없던 기술은 사회에 긍정적인 변혁의 가능성도 제공하지만 기술에 적응하지 못한 사람들에게는 부정적인 영향도 미치기도 한다. 사이버범죄는 첨단 기법을 토대로 일반인들이 파악하기 어려운 형태로

발생하는 경우가 많다. 때문에 어떤 위험요소보다도 해당 정보를 지속적으로 전달해야할 필요성이 있다. 사이버범죄의 유형이나 수법 등에 대한 지속적인 정보 전달이 일반인에게 이루어진다면 범죄에 대한 인식은 확대되고 범죄의 발생률은 더욱 낮아질 수 있을 것이다.

본 연구는 사이버범죄에 대한 대학생들의 위험인식을 파악하고자 하였다. 사이버범죄의 유형이 급속하게 늘어나고 발생 빈도도 높아지고 있는 시점에서 미디어의 이용환경에 따라 각 개인별로 위험인식의 차이가 있다는 것과 사이버범죄의 영역에서도 미디어 노출에 따른 위험인식이 변화되고 있음을 확인한데 의의가 있다. 하지만 특정 대상을 중심으로 연구를 진행하여 전체 인구에 대한 일반화의 문제는 제한적일 수밖에 없으며 각 사이버범죄에 대한 위험인식을 구체적으로 확인하기는 어려웠다. 따라서 사이버범죄와 관련된 위험인식 및 미디어의 영향력을 확인하기 위해서 후속연구에서는 표본의 확대와 더불어 사이버범죄의 세부적 특성을 반영하여 세부적으로 측정한다면 일반 대중의 위험인식을 보다 정확하게 파악하고자 한다.

ACKNOWLEDGMENTS

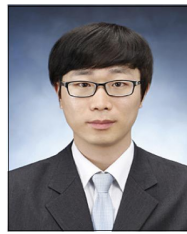
This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government(NRF-2014S1A3A2044217).

REFERENCES

- [1] U. Beck, "World Risk Society". Polity Press, 1999.
- [2] Hyeon-Ho Park, Hee-Ock Nho, Yong-Ho Kim, "The Impact of Perceived IT Threat on Convergence Information System Performance", Journal of the Korea Convergence Society, Vol. 6, No. 3, pp. 65-71, 2015.
- [3] S. Y. OH, "The application of digital forensic investigation for response of cyber-crimes", Journal of Digital Convergence, The Society of Digital Policy & Management, Vol. 13, No. 4, pp. 81-87, 2015.
- [4] K. W. Kim, J. W. Seo, "Exploring Typology of Cybercrime", Korean Public Management Review, Vol. 23, No. 4, pp. 95-118, 2009.
- [5] J. Davis-Berman, D. Berman, "Risk and Anxiety in Adventure Programming", The Journal of Experiential Education, Vol. 25, pp. 305-310, 2002.
- [6] J. S. Lee, "The Effect of Media Modality and The Value of Risk Messages on Affective Risk Perception and Behavioral Intention", Korean Journal of Cognitive Science, Vol. 23, No. 4, pp. 457-485, 2012.
- [7] H. R. Song, W. J. Kim, "Effects of Risk Characteristic and Risk Perception on Risk Severity of Natural Disaster", Journal of The Korea Contents Association, Vol 13, No. 4, pp. 198-207, 2013.
- [8] M. Riek, R. Böhme, T. Moore, "Understanding the influence of Cybercrime risk on the e-service adoption of European Internet Users", Workshop on the Economics of Information Security, 2014.
- [9] S. Gordon, R. Ford, "On the Definition and Classification of Cybercrime", Journal in Computer Virology, Vol. 2, No. 1, pp. 13-20, 2006.
- [10] H. R. Song, C. W. Kim, W. J. Kim. "Effect of publics' risk characteristic of cyber crime and fear on perceived severity of consequences", Journal of Political Communication, Vol. 32, pp. 129-156, 2014.
- [11] National Police Agency Cyber Bureau Website, (<http://cyberbureau.police.go.kr/index.do>).
- [12] T. Tyler, F. L. Cook, "The mass media and judgments of risk: Distinguishing impact on personal and societal level judgments", Journal of Personality and Social Psychology, Vol. 47, No. 4, pp. 693-708, 1984.
- [13] D. A. Scheufele, "Framing as a Theory of Media effects", Journal of Communication, Vol. 49, No. 1, pp. 103-122, 1999.
- [14] D. P. Cha. "The Effects of Mass Communication and Interpersonal Communication on College Students' Perceptions of Risk to Youth Unemployment", Journal of Communication Science, Vol. 11, No. 3, pp. 325-348, 2011.

- [15] J. Y. Kim. "A study of media dependency theory : The relationships of International students' Internet use, national identity, information needs, media dependency, and cognitive and behavioral effects", *Journal of Communication Science*, Vol. 3, No. 2, pp. 119-154, 2003.
- [16] B. K. Jwa, M. Y. Yun, H. K. Park. "Media, Risk Characteristics, and Risk Perceptions : The Context of Carcinogenic Hazards, *Journal of Public Relations*", Vol. 17, No. 4, pp. 72-109, 2013.
- [17] I. J. Chung. "A Study of Risk Perception and Policy Implication : A Psychometric Analysis of Korean Perception for Technological Risks, *Journal of The Korean Society of Safety*", Vol. 29, No. 1, pp.80-85, 2014.
- [18] S. Y. Heo, S. W. Yoon. "Analysis of Consumer's Risk Perception about Food Safety through the Analysis Lens of Psychometric Paradigm, *Korean Journal of Food Marketing and Economics*", Vol. 30, No. 2, pp. 97-116, 2013.
- [19] H. R. Song, W. J Kim. "Effects of Trust, Stigma, Optimistic Bias on Risk Perception of Nuclear Power Plants", *Journal of the Korea Contents Association*, Vol. 13, No. 3, pp. 162-173, 2013.
- [20] P. Slovic, "Terrorism as hazard: A new species of trouble", *Risk Analysis, Society for Risk Analysis*, Vol. 22, No. 3, pp. 425-426, 2002.
- [21] Y. J. Cha. "A Study of Risk Perception, *Korean Policy Sciences Review, Korean Association For Policy Science*", Vol. 10, No. 4, pp. 181-201, 2006.
- [22] Y. J. Cha. "The Trend of Nuclear Risk Perception and Policy Implications : With Focus on the Lay People in the Capital Region", *The Journal of Korean Policy Studies*, Vol. 12, No. 1, pp. 1-20, 2012.
- [23] Jun-Young Go, Keun-Ho Lee, "SNS disclosure of personal information in M2M environment threats and countermeasures", *Journal of the Korea Convergence Society*, Vol. 5, No. 1, pp. 29-34, 2014.

고 두 희(Ko, Du Hee)



- 2009년 2월 : 성균관대학교 신문방송학과(학사)
- 2011년 8월 : 성균관대학교 신문방송학과(석사)
- 2012년 3월 ~ 현재 : 성균관대학교 신문방송학과 박사과정 수료
- 관심분야 : 리스크, 디지털미디어
- E-Mail : jongsinyang@naver.com

원 영 아(Won, Young A)



- 2008년 2월 : 금강대학교 일본어통역학과(학사)
- 2011년 9월 : 일본 와세다대학교 정치학연구과(석사)
- 2013년 3월 ~ 현재 : 성균관대학교 신문방송학과 박사과정 수료
- 관심분야 : SNS, 사이버커뮤니케이션
- E-Mail : youngawon@naver.com