한국경호경비학회 – 제61호(2019): 59–85
https://doi.org/10.36623/KSSR.2019.61.3

투고일 2019. 11. 13 심사일 2019. 11. 26 게재확정일 2019. 12. 10

집단지성 네트워크형 사이버폴리스 자원봉사시스템 구축에 관한 연구

KSA

김 두 현 · 박 성 준 · 나 기 성

집단지성 네트워크형 사이버폴리스 자원봉사시스템 구축에 관한 연구

김 두 현* · 박 성 준** · 나 기 성***

〈요 약〉

4차 산업혁명으로 현실세계와 가상세계의 경계가 사라지는 현실에서 시공간을 초월하여 발생하는 사이버범죄에 대하여 실정법 체계 하에 구축된 정부조직의 경찰 공권력으로만 경찰의 임무를 다 하는데 분명한 한계를 갖고 있다.

본 논문은 문헌적 연구와 보안업무 경험을 토대로 사이버범죄에 대하여 실시간 대응할 수 있도록 각 사회분야의 집단지성이 자발적으로 참여할 수 있는 사회적 시스템을 구축하여 사이버공간에서의 범죄를 예방하고 사회적 공감대를 형성할 수 있는 대책방안을 제시하는 것을 목적으로 연구하였다.

집단지성 네트워크형 사이버폴리스 자원봉사시스템 구축을 위한 방안으로 우선, 집단지성 네트워크형 사이버폴리스 자원봉사시스템 구축이 필요하다. 이 구성은 제반 안전관리 전문가 등으로 구성한다.

그리고 경찰청의 경비업법상 민간조사업무 규정이 신설되어야 한다.

또한 집단지성 사이버폴리스 자원봉사시스템의 안전지킴이 봉사활동을 강화해야 하며, 선진국들의 사이버범죄에 대한 연구교훈 및 법적 대응방안이 도입되어야 한다.

끝으로 개인정보 보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 신용정보의 이용 및 보호에 관한 법률 등의 과도한 규제 규정을 개정하여야 하며, 경찰관은 사전예방 활동을 위한 사이버범죄 위해 인지능력을 배양해야 한다.

주제어 : 사이버범죄, 집단지성, 네트워크, 사이버폴리스, 자원봉사시스템, 지식나눔 봉사활동

* 한국체육대학교 안전관리학 교수, 안전관리연구소장 (주저자)

** 한국체육대학교 안전관리연구소 소방안전위원회 위원장 (교신저자)

*** 한국체육대학교 안전관리연구소 생활안전위원회 위원 (공동저자)

목 차

Ⅰ. 서론
Ⅱ. 이론적 고찰
Ⅲ. 사이버폴리스 자원봉사시스템의 실태 및 범죄 유형
Ⅳ. 집단지성 네트워크 사이버폴리스 자원봉사시스템 구축 방안
Ⅴ. 결론 및 제언

Ⅰ. 서 론

21세기 정보통신 기술의 발달과 화석연료의 급속한 수요증가로 인한 기상이변 등으로 인한 자연재해의 대규모화, 화재·붕괴사고 등의 인적재난 증가, 국민경제와 사회 안정에 큰 영향을 미치는 국가기반시설 등과 관련된 집단 이기주의적 갈등 및 물리적 사고의 빈발 등 다양한 형태의 재난이 끊임없이 발생하고 있다. 특히 에너지, 정보·통신, 교통수송, 금융, 보건의료, 원자력, 환경 등의 기능이 마비되면 막대한 인명과 재산피해 및 국민경제에 심각한 영향을 미칠 수 있다(김하연·이정일, 2017: 3).

그리고 인터넷과 스마트폰의 출현과 보급급증은 소셜네트워크(Social Network Service)같은 사이버공간을 탄생시켰으며 그 사이버공간에서 새로운 첨단기술을 활용한 사이버범죄가 난립하게 되었다. 해커들은 스마트폰을 해킹하여 사용자의 개인정보를 알아내어 범죄에 악용하고, 소셜네트워크에서는 새로운 유형의 피싱(Phishing)이나 사이버폭력(Bullying) 등이 새로운 범죄유형으로 진화하고 있다(이상현, 2010:3).

이와 같이 사이버범죄(cyber crime)는 컴퓨터 통신 등을 악용하여 사이버 공간에서 행하는 범죄, 인터넷과 같은 정보 통신망으로 연결된 컴퓨터 시스템이나 이들을 매

개로 한 사이버 공간을 이용하여 공공복리를 저해하고, 건전한 사이버 문화에 해를 끼치는 행위이다. 이것은 그 범행 목적에 따라 해킹, 컴퓨터 바이러스 등과 같은 사이버 테러형 범죄가 있고, 사이버 명예 훼손과 전자상거래 사기, 개인 정보 침해, 불법 사이트 개설, 디지털 저작권 침해 등과 같은 일반 사이버 범죄로 나뉜다.

사이버 테러형 범죄는 해킹, 컴퓨터 바이러스와 같은 유형의 범죄이고, 일반 사이버 범죄는 사이버 명예 훼손과 전자상거래 사기, 개인 정보 침해, 불법 사이트 개설, 디지털 저작권 침해 등을 말한다.

또한 미국 9·11테러에서는 급격히 발달한 과학기술을 바탕으로 개발된 대량살상무기를 이용하여 다중 시설물 파괴와 불특정다수의 인명살상을 자행하고 있다. 또한 이제는 테러가 단순한 총칼에 의한 것이 아니고 사이버·레이저·생물·전자무기 및 독소무기 등 다양한 테러공격무기가 동원되고 테크노테러의 양상을 보이면서 뉴테러 혹은 슈퍼테러로서의 성격을 띠고 있다(김두현·김정현, 2009: 3).

현대사회는 복잡계(Complexity System)와 4차 산업의 도래, 국경과 시공간을 넘어 온갖 유·무선으로 초 연결된 디지털 사이버 세계와 접속되어 살아갈 수밖에 없는 사회가 되었다. 사이버 가상 세계를 벗어나서 살 수 없는 현실에서 현대인은 가상세계에 접목되어 있지 않으면 생존경쟁에서 탈락하는 시대가 되었고 지금까지 학습한 상식이나 질서(관습·법률)로 판단을 가늠할 수 없는 디지털 진화(Digital Evolution)를 넘어 디지털 혁명(Digital Revolution)인 사이버 세계로 진입하고 있다. 이 새로운 유·무형의 서비스(공유경제, Mobility, 클라우드, 블록체인, MR, 5G, 드론, AI, 로봇, 컴퓨팅 파워 등)가 국경을 넘어 이미 우리의 삶과 뒤엉켜져 지금까지 합의된 시스템(법·제도)으로는 국민안전에 어떤 정신적·물질적 영향을 미칠지 예측할 수 할 수 없다. 우리 스스로가 일상에 쏟아지는 기가톤급 정보와 4차산업 부산물들이"과연 우리에게 정말 유익한 것인가?"라는 의문을 가질 수밖에 없는 상황에 이르게 되었다.

그리고 인간을 대신할 AI는 인간의 사고와 모방, 시행착오로 얻은 사용자경험(UI·UX)을 아무런 제약 없이 상품이나 서비스 개발, 로봇과 AI(머신러닝과 딥러닝) 기술 등에 사용되고 있고 이를 활용한 사이버범죄는 고도의 정보처리 기술을 범죄수단에 빠르게 이용되면서 진화하고 있다.

그럼에도 불구하고 경찰청은 사이버안전국 산하에 각 지방경찰청에 사이버수사대(서울, 경기남북부, 인천, 부산, 대구경찰청에는 사이버안전과 설치)를 두고 있으며, 총 인력은 1,800여명 정도 투입되어 있지만 사이버 범죄의 기술발달에 대처할 수

있는 한계에 도달 할 수밖에 없는 실정이다.

따라서 현실적으로 수사기관이 사이버 범죄의 사전인지와 피의자 발견이 불가능하고 국경을 초월하여 발생하고 있으나 수사기관의 공권력 범위와 한계를 벗어나 대다수의 사이버범죄는 방치되어 국가·사회적으로 심각한 피해를 초래하고 있다. 사이버범죄는 국가안보와 국민안전을 위협하는 치안위해요소로 진화 되었고, 국가간 사이버 전쟁수준으로 확대되었으며, 최근 소니픽처스와 한국수력원자원 해킹 사건은 사이버테러가 시스템 파괴·군사기밀 유출 등 군사기반시설을 대상으로 한 지능형범죄로 진화되기에 이르렀다.

이제는 국민참여형“집단지성(Collective Intelligence) 네트워크 사이버 폴리스 자원봉사 시스템”과 같은 가상세계에서의 국민참여활동을 국가 및 지방자치단체의 용도(계몽·행사 등)에 맞게 사용할 수 있도록 클라우드 서비스 방식에 대한 적용·개발이 필요하다.

선행연구로는 2016년 박정우 외 3명이 “사이버 범죄 해결사 디지털 포렌식”에 대한 번역서가 출판되었고 2010년에는 이상현 교수가 “미국 사이버범죄의 현실, 법, 실무(Cyber Crime in the U.S. : Realities, Law & Practices)”라는 보고서를 통해서 선진국들의 사이버범죄에 대한 연구가 있었지만 우리나라에서 운영될 수 있는 집단지성 네트워크 사이버폴리스 자원봉사시스템 연구에 대해서는 전무한 상태에서 본 연구의 필요성을 절감하게 되었다.

따라서 본 논문의 연구방법은 문헌적 연구와 보안업무 경험을 토대로 연구하였다. 이 논문의 연구목적은 법·제도화 이전 시공간을 초월하여 발생하고 있는 사이버범죄에 대하여 실시간 대응할 수 있도록 각 사회분야의 집단지성이 자발적으로 참여할 수 있는 사회적 시스템을 구축하여 사이버공간에서의 범죄유형을 실시간 정의하고 정의된 범죄에 대하여 국민 스스로가 예방하고 사회적 공감대를 형성할 수 있는 대책방안을 제시함으로써 전 국민들이 안전한 나라에서 행복한 생활을 영위 할 수 있을 것이다..

Ⅱ. 이론적 고찰

1. 경찰청의 범죄예방

경찰관직무집행법상 경찰관의 직무의 범위를 보면 국민의 생명·신체 및 재산의 보호, 범죄의 예방·진압 및 수사, 치안정보의 수집·작성 및 배포 등을 정하고 있어 국민의 생명·신체 및 재산의 보호를 위한 범죄의 예방이 무엇보다 중요함을 알 수가 있다(동법 제2조).

따라서 경찰의 행정경찰로서의 주요활동을 보면, 불심검문, 보호조치 등, 위험 발생의 방지 등, 범죄의 예방과 제지, 위험 방지를 위한 출입, 사실의 확인 등을 규정하고 있다(김두현. 2017: 78).

2. 소방청의 재난예방

소방청의 주요 봉사활동 분야는 소방도로 및 소방통로 위반행위(소방기본법), 소방 시설 및 방화시설 위반행위 및 소방안전관리 위반행위(소방시설법), 위험물시설 위반행위(위험물안전관리법), 재난시설 위반행위(재난안전법), 가스시설 위반행위(가스안전관리법), 전기시설 위반행위(전기사업법), 교통시설 위반행위(교통안전법) 등에 대한 시정계도 및 예방활동을 시행하고 있다.

3. 국가정보원의 테러예방

국민보호와 공공안전을 위한 테러방지법에 의하여 테러예방을 위한 안전관리대책으로 테러위험인물에 대한 정보 수집 등, 테러예방을 위한 안전관리대책의 수립, 테러취약요인의 사전제거, 테러선동·선전물 긴급 삭제 등 요청, 외국인테러전투원에 대한 규제를 하도록 규정하고 있다.

우선 국가정보원장은 테러위험인물에 대하여 출입국·금융거래 및 통신이용 등 관련 정보를 수집할 수 있다.

그리고 테러예방을 위한 안전관리대책의 수립의 일환으로 테러예방을 위한 안전관리 관계기관의 장은 국가중요시설과 많은 사람이 이용하는 시설 및 장비에 대한

테러예방대책과 테러의 수단으로 이용될 수 있는 폭발물·총기류·화생방물질, 국가중요행사에 대한 안전관리 대책을 수립하여야 한다.

또한 테러취약요인의 사전제거를 위하여 테러대상시설 및 테러이용수단의 소유자 또는 관리자는 관계기관의 장을 거쳐 대테러센터장에게 테러예방 및 안전관리에 관하여 적정성 평가, 현장지도 등 지원을 요청할 수 있다.

끝으로 테러선동·선전물 긴급 삭제 등의 요청으로 관계기관의 장은 테러를 선동·선전하는 글 또는 그림, 상징적 표현물, 테러에 이용될 수 있는 폭발물 등 위험물 제조법 등이 인터넷이나 방송·신문, 게시판 등을 통해 유포될 경우 해당기관의 장에게 긴급 삭제 또는 중단, 감독 등의 협조를 요청할 수 있다(김두현. 2017: 90-92).

4. 민간경비원의 범죄예방

경비업법에 의하여 경비업자, 경비지도사 및 경비원은 시설·건물 등의 시설경비, 현금·유가증권·귀금속 등 호송경비, 사람의 생명·신체에 대한 신변보호, 경비대상시설에 기기설치로 도난, 화재 등의 기계경비, 공항, 항만 등 국가중요시설에 대한 특수경비 등의 관리권행사의 범위 안에서 위험발생 방지권을 갖는다.

이 경비업의 역할과 관련하여 치안서비스 공동생산이론은 치안환경과 관련하여 치안서비스 생산과정에 있어서 경찰과 같은 공공부문의 역할 증대뿐만 아니라 민간부문의 참여를 활성화를 시키고 있다. 이는 공공경찰이 근본적으로 안고 있는 한계를 일부 극복하고 시민의 안전욕구를 충족시키기 위하여 민간부문의 능동적인 참여를 다각적으로 유도하고 있는 것이다.

민간부문은 서비스 수혜자인 시민과 영리목적의 민간경비 등을 들 수 있다. 과거에는 이들 민간부문을 치안활동의 보조적 차원과 별개의 차원에서 인식되어 왔으나, 이들을 능동적・주체적으로 인식하고 있는 것이다. 이는 경찰의 보조적 차원이 아닌 주체적 차원으로 인식함으로써 이들이 가지고 있는 인적・물적 안전 자원을 보다 효율적이고 체계적으로 활용할 수 있다.

치안활동에 있어서 민간부문의 참여는 경비업법 등을 통해 필연성으로 받아들여지고, 공공부문과 민간부문이 구별된 것이 아니라 다양한 네트워크(net-work)에 의해서 이루어지고 있다.

미국・영국 등 선진국에서는 치안활동에 대한 접근에 있어서 서비스주체의 다원

화에 초점을 두고 있다. 치안활동에 있어서 다원화는 경찰이 독자적으로 치안서비스를 수행하는 것이 아니라 민간부문이 하나의 독립된 주체로서 참여하게 된 것이다. 이러한 견해는 치안활동은 곧 공공경찰이라는 전통적 견해에서 보다 발전된 것이다.

이 과정 속에서 치안서비스의 공동생산론적 접근은 치안서비스의 생산성을 높이는 중요한 대안으로 등장하고, 이를 통해 공공부문과 민간부문의 상호 역할정립 및 상호관계를 이론적・실천적으로 체계화시켜 줄 수 있을 것이다(김두현. 2018: 338-339; 김두현·박형규. 2018: 25).

5. 자원봉사자의 범죄예방

자원봉사활동기본법에서는 "자원봉사활동"이라 함은 개인 또는 단체가 지역사회·국가 및 인류사회를 위하여 대가없이 자발적으로 시간과 노력을 제공하는 행위를 말하며, "자원봉사자"라 함은 자원봉사활동을 행하는 자를 말한다.

이 자원봉사활동은 무보수성·자발성·공익성·비영리성·비정파성·비종파성의 원칙 아래 수행될 수 있도록 하여야 하며, 이 진흥을 위한 정책은 민·관 협력의 기본정신을 바탕으로 하여 추진하여야 하는 등의 기본방향으로 하여야 한다.

자원봉사활동의 범위는 사회복지 및 보건 증진에 관한 활동, 지역사회개발·발전에 관한 활동, 인권옹호 및 평화구현에 관한 활동, 범죄예방 및 선도에 관한 활동, 재난관리 및 재해구호에 관한 활동, 국제협력 및 해외봉사활동, 공공행정분야 사무지원에 관한 활동 등을 규정하고 있어 범죄예방 활동도 그 범위를 정하고 있다(김두현. 2012: 14-15).

Ⅲ. 사이버폴리스 자원봉사시스템의 실태 및 범죄 유형

1. 현행 경찰청 사이버폴리스의 실태 및 제도

경찰청은 민간 IT 전문가의 경찰관·연구직 특채, 전문교육 프로그램개발 및 위탁교육, 사이버범죄 예방 앱(사이버캅) 등으로 사이버범죄 예방활동을 강화하고 있다.

우선 사이버 수사역량 제고에 가장 중요한 것은 전문인력의 확충으로 경찰청은

‘경찰관·연구직공무원 특별채용제도’를 운영하고 있다. 경찰관·연구직 특별채용은 해킹, 악성코드, 암호 등 첨단기술분야에 대한 석·박사급의 고급인력을 충원하고 디지털 증거분석 역량을 제고하기 위한 제도이다. 이 제도를 통해 채용된 인력들은 IT기술과 법률지식을 겸비한 정예 사이버 수사 핵심인력으로 역할을 수행하고 있다. 사이버 경력채용은 2000년 76명을 채용한 것을 시작으로 매년 채용하여 2017년 현재 500여명이 사이버수사분야에서 근무를 하고 있다. 특히 연구직 특별채용은 2007년 5명을 채용한 것을 시작으로‘모바일포렌식분야’등 전문분야에 인력을 매년 증원하여 현재 정찰청 사이버 안전국 디지털포렌식 센터에서 13명이 근무하고 있다.

그리고 그동안 정찰의 사이버수사 노하우를 집대성하여 경찰수사연수원에 사이버 범죄수사과정, 디지털포렌식 과정, 해킹범죄수사 과정 등 전문교육 프로그램을 개설하여 연간 300명을 교육하고 있으며, 이 분야의 전문성에 대한 공인의 중요성을 인식하게 되어 2010년부터 매년 국제 공인 디지털포렌식 자격증(EnCE) 취득을 지원하는 한편 2012년에는 맞춤형 석사과정을 고려대학교 정보보호대학원과 연세대학교 정보대학원에 디지털포렌식학과를 각각 신설하여 사이버수사요원의 학위취득을 적극 지원하여 현재까지 약 120명의 위탁교육생을 선발하여 교육을 진행해 왔다.

또한 민간참여와 법집행기관 및 해외기업 등과의 사이버 범죄예방 활동을 하고 있다.

우선 사이버 치안수요의 증가로 전술한바와 같이 불법·유해정보를 근절하는데 경찰의 노력만으로는 한계가 있어, 민간참여를 통한 사이버범죄 예방활동을 위해 전국 지방경찰청 사이버 명예경찰‘누리캅스’를 운영하여 2007년부터 인터넷에 능숙하고 신고정신이 투철한 네티즌 중 소정의 절차를 거쳐 선발한 회원을 사이버 명예경찰 ‘누리캅스’로 위촉하여 사이버공간에서의 민·경 협력 체제를 구축하고 있다. 2017년에는 807명의 회원을 위촉하여 유해정보 신고활동을 실시하고 있다.

그리고 해외법집행기관, 글로벌 SNS기업 등과의 협력을 확대하고 있다. 사이버범죄는 대표적인‘국경 없는 범죄’로 인터폴(Interpol), 유로폴(Europo1) 및 외국 수사기관과의 국제공조가 필수적이므로 사이버안전국은 미국, 영국, 프랑스, 독일, 네덜란드, 오만 등 외국수사기관과 협력약정을 체결하여 원활한 국제공조를 위한 근거를 마련하였다. 사이버안전국은 해외법집행기관 뿐만 아니라 구글, 페이스북, 트위터 등 공조수요가 높은 글로벌 IT 기업 및 카스퍼스키, 시만택, 파이어아이 등 사이버 보안업체와도 교류를 확대해 오고 있다.

특히 국가 사이버테러 대응활동으로'아동음란물 프로파일링시스템'을 구축하는 등 사이버범죄 수사 기법의 개발 및 발굴, 사이버 범죄 신고대응반의 운영, 한국인터넷진흥원 내 사이버원스톱센터 운영에 노력하고 있다. 경찰청 사이버안전국은 사이버안전국 홈페이지(cyberbureau.police.go.kr) 및 사이버캅 앱을 통해 접수되는 사이버범죄신고·상담민원을 처리하고 있으며, 2017년에는 신고민원 건수가 2016년에 비해 24.87% 감소하였으나 상담건수는 168.7% 증가하였으며, 상반기 랜섬웨어 감염신고가 10.7%나 증가하였고 관련 상담건수는 275%로 증가하였다. 디지털 증거분석 인적 인프라 구축을 위해 2017년 현재 디지털포렌식 전담인력이 전국적으로 74명이 활동하고 있고, 투명하고 공정한 디지털 포렌식 구축을 위해 2015년에'디지털 증거 수집 및 처리 등에 관한 규칙'을 제정한 이후 판례 및 법원의 영장실무변화 등을 반영하여 규칙을 개정하여 왔다.

아울러 최근 스마트카, 드론, 사물인터넷(IoT), VR(가상현실) 등 4차산업혁명 대비 및 진화한 ICT 기술에 선제적 대응을 위해 드론포렌식기술연구, 네트워크 추적기술연구, 최신 ICT 분석기술 연구, 안티포렌식 기술연구 등이 한창이며, 과학기술정보통신부와 최신 기술융합기기 디지털포렌식 연구개발 (R&D)을 진행중이긴 하지만 아직 구체적인 결과물은 없어서 본 논문과 같은 내용의 필요성이 강조될 수밖에 없다 (경찰청. 2019: 223-233).

2. 경찰의 주요 사이버범죄 유형별 분석

사이버범죄는 올해 3분기까지 총 108,825건이 발생하여 하루에 약 399건으로 약 3분 40초마다 1건이 발생하고 있는 셈이다. 한 예로 최근 연예인 설리가 죽음을 선택한 이유는 아마 연예인으로서 겪는 고통 중 많은 부분은 유튜브(YouTube) 등의 악플이 작용했을 것으로 경찰은 추정하고 있다.

경찰청의 2017년 주요 사이버범죄 유형별로 보면, 해킹·DDoS 등정보통신망 침해행위, 인터넷사기, 사이버 금융사기, 도박사이트, 인터넷 음란물, 개인정보 침해 등이 있다. 해킹·디도스·악성코드 범죄 특별단속을 실시한 결과 정보통신망 침해범죄 검거 율을 2016년 대비 11.1% 제고하는 한편, 국내 ATM기를 해킹하여 23만 건 금융거래정보를 탈취·유통한 피의자를 검거하는 등 의미 있는 성과를 거두었다.

그리고 인터넷사기 2017년 인터넷사기는 92,636건이 발생하여 807,40건을 검거하

여, 전체 발생 사이버범죄(131,734건) 중 70.3%를 차지하고 있으며, 2016년에 비해 발생건수가 소는 지속적인 특별단속 및 홍보·예방활동, 탐지기술의 발달 악성코드유포 시 신속한 백신 반영 폭이 감소하긴 하였으나 최근 4년간 지속적으로 증가추세에 있다.

또한 사이버금융사기는 파밍, 스미싱, 메모리해킹 등 사이버금융사기 등으로 2014년 이래 지속적으로 감소하는 추세이다. 특히, 스미싱은 2013년 29,761건에서 2017년 83건으로, 메모리해킹은 2013년 463건에서 2017년 6건으로 최근 4년간 각각 98%가량 대폭 감소하였는데, 이는 웹발신 문자표시, 휴대폰 발송 변호변경 문자차단, 금융권 키보드 보안프로그램 강화 등 범정부적 예방대책의 효과라고 생각되지만, 신종 유형인 몸캠피싱은 2015년 102건에서 2017년 1,234건으로 10배 이상 증가추세를 보이고 있다.

그리고 불법인터넷도박은 인터넷 및 모바일기기의 발달로 인한 접근이 용이하며, 시·공간의 제약이 없는 특성으로 인해 각 연령층에서 성행하고 있으며, 도박자금 마련을 위한 사기·절도 등 2차 범죄까지 양산하는 등 사회적 폐해를 발생시키고 있다. 불법 인터넷 도박사이트 운영은 서버 및 사무실의 해외 이전, 운영자들의 대포통장 이용, 불법수익금 세탁 및 현금화 등으로 수사기관의 단속을 회피하기 위한 수법이 날로 지능화되고 있다는 점에서 본 논문의 필요성이 절실하다고 본다.

경찰은 2017년 한 해 동안 불법인터넷도박으로 5130건, 5,080명을 검거하였으나 매우 저조한 실적이다.

또한 인터넷과 스마트폰의 보급률이 지속적·과학적으로 증가하면서 온라인상

음란물의 국경과 사법권의 경계가 없어 음란물근절을 위한 다각도의 노력에도 불구하고 유통경로가 다변화되고 있다. 사이버 명예경찰'누리캅스'와 협력하여 '인터넷 음란물집중모니터링활동'을 전개하고 있지만 최근에는 P2P 토렌트(Torrent) 등 SNS (랜덤채팅, 폐쇄형그룹방 등)을 통해 음란물이 유통되는 것으로 추정되어 이것에 대한 예방활동이 쉽지가 않다.

끝으로 개인정보 침해를 보면 2012년 발생건수 2,561건 중 검거건수 1,840건으로 71.8%이었으나 2017년에는 발생건수 413건 중 검거건수 298건으로 72.2%이었으나 개인정보보호법이 2011년 제정된 후 국민인식 향상과 경찰의 지속적인 단속으로 2015년까지 계속해서 발생건수가 감소하였다. 그러나 2016년부터 개인정보 탈취수법이 고도화·지능화됨에 따라 불법으로 개인정보를 수집·매매하고 이를 이용한 2차 범죄를 적극적으로 단속하여 높은 검거율을 기록하게 되었다. 또한 스마트기기 사용

의 활성화로 보안이 취약한 어플리케이션의 개인정보 유출사건이 계속 발생하여 국민 불신은 여전한 상태이다(경찰청. 2019: 234-239).

그러나 IP 경유 프로그램을 이용한 범행IP 세탁 등 추적 회피기술의 발달로 정보통신망 침해행위에 대한 추적수사는 나날이 어려워지고 있어서 본 논문의 필요성이 또한 절실하다고 본다.

지난 2001년 9월 11일 발생된 미국의 동시다발 테러사건을 지켜보면서 테러사건이거나 일반범죄이건 간에 사후조치 보다는 사전예방에 최우선을 두어야 한다는 사실을 다시한번 되새겨 보는 계기였음이 틀림없다.

아울러 한국의 일반 범죄율은 지난 30여 년간 2배 이상 증가하였다. 1981년 인구 10만 명당 935건에서 1991년 558건까지 감소했다가 그 이후로는 지속적으로 증가해 왔다. 1997년 경제위기의 영향으로 1998년에 범죄율 증가폭이 커졌고, 2002년과 2003년에 가장 급격하게 증가하는 추세를 보이고 있어 범죄발생의 심각성은 최근 들어 더욱 악화되고 있을 뿐만 아니라 아직도 그 검거 율은 2010년 84%, 2011년 78.3%, 2012년 76%, 2014년 78%로 경찰의 범죄 검거 율은 갈수록 하락하고 있는 실정이다.

그런데 제한된 검찰과 경찰인력 및 장비의 한정으로 인해 모든 국민들이 안전하게 생활을 영위 할 수 있는 서비스가 충족되지 못하고 있으며, 경비회사 등 민간차원의 역할이 더욱 중요한 실정이다.

이와 같은 역할을 수행하는 민간조사원(private investigator)은 탐정, 민간조사자, 조사자 등으로 사용되고 있다.

그럼에도 불구하고 민간조사업과 같은 사업을 서방국가들에서는 일반인들이 생각하는 우리의 탐정이나 흥신소 등과는 많이 다른 모습으로 발전되어 왔으나 아직도 한국 및 일부 아시아 국가에서는 일반인들의 부정적인 시각들 속에 비쳐지고 있고, 아울러 경찰과의 업무상 마찰우려, 법무부와 경찰청 간의 소관 다툼, 신용정보사업 관련 법규상 탐정 용어의 사용금지, 그리고 민간조사 업무 부분의 한계성 주장 등 오히려 민간조사업 제도 도입에 대한 제한적 요소로 작용하고 있다(김두현·박형규. 2018: 388-389).

한국의 심부름센터는 아무런 법적 근거도 없이 운영되어 온 것으로, 서울에 약 1천개를 포함하여 전국에 약 3천여 개가 있다. 다만, 신용정보의 이용 및 보호에 관한 법률이 금융감독위원회 소관법으로 1995년에 제정되어 신용정보업이 합법적으로 운영되어 오고 있다.

그리고 국내에서의 민간조사원을 양성하기 위하여 설립된 사설교육기관인 한국민간조사교육원(Korea Private Investigator Education), 대한민간조사협회(한국특수직능교육재단) 등이 운영되고 있으며, 연구기관으로서는 한국경호경비학회, 대한민조사학회 등이 있다.

이 교육원 등은'PI 민간조사원과정'에서 민간조사학개론, 범죄학 및 범죄심리학, 법학개론, 민간조사 관계법, 민간조사실무 등을 개설하여 기업 간 정보수집 등의 상업조사, 생명보험·손해보험 등 보험관련 부분에 대해 보험회사의 위임사항 및 보험관련 업체 취업을 통한 보험범죄 조사, 사이버 범죄의 예방과 적발을 전문적으로 하는 사이버 PI, 자원봉사단체와 함께 시민을 위한 각종 조사를 수행하는 자원봉사 PI, 의료분쟁의 원인분석을 통해 분쟁해결에 도움을 주는 의료 PI 등 국민의 권리신장과 함께 사회 각 분야에 필요한 민간조사 전문가를 양성하고 있다.

한편 국세청에서 영업에 대한 과세를 위한 소득표준을 분류코드에 따라 민간조사업(탐정업)을 신고하며 사업자등록증을 발급해 주고 영업을 가능하게 하고 있는 실정이다.

현재 국내법상 합법적으로 업무가 가능한 신용정보업법의 내용을 보면 다음과 같다.

신용정보업자는 신용정보업을 영위하고자 하는 사람이 신용보증기금법에 의한 기술신용보증기금, 일반신용보증, 지역신용보증재단법에 의하여 설립된 신용보증재단, 대통령령이 정하는 금융기관이 50% 이상 출자한 시설 및 설비를 갖춘 법인으로서, 신용정보업을 행하기 위해서 신용조사 업무, 신용조회 업무, 채권추심 업무 및 신용평가 업무 등 4종류의 업종별로 금융감독위원회 허가를 받아야 한다.

따라서 신용정보업자는 ① 타인의 의뢰를 받아서 신용정보를 조사하고 이를 그 의뢰인에게 제공하는 업무, ② 신용정보를 수집·정리 또는 처리하고 의뢰인의 조회에 따라 신용정보를 제공하는 업무, ③ 채권추심업무, 즉 신용정보제공·이용자인 채권자의 위임을 받아서 신용불량자에 대한 재산조사, 변제의 촉구 또는 채무자로부터의 변제금 수령을 통하여 채권자를 대신하여 채권을 행사하는 행위 등을 행할 수 있다.

아무튼 외국인 민간조사업체 30여개가 우리 국내에서 활동하고 있는 실정을 고려해 볼 때 민간조사업 제도의 입법화가 이루어져야 할 것이다(김두현. 2001: 144).

민간차원의 사이버범죄 예방과 방지를 위한 봉사활동은 미흡하며 정부의 자원봉

사시스템은 육체적 기준의 자원봉사만을 인정하고 인센티브제도로서 봉사마일리지 제도를 운영하고 있는 실정이다. 국내적으로는 행정안전부 1365에서 2018년 자원봉사 활동자는 4,290,985명이고, 보건복지부 VMS 에서는 2018년 자원봉사 활동자는 1,133,185명에 이르고 있다.

국제적으로도 “집단지성(Collective Intelligence) 네트워크 사이버폴리스 자원봉사시스템”은 전 세계적으로 없는 실정이다.

아무튼 외국인 민간조사업체 30여개가 우리 국내에서 활동하고 있는 실정을 고려해 볼 때 민간조사업 제도의 입법화가 이루어져야 할 것이다(김두현. 2001: 144).

민간차원의 사이버범죄 예방과 방지를 위한 봉사활동은 미흡하며 정부의 자원봉사시스템은 육체적 기준의 자원봉사만을 인정하고 인센티브제도로서 봉사마일리지 제도를 운영하고 있는 실정이다. 국내적으로는 행정안전부 1365에서 2018년 자원봉사 활동자는 4,290,985명이고, 보건복지부 VMS 에서는 2018년 자원봉사 활동자는 1,133,185명에 이르고 있으나 시간기준의 봉사활동에 대한 대가로 봉사마일리지를 제공하고 있고 재난신고에 대한 보상대가는 제보유형의 경중에 상관없이 일률적으로 동일 봉사대가 기준을 정해주고 있으나 사이버상에 일어나는 범죄유형 예방과 신고기준 등 사회적 의견을 수렴한 적이 없는 것이 작금의 현실이다.

더욱이 인터넷 특성상 우리나라의 법적 적용이 불가능해 인터넷업체와의 ‘해외직구’와 블록체인 거래 등에 사이버범죄 등이 수시로 발생하고 있으나 정부의 법적 제도가 맞추어 따라갈 수 없어 민간이 주도하고 예방할 수 있는 “집단지성(Collective Intelligence) 네트워크 사이버폴리스 자원봉사시스템”이 필요하다.

Ⅳ. 집단지성 네트워크 사이버폴리스 자원봉사시스템 구축방안

1. 집단지성 사이버폴리스 자원봉사시스템 구축

우선 집단지성 사이버폴리스 자원봉사자 그룹 구성은 전문성과 경험을 중심으로 ① 컴퓨터 관련 전문가 그룹(전국 대학의 컴퓨터공학과, 디지털포렌식학과, 정보보호학과 등), ② 안전 및 안보 전문가 그룹(안전관리학과, 경호학과, 경찰행정학과, 경찰경호학과, 보안관리학과, 항공보안학과, 경호비서학과, 소방행정학과, 소방공학과

등 경호보안관련학과 교수와 석·박사학위소지자, ③ 대통령경호처, 국가정보원, 경찰청, 소방청 등의 퇴직공무원, ④ 현재 활동준인 전문가 그룹(경비·보안기업 및 단체, 민간조사원, 컨설턴트, 산업안전요원, 컴퓨터 안전요원, 은행안전요원(청원경찰), 학교안전요원(보안원), 호텔안전요원, 항공안전요원, 병원안전요원, 경호·경비·소방·경찰·교통 ·정보·보안·국방 및 국민안전연구소 등 제반 안전관리연구소 연구원) 등으로 분류 한다(김두현·최선태. 2002: 60-71).

그리고 4차 산업기술의 발달과 AI 디바이스와 IoT 접속영역 확산에 따라 집단지성 사이버폴리스 봉사활동의 대상으로는 ① 사이버 범죄(사이버 금융사기, 허위사실유포 및 명예훼손, 사이버스토킹, 콘텐츠 불법유통·배포, 사이버테러<해킹·도청·DDos 등>, 스마트오피스 보안위협, 파밍, 랜썸웨어, 음란물, 도박, 불법복제, 성추행·성폭력, 권한탈취, 협박·공갈 등), ② 가상통화 채굴 악성코드 유포사건(Crytojacking), IP 카메라 해킹 사건, 몸캠피싱(스마트폰 채팅앱을 통해 피해자에게 접근해 음란채팅을 하자고 권유하면서 스마트폰에 악성코드를 설치하게 하고, 이를 통해 녹화된 동영상을 유포하겠다고 피해자를 협박하여 금원을 갈취하는 범죄), 사이버도박, 다크넷(Dark Net)상의 신종 사이버 범죄(시민이 자율적으로 참여하여 효과를 극대화할 수 있는 사회적 집단지성 블록체인 공동감시망 구축·정보통신망 침해형 범죄유형) 등과 같은 유형으로 분류할 수 있다.

따라서 사이버범죄에 대한 국민의 협조를 얻는 개선방안으로는 평소의 방범진단과 피해시 급보방법 등 구체적인 협조방법의 계도 및 수사에 대한 협조의식 제고, 정보 및 수배망 등 주민협력체제의 구축, 협력자에 대한 보상제도의 확정 및 유대강화, 효과적인 홍보활동 강화, 경비원과 경비지도사 및 청원경찰 등 교양철저, 공개수사제도의 효율적 운용, 반상회 등 주민들의 협조 분위기 조성 등 강화(이만종, 2007: 66).

그리고 “집단지성 네트워크 사이버폴리스 자원봉사활동”을 통하여 현존하는 범죄율 하락에 기여함은 물론 수사기관의 공권력이 미치지 못하는 사이버영역에 대하여 예방 가이드라인을 제시하여 사이버 범죄예방을 위한 민간참여 공간과 정신적 봉사활동에 대한 인센티브 적용이 불가함으로 사이버 범죄예방을 위한 CPS(Cyber Physical System) 구축이 필요하다.

참여자 및 집단지성 인센티브 모델은 미국 스타트업 ‘스팀잇’ 비즈니스 모델을 참고로 하여 참여활동에 대한 인센티브 모델을 적용할 수 있다. 스팀잇은 암호화폐 보상을 통해 커뮤니티 발전과 사회적 상호 작용을 창출하기 위해서 만들어진 블록체

인 데이터베이스이며, 스팀의 소셜 미디어 플랫폼으로 이용자가 해당 플랫폼에 컨텐츠를 포스팅하면 그 기여도에 대한 일종의 보상으로 스팀달러(SBD)와 스팀잇 내의 의결권인 스팀 파워(SP)를 50대 50의 비율로 제공한다. 스팀파워(SP)를 많이 보유할수록 큐레이션에 참여할 때 더 많은 스팀 토큰을 보상으로 받게 되며, 해당 스팀파워 보유자가 업보트(Up Vote)한 콘텐츠의 제작자에게도 더 많은 스팀 토큰이 보상으로 주어진다. 이 인센티브 모델을 적용하면 지역상권 활성화를 위하여 "집단지성 사이버 폴리스 자원봉사시스템" 활동으로 보상받은 인센티브를 지역화폐(온누리 상품권)와 교환할 수 있도록 개발하고, 인센티브 재원은 공공기관의 CSR(Corporative Social Responsibility) 기금참여를 유도할 수 있는 방안을 모색할 수 있다.

따라서 집단지성 참여 구성시스템은 다음 <그림 1>과 같이 국민들이 명예와 결정을 믿고 따를 수 있는 대학교(교수)·연구소(전문인)·단체(민간·법률)·기관 등으로 집단지성 네트워크를 구성한다.[1)]

아래의 그림을 구체적으로 설명하자면, ① 사이버범죄 신고(게재, 투고, 자문·요청 등) → ② 집단지성 대응(자문·상담·가이드라인·신고 등) → ③ 신고중요도에 따라 인센티브지급(51%의 참여자와 인센티브 재원 제공자 의견 반영) → ④ 집단지성인

〈그림 1〉 집단지성 사이버폴리스 자원봉사 시스템

1) 이상현 연구에서는 집단지성 구성자로 우선 대응자(First Responders), 수사관, 포렌식 분석가, 사설경찰, 해당분야 전문가(subject matter experts) 등으로 제시하고 있다.

센티브의 지급은 ①-1/n로 한다.

2. 경비업법상 민간조사업규정 신설

민간조사업은 국가의 공권력을 행사하는 법집행기관에 의해서 발생된 사건의 해결이 미흡하거나 사건이 미제사건으로서 장기간 방치될 수 있는 경우, 의뢰인의 요구로 각종 조사 등을 실시하여 조사한 내용을 의뢰인에게 제공함으로써 국민의 법률생활의 편안을 도모하고, 국민의 권리를 보호하는데 이바지하기 위한 목적으로 설립되어야 할 제도라고 할 것이다.

공인탐정제도 법안은 국회에서 꾸준히 발의했지만 매번 무산되어 왔다. 현재 2017년 발의한 '공인 탐정 및 공인탐정업에 관한 법률안'등 2건이 국회에 계류 중이다. 바람직한 입법화 방안으로는 현재 운영되고 있는 경비업법을 개정하여 경비업의 종류로 민간조사업무를 추가하는 것이다.

경비업법 제2조 제1호에 의하면, 경비업이라 함은 시설경비업무, 호송경비업무, 신변보호업무, 기계경비업무, 특수경비업무의 전부 또는 일부를 도급받아 행하는 영업으로 규정하고 있는바, 여기에 민간조사업무를 추가하기 위한 개정방안을 생각해 볼 수 있을 것이다. 민간조사업무가 경비업의 업무와 유사한 것일 뿐만 아니라 민간조사업의 선진국이라고 할 수 있는 미국의 민간조사요원들의 75% 이상이 경찰・군・경비회사 출신 등이며, 총 민간조사요원 중 약 25%가 보디가드 경력을 보유하고 있는 실정임을 고려하고 개정입법의 용이성 측면을 보았을 때 고려해 볼만한 것이다. 또한 경비원교육과 경비지도사의 자격시험 및 기본교육이 민간조사원교육과 대동소이하므로 교육의 중복을 피할 수 있을 것이다(김두현・박형규. 2018b: 393-394)[2)]

3. 국민생활의 안정을 위한 집단지성 사이버폴리스 자원봉사시스템의 안전지킴이 봉사활동 강화

"집단지성 사이버폴리스 자원봉사시스템"은 우리경제 규모, k-POP, K-Culture 등

2) 반면에 손동운 외 2명이 연구한 "민간경비업과 민간조사업의 차이점 연구"에서 민간경비업의 업무성격, 비용, 공권력영역, 법제유무, 위협대상, 조직규모의 차이를 확인 할 수 있었음으로 경비업법을 개정하여 민간조사업을 추가시키는 것은 신중을 기해야 한다고 주장하고 있다(손동운 외 2, 민간경비업과 민간조사업의 차이점 연구, 한국경호경비학회지 제39호, 2014, 312면)

글로벌화와 국경을 초월한 글로벌 Commerce에 대응하기 위하여 세계 곳곳에서의 사이버범죄에 대한 자문과 상담, 가이드라인 등과 국내의 대형 재난사고(대구 지하철사고, 장성 요양병원 화재, 고양 종합터미널 화재, 세월호 사고, 수원메타폴리스 화재, 시장화재(대구 서문시장, 여수수산시장, 소래포구시장 등), 제천 스포츠센터 화재사고, 밀양세종병원 화재참사)가 발생할 수 있는 글로벌 안전사고 예방을 위하여 안전분야 전문가(퇴직소방공무원을 비롯한 의용소방대원, 재난관리사 등 소방・안전전문 인력)의 전문성과 경험을 활용한 공익신고 및 안전관리 Consulting을 "집단지성 사이버 폴리스 시스템 구축"을 통하여 시민들의 안전의식 고취와 일상생활에서 발생할 우려가 있는 각종사고 등 재난안전 위해요인을 발굴하고 시정함으로서 각종 재난으로부터 안전한 국민의 안전을 책임지는 범시민 안전지킴이 지식 나눔 봉사활동을 전개한다.

이 봉사활동의 구체적 범위는 국민생활(건강, 안전, 환경, 소비자의 이익, 공정한 경쟁)의 안정을 위한 공익침해 행위신고와 대상법령(공익신고자 보호법 제2조 제1호)에 따라 건축법, 소방시설법, 액화석유가스의 안전관리 및 사업법 등 안전과 관련된 284개 법령을 대상으로 봉사활동을 실시하며 ① 각종사고 등 재난안전(생활안전, 소방안전, 재난안전, 전기・가스・교통안전, 위험물 및 환경폐기물 안전 등) 위해요인 제거, ② 생활주변 화재 등 재난취약지역 예방순찰 및 위험요소 발굴・제보, 개선방안 제시, ③ 각종사고 등 재난안전 위해요인 시정방안 상담 및 봉사활동 전개, ④ 재난안전 관련 지역불안사항 여론수렴 및 아이디어 발굴・제안 등을 실시한다(박성준. 2019, : 1-7).

4. 선진국의 사이버범죄에 대한 연구 교훈 및 법적 대응방안 도입

사이버 범죄는 국내 국외에 동시에 발생할 수 있다는 특성을 갖고 있으므로 이에 대처하기 위해 국가 간의 법 제도의 상이성을 초월한 국제적인 형사 사법의 규칙이 필요하다.

우선 미국 등 선진국들의 사이버범죄에 대한 연구로부터의 교훈을 얻어야 한다. 인터넷 이용을 통한 세계화는 지역적 경계를 넘어 세계에 흩어져 있는 컴퓨터 네트워크를 통합하고 있다. 컴퓨터의 광범한 사용과 세계화 경향 하에, 대부분의 국가들이 사이버범죄와 이를 차단하는 보안상의 문제에 직면해왔고 이 문제는 그 극복을

위해 그들의 노력을 투입해야 하는 공통된 도전이 되었다. 미국 등 선진 국가들이 사이버범죄, 입법 및 그 사이버범죄를 규제하는 실무의 검토는 사이버범죄를 통제하는 법제화 또는 입법 시행절차를 시작하기 전에 주목할 중요한 자료일 것이다.

특히 1970년대 이래, 미국은 사이버범죄의 진화를 경험해 왔고 그 범죄를 새로운 법의 법제화 및 실행을 해 왔으며, 이 범죄를 다루는 실무적 지혜는 서적, 리포트 및 학술논문을 통해 축적되어 왔다.

이 발전된 입법은 법적 문제를 극복하고 사이버범죄자를 처벌하기 위한 효과적인 근간으로서 작용한다. 법집행기관의 사적 영역과의 협력은 포렌식 과학의 발전을 뒷받침하고 공적 영역에서 컴퓨터 네트워크의 섬세한 구조에 대한 지식을 쌓고 불충분한 기술적 실력을 극복하는데 기여한다. 법의 전반적 발전, 제도적 반응, 각 관할에서의 업무 배분, 공적 영역과 사적 영역의 협력이 다른 국가에 의해 고려되고 채택될 만한 가치가 있는 중요한 부분들이다.

그리고 사이버범죄에 대한 법적 대응방안을 강구해야 한다. 법제화에 시간이 소요되는 법체제가 장래 고도의 기술적 범죄를 잘 통제할 수 있을지에 관한 어려움이 있다. 기술은 입법보다 더 빨리 바뀌고 있어서 코드에 기초한 규제는 범죄를 통제하는 대체수단 일수가 없다. 이 코드에 기초한 규제는 기술의 최신 발전과 관련 있는 사이버범죄의 남용을 막는 코드의 사용을 통해 효과적으로 통제될 수 있을 것이다. 그러나 범죄를 행하는 것을 방조하기 위해 제작된 소프트웨어는 사이버범죄를 활성화 해왔다는 점(바이러스 프로그램, 악성코드 등)이 주목되어야 한다. 그러므로 코드에 기초한 규제는 형법의 허점 들을 보충하는 역할을 할 것으로 기대되므로 법적 관점에서, 형법은 사이버 공격의 불법행위를 처벌하기 위해 법제화되어야 한다.

반 사이버범죄 법규의 기초위에, 사이버공간에서 새로운 범죄현상으로 부터 적절한 사법적 논증 제시가 파생될 수 있다.

그리고, 법집행기관들은 전문직업적 방법으로 사이버범죄를 다루기 위해 훈련되고 운영되어야 한다. 사이버범죄를 막는데 공적자금의 사용을 통해 훈련된 경찰이 사적 영역으로 이동하는 것이 정책 결정권자의 용기를 잃게 할지라도, 컴퓨터 포렌식 분야에서 개인을 교육하고 훈련하기 위해 자금을 투자 하는 것은 법집행기관의 능력을 향상시키기 위해 필요하다.

코드에 기초한 규제, 법적 대응과 법집행기관의 훈련은, 만약 인터넷을 사용하는 공중이 사이버범죄 및 그 양태를 알지 못한다면, 불충분한 방법으로 작용할 것이므

로 인터넷 사용자가 잠재적 피해자로 전락하는 것을 막기 위해서는 대상물 강화의 절차가 필요하다. 이 절차는 사이버범죄의 알려지지 않은 유형과 그들의 피해에 대한 설명과 사이버범죄로부터 그들을 보호하는 간편한 방법으로 인터넷 사용자를 계몽하는 것을 포함한다.

또한 사이버범죄에 대한 예방조치 방안으로 사이버범죄를 통제하는 입법의 발전, 보안조치의 장려, 교육과 혜택을 통한 전문직 양성 등이 필요하다.

우선 사이버범죄를 통제하는 입법의 발전측면에서 사이버범죄 발생의 속도를 따라잡기 어려운 점을 고려하여, 컴퓨터범죄의 법률은 기술 중립적이어야 하며 네트워크, 특히 인터넷을 사용하는 점에 대한 사용자의 책임을 정립해야 한다. 그리고 정보기술의 신속한 진보의 과정에서도 그 유효성을 유지해야 한다. 입법 상 사이버범죄의 구성요건 요소 상 쟁점들(고의 또는 네트워크 침입 등)이 기술의 급격한 발전 아래 여러 가지 수단에 대한 광범위한 처벌 기반을 제공해야 한다는 점에서 수용될 여지가 있으나 새로운 유형의 기술 기기와 파생적 형사 범죄행위는 때때로 구법(舊法)과 조항들로는 포섭하기가 매우 어렵기 때문에, 사이버범죄의 다양한 도전에 효과적으로 대처하기 위해 새로운 법과 조항들이 법제화될 필요가 있다.

그리고 보안조치의 장려측면에서는 사이버범죄를 효과적으로 다루고 처벌하기 위한 법적 그리고 정치적 조치들 외에도, 사전에 이 범죄들을 막기 위한 보안조치들이 같은 정도의 중요성으로 강조되어야 한다. 국가는 산업부분과의 협력 하에서 정보보안의 필요성에 대한 공공의 인식을 증진하는데 중요한 역할을 해 왔으나 장래정책의 초점은 정보기술의 발전만큼 정보보안의 발전에도 맞추어져야만 한다.

또한 교육과 혜택을 통한 전문직 양성측면에서 장학금, 협력과 지원금으로 정보보안과 사이버범죄 예방에 대한 전문 직업교육을 활성화 시켜야 한다. 그동안 국가정보원과 경찰은 정보보안 전문가를 양성하기 위한 범국가적 전문 직업교육을 후원해 왔고 정보보안을 연구하는 학회에 후원하기 위한 지원금을 제공해 왔으나 보다 적극적인 예산지원과 전문 직업 인증 훈련 프로그램운영이 필요하다. 미국 등 다른 국가의 정부들도 교육 및 전문 직업시스템을 고려하여 자신의 독자적 시스템을 설립하고 있는데, 이는 이 분야의 공식적 교육시스템과 전문가 그룹이 사이버상의 보안을 발전시킬 수 있는 잠재적 자원 및 그 생산기반으로서 작용하고 있다(이상현, 2010:123-127).

따라서 개인정보 보호법·정보통신망법(정보통신망 이용촉 진 및 정보보호 등에

관한 법률)·신용정보법(신용 정보의 이용 및 보호에 관한 법률)의 데이터경제 3법, 소재·부품산업 특별법 등의 과도 및 중복규제 규정을 개정하여 집단지성 네트워크 사이버폴리스 자원봉사시스템 구축에 관한 연구가 활성화 될 수 있도록 해야 한다.

5. 경찰관의 사전예방활동을 위한 사이버범죄 위해인지능력 배양

심리학과 범죄학의 발달과정이 동시대의 과학의 발달과정과 밀접한 영향을 미치며 전개되어져 온 것과 마찬가지로 형법상의 행위론도 인과적 행위론에서 목적적 행위론에 이르기까지는 동시대의 과학사의 발달과정들이 어느 정도 반영되어 그에 따른 입장의 변화에 따라 목적적 행위론은 인과적 행위론을 비판하면서 행위론을 정립하였다.

그러나 행위에 있어서의 목적지향성을 확인한 후부터 오늘날 인지과학적 관점이 대두되어지기 이전까지는 인간의 행동원리에 대한 관점에 큰 변화가 나타나지 않았으며, 형법상 행위론에서도 행위의 내적 측면이 아닌 그 사회적 의미에 핵심을 두는 사회적 행위론이 형성되었고, 오늘날까지의 지배적 견해로서 자리매김하고 있다. 이에 오늘날 인간 행동원리에 대한 관점이라고 할 수 있는 인지과학적 관점을 행위론에 적용하고자 시도하는 것이 과학사의 발달과 연관된 행위론의 발달사라는 측면에서도 의미 있는 순차적 시도인 것이다.

인간의 인지(이성)에는 항상 정서(감정)가 밑바탕에 놓여 있다는 인지신경과학의 연구결과를 기초로 형법상 행위론을 구성함에 있어, 카글(Kargl)은 기존의 인과적 행위론이 "유의적 거동의 결과" 라는 인과의 과정을 확정하고, 목적적 행위론이 유의적인 것의 의미를 "목적적 지배조종"으로 정의하면서 의사적 요소를 부각한 것에 더하여, 인지의 중요 작용요소의 하나로 확인되어진 정서 개념을 행위론 구성에서도 적용하여 인식·의사·정서의 상호연계적 "정서논리체계" 하에 형법상 행위론을 구성하는 인지적 행위론을 주장한다.

그는 행위론과 질서론의 극단적 입장을 통합하기 위해 파슨스의 "체계의 네 가지 기능적 요소(적응·목표설정·통합·잠재)에 대한 도식"과 마투라나(Maturana)의 인지생물학(Er-kenntnisbiologie)적 이론에서 등장하는 생명체의 "자기재생산 개념"을 이론적 기반으로 하여, 파슨스의 네 가지 기능요소 도식에 이 "자기재생산 개념"을 수렴하여 논리를 전개하였다.

이러한 기초 위에서 인과적 행위론과 목적적 행위론의 두 가지 관점을 동시에 취하여 인지과학적 관점에서 행위를 분석하면, 결국 행위한다는 것(Handeln)은 A와 B 가운데에서 제한적인 자유로운 선택행동이 아닌 각각의 행위자 자신의 자기재생산적 작용에 의해 형성되어져 존재하는 정서논리체계의 상태에 의해서 상황 지워진 결정행동, 즉 그 정서논리체계 경과에 따르는 결정행동이라고 정의할 수 있을 것이다.

인지과학적 관점에 의한 행위론을 통해 위해행위의 결정구조에 대해 개략적으로 살펴보았는바, 이러한 관점은 행위요소를 그 본래의 주류적 영역에서의 연구 성과를 빌어 심도 있게 파악해 보고자 하는 시도로, 나아가 형법상 범죄행위를 논의함에 있어 그 논의의 기초로서 인지심리학적·인지과학적 관점에서의 행위요소에 대한 새로운 시각을 제시하고자 한 것이다. 사이버스토킹, 랜섬웨어, 사이버테러 등 과학의 발달은 아무도 예측할 수 없다. 그러나 적어도 오늘까지 진행되어 입증되어진 과학적 사실 관계를 적용하려는 시도는 의미 있는 작업이라고 생각된다.

이에 이러한 인지과학의 발달로 발견되어진 사고시스템을 통해 형법상 행위에 대한 범죄학적 관점 이라고 할 수 있는 사이버위해행위에 대한 시각이 재조명되어져야 할 필요성과 타당성이 존재한다고 생각한다. 즉 사이버위해행위에 대한 인지과학적 관점에서의 이해는 이러한 위해행위를 차단하기 위한 과학적·예방적 사회 안전대책의 수립을 가능하게 하는 기초가 되며, 이에 이러한 인지과학적 관점에 대한 이해의 필요성이 존재하는 것이다.

따라서 사이버수사대는 이상과 같은 사이버 위해행위요소에 대한 인지과학에 대한 강의 및 연구를 통해서 사전 예방적 활동이 될 수 있도록 하여 노무현 전(前) 대통령 자살사건, 김영삼 전 대통령 계란 페인트 투척사건, 10.26 박정희 전 대통령 시해사건 등과 같이 국가 안보와 직결될 수 있는 일들이 발생되지 않도록 하였으면 한다. 아울러 지금까지는 범인을 연구하는 범죄학 중심이었지만 이제는 피해자를 보호할 수 있는 피해자학도 중요시 여기는 만큼 위해대상자와 그 사이버환경의 연구도 필수적이라고 본다(김두현. 2018a: 422-424).

특히 사이범죄의 위해적 환경을 극복하고 범죄를 사전에 예방하기 위해서는 가칭 "사이버범죄예방론"이라는 연구도 필요하다고 본다.

Ⅴ. 결론 및 제언

본 논문의 연구는 문헌적 연구와 보안업무 경험을 토대로 연구하였다. 이 논문의 연구 목적은 수사 기관의 공권력이 미치지 못하는 법·제도화 이전의 사이버상 수많은 범죄의 유형과 범죄행태에 대하여 올바른 사회적 규범·합의와 도출을 위한 "집단지성 네트워크 사이버폴리스 자원봉사 시스템" 구축의 필요성을 제안하여 각종 사이버 범죄를 예방할 수 있는 시스템 구축 및 대책방안을 제시하는데 있다.

집단지성 사이버폴리스 자원봉사자 구성은 전국 대학의 컴퓨터공학과, 디지털포렌식학과, 정보보호학과, 안전관리학과, 경호학과, 경찰행정학과, 보안관리학과, 소방행정학과, 소방공학과 등 경호보안 관련학과 교수와 대통령경호처, 국가정보원, 경찰청, 소방청 등의 퇴직공무원, 경비·보안기업 및 단체, 민간조사원, 경호·경비·소방·경찰·교통·정보·보안·국방 및 국민안전연구소 등 제반 안전관리연구 전문가로 구성한다.

이 사이버폴리스 자원봉사시스템 구축방안으로는 첫째, 집단지성 네트워크형 사이버폴리스 자원 봉사시스템 구축이 필요하다.

둘째, 경비업법상 민간조사업규정이 신설되어야 한다.

셋째, 국민생활의 안정을 위한 집단지성 사이버폴리스 자원봉사시스템의 안전지킴이 봉사활동을 강화해야 한다.

넷째, 선진국들의 사이버범죄에 대한 연구 교훈 및 법적 대응방안이 도입되어야 한다.

다섯째, 개인정보 보호법·정보통신망법·신용정보법 등 데이터경제 3법, 소재·부품산업 특별법 등의 과도 및 중복규제 규정을 개정하여야 한다.

여섯째, 경찰관은 사전예방활동을 위한 사이버범죄 위해인지능력을 배양해야 한다.

결론적으로 사이버범죄는 사후조치보다는 사전에 예방하는 것이 매우 중요하고 국가안보와도 직결된다는 점에서 경찰력뿐만이 아니라 민·관·군의 모든 협력체계와 전 국민의 협조를 통하여 최선을 다해야 한다는 점이다.

참고문헌

1. 국내문헌

경찰청 (2019). **2018 경찰백서**. 서울: 경찰청.

김두현 (2001). 공인민간조사제도의 입법화 방안. **한국체육대학교 논문집, 24**, 433-472.

김두현 (2012). **현대자원봉사의 이론과 실제**. 서울: 대한미디어출판사.

김두현 (2017). **경비업법**. 서울: 시큐에듀.

김두현 (2018). **경호학개론**. 서울: 엑스퍼트출판사.

김두현, 김정현 (2009). **현대테러리즘의 이해**. 서울: 도서출판 두남.

김두현, 박형규 (2018). **신민간경비론**. 서울: 솔과학출판사.

김두현, 최선태 (2002). **안전관리론**. 서울: 백산출판사.

김하연, 이정일 (2017). **안전관리론**. 서울: 화수목출판사.

박정우, 이루리, 김지선, 이현정 역 (2016). **사이버 범죄 해결사 디지털 포렌식 [컴퓨터 과학과 고고학의 만남]**. (Michael W. Graves. *Digital Archaeology: The Art and Science of Digital Forensics*), 서울: 에이콘출판사.

손동운, 조성구, 김동제 (2014). 민간경비업과 민간조사업의 차이점 연구. **한국경호경비학회지, 39**, 295-317.

이만종 (2007). **경찰수사총론**. 서울: 청목출판사.

이상현 (2010). **미국 사이버범죄의 현실, 법, 실무**(Cyber Crime in the U.S.: Realities, Law & Practices). 한국형사정책연구원.

2. 기타

국가법령정보센터(http://www.law.go.kr/) : 공익신고보호법

박성준 (2018). **수도서울을 안전하게 책임지는 119안전지킴이 지식나눔 봉사활동 계획 보고서**. 대한민국 재향소방동우회.

【Abstract】

A Study on the Development of Cyberpolice Volunteer System Using the Collective Intellectual Network

Kim, Doo-Hyun · Park, Sung-Joon · Na, Gi-Sung

In the reality that the boundary between the real world and the virtual world disappears with the 4th Industrial Revolution, cyber crimes that occur beyond time and space have clear limitations in fulfilling their duties only with the police force of government organizations established under the real law system.

The research method of this thesis is based on the literature research and the experience of security work. The purpose of this paper is to establish a social system where collective intelligence of each social field can participate voluntarily to respond to cyber crimes occurring beyond the time and space before the law and institutionalization. In addition, the social system in which collective intelligence in each social sector can participate voluntarily was established to define crime types in cyberspace in real time and to prevent crimes defined by the people themselves and the counter-measures had been proposed in order to form social consensus.

First, it is necessary to establish a collective intelligent network-type cyberpolice volunteer system. The organization consists of professors of security and security related departments at universities nationwide, retired public officials from the National Intelligence Service, the National Police Agency, and the National Emergency Management Agency, security companies and the organizations, civilian investigators, security & guard, firefighting, police, transportation, intelligence, security, national security, and research experts.

Second, private sector regulation should be established newly under the Security Business Act.

Third, the safety guard of the collective intelligent cyberpolice volunteer system for the stability of the people's lives should strengthen volunteer work.

Fourth, research lessons and legal countermeasures against cybercrime in advanced countries should be introduced.

Fifth, the Act on the Protection of Personal Information, the Act on Promotion of Information and Communication Network Utilization and Information Protection, the Act on the Utilization and Protection of Credit Information, and the Special Act on the Materials and Parts Industry should be amended.

Sixth, police officers should develop cybercrime awareness skills for proactive prevention activities.

Keywords: Cybercrime, Collective intelligence, Network, Cyberpolice, Volunteer system, Knowledge sharing voluntary service activities