Journal of the Korea Academia-Industrial cooperation Society
Vol. 21, No. 6 pp. 646-661, 2020

https://doi.org/10.5762/KAIS.2020.21.6.646
ISSN 1975-4701 / eISSN 2288-4688

체계적 문헌 연구를 통한 사이버범죄 비즈니스 모델(CBM) 구축

박지용, 이희상*
성균관대학교 기술경영학과

A Study on the Establishment of Cybercrime Business Model(CBM) through a Systematic Literature Review

Ji-Yong Park, Heesang Lee*
Department of Management of Technology, Sungkyunkwan University

요 약 기술의 혁신과 빠르게 성장하는 새로운 인터넷 비즈니스는 기존 기업 경영의 패러다임을 바꾸고 사회에 다양한 영향을 주고 있다. 인터넷 기술의 발달은 기술 혁신에 대한 역효과 또한 상승시키고 있고, 특히 컴퓨터와 관련된 사이버범죄는 기술의 혁신과 함께 지속적으로 증가하고 있다. 본 연구의 목적은 사이버범죄를 줄이기 위해 비즈니스 모델 캔버스(BMC: Business Model Canvas) 이론을 사이버범죄에 활용하여 사이버범죄 비즈니스 모델(CBM: Cybercrime Business Model)을 구축하고 이 모델을 한국의 사이버범죄 유형에 적용시켜 분석하는 것이다. 본 연구에서는 사이버범죄의 구성요소를 찾기 위해 체계적 문헌 연구를 실시했으며, 이를 통해 키워드 기반의 문헌 탐색을 통해 적합한 60개의 문헌을 발굴하여 분류하였다. 또한 분류된 문헌의 정성적 연구를 수행해 사이버범죄의 구성 요소를 18개의 서브블록(sub-blocks)과 9개의 빌딩블록(building blocks)으로 도출하고 이를 BMC 이론에 대입하고 적절한 재정의를 통해 CBM을 구축하였다. 마지막으로 개발한 CBM을 한국의 사이버범죄에 적용하여 사이버 침해사고 대응 인력들에게 사이버범죄에 대한 분석적 이해를 도울 수 있었다. 본 연구는 사이버범죄를 감소시킬 수 있는 새로운 분석 틀을 마련하는데 기여하였다.

Abstract Technological innovations and fast-growing new internet businesses are changing the paradigm of traditional business management, having various impacts on society. The development of internet technology is also increasing the adverse effects on technological innovation, and in particular, cybercrime related to computers continues to increase with each technological innovation. The purpose of this study is to construct a cybercrime business model (CBM) by using the business model canvas (BMC) theory for cybercrime in order to reduce cybercrime, and this model is applied and analyzed based on types of Korean cybercrimes. For this study, a systematic literature review was conducted to determine the components of cybercrime, and 60 relevant documents were classified through a keyword-based literature search. Besides, qualitative research in the classified literature has led to the derivation of cybercrime into 18 sub-blocks and nine building blocks. This study applies BMC theory to this derivation of cybercrime and builds the CBM through proper redefinition. Lastly, the developed CBM could be applied to cybercrime in Korea to help cyber incident-response staff understand cybercrimes analytically. This study contributes to the development of a new analysis framework that can reduce cybercrime.

Keywords : Cybercrime business model, Cybercrime management, Business model, Cybercrime, Cybercrime in Korea

이 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No.2018R1D1A1B07050139)
*Corresponding Author : Heesang Lee(Sungkyunkwan University)
email: leehee@skku.edu
Received March 2, 2020 Revised April 20, 2020
Accepted June 5, 2020 Published June 30, 2020

1. 서론

컴퓨터의 기술 발달은 새로운 기업 경영에 혁신적인 방법을 제시하였다. 과거 기업은 오프라인을 통해 경영활동이 이루어졌으나 현재 기업은 인터넷 기술 혁신을 통해 일상생활과 관련된 비즈니스를 쉽고 빠르게 활용한다[1]. 이러한 컴퓨터의 기술 발달은 인류의 문화, 경제, 사회 전반에 걸쳐서 큰 변화를 주었지만, 컴퓨터 기술의 향상은 컴퓨터와 관련된 범죄의 급격한 상승을 초래하고 있다[2]. 예를 들어 한국 경찰청 통계에 따르면 한국의 사이버범죄는 2014년에 110,109건에서 2019년 180,499건으로 빠르게 성장하고 있다[3]. 이와 함께 사이버 세상에서의 범죄는 오프라인 방식의 범죄에서 인터넷을 이용한 새로운 방식으로 진화하고 있다[4]. 따라서 새롭게 변화와 진화하고 있는 사이버범죄에 대한 연구는 사이버 세상의 범죄의 위험을 낮추고 인터넷 기술이 보다 안전하고 유용하게 활용될 수 있는데 기여할 것이다[5].

그동안의 사이버범죄는 많은 변화를 이루었으며 개인적인 지적 호기심 또는 자기 과시를 통한 해킹에서 변화하여 금전적 갈취, 집단적인 사회 위협, 사이버 테러 등 조직적이고 체계적인 범죄 행위가 큰 비중으로 발전하고 있다[6]. 본 연구는 사이버범죄자들이 범죄를 계획하고 실행하여 범죄 피해자로부터 의도한 결과를 얻는 것을 기업가들이 비즈니스 모델을 통해 고객들에게 가치를 창출하는 것에 비교하여 파악하는 것은 사이버범죄를 분석하는 좋은 접근법이라는 아이디어로 연구가 시작되었다. 따라서 본 논문은 사이버범죄에 대한 구조적 파악을 위해 비즈니스 모델 분석에서 널리 쓰이는 비즈니스 모델 캔버스(BMC: Business Model Canvas, 이하 BMC) 이론을 차용하였다. 즉, 그간의 사이버범죄 분야의 문헌 연구를 정성적 코딩으로 분석하여 BMC의 9개의 빌딩블록 각각에 해당하는 사이버범죄의 구성 요소들을 도출하고, 도출된 구성 요소들을 사이버범죄의 서브블록과 빌딩블록으로 계층화하여 사이버범죄 비즈니스 모델(CBM: Cybercrime Business Model, 이하 CBM)을 구축하였다. 본 연구는 빠른 인터넷과 국민 대다수의 사용으로 사이버범죄가 급격히 상승한 한국의 사례를 CBM에 적용하여 분석하였다[3, 4]. 사이버범죄 핵심 구성 요소를 찾아보고 이를 통해 CBM을 만드는 과정은 사이버범죄의 구조와 특성을 알아볼 수 있는 좋은 방법이고, 제안된 CBM은 사이버범죄의 개별 행위에 대한 구체화된 분석에 도움을 줄 것이다[7].

본 연구의 1장은 사이버범죄와 CBM 구축에 대한 배경을 기술하였다. 2장은 사이버범죄에 대한 연구와 인터넷 비즈니스 모델에 대한 연구를 기술하였다. 3장의 연구 방법 및 결과는 정성적 문헌 분석을 통해 사이버범죄 서브블록, 빌딩블록, CBM과 이를 한국의 사이버범죄에 적용시켜 분석하여 사이버범죄 특성 및 현상을 도출한 결과를 보여준다. 4장은 결론 및 향후 연구 방향을 담았다.

2. 문헌연구

문헌 연구의 범위는 사이버범죄와 비즈니스 모델로 나누어 설명하였다. 사이버범죄는 그간의 사이버범죄의 정의와 사이버범죄에 대한 분류를 정리하였다. 비즈니스 모델의 문헌 연구는 그 간의 비즈니스 모델의 다양한 문헌 연구의 문제점을 지적하고 인프라, 재무, 가치제안, 고객 측면에서 비즈니스 모델을 분석할 수 있는 BMC 이론[8]을 중심으로 정리하였다.

2.1 사이버범죄와 분류

현대 사회는 PC와 스마트폰을 일상생활에서 많이 사용하고 있고 이와 함께 사이버 상에서 비즈니스는 지속적으로 늘어나고 있다. 사이버범죄는 인터넷 통신망을 이용하여 사이버 공간에서 이루어지는 범죄를 말한다[6,9]. 과거 사이버범죄는 컴퓨터와 네트워크에 집중되어 있었다면 최근의 사이버범죄는 이를 넘어서는 모바일 등의 다양한 기기를 통한 사이버 공간에서 행해지는 모든 유형의 범죄로 넓혀지고 있다[10].

사이버범죄의 유형에 관한 연구는 사이버범죄의 진화와 함께 지속적으로 이루어지고 있다. Table 1에서 Shinder와 Tittel은 다양한 사이버범죄를 통해 사람들에게 가해지는 폭력성이나 비폭력성을 사이버범죄의 구분에 중요한 요소로 보았고 이러한 인식은 피해자의 관점에서 발생하는 폭력성을 통한 구분에 근거하고 있다[11]. Dubey는 사이버범죄에 대상에 대해 사람, 사물, 정부, 회사, 사회로 구분하였고, 이러한 관점에서 사이버범죄는 사이버범죄 발생이 어떤 대상에게 발생하는지를 중심으로 나누어 연구해야 한다고 보았다[12]. Wall은 컴퓨터 무결성 범죄, 컴퓨터 지원 범죄, 컴퓨터 콘텐츠 범죄로 사이버범죄를 분류하여 컴퓨터를 활용하는 기술적 요소를 사이버범죄 구분의 중요한 요소로 보았다[13]. 한국 경찰청은 정보통신망의 침입・훼손・멸실하는 행위, 정보통신망을 주요 수단으로 범죄에 이용하는 행위, 불법콘텐츠 관련 범죄를 사이버범죄의 주요한 구분으로 보고 있고

[14-17] 범죄 행위의 유형에 근거하여 구분하고 있다. 사이버범죄 분류는 범죄 발생 시 특성 별 원인 분석에 꼭 필요하고 범죄 대응력 강화를 위해 필수적인 연구이다. 하지만 그동안의 사이버범죄 분류 연구는 피해자 유형, 폭력성 유무, 기술적 요소, 범죄 행위 유형 등 하나의 분류 기준만을 사용하여 구분하는 한계가 있었다. 또한 이러한 유형 연구는 범죄자, 피해자, 범죄 파트너 등 다양한 행위 주체들의 결합 유형과 이들 사이에 발생하는 범죄 행위 및 관련한 채널, 역량, 수익, 비용 등을 구조적이고 체계적으로 파악하기 어렵다는 약점이 있다.

Table 1. Types of Cybercrime

Researcher	Types of Cybercrime
Shinder and Tittel (2002)[11]	Violent or Potentially Violent Cybercrime Categories (Cyberterrorism, Assault by threat, Cyberstalking, Child pornography), Nonviolent Cybercrime Categories (Cybertrepass, Cyber theft, Cyberfraud, Destructive cybercrimes, Other cybercrimes)
Dubey (2004)[12]	Person(Defamation, Email, Spoofing, Unauthorized access・control), Property(Intellectual property crimes, Netrespass, Transmitting virus etc.), Government(Cyber terrorism financial etc.), Firm・Company(Distribution of pirated software, etc.), Society(Pornography crimes, etc.)
Wall (2007)[13]	Computer Integrity Crime(Hacking and Cracking, Denial of Service), Computer-Assisted Crime(Virtual Robberies, Scams and Thefts), Computer Content Crime(Pornography, Violence, Offensive Communication)
Korean National Police Agency (2019) [14-17]	Information Network Infringement Crime(Hacking, DDoS, Malicious program), Information Network Crime(Internet fraud, Cyber financial crime, Privacy·Location infringement, Cyber copyright infringement, Spam mail), Illegal content crime(Cyber pornography, Cyber gambling, Cyber defamation or stalking)

2.2 비즈니스 모델과 비즈니스 모델 캔버스(BMC)

비즈니스 모델(Business Model)이란 기업이 만든 가치를 고객에게 제공하는 것을 의미하고 이와 함께 금전적 이윤을 추구하는 것을 말한다[18]. 비즈니스 모델에 대한 연구는 인터넷 산업의 급속한 성장과 함께 1990년대 말 이후에 인터넷 비즈니스를 대상으로 많이 이루어졌다[19-20]. 그간의 비즈니스 모델에 대한 정의가 다양하고 비즈니스 모델의 개념과 핵심요소를 구성하는 방법론이 많아서 하나의 개념으로 정립하는 데에 문제가 있어 특정 비즈니스 모델에 적용하기가 쉽지 않고 실무적 관점에서 특성을 분석하기 어렵다는 비판이 있었다[21]. 따라서 본 논문은 실무적으로 뛰어나다고 평가받고 있고, 다음과 같이 비즈니스 모델의 구성 요소를 9개의 빌딩블록으로 나누어서 구조화하기 쉬운 BMC 이론을 활용하고자 한다[8].

Osterwalder와 Pignneur는 BMC 이론을 통해 조직, 고객, 이해 관계자들의 연결 및 가치 창출을 할 수 있는 비즈니스 전체에 대한 사업구조를 다음과 같이 설명하였다[8]. BMC 이론은 핵심파트너, 핵심활동, 핵심자원, 가치제안, 고객관계, 채널, 고객 세그먼트, 비용구조, 수익구조라는 9개의 빌딩블록을 Table 2와 같이 분류하고 Fig. 1과 같이 시각화하여 비즈니스 모델에 대한 새로운 이론을 정립하였다[22].

Table 2. Business model canvas's 9 building blocks[8]

Building blocks	Definition
Key Partnerships	It is a network of 'suppliers-partners' that can make business models run smoothly.
Key Activities	It is important things companies must do to do their business well.
Key Resources	It is the most important asset that is most necessary for the business to work.
Value Proposition	A combination of goods or services that create the value needed by a particular customer segment.
Customer Relationships	It refers to a form of relationship with a specific customer segment.
Channels	It is a way for companies to communicate and deliver goods or services to offer value to customer segment.
Customer Segments	It defines how different companies are targeting different types of people or organizations.
Cost Structure	All costs incurred in running a business model.
Revenue Stream	Revenue sources refer to the cash a company's working from customer segment.

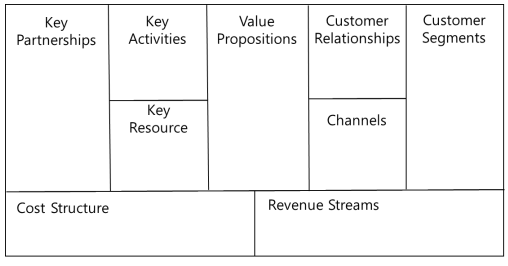

Fig. 1. Osterwalder's Business Model Canvas[8]

BMC 이론에서 핵심파트너(Key Partnerships)는 생산자가 모든 생산 활동을 할 수 없어 상호 간의 협력을 통해 효율성을 높일 수 있는 파트너를 의미한다. 생산자는 고객 확보를 위해 전략적 제휴나 타 기업의 지식을 확

보하는 방법을 통해서 핵심파트너를 확보한다[23].

BMC 이론에서 핵심활동(Key Activities)은 기업을 운영하기 위해 중요한 행동들을 말하고 가치제안, 채널, 고객관계를 창출하기 위해 필요한 활동을 의미한다[24]. 생산자의 핵심활동은 생산 활동, 문제해결, 플랫폼・네트워크 형성 활동을 말하고 이를 통해 비즈니스가 발생한다[8].

BMC 이론에서 핵심자원(Key Resources)은 생산자의 가치제안, 채널, 고객관계를 형성하기 위한 핵심적 수익창출원이다. 핵심자원은 크게 물적, 지적, 인적, 재무자원으로 구분된다[25].

BMC 이론에서 가치제안(Value Propositions)은 고객의 필요성을 채워주고 필요한 제품이나 서비스를 제공하는 가치를 의미한다[26]. 가치는 다양한 형태의 요청으로 창출되고 고객은 니즈에 의한 제품이나 서비스의 효용만 가치로 느끼는 것이 아니므로 가격 역시도 가치제안이라고 볼 수 있다[8].

BMC 이론에서 고객관계(Customer Relationships)는 생산자와 소비자 사이의 관계 형성을 의미한다. 기업은 고객관계를 통해 고객이 구매를 촉진하고 서비스를 받도록 유도할 수 있다[27].

BMC 이론에서 채널(Channels)은 생산자와 소비자 사이의 제품이나 서비스를 전달할 수 있는 방법이고 채널은 생산자가 제공하는 제품이나 서비스의 이해 및 고객평가를 높이는 방법으로도 사용됨을 의미한다[28]. 채널은 생산자가 직영점이나 파트너를 통해 판매할 수 있는 조직을 말하고 최근에는 웹사이트도 이에 해당한다[8].

BMC 이론에서 고객 세그먼트(Customer Segments)는 다양한 고객 중에서 기업이 자신의 사업이 목표로 하는 고객 그룹을 의미한다. 고객은 원하는 것이 다양하고 고객마다 다른 욕구를 가지고 있어 생산자가 필요한 요소를 정확히 인식하여 고객에게 필요한 제화를 제공해야 한다[29].

BMC 이론에서 비용구조(Cost Structure)는 가치창출, 채널, 수익구조의 형성을 위해서 발생하는 비용을 의미한다. 생산자는 비용을 최소한으로 하여 비즈니스를 구성하여야 최대의 이익을 얻을 수 있다[30].

BMC 이론에서 수익구조(Revenue Stream)는 생산자가 소비자로부터 얻는 수익을 의미한다. 다양한 비즈니스의 발달로 인하여 수익구조는 단순 판매를 통해 얻는 수익뿐만 아니라 서비스를 제공하고 얻는 부과 수익과 가입비 등도 해당한다[31].

본 논문은 BMC 이론의 9개 빌딩블록을 활용하여 사이버범죄의 핵심 요소를 정의하고 이를 통해 CBM을 구축하였다. CBM은 일반 비즈니스 모델이 아닌 사이버범죄에 대한 모델이므로 범죄에 대한 프로세스나 범죄 구조의 파악이 일반 비즈니스와는 다르므로 BMC 이론을 그대로 적용하는 것은 무리가 있다. 따라서 본 연구는 사이버범죄의 구조를 파악하기 위해, 일차적으로는 BMC 이론이 제공하는 블록구조를 연역적으로 사용하고, 이를 서브블록으로 세분화한 후, 이차적으로는 세분화된 서브블록에서 다시 상위 개념으로 계층화하면서 블록의 이름을 다시 재정의하는 귀납적 과정을 사용하였다.

3. 연구 방법 및 결과

3.1 연구 방법

본 논문은 사이버범죄를 비즈니스 관점에서 분석하는 관련 연구가 많이 진행되지 않았기 때문에 아직까지 정확하게 정의되지 않은 문제에 대해 이론을 만들어 가는 근거 이론(Ground theory)에 기반을 두어 연구를 진행하였다[32]. Strauss와 Corbin이 주장한 근거 이론은 데이터를 정성적으로 분석(Qualitative data analysis)[33-34]하고 이를 코딩하여 이론을 정립하는 방법론이다[35]. 또한 키워드 기반의 탐색적 문헌연구와 체계적 문헌 고찰(Systematic Literature Review)을 이용하여 근거 이론의 데이터를 확보하여 정성적 코딩을 수행하였다[36-37].

Fig. 2는 본 논문의 연구 방법과 절차에 관해 설명하고 있다. 이 논문은 60개의 연구를 체계적 문헌 고찰 방법[36-37]으로 문헌의 내용 데이터를 해체하여 키워드를 찾아내는 방식인 오픈 코딩(Open Coding)[35]을 통한 범주화 작업을 수행하였다. 문헌 고찰을 위해서는 세계 최대 규모의 학술 문헌 데이터인 SCOPUS를 통해 검색하였다.

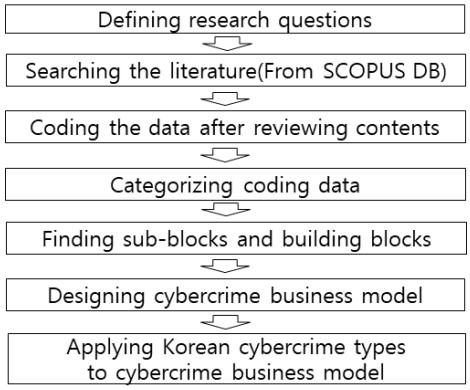

Fig. 2. Building the theory through qualitative data analysis

Fig. 3은 Fig. 2의 문헌 수집 및 선정과정을 설명한다. 우선 사이버범죄의 핵심 요소를 찾기 위해 'Cybercrime' 용어 및 'Cyber incident' 용어가 나오는 문헌을 SCOPUS에서 검색하였다. 2000년 이후로부터 2019년 10월까지의 검색된 420개의 문헌 중 다른 연구자들에게 인용을 통해 입증된 피인용 횟수가 1회 이상인 232개의 문헌을 선별하였다. 본 논문은 연구자 2인의 초록 리뷰를 통해 사이버범죄 블록 추출에 적합한 60개의 문헌을 최종으로 선택하였다. 초록 리뷰 시 문헌의 선택 기준은 관련 주제인 사이버범죄와의 연관성이 명확히 제시되어 있거나 사이버범죄에 대한 세부 분류의 연구가 포함된 문헌을 대상으로 선택하였다.

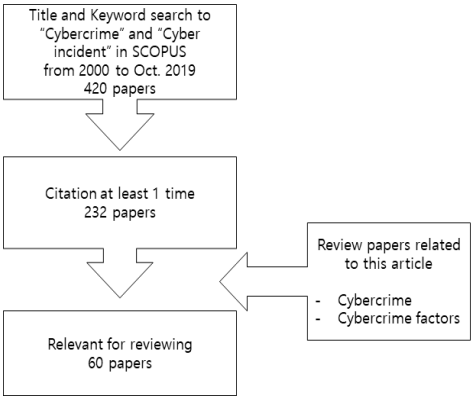

Fig. 3. Search method and process

Fig. 4는 상위 개념으로 카테고리화하기 위해 관련 논문을 오픈 코딩 작업을 거쳐 개념으로 도출하고 범주화를 거쳐 사이버범죄 서브블록과 빌딩블록을 도출하는 것

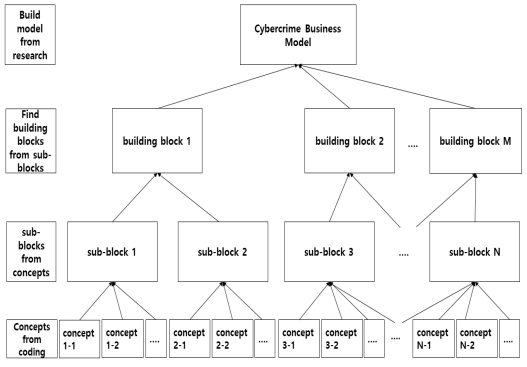

Fig. 4. Process of categorizing from sources and building theory

을 설명한다. 오픈 코딩은 60편의 논문의 초록 리뷰를 통해 관련된 연관성 있는 논문에서 서브블록 도출 시 문헌 중복 적용을 허용하였다. 도출된 개념은 상위 개념인 18개의 서브블록으로 카테고리화하였고, 이를 통해 BMC 이론의 빌딩블록에 대응하는 범주화된 9개의 빌딩블록이 귀납적으로 도출되었다. 최종적으로 본 논문은 위에서 도출된 사이버범죄의 서브블록과 빌딩블록의 명칭을 재정의하여 CBM을 구축하였다.

3.2 연구 결과

3.2.1 사이버범죄 블록 및 사이버범죄 비즈니스 모델 (CBM) 구축

BMC 이론의 첫 번째 빌딩블록인 핵심파트너는 해당 기업이 최소한의 비용을 가지고 최대의 자원을 확보하여 경쟁력 있는 사업 전개를 위한 필수적인 외부 조직이다[23]. 앞서 체계적 문헌 분석에서 찾은 60개의 문헌에서 BMC 이론의 핵심파트너에 해당하는 CBM의 관련 요소를 Table 3의 문헌들에 기반을 두어 다음과 같이 도출하였다.

먼저 Table 3에 언급된 문헌[38-43]은 범죄자가 사이버범죄의 성공을 위해 필요한 역량을 가진 개인이나 집단의 협력을 통해 자신이 부족한 역량과 자원을 보완하여 사이버범죄를 실행하는 것을 논의하고 있어 이와 같은 요소를 "범죄 종범(Crime Accomplice)"이라는 이름으로 첫 번째 서브블록으로 도출하였다. 다음으로 문헌[39,43-45]은 서비스 거부 공격을 위한 좀비 PC, 악성코드 감염을 통한 정보 유출, 통장 명의 도용자 등과 같이 범죄자가 타인의 자원이나 역량을 당사자 모르게 악용하는 것에 대해 논의하고 있음으로 이와 같은 요소를 "비자발적 협력자(Unintentional Cooperator)"이라는 이름으로 서브블록을 카테고리화하였다. 사이버범죄의 경우 일반 비즈니스에서의 파트너십과는 달리 이와 같은 비자발적인 외부 협력도 매우 중요한 특징을 가지고 있다. 이 두 가지 서브블록의 내용을 검토하여 상위 개념으로 범주화한 BMC 이론의 핵심파트너에 해당하는 CBM의 빌딩블록은 사이버범죄 실행을 위해 범죄자의 외부에서 사이버범죄를 도와주거나 이용되는 "사이버범죄 파트너쉽(Cybercrime Partnerships)"라고 정의하였다.

BMC 이론의 두 번째 빌딩블록인 핵심활동은 기업이 비즈니스 상에서 꼭 필요한 활동을 수행하는 것을 의미하고, 기업은 핵심활동을 통해 핵심자원을 이용하며 핵심파트너를 활용하여 가치제안을 만들어 내는 것이다[24].

Table 3에 언급된 문헌[42,46-58]은 인터넷 사기, 인터넷 금융사기(피싱, 파밍, 스미싱) 등의 다양한 수단을 통해 범죄자가 피해자에게서 금전적 이익을 취하는 범죄활동이다. 따라서 이러한 행위를 "경제범죄행위(Economic Crime Activities)"라는 이름의 서브블록으로 도출하였다. 다음으로 문헌[44,46,52,54,59]은 사이버 명예훼손 및 모욕과 사이버 스토킹의 다양한 수단을 통해 범죄자가 피해자의 명예를 훼손하거나, 사회적 평판을 파괴하는 범죄활동에 대해 논의하고 있다. 따라서 이러한 행위를 "사회범죄행위(Social Crime Activities)"라는 이름의 서브블록으로 카테고리화하였다. 사이버범죄의 경우 일반적인 비즈니스의 핵심활동과는 달리 고객에게 제공하는 가치를 높이기 위해 수행되는 것이 아니라 자신의 경제적 이득이나 피해자의 사회적 가치의 훼손을 추구한다는 점이 큰 특징이다. 따라서 BMC 이론의 핵심활동에 해당하는 CBM의 빌딩블록은 "범죄 행위(Criminal Activities)"라는 이름으로 정의하였다.

BMC 이론의 세 번째 빌딩블록인 핵심자원은 생산자의 원활한 비즈니스 진행을 위해 가장 필요한 중요자산을 의미하고, 물적, 지적, 인적, 재무적 자원을 말한다[25]. Table 3에서 말하고 있는 문헌 [49,59-63]은 범죄자가 성공적 범죄 수행을 위해 취약점을 찾아 범죄 행위를 하여 범죄 수익을 발생하는 전체적 범죄 수행 능력을 "범죄자 역량(Offender's Capabilities)"이라는 이름으로 서브블록을 도출하였다. 앞에서 말한 범죄자 역량은 사이버범죄 성립에서 중요한 부분이며, 이 빌딩블록은 하나의 서브블록만으로 상위 개념으로 범주화를 수행하여 "범죄 역량(Criminal Capabilities)"으로 정의하였다.

Table 3. Categories through literature sources

BMC building blocks	CBM building blocks	CBM sub-blocks	Sources
Key Partnerships	Cybercrime Partnerships	Criminal Accomplice	Al-Mhiqani(2018)[38], Dupont(2017)[39], Kao(2017)[40], Al-garadi(2016)[41], Prayudi(2015)[42], de Graaf(2013)[43]
		Unintentional Cooperator	Dupont(2017)[39], Sood(2017)[44], de Graaf(2013)[43], Skopik(2013)[45]
Key Activities	Criminal Activities	Economic Crime Activities	e Silva(2018)[46], Leukfeldt(2017)[47], Hui(2017)[48], Kao(2016)[49], Konradt(2016)[50], Prayudi(2015)[42], Pieschl(2015)[51], Holt(2013)[52], Sood(2013)[53], Soudijn(2012)[54], Kuzmin(2012)[55], Kigerl(2011)[56], Redford(2011)[57], McCombie(2009)[58]
		Social Crime Activities	Gassó(2019)[59], e Silva(2018)[46], Sood(2017)[44], Holt(2013)[52], Soudijn(2012)[54]
Key Resources	Criminal Capabilities	Offender's Capabilities	Gassó(2019)[59], Ahmed(2018)[60], Kao(2016)[49], Vasilomanolakis(2015)[61], Tariq(2012)[62], Sukhai(2004)[63]
Value Propositions	Cyber Attack	Cyber Trick	Nadir(2018)[64], Mbaziira(2018)[65], Kigerl(2011)[56], McCombie(2009)[58]
		Secretly Intrusion	Kao(2017)[40], Settanni(2016)[66], Eddolls(2016)[67], Ionita(2015)[68], Prayudi(2015)[42], de Graaf(2013)[43]
Customer Relationships	Exploring Vulnerabilities	Software/Hardware Vulnerabilities	Alrimawi(2017)[69], Hopkins(2015)[70], Armin(2015)[71], Eriksen-Jensen(2013)[72]
		Social Engineering	Virtanen(2017)[73], Bentaleb(2015)[74], Leukfeldt(2014)[75]
Channels	Cyber Connections	Wireless Connection	Al-garadi(2016)[41], Bele(2014)[76], Gerard(2013)[77], Lin(2011)[78]
		Wired Connection	Al-garadi(2016)[41], Bargh(2012)[79], Davis(2009)[80], Redford(2011)[57]
		Phone Connection	Manky(2013)[81]
Customer Segments	Victim	Targeted Victim	Reep-van den Bergh(2018)[82], van de Weijer(2018)[83], Kaakinen(2018)[84], Junger(2017)[85], van de Weijer(2017)[86], Al-garadi(2016)[41], Pieschl(2015)[51], Al-Nemrat(2015)[87], Goucher(2010)[88]
		Untargeted Victim	Dupont(2017)[39], Sood(2017)[44], Junger(2017)[85], van de Weijer(2017)[86], Konradt(2016)[50], De Graaf(2013)[43], Goucher(2010)[88], McCombie(2009)[58]
Cost Structure	Criminal Costs	Criminal Technical Costs	Allodi(2016)[89], Nagurney(2015)[90], Alazab(2013)[91]
		Criminal Effort	Dupont(2017)[39], Sood(2017)[44], Holt(2013)[52], de Graaf(2013)[43]
Revenue Stream	Criminal Revenue	Social Chaos	Dupont(2017)[39], Sood(2017)[44], Hui(2017)[48], Settanni(2016)[93]
		Crime Money	Nadir(2018)[64], Leukfeldt(2017)[47], Hui(2017)[48], Romanosky(2016)[94], Hopkins(2015)[70], Doyon-Martin(2015)[95], Redford(2011)[57], Joode(2011)[96], Joffee(2010)[97], Ben-Itzhak(2009)[98]

BMC 이론의 네 번째 빌딩블록인 가치제안은 고객 세그먼트가 필요로 하는 가치를 위한 상품이나 서비스의 조합이고 고객에게 무엇을 줄 수 있는지를 말한다[26]. Table 3의 문헌 [56,58,64-65]은 사이버범죄를 위해 사이버 상에서 피해자에게 거짓 믿음을 통해 물품이나 용역을 제공할 것처럼 속이는 것, 가짜의 물품으로 속여서 파는 것 등의 "속이는 기술(Cyber Trick)"로 서브블록을 카테고리화하였다. 문헌[40,42-43,66-68]은 기업이나 개인의 시스템, PC, 모바일 폰 등에 비밀스럽게 침투하여 피해자에게 모르게 피해를 일으키는 작업을 논의하고 있어, 시스템에 침투하여 범죄를 수행하는 "침투 기술(Secretly Intrusion)"로 서브블록을 도출하였다. "속이는 기술(Cyber Trick)"과 "침투 기술(Secretly Intrusion)"의 서브블록은 BMC 이론의 가치제안을 검토하여 CBM의 빌딩블록으로 "사이버 공격(Cyber Attack)"으로 정의하였다.

BMC 이론의 다섯 번째 빌딩블록인 고객관계는 생산자가 고객 확보・유지・촉진을 위해 어떠한 관계를 맺을 것인가를 의미하고 고객들에게 어떠한 재화나 서비스를 제공할지를 의미한다[27]. 범죄자가 피해자의 소프트웨어・하드웨어의 취약점을 찾아내어 범죄를 수행하는 것으로 Table 3의 문헌[69-72]을 검토하여 서브블록으로 "소프트웨어・하드웨어 취약점(Software/Hardware Vulnerabilities)"으로 카테고리화하였다. 문헌[73-75]은 범죄 수행 시 피해자에게 비기술적인 사회 공학 방법으로 피해자에게 겁을 주거나 약점을 이용하여 범죄를 수행하는 것을 의미하므로 서브블록으로 "사회 공학(Social Engineering)"을 도출하였다. BMC 이론의 고객관계는 두 개의 서브블록을 상위 개념화하여 빌딩블록인 "취약점 공략(Exploring Vulnerabilities)"으로 정의하였다.

BMC 이론의 여섯 번째 빌딩블록인 채널은 생산자가 고객에게 가치를 제공할 수 있는 방법을 말하고, 제품이나 서비스를 전달하는 방법을 의미한다[28]. 따라서 채널은 CBM에서 사이버 연결에 해당하고 사이버범죄는 사이버 공격을 수행하기 위해 피해자와의 연결할 수 있는 방법이 필요하다. Table 3의 문헌[41,76-78]은 사이버범죄 수행 시 사용하는 연결 방법으로 "무선연결(Wireless Connection)"로 카테고리화했고, 문헌[41,57,79-80]은 사이버범죄에 사용되는 연결 방법 중 "유선연결(Wired Connection)"로 서브블록을 도출하였다. 이와 함께 문헌[81]은 사이버 공격 방법은 사회 공학적인 방법으로 유행하고 있는 "전화 연결(Phone Connection)"를 이용한 방법으로 카테고리화하였다. 사이버범죄는 사이버 공격을 수행하기 위해 피해자와의 연결할 수 있는 방법이 필요하고 BMC 이론의 채널은 세 개의 서브블록을 범주화하여 빌딩블록으로 "사이버 연결(Cyber Connections)"로 정의하였다.

BMC 이론의 일곱 번째 고객 세그먼트는 생산자가 비즈니스 상에서 고객의 필요한 제품이나 서비스를 파악하는 것이고, 고객별로 원하는 니즈를 찾아 이를 충족하여 성공적 사업을 이루는 것을 말한다[29]. 사이버범죄는 범죄의 발생 요인으로 피해자가 필요하고 범죄가 만일 피해자가 없다면 더 이상의 범죄가 발생 되지 않을 것이다. Table 3의 문헌[41,51,82-88]은 범죄 피해자를 특정 대상으로 하는 범죄로 서브블록을 "특정 대상 피해자(Targeted Victim)"로 카테고리화하였다. 문헌[39,43-44,50,58,85-86,88]은 범죄의 대상 범위를 넓게 보고 있고 특정 대상으로 하지 않는 범죄로서 서브블록을 "불특정 대상 피해자(Untargeted Victim)"로 도출하였다. BMC 이론의 고객 세그먼트는 위의 두 개의 서브블록을 상위 개념화하여 빌딩블록인 "피해자(Victim)"로 정의하였다.

BMC 이론의 여덟 번째 빌딩블록인 비용구조는 생산자가 고객에게 가치 제공, 채널, 고객관계, 핵심활동, 핵심파트너를 통해 기업을 운영하는 데 필요한 비용을 의미하고[30] CBM에서의 비용구조는 사이버범죄를 수행하는 범죄 비용에 해당한다. Table 3의 문헌[89-91]은 범죄 수행을 위해 사이버범죄에 기술적으로 필요한 "범죄 기술 비용(Criminal Technological Costs)"으로 서브블록을 카테고리화하였다. 문헌[39,43-44,52]은 서브블록으로 범죄의 성공을 위한 "다각적 범죄 수행 노력(Criminal Effort)"으로 도출하였다. BMC 이론의 비용구조는 두 개의 서브블록을 범주화하여 빌딩블록을 "범죄 비용(Criminal Costs)"으로 정의하였다.

BMC 이론의 아홉 번째 빌딩블록인 수익원은 생산자가 고객으로부터 얻은 수입을 의미하고, 비즈니스 모델을 통해 창출된 전체 수익을 말한다[31]. 사이버 범죄자들의 목표는 범죄를 통해 얻어지는 비경제적 또는 경제적 수익이다. 사이버범죄가 범죄자의 만족감을 성취하기 위해 일어난다는 연구[92]가 있으며, Table 3의 문헌[39,44,48,93]은 정치적 목적을 가지고 사이버범죄를 수행하는 방법을 "사회 혼란(Social Chaos)"이란 서브블록으로 카테고리화하였다. 문헌[47-48,57,64,70,94-98]은 사이버범죄의 범죄자들의 주된 원인인 경제적 부분을 논의하고 있어 서브블록을 "금전 수익(Crime Money)"으로 도출하였다. BMC 이론의 수익원은 두 개의 서브블록

을 상위 개념화하여 “범죄 수익(Criminal Revenue)”이라는 빌딩블록으로 정의하였다.

Fig. 5은 연역적 코딩으로 BMC 이론의 빌딩블록에 해당하는 개념들을 도출하고 이를 귀납적 코딩을 통해 서브블록으로 카테고리화하고 이를 다시 CBM의 빌딩블록으로 범주화한 결과를 보여준다.

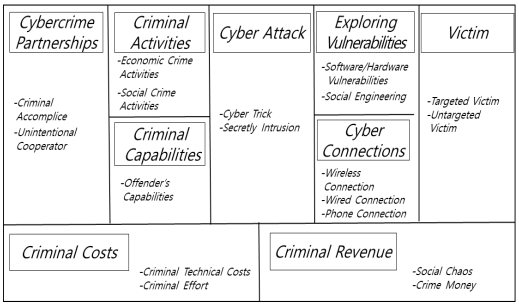

Fig. 5. Drawing Cybercrime Business Model through building blocks and sub-blocks.

정성적 코딩에 의해 도출된 9개의 빌딩블록은 사이버범죄 파트너쉽, 범죄 행위, 범죄 역량, 사이버 공격, 취약점 공략, 사이버 연결, 피해자, 범죄 비용, 범죄 수익이다. BMC 이론의 빌딩블록 9가지를 통해 빌딩블록별로 개념을 도출한 문헌의 수는 Fig. 6과 같다. 중복을 허용하여 코딩을 진행하였으므로 Fig. 6의 문헌 수의 합은 Table 3에 사용된 문헌의 수인 60개보다 크다.

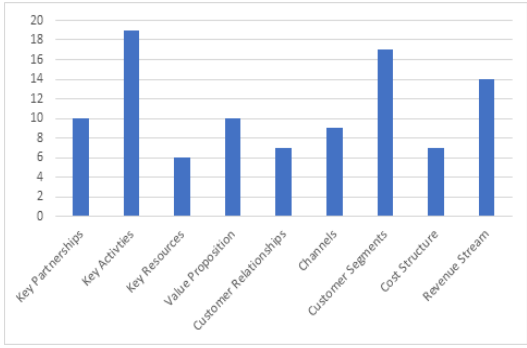

Fig. 6. Documents of the blocks by category

Table 4는 BMC 이론의 빌딩블록들과 새롭게 구축된 CBM의 빌딩블록의 차이를 설명하였으며 이 표에 기반하여 CBM의 빌딩블록의 이름들이 BMC 빌딩블록의 이름과는 다른 이름을 갖게 되었다. 표에서 보듯이 가장 큰 차이는 BMC에서의 가치제안 빌딩블록에서는 고객에게 가치를 제안하는 것으로, 고객은 이러한 가치제안에 기반하여 기업이 제공하는 제품이나 서비스를 구매하는 것으로 가치를 획득하고 기업은 이를 통해 이익을 달성하고자 비즈니스가 작동하였다. 하지만 CBM에서는 범죄자가 자신의 이익만을 위해 피해자에게 손해를 끼치는 일방적이고 범죄적인 구조이다. 따라서 CBM의 해당 빌딩블록의 명칭을 사이버 공격이라는 이름으로 정의하였다. 사이버 공격으로 범죄 행위가 진행됨에 따라 BMC의 고객관

Table 4. Renaming from BMC building blocks to CBM building blocks

BMC Building Blocks	CBM Building blocks	Difference
Key Partnerships	Cybercrime Partnerships	In BMC, the term, ‘key’ is appropriate to provide core value to customers, but in CBM, the term is changed as ‘cybercrime’ because a partnership is established to achieve ‘cybercrime’.
Key Activities	Criminal Activities	In BMC, the term, ‘key’ is appropriate to provide important business operation, but in CBM, the term is changed as ‘criminal’ because activities are performed for generating criminal profit.
Key Resources	Criminal Capabilities	In BMC, the term, ‘key’ is appropriate to supply important resources to the companies for key activities, but in CBM, criminal capabilities of criminals are critical resources for criminal activities. .
Value Proposition	Cyber Attack	In BMC, the business is established bilaterally by offering value from the company and by accepting the offered value by customers, but in CBM, cyber attacks are conducted to damage victims unilaterally.
Customer Relationships	Exploring Vulnerabilities	In BMC, business needs a way to establish an effective customer relationship, but in CBM, criminals seek a way to attack vulnerabilities of victims.
Channels	Cyber Connections	In BMC, companies can provide value to customers via marketing channels, but in CBM, criminals exploit suitable connection method for conducting cybercrime.
Customer Segments	Victim	In BMC, companies need to find suitable customer segments for their business orientation, but in CBM, criminals explore victims for their crimal activities.
Cost Structure	Criminal Costs	In BMC, business generates various business costs, and in CBM, criminals also needs financial costs and efforts required to conduct the crime.
Revenue Stream	Criminal Revenue	In BMC, value offering to the custmers returns revenue to companies, and in CBM, criminal revenue is generated by criminal activities.

계는 CBM에서는 취약점 공략, BMC의 채널은 CBM에서는 사이버 연결, BMC의 고객 세그먼트는 CBM에서는 피해자가 되어 BMC의 고객가치를 위해 작동하던 빌딩블록들이 CBM에서는 모두 범죄자의 이익과 피해자 손해라는 범죄 행위를 반영하는 빌딩블록 명칭으로 변경되었다. BMC의 다른 5가지 빌딩블록인 핵심파트너, 핵심활동, 핵심자원, 비용구조, 수익구조가 CBM에서 사이버범죄 파트너쉽, 범죄 행위, 범죄 역량, 범죄 비용, 범죄 수익 등으로 수정되는 것 역시 이처럼 CBM이 가치제안 대신에 사이버 공격이라는 범죄 행위로 작동되는 CBM의 특성에 따른 적절한 용어 수정이 된다.

3.2.2 사이버범죄 비즈니스 모델(CBM)의 적용

한국의 사이버범죄는 다양한 종류로 진화하고 급증하고 있으며[3], 한국에서의 사이버범죄 연구는 다른 국가에 비해 활발하게 진행되고 있다[4]. 다양한 범죄를 처리한 한국 경찰청의 사이버범죄 분류는 한국의 사이버범죄를 분류하기에는 적합하다고 판단하여 본 논문에서 구축한 사이버범죄 비즈니스 모델의 서브블록과 빌딩블록을 한국 경찰청에서 분류한 한국의 사이버범죄 분류 체계에 적용해 보았다[14-17]. Table 5는 CBM을 한국의 경찰청이 분류한 11개의 사이버범죄에 대입하여 분석한 결과이다. 한국 경찰청은 사이버범죄에 대해 해킹(Hacking), 서비스거부공격(DDoS), 악성프로그램(Malicious program), 인터넷 사기(Internet fraud), 사이버금융범죄(Cyber financial crime), 개인・위치정보 침해(Privacy・Location infringement), 사이버 저작권 침해(Cyber copy right infringement), 스팸메일(Spam mail), 사이버음란물(Cyber pornography), 사이버도박(Cyber gambling), 사이버 명예훼손・스토킹(Cyber defamation or stalking) 의 기술적 유형에 의해 11개로 분류하고 있다[14-17].

Table 5의 서브블록에서 행(row)은 CBM의 요소이고 열(column)은 한국 경찰청의 사이버범죄 유형이다. 본 연구는 한국의 사이버범죄를 경찰청 사이버범죄 유형(Table 5의 열)별로 구분하여 CBM을 적용하여 기존의 한국의 사이버 범죄가 유형별로 CBM의 빌딩블록, 서브블록의 내용이 어떻게 구성되는지를 분석하였다. Table 5의 셀에서 ◎는 대응하는 서브블록 행에 해당하는 사이버범죄 유형 열이 다른 범죄 유형보다 발생 요인이 높다는 의미이고, ○는 다소 있음을 의미한다. 반면, △는 다른 사이버범죄 유형보다 발생 요인이 낮고, X는 없음을 의미한다.

Table 5에서 해킹과 악성 프로그램의 열은 범죄 종범, 경제범죄행위, 범죄자 역량, 침투 기술, 소프트웨어・하드웨어 취약점, 범죄 기술 비용, 다각적 범죄 수행 노력, 사회 혼란, 금전 수익 등의 서브블록 행에서 ◎를 가지고 있어 다른 개인이나 집단의 협력과 금전적 피해가 많이 발생하고 다른 사이버범죄 유형보다 범죄자의 능력을 통한 기술적 침투나 소프트웨어・하드웨어 취약점을 이용한 범죄 수행을 특징으로 한다. 또한 해킹과 악성 프로그램의 열은 범죄 수행의 기술적 비용과 범죄의 수행 노력 서브블록 행이 매우 중요하고 다른 범죄에 비해 사회적 혼란을 이야기할 수 있는 범죄적 특징을 가지고 있음을 알 수 있다. 서비스 거부 공격 열은 범죄 종범, 비자발적 협력자, 경제범죄행위, 특정 대상 피해자, 범죄 기술 비용, 다각적 범죄 수행 노력, 사회 혼란, 금전 수익 등의 서브블록 행에 대응하는 셀에서 ◎를 가지고 있어 다른 개인이나 집단의 협력과 비자발적 협력이 필요하고 금전적 피해를 특정 대상으로 하는 범죄적 특징을 보여준다. 그리고 서비스 거부 공격 열은 해킹과 악성 프로그램의 열과 같이 기술적 비용이나 다각적 범죄 수행 노력 서브블록 행이 연관이 크므로 사회적 혼란이나 금전 수익을 목표로 한다. 인터넷 사기 열은 경제범죄행위, 속이는 기술, 사회 공학, 금전 수익 등의 서브블록 행에 대응해서 ◎를 가지고 있어 범죄를 통해 금전적 이익을 추구하고 속이는 기술을 사용하여 기술적 측면보다는 사람의 마음을 움직이는 사회 공학적 방법을 이용하는 특징이 있음을 알 수 있다. 사이버금융범죄 열은 범죄 종범, 비자발적 협력자, 경제범죄행위, 속이는 기술, 사회 공학, 전화 연결, 불특정 대상 피해자, 다각적 범죄 수행 노력, 금전 수익 등의 서브블록 행에 대응해서 ◎를 가지고 있어 다른 개인이나 집단의 협력과 속이는 기술을 통해 비자발적 협력이 필요하고 사회 공학적 방법을 사용하여 금전적 이익이 발생하는 특징을 보인다. 또한 사이버금융범죄 열은 불특정 다수에게 범죄를 수행하기 위해 다각적인 수행 노력이 필요하고 다른 범죄 유형에 비해 유일하게 전화 연결 서브블록 행에 대응하는 특징을 가지고 있다. 개인・위치정보 침해 열은 범죄 종범, 비자발적 협력자, 금전 수익 등의 서브블록 행에 대응해서 ◎를 가지고 있어 다른 개인이나 집단의 협력과 비자발적 협력이 필요하고 금전적 이익을 중요시한다. 사이버 저작권 침해 열은 비자발적 협력자, 경제범죄행위, 특정 대상 피해자, 금전 수익 등의 서브블록 행에 대응해서 ◎를 가지고 있어 비자발적 협력을 통해 경제적 수익을 창출하고 특정 대상의 피해자에게 금전적 수익을 위한 범죄 수행이 특징이다.

스팸메일 열은 범죄 종범, 불특정 대상 피해자, 금전 수익 등의 서브블록 행에 대응해서 ◎를 가지고 있어 다른 개인이나 집단의 협력을 사용하여 불특정 대상자에게 손해를 입히고 금전 이익을 목표로 하는 범죄 특징을 가지고 있다. 사이버음란물과 사이버도박의 열은 경제범죄행위, 불특정 대상 피해자, 금전 수익 등의 서브블록 행에 대응해서 ◎를 가지고 있어 불특정 다수에게 금전적 이익을 얻기 위해 범죄를 수행한다. 마지막으로 사이버 명예훼손・스토킹 열은 사회범죄행위와 특정 대상 피해자 등의 서브블록 행에 대응해서 ◎를 가지고 있어 특정인에게 명예나 사회적 평판을 낮추는 범죄적 특징을 가지고 있다.

Table 5의 마지막 행은 우리나라에서 2019년 발생한 경찰청의 사이버범죄 유형별 사이버범죄 건수를 보여준다. 이 중 인터넷사기, 사이버 명예훼손・스토킹, 사이버 금융범죄의 비중이 상대적으로 높음을 알 수 있다. 본 연구에서 제안한 CBM을 통해 우리나라에서 상대적으로 자주 발생하는 이들 3가지 사이버 범죄에 대해 대응책을 모색하면 다음과 같다.

첫째, 인터넷사기는 CBM의 서브블록 중 '경제범죄행위, 속이는 기술, 사회 공학, 금전 수익' 등 4개의 서브블록에서 ◎를 가지고 있다. 이중 '속이는 기술, 사회 공학, 금전 수익' 등의 서브블록을 주목하면 다음과 같은 대책이 수립될 수 있다. 즉, 인터넷사기의 사이버 공격의 주된 발생 요인인 '속이는 기술' 서브블록에 대응하여 범죄의

Table 5. Korean cybercrime types apply to Cybercrime Business Model

CBM building blocks	CBM sub-blocks	Hacking	DDoS	Malicious program	Internet fraud	Cyber financial crime	Privacy· Location infringement	Cyber copyright infringement	Spam mail	Cyber pornography	Cyber gambling	Cyber defamation or stalking	etc.
Cybercrime Partnerships	Criminal Accomplice	◎	◎	◎	○	◎	◎	○	◎	○	○	○	
	Unintentional Cooperator	◎	◎	○	X	◎	◎	◎	△	△	X	○	
Criminal Activities	Economic Crime Activities	◎	◎	◎	◎	◎	○	◎	○	◎	◎	△	
	Social Crime Activities	○	○	○	△	△	○	○	△	○	X	◎	
Criminal Capabilities	Offender's Capabilities	◎	○	◎	○	○	○	○	△	△	○	△	
Cyber Attack	Cyber Trick	○	○	○	◎	◎	○	○	△	X	△	X	
	Secretly Intrusion	◎	○	◎	△	△	○	○	X	X	X	X	
Exploring Vulnerabilities	Software/ Hardware Vulnerabilities	◎	○	◎	△	△	△	X	X	X	X	X	
	Social Engineering	○	○	○	◎	◎	○	△	○	△	X	△	
Cyber Connections	Wireless Connection	○	○	○	○	○	○	○	○	○	○	○	
	Wired Connection	○	○	○	○	○	○	○	○	○	○	○	
	Phone Connection	X	X	X	X	◎	X	X	X	△	△	△	
Victim	Targeted Victim	○	◎	○	○	○	○	◎	○	△	△	◎	
	Untargeted Victim	○	○	○	○	◎	○	X	◎	◎	◎	X	
Criminal Costs	Criminal Technical Costs	◎	◎	◎	△	○	○	○	○	△	○	△	
	Criminal Effort	◎	◎	◎	○	◎	△	△	○	△	△	△	
Criminal Revenue	Social Chaos	◎	◎	◎	X	X	△	△	△	△	△	△	
	Crime Money	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	△	
2019 Cases[3]		2,664	35	270	136,074	10,542	179	2,562	2,559	2,690	5,346	16,658	920

※ Criminal impact High : ◎, Medium: ○ , Low : △, N/A : X

교육과 홍보를 강조하고, 취약점 공략을 위해 피해자에게 겁을 주거나 약점을 이용하는 '사회 공학'으로 접근하는 것에 대비하여, 심리적 약점을 극복하고 신고를 통해 대비해야 한다. 둘째, 사이버 명예훼손·스토킹은 '사회범죄행위, 특정 대상 피해자'의 2개의 서브블록에서 ◎를 가지고 있다. 이 중 '특정 대상 피해자' 서브블록이 발생빈도가 높다는 점을 유의하면, 이들에게 발송되는 문자나 메일을 인터넷 서비스 제공자(Internet Service Provider)를 통한 차단 정책을 적용하는 것이 효과적일 것이다. 또한 명예훼손·스토킹 범죄자들의 '사회범죄행위'의 규모와 사이버 명예훼손·스토킹 사건의 빈도수를 적극적으로 홍보할 필요가 있다. 셋째, 사이버금융범죄는 '범죄 종범, 비자발적 협력자, 경제범죄행위, 속이는 기술, 사회 공학, 전화 연결, 불특정 대상 피해자, 다각적 범죄 수행 노력, 금전 수익' 등 9개의 서브블록에서 ◎를 가지고 있다. 이 중 '범죄 종범' 및 '비자발적 협력자'라는 서브블록의 발생빈도가 높은 것을 주목하면, 범죄자들의 협력관계를 끊기 위한 잠재적 범죄 종범 및 비자발적 협력자에 대한 모니터링 및 검거를 강화하여야 할 것이다. '속이는 기술, 사회 공학, 전화 연결' 등의 서브블록이 발생 빈도가 높은 것을 주목하면, 범죄의 연결 고리인 피싱(Phishing)과 스미싱(Smishing) 등의 전화 연결, 문자, 메일을 정부 차원에서 차단하고, 일반 국민에 대해 '속이는 기술, 사회 공학' 등 범죄자들이 공략하는 수법에 대한 지속적인 교육과 홍보를 통해 범죄자에게 속지 않도록 해야 하여야 할 것이다.

4. 결론 및 향후 연구

본 연구는 사이버범죄 감소를 위해 BMC 이론과 근거이론에 기반한 데이터의 정성적 코딩을 통해 사이버범죄의 주요 요소를 도출하고 새롭게 CBM을 구축하였다. 그간의 범죄 연구는 범죄의 원인을 추측하는 등의 범죄 이론에 대한 연구가 많이 있었고, 이를 통해 범죄를 원인을 제거하려는 노력을 많이 하였다. 이 논문은 비즈니스 모델 관점에서 사이버범죄를 연구함으로써 범죄인의 범죄 행위의 주요 구성요인을 이해하여 사이버범죄를 감소시키고자 하는 새로운 관점의 연구였다. CBM이 제공하는 사이버범죄의 주요 요소인 18개의 서브블록과 9개의 빌딩블록은 사이버범죄의 세부적 내용을 새롭게 분석하게 해주었고 이를 통해 범죄의 발생 시 어떤 특성이 있는지와 어떻게 작동하는지에 대해 새로운 시각을 주었다고 판단한다. CBM 구축과 사례 연구는 사이버범죄에 대한 현상을 새로운 분석 틀로 활용함으로써 인터넷 정책 결정자, 수사기관, 인터넷 보안 기업에서 사이버범죄를 감소시키는데 사용될 수 있고, 사이버범죄에 대한 영향력 감소에 기여를 할 수 있을 것이다.

진화하고 있는 사이버범죄는 새로운 범죄 방법이나 기술들의 발생으로 인해 기존의 기술적 유형 분류에 의존한 분석 틀로는 쉽게 인지하기 어렵다. 따라서 본 논문이 제안한 CBM을 사용한다면 새롭게 등장하는 사이버범죄의 빌딩블록과 서브블록을 파악하면 사이버범죄의 분석에 도움을 받을 수 있을 것이다. 또한 궁극적으로 이러한 과정을 통해 사이버범죄 대응 인력이 진화하는 사이버범죄에 대한 신속한 대응과 빠른 범죄 인지를 통해 범죄 감소에 기여할 것이다.

본 연구의 한계점은 보안 사고의 보다 세부적인 실증적 검증과 새로운 사고 유형의 출현으로 본 연구가 도출한 서브블록과 빌딩블록이 개선할 필요가 있을 수 있다는 점이다. 따라서 향후 관심 있는 연구자는 CBM에 향후 출현할 새로운 사이버 사고 유형을 대입하여 빌딩블록과 서브블록에 대한 보완적 연구를 진행할 필요성이 있고 이를 통해 본 연구가 제안한 CBM은 완성도가 높아질 것이다.

References

[1] D. J. Teece, "Business Models, Business Strategy and Innovation", Long Range Planning, Vol.43, Issues2-3, pp.172-194, 2001.
DOI: https://doi.org/10.1016/j.lrp.2009.07.003

[2] B. Moon, J. D. McCluskey, & C. P. McCluskeyd, "A general theory of crime and computer crime: An empirical test", Journal of Criminal Justice, vol.38, Issue4, pp.767-772, 2010.
DOI: https://doi.org/10.1016/j.jcrimjus.2010.05.003

[3] https://www.police.go.kr/www/open/publice/publice0204.jsp

[4] S. Caneppele, & M. F. Aebi, "Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes", Policing, Vol.13, Issue1, Pages 66-79, 2017.
DOI: https://doi.org/10.1093/police/pax055

[5] P. Hunton, "The growing phenomenon of crime and the internet: A cyber crime execution and analysis model", Computer Law & Security Review, Vol.25, Issue6, pp.528-535, 2009.
DOI: https://doi.org/10.1016/j.clsr.2009.09.005

[6] R. Bryant, Investigating digital crime, Wildy, 2008, pp.79-93.

[7] E. Kraemer-Mbula, P. Tang, & H. Rush, "The cyber crime ecosystem; Online innovation in the shadows?", Technological Forecasting & Social Change, Vol.80, Issue3, pp.541-555, 2013.
DOI: https://doi.org/10.1016/j.techfore.2012.07.002

[8] A. Osterwalder & Y. Pigneur, Business Model Generation, Wiley, 2010, pp.20-57.

[9] http://en.wikipedia.org/wiki/Computer_crime.

[10] D. Halde, & K. Jaishankar, Cyber crime and the Victimization of Women: Laws, Rights, and Regulations, IGI Global, 2011, pp.12-33.

[11] D. L. Shinder, & E. Tittel, Scene of the cyber crime: Computer forensics handbook, Syngress Publishing, 2002, pp.18-33.

[12] http://www.mondaq.com/article.asp?articleid=28603

[13] D. Wall, Cybercrime: The transformation of crime in the information age, Malden, MA, Polity Press, 2007, pp.30-130.

[14] http://www.police.go.kr/www/security/cyber/cyber01.jsp

[15] https://cyberbureau.police.go.kr/prevention/nw/sub2_notitle.jsp?mid=010201

[16] https://cyberbureau.police.go.kr/prevention/nw/sub2_2_notitle.jsp?mid=010202

[17] https://cyberbureau.police.go.kr/prevention/nw/sub2_3_notitle.jsp?mid=010203

[18] A. Afuah, & C. L. Tucci, Internet Business Models and Strategies, McGraw-Hill, 2001, p.9-12.

[19] A. Osterwalder, Y. Pigneur, & C. L. Tucci, "Clarifying Business Models: Origins, Present, and Future of the Concept", Communications of the Association or information Systems, Vol.16, No.1, pp.1-25, 2005.
DOI: https://doi.org/10.17705/1CAIS.01601

[20] R. Alt, & H. Zimmermann, "Introduction to Special Section - Business Models", Electronic Markets, Vol.11, No.1, 2001.
DOI: https://doi.org/10.1080/713765630

[21] C. Zott, R. Amit, & L. Massa, "The business model: Theoretical roots, recent developments, and future research", IESE Business School Working Paper, University of Navarra, Barcelona, Spain, No.862. 2010.

[22] J. Ojasalo, & K. Ojasalo, "Service Logic Business Model Canvas", Journal of Research in Marketing and Entrepreneurship, Vol.20, No.1, pp.70-98, 2018.
DOI: https://doi.org/10.1108/JRME-06-2016-0015

[23] S. Keane, K. Cormican, & J. Sheahan, "Comparing how entrepreneurs and managers represent the elements of the business model canvas", Journal of Research in Marketing and Entrepreneurship, Vol.9, pp.65-74, 2018.
DOI: https://doi.org/10.1016/j.jbvi.2018.02.004

[24] A. Joyce, & R. Paquin, "The triple layered business model canvas: A tool to design more sustainable business models", Journal of Cleaner Production, Vol.135, pp.1474-1486, 2016.
DOI: https://doi.org/10.1016/j.jclepro.2016.06.067

[25] E. Türko, "Business plan vs business model canvas in entrepreneurship training: A comparison of students' perceptions", Asian Social Science, Vol.12, No.10, pp.55-62, 2016.
DOI: http://dx.doi.org/10.5539/ass.v12n10p55

[26] M. Urban, M. Klemm, K. Ploetner, & M. Hornung, "Airline categorisation by applying the business model canvas and clustering algorithms", Journal of Business Venturing Insights, Vol.71, pp.175-192, 2018.
DOI: https://doi.org/10.1016/j.jairtraman.2018.04.005

[27] M. Toro-Jarrín, I. Ponce-Jaramillo, & D. Güemes-Castorena, "Methodology for the of building process integration of Business Model Canvas and Technological Roadmap", Technological Forecasting and Social Change, Vol.110, pp.213-225, 2016.
DOI: https://doi.org/10.1016/j.techfore.2016.01.009

[28] B. Fritscher, & Y. Pigneur, "Classifying business model canvas usage from novice to master: A dynamic perspective", Lecture Notes in Business Information Processing, Vol.257, pp.134-151, 2016.
DOI: http://dx.doi.org/10.1007%2F978-3-319-40512-4_8

[29] M. Dudin, G. Kutsuri, I. Fedorova, S. Dzusova, & A. Namitulina, "The Innovative Business Model Canvas in the System of Effective Budgeting", Asian Social Science, Vol.11, No.7, pp.290-296, 2015.
DOI: http://dx.doi.org/10.5539/ass.v11n7p290

[30] B. Fritscher, & Y. Pigneur, "Visualizing business model evolution with the Business Model Canvas: Concept and tool", 16th IEEE Conference on Business Informatics, IEEE, Geneva, Switzerland, pp.151-158, 2014.
DOI: https://doi.org/10.1109/CBI.2014.9

[31] T. O'Neill, "The innovative business model canvas in the system of effective budgeting", Reference Services Review, Vol.43, No.3, pp.450-460, 2015.
DOI: http://dx.doi.org/10.1108/RSR-02-2015-0013

[32] B. Glaser, & A. Strauss(1967), The Discovery of Grounded Theory: Strategies for Qualitative research, Routledge, 2000, pp.21-160.

[33] E. Babbie, The practice of social research, Wadsworth Publishing, 2012, pp.88-122.

[34] A. Bryman, & E. Bell, Business research methods, Oxford University Press, 2015, pp. 578-604.

[35] J. M. Corbin, & A. L. Straus, Basics of qualitative research: Techniques and procedures for developing grounded theory, Sage publications, 2007, pp. 65-297.

[36] S. Green, "Systematic reviews and meta-analysis", Singapore medical journal, vol.46, no.6, pp.270-274,

2005.

[37] B. Paek, & H. Lee, "Exploratory research on the dynamic capabilities of leading firms: Research framework building", Journal of the Korea Academia-Industrial cooperation Society, Vol.16, No.12, pp.8262-8273, 2015.
DOI: https://doi.org/10.5762/KAIS.2015.16.12.8262

[38] M. N. Al-Mhiqani, R. Ahmad, W. Yassin, A. Hassan, Z. Z. Abidin, N. S. Ali, & K. H. Abdulkareem, "Cyber-Security Incidents: A Review Cases in Cyber-Physical Systems", International Journal of Advanced Computer Science and Applications, Vol.9, Issue1, pp.499-508, 2018.
DOI: https://doi.org/10.14569/IJACSA.2018.090169

[39] B. Dupont, "Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime", Crime, Law and Social Change, Vol.67, pp. 97-116, 2017.
DOI: https://doi.org/10.1007%2Fs10611-016-9649-z

[40] D. Kao, "Exploring the cybercrime investigation framework of ATM Heist from ISO/IEC 27043:2015", International Conference on Advanced Communication Technology, Vol.67, Issue1, pp.177-182, 2017.
DOI: https://doi.org/10.23919/ICACT.2017.7890079

[41] M. A. Al-garadi, K. D. Varathan, & S. D. Ravana, "Cybercrime detection in online communications: The experimental case of cyberbullying detection in the Twitter network", Computers in Human Behavior, Vol.63, pp.433-443, 2016.
DOI: https://doi.org/10.1016/j.chb.2016.05.051

[42] Y. Prayudi,, & S. Yusirwan, "The recognize of malware characteristics through static and dynamic analysis approach as an effort to prevent cybercrime activities", Journal of Theoretical and Applied Information Technology, Vol.77, No.3, pp.438-445, 2015.

[43] D. de Graaf, A. F. Shosha, & P. Gladyshev, "BREDOLAB: Shopping in the Cybercrime Underworld", International Conference on Digital Forensics and Cyber Crime, Indiana, USA, pp.302-313, 2013.
DOI: https://doi.org/10.1007/978-3-642-39891-9_19

[44] A. K Sood, S. Zeadally, & R. Bansal, "Cybercrime at a Scale: A Practical Study of Deployments of HTTP-Based Botnet Command and Control Panels", IEEE Communications Magazine, Vol.55, Issue7, pp.22-28, 2017.
DOI: https://doi.org/10.1109/MCOM.2017.1600969

[45] F. Skopik, & Q. Li, "Trustworthy incident information sharing in social cyber defense alliances", IEEE Symposium on Computers and Communications, IEEE, Split, Croatia, pp.233-239, 2013.
DOI: https://doi.org/10.1109/ISCC.2013.6754951

[46] K. K. e Silva, "Vigilantism and cooperative criminal justice: is there a place for cybersecurity vigilantes in cybercrime fighting?", International Review of Law, Computers & Technology, Vol.32, Issue1, pp.21-36, 2018.
DOI: https://doi.org/10.1080/13600869.2018.1418142

[47] E. R. Leukfeldt, A. Lavorgna, & E. R. Kleemans, "Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime", European Journal of Criminal Policy and Research, Vol.23, No.3, pp.287-300, 2017.
DOI: http://dx.doi.org/10.1007/s10610-016-9332-z

[48] K. Hui, S. Kim, & Q. Wang, "Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks", MIS Quarterly, Vol.41, No.2, pp.497-523, 2017.
DOI: http://dx.doi.org/10.25300/MISQ/2017/41.2.08

[49] D. Kao, "Cybercrime investigation countermeasure using created-accessed-modified model in cloud computing environments", The Journal of Supercomputing, Vol.72, Issue1, pp.141-160, 2016.
DOI: https://doi.org/10.1007/s11227-015-1516-7

[50] C. Konradt, A. Schillingb, & B. Wernersb, "Phishing: An economic analysis of cybercrime perpetrators", Computers and Security, Vol.58, pp.39-46, 2016.
DOI: https://doi.org/10.1016/j.cose.2015.12.001

[51] S. Pieschl, C. Kuhlmann & T. Porsch, "Beware of Publicity! Perceived Distress of Negative Cyber Incidents and Implications for Defining Cyberbullying", Journal of School Violence, Vol.14, No.1, pp.111-132, 2015.
DOI: https://doi.org/10.1080/15388220.2014.971363

[52] T. J. Holt, "Examining the Forces Shaping Cybercrime Markets Online", Social Science Computer Review, Vol.31, Issue2, pp.165-177, 2013.
DOI: https://doi.org/10.1177/0894439312452998

[53] A. K. Sood., R. Bansal, & R. J. Enbody, "Cybercrime: Dissecting the state of underground enterprise", IEEE Internet Computing, Vol.17, Issue1, pp.60-68, 2013.
DOI: https://doi.org/10.1109/MIC.2012.61

[54] M. R. J. Soudijn, & B. C. H. T Zegers, "Cybercrime and virtual offender convergence settings", Trends in Organized Crime, Vol.15, Issue2-3, pp.111-129, 2012.
DOI: https://doi.org/10.1007/s12117-012-9159-z

[55] A. Kuzmin, "State and trends of Russian cybercrime in 2011", 2012 IV International Congress on Ultra Modern Telecommunications and Control Systems, IEEE, St. Petersburg, Russia, pp.933-939, 2012.
DOI: https://doi.org/10.1109/ICUMT.2012.6459794

[56] A. Kigerl, "Routine Activity Theory and the Determinants of High Cybercrime Countries", Social Science Computer Review, Vol.30, Issue4, pp.470-486, 2011.
DOI: https://doi.org/10.1177/0894439311422689

[57] M. Redford, "U.S. and EU Legislation on Cybercrime", 2011 European Intelligence and Security Informatics Conference, IEEE, Athens, Greece, pp.34-37, 2011.

DOI: https://doi.org/10.1109/EISIC.2011.38

[58] S. McCombie, J. Pieprzyk, & P. Watters, "Cybercrime Attribution: An Eastern European Case Study", Proceedings of the 7th Australian Digital Forensics Conference, Edith Cowan University, Australian, pp.41-51, 2009.
DOI: https://doi.org/10.4225/75/57b2880840ccf

[59] A. M. Gassó, V. Fernández-Cruz, I. Montiel, C. Martin-Fumadó, & J. R. Agustina, "Retos forenses ante la cibercriminalidad social en menoresForensic challenges presented by social cybercrime in minors", Revista Española de Medicina Legal, Vol.45, Issue2, pp.73-76, 2019.
DOI: https://doi.org/10.1016/j.reml.2018.11.003

[60] A. S. Ahmed, S. Deb, A. S. B. Habib, M. N. Mollah, & A. S. Ahmad, "Simplistic Approach to Detect Cybercrimes and Deter Cyber Criminals", 2018 International Conference on Computer, Communication, Chemical, Material and Electronic Engineering, IEEE, Rajshahi, Bangladesh, 2018.
DOI: https://doi.org/10.1109/IC4ME2.2018.8465618

[61] E. Vasilomanolakis, S. Karuppayah, P. Kikiras, & M. Mühlhäuser, "A honeypot-driven cyber incident monitor: lessons learned and steps ahead", Proceedings of the 8th International Conference on Security of Information and Networks, ACM International Conference, Sochi, Russia, pp.158-164, 2015.
DOI: https://doi.org/10.1145/2799979.2799999

[62] M. Tariq, B. Aslam, I. Rashid, & A. Waqar, "Cyber threats and incident response capability - a case study of Pakistan", 2013 2nd National Conference on Information Assurance, IEEE, Rawalpindi, Pakistan, pp.15-20, 2013.
DOI: https://doi.org/10.1109/NCIA.2013.6725319

[63] N. B. Sukhai, "Hacking and cybercrime", 2004 Information Security Curriculum Development Conference, ACM International Conference, NY, USA, pp.128-132, 2004.
DOI: https://doi.org/10.1145/1059524.1059553

[64] I.. Nadir, & T. Bakhshi, "Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques", 2018 International Conference on Computing, Mathematics and Engineering Technologies, IEEE, Sukkur, Pakistan, March 2018.
DOI: https://doi.org/10.1109/ICOMET.2018.8346329

[65] A. V. Mbaziira, & D. R. Murphy, "An Empirical Study on Detecting Deception and Cybercrime Using Artificial Neural Networks", Proceedings of the 2nd International Conference on Compute and Data Analysis, ICCDA, IL, USA, pp.42-46, 2018.
DOI: https://doi.org/10.1145/3193077.3193080

[66] G. Settanni, Y. Shovgenya, F. Skopik, R. Graf, M. Wurzenberger & R. Fiedler, "Correlating cyber incident information to establish situational awareness in Critical Infrastructures", 2016 14th Annual Conference on Privacy, Security and Trust, IEEE, Auckland, New Zealand, pp.78-81, 2016.
DOI: https://doi.org/10.1109/PST.2016.7906940

[67] M. Eddolls, "Making cybercrime prevention the highest priority", Network Security, Vol.2016, Issue8, pp.5-8, 2016.
DOI: https://doi.org/10.1016/S1353-4858(16)30075-7

[68] M. Ionita, & V. Patriciu, "Cyber Incident Response Aided by Neural Networks and Visual Analytics", 2015 20th International Conference on Control Systems and Computer Science, IEEE, Bucharest, Romania, pp.229-233, 2015.
DOI: https://doi.org/10.1109/CSCS.2015.41

[69] F. Alrimawi, L. Pasquale, & B. Nuseibeh, "Software engineering challenges for investigating cyber-physical incidents", 2017 IEEE/ACM 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems, IEEE, Buenos Aires, Argentina, pp.34-40, 2017.
DOI: https://doi.org/10.1109/SEsCPS.2017.9

[70] M. Hopkins, & A. Dehghantanha, "Exploit Kits: The production line of the Cybercrime economy?", 2015 Second International Conference on Information Security and Cyber Forensics, IEEE, Cape Town, South Africa, pp.23-27, 2015.
DOI: https://doi.org/10.1109/InfoSec.2015.7435501

[71] J. Armin, P. Foti, & M. Cremonini, "0-Day Vulnerabilities and Cybercrime", 10th International Conference on Availability, Reliability and Security, IEEE, Toulouse, France, pp.711-718, 2015.
DOI: https://doi.org/10.1109/ARES.2015.55

[72] M. Eriksen-Jensen, "Holding back the tidal wave of cybercrime", Computer Fraud and Security, Vol.2013, No.3, pp.10-16, 2013.
DOI: https://doi.org/10.1016/S1361-3723(13)70028-9

[73] S. M. Virtanen, "Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities", Psychiatry, Psychology and Law, Vol.23, Issue3, pp.323-338 , 2017.
DOI: https://doi.org/10.1080/13218719.2017.1315785

[74] Y. Bentaleb, A. Abarda, H. Mharzi, & S. E. Hajji, "Application of latent class analysis to identify the youth population who risk being cybercrime victim on social networks", Contemporary Engineering Sciences, Vol.8, No.32, pp.1529-1534, 2015.
DOI: https://doi.org/10.12988/ces.2015.58261

[75] E. R. Leukfeldt, "Cybercrime and social ties: Phishing in Amsterdam", Trends in Organized Crime, Vol.17, Issue4, pp.231-249, 2014.
DOI: https://doi.org/10.1007/s12117-014-9229-5

[76] J. L. Bele, M. Dimc, D. Rozman, & A. S. Jemec, "Rasing awarenss of cybercrime - the use of education as a means of prevention and protection", 10th International Conference Mobile Learning 2014, Madrid, Spain, pp.281-284, 2014.

[77] P. Gerard, N. Kapadia, J. Acharya, P. T. Chang, & Z. Lefkovitz, "Cybersecurity in Radiology: Access of Public Hot Spots and Public Wi-Fi and Prevention of Cybercrimes and HIPAA Violations", American Journal of Roentgenology, Vol.201, No.6, pp.1186-1189, 2013. DOI: https://doi.org/10.2214/AJR.12.9651

[78] I. Lin, Y. Yen, & A. Chang, "A Study on Digital Forensics Standard Operation Procedure for Wireless Cybercrime", 2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IEEE, Seoul, South Korea, pp.543-548, 2011.
DOI: https://doi.org/10.1109/IMIS.2011.58

[79] M. S. Bargh, S. Choenni, I. Mulder, & R. Pastoor, "Exploring a Warrior Paradigm to Design Out Cybercrime", 2012 European Intelligence and Security Informatics Conference, IEEE, Odense, Denmark, pp.84-90, 2012.
DOI: https://doi.org/10.1109/EISIC.2012.40

[80] G. Davis, A. Garcia, & W. Zhang "Empirical Analysis of the Effects of Cyber Security Incidents", Risk Analysis, Vol.29, No.9, pp.1304-1316, 2009.
DOI: https://doi.org/10.1111/j.1539-6924.2009.01245.x

[81] D. Manky, "Cybercrime as a service: a very modern business", Computer Fraud & Security, Vol.2013, Issue6, pp.9-13, 2013.
DOI: https://doi.org/10.1016/S1361-3723(13)70053-8

[82] C. M. M. Reep-van den Bergh, & M. Junger, "Victims of cybercrime in Europe: a review of victim surveys", Crime Science, Vol.7, No.5, 2018.
DOI: https://doi.org/10.1186/s40163-018-0079-3

[83] S. G. A. van de Weijer, R. Leukfeldt, & W. Bernasco, "Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking", European Journal of Criminology, Vol.16, Issue4, pp.486-508, 2018.
DOI: https://doi.org/10.1177/1477370818773610

[84] M. Kaakinen, T. Keipi, P. Räsänen, & A. Oksanen, "Cybercrime Victimization and Subjective Well-Being: An Examination of the Buffering Effect Hypothesis Among Adolescents and Young Adults", Cyberpsychology, Behavior, and Social Networking, Vol.21, No.20, pp.129-137, 2018.
DOI: https://doi.org/10.1089/cyber.2016.0728

[85] M. Junger, L. Montoya, P. Hartel, & M. Heydari, "Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in europe", 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment, Cyber SA, IEEE, London, UK, June 2017.
DOI: https://doi.org/10.1109/CyberSA.2017.8073391

[86] S. G. A. van de Weijer, & E. R. Leukfeldt, "Big Five Personality Traits of Cybercrime Victims", Cyberpsychology, Behavior, and Social Networking, Vol.20, No.7, 2017.
DOI: https://doi.org/10.1089/cyber.2017.0028

[87] A. Al-Nemrat, & C. Benzaid, "Cybercrime Profiling: Decision-Tree Induction, Examining Perceptions of Internet Risk and Cybercrime Victimisation", 214th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, Helsinki, Finland, pp.1380-1385, August 2015.
DOI: https://doi.org/10.1109/Trustcom.2015.534

[88] W. Goucher, "Being a cybercrime victim", Computer Fraud and Security, Vol.2010, Issue10, pp.16-18, 2010.
DOI: https://doi.org/10.1016/S1361-3723(10)70134-2

[89] L. Allodi, M. Corradin, & F. Massacci, "Then and Now: On the Maturity of the Cybercrime Markets The Lesson That Black-Hat Marketeers Learned", IIEEE Transactions on Emerging Topics in Computing, Vol.4. No.1, pp.35-46, 2016.
DOI: https://doi.org/10.1109/TETC.2015.2397395

[90] A. Nagurney, "A Multiproduct Network Economic Model of Cybercrime in Financial Services", Service Science, Vol.7, No.1, pp.70-81, 2015.
DOI: https://doi.org/10.1287/serv.2015.0095

[91] A. Alazab, J. Abawajy, M. Hobbs, R. Layton, & A. Khraisat., "Crime toolkits: The productisation of cybercrime", 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, Melbourne, Australia, pp.1626-1632, 2013.
DOI: https://doi.org/10.1109/TrustCom.2013.273

[92] K. L. Modecki, B. L. Barber, & L. Vernon, "Mapping Developmental Precursors of Cyber-Aggression: Trajectories of Risk Predict Perpetration and Victimization", Journal of Youth and Adolescence, Vol.42, Issue5, pp.651-661, 2013.
DOI: http://dx.doi.org/10.1007/s10964-013-9938-0

[93] G. Settanni, F. Skopik, Y. Shovgenya, & R. Fiedler, "A Collaborative Analysis System for Cross-organization Cyber Incident Handling", Proceedings of the 2nd International Conference on Information Systems Security and Privacy, ICISSP, Rome, Italy, pp.105-116, 2016.
DOI: https://doi.org/10.5220/0005688301050116

[94] S. Romanosky, "Examining the costs and causes of cyber incidents", Journal of Cybersecurity, Vol.2, Issue2, pp. 121-135, 2016.
DOI: https://doi.org/10.1093/cybsec/tyw001

[95] J. Doyon-Martin, "Cybercrime in West Africa as a Result of Transboundary E-Waste", Journal of Applied Security Researchy, Vol.10, Issue2, pp.207-220, 2015.
DOI: https://doi.org/10.1080/19361610.2015.1004511

[96] A. Joode, "Effective corporate security and cybercrime", Network Security, Vol. 2011, Issue 9, pp.16-18, 2011.
DOI: https://doi.org/10.1016/S1353-4858(11)70097-6

[97] R. Joffee, "Cybercrime: the global epidemic at your network door", Network Security, Vol.2010, Issue7, pp.4-7, 2010.
DOI: https://doi.org/10.1016/S1353-4858(10)70091-X

[98] Y. Ben-Itzhak, “Organised cybercrime and payment cards”, Card Technology Today, Vol. 21, Issue2, pp.10-11, 2009.
DOI: https://doi.org/10.1016/S0965-2590(09)70057-X

박 지 용(Ji-Yong Park) [정회원]

- 2001년 5월 : Baylor University, Waco, TX, USA (B.B.A. with a concentration in Management Information Systems)
- 2002년 7월 ~ 2005년 2월 : 한국국제협력단(KOICA) 국제협력요원
- 2006년 2월 ~ 2007년 5월 : 한국국제협력단(KOICA)
- 2007년 5월 ~ 현재 : 한국인터넷진흥원(KISA) 책임연구원
- 2009년 9월 : 연세대학교 행정대학원 (국제관계학석사)
- 2011년 9월 ~ 현재 : 성균관대학교 기술경영학 (공학박사 과정 중)

〈관심분야〉
정보보호, 비즈니스모델, 사이버범죄, 사이버범죄경영

이 희 상(Heesang Lee) [정회원]

- 1983년 2월 : 서울대학교 산업공학과 (공학사)
- 1985년 2월 : 서울대학교 산업공학과 (공학석사)
- 1991년 3월 : Georgia Institute of Technology, Industrial & Systems Engineering, (Ph.D)
- 1991년 9월 ~ 1995년 2월 : KT 통신망연구소 선임연구원
- 1995년 3월 ~ 1995년 2월 : 한국외국어대학교 산업공학과 조교수/부교수
- 2003년 3월 ~ 현재 : 성균관대학교 시스템경영공학과/기술경영전문대학원 교수

〈관심분야〉
기술경영, 기술전략, 오픈 이노베이션, 경영과학